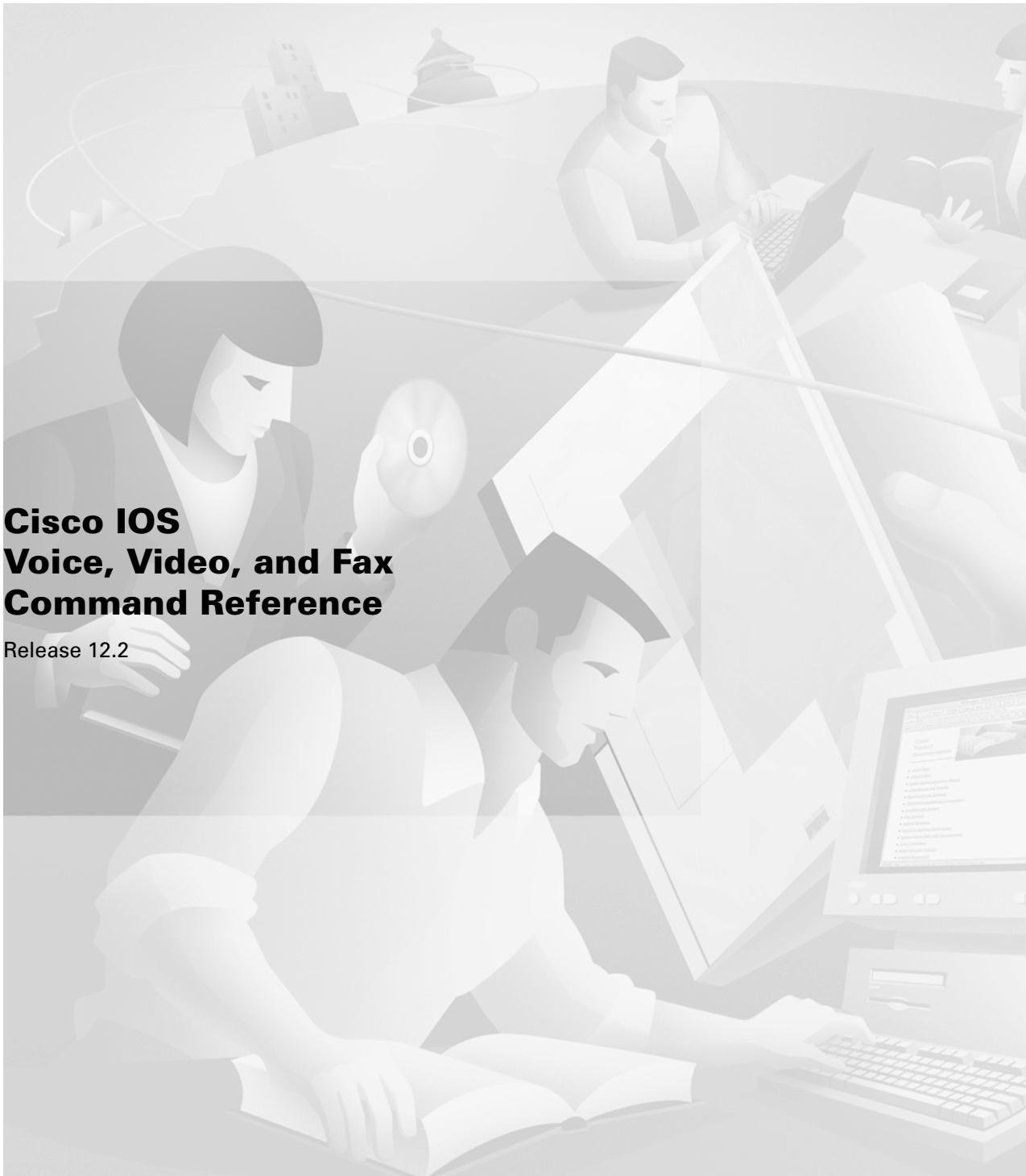




Cisco IOS Voice, Video, and Fax Command Reference

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-7812101=
Text Part Number: 78-12101-02

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

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

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

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

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

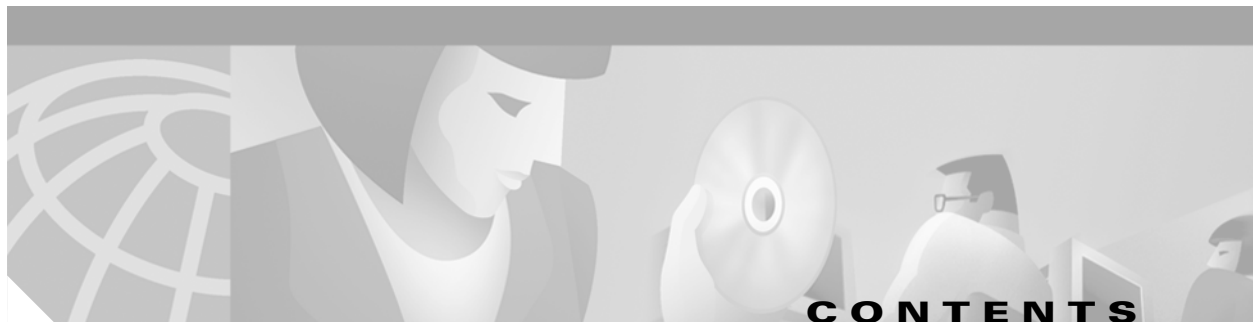
AccessPath, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco *NetWorks* logo, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, 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, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, 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 brands, names, or 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. (0102R)

Cisco IOS Voice, Video, and Fax Command Reference

Copyright © 2001–2006 Cisco Systems, Inc.

All rights reserved.



About Cisco IOS Software Documentation v

Using Cisco IOS Software xiii

**Cisco IOS Voice, Video, and Fax Commands:
A Through C** VR-1

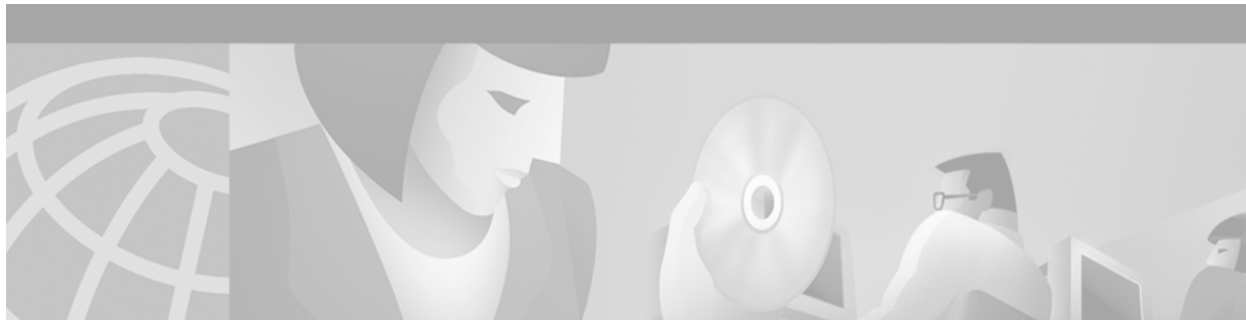
**Cisco IOS Voice, Video, and Fax Commands:
D Through F** VR-233

**Cisco IOS Voice, Video, and Fax Commands:
G Through P** VR-339

**Cisco IOS Voice, Video, and Fax Commands:
R Through Sh** VR-561

**Cisco IOS Voice, Video, and Fax Commands:
Si Through Z** VR-871

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.

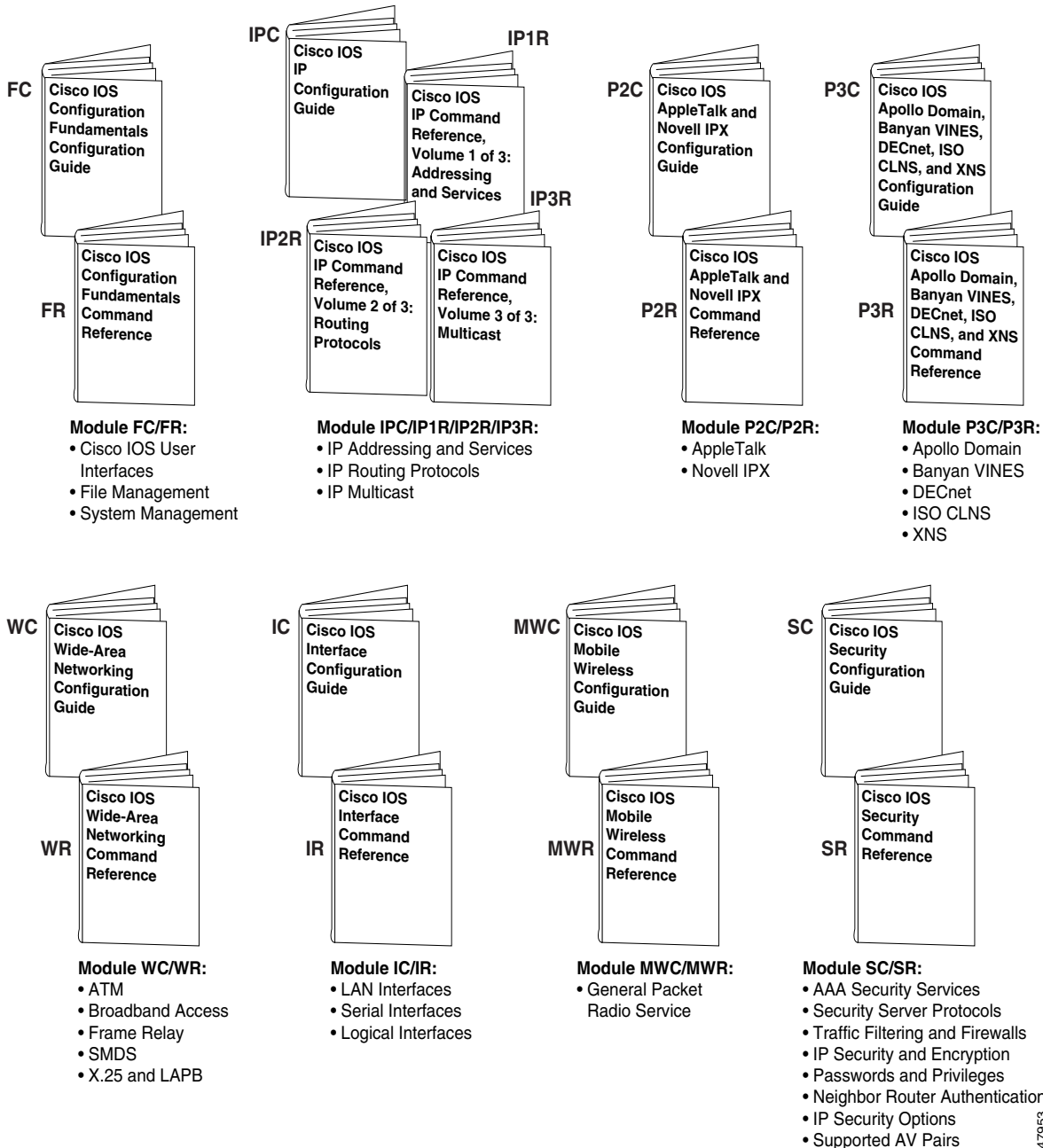
Figure 1 shows the Cisco IOS software documentation modules.



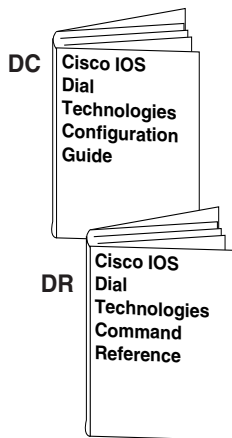
Note

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.

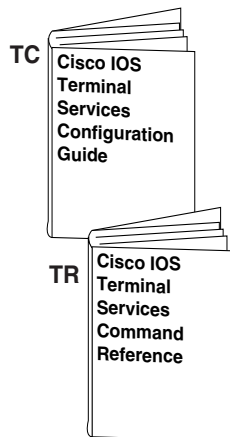
Figure 1 Cisco IOS Software Documentation Modules



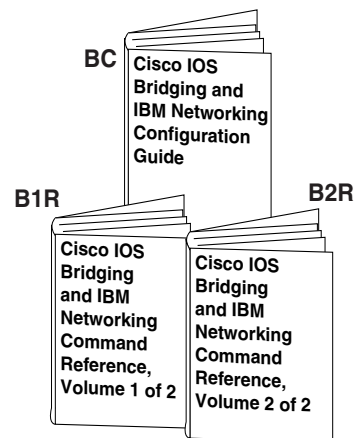
47953

**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:**

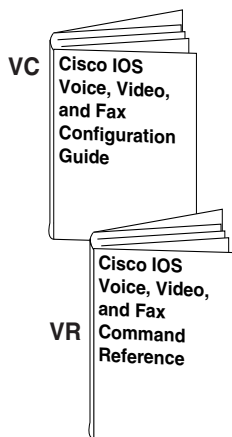
- ARA
- LAT
- NAS1
- Telnet
- TN3270
- XRemote
- X.28 PAD
- Protocol Translation

**Module BC/B1R:**

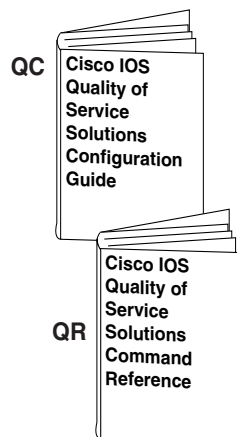
- Transparent Bridging
- SRB
- Token Ring Inter-Switch Link
- Token Ring Route Switch Module
- RSRB
- DLSw+
- Serial Tunnel and Block Serial Tunnel
- LLC2 and SDLC
- IBM Network Media Translation
- SNA Frame Relay Access
- NCIA Client/Server
- Airline Product Set

Module BC/B2R:

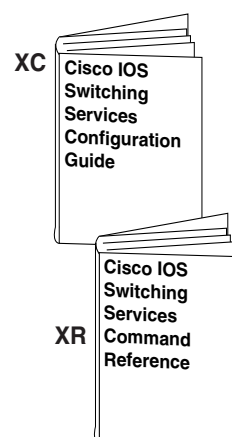
- DSPU and SNA Service Point
- SNA Switching Services
- Cisco Transaction Connection
- Cisco Mainframe Channel Connection
- CLAW and TCP/IP Offload
- CSNA, CMPC, and CMPC+
- TN3270 Server

**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>.

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
boldface	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
<code>screen</code>	Examples of information displayed on the screen are set in Courier font.
<code>boldface screen</code>	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.

Convention	Description
!	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

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
- 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.

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>

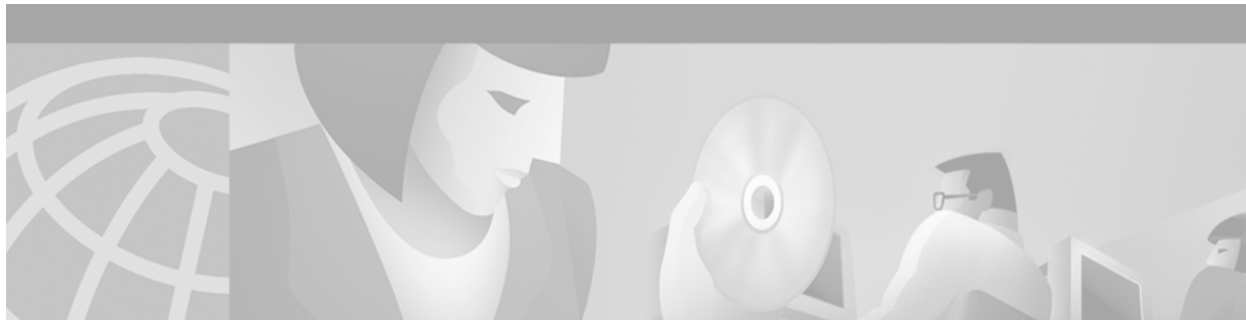
Contacting TAC by Telephone

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 logout command.
Privileged EXEC	From user EXEC mode, use the enable EXEC command.	Router#	To return to user EXEC mode, use the disable command.
Global configuration	From privileged EXEC mode, use the configure terminal privileged EXEC command.	Router(config)#	To return to privileged EXEC mode from global configuration mode, use the exit or end command, or press Ctrl-Z .
Interface configuration	From global configuration mode, specify an interface using an interface command.	Router(config-if)#	To return to global configuration mode, use the exit command. To return to privileged EXEC mode, use the end command, or press Ctrl-Z .
ROM monitor	From privileged EXEC mode, use the reload EXEC command. Press the Break key during the first 60 seconds while the system is booting.	>	To exit ROM monitor mode, use the continue command.

For more information on command modes, 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
help	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.
?	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
Router> enable Password: <password> Router#	Enter the enable command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to Router#.
Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	Enter the configure terminal privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to Router(config)#.
Router(config)# interface serial ? <0-6> Serial interface number Router(config)# interface serial 4 ? / Router(config)# interface serial 4/ ? <0-3> Serial interface number Router(config)# interface serial 4/0 Router(config-if)#	Enter interface configuration mode by specifying the serial interface that you want to configure using the interface serial global configuration command. Enter ? to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash. You are in interface configuration mode when the prompt changes to Router(config-if)#.

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

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

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

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

Using the no and default Forms of Commands

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

Configuration commands 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. 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:

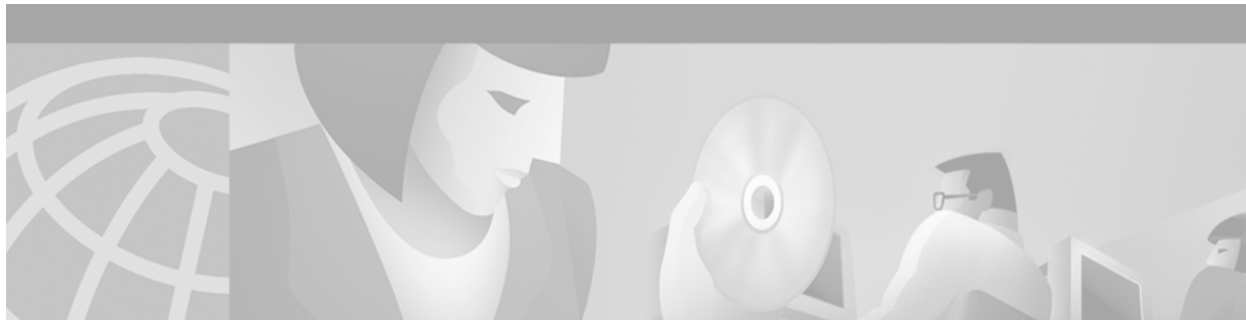
<http://www.cisco.com/go/fn>

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.



Cisco IOS Voice, Video, and Fax Commands: A Through C

This chapter presents the commands to configure and maintain Cisco IOS voice, video, and fax applications. The commands are presented in alphabetical order. Some commands required for configuring voice, video, and fax may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice, Video, and Fax Configuration Guide*.

aaa nas port voip

To send out the standard NAS-Port attribute (RADIUS IETF Attribute 5) on voice interfaces, use the **aaa nas port voip** command in global configuration mode. To disable the command, use the **no** form of the command.

aaa nas port voip

no aaa nas port voip

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)T	This command was introduced on the Cisco AS5300.

Usage Guidelines

This command brings back the original behavior of the AAA NAS-Port on Voice over IP (VoIP) interfaces. By default this feature should not be enabled.



Note

Some customers using the Cisco AS5300 voice gateway have had the Debit Card application stop working after upgrading from 12.1(5)T to 12.1(5.3)T.

Examples

The following example shows how to return to the original behavior of the AAA NAS-Port:

```
aaa nas port voip
```

Related Commands

Command	Description
aaa nas port extended	Replaces the NAS-port attribute with RADIUS IETF attribute 26 and displays extended field information.

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

Syntax Description

best-effort	Indicates that Resource Reservation Protocol (RSVP) makes no bandwidth reservation. This is the default.
controlled-load	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.
guaranteed-delay	Indicates that RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded.

Defaults

best-effort

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.
12.1(5)T	The description of the command was modified.

Usage Guidelines

This command is applicable only to VoIP dial peers.

When VoIP dial peers are used, the Cisco IOS software uses RSVP to reserve a certain amount of bandwidth so that the selected QoS can be provided by the network. Call setup is aborted if the RSVP resource reservation does not satisfy the acceptable QoS for both peers.

To select the most appropriate value for this command, you need to be familiar with the amount of traffic this connection supports and what kind of impact you are willing to have on it. The Cisco IOS software generates a trap message when the bandwidth required to provide the selected quality of service is not available.

Examples

The following example selects **guaranteed-delay** as the acceptable QoS for inbound and outbound calls on VoIP dial peer 10:

```
dial-peer voice 10 voip
  acc-qos guaranteed-delay
```

Related Commands	Command	Description
	req-qos	Requests a particular QoS using RSVP to be used in reaching a specified dial peer in VoIP.

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

Syntax Description	blue	Specifies the alarm type to be sent is “blue,” also known 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.

Defaults	No alarm is sent.

Command Modes	Controller configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600, 3600, and MC3810 multiservice concentrator.

Usage Guidelines	Any monitored time slot can be used for either permanent trunk connections or switched connections. Permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) can be combined on a T1 or E1 controller and monitored for alarm conditioning.

An alarm is sent only if all of the time slots configured for alarm conditioning on a T1 or E1 controller are out of service. If one monitored time slot remains in service or returns to service, no alarm is sent.

Examples	The following example configures T1 0 to send a blue (AIS) alarm if DS0 groups 0 and 1 are out of service:

```
controller t1 0
alarm-trigger blue 0,1
exit
```

Related Commands	Command	Description
	busyout monitor	Configures a voice port to monitor an interface for events that would trigger a voice-port busyout.
	connection trunk	Creates a permanent trunk connection (private line or tie-line) between a voice port and a PBX.
	voice class permanent	Creates a voice class for a Cisco or FRF-11 permanent trunk.

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*]

Syntax Description	
<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).
gkid <i>gatekeeper-name</i>	Name of the local gatekeeper of whose zone this node is a member.
ras <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).
terminal	(Optional) Indicates that the alias refers to a terminal.
mcu	(Optional) Indicates that the alias refers to a multiple control unit (MCU).
gateway	(Optional) Indicates that the alias refers to a gateway.
h320	(Optional) Indicates that the alias refers to an H.320 node.
h323-proxy	(Optional) Indicates that the alias refers to an H.323 proxy.
voip	(Optional) Indicates that the alias refers to VoIP.
e164 <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 alias static commands with the same call signaling address and different aliases.
h323id <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 alias static commands with the same call signaling address and different aliases.

Defaults

No static aliases exist.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 and 3600 series.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

The local alias table can be used to load static entries by performing as many of the commands as necessary. Aliases for the same IP address can be added in different commands, if required.

Typically, static aliases are needed to access endpoints that do not belong to a zone (that is, they are not registered with any gatekeeper) or whose gatekeeper is inaccessible for some reason.

Examples

The following example creates a static terminal alias in the local zone:

```
zone local gk.zone1.com zone1.com
alias static 191.7.8.5 gkid gk.zone1.com terminal e164 14085551212 h323id bobs_terminal
```

alt-dial

To configure an alternate dial-out string for dial peers on the Cisco MC3810 multiservice concentrator, 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.

Defaults

No alternate dial-out string is configured.

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

This command applies to Cisco MC3810 multiservice concentrator plain old telephone service (POTS), Voice over Frame Relay (VoFR), and Voice over ATM (VoATM) dial peers.

The **alt-dial** command is used for the on-net-to-off-net alternative dialing function. The string replaces the destination-pattern string for dialing out.

Examples

The following example configures an alternate dial-out string of 9,5559871:

```
alt-dial 9,5559871
```

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	
+	(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: • Digits 0 through 9, letters A through D, pound sign (#), and asterisk (*), which represent specific digits that can be entered. • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit.
T	(Optional) Control character indicating that the answer-address value is a variable-length dial string.

Defaults The default value is enabled with a null string.

Command Modes Dial peer configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on Cisco 3600 series routers.

Usage Guidelines Use the **answer-address** command to identify the origin (or dial peer) of incoming calls from the IP network. Cisco IOS software identifies the dial peers of a call in one of two ways: either by identifying the interface through which the call is received or through the telephone number configured with the **answer-address** command. In the absence of a configured telephone number, the peer associated with the interface will be associated with the incoming call.

For calls coming in from a POTS interface, the **answer-address** command is not used to select an incoming dial peer. The incoming POTS dial peer is selected on the basis of the port configured for that dial peer.

There are certain areas in the world (for example, in certain European countries) where valid telephone numbers can vary in length. Use the optional control character **T** to indicate that a particular **answer-address** value is a variable-length dial string. In this case, the system will not match the dialed numbers until the interdigit timeout value has expired.

**Note**

The Cisco IOS software does not check the validity of the E.164 telephone number; it accepts any series of digits as a valid number.

Examples

The following example configures the E.164 telephone number 555-9626 as the dial peer of an incoming call:

```
dial-peer voice 10 pots
answer-address +5559626
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer.
port (dial peer)	Enables an interface on a PA-4R-DTR port adapter to operate as a concentrator port.
prefix	Specifies the prefix of the dialed digits for this dial peer.

application

To enable a specific interactive voice response (IVR) 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**]

Syntax Description

<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. For Media Gateway Control Protocol (MGCP) or Simple Gateway Control Protocol (SGCP) networks, see the usage guidelines below for valid application names.
out-bound	The named application will handle the MMoIP dial peer in the outgoing mode.

Defaults

No default behavior or values.

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the Cisco 2500 series, 3600 series, and AS5300.
12.0(5)T	The SGCPAPP application was supported initially on the Cisco AS5300 universal access server in a private release that was not generally available.
12.0(7)XK	Support for the SGCPAPP application was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	The MGCPAPP application was supported initially on the Cisco AS5300 universal access server.
12.1(3)XI	The out-bound keyword was added for the store-and-forward fax feature on the Cisco AS5300 universal access server.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

Use this command to associate a predefined session application with an incoming POTS dial peer or an outgoing MMoIP dial peer. Calls using this incoming POTS dial peer or this outgoing MMoIP dial peer will be handed to the predefined specified session application.

SGCP Networks

For SGCP networks, enter **SGCPAPP** in uppercase characters. This application can be applied only to POTS dial peers. Note that SGCP dial peers do not use dial peer hunting.



Note In Cisco IOS Release 12.2, you cannot mix SGCP and non-SGCP endpoints in the same T1 controller. You also cannot mix SGCP and non-SGCP endpoints in the same DS0 group.

MGCP Networks

For MGCP networks, enter **MGCPAPP** in upper-case characters. This application can be applied only to POTS dial peers. Note that MGCP dial peers do not use dial peer hunting.

Examples

The following example shows how to define an application and how to apply it to an outbound MMoIP dial peer for the fax onramp operation:

```
call application voice fax_on_vfc_onramp http://santa/username/clid_4digits_npw_3.tcl
dial-peer voice 3 mmoup
  application fax_on_vfc_onramp out-bound
  destination-pattern 57108..
  session target mailto:$d$@mail-server.cisco.com
```

The following example shows how to apply the MGCP application to a dial peer:

```
dial-peer voice 1 pots
  application MGCPAPP
```

Related Commands

Command	Description
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
mgcp	Starts the MGCP daemon.
sgcp	Starts and allocates resources for the SCGP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.

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.

Defaults

The gatekeeper accepts and processes all incoming ARQs.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(6)Q, 11.3(7)NA	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

Use the **arq reject-unknown-prefix** command to configure the gatekeeper to reject any incoming ARQs for a destination E.164 address that does not match any of the configured zone prefixes.

When an endpoint or gateway initiates an H.323 call, it sends an ARQ to its gatekeeper. The gatekeeper uses the configured list of zone prefixes to determine where to direct the call. If the called address does not match any of the known zone prefixes, the gatekeeper attempts to *hairpin* the call out through a local gateway. If you do not want your gateway to do this, then use the **arq reject-unknown-prefix** command. (The term *hairpin* is used in telephony. It means to send a call back in the direction from which it came. For example, if a call cannot be routed over IP to a gateway that is closer to the target phone, the call is typically sent back out through the local zone, back the way it came.)

This command is typically used to either restrict local gateway calls to a known set of prefixes or deliberately fail such calls so that an alternate choice on a gateway's rotary dial peer is selected.

Examples

Consider a gatekeeper configured as follows:

```
zone local gk408 cisco.com
zone remote gk415 cisco.com 172.21.139.91
zone prefix gk408 1408.....
zone prefix gk415 1415.....
```

In this example configuration, the gatekeeper manages a zone containing gateways to the 408 area code, and it knows about a peer gatekeeper that has gateways to the 415 area code. Using the **zone prefix** command, the gatekeeper is then configured with the appropriate prefixes so that calls to those area codes hop off in the optimal zone.

If the **arq request-unknown-prefix** command is not configured, the gatekeeper handles calls in the following way:

- A call to the 408 area code is routed out through a local gateway.
- A call to the 415 area code is routed to the gk415 zone, where it hops off on a local gateway.
- A call to the 212 area code is routed to a local gateway in the gk408 zone.

If the **arq reject-unknown-prefix** command is configured, the gatekeeper handles calls in the following way:

- A call to the 408 area code is routed out through a local gateway.
- A call to the 415 area code is routed to the gk415 zone, where it hops off on a local gateway.
- A call to the 212 area code is rejected because the destination address does not match any configured prefix.

as

To define an application server for backhaul, use the **as** command in IUA configuration mode. To disable, use the **no** form of this command.



Note

All of the ASPs in an application server must be removed before an application server can be unconfigured.

```
as as-name {localip1 [localip2]} [local-sctp-port] | [fail-over-timer] [sctp-startup-rtx]
[sctp-streams] [sctp-t1init]
```

```
no as as-name
```

Syntax Description

<i>as-name</i>	Defines the protocol name (only ISDN is supported).
localip1	Defines the local IP address(es) for all the ASPs in a particular AS.
localip2	Defines the local IP address(es) for all the ASPs in a particular AS.
local-sctp-port	Defines a specific local SCTP port rather than an IUA well-known port.
fail-over-timer	(Optional) Configures the failover timer for a particular AS.
sctp-startup-rtx	(Optional) Configures the SCTP maximum startup retransmission timer.
sctp-streams	(Optional) Configures the number of SCTP streams for a particular AS.
sctp-t1init	(Optional) Configures the SCTP t1 init timer.

Defaults

No default behavior or values.

Command Modes

IUA configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300 platform.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T on Cisco 2420, Cisco 2600, Cisco 3600, Cisco 3700, Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

Usage Guidelines

A maximum of two local IP addresses can be specified (note that SCTP has built-in support for multi-homed machines).

The default value of the SCTP streams is determined by the hardware that you have installed. The value of failover timer is found in the **show iua as all** command output.

The number of streams to assign to a given association is implementation dependent. During the initialization of the IUA association, you need to specify the total number of streams that can be used. Each D channel is associated with a specific stream within the association. With multiple trunk group support, every interface can potentially be a separate D channel.

At start-up the IUA code checks for all the possible T1, E1, or T3 interfaces and sets the total number of inbound and outbound streams supported accordingly. In most cases, there is only a need for one association between the GW and the MGC. For the rare case that you are configuring multiple AS associations to various MGCs, the overhead from the unused streams would have minimal impact. The NFAS D channels are configured for one or more interfaces, where each interface is assigned a unique stream ID.

The total number of streams for the association needs to include an additional stream for the SCTP management messages. So during start-up the IUA code adds one to the total number of interfaces (streams) found.

You have the option to manually configure the number of streams per association. In the backhaul scenario, if the number of D channel links is limited to one, allowing the number of streams to be configurable avoids the unnecessary allocation of streams in an association that will never be used. For multiple associations between a GW and multiple MGCs, the configuration utility is useful in providing only the necessary number of streams per association. The overhead from the streams allocated but not used in the association is negligible.

If the number of streams is manually configured through the CLI, the IUA code cannot distinguish between a start-up event, which automatically sets the streams to the number of interfaces, or if the value is set manually during runtime. If you are configuring the number of SCTP streams manually, you must add one plus the number of interfaces using the **sctp-streams** keyword. Otherwise, IUA needs to always add one for the management stream, and the total number of streams increments by one after every reload.

When you set the SCTP stream with CLI, you cannot change the inbound and outbound stream support once the association is established with SCTP. The value takes effect when you first remove the IUA AS configuration and then configure it back as the same AS or a new one. The other option is to reload the router.

Examples

An application server (AS) and the application server process (ASP) should be configured first to allow a National ISDN-2 with Cisco extensions (NI2+) to be bound to this transport layer protocol. The AS is a logical representation of SCTP local end point. The local end point can have more than one IP address but must use the same port number.

The following is an example of an AS configuration on a gateway:

```
Router(config-iua)# as as5400-3 10.1.2.34, 10.1.2.35 2577
```

In the configuration above, an AS named *as5400-3* is configured to use two local IP addresses and a port number of 2577.

The following output shows options available when you use this command:

```
Router(config-iua)# as as5400-3 fail-over ?
```

```
<1000-10000> set Fail-Over time (in milliseconds) between 1 and 10 seconds
```

```
Router(config-iua)# as as5400-3 sctp-stre ?
```

```
<2-57> Specify number of SCTP streams for association
```

```
Router(config-iua)# as as5400-3 sctp-startup ?
```

<2-20> Set Sctp Maximum Startup Retransmission Interval

Router(config-iaua)# **as as5400-3 sctp-t1init ?**

<1000-60000> Set Sctp T1 init timer (in milliseconds)

Related Commands

Command	Description
asp	Defines an ASP for backhaul.

asp

To define an ASP for backhaul, use the **asp** command in IUA configuration mode. To disable, use the **no** form of this command.



Note

All of the ASPs in an application server must be removed before an application server can be unconfigured.

```
asp asp-name as as-name {remoteip1 [remoteip2]} [remote-sctp-port] | [ip-precedence
sctp-keepalives] [sctp-max-associations] [sctp-path-retransmissions] [sctp-t3-timeout]
```

```
no asp asp-name
```

Syntax Description

<i>asp-name</i>	Names the current ASP.
as	The application server to which the ASP belongs.
<i>as-name</i>	Name of the application server to which the ASP belongs.
remoteip1	Designates the remote IP address for this SCTP association.
remoteip2	Designates the remote IP address for this SCTP association.
remote-sctp-port	Connects to a remote SCTP port rather than the IUA well-known port.
ip-precedence	(Optional) Sets IP Precedence bits for protocol data units (PDUs). IP precedence is expressed in the type of service (ToS) field of the show ip sctp association parameters output. Default ToS is 0.
sctp-keepalives	(Optional) Modifies the keepalive behavior of an IP address in a particular ASP. The default is 500 ms (see the show ip sctp association parameters output under heartbeats).
sctp-max-associations	(Optional) Sets the SCTP max association retransmissions for a particular ASP. The default value is 3.
sctp-path-retransmissions	(Optional) Sets the SCTP path retransmissions for a particular ASP. The default value is 5.
sctp-t3-timeout	(Optional) Sets the SCTP T3 retransmission timeout for a particular ASP. The default value is 900 ms.

Defaults

No default behavior or values.

Command Modes

IUA configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release Cisco IOS Release 12.2(11)T on Cisco 2420, Cisco 2600, Cisco 3600, Cisco 3700, Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

Usage Guidelines

This command establishes SCTP associations. There can be only a maximum of three ASPs configured per AS. IP precedence is expressed in the ToS field of **show ip sctp association parameters** output. Default ToS is 0.

You can configure the precedence value in IUA in the range of 0 through 7 for a given IP address. Within IUA, the upper three bits representing the IP precedence in the ToS byte (used in the IP header) is set based on the user input before passing down the value to SCTP. In turn, SCTP passes the ToS byte value to IP. The default value is 0 for “normal” IP precedence handling.

The *asp-name* argument specifies the name of this ASP. The **ip-precedence** keyword sets the precedence and ToS field. The *remote-ip_address* argument specifies the IP address of the remote end-point (the address of MGC, for example). The *number* argument can be any IP precedence bits in the range 1 through 255.

The **no** form of the command results in precedence bits not being explicitly set by SCTP. The default is to set all bits in the ToS field to zero by SCTP.

In the case of a hot-standby PGW pair, from the GW perspective there is usually be one ASP active and another in the INACTIVE state. The ASP_UP message is used to bring the ASP state on the GW to the INACTIVE state, followed by the ASPTM message, ASP_ACTIVE to ready the IUA link for data exchange (eventually the QPTM Establish Request message actually initiates the start of the D channel for the given interface). In the event that the GW detects a failure on the active ASP, it can send a NTFY message to the standby ASP to request that it become active.

Examples

An ASP can be viewed as a local representation of an SCTP association since it specifies a remote end point that will be in communication with an AS local end point. An ASP is defined for a given AS. For example, the following configuration defines a remote signaling controller *asp-name* at two IP addresses for AS *as-name*. The remote SCTP port number is 2577:

```
AS as-name 10.4.8.69, 10.4.9.69 2477
```

```
ASP asp-name AS as-name 10.4.8.68 10.4.9.68 2577
```

Multiple ASPs can be defined for a single AS for the purpose of redundancy, but only one ASP can be active. The ASPs are inactive and only become active after fail-over.

In the Cisco MGC solution, a signaling controller is always the client that initiates the association with a gateway. During the initiation phase, you can request outbound and inbound stream numbers, but the gateway only allows a number that is at least one digit higher than the number of interfaces (T1/E1) allowed for the platform.

The following shows options for this command:

```
Router(config-iua)# asp asp-name ip-precedence 10.1.2.345 ?
```

```
<0-7>    specify precedence level (0 - 7)
```

```
default  use default value of IP precedence for this address
```

```
Router(config-iua)# asp asp-name sctp-keep ?
```

```
A.B.C.D  specify the IP address to enable/disable keep alive
```

```
Router(config-iua)# asp asp-name sctp-keep 10.1.2.234 ?
```

```
<1000-60000> specify keep alive interval (in milliseconds)
```

```
Router(config-iua)# asp asp-name sctp-max-ass ?
```

```
<2-20>    specify maximum associations
```

```
default  use default value of max associations for this address
```



```
Router(config-ia)# asp asp-name sctp-path-retran ?
```

```
<2-10>    specify maximum path retransmissions  
default   use default value of max path retrans for this address
```

```
Router(config-ia)# asp asp-name sctp-t3-time ?
```

```
<300-60000> specify T3 retransmission timeout (in milliseconds)  
default      use default value of T3 for this address
```

Related Commands

Command	Description
as	Defines an application server (AS) for backhaul.

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.

Defaults	By default, payload scrambling is set off.

Command Modes	Interface configuration

Command History	Release	Modification
	12.0(5)XK	This command was introduced for ATM interface configuration on the Cisco MC3810 multiservice concentrator.
	12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines	Enable scrambling on E1 links only. On T1 links, the default B8ZS line encoding normally ensures sufficient reliability. Scrambling improves data reliability on E1 links by randomizing the ATM cell payload frames to avoid continuous nonvariable bit patterns and to improve the efficiency of the ATM cell delineation algorithms. The scrambling setting must match that of the far end.

Examples	On a Cisco MC3810, the following example shows how to set the ATM0 E1 link to scramble payload: <pre>interface atm0 atm scramble-enable</pre>

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.

Defaults	default

Command Modes	ATM Interface configuration

Command History	Release	Modification
	12.0(5)XK	This command was introduced for ATM interface configuration on the Cisco MC3810 multiservice concentrator.
	12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines	You cannot specify the ATM interface NSAP address in its entirety. The system creates either all of the address or part of it, depending on how you use this command.

Examples	On a Cisco MC3810 multiservice concentrator, the following example shows the ATM interface NSAP address set automatically:

```
interface atm0
 atm video aesa default
```

On a Cisco MC3810 multiservice concentrator, the following example shows the ATM interface NSAP address set to a specific ESI value:

```
interface atm0/1
 atm video aesa 444444444444
```

Related Commands	Command	Description
	show atm video-voice address	Displays the NSAP address for the ATM interface.

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.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(6)NA2	This command was introduced.

Usage Guidelines

The first time the interactive voice response (IVR) application plays a prompt, it reads it from the URL (or the specified location for the .au file, such as Flash or TFTP) into RAM. Then it plays the script from RAM. An example of the sequence of events is as follows:

- When the first caller is asked to enter the account and personal identification numbers (PINs), the enter_account.au and enter_pin.au files are loaded into RAM from Flash memory.
- When the next call comes in, these prompts are played from the RAM copy.
- If all callers enter valid account numbers and PINs, then the auth_failed.au file is not loaded from Flash memory into RAM memory.

The router will load the audio file only when the script initially plays that prompt after the router restarts. If the audio file is changed, you must run this EXEC command to reread the file. This will generate an error message if the file is not accessible or if there is a format error.



Note

With Cisco IOS Release 11.3(6)NA2, the URL pointer refers to the directory where Flash memory is stored.

Examples

The following example shows how to load the enter_pin.au audio file from Flash memory into RAM:

```
audio-prompt load flash:enter_pin.au
```

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.

Defaults

Auto-cut-through is enabled.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series routers.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The **auto-cut-through** command applies to ear and mouth (E&M) voice ports only.

Examples

The following example shows enabling of call completion on a Cisco MC3810 multiservice concentrator when a PBX does not provide an M-lead response:

```
voice-port 1/1
 auto-cut-through
```

The following example shows enabling of call completion on a Cisco 2600 or 3600 router when a PBX does not provide an M-lead response:

```
voice-port 1/0/0
 auto-cut-through
```

Related Commands

Command	Description
show voice port	Displays voice port configuration information.

backhaul-session-manager

To enter backhaul session manager configuration mode, use the **backhaul-session-manager** command in global configuration mode.

backhaul-session-manager

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced.

Usage Guidelines Use the **backhaul-session-manager** command to enter the backhaul session manager configuration mode. [Table 3](#) lists the backhaul session manager configuration mode commands:

Table 3 Backhaul Session Manager Configuration Mode Commands

Command	Description
group	Creates a session-group and associates it with a specified session-set.
group auto-reset	Configures the maximum auto-reset value.
group cumulative-ack	Configures maximum cumulative acknowledgments.
group out-of-sequence	Configures maximum out-of-sequence segments that are received before an EACK is sent.
group receive	Configures maximum receive segments.
group retransmit	Configures maximum retransmits.
group timer cumulative-ack	Configures cumulative acknowledgment timeout.
group timer keepalive	Configures keepalive (or null segment) timeout.
group timer retransmit	Configures retransmission timeout.
group timer transfer	Configures state transfer timeout.
session group	Associates a transport session with a specified session-group.
set	Creates a fault-tolerant or non-fault-tolerant session-set with the client or server option.

Examples

The following example shows how to enter backhaul-session-manager configuration mode:

```
Router(config)# backhaul-session-manager
Router(config-bsm)#
```

Related Commands

Command	Description
clear backhaul-session-manager group	Resets the statistics or traffic counters for a specified session-group.
clear rudpv1 statistics	Clears the RUDP statistics and failure counters.
group	Creates a session-group and associates it with a specified session-set.
group auto-reset	Configures the maximum auto-reset value.
group cumulative-ack	Configures maximum cumulative acknowledgments.
group out-of-sequence	Configures maximum out-of-sequence segments that are received before an EACK is sent.
group receive	Configures maximum receive segments.
group retransmit	Configures maximum retransmits.
group timer cumulative-ack	Configures cumulative acknowledgment timeout.
group timer keepalive	Configures keepalive (or null segment) timeout.
group timer retransmit	Configures retransmission timeout.
group timer transfer	Configures state transfer timeout.
isdn bind-l3	Configures the ISDN serial interface for backhaul.
session group	Associates a transport session with a specified session-group.
set	Creates a fault-tolerant or non-fault-tolerant session-set with the client or server option.
show backhaul-session-manager group	Displays status, statistics, or configuration of a specified or all session-groups.
show backhaul-session-manager session	Displays status, statistics, or configuration of sessions.
show backhaul-session-manager set	Displays session-groups associated with a specific or all session-sets.
show rudpv1	Displays RUDP statistics.

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

interzone	Specifies the maximum bandwidth for H.323 traffic between one zone and another zone.
total	Specifies the maximum bandwidth for H.323 traffic within a zone and between zones (intrazone and interzone).
session	Specifies the maximum bandwidth allowed for a single session in a specific zone or in all zones.
default	Specifies the maximum bandwidth for all applicable zones, depending on the keyword with which it is used.
zone	Specifies a particular zone.
<i>zone-name</i>	Names the particular zone.
<i>bandwidth-size</i>	Maximum bandwidth. For interzone and total , the range is from 1 to 10,000,000 kbps. For session , the range is from 1 to 5000 kbps.

Defaults

None

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 series and 3600 series routers and on the AS5300 universal access server.
12.1(5)T	The bandwidth command replaced the zone bw command.

Usage Guidelines

The functionality of this command in previous Cisco IOS software releases was enabled by using the **zone bw** command.

To specify maximum bandwidth for traffic between one zone and any other zone, use the **default** keyword with the **interzone** keyword.

To specify maximum bandwidth for traffic within one zone or for traffic between that zone and another zone (interzone and intrazone), use the **default** keyword with the **total** keyword.

To specify maximum bandwidth for a single session within a specific zone, use the **zone** keyword with the **session** keyword.

To specify maximum bandwidth for a single session within any zone, use the **default** keyword with the **session** keyword.

Examples

The following example configures the default maximum bandwidth for traffic between one zone and another zone to 5000 kbps:

```
gatekeeper
 bandwidth interzone default 5000
```

The following example configures the default maximum bandwidth for all zones to 5000 kbps:

```
gatekeeper
 bandwidth total default 5000
```

The following example configures the default maximum bandwidth for a single session within any zone to 2000 kbps:

```
gatekeeper
 bandwidth session default 2000
```

The following example configures the default maximum bandwidth for a single session with a specific zone to 1000 kbps:

```
gatekeeper
 bandwidth session zone denver 1000
```

Related Commands

Command	Description
bandwidth remote	Specifies the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper.
h323 interface	Defines on which port the proxy will listen.
h323 t120	Enables the T.120 capabilities on your router and specifies bypass or proxy mode.

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 the total bandwidth specified, 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.

Defaults	None

Command Modes	Gatekeeper configuration

Command History	Release	Modification
	12.1(5)T	This command was introduced on the Cisco 2600, 3600, and 7200 series routers and on the MC3810 multiservice concentrator.

Usage Guidelines	The functionality of this command in previous Cisco IOS software releases was enabled by using the zone gatekeeper command.

Examples	The following example configures the remote maximum bandwidth to 100,000 kbps: <pre>gatekeeper bandwidth remote 100000</pre>

Related Commands	Command	Description
	bandwidth	Specifies the maximum aggregate bandwidth for H.323 traffic from a zone to another zone, within a zone, or for a session in a zone.
	h323 interface	Defines which port the proxy will listen on.
	h323 t120	Enables the T.120 capabilities on your router and specifies bypass or proxy mode.

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.

Defaults Battery reversal is enabled.

Command Modes Voice-port configuration

Command History	Release	Modification
	12.0(7)XK	This command was introduced on the Cisco 2600 and 3600 series routers and on the MC3810 multiservice concentrator.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines The **battery-reversal** command applies to FXO and FXS voice ports. On Cisco 2600 and 3600 series routers, only analog voice ports in VIC-2FXO-M1 and VIC-2FXO-M2 voice interface cards are able to detect battery reversal; analog voice ports in VIC-2FXO and VIC-2FXO-EU voice interface cards do not detect battery reversal. On digital voice ports, battery reversal is supported only on E1 Mercury Exchange Limited Channel Associated Signaling (MELCAS); it is not supported in T1 channel associated signaling (CAS) or E1 CAS.

FXS ports normally reverse battery upon call connection. If an FXS port is connected to an FXO port that does not support battery reversal detection, you can use the **no battery-reversal** command on the FXS port to prevent unexpected behavior.

FXO ports in loopstart mode normally disconnect calls when they detect a second battery reversal (back to normal). You can use the **no battery-reversal** command on FXO ports to disable this action.

The **battery-reversal** command restores voice ports to their default battery-reversal operation.

Examples The following example disables battery reversal on voice port 1/1 on a Cisco MC3810:

```
voice-port 1/1
 no battery-reversal
```

The following example disables battery reversal on voice port 1/0/0 on a Cisco 2600 or 3600 series router:

```
voice-port 1/0/0
 no battery-reversal
```

Related Commands

Command	Description
show voice port	Displays voice port configuration information.

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*

Syntax Description

number	Specifies the telephone number to block. You can use a period (.) as a digit wildcard. For example, the command block-caller 5.51234 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.

Defaults

Call blocking is disabled; the router does not block any calls for any listed directory numbers (LDNs) based on caller ID numbers.

Command Modes

Dial peer voice configuration

Command History

Release	Modification
12.1.(2)XF	This command was introduced on the Cisco 800 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

This command is available on Cisco 800 series routers that have plain old telephone service (POTS) ports. For each dial peer, you can enter up to ten caller ID numbers to block. The routers do not accept additional caller ID numbers if ten numbers are already present. In that case, a number must be removed before another caller ID number can be added for blocking.

If you do not specify the **block-caller** command for a local directory, all voice calls to that local directory are accepted. If you specify the **block-caller** command for a local directory, the router verifies that the incoming calling-party number does not match any caller ID numbers in that local directory before processing or accepting the voice call. Each specified caller ID number and incoming calling-party number is compared from right to left, up to the number of digits in the specified caller ID number or incoming calling-party number, whichever has fewer digits.

This command is effective only if you subscribe to caller ID service. If you enable call blocking on caller ID without subscribing to the caller ID service, the routers do not perform the verification process on calling-party numbers and do not block any calls.

Examples

The following example configures a router to block calls from a caller whose caller ID number is 408-555-1234.

```
dial-peer voice 1 pots
block-caller 4085551234
```

Related Commands

Command	Description
caller-id	Identifies incoming calls with caller ID.
debug pots csm csm	Activates events from which an application can determine and display the status and progress of calls to and from POTS ports.
isdn i-number	Configures several terminal devices to use one subscriber line.
pots call-waiting	Enables local call waiting on a router.
registered-caller ring	Configures the Nariwake service registered caller ring cadence.

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

Syntax Description

This command has no arguments or keywords.

Defaults

The voice-port is not in the busyout state.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series routers. On the Cisco MC3810, the voice-port busyout command was eliminated in favor of this command.
12.1(2)T	The modifications in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

If a voice port is in the forced busyout state, only the **no busyout forced** command can restore the voice port to service.

To avoid conflicting command-line interface (CLI) commands, do not use the **busyout forced** command and the **ds0 busyout** command on the same controller.

Examples

The following example forces analog voice port 1/1 on a Cisco MC3810 multiservice concentrator into the busyout state:

```
voice-port 1/1
  busyout forced
```

The following example forces digital voice port 0:8 on a Cisco MC3810 multiservice concentrator into the busyout state:

```
voice-port 0:8
  busyout forced
```

The following example forces analog voice port 3/1/1 on a Cisco 3600 router into the busyout state:

```
voice-port 3/1/1
  busyout forced
```


The following example forces digital voice port 0/0:12 on a Cisco 3600 router into the busyout state:

```
voice-port 0/0:12
  busyout forced
```

Related Commands

Command	Description
busyout-monitor interface	Configures a voice port to monitor a serial interface for events that would trigger a voice-port busyout.
busyout seize	Changes the busyout seize procedure for a voice port.
show voice busyout	Displays information about the voice busyout state.

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* }

Syntax Description

serial	Specifies monitoring of a serial interface. More than one interface can be entered for a voice port.
ethernet	Specifies monitoring of an Ethernet interface. 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.
in-service	(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).

Defaults

The voice port does not monitor any interfaces.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(5)XE	This command was implemented on the Cisco 7200 series routers.
12.0(5)XK	This command was implemented on the Cisco 2600 and 3600 series routers.
12.0(7)T	The Cisco 2600 and 3600 series router implementation was integrated into Cisco IOS Release 12.0(7)T.
12.0(7)XK	The ability to monitor an Ethernet port was introduced and the in-service keyword was added. The serial keyword was first supported on the Cisco 2600 and 3600 series routers.
12.1(1)T	The implementation of this command on the Cisco 7200 series routers was integrated into Cisco IOS Release 12.1(1)T.
12.1(2)T	The serial and ethernet keywords were added, the in-service keyword was integrated into Cisco IOS Release 12.1(2)T, and the <i>interface number</i> argument was changed to go with the serial and Ethernet keywords.
12.1(3)T	The interface keyword was removed.

Usage Guidelines

When you place a voice port in the busyout monitor state, the voice port monitors the specified interface and enters the busyout state when the interface is down. This down state forces the rerouting of calls.

The command monitors only the up or down status of an interface—not end-to-end TCP/IP connectivity.

When an interface is operational, a busied-out voice port returns to its normal state.

This feature can monitor LAN, WAN, and virtual interfaces as well as subinterfaces.

The Cisco 2600 and 3600 series routers and the MC3810 multiservice concentrator support ATM interfaces. To monitor an ATM interface, enter **ATM** and the interface number.

A voice port can monitor multiple interfaces at the same time. To configure a voice port to monitor multiple interfaces, reenter the **busyout monitor** command for each additional interface to be monitored.

If you specify more than one monitored interface for a voice port, all the monitored interfaces must be down to trigger busyout on the voice port.

You can combine in-service and out-of-service monitoring on a voice port. The following rule describes the actions if monitored interfaces change state.

A voice port is busied out if either of the following occurs:

- Any interface monitored for coming into service comes up.
- All interfaces monitored for going out of service go down.

Examples

The following example shows configuration of analog voice port 1/1 on a Cisco MC3810 multiservice concentrator to busyout if serial ports 1 and 0:0 both go out of service:

```
voice-port 1/1
  busyout monitor serial 0:0
  busyout monitor serial 1
```

The following example shows configuration of analog voice port 1/2 on a Cisco MC3810 multiservice concentrator to busy out if serial port 0 or 1 comes into service:

```
voice-port 1/2
  busyout monitor serial 0 in-service
  busyout monitor serial 1 in-service
```

The following example shows configuration of digital voice port 1/2/2 on a Cisco 3600 series router to busy out if serial port 0 goes out of service:

```
voice-port 1/2/2
  busyout monitor serial 0
```

The following example shows configuration of digital voice port 0:6 on a Cisco MC3810 multiservice concentrator to busy out if both Ethernet port 0 and serial port 0 go out of service:

```
voice-port 0:6
  busyout monitor ethernet 0
  busyout monitor serial 0
```

The following example shows configuration of the voice port to monitor two serial interfaces and an Ethernet interface. When all these interfaces are down, the voice port is busied out. When at least one interface is operating, the voice port is put back into a normal state.

```
voice-port 3/0:0
  busyout monitor ethernet 0/0
  busyout monitor serial 1/0
  busyout monitor serial 2/0
```

Related Commands	Command	Description
	busyout forced	Forces a voice port into the busyout state.
	busyout monitor probe	Configures a voice port to enter the busyout state if a Service Assurance Agent (SAA) probe signal returned from a remote, IP-addressable interface crosses a specified delay or loss threshold.
	busyout seize	Changes the busyout seize procedure for a voice port.
	show voice busyout	Displays information about the voice busyout state.
	voice-port busyout	Places all voice ports associated with a serial or ATM interface into a busyout state.

busyout monitor probe

To configure a voice port to enter the busyout state if a Service Assurance Agent (SAA) 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 SAA 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*

Syntax Description

<i>ip-address</i>	The IP address of a target interface for the SAA probe signal.
codec	(Optional) Configures the profile of the SAA probe signal to mimic the packet size and interval of a specific codec type.
<i>codec-type</i>	(Optional) The codec type for the SAA probe signal. Available options are as follows: - g711a—G.711 A-law - g711u—G.711 U-law (the default) - g729—G.729 - g729a—G.729
icpif	(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.
loss	(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.
delay	(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.

Defaults

If the **busyout monitor probe** command is not entered, the voice port does not monitor SAA probe signals.

If the **busyout monitor probe** command is entered with no optional keywords or arguments, the default codec type is G.711 alaw, and the default loss and delay thresholds are the threshold values configured with the **pstn fallback** command.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 and 3600 series and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

A voice port can monitor multiple interfaces at the same time. To configure a voice port to monitor multiple interfaces, enter the **busyout monitor probe** command for each additional interface to be monitored.

The **busyout monitor probe** command is effective only if the call fallback function is enabled on this router and the SAA responder is enabled on the target router.

The SAA probe is transmitted periodically with a period determined by the call fallback function.

Refer to the *PSTN Fallback* feature module for Cisco IOS Release 12.1(3)T for details of the call fallback function and ICPIF values.

Lower thresholds of ICPIF, loss, and delay result in earlier busyout when the link deteriorates, thereby raising the voice minimum quality level. Higher thresholds prevent busyout until loss and delay are greater, allowing transmission of lower-quality voice.

**Caution**

If thresholds are set too low, the link can alternate between in-service and out-of-service states, causing repeated interruptions of traffic.

Examples

The following example configures analog voice port 1/1 on a Cisco MC3810 multiservice concentrator to use an SAA probe with a G.711alaw profile to probe the link to two remote interfaces that have IP addresses and to busy out the voice port. Both links have a loss exceeding 25 percent or a packet delay of more than 1.5 seconds.

```
voice-port 1/1
  busyout monitor probe 209.165.202.128 codec g711a loss 25 delay 1500
  busyout monitor probe 209.165.202.129 codec g711a loss 25 delay 1500
```

Related Commands

Command	Description
busyout monitor	Places a voice port into the busyout monitor state.
pstn fallback	Forces a voice port into the busyout state.
show voice busyout	Displays information about the voice busyout state.
voice class busyout	Creates a voice class for local voice busyout functions.

busyout seize

To change the busyout action for a 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

ignore	Specifies the type of ignore procedure, depending on the type of voice port signaling. See Table 4 for more information.
repeat	Specifies the type of repeat procedure, depending on the type of voice port signaling. See Table 4 for more information.

Defaults

See [Table 4](#) for the default actions for different voice ports and signaling types.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	This command was first supported on Cisco 2600 and 3600 series routers.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The **busyout seize** command is valid for both analog and digital voice ports. On digital voice ports, the busyout actions are valid whether the busyout results from a voice-port busyout event or from the **ds0-busyout** command.

The voice port returns to an idle state when the event that triggered the busyout disappears.

[Table 4](#) describes the busyout actions for the **busyout seize** settings on each voice port type.

The busyout action for E and M voice ports is to seize the far end by setting lead busy.

Table 4 *Busyout Seize Actions for Voice Ports*

Voice Port Signaling Type	Procedure Setting (busyout-option command)	Busyout Actions
FXS loop start	Default	Removes the power from the loop. For analog voice ports, this is equivalent to removing the ground from the tip lead. For digital voice ports, the port will generate the bit pattern equivalent to removing the ground from the tip lead, or it will busy out if the bit pattern exists.
FXS loop start	Ignore	Ignores the ground on the ring lead.
FXS ground start	Default	Grounds the tip lead and stays at this state.
FXS ground start	Ignore	1. Leaves the tip lead open. 2. Ignores the ground on the ring lead.
FXS ground start	Repeat	1. Grounds the tip lead. 2. Waits for the far end to close the loop. 3. The far end closes the loop. 4. If the far end then opens the loop, FXS removes the ground from the tip lead. 5. FXS waits for several seconds before returning to Step 1.
FXO loop start	Default	Closes the loop and stays at this state.
FXO loop start	Ignore	1. Leaves the loop open. 2. Ignores the ringing current on the ring level.
FXO loop start	Repeat	1. Closes the loop. 2. After the detected far end starts the power denial procedure, FXO opens the loop. 3. After the detected far end has completed the power denial procedure, FXO waits for several seconds before returning to Step 1.
FXO ground start	Default	Grounds the tip lead.
FXO ground start	Ignore	1. Leaves the loop open. 2. Ignores the running current on the ring lead, or the ground current on the tip lead.
FXO ground start	Repeat	1. Grounds the ring lead. 2. Removes the ground from the ring lead and closes the loop after the detected far end grounds the tip lead. 3. When the detected far end removes the ground from tip lead, FXO opens the loop. 4. FXO waits for several seconds before returning to Step 1.

Examples

The following example shows configuration of analog voice port 1/1 to perform the ignore actions when busied out:

```
voice-port 1/1
  busyout seize ignore
```

The following example shows configuration of digital voice port 0:2 to perform the repeat actions when busied out:

```
voice-port 0:2
  busyout seize repeat
```

Related Commands

Command	Description
busyout forced	Forces a voice port into the busyout state.
busyout-monitor interface	Configures a voice port to monitor an interface for events that would trigger a voice port busyout.
ds0 busyout	Forces a DS0 time slot on a controller into the busyout state.
show voice busyout	Displays information about the voice busyout state.
voice-port busyout	Places all voice ports associated with a serial or ATM interface into a busyout state.

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

No arguments or keywords

Defaults

The Cisco MC3810 multiservice concentrator is enabled as a CAC slave.

Command Modes

Voice-service configuration

Command History

Release	Modification
12.1(1)XA	The command was introduced for the Cisco MC3810 multiservice concentrator.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

You should configure the Cisco MC3810 multiservice concentrators at opposite ends of an AAL2 trunk for the opposite CAC operation—master at one end and slave at the other end.

A Cisco MC3810 multiservice concentrator configured as a master always performs CAC during fax/modem upspeed. A Cisco MC3810 multiservice concentrator configured as a slave sends a request for CAC to the CAC master.

Examples

The following example shows configuration of the CAC operation of a Cisco MC3810 multiservice concentrator as master:

```
voice service voatm
 session protocol aal2
 cac master
```

The following example shows the CAC operation of a Cisco MC3810 multiservice concentrator being returned to slave:

```
voice service voatm
 session protocol aal2
 no cac master
```

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.

Defaults

No cadence pattern is configured.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 and Cisco 3600 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

A cadence list enables the router to match a complex tone pattern from a PBX or public switched telephone network (PSTN). A tone is detected if it matches any configured cadence list. You can create up to ten cadence lists, enabling the router to detect up to ten different tone patterns. If the tone to be detected consists of only one on-off cycle, you can configure this in either of two ways:

- Create a cadence list using only the *cycle-1-on-time* and *cycle-1-off-time* variables.
- Use the **cadence-max-off-time** and **cadence-min-on-time** commands.

You must also configure the times of the **cadence-max-off-time** and **cadence-min-on-time** commands to be compatible with the on and off times specified by the **cadence-list** command. The time of the **cadence-max-off-time** must be equal to or greater than the longest off-time in the cadence list; the **cadence-min-on-time** must be equal to or less than the shortest on-time in the cadence list.

Examples

The following example shows configuration of cadence list 1 with three on/off cycles and cadence list 2 with two on/off cycles for voice class 100:

```
voice class dualtone 100
cadence-list 1 100 100 300 300 100 200
cadence-list 2 100 200 100 400
```

Related Commands

Command	Description
cadence-max-off-time	Specifies the maximum off duration for detection of a tone.
cadence-min-on-time	Specifies the minimum on duration for detection of a tone.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

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

Syntax Description	<i>time</i>	The maximum off time of a 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.

Defaults	No cadence maximum off time is configured.

Command Modes	Voice-class configuration

Related Commands	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 and 3600 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines	You must specify a time value greater than the off time of the tone to be detected. You must specify a time value greater than 0 to enable detection of a tone. With the default (0), the router will detect only a continuous tone.

Examples	The following example shows configuration of a maximum off duration of 20 seconds for voice class 100:

```
voice class dualtone 100
cadence-max-off-time 2000
```

Related Commands	Command	Description
	cadence-min-on-time	Specifies the minimum on duration for detection of a tone.
	cadence-variation	Specifies the cadence variation time allowed for detection of a tone.
	voice class dualtone	Creates a voice class for FXO tone detection parameters.

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

Syntax Description

<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.

Defaults

No cadence minimum on time is configured.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 and 3600 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

You must specify a time value shorter than the on time of the tone to be detected. With the default (0), a tone of any length will be detected.

Examples

The following example shows configuration of a minimum on duration of 30 milliseconds for voice class 100:

```
voice class dualtone 100
 cadence-min-on-time 3
```

Related Commands

Command	Description
cadence-max-off-time	Specifies the maximum <i>off</i> duration for detection of a tone.
cadence-variation	Specifies the cadence variation time allowed for detection of a tone.
voice class dualtone	Creates a voice class for Foreign Exchange Office (FXO) tone detection parameters.

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

Syntax Description

<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.

Defaults

Zero for zero millisecond cadence variation allowed

Command Modes

Voice-class configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 and 3600 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

You should specify a time value greater than the cadence variation of the tone to be detected. With the default of 0, only those tones that match the configured cadence will be detected.

Examples

The following example shows configuration of a cadence variation time of 30 milliseconds for voice class 100:

```
voice class dualtone 100
 cadence-variation 30
```

Related Commands

Command	Description
cadence-max-off-time	Specifies the maximum off duration for detection of a tone.
cadence-min-on-time	Specifies the minimum on duration for detection of a tone.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

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

Syntax Description	<i>bg-minutes</i> 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: • 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. • 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.	
Defaults	30 minutes	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco AS5300 universal access server.
Examples	The following example displays the call application cache reload time command configured to specify 30 minutes before a background process is awakened: <pre>call application cache reload time 30</pre>	
Related Commands	Command	Description
	call application voice load	Allows reload of an application that was loaded via the MGCP scripting package.
	show call application voice	Displays all TCL or MGCP scripts that are loaded.

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}*

Syntax Description	<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.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced on the Cisco AS5300 universal access server.
	12.1(3)T	The <i>word</i> argument was added for attribute-value (AV) pairs.

Usage Guidelines Use this command when configuring interactive voice response (IVR) or one of the IVR-related features (such as Debit Card) to define the name of an application and to identify the location of the TCL script associated with this application.

**Note**

The command **no call application voice** *application-name* removes the entire application and all parameters, if configured.

Examples This example shows how to define the application “prepaid” and the TFTP server location of the associated TCL script:

```
call application voice prepaid tftp://keyer/debitcard.tcl
```

The following is an example of AV pair configuration:

```
set avsend(h323-ivr-out,)) "payphone:true"  
set avsend(323-ivr-out,1) "creditTime:3400"
```

The AV pair (after the array is defined, as in the prior example) must be sent to the server, using the authentication, authorization, and accounting (AAA) authenticate or AAA authorize verbs as follows:

```
aaa authenticate $account $password $avsend
```

The script would use this AV pair whenever it is needed to convey information to the RADIUS server that cannot be represented by the standard vendor-specific attributes (VSAs).

Related Commands	Command	Description
	call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
	call application voice load	Reloads the designated TCL script.
	call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
	call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.
	call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
	call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
	call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
	call application voice warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time runs out for the designated application.

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**

Syntax Description

<i>application-name</i>	The name of the application.
prompt-user	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.
redialer	Specifies that no DID is set in the incoming POTS dial peer and that the redialer device will be used for two-stage dialing.

Defaults

Prompt-user when DID is not set in the dial peer

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 universal access server.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

Use the call application voice access-method command to specify the access method for two-stage dialing when DID is disabled in the POTS dial peer.

Examples

The following example specifies **prompt-user** as the access method for two-stage dialing for the app_libretto_onramp9 IVR application:

```
call application voice app_libretto_onramp9 access-method prompt-user
```

Related Commands

Command	Description
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reloads the designated TCL script.

Command	Description
call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines the number of warning seconds a user receives before the allowed calling time runs out for the designated application.

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**

Syntax Description	<i>application-name</i> The name of the application.

Defaults	Disabled

Command Modes	Global configuration

Command History	Release	Modification
	12.1(3)XI	This command was introduced on the Cisco AS5300 universal access server.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines	This command enables AAA accounting services if an AAA accounting method list has been defined using both the aaa accounting command and the mmoip aaa method fax accounting command. This command applies to off-ramp store-and-forward fax functions on Cisco AS5300 universal access server voice feature cards (VFCs). It is not used on modem cards.

Examples	The following example enables AAA accounting to be used with outbound store-and-forward fax: <pre>configure terminal call application voice app_libretto_onramp9 accounting enable</pre>

Related Commands	Command	Description
	mmoip aaa method fax accounting	Defines the name of the method list to be used for AAA accounting with store-and-forward fax.

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*

Syntax Description

<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.

Defaults

No AAA accounting method list is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 universal access server.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

This command defines the name of the accounting feature of the authentication, authorization, and accounting (AAA) method list to be used with store-and-forward fax. The method list itself, which defines the type of accounting services provided for store-and-forward fax, is defined using the **aaa accounting** global configuration command. Unlike standard AAA (where each defined method list can be applied to specific interfaces and lines), the AAA accounting method lists used in store-and-forward fax are applied globally on the Cisco AS5300 universal access server.

After the accounting method lists have been defined, they are enabled by using the **mmoip aaa receive-accounting enable** command.

This command applies to both on-ramp and off-ramp store-and-forward fax functions on Cisco AS5300 universal access server voice feature cards. It is not used on modem cards.

Examples

The following example defines a AAA accounting method list (called “sherman”) to be used with store-and-forward fax:

```
aaa new-model
call application voice app_libretto_onramp9 accounting-list sherman
```

Related Commands

Command	Description
call application voice accounting enable	Enables on-ramp AAA accounting services.

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*

Syntax Description

<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.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 universal access server.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

This command defines the name of the authentication, authorization, and accounting (AAA) authentication method list to be used with fax applications on voice feature cards. The method list itself, which defines the type of authentication services provided for store-and-forward fax, is defined using the **aaa authentication** global configuration command. Unlike standard AAA (where each defined method list can be applied to specific interfaces and lines), AAA authentication method lists used with fax applications are applied globally on the Cisco AS5300 universal access server.

After the authentication method lists have been defined, they are enabled by using the **call application voice authentication enable** command.

Examples

The following example defines an AAA authentication method list (called “fax”) to be used with T.38 fax relay and T.37 store-and-forward fax:

```
configure terminal
call application voice app_libretto_onramp9 authen-list fax
```

Related Commands	Command	Description
	call application voice authentication enable	Enables AAA authentication services for a TCL application.
	call application voice authen-method	Specifies the authentication method for a TCL application.

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** }

Syntax Description

<i>application-name</i>	The name of the application.
prompt-user	Indicates that the user is prompted for the TCL application account identifier.
ani	Indicates that the calling-party telephone number (automatic number identification [ANI]) is used as the TCL application account identifier.
dnis	Indicates that the called party telephone number (dialed number identification service [DNIS]) is used as the TCL application account identifier.
gateway	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> .
redialer-id	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.
redialer-dnis	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.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 universal access server.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With T.37 store-and-forward fax and T.38 real-time fax, you can specify that the ANI, DNIS, gateway identification (ID), redialer ID, or redialer DNIS be used to identify the user for authentication or that the user be prompted for the TCL application.

Examples

The following example shows how to configure the router-specific name derived from the host name and domain name as the TCL application account identifier for the app_libretto_onramp9 TCL application:

```
call application voice app_libretto_onramp9 authen-method gateway
```

Related Commands

Command	Description
call application voice authentication enable	Enables AAA authentication services for a TCL application.
call application voice authen-list	Specifies the name of an authentication method list for a TCL application.

call application voice authentication enable

To enable AAA authentication services for a tool command line (TCL) application, use the **call application voice authentication enable** command in global configuration mode. To disable authentication for a TCL application, use the **no** form of this command.

call application voice *application-name* **authentication enable**

no call application voice *application-name* **authentication enable**

Syntax Description	<i>application-name</i>	The name of the application.

Defaults	No default behavior or values.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(3)XI	This command was introduced on the Cisco AS5300 universal access server.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines	This command enables AAA authentication services for a TCL application if a AAA authentication method list has been defined using both the aaa authentication command and the call application voice authen-list command.

Examples	The following example enables a AAA authentication method list (called peabody) to be used with outbound store and forward fax.

```
configure terminal
aaa new-model
call application voice app_onramp6 authen-list peabody
call application voice app_onramp6 authentication enable
```

Related Commands	Command	Description
	call application voice authen-list	Specifies the name of an authentication method list for a TCL application.
	call application voice authen-method	Specifies the authentication method for a TCL application.

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*

Syntax Description

<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.

Defaults

No password is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 universal access server.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

CiscoSecure for Windows NT might require a separate password to complete authentication, no matter what security protocol you use. This command defines the password to be used with CiscoSecure for Windows NT. All records on the Windows NT server use this defined password.

This command applies to on-ramp store-and-forward fax functions on Cisco AS5300 universal access server voice feature cards. It is not used on modem cards.

Examples

The following example shows a password (abercrombie) being used by AAA for the app_libretto_onramp9 TCL application:

```
call application voice app_libretto_onramp9 global-password abercrombie
```

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*

Syntax Description	<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:
		• en—English • sp—Spanish • ch—Mandarin • aa—all

Defaults	No default behavior or values.

Command Modes	Global configuration mode

Command History	Release	Modification
	12.0(7)T	This command was introduced.

Usage Guidelines

Use this command when configuring interactive voice response (IVR)—depending on the Tool Command Language (TCL) script being used—or one of the IVR-related features (such as Debit Card) to define the language of the audio file for the specified application and to pass that information to the specified application.

[Table 5](#) lists TCL script names and the corresponding parameters that are required for each TCL script.

Table 5 *TCL Scripts and Parameters*

TCL Script Name	Description	Parameters to Configure
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and personal identification number (PIN), respectively, using automatic number identification (ANI) and NULL. The numbers of digits allowed for the account number and password, respectively, are configurable through the command-line interface (CLI). If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	• call application voice uid-len minimum = 1, maximum = 20, default = 10 • call application voice pin-len minimum = 0, maximum = 10, default = 4 • call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN, respectively, using ANI and NULL. If the authentication fails, it allows the caller to retry. The retry number is configured through CLI. The account number and PIN are collected separately.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and dialed number identification service (DNIS). If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_col_npw_3_cli.tcl	This script authenticates using ANI and NULL for account numbers and PINs, respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and NULL for account and PIN, respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	• call application voice retry-count minimum = 1, maximum = 5, default = 3

Examples

The following example shows how to define English and Spanish as the languages of the audio files associated with the application (named “prepaid”):

```
call application voice prepaid language 1 en
call application voice prepaid language 2 sp
```

Related Commands	Command	Description
	call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
	call application voice load	Reload the designated TCL script.
	call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
	call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.
	call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
	call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
	call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application. the application.
	call application voice warning-time	Defines the number of second's warning a user receives before the allowed calling time runs out for the designated application.

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*

Syntax Description

<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.

Defaults

TCL or scripts are not loaded.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco 2600 series routers, Cisco 3600 series (except for the 3660), and on the Cisco AS5300.
12.1(3)T	Support for dynamic script loading of MGCP scripts was added.

Usage Guidelines

The software checks the signature lock to ensure that it is a Cisco-supported TCL script.

If the TCL script does not have a valid Cisco-supported signature, the software fails to load the script and generates the following error message:

```
00:02:54: %IVR-3-BAD_IVR_SIG: Script signature is invalid
```

Examples

The following example shows the loading of a MGCP script package:

```
Router# call application voice load mgcp-script-pkg
```

Related Commands

Command	Description
call application cache reload time	Configures the interval for reloading MGCP scripts.
call application voice	Creates and calls the application that will interact with the IVR feature.
show call application voice	Displays a list of the voice applications that are configured.

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	application-name	The name of the application to which the PIN length parameter is being passed.
	number	Defines the number of allowable characters in PINs associated with the specified application. Valid entries are from 0 to 10.
Defaults	No default behavior or values.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.0(7)T	This command was introduced in the Cisco 2600 series routers, Cisco 3600 series routers, and Cisco AS5300 universal access routers.
Usage Guidelines	Use this command when configuring interactive voice response (IVR)—depending on the TCL script being used—or one of the IVR-related features (such as Debit Card) to define the number of allowable characters in a PIN for the specified application and to pass that information to the specified application. Table 6 lists TCL script names and the corresponding parameters that are required for each TCL script.	

Table 6 *TCL Scripts and Parameters*

TCL Script Name	Description	Parameters to Configure
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN, respectively, using automatic number identification (ANI) and NULL. The number of digits allowed for the account number and password, respectively, are configurable through the command-line interface (CLI). If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	• call application voice uid-len minimum = 1, maximum = 20, default = 10 • call application voice pin-len minimum = 0, maximum = 10, default = 4 • call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN, respectively, using ANI and NULL. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and dialed number identification service (DNIS). If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_col_npw_3_cli.tcl	This script authenticates using ANI and NULL for account numbers and PINs, respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and NULL for account and PIN, respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	• call application voice retry-count minimum = 1, maximum = 5, default = 3

Examples

The following example shows how to define a PIN length of four characters for the application (named “prepaid”):

```
call application voice prepaid pin-len 4
```

Related Commands

Command	Description
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reload this designated TCL script.
call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time runs out for the designated application.

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.

Defaults	No default behavior or values.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced on the Cisco 2600 series routers, 3600 series routers , and the AS5300 universal access server.

Usage Guidelines	Use this command when configuring interactive voice response (IVR)—depending on the Tool Command Language (TCL) script being used—or one of the IVR-related features (such as Debit Card) to define the telephone number to which a call will be redirected.

Table 7 lists TCL script names and the corresponding parameters that are required for each TCL script.

Table 7 *TCL Scripts and Parameters*

TCL Script Name	Description	Parameters to Configure
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and personal identification number (PIN), respectively, using automatic number identification (ANI) and NULL. The number of digits allowed for the account number and password, respectively, are configurable through the command-line interface (CLI). If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	• call application voice uid-len minimum = 1, maximum = 20, default = 10 • call application voice pin-len minimum = 0, maximum = 10, default = 4 • call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN, respectively, using ANI and NULL. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and dialed number identification service (DNIS). If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_col_npw_3_cli.tcl	This script authenticates using ANI and NULL for account and PIN, respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and NULL for account numbers and PINs, respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	• call application voice retry-count minimum = 1, maximum = 5, default = 3

Examples

The following example shows how to define a redirect number for the application (named “prepaid”):

```
call application voice prepaid redirect-number 5551111
```

Related Commands	Command	Description
	call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
	call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
	call application voice load	Reloads the designated TCL script.
	call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
	call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
	call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
	call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
	call application voice warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time runs out for the designated application.

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	application-name	The name of the application to which the number of possible retries is being passed.
	number	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.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the AS5300.

Usage Guidelines Use this command when configuring interactive voice response (IVR)—depending on the Tool Command Language (TCL) script being used—or one of the IVR-related features (such as Debit Card) to define how many times a user can reenter a PIN.

Table 8 lists TCL script names and the corresponding parameters that are required for each TCL script.

Table 8 *TCL Scripts and Parameters*

TCL Script Name	Description Summary	Parameters to Configure
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN, respectively, using automatic number identification (ANI) and NULL. The number of digits allowed for the account number and password, respectively, are configurable through the command-line interface (CLI). If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	• call application voice uid-len minimum = 1, maximum = 20, default = 10 • call application voice pin-len minimum = 0, maximum = 10, default = 4 • call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN, respectively, using ANI and NULL. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and dialed number identification service (DNIS). If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_col_npw_3_cli.tcl	This script authenticates using ANI and NULL for account numbers and PINs, respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and NULL for account and PIN, respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	• call application voice retry-count minimum = 1, maximum = 5, default = 3

Examples

The following example shows how to define that a user can re-enter a PIN three times before being disconnected for the application (named “prepaid”):

```
call application voice prepaid retry-count 3
```


Related Commands	Command	Description
	call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
	call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
	call application voice load	Reloads the designated TCL script.
	call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
	call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.
	call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
	call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application. the application.
	call application voice warning-time	Defines the number of second's warning a user receives before the allowed calling time runs out for the designated application.

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 set-location parameters are being passed.
	<i>language</i>	Defines the language associated with the audio files. Possible values for this parameter are as follows: • en = English • ch = Mandarin • sp = Spanish
	<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.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the AS5300.

Usage Guidelines Use this command when configuring interactive voice response (IVR)—depending on the TCL script being used—or one of the IVR-related features (such as Debit Card) to define the location, language, and category of the audio files for the designated application and pass that information to the application.

Table 9 lists TCL script names and the corresponding parameters that are required for each TCL script.

Table 9 *TCL Scripts and Parameters*

TCL Script Name	Description	Parameters to Configure
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN, respectively, using automatic number identification (ANI) and NULL. The number of digits allowed for the account number and password, respectively, are configurable through the command-line interface (CLI). If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	• call application voice uid-len minimum = 1, maximum = 20, default = 10 • call application voice pin-len minimum = 0, maximum = 10, default = 4 • call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN, respectively, using ANI and NULL. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and dialed number identification service (DNIS). If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_col_npw_3_cli.tcl	This script authenticates using ANI and NULL for account and PIN respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and NULL for account numbers and PINs, respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	• call application voice retry-count minimum = 1, maximum = 5, default = 3

Examples

The following example shows how to configure the **call application voice set-location** command for the application (named “prepaid”). In this example, the language defined is English, the category into which the audio files are group is Category 0 (meaning all), and the location is the keyer directory on the TFTP server.

```
call application voice prepaid set-location en 0 tftp://keyer/
```

Related Commands	Command	Description
	call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
	call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
	call application voice load	Reloads the designated TCL script.
	call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
	call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.
	call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
	call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application. the application.
	call application voice warning-time	Defines the number of seconds of warning that a user is warned before their allowed calling time runs out for the designated application.

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 delete the specification of the number of characters in the user identification number, use the **no** form of this command.

call application voice *application-name* **uid-length** *number*

no call application voice *application-name* **uid-length** *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.

Defaults	No default behavior or values.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced on the Cisco 2600 series routers, Cisco 3600 series, and on the Cisco AS5300.

Usage Guidelines	Use this command when configuring interactive voice response (IVR), depending on the Tool Command Language (TCL) script being used or one of the IVR-related features (such as Debit Card) to define the number of allowable characters in a UID for the specified application and to pass that information to the specified application.

Table 7 lists TCL script names and the corresponding parameters that are required for each TCL script.

Table 10 *TCL Script Names and Parameters*

TCL Script Name	Description	Parameters to Configure
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN, respectively, using automatic number identification (ANI) and NULL. The number of digits allowed for the account number and password, respectively, are configurable through the command-line interface (CLI). If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	• call application voice uid-len minimum = 1, maximum = 20, default = 10 • call application voice pin-len minimum = 0, maximum = 10, default = 4 • call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_authen_col_npw_cli.tcl	This script authenticates the account number and personal identification number (PIN), respectively, using ANI and NULL. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and dialed number identification service (DNIS). If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_col_npw_3_cli.tcl	This script authenticates using ANI and NULL for account numbers and PINs, respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and NULL for account numbers and PINs, respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	• call application voice retry-count minimum = 1, maximum = 5, default = 3

Examples

The following example shows how to configure four allowable characters in the UID for the application (named “prepaid”):

```
call application voice prepaid uid-len 4
```

Related Commands	Command	Description
	call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
	call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
	call application voice load	Reloads the designated TCL script.
	call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
	call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.
	call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
	call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
	call application voice warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time runs out for the designated application.

call application voice warning-time

To define the number of seconds of 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.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco 2600 series routers, 3600 series routers, and AS5300 universal access server.

Usage Guidelines

Use this command when configuring interactive voice response (IVR)—depending on the Tool Command Language (TCL) script being used—or one of the IVR-related features (such as Debit Card) to define how many seconds in the warning period before the allowed calling time runs out for the specified application and to pass that information to the specified application.

[Table 11](#) lists TCL script names and the corresponding parameters that are required for each TCL script.

Table 11 TCL Scripts and Parameters

TCL Script Name	Description	Parameters to Configure
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN, respectively, using automatic number identification (ANI) and NULL. The number of digits allowed for the account number and password, respectively, are configurable through the command-line interface (CLI). If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	• call application voice uid-len minimum = 1, maximum = 20, default = 10 • call application voice pin-len minimum = 0, maximum = 10, default = 4 • call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_authen_col_npw_cli.tcl	This script authenticates the account number and personal identification number (PIN), respectively, using ANI and NULL. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and dialed number identification service (DNIS). If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_col_npw_3_cli.tcl	This script authenticates using ANI and NULL for account and PIN, respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	• call application voice retry-count minimum = 1, maximum = 5, default = 3
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and NULL for account numbers and PINs, respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	• call application voice retry-count minimum = 1, maximum = 5, default = 3

Examples

The following example shows how to configure a 30-second warning time for the application (named "prepaid"):

```
call application voice prepaid warning-time 30
```

Related Commands	Command	Description
	call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
	call application voice load	Reloads the designated TCL script.
	call application voice location	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
	call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
	call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.
	call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
	call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
	call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application. the application.

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.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the MC3810 multiservice concentrator.

Usage Guidelines

Enabling the **call fallback active** command determines whether calls should be accepted or rejected based on probing of network conditions. The command **call fallback active** checks each H.323 call request and rejects the call if the network congestion parameters are greater than the value of the configured threshold parameters of the destination. If this is the case, alternative dial peers are tried from the session application layer.

Use the **call fallback threshold delay loss** or **call fallback threshold icpif** command to set the threshold parameters.

Connected calls are not affected by this feature.

Examples

The following example enables the **call fallback active** command:

```
call fallback active
```

Related Commands

Command	Description
call fallback cache-size	Specifies the call fallback cache size for network traffic probe entries.
call fallback cache-timeout	Specifies the time after which the cache entries of network conditions are purged.
call fallback instantaneous-value-weight	Configures the call fallback subsystem to take an average from the last two cache entries for call requests.

Command	Description
call fallback jitter-probe num-packets	Specifies the number of packets in a jitter probe used to determine network conditions.
call fallback jitter-probe precedence	Specifies the priority of the jitter-probe transmission.
call fallback jitter-probe priority-queue	Assigns a priority-queue for jitter-probe transmissions.
call fallback key-chain	Specifies use of MD5 authentication for sending and receiving SAA probes.
call fallback map address-list	Configures the call fallback router to keep a cache table by IP addresses of distances for several destination peers sitting behind the router.
call fallback map subnet	Configures the call fallback router to keep a cache table by subnet addresses of distances for several destination peers sitting behind the router.
call fallback probe-timeout	Sets the timeout for a SAA probe for call fallback purposes.
call fallback threshold delay loss	Configures the call fallback threshold to use solely packet delay and loss values.
call fallback threshold icpif	Configures call fallback to use the Impairment/Calculated Planning Impairment Factor (ICPIF) threshold.
show call fallback config	Displays the call fallback configuration.

call fallback cache-size

To specify the call fallback 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.

Defaults	128 entries

Command Modes	Global configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the MC3810 multiservice concentrator.

Usage Guidelines	The cache size can be changed only when the call fallback active command is not enabled. The pverflow process deletes up to one-fourth of the cache entries to allow for additional calls beyond the specified cache size. The cache entries chosen for deletion are the oldest entries in the cache.

Examples	The following example specifies 120 cache entries: <pre>call fallback cache-size 120</pre> When call fallback is already configured, the output is as follows: <pre>call fall cache-size 128 Cache size left unchanged (can be changed only when Fallback is OFF (use no call fallback))</pre>

Related Commands	Command	Description
	call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
	call fallback cache-timeout	Specifies the time after which the cache entry is purged.
	show call fallback cache	Displays the current IPCIF estimates for all IP addresses in the cache.
	show call fallback config	Displays the call fallback configuration.

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*

Syntax Description	<i>seconds</i>	Specifies the cache timeout value in seconds. The valid range is from 1 to 2,147,483.
Defaults	600 seconds	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the MC3810 multiservice concentrator.

Usage Guidelines

Enabling the **call fallback cache-timeout** command sends a Service Assurance Agent (SAA) probe out to the network to determine the amount of congestion in terms of configured thresholds. The network condition terms are based on delay and loss, or Impairment/Calculated Planning Impairment Factor (ICPIF) thresholds. Use the **call fallback threshold delay loss** or **call fallback threshold icpif** command to set the threshold parameters.

The cache keeps entries for every network congestion-checking probe sent and received between timeouts. The cache updates after each probe returns the current condition of network traffic. To set the probe frequency, use the **call fallback probe-timeout** command.

A call comes into the router. The router matches a dial peer and obtains the destination information. The router calls the fall back subsystem to look up the specified destination in its network traffic cache. If the delay and loss or ICPIF threshold exists and is current, then the router uses that value to decide whether to permit the call into the VoIP network. If the router determines that the network congestion is below the configured threshold (by looking at the value in the cache), then the call is connected.

After each call request, the timer is reset. Purging of the cache occurs only when the cache has received no call requests during the timeout (*seconds*) period. When the cache timeout expires, the entire cache is deleted, and a probe is sent to start a new cache entry. A call cannot be completed until this probe returns with network traffic information.

The network congestion probes continue in the background as long as the entry for the last call request remains in the cache.

Examples

The following example specifies 1200 seconds before the cache times out:

```
call fallback cache-timeout 1200
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback cache-size	Specifies the call fallback cache size.
call fallback probe-timeout	Specifies the call fallback probe timeout.
call fallback threshold delay loss	Configures the call fallback threshold to use only packet delay and loss values.
call fallback threshold icpif	Configures the call fallback to use the ICPIF threshold.
show call fallback cache	Displays the current ICPIF estimates for all IP addresses in the cache.
show call fallback config	Displays the call fallback configuration.

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*

Syntax Description	<i>weight</i>	Specifies the instantaneous value weight. The valid range is from 0 to 100 percent.

Defaults	66 percent

Command Modes	Global configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the MC3810 multiservice concentrator.

Usage Guidelines	Probes returning with network congestion information are logged into the cache to determine whether the next call request will be granted. The network can be busy regularly, and the cache entries reflect these heavy traffic conditions. However, one probe may return with low traffic conditions, which are in contrast to normal conditions. All call requests received between the time of this probe and the next use this entry to determine call acceptance. These calls are allowed through the network, but before the next probe is sent and received, the normal heavy traffic conditions may have returned. The calls sent through congest the network and result in worse traffic conditions.

Use the **call fallback instantaneous-value-weight** command to recover gradually from heavy traffic network conditions. While the system waits for a call, probes are received updating the cache. When a new probe is received, the *weight* calculates how much to rely upon the new probe and how much to rely upon the previous cache entry. If the *weight* is set to 50(%), the system enters a cache entry based on an average from the new probe and the most recent entry in the cache. Call requests use this blended entry to determine acceptance. This system allows the call fallback subsystem to keep conservative measures of network congestion.

The configured *weight* applies to the new probe first. If the **call fallback instantaneous-value-weight** command is configured with the default *weight* of 66(%), the new probe is given a higher value than the earlier one in calculating the average for the new cache entry.

Examples	The following example specifies a fall back value weight of 50 percent:

```
call fallback instantaneous-value-weight 50
```


Related Commands	Command	Description
	call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
	show call fallback config	Displays the call fallback configuration.

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*

Syntax Description	<i>number-of-packets</i>	Specifies the number of packets value. The valid range is from 2 to 50.

Defaults	15 packets

Command Modes	Global configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the MC3810 multiservice concentrator.

Usage Guidelines	A jitter probe, consisting of 2 to 50 packets, details the conditions of the network. More than one packet is used by the probe to calculate an average of delay and loss or Impairment/Calculated Planning Impairment Factor (ICPIF). After the packets return to the probe, the probe delivers the traffic information to the cache, where it is logged for call acceptance or denial. Use the call fallback threshold delay loss or call fallback threshold icpif command to set the threshold parameters. To get a more realistic estimate of the network congestion, increase the number of packets. More probing packets give better estimates of network conditions, but also negatively affect the bandwidth for other network operations. Use fewer packets when you need to focus on bandwidth.

Examples	The following example specifies 20 packets for jitter: <pre>call fallback jitter-probe num-packets 20</pre> If the call fallback command has been enabled before configuring the number of jitter-probe packets, the output is as follows: <pre>call fallback jitter-probe num-packets 20</pre> The new num-packets will take effect only for new probes

Related Commands	Command	Description
	call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
	call fallback jitter-probe precedence	Specifies the jitter-probe precedence.
	call fallback jitter-probe priority-queue	Assigns a priority queue for jitter-probe transmissions.
	show call fallback config	Displays the call fallback configuration.

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*

Syntax Description	<i>precedence-value</i>	Specifies the jitter-probe precedence. The valid range is from 0 to 6.

Defaults	Precedence of 2

Command Modes	Global configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the MC3810 multiservice concentrator.

Usage Guidelines	In every IP packet, there is a precedence header. Precedence is used by various queueing mechanisms in different companies' routers to determine the priority of allowing traffic through the system.
	Use the call fallback jitter-probe precedence command if there are different queueing mechanisms in your network. Enabling the call fallback jitter-probe precedence command sets the precedence for jitter probes to pass through your network.
	If you require your probes to be sent and returned quickly, set the <i>precedence</i> to a low number (zero or one): the lower the precedence, the higher the priority given.

Examples	The following example specifies a jitter-probe precedence of 5, or low priority:

```
call fallback jitter-probe precedence 5
```

Related Commands	Command	Description
	call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
	call fallback jitter-probe num-packets	Specifies the number of packets in a jitter probe used to determine network conditions.
	call fallback jitter-probe priority-queue	Assigns a priority queue for jitter-probe transmissions.
	show call fallback config	Displays the call fallback configuration.

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

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the MC3810 multiservice concentrator.

Usage Guidelines

This command is applicable only if the queueing method used is IP RTP Priority. This command is unnecessary when low latency queueing (LLQ) is used because these packets follow the priority queue path (or not) based on the LLQ classification criteria and not this command.

The command works by choosing between sending the probe on an odd or even RTP port number. The Service Assurance Agent (SAA) probe packets go out on randomly selected ports chosen from within the top end of the audio User Datagram Protocol (UDP) defined port range (16384–32767). The port pair (Real-Time Transport Protocol [RTP] & Real-Time Transport Control Protocol [RTCP] port) is selected, and, by default, SAA probes for call fallback use the RTCP port (odd) to avoid going into the priority queue, if enabled. If call fallback is configured to use the priority queue, the RTP port (even) is selected.

Examples

The following example specifies the setting of the **call fallback jitter-probe priority queue** command:

```
call fallback jitter-probe priority-queue
```

Warning: In order for this command to have any affect on the probes, IP priority queueing must be set for UDP voice ports 16384–32767.

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback jitter-probe num-packets	Specifies the number of packets in a jitter probe used to determine network conditions.

Command	Description
call fallback jitter-probe precedence	Specifies the jitter-probe precedence.
ip rtp priority	Provides a strict priority queueing scheme for delay-sensitive data.
show call fallback config	Displays the call fallback configuration.

call fallback key-chain

To specify use of Message Digest 5 (MD5) authentication for sending and receiving Service Assurance Agent (SAA) 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*

Syntax Description	<i>name-of-chain</i>	Specifies the name of the chain. This line is to be alphanumeric and case-sensitive text.

Defaults	No call fallback key chain is defined.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the MC3810 multiservice concentrator.

Usage Guidelines	This command is used to enable Service Assurance Agent (SAA) probe authentication using MD5. If authentication is used, the keys on the sender and receiver routers must match.

Examples	The following example specifies “secret” as the fall back key chain: <pre>call fallback key-chain secret</pre>

Related Commands	Command	Description
	call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
	key chain	Enables authentication for routing protocols by identifying a group of authentication keys.
	key-string	Specifies the authentication string for a key.
	show call fallback config	Displays the call fallback configuration.

call fallback map target address-list

To configure the call fallback router to keep a cache table by IP addresses of distances for several destination peers sitting behind the router, use the **call fallback map target 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.
target <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.

Defaults

No call fallback maps are defined.

Command Modes

Global configuration

Command History

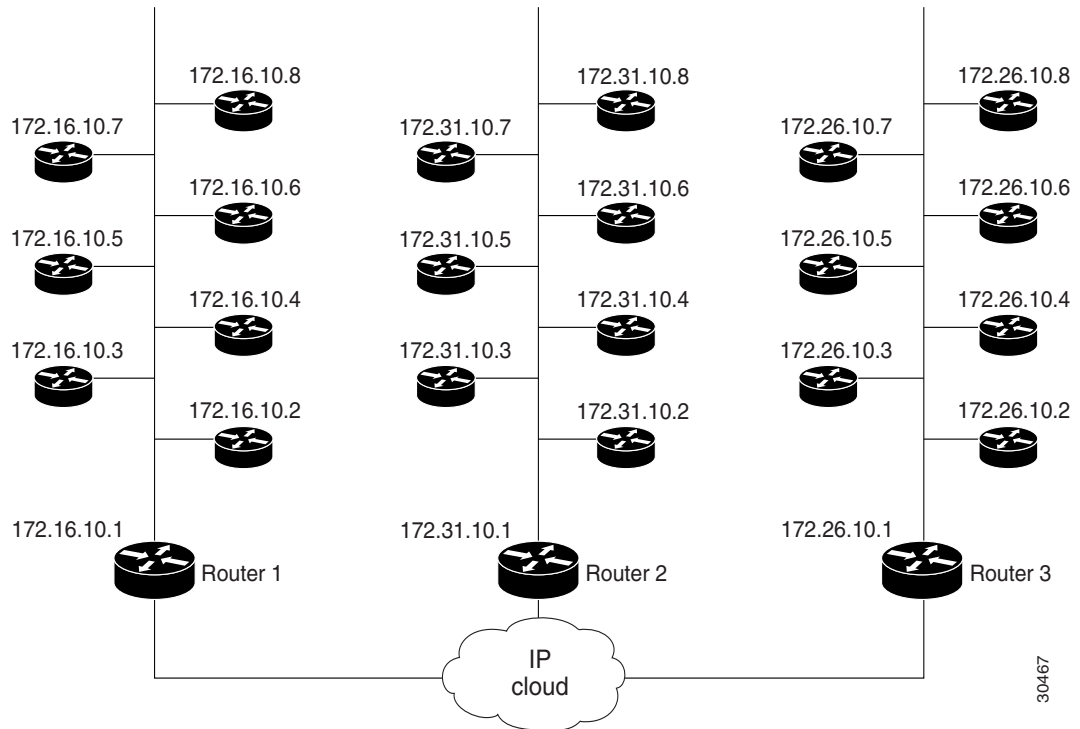
Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the MC3810 multiservice concentrator.

Usage Guidelines

Use this command when several destination peers are connected to a single access point.

Call fallback map setup allows the decongestion of traffic caused by a high volume of call probes sent across a network to query a large number of dial peers. One router/common node can keep the distances in a cache table to numerous IP addresses or destination peers in a network. When the fall back is queried for network congestion to a particular IP address (that is, the common node), the map addresses are searched to find the target IP address. If a match is determined, the probes are sent to the target address rather than to the particular IP address.

In [Figure 2](#), the three routers (1, 2, and 3) keep the cache tables of distances for the destination peers behind them. When a call probe comes from somewhere in the IP cloud, the cache routers check their distance tables for the IP address or destination peer where the call probe is destined. This distance checking limits congestion on the networks behind these routers by directing the probe to the particular IP address and not to the entire network.

Figure 2 Call Fallback Map with IP Addresses

30467

Examples

The following example specifies **call fallback map target address-list** configurations for 172.31.10.1 and 172.26.10.1:

```
call fallback map 1 target 172.31.10.1
address-list 172.31.10.2 172.31.10.3 172.31.10.4 172.31.10.5
172.31.10.6 172.31.10.7 172.31.10.8
call fallback map 2 target 172.26.10.1
address-list 172.26.10.2 172.26.10.3 172.26.10.4 172.26.10.5
172.26.10.6 172.26.10.7 172.26.10.8
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback map target subnet	Specifies the call fallback router to keep a cache table (by subnet addresses) of distances for several destination peers sitting behind the router.
show call fallback config	Displays the call fallback configuration.

call fallback map target subnet

To configure the call fallback router to keep a cache table by subnet addresses of distances for several destination peers sitting behind the router, use the **call fallback map target 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.
target <i>ip-address</i>	Specifies the target IP address.
subnet <i>ip-network</i>	Specifies the subnet IP address.
<i>netmask</i>	Specifies the network mask number.

Defaults

No call fallback maps are defined.

Command Modes

Global configuration

Command History

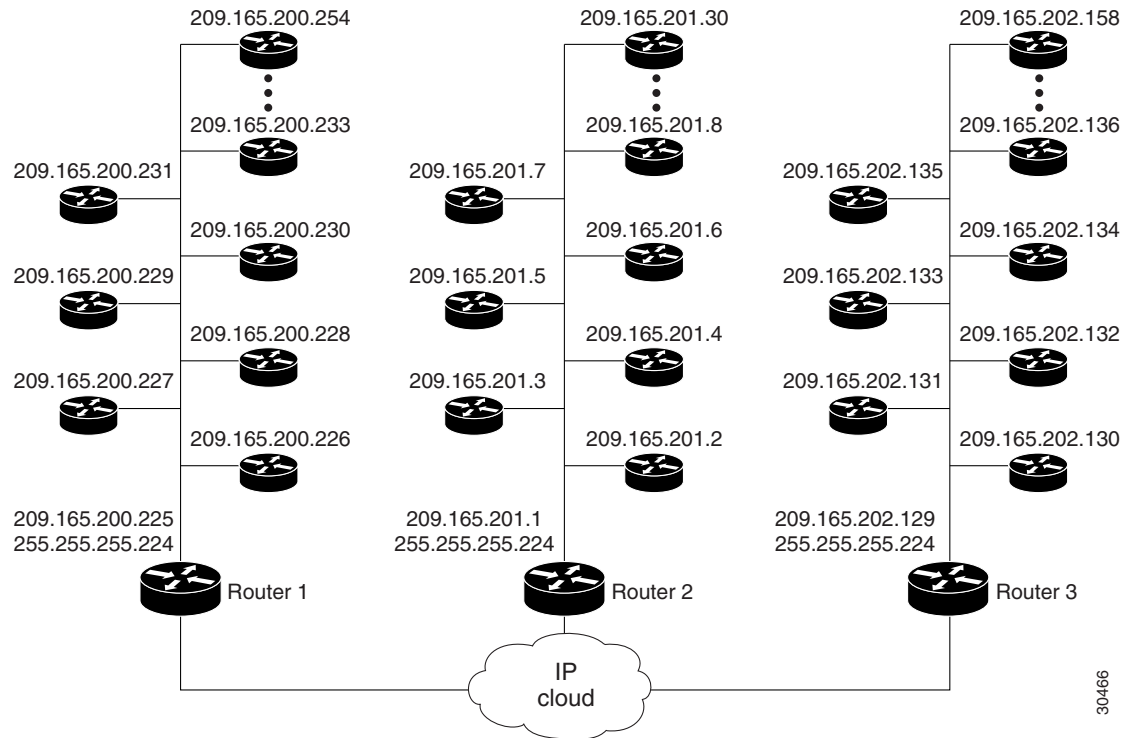
Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the MC3810 multiservice concentrator.

Usage Guidelines

Use this command when several destination peers are sitting behind one common node.

call fallback map setup allows the decongestion of traffic caused by a high volume of call probes sent across a network to query a large number of dial peers. One router/common node can keep the distances in a cache table to numerous IP addresses within a subnet (destination peers) in a network. When the fall back is queried for network congestion to a particular IP address (that is, the common node), the map addresses are searched to find the target IP address. If a match is determined, the probes are sent to the target address rather than to the particular IP address.

In [Figure 3](#), the three routers (1, 2, and 3) keep the cache tables of distances for the destination peers behind them. When a call probe comes from somewhere in the IP cloud, the cache routers check their distance tables for the subnet address/destination peer where the call probe is destined. This distance checking limits congestion on the networks behind these routers by directing the probe to the particular subnet address and not to the entire network.

Figure 3 Call Fallback Map with Subnet Addresses**Examples**

The following example specifies the **call fallback map target subnet** command configuration for 209.165.201.225:

```
call fall back map 1 209.165.201.225 subnet
 209.165.201.224 255.255.255.224
call fall back map 2 209.165.202.225 subnet
 209.165.202.224 255.255.255.224
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback map target address-list	Specifies the call fallback router to keep a cache table (by IP addresses) of distances for several destination peers sitting behind the router.
show call fallback config	Displays the call fallback configuration.

call fallback monitor

To enable the monitoring of destinations with no provision for call fallback to alternate dial peers, use the **call fallback monitor** command in global configuration mode. To disable monitoring without fallback, use the **no** form of this command.

call fallback monitor

no call fallback monitor

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default.

Command Modes Global configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the MC3810 multiservice concentrator.

Usage Guidelines The **call fallback monitor** command is used as a statistics collector of network conditions based on probes (detailing network traffic) and connected calls. There is no H.323 call checking and rejecting as with the **call fallback active** command. All call requests are granted, regardless of network traffic conditions.

Configure the **call fallback threshold delay loss** or **call fallback threshold icpif** command to set threshold parameters. The thresholds are ignored, but for statistics collecting, configuring one of the thresholds allows you to monitor cache entries for either delay and loss or Impairment/Calculated Planning Impairment Factor (ICPIF) values.

Examples The following example shows that the **call fallback monitor** command has been enabled:

```
call fallback monitor
```

Related Commands	Command	Description
	show call fallback config	Displays the call fallback configuration.

call fallback probe-timeout

To set the timeout for a Service Assurance Agent (SAA) probe for call fallback 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.

Defaults	30 seconds

Command Modes	Global configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the MC3810.

Usage Guidelines	SAA probes collect network traffic information based on configured delay and loss or Impairment/Calculated Planning Impairment Factor (ICPIF) values and report this information to the cache for call request determinations. Use the call fallback threshold delay loss or call fallback threshold icpif command to set the threshold parameters. When the probe timeout expires, a new probe is sent to collect network statistics. To reduce the bandwidth taken up by the probes, increase the probe-timeout interval (<i>seconds</i>). Probes do not have a great affect upon bandwidth unless several thousand destinations are involved. If this is the case in your network, use a longer timeout. If you need more network traffic information and bandwidth is not an issue, use a lower timeout. The default interval, 30 seconds, is a low timeout. When the call fallback cache-timeout command is configured or expires, new probes are initiated for data collection.

Examples	The following example configures a 120-second interval: <pre>call fallback probe-timeout 120</pre>

Related Commands	Command	Description
	call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
	show call fallback config	Displays the call fallback configuration.

call fallback threshold delay loss

To configure the call fallback 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.

Defaults There are no values set for delay and loss by default.

Command Modes Global configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the MC3810 multiservice concentrator.

Usage Guidelines For voice traffic, delays and loss of voice packets create unhappy customers. During times of heavy voice traffic, two parties in a conversation may notice a significant delay in transmission or hear only part of a conversation due to loss of voice packets.

Use the **call fallback threshold delay loss** command to configure parameters for voice quality. Lower values of delay and loss allow higher quality of voice. Call requests match the network information in the cache with the configured thresholds of delay and loss. If you enable **call fallback active**, the call fallback subsystem uses the last cache entry compared with the configured delay and loss threshold to determine whether the call is connected or denied. If you enable **call fallback monitor**, all calls are connected, regardless of the configured threshold or voice quality. In this case, configuring the **call fallback threshold delay loss** command allows you to collect network statistics for further tracking.



Note The **call fallback threshold delay loss** command differs from the **call fallback threshold icpif** command because the **call fallback threshold delay loss** command uses only packet delay and loss parameters. The **call fallback threshold icpif** command uses packet delay and loss plus other ITU G.113 factors to gather impairment information.

Setting this command does not affect bandwidth. Available bandwidth for call requests is determined by the call fallback subsystem using probes. The number of probes on the network affects bandwidth.

Examples

The following example configures a threshold delay of 20 milliseconds and a threshold loss of 50 percent:

```
call fallback threshold delay 20 loss 50
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback threshold icpif	Specifies the ICPIF threshold.
show call fallback config	Displays the call fallback configuration.

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.
Defaults	ICPIF threshold of 5	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the MC3810 multiservice concentrator.

Usage Guidelines

During times of heavy voice traffic, two parties in a conversation may notice a significant delay in transmission or hear only part of a conversation because of loss of voice packets.

Use the **call fallback threshold icpif** command to configure parameters for voice quality. A low ICPIF value allows for higher quality of voice. Call requests match the network information in the cache with the configured ICPIF threshold. If you enable the **call fallback active** command, the call fallback subsystem uses the last cache entry compared with the configured ICPIF threshold to determine whether the call is connected or denied. If you enable the **call fallback monitor** command, all calls are connected regardless of the configured threshold or voice quality. In this case, configuring the **call fallback threshold icpif** command allows you to collect network statistics for further tracking.

A lower value of ICPIF tolerates less delay and loss (according to ICPIF calculations) of voice packets. Use lower values for higher quality of voice. Configuring a value of 34 equates to 100 percent packet loss.

The ICPIF is calculated and used according to the International Telecommunication Union (ITU) G.113 specifications.



Note

The **call fallback threshold delay loss** command differs from the **call fallback threshold icpif** command because the **call fallback threshold delay loss** command uses only packet delay and loss parameters. The **call fallback threshold icpif** command uses packet delay and loss plus other ITU G.113 factors to gather impairment information.

Setting this command does not affect bandwidth. Available bandwidth for call requests is determined by the call fallback subsystem using probes. The number of probes on the network affect bandwidth.

Examples

The following example sets the ICPIF threshold to 20:

```
call fallback threshold icpif 20
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback threshold delay loss	Specifies the call fallback threshold delay and loss values.
show call fallback config	Displays the call fallback configuration.

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.

Defaults

Synchronization is enabled between RSVP and the voice signaling protocol (for example, H.323).

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco 2600 series routers, 3600 series, and 7200 series and on the AS5300, AS5800, and MC3810.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

The **call rsvp-sync** command is enabled by default.

Examples

The following example enables synchronization between RSVP and the voice signaling protocol:

```
call rsvp-sync
```

Related Commands

Command	Description
call rsvp-sync resv-timer	Sets the timer for reservation requests.
call start	Forces the H.323 Version 2 gateway to use fast connect or slow connect procedures for a dial peer.
debug call rsvp-sync events	Displays the events that occur during RSVP synchronization.
h323 call start	Forces an H.323 Version 2 gateway to use fast connect or slow connect procedures for all VoIP services.
ip rsvp bandwidth	Enables the use of RSVP on an interface.
show call rsvp-sync conf	Displays the RSVP synchronization configuration.
show call rsvp-sync stats	Displays statistics for calls that have attempted RSVP reservation.

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

Syntax Description	<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.

Defaults	The timer default is 10 seconds.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(3)XI	This command was introduced on the Cisco 2600 series routers, 3600 series, and 7200 series and on the AS5300, AS5800, and MC3810.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines	The reservation timer is started on the terminating gateway when the session protocol receives an indication of the incoming call. This timer is not set on the originating gateway because the resource reservation is confirmed at the terminating gateway. If the reservation timer expires before the RSVP setup is complete, the outcome of the call depends on the acceptable quality of service (QoS) level configured in the dial peer; either the call proceeds without any bandwidth reservation or it is released. The timer must be set long enough to allow calls to complete but short enough to free up resources. The optimum number of seconds depends on the number of hops between the participating gateways and the delay characteristics of the network.

Examples	The following example sets the reservation timer to 30 seconds: call rsvp-sync resv-timer 30

Related Commands	Command	Description
	call rsvp-sync	Enables synchronization of RSVP and the H.323 voice signaling protocol.
	debug call rsvp-sync events	Displays the events that occur during RSVP synchronization.
	show call rsvp-sync conf	Displays the RSVP synchronization configuration.
	show call rsvp-sync stats	Displays statistics for calls that have attempted RSVP reservation.

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

Syntax Description

fast	Gateway uses H.323 Version 2 (fast connect) procedures.
slow	Gateway uses H.323 Version 1 (slow connect) procedures.
system	Gateway defaults to the voice service configuration that is defined using the h323 call start command in voice-service configuration mode.

Defaults

The default is **system**.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco 2600 series routers, 3600 series, and 7200 series and on the AS5300, AS5800, and MC3810.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

In Cisco IOS Release 12.1(3)XI and later, H.323 Voice over IP (VoIP) gateways by default use H.323 Version 2 (fast connect) for all calls, including those initiating RSVP. Previously, gateways used only slow connect procedures for RSVP calls. To enable Cisco IOS Release 12.1(3)XI gateways to be backward compatible with earlier releases of Cisco IOS Release 12.1 T, the **call start** command allows the originating gateway to initiate calls using slow connect.

The **call start** command is configured as part of the voice class assigned to an individual VoIP dial peer. It takes precedence over the **h323 call start** voice-service configuration command, which applies globally to all VoIP calls, unless the **system** keyword is selected. If the **system** keyword is used for the **call start** voice-class command, the gateway defaults to the voice-service configuration.

Examples

The following example selects slow connect for voice class 1000:

```
voice class h323 1000
  call start slow
!
dial-peer voice 210 voip
  voice-class h323 1000
```

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

Syntax Description	This command has no arguments or keywords.

Defaults	Call waiting is enabled.

Command Modes	Interface configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced on the Cisco 800 series.

Usage Guidelines	This command is applicable to Cisco 800 series routers. You must specify this command when creating a dial peer. This command will not work if it is not specified within the context of a dial peer. For information on creating a dial peer, refer to the <i>Cisco 800 Series Routers Software Configuration Guide</i>.

Examples	The following example disables call waiting: <pre>no call-waiting</pre>

Related Commands	Command	Description
	destination-pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
	dial peer voice	Enters dial peer configuration mode, defines the type of dial peer, and defines the tag number associated with a dial peer.
	port (dial peer)	Enables an interface on a PA-4R-DTR port adapter to operate as a concentrator port.
	ring	Sets up a distinctive ring for telephones, fax machines, or modems connected to a Cisco 800 series router.
	show dial peer voice	Displays configuration information and call statistics for dial peers.

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.

Defaults	This command is disabled.

Command Modes	Dial peer configuration

Command History	Release	Modification
	12.0(4)T	This command was introduced on the Cisco 2600 and 3600 series.

Usage Guidelines	This command applies to the Cisco 2600 and 3600 series routers only. It is ignored on the Cisco MC3810 multiservice concentrator and on the Cisco 7200 series routers.

The **called-number** command is used only when the dial peer type is VoFR and you are using the frf11-trunk (FRF.11) session protocol. It is ignored at all times on the Cisco MC3810 multiservice concentrator and on all other platforms when using the Cisco-switched session protocol.

Because FRF.11 does not provide any end-to-end messaging to manage a trunk, the **called-number** command is necessary to allow the router to establish an incoming trunk connection. The E.164 number is used to find a matching dial peer during call setup.

Examples	The following example shows how to configure a Cisco 2600 series routers or 3600 series router for a static FRF.11 trunk connection to a specific telephone number (555-2150), beginning in global configuration mode:

```
voice-port 1/0/0
 connection trunk 55Router0
 exit

dial-peer voice 100 pots
 destination pattern 5552150
 exit

dial-peer voice 200 vofr
 session protocol frf11-trunk
```

```
called-number 5552150
destination pattern 55Router0
```

Related Commands

Command	Description
codec (dial peer)	Specifies the voice coder rate of speech for a VoFR dial peer.
connection	Specifies a connection mode for a voice port.
destination-pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dtmf-relay (VoFR)	Enables the generation of FRF.11 Annex A frames for a dial peer.
fax-rate	Establishes the rate at which a fax will be sent to the specified dial peer.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.
session protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
vad (dial peer)	Enables voice-activated dialing (VAD) for the calls using a particular 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 contains no arguments or keywords.

Defaults	Caller ID is disabled.

Command Modes	Dial peer configuration

Command History	Release	Modification
	12.1(2)XF	This command was introduced on the Cisco 800 series routers.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines	This command is available on Cisco 800 series routers that have plain old telephone service (POTS) ports. The command is effective only if you subscribe to caller ID service. If you enable caller ID on a router without subscribing to the caller ID service, caller ID information does not appear on the telephone display.

The configuration of caller ID must match the device connected to the POTS port. That is, if a telephone supports the caller ID feature, use the command **caller-id** to enable the feature. If the telephone does not support the caller ID feature, use the command default or disable the caller ID feature. Odd ringing behavior might occur if the caller ID feature is disabled when it is a supported telephone feature or enabled when it is not a supported telephone feature.



Note	Specific hardware is required to provide full support for the Caller ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on Cisco.com.

Examples	The following example enables a router to use the caller ID feature:

```
dial-peer voice 1 pots
caller-id
```


Related Commands	Command	Description
	block-caller	Configures call blocking on caller ID.
	debug pots csm csm	Activates events from which an application can determine and display the status and progress of calls to and from POTS ports.
	isdn i-number	Configures several terminal devices to use one subscriber line.
	pots call-waiting	Enables local call waiting on a router.
	registered-caller ring	Configures the Nariwake service-registered caller ring cadence.

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 contains no keywords or arguments.

Defaults No pre-allocation of DSP resources

Command Modes Voice-port configuration

Command History	Release	Modification
	12.1(2)XH	This command was implemented for the Cisco MC3810 multiservice concentrator and for Cisco 2600 and 3600 series routers.
	12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines The **caller-id alerting dsp-pre-alloc** command may be required on an FXO port if the central office uses line polarity reversal to signal the start of Caller-ID information transmission. Pre-allocating a DSP allows the DSP to listen for Caller-ID information continuously without requiring an alerting signal from the CO.

This command is the FXO counterpart to the **caller-id alerting line-reversal** command, which is applied to the Foreign Exchange Station (sending) end of the Caller-ID call.

This command applies to the Cisco MC3810 multiservice concentrator and to Cisco 2600 and 3600 series routers.



Note Specific hardware is required to provide full support for the Caller ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on Cisco.com.

Examples The following example configures a voice port on a Cisco 2600 or 3600 router where Caller-ID information is received:

```
voice-port 1/0/1
 cptone US
 caller-id enable
 caller-id alerting line-reversal
```

```
caller-id alerting dsp-pre-alloc
```

The following example configures a voice port on a Cisco MC3810 multiservice concentrator where Caller-ID information is received:

```
voice-port 1/0
  cptone northamerica
  caller-id enable
  caller-id alerting line-reversal
  caller-id alerting dsp-pre-alloc
```

Related Commands

Command	Description
caller-id alerting line-reversal	Sets the line-reversal method of Caller-ID call alerting.

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.

Defaults No line-reversal alert

Command Modes Voice-port configuration

Command History	Release	Modification
	12.1(2)XH	This command was implemented for the Cisco MC3810 multiservice concentrator and for Cisco 2600 and 3600 series routers.
	12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines This command is only required when the telephone device attached to an FXS port requires the line-reversal method to signal the start of a Caller-ID transmission. Use it on FXS voice ports that send Caller-ID information.

This command is the FXS counterpart to the **caller-id alerting dsp-pre-alloc** command, which is applied to the FXO (receiving) end of the Caller-ID call with the line-reversal alerting method.

This command applies to the Cisco MC3810 multiservice concentrator and to Cisco 2600 and 3600 series routers.



Note Specific hardware is required to provide full support for the Caller ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on Cisco.com.

Examples The following example configures a voice port on a Cisco 2600 or 3600 series router from which Caller-ID information is sent:

```
voice-port 1/0/1
  cptone US
  station name A. Person
  station number 4085551111
  caller-id alerting line-reversal
  caller-id alerting dsp-pre-alloc
```

The following example configures a voice port on a Cisco MC3810 multiservice concentrator from which Caller-ID information is sent:

```
voice-port 1/0
  cptone northamerica
  station name A. Person
  station number 4085551111
  caller-id alerting line-reversal
  caller-id alerting dsp-pre-alloc
```

Related Commands

Command	Description
caller-id alerting dsp-pre-alloc	At the receiving end of a line-reversal alerting Caller-ID call, pre-allocates DSPs for caller ID calls.

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 keywords or arguments.

Defaults No pre-ring alert

Command Modes Voice-port configuration

Command History

Release	Modification
12.1(2)XH	This command was implemented for the Cisco MC3810 multiservice concentrator and for Cisco 2600 and 3600 series routers.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

This command is required only when the telephone device attached to an FXS port requires the pre-ring (immediate ring) method to signal the start of caller ID transmission. Use it on FXS voice ports that send caller ID information. This command allows the FXS port to send a short pre-ring preceding the normal ring cadence. On an FXO port, an incoming pre-ring (immediate ring) is simply counted as a normal ring using the **caller-id alerting ring** command.

This command applies to the Cisco MC3810 multiservice concentrator and to Cisco 2600 and 3600 series routers.



Note Specific hardware is required to provide full support for the Caller ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on Cisco.com.

Examples

The following example configures a voice port on a Cisco 2600 or 3600 series router from which caller ID information is sent:

```
voice-port 1/0/1
  cptone US
  station name A. Person
  station number 4085551111
  caller-id alerting pre-ring
```

The following example configures a voice port on a Cisco MC3810 multiservice concentrator from which caller ID information is sent:

```
voice-port 1/0
  cptone northamerica
  station name A. Person
  station number 4085551111
  caller-id alerting pre-ring 1
```

Related Commands	Command	Description
	caller-id alerting line-reversal	Enables caller ID operation and sets the line-reversal alerting type at an FXS port.
	caller-id alerting ring	Enables caller ID operation and sets an alerting ring type at an FXO or FXS port.

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).

Defaults

The default value is 1.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(2)XH	This command was implemented for the Cisco MC3810 multiservice concentrator and for Cisco 2600 and 3600 series routers.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

This setting is determined by the Bellcore/Telcordia or ETSI standard that your telephone service provider uses for caller ID. Use it on FXO loop-start and ground-start voice ports where caller ID information arrives and on FXS voice ports from which caller ID information is sent.

This setting must match on the sending and receiving ends on both ends of the telephone line connection.

This command applies to the Cisco MC3810 multiservice concentrator and to Cisco 2600 and 3600 series routers.



Note

Specific hardware is required to provide full support for the Caller ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on Cisco.com.

Examples

The following example configures a Cisco 2600 or 3600 series router voice port where caller ID information is received:

```
voice-port 1/0/1
  cptone US
  caller-id alerting ring 1
```

The following example configures a Cisco 2600 or 3600 series router voice port from which caller ID information is sent:

```
voice-port 1/0/1
  cptone northamerica
  station name A. Person
  station number 4085551111
  caller-id alerting ring 1
```

The following example configures a Cisco MC3810 multiservice concentrator voice port where caller ID information is received:

```
voice-port 1/0
  cptone northamerica
  caller-id alerting ring 1
```

The following example configures a Cisco MC3810 multiservice concentrator voice port from which caller ID information is sent:

```
voice-port 1/0
  cptone northamerica
  station name A. Person
  station number 4085551111
  caller-id alerting ring 1
```

Related Commands

Command	Description
caller-id alerting line-reversal	Enables caller ID operation and sets the line-reversal alerting type at an FXS port.
caller-id alerting pre-ring	Enables caller ID operation and sets the pre-ring alerting method at an FXS port.

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

<i>attenuation</i>	Specifies the attenuation. Valid values are from 0 to 64.

Defaults

The default value is 14 decibels (dB), signal level of -14 dBm.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(2)XH	This command was implemented for the Cisco MC3810 multiservice concentrator and for Cisco 2600 and 3600 series routers.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

Use this setting to specify the attenuation for a caller ID FXO port. If the setting is not used, the attenuation is set to 14 decibels (dB), signal level of -14 dBm.

This command applies to the Cisco MC3810 multiservice concentrator and to Cisco 2600 and 3600 series routers.



Note

Specific hardware is required to provide full support for the Caller ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on Cisco.com.

Examples

The following example configures a Cisco 2600 or 3600 series router voice port where caller ID information is received:

```
voice-port 1/0/1
  cptone US
  caller-id attenuation 0
```

The following example configures a Cisco MC3810 multiservice concentrator voice port where caller ID information is received:

```
voice-port 1/0
  cptone northamerica
  caller-id attenuation 0
```

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 keywords or arguments.

Defaults	No blocking of caller ID information

Command Modes	Voice-port configuration

Command History	Release	Modification
	12.1(2)XH	This command was implemented for Cisco MC3810 multiservice concentrator and for Cisco 2600 and 3600 series routers.
	12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines	This command is used on FXS voice ports that are used to originate on-net telephone calls. This command affects all calls sent to a far-end FXS station from the configured originating FXS station. Calling number and called number are provided in the H.225 setup message for VoIP, through the H.225 Octet 3A field. Calling name information is included in a display information element.

**Note**

Cisco-switched calls using Voice over Frame Relay (VoFR) and Voice over ATM (VoATM) carry calling party information in the Cisco proprietary setup message. For standards-based, point-to-point VoFR (FRF.11) trunks where transparent signaling is applied for FXS-to-FXO calls, only pass-through of in-band Automatic Number Identification (ANI) is supported. ANI information is always unblocked for these communications. Interface technology using transparent channel associated signaling (CAS) can support only ANI through Feature Group D (in-band MF signaling). The Caller ID feature cannot be used with fixed point-to-point trunk connects created using the **connection trunk** command.

This command applies to the Cisco MC3810 multiservice concentrator and to Cisco 2600 and 3600 series routers.

**Note**

Specific hardware is required to provide full support for the Caller ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on Cisco.com.

Examples

The following example configures a Cisco 2600 or 3600 series router voice port from which caller ID information is sent:

```
voice-port 1/0/1
  cptone US
  station name A. Person
  station number 4085551111
  caller-id block
```

The following example configures a Cisco MC3810 multiservice concentrator voice port from which caller ID information is sent:

```
voice-port 1/0
  cptone northamerica
  station name A. Person
  station number 4085551111
  caller-id block
```

Related Commands

Command	Description
caller-id enable	Enables caller ID operation.

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 keywords or arguments.

Defaults

No sending or receiving of caller ID information

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(2)XH	This command was implemented for the Cisco MC3810 multiservice concentrator and for Cisco 2600 and 3600 series routers.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

This command applies to FXS voice ports that send caller ID information and to FXO ports that receive caller ID information. Calling number and called number are provided in the H.225.0 setup message for VoIP, through the H.225.0 Octet 3A field. Calling name information is included in a display information element.



Note

Cisco-switched calls using Voice over Frame Relay (VoFR) and Voice over ATM (VoATM) carry calling party information in the Cisco proprietary setup message. For standards-based, point-to-point VoFR (FRF.11) trunks where transparent signaling is applied for FXS-to-FXO calls, only pass-through of in-band Automatic Number Identification (ANI) is supported. ANI information is always unblocked for these communications. Interface technology using transparent channel associated signaling (CAS) can support only ANI through Feature Group D (in-band MF signaling). The Caller ID feature cannot be used with fixed point-to-point trunk connects created using the **connection trunk** command.

If the **station name**, **station number**, or a **caller-id alerting** command is configured on the voice port, these automatically enable caller ID, and the **caller-id enable** command is not necessary.

This command applies to the Cisco MC3810 multiservice concentrator and to Cisco 2600 and 3600 series routers.

**Note**

Specific hardware is required to provide full support for the Caller ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on Cisco.com.

Examples

The following example configures a Cisco 2600 or 3600 series router voice port where caller ID information is received:

```
voice-port 1/0/1
  cptone US
  caller-id enable
```

The following example configures a Cisco 2600 or 3600 series router voice port from which caller ID information is sent:

```
voice-port 1/0/1
  cptone northamerica
  station name A. Person
  station number 4085551111
  caller-id enable
```

The following example configures a Cisco MC3810 multiservice concentrator voice port where caller ID information is received:

```
voice-port 1/0
  cptone northamerica
  caller-id enable
```

The following example configures a Cisco MC3810 multiservice concentrator voice port from which caller ID information is sent:

```
voice-port 1/0
  cptone northamerica
  station name A. Person
  station number 4085551111
  caller-id enable
```

Related Commands

Command	Description
caller-id alerting line-reversal	Enables caller ID operation and sets the line-reversal alerting type at an FXS port.
caller-id alerting pre-ring	Enables caller ID operation and sets the pre-ring alerting method at an FXS port.
caller-id alerting ring	Enables caller ID operation and sets an alerting ring type at an FXO or FXS port.
caller-id block	Disables the sending of caller ID information from an FXS port.
station name	Enables caller ID operation and sets the name sent from an FXS port.
station number	Enables caller ID operation and sets the number sent from an FXS port.

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	range	Generates the sequence of ANI by rotating through the specified range (<i>string1</i> to <i>string2</i>).
	sequence	Configures a sequence of discrete strings (<i>string1... string5</i>) to be passed out as ANI for successive calls using the peer.
	null	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.

Defaults No outbound calling number is specified.

Command Modes Dial peer configuration
Voice-port configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines This command is effective only for Feature Group D-Exchange Access North American (FGD-EANA) signaling.

Examples Use the **calling-number outbound** command to enable or disable the passing of ANI on T1-CAS FGD-EANA configured T1 interface for outgoing calls. Syntax for this command is the same for both voice-port mode and dial peer mode. Examples are given for both modes.

calling-number outbound Range

calling-number outbound range *string1 string2*

The values *string1* and *string2* are valid E.164 telephone number strings. Both strings must be of the same length and cannot be more than 32 digits long. Only the last four digits are used for specifying the range (*string1* to *string2*) and for generating the sequence of ANI by rotating through the range until *string2* is reached and then starting from *string1* again. If strings are less than four digits in length, then entire strings will be used.

ANI will be generated by using the 408555 prefix and by rotating through 6000 to 6001 for each call using this peer.

Dial peer configuration mode:

```
dial-peer voice 1 pots
calling-number outbound range 4085556000 4085556001
calling Number Outbound is effective only for fgd_eana signaling
```

Voice-port configuration mode:

```
voice-port 1:D
calling-number outbound range 4085556000 4085556005
Calling Number Outbound is effective only for fgd_eana signaling
```

calling-number outbound Sequence

```
calling-number outbound sequence string1 string2 string3
string4 string5
```

This option configures a sequence of discrete strings (*string1...string5*) to be passed out as ANI for successive calls using the peer. The limit is five strings. All strings must be valid E.164 numbers, up to 32 digits in length.

Dial peer configuration mode:

```
dial-peer voice 1 pots
calling-number outbound sequence 6000 6006 4000 5000 5025
Calling Number Outbound is effective only for fgd_eana signaling
```

Voice-port configuration mode:

```
voice-port 1:D
calling-number outbound sequence 6000 6006 4000 5000 5025
Calling Number Outbound is effective only for fgd_eana signaling
```

calling-number outbound Null

```
calling-number outbound null
```

This option suppresses ANI. If used, no ANI will be passed when this dial peer is selected.

Dial peer configuration mode:

```
dial-peer voice 1 pots
calling-number outbound null
Calling Number Outbound is effective only for fgd_eana signaling
```

Voice-port configuration mode:

```
voice-port 1:D
calling-number outbound null
Calling Number Outbound is effective only for fgd_eana signaling
```

Related Commands

Command	Description
info-digits string1	Configures two information digits to be prepended to the ANI string.

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.

Defaults	No default behavior or values.

Command Modes	Global configuration

Command History	Release	Modification
	11.3 NA	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines	When VCWare is unbundled, it automatically adds DSPWare to Flash memory, creates both the capability and default file lists, and populates these lists with the default files for the particular version of VCWare. The capability list defines the available voice codecs for H.323 capability negotiation. Use the cap-list vfc command to add the indicated voice codec overlay file (defined by <i>filename</i>) to the capability file list in Flash memory.

Examples	The following example adds the following codec to the list included in Flash memory:

```
config terminal
cap-list cdc-g711-1.0.14.0.bin vfc 0
```

Related Commands	Command	Description
	default-file vfc	Specifies an additional (or different) file from the ones in the default file list and stored in VFC Flash memory.

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

t1	Specifies T1 connectivity of 1.544 Mbps through the telephone switching network, using AMI or B8ZS coding.
e1	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).

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Examples

The following example configures T1 data transmission on port 1 on the Cisco 7200 series routers router:

```
card type t1 1/0
```

ccm-manager application redundant-link port

To configure the port number for the redundant link application, use the **ccm-manager application redundant-link port** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ccm-manager application redundant-link port *number*

no ccm-manager application

Syntax Description

<i>number</i>	Port number for the transport protocol. The protocol may be the User Data Protocol (UDP), Reliable User Datagram Protocol (RDUP), or Transmission Control Protocol (TCP). Permitted values are from 0 to 65535, and it must not be a well-known reserved port number.

Defaults

Port 2428

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced with Cisco CallManager Version 3.0 and the Cisco Voice Gateway 200 (VG200).
12.2(2)XA	The command was implemented on Cisco 2600 series and Cisco 3600 series.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T.

Usage Guidelines

This command is optional. Use this command only when defining an application-specific port other than the default.

Examples

In the following example, the port number of the redundant link application is 2429:

```
ccm-manager application redundant-link port 2429
```

Related Commands

Command	Description
ccm-manager redundant-host	Configures the IP address or the DNS name of up to two backup Cisco CallManagers.
ccm-manager switchback	Configures the switchback mode that determines when the primary Cisco CallManager will be used if it becomes available again while a backup Cisco CallManager is being used.

ccm-manager mgcp

To allow a gateway to communicate with the Cisco CallManager by means of Media Gateway Control Protocol (MGCP) and supply redundant services, use the **ccm-manager mgcp** command in global configuration mode. To disable this command, use the **no** form of this command.

ccm-manager mgcp

no ccm-manager mgcp

Syntax Description

This command has no arguments or keywords.

Defaults

Cisco CallManager does not communicate with the gateway through MGCP

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced with Cisco CallManager Version 3.0 and the Cisco Voice Gateway 200 (VG200).
12.2(2)XA	The command was implemented on Cisco 2600 series and Cisco 3600 series routers.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T.

Usage Guidelines

This command sets the gateway to MGCP mode. In MGCP mode, the gateway can communicate with the Cisco CallManager through MGCP, and it can enable redundancy when a backup Cisco CallManager is available.

Examples

In the following example, support for Cisco CallManager and redundancy is enabled within MGCP:

```
ccm-manager mgcp
```

Related Commands

Command	Description
mgcp	Enables Media Gateway Control Protocol mode.
ccm-manager redundant-host	Configures the IP address or the DNS name of up to two backup Cisco CallManagers.
ccm-manager switchback	Configures the switchback mode that determines when the primary Cisco CallManager will be used if it becomes available again while a backup Cisco CallManager is being used.

ccm-manager redundant-host

To configure the IP address or the DNS name of up to two backup Cisco CallManagers, use the **ccm-manager redundant-host** command in global configuration mode. To disable the configuration of a backup Cisco CallManager, use the **no** form of this command.

ccm-manager redundant-host {*ip-address* | *DNS-name*} [*ip-address* | *DNS-name*]

no ccm-manager redundant-host {*ip-address* | *DNS-name*} [*ip-address* | *DNS-name*]

Syntax Description

<i>ip-address</i>	Internet protocol address of the backup Cisco CallManager.
<i>DNS-name</i>	Domain name system of the backup Cisco CallManager.

Defaults

If you do not configure a backup Cisco CallManager, the redundancy feature is considered to be off

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced with Cisco CallManager Version 3.0 and the Cisco Voice Gateway 200 (VG200).
12.2(2)XA	The command was implemented on Cisco 2600 series and Cisco 3600 series. The <i>DNS-name</i> argument was added.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T.

Usage Guidelines

You must configure one backup Cisco CallManager, and you can configure a maximum of two backup Cisco CallManagers. The list of IP addresses or DNS names is an ordered list. The Cisco CallManager defined in the **mgcp call-agent** command has the highest priority (that is, it is the primary Cisco CallManager). The gateway selects a Cisco CallManager based on the order in which it appears in this list.

Examples

In the following example, the IP address of the backup Cisco CallManager is 10.0.0.50:

```
ccm-manager redundant-host 10.0.0.50
```

Related Commands

Command	Description
ccm-manager application	Configures the port number for the redundant link application.
ccm-manager switchback	Configures the switchback mode that determines when the primary Cisco CallManager will be used if it becomes available again while a backup Cisco CallManager is being used.

ccm-manager switchback

To specify when to use the primary Cisco CallManager once it becomes available again, use the **ccm-manager switchback** command in global configuration mode. To disable switchback, use the **no** form of this command.

ccm-manager switchback { **graceful** | **immediate** | **schedule-time** *hh:mm* | **uptime-delay** *minutes* }

no ccm-manager switchback

Syntax Description		
graceful		After the last active call ends (when there is no voice call in setup mode on the gateway), control returns to the primary Cisco CallManager.
immediate		Regardless of the current conditions, when the TCP link to the primary Cisco CallManager is established, control switches back immediately to the primary Cisco CallManager.
schedule-time <i>hh:mm</i>		At a specified hour and minute, based on a 24-hour clock, control returns to the primary Cisco CallManager. If the specified time is earlier than the current time, the switchback occurs at the specified time on the following day.
uptime-delay <i>minutes</i>		When the primary Cisco CallManager has run for a specified number of minutes after a network connection has been reestablished to that CallManager, control is returned to the primary Cisco CallManager. Permitted values are from 1 to 1440 (from 1 minute to 24 hours).

Defaults Graceful

Command Modes Global configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced with Cisco CallManager Version 3.0 and the Cisco Voice Gateway 200 (VG200).
	12.2(2)XA	The command was implemented on Cisco 2600 series and Cisco 3600 series routers.
	12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T.

Usage Guidelines This command allows you to configure switchback to the higher priority Cisco CallManager when it becomes available. Switchback allows call control to revert back to the original (primary) Cisco CallManager once service has been restored.

Examples In the following example, the primary Cisco CallManager will be used as soon as it becomes available:

```
ccm-manager switchback immediate
```

ccs connect (interface)

Command	Description
ccm-manager application	Configures the port number for the redundant link application.
ccm-manager redundant-host	Configures the IP address or the DNS name of up to two backup Cisco CallManagers.
ccm-manager switchover-to-backup	Manually redirects a Cisco 2600 series or Cisco 3600 series router to the backup Cisco CallManager.

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

serial	Makes a serial CCS connection for Frame Relay.
atm	Makes an ATM CCS connection for ATM.
<i>dlci</i>	(Optional) Specifies the data link connection identifier (DLCI) number.
pvc vpi/vci	(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.
pvc name	(Optional) Specifies the PVC string that names the PVC for recognition.
<i>cidnumber</i>	(Optional) If you have executed the ccs encap frf11 command, the <i>cidnumber</i> option allows you to specify any channel identification (CID) number from 5 to 255.

Defaults

No CCS connection is made.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(2)T	This command was introduced for the Cisco MC3810 multiservice concentrator.
12.0(7)XK	The CID syntax was added; the dlci keyword and vcd options were removed.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use this command to configure a CCS connection. If the CCS connection is over Frame Relay, specify a serial interface and the DLCI. If the CCS connection is over ATM, specify **atm**, the interface number (0), and the PVC. If you have executed the **ccs encap frf11** command, the *cidnumber* option allows you to specify any CID from 5 to 255. If you do not issue the **ccs encap frf11** command, Cisco encapsulation is used, and any CID value other than 254 is ignored.



Note CDP and keepalives are disabled by default on a D-channel interface.

This configuration is applicable to only the MC3810 multiservice concentrator.

Examples

To configure a frame relay CCS frame-forwarding connection on DLCI 100 by using the default CID of 254, enter the following command:

```
ccs connect serial 1 100
```

or:

```
ccs connect serial 1 100 10
```

To configure a CCS frame-forwarding connection over an ATM PVC, enter the following command:

```
ccs connect atm0 pvc 100/10
```

or:

```
ccs connect atm0 pvc 10/100 21
```

or:

```
ccs connect atm0 pvc mypvc_10 21
```

To configure a Frame Relay CCS frame-forwarding connection on DLCI 100 using a CID of 110, enter the following command:

```
ccs connect serial 1 100 110
```

Related Commands

Command	Description
ccs encap frf11	Allows the specification of the standard Annex-C FRF.11 format.

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

serial	Makes a serial CCS connection for Frame Relay.
atm	Makes an ATM CCS connection.
<i>dlci</i>	(Optional) Specifies the data link connection identifier (DLCI) number.
pvc <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.
pvc name	(Optional) Specifies the PVC string that names the PVC for recognition.
<i>cidnumber</i>	(Optional) If you have executed the ccs encap frf11 command, the <i>cidnumber</i> option allows you to specify any channel identification (CID) number from 5 to 255.

Defaults

No CCS connection is made.

Command Modes

Controller configuration

Command History

Release	Modification
12.0(2)T	This command was introduced for the Cisco MC3810 multiservice concentrator.
12.0(7)XK	The CID syntax was added; the dlci keyword and vcd options were removed.
12.1(2)T	The CID syntax addition and removal of the dlci keyword and vcd options were integrated into Cisco IOS Release 12.1(2)T.
12.1(2)XH	This command was supported on the Cisco 2600 series routers, Cisco 3600 series routers, Cisco 7200 series routers, and Cisco 7500 series routers.
12.1(3)T	Support on the Cisco 2600 series routers, Cisco 3600 series routers, Cisco 7200 series routers, and Cisco 7500 series routers was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

Use this command to configure a CCS connection. If the CCS connection is over Frame Relay, specify a serial interface and the DLCI. If the CCS connection is over ATM, specify **atm**, the slot number (0 only on the Cisco MC3810), and the PVC.

If you have executed the **ccs encap frf11** command, the *cidnumber* option allows you to specify any CID from 5 to 255. If you do not issue the **ccs encap frf11** command, Cisco encapsulation is used, and any CID value other than 254 is ignored.



Note CDP and keepalives are disabled by default on a D-channel interface.

Examples

To configure a Frame Relay CCS frame-forwarding connection on DLCI 100 by using the default CID of 254, enter the following command:

```
ccs connect serial 1 100
```

or:

```
ccs connect serial 1 100 10
```

To configure a CCS frame-forwarding connection over an ATM PVC, enter the following command:

```
ccs connect atm0 pvc 100/10
```

or:

```
ccs connect atm0 pvc 10/100 21
```

or:

```
ccs connect atm0 pvc mypvc_10 21
```

To configure a Frame Relay CCS frame-forwarding connection on DLCI 100 using a CID of 110, enter the following command:

```
ccs connect serial 1 100 110
```

Related Commands

Command	Description
ccs encap frf11	Allows the specification of the standard Annex-C FRF.11 format.

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 keywords or arguments.

Defaults

By default, the format is a Cisco packet format, using a channel ID (CID) of 254.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced for the Cisco MC3810 multiservice concentrator.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(2)XH	This command was supported on the Cisco 2600 series routers, 3600 series, 7200 series, and 7500 series routers.
12.1(3)T	The Cisco 2600 series routers, 3600 series, 7200 series, and 7500 series router support was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

This command allows the specification of the standard Annex-C format. Use this command to define the packet format for the CCS packet; it places the FRF.11 Annex-C (Data Transfer Syntax) standard header on the CCS packets only.

Once the **ccs encap frf11** command is executed, you can use the **ccs connect** command to specify a CID other than 254.

Examples

The following example shows how to configure a serial interface for Frame Relay:

```
interface Serial1:15
  ccs encap frf11
  ccs connect Serial0 990 100
```

Related Commands

Command	Description
mode ccs frame-forwarding	Set to forward frames on the controller.

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 2,147,483,647.

Defaults	2500 milliseconds

Command Modes	Interface configuration

Command History	Release	Modification
	11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines	This command applies to ATM configuration on the Cisco MC3810 multiservice concentrator. This command is supported on serial ports 0 and 1 with encapsulation atm-ces .

Examples	The following example configures the CES cell-loss integration period on serial port 0 to 1056: <pre>interface serial 0 ces cell-loss-integration-period 1056</pre>

Related Commands	Command	Description
	cbr	Configures the CBR for the ATM CES for an ATM PVC on the Cisco MC3810 multiservice concentrator.
	ces clockmode synchronous	Configures the ATM CES synchronous clock mode on the Cisco MC3810 multiservice concentrator.
	ces connect	Maps the CES service to an ATM PVC on the Cisco MC3810 multiservice concentrator.
	ces initial-delay	Configures the size of the receive buffer of a CES circuit on the Cisco MC3810 multiservice concentrator.
	ces max-buf-size	Configures the send buffer of a CES circuit on the Cisco MC3810 multiservice concentrator.

Command	Description
ces partial-fill	Configures the number of user octets per cell for the ATM CES on the Cisco MC3810 multiservice concentrator.
ces service	Configures the ATM CES type on the Cisco MC3810 multiservice concentrator.
encapsulation atm-ces	Enables CES ATM encapsulation on the Cisco MC3810 multiservice concentrator.

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**}

Syntax Description

adaptive	Adjusts output clock on a received ATM Adaptation Layer 1 (AAL1) on first-in, first-out basis. Use in unstructured mode.
srts	Sets the clocking mode to synchronous residual time stamp.
synchronous	Configures the timing recovery to synchronous for structured mode.

Defaults

The default setting is synchronous.

Command Modes

Controller configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

This command is used on Cisco 3600 series routers that have OC-3/STM-1 ATM CES network modules.

Examples

The following example configures the CES clock mode for synchronous residual time stamp:

```
ces-clock srts
```

Related Commands

Command	Description
controller	Configures the T1 or E1 controller.

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.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

This command applies to ATM configuration on the Cisco MC3810 multiservice concentrator.

This command maps into the transmit clock source of the constant bit rate (CBR) interface. This command is supported on serial ports 0 and 1 when set for CES ATM encapsulation.

Examples

The following example sets the ATM CES clock to synchronous mode on serial port 0:

```
interface serial 0
  ces clockmode synchronous
```

Related Commands

Command	Description
encapsulation atm-ces	Enables CES ATM encapsulation on the Cisco MC3810 multiservice concentrator.

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*}

Syntax Description

<i>atm-interface</i>	Number of the ATM interface. The only valid option on the Cisco MC3810 multiservice concentrator is ATM0.
pvc	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.

Defaults

No ATM interface is defined.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

This command applies to ATM configuration on the Cisco MC3810.

This command is supported on serial ports 0 and 1. The ATM interface must be configured to **encapsulation atm-ces**, and the *vpi/vci* must be defined on the interface.

Examples

The following example maps the CES service to PVC 20 on ATM port 0:

```
ces connect atm0 pvc 20
```

Related Commands

Command	Description
cbr	Configures the CBR for the ATM CES for an ATM PVC on the Cisco MC3810 multiservice concentrator.
ces cell-loss-integration-period	Sets the CES cell-loss integration period on the Cisco MC3810 multiservice concentrator.
ces clockmode synchronous	Configures the ATM CES synchronous clock mode on the Cisco MC3810 multiservice concentrator.

Command	Description
ces initial-delay	Configures the size of the receive buffer of a CES circuit on the Cisco MC3810 multiservice concentrator.
ces max-buf-size	Configures the send buffer of a CES circuit on the Cisco MC3810 multiservice concentrator.
ces partial-fill	Configures the number of user octets per cell for the ATM CES on the Cisco MC3810 multiservice concentrator.
ces service	Configures the ATM CES type on the Cisco MC3810 multiservice concentrator.
encapsulation atm-ces	Enables CES ATM encapsulation on the Cisco MC3810 multiservice concentrator.

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*

Syntax Description	<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.

Defaults	4000 bytes

Command Modes	Interface configuration

Command History	Release	Modification
	11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines	This command applies to ATM configuration on the Cisco MC3810 multiservice concentrator.

Examples	The following example shows configuration of the transmit buffer of the CES circuit to 8,000 bytes: ces initial-delay 8000

Related Commands	Command	Description
	ces cell-loss-integration-period	Sets the CES cell-loss integration period on the Cisco MC3810 multiservice concentrator.
	ces clockmode synchronous	Configures the ATM CES synchronous clock mode on the Cisco MC3810 multiservice concentrator.
	ces connect	Maps the CES service to an ATM PVC on the Cisco MC3810 multiservice concentrator.
	ces max-buf-size	Configures the send buffer of a CES circuit on the Cisco MC3810 multiservice concentrator.

Command	Description
ces partial-fill	Configures the number of user octets per cell for the ATM CES on the Cisco MC3810 multiservice concentrator.
ces service	Configures the ATM CES type on the Cisco MC3810 multiservice concentrator.

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*

Syntax Description

size

Maximum size of the transmit buffer for the CES. Possible values are from 80 to 1520.

Defaults

256

Command Modes

Interface configuration

Command History

Release

11.3(1)MA

Modification

This command was introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

This command applies to ATM configuration on the Cisco MC3810.

This command causes incoming bytes received on a CES port to be buffered by the amount configured and sent to the ATM Adaptation Layer 1 (AAL1) process as a block of data.

This command is supported on serial ports 0 and 1 when the **encapsulation atm-ces** command is enabled.

Examples

The following example shows configuration of the maximum CES reassembly buffer size to 1520:

```
ces max-buf-size 1520
```

Related Commands

Command

Description

ces cell-loss-integration-period

Sets the CES cell-loss integration period on the Cisco MC3810 multiservice concentrator.

ces clockmode synchronous

Configures the ATM CES synchronous clock mode on the Cisco MC3810 multiservice concentrator.

ces connect

Maps the CES service to an ATM PVC on the Cisco MC3810 multiservice concentrator.

ces initial-delay

Configures the size of the receive buffer of a CES circuit on the Cisco MC3810 multiservice concentrator.

Command	Description
ces partial-fill	Configures the number of user octets per cell for the ATM CES on the Cisco MC3810 multiservice concentrator.
ces service	Configures the ATM CES type on the Cisco MC3810 multiservice concentrator.

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

Syntax Description	structured	Specifies that the ATM CES type is structured. Structured is the only option supported in this release.

Defaults	Structured

Command Modes	Interface configuration

Command History	Release	Modification
	11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines	This command applies to ATM configuration on the Cisco MC3810.
	This command is supported on serial ports 0 and 1 when the encapsulation atm-ces command is enabled.

Examples	The following example sets the CES service to structured for serial port 0:

```
interface serial 0
  ces service structured
```

Related Commands	Command	Description
	ces cell-loss-integration-period	Sets the CES cell-loss integration period on the Cisco MC3810 multiservice concentrator.
	ces clockmode synchronous	Configures the ATM CES synchronous clock mode on the Cisco MC3810 multiservice concentrator.
	ces connect	Maps the CES service to an ATM PVC on the Cisco MC3810 multiservice concentrator.
	ces initial-delay	Configures the size of the receive buffer of a CES circuit on the Cisco MC3810 multiservice concentrator.

Command	Description
ces max-buf-size	Configures the send buffer of a CES circuit on the Cisco MC3810 multiservice concentrator.
ces partial-fill	Configures the number of user octets per cell for the ATM CES on the Cisco MC3810 multiservice concentrator.

clear backhaul-session-manager group

To reset the statistics or traffic counters for a specified session-group, use the **clear backhaul-session-manager group** command in privileged EXEC mode.

clear backhaul-session-manager group stats { all | name *group-name* }

Syntax Description

all	All available session-groups.
name <i>group-name</i>	A specified session-group.

Defaults

The statistical information accumulates.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

A session is the connection between a client and a server, and a session-group is a collection of sessions in a group to implement switchover in case of a session failure. This command clears all statistics.

Examples

To clear all statistics for all available session-groups, see the following example:

```
Router# clear backhaul-session-manager group stats all
```

Related Commands

Command	Description
show backhaul-session-manager group	Displays status, statistics, or configuration of a specified or all session-groups.

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*]

Syntax Description	<i>ip-address</i> (Optional) Specifies the target IP address.	
Defaults	None	
Command Modes	EXEC	
Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 and 3600 series and on the MC3810 multiservice concentrator.
Usage Guidelines	If no IP address is specified, the command will clear the cache of all ICPIF estimates for all IP addresses. There is no no form of this command.	
Examples	The following example clears the cache of the ICPIF estimate for IP address 209.165.200.225: <pre>clear call fallback cache 209.165.200.225</pre>	
Related Commands	Command	Description
	show call fallback cache	Displays the current ICPIF estimates for all IP addresses in the cache.

clear call fallback stats

To clear the call fallback statistics, use the **clear call fallback stats** command in EXEC mode.

clear call fallback stats

Syntax Description	This command has no arguments or keywords.

Defaults	There are no defaults.

Command Modes	EXEC

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 and 3600 series and on the MC3810 multiservice concentrator.

Usage Guidelines	There is no no form of this command.

Examples	The following example clears the call fallback statistics. clear call fallback stats

Related Commands	Command	Description
	show call fallback stats	Displays the call fallback statistics.

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]

Syntax Description	t1 e1	Specifies the type of controller. If the t1 or e1 keyword is specified, then the command acts on the individual controller specified in <i>number</i> . In this case, the additional options of system-hwm or all 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> .
	system-hwm	(Optional) Clears the system's HWM only (not the individual controllers).
	all	(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 clear controllers command on that controller.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	12.0(1)T	This command was introduced.
	12.1(1)T	This command was applied to voice/WAN interface cards (VWICs) for Cisco 2600 and Cisco 3600 series routers.
	12.1(2)T	This command was integrated into the Cisco AS5300 and AS5800.

Usage Guidelines The **clear controllers call-counters all** command clears the system's DS0s HWM and all individual controller statistics, including the controllers' DS0s HWM, Total Calls, and Total Duration. The **clear controllers call-counters system-hwm** command clears the system's DS0s HWM and leaves all other call-counter statistics untouched.

Refer to the following comments for the meaning of call counters displayed before and after executing **clear controllers call-counters** related commands.

- The numbers displayed under TotalCalls for each time slot represent *total* calls that were connected successfully. Note that if a first call comes in on time slot 10, then **show controllers t1 call-counters** displays 1 under the TotalCalls column for time slot 10. A value of 20 displayed under TotalCalls for time slot 10 indicates a total of 20 calls connected on time slot 10 since *the last time call counters were cleared*.

TotalCalls for time slots are set to *zero* when **clear controllers t1 1/0/0 call-counters timeslot 10** is executed or **clear controllers t1 1/0/0 call-counters** is executed at a controller level.

The TotalCalls figures for the time slots are not the number of active calls in the controller—they just display the time slot usage as the number of calls connected since the last clear was done.

This is also true for the TotalDuration displayed for the time slots—it indicates the total time usage on time slots for the calls that were completed.

- DS0s Active: Indicates the number of active calls on the specified controller. This number indicates the current number of calls on the controller at any given time.
- DS0s Active High Water Mark: Indicates the peak number of calls on the controller since the last **clear controllers t1 1/0/0 call-counters** command was entered. If the number of active calls “DS0s Active” is less than DS0s HWM, then HWM remains untouched. If new calls come in and the active DS0s are more than the HWM, then the HWM is incremented to reflect the new peak number of calls on that controller.

This value is reset to *current* active DS0s when the command **clear controllers t1 1/3/0 call-counters** is entered. For example, in the beginning, the HWM is 0. A new call comes in. The HWM is 1. When the next call comes in, the HWM is 2. If 20 calls come in, the HWM is 20 and also-active DS0s are 20. If 5 calls get disconnected, the DS0 active is 15, but the HWM is 20. A **clear controllers** command is input for the specified controller. The HWM is reset to 15, which is current active DS0s. The HWM is 15 and active DS0s are also 15. Ten calls get disconnected. Active DS0s is 5 and the HWM remains at 15 until another **clear controllers** command is input. If Active DS0s exceed 15, then the HWM is updated.

- System DS0s High Water Mark: Same point as number 3, but this value reflects the HWM at a system level, including DS0s of all controllers.

Examples

The examples below show two controllers: 1/3/0:3 and 1/3/0:8. Note the semantics of output shown by **show controllers t1 call-counters** and how **clear controllers call-counters** affects them.

The following example shows the system in the beginning state (with no calls):

```
Router# show users
      Line      User      Host(s)      Idle      Location
*  0 con 0
      idle
      00:00:00

      Interface  User      Mode      Idle Peer Address

Router# show controllers t1 call-counters
T1 1/3/0:3:
DS0's Active: 0
DS0's Active High Water Mark: 0
TimeSlot  Type  TotalCalls  TotalDuration
  1      pri      0          00:00:00
  2      pri      0          00:00:00
  3      pri      0          00:00:00
  4      pri      0          00:00:00
  5      pri      0          00:00:00
```

```

        6      pri      0      00:00:00
        7      pri      0      00:00:00
        8      pri      0      00:00:00
        9      pri      0      00:00:00
       10      pri      0      00:00:00
       11      pri      0      00:00:00
       12      pri      0      00:00:00
       13      pri      0      00:00:00
       14      pri      0      00:00:00
       15      pri      0      00:00:00
       16      pri      0      00:00:00
       17      pri      0      00:00:00
       18      pri      0      00:00:00
       19      pri      0      00:00:00
       20      pri      0      00:00:00
       21      pri      0      00:00:00
       22      pri      0      00:00:00
       23      pri      0      00:00:00

```

T1 1/3/0:8:

DS0's Active: 0

DS0's Active High Water Mark: 0

TimeSlot	Type	TotalCalls	TotalDuration
1	pri	0	00:00:00
2	pri	0	00:00:00
3	pri	0	00:00:00
4	pri	0	00:00:00
5	pri	0	00:00:00
6	pri	0	00:00:00
7	pri	0	00:00:00
8	pri	0	00:00:00
9	pri	0	00:00:00
10	pri	0	00:00:00
11	pri	0	00:00:00
12	pri	0	00:00:00
13	pri	0	00:00:00
14	pri	0	00:00:00
15	pri	0	00:00:00
16	pri	0	00:00:00
17	pri	0	00:00:00
18	pri	0	00:00:00
19	pri	0	00:00:00
20	pri	0	00:00:00
21	pri	0	00:00:00
22	pri	0	00:00:00
23	pri	0	00:00:00

System's DS0's Active High Water Mark: 0

All the fields are zero—indicating that no calls have come in since system startup or since the last clear was made on controllers by the **clear controllers** command.

The following example shows that four calls have been initiated on these controllers:

Router# **show users**

Line	User	Host(s)	Idle	Location
* 0 con 0		idle	00:00:00	
tty 1/5/12	Router Async	interface	00:01:05	PPP: 55.61.1.1
tty 1/5/13	Router Async	interface	00:00:48	PPP: 55.62.1.1
tty 1/5/14	Router Async	interface	00:00:33	PPP: 55.54.1.1
tty 1/5/15	Router Async	interface	00:00:19	PPP: 55.52.1.1

Interface	User	Mode	Idle	Peer	Address

clear controllers call-counters

```

Router# show controllers t1 call-counters
Tl 1/3/0:3:
  DS0's Active: 2
  DS0's Active High Water Mark: 2
  TimeSlot   Type   TotalCalls   TotalDuration
    1         pri         0         00:00:00
    2         pri         0         00:00:00
    3         pri         0         00:00:00
    4         pri         0         00:00:00
    5         pri         0         00:00:00
    6         pri         0         00:00:00
    7         pri         0         00:00:00
    8         pri         0         00:00:00
    9         pri         0         00:00:00
   10         pri         0         00:00:00
   11         pri         0         00:00:00
   12         pri         0         00:00:00
   13         pri         0         00:00:00
   14         pri         0         00:00:00
   15         pri         0         00:00:00
   16         pri         0         00:00:00
   17         pri         0         00:00:00
   18         pri         0         00:00:00
   19         pri         0         00:00:00
   20         pri         0         00:00:00
   21         pri         0         00:00:00
   22         pri         1         00:01:58
   23         pri         1         00:02:27

Tl 1/3/0:8:
  DS0's Active: 2
  DS0's Active High Water Mark: 2
  TimeSlot   Type   TotalCalls   TotalDuration
    1         pri         0         00:00:00
    2         pri         0         00:00:00
    3         pri         0         00:00:00
    4         pri         0         00:00:00
    5         pri         0         00:00:00
    6         pri         0         00:00:00
    7         pri         0         00:00:00
    8         pri         0         00:00:00
    9         pri         0         00:00:00
   10         pri         0         00:00:00
   11         pri         0         00:00:00
   12         pri         0         00:00:00
   13         pri         0         00:00:00
   14         pri         0         00:00:00
   15         pri         0         00:00:00
   16         pri         0         00:00:00
   17         pri         0         00:00:00
   18         pri         0         00:00:00
   19         pri         0         00:00:00
   20         pri         0         00:00:00
   21         pri         0         00:00:00
   22         pri         1         00:02:14
   23         pri         1         00:02:46

System's DS0's Active High Water Mark: 4

```

Controllers 1/3/0:3 and 1/3/0:8 both have DS0 Active 2, DS0s HWM 2. The TotalCalls field represents the total number of calls on that time slot since the controller was cleared. This accumulates for every call made on that time stamp and will be set to zero on individual controllers when the **clear controllers**

t1 1/3/0:8 call-counters command is entered or at the system level when the **clear controllers call-counters all** command is entered. TotalDuration is the same as TotalCalls except that it reflects the accumulated connection time on that time slot.

This has nothing to do with active calls, If a **clear controllers** command is entered for a controller that has active calls, which have been connected from the past 30 minutes, the TotalCalls and TotalDuration are reset to zero. In the following example, the controller is 1/3/0:3, with time slots 22 and 23 connected and active. When the **clear controllers t1 1/3/0:3 call-counters** command is entered, the corresponding fields are set to zero.

The following is an example of output when the **show controllers t1 call-counters** command is used:

```
Router# show controllers t1 call-counters
T1 1/3/0:3:
DS0's Active: 2
DS0's Active High Water Mark: 2
TimeSlot  Type  TotalCalls  TotalDuration
   1       pri         0         00:00:00
   2       pri         0         00:00:00
   3       pri         0         00:00:00
   4       pri         0         00:00:00
   5       pri         0         00:00:00
   6       pri         0         00:00:00
   7       pri         0         00:00:00
   8       pri         0         00:00:00
   9       pri         0         00:00:00
  10       pri         0         00:00:00
  11       pri         0         00:00:00
  12       pri         0         00:00:00
  13       pri         0         00:00:00
  14       pri         0         00:00:00
  15       pri         0         00:00:00
  16       pri         0         00:00:00
  17       pri         0         00:00:00
  18       pri         0         00:00:00
  19       pri         0         00:00:00
  20       pri         0         00:00:00
  21       pri         0         00:00:00
  22       pri         1         00:29:14
  23       pri         1         00:29:47
```

```
Router# clear controllers t1 1/3/0:3 call-counters
```

```
Router# show controllers t1 call-counters
T1 1/3/0:3:
DS0's Active: 2
DS0's Active High Water Mark: 2
TimeSlot  Type  TotalCalls  TotalDuration
   1       pri         0         00:00:00
   2       pri         0         00:00:00
   3       pri         0         00:00:00
   4       pri         0         00:00:00
   5       pri         0         00:00:00
   6       pri         0         00:00:00
   7       pri         0         00:00:00
   8       pri         0         00:00:00
   9       pri         0         00:00:00
  10       pri         0         00:00:00
  11       pri         0         00:00:00
  12       pri         0         00:00:00
  13       pri         0         00:00:00
  14       pri         0         00:00:00
  15       pri         0         00:00:00
```

clear controllers call-counters

```

16      pri      0      00:00:00
17      pri      0      00:00:00
18      pri      0      00:00:00
19      pri      0      00:00:00
20      pri      0      00:00:00
21      pri      0      00:00:00
22      pri      0      00:00:10  <<<<<<
23      pri      0      00:00:10  <<<<<<

```

Now a call is brought down (on 1/5/12).

```
Router# clear line 1/5/12
```

```
[confirm]
```

```
[OK]
```

```
Router# show users
```

Line	User	Host(s)	Idle	Location
* 0 con 0		idle	00:00:00	
tty 1/5/13	Router Async interface		00:03:04	PPP: 55.62.1.1
tty 1/5/14	Router Async interface		00:02:49	PPP: 55.54.1.1
tty 1/5/15	Router Async interface		00:02:35	PPP: 55.52.1.1

Interface	User	Mode	Idle	Peer Address

```
Router# show controllers t1 call-counters
```

```
T1 1/3/0:3:
```

```
DS0's Active: 2
```

```
DS0's Active High Water Mark: 2
```

TimeSlot	Type	TotalCalls	TotalDuration
1	pri	0	00:00:00
2	pri	0	00:00:00
3	pri	0	00:00:00
4	pri	0	00:00:00
5	pri	0	00:00:00
6	pri	0	00:00:00
7	pri	0	00:00:00
8	pri	0	00:00:00
9	pri	0	00:00:00
10	pri	0	00:00:00
11	pri	0	00:00:00
12	pri	0	00:00:00
13	pri	0	00:00:00
14	pri	0	00:00:00
15	pri	0	00:00:00
16	pri	0	00:00:00
17	pri	0	00:00:00
18	pri	0	00:00:00
19	pri	0	00:00:00
20	pri	0	00:00:00
21	pri	0	00:00:00
22	pri	1	00:03:44
23	pri	1	00:04:14

```
T1 1/3/0:8:
```

```
DS0's Active: 1
```

```
DS0's Active High Water Mark: 2
```

TimeSlot	Type	TotalCalls	TotalDuration
1	pri	0	00:00:00
2	pri	0	00:00:00
3	pri	0	00:00:00
4	pri	0	00:00:00
5	pri	0	00:00:00
6	pri	0	00:00:00
7	pri	0	00:00:00
8	pri	0	00:00:00
9	pri	0	00:00:00

10	pri	0	00:00:00
11	pri	0	00:00:00
12	pri	0	00:00:00
13	pri	0	00:00:00
14	pri	0	00:00:00
15	pri	0	00:00:00
16	pri	0	00:00:00
17	pri	0	00:00:00
18	pri	0	00:00:00
19	pri	0	00:00:00
20	pri	0	00:00:00
21	pri	0	00:00:00
22	pri	1	00:04:00
23	pri	1	00:03:34

System's DS0's Active High Water Mark: 4

After a call gets disconnected, only the DS0's Active field will change to reflect the current active call on the controller. In the above example, 1/3/0:8 Active DS0 is changed to 1.

Now, call counters are cleared for an individual controller (for 1/3/0:8):

```
Router# clear controllers t1 1/3/0:8 ?
call-counters  T1 call counters
<cr>
```

```
Router# clear controllers t1 1/3/0:8 call-counters
```

```
Router# show controllers t1 call-counters
```

T1 1/3/0:3:

DS0's Active: 2

DS0's Active High Water Mark: 2

TimeSlot	Type	TotalCalls	TotalDuration
1	pri	0	00:00:00
2	pri	0	00:00:00
3	pri	0	00:00:00
4	pri	0	00:00:00
5	pri	0	00:00:00
6	pri	0	00:00:00
7	pri	0	00:00:00
8	pri	0	00:00:00
9	pri	0	00:00:00
10	pri	0	00:00:00
11	pri	0	00:00:00
12	pri	0	00:00:00
13	pri	0	00:00:00
14	pri	0	00:00:00
15	pri	0	00:00:00
16	pri	0	00:00:00
17	pri	0	00:00:00
18	pri	0	00:00:00
19	pri	0	00:00:00
20	pri	0	00:00:00
21	pri	0	00:00:00
22	pri	1	00:07:46
23	pri	1	00:08:15

T1 1/3/0:8:

DS0's Active: 1

DS0's Active High Water Mark: 1

TimeSlot	Type	TotalCalls	TotalDuration
1	pri	0	00:00:00
2	pri	0	00:00:00
3	pri	0	00:00:00
4	pri	0	00:00:00
5	pri	0	00:00:00

clear controllers call-counters

6	pri	0	00:00:00
7	pri	0	00:00:00
8	pri	0	00:00:00
9	pri	0	00:00:00
10	pri	0	00:00:00
11	pri	0	00:00:00
12	pri	0	00:00:00
13	pri	0	00:00:00
14	pri	0	00:00:00
15	pri	0	00:00:00
16	pri	0	00:00:00
17	pri	0	00:00:00
18	pri	0	00:00:00
19	pri	0	00:00:00
20	pri	0	00:00:00
21	pri	0	00:00:00
22	pri	0	00:00:35
23	pri	0	00:00:00

System's DS0's Active High Water Mark: 4

After clearing call counters for controller 1/3/0:8, as shown earlier, TotalCalls and TotalDuration reset. In addition DS0's High Water Mark is also *cleared* to the number of active DS0s. Whenever the DS0s' HWM is cleared it will not reset to zero, but rather it will be set to Active DS0s for that instance. So for 1/3/0:8, the HWM is 1 after clearing since DS0 Active is 1 (1 active call). TotalDuration is 35 seconds for time slot 22 and TotalCall is 0 since they got reset when the **clear call-counters** command was entered. Total calls on this time slot will be incremented when a new call comes in on this time slot.

Use the system HWM option:

```
Router# clear controllers ?
T1          T1 controller
T3          T3 controller
call-counters  system call counters

Router# clear controllers call-counters ?
all          all controllers
system-hwm   system High Water Mark

Router# clear controllers call-counters system-hwm
Router# show controllers t1 call-counters
T1 1/3/0:3:
DS0's Active: 2
DS0's Active High Water Mark: 2
TimeSlot  Type  TotalCalls  TotalDuration
  1        pri      0      00:00:00
  2        pri      0      00:00:00
  3        pri      0      00:00:00
  4        pri      0      00:00:00
  5        pri      0      00:00:00
  6        pri      0      00:00:00
  7        pri      0      00:00:00
  8        pri      0      00:00:00
  9        pri      0      00:00:00
 10        pri      0      00:00:00
 11        pri      0      00:00:00
 12        pri      0      00:00:00
 13        pri      0      00:00:00
 14        pri      0      00:00:00
 15        pri      0      00:00:00
 16        pri      0      00:00:00
 17        pri      0      00:00:00
 18        pri      0      00:00:00
```

```

19      pri      0      00:00:00
20      pri      0      00:00:00
21      pri      0      00:00:00
22      pri      1      00:08:51
23      pri      1      00:09:21
T1 1/3/0:8:
DS0's Active: 1
DS0's Active High Water Mark: 1
TimeSlot  Type  TotalCalls  TotalDuration
1         pri      0      00:00:00
2         pri      0      00:00:00
3         pri      0      00:00:00
4         pri      0      00:00:00
5         pri      0      00:00:00
6         pri      0      00:00:00
7         pri      0      00:00:00
8         pri      0      00:00:00
9         pri      0      00:00:00
10        pri      0      00:00:00
11        pri      0      00:00:00
12        pri      0      00:00:00
13        pri      0      00:00:00
14        pri      0      00:00:00
15        pri      0      00:00:00
16        pri      0      00:00:00
17        pri      0      00:00:00
18        pri      0      00:00:00
19        pri      0      00:00:00
20        pri      0      00:00:00
21        pri      0      00:00:00
22        pri      0      00:01:39
23        pri      0      00:00:00

```

System's DS0's Active High Water Mark: 3

The system HWM is reset to Total number of active calls in the system, which is 3; earlier it was 4.

Bring down another two calls and check output from the command **show controllers t1 call-counters**:

```

Router# show users
   Line      User      Host(s)      Idle      Location
*  0 con 0      idle      00:00:00
tty 1/5/13  Router Async interface  00:09:49  PPP: 55.62.1.1
tty 1/5/14  Router Async interface  00:09:35  PPP: 55.54.1.1
tty 1/5/15  Router Async interface  00:09:20  PPP: 55.52.1.1

```

```

Interface  User      Mode      Idle Peer Address

```

```

Router# clear line 1/5/13

```

```

[confirm]

```

```

[OK]

```

```

Router# clear line 1/5/14

```

```

[confirm]

```

```

[OK]

```

```

Router# show users
   Line      User      Host(s)      Idle      Location
*  0 con 0      idle      00:00:00
tty 1/5/15  Router Async interface  00:09:46  PPP: 55.52.1.1

```

```

Interface  User      Mode      Idle Peer Address

```

```

Router# show controllers t1 call-counters

```

```

T1 1/3/0:3:

```

clear controllers call-counters

DS0's Active: 1

DS0's Active High Water Mark: 2

TimeSlot	Type	TotalCalls	TotalDuration
1	pri	0	00:00:00
2	pri	0	00:00:00
3	pri	0	00:00:00
4	pri	0	00:00:00
5	pri	0	00:00:00
6	pri	0	00:00:00
7	pri	0	00:00:00
8	pri	0	00:00:00
9	pri	0	00:00:00
10	pri	0	00:00:00
11	pri	0	00:00:00
12	pri	0	00:00:00
13	pri	0	00:00:00
14	pri	0	00:00:00
15	pri	0	00:00:00
16	pri	0	00:00:00
17	pri	0	00:00:00
18	pri	0	00:00:00
19	pri	0	00:00:00
20	pri	0	00:00:00
21	pri	0	00:00:00
22	pri	1	00:11:04
23	pri	1	00:10:20

T1 1/3/0:8:

DS0's Active: 0

DS0's Active High Water Mark: 1

TimeSlot	Type	TotalCalls	TotalDuration
1	pri	0	00:00:00
2	pri	0	00:00:00
3	pri	0	00:00:00
4	pri	0	00:00:00
5	pri	0	00:00:00
6	pri	0	00:00:00
7	pri	0	00:00:00
8	pri	0	00:00:00
9	pri	0	00:00:00
10	pri	0	00:00:00
11	pri	0	00:00:00
12	pri	0	00:00:00
13	pri	0	00:00:00
14	pri	0	00:00:00
15	pri	0	00:00:00
16	pri	0	00:00:00
17	pri	0	00:00:00
18	pri	0	00:00:00
19	pri	0	00:00:00
20	pri	0	00:00:00
21	pri	0	00:00:00
22	pri	0	00:02:50
23	pri	0	00:00:00

System's DS0's Active High Water Mark: 3



Note

Whenever a call goes down, HWM values are untouched. Only the DS0 Active changes. Now there is only one call on 1/3/0:3. Observe the HWM for individual controllers. Total number of active calls is 1.

Clear the system-hwm with the following command:

Router# **clear controllers call-counters system-hwm**

Router# **show controllers t1 call-counters**

T1 1/3/0:3:

DS0's Active: 1

DS0's Active High Water Mark: 2

TimeSlot	Type	TotalCalls	TotalDuration
1	pri	0	00:00:00
2	pri	0	00:00:00
3	pri	0	00:00:00
4	pri	0	00:00:00
5	pri	0	00:00:00
6	pri	0	00:00:00
7	pri	0	00:00:00
8	pri	0	00:00:00
9	pri	0	00:00:00
10	pri	0	00:00:00
11	pri	0	00:00:00
12	pri	0	00:00:00
13	pri	0	00:00:00
14	pri	0	00:00:00
15	pri	0	00:00:00
16	pri	0	00:00:00
17	pri	0	00:00:00
18	pri	0	00:00:00
19	pri	0	00:00:00
20	pri	0	00:00:00
21	pri	0	00:00:00
22	pri	1	00:12:16
23	pri	1	00:10:20

T1 1/3/0:8:

DS0's Active: 0

DS0's Active High Water Mark: 1

TimeSlot	Type	TotalCalls	TotalDuration
1	pri	0	00:00:00
2	pri	0	00:00:00
3	pri	0	00:00:00
4	pri	0	00:00:00
5	pri	0	00:00:00
6	pri	0	00:00:00
7	pri	0	00:00:00
8	pri	0	00:00:00
9	pri	0	00:00:00
10	pri	0	00:00:00
11	pri	0	00:00:00
12	pri	0	00:00:00
13	pri	0	00:00:00
14	pri	0	00:00:00
15	pri	0	00:00:00
16	pri	0	00:00:00
17	pri	0	00:00:00
18	pri	0	00:00:00
19	pri	0	00:00:00
20	pri	0	00:00:00
21	pri	0	00:00:00
22	pri	0	00:02:50
23	pri	0	00:00:00

System's DS0's Active High Water Mark: 1



Note Only the system HWM is reset to Active calls; for example, 1. For controllers 1/3/0:3 and 1/3/0:8, the HWMs are untouched.

Bring down another call, and display what the output will be:

```
Router# clear line 1/5/15
[confirm]
[OK]
Router# show controllers t1 call-counters
T1 1/3/0:3:
DS0's Active: 0
DS0's Active High Water Mark: 2
TimeSlot  Type  TotalCalls  TotalDuration
1         pri      0         00:00:00
2         pri      0         00:00:00
3         pri      0         00:00:00
4         pri      0         00:00:00
5         pri      0         00:00:00
6         pri      0         00:00:00
7         pri      0         00:00:00
8         pri      0         00:00:00
9         pri      0         00:00:00
10        pri      0         00:00:00
11        pri      0         00:00:00
12        pri      0         00:00:00
13        pri      0         00:00:00
14        pri      0         00:00:00
15        pri      0         00:00:00
16        pri      0         00:00:00
17        pri      0         00:00:00
18        pri      0         00:00:00
19        pri      0         00:00:00
20        pri      0         00:00:00
21        pri      0         00:00:00
22        pri      1         00:12:40
23        pri      1         00:10:20
T1 1/3/0:8:
DS0's Active: 0
DS0's Active High Water Mark: 1
TimeSlot  Type  TotalCalls  TotalDuration
1         pri      0         00:00:00
2         pri      0         00:00:00
3         pri      0         00:00:00
4         pri      0         00:00:00
5         pri      0         00:00:00
6         pri      0         00:00:00
7         pri      0         00:00:00
8         pri      0         00:00:00
9         pri      0         00:00:00
10        pri      0         00:00:00
11        pri      0         00:00:00
12        pri      0         00:00:00
13        pri      0         00:00:00
14        pri      0         00:00:00
15        pri      0         00:00:00
16        pri      0         00:00:00
17        pri      0         00:00:00
18        pri      0         00:00:00
19        pri      0         00:00:00
20        pri      0         00:00:00
21        pri      0         00:00:00
```

```

22      pri      0      00:02:50
23      pri      0      00:00:00

```

System's DS0's Active High Water Mark: 1

Now use the **all** option, clearing at the system level:

```
Router# clear controllers call-counters all
```

```
Router# show controllers t1 call-counters
```

```
T1 1/3/0:3:
```

```
DS0's Active: 0
```

```
DS0's Active High Water Mark: 0
```

TimeSlot	Type	TotalCalls	TotalDuration
1	pri	0	00:00:00
2	pri	0	00:00:00
3	pri	0	00:00:00
4	pri	0	00:00:00
5	pri	0	00:00:00
6	pri	0	00:00:00
7	pri	0	00:00:00
8	pri	0	00:00:00
9	pri	0	00:00:00
10	pri	0	00:00:00
11	pri	0	00:00:00
12	pri	0	00:00:00
13	pri	0	00:00:00
14	pri	0	00:00:00
15	pri	0	00:00:00
16	pri	0	00:00:00
17	pri	0	00:00:00
18	pri	0	00:00:00
19	pri	0	00:00:00
20	pri	0	00:00:00
21	pri	0	00:00:00
22	pri	0	00:00:00
23	pri	0	00:00:00

```
T1 1/3/0:8:
```

```
DS0's Active: 0
```

```
DS0's Active High Water Mark: 0
```

TimeSlot	Type	TotalCalls	TotalDuration
1	pri	0	00:00:00
2	pri	0	00:00:00
3	pri	0	00:00:00
4	pri	0	00:00:00
5	pri	0	00:00:00
6	pri	0	00:00:00
7	pri	0	00:00:00
8	pri	0	00:00:00
9	pri	0	00:00:00
10	pri	0	00:00:00
11	pri	0	00:00:00
12	pri	0	00:00:00
13	pri	0	00:00:00
14	pri	0	00:00:00
15	pri	0	00:00:00
16	pri	0	00:00:00
17	pri	0	00:00:00
18	pri	0	00:00:00
19	pri	0	00:00:00
20	pri	0	00:00:00
21	pri	0	00:00:00
22	pri	0	00:00:00
23	pri	0	00:00:00

System's DS0's Active High Water Mark: 0

Clearing at the system level using the **clear controllers call-counters** command clears all DS0 controllers in the system and also clears the system's HWM.

Now bring four calls up and show the call-counters output:

Router# **show users**

Line	User	Host(s)	Idle	Location
* 0 con 0		idle	00:00:00	
tty 1/5/16	Router Async interface		00:01:01	PPP: 55.1.1.1
tty 1/5/17	Router Async interface		00:00:47	PPP: 55.2.1.1
tty 1/5/18	Router Async interface		00:00:28	PPP: 55.3.1.1
tty 1/5/19	Router Async interface		00:00:14	PPP: 55.4.1.1

Interface	User	Mode	Idle	Peer	Address

Router# **show controllers t1 call-counters**

T1 1/3/0:3:

DS0's Active: 2

DS0's Active High Water Mark: 2

TimeSlot	Type	TotalCalls	TotalDuration
1	pri	0	00:00:00
2	pri	0	00:00:00
3	pri	0	00:00:00
4	pri	0	00:00:00
5	pri	0	00:00:00
6	pri	0	00:00:00
7	pri	0	00:00:00
8	pri	0	00:00:00
9	pri	0	00:00:00
10	pri	0	00:00:00
11	pri	0	00:00:00
12	pri	0	00:00:00
13	pri	0	00:00:00
14	pri	0	00:00:00
15	pri	0	00:00:00
16	pri	0	00:00:00
17	pri	0	00:00:00
18	pri	0	00:00:00
19	pri	0	00:00:00
20	pri	0	00:00:00
21	pri	0	00:00:00
22	pri	1	00:00:57
23	pri	1	00:01:30

T1 1/3/0:8:

DS0's Active: 2

DS0's Active High Water Mark: 2

TimeSlot	Type	TotalCalls	TotalDuration
1	pri	0	00:00:00
2	pri	0	00:00:00
3	pri	0	00:00:00
4	pri	0	00:00:00
5	pri	0	00:00:00
6	pri	0	00:00:00
7	pri	0	00:00:00
8	pri	0	00:00:00
9	pri	0	00:00:00
10	pri	0	00:00:00
11	pri	0	00:00:00
12	pri	0	00:00:00
13	pri	0	00:00:00
14	pri	0	00:00:00
15	pri	0	00:00:00
16	pri	0	00:00:00
17	pri	0	00:00:00


```
18      pri      0      00:00:00
19      pri      0      00:00:00
20      pri      0      00:00:00
21      pri      0      00:00:00
22      pri      1      00:01:12
23      pri      1      00:01:45
```

System's DS0's Active High Water Mark: 4

Related Commands

Command	Description
controller	Sets the router in controller configuration mode from global configuration mode.

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*]

Syntax Description

<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.

Defaults

There are no defaults.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 NA	This command was introduced.

Usage Guidelines

Use the **clear csm-statistics modem** command to clear CSM statistics for a particular modem or group of modems. If the *slot/port* argument is specified, the CSM call statistics for calls using the identified modem will be cleared. If a modem group number is specified, then the CSM call statistics for calls using the modems associated with that group will be cleared. If no argument is specified, all CSM call statistics for all modems will be cleared.

Examples

The following example clears CSM call statistics for calls coming in on modems associated with modem group 2:

```
Router# clear csm-statistics modem 2
```

Related Commands

Command	Description
clear csm-statistics voice	Clears the CSM statistics for a particular or for all DSP channels.

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/dsp/dsp-channel*]

Syntax Description	<i>slot/dsp/dsp-channel</i> (Optional) Identifies the location of a particular DSP channel.	
Defaults	There are no defaults.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	11.3 NA	This command was introduced.
Usage Guidelines	Use the clear csm-statistics voice command to clear CSM statistics for a particular DSP channel. If the <i>slot/dsp/dsp/dsp-channel</i> argument is specified, the CSM call statistics for calls using the identified DSP channel will be cleared. If no argument is specified, all CSM call statistics for all DSP channels will be cleared.	
Examples	The following example clears CSM call statistics for calls coming in on all DSP channels: Router# clear csm-statistics voice	
Related Commands	Command	Description
	clear csm-statistics modem	Clears the CSM statistics for a modem or group of modems.

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*}

Syntax Description

all	Forces all active calls currently associated with this gatekeeper to be disconnected.
local-callID	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.

Defaults

There are no defaults.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced on the Cisco 2600 series routers, 3600 series, and on the MC3810 multiservice concentrator.

Usage Guidelines

If you want to force a particular call to be disconnected (as opposed to all active calls on the gatekeeper), use the CallID number to identify that specific call. You can find the local CallID number for a specific call by using the **show gatekeeper calls** command; the ID number is displayed in the LocalCallID column. The “show gatekeeper calls Command Output” example shows output from the **show gatekeeper calls** command.

Examples

The following example forces an active call on the gatekeeper to be disconnected. The local ID number of the active call is 12-3339.

```
enable
clear h323 gatekeeper call local-callID 12-3339
```

The following example forces all active calls on the gatekeeper to be disconnected:

```
enable
clear h323 gatekeeper call all
```

Router# **show gatekeeper calls**

Total number of active calls =1

Gatekeeper Call Info

=====

LocalCallID		Age (secs)	BW			
12-3339		94	768	(Kbps)		
Endpt(s):	Alias	E.164Addr	CallSignalAddr	Port	RASSignalAddr	Port
src EP:	epA		10.0.0.11	1720	10.0.0.11	1700
dst EP:	epB2zoneB.com					
src PX:	pxA	10.0.0.1		1720	10.0.0.11	24999
dst PX:	pxB	172.21.139.90		1720	172.21.139.90	24999

Related Commands

Command	Description
show gatekeeper calls	Displays the status of each ongoing call of which a gatekeeper is aware.

clear ip sctp statistics

To clear statistics counts for SCTP, enter the **clear ip sctp statistics** command in privileged EXEC mode.

clear ip sctp statistics

Syntax Description There are no arguments or keywords for this command.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)T	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300.

Usage Guidelines This command clears both individual and overall statistics.

Examples No output is generated from this command.

```
Router# clear ip sctp statistics
```

Related Commands	Command	Description
	show ip sctp association list	Shows a list of all current SCTP associations.
	show ip sctp association parameters	Shows the parameters configured for the association defined by the association ID.
	show ip sctp association statistics	Shows the current statistics for the association defined by the association ID.
	show ip sctp errors	Shows error counts logged by SCTP.
	show ip sctp instances	Shows all currently defined SCTP instances.
	show ip sctp statistics	Shows overall statistics counts for SCTP.
	show iua as	Shows information about the current condition of an AS.
	show iua asp	Shows information about the current condition of an ASP.

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

Syntax Description	This command has no arguments or keywords.

Defaults	There are no defaults.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
	12.1(3)T	Support for this command was extended to the Cisco 3660, Cisco uBR924, and Cisco 2600 series routers platforms.

Usage Guidelines	None

Examples	The following is an example of how to enter the command. Router# clear mgcp statistics

Related Commands	Command	Description
	mgcp	Starts the MGCP daemon.
	show mgcp statistics	Displays statistics for received and transmitted packets.

clear rlm group

To clear all time stamps to zero, use the **clear rlm group link** command in privileged EXEC mode.

clear rlm group *group-number* **link**

Syntax Description

group-number RLM group number (0 to 255).

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(7)	This command was introduced.

Examples

The following example clears the time stamps on RLM group 1:

```
Router# clear rlm group 1 link
```

```
Router#
02:48:17: rlm 1: [State_Up, rx ACTIVE_LINK_BROKEN] over link [10.1.1.1(Loopback1),
10.1.4.1]
02:48:17: rlm 1: link [10.1.1.2(Loopback2), 10.1.4.2] requests activation
02:48:17: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] is deactivated
02:48:17: rlm 1: [State_Recover, rx LINK_BROKEN] over link [10.1.1.2(Loopback2), 10.1.4.2]
02:48:17: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] = socket[10.1.1.1, 10.1.4.1]
02:48:17: rlm 1: [State_Recover, rx USER_SOCKET_OPENED] over link [10.1.1.1(Loopback1),
10.1.4.1] for user RLM_MGR
02:48:17: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] is opened
02:48:17: rlm 1: link [10.1.1.2(Loopback2), 10.1.4.2] = socket[10.1.1.2, 10.1.4.2]
02:48:17: rlm 1: [State_Recover, rx USER_SOCKET_OPENED] over link [10.1.1.2(Loopback2),
10.1.4.2] for user RLM_MGR
02:48:17: rlm 1: link [10.1.1.2(Loopback2), 10.1.4.2] is opened
02:48:17: rlm 1: link [10.1.1.1(Loopback1), 10.1.5.1] = socket[10.1.1.1, 10.1.5.1]
02:48:17: rlm 1: [State_Recover, rx USER_SOCKET_OPENED] over link [10.1.1.1(Loopback1),
10.1.5.1] for user RLM_MGR
02:48:17: rlm 1: link [10.1.1.1(Loopback1), 10.1.5.1] is opened
02:48:17: rlm 1: link [10.1.1.2(Loopback2), 10.1.5.2] = socket[10.1.1.2, 10.1.5.2]
02:48:17: rlm 1: [State_Recover, rx USER_SOCKET_OPENED] over link [10.1.1.2(Loopback2),
10.1.5.2] for user RLM_MGR
02:48:17: rlm 1: link [10.1.1.2(Loopback2), 10.1.5.2] is opened
02:48:17: rlm 1: [State_Recover, rx LINK_OPENED] over link [10.1.1.1(Loopback1), 10.1.4.1]
02:48:17: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] requests activation
02:48:17: rlm 1: [State_Recover, rx LINK_OPENED] over link [10.1.1.2(Loopback2), 10.1.4.2]
02:48:17: rlm 1: [State_Recover, rx START_ACK] over link [10.1.1.1(Loopback1), 10.1.4.1]
02:48:17: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] is activated
```


Related Commands	Command	Description
	clear interface	Resets the hardware logic on an interface.
	interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
	link (RLM)	Specifies the link preference.
	protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
	retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
	server (RLM)	Defines the IP addresses of the server.
	show rlm group statistics	Displays the network latency of the RLM group.
	show rlm group status	Displays the status of the RLM group.
	show rlm group timer	Displays the current RLM group timer values.
	timer	Overwrites the default setting of timeout values.

clear rudpv0 statistics

To clear the counters that track RUDP statistics, enter the **clear rudpv0 statistics** command in privileged EXEC mode.

clear rudpv0 statistics

Syntax Description This command has no arguments or keywords.

Defaults The statistical information accumulates.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(7)XR	This command was introduced.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples The following example shows how to clear RUDP statistics on a Cisco 2611 (Cisco SLT):

```
clear rudpv0 statistics
```

Related Commands	Command	Description
	show rudpv0 failures	Displays RUDP information about failed connections and the reasons for them. clear rudpv0 statistics resets the counters for these statistics to 0.
	show rudpv0 statistics	Displays RUDP information about number of packets sent, received, and so forth. clear rudpv0 statistics resets the counters for these statistics to 0.

clear rudpv1 statistics

To clear the counters that track Reliable User Datagram Protocol (RUDP) statistics, use the **clear rudpv1 statistics** command in privileged EXEC mode.

clear rudpv1 statistics

Syntax Description	This command has no arguments or keywords.

Defaults	The statistical information accumulates.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced.

Usage Guidelines	This command clears all statistics.

Examples	To clear all RUDP statistics for all available session-groups, see this example: Router# clear rudpv1 statistics

Related Commands	Command	Description
	debug rudpv1	Displays debugging information for RUDP.
	show rudpv1	Displays RUDP information.

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.

Defaults There are no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
	12.0(7)XK	Support for this command was extended to the Cisco MC3810 and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T on the Cisco MC3810 multiservice concentrator and Cisco 3600 series routers and was made generally available.

Usage Guidelines None

Examples The following example shows all SGCP statistics being cleared:

```
Router# clear sgcp statistics
```

Related Commands	Command	Description
	show sgcp statistics	Displays global statistics for SGCP packet counts.

clear ss7 sm stats

To clear the counters that track Session Manager statistics, use the **clear ss7 sm stats** command in privileged EXEC mode.

clear ss7 sm stats

Syntax Description	This command has no arguments or keywords.

Defaults	The statistical information accumulates.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(7)XR	This command was introduced.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples	The following example shows how to clear Session Manager statistics on a Cisco 2611:

```
clear ss7 sm stats
```

Related Commands	Command	Description
	show ss7 sm stats	Displays Session Manager information about number of packets queued, received, and so forth. clear ss7 sm stats resets the counters for these statistics to 0.

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	<i>slot/port</i>	(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.

Defaults	There are no defaults.

Command Modes	Privileged EXEC

Command History	Release	Modification
	11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines	If you do not specify a voice port, all calls on all voice ports are cleared. A confirmation prompt is displayed. There is no no form of this command.

Examples	The following example clears all calls on voice port 1/2 on the Cisco MC3810: <pre>Router# clear voice port 1/2</pre>

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*

Syntax Description	<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.

Defaults	There are no defaults.

Command Modes	CES configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced on the Cisco 3600 series routers.

Usage Guidelines

This command is used on Cisco 3600 series routers that have OC-3/STM-1 ATM CES network modules. To support synchronous or synchronous residual time stamp (SRTS) clocking modes, you must specify a primary reference source to synchronize the flow of constant bit rate (CBR) data from its source to its destination.

You can specify up to four clock priorities. The highest priority active interface in the router supplies primary reference source to all other interfaces that require network clock synchronization services. The fifth priority is the local oscillator on the network module.

Use the **show ces clock-select** command to display the currently configured clock priorities on the router.

Examples	The following example defines two clock priorities on the router:

```
clock-select 1 cbr 2/0
clock-select 2 atm 2/0
```

Related Commands	Command	Description
	channel-group	Configures the timing recovery clock for the CES interface.
	clock source	Configures a transmit clock source for the CES interface.
	show ces clock	Displays which ports are designated as network clock sources.

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 7200 and 7500 Series Routers

```
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 AS5300 and AS5800 Universal Access Servers

```
codec codec {g711alaw | g711ulaw | g723ar53 | g723ar63 | g723r53 | g723r63 | g726r16 | g726r24 |
g726r32 | g726r53 | g726r63 | g728 | g729abr8 | g729ar8 | g729br8 | g729r8 | gsmefr | gsmfr}
[bytes payload_size]
```

```
no codec {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 7200 and 7500 Series Routers:**

codec	Sets the codec options that you can use when you execute this command.
<i>codec</i>	Codec options are as follows: • clear-channel—Clear channel at 64,000 bits per second (bps). • g711alaw—G.711 a-Law at 64,000 bits per second. • g711ulaw—G.711 u-Law at 64,000 bps. • g723ar53—G.723.1 Annex A at 5300 bps. • g723ar63—G.723.1 Annex A at 6300 bps. • g723r53—G.723.1 at 5300 bps. • g723r63—G.723.1 at 6300 bps. • g726r16—G.726 at 16,000 bps. • g726r24—G.726 at 24,000 bps. • g726r32—G.726 at 32,000 bps. • g728—G.728 at 16,000 bps. • g729abr8—G.729 Annex A and B at 8000 bps. • g729ar8—G.729 Annex A at 8000 bps. • g729br8—G.729 Annex B at 8000 bps. • g729r8—G.729 at 8000 bps. This is the default codec. • gsmefr—Global System for Mobile Communications Enhanced Rate Codecs (GSMEFR) at 12,200 bps. • gsmfr—Global System for Mobile Communications Full Rate (GSMFR) at 13200 bps.
bytes	(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 12 for valid entries and default values.

For the Cisco AS5300 and AS5800 Universal Access Servers:

codec	Sets the codec options that you can use when you execute this command.
<i>codec</i>	Codec options are as follows: • g711alaw—G.711 a-Law at 64,000 bits per second. • g711ulaw—G.711 u-Law at 64,000 bps. • g723ar53—G.723.1 Annex A at 5300 bps. • g723ar63—G.723.1 Annex A at 6300 bps. • g723r53—G.723.1 at 5300 bps. • g723r63—G.723.1 at 6300 bps. • g726r16—G.726 at 16,000 bps. • g726r24—G.726 at 24,000 bps. • g726r32—G.726 at 32,000 bps. • g728—G.728 at 16,000 bps. • g729abr8—G.729 Annex A and B at 8000 bps. • g729ar8—G.729 Annex A at 8000 bps. • g729br8—G.729 Annex B at 8000 bps. • g729r8—G.729 at 8000 bps. This is the default codec. • gsmefr—Global System for Mobile Communications Enhanced Rate Codecs (GSMEFR) at 12,200 bps. • gsmfr—Global System for Mobile Communications Full Rate (GSMFR) at 13200 bps.
bytes	(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 12 for valid entries and default values.

For the Cisco MC3810 Multiservice Concentrators:

codec	Sets the codec options that you can use when you execute this command.
<i>codec</i>	Codec options are as follows: • clear-channel—Clear channel at 64,000 bits per second (bps). • g711alaw—G.711 a-Law at 64,000 bits per second. • g711ulaw—G.711 u-Law at 64,000 bps. • g723ar53—G.723.1 Annex A at 5300 bps. • g723ar63—G.723.1 Annex A at 6300 bps. • g723r53—G.723.1 at 5300 bps. • g723r63—G.723.1 at 6300 bps. • g726r16—G.726 at 16,000 bps. • g726r24—G.726 at 24,000 bps. • g726r32—G.726 at 32,000 bps. • g728—G.728 at 16,000 bps. • g729abr8—G.729 Annex A and B at 8000 bps. • g729ar8—G.729 Annex A at 8000 bps. • g729br8—G.729 Annex B at 8000 bps. • g729r8—G.729 at 8000 bps. This is the default codec. • gsmeifr—Global System for Mobile Communications Enhanced Rate Codecs (GSMEFR) at 12,200 bps. • gsmfr—Global System for Mobile Communications Full Rate (GSMFR) at 13,200 bps.
<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 12 for valid entries and default values.

Defaults

g729r8, 30-byte payload for VoFR and VoATM
g729r8, 20-byte payload for VoIP

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This VoIP dial peer configuration command was introduced on the Cisco 3600 series routers.
11.3(3)T	Support for Cisco 2600 series routers was added.
12.0(3)T	Support for the Cisco AS5300 universal access server was added. The clear-channel keyword is not supported.

Release	Modification
12.0(4)T	Support was added for the Cisco 3600 and 7200 series routers and for the MC3810 multiservice concentrator. The command was modified for Voice over Frame Relay (VoFR) dial peers.
12.0(5)XE	Additional <i>codec</i> choices and other options were added.
12.0(5)XK	The g729br8 and pre-ietf <i>codec</i> choices were added for the Cisco 2600 and 3600 series routers.
12.0(7)T	Support for the Cisco AS5800 universal gateway was added. Additional voice coder rates of speech were added. There is no support for the clear-channel keyword.
12.0(7)XK	The g729abr8 and g729ar8 <i>codec</i> choices were added for the Cisco MC3810 multiservice concentrator, and the keyword pre-ietf was deleted.
12.1(1)T	The <i>codec</i> keyword additions and the pre-ietf deletion in Cisco IOS Release 12.0(7)XK were integrated in Cisco IOS Release 12.1(1)T.
12.1(5)	The gsmefr and gsmfr <i>codec</i> keywords were added.

Usage Guidelines



Note

VoFR and VoATM do not support the gsmefr and gsmfr codecs.

Use this command to define a specific voice coder rate of speech and payload size for a VoIP dial peer or for a VoFR dial peer. This command is also used for VoATM.

A specific *codec* type can be configured on the dial peer as long as it is supported by the setting used with the **codec complexity** voice-card configuration command. The **codec complexity** command is voice-card specific and platform specific. The **codec complexity** voice-card configuration command is set to either high or medium.

If the **codec complexity** command is set to **high**, the following options are available: **g711alaw**, **g711ulaw**, **g723ar53**, **g723ar63**, **g723r53**, **g723r63**, **g726r16**, **g726r24**, **g726r32**, **g728**, **g729r8**, or **g729br8**.

If the **codec complexity** command is set to **medium**, the following options are available: **g711alaw**, **g711ulaw**, **g726r16**, **g726r24**, **g726r32**, **g729r8**, or **g729br8**.

The **codec** dial peer configuration command is particularly useful when you must change to a small-bandwidth codec. Large-bandwidth codecs, such as G.711, do not fit in a small-bandwidth link. However, the **g711alaw** and **g711ulaw** codecs provide higher quality voice transmission than other codecs. The **g729r8** codec provides near-toll quality with considerable bandwidth savings.

If codec values for the dial peers of a connection do not match, the call fails.

You can change the payload of each VoIP frame by using the *bytes* setting; you can change the payload of each VoFR frame by using the **bytes** keyword with the *payload_size* setting. However, increasing the payload size can add processing delay for each voice packet.

Table 12 describes the voice payload options and default values for the codecs and packet voice protocols.

Table 12 Voice Payload-per-Frame Options and Defaults

Codec	Protocol	Voice Payload Options (in bytes)	Default Voice Payload (in bytes)
g711alaw	VoIP	80, 160	160
g711ulaw	VoFR	40 to 240 in multiples of 40	240
	VoATM	40 to 240 in multiples of 40	240
g723ar53	VoIP	20 to 220 in multiples of 20	20
g723r53	VoFR	20 to 240 in multiples of 20	20
	VoATM	20 to 240 in multiples of 20	20
g723ar63	VoIP	24 to 216 in multiples of 24	24
g723r63	VoFR	24 to 240 in multiples of 24	24
	VoATM	24 to 240 in multiples of 24	24
g726r16	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
g726r24	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
g726r32	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
g728	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
g729abr8	VoIP	10 to 230 in multiples of 10	20
g729ar8	VoFR	10 to 240 in multiples of 10	30
g729br8	VoATM	10 to 240 in multiples of 10	30
g729r8			

For toll quality, use the **g711alaw** or **g711ulaw** keyword. These values provide high-quality voice transmission but use a significant amount of bandwidth. For nearly toll quality (and a significant savings in bandwidth), use the **g729r8** keyword.

On the Cisco MC3810 multiservice concentrator, this command was first supported as a voice port command. On the Cisco MC3810 multiservice concentrator, you can also assign codec values to the voice port. If configuring calls to a Cisco MC3810 multiservice concentrator running software versions prior to 12.0(4)T, configure the **codec** command on the voice port. If configuring Cisco trunk permanent calls, configure the **codec** command on the dial peer. If you configure the **codec** command on the dial peer for VoFR permanent calls on the Cisco MC3810, the dial peer **codec** command setting overrides the **codec** setting configured on the voice port.

**Note**

For regular switched calls on the Cisco MC3810 multiservice concentrator, the codec value must be configured on the voice port, and the voice payload size is not configurable.

**Note**

The **clear-channel** keyword is not supported on Cisco AS5300 and AS5800 universal gateways.

Examples

The following example shows how to configure a voice coder rate that provides toll quality voice with a payload of 120 bytes per voice frame on a Cisco 2600 series routers or 3600 series router acting as a terminating node. The example configuration begins in global configuration mode and is for VoFR dial peer 200.

```
dial-peer voice 200 vofr
  codec g711alaw bytes 120
```

The following example configures a voice coder rate for VoIP dial peer 10 that provides toll quality but uses a relatively high amount of bandwidth:

```
dial-peer voice 10 voip
  codec g711alaw
```

Related Commands

Command	Description
codec complexity	Specifies call density and codec complexity based on the codec used.
codec (DSP interface dsp farm)	Specifies call density and codec complexity.
codec (voice port)	Specifies voice compression on the Cisco MC3810 multiservice concentrator voice port.
show dial peer voice	Displays the codec setting for dial peers.

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.

Defaults

Medium complexity

Command Modes

DSP interface dsp farm

Command History

Release	Modification
12.0(5)XE	This command was introduced on the Cisco 7200 series routers.
12.1(1)T	This command was integrated into Cisco Release 12.1(1)T.
12.1(3)T.	Support was added for the Cisco 7500 series routers.

Usage Guidelines

This command is supported on only the Cisco 7200 and 7500 series routers.

Codec complexity refers to the amount of processing required to perform compression. Codec complexity affects the number of calls, referred to as call density, that can take place on the DSPfarm interfaces. The greater the codec complexity, the fewer the calls that are handled. For example, G.711 requires less DSP processing than G.728, so as long as the bandwidth is available, more calls can be handled simultaneously by using the G.711 standard than by using G.728.

The DSPinterface dspfarm **codec** complexity setting affects the options available for the **codec** dial peer configuration command.

To change codec complexity, you must first remove any configured channel associated signaling (CAS) or DS0 groups and then reinstate them after the change.



Note

On the Cisco 2600 series routers, 3600 series, and MC3810 multiservice concentrator, codec complexity is configured using the **codec complexity** command in voice-card configuration mode.

Examples

The following example configures the DSPfarm interface 1/0 on the Cisco 7200 series routers to support high compression:

```
dspint DSPFarm 1/0
  codec high
```

Related Commands	Command	Description
	codec (dial peer)	Specifies the voice codec rate of speech for a dial peer.
	codec complexity	Specifies call density and codec complexity based on the codec standard you are using.

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 { **itut** | **atmf** | **custom** } *profile-number* *codec*

no codec aal2-profile

Syntax Description

itut	Specifies the <i>profile-number</i> as an ITU-T type.
atmf	Specifies the <i>profile-number</i> as an ATMF type.
custom	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: • 1 = G.711ulaw • 2 = G.711ulaw with silence insertion descriptor (SID) • 7 = G.711ulaw and G.729ar8 For ATMF: None. ATMF is not supported. For custom: • 100 = G.711ulaw and G.726r32 • 110 = G.711ulaw, G.726r32, and G.729ar8
<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: • For ITU 1—g711ulaw • For ITU 2—g711ulaw • For ITU 7—g711ulaw or g729ar8 • For custom 100—g711ulaw or g726r32 • For custom 110—g711ulaw or g726r32 or g729ar8

Defaults

The default is ITU profile 1 (G.711ulaw).

Command Modes

Dial peer configuration

Command History

Release	Modification
12.1(1)XA	The command was introduced for the Cisco MC3810 multiservice concentrator.
12.1(2)T	This command was integrated into the 12.1(2)T release.

Usage Guidelines

Use this command to configure the DSP to operate with a specified profile type and codec.

You must enter the **session protocol aal2-trunk** command before configuring the codec AAL2 profile.

This command is used instead of the **codec** command for ATM Adaptation Layer 2 (AAL2) trunk applications.

Examples

The following example sets the codec AAL2 profile type to ITU and configures a profile number of 7, enabling codec G.729ar8:

```
dial-peer voice 100 voatm
 session protocol aal2-trunk
 codec aal2-profile itu 7 g729ar8
```

The following example sets the codec AAL2 profile type to custom and configures a profile number of 100, enabling codec G.726r32:

```
dial-peer voice 200 voatm
 session protocol aal2-trunk
 codec aal2-profile custom 100 g726r32
```

Related Commands

Command	Description
session protocol (dial peer)	Establishes a session protocol for calls between the local and remote routers via the packet network.

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: • g711alaw—G.711 A-law 64,000 bps. • g711ulaw—G.711 U-law 64,000 bps. • g723ar53—G.723.1 Annex A 5300 bps. • g723ar63—G.723.1 Annex A 6300 bps. • g723r53—G.723.1 5300 bps. • g723r63—G.723.1 6300 bps. • g723r16—G.726 16,000 bps. • g726r24—G.726 24,000 bps. • g726r32—G.726 32,000 bps. • g728—G.728 16,000 bps. • g729r8—G.729 8000 bps. (default) • g729br8—G.729 Annex B 8000 bps. • fax relay—2400 bps, 4800 bps, 7200 bps, 9600 bps, 12 kbps, and 14.4 kbps.
medium	Each DSP supports four voice channels encoded in any of the following formats: • g711alaw—G.711 a-Law 64,000 bps. • g711ulaw—G.711 u-Law 64,000 bps. • g726r16—G.726 16,000 bps. • g726r24—G.726 24,000 bps. • g726r32—G.726 32,000 bps. • g729r8—G.729 Annex A 8000 bps. • G729br8—G.729 Annex B with Annex A 8000 bps. • fax relay—2400 bps, 4800 bps, 7200 bps, 9600 bps, 12 kbps, and 14.4 kbps.

Defaults medium complexity

Command Modes Voice-card configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced for the Cisco 2600 and Cisco 3600 series routers.
12.0(7)T	This command was integrated into the 12.0(7)T release.
12.0(7)XK	This command was first supported on the Cisco MC3810 multiservice concentrator series for use with the high-performance compression module (HCM).
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Codec complexity refers to the amount of processing required to perform voice compression. Codec complexity affects the call density—the number of calls that can take place on the DSPs. With higher codec complexity, fewer calls can be handled. Select a higher codec complexity if that is required to support a particular codec or combination of codecs. Select a lower codec complexity to support the greatest number of voice channels, provided that the lower complexity is compatible with the particular codecs in use.

To change codec complexity, all the DSP voice channels must be in the idle state.

**Note**

In the Cisco MC3810 multiservice concentrator, this command is valid only with one or more HCMs installed, and you must specify voice card 0 in the command mode. If two HCMs are installed, the **codec complexity** command configures both HCMs at once.

Examples

The following example sets the codec complexity to high on a Cisco MC3810 multiservice concentrator containing one or two HCMs:

```
voice-card 0
  codec complexity high
```

The following example sets the codec complexity to high on voice card 1 in a Cisco 2600 or 3600 series router:

```
voice-card 1
  codec complexity high
```

Related Commands

Command	Description
ds0-group	Defines T1/E1 channels for compressed voice calls and the CAS method by which the router connects to the PBX or PSTN.
show voice dsp	Shows the current status of all DSP voice channels.

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*

Syntax Description		
<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. • clear-channel—Clear Channel 64,000 bps • g711alaw—G.711 A Law 64,000 bps • g711ulaw—G.711 u Law 64,000 bps • g723ar53—G.723.1 ANNEX-A 5,300 bps • g723ar63—G.723.1 ANNEX-A 6,300 bps • g723r53—G.723.1 5,300 bps • g723r63—G.723.1 6,300 bps • g726r16—G.726 16,000 bps • g726r24—G.726 24,000 bps • g726r32—G.726 32,000 bps • g728—G.728 16,000 bps • g729abr8—G.729 ANNEX-A & B 8,000 bps • g729br8—G.729 ANNEX-B 8,000 bps • g729r8—G.729 8000 bps • gsmefr—Global System for Mobile Communications Enhanced Full Rate (GSMEFR) 12,200 bps • gsmfr—Global System for Mobile Communications (GSM) Full Rate (GSMFR) 13,200 bps
bytes		(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.

Defaults No default behavior or values.

Command Modes Voice-class configuration

Command History

Release	Modification
12.0(2)XH	This command was introduced on the Cisco AS5300 universal access server.
12.0(7)T	This command was first supported on the Cisco 2600 and 3600 series routers.
12.0(7)XK	This command was first supported on the Cisco MC3810 multiservice concentrator.
12.1(2)T	Support for the Cisco MC3810 multiservice concentrator was integrated into Cisco Release IOS 12.1(2)T.
12.1(5)T	The codecs gsmefr and gsmfr were added.

Usage Guidelines

The routers at opposite ends of the WAN may have to negotiate the codec selection for the network dial peers. The codec preference command specifies the order of preference for selecting a negotiated codec for the connection. [Table 13](#) describes the voice payload options and default values for the codecs and packet voice protocols.

Table 13 Voice Payload-per-Frame Options and Defaults

Codec	Protocol	Voice Payload Options (in bytes)	Default Voice Payload (in bytes)
g711alaw g711ulaw	VoIP VoFR VoATM	80, 160 40 to 240 in multiples of 40 40 to 240 in multiples of 40	160 240 240
g723ar53 g723r53	VoIP VoFR VoATM	20 to 220 in multiples of 20 20 to 240 in multiples of 20 20 to 240 in multiples of 20	20 20 20
g723ar63 g723r63	VoIP VoFR VoATM	24 to 216 in multiples of 24 24 to 240 in multiples of 24 24 to 240 in multiples of 24	24 24 24
g726r16	VoIP VoFR VoATM	20 to 220 in multiples of 20 10 to 240 in multiples of 10 10 to 240 in multiples of 10	40 60 60
g726r24	VoIP VoFR VoATM	30 to 210 in multiples of 30 15 to 240 in multiples of 15 30 to 240 in multiples of 15	60 90 90
g726r32	VoIP VoFR VoATM	40 to 200 in multiples of 40 20 to 240 in multiples of 20 40 to 240 in multiples of 20	80 120 120
g728	VoIP VoFR VoATM	10 to 230 in multiples of 10 10 to 240 in multiples of 10 10 to 240 in multiples of 10	40 60 60
g729abr8 g729ar8 g729br8 g729r8	VoIP VoFR VoATM	10 to 230 in multiples of 10 10 to 240 in multiples of 10 10 to 240 in multiples of 10	20 30 30

Examples

The following example creates codec preference list 99 and applies it to dial peer 1919:

```
voice class codec 99
codec preference 1 g711alaw
codec preference 2 g711ulaw bytes 80
codec preference 3 g723ar53
codec preference 4 g723ar63 bytes 144
codec preference 5 g723r53
codec preference 6 g723r63 bytes 120
codec preference 7 g726r16
codec preference 8 g726r24
codec preference 9 g726r32 bytes 80
codec preference 10 g729br8
codec preference 11 g729r8 bytes 50
codec preference 12 gsmefr
end
dial-peer voice 1919 voip
voice-class codec 99
```

Related Commands

Command	Description
voice class codec	Enters voice-class configuration mode and assigns an identification tag number to a codec voice class.
voice-class codec (dial peer)	Assigns a previously configured codec selection preference list to a dial peer.

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.

Defaults	Enabled

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 series routers.

Usage Guidelines	Use the comfort-noise command to generate background noise to fill silent gaps during calls if VAD is activated. If the comfort-noise command is not enabled, and VAD is enabled at the remote end of the connection, the user will hear dead silence when the remote party is not speaking.

The configuration of the **comfort-noise** command only affects the silence generated at the local interface; it does not affect the use of VAD on either end of the connection or the silence generated at the remote end of the connection.



Note	On the Cisco MC3810 multiservice concentrator, this command cannot be disabled.

Examples	The following example enables background noise on the Cisco 3600 series routers:

```
voice-port 1/0/0
 comfort-noise
```

Related Commands	Command	Description
	vad (dial peer configuration)	Enables VAD for the calls using a particular dial peer.
	vad (voice-port configuration)	Enables VAD for the calls using a particular voice port on the Cisco MC3810 multiservice concentrator.

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

u-law	Specifies the North American U-law ITU-T PCM encoding standard.
a-law	Specifies the European a-law ITU-T PCM encoding standard.

Defaults

u-law (T1 digital)
a-law (E1 digital)

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was first introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

If you have a Cisco MC3810 multiservice concentrator or Cisco 3660 router, the **compand-type a-law** command must be configured on the analog ports only. The Cisco 2660, 3620, and 3640 routers do not require configuration of the **compand-type a-law** command, however, if you request a list of commands, the **compand-type a-law** command will display.



Note On the Cisco 3600 series routers router, the U-law and a-law settings are configured using the **codec** dial peer configuration command.

Examples

The following example configures a-law encoding on voice port 1/1 on the Cisco MC3810 multiservice concentrator:

```
voice-port 1/1
 compand-type a-law
```

Related Commands

Command	Description
codec (voice-port configuration)	Configures voice compression on the Cisco MC3810 multiservice concentrator voice port.

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

tx-a-bit	Sends A bit.
tx-b-bit	Sends B bit.
tx-c-bit	Sends C bit.
tx-d-bit	Sends D bit.
rx-a-bit	Receives A bit.
rx-b-bit	Receives B bit.
rx-c-bit	Receives C bit.
rx-d-bit	Receives D bit.
on	Forces the bit state to be 1.
off	Forces the bit state to be 0.
invert	Inverts the bit state.

Defaults

The signaling format is not manipulated (for all sent or received A, B, C, and D bits).

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series routers.
12.1(2)T	The modifications in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use the **condition** command to manipulate the sent or received bit patterns to match expected patterns on a connected device. Be careful not to destroy the information content of the bit pattern. For example, forcing the A-bit on or off will prevent Foreign Exchange Office (FXO) interfaces from being able to generate both an on-hook and off-hook state.

The **condition** command is applicable to digital voice ports only.

Examples

The following example manipulates the signaling format bit pattern on digital voice port 0:5 on a Cisco MC3810 multiservice concentrator:

```
voice-port 0:5
 condition tx-a-bit invert
 condition rx-a-bit invert
```

The following example manipulates the signaling format bit pattern on voice port 1/0:0 on a Cisco 2600 or Cisco 3600 router:

```
voice-port 1/0:0
 condition tx-a-bit invert
 condition rx-a-bit invert
```

Related Commands

Command	Description
define	Defines the transmit and receive bits for North American E&M and E&M MELCAS voice signaling.
ignore	Configures the North American E&M or E&M MELCAS voice port to ignore specific receive bits.

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.
atm	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).
T1	Specifies a T1 port.
E1	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 tdm-group command. Valid values are from 0 to 23 for T1 and from 0 to 30 for E1.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced for ATM interfaces on the Cisco 2600 and 3600 series routers.

Usage Guidelines

This command is used on Cisco 2600 and 3600 series routers to provide connections between T1/E1 and ATM interfaces. This command is used after all interfaces are configured.

Once TDM groups are created on two different physical ports, you can use the **connect** command to start the passage of data between the ports. If a crosspoint switch is provided in the advanced integration module (AIM) slot, the connections can extend between ports on different cards. Otherwise, the connection will be restricted to ports on the same VWIC card.

The voice/WAN interface card (VWIC) can make a connection only if the number of time slots at the source and destination are the same. For the connection to be error free, the two ports must be driven by the same clock source; otherwise, slips will occur.

Examples

The following example shows how the ATM permanent virtual circuit (PVC) and T1 TDM group are set up and then connected:

```
interface atm 1/0
 pvc pvc1 0/100 ces
 exit
controller T1 1/1
 tdm-group 3 timeslots 13-24 type e&m
 exit
connect tdm1 atm 1/0 pvc1 0/100 T1 1/1 3
```

Related Commands

Command	Description
tdm-group	Creates TDM groups that can be connected.

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.
t1	Specifies a T1 port.
e1	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 tdm-group 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 tdm-group command. Valid values are from 0 to 23 for T1 and from 0 to 30 for E1.

Defaults

There is no drop-and-insert connection between the ports.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XK	The command was introduced on the Cisco 2600 and 3600 series.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.1(1)T	The command was modified to accommodate two channel groups on a port for 1- and 2-port T1/E1 multiflex voice/WAN interface cards (VWICs) on the Cisco 3600 series routers.

Usage Guidelines

The **connect** command creates a named connect between two TDM groups associated with drop-and-insert ports on T1 or E1 interfaces where you have already defined the groups by using the **tdm-group** command.

connect (drop-and-insert)

Once TDM groups are created on two different physical ports, you can use the **connect** command to start the passage of data between the ports. If a crosspoint switch is provided in the AIM slot, the connections can extend between ports on different cards. Otherwise, the connection will be restricted to ports on the same VWIC card.

The VWIC card can make a connection only if the number of time slots at the source and destination are the same. For the connection to be error-free, the two ports must be driven by the same clock source; otherwise, “slips” will occur.

Examples

The following example shows a fractional T1 terminated on port 0 using time slots 1 through 8; a fractional T1 is terminated on port 1 using time slots 2 through 12; and time slots 13 through 20 from port 0 are connected to time slots 14 through 21 on port 1 by using the **connect** command:

```
controller t1 0/0
 channel-group 1 timeslots 1-8
 tdm-group 1 timeslots 13-20
 exit
controller t1 0/1
 channel-group 1 timeslots 2-12
 tdm-group 2 timeslot 14-21
 exit
connect exampleconnection t1 0/0 1 t1 0/1 2
```

Related Commands

Command	Description
show connect	Displays configuration information about drop-and-insert connections that have been configured on a router.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for TDM cross-connect.

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	
plar	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.
tie-line	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.
plar-opx	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.
trunk	Specifies a connection that emulates a permanent trunk connection to a PBX. A trunk connection remains permanent in the absence of any active calls.
answer-mode	(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 trunk keyword.

Defaults No connection mode is specified.

Command Modes Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 series routers.
	11.3(1)MA1	This command was first supported on the Cisco MC3810 multiservice concentrator, and the tie-line keyword was first made available on the Cisco MC3810 multiservice concentrator.
	11.3(1)MA5	The plar-opx keyword was first made available on the Cisco MC3810 multiservice concentrator as the plar-opx-ringrelay keyword. The keyword was shortened in a subsequent release.
	12.0(2)T	This command was integrated into Cisco IOS Release 12.0(2)T.

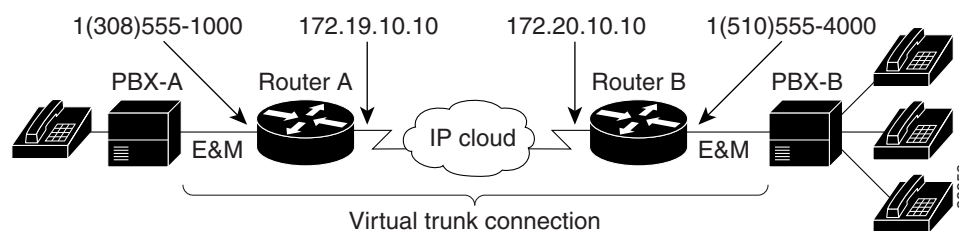
Release	Modification
12.0(3)XG	The trunk keyword was made available on the Cisco MC3810 multiservice concentrator. The trunk answer-mode option was added.
12.0(4)T	The trunk and trunk answer-mode additions were integrated in Cisco IOS Release 12.0(4)T.
12.0(7)XK	This command was unified across the Cisco 2600, 3600, and MC3810 multiservice concentrator platforms.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use the **connection** command to specify a connection mode for a specific interface. For example, use the **connection plar** command to specify a PLAR interface. The string you configure for this command is used as the called number for all incoming calls over this connection. The destination peer is determined by the called number.

Use the **connection trunk** command to specify a permanent tie-line connection to a PBX. Voice over IP simulates a trunk connection by creating virtual trunk tie lines between PBXs connected to Cisco devices on each side of a VoIP connection (see Figure 4). In this example, two PBXs are connected using a virtual trunk. PBX-A is connected to Router A via an E&M voice port; PBX-B is connected to Router B via an E&M voice port. The Cisco routers spoof the connected PBXs into believing that a permanent trunk tie line exists between them.

Figure 4 Virtual Trunk Connection



In configuring virtual trunk connections in Voice over IP, the following restrictions apply:

- You can use the following voice port combinations:
 - Ear and mouth (E&M) to E&M (same type)
 - Foreign Exchange Station (FXS) to Foreign Exchange Office (FXO)
 - FXS to FXS (with no signaling)
- Do not perform number expansion on the destination pattern telephone numbers configured for trunk connection.
- Configure both end routers for trunk connections.
- The connected Cisco routers must be Cisco 2600 or Cisco 3600 series routers.



Note Because virtual trunk connections do not support number expansion, the destination patterns on each side of the trunk connection must match exactly.

To configure one of the devices in the trunk connection to act as slave and only receive calls, use the **answer-mode** option with the **connection trunk** command when configuring that device.

**Note**

When using the **connection trunk** command, you must enter the **shutdown** command followed by the **no shutdown** command on the voice port.

VoIP establishes the trunk connection immediately after it is configured. Both ports on either end of the connection are dedicated until you disable trunking for that connection. If for some reason the link between the two switching systems goes down, the virtual trunk reestablishes itself after the link comes back up.

Use the **connection tie-line** command when the dial plan requires that additional digits be added in front of any digits dialed by the PBX and that the combined set of digits be used to route the call onto the network. The operation is similar to the **connection plar** command operation, but in this case the tie-line port waits to collect digits from the PBX. The tie-line digits are automatically stripped by a terminating port.

If the **connection** command is not configured, the standard session application outputs a dial tone when the interface goes off-hook until enough digits are collected to match a dial peer and complete the call.

Examples

The following example shows PLAR selected as the connection mode on a Cisco 3600 series routers router, with a destination telephone number of 555-9262:

```
voice-port 1/0/0
connection trunk 5559262
```

The following example shows the tie-line selected as the connection mode on a Cisco MC3810, with a destination telephone number of 555-9262:

```
voice-port 1/1
connection tie-line 5559262
```

The following example specifies a PLAR off-premises extension connection on a Cisco 3600 series routers router, with a destination telephone number of 555-9262:

```
voice-port 1/0/0
connection plar-opx 5559262
```

The following example shows configuration of a Cisco 3600 series routers router for a trunk connection and specifies that it will establish the trunk only when it receives an incoming call:

```
voice-port 1/0/0
connection trunk 5559262 answer-mode
```

The following examples show configuration of the routers on both sides of a VoIP connection (as illustrated in [Figure 4](#)) to support trunk connections.

Router A

```
voice-port 1/0/0
connection trunk +15105554000
dial-peer voice 10 pots
destination-pattern +13085551001
port 1/0/0
dial-peer voice 100 voip
session-target ipv4:172.20.10.10
destination-pattern +15105554000
```

Router B

```
voice-port 1/0/0
 connection trunk +13085551000
dial-peer voice 20 pots
 destination-pattern +15105554001
 port 1/0/0
dial-peer voice 200 voip
 session-target ipv4:172.19.10.10
 destination-pattern +13085551000
```

Related Commands

Command	Description
destination-pattern	Specifies the prefix or the full E.164 telephone number for a dial peer.
dial peer voice	Enters dial peer configuration mode and specifies the voice encapsulation type.
session-protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.
session-target	Configures a network-specific address for a dial peer.
voice-port	Enters voice-port configuration mode.

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*

Syntax Description

<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.

Defaults

The default connection timeout is 3600 seconds (1 hour).

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 and Cisco 3600 series and on the Cisco AS5300 universal access server.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

The router maintains the connection for the configured period in anticipation of future communication exchanges to the same server.

Examples

The following example shows a connection configured to be maintained for 3600 seconds after completion of a communications exchange:

```
settlement 0
connection-timeout 3600
```

Related Commands

Command	Description
customer-id	Sets the customer identification.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.

Command	Description
session-timeout	Sets the session timeout.
settlement	Enters the settlement configuration mode.
show settlement	Displays the configuration for all settlement server transactions.
shutdown	Brings up/shuts down the settlement provider.
type	Specifies the provider type.
url	Specifies the Internet service provider address.

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*

Syntax Description

<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.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

Use the **copy flash vfc** command to use the standard copy user interface to copy a new version of VCWare from the Cisco AS5300 universal access server motherboard to VFC Flash memory. The VFC is a plug-in feature card for the Cisco AS5300 universal access server and has its own Flash memory storage for embedded firmware. For more information about VFCs, refer to *Installing Voice over IP Feature Cards in Cisco AS5300 Universal Gateways*.

Once the VCWare file has been copied, use the **unbundle vfc** command to uncompress and install VCWare.

Examples

The following example copies a new version of VCWare from the Cisco AS5300 universal access server motherboard to VFC Flash memory:

```
Router# copy flash vfc 0
```

Related Commands

Command	Description
copy tftp vfc	Copies a new version of VCWare from a TFTP server to VFC Flash memory.
unbundle vfc	Unbundles the current running image of VCWare or DSPWare into separate files.

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*

Syntax Description

<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.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

Use the **copy tftp vfc** command to copy a new version of VCWare from a TFTP server to VFC Flash memory. The VFC is a plug-in feature card for the Cisco AS5300 universal access server and has its own Flash storage for embedded firmware. For more information about VFCs, refer to *Installing Voice Over IP Feature Cards in Cisco AS5300 Universal Gateways*.

Once the VCWare file has been copied, use the **unbundle vfc** command to uncompress and install VCWare.

Examples

The following example copies a file from the TFTP server to VFC Flash memory:

```
Router# copy tftp vfc 0
```

Related Commands

Command	Description
copy flash vfc	Copies a new version of VCWare from the Cisco AS5300 universal access server motherboard to VFC Flash memory.
unbundle vfc	Unbundles the current running image of VCWare or DSPWare into separate files.

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 14 . Keywords for ISDN PRI signaling are contained in Table 14 . 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.

Defaults

The **northamerica** keyword is for the Cisco MC3810 multiservice concentrator for versions prior to Cisco IOS Release 12.0(4)T and for ISDN PRI.

The **us** keyword is for the Cisco MC3810 multiservice concentrator for Cisco IOS Release 12.0(4)T and higher and for E1 R2 signaling.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.
11.3(1)MA	The full keyword names for the countries were first supported on the Cisco MC3810 multiservice concentrator.
12.0(4)T	Support was added for the ISO 3166 two-letter country codes on the Cisco MC3810 multiservice concentrator.
12.1(5)XM	The keywords for Egypt, Ghana, Jordan, Kenya, Lebanon, Nepal, Nigeria, Pakistan, Panama, Saudi Arabia, and Zimbabwe were added.

Usage Guidelines

Use the **cptone** command to specify a regional analog voice interface-related default tone, ring, and cadence setting for a specified voice port.

This command affects only the tones generated at the local interface. It does not affect any information passed to the remote end of a connection or any tones generated at the remote end of a connection.

If your device is configured to support E1 R2 signaling, the E1 R2 signaling type (whether ITU, ITU variant, or local variant as defined by the **cas-custom** command) must match the appropriate pulse code modulation (PCM) encoding type as defined by the **cptone** command. For countries for which a **cptone** value has not yet been defined, you can try the following:

- If the country uses a-Law E1 R2 signaling, use the **gb** value for the **cptone** command.
- If the country uses U-law E1 R2 signaling, use the **us** value for the **cptone** command.

Table 14 lists valid entries for the *locale* argument.

Table 14 *cptone locale Argument Values*

Argument Value	Country
ar	Argentina
au	Australia
at	Austria
be	Belgium
br	Brazil
ca	Canada
cn	China
co	Colombia
cz	Czech Republic
dk	Denmark
eg	Egypt
fi	Finland
fr	France
de	Germany
gb	Great Britain
gh	Ghana
gr	Greece
hk	Hong Kong
hu	Hungary
is	Iceland
in	India
id	Indonesia
ie	Ireland
il	Israel
it	Italy
jo	Jordan
jp	Japan
ke	Kenya
kr	Korea Republic

Table 14 *cptone locale Argument Values (continued)*

Argument Value	Country
lb	Lebanon
lu	Luxembourg
my	Malaysia
mx	Mexico
ng	Nigeria
nl	Netherlands
np	Nepal
nz	New Zealand
no	Norway
pa	Panama
pe	Peru
ph	Philippines
pk	Pakistan
pl	Poland
pt	Portugal
ru	Russian Federation
sa	Saudi Arabia
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
zw	Zimbabwe

Table 15 describes the argument values for ISDN PRI signaling.

Table 15 *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.
china	Specifies an analog voice interface-related default tone, ring, and cadence setting for China.
finland	Specifies an analog voice interface-related default tone, ring, and cadence setting for Finland.
france	Specifies an analog voice interface-related default tone, ring, and cadence setting for France.
germany	Specifies an analog voice interface-related default tone, ring, and cadence setting for Germany.
japan	Specifies an analog voice interface-related default tone, ring, and cadence setting for Japan.
northamerica	Specifies an analog voice interface-related default tone, ring, and cadence setting for North America.
sweden	Specifies an analog voice interface-related default tone, ring, and cadence setting for Sweden.
unitedkingdom	Specifies an analog voice interface-related default tone, ring, and cadence setting for the United Kingdom.

Examples

The following example configures United States as the call progress tone locale on the Cisco 3600 series routers, beginning in global configuration mode:

```
voice-port 1/0/0
cptone us
```

The following example configures Singapore as the call progress tone locale on the Cisco MC3810 multiservice concentrator, beginning in global configuration mode:

```
voice-port 1/1
cptone sg
```

The following example configures Japan as the call progress tone locale:

```
voice-port 0:D
cptone japan
```

The following example configures Brazil as the call progress tone locale on the Cisco AS5300 universal access server:

```
voice-port 1:0
cptone BR
description Brasil Tone
```

Related Commands

Command	Description
voice-port	Opens voice-port configuration mode.

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 Traffic 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.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

This command applies to Voice over Frame Relay and Voice over ATM on the Cisco MC3810.

Examples

The following example configures a pass-through cross-connect from serial port 0 to controller T1 1 on TDM group 20:

```
cross-connect 10 serial0 T1 1 20
```

Related Commands

Command	Description
supervisory disconnect	Configures a list of time slots for creating clear channel groups (pass-through) for TDM cross-connect.

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*

Syntax Description

<i>number</i>	Customer ID number as provided by the settlement server. The value range is from 0 to 2,147,483,647.

Defaults

The default customer ID is 0.

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 and 3600 series and on the AS5300.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

It is optional to identify a carrier or ISP with a settlement provider.

Examples

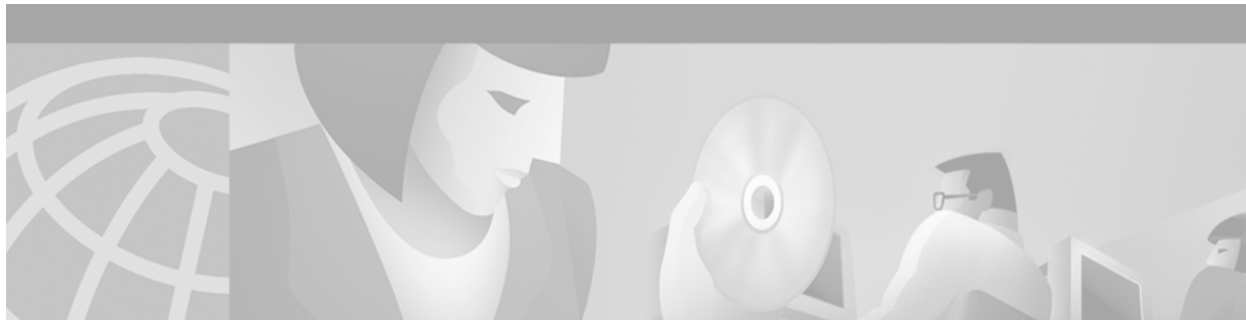
The following example identifies a carrier or service provider with the ID number of 1000:

```
settlement 0
 custom id 1000
```

Related Commands

Command	Description
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum number of simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters the settlement configuration mode.
show settlement	Displays the configuration for all settlement server transactions.

Command	Description
shutdown	Shuts down the settlement provider.
type	Specifies the provider type.
url	Specifies the Internet service provider address.



Cisco IOS Voice, Video, and Fax Commands: D Through F

This chapter presents the commands to configure and maintain Cisco IOS voice, video, and fax applications. The commands are presented in alphabetical order beginning with the letter D. Some commands required for configuring voice, video, and fax may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice, Video, and Fax Configuration Guide*.

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

inband-alerting	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.
max-forwards	Resets max-forwards to its default of 6.
retry {invite response bye cancel}	Resets the specified retry to its default (6 for invite and response; 10 for bye and cancel).
sip-server	Resets the sip-server to a null value.
timers {trying connect disconnect expires}	Resets the specified timer to its default (500 for trying, connect, and disconnect; 180,000 for expires).
transport	Resets transport to the default of both User Datagram Protocol (UDP) and TCP enabled.

Defaults

No default behavior or values.

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 and 3600 series routers and on the CiscoAS5300 universal access server.

Examples

The following example sets inband-alerting to its default.

```
sip-ua
 default inband-alerting
```

Related Commands

Command	Description
cap-list vfc	Adds a voice codec overlay file to the capability file list.

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.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)NA	This command was introduced on the Cisco AS5300 universal access server.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

When VCWare is unbundled, it automatically adds DSPWare to Flash memory, creates both the capability and default file lists, and populates these lists with the default files for that version of VCWare. The default file list includes the files that will be used to boot up the system.

Use the **default-file vfc** command to add a specified file to the default file list, replacing the existing default for that extension type.

Examples

The following example specifies that the bas-vfc-1.0.14.0.bin file, which is stored in VFC Flash memory, be added to the default file list:

```
default-file bas-vfc-1.0.14.0.bin vfc 0
```

Related Commands

Command	Description
cap-list vfc	Adds a voice codec overlay file to the capability file list.
delete vfc	Deletes a file from VFC Flash memory.

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

tx-bits	The bit pattern applies to the transmit signaling bits.
rx-bits	The bit pattern applies to the receive signaling bits.
seize	The bit pattern defines the seized state.
idle	The bit pattern defines the idle state.
0000 through 1111	Specifies the bit pattern.

Defaults

The default is to use the preset signaling patterns as defined in American National Standards Institute (ANSI) and European Conference of Postal and Telecommunications Administrations (CEPT) standards, as follows:

- For North American E&M:
 - tx-bits idle 0000 (0001 if on E1 trunk)
 - tx-bits seize 1111
 - rx-bits idle 0000
 - rx-bits seize 1111
- For E&M MELCAS:
 - tx-bits idle 1101
 - tx-bits seize 0101
 - rx-bits idle 1101
 - rx-bits seize 0101

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA3	This command was introduced on the Cisco MC3810 multiservice concentrator.

Release	Modification
12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series routers.
12.1(2)T	The support for Cisco 2600 and 3600 series routers was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The **define** command applies to E&M digital voice ports associated with T1/E1 controllers.

Use the **define** command to match the E&M bit patterns with the attached telephony device. Be careful not to define invalid configurations, such as all 0000 on E1, or identical seized and idle states. Use this command with the **ignore** command.

Examples

To configure a voice port on a Cisco 2600 or 3600 series router that is sending traffic in North American E&M signaling format to convert the signaling to MELCAS format, enter the following commands:

```
voice-port 1/0/0
 define rx-bits idle 1101
 define rx-bits seize 0101
 define tx-bits idle 1101
 define tx-bits seize 0101
```

To configure a voice port on a Cisco MC3810 multiservice concentrator that is sending traffic in North American E&M signaling format to convert the signaling to MELCAS format, enter the following commands:

```
voice-port 0/8
 define rx-bits idle 1101
 define rx-bits seize 0101
 define tx-bits idle 1101
 define tx-bits seize 0101
```

Related Commands

Command	Description
condition	Manipulates the signaling bit-pattern for all voice signaling types.
ignore	Configures a North American E&M or E&M MELCAS voice port to ignore specific receive bits.

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.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(1)NA	This command was introduced on the Cisco AS5300 universal access server.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

Use the **delete vfc** command to delete a specific file from VFC Flash memory and to remove the file from the default list or capability list if the specified file is included in those lists.



Note

Deleting a file from VFC Flash memory does not free the VFC Flash memory space that the file occupied. To free VFC Flash memory space, use the **erase vfc** command.

Examples

The following example deletes the bas-vfc-1.0.14.0.bin file, which is stored in VFC Flash memory of the VFC located in slot 0:

```
Router# delete bas-vfc-1.0.14.0.bin vfc 0
```

Related Commands

Command	Description
default-file vfc	Specifies an additional (or different) file from the ones in the default file list and stored in VFC Flash memory.
erase vfc	Erases the Flash memory of a specified VFC.
show vfc directory	Displays the list of all files that reside on this VFC.

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

<i>string</i>	Character string from 1 to 80 characters.

Defaults

Enabled with a null string.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers router.
11.3(1)MA	This command was implemented on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

Use the **description** command to include descriptive text about the DSP interface connection. This information is displayed when a **show** command is issued, and it does not affect the operation of the interface in any way.

Examples

The following example identifies voice port 1/0/0 on the Cisco 3600 series routers as being connected to the purchasing department:

```
voice-port 1/0/0
 description purchasing_dept
```

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

<i>string</i>	Character string from 1 to 80 characters.

Defaults

Enabled with a null string.

Command Modes

DSPfarm interface configuration

Command History

Release	Modification
11.3(1)T	This command was introduced for the Cisco 7200 series routers.
12.0(5)XE	The command was modified to reduce the maximum number of allowable characters in a text string from 255 to 80.
12.1(1)T	The 12.0(5)XE modifications were integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Use the **description** command to include descriptive text about this DSP interface connection. This information is displayed when you issue a **show** command and does not affect the operation of the interface in any way.

Examples

The following example identifies DSPfarm interface 1/0 on the Cisco 7200 series routers router as being connected to the marketing department:

```
dspint dspfarm 1/0
description marketing_dept
```

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]**

Syntax Description

+	(Optional) Character indicating an E.164 standard number.
<i>string</i>	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: • The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). • Percent sign (%), which indicates that the previous digit/pattern occurred zero or multiple times, similar to the wildcard usage in the regular expression. • Plus sign (+), which matches a sequence of one or more matches of the character/pattern.  Note 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. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign (\$), which matches the null string at the end of the input string. • 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). • Question mark (?), which indicates that the previous digit occurred zero or one time. • 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. • Parentheses “()”, which indicate a pattern and is the same as the regular expression rule.
T	(Optional) Control character indicating that the destination-pattern value is a variable length dial string.

Defaults

Enabled with a null string.

Command Modes Dial-peer configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 series routers.
	11.3(1)MA	This command was implemented on the Cisco MC3810 multiservice concentrator.
	12.0(4)XJ	This command was modified for store and forward fax.
	12.1(1)	The command as modified for store and forward fax was integrated into Cisco IOS Release 12.1(1).
	12.0(7)XR	Support for the plus sign, percent sign, question mark, brackets, and parentheses symbols in the dial string was added to the Cisco AS5300 universal access server.
	12.0(7)XK	Support for the plus sign, percent sign, question mark, brackets, and parentheses in the dial string was added to the Cisco 2600, Cisco 3600, and Cisco MC3810 multiservice concentrator.
	12.1(1)T	The modifications made in Cisco IOS Release 12.0(7)XR for the Cisco AS5300 were first supported in Cisco IOS Release 12.1(1)T and were first supported on the T train for the following additional platforms: Cisco 1750, Cisco 2600 series routers, Cisco 3600 series routers, Cisco 7200, and Cisco 7500.
	12.1(2)T	The modifications made in Cisco IOS Release 12.0(7)XK for the Cisco MC3810 multiservice concentrator were first supported on the T train.

Usage Guidelines

Use the **destination-pattern** command to define the E.164 telephone number for a dial peer.

This pattern is used to match dialed digits to a dial peer. The dial peer is then used to complete the call. When a router receives voice data, it compares the called number (the full E.164 telephone number) in the packet header with the number configured as the destination pattern for the voice-telephony peer. The router then strips out the left-justified numbers corresponding to the destination pattern. If you have configured a prefix, the prefix is appended to the front of the remaining numbers, creating a dial string, which the router then dials. If all numbers in the destination pattern are stripped out, the user receives a dial tone.

There are certain areas in the world (for example, in certain European countries) where valid telephone numbers can vary in length. Use the optional control character **T** to indicate that a particular **destination-pattern** value is a variable-length dial string. In this case, the system does not match the dialed numbers until the interdigit timeout value has expired.



Note

Cisco IOS software does not check the validity of the E.164 telephone number; it accepts any series of digits as a valid number.

Examples

The following example shows configuration of the E.164 telephone number 555-7922 for a dial peer:

```
dial-peer voice 10 pots
 destination-pattern +5557922
```

The following example shows configuration of a destination pattern in which the pattern “43” is repeated multiple times preceding the digits “555”:

```
dial-peer voice 1 voip
destination-pattern 555(43)+
```

The following example shows configuration of a destination pattern in which the preceding digit/pattern was repeated multiple times:

```
dial-peer voice 2 voip
destination-pattern 555%
```

The following example shows configuration of a destination pattern in which the digit numbers range between 5553409 and 5559499:

```
dial-peer voice 3 vofr
destination-pattern 555[3-9]4[0=9]9
```

The following example shows configuration of a destination pattern in which the digit numbers range between 5551439, 5553439, 5555439, 5557439, and 5559439:

```
dial-peer voice 4 voatm
destination-pattern 555[13579]439
```

Related Commands

Command	Description
answer-address	Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call.
prefix	Specifies the prefix of the dialed digits for this dial peer.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.

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

Syntax Description

<i>isdn</i>	Local ISDN directory number assigned by your telephone service provider.

Defaults

A default ISDN directory number is not defined for this interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series routers.

Usage Guidelines

This command is applicable to the Cisco 800 series routers.

You must specify this command when creating a dial peer. This command does not work if it is not specified within the context of a dial peer. For information on creating a dial peer, refer to the *Cisco 800 Series Routers Software Configuration Guide*.

Do not specify an area code with the local ISDN directory number.

Examples

The following example specifies 555-1111 as the local ISDN directory number:

```
destination-pattern 5551111
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode, defines the type of dial peer, and defines the tag number associated with a dial peer.
no call-waiting	Disables call waiting.
port (dial-peer)	Enables an interface on a PA-4R-DTR port adapter to operate as a concentrator port.
ring	Sets up a distinctive ring for telephones, fax machines, or modems connected to a Cisco 800 series router.
show dial-peer voice	Displays configuration information and call statistics for dial peers.

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).

Defaults

V.54 loopback detection is disabled.

Command Modes

Controller configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 and 3600 series routers.

Usage Guidelines

Use the **detect v54 channel-group** controller configuration command to enable V.54 loopback detection. The remote device will send a loopup inband payload command sequence in fractional T1 (FT1).

Examples

The following example sets the loopback detection for channel-group 1; then the loopback detection is disabled for channel-group 1.

```
detect v54 channel-group 1
no detect v54 channel-group 1
```

Related Commands

Command	Description
loopback remote v54 channel-group	Activates a remote V.54 loopback for the channel group on the far end.

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.

Defaults	The default device ID is 0.

Command Modes	Settlement configuration

Command History	Release	Modification
	12.0(4)XH1	This command was introduced on the Cisco 2600 and 3600 series routers and on the AS5300 access server.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines	It is optional to identify a gateway associated with a settlement provider.

Examples	The following example sets the device-id to 1000:

```
settlement 0
 device-id 1000
```

Related Commands	Command	Description
	customer-id	Identifies a carrier or Internet service provider with the settlement provider.
	settlement	Enters settlement configuration mode.

dial-control-mib

To specify attributes for the call history table, use the **dial-control-mib** command in global configuration mode. To restore the default maximum size or retention time of the call history table, use the **no** form of this command.

dial-control-mib {**max-size** *number* | **retain-timer** *number*}

no dial-control-mib {**max-size** *number* | **retain-timer** *number*}

Syntax Description

max-size <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.
retain-timer <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.

Defaults

The default call history table length is 50 table entries. The default retain timer is 15 minutes.

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.
12.0(1)XA	This command was first applied to the CDR feature on the Cisco MC3810 multiservice concentrator.
12.0(2)T	The 12.0(1)XA application on the Cisco MC3810 multiservice concentrator was integrated into Cisco IOS Release 12.0(2)T.

Examples

The following example configures the call history table to hold 400 entries, with each entry remaining in the table for 10 minutes:

```
dial-control-mib max-size 400
dial-control-mib retain-timer 10
```

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

Syntax Description	<i>hunt-order-number</i> A number from 0 to 7 that selects a predefined hunting selection order: 0—Longest match in phone number, explicit preference, random selection. This is the default hunt order number. 1—Longest match in phone number, explicit preference, least recent use. 2—Explicit preference, longest match in phone number, random selection. 3—Explicit preference, longest match in phone number, least recent use. 4—Least recent use, longest match in phone number, explicit preference. 5—Least recent use, explicit preference, longest match in phone number. 6—Random selection. 7—Least recent use.

Defaults	The default is the longest match in the phone number, explicit preference, random selection (hunt order number 0).

Command Modes	Dial-peer configuration

Command History	Release	Modification
	12.0(7)XK	This command was introduced and supported on the Cisco 2600, 3600, and 7200 series routers, the Cisco MC3810 multiservice concentrator, and the Cisco AS5300 universal access servers.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use the **dial-peer hunt** dial-peer configuration command if you have configured hunt groups. “Longest match in phone number” refers to the destination pattern that matches the greatest number of the dialed digits. “Explicit preference” refers to the **preference** setting in the dial-peer configuration. “Least recent use” refers to the destination pattern that has waited the longest since being selected. “Random selection” weights all of the destination patterns equally in a random selection mode.

This command applies to POTS, Voice over IP (VoIP), Voice over Frame Relay (VoFR), Voice over ATM (VoATM), and Multimedia Mail over Internet Protocol (MMOIP) dial peers.

Examples

The following example configures the dial peers to hunt in the following order: (1) longest match in phone number, (2) explicit preference, (3) random selection.

```
dial-peer hunt 0
```

Related Commands

Command	Description
destination-pattern	Specifies the prefix or the complete telephone number for a dial peer.
preference	Specifies the preferred selection order of a dial peer within a hunt group.
show dial-peer voice	Displays configuration information for dial peers.

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

Syntax Description

<i>character</i>	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 #.

Defaults

The default terminating character is #.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.
12.0(7)XK	Usage was restricted to variable-length dialed numbers. The command was implemented on the Cisco 2600 and 3600 series routers and on the MC3810 multiservice concentrator.
12.1(2)T	The modifications made in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

There are certain areas in the world (for example, in certain European countries) where telephone numbers can vary in length. When a dialed-number string has been identified as a variable length dialed-number, the system does not place a call until the configured value for the **timeouts interdigits** command has expired or until the caller dials the terminating character. Use the **dial-peer terminator** global configuration command to change the terminating character.

Examples

The following example shows that “9” has been specified as the terminating character for variable-length dialed numbers:

```
dial-peer terminator 9
```

Related Commands	Command	Description
	answer-address	Specifies the preferred selection order of a dial peer within a hunt group.
	destination-pattern	Specifies the prefix or the complete telephone number for a dial peer.
	timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
	show dial-peer voice	Displays configuration information for dial peers.

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** }

Syntax Description

<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.
videocodec	Specifies a local video codec connected to the router.
videoatm	Specifies a remote video codec on the ATM network.

Defaults

No video dial peer is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced for ATM interface configuration on the Cisco MC3810 multiservice concentrator.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

The *tag* value must be unique to the device.

Examples

On a Cisco MC3810 multiservice concentrator, the following example sets up a local video dial peer designated as 10:

```
dial-peer video 10 videocodec
```

Related Commands

Command	Description
show dial-peer video	Displays dial-peer configuration.

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 7204 VXR and Cisco 7206 VXR Routers

```
dial-peer voice tag {pots | voatm | vofr | voip}

no dial-peer voice tag {pots | voatm | vofr | voip}
```

Cisco AS5300 Universal Access Server

```
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 | voip}

no dial-peer voice tag {pots | voatm | vofr | voip}
```

Syntax Description

<i>tag</i>	Digits that define a particular dial peer. Valid entries are from 1 to 2,147,483,647.
mmoip	Indicates that this is a multimedia mail peer using IP encapsulation on the IP backbone. Note On the Cisco AS5300 universal access server, MMoIP is available only if you have modem ISDN channel aggregation (MICA) technologies modems.
pots	Indicates that this is a plain old telephone service (POTS) peer using Voice over IP encapsulation on the IP backbone.

dial-peer voice

voatm	(Cisco 3600 series routers, Cisco MC3810 multiservice concentrators, Cisco 7204 VXR routers, and Cisco 7206 VXR routers only) Specifies that this is a Voice over ATM dial peer using the real-time AAL5 voice encapsulation on the ATM backbone network.
vofr	Specifies that this is a Voice over Frame Relay dial peer using FRF.11 encapsulation on the Frame Relay backbone network.
voip	Indicates that this is a VoIP peer using voice encapsulation on the POTS network.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.
11.3(1)MA	This command was first supported on the Cisco MC3810 multiservice concentrator, with support for the pots , voatm , vofr , and vohdnc keywords.
12.0(3)T	This command was first supported on the AS5300, with support for the pots and voip keywords.
12.0(3)XG	The vofr keyword was added for the Cisco 2600 series routers and Cisco 3600 series platforms.
12.0(4)T	The vofr keyword was integrated into Cisco IOS Release 12.0(4)T. The vofr keyword was added to the Cisco 7200 series routers platform.
12.0(4)XJ	The mmoip keyword was added for the Cisco AS5300 universal access server platform. Also, the dial-peer voice command was implemented for store and forward fax.
12.0(7)XK	The voip keyword was added for the Cisco MC3810 multiservice concentrator, and the voatm keyword was added for the Cisco 3600 series routers router. Support for vohdnc on the Cisco MC3810 multiservice concentrator was removed in this release.
12.1(1)	The mmoip keyword addition in Cisco IOS Release 12.0(4)XJ was integrated into Cisco IOS Release 12.1(1). The dial-peer voice implementation for store and forward fax was also integrated into this mainline release.
12.1(2)T	The keyword changes in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use the **dial-peer voice** global configuration command to switch to dial-peer configuration mode from global configuration mode and to define a particular dial peer. Use the **exit** command to exit dial-peer configuration mode and return to global configuration mode.

After you have created a dial peer, that dial peer remains defined and active until you delete that particular dial peer. To delete a dial peer, use the **no** form of this command. To disable a dial peer, use the **shutdown** command in dial-peer configuration mode.

In store and forward fax on the Cisco AS5300 universal access server, the POTS dial peer defines the inbound faxing line characteristics from the sending fax device to the receiving Cisco AS5300 universal access server and the outbound line characteristics from the sending Cisco AS5300 universal access server to the receiving fax device. The Multimedia Mail over Internet Protocol (MMoIP) dial peer defines the inbound faxing line characteristics from the Cisco AS5300 universal access server to the receiving Simple Mail Transfer Protocol (SMTP) mail server. This command applies to both on-ramp and off-ramp store and forward fax functions.

**Note**

On the Cisco AS5300 universal access server, MMoIP is available only if you have modem ISDN channel aggregation (MICA) technologies modems.

Examples

The following example shows how to access dial-peer configuration mode and configure a POTS peer identified as dial peer 10 and an MMoIP dial peer identified as dial peer 20:

```
dial-peer voice 10 pots
dial-peer voice 20 mmoidp
```

The following example deletes the MMoIP peer identified as dial peer 20:

```
no dial-peer voice 20 mmoidp
```

Related Commands

Command	Description
codec (dial-peer)	Specifies the voice coder rate of speech for a Voice over Frame Relay dial peer.
destination-pattern	Specifies the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dtmf-relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.
sequence-numbers	Enables the generation of sequence numbers in each frame generated by the DSP for Voice over Frame Relay applications.
session protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
voice-port	Enters voice-port configuration mode.

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

dtmf	Dual tone multifrequency (DTMF) touch-tone dialing.
pulse	Pulse (rotary) dialing.
mf	Multifrequency tone dialing.

Defaults

dtmf

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.
11.3(1)MA3	The pulse keyword was added. This command was implemented on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	The mf keyword was added.
12.1(2)T	The pulse and mf keyword additions and the MC3810 multiservice concentrator platform implementation were integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use the **dial-type** command to specify an out-dialing type for a Foreign Exchange Office (FXO) or ear and mouth (E&M) voice port interface. This command specifies the tone type for digit detection and out-pulsing. This command is not applicable to Foreign Exchange Station (FXS) voice ports because the ports do not generate out-dialing. This command also specifies the detection direction. MF is not supported for FXS and FXO.

Voice ports can always detect DTMF and pulse signals. This command does not affect voice port dialing detection.

The **dial-type** command affects out-dialing as configured for the dial peer.

The **dial-type** command is not supported on FXO voice port interfaces on the Cisco MC3810 multiservice concentrator. If you are using the **dial-type** command with E&M WinkStart, use the **dtmf** or **mf** option.

SGCP 1.1+ does not support pulse dialing.

Examples

The following example shows a voice port configured on the Cisco MC3810 multiservice concentrator to support a rotary (pulse tone) dialer:

```
voice-port 1/1
 dial-type pulse
```

The following example shows a voice port configured on the Cisco MC3810 multiservice concentrator to support a DTMF (touch-tone) dialer:

```
voice-port 1/1
 dial-type dtmf
```

The following example shows a voice port configured on the Cisco MC3810 multiservice concentrator to support a multifrequency tone dialer:

```
voice-port 1/1
 dial-type mf
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.

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.

Defaults Digit stripping is enabled.

Command Modes Dial-peer configuration

Command History	Release	Modification
	12.0(7)XR1	This command was introduced for Voice over IP (VoIP) on the Cisco AS5300.
	12.0(7)XK	This command was first supported for the following voice technologies on the following platforms: - VoIP (Cisco 2600 series routers, Cisco 3600 series routers, Cisco MC3810 multiservice concentrator) - Voice over Frame Relay (VoFR)—Cisco 2600 series routers, Cisco 3600 series routers, Cisco MC3810 multiservice concentrator) - Voice over ATM (VoATM)—Cisco 3600 series routers and Cisco MC3810 multiservice concentrator
	12.1(1)T	The modifications made in Cisco IOS Release 12.0(7)XK were first supported in Cisco IOS Release 12.1(1)T:
	12.1(2)T	This command was first implemented in Cisco IOS Release 12.1(2)T for the following voice technologies on the following platforms: - VoIP (Cisco MC3810 multiservice concentrator) - VoFR (Cisco 2600 series routers, Cisco 3600 series routers, and Cisco MC3810 multiservice concentrator) - VoATM (Cisco 3600 series routers, Cisco MC3810 multiservice concentrator)

Usage Guidelines

The **digit-strip** command is supported on POTS dial peers only.

When a called number is received and matched to a POTS dial peer, the matched digits are stripped and the remaining digits are forwarded to the voice interface.

[Table 16](#) lists a series of dial peers configured with a specific destination pattern and shows the longest matched number after the digit is stripped based on the dial string 408 555-3048.

Table 16 *Dial Peer Configurations with Longest Matched Number*

Dial Peer	Destination Pattern	Preference	Session Target	Longest Matched Number
1	4085553048	0 (highest)	100-voip	10
2	408[0-9]553048	0	200-voip	9
3	408555	0	300-voip	6
4	408555	1(lower)	400-voip	6
5	408%	1	500-voip	3
6		0	600-voip	0
7		1	1:D (interface)	0

[Table 17](#) lists a series of dial peers configured with a specific destination pattern and shows the number after the digit strip based on the dial string 408 555-3048 and the different dial peer symbols applied.

Table 17 *Dial Peer Configurations with Digits Stripped*

Dial Peer	Destination Pattern	Number After the Digit Strip
1	408555....	3048
2	408555.%	3048
3	408525.+	3048
4	408555.?	3048
5	408555+	3048
6	408555%	53048
7	408555?	53048
8	408555[0-9].%	3048
9	408555(30).%	3048
10	408555(30)%	3048
11	408555..48	3048

Examples

The following example disables digit stripping on a POTS dial peer:

```
dial-peer voice 100 pots
no digit-strip
```

Related Commands	Command	Description
	numbering-type	Specifies number type for the VoIP or POTS dial peer.
	rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
	show translation-rule	Displays the contents of all the rules that have been configured for a specific translation name.
	test translation-rule	Tests the execution of the translation rules on a specific name-tag.
	translation-rule	Creates a translation name and enters translation-rule configuration mode.
	voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

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.

Defaults

Disabled

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)NA	This command was introduced on the Cisco AS5300 universal access server.
12.0(4)XJ	This command was implemented for store and forward fax.
12.1(1)	The implementation of the command for store and forward fax was integrated into Cisco IOS Release 12.1(1).

Usage Guidelines

Use the **direct-inward-dial** command to enable the DID call treatment for the incoming called numbers. When this feature is enabled, the incoming call is treated as if the digits were received from the DID trunk. The called number is used to select the outgoing dial peer. No dial tone is presented to the caller.

Use the **no** form of this command to disable DID. When disabled, the called number is used to select the outgoing dial peer. The caller will be prompted for a called number via dial tone.

This command is applicable only to plain old telephone service (POTS) dial peers. This command applies to on-ramp store and forward fax functions.

Examples

The following example enables DID call treatment for incoming called numbers:

```
dial peer voice 10 pots
direct-inward-dial
```

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.

Defaults

The gateway does not disconnect a call when it receives a Disconnect message with a PI value.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(5)T	This command was introduced on the Cisco 2600 series routers, 3600 series, 7200 series, 7500 series, AS5300, AS5800, and MC3810 multiservice concentrator.

Usage Guidelines

The **disc_pi_off** voice-port command is valid only if the Disconnect with PI is received on the inbound call leg. For example, if this command is enabled on the voice port of the originating gateway, and a Disconnect with PI is received from the terminating switch, the Disconnect with PI is converted to a Disconnect. But if this command is enabled on the voice port of the terminating gateway, and a Disconnect with PI is received from the terminating switch, the Disconnect message is not converted to a standard Disconnect because the Disconnect message is received on the outbound call leg.



Note

The **disc_pi_off** voice-port configuration command is valid only for the default session application; it does not work for interactive voice response (IVR) applications.

Examples

The following example handles a Disconnect message with a PI value the same as a standard Disconnect message for voice port 0:23:

```
voice-port 0:23
 disc_pi_off
```

Related Commands

Command	Description
isdn t306	Sets a timer for Disconnect messages.

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.

Defaults

FXS voice ports return an acknowledgment upon receipt of a disconnect signal.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series routers.
12.1(2)T	The support for the Cisco 2600 and 3600 series routers was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The **disconnect-ack** command configures an FXS voice port to remove line power if the equipment on an FXS loop-start trunk disconnects first.

Examples

The following example, which begins in global configuration mode, turns off the disconnect acknowledgment signal on voice port 1/1 on a Cisco MC3810 multiservice concentrator:

```
voice-port 1/1
no disconnect-ack
```

The following example, which begins in global configuration mode, turns off the disconnect acknowledgment signal on voice port 1/1/0 on a Cisco 2600 or 3600 series router:

```
voice-port 1/0/0
no disconnect-ack
```

Command History

Command	Description
show voice port	Displays voice port configuration information.

ds0 busyout (voice)

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.

Defaults

DS0 time slots are not in busyout state.

Command Modes

Controller configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on Cisco MC3810 multiservice concentrator and Cisco 2600 and 3600 series routers.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The **ds0 busyout** command affects only DS0 time slots that are configured into a DS0 group and that function as part of a digital voice port. If multiple DS0 groups are configured on a controller, any combination of DS0 time slots can be busied out, provided that each DS0 time slot to be busied out is part of a DS0 group.

If a DS0 time slot is in the busyout state, only the **no ds0 busyout** command can restore the DS0 time slot to service.

To avoid conflicting command-line interface (CLI) commands, do not use the **ds0 busyout** command and the **busyout forced** command on the same controller.

Examples

The following example configures DS0 time slot 6 on controller T1 0 to be forced into the busyout state:

```
controller t1 0
 ds0 busyout 6
```

The following example configures DS0 time slots 1, 3, 4, 5, 6, and 24 on controller E1 1 to be forced into the busyout state:

```
controller e1 1
 ds0 busyout 1,3-6,24
```

Related Commands

Command	Description
busyout seize	Changes the busyout seize procedure for a voice port.
show running configuration	Determines which DS0 time slots have been forced into the busyout state.

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 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}
```

```
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.
timeslots <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, allowable values are from 1 to 24. Examples are as follows: • 2 • 1-15,17-24 • 1-23 • 2,4,6-12

type

The signaling method selection for the **type** 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:

- **e&m-delay-dial**—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.
 - **e&m-fgd**—E&M Type II Feature Group D.
 - **e&m-immediate-start**—E&M immediate start.
 - **e&m-wink-start**—E&M Mercury Exchange Limited Channel-Associated Signaling (MELCAS) wink-start signaling support.
 - **ext-sig**—An option available only when the **mode CCS** command is enabled on the Cisco MC3810 multiservice concentrator for FRF.11 transparent common channel signaling (CCS) support.
 - **fgd-eana**—Feature Group D exchange access North American.
 - **fxo-ground-start**—FXO ground-start signaling support.
 - **fxo-loop-start**—FXO loop-start signaling support.
 - **fxs-ground-start**—FXS ground-start signaling support.
 - **fxs-loop-start**—FXS loop-start signaling support.
-

For the Cisco 2600 and 3600 Series Routers and Cisco MC3810 Multiservice Concentrators—E1:

<i>ds0-group-no</i>	An identifying value from 0 to 14 and 16 to 30. 15 is reserved.
timeslots <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 E1, allowable values are from 1 to 31. Examples are as follows: • 2 • 1-15,17-31 • 1-31 • 2,4,6-12, 17-31
type	The signaling method selection for the type 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: • e&m-delay-dial—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. • e&m-immediate-start—E&M immediate start. • e&m-melcas-delay—E&M MELCAS delay-start signaling support. • e&m-melcas-immed—E&M MELCAS immediate-start signaling support. • e&m-melcas-wink—E&M MELCAS wink-start signaling support. • e&m-wink-start—The originating endpoint sends an off-hook signal and waits for a wink start from the destination. • ext-sig—An option available only when the mode CCS command is enabled on the Cisco MC3810 multiservice concentrator for FRF.11 transparent CCS support. • fgd-eana—Feature Group D exchange access North American. • fxo-ground-start—Specifies FXO ground-start signaling. • fxo-loop-start—Specifies FXO loop-start signaling. • fxo-melcas—MELCAS FXO signaling. • fxs-ground-start—FXS ground-start signaling. • fxs-loop-start—FXS loop-start signaling. • fxs-melcas—MELCAS FXS signaling. • r2-analog—Specifies R2 analog line signaling. • r2-digital—Specifies R2 digital line signaling. • r2-pulse—Specifies 7-pulse line signaling, a transmitted pulse that indicates a change in the line state.

For the Cisco 7200 and 7500 Series Routers—T1 and E1:

<i>ds0-group-no</i>	For T1, a value from 0 to 23 that identifies the DS0 group. For E1, a value from 0 to 14 and 16 to 30. 15 is reserved
timeslots <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, allowable values are from 1 to 24. For E1, allowable values are from 1 to 31. Examples are as follows: • 2 • 1-15,17-24 • 1-31 • 2,4,6-12
type	The signaling method selection for the type 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: • e&m-delay-dial—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. • e&m-fgd—E&M Type II Feature Group D. • e&m-immediate-start—E&M immediate start. • e&m-wink-start—E&M MELCAS wink-start signaling support. • fxs-ground-start—FXO ground-start signaling support. • fxs-loop-start—FXS loop start. • fxo-ground-start—Specifies FXO ground-start signaling. • fxo-loop-start—FXO loop-start signaling support.

For the Cisco AS5300 Universal Access Server—T1:

<i>ds0-group-no</i>	A value from 0 to 23 that identifies the DS0 group.
timeslots <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. Allowable values are from 1 to 24. Examples are as follows: • 2 • 1-15,17-24 • 1-23 • 2,4,6-12
service <i>service-type</i>	(Optional) Indicates the type of calls to be handled by this DS0 group— data , fax , voice , or mgcp .
type	(Optional) The signaling method selection for the type 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. Types are the following: • e&m-fgb—E&M Type II Feature Group B. • e&m-fgd—E&M Type II Feature Group D. • e&m-immediate-start—E&M immediate start. • fxs-ground-start—FXS ground start. • fxs-loop-start—FXS loop start. • fgd-eana—Feature Group D exchange access North American. • fgd-os—Feature Group D operator services. • r1-itu—Line signaling based on international signaling standards. • sas-ground-start—Single attachment station (SAS) ground start. • sas-loop-start—SAS loop start. • none—Null signaling for external call control.
tone <i>type</i>	(Optional) Specifies the tone as dtmf or mf .
addr info	(Optional) Specifies the calling/called party.

For the Cisco AS5300 Universal Access Server—E1:

<i>ds0-group-no</i>	An identifying value from 0 to 14 and 16 to 30. 15 is reserved.
timeslots <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. Allowable values are from 1 to 31. Examples are as follows: • 2 • 1-15,17-31 • 1-31 • 2,4,6-12, 24
type	The signaling method selection for the type keyword depends on the connection that you are making. Types are the following: • none—Null signaling for external call control. • p7—Specifies the p7 switch type. • r2-analog—Specifies R2 analog line signaling. • r2-digital—Specifies R2 digital line signaling. • r2-lsv181-digital—Specifies a specific R2 digital line. • r2-pulse—Specifies 7-pulse line signaling, a transmitted pulse that indicates a change in the line state.

For the Cisco AS5300 Universal Access Server—T1:

<i>ds0-group-no</i>	A value from 0 to 23 that identifies the DS0 group.
timeslots <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. Allowable values are from 1 to 24. Examples are as follows: • 2 • 1-15,17-24 • 1-23 • 2,4,6-12
type	The signaling method selection for the type 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. Types are the following: • e&m-fgb—E&M Type II Feature Group B. • e&m-fgd—E&M Type II Feature Group D. • e&m-immediate-start—E&M immediate start. • fxs-ground-start—FXS ground start. • fxs-loop-start—FXS loop start. • fgd-eana—Feature Group D exchange access North American. • r1-itu—A line signaling based on international signaling standards. • r1-modified—An international signaling standard that is common to channelized T1/E1 networks. • r1-turkey—A signaling standard used in Turkey. • sas-ground-start—SAS ground start. • sas-loop-start—SAS loop start. • none—Null signaling for external call control.

For the Cisco AS5800 Universal Access Server—E1:

<i>ds0-group-no</i>	An identifying value from 0 to 14 and 16 to 30. 15 is reserved.
timeslots <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. Allowable values are from 1 to 31. Examples are as follows: • 2 • 1-15,17-31 • 1-31 • 2,4,6-12, 18-31
type	The signaling method selection for the type 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. Types are the following: • e&m-fgb—E&M Type II Feature Group B. • e&m-fgd—E&M Type II Feature Group D. • e&m-immediate-start—E&M immediate start. • fxs-ground-start—FXS ground start. • fxs-loop-start—FXS loop start. • p7—Specifies the p7 switch type. • r2-analog—Specifies R2 analog line signaling. • r2-digital—Specifies R2 digital line signaling. • r2-pulse—Specifies 7-pulse line signaling, a transmitted pulse that indicates a change in the line state. • sas-ground-start—SAS ground start. • sas-loop-start—SAS loop start. • none—Null signaling for external call control.

Defaults

No DS0 group is defined.

Command Modes

Controller configuration

Command History

Release	Modification
11.2	This command was introduced for the Cisco AS5300 universal access server as the cas-group command.
11.3(1)MA	The command was introduced as the voice-group command for the Cisco MC3810 multiservice concentrator.
12.0(1)T	The cas-group command was introduced for the Cisco 3600 series routers.

Release	Modification
12.0(5)T	The command was renamed ds0-group on the Cisco AS5300 and Cisco 2600 and 3600 series routers. Some keyword modifications were implemented.
12.0(5)XE	This command was introduced for the Cisco 7200 series.
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator. When the ds0-group command became available on the Cisco MC3810 multiservice concentrator, the voice-group command was removed and no longer supported. The ext-sig keyword replaced the ext-sig-master and ext-sig-slave keywords that were available with the voice-group command.
12.0(7)XR	The mgcp service type was added.
12.1(1)T	The ds0-group command was implemented for the Cisco 7200 series.
12.1(2)XH	The e&m-fgd and fgd-eana keywords were added for Feature Group D signaling.
12.1(3)T	The command was modified for the Cisco 7500 series routers. The fgd-os signaling type and the voice service type were added.

Usage Guidelines

The **ds0-group** command automatically creates a logical voice port that is numbered as follows:

- Cisco 2600, 3600, and 7200 series routers:
 - slot/port:ds0-group-no
- Cisco MC3810 multiservice concentrators:
 - slot:ds0-group-no

On the Cisco MC3810 multiservice concentrator, the *slot* number is the controller number.

Although only one voice port is created for each group, applicable calls are routed to any channel in the group.



Note

Channel groups, CAS voice groups, DS0 groups, and TDM groups all use group numbers. All group numbers configured for channel groups, CAS voice groups, DS0 groups, and TDM groups must be unique on the local router. For example, you cannot use the same group number for a channel group and for a TDM group.

Examples

The following example shows ranges of T1 controller time slots configured for FXS ground-start and FXO loop-start signaling on a Cisco 2600 or 3600 series router:

```
T1 1/0
 framing esf
 linecode b8zs
 ds0-group 1 timeslots 1-10 type fxs-ground-start
 ds0-group 2 timeslots 11-24 type fxo-loop-start
```

The following example shows DS0 groups 1 and 2 on controller T1 1 configured on the Cisco MC3810 multiservice concentrator to support Transparent CCS:

```
controller T1 1
 mode ccs cross-connect
```

■ ds0-group

```
ds0-group 1 timeslots 1-10 type ext-sig  
ds0-group 2 timeslots 11-24 type ext-sig
```

Related Commands

Command	Description
codec	Specifies the voice coder rate of speech for a dial peer.
codec complexity	Specifies call density and codec complexity based on the codec standard you are using.

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	delay	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 delayed. The definition of delay is made by each mailer and is not controllable by the sender (the Cisco AS5300 universal access server). Each mailer in the path to the recipient that supports the delivery status notification (DSN) extension receives the same request.
	failure	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.
	success	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.



Note In the absence of any other DSN settings (“no dsn” or a mailer in the path that does not support the DSN extension), a failure to deliver always causes a nondelivery message to be generated. This nondelivery message is colloquially termed a “bounce.”

Defaults The default is **success** and **failure**.

Command Modes Dial-peer configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced.
	12.1(1)	This command was integrated into Cisco IOS Release 12.1(1).

Usage Guidelines This command is applicable to Multimedia Mail over Internet Protocol (MMoIP) dial peers. DSNs are messages or responses that are automatically generated and sent to the sender or originator of an e-mail message by the Simple Mail Transfer Protocol (SMTP) server, notifying the sender of the status of the e-mail message. Specifications for DSN are described in RFC 1891, RFC 1892, RFC 1893, and RFC 1894.

The on-ramp DSN request is included as part of the fax-mail message sent by the on-ramp gateway when the matching MMoIP dial peer has been configured. The on-ramp DSN response is generated by the SMTP server when the fax-mail message is accepted. The DSN is sent back to the user defined in the **mta send mail-from** command. The off-ramp DSN is requested by the e-mail client. The DSN response is generated by the SMTP server when it receives a request as part of the fax-mail message.



Note DSNs can be generated only if the mail client on the SMTP server is capable of responding to a DSN request.

Because the SMTP server generates the DSNs, configure both the **mail from:** and **rcpt to:** commands for the DSN feature to be operational, for example:

```
mail from: <user@mail-server.company.com>
rcpt to: <fax=555-1212@company.com> NOTIFY=SUCCESS,FAILURE,DELAY
```

There are three different states that can be reported back to the sender:

- Delay—Indicates that, for some reason, the message was delayed while being delivered to the recipient.
- Success—Indicates that the message was successfully delivered to the recipient's mailbox.
- Failure—Indicates that, for some reason, the SMTP server was unable to deliver the message to the recipient.

Because these delivery states are not mutually exclusive, store and forward fax can be configured to generate these messages for all or any combination of these events.

DSN messages notify the sender of the status of a particular e-mail message containing a fax Tag Image File Format (TIFF) image. Use the **dsn** command to specify which notification messages will be sent to the user.

The **dsn** command allows you to select more than one notification option by reissuing the command, specifying a different notification option each time. To discontinue a specific notification option, use the **no** form of the command for that specific keyword.



Note If the **failure** keyword is not included when configuring DSN, the sender will receive absolutely no notification of message delivery failure. Because a failure is usually significant, care should be taken to always include the **failure** keyword as part of the **dsn** command configuration.

This command applies to on-ramp store and forward fax functions.

Examples

The following example specifies that a DSN message be returned to the sender when the e-mail message containing the fax has been successfully delivered to the recipient or if the message containing the fax has failed, for whatever reason, to be delivered:

```
dial-peer voice 10 mmoup
 dsn success
 dsn failure
```

The following example specifies that a DSN message be returned to the sender either when the e-mail message containing the fax has been successfully delivered to the recipient or when the message has been delayed:

```
dial-peer voice 10 mmoup
 dsn success
```

dsn delayed

Related Commands	Command	Description
	mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from or the Return-Path address).

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.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced on the Cisco 7200 series routers.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

To disable the DSPfarm interface, enter the **no shutdown** command.

Examples

The following example creates a DSPfarm interface with a slot number of 1 and a port number of 0.

```
dspint dspfarm 1/0
```

Related Commands

Command	Description
show interfaces dspfarm dsp	Displays information about the DSP 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		
cisco-rtp		(Optional) Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with a Cisco proprietary payload type.
h245-alphanumeric		(Optional) Forwards DTMF tones by using the H.245 “alphanumeric” User Input Indication method. Supports tones 0-9, *, #, and A-D.
h245-signal		(Optional) Forwards DTMF tones by using the H.245 “signal” User Input Indication method. Supports tones 0-9, *, #, and A-D.

Defaults No default behavior or values.

Command Modes Dial-peer configuration

Command History	Release	Modification
	11.3(2)NA	This command was introduced on the Cisco AS5300 universal access server.
	12.0(2)XH	The cisco-rtp , h245-alphanumeric , and h245-signal keywords were added.
	12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
	12.0(7)XK	This command was first supported for Voice over IP (VoIP) on the MC3810 multiservice concentrator.
	12.1(2)T	Changes made in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines DTMF is the tone generated when you press a digit on a touch-tone phone. This tone is compressed at one end of a call; when the tone is decompressed at the other end, it can become distorted, depending on the codec used. The DTMF relay feature transports DTMF tones generated after call establishment out of band using a standard H.323 out-of-band method and a proprietary RTP-based mechanism.

The **dtmf-relay** command determines the outgoing format of relayed DTMF tones. The gateway automatically accepts all formats.

The gateway sends DTMF tones in the format that you specify only if the remote device supports it. If the remote device supports multiple formats, the gateway chooses the format based on the following priority:

1. cisco-rtp (highest priority)
2. h245-signal
3. h245-alphanumeric
4. None—DTMF sent in-band

The principal advantage of the **dtmf-relay** command is that it sends DTMF tones with greater fidelity than is possible in-band for most low-bandwidth codecs, such as G.729 and G.723. Without the use of DTMF relay, calls established with low-bandwidth codecs may have trouble accessing automated DTMF-based systems, such as voice mail, menu-based ACD systems, and automated banking systems.

**Note**

The **cisco-rtp** option of the **dtmf-relay** command is a proprietary Cisco implementation and operates only between two Cisco AS5800 universal access servers running Cisco IOS Release 12.0(2)XH, or between Cisco AS5800 universal access servers or Cisco 2600 or 3600 modular access routers running Cisco IOS Release 12.0(2)XH or later releases. Otherwise, the DTMF relay feature does not function, and the gateway sends DTMF tones in-band.

**Note**

The **h245-alphanumeric** and **h245-signal** DTMF settings on an MC3810 multiservice concentrator require a high-performance compression module (HCM) and are not supported on an MC3810 multiservice concentrator with a non-HCM voice compression module (VCM).

Examples

The following example configures DTMF relay with the **cisco-rtp** option when sending DTMF tones to dial peer 103:

```
dial-peer voice 103 voip
 dtmf-relay cisco-rtp
end
```

The next example configures DTMF relay with the **cisco-rtp** or **h245-signal** options when sending DTMF tones to dial peer 103:

```
dial-peer voice 103 voip
 dtmf-relay cisco-rtp h245-signal
end
```

The next example configures the gateway to send DTMF in-band (the default) when sending DTMF tones to dial peer 103:

```
dial-peer voice 103 voip
 no dtmf-relay
end
```

Related Commands

Command	Description
dial-peer voice	Specifies the method of voice-related encapsulation.

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.

Defaults	Disabled

Command Modes	Dial-peer configuration

Command History	Release	Modification
	12.0(3)XG	This command was introduced on the Cisco 2600 series routers, 3600 series, and MC3810 multiservice concentrator.
	12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T, and support for the Cisco 7200 series router was added.

Usage Guidelines	This command applies to all Voice over Frame Relay (VoFR) and Voice over ATM (VoATM) applications on the Cisco MC3810 multiservice concentrator and to VoFR applications on the Cisco 2600 series routers and 3600 series routers. Cisco recommends that this command be used with low bit-rate codecs. When dtmf-relay (VoFR) is enabled, the digital signal processor (DSP) generates Annex A frames instead of passing a dual tone multifrequency (DTMF) tone through the network as a voice sample. For information about the payload format of FRF.11 Annex A frames, refer to the <i>Cisco IOS Wide-Area Networking Configuration Guide</i> and <i>Cisco IOS Wide-Area Networking Command Reference, Release 12.2</i>.

Examples	The following example shows how to enable FRF.11 Annex A frames on a Cisco 2600 series routers or 3600 series router or on an MC3810 multiservice concentrator for VoFR dial peer 200, starting from global configuration mode:

```
dial-peer voice 200 vofr
dtmf-relay
```

Related Commands	Command	Description
	called-number (dial-peer)	Enables an incoming VoFR call leg to get bridged to the correct POTS call leg when using a static FRF.11 trunk connection.
	codec (dial-peer)	Specifies the voice coder rate of speech for a VoFR dial peer.
	connection	Specifies a connection mode for a voice port.
	cptone	Specifies a regional analog voice interface-related tone, ring, and cadence setting.
	destination-pattern	Specifies the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
	preference	Indicates the preferred order of a dial peer within a rotary hunt group.
	session protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.
	session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
	signal-type	Sets the signaling type to be used when connecting to a dial peer.

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	<i>milliseconds</i>	DTMF interdigit timer duration, in milliseconds. The valid range is from 250 to 3000. The default is 3000 milliseconds.

Defaults	3000 milliseconds

Command Modes	T1 controller configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines	Use the dtmf timer inter-digit command to specify the duration in milliseconds the router waits to detect the end of DTMF digits. After this period, the router expects no more digits to arrive and establishes the call.

Examples	The following example, beginning in global configuration mode, sets the DTMF interdigit timer value to 250 milliseconds:

```
controller T1 2
ds0-group 2 timeslots 4-10 type e&m-fgb dtmf dnis
cas-custom 2
dtmf timer inter-digit 250
```

Related Commands	Command	Description
	cas-custom	Customizes E1 R2 signaling parameters for a particular E1 channel group on a channelized E1 line.
	ds0-group	Configures channelized T1 time slots, which enables a Cisco AS5300 universal access server modem to answer and send an analog call.

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.

Defaults No default behavior or values.

Command Modes Controller configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced on the Cisco 3600 series routers.

Usage Guidelines Use the **echo-cancel comfort-noise** command to generate background noise to fill silent gaps during calls if voice activated dialing (VAD) is activated. If comfort noise is not enabled and VAD is enabled at the remote end of the connection, the user hears nothing or silence when the remote party is not speaking.

The configuration of comfort noise affects only the silence generated at the local interface; it does not affect the use of VAD on either end of the connection or the silence generated at the remote end of the connection.

For the OC-3/STM-1 ATM Circuit Emulation Service network module, echo cancellation must be enabled.

Examples The following example enables comfort noise on a T1 controller:

```
controller T1 0/0
 echo-cancel enable
 echo-cancel comfort-noise
```

Related Commands	Command	Description
	echo-cancel enable (controller)	Enables echo cancellation on a voice port.
	voice port	Specifies which port is used for voice traffic.

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.

Defaults No default behavior or values.

Command Modes Controller configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced on the Cisco 2600 series routers.

Usage Guidelines Use the **echo-cancel compensation** command to add attenuation control to the T1 or E1 controller. When this command is enabled, 6 decibels of attenuation are inserted if the signal level from the receive direction is loud. When loud signals are not received, the attenuation is removed.

For the OC-3/STM-1 ATM Circuit Emulation Service network module, echo cancellation must be enabled.

Examples The following example enables attenuation control on a T1 controller:

```
controller T1 0/0
 echo-cancel enable
 echo-cancel compensation
```

Related Commands	Command	Description
	echo-cancel enable (controller)	Enables echo cancellation on a voice port.
	voice port	Specifies which port is used for voice traffic.

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

Syntax Description	8	8 milliseconds.
	16	16 milliseconds.
	24	24 milliseconds.
	32	24 milliseconds.

Defaults 16 milliseconds

Command Modes Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 series routers.
	11.3(1)MA	This command was implemented on the Cisco MC3810 multiservice concentrator.
	12.0(5)XK	The command was modified to add the 8-millisecond option.
	12.0(5)XE	The command was modified to support the Cisco 7200 router platform.
	12.1(1)T	The Cisco IOS Release 12.0(5)XK and 12.0(5)XE changes were integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines Use the **echo-cancel coverage** command to adjust the coverage size of the echo canceller. This command enables cancellation of voice that is sent out the interface and received back on the same interface within the configured amount of time. If the local loop (the distance from the interface to the connected equipment that is producing the echo) is longer, the configured value of this command should be extended.

If you configure a longer value for this command, it takes the echo canceller longer to converge; in this case, the user might hear a slight echo when the connection is initially set up. If the configured value for this command is too short, the user might hear some echo for the duration of the call because the echo canceller is not cancelling the longer delay echoes.

There is no echo or echo cancellation on the network side (for example, the non-POTS side) of the connection.

**Note**

This command is valid only if the echo cancel feature has been enabled. For more information, see the **echo-cancel enable** command.

Examples

The following example adjusts the size of the echo canceller to 8 milliseconds on the Cisco 7200 series routers:

```
voice-port 1/0:0
echo-cancel enable
echo-cancel coverage 8
```

Related Commands

Command	Description
echo-cancel enable (controller)	Enables echo cancellation on a voice port.
echo-cancel enable	Enable echo cancellation on a voice port.

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.

Defaults

Enabled for all interface types.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced for the Cisco 3600 series routers.

Usage Guidelines

The **echo-cancel enable** command enables cancellation of voice that is sent out the interface and is received back on the same interface; sound that is received back in this manner is perceived by the listener as an echo. Disabling echo cancellation might cause the remote side of a connection to hear an echo. Because echo cancellation is an invasive process that can minimally degrade voice quality, this command should be disabled if it is not needed.

The **echo-cancel enable** command does not affect the echo heard by the user on the analog side of the connection.

There is no echo path for a 4-wire ear and mouth (E&M) interface. The echo canceller should be disabled for this interface type.



Note

This command is valid only if the **echo-cancel coverage** command has been configured. For more information, refer to the **echo-cancel coverage** command.

Examples

The following example enables the echo cancellation feature and adjusts the size of the echo canceller to 16 milliseconds on the Cisco 3600 series routers:

```
voice-port 1/0/0
 echo-cancel enable
 echo-cancel coverage 16
```

The following example enables the echo cancellation feature and adjusts the size of the echo canceller to 16 milliseconds on the Cisco MC3810 multiservice concentrator:

```
voice-port 1/1
```

```
echo-cancel enable
echo-cancel coverage 16
```

Related Commands

Command	Description
echo-cancel coverage	Specifies the amount of coverage for echo cancellation.
echo-cancel enable (controller)	Enables the echo cancellation on a voice port.
non-linear	Enables nonlinear processing in the echo canceler.

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.

Defaults Enabled for all interface types.

Command Modes Controller configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced for the OC-3/STM-1 ATM Circuit Emulation Service network module on the Cisco 3600 series routers.

Usage Guidelines The **echo-cancel enable** command enables cancellation of voice that is sent out of the interface and received back on the same interface. Disabling echo cancellation might cause the remote side of a connection to hear an echo. Because echo cancellation is an invasive process that can minimally degrade voice quality, this command should be disabled if it is not needed.

The **echo-cancel enable** command does not affect the echo heard by the user on the analog side of the connection.



Note This command is valid only if the **echo-cancel coverage** command has been configured.

The following example enables the echo cancel feature on a T1 controller:

```
controller T1 0/0
 echo-cancel enable
 echo-cancel coverage 32
```

Related Commands	Command	Description
	echo-cancel coverage	Specifies the amount of coverage for echo cancellation.
	echo-cancel enable	Enables the echo cancellation on a voice port.
	non-linear	Enables nonlinear processing in the echo canceler.
	voice port	Configures the voice port.

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.

Defaults

No default behavior or values.

Command Modes

Controller configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the Cisco 3600 series routers.

Usage Guidelines

Use an **echo-cancel loopback** test on lines to detect and distinguish equipment malfunctions caused by either the line or the interface. If correct echo cancellation is not possible when an interface is in loopback mode, the interface is the source of the problem.

Examples

On a Cisco 3600 series routers router, the following example sets up echo cancellation loopback diagnostics:

```
controller T1 0/0
 echo-cancel enable
 echo-cancel coverage 32
 echo-cancel loopback
```

Related Commands

Command	Description
echo-cancel enable (controller)	Enables echo cancellation on a voice port.

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.

Defaults No default behavior or values.

Command Modes Interface configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0	This command was integrated into Cisco IOS Release 12.0.

Usage Guidelines This command applies to ATM configuration on the Cisco MC3810 multiservice concentrator. This command is supported only on serial ports 0 and 1.

Examples

The following example enables CES ATM encapsulation on serial port 0 on the Cisco MC3810 multiservice concentrator:

```
interface serial 0
 encapsulation atm-ces
```

Related Commands

Command	Description
ces cell-loss-integration-period	Sets the CES cell-loss integration period on the Cisco MC3810 multiservice concentrator.
ces clockmode synchronous	Configures the ATM CES synchronous clock mode on the Cisco MC3810 multiservice concentrator.
ces connect	Maps the CES service to an ATM PVC on the Cisco MC3810 multiservice concentrator.
ces initial-delay	Configures the size of the receive buffer of a CES circuit on the Cisco MC3810 multiservice concentrator.

Command	Description
ces max-buf-size	Configures the send buffer of a CES circuit on the Cisco MC3810 multiservice concentrator.
ces partial-fill	Configures the number of user octets per cell for the ATM CES on the Cisco MC3810 multiservice concentrator.
ces service	Configures the ATM CES type on the Cisco MC3810 multiservice concentrator.

encapsulation ftc-trunk

This command was removed in Cisco IOS Release 12.1(2)T and is no longer supported in Cisco IOS Release 12.2.

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 }
```

Syntax Description

des-cbc-sha	Encryption type ssl_rsa_with_des_cbc_sha cipher suite.
des40-cbc-sha	Encryption type ssl_rsa_export_with_des40_cbc_sha cipher suite.
dh-des-cbc-sha	Encryption type ssl_dh_rsa_with_des_cbc_sha cipher suite.
dh-des40-cbc-sha	Encryption type ssl_dh_rsa_export_with_des40_cbc_sha cipher suite.
null-md5	Encryption type ssl_rsa_with_null_md5 cipher suite.
null-sha	Encryption type ssl_rsa_with_null_sha cipher suite.
all	All encryption methods are used in the Secure Socket Layer (SSL).

Defaults

The default encryption method is **all**. If none of the encryption methods is configured, the system uses all of the encryption methods in the SSL session negotiation.

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 and 3600 series and on the Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

For Cisco IOS Release 12.0(4)XH1, only one encryption method is allowed for each provider.

Examples

The following example sets the algorithm to be negotiated with the provider, using the **encryption** command:

```
settlement 0
 encryption des-cbc-sha
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device identification.
max-connection	Sets the maximum number of simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters settlement configuration mode.
show settlement	Displays the configuration for all settlement server transactions.
shutdown	Disables the settlement provider.
type	Specifies the provider type.
url	Specifies the ISP address.

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*

Syntax Description	<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.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	11.3(1)MA	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines	Use the erase vfc command to erase the contents of Flash memory for a specified VFC (thereby freeing space in VFC Flash memory) including the default file list and the capability file list.

Examples	The following example erases the Flash memory on the VFC located in slot 0: Router# erase vfc 0

Related Commands	Command	Description
	delete vfc	Deletes a file from VFC Flash memory.

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*

Syntax Description	<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.

Defaults	0

Command Modes	Dial-peer configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 series routers.

Usage Guidelines	This command applies to Voice over IP (VoIP) dial peers.
	VoIP monitors the quality of voice received over the network. Use the expect-factor command to specify when the router generates a Simple Network Management Protocol (SNMP) trap to the network manager.

Examples	The following example configures toll quality of voice when connecting to a dial peer:

```
dial-peer voice 10 voip
  expect-factor 0
```


fax interface-type

To specify the voice feature card (VFC) to be used for a fax call, use the **fax interface-type** command in global configuration mode. To return to the default fax protocol, use the **no** form of this command.

fax interface-type {**modem** | **vfc**}

no fax interface-type {**modem** | **vfc**}

Syntax Description	modem	Specifies modem fax calls.
	vfc	Specifies the VFC fax calls.

Defaults	None

Command Modes	Global configuration

Command History	Release	Modification
	12.1(3)XI	This command was introduced on the Cisco AS5300 access server.
	12.1(5)T	This command was integrated into the Cisco IOS Release 12.1(5)T.

Usage Guidelines	When using this command to change the interface type for fax calls, you must reload (reboot or reset) the router.

On the Cisco AS5300 access server, the keyword **vfc** maps to the **fax-mail** keyword. If you enter the **show run** command, the **fax-mail** keyword will display. The voice gateway defaults are as follows:

- If the gateway has modem cards only, the default is the **modem** keyword.
- If the gateway has voice cards only, the default is the **fax-mail** keyword. The **modem** keyword is unavailable. This applies to all platforms except the Cisco AS5300 access server.
- If the gateway has both modems and voice cards, the default is the **modem** keyword.

Examples	The following example specifies the use of a VFC interface for fax calls:

```
configure terminal
fax interface-type vfc
```

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 **system** keyword. 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

Syntax Description	cisco	Cisco proprietary fax protocol.
	t38	ITU-T T.38 standard fax protocol.
	ls_redundancy <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 ls_redundancy parameter refers to data redundancy in the low-speed V.21-based T.30 fax machine protocol.
	hs_redundancy <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 hs_redundancy 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.
	system	Global fax protocol when neither cisco nor t38 is specified. The value is taken from the global configuration by default.

Defaults The default protocol is system.

Command Modes Dial-peer configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series routers, Cisco 3600 series routers, and Cisco MC3810 multiservice concentrators.

Usage Guidelines Use the **fax protocol t38** command to configure T.38 Fax Relay for a specific dial peer. The **t38** keyword enables the T.38 Fax Relay protocol. The **cisco** keyword selects the original Cisco proprietary fax protocol. When the **system** keyword is selected in the dial peer, it specifies the global default fax protocol used by a dial peer, set by the **fax protocol t38** command. The optional **ls_redundancy** and **hs_redundancy** parameters are used to send redundant T.38 fax packets.



Note The **ls_redundancy** and **hs_redundancy** parameters are applicable only to the T.38 Fax Relay protocol.

The **ls_redundancy** parameter refers to data redundancy in the low-speed, V.21-based T.30 fax machine protocol. For the **ls_redundancy** parameter, the *value* can be from 0 to 5. The default is 0 (no redundancy). The parameter *value* sets the redundancy factor for T.38 Fax Relay.

The **hs_redundancy** 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. For the **hs_redundancy** parameter, the *value* can be from 0 to 2. The default is 0 (no redundancy). The parameter *value* sets the redundancy factor for T.38 Fax Relay.



Note Setting the **hs_redundancy** parameter to a value greater than 0 causes a significant increase in the network bandwidth consumed by the fax call.

Examples

The following example configures T.38 Fax Relay for VoIP, beginning in global configuration mode:

```
dial-peer voice 99 voip
 fax protocol t38
```

Related Commands

Command	Description
fax rate	Establishes the rate at which a fax is sent to the specified dial peer.

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

cisco	Cisco proprietary fax protocol.
t38	ITU-T T.38 standard fax protocol.
ls_redundancy <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 ls_redundancy parameter refers to data redundancy in the low-speed V.21-based T.30 fax machine protocol.
hs_redundancy <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 hs_redundancy 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.

Defaults

Cisco fax protocol

Command Modes

Voice-service configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series routers, Cisco 3600 series routers, and Cisco MC3810 multiservice concentrators.

Usage Guidelines

Use the **fax protocol t38** command to configure T.38 Fax Relay for VoIP. The **t38** keyword enables the T.38 Fax Relay protocol. The **cisco** keyword selects the original Cisco proprietary fax protocol. When the **system** keyword is selected in the dial peer, it specifies the global default fax protocol used by a dial peer, set by the **fax protocol t.38** command. The optional **ls_redundancy** and **hs_redundancy** parameters are used to send redundant T.38 fax packets.



Note

The **ls_redundancy** and **hs_redundancy** parameters are applicable only to the T.38 Fax Relay protocol.

The **ls_redundancy** parameter refers to data redundancy in the low-speed V.21-based T.30 fax machine protocol. For the **ls_redundancy** parameter, the *value* can be from 0 to 5. The default is 0 (no redundancy). The parameter *value* sets the redundancy factor for T.38 Fax Relay.

The **hs_redundancy** 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. For the **hs_redundancy** parameter, the *value* can be from 0 to 2. The default is 0 (no redundancy). The parameter *value* sets the redundancy factor for T.38 Fax Relay.



Note Setting the **hs_redundancy** parameter to a value greater than 0 causes a significant increase in the network bandwidth consumed by the fax call.

Examples

The following example configures the T.38 fax protocol for VoIP, beginning in global configuration mode:

```
voice service voip
  fax protocol t38
```

Related Commands

Command	Description
fax protocol (dial-peer)	Specifies the fax protocol for a specific VoIP dial peer.
fax protocol t.38	

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 rate**]

no fax rate

Syntax Description	
2400	Specifies a fax transmission speed of 2400 bits per second (bps).
4800	Specifies a fax transmission speed of 4800 bps.
7200	Specifies a fax transmission speed of 7200 bps.
9600	Specifies a fax transmission speed of 9600 bps.
12000	Specifies a fax transmission speed of 12,000 bps.
14400	Specifies a fax transmission speed of 14,400 bps.
disable	Disables Fax Relay transmission capability.
voice	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 64-k voice rate. If the voice codec is G.729 (8k), the fax transmission speed will be 7200 bps.
bytes rate	(Optional) Specifies fax packetization rate, in milliseconds. Range is 20 to 48. Default is 20. - For Cisco fax relay, this keyword-argument pair is valid only on Cisco 2600 series, Cisco 3600 series, Cisco 5300, and Cisco 7200 series routers. - For T.38 fax relay, this keyword-argument pair is valid only on Cisco 5350, Cisco 5400, and Cisco 5850 routers. For other routers, the packetization rate for T.38 fax relay is fixed at 40 ms and cannot be changed.

Defaults Voice calls

Command Modes Dial-peer configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced as the fax-rate command on the Cisco 3600 series routers.
	12.0(2)XH	The fax transmission rate of 12000 was added.
	12.0(4)T	This command was supported on the Cisco MC3810 multiservice concentrator.
	12.1(3)T	The command name changed from fax-rate to fax rate (nonhyphenated).

Release	Modification
12.1(3)XI	This command was implemented on the Cisco AS5300 universal access server.
12.1(5)T	The modifications made in Cisco IOS Release 12.1(3)XI were integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

Use the **fax rate** command to specify the fax transmission rate to the specified dial peer.

The values for this command apply only to the fax transmission speed and do not affect the quality of the fax itself. The higher transmission speed values (14,400 bps) provide a faster transmission speed but monopolize a significantly large portion of the available bandwidth. The lower transmission speed values (2400 bps) provide a slower transmission speed and use a relatively smaller portion of the available bandwidth.



Note The fax call will not get compressed using the **ip rtp header-compression** command because User Datagram Protocol (UDP) is being used and not Real-Time Transport Protocol (RTP). For example, a 9600 bps fax call will take approximately 24 kbps.

If the fax rate transmission speed is set higher than the codec rate in the same dial peer, the data sent over the network for fax transmission will be above the bandwidth reserved for Resource Reservation Protocol (RSVP).



Tips

Because a large portion of the available network bandwidth will be monopolized by the fax transmission, Cisco does not recommend setting the fax rate value higher than the value of the selected codec. If the fax rate value is set lower than the codec value, faxes will take longer to send but will use less bandwidth.

The **voice** keyword specifies the highest possible transmission speed allowed by the voice rate. For example, if the voice codec is G.711, the fax transmission may occur up to 14,400 bps because 14,400 bps is less than the 64-k voice rate. If the voice codec is G.729 (8k), the fax transmission speed will be 7200 bps.

Examples

The following example configures a fax rate transmission speed of 9600 bps for faxes sent using a dial peer:

```
dial-peer voice 100 voip
  fax rate 9600 voice
```

The following example sets a fax rate transmission speed at 12,000 bps and the packetization rate at 20 milliseconds:

```
fax rate 12000 bytes 20
```

Related Commands

Command	Description
codec (dial-peer)	Specifies the voice coder rate of speech for a dial peer.
fax protocol (dial-peer)	Specifies the fax protocol for a specific VoIP dial peer.

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*}

Syntax Description	\$d\$	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.

Defaults	Enabled with a null string

Command Modes	Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
	12.1(1)	This command was integrated into Cisco IOS Release 12.1(1).

Usage Guidelines

Use the **fax receive called-subscriber** command to define the number displayed in the liquid crystal display (LCD) of the sending fax device when you are sending a fax to a recipient. Typically, with a standard Group 3 fax device, this is the telephone number associated with the receiving fax device. The command defines the CSI.

This command applies to on-ramp store and forward fax functions.

Examples

The following example configures 555-1234 as the called-subscriber number:

```
fax receive called-subscriber 5551234
```


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.

Defaults	Fax-relay ECM is enabled.

Command Modes	Dial-peer configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced.

Usage Guidelines	When this command is entered, the digital signal processor (DSP) fax-relay firmware disables ECM by modifying the Digital Information Signal (DIS) T.30 message. This is performed on DIS signals in both directions so that ECM is disabled in both directions even if only one gateway is configured with ECM disabled.

This setting is provisioned when the DSP channel starts fax relay and cannot be changed during the fax relay session.

Examples	The following dial-peer configuration disables ECM on the voice dial peer:

```
fax-relay ecm disable
```

The following dial-peer configuration enables ECM on the voice dial peer:

```
no fax-relay ecm disable
```

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		
<i>\$a\$</i>		Wildcard that inserts the date in the selected position.
<i>\$d\$</i>		Wildcard that inserts the destination address in the selected position.
<i>\$p\$</i>		Wildcard that inserts the page count in the selected position.
<i>\$s\$</i>		Wildcard that inserts the sender address in the selected position.
<i>\$t\$</i>		Wildcard that inserts the transmission time in the selected position.
<i>string</i>		Text string providing information (in addition to any preset wildcard values) included in the text header of the fax message. Valid characters include any text string by itself or a string of text in combination with command-specific wildcards—for example, a text string displaying the sender's company name or a combinational string like Time:\$t\$.

Defaults No center header information is displayed by default.

Command Modes Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
	12.1(1)	This command was integrated into Cisco IOS Release 12.1(1).

Usage Guidelines Mail messages that contain only text or that contain text attachments (Multipurpose Internet Mail Extensions [MIME] media-type text) can be converted by the off-ramp Cisco AS5300 into a format understood by fax machines using the Cisco AS5300 universal access server text-to-fax converter. When this conversion is performed, this **fax send center-header** command is used to indicate what header information should be added to the center top of pages.

Mail messages with Tag Image File Format (TIFF) attachments (MIME media image and subtype of TIFF) are expected to include their own per-page headers. Cisco AS5300 software does not modify TIFF attachments.

**Note**

Because the Cisco AS5300 universal access server does not alter fax TIFF attachments, you cannot configure faxed header information for faxes being converted from TIFF files to standard fax transmissions.

This command lets you configure multiple options at once—meaning that you can combine one or more wildcards with text string information to personalize your fax header information.

**Note**

If the information selected for the **fax send center-header** command exceeds the space allocated for the center fax header, the information is truncated.

This command applies to off-ramp store and forward fax functions.

Examples

The following example selects the transmission time of the fax as the center fax header information:

```
fax send center-header $t$
```

The following example configures the company name abc and its address as the center fax header information:

```
fax send center-header abc $$
```

Related Commands

Command	Description
fax send left-header	Specifies the data that will appear on the left in the fax header information.
fax send right-header	Specifies the data that will appear on the right in the fax header information.

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.

Defaults	No coverpage comment is displayed by default.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
	12.1(1)	This command was integrated into Cisco IOS Release 12.1(1).

Usage Guidelines	The fax send coverpage comment command can be overridden by the fax send coverpage e-mail controllable command.

This command applies to off-ramp store and forward fax functions.

Examples	The following example configures an individualized title comment of ABC Fax Services for generated fax cover sheets:

```
fax send coverpage enable
fax send coverpage comment ABC Fax Services
```

Related Commands	Command	Description
	fax send coverpage e-mail-controllable	Defers to the cover page setting in the e-mail header to generate a standard fax cover sheet.
	fax send coverpage enable	Enables the Cisco AS5300 universal access server to generate fax cover sheets for faxes that originate from e-mail messages.
	fax send coverpage show-detail	Prints all of the e-mail header information as part of the fax cover sheet.

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.							
Defaults	No default behavior or values.							
Command Modes	Global configuration							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.0(4)XJ</td><td>This command was introduced on the Cisco AS5300 universal access server.</td></tr><tr><td>12.1(1)</td><td>This command was integrated into Cisco IOS Release 12.1(1).</td></tr></table>		Release	Modification	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.	12.1(1)	This command was integrated into Cisco IOS Release 12.1(1).
Release	Modification							
12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.							
12.1(1)	This command was integrated into Cisco IOS Release 12.1(1).							
Usage Guidelines	Also use the destination address of an e-mail message to control the cover page generation on a per-recipient basis. Use the fax send coverpage e-mail-controllable command to configure the router to defer to the cover page setting in the e-mail header. In essence, the off-ramp router defers to the setting configured in the e-mail address itself. For example, if the address has a parameter set to cover=no, this parameter will override the setting for the fax send coverpage enable command and the off-ramp gateway will not generate and send a fax cover page. If the address has a parameter set to cover=yes, the off-ramp gateway will defer to this parameter and generate and send a fax cover page. This command applies to off-ramp store and forward fax functions. Table 18 shows examples of what the user would enter in the To: field of the e-mail message.							

Table 18 Example Entries for the To: Field

To: Field Entry	Description
FAX=+1-312-555-3260@fax.com	Fax sent to an E.164-compliant long distance telephone number in the United States. If the fax send coverpage enable command has been configured, store and forward fax will generate a fax cover page.
FAX=+1-312-555-3260/cover=no@fax.com	Fax sent to an E.164-compliant long distance telephone number in the United States. In this example, the fax send coverpage enable command is superseded by the cover=no statement. No cover page will be generated.
FAX=+1-312-555-3260/cover=yes@fax.com	Fax sent to an E.164-compliant long distance telephone number in the United States. In this example, the fax send coverpage enable command is superseded by the cover=yes statement. Store and forward fax will generate a fax coverpage.

Examples

The following example enables standard generated fax cover sheets:

```
fax send coverpage enable
fax send coverpage e-mail-controllable
```

Related Commands

Command	Description
fax send coverpage comment	Defines personalized text for the title field of a fax cover sheet.
fax send coverpage enable	Enables the Cisco AS5300 universal access server to generate fax cover sheets for faxes that originate from e-mail messages.
fax send coverpage show-detail	Prints all of the e-mail header information as part of the fax cover sheet.

fax send coverpage 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 coverpage enable** command in global configuration mode. To disable the generation of fax cover sheets, use the **no** form of this command.

fax send coverpage enable

no fax send coverpage enable

Syntax Description	This command has no arguments or keywords.

Defaults	This feature is disabled by default.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
	12.1(1)	This command was integrated into Cisco IOS Release 12.1(1).

Usage Guidelines	This command is applicable only for faxes that originate as e-mail messages. The Cisco AS5300 does not alter fax Tag Image File Format (TIFF) attachments. Therefore, this command cannot be used to enable the AS5300 to generate fax cover pages for faxes that are being converted from TIFF files to standard fax transmissions.

This command applies to off-ramp store and forward fax functions.

Examples	The following example enables the Cisco AS5300 universal access server to generate fax cover sheets: <pre>fax send coverpage enable</pre>

Related Commands	Command	Description
	fax send coverpage comment	Defines personalized text for the title field of a fax cover sheet.
	fax send coverpage e-mail-controllable	Defers to the cover page setting in the e-mail header to generate a standard fax cover sheet.
	fax send coverpage show-detail	Prints all of the e-mail header information as part of the fax cover sheet.

fax send coverpage show-detail

To print all of the e-mail header information as part of the fax cover sheet, use the **fax send coverpage 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 coverpage show-detail

no fax send coverpage show-detail

Syntax Description This command has no arguments or keywords.

Defaults No coverpage details are displayed by default.

Command Modes Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
	12.1(1)	This command was integrated into Cisco IOS Release 12.1(1).

Usage Guidelines This command applies to off-ramp store and forward fax functions.

This command is applicable only for faxes that originate as e-mail messages. The Cisco AS5300 does not alter fax Tag Image File Format (TIFF) attachments. Therefore, this command cannot be used to enable the AS5300 to display additional fax cover page information for faxes that are being converted from TIFF files to standard fax transmissions.

Examples The following example configures an individualized generated fax cover sheet that contains the e-mail header text:

```
fax send coverpage enable
no fax send coverpage e-mail-controllable
fax send coverpage show-detail
```

Related Commands	Command	Description
	fax send coverpage comment	Defines personalized text for the title field of a fax cover sheet.
	fax send coverpage e-mail-controllable	Defers to the cover page setting in the e-mail header to generate a standard fax cover sheet.
	fax send coverpage enable	Enables the Cisco AS5300 universal access server to generate fax cover sheets for faxes that originate from e-mail messages.

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*}

Syntax Description	<i>\$a\$</i>	Wildcard that inserts the date in the selected position.
	<i>\$d\$</i>	Wildcard that inserts the destination address in the selected position.
	<i>\$p\$</i>	Wildcard that inserts the page count in the selected position.
	<i>\$s\$</i>	Wildcard that inserts the sender address in the selected position.
	<i>\$t\$</i>	Wildcard that inserts the transmission time in the selected position.
	<i>string</i>	Text string providing information (in addition to any preset wildcard values) included in the text header of the fax message. Valid characters include any text string by itself or a string of text in combination with command-specific wildcards—for example, a text string displaying the sender's company name or a combinational string like Time: <i>\$t\$</i> .

Defaults No left header information is displayed by default.

Command Modes Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
	12.1(1)	This command was integrated into Cisco IOS Release 12.1(1).

Usage Guidelines Mail messages that contain only text or that contain text attachments (Multipurpose Internet Mail Extensions [MIME] media text) can be converted by the off-ramp Cisco AS5300 into a format understood by fax machines using the Cisco AS5300 text-to-fax converter. When this conversion is performed, this **fax send left-header** command is used to indicate what header information should be added to the left top of pages.

Mail messages with Tag Image File Format (TIFF) attachments (MIME media image and subtype of TIFF) are expected to include their own per-page headers. Cisco AS5300 software does not modify TIFF attachments.

This command lets you configure multiple options at once—meaning that you can combine one or more wildcards with text string information to personalize your fax header information.

**Note**

If the information selected for the **fax send left-header** command exceeds the space allocated for the left fax header, the information is truncated.

This command applies to off-ramp store and forward fax functions.

Examples

The following example selects the transmission time of the fax as the left fax header information:

```
fax send left-header $t$
```

The following example configures the company name Widget and its address as the left fax header information:

```
fax send left-header widget $$s$
```

Related Commands

Command	Description
fax send center-header	Specifies the data that will appear in the center position of the fax header information.
fax send right-header	Specifies the data that will appear on the right in the fax header information.

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.

Defaults	14400 bps

Command Modes	Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
	12.1(1)	This command was integrated into Cisco IOS Release 12.1(1).

Usage Guidelines	This command applies to off-ramp store and forward fax functions.

Examples	The following example sets the outbound fax transmission rate at 2400 bps: fax send max-speed 2400

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		
	<i>\$a\$</i>	Wildcard that inserts the date in the selected position.
	<i>\$d\$</i>	Wildcard that inserts the destination address in the selected position.
	<i>\$p\$</i>	Wildcard that inserts the page count in the selected position.
	<i>\$s\$</i>	Wildcard that inserts the sender address in the selected position.
	<i>\$t\$</i>	Wildcard that inserts the transmission time in the selected position.
	<i>string</i>	Text string providing information (in addition to any preset wildcard values) included in the text header of the fax message. Valid characters include any text string by itself or a string of text in combination with command-specific wildcards—for example, a text string displaying the sender's company name or a combinational string like Time:\$t\$.

Defaults No right header information is displayed by default.

Command Modes Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
	12.1(1)	This command was integrated into Cisco IOS Release 12.1(1).

Usage Guidelines Mail messages that contain only text or contain text attachments (Multipurpose Internet Mail Extensions [MIME] media text) can be converted by the off-ramp Cisco AS5300 into a format understood by fax machines using the Cisco AS5300 text-to-fax converter. When this conversion is performed, this **fax send right-header** command is used to indicate what header information should be added to right top of pages.

Mail messages with Tag Image File Format (TIFF) attachments (MIME media image and subtype of TIFF) are expected to include their own per-page headers. Cisco AS5300 software does not modify TIFF attachments.

This command lets you configure multiple options at once—meaning that you can combine one or more wildcards with text string information to personalize your fax header information.

**Note**

If the information selected for the **fax send right-header** command exceeds the space allocated for the right fax header, the information is truncated.

This command applies to off-ramp store and forward fax functions.

Examples

The following example selects the date of the fax as the right fax header information:

```
fax send right-header $a$
```

The following example configures the company name Widget and its address as the right fax header information:

```
fax send right-header widget $$
```

Related Commands

Command	Description
fax send center-header	Specifies the data that will appear in the center position of the fax header information.
fax send left-header	Specifies the data that will appear on the left in the fax header information.

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*}

Syntax Description	<i>\$s\$</i>	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>	Originating 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.

Defaults No TSI information is displayed by default.

Command Modes Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
	12.1(1)	This command was integrated into Cisco IOS Release 12.1(1).

Usage Guidelines The transmitting subscriber number is the number displayed in the liquid crystal display (LCD) of the receiving fax device. Typically, with a standard Group 3 fax device, this is the telephone number associated with the transmitting or sending fax device. This command defines the TSI.

This command applies to off-ramp store and forward fax functions.

Examples The following example configures the company name (as captured by the on-ramp from the sending fax machine as +18005551234) as the TSI:

```
fax send transmitting-subscriber +18005551234
```

forward-alarms

To turn on alarm forwarding so that alarms arriving on one T1/E1 port are sent to the other port on dual-mode multiflex trunk interface cards, use the **forward-alarms** command in controller configuration mode on the one port. To restore the default value so that no alarms are forwarded, use the **no** form of this command.

forward-alarms

no forward-alarms

Syntax Description	This command has no arguments or keywords.

Defaults	Alarm forwarding is disabled.

Command Modes	Controller configuration

Command History	Release	Modification
	12.0(7)XR	This command was introduced.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines	When you enter this command, physical-layer alarms on the configured port are forwarded to the other port on dual-port cards, simulating a one-way repeater operation. The system forwards RAIs (remote alarm indications, Yellow Alarms), alarm indication signals (AIS, or Blue Alarms), losses of frame (LOF alarms or Red Alarms), and losses of signaling (LOS alarms or Red Alarms).

Examples	The following example shows how to turn on alarm forwarding on controller E1 0/0 of a Cisco 2600 series router:

```
controller e1 0/0
forward-alarms
```

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

Syntax Description		
	<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 no forward-digits command.
	all	Forwards all digits. If all is entered, the full length of the destination pattern is used.
	extra	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.

Defaults	Dialed digits not matching the destination pattern are forwarded.

Command Modes	Dial-peer configuration

Command History	Release	Modification
	11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.
	12.0(2)T	The implicit option was added.
	12.0(4)T	This command was modified to support ISDNBF PRI QSIG signaling calls.
	12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series routers, the implicit keyword was removed, and the extra keyword was added.
	12.1(2)T	The modifications made in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command applies only to plain old telephone service (POTS) dial peers. Forwarded digits are always right justified so that extra leading digits are stripped. The destination pattern includes both explicit digits and wildcards if present. Use the default form of this command if a nondefault digit-forwarding scheme was entered previously and you wish to restore the default.

For QSIG ISDN connections, entering the **forward-digits all** command implies that all the digits of the called party number are sent to the ISDN connection. When the **forward-digits num-digit** command and a number from 1 to 32 are entered, the number of digits of the called party number specified (right justified) are sent to the ISDN connection.

Examples

The following example shows that all digits in the destination pattern of a POTS dial peer are forwarded:

```
dial-peer voice 1 pots
 destination-pattern 8...
 forward-digits all
```

The following example shows that four of the digits in the destination pattern of a POTS dial peer are forwarded:

```
dial-peer voice 1 pots
 destination-pattern 555....
 forward-digits 4
```

The following example shows that the extra right-justified digits that exceed the length of the destination pattern of a POTS dial peer are forwarded:

```
dial-peer voice 1 pots
 destination-pattern 555....
 forward-digits extra
```

Related Commands

Command	Description
destination-pattern	Defines the prefix or the full E.164 telephone number to be used for a dial peer.
show dial-peer voice	Displays configuration information for dial peers.

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*

no frame-relay voice bandwidth *bps-reserved*

Syntax Description	<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.

Defaults	Disabled (zero)

Command Modes	Map-class configuration

Command History	Release	Modification
	12.0(3)XG	This command was introduced on the Cisco 2600 series routers, 3600 series, 7200 series, and on the MC3810 multiservice concentrator.
	12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
	12.0(5)T	The queue depth keyword and argument option was added.
	12.2(1)	The queue depth keyword and argument option was deleted.

Usage Guidelines	To use this command, you must first associate a Frame Relay map class with a specific DLCI and then enter map-class configuration mode and set the amount of bandwidth to be reserved for voice traffic for that map class.

If a call is attempted and there is not enough remaining bandwidth reserved for voice to handle the additional call, the call will be rejected. For example, if 64 kbps is reserved for voice traffic and a codec and payload size is being used that requires 10 kbps of bandwidth for each call, the first six calls attempted will be accepted, but the seventh call will be rejected.

Reserve queues are not required for Voice over Frame Relay (VoFR).



Note

Cisco strongly recommends that you set voice bandwidth to a value less than the committed information rate (CIR) if Frame Relay traffic shaping is configured. Cisco also strongly recommends that you set the minimum CIR (using the **frame-relay mincir** command) to be at least equal to or greater than the voice bandwidth.

Calculating Required Bandwidth

The bandwidth required for a voice call depends on the bandwidth of the codec, the voice packetization overhead, and the voice frame payload size. The smaller the voice frame payload size, the higher the bandwidth required for the call. To make the calculation, use the following formula:

$$\text{required\_bandwidth} = \text{codec\_bandwidth} \times (1 + \text{overhead} / \text{payload\_size})$$

As an example, the overhead for a VoFR voice packet is between 6 and 8 bytes: a 2-byte Frame Relay header, a 1- or 2-byte FRF.11 header (depending on the CID value), a 2-byte cyclic redundancy check (CRC), and a 1-byte trailing flag. If voice sequence numbers are enabled in the voice packets, there is an additional 1-byte sequence number. Table 19 shows the required voice bandwidth for the G.729 8000-bps speech coder for various payload sizes.

Table 19 Required Voice Bandwidth Calculations for G.729

Codec	Codec Bandwidth	Voice Frame Payload Size	Required Bandwidth per Call (6-Byte OH)	Required Bandwidth per Call (8-Byte OH)
G.729	8000 bps	120 bytes	8400 bps	8534 bps
G.729	8000 bps	80 bytes	8600 bps	8800 bps
G.729	8000 bps	40 bytes	9200 bps	9600 bps
G.729	8000 bps	30 bytes	9600 bps	10134 bps
G.729	8000 bps	20 bytes	10400 bps	11200 bps

To configure the payload size for the voice frames, use the **codec** command from dial-peer configuration mode.

Examples

The following example shows how to reserve 64 kbps for voice traffic for the “vofr” Frame Relay map class on a Cisco 2600 series routers, 3600 series, or 7200 series router or on an MC3810 multiservice concentrator:

```
interface serial 1/1
 frame-relay interface-dlci 100
  class vofr
  exit
map-class frame-relay vofr
 frame-relay voice bandwidth 64000
```

Related Commands

Command	Description
codec (dial-peer)	Specifies the voice coder rate of speech for a VoFR dial peer.
frame-relay fair-queue	Enables weighted fair queueing for one or more Frame Relay PVCs.
frame-relay fragment	Enables fragmentation for a Frame Relay map class.
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface on the router or access server.
frame-relay mincir	Assigns the minimum CIR for Frame Relay traffic shaping.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.

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

This command is not supported in Cisco IOS Release 12.2. This command was added in Cisco IOS Release 12.2(2)T. For information about this command, refer to the *Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2 T*, at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tvr/index.htm>

freq-max-deviation

This command is not supported in Cisco IOS Release 12.2. This command was added in Cisco IOS Release 12.2(2)T. For information about this command, refer to the *Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2 T*, at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tvr/index.htm>

freq-max-power

This command is not supported in Cisco IOS Release 12.2. This command was added in Cisco IOS Release 12.2(2)T. For information about this command, refer to the *Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2 T*, at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tvr/index.htm>

freq-min-power

This command is not supported in Cisco IOS Release 12.2. This command was added in Cisco IOS Release 12.2(2)T. For information about this command, refer to the *Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2 T*, at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tvr/index.htm>

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*

Syntax Description	<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.

Defaults	No tone is specified for detection.

Command Modes	Voice-class configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 and 3600 series routers and on the MC3810 multiservice concentrator.

Usage Guidelines	To detect a tone with two frequency components (a dualtone), configure frequencies for <i>frequency-1</i> and <i>frequency-2</i>. To detect a tone with only one frequency component, configure a frequency for <i>frequency-1</i> and enter 0 for <i>frequency-2</i>. You can configure a router to detect up to 16 tones.

Examples	The following example configures tone number 1 (tone-id 1) with frequency components of 480 Hz and 2400 Hz:

```
voice class dualtone 100
  freq-pair 1 480 2400
exit
```

The following example configures tone number 1 (tone-id 1) with frequency components of 480 Hz and 2400 Hz and tone number 2 (tone-id 2) with frequency components of 560 Hz and 880 Hz:

```
voice class dualtone 50
  freq-pair 1 480 2400
  freq-pair 2 560 880
exit
```

■ freq-pair

Related Commands	Command	Description
	voice class dualtone	Creates a voice class for FXO tone detection parameters.

freq-power-twist

This command is not supported in Cisco IOS Release 12.2. This command was added in Cisco IOS Release 12.2(2)T. For information about this command, refer to the *Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2 T*, at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tvr/index.htm>

ftc-trunk frame-relay-dlci

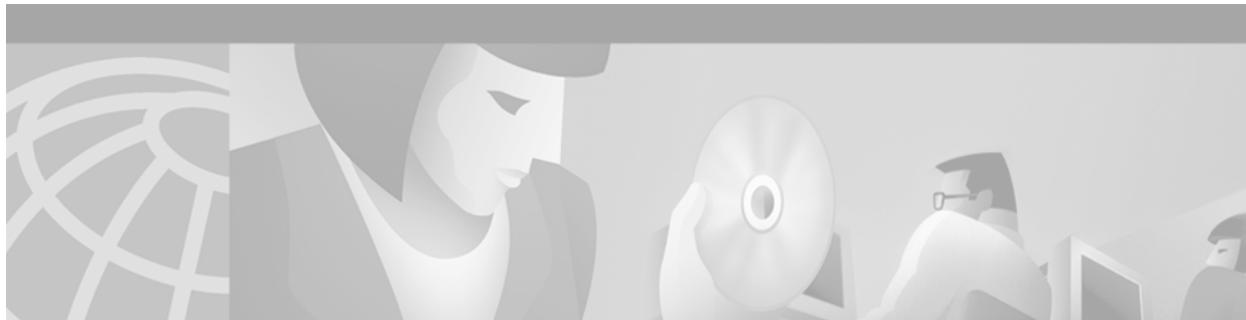
This command was removed in Cisco IOS Release 12.1(2)T and is no longer supported in this release.

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.



Cisco IOS Voice, Video, and Fax Commands: G Through P

This chapter presents the commands to configure and maintain Cisco IOS voice, video, and fax applications. The commands are presented in alphabetical order beginning with G. Some commands required for configuring voice, video, and fax may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice, Video, and Fax Configuration Guide*.

gatekeeper

To enter gatekeeper configuration mode, use the **gatekeeper** command in global configuration mode.

gatekeeper

Syntax Description	This command has no arguments or keywords.

Defaults	Disabled

Command Modes	Global configuration

Command History	Release	Modification
	11.3(2)NA	This command was introduced on the Cisco 2500 and 3600 series routers.
	12.0(3)T	This command was integrated into the Cisco IOS Release 12.0(3)T and, support for the Cisco MC3810 multiservice concentrator was added.

Usage Guidelines	Press Ctrl-Z or use the exit command to exit gatekeeper configuration mode.

Examples	The following example brings the gatekeeper online:

```
gatekeeper
no shutdown
```


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.

Defaults

The gateway is unregistered.

Command Modes

Global configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the Cisco 3600 series routers and Cisco AS5300 and Cisco AS5800 universal access servers.

Usage Guidelines

Use the **gateway** command to enable H.323 VoIP gateway functionality. After you enable the gateway, it will attempt to discover a gatekeeper by using the H.323 RAS GRQ message. If you enter **no gateway voip**, the VoIP gateway will unregister with the gatekeeper via the H.323 RAS URQ message.

Examples

The following example enables the gateway:

```
gateway
```

group

To create a session-group and associate it with a specified session-set, use the **group** command in backhaul session manager configuration mode. To delete the group, use the **no** form of this command.

group *group-name* **set** *set-name*

no group *group-name* **set** *set-name*

Syntax Description

<i>group-name</i>	Session-group name.
set <i>set-name</i>	Session-set name.

Defaults

No default behavior or values.

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

To associate the group named Group5 with the set named Set1, see the following example:

```
Router(config-bsm) # group group5 set set1
```

Related Commands

Command	Description
group auto-reset	Configures the maximum auto-reset value.
group cumulative-ack	Configures maximum cumulative acknowledgments.
group out-of-sequence	Configures maximum out-of-sequence segments that are received before an EACK is sent.
group receive	Configures maximum receive segments.
group retransmit	Configures maximum retransmits.
group timer cumulative-ack	Configures cumulative acknowledgment timeout.
group timer keepalive	Configures keepalive (or null segment) timeout.
group timer retransmit	Configures retransmission timeout.
group timer transfer	Configures state transfer timeout.

group auto-reset

To configure the maximum auto-reset value, use the **group auto-reset** command in backhaul session manager configuration mode. To set the value to the default value, use the **no** form of this command.

group *group-name* **auto-reset** *count*

no group *group-name* **auto-reset** *count*



Caution

Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

<i>group-name</i>	Session-group name.
auto-reset <i>count</i>	Maximum number of auto-resets. Range is 0 through 255.

Defaults

5

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

To configure the maximum auto-reset value for the group named Group5 to 6, see the following example:

```
Router(config-bsm)# group group5 auto-reset 6
```

Related Commands

Command	Description
group cumulative-ack	Configures maximum cumulative acknowledgments.
group out-of-sequence	Configures maximum out-of-sequence segments that are received before an EACK is sent.
group receive	Configures maximum receive segments.
group retransmit	Configures maximum retransmits.

group cumulative-ack

To configure maximum cumulative acknowledgments, use the **group cumulative-ack** command in backhaul session manager configuration mode. Maximum cumulative acknowledgments are the maximum number of segments that are received before an acknowledgment is sent. To set the value to the default value, use the **no** form of this command.

group *group-name* **cumulative ack** *count*

no group *group-name* **cumulative ack** *count*



Caution

Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

<i>group-name</i>	Session-group name.
cumulative ack <i>count</i>	Maximum number of segments received before acknowledgment. Range is 0 through 255.

Defaults

3

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

To set the cumulative acknowledgment maximum for Group5 to 4, see the following example:

```
Router(config-bsm) # group group5 cumulative-ack 4
```

Related Commands

Command	Description
group auto-reset	Configures the maximum auto-reset value.
group out-of-sequence	Configures maximum out-of-sequence segments that are received before an EACK is sent.
group receive	Configures maximum receive segments.
group retransmit	Configures maximum retransmits.

group out-of-sequence

To configure maximum out-of-sequence segments that are received before an EACK is sent, use the **group out-of-sequence** command in backhaul session manager configuration mode. To set the value to the default value, use the **no** form of this command.

group *group-name* **out-of-sequence** *count*

no **group** *group-name* **out-of-sequence** *count*



Caution

Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

<i>group-name</i>	Session-group name.
out-of-sequence <i>count</i>	Maximum number of out-of-sequence segments. Range is 0 through 255.

Defaults

3

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

To set the out-of-sequence maximum for Group5 to 4, see the following example:

```
Router(config-bsm)# group group5 out-of-sequence 4
```

Related Commands

Command	Description
group auto-reset	Configures the maximum auto-reset value.
group cumulative-ack	Configures maximum cumulative acknowledgments.
group receive	Configures maximum receive segments.
group retransmit	Configures maximum retransmits.

group receive

To configure maximum receive segments, use the **group receive** command in backhaul session manager configuration mode. To set the value to the default value, use the **no** form of this command.

group *group-name* **receive** *count*

no **group** *group-name* **receive** *count*



Caution

Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

<i>group-name</i>	Session-group name.
receive <i>count</i>	Maximum number of segments in our receive window. The other side should send no more than this number of segments before receiving an acknowledgment for the oldest outstanding segment. Range is 1 through 64.

Defaults

32

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

To set the receive maximum to 10 for Group5, see the following example:

```
Router(config-bsm) # group group5 receive 10
```

Related Commands

Command	Description
group auto-reset	Configures the maximum auto-reset value.
group cumulative-ack	Configures maximum cumulative acknowledgments.
group out-of-sequence	Configures maximum out-of-sequence segments that are received before an EACK is sent.
group retransmit	Configures maximum retransmits.

group retransmit

To configure maximum retransmits, use the **group retransmit** command in backhaul session manager configuration mode. To set the value to the default value, use the **no** form of this command.

group *group-name* **retransmit** *count*

no group *group-name* **retransmit** *count*

**Caution**

Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

<i>group-name</i>	Session-group name.
retransmit <i>count</i>	Maximum number of retransmits. Range is 0 through 255.

Defaults

2

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

To set the retransmit maximum for Group5 to 3, see the following example:

```
Router(config-bsm)# group group5 retrans 3
```

Related Commands

Command	Description
group auto-reset	Configures the maximum auto-reset value.
group cumulative-ack	Configures maximum cumulative acknowledgments.
group out-of-sequence	Configures maximum out-of-sequence segments that are received before an EACK is sent.
group receive	Configures maximum receive segments.

group timer cumulative-ack

To configure cumulative acknowledgment timeout, use the **group timer cumulative ack** command in backhaul session manager configuration mode. Cumulative acknowledgment timeout is the maximum number of milliseconds RUDP will delay before sending an acknowledgment for a received segment. To set the value to the default value, use the **no** form of this command.

group *group-name* **timer cumulative ack** *time*

no group *group-name* **timer cumulative ack** *time*



Caution

Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

<i>group-name</i>	Session-group name.
timer cumulative ack <i>time</i>	Number of milliseconds RUDP will delay. Range is 100 through 65535.

Defaults

100

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

To set the cumulative acknowledgment timer for Group5 to 325, see the following example:

```
Router(config-bsm)# group group5 timer cumulative-ack 325
```

Related Commands

Command	Description
group timer keepalive	Configures keepalive (or null segment) timeout.
group timer retransmit	Configures retransmission timeout.
group timer transfer	Configures state transfer timeout.

group timer keepalive

To configure keepalive (or null segment) timeout, use the **group timer keepalive** command in backhaul session manager configuration mode. Keepalive timeout is the number of milliseconds RUDP will wait before sending a keepalive segment. To set the value to the default value, use the **no** form of this command.

group *group-name* **timer keepalive** *time*

no **group** *group-name* **timer keepalive** *time*



Caution

Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

<i>group-name</i>	Session-group name.
timer keepalive <i>time</i>	Number of milliseconds before RUDP sends a keepalive segment. Range is 100 through 65535.

Defaults

1000

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

To configure the keepalive timer for Group5 to 2050 milliseconds, see the following example:

```
Router(config-bsm)# group group5 timer keepalive 2050
```

Related Commands

Command	Description
group timer cumulative-ack	Configures cumulative acknowledgment timeout.
group timer retransmit	Configures retransmission timeout.
group timer transfer	Configures state transfer timeout.

group timer retransmit

To configure retransmission timeout, use the **group timer retransmit** command in backhaul session manager configuration mode. Retransmission timeout is the number of milliseconds RUDP will wait to receive an acknowledgment for a segment. To set the value to the default value, use the **no** form of this command.

group *group-name* **timer retransmit** *time*

no group *group-name* **timer retransmit** *time*



Caution

Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

<i>group-name</i>	Session-group name.
timer retransmit <i>time</i>	Number of milliseconds RUDP will delay. Range is 100 through 65535.

Defaults

300

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

The retransmit timer must be greater than the cumulative-ack timer.

Examples

To set the retransmit timer for Group5 to 650, see the following example:

```
Router(config-bsm) # group group5 timer retransmit 650
```

Related Commands

Command	Description
group timer cumulative-ack	Configures cumulative acknowledgment timeout.
group timer keepalive	Configures keepalive (or null segment) timeout.
group timer transfer	Configures state transfer timeout.

group timer transfer

To configure state transfer timeout, use the **group timer transfer** command in backhaul session manager configuration mode. To set the value to the default value, use the **no** form of this command.

group *group-name* **timer transfer** *time*

no group *group-name* **timer transfer** *time*

**Caution**

Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

<i>group-name</i>	Session-group name.
timer transfer <i>time</i>	Maximum number of milliseconds RUDP will wait for a transfer request. The range is 0 to 65535 milliseconds.

Defaults

2000

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

To set the state transfer timer for Group5 to 1800, see the following example:

```
Router(config-bsm)# group group5 timer transfer-state 1800
```

Related Commands

Command	Description
group timer cumulative-ack	Configures cumulative acknowledgment timeout.
group timer keepalive	Configures keepalive (or null segment) timeout.
group timer retransmit	Configures retransmission timeout.

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.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced for the Cisco 2500 and 3600 series routers and the AS5300 universal access server.
12.0(7)T	The vsa keyword was added.
12.1(1)T	The voip keyword was added.

Usage Guidelines

To collect basic start-stop connection accounting data, the gateway must be configured to support gateway-specific H.323 accounting functionality. The **gw-accounting** command enables you to send accounting data to the RADIUS server in one of four ways:

- Using standard IETF RADIUS accounting attribute/value (AV) pairs—This method is the basic method of gathering accounting data (connection accounting) according to the specifications defined by the IETF. Use the **gw-accounting h323** command to configure the standard IETF RADIUS method of applying H.323 gateway-specific accounting. [Table 20](#) shows the IETF RADIUS attributes supported.

Table 20 Supported IETF RADIUS Accounting Attributes

Number	Attribute	Description
30	Called-Station-Id	Allows the network access server to send the telephone number that the user called as part of the Access-Request packet (using Dialed Number Identification [DNIS] or similar technology). This attribute is supported only on ISDN, and modem calls on the Cisco AS5200 and Cisco AS5300 universal access server if used with ISDN PRI.
31	Calling-Station-Id	Allows the network access server to send the telephone number that the call came from as part of the Access-Request packet (using Automatic Number Identification or similar technology). This attribute has the same value as “remote-addr” from TACACS+. This attribute is supported only on ISDN, and modem calls on the Cisco AS5200 and Cisco AS5300 universal access server if used with ISDN PRI.
42	Acct-Input-Octets	Indicates how many octets have been received from the port over the course of the accounting service being provided.
43	Acct-Output-Octets	Indicates how many octets have been sent to the port over the course of delivering the accounting service.
44	Acct-Session-Id	Indicates a unique accounting identifier that makes it easy to match start and stop records in a log file. Acct-Session-Id numbers restart at 1 each time the router is power-cycled or the software is reloaded.
47	Acct-Input-Packets	Indicates how many packets have been received from the port over the course of this service being provided to a framed user.
48	Acct-Output-Packets	Indicates how many packets have been sent to the port in the course of delivering this service to a framed user.

For more information about RADIUS and the use of IETF-defined attributes, see the *Cisco IOS Security Configuration Guide*.

- Overloading the Acct-Session-Id field—Attributes that cannot be mapped to standard RADIUS are packed into the Acct-Session-Id attribute field as ASCII strings separated by the character “/”. The Acct-Session-Id attribute is defined to contain the RADIUS account session ID, which is a unique identifier that links accounting records associated with the same login session for a user. To support additional fields, we have defined the following string format for this field:

```
<session id>/<call leg setup time>/<gateway id>/<connection id>/<call origin>/
<call type>/<connect time>/<disconnect time>/<disconnect cause>/<remote ip address>
```

Table 21 shows the field attributes that you use with the overloaded session-ID method and a brief description of each.

Table 21 *Field Attributes in Overloaded Acct-Session ID*

Field Attribute	Description
Session-Id	Specifies the standard RADIUS account session ID.
Setup-Time	Provides the Q.931 setup time for this connection in Network Time Protocol (NTP) format. NTP time formats are displayed as %H: %M: %S %k %Z %tw %tn %td %Y where: %H is hour (00 to 23). %M is minutes (00 to 59). %S is seconds (00 to 59). %k is milliseconds (000 to 999). %Z is timezone string. %tw is day of week (Saturday through Sunday). %tn is month name (January through December). %td is day of month (01 to 31). %Y is year including century (for example, 1998).
Gateway-Id	Indicates the name of the underlying gateway in the form "gateway.domain_name."
Call-Origin	Indicates the origin of the call relative to the gateway. Possible values are originate and answer .
Call-Type	Indicates the call leg type. Possible values are telephony and VoIP .
Connection-Id	Specifies the unique global identifier used to correlate call legs that belong to the same end-to-end call. The field consists of 4 long words (128 bits). Each long word is displayed as a hexadecimal value and is separated by a space character.
Connect-Time	Provides the Q.931 connect time for this call leg, in NTP format.
Disconnect-Time	Provides the Q.931 disconnect time for this call leg, in NTP format.
Disconnect-Cause	Specifies the reason a call was taken offline as defined in the Q.931 specification.
Remote-Ip-Address	Indicates the address of the remote gateway port where the call is connected.

Because of the limited size of the Acct-Session-Id string, it is not possible to embed very many information elements in it. Therefore, this feature supports only a limited set of accounting information elements.

Use the **gw-accounting h323** command to configure the overloaded session ID method of applying H.323 gateway-specific accounting.

- Using vendor-specific RADIUS attributes—The IETF draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (Attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor-ID is 9, and the supported option has vendor-type 1, which is named “cisco-avpair.” The value is a string of the format:

```
protocol: attribute sep value *
```

“Protocol” is a value of the Cisco “protocol” attribute for a particular type of authorization. “Attribute” and “value” are an appropriate attribute/value (AV) pair defined in the Cisco TACACS+ specification, and “sep” is “=” for mandatory attributes and “*” for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

The VSA fields and their ASCII values are listed in [Table 22](#).

Table 22 VSA Fields and Their ASCII Values

IETF RADIUS Attribute	Vendor-Specific Company Code	Subtype Number	Attribute Name	Description
26	9	23	h323-remote-address	Indicates the IP address of the remote gateway.
26	9	24	h323-conf-id	Identifies the conference ID.
26	9	25	h323-setup-time	Indicates the setup time for this connection in Coordinated Universal Time (UTC) formerly known as Greenwich Mean Time (GMT) and Zulu time.
26	9	26	h323-call-origin	Indicates the origin of the call relative to the gateway. Possible values are originating and terminating (answer).
26	9	27	h323-call-type	Indicates the call leg type. Possible values are telephony and VoIP .
26	9	28	h323-connect-time	Indicates the connection time for this call leg in UTC.
26	9	29	h323-disconnect-time	Indicates the time this call leg was disconnected in UTC.
26	9	30	h323-disconnect-cause	Specifies the reason a connection was taken offline per the Q.931 specification.
26	9	31	h323-voice-quality	Specifies the impairment factor (ICPIF) affecting voice quality for a call.
26	9	33	h323-gw-id	Indicates the name of the underlying gateway.

Use the **gw-accounting h323 vsa** command to configure the VSA method of applying H.323 gateway-specific accounting.

- Using syslog records—The syslog accounting option exports the information elements associated with each call leg through a system log message, which can be captured by a syslog daemon on the network. The syslog output consists of the following:

```
<server timestamp> <gateway id> <message number> : <message label> : <list of AV pairs>
```

The syslog messages fields are listed in [Table 23](#).

Table 23 Syslog Message Output Fields

Field	Description
server timestamp	The time stamp created by the server when it receives the message to log.
gateway id	The name of the gateway that emits the message.
message number	The number assigned to the message by the gateway.
message label	A string used to identify the message category.
list of AV pairs	A string that consists of <attribute name> <attribute value> pairs separated by commas.

Use the **gw-accounting syslog** command to configure the syslog record method of gathering H.323 accounting data.

Examples

The following example configures basic H.323 accounting using IETF RADIUS attributes:

```
gw-accounting h323
```

The following example configures H.323 accounting using VSA RADIUS attributes:

```
gw-accounting h323 vsa
```


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#.
hopoff <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.
seq blast		(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.
default-technology		(Optional) Gateways registering with this prefix option are used as the default for routing any addresses that are otherwise unresolved.
gw ipaddr <i>ipaddr</i> [<i>port</i>]		(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.

Defaults By default, no technology prefix is defined, and LRQs are sent sequentially to all the gatekeepers listed.

Command Modes Gatekeeper configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the Cisco 2500 and 3600 series routers and the AS5300 universal access server.
12.1(1)T	This command was modified to allow the user to specify multiple hopoffs.
12.1(2)T	This command was modified to allow the user to specify whether LRQs should be sent simultaneously or sequentially to the gatekeepers.

Usage Guidelines

More than one gateway can register with the same technology prefix. In such cases, a random selection is made of one of them.

You do not have to define a technology prefix to a gatekeeper if there are gateways configured to register with that prefix and if there are no special flags (**hopoff** *gkid* or **default-technology**) that you want to associate with that prefix.

You need to configure the gateway type prefix of all remote technology prefixes that will be routed through this gatekeeper.

Examples

The following example defines two gatekeepers for technology zone 3:

```
gw-type-prefix 3#* hopoff c2600-1-gk hopoff c2514-1-gk
```

Related Commands

Command	Description
show gatekeeper gw-type-prefix	Displays the list of currently defined technology zones and the gatekeepers responsible for each.
zone prefix	Configures the gatekeeper with knowledge of its own prefix and the prefix of any remote zone.

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

Syntax Description

<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.

Defaults

The default timeout value is 15 seconds.

Command Modes

Voice class configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the Cisco 1700, 2500, 2600, 3600, 7200 series routers, AS5300 universal access server, uBR900 series, and uBR924.

Examples

The following example configures a timeout of 10 seconds, which is associated with the H.323 voice class labeled 1:

```
voice class h323 1
 h225 timeout tcp establish 10
```

Related Commands

Command	Description
voice class h323	Establishes an H.323 voice class.

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*]

Syntax Description

bandwidth <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.

Defaults

ASR is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 and 3600 series routers.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

This command is independent of the **h323 interface** command.

This command is not supported on Frame Relay or ATM interfaces for the Cisco MC3810 multiservice concentrator.



Note

Specifying the **no h323 asr bandwidth** *max-bandwidth* command removes the bandwidth setting but leaves ASR enabled. You must enter the **no h323 asr** command to disable ASR.

Examples

The following example enables ASR and specifies a maximum bandwidth of 10,000 kbps:

```
h323 asr bandwidth 10000
```

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	fast	Gateway uses H.323 Version 2 (Fast Connect) procedures.
	slow	Gateway uses H.323 Version 1 (Slow Connect) procedures.

Defaults The default is **fast**.

Command Modes Voice-service configuration

Command History	Release	Modification
	12.1(3)XI	This command was introduced on the Cisco 2600, 3600, and 7200 series routers, the AS5300 universal access server and AS5800 universal gateways, and on the Cisco MC3810 multiservice concentrator.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines In Cisco IOS Release 12.1(3)XI and later releases, H.323 Voice over IP (VoIP) gateways by default use H.323 Version 2 (Fast Connect) for all calls including those initiating RSVP. Previously, gateways used only Slow Connect procedures for RSVP calls. To enable Cisco IOS Release 12.1(3)XI gateways to be backward compatible with earlier releases of Cisco IOS Release 12.1 T, the **h323 call start** command forces the originating gateway to initiate calls using Slow Connect.

This **h323 call start** command is configured as part of the global voice-service configuration for VoIP services. It does not take effect unless the **call start system** voice-class configuration command is configured in the VoIP dial peer.

Examples The following example selects Slow Connect procedures for the gateway:

```
voice service voip
  h323 call start slow
```

Related Commands	Command	Description
	call rsvp-sync	Enables synchronization between RSVP and the H.323 voice signaling protocol.
	call rsvp-sync resv-timer	Sets the timer for RSVP reservation setup.
	call start	Selects whether the H.323 gateway uses Fast Connect or Slow Connect procedures for the specific VoIP dial peer.
	debug call rsvp-sync events	Displays the events that occur during RSVP synchronization.
	show call rsvp-sync conf	Displays the RSVP synchronization configuration.
	show call rsvp-sync stats	Displays statistics for calls that attempted RSVP reservation.
	voice service	Enters voice-service configuration mode and specifies the voice encapsulation type.

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

id <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.
ipaddr <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.
multicast	If this parameter is specified, the gatekeeper discovery message will be multicast to the well-known RAS multicast address and port.

Defaults

No gatekeeper is configured for the proxy.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 and 3600 series routers.

Usage Guidelines

You must enter the **h323 interface** and **h323 h323-id** commands before using this command. The **h323 gatekeeper** command must be specified on your Cisco IOS platform or the proxy will not go online. The proxy will use the interface address as its RAS signaling address.

Examples

The following example sets up a unicast discovery to a gatekeeper whose name is unknown:

```
h323 gatekeeper ipaddr 192.168.5.2
```

The following example sets up a multicast discovery for a gatekeeper of a particular name:

```
h323 gatekeeper id gk.zone5.com multicast
```

Related Commands	Command	Description
	h323 h323-id	Registers an H.323 proxy alias with a gatekeeper.
	h323 interface	Specifies the interface from which the proxy will take its IP address.

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.

Defaults

No default behaviors or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the Cisco 1700, 2500, 2600, 3600, and 7200 series routers, the AS5300 universal access server, and the uBR924.

Usage Guidelines

You can issue this command on any interface in the router. You do not have to issue it on the interface that you defined as the voice gateway interface (although it may be more convenient to do so). Issuing the command for one interface assigns the source IP address for the entire router.

Examples

The following example assigns a source IP address of 10.1.1.1:

```
h323-gateway voip bind srcaddr 10.1.1.1
```

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*

Syntax Description

<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.

Defaults

No gateway identification is defined.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the Cisco 2500 and 3600 series routers and the Cisco AS5300 universal access server.

Examples

The following example configures Ethernet interface 0/0 as the gateway interface. In this example, the gateway ID is GW13@cisco.com.

```
interface Ethernet0/0
 ip address 172.16.53.13 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK15.cisco.com ipaddr 172.16.53.15 1719
 h323-gateway voip h323-id GW13@cisco.com
 h323-gateway voip tech-prefix 13#
```

Related Commands

Command	Description
h323-gateway voip id	Defines the name and location of the gatekeeper for this gateway.
h323-gateway voip interface	Configures an interface as an H.323 interface.
h323-gateway voip tech-prefix	Defines the technology prefix that the gateway will register with the gatekeeper.

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]
```

Syntax Description	<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> .
	ipaddr	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.
	multicast	Indicates that the gateway will use multicast to locate the gatekeeper.
	priority number	(Optional) The priority of this gatekeeper. The range is 1 through 127, and the default value is 127.

Defaults No gatekeeper identification is defined.

Command Modes Interface configuration

Command History	Release	Modification
	11.3(6)NA2	This command was introduced on the Cisco 2500 and 3600 series routers and the Cisco AS5300 universal access server.
	12.0(7)T	The priority number keyword and argument option was added.

Usage Guidelines

This command tells the H.323 gateway associated with this interface which H.323 gatekeeper to talk to and where to locate it. The gatekeeper ID configured here must exactly match the gatekeeper ID in the gatekeeper configuration.

You can configure up to two alternate gatekeepers.

The IP address of the gatekeeper does not have to be explicit; you can also use the multicast option. Multicasting saves bandwidth by forcing the network to replicate packets only when necessary. The multicast option, shown below, notifies every gatekeeper in the LAN using a universal address, 224.0.1.41.

```
h323-gateway voip id GK1 multicast
h323-gateway voip id GK2 ipaddr 172.18.193.65 1719
```

Examples

The following example configures Ethernet interface 0.0 as the gateway interface and defines a specific gatekeeper for it. In this example, the gatekeeper ID is GK15.cisco.com and its IP address is 172.16.53.15 (using port 1719).

```
interface Ethernet0/0
 ip address 172.16.53.13 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK15.cisco.com ipaddr 172.16.53.15 1719
 h323-gateway voip h323-id GW13@cisco.com
 h323-gateway voip tech-prefix 13#
```

Related Commands

Command	Description
h323-gateway voip h323-id	Configures the H.323 name of the gateway that identifies this gateway to its associated gatekeeper.
h323-gateway voip interface	Configures an interface as an H.323 interface.
h323-gateway voip tech-prefix	Defines the technology prefix that the gateway will register with the gatekeeper.

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

Syntax Description	This command has no arguments or keywords.

Defaults	Disabled

Command Modes	Interface configuration

Command History	Release	Modification
	11.3(6)NA2	This command was introduced on the Cisco 2500 and 3600 series routers and the AS5300 universal access server.

Examples	The following example configures Ethernet interface 0.0 as the gateway interface. In this example, the h323-gateway voip interface command configures this interface as an H.323 interface.

```
interface Ethernet0/0
 ip address 172.16.53.13 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK15.cisco.com ipaddr 172.16.53.15 1719
 h323-gateway voip h323-id GW13@cisco.com
 h323-gateway voip tech-prefix 13#
```

Related Commands	Command	Description
	h323-gateway voip h323-id	Configures the H.323 name of the gateway that identifies this gateway to its associated gatekeeper.
	h323-gateway voip id	Defines the name and location of the gatekeeper for this gateway.
	h323-gateway voip tech-prefix	Defines the technology prefix that the gateway will register with the gatekeeper.

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*

Syntax Description

<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 (*).

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the Cisco 2500 and 3600 series routers and the Cisco AS5300 universal access server.

Usage Guidelines

This command defines a technology prefix that the gateway will then register with the gatekeeper. Technology prefixes can be used as a discriminator so that the gateway can tell the gatekeeper that a certain technology is associated with a particular call (for example, 15# could mean a fax transmission), or it can be used like an area code for more generic routing. No standard currently defines what the numbers in a technology prefix mean. By convention, technology prefixes are designated by a pound symbol (#) as the last character.



Note

Cisco gatekeepers use the asterisk (*) as a reserved character. If you are using Cisco gatekeepers, do not use the asterisk as part of the technology prefix.

Examples

The following example configures Ethernet interface 0/0 as the gateway interface. In this example, the technology prefix is defined as 13#.

```
interface Ethernet0/0
 ip address 172.16.53.13 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK15.cisco.com ipaddr 172.16.53.15 1719
 h323-gateway voip h323-id GW13@cisco.com
 h323-gateway voip tech-prefix 13#
```

Related Commands	Command	Description
	h323-gateway voip h323-id	Configures the H.323 name of the gateway that identifies this gateway to its associated gatekeeper.
	h323-gateway voip id	Defines the name and location of the gatekeeper for this gateway.
	h323-gateway voip interface	Configures an interface as an H.323 interface.

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*

Syntax Description

<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.

Defaults

No H.323 proxy alias is registered.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 and 3600 series routers.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

Each entry registers a specified H.323 ID proxy alias to a gatekeeper. Typically, these aliases are either simple text strings or legitimate e-mail IDs.



Note

You must enter the **h323 interface** command before using this command. The **h323 h323-id** command must be entered on the same interface as the **h323 gatekeeper** command. The proxy will not go online without the **h323 interface** command.

Examples

The following example registers an H.323 proxy alias called proxy1@zone5.com with a gatekeeper:

```
h323 h323-id proxy1@zone5.com
```

Related Commands

Command	Description
h323 gatekeeper	Specifies the gatekeeper associated with a proxy and controls how the gatekeeper is discovered.
h323 interface	Specifies the interface from which the proxy will take its IP address.

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** command and then the **h323 interface** command.

h323 interface [*port-number*]

no h323 interface [*port-number*]

Syntax Description

<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.

Defaults

Default port number is image dependent as described in the Syntax Description.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 and 3600 series routers.
12.1(5)T	The ability to specify the proxy port number was added on the 2600, 3600, and 7200 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

At proxy startup, Cisco IOS software checks for the presence of the VoIP gateway subsystem. If the subsystem is found to be present, the proxy code opens and listens for call setup requests on the new port. The proxy then registers this port with the gatekeeper.

Examples

The following example shows how to configure Ethernet interface 0 for incoming call setup requests:

```
interface ethernet0
 h323 interface
```

Related Commands	Command	Description
	bandwidth	Specifies the maximum aggregate bandwidth for H.323 traffic from a zone to another zone, within a zone, or for a session in a zone.
	bandwidth remote	Specifies the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper.
	h323 qos	Enables QoS on the proxy.
	h323 t120	Enables the T.120 capabilities on your router and specifies bypass or proxy mode.

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

ip-precedence <i>value</i>	Specifies that RTP streams should set their IP precedence bits to the specified value.
rsvp controlled-load	Specifies controlled load class of service.
rsvp guaranteed-qos	Specifies guaranteed QoS class of service.

Defaults

No QoS is configured.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 and 3600 series routers.

Usage Guidelines

You must execute the **h323 interface** command before using this command.

Both IP precedence and RSVP QoS can be configured by invoking this command twice with the two different QoS forms.

Examples

The following example enables QoS on the proxy:

```
interface Ethernet0
 ip address 172.21.127.38 255.255.255.192
 no ip redirects
 ip rsvp bandwidth 7000 7000
 ip route-cache same-interface
 fair-queue 64 256 1000
 h323 interface
 h323 qos rsvp controlled-load
 h323 h323-id px1@zone1.com
 h323 gatekeeper ipaddr 172.21.127.39
```

Related Commands

Command	Description
h323 interface	Specifies the interface from which the proxy will take its IP address.

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

bypass	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.
proxy	Proxy mode. In this mode, T.120 features function properly.

Defaults

Bypass mode

Command Modes

Interface configuration

Command History

Release	Modification
12.1(5)T	This command was introduced on the Cisco 2600, 3600, and 7200 series routers and the Cisco MC3810 multiservice concentrator.

Usage Guidelines

The **no** form of this command has no function—the only possible commands are **h323 t120 bypass** and **h323 t120 proxy**.

Examples

The following example shows how to enable the T.120 capabilities:

```
proxy h323
interface ethernet0
 h323 t120 proxy
```

Related Commands

Command	Description
bandwidth	Specifies the maximum aggregate bandwidth for H.323 traffic from a zone to another zone, within a zone, or for a session in a zone.
bandwidth remote	Specifies the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper.
h323 interface	Defines which port the proxy will listen on.

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.

Defaults

Disabled

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.0(5)T	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	Support for this command was extended to the Cisco 2600 and 3600 series routers.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Once you enter this command, no further hunting is allowed if a call fails on the specified dial peer.



Note

This command can be used with all types of dial peers.

Examples

The following example shows how to disable dial-peer hunting on a specific dial peer:

```
dial peer voice 100 vofr
  huntstop
```

The following example shows how to reenable dial-peer hunting on a specific dial peer:

```
dial peer voice 100 vofr
  no huntstop
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice-related encapsulation.

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 20.

Defaults

20

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.
12.0(7)XK	This command was first supported on the Cisco MC3810 multiservice concentrator.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command is applicable only to Voice over IP (VoIP) dial peers.

Use the **icpif** command to specify the maximum acceptable impairment factor for the voice calls sent by the selected dial peer.

Examples

The following example disables the **icpif** command:

```
dial-peer voice 10 voip
 icpif 0
```

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

high	The talk-battery (tip-to-ring) voltage is high (–48V) when the FXS port is idle.
low	The talk-battery (tip-to-ring) voltage is low (–24V) when the FXS port is idle.

Defaults

The idle voltage is –24V.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.0(4)T	This command was introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

Some fax equipment and answering machines require a –48V idle voltage to be able to detect an off-hook condition in a parallel phone.

If the idle voltage setting is **high**, the talk battery reverts to –24V whenever the voice port is active (off hook).

The **idle-voltage** command applies only to FXS voice ports on Cisco MC3810 multiservice concentrators.

Examples

The following example sets the idle voltage to –48V on voice port 1/1 on a Cisco MC3810 multiservice concentrator:

```
voice-port 1/1
 idle-voltage high
```

The following example restores the default idle voltage (–24V) on voice port 1/1 on a Cisco MC3810 multiservice concentrator:

```
voice-port 1/1
 no idle-voltage
```

 idle-voltage

Related Commands	Command	Description
	show voice port	Displays voice port configuration information.

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

rx-a-bit	Ignores the receive A bit.
rx-b-bit	Ignores the receive B bit.
rx-c-bit	Ignores the receive C bit.
rx-d-bit	Ignores the receive D bit.

Defaults

The default is mode-dependent:

- North American E&M:
 - The receive B, C, and D bits are ignored.
 - The receive A bit is not ignored.
- E&M MELCAS:
 - The receive A bit is ignored.
 - The receive B, C, and D bits are not ignored.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series routers.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The **ignore** command applies to E&M digital voice ports associated with T1/E1 controllers. Repeat the command for each receive bit to be configured. Use this command with the **define** command.

Examples

To configure voice port 1/1 on a Cisco MC3810 multiservice concentrator to ignore receive bits A, B, and C and to monitor receive bit D, enter the following commands:

```
voice-port 1/1
 ignore rx-a-bit
 ignore rx-b-bit
```

ignore

```
ignore rx-c-bit
no ignore rx-d-bit
```

To configure voice port 1/0/0 on a Cisco 3600 series router to ignore receive bits A, C, and D and to monitor receive bit B, enter the following commands:

```
voice-port 1/0/0
ignore rx-a-bit
ignore rx-c-bit
ignore rx-d-bit
no ignore rx-b-bit
```

Related Commands

Command	Description
condition	Manipulates the signaling bit pattern for all voice signaling types.
define	Defines the transmit and receive bits for North American E&M and E&M MELCAS voice signaling.
show voice port	Displays configuration information for voice ports.

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

mh	Specifies Modified Huffman image encoding. This is the IETF standard.
mr	Specifies Modified Read image encoding.
mmr	Specifies Modified Modified Read image encoding.
passthrough	Specifies that the image will not be modified by an encoding method.

Defaults

passthrough

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Use the **image encoding** command to specify an encoding method for e-mail fax TIFF images for a specific MMoIP dial peer. This command applies primarily to the on-ramp MMoIP dial peer. Although you can optionally create an off-ramp dial peer and configure a particular image encoding value for that off-ramp call leg, store and forward fax ignores the off-ramp MMoIP setting and sends the file using Modified Huffman encoding.

There are four available encoding methods:

- **Modified Huffman (MH)**—One-dimensional data compression scheme that compresses data in only one direction (horizontal). Modified Huffman compression does not allow the transmission of redundant data. This encoding method produces the largest image file size.
- **Modified Read (MR)**—Two-dimensional data compression scheme (used by fax devices) that handles the data compression of the vertical line and that concentrates on the space between lines and within given characters.
- **Modified Modified Read (MMR)**—Data compression scheme used by newer Group 3 fax devices. This encoding method produces the smallest possible image file size and is slightly more efficient than Modified Read.
- **Passthrough**—No encoding method will be applied to the image—meaning that the image will be encoded by whatever encoding method is used by the fax device.

The IETF standard for sending fax TIFF images is Modified Huffman encoding with fine or standard resolution. RFC 2301 requires that compliant receivers support TIFF images with MH encoding and fine or standard resolution. If a receiver supports features beyond this minimal requirement, you might want to configure the Cisco AS5300 universal access server to send enhanced-quality documents to that receiver.

The primary reason to use a different encoding scheme from MH is to save network bandwidth. MH ensures interoperability with all Internet fax devices, but it is the least efficient of the encoding schemes for sending fax TIFF images. For most images, MR is more efficient than MH, and MMR is more efficient than MR. If you know that the recipient is capable of receiving more efficient encodings than just MH, store and forward fax allows you to send the most efficient encoding that the recipient can process. For end-to-end closed networks, you can choose any encoding scheme because the off-ramp gateway can process MH, MR, and MMR.

Another factor to consider is the viewing software. Many viewing applications (for example, those that come with Windows 95 or Windows NT) are able to display MH, MR, and MMR. Therefore you should decide, based on the viewing application and the available bandwidth, which encoding scheme is right for your network.

This command applies to both on-ramp and off-ramp store and forward fax functions.

Examples

The following example selects Modified Modified Read as the encoding method for fax TIFF images sent by MMoIP dial peer 10:

```
dial-peer voice 10 mmoup
  image encoding mmr
```

Related Commands

Command	Description
image resolution	Specifies a particular fax image resolution for a specific MMoIP dial peer.

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

fine	Configures the fax TIFF image resolution to be 204-by-196 pixels per inch.
standard	Configures the fax TIFF image resolution to be 204-by-98 pixels per inch.
superfine	Configures the fax TIFF image resolution to be 204-by-391 pixels per inch.
passthrough	Indicates that the resolution of the fax TIFF image will not be altered.

Defaults

passthrough

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Use the **image resolution** command to specify a specific resolution (in pixels per inch) for e-mail fax TIFF images sent by the specified MMoIP dial peer. This command applies primarily to the on-ramp MMoIP dial peer. Although you can optionally create an off-ramp dial peer and configure a particular image resolution value for that off-ramp call leg, store and forward fax ignores the off-ramp MMoIP setting and sends the file using fine resolution.

This command enables you to increase or decrease the resolution of a fax TIFF image, thereby changing not only the resolution but also the size of the fax TIFF file. The IETF standard for sending fax TIFF images is Modified Huffman encoding with fine or standard resolution. The primary reason to configure a different resolution is to save network bandwidth.

This command applies to both on-ramp and off-ramp store and forward fax functions.

Examples

The following example selects the fine resolution (meaning 204-by-196 pixels per inch) for e-mail fax TIFF images associated with MMoIP dial peer 10:

```
dial-peer voice 10 mmoidp
  image encoding mh
  image resolution fine
```

■ image resolution

Related Commands	Command	Description
	image encoding	Selects a specific encoding method for fax images associated with an MMoIP dial peer.

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

600c	Specifies 600 ohms (complex).
600r	Specifies 600 ohms (real).
900c	Specifies 900 ohms (complex).
complex1	Specifies complex 1.
complex2	Specifies complex 2.

Defaults

600r

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.

Usage Guidelines

Use the **impedance** command to specify the terminating impedance of an Foreign Exchange Office (FXO) voice-port interface. The impedance value selected needs to match the specifications from the specific telephony system to which it is connected. Different countries often have different standards for impedance. CO switches in the United States are predominantly 600r. PBXs in the United States are normally either 600r or 900c.

If the impedance is set incorrectly (if there is an impedance mismatch), there will be a significant amount of echo generated (which could be masked if the **echo-cancel** command has been enabled). In addition, gains might not work correctly if there is an impedance mismatch.

Configuring the impedance on a voice port will change the impedance on both voice ports of a VPM card. This voice port must be shut down and then opened for the new value to take effect.

Examples

The following example configures an FXO voice port on the Cisco 3600 series router for a terminating impedance of 600 ohms (real):

```
voice-port 1/0/0
 impedance 600r
```

The following example configures an E&M voice port on the Cisco MC3810 multiservice concentrator for a terminating impedance of 900 ohms (complex):

```
voice-port 1/1
 impedance 900c
```

incoming called-number

To specify a digit string that can be matched by an incoming call to associate the call with a 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*

Syntax Description

<i>string</i>	Specifies the incoming called telephone number. Valid entries are any series of digits that specify the E.164 telephone number.

Defaults

No incoming called number is defined.

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.
11.3NA	This command was introduced on the Cisco AS5800 universal gateway.
12.0(4)XJ	This command was modified for store and forward fax.
12.0(7)XK	This command was first supported on the Cisco MC3810 multiservice concentrator platform.
12.1(2)T	This command was integrated into the Cisco IOS Release 12.1(2)T.

Usage Guidelines

When a Cisco device (such as a Cisco AS5300 universal access server or Cisco AS5800 universal gateway) is handling both modem and voice calls, it needs to be able to identify the service type of the call—meaning whether the incoming call to the server is a modem or a voice call. When the access server handles only modem calls, the service type identification is handled through modem pools. Modem pools associate calls with modem resources based on the called number (DNIS). In a mixed environment, in which the server receives both modem and voice calls, you need to identify the service type of a call by using the **incoming called-number** command.

If you do not use the **incoming called-number** command, the server attempts to resolve whether an incoming call is a modem or voice call based on the interface over which the call comes. If the call comes in over an interface associated with a modem pool, the call is assumed to be a modem call; if a call comes in over a voice port associated with a dial peer, the call is assumed to be a voice call.

By default, there is no called number associated with the dial peer, which means that incoming calls will be associated with dial peers based on matching calling number with answer address, call number with destination pattern, or calling interface with configured interface.

Use the **incoming called-number** command to define the destination telephone number for a particular dial peer. For the on-ramp POTS dial peer, this telephone number is the DNIS number of the incoming fax call. For the off-ramp MMoIP dial peer, this telephone number is the destination fax machine telephone number.

This command applies to both Voice over IP (VoIP) and POTS dial peers and applies to both on-ramp and off-ramp store and forward fax functions.

This command is also used to provide a matching VoIP dial peer on the basis of called number when fax or modem pass-through with named service events (NSEs) is defined globally on a terminating gateway.

You can ensure that all calls will match at least one dial peer by using the following commands:

```
Router(config)# dial-peer voice tag voip
Router(config-dial-peer)# incoming called-number .
```

Examples

The following example configures calls coming in to the server with a called number of 3799262 as being voice calls:

```
dial-peer voice 10 pots
incoming called-number 3799262
```

The following example configures the number (310) 555-9261 as the incoming called number for MMoIP dial peer 10:

```
dial-peer voice 10 mmoip
incoming called-number 3105559261
```

info-digits

To automatically prepend two information digits to the beginning of a dialed number associated with the given POTS dial peer, use the **info-digits** command in dial-peer configuration mode. To keep the router from automatically prepending the two-digit information numbers to the beginning of the POTS dial peer, use the **no** form of this command.

info-digits *string*

no info-digits

Syntax Description

string

Specifies the two-digit prefix that the router will automatically prepend to the dialed number for the given POTS dial peer.

Note This string cannot contain any more or any less than two digits.

Defaults

No default behavior or values.

Command Modes

Dial-peer configuration

Command History

Release

Modification

12.2(1)T

This command was introduced on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers and on Cisco AS5300 series universal access servers.

Usage Guidelines

This command is designed to prepend a pair of information digits to the beginning of the dialed number string for the POTS dial peer that will enable you to dynamically redirect the outgoing call. The **info-digits** command is only available for POTS dial peers.

Examples

The following example prepends the information number string 91 to the beginning of the dialed number for POTS dial peer 10:

```
dial-peer voice 10 pots
info-digits 91
```

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 }

Syntax Description	fax	Indicates that the information type has been set to store and forward fax.
	voice	Indicates that the information type has been set to voice.

Defaults	Voice

Command Modes	Dial-peer configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 series routers.
	12.0(4)XJ	This command was modified for store and forward fax.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines	This command applies to both on-ramp and off-ramp store and forward fax functions.

Examples	The following example sets the information type for MMoIP dial peer 10 to fax: dial-peer voice 10 mmoup information-type fax

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*

Syntax Description	<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.

Defaults	Zero (0) decibels

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced.
	11.3(1)MA	This command was first supported on the Cisco MC3810 multiservice concentrator.

Usage Guidelines	A system-wide loss plan must be implemented using both the input gain and output attenuation commands. Other equipment (including PBXs) in the system must be considered when creating a loss plan. The default value for this command assumes that a standard transmission loss plan is in effect, meaning that there must be an attenuation of –6 dB between phones. Connections are implemented to provide –6 dB of attenuation when the input gain and output attenuation commands are configured with the default value of 0 dB. You cannot increase the gain of a signal to the Public Switched Telephone Network (PSTN), but you can decrease it. If the voice level is too high, you can decrease the volume by either decreasing the input gain or increasing the output attenuation. You can increase the gain of a signal coming into the router. If the voice level is too low, you can increase the input gain by using the input gain command.

Examples	The following example configures a 3-dB gain to be inserted at the receiver side of the interface in the Cisco 3600 series router:

```
port 1/0/0
 input gain 3
```

The following example configures a 3-dB gain to be inserted at the receiver side of the interface in the Cisco MC3810 multiservice concentrator:

```
port 1/1
 input gain 3
```

Related Commands

Command	Description
output attenuation	Configures a specific output attenuation value for a voice port.

interface (RLM server)

To define the IP addresses of the Redundant Link Manager (RLM) server, use the **interface** command in interface configuration mode. To disable this function, use the **no** form of this command.

interface *name-tag*

no interface *name-tag*

Syntax Description	<i>name-tag</i>	Name to identify the server configuration so that multiple entries of server configuration can be entered.

Defaults	Disabled

Command Modes	Interface configuration

Command History	Release	Modification
	11.3(7)	This command was introduced.

Usage Guidelines	Each server can have multiple entries of IP addresses or aliases.

Examples	The following example shows how to configure the access server interfaces for RLM servers named Loopback1 and Loopback2:

```
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
interface Loopback2
 ip address 10.1.1.2 255.255.255.255
rlm group 1
 server r1-server
 link address 10.1.4.1 source Loopback1 weight 4
 link address 10.1.4.2 source Loopback2 weight 3
```

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

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

<i>number</i>	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.

Defaults

The default value for this command is zero (0).

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)NA	This command was introduced on the Cisco 2500, 3600 series routers and the Cisco AS5300 universal access server.

Usage Guidelines

Use the **ip precedence** (dial-peer) command to configure the value set in the IP precedence field when voice data packets are sent over the IP network. This command should be used if the IP link utilization is high and the quality of service for voice packets needs to have a higher priority than other IP packets. The **ip precedence** (dial-peer) command should also be used if RSVP is not enabled and the user would like to give voice packets a higher priority than other IP data traffic.

This command applies to Voice over IP (VoIP) peers.

Examples

The following example sets the IP precedence to 5:

```
dial-peer voice 10 voip
 ip precedence 5
```


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.

Defaults

Disabled

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.

Usage Guidelines

Use the **ip udp checksum** command to enable UDP checksum calculation for each of the outbound voice packets. This command is disabled by default to speed up the transmission of the voice packets. If you suspect that the connection has a high error rate, you should enable the **ip udp checksum** command to prevent corrupted voice packets forwarded to the digital signal processor (DSP).

This command applies to Voice over IP (VoIP) peers.

Examples

The following example calculates the UDP checksum for voice packets sent by dial peer 10:

```
dial-peer voice 10 voip
 ip udp checksum
```

Related Commands

Command	Description
loop-detect	Enables loop detection for T1 for Voice over ATM, Voice over Frame Relay, and Voice over HDLC.

isdn bind-l3

To configure the ISDN serial interface for backhaul, use the **isdn bind-l3** command in interface configuration mode. To disable backhaul on the interface, use the **no** form of this command.

```

isdn bind-l3 set-name

no isdn bind-l3 set-name
    
```

Syntax Description	<i>set-name</i> Session-set name.

Defaults	No default behavior or values.

Command Modes	Interface configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced.

Examples	To configure the ISDN serial interface for backhaul for the set named Set1, see the following example: <pre>Router(config-if)# isdn bind-l3 set1</pre>

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.

Defaults

By default, contiguous B channel handling is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco 2500, 3600, and 7200 series routers and on the Cisco MC3810 multiservice concentrator.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use the **isdn contiguous-bchan** command to specify contiguous bearer channel handling so that B channels 1 through 30, skipping 16, map to time slots 1 through 31. This is available for E1 PRI interfaces only, when the **primary-qsig** switch type option is configured by using the **isdn switch-type** command.

Examples

The following example shows the command configuration on the E1 interface of a Cisco 3660 series router E1 interface:

```
interface Serial15/0:15
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn overlap-receiving
 isdn incoming-voice voice
 isdn contiguous-bchan
```

Related Commands

Command	Description
isdn switch-type primary-qsig	Configures the primary-qsig switch type for PRI support.

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.

Defaults

Passage of messages is disabled by default; “release” and “release complete” messages terminate locally by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the Cisco 2600, 3600, and 7200 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

Enter this command under the isdn interface with switch type bri-qsig or pri-qsig. Use the **isdn global-disconnect** command to allow passage of “release” and “release complete” messages end-to-end across the network. This is required for certain types of QSIG PBXs whose software or features require either Facility or User Info IEs in those messages to be passed end-to-end between the PBXs. All QSIG interfaces that connect the PBXs to the routers must have this command enabled. This command is available when using the BRI QSIG or PRI QSIG switch type in either master or slave mode.

Examples

The following example shows command configuration on the T1 PRI interface of a Cisco 3660 series router:

```
interface Serial5/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn global-disconnect
 isdn overlap-receiving
 isdn incoming-voice voice
```

Related Commands	Command	Description
	isdn protocol-emulate	Configures the interface to serve as either the QSIG slave or the QSIG master.
	isdn switch-type	Configures the switch type for BRI or PRI support.

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 plain old telephone service (POTS) port.

Defaults

Each terminal device uses one subscriber line.

Command Modes

Interface configuration

Command History

Release	Modification
12.1.(2)XF	This command was introduced on the Cisco 800 series routers.

Usage Guidelines

Enter the **interface bri** command before entering the **isdn i-number** command.

Examples

The following example shows screen output for two LDNs configured under BRI interface 0:

```
interface bri0
  isdn i-number 1 5551234
  isdn i-number 2 5556789
  exit
dial-peer voice 1 pots
  destination-pattern 5551234
  exit
dial-peer voice 2 pots
  destination-pattern 5556789
  exit
```

Related Commands

Command	Description
interface bri	Specifies a BRI interface and enters interface configuration mode.

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

value Number from 1 to 127. See [Table 24](#) for a list of failure cause code values.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(2)T	This command was introduced to the Cisco IOS 12.1(2)T on the Cisco 2600, 3600, and 7200 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

The PBX can reroute calls based on the cause code returned by the router.

This command allows the original cause code to be changed to the value specified if the original cause code is not one of the following:

- NORMAL_CLEARING (16)
- USER_BUSY (17)
- NO_USER_RESPONDING (18)
- NO_USER_ANSWER (19)
- NUMBER_CHANGED (22)
- INVALID_NUMBER_FORMAT (28)
- UNSPECIFIED_CAUSE (31)
- UNASSIGNED_NUMBER (1)

[Table 24](#) describes the cause codes.

Table 24 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.
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.

Table 24 ISDN Failure Cause Codes (continued)

Failure Cause Code	Meaning
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.
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.

Examples

The following is an example of specifying a cause code to pass to a PBX when a call cannot be placed or completed of internal network failures:

```
isdn network-failure-cause 28
```

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	url	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.

Defaults	No URL is defined.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced on the Cisco 2600 and 3600 series routers and the Cisco AS5300 universal access server.

Usage Guidelines

The index file contains a list of audio files (URL) that can be downloaded from the TFTP server. Use the **ivr autoloading** command to download audio files from TFTP to memory. The command only starts up a background process. The background process (loader) does the actual down loading of the files.

The background process first reads the index file from either Flash or TFTP. It parses the files line by line looking for the URL. It ignores lines that start with # as comment lines. Once it has a correct URL, it tries to read that .au file into memory and creates a media object. If there are any errors during the reading of the file, it retries the configured number of times. If the mode is set to “verbose,” the loader logs the transaction to console. Once parsing has reached the end of the index file, the background process exits memory.

Perform the following checks before initiating the background process. If one of the checks fail, it indicates the background process is not started, and instead you will see an error response to the command.

- Check if any prompt is being actively used (IVR is actively playing some prompts). If there are active prompts, the command fails, displaying the following error message (.au files are also referred to as prompts):

```
command is not allowed when prompts are active
```
- Check if there is already a background process in progress. If there is a process, the command fails, displaying the following error:

```
previous autoloading command is still in progress
```

- Check if an earlier **ivr autoload** command has already been configured. If an **ivr autoload** command has already been configured, the user sees the following response when the command is issued:

```
previous command is being replaced
```

- When the **no ivr autoload** command is issued, if there was already an **ivr autoload** command in progress, it will be aborted.

The audio files (prompts) loaded using the **ivr autoload** command are not dynamically swapped out of memory. They are considered as autoloaded prompts as opposed to “dynamic” prompts. (See the **ivr prompt memory** command for details on dynamic prompts.)

Examples

The following example loads audio files from the TFTP server (located at `//jurai/mgindi/tclware/index4`):

```
ivr autoload url tftp://jurai/mgindi/tclware/index4
```

The index file for this example `index4` is shown as follows:

```
more index4
tftp://jurai/mgindi/tclware/au/en/en_one.au
tftp://jurai/mgindi/tclware/au/ch/ch_one.au
tftp://jurai/mgindi/tclware/au/ch/ch_one.au
```

An example of an index file on Flash is shown as follows:

```
flash:index
```

Related Commands

Command	Description
ivr prompt memory	Configures the maximum amount of memory that the dynamic audio files (prompts) occupy in memory.

ivr autoload 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 autoload retry** command in global configuration mode. To disable this function, use the **no** form of this command.

ivr autoload retry *number*

no ivr autoload retry *number*

Syntax Description

<i>number</i>	Number from 1 to 5. The default value is 3.

Defaults

Three times

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco 2600 and 3600 series routers and on the Cisco AS5300 universal access server.

Examples

The following example configures the system to try three times to load audio files:

```
ivr autoload retry 3
```

Related Commands

Command	Description
ivr prompt memory	Configures the maximum amount of memory that the dynamic audio files (prompts) occupy in memory.

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

verbose	Displays the file transfer activity to the console. This mode is recommended while debugging.
url	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.
retry	(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.
silent	Performs the file transfer in silent mode, meaning that no file transfer activity is displayed to the console.

Defaults

Silent mode

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco 2600 and 3600 series routers and on the Cisco AS5300 universal access server.

Usage Guidelines

The index file contains a list of audio files (URL) that can be downloaded from the TFTP server. Use the **ivr autoload** command to download audio files from TFTP to memory. The command only starts up a background process. The background process (loader) does the actual downloading of the files.

The background process first reads the index file from either Flash or TFTP. It parses the files line by line looking for the URL. It ignores lines that start with # as comment lines. Once it has a correct URL, it tries to read that.au file into memory and creates a media object. If there are any errors during the reading of the file, it retries the configured number of times. If the mode is set to **verbose**, the loader logs the transaction to console. Once parsing has reached the end of the index file, the background process exits memory.

Perform the following checks before initiating the background process. If one of the checks fails, it indicates the background process is not started, and instead you will see an error response to the command.

- Check if any prompt is being actively used (IVR is actively playing some prompts). If there are active prompts, the command fails, displaying the following error message (.au files are also referred to as prompts):
command is not allowed when prompts are active
- Check if there is already a background process in progress. If there is a process, the command fails, displaying the following error:
previous autoload command is still in progress
- Check if an earlier **ivr autoload** command has already been configured. If an **ivr autoload** command has already been configured, the user sees the following response when the command is issued:
previous command is being replaced
- When the **no ivr autoload** command is issued, if there was already an **ivr autoload** command in progress, it will be aborted.

The audio files (prompts) loaded using the **ivr autoload** command are not dynamically swapped out of memory. They are considered as autoloaded prompts as opposed to “dynamic” prompts. (See the **ivr prompt memory** command for details on dynamic prompts.)

Examples

The following example configures verbose mode:

```
ivr autoload mode verbose url tftp://jurai/mgindi/tclware/index4 retry 3
```

The index file for the example index4 is shown as follows:

```
more index4
tftp://jurai/mgindi/tclware/au/en/en_one.au
tftp://jurai/mgindi/tclware/au/ch/ch_one.au
tftp://jurai/mgindi/tclware/au/ch/ch_one.au
```

The following is an example of index file on Flash:

```
flash:index
```

Related Commands

Command	Description
ivr prompt memory	Configures the maximum amount of memory that the dynamic audio files (prompts) occupy in memory.

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.
	files <i>number</i>	Specifies the number of files that can stay in memory. Valid entries for the number argument are 50 to 1000.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced on the Cisco 2600 and 3600 series routers and on the Cisco AS5300 universal access server.

Usage Guidelines	When both the <i>number</i> and <i>size</i> parameters are specified, the minimum memory out of the two will be used for memory calculations.
	All the prompts that are not autoloaded or fixed are considered dynamic. Dynamic prompts are loaded in to memory from TFTP or Flash, as and when they are needed. When they are actively used for playing prompts, they are considered to be in “active” state. However, once the prompt playing is complete, these prompts are no longer active and are considered to be in “free” state.
	The free prompts either stay in memory or are removed from memory depending on the availability of space in memory for these free prompts. The prompt-mem command essentially specifies a maximum memory to be used for these free prompts.
	The free prompts are saved in memory and are queued in a waitQ. When the waitQ is full (either because the totally memory occupied by the free prompts exceeds the maximum configured value or the number of files in the waitQ exceeds maximum configured), oldest free prompts are removed from memory.

Examples	The following example shows how to use the ivr prompt memory command:
	<pre>ivr prompt memory 2048 files 500</pre>

Related Commands	Command	Description
	ivr autoloading	Loads files from a particular TFTP server.
	show call	Displays the memory site use by prompts.
	prompt-mem-usage	

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.

Defaults

The BRI port does not supply line power.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(4)T	This command was integrated into the Cisco IOS Release 12.0(4)T.
12.1(3)XI	This command was added for the Cisco 2600 and Cisco 3600 series router.

Usage Guidelines

This command is supported only if an installed BRI voice module (BVM) or BRI VIC is equipped to supply line power (phantom power).

This command is used only on a BRI port that is operating in NT mode. A BRI port that is operating in TE mode is automatically disabled as a source of line power, and the **line-power** command is rejected.

When you use the **line-power** command, the line power provision is activated on a BRI port if the port is equipped with the hardware to supply line power. When you enter the **no line-power** command, the line power provision is deactivated on a BRI port.

Examples

The following example configures a BRI port to supply power to an attached TE device:

```
interface bri 1
 line-power
```

line-termination

To set the line termination on an E1 controller, use the **line-termination** command in controller configuration mode. To restore the default value, use the **no** form of this command.

line-termination { 75-ohm | 120-ohm }

no line-termination

Syntax Description

75-ohm	Matches the balanced BNC 75-ohm interface.
120-ohm	Matches the unbalanced twisted-pair 120-ohm interface.

Defaults

The default value is 120-ohm.

Command Modes

Controller configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

This command applies to E1 controllers only.

Examples

The following example shows how to set controller E1 0/0 to a line-termination of 75-ohm:

```
controller e1 0/0
 line-termination 75-ohm
```

link (RLM)

To enable a Redundant Link Manager (RLM) link, use the **link** command in RLM configuration mode. To disable this function, use the **no** form of this command.

link {*hostname name* | *address ip-address*} **source** *loopback-source* **weight** *factor*

no link {*hostname name* | *address ip-address*} **source** *loopback-source* **weight** *factor*

Syntax Description		
hostname <i>name</i>		RLM host name. If host name is used, RLM will look up the DNS server periodically for the host name configured until lookup is successful or the configuration is removed.
address <i>ip-address</i>		IP address of the link.
source <i>loopback-source</i>		Loopback interface source. We recommend you use the loopback interface as the source, so that it is independent of the hardware condition. Also, the source interface should be different in every link to avoid falling back to the same routing path. If you intend to use the same routing path for the failover, a single link is sufficient to implement it.
weight <i>factor</i>		An arbitrary number that sets link preference. The higher the weighting factor number assigned, the higher priority it gets to become the active link. If all entries have the same weighting factor assigned, all links will be treated equally. There is no preference among servers according to the assumption that only one server will accept the connection requests at any given time. Otherwise, preferences are extended across all servers.

Defaults	Disabled

Command Modes	RLM configuration

Command History	Release	Modification
	11.3(7)	This command was introduced.

Usage Guidelines	This command is a preference-weighted multiple entries command. Within the same server, the link preference is specified in weighting.

Examples	The following example specifies the RLM group (network access server), the device name, and the link addresses and their weighting preferences:

```
rlm group 1
server r1-server
  link address 10.1.4.1 source Loopback1 weight 4
  link address 10.1.4.2 source Loopback2 weight 3
```

Related Commands	Command	Description
	clear interface	Resets the hardware logic on an interface.
	clear rlm group	Clears all RLM group time stamps to zero.
	interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
	protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
	retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
	server (RLM)	Defines the IP addresses of the server.
	show rlm group statistics	Displays the network latency of the RLM group.
	show rlm group status	Displays the status of the RLM group.
	show rlm group timer	Displays the current RLM group timer values.
	shutdown (RLM)	Shuts down all of the links under the RLM group.
	timer	Overwrites the default setting of timeout values.

protocol rlm port

To configure the RLM port number, use the **protocol rlm port** RLM configuration command. To disable this function, use the **no** form of this command.

protocol rlm port *port-number*

no protocol rlm port *port-number*

Syntax Description	<i>port-number</i>	RLM port number. See Table 87 for the port number choices.

Defaults	3000

Command Modes	RLM configuration

Command History	Release	Modification
	11.3(7)	This command was introduced.

Usage Guidelines	The port number for the basic RLM connection can be reconfigured for the entire RLM group. Table 87 lists the default RLM port numbers.

Table 25 *Default RLM Port Number*

Protocol	Port Number
RLM	3000
ISDN	Port[RLM]+1

Related Commands	Command	Description
	clear interface	Resets the hardware logic on an interface.
	clear rlm group	Clears all RLM group time stamps to zero.
	interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
	link (RLM)	Specifies the link preference.
	retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
	server (RLM)	Defines the IP addresses of the server.
	show rlm group statistics	Displays the network latency of the RLM group.
	show rlm group status	Displays the status of the RLM group.
	show rlm group timer	Displays the current RLM group timer values.
	shutdown (RLM)	Shuts down all of the links under the RLM group.
	timer	Overwrites the default setting of timeout values.

loopback

To set the loopback method for testing a T1 or E1 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

diagnostic	Loops the outgoing transmit signal back to the receive signal.
local	Places the interface into local loopback mode.
payload	Places the interface into external loopback mode at the payload level.
line	Places the interface into external loopback mode at the line level.
remote	Keeps the local end of the connection in remote loopback mode.
v54 channel-group	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.
iboc	Sends an in band bit oriented code to the far end to cause it to go into line loopback.
esf	Specifies Extended Super Frame (ESF) as the T1 or E1 frame type. Only available under T1 or E1 controllers when ESF is configured on the controller. The following are keywords: • payload—Activates remote payload loopback by sending Facility Data Link (FDL) code. FDL is a 4-kbps out-of-band signaling channel in ESF. • line—Activates remote line loopback by sending FDL code.

Defaults

No loopback is configured.

Command Modes

Controller configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced as a controller configuration command for the Cisco MC3810 multiservice concentrator.
12.0(5)T and 12.0(5)XK	The command was introduced as an ATM interface configuration command for the Cisco 2600 and 3600 series router.
12.0(5)XE	The command was introduced as an ATM interface configuration command for the Cisco 7200 and 7500 series.

Release	Modification
12.0(5)XK and 12.0(7)T	The command was introduced as a controller configuration command for the Cisco 2600 and 3600 series router.
12.1(1)T	The command was modified as a controller configuration command for the Cisco 2600 series.

Usage Guidelines

You can use a loopback test on lines to detect and distinguish equipment malfunctions caused either by the line and channel service unit/digital service unit (CSU/DSU) or by the interface. If correct data transmission is not possible when an interface is in loopback mode, the interface is the source of the problem.

Examples

The following example shows how to set the diagnostic loopback method on controller T1 0/0:

```
controller t1 0/0
  loopback diagnostic
```

The following example shows how to set the payload loopback method on controller E1 0/0:

```
controller e1 0/0
  loopback local payload
```


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.

Defaults

Loop detection is disabled.

Command Modes

Controller configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

This command applies to Voice over Frame Relay and Voice over ATM on the Cisco MC3810 multiservice concentrator.

Examples

The following example configures loop detection for controller T1 0:

```
controller t1 0
 loop-detect
```

Related Commands

Command	Description
loopback (interface)	Diagnoses equipment malfunctions between an interface and a device.

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

plan1	FXO: A-D gain = 0 dB, D-A gain = 0 dB. FXS: A-D gain = -3 dB, D-A gain = -3 dB.
plan2	FXO: A-D gain = 3 dB, D-A gain = 0 dB. FXS: A-D gain = 0 dB, D-A gain = -3 dB.
plan3	FXO: A-D gain = -3 dB, D-A gain = 0 dB. FXS: Not applicable.
plan4	FXO: A-D gain = -3 dB, D-A gain = -3 dB. FXS: Not applicable.
plan5	FXO: Not applicable. FXS: A-D gain = -3 dB, D-A gain = -10 dB.
plan6	FXO: Not applicable. FXS: A-D gain = 0 dB, D-A gain = -7 dB.
plan7	FXO: A-D gain = 7 dB, D-A gain = 0 dB. FXS: A-D gain = 0 dB, D-A gain = -6 dB.
plan8	FXO: A-D gain = 5 dB, D-A gain = -2 dB. FXS: Not applicable.
plan9	FXO: A-D gain = 6 dB, D-A gain = 0 dB. FXS: Not applicable.

Defaults

FXO: A-D gain = 0 dB, D-A gain = 0 dB (loss plan 1)
FXS: A-D gain = -3 dB, D-A gain = -3 dB (loss plan 1)

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	The following additional signal level choices were added: plan 3, plan 4, plan 8, and plan 9.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The **loss-plan** command sets the analog signal level difference (offset) between the analog voice port and the digital signal processor (DSP). Each loss plan specifies a level offset in both directions—from the analog voice port to the DSP (A-D) and from the DSP to the analog voice port (D-A).

Use this command to obtain the required levels of analog voice signals to and from the DSP.

The **loss-plan** command is supported only on Cisco MC3810 multiservice concentrators, on FXO and FXS analog voice ports.

Examples

The following example configures FXO voice port 1/6 for a –3 dB offset from the voice port to the DSP and for a 0 dB offset from the DSP to the voice port:

```
voice-port 1/6
 loss-plan plan3
```

The following example configures FXS voice port 1/1 for a 0 dB offset from the voice port to the DSP and for a –7 dB offset from the DSP to the voice port:

```
voice-port 1/1
 loss-plan plan6
```

Related Commands

Command	Description
impedance	Specifies the terminating impedance of a voice port interface.
input gain	Specifies the gain applied by a voice port to the input signal from the PBX or other customer premises equipment.
output attenuation	Specifies the attenuation applied by a voice port to the output signal toward the PBX or other customer premises equipment.

lrq 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 **lrq forward-queries** command in gatekeeper configuration mode. To disable this function, use the **no** form of this command.

lrq forward-queries

no lrq forward-queries

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 2500, 3600 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

LRQ forwarding is dependent on a Cisco nonstandard field that first appeared in Cisco IOS Release 12.0(3)T. This means that any LRQ received from a non-Cisco gatekeeper or any gatekeeper running a Cisco IOS software image prior to Cisco IOS Release 12.0(3)T will not be forwarded.

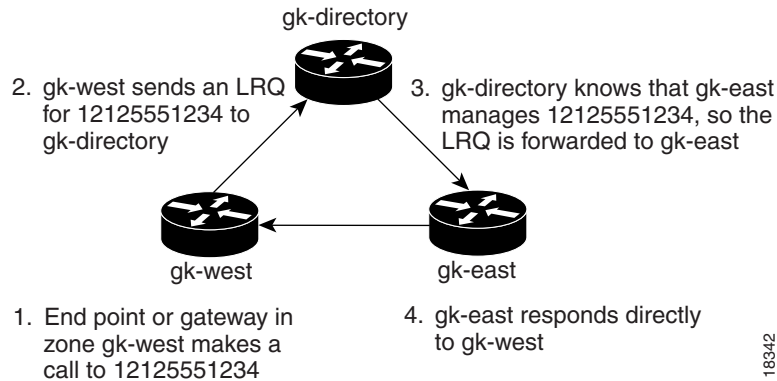
The routing of E.164-addressed calls is dependent on the configuration of zone prefix tables (for example, area code definitions) on each gatekeeper. Each gatekeeper is configured with a list of prefixes controlled by itself and by other remote gatekeepers. Calls are routed to the zone that manages the matching prefix. Thus, in the absence of a directory service for such prefix tables, you, the network administrator, may have to define extensive lists of prefixes on all the gatekeepers in your administrative domain.

To simplify this task, you can select one of your gatekeepers as the “directory” gatekeeper and configure that gatekeeper with the complete list of prefixes and the **lrq forward-queries** command. You can then simply configure all the other gatekeepers with their own prefixes and the wildcard prefix “*” for your directory gatekeeper.

This command affects only the forwarding of LRQs for E.164 addresses. LRQs for H.323-ID addresses are never forwarded.

Examples

The following example shows how this command is used to simplify configuration by selecting one gatekeeper as the directory gatekeeper. Refer to [Figure 5](#).

Figure 5 Example Scenario with Directory Gatekeeper and Two Remote Gatekeepers**Configuration on gk-directory**

On the directory gatekeeper called gk-directory, identify all the prefixes for all the gatekeepers in your administrative domain:

```
zone local gk-directory cisco.com
zone remote gk-west cisco.com 172.16.1.1
zone remote gk-east cisco.com 172.16.2.1

zone prefix gk-west 1408.....
zone prefix gk-west 1415.....
zone prefix gk-west 1213.....
zone prefix gk-west 1650.....

zone prefix gk-east 1212.....
zone prefix gk-east 1617.....

lrq forward-queries
```

Configuration on gk-west

On the gatekeeper called gk-west, configure all the locally managed prefixes for that gatekeeper:

```
zone local gk-west cisco.com
zone remote gk-directory cisco.com 172.16.2.3

zone prefix gk-west 1408.....
zone prefix gk-west 1415.....
zone prefix gk-west 1213.....
zone prefix gk-west 1650.....
zone prefix gk-directory *
```

Configuration on gk-east

On the gatekeeper called gk-east, configure all the locally managed prefixes for that gatekeeper:

```
zone local gk-east cisco.com
zone remote gk-directory cisco.com 172.16.2.3

zone prefix gk-east 1212.....
zone prefix gk-east 1617.....
zone prefix gk-directory *
```

Now when an endpoint or gateway in zone gk-west makes a call to 12125551234, gk-west will send an LRQ for that E.164 address to gk-directory, which forwards the LRQ to gk-east. Gatekeeper gk-east responds directly to gk-west.

Related Commands

Command	Description
lrq reject-unknown-prefix	Enables the gatekeeper to reject all LRQs for zone prefixes that are not configured.

lrq reject-unknown-prefix

To enable the gatekeeper to reject all Location Requests (LRQs) for zone prefixes that are not configured, use the **lrq reject-unknown-prefix** command in gatekeeper configuration mode. To reenable the gatekeeper to accept and process all incoming LRQs, use the **no** form of this command.

lrq reject-unknown-prefix

no lrq reject-unknown-prefix

Syntax Description

This command has no arguments or keywords.

Defaults

The gatekeeper accepts and processes all incoming LRQs.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the Cisco 2500 and 3600 series routers.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

Use the **lrq reject-unknown-prefix** command to configure the gatekeeper to reject any incoming LRQs for a destination E.164 address that does not match any of the configured zone prefixes.

Whether or not you enable the **lrq reject-unknown-prefix** command, the following is true when the E.164 address matches a zone prefix:

- If the matching zone prefix is local (that is, controlled by this gatekeeper), the LRQ is serviced.
- If the matching zone prefix is remote (that is, controlled by some other gatekeeper), the LRQ is rejected.

If you do not enable the **lrq reject-unknown-prefix** command and the target address does not match any known local or remote prefix, the default behavior is to attempt to service the call using one of the local zones. If this default behavior is not suitable for your site, configure the **lrq reject-unknown-prefix** command on your router to force the gatekeeper to reject such requests.

Examples

Consider the following gatekeeper configuration:

```
zone local gk408 cisco.com
zone local gk415 cisco.com
zone prefix gk408 1408.....
zone prefix gk415 1415.....
lrq reject-unknown-prefix
```

lrq reject-unknown-prefix

In this sample configuration, the gatekeeper is configured to manage two zones. One zone contains gateways with interfaces in the 408 area code, and the second zone contains gateways in the 415 area code. Then using the **zone prefix** command, the gatekeeper is configured with the appropriate prefixes so that calls to those area codes hop off in the optimal zone.

Now say some other zone has been erroneously configured to route calls to the 212 area code to this gatekeeper. When the LRQ for a number in the 212 area code arrives at this gatekeeper, the gatekeeper fails to match the area code, and the LRQ is rejected.

If this was your only site that had any gateways in it and you wanted your other sites to route all calls that require gateways to this gatekeeper, you can undo the **lrq reject-unknown-prefix** command by simply using the **no lrq reject-unknown-prefix** command. Now when the gatekeeper receives an LRQ for the address 12125551234, it will attempt to find an appropriate gateway in either one of the zones gk408 or gk415 to service the call.

Related Commands

Command	Description
lrq forward-queries	Enables a gatekeeper to forward LRQs that contain E.164 addresses that match zone prefixes controlled by remote gatekeepers.

lrq timeout blast window

To configure the timeout window for use when sending multiple Location Requests (LRQs) (either sequentially or simultaneously), use the **lrq timeout blast window** command in gatekeeper configuration mode. To return to the default value, use the **no** form of this command.

lrq timeout blast window *seconds*

no lrq timeout blast window

Syntax Description	<i>seconds</i>	The duration of the window, in seconds. Possible values are 1 through 10. The default is 6.

Defaults	By default, the duration of the window is 6 seconds.

Command Modes	Gatekeeper configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced on the Cisco 2500, 2600, 3600, and 7200 series routers and on the Cisco MC3810 multiservice concentrator.

Examples	The following example sets the window to 3 seconds: <pre>lrq timeout blast window 3</pre>

Related Commands	Command	Description
	gatekeeper gw-type-prefix	Sets the gatekeepers responsible for each technology prefix.
	zone prefix	Adds a prefix to a gatekeeper's zone list.

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	<i>value</i>	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).

Defaults	By default, the duration of the window is five 100 millisecond units (500 ms or 0.5 seconds)

Command Modes	Gatekeeper configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced on the Cisco 2500, 2600, 3600, and 7200 series routers, and on the Cisco MC3810 multiservice concentrator.

Examples	The following example sets the window to 300 milliseconds: lrq timeout seq delay 3

Related Commands	Command	Description
	gatekeeper gw-type-prefix	Sets the gatekeepers responsible for each technology prefix.
	zone prefix	Adds a prefix to a gatekeeper's zone list.

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

<i>number</i>	Specifies the maximum number of connections for this dial peer. Valid values for this field are 1 to 2,147,483,647.

Defaults

The **no** form of this command is the default, meaning an unlimited number of connections.

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series router.
12.0(4)XJ	This command was modified for store and forward fax on the Cisco AS5300 universal access server.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

This command applies to both VoIP and POTS dial peers. Use the **max-conn** command to define the maximum number of connections used simultaneously on the Cisco AS5300 universal access server to send fax-mail.

This command applies to off-ramp store and forward fax functions.

Examples

The following example configures the maximum number of connections for VoIP dial peer 10 as 5:

```
dial-peer voice 10 voip
max-conn 5
```

Related Commands

Command	Description
mta receive maximum-recipients	Specifies the maximum recipients for all SMTP connections.

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

<i>number</i>	Specifies the maximum number of HTTP connections to a settlement provider.

Defaults

The default is 10 connections.

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 and Cisco 3600 series routers and on the Cisco AS5300 universal access server.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples

The following command sets the maximum number of simultaneous connections to 10:

```
settlement 0
max-connection 10
```

Related Commands

Command	Description
connection-timeout	Configures the time that a connection is maintained after completing a communication exchange.
customer-id	Sets the customer identification.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
response-timeout	Configures the maximum time to wait for a response from a server.
retry-delay	Sets the time between attempts to connect with the settlement provider.
retry-limit	Sets the maximum number of connection attempts to the provider.
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.

Command	Description
shutdown	Brings up the settlement provider.
type	Configures an SAA-RTR operation type.
url	Configures the ISP address.

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

Syntax Description	<i>number</i>	Number of hops. Possible values are 1 through 15. The default is 6.

Defaults	The default number of hops is 6.

Command Modes	SIP user agent configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 and Cisco 3600 series routers and on the Cisco AS5300 universal access server.

Usage Guidelines	To reset this command to the default value, you can also use the default command.

Examples	The following is an example of forwarding requests to proxy or redirect servers:

```

sip-ua
max-forwards 2

```

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

Syntax Description	<i>number</i>	Maximum number of redirect servers that a call can traverse. Possible values are 1 through 10.

Defaults	The default number of redirects is 1.

Command Modes	Dial-peer configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced on the Cisco 2600 and Cisco 3600 series routers and on the Cisco AS5300 universal access server.

Examples	The following is an example of setting the maximum number of redirect servers that the user agent allows:

```
dial-peer voice 102 voip
max-redirects 2
```

Related Commands	Command	Description
	dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice-related encapsulation.

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

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Dial-peer configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access router.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines Message disposition notification is an e-mail message that is generated and sent to the sender when the message is opened by the receiver. Use the **mdn** command to request that an e-mail response message be sent to the sender when the e-mail that contains the fax TIFF image has been opened.

This command applies to on-ramp store and forward fax functions.

Examples The following example requests that a message disposition notice be generated by the recipient:

```
dial-peer voice 10 mmoip
mdn
```

Related Commands	Command	Description
	mta receive generate-mdn	Specifies that the off-ramp gateway process a response MDN from an SMTP server.
	mta send return-receipt-to	Specifies the address where MDNs are sent.

mgcp

To allocate resources for the media gateway control protocol (MGCP) and start the MGCP 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

Syntax Description

<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.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
12.1(3)T	Support for this command was extended to the Cisco 3660, Cisco uBR924, and Cisco 2600 series router router platforms.

Usage Guidelines

Once you start the MGCP daemon using the **mgcp** command, you can suspend it (for example, for maintenance) by using the **mgcp block-newcalls** command. When you are ready to resume normal MGCP operations, use the **no mgcp block-newcalls** command. Use the **no mgcp** command only if you intend to terminate all MGCP applications and protocols.

When the MGCP daemon is not active, all MGCP messages are ignored.

Examples

The following example shows how to initiate the MGCP daemon:

```
mgcp
```

Related Commands

Command	Description
debug mgcp	Enables debugging on MGCP.
mgcp ip-tos	Terminates all MGCP activity in an orderly manner.
mgcp request retries	Specifies the number of times to retry sending the mgcp command.

mgcp block-newcalls

To block new calls while maintaining existing calls, use the **mgcp block-newcalls** command in global configuration mode. To resume media gateway control protocol (MGCP) operation, use the **no** form of this command.

mgcp block-newcalls

no mgcp block-newcalls

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
	12.1(3)T	Support for this command was extended to the Cisco 3660, Cisco uBR924, and Cisco 2600 series router router platforms.

Usage Guidelines This command is valid only if the **mgcp** command is enabled.

Once you issue this command, all requests for new connections (CreateConnection requests) are denied. All existing calls will be maintained until participants terminate them or you use the **no mgcp** command. When the last active call is terminated, the MGCP daemon will be terminated and all resources allocated to it will be released. The **no mgcp block-newcalls** command returns the router to normal MGCP operations.

Examples The following example shows how to prevent the gateway from receiving new calls:

```
mgcp block-newcalls
```

Related Commands	Command	Description
	mgcp	Allocates resources for the MGCP and starts the daemon.

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

Syntax Description

<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 User Datagram Protocol (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.
service-type <i>type</i>	(Optional) Specifies the type of gateway control service to be supported by the call agent. Valid values are mgcp and sgcp .

Defaults

MGCP service-type

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
12.1(3)T	The service-type <i>type</i> option was added.

Usage Guidelines

Use this command on any platform and media gateway.

If you do not specify a UDP port from the command line, media gateway control protocol (MGCP) will use 2427 as the default call agent UDP port.

When **service-type** is set to **mgcp**, the call agent processes the Restart in Progress (RSIP) error messages sent by the gateway. When **service-type** is set to **sgcp**, the call agent ignores the RSIP messages.

Examples

The following examples illustrate several formats for specifying the call agent (use any one of these formats):

```
mgcp call-agent 209.165.200.225 service-type sgcp
mgcp call-agent 209.165.200.225 5530 service-type mgcp
mgcp call-agent igloo service-type sgcp
mgcp call-agent igloo 2009 service-type mgcp
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

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

Syntax Description	<i>type</i>	Specifies the types of codec supported. Valid codecs are G711alaw, G711ulaw, G723ar53, G723ar63, G723r53, G723r63, G729ar8, G729br8, and G729r8.
	packetization-period <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.

Defaults G711ulaw

Command Modes Global configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
	12.1(3)T	Support for this command was extended to the Cisco 3660, Cisco uBR924, and Cisco 2600 series router router platforms.

Examples This example shows how to specify the default codec type:

```
mgcp codec g711alaw
```

The following example specifies the codec type and sets the packetization period:

```
mgcp codec g729r8 packetization-period 150
```

Related Commands	Command	Description
	mgcp	Starts the MGCP daemon.

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}

Syntax Description

as-package	Announcement server package.
dtmf-package	DTMF package.
gm-package	Generic media package.
line-package	Line package.
rtp-package	RTP package.
trunk-package	Trunk package.

Defaults

For residential gateways (RGWs): **line-package**
For trunking gateways (TGWs): **trunk-package**

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
12.1(3)T	The line-package keyword and a distinction between residential and trunking gateways were added.

Usage Guidelines

This command is helpful when the Media Gateway Controller does not provide the package capability to be used for the given connection.

Before selecting a package as the default, use the **show mgcp** command to ensure that the package is actively supported. If the package you want does not appear in the display, use the **mgcp package-capability** command to add the package to the supported list.

If only one package is actively supported, it becomes the default package.

mgcp default-package**Examples**

The following example shows how to set the default package:

```
mgcp default-package as-package
! The announcement server package type will be the new default package type.
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp package-capability	Includes a specific MGCP package that is supported by the gateway.

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

Syntax Description

codec	Specifies use of either a G.711 or a G.726 codec.
low-bit-rate	Specifies a low-bit-rate codec other than G.711 and G.726.
mode	Specifies the mode.
cisco	This mode removes the DTMF tone from the voice stream and sends FRF.11 with a special payload 121 for the DTMF digits.
out-of-band	This mode removes the DTMF tone from the voice stream and does not send FRF.11.

Defaults

Non compressed codecs are disabled.

Command Modes

Controller configuration

Command History

Release	Modification
12.1(3)T	This command was first supported by media gateway control protocol (MGCP) on the Cisco 2600 and Cisco 3600 series routers, the Cisco AS5300 universal access server, and the Cisco uBR924 cable access router.

Usage Guidelines

Use this command to access an announcement server or a voice mail server that does not have the capability to decode RTP packets containing DTMF digits. When the **mgcp dtmf-relay** command is active, the DTMF digits are removed from the voice stream and carried by FRF.11 so that the server can decode the digits.

Examples

The following example shows how to remove the DTMF tone from the voice stream and send FRF.11 with a special payload for the DTMF digits:

```
mgcp dtmf-relay codec mode cisco
```

Related Commands

Command	Description
mgcp	Allocates resources of the MGCP and starts the daemon.

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

high-reliability	Specifies high-reliability ToS.
high-throughput	Specifies high-throughput ToS.
low-cost	Specifies low-cost ToS.
low-delay	Specifies low-delay ToS.
precedence <i>value</i>	Specifies the value of the IP precedence bit. Valid values are from 0 to 7. The default IP precedence value is 3.

Defaults

Services disabled; precedence is 3.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
12.1(3)T	Support for this command was extended to the Cisco 3660, Cisco uBR924, and Cisco 2600 series router router platforms.

Usage Guidelines

Only one of the high-reliability, high-throughput, low-cost, or low-delay parameters can be enabled at any given time. Enabling one parameter disables any other that was active. Enabling one parameter has no effect on the precedence parameter. When you configure a new value for the precedence parameter, the old value is erased.

The **no** form of the **mgcp ip-tos** command disables the first four parameters and sets the precedence parameter back to 3.

Examples

In the following example, activating the **low-delay** keyword disables the other three parameters.

```
mgcp ip-tos high-reliability
mgcp ip-tos high-throughput
mgcp ip-tos low-cost
mgcp ip-tos low-delay
mgcp ip-tos precedence 4
```


Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp max-waiting-delay

To specify the media gateway control protocol (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).	
Defaults	3000 milliseconds	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
	12.1(3)T	Support for this command was extended to the Cisco 3660, Cisco uBR924, and Cisco 2600 series router platforms.
Usage Guidelines	Use the maximum waiting delay to send out an RSIP message to the call agent with the restart method. This command helps prevent traffic bottlenecks caused by MGCP gateways all trying to connect at the same time after a restart.	
Examples	The following example shows how to set the MGCP maximum waiting delay to 600 milliseconds: <pre>mgcp max-waiting-delay 600</pre>	
Related Commands	Command	Description
	mgcp	Starts the MGCP daemon.
	mgcp restart-delay	Configures the graceful tear down method sent in the RSIP message.

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

Syntax Description	cisco	When the gateway detects a modem/fax tone, the gateway switches the codec to G.711 to allow the analog data to pass through.
	ca	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.

Defaults	ca

Command Modes	Controller configuration

Command History	Release	Modification
	12.1(3)T	This command was added to MGCP.

Usage Guidelines	When the cisco keyword is activated and the gateway detects a modem/fax tone, the gateway switches the codec to G.711 then sends the analog data to a remote gateway. The remote gateway also switches the codec on its side of the call to G.711 to allow the analog data to pass through.
	When the ca keyword is activated and 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. The call agent must send an MDCX signal to the G.711 codec for successful data pass-through.

Examples	The following example configures a gateway to send and receive modem or fax data:
	<pre>mgcp modem passthru cisco</pre>

Related Commands	Command	Description
	mgcp	Starts the MGCP daemon.

mgcp package-capability

To specify a media gateway control protocol (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}
```

Syntax Description

line-package	Line package.
trunk-package	Trunk package.
dtmf-package	DTMF package.
gm-package	Generic media package.
rtp-package	RTP package.
as-package	Announcement server package.
script-package	Script package.

Defaults

For all residential gateways (RGWs): **line-package**

For all trunking gateways (TGWs): **trunk-package**

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
12.1(3)T	The command was expanded to the Cisco uBR924, Cisco 2600 series router router, and Cisco 3660 platforms. The line-package , rtp-package , and script-package keywords were added.

Usage Guidelines

Select packages that are supported by your call agent. Events specified in the MGCP messages from the call agent must belong to one of the supported packages. Otherwise, the connection requests are refused by the media gateway.

Use this command before specifying a default package using the **mgcp default-package** command. Specify at least one package to have a default.

Enter each package as a separate command.

Examples

The following example shows how to specify an MGCP package capability for a gateway:

```
mgcp package-capability trunk-package
mgcp package-capability dtmf-package
mgcp package-capability script-package
mgcp default-package trunk-package
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp default-package	Configures the default package capability type for the media gateway.

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

adaptive <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> .
fixed <i>init-value</i>	Specifies a fixed size (in milliseconds) for the jitter buffer packet size. Valid values are from 4 to 250.

Defaults

adaptive 60 4 200
No default for **fixed**.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
12.1(3)T	Support for this command was extended to the Cisco 3660, Cisco uBR924, and Cisco 2600 series router router platforms.

Examples

The following example illustrates a jitter buffer configuration with an initial playout of 100, a minimum buffer size of 50, and a maximum buffer size of 150:

```
mgcp playout adaptive 100 50 150
```

The following example illustrates setting the jitter buffer to a fixed playout of 120:

```
mgcp playout fixed 120
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

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

hwm-jitter-buffer <i>value</i>	Specifies the high-water-mark jitter buffer size. Valid range is from 100 to 200 the default value is 150 milliseconds.
hwm-latency <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.
hwm-packet-loss <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.
lwm-jitter-buffer <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.
lwm-latency <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.
lwm-packet-loss <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.

Defaults

The voice quality parameter defaults are (in milliseconds): **hwm-jitter-buffer** 150, **hwm-latency** 300, **hwm-packet-loss** 10,000, **lwm-jitter-buffer** 30, **lwm-latency** 150, and **lwm-packet-loss** 1000.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
12.1(3)T	Support for this command was extended to the Cisco 3660, Cisco uBR924, and Cisco 2600 series router router platforms.

Usage Guidelines

The following parameters impact the quality of voice calls:

- Jitter buffer (storage area containing active call voice packets that have been received from the network and are waiting to be decoded and played)
- Latency (network delay in sending/receiving packets)
- Packet loss (number of packets lost per 100,000 packets for a given call)

For good voice quality, the system should perform below the **lwm** values. As the values go higher, voice quality degrades. The system generates a report when the values go above the **hwm** levels. Set the **hwm** and **lwm** values sufficiently apart so that you receive reports on poor performance, but not so close together that you receive too much feedback.

Enter each parameter as a separate command.

Examples

The following example shows how the different parameters can be set to new values:

```
mgcp quality-threshold hwm-jitter-buffer 100
mgcp quality-threshold hwm-latency 250
mgcp quality-threshold hwm-packet-loss 5000
mgcp quality-threshold lwm-jitter-buffer 50
mgcp quality-threshold lwm-latency 200
mgcp quality-threshold lwm-packet-loss 20
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp playout	Tunes the jitter buffer packet size.

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

Syntax	Description
<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.

Defaults	Three times

Command Modes	Global configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
	12.1(3)T	Support for this command was extended to the Cisco 3660, Cisco uBR924, and Cisco 2600 series router router platforms.

Usage Guidelines	This command applies to a trunking gateway.

Examples	The following example shows that the system will try to send the mgcp command 10 times before dropping the request: mgcp request retries 10

Related Commands	Command	Description
	mgcp	Starts the MGCP daemon.
	mgcp request timeout	Specifies how long the system waits for a response to a request.

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

Syntax Description	<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).

Defaults	500 milliseconds

Command Modes	Global configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
	12.1(3)T	Support for this command was extended to the Cisco 3660, Cisco uBR924, and Cisco 2600 series router router platforms.

Examples	The following example configures the system to wait 40 milliseconds for a reply to a request:
	<code>mgcp request timeout 40</code>

Related Commands	Command	Description
	mgcp	Starts the MGCP daemon.
	mgcp request retries	Specifies the number of times to retry sending the mgcp command.

mgcp restart-delay

To select the delay value sent in the Restart in Progress (RSIP) graceful tear down, 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

Syntax Description	<i>seconds</i>	Specifies the restart delay value in seconds. The valid range is from 0 to 600.

Defaults	Zero (0) seconds

Command Modes	Global configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
	12.1(3)T	Support for this command was extended to the Cisco 3660, Cisco uBR924, and Cisco 2600 series router router platforms.

Usage Guidelines	Use the restart value to send a RSIP message that indicates when the connection in the gateway will be torn down.

Examples	The following example sets the restart delay to 30 seconds: mgcp restart-delay 30

Related Commands	Command	Description
	mgcp	Starts the MGCP daemon.
	mgcp max-waiting-delay	Specifies the MGCP MWD after a restart.

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.

Defaults

no mgcp sdp simple

Command Modes

Controller configuration

Command History

Release	Modification
12.1(3)T	This command was added to the media gateway control protocol (MGCP).

Usage Guidelines

When the **mgcp sdp simple** command is enabled, the gateway will not generate three SDP fields: time, session name, and other (username, session id, sdp version, network type, address type, or address). Certain call agents require this modified SDP protocol to send data through the network.

Examples

The following example configures the modified SDP protocol:

```
mgcp sdp simple
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp vad

To set the default VAD parameter for the media gateway control protocol (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.

Defaults	Disabled

Command Modes	Global configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
	12.1(3)T	Support for this command was extended to the Cisco 3660, Cisco uBR924, and Cisco 2600 series router router platforms.

Usage Guidelines	Use the MGCP VAD parameter to tell the MGCP gateway to turn silence suppression on or off.

Examples	The following example turns silence suppression on: mgcp vad

Related Commands	Command	Description
	mgcp	Starts the MGCP daemon.

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}

Syntax Description

t1	Specifies T1.
e1	Specifies E1.
x/y	Controller slot and unit numbers.

Defaults

No microcode reload activity is initiated.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(2)XH	This command was introduced on the Cisco 2600 and Cisco 3600 series routers.

Usage Guidelines

Configurations such as channel groups, TDM connections, and loopbacks and so on in the running configuration are restored after this command is issued. If either of the controller ports on the WIC is in a looped state before this command is issued, the looped condition is dropped. You have to reinitiate the loopbacks from the remote end by doing “no loop” and “loop remote” from the controller configuration. If the BERT test is running, that test will be aborted for the microcode reload.

mmoip aaa global-password

To define a password to be used with CiscoSecure for Windows NT when using store and forward fax, use the **mmoip aaa global-password** command in global configuration mode. To restore the default state, use the **no** form of this command.

mmoip aaa global-password *password*

no mmoip aaa global-password *password*

Syntax Description

<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.

Defaults

No password is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

CiscoSecure for Windows NT might require a separate password in order to complete authentication, no matter what security protocol you use. This command defines the password to be used with CiscoSecure for Windows NT. All records on the Windows NT server use this defined password.

This command applies to on-ramp store and forward fax functions when using a modem card. It is not used with voice feature cards.

Examples

The following example defines a password (password) when CiscoSecure for Windows NT is used with store and forward fax:

```
mmoip aaa global-password password
```

mmoip aaa method fax accounting

To define the name of the method list to be used for authentication, authorization, and accounting (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*

Syntax Description

<i>method-list-name</i>	Character string used to name a list of accounting methods to be used with store and forward fax.

Defaults

No AAA accounting method list is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

This command defines the name of the AAA accounting method list to be used with store and forward fax. The method list itself, which defines the type of accounting services provided for store and forward fax, is defined using the **aaa accounting** global configuration command. Unlike standard AAA (where each defined method list can be applied to specific interfaces and lines), the AAA accounting method lists used in store and forward fax are applied globally on the Cisco AS5300 universal access server.

After the accounting method lists have been defined, they are enabled by using the **mmoip aaa receive-accounting enable** command.

This command applies to both on-ramp and off-ramp store and forward fax functions when using a modem card. It is not used with voice feature cards.

Examples

The following example defines a AAA accounting method list (called sherman) to be used with store and forward fax:

```
aaa new-model
mmoip aaa method fax accounting sherman
```


Related Commands	Command	Description
	aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
	mmoip aaa receive-accounting enable	Enables on-ramp store and forward fax AAA accounting services.

mmoip aaa method fax authentication

To define the name of the method list to be used for authentication, authorization, and accounting (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*

Syntax Description	<i>method-list-name</i>	Character string used to name a list of authentication methods to be used with store and forward fax.

Defaults	No AAA authentication method list is defined.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines	This command defines the name of the AAA authentication method list to be used with store and forward fax. The method list itself, which defines the type of authentication services provided for store and forward fax, is defined using the aaa authentication global configuration command. Unlike standard AAA (where each defined method list can be applied to specific interfaces and lines), AAA authentication method lists used with store and forward fax are applied globally on the Cisco AS5300 universal access server.

After the authentication method lists have been defined, they are enabled by using the **mmoip aaa receive-authentication enable** command.

This command applies to both on-ramp and off-ramp store and forward fax functions.

Examples	The following example defines a AAA authentication method list (called xyz) to be used with store and forward fax:

```
aaa new-model
mmoip aaa method fax authentication xyz
```

Related Commands	Command	Description
	aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
	mmoip aaa receive-authentication enable	Enables on-ramp store and forward fax AAA authentication services.

mmoip aaa receive-accounting enable

To enable on-ramp authentication, authorization, and accounting (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

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
12.1(1T)	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

This command enables AAA accounting services if a AAA accounting method list has been defined using both the **aaa accounting** command and the **mmoip aaa method fax accounting** command.

This command applies to on-ramp store and forward fax functions.

Examples

The following example enables a AAA accounting method list (called xyz) to be used with inbound store and forward fax. In this example, store and forward fax is being configured to track start and stop connection accounting records.

```
aaa new-model
mmoip aaa method fax accounting xyz
aaa accounting connection sherman stop-only radius
mmoip aaa receive-accounting enable
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa method fax accounting	Defines the name of the method list to be used for AAA accounting with store and forward fax.

mmoip aaa receive-authentication enable

To enable on-ramp authentication, authorization, and accounting (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.

Defaults	Disabled

Command Modes	Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines	This command enables AAA authentication services if an AAA authentication method list has been defined using both the aaa authentication command and the mmoip aaa method fax authentication command.

This command applies to on-ramp store and forward fax functions.

Examples	The following example enables a AAA authentication method list (called xyz) to be used with inbound store and forward fax. In this example, RADIUS authentication (and if the RADIUS server fails, then local authentication) is being configured for store and forward fax.

```
aaa new-model
mmoip aaa method fax authentication xyz
aaa authentication login peabody radius local
mmoip aaa receive-authentication enable
```

Related Commands	Command	Description
	aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
	mmoip aaa method fax authentication	Defines the name of the method list to be used for AAA authentication with store and forward fax.

mmoip aaa receive-id primary

To specify the primary location where the authentication, authorization, and accounting (AAA) protocol 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		
ani		Indicates that AAA uses the calling party telephone number (automatic number identification or ANI) as the AAA account identifier.
dnis		Indicates that AAA uses the called party telephone number (dialed number identification service or DNIS) as the AAA account identifier.
gateway		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> .
redialer-id		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.
redialer-dnis		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.

Defaults	No account identification source is defined.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store and forward fax, you can specify that the ANI, DNIS, gateway ID, redialer ID, or redialer DNIS be used to identify the user for authentication. This command defines what AAA uses for the primary identifier for inbound or on-ramp user authentication with store and forward fax.

Store and forward fax allows you to define either a primary or a secondary identifier. (You configure the secondary identifier using the **mmoip aaa receive-id secondary** command.)

AAA does not use these methods sequentially—meaning that if the primary identifier is defined and AAA cannot authenticate the primary identifier information, it will not use the secondary identifier for authentication. Authentication simply fails.

Defining only the secondary identifier enables you to service two different scenarios simultaneously—for example, if you are offering fax services to two different companies, one of which uses redialers and the other does not. In this case, configure the **mmoip aaa receive-id primary** command to use the redialer DNIS, and configure the **mmoip aaa receive-id secondary** command to use ANI. With this configuration, when a user dials in and the redialer DNIS is not null, the redialer DNIS is used as the authentication identifier. If a user dials in and the redialer DNIS is null, ANI is used as the authentication identifier.

This command applies to on-ramp store and forward fax functions.

Examples

The following example defines the DNIS captured by the redialer as the AAA authentication identifier for store and forward fax:

```
aaa new-model
mmoip aaa receive-id primary redialer-dnis
```

Related Commands

Command	Description
mmoip aaa receive-id secondary	Specifies the secondary location where AAA retrieves its account identification information for on-ramp faxing if the primary identifier has not been defined.

mmoip aaa receive-id secondary

To specify the secondary location where the authentication, authorization, and accounting (AAA) protocol 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		
ani		Indicates that AAA uses the calling party telephone number (automatic number identification or ANI) as the AAA account identifier.
dnis		Indicates that AAA uses the called party telephone number (dialed number identification service or DNIS) as the AAA account identifier.
gateway		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> .
redialer-id		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.
redialer-dnis		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.

Defaults	No account identification source is defined.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store and forward fax, you can specify that the ANI, DNIS, gateway ID, redialer DNIS, or redialer ID be used to identify the user for authentication. This command defines what AAA uses for the secondary identifier for inbound or on-ramp user authentication with store and forward fax if the primary identifier has not been defined.

Store and forward fax allows you to define either a primary or a secondary identifier. (You configure the primary identifier using the **mmoip aaa receive-id primary** command.)

AAA does not use these methods sequentially—meaning that if the primary identifier is defined and AAA cannot match the primary identifier information, it will not use the secondary identifier for authentication. Authentication simply fails.

Defining only the secondary identifier enables you to service two different scenarios simultaneously—for example, if you are offering fax services to two different companies, one of which uses redialers and the other does not. In this case, configure the **mmoip aaa receive-id primary** command to use the redialer DNIS, and configure the **mmoip aaa receive-id secondary** command to use ANI. With this configuration, when a user dials in and the redialer DNIS is not null, the redialer DNIS is used as the authentication identifier. If a user dials in and the redialer DNIS is null, ANI is used as the authentication identifier.

This command applies to on-ramp store and forward fax functions.

Examples

The following example defines the DNIS captured by the redialer as the secondary AAA authentication identifier for store and forward fax:

```
aaa new-model
mmoip aaa receive-id secondary redialer-dnis
```

Related Commands

Command	Description
mmoip aaa receive-id primary	Specifies the primary location where AAA retrieves its account identification information for on-ramp faxing.

mmoip aaa send-accounting enable

To enable off-ramp authentication, authorization, and accounting (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.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines This command enables AAA accounting services if an AAA accounting method list has been defined using both the **aaa accounting** command and the **mmoip aaa method fax accounting** command.

This command applies to off-ramp store and forward fax functions when using a modem card. It is not used with voice feature cards.

Examples The following example enables an AAA accounting method list (called xyz) to be used with outbound store and forward fax. In this example, store and forward fax is being configured to track start and stop connection accounting records.

```
aaa new-model
mmoip aaa method fax accounting xyz
aaa accounting connection sherman stop-only radius
mmoip aaa send-accounting enable
```

Related Commands	Command	Description
	aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
	mmoip aaa method fax accounting	Defines the name of the method list to be used for AAA accounting with store and forward fax.

mmoip aaa send-authentication enable

To enable off-ramp authentication, authorization, and accounting (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.

Defaults	Disabled

Command Modes	Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines	This command enables AAA authentication services if an AAA authentication method list has been defined using both the aaa authentication command and the mmoip aaa method fax authentication command.

This command applies to off-ramp store and forward fax functions.

Examples	The following example enables an AAA authentication method list (called xyz) to be used with outbound store and forward fax. In this example, RADIUS authentication (and if the RADIUS server fails, then local authentication) is being configured for store and forward fax.

```
aaa new-model
mmoip aaa method fax authentication xyz
aaa authentication login peabody radius local
mmoip aaa send-authentication enable
```

Related Commands	Command	Description
	aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
	mmoip aaa method fax authentication	Defines the name of the method list to be used for AAA authentication with store and forward fax.

mmoip aaa send-id primary

To specify the primary location where the authentication, authorization, and accounting (AAA) protocol 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

account-id	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.
envelope-from	Indicates that AAA uses the account username from the fax-mail header as the AAA account identifier.
envelope-to	Indicates that AAA uses the recipient derived from the fax-mail header as the AAA account identifier.
gateway	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> .

Defaults

No account identification source is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store and forward fax, you can specify that the account ID, username, or recipient name from the e-mail header information be used to identify the user for authentication. This command defines what AAA uses for the primary identifier for outbound or off-ramp user authentication with store and forward fax.

Store and forward fax allows you to define either a primary or a secondary identifier. (You configure the secondary identifier using the **mmoip aaa send-id secondary** command.) AAA extracts the authentication identifier information from the defined sources. If the field is blank (meaning undefined), AAA will use the secondary identifier source if configured. The secondary identifier is used only when the primary identifier is null. In this case, when AAA sees that the primary identifier is null, it will check to see if a secondary identifier has been defined and use that value for user authentication.

AAA does not use these methods sequentially—meaning that if the primary identifier is defined and AAA cannot authenticate the primary identifier information, it will not use the secondary identifier for authentication. Authentication simply fails.

When you enable authentication, the on-ramp gateway inserts whatever value you configure for the **mmoip aaa receive-id primary** command in the X-account ID field of the e-mail header. This X-account ID field contains the value that is used for authentication and accounting by the on-ramp gateway. For example, if the **mmoip aaa receive-id primary** command is set to **gateway**, the on-ramp gateway name (for example, hostname.domain-name) is inserted in the X-account ID field of the e-mail header of the fax-mail message.

If you want to use this configured gateway value in the X-account ID field, you must configure the **mmoip aaa send-id primary** command with the **account-id** keyword. This particular keyword enables store and forward fax to generate end-to-end authentication and accounting tracking records. If you do not enable authentication on the on-ramp gateway, the X-account ID field is left blank.

This command applies to off-ramp store and forward fax functions.

Examples

The following example defines the recipient name as defined in the envelope-to field of the e-mail header to be used as the AAA authentication identifier for store and forward fax:

```
aaa new-model
mmoip aaa send-id primary envelope-to
```

Related Commands

Command	Description
mmoip aaa send-id primary	Specifies the primary location where AAA retrieves its account identification information for off-ramp faxing.
mmoip aaa send-id secondary	Specifies the secondary location where AAA retrieves its account identification information for off-ramp faxing.

mmoip aaa send-id secondary

To specify the secondary location where the authentication, authorization, and accounting (AAA) protocol 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		
account-id		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.
envelope-from		Indicates that AAA uses the account username from the fax-mail header as the AAA account identifier.
envelope-to		Indicates that AAA uses the recipient derived from the fax-mail header as the AAA account identifier.
gateway		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> .

Defaults	No account identification source is defined.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store and forward fax, you can specify that the account ID, username, or recipient name from the e-mail header information be used to identify the user for authentication. This command defines what AAA uses for the secondary identifier for outbound or off-ramp user authentication with store and forward fax.

Store and forward fax allows you to define either a primary or a secondary identifier. (You configure the primary identifier using the **mmoip aaa send-id primary** command.) AAA extracts the authentication identifier information from the defined sources. If the field is blank (meaning undefined), AAA will use the secondary identifier source if configured. The secondary identifier is used only when the primary identifier is null. In this case, when AAA sees that the primary identifier is null, it will check to see if a secondary identifier has been defined and use that value for user authentication.

AAA does not use these methods sequentially—meaning that if the primary identifier is defined and AAA cannot match the primary identifier information, it will not use the secondary identifier for authentication. Authentication simply fails.

When you enable authentication, the on-ramp gateway inserts whatever value you configure for the **mmoip aaa receive-id secondary** command in the X-account ID field of the e-mail header (if store-and-forward uses the defined secondary identifier). This X-account ID field contains the value that is used for authentication and accounting by the on-ramp gateway. For example, if the **mmoip aaa receive-id secondary** command is set to **gateway**, the on-ramp gateway name (for example, hostname.domain-name) is inserted in the X-account ID field of the e-mail header of the fax-mail message.

If you want to use this configured gateway value in the X-account ID field, you must configure the **mmoip aaa send-id secondary** command with the **account-id** keyword. This particular keyword enables store and forward fax to generate end-to-end authentication and accounting tracking records. If you do not enable authentication on the on-ramp gateway, the X-account ID field is left blank.

This command applies to off-ramp store and forward fax functions.

Examples

The following example defines the recipient name as defined in the envelope-to field of the e-mail header to be used as the AAA authentication identifier for store and forward fax:

```
aaa new-model
mmoip aaa send-id secondary envelope-to
```

Related Commands

Command	Description
mmoip aaa send-id primary	Specifies the primary location where AAA retrieves its account identification information for off-ramp faxing.
mmoip aaa send-id secondary	Specifies the secondary location where AAA retrieves its account identification information for off-ramp faxing.

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

atm	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 HDB3 for E1. When you remove ATM mode by entering the no mode atm command, ATM interface 0 is deleted. ATM mode is supported only on controller 0 (T1 or E1 0).
cas	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.

Defaults

No mode is configured.

Command Modes

Controller configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

This command applies to the Cisco MC3810 multiservice concentrator with the digital voice module (DVM) installed.

When no mode is selected, channel groups and clear channels (data mode) can be created using the **channel-group** and **tdm-group** commands, respectively.

On the Cisco MC3810 multiservice concentrator, some DS0s are used exclusively for different signaling modes. The DS0 channels have the following limitations when mixing different applications (such as voice and data) on the same network trunk:

- On E1 controllers, DS0 16 is used exclusively for either CAS or CCS, depending on which mode is configured.
- On T1 controllers, DS0 24 is used exclusively for CCS.

Examples

The following example configures ATM mode on controller T1 0. This is required for Voice over ATM.

```
controller T1 0
mode atm
```

The following example configures CAS mode on controller T1 1:

```
controller T1 1
mode cas
```

Related Commands

Command	Description
channel-group	Defines the time slots that belong to each T1 or E1 circuit.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for TDM cross-connect.

mode ccs

To configure the T1/E1 controller to support common channel signaling (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

cross-connect	Enables CCS cross-connect on the controller.
frame-forwarding	Enables CCS frame forwarding on the controller.

Defaults

No CCS mode is configured.

Command Modes

Controller configuration

Command History

Release	Modification
12.0(2)T	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.1(2)XH	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers.
12.1(3)T	The modifications in 12.1(2)XH were integrated into 12.1(3)T.

Examples

To enable CCS cross-connect on controller T1 1, enter the following commands:

```
controller T1 1
 mode ccs cross-connect
```

To enable CCS frame forwarding on controller T1 1, enter the following commands:

```
controller T1 1
 mode ccs frame-forwarding
```

Related Commands

Command	Description
ccs connect	Configures a CCS connection on an interface configured to support CCS frame forwarding.

modem passthrough (dial-peer)

To configure modem passthrough over VoIP for a specific dial peer, use the **modem passthrough** command in dial-peer configuration mode. To disable modem passthrough 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	
system	Defaults to the global configuration.
nse	Named signaling event.
payload-type	(Optional) NSE payload type.
<i>number</i>	(Optional) The value of the payload type (96–119).
codec	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.
g711ulaw	Codec G.711 u-Law 64000 bits per second for T1.
g711alaw	Codec G.711 A-Law 64000 bits per second for E1.
redundancy	(Optional) Packet redundancy (RFC 2198) for modem traffic.

Defaults Defining **system** as the method in dial peer points to the voice service Voice over IP (VoIP) configuration default and is intended to simplify gateway configuration. The default is **modem passthrough system**. As required, the gateway defaults to **no modem passthrough**.

Command Modes Dial-peer configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced for the Cisco AS5300 universal access server.

Usage Guidelines Use the **modem passthrough** dial-peer configuration command to configure modem passthrough over VoIP for a specific dial peer. The payload type is an optional parameter for the **nse** keyword. Use the same **payload-type number** for both the originating gateway and the terminating gateway. The **payload-type number** can be set from 96 to 119. If you do not specify the **payload-type number**, the *number* defaults to 100.

Use the same codec type for both the originating gateway and the terminating gateway. **g711ulaw** codec is required for T1, and **g711alaw** codec is required for E1.

The **redundancy** keyword is an optional parameter for sending redundant packets for modem traffic.

modem passthrough (dial-peer)

When the **system** keyword is enabled, the following parameters are not available: **nse**, **payload-type**, **codec**, and **redundancy**. The **system** keyword overrides the configuration for the dial peer, and the values from the global configuration are used.

Examples

The following example shows how modem passthrough over VoIP is configured for a specific dial peer in dial-peer configuration mode:

```
modem passthrough nse codec g711ulaw redundancy
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode.

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 passthrough, 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	
nse	Named signaling event.
payload-type	(Optional) NSE payload type.
<i>number</i>	(Optional) The value of the payload type. The number can be from 96 to 119.
codec	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.
g711ulaw	Codec G.711 u-Law 64000 bits per second for T1.
g711alaw	Codec G.711 A-Law 64000 bits per second for E1.
redundancy	(Optional) Packet redundancy (RFC 2198) for modem traffic.
maximum-sessions	(Optional) Maximum number of simultaneous modem passthrough 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.

Defaults	Disabled

Command Modes	Voice-service configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced for the Cisco AS5300 universal access server.

Usage Guidelines

Use the **modem passthrough** command to configure modem passthrough over Voice over IP (VoIP) for the Cisco AS5300 universal access server. The default behavior for the **voice service voip** command is **no modem passthrough**.

The payload type is an optional parameter for the **nse** keyword. Use the same **payload-type number** for both the originating gateway and the terminating gateway. The **payload-type number** can be set from 96 to 119. If you do not specify the **payload-type number**, the *number* defaults to 100.

Use the same codec type for both the originating gateway and the terminating gateway. **g711ulaw** codec is required for T1, and **g711alaw** codec is required for E1.

The **redundancy** keyword is an optional parameter for sending redundant packets for modem traffic.

The **maximum-sessions** keyword is an optional parameter for the **modem passthrough** command. This parameter determines the maximum number of simultaneous modem passthrough sessions. The recommended *value* for the **maximum-sessions** keyword is 16. The value can be set from 1 to 26.

When using the **voice service voip** and **modem passthrough nse** commands on a terminating gateway to globally set up fax or modem pass-through with NSEs, you must also ensure that each incoming call will be associated with a VoIP dial peer to retrieve the global fax or modem configuration. You associate calls with dial peers by using the **incoming called-number** command to specify a sequence of digits that incoming calls can match. You can ensure that all calls will match at least one dial peer by using the following commands:

```
Router(config)# dial-peer voice tag voip
Router(config-dial-peer)# incoming called-number .
```

Examples

The following example shows modem pass-through configuration in voice-service configuration mode for NSE payload type 101 using codec G.711:

```
modem passthrough nse payload-type 101 codec g711ulaw redundancy maximum-sessions 1
```

Related Commands

Command	Description
incoming called-number	Defines an incoming called number to match a specific dial peer.
voice service voip	Enters voice-service configuration mode and specifies the voice encapsulation type.

mta receive aliases

To specify a host name accepted as a Simple Mail Transfer Protocol (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*

Syntax Description	<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].

Defaults	Enabled with an empty string

Command Modes	Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 and Cisco AS5800 universal access servers.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines	This command creates an accept or reject alias list. The first alias is used by the mailer to identify itself in SMTP banners and when generating its own RFC 822 Received: header.



Note

This command does not automatically include reception for a domain IP address—it must be explicitly added. To explicitly add a domain IP address, use the following format: **mta receive aliases** [*ip-address*]. Use the IP address of the Ethernet or the FastEthernet interface of the off-ramp gateway.

This command applies to on-ramp store and forward fax functions.

Examples	The following example specifies the host name seattle-fax-offramp.example.com as the alias for the SMTP server:
	<pre>mta receive aliases seattle-fax-offramp.example.com</pre>
	The following example specifies the IP address 172.166.0.0 as the alias for the SMTP server:
<pre>mta receive aliases [172.16.0.0]</pre>	

Related Commands	Command	Description
	mta receive generate-mdn	Specifies that the off-ramp gateway process a response MDN from an SMTP server.
	mta receive maximum-recipients	Specifies the maximum number of recipients for all SMTP connections.

mta receive generate-mdn

To specify that the off-ramp gateway process a response message disposition notice (MDN) from a Simple Mail Transfer Protocol (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

Syntax Description	This command has no arguments or keywords.

Defaults	Disabled

Command Modes	Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 and Cisco AS5800 universal access servers.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines	When message delivery notification is enabled on a sending Cisco AS5300 universal access server, the device inserts a flag in the off-ramp message e-mail header, requesting that the receiving Cisco AS5300 universal access server generate the message delivery notification and return that message to the sender when the e-mail message that contains the fax image is opened. Use the mta receive generate-mdn command to enable the receiving device—the off-ramp gateway—to process the response message delivery notification.

Depending on the configuration, usage, and features of the mailers used at a site, it might be desirable to enable or disable MDN generation. (DSN generation cannot be disabled.)

Specifications for MDN are described in RFC 2298.

This command applies to off-ramp store and forward fax functions.

Examples	The following example enables the receiving device to generate message delivery notices:

```
mta receive generate-mdn
```

Related Commands	Command	Description
	mdn	Requests that a message disposition notice be generated when the fax-mail message is processed (opened).

Command	Description
mta receive aliases	Specifies a host name accepted as an SMTP alias for off-ramp faxing.
mta receive maximum-recipients	Specifies the maximum number of recipients for all SMTP connections.

mta receive maximum-recipients

To specify the maximum number of recipients for all Simple Mail Transfer Protocol (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

Syntax Description

<i>number</i>	Specifies the maximum number of recipients for all SMTP connections. Valid entries are from 0 to 1024.

Defaults

The default is 0 recipients, meaning that incoming mail messages will not be accepted; therefore, no faxes are sent by the off-ramp gateway.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300 and Cisco AS5800 universal access servers.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

This command applies to off-ramp store and forward fax functions.



Note Unless the sending mailer supports the X-SESSION SMTP service extension, each incoming SMTP connection will be allowed to send only to one recipient and thus consume only one outgoing modem.

Use the **mta receive maximum-recipients** command to configure the maximum number of modems that you want to allocate for fax usage at any one time. You can use this command to limit the resource usage on the gateway. When the value for the *number* argument is set to 0, no new connections can be established. This is particularly useful when preparing to shut down the system.

Examples

The following example defines 10 as the maximum number of recipients for all SMTP connections:

```
mta receive maximum-recipients 10
```

 **mta receive maximum-recipients**

Related Commands	Command	Description
	mta receive aliases	Specifies a host name accepted as an SMTP alias for off-ramp faxing.
	mta receive generate-mdn	Specifies that the off-ramp gateway process a response MDN from an SMTP server.

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 \$\$* }

Syntax Description

hostname string	Text string that specifies the Simple Mail Transfer Protocol (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].
username string	Text string that specifies the sender username.
username \$\$	Wildcard that specifies that the username will be derived from the calling number.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300 and Cisco AS5800 universal access servers.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Use the **mta send mail-from** command to designate the sender of the fax TIFF attachment. This value is equivalent to the return path information in an e-mail message.

The postmaster address, configured with the **mta send postmaster** command, is used if the mail-from address is blank.

This command applies to on-ramp store and forward fax functions.

Examples

The following example specifies that the mail-from username information will be derived from the calling number of the sender:

```
mta send mail-from username $$
```

Related Commands	Command	Description
	mta send origin-prefix	Adds information to the e-mail prefix header.
	mta send postmaster	Defines where an 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	Specifies the address where MDNs are sent.
	mta send server	Specifies a destination mail server or servers.
	mta send subject	Specifies the subject header of the e-mail message.

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*

Syntax Description	<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 ("abc xyz").

Defaults	Null string

Command Modes	Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 and Cisco AS5800 universal access servers.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines	Normally, the store and forward fax feature provides the slot and port number from which the e-mail came in the e-mail prefix header information. Use this command to append the defined text string to the front of the e-mail prefix header information. This test string is a prefix string that is appended with the modem port and slot number and passed in the originator_comment field of the esmtp_client_engine_open() call. Eventually, this ends up in the received header field of the fax-mail message, for example:

```
Received (test onramp Santa Cruz slot1 port15) by router-5300.cisco.com for
<test-test@cisco.com> (with Cisco NetWorks); Fri, 25 Dec 1998 001500 -0800
```

In other words, using the command **mta send origin-prefix dog** causes the Received header to contain the following information:

```
Received (dog, slot 3 modem 8) by as5300-sj.example.com....
```

This command applies to on-ramp store and forward fax functions.

Examples	The following example shows how to add information to the e-mail prefix header: <pre>mta send origin-prefix "Cisco-Powered Fax System"</pre>

Related Commands	Command	Description
	mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
	mta send postmaster	Defines where an 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	Specifies the address where MDNs are sent.
	mta send server	Specifies a destination mail server or servers.
	mta send subject	Specifies the subject header of the e-mail message.

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*

Syntax Description

<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.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300 and Cisco AS5800 universal access servers.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

If you have configured the Cisco AS5300 universal access server to generate DSNs and MDNs but you have not configured the sender information (using the **mta send mail-from** command) or the Simple Mail Transfer Protocol (SMTP) server, DSNs and MDNs are delivered to the e-mail address determined by this command.

The address defined by this command is used as the **mta send mail-from** address if the evaluated string is blank. An address, such as fax-administrator@example.com, is recommended (where example.com is replaced with your domain name, and fax-administrator is aliased to the person responsible for the operation of the AS5300 universal access server fax functions). At some sites, this may be the same person as the e-mail postmaster, but at most sites this is likely to be a different person and thus should be a different e-mail address.

This command applies to on-ramp store and forward fax functions.

Examples

The following example configures the e-mail address fax-admin@example.com as the sender for all incoming faxes. Thus, any returned DSNs will be delivered to fax-admin@example.com if the mail-from field is otherwise blank.

```
mta send postmaster fax-admin@example.com
```

Related Commands	Command	Description
	mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
	mta send origin-prefix	Adds information to the e-mail prefix header.
	mta send return-receipt-to	Specifies the address where MDNs are sent.
	mta send server	Specifies a destination mail server or servers.
	mta send subject	Specifies the subject header of the e-mail message.

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 \$\$* }

Syntax Description

hostname string	Text string that specifies the Simple Mail Transfer Protocol (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].
username string	Text string that specifies the sender username where MDNs are sent.
username \$\$	Wildcard that specifies that the username are derived from the calling number.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300 and Cisco AS5800 universal access servers.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Use the **mta send return-receipt-to** command to define where you want MDNs to be sent after the fax-mail is opened.



Note

Store and forward fax supports the Eudora proprietary format, meaning that the header that store and forward fax generates is in compliance with RFC 2298 (MDN).



Note

Multimedia Mail over Internet Protocol (MMoIP) dial peers must have MDN enabled to generate return receipts in off-ramp fax-mail messages.

This command applies to on-ramp store and forward fax functions.

Examples

The following example configures scoobee as the SMTP mail server to which DSNs are sent:

```
mta send return-receipt-to hostname server.com
mta send return-receipt-to username scoobee
```

Related Commands	Command	Description
	mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
	mta send origin-prefix	Adds information to the e-mail prefix header.
	mta send postmaster	Defines where an e-mail message should be delivered (the mail server postmaster account) if it cannot be delivered to the defined destination.
	mta send server	Specifies a destination mail server or servers.
	mta send subject	Specifies the subject header of the e-mail message.

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.

Defaults

IP address defined as 0.0.0.0

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300 and Cisco AS5800 universal access servers.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Use the **mta send server** command to provide a backup destination server in case the first configured mail server is unavailable. (This command is not intended to be used for load distribution.)

You can configure up to ten different destination mail servers using the **mta send server** command. If you configure more than one destination mail server, the Cisco AS5300 universal access server attempts to contact the first mail server configured. If that mail server is unavailable, it will contact the next configured destination mail server.

DNS MX records are not used to look up host names provided to this command.



Note

When you use the **mta send server** command, you should configure the Cisco AS5300 universal access server to perform name lookups using the **ip name-server** command.

This command applies to on-ramp store and forward fax functions.

Examples

The following example defines the mail servers scoobee.example.com and doogie.example.com as the destination mail servers:

```
mta send server scoobee.example.com
mta send server doogie.example.com
```

Related Commands	Command	Description
	ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
	mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
	mta send origin-prefix	Adds information to the e-mail prefix header.
	mta send postmaster	Defines where an 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	Specifies the address where MDNs are sent.
	mta send subject	Specifies the subject header of the e-mail message.

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.

Defaults	Null string

Command Modes	Global configuration

Command History	Release	Modification
	12.0(4)XJ	This command was introduced on the Cisco AS5300 and Cisco AS5800 universal access servers.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines	This command applies to on-ramp store and forward fax functions.

**Note**

The string does not need to be enclosed in quotation marks.

Examples	The following example defines the subject header of an e-mail message as “fax attachment”: mta send subject fax attachment

Related Commands	Command	Description
	mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
	mta send origin-prefix	Adds information to the e-mail prefix header.
	mta send postmaster	Defines where an 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	Specifies the address where MDNs are sent.
	mta send server	Specifies a destination mail server or servers.

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.

Defaults	–38 dB

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced for the Cisco 3600 series router.
	12.0(4)T	Support was added for the Cisco MC3810 multiservice concentrator.

Usage Guidelines

Use this command to specify the decibel level of music played when calls are put on hold. This command tells the firmware to pass steady data above the specified level. It only affects the operation of voice activity detection (VAD) when receiving voice.

If the value for this command is set too high, VAD interprets music-on-hold as silence, and the remote end does not hear the music. If the value for this command is set too low, VAD compresses and passes silence when the background is noisy, creating unnecessary voice traffic.

Examples

The following example sets the decibel threshold to –35 for the music played when calls are put on hold:

```
voice port 0:D
 music-threshold -35
```

The following example sets the decibel threshold to –35 for the music played when calls are put on hold on the Cisco 3600 series router:

```
voice-port 1/0/0
 music-threshold -35
```

The following example sets the decibel threshold to –35 for the music played when calls are put on hold on the Cisco MC3810 multiservice concentrator:

```
voice-port 1/1
 music-threshold -35
```


Related Commands

Command	Description
voice-port	Enters voice-port configuration mode.

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}

Syntax Description	56k	Sets the network clock base rate to 56 kbps.
	64k	Sets the network clock base rate to 64 kbps.

Defaults	56 kbps

Command Modes	Global configuration

Command History	Release	Modification
	11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines	This command applies to Voice over Frame Relay and Voice over ATM on the Cisco MC3810 multiservice concentrator.

Examples	The following example sets the network clock base rate to 64 kbps:

```
network-clock base-rate 64k
```

Related Commands	Command	Description
	network-clock-select	Uses the network clock source to provide timing to the system backplane PCM bus.
	network-clock-switch	Configures the switch delay time to the next priority network clock source when the current network clock source fails.

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

Syntax Description	<i>switch-delay</i>	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.
	never	Indicates no delay time before the current network clock source recovers.
	<i>restore-delay</i>	The delay time before the current network clock source recovers. The range is from 0 to 99 seconds.
	never	Indicates no delay time, in seconds, before the next priority network clock source is used when the current network clock source fails.

Defaults	10 seconds

Command Modes	Global configuration

Command History	Release	Modification
	11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.

Examples	The following command switches the network clock source after 20 seconds and sets the delay time before the current network clock source recovers to 20 seconds:
	<pre>network-clock-switch 20 20</pre>

Related Commands	Command	Description
	network-clock-select	Uses the network clock source to provide timing to the system backplane PCM bus.

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

Syntax Description	This command has no arguments or keywords.

Defaults	Enabled

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 series router.

Usage Guidelines	The function enabled by the non-linear command is also generally known as residual echo suppression. This command is associated with the echo canceller operation. The echo-cancel enable command must be enabled for the non-linear command to take effect. Use the non-linear command to shut off any signal if no near-end speech is detected.

Enabling the **non-linear** command normally improves performance, although some users might perceive truncation of consonants at the end of sentences when this command is enabled.

Examples	The following example enables nonlinear call processing on the Cisco 3600 series router:

```
voice-port 1/0/0
 non-linear
```

The following example enables nonlinear call processing on the Cisco MC3810 multiservice concentrator:

```
voice-port 1/1
 non-linear
```

Related Commands	Command	Description
	echo-cancel enable	Enables the cancellation of voice that is sent out the interface and is received on the same interface.

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

Syntax Description	<i>nsap-address</i>	A 40-digit hexadecimal number; the number must be unique on the device.

Defaults	No NSAP address for a video dial peer is configured.

Command Modes	Dial-peer configuration

Command History	Release	Modification
	12.0(5)XK	This command was introduced for ATM video dial-peer configuration on the Cisco MC3810 multiservice concentrator.
	12.0(7)T	This command was integrated into Cisco IOS Release 12.0(9)T.

Usage Guidelines	The address must be unique on the router.

Examples	On a Cisco MC3810 multiservice concentrator, the following example sets up an NSAP address for the local video dial peer designated as 10:
	<pre>dial-peer video 10 videocodec nsap 47.0091810000000002F26D4901.333333333332.02</pre>

Related Commands	Command	Description
	dial-peer video	Defines a video ATM dial peer for a local or remote video codec, specifies video-related encapsulation, and enters dial-peer configuration mode.
	show dial-peer video	Displays dial-peer configuration.

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.

Defaults

No number expansion is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series router.
12.0(3)T	This command was supported on the Cisco AS5300 universal access server.
12.0(4)XL	This command was supported on the Cisco AS5800 universal gateway.
12.0(7)T	The modifications in 12.0(4)XL were integrated in 12.0(7)T.
12.0(7)XK	This command was supported on the Cisco MC3810 multiservice concentrator platform.
12.1(2)T	The modifications in 12.0(7)XK were integrated in 12.1(2)T.

Usage Guidelines

Use the **num-exp** global configuration command to define how to expand a particular set of numbers (for example, a telephone extension number) into a particular destination pattern. With this command, you can bind specific extensions and expanded numbers together by explicitly defining each number, or you can define extensions and expanded numbers using variables. You can also use this command to convert seven-digit numbers to numbers containing less than seven digits.

Use a period (.) as a variable or wildcard, representing a single number. Use a separate period for each number that you want to represent with a wildcard—for example, if you want to replace four numbers in an extension with wildcards, type in four periods.

Examples

The following example expands the extension number 55541 to the number 14085555541:

```
num-exp 55541 14085555541
```

The following example expands all five-digit extensions beginning with 5 such that the 5 is replaced with the digits 1408555 at the beginning of the extension number:

```
num-exp 5.... 1408555....
```

Related Commands

Command	Description
dial-peer terminator	Designates a special character to be used as a terminator for variable length dialed numbers.
forward-digits	Specifies which digits to forward for voice calls.
prefix	Specifies a prefix for a dial peer.

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

international	Specifies international numbering type.
abbreviated	Specifies abbreviated numbering type.
national	Specifies national numbering type.
network	Specifies network numbering type.
reserved	Specifies reserved numbering type.
subscriber	Specifies subscriber numbering type.
unknown	Specifies if the numbering type is unknown.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced for Voice over IP on the Cisco AS5300 universal access server.
12.0(7)XK	This command was first supported for the following voice technologies on the following platforms: - Voice over IP (Cisco 2600 series router router, Cisco 3600 series router, Cisco MC3810 multiservice concentrator) - Voice over Frame Relay (Cisco 2600 series router router, Cisco 3600 series router, Cisco MC3810 multiservice concentrator) - Voice over ATM (Cisco 3600 series router, Cisco MC3810 multiservice concentrator)

Release	Modification
12.1(1)T	This command was first supported on the T train for the following voice technology on the following platforms: Voice over IP (Cisco 1750, Cisco 2600 series router, Cisco 3600 series router, Cisco AS5300 universal access server, Cisco 7200 series router, and Cisco 7500 series)
12.1(2)T	This command was first supported on the T train for the following voice technologies on the following platforms: - Voice over IP (Cisco MC3810 multiservice concentrator) - Voice over Frame Relay (Cisco 2600 series router, Cisco 3600 series router, Cisco MC3810 multiservice concentrator) - Voice over ATM (Cisco 3600 series router, Cisco MC3810 multiservice concentrator)

Usage Guidelines

The **numbering-type** command is supported for plain old telephone service (POTS), VoIP, VoFR, and VoATM dial peers. The numbering type options are implemented as defined by the ITU Q.931 specification.

Examples

The following example shows how to configure a POTS dial peer for network usage:

```
dial-peer voice 100 pots
 numbering-type network
```

The following example shows how to configure a VoIP dial peer for subscriber usage:

```
dial-peer voice 200 voip
 numbering-type subscriber
```

Related Commands

Command	Description
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
show translation-rule	Displays the contents of all the rules that have been configured for a specific translation name.
test translation-rule	Tests the execution of the translation rules on a specific name-tag.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

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}

Syntax Description

2-wire	Specifies a 2-wire E&M cabling scheme.
4-wire	Specifies a 4-wire E&M cabling scheme.

Defaults

2-wire operation

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series..
11.3(1)MA	Support was added for the Cisco MC3810 multiservice concentrator.

Usage Guidelines

This command applies to both the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator.

The **operation** command affects only voice traffic. Signaling is independent of 2-wire versus 4-wire settings. If the wrong cable scheme is specified, the user might get voice traffic in only one direction.

Configuring the **operation** command on a voice port changes the operation of both voice ports on a VPM card. The voice port must be shut down and then opened again for the new value to take effect.

This command is not applicable to FXS or FXO interfaces because they are, by definition, 2-wire interfaces.

On the Cisco MC3810 multiservice concentrator, this command applies only to the analog voice module (AVM).

Examples

The following example specifies that an E&M port on the Cisco 3600 series router uses a 4-wire cabling scheme:

```
voice-port 1/0/0
 operation 4-wire
```

The following example specifies that an E&M port on the Cisco MC3810 multiservice concentrator uses a 2-wire cabling scheme:

```
voice-port 1/1
 operation 2-wire
```

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

Syntax Description

<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.

Defaults

The default value for FXO, FXS, and E&M ports is 0.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series router.
11.3(1)MA	Support was added for the Cisco MC3810 multiservice concentrator.

Usage Guidelines

A system-wide loss plan must be implemented using both the **input gain** and **output attenuation** commands. Other equipment (including PBXs) in the system must be considered when creating a loss plan. The default value for this command assumes that a standard transmission loss plan is in effect, meaning that there must be an attenuation of –6 dB between phones. Connections are implemented to provide –6 dB of attenuation when the **input gain** and **output attenuation** commands are configured with the default value of 0 dB.

You cannot increase the gain of a signal to the Public Switched Telephone Network (PSTN), but you can decrease it. If the voice level is too high, you can decrease the volume by either decreasing the input gain or increasing the output attenuation.

You can increase the gain of a signal coming into the router. If the voice level is too low, you can increase the input gain by using the **input gain** command.

Examples

On the Cisco 3600 series router, the following example configures a 3-dB gain to be inserted at the transmit side of the interface:

```
voice-port 1/0/0
 output attenuation 3
```

On the Cisco AS5300 universal access server, the following example configures a 3-dB gain to be inserted at the transmit side of the interface:

```
voice-port 0:D
 output attenuation 3
```

output attenuation

On the Cisco MC3810 multiservice concentrator, the following example configures a 6-dB gain to be inserted at the transmit side of the interface:

```
voice-port 1/1
 output attenuation 6
```

Related Commands

Command	Description
input gain	Configures a specific input gain value for a voice port.

playout-delay (dial-peer)

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** } }

Syntax Description

nominal *milliseconds*

The **nominal** 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.

The *milliseconds* 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 **codec complexity** command.)

If the voice card is configured for high codec complexity, the highest value that can be configured for **nominal** for compressed codecs is 250 ms. For medium-complexity codec configurations, the highest **nominal** 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.

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.

■ **playout-delay (dial-peer)**

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.

Defaults

The default for nominal is 200 milliseconds.

The default for maximum is 200 milliseconds.

The default for minimum is 40 milliseconds.

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator in the voice-port configuration mode.
12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series router routers.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)XI	This command was first supported on the Cisco ICS 7750.
12.1(5)T	The minimum keyword was introduced, and support for dial-peer configuration mode was added on the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers, Cisco MC3810 multiservice concentrator, and Cisco AS5200, Cisco AS5300, Cisco AS5400, and Cisco AS5800 universal access servers.

Usage Guidelines

Before Cisco IOS Release 12.1(5)T, the **playout-delay** command was configured in voice-port configuration mode. For Cisco IOS Release 12.1(5)T and later releases, in most cases playout delay should be configured in dial-peer configuration mode on the Voice over IP (VoIP) dial peer that is on the receiving end of the voice traffic that is to be buffered. This dial peer senses network conditions and relays them to the DSPs, which adjust the jitter buffer as necessary. When multiple applications are configured on the gateway, playout delay should be configured in dial-peer configuration mode. When there are numerous dial peers to configure, it might be simpler to configure playout delay on a voice port. If conflicting playout delay values have been configured on a voice port and on a dial peer, the dial-peer configuration takes precedence.

Playout delay is the amount of time that elapses between the time that a voice packet is received at the jitter buffer on the DSP and the time that it is played out to the codec. In most networks with normal jitter conditions, the defaults are adequate and you will not need to configure the **playout-delay** command.

In situations in which you want to improve voice quality by reducing jitter or you want to reduce network delay, you can configure **playout-delay** parameters. The parameters are slightly different for each of the two playout delay modes, adaptive and fixed (see the **playout-delay mode** command).

In adaptive mode, the average delay for voice packets varies depending on the amount of interarrival variation that packets have as the call progresses. The jitter buffer grows and shrinks to compensate for jitter and to keep voice packets playing out smoothly, within the maximum and minimum limits that have been configured. The maximum limit establishes the highest value to which the adaptive delay will be set. The minimum limit is the low-end threshold for the delay of incoming packets by the adaptive jitter buffer. Algorithms in the DSPs that control the growth and shrinkage of the jitter buffer are weighted toward the improvement of voice quality at the expense of network delay: jitter buffer size increases rapidly in response to spikes in network transmissions and decreases slowly in response to reduced congestion.

In fixed mode, the nominal value is the amount of playout delay applied at the beginning of a call by the jitter buffer in the gateway and is also the maximum size of the jitter buffer throughout the call.

As a general rule, if there is excessive breakup of voice due to jitter with the default playout delay settings, increase playout delay times. If your network is small and jitter is minimal, decrease playout delay times for a smaller overall delay.

When there is bursty jitter in the network, voice quality can be degraded even though the jitter buffer is actually adjusting the playout delay correctly. The constant readjustment of playout delay to erratic network conditions causes voice quality problems that are usually alleviated by increasing the minimum playout delay value in adaptive mode or by increasing the nominal delay for fixed mode.

Use the **show call active voice** command to display the current delay, as well as high- and low-water marks for delay during a call. Other fields that can help determine the size of a jitter problem are **ReceiveDelay**, **GapFillWith...**, **LostPackets**, **EarlyPackets**, and **LatePackets**. The following is an example of the output from the **show call active voice** command:

```
VOIP:
ConnectionId[0xECDE2E7B 0xF46A003F 0x0 0x47070A4]
IncomingConnectionId[0xECDE2E7B 0xF46A003F 0x0 0x47070A4]
RemoteIPAddress=192.168.100.101
RemoteUDPPort=18834
RoundTripDelay=26 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=TRUE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=cisco
SessionTarget=
OnTimeRvPlayout=417000
GapFillWithSilence=850 ms
GapFillWithPrediction=2590 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=70 ms
LoWaterPlayoutDelay=29 ms
ReceiveDelay=39 ms
LostPackets=0
EarlyPackets=0
LatePackets=86
```

■ playout-delay (dial-peer)

Examples

The following example uses the default adaptive mode for the **playout-delay** command with a minimum playout delay of 10 milliseconds and a maximum playout delay of 60 milliseconds, on the VoIP dial peer tagged 80. The size of the jitter buffer will be adjusted up and down on the basis of the amount of jitter that the DSP finds, but will never be smaller than 10 milliseconds, and never larger than 60 milliseconds.

```
dial-peer 80 voip
  playout-delay minimum low
  playout-delay maximum 60
```

Related Commands

Command	Description
playout-delay mode	Selects fixed or adaptive mode for the jitter buffer on DSPs.
show call active voice	Displays active call information for voice calls.

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

maximum	The delay time that the digital signal processor (DSP) allows before starting to discard voice packets. The default is 160 milliseconds.
nominal	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.

Defaults

The default for maximum delay is 160 milliseconds. The default for nominal delay is 80 milliseconds.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	This command was first supported on Cisco 2600 and 3600 series routers.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

If there is excessive breakup of voice due to jitter with the default playout delay settings, increase the delay times. If your network is small and jitter is minimal, decrease the delay times to reduce delay.

Examples

The following example configures a nominal playout delay of 80 milliseconds and a maximum playout delay of 160 milliseconds on voice port 1/1 on a Cisco MC3810 multiservice concentrator:

```
voice-port 1/1
 playout-delay nominal 80
 playout-delay maximum 160
```

The following example configures a nominal playout delay of 80 milliseconds and a maximum playout delay of 160 milliseconds on voice port 1/0/0 on the Cisco 2600 or 3600:

```
voice-port 1/0/0
 playout-delay nominal 80
 playout-delay maximum 160
```

■ **playout-delay (voice-port)**

Related Commands	Command	Description
	vad	Enables voice activity detection.

playout-delay mode (dial-peer)

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. To restore the default value, use the **no** form of this command.

playout-delay mode {adaptive | fixed}

no playout-delay mode {adaptive | fixed}

Syntax Description

adaptive	Jitter buffer size and amount of playout delay are adjusted during a call, on the basis of current network conditions.
fixed	Jitter buffer size does not adjust during a call; a constant playout delay is added.

Defaults

The default is the **adaptive** keyword.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.1(5)T	Support for this command was added on the Cisco 2600 and Cisco 3600 series routers, Cisco MC3810 multiservice concentrator, and the Cisco ICS 7750. In addition, the no-timestamps keyword was removed from the syntax.

Usage Guidelines

Before Cisco IOS Release 12.1(5)T, the **playout-delay** command was configured only in voice-port configuration mode. For Cisco IOS Release 12.1(5)T and later releases, in most cases playout delay should be configured in dial-peer configuration mode on the VoIP dial peer that is on the receiving end of the voice traffic that is to be buffered. This dial peer senses network conditions and relays them to the DSPs, which adjust the jitter buffer as necessary. When multiple applications are configured on the gateway, playout delay should be configured in dial-peer configuration mode.



Tips

When there are numerous dial peers to configure, it might be simpler to configure playout delay on a voice port. If conflicting playout delay values have been configured on a voice port and on a dial peer, the dial-peer configuration takes precedence.

In most networks with normal jitter conditions, the default is adequate and you do not need to configure the **playout-delay mode** command.

The default is adaptive mode, in which the average delay for voice packets varies depending on the amount of interarrival variation that packets have as the call progresses. The jitter buffer grows and shrinks to compensate for jitter and to keep voice packets playing out smoothly, within the maximum and minimum limits that have been configured.

■ playout-delay mode (dial-peer)

Select fixed mode only when you understand your network conditions well, and when you have a network with very poor quality of service (QoS) or when you are interworking with a media server or similar transmission source that tends to create a lot of jitter at the transmission source. In most situations it is better to configure adaptive mode and let the DSP size the jitter buffer according to current conditions.

Examples

The following example configures adaptive playout-delay mode with the minimum delay set at high (80 milliseconds), on a VoIP dial peer that has a tag of 80:

```
dial-peer 80 voip
  playout-delay mode adaptive
  playout-delay minimum high
```

Related Commands

Command	Description
playout-delay	Tunes the jitter buffer on DSPs for playout delay of voice packets.
show call active voice	Displays active call information for voice calls.

playout-delay mode (voice-port)

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 voice port configuration mode. To restore the default value, use the **no** form of this command.

playout-delay mode { **adaptive** | **fixed** }

no playout-delay mode { **adaptive** | **fixed** }

Syntax Description

adaptive	Jitter buffer size and amount of playout delay are adjusted during a call, on the basis of current network conditions.
fixed	Jitter buffer size does not adjust during a call; a constant playout delay is added.

Defaults

The default is the **adaptive** keyword.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	The playout-delay command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	The playout-delay command was first supported on the Cisco 2600 and Cisco 3600 series routers.
12.1(2)T	The playout-delay command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)XI	The keyword mode was introduced, and the playout-delay mode command was first supported on the Cisco ICS 7750.
12.1(5)T	The no-timestamps keyword was removed from the syntax.

Usage Guidelines

Before Cisco IOS Release 12.1(5)T, the **playout-delay** command was configured only in voice-port configuration mode. For Cisco IOS Release 12.1(5)T and later releases, in most cases playout delay should be configured in dial-peer configuration mode on the VoIP dial peer that is on the receiving end of the voice traffic that is to be buffered. This dial peer senses network conditions and relays them to the DSPs, which adjust the jitter buffer as necessary. When multiple applications are configured on the gateway, playout delay should be configured in dial-peer configuration mode.



Tips

When there are numerous dial peers to configure, it might be simpler to configure playout delay on a voice port. If conflicting playout delay values have been configured on a voice port and on a dial peer, the dial-peer configuration takes precedence.

■ playout-delay mode (voice-port)

In most networks with normal jitter conditions, the default is adequate and you do not need to configure the **playout-delay mode** command.

The default is adaptive mode, in which the average delay for voice packets varies depending on the amount of interarrival variation that packets have as the call progresses. The jitter buffer grows and shrinks to compensate for jitter and to keep voice packets playing out smoothly, within the maximum and minimum limits that have been configured.

Select fixed mode only when you understand your network conditions well, and when you have a network with very poor quality of service (QoS) or when you are interworking with a media server or similar transmission source that tends to create a lot of jitter at the transmission source. In most situations it is better to configure adaptive mode and let the DSP size the jitter buffer according to current conditions.

Examples

The following example configures fixed mode on a Cisco 3640 voice port, with a nominal delay of 80 milliseconds.

```
voice-port 1/1/0
  playout-delay mode fixed
  playout-delay nominal 80
```

Related Commands

Command	Description
playout-delay	Tunes the jitter buffer on DSPs for playout delay of voice packets.
show call active voice	Displays active call information for voice calls.

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.
:D	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.
:D	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.

Defaults

No port is configured.

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced (Cisco 3600 series router).
11.3(3)T	Port-specific values for the Cisco 2600 were added.
11.3(1)MA	Port-specific values for the Cisco MC3810 multiservice concentrator were added.
12.0(3)T	Port-specific values for the Cisco AS5300 universal access server were added.
12.0(4)T	Support was added for the Cisco uBR924 platform.
12.0(7)T	Port-specific values for the Cisco AS5800 universal gateway were added.

Usage Guidelines

This command is used for calls incoming from a telephony interface to select an incoming dial peer and for calls coming from the VoIP network to match a port with the selected outgoing dial peer.

This command applies only to POTS peers.

Examples

The following example associates a Cisco 3600 series router POTS dial peer 10 with voice port 1, which is located on subunit 0, and accessed through port 0:

```
dial-peer voice 10 pots
  port 1/0/0
```

The following example associates a Cisco MC3810 multiservice concentrator POTS dial peer 10 with voice port 0, which is located in slot 1:

```
dial-peer voice 10 pots
  port 1/0
```

The following example associates a Cisco AS5300 universal access server POTS dial peer 10 with voice port 0:D:

```
dial-peer voice 10 pots
  port 0:D
```

The following example associates a Cisco AS5800 universal gateway POTS dial peer 10 with voice port 1/0/0:D (T1 card):

```
dial-peer voice 10 pots
  port 1/0/0:D
```

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

interface

Serial interface to which the local codec is connected. Valid entries are the numbers 0 or 1.

Defaults

No interface is specified.

Command Modes

Video dial-peer configuration

Command History

Release

Modification

12.0(5)XK

This command was introduced for ATM video dial-peer configuration on the Cisco MC3810 multiservice concentrator.

12.0(7)T

This command was integrated into Cisco IOS Release 12.0(7)T.

Examples

On a Cisco MC3810 multiservice concentrator local video dial peer designated as 10, the following example shows serial interface 0 as the specified interface for the codec:

```
dial-peer video 10 videocodec
port media Serial0
```

Related Commands

Command

Description

port signal

Specifies the slot location of the VDM and the port location of the EIA/TIA-366 interface for signaling.

show dial-peer video

Displays dial-peer configuration.

port signal

To specify the slot location of the video dialing module (VDM) and the port location of the EIA/TIA-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 EIA/TIA-366 interface. The Cisco MC3810 multiservice concentrator VDM has only one port, so the <i>port</i> value is always 0.

Defaults	No locations are specified.

Command Modes	Video dial-peer configuration

Command History	Release	Modification
	12.0(5)XK	This command was introduced for ATM video dial-peer configuration on the Cisco MC3810 multiservice concentrator.
	12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Examples	On a Cisco MC3810 multiservice concentrator, the following example shows how to set up the VDM and EIA/TIA-366 interface locations for the local video dial peer designated as 10:

```
dial-peer video 10 videocodec
port signal 1/0
```

Related Commands	Command	Description
	port media	Specifies the serial interface to which the local video codec is connected.
	show dial-peer video	Displays dial-peer configuration.

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

local	Enable call waiting on a local basis for the routers.
remote	Rely on the network provider service instead of the router to hold calls.

Defaults

The call waiting default is **remote** if the Call Waiting feature is not configured. In that case, the call holding pattern follows the settings of the service provider rather than those of the router.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)XF	The command pots call-waiting was introduced on the Cisco 800 series routers.

Usage Guidelines

To display the call waiting setting, use the **show running-config** or **show pots status** command. The ISDN call waiting service is used if it is available on the ISDN line connected to the router even if local call waiting is configured on the router. That is, if the ISDN line supports call waiting, the local call waiting configuration on the router is ignored.

Examples

The following example enables local call waiting on a router:

```
pots call-waiting local
```

Related Commands

Command	Description
call-waiting	Configure Call Waiting for a specific dial peer.

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 located.

Defaults

A default country is not defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series routers.

Usage Guidelines

This command applies to the Cisco 800 series routers.

If you need to change a country-specific default setting of a physical characteristic, you can use the associated command listed in the “Related Commands” section. Enter the **pots country ?** command to get a list of supported countries and the code you must enter to indicate a particular country.

Examples

The following example specifies that the devices connected to the telephone ports use default settings specific to Germany for the physical characteristics:

```
pots country de
```

Related Commands

Command	Description
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).

Command	Description
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

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

overlap	The router sends each digit dialed in a separate message.
enblock	The router collects all digits dialed and sends the digits in one message.

Defaults

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series routers.

Usage Guidelines

This command applies to Cisco 800 series routers.

To interrupt the collection and transmission of dialed digits, enter a pound sign (#), or stop dialing digits until the interdigit timer runs out (10 seconds).

Examples

The following example specifies that the router uses the enblock dialing method:

```
pots dialing-method enblock
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.

Command	Description
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

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

osi	Open switching interval (OSI) is the duration for which DC voltage applied between tip and ring conductors of a telephone port is removed.
reversal	Polarity reversal of tip and ring conductors of a telephone port.

Defaults

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series routers.

Usage Guidelines

This command applies to Cisco 800 series routers.

Most countries except Japan typically use the **osi** option. Japan typically uses the **reversal** option.

Examples

The following example specifies that the router uses the OSI disconnect method:

```
pots disconnect-supervision osi
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.

Command	Description
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

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).

Defaults	The default depends on the setting of the pots country command. For more information, see the pots country command.	

Command Modes	Global configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced on the Cisco 800 series routers.

Usage Guidelines	This command applies to Cisco 800 series routers. The pots disconnect-supervision command configures the disconnect method.	

Examples	The following example specifies that the connected devices apply the configured disconnect method for 100 milliseconds after a calling party disconnects: <pre>pots disconnect-time 100</pre>	

Related Commands	Command	Description
	pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
	pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
	pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
	pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).

Command	Description
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

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).

Defaults	The default depends on the setting of the pots country command. For more information, see the pots country command.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced on the Cisco 800 series routers.

Usage Guidelines	This command applies to Cisco 800 series routers.

Examples	The following example specifies that a telephone port can be rung 100 milliseconds after a previous call is disconnected: <pre>pots distinctive-ring-guard-time 100</pre>

Related Commands	Command	Description
	pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
	pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
	pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
	pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
	pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.

Command	Description
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
ring	Sets up a distinctive ring for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

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

alaw	International Telecommunication Union Telecommunication Standardization Section (ITU-T) PCM encoding scheme used to represent analog voice samples as digital values.
ulaw	North American PCM encoding scheme used to represent analog voice samples as digital values.

Defaults

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series routers.

Usage Guidelines

This command applies to Cisco 800 series routers.

Europe typically uses the **alaw** option. North America typically uses the **ulaw** option.

Examples

The following example specifies **alaw** as the PCM encoding scheme:

```
pots encoding alaw
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.

Command	Description
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

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

type1	Runs at 600 ohms.
type2	Runs at 900 ohms.
type3	Runs at 300 or 400 ohms.

Defaults

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series routers.

Usage Guidelines

This command applies to Cisco 800 series routers.

Examples

The following example specifies type1 as the line type:

```
pots line-type type1
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.

Command	Description
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

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	20Hz	Connected devices ring at 20 Hz.
	25Hz	Connected devices ring at 25 Hz.
	50Hz	Connected devices ring at 50 Hz.

Defaults	The default depends on the setting of the pots country command. For more information, see the pots country command.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced on the Cisco 800 series routers.

Usage Guidelines	This command applies to Cisco 800 series routers.

Examples	The following example specifies a ringing frequency of 50 Hz: <pre>pots ringing-freq 50Hz</pre>

Related Commands	Command	Description
	pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
	pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
	pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
	pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.

Command	Description
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

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*

Syntax Description	<i>interval</i>	Number from 0 to 10 (seconds).

Defaults	The default depends on the setting of the pots country command. For more information, see the pots country command.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced on the Cisco 800 series routers.

Usage Guidelines	This command applies to Cisco 800 series routers.

Examples	The following example specifies 10 seconds as the interval of silence:

```
pots silence-time 10
```

Related Commands	Command	Description
	pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
	pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
	pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
	pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
	pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).

Command	Description
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

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}

Syntax Description

local	Router supplies the tones.
remote	Telephone switch supplies the tones.

Defaults

The default setting is **local**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series routers.

Usage Guidelines

This command applies to Cisco 800 series routers.

This command applies only to ISDN lines connected to a EURO-ISDN (NET3) switch.

Examples

The following example specifies **remote** as the tone source:

```
pots tone-source remote
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.

Command	Description
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

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

Syntax Description	<i>seconds</i>	Delay, in seconds, before signaling begins. Valid values are from 0 to 10.

Defaults	The default setting is 1 second.

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.(7)T	This command was introduced on the Cisco 3600 series routers.
	12.0(2)T	This command was integrated into 12.0(2)T.

Usage Guidelines	This command applies to Cisco 3600 series routers.
	To disable the command, set the delay to 0. When an FXO interface begins to draw loop current (off-hook state), a delay is required between the initial flow of loop current and the beginning of signaling. Some devices initiate signaling too quickly, resulting in redial attempts. The pre-dial delay command allows a signaling delay.

Examples	The following example sets a predial delay value of 3 seconds on the FXO port of a Cisco 3600 series router:
	<pre>voice-port 1/0/0 pre-dial delay 3</pre>

Related Commands	Command	Description
	timeouts initial	Configures the initial digit timeout value for a specified voice port.
	timing delay-duration	Configures delay dial signal duration for a specified voice port.

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).

Defaults

0 (highest preference)

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(3)T	This command was supported on the Cisco 2600 series router and 3600 series routers.
12.0(4)T	Support was added for VoFR dial peers on the Cisco 2600 series router and 3600 series routers.

Usage Guidelines

This command applies to plain old telephone service (POTS) dial peers, Voice over IP (VoIP) dial peers, Voice over Frame Relay (VoFR) dial peers, and Voice over ATM (VoATM) dial peers on the Cisco MC3810 multiservice concentrator.

Use the **preference** command to indicate the preference order for matching dial peers in a rotary group. Setting the preference enables the desired dial peer to be selected when multiple dial peers within a hunt group are matched for a dial string.



Note

If POTS and voice-network peers are mixed in the same hunt group, the POTS dial peers must have priority over the voice-network dial peers.

Use this command with the Rotary Calling Pattern feature.

The hunting algorithm precedence is configurable. For example, if you wish a call processing sequence to go to destination A first, to destination B second, and to destination C third, you would assign preference (0 being the highest priority) to the destinations in the following order:

- Preference 0 to A
- Preference 1 to B
- Preference 2 to C

Examples

The following example configures POTS dial peer 10 with a preference of 1, POTS dial peer 20 with a preference of 2, and VoFR dial peer 30 to a preference of 3:

```
dial-peer voice 10 pots
 destination pattern 5552150
 preference 1
 exit
```

```
dial-peer voice 20 pots
 destination pattern 5552150
 preference 2
 exit
```

```
dial-peer voice 30 vofr
 destination pattern 5552150
 preference 3
 exit
```

The following examples show different dial peer configurations using the **preference** command:

Dialpeer	destpat	preference	session-target
1	4085551048	0 (highest)	jmmurphy-voip
2	408555	0	sj-voip
3	408555	1 (lower)	backup-sj-voip
4		1	0:D (interface)
5		0	anywhere-voip

If the destination number is 4085551048, the order of attempts will be 1, 2, 3, 5, 4:

Dialpeer	destpat	preference
1	408555	0
2	4085551048	1
3	4085551	0
4	4085551.....	0

If the number dialed is 4085551048, the order will be 2, 3, 4, 1.



Note

The default behavior is that the longest matching dial peer supersedes the preference value.

Related Commands	Command	Description
	called-number (dial-peer)	Enables an incoming VoFR call leg to get bridged to the correct POTS call leg when using a static FRF.11 trunk connection.
	codec (dial-peer)	Specifies the voice coder rate of speech for a Voice over Frame Relay dial peer.
	cptone	Specifies a regional analog voice interface-related tone, ring, and cadence setting.
	destination-pattern	Specifies the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
	dtmf-relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
	session protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.
	session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
	signal-type	Sets the signaling type to be used when connecting to a dial peer.

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.

Defaults	Null string

Command Modes	Dial-peer configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 series routers.
	12.0(4)XJ	This command was modified for store and forward fax and to add support on the Cisco AS5300 universal access server.
	12.1(1)T	Modifications in Cisco IOS Release 12.0(4)XJ were integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Use the **prefix** command to specify a prefix for a specific dial peer. When an outgoing call is initiated to this dial peer, the **prefix** *string* value is sent to the telephony interface first, before the telephone number associated with the dial peer.

If you want to configure different prefixes for dialed numbers on the same interface, you need to configure different dial peers.

This command is applicable only to plain old telephone service (POTS) dial peers. This command applies to off-ramp store and forward fax functions.

Examples

The following example specifies a prefix of 9 and then a pause:

```
dial-peer voice 10 pots
prefix 9,
```

Related Commands	Command	Description
	answer-address	Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call.
	destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer.

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

timeslots <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.

Defaults

There is no ISDN-PRI group configured.

Command Modes

Controller configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(2)T	This command was introduced for the Cisco MC3810 multiservice concentrator.
12.0(7)XK	This command was introduced for the Cisco 2600 and Cisco 3600 series routers.
12.1(2)T	The modifications in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The **pri-group** command applies to the configuration of Voice over Frame Relay and Voice over ATM on the Cisco MC3810 multiservice concentrator and the Cisco 2600 and Cisco 3600 series routers.

Before you enter the **pri-group** command, you must specify an ISDN-PRI switch type and an E1 or T1 controller.



Note

Only one PRI group can be configured on a controller.

Examples

The following example configures ISDN-PRI on all time slots of controller E1 on a Cisco 2600 series router:

```
controller E1 4/1
pri-group timeslots 1-7,16
```

Related Commands	Command	Description
	isdn switch-type	Configures the Cisco 2600 series router router PRI interface to support QSIG signaling.

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.
pbx-port <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.

Defaults

Port number 55000

Command Modes

Controller configuration

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5300 universal access server.
12.2(1)	This command was modified to add support for Setup messages from a POTS dial peer.

Usage Guidelines

This command is used only if the PBX in your configuration is an NEC PBX, and if you are configuring it to run FCCS and not QSIG signaling.

Examples

The following example shows how to configure this NEC PBX to use FCCS:

```
pri-group nec-fusion 172.31.255.255 pbx-port 60000
```

Related Commands

Command	Description
isdn protocol-emulate	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality.
isdn switch type	Configures the Cisco AS5300 universal access server PRI interface to support QSIG signaling.
show cdapi	Displays the CDAPI.
show rawmsg	Displays the raw messages owned by the required component.

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

setup	Sets the progress indicator for Setup messages.
connect	Sets the progress indicator for Connect messages.
progress	Sets the progress indicator for Progress messages.
alert	Sets the progress indicator for Alert messages.
enable	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 plain old telephone service (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.
disable	Disables the user configuration of the progress indicator.

Defaults

The default progress indicator from the switch is not intercepted or modified.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco 7500 series routers, Cisco MC3810 multiservice concentrator, and Cisco AS5300 and Cisco AS5800 universal access servers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(1)	This command was modified to add support for Setup messages from a POTS dial peer.

Usage Guidelines

The **progress_ind** command overrides the default progress indicator that is sent by the switch. This enables you to set the progress indicator at the H.323 gateway, if necessary, to ensure the proper end-to-end signaling for VoIP calls. This command sets the progress indicator only in messages from

outbound dial peers that have a set destination pattern, configured by using the **destination-pattern** command. If a message contains multiple progress indicators, the **progress_ind** command overrides only the first progress indicator in the message.

The **disable** and **no** forms of the **progress_ind** command have the same result: The call messages are not intercepted by the session application, and the default progress indicator, if any, is forwarded unmodified.

**Note**

A progress indicator that is configured by using the **progress_ind** command will not override the default progress indicator in a Progress message, if the Progress message is sent after backward cut-through has occurred (for example, because an Alert message with a progress indicator of 8 was sent before the Progress message).

Examples

The following example sets the progress indicator to 1 in Progress and Connect messages from the number 3 POTS dial peer:

```
dial-peer voice 3 pots
destination-pattern 55275
progress_ind progress enable 1
progress_ind connect enable 1
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and configures a VoIP or POTS dial peer.
destination-pattern	Specifies the telephone number that is used to identify the outbound dial peer for the call.

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.

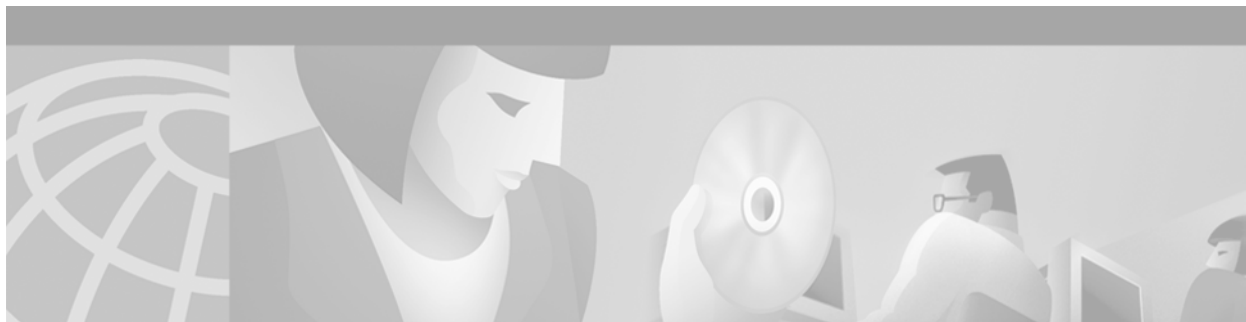
Defaults	Disabled

Command Modes	Global configuration

Command History	Release	Modification
	11.3(2)NA	This command was introduced on the Cisco 2500 series and Cisco 3600 series routers.

Usage Guidelines	If the multimedia interface is not enabled using the proxy h323 command, or if no gatekeeper is available, starting the proxy allows it to attempt to locate these resources. No calls will be accepted until the multimedia interface and the gatekeeper are found.

Examples	The following example turns on the proxy feature: proxy h323



Cisco IOS Voice, Video, and Fax Commands: R Through Sh

This chapter presents the commands to configure and maintain Cisco IOS voice, video, and fax applications. The commands are presented in alphabetical order beginning with R. Some commands required for configuring voice, video, and fax may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice, Video, and Fax Configuration Guide*.

register e164

To configure a gateway to register or deregister (remove the registration for) a fully qualified plain old telephone service (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 keywords or arguments.

Defaults

No E.164 addresses are registered until you enter this command.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.0(5)T	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

Use this command to register the E.164 address of an analog telephone line attached to a Foreign Exchange Station (FXS) port on a router. The gateway automatically registers fully qualified E164 addresses. Use the **no register e164** command to deregister an address. Use the **register e164** command to register a deregistered address.

Before you automatically or manually register an E.164 address with a gatekeeper, you must create a dial peer (using the **dial-peer** command), assign an FXS port to the peer (using the **port** command), and assign an E.164 address (using the **destination-pattern** command). The E.164 address must be a fully qualified address. For example, +5551212, 5551212, and 4085551212 are fully qualified addresses; 408555.... is not a fully qualified address. E.164 addresses are registered only for active interfaces—those that are not shut down. If an FXS port or its interface is shut down, the corresponding E.164 address is deregistered.



Tips

You can use the **show gateway** command to find out if the gateway is connected to a gatekeeper and if a fully qualified E.164 address is assigned to the gateway. Use the **zone-prefix** command at the gatekeeper to define prefix patterns, such as 408555....., that apply to one or more gateways.

Examples

The following command sequence places the gateway in dial-peer configuration mode, assigns an E.164 address to the interface, and registers that address with the gatekeeper:

```
dial-peer voice 111 pots
port 1/0/0
destination-pattern 5551212
register e164
```

The following commands deregister an address with the gatekeeper:

```
dial-peer voice 111 pots
no register e164
```

The following example shows that you must have a connection to a gatekeeper and define a unique E.164 address before you can register an address:

```
dial-peer voice 222 pots
port 1/0/0
destination 919555...
register e164
```

```
ERROR-register-e164:Dial-peer destination-pattern is not a full E.164 number
```

```
no gateway
dial-peer voice 111 pots
register e164
```

```
ERROR-register-e164:No gatekeeper
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dial-peer	Enters dial-peer configuration mode, defines the type of dial peer, and defines the tag number associated with a dial peer.
port	Enables an interface on a PA-4R-DTR to operate as a concentrator port.
show gateway	Displays the current gateway status.
zone prefix	Configures the gatekeeper with knowledge of its own prefix and the prefix of any remote zone.

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*

Syntax Description

<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.

Defaults

The default Nariwake service registered caller ring cadence is ring 1.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.1.(2)XF	The command registered-caller ring was introduced on the Cisco 800 series routers.

Usage Guidelines

If your ISDN line is provisioned for the I Number or dial-in services, you must also configure a dial peer by using the **destination-pattern not-provided** command. Either port 1 or port 2 can be configured under this dial peer. The router then forwards the incoming call to voice port 1. (See the “Examples” section below.)

If more than one dial peer is configured with the **destination-pattern not-provided** command, the router uses the first configured dial peer for the incoming calls. To display the Nariwake ring cadence setting, use the **show run** command.

Examples

The following example sets the ring cadence for registered callers to 2.

```
pots country jp
dial-peer voice 1 pots
  registered-caller ring 2
```


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

best-effort	Indicates that Resource Reservation Protocol (RSVP) makes no bandwidth reservation.
controlled-load	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.
guaranteed-delay	Indicates that RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded.

Defaults

best-effort

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.

Usage Guidelines

This command is applicable only to VoIP dial peers.

Use the **req-qos** command to request a specific quality of service to be used in reaching a dial peer. Like **acc-qos**, when you issue this command, the Cisco IOS software reserves a certain amount of bandwidth so that the selected quality of service can be provided. Cisco IOS software uses Resource Reservation Protocol (RSVP) to request quality of service guarantees from the network.

Examples

The following example configures **guaranteed-delay** as the desired (requested) quality of service to a dial peer:

```
dial-peer voice 10 voip
 req-qos guaranteed-delay
```

Related Commands

Command	Description
acc-qos	Defines the acceptable QoS for any inbound and outbound call on a VoIP dial peer.

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.

Defaults	No default behavior or values.	

Command Modes	Global configuration	

Command History	12.0(5)XE	This command was introduced on the Cisco 7200 series routers.
	12.0(7)T	This command was integrated into the Cisco IOS Release 12.0(7)T.

Examples	The following example displays the reset command configuration for DSP 1: reset 1 01:24:54:%DSPRM-5-UPDOWN: DSP 1 in slot 1, changed state to up	

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

Syntax Description	all	(Optional) Applies the high- and low- parameter settings to all monitored H.323 resources. This is the default condition.
	high <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.
	low <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 low parameter. The default is 90 percent.

Defaults	Reports low resources when 90 percent of resources are in use, and reports resource availability when resource use drops below 90 percent.

Command Modes	Gateway configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines	The resource threshold command defines the resource load levels that trigger Resource Availability Indicator (RAI) messages. To view the monitored resources, enter the show gateway command. The monitored H.323 resources include digital signal processor (DSP) channels and DS0s. Use the show call resource voice stats command to see the total amount of resources available for H.323 calls.

**Note**

The DS0 resources that are monitored for H.323 calls are limited to the ones that are associated with a voice POTS dial peer.

See the **dial-peer** configuration commands for details on how to associate a dial peer with a PRI or CAS group.

When any monitored H.323 resources exceed the threshold level defined by the **high** parameter, the gateway sends an RAI message to the gatekeeper with the AlmostOutOfResources field flagged. This message reports high resource usage.

When all gateway H.323 resources drop below the level defined by the **low** parameter, the gateway sends the RAI message to the gatekeeper with the AlmostOutOfResources field cleared.

When a gatekeeper can choose between multiple gateways for call completion, the gatekeeper uses internal priority settings and gateway resource statistics to determine which gateway to use. When all other factors are equal, a gateway that has available resources will be chosen over a gateway that has reported limited resources.

Examples

The following command defines the H.323 resource limits for a gateway:

```
resource threshold high 70 low 60
```

Related Commands

Command	Description
show call resource voice stats	Displays resource statistics for an H.323 gateway.
show call resource voice threshold	Displays the threshold configuration settings and status for an H.323 gateway.
show gateway	Displays the current gateway status.

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*

Syntax Description

<i>number</i>	Response waiting time in seconds.

Defaults

The default response timeout is one (1) second.

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and the Cisco AS5300 universal access server.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

If no response is received within the response-timeout time limit, the current connection ends, and the router attempts to contact the next service point.

Examples

The following example illustrates a response-timeout set to 1 second.

```
settlement 0
  response-timeout 1
```

Related Commands

Command	Description
connection-timeout	Configures the time for which a connection is maintained after completion of a communication exchange.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
retry-delay	Sets the time between attempts to connect with the settlement provider.
retry-limit	Sets the maximum number of attempts to connect to the provider.

Command	Description
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement mode and specifies the attributes specific to a settlement provider.
show settlement	Displays the configuration for all settlement server transactions.
shutdown/no shutdown	Deactivates the settlement provider/activates the settlement provider.
type	Configures an SAA-RTR operation type.
url	Specifies the Internet service provider address.

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**

Syntax Description

<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.

Defaults

The default retry delay is two seconds.

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 and 3600 series routers and the Cisco AS5300 universal access server.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

After exhausting all service points for the provider, the router is delayed for the specified length of time before resuming connection attempts.

Examples

The following example sets a retry value of 15 seconds:

```
settlement 0
  relay-delay 15
```

Related Commands

Command	Description
connection-timeout	Configures the time for which a connection is maintained after completion of a communication exchange.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response-timeout	Configures the maximum time to wait for a response from a server.
retry-limit	Sets the maximum number of attempts to connect to the provider.

Command	Description
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.
show settlement	Displays the configuration for all settlement server transactions.
shutdown/no shutdown	Deactivates the settlement provider/activates the settlement provider.
type	Configures an SAA-RTR operation type.

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.

Defaults

The default retry limit is one (1) retry.

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

If no connection is established after the configured retries, the router ceases connection attempts. The retry limit number does not count the initial connection attempt. A retry limit of one (default) results in a total of two connection attempts to every service point.

Examples

The following example sets the number of retries to 1:

```
settlement 0
retry-limit 1
```

Related Commands

Command	Description
connection-timeout	Configures the time for which a connection is maintained after a communication exchange is complete.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response-timeout	Configures the maximum time to wait for a response from a server.
retry-delay	Sets the time between attempts to connect with the settlement provider.

Command	Description
session-timeout	Sets the length of interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement mode and specifies the attributes specific to a settlement provider.
show settlement	Displays the configuration for all settlement server transactions.
shutdown	Brings up the settlement provider.
type	Configures an SAA-RTR operation type.

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

invite <i>number</i>	Number of INVITE retries: 1 through 10 are valid inputs; default = 6.
response <i>number</i>	Number of RESPONSE retries: 1 through 10 are valid inputs; default = 6.
bye <i>number</i>	Number of BYE retries: 1 through 10 are valid inputs; default = 10.
cancel <i>number</i>	Number of CANCEL retries: 1 through 10 are valid inputs; default = 10.

Defaults

invite: 6
response: 6
bye: 10
cancel: 10

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.

Usage Guidelines

To reset this command to the default value, you can also use the **default** command.

Examples

In the following example, the number of invite retries has been set to 5.

```
sip-ua
retry invite 5
```

Related Commands

Command	Description
sip-ua	Enables the sip-ua configuration commands, with which you configure the user agent.

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	cadence-number	Number from 0 through 2: - Type 0 is a primary ringing cadence—default ringing cadence for the country your router is in. - Type 1 is a distinctive ring—0.8 seconds on, 0.4 seconds off, 0.8 seconds on, 0.4 seconds off. - 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.

Defaults	The default is 0.

Command Modes	Interface configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced on the Cisco 800 series router.

Usage Guidelines	This command applies to Cisco 800 series routers. You can specify this command when creating a dial peer. This command will not work if it is not specified within the context of a dial peer. For information on creating a dial peer, refer to the <i>Cisco 800 Series Routers Software Configuration Guide</i>.

Examples	The following example specifies the type 1 distinctive ring: <pre>ring 1</pre>

Related Commands	Command	Description
	destination-pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
	dial-peer voice	Enters dial-peer configuration mode, defines the type of dial peer, and defines the tag number associated with a dial peer.
	no call-waiting	Disables call waiting.
	port (dial-peer)	Enables an interface on a PA-4R-DTR port adapter to operate as a concentrator port.
	pots distinctive-ring-guard-time	Specifies a delay in which a telephone port can be rung after a previous call is disconnected (for Cisco 800 series routers).
	ring	Sets up a distinctive ring for telephones, fax machines, or modems connected to a Cisco 800 series router.
	show dial-peer voice	Displays configuration information and call statistics for dial peers.

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. pattern01—2 seconds on, 4 seconds off pattern02—1 second on, 4 seconds off pattern03—1.5 seconds on, 3.5 seconds off pattern04—1 second on, 2 seconds off pattern05—1 second on, 5 seconds off pattern06—1 second on, 3 seconds off pattern07—0.8 second on, 3.2 seconds off pattern08—1.5 seconds on, 3 seconds off pattern09—1.2 seconds on, 3.7 seconds off pattern09—1.2 seconds on, 4.7 seconds off pattern11—0.4 second on, 0.2 second off, 0.4 second on, 2 seconds off pattern12—0.4 second on, 0.2 second off, 0.4 second on, 2.6 seconds off
define	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.

Defaults

Ring cadence defaults to the pattern you specify with the **cptone** command.

Command Modes Voice-port configuration

Command History	Release	Modification
	11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.
	12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series routers, and the patternXX keyword was introduced.
	12.1(2)T	This command was integrated into the 12.1(2)T release.

Usage Guidelines The **patternXX** keyword provides preset ring cadence patterns for use on any platform. The **define** keyword allows you to create a custom ring cadence. On the Cisco 2600 and 3600 series routers, only one or two pairs of digits can be entered under the **define** keyword.

Examples The following example configures the ring cadence for 1 second on and 4 seconds off on voice port 1/1 on a Cisco MC3810 multiservice concentrator:

```
voice-port 1/1
 ring cadence pattern02
```

The following example configures the ring cadence for 1 second on, 1 second off, 1 second on, and 5 seconds off on voice port 1/2 on a Cisco MC3810 multiservice concentrator:

```
voice-port 1/2
 ring cadence define 10 10 10 50
```

The following example configures the ring cadence for 1 second on and 2 seconds off on voice port 1/0/0 on a Cisco 2600 or 3600 series router:

```
voice-port 1/0/0
 ring cadence pattern04
```

Related Commands	Command	Description
	ring frequency	Specifies the ring frequency for a specified FXS voice port.
	cptone	Specifies the default tone, ring, and cadence settings according to country.

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.

Defaults

25 Hz on the Cisco 3600 series routers and 20 Hz on the Cisco MC3810 multiservice concentrators.

Command Modes

Voice-port configuration

Command History

Release

Modification

11.3(1)T

This command was introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

Use the **ring frequency** command to select a specific ring frequency for an FXS voice port. Use the **no** form of this command to reset the default value. The ring frequency you select must match the connected equipment. If set incorrectly, the attached phone might not ring or might buzz. In addition, the ring frequency is usually country-dependent. You should take into account the appropriate ring frequency for your area before configuring this command.

This command does not affect ringback, which is the ringing a user hears when placing a remote call.

Examples

The following example configures the ring frequency on the Cisco 3600 series for 25 Hz:

```
voice-port 1/0/0
 ring frequency 25
```

The following example configures the ring frequency on the Cisco MC3810 multiservice concentrator for 20 Hz:

```
voice-port 1/1
 ring frequency 20
```


Related Commands	Command	Description
	ring cadence	Specifies the ring cadence for an FXS voice port on the Cisco MC3810 multiservice concentrator.
	ring number	Specifies the number of rings for a specified FXO voice port.

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

<i>number</i>	Number of rings detected before answering the call. Valid entries are numbers from 1 to 10. The default is 1.

Defaults

One ring

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series router.

Usage Guidelines

Use the **ring number** command to set the maximum number of rings to be detected before answering a call over an FXO voice port. Use the **no** form of this command to reset the default value, which is one ring.

Normally, this command should be set to the default so that incoming calls are answered quickly. If you have other equipment available on the line to answer incoming calls, you might want to set the value higher to give the equipment sufficient time to respond. In that case, the FXO interface would answer if the equipment online did not answer the incoming call in the configured number of rings.

This command is not applicable to Foreign Exchange Station (FXS) or E&M interfaces because they do not receive ringing on incoming calls.

Examples

The following example on the Cisco 3600 series sets five rings as the maximum number of rings to be detected before closing a connection over this voice port:

```
voice-port 1/0/0
 ring number 5
```

The following example on the Cisco MC3810 multiservice concentrator sets five rings as the maximum number of rings to be detected before closing a connection over this voice port:

```
voice-port 1/1
 ring number 5
```

Related Commands

Command	Description
ring frequency	Specifies the ring frequency for a specified FXS voice port.

roaming (dial-peer)

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.

Defaults	No roaming

Command Modes	Dial-peer configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.

Usage Guidelines	Enable the roaming capability of a dial peer if that dial peer can terminate roaming calls. If a dial peer is dedicated to local calls only, disable the roaming capability.

The roaming dial peer must work with a roaming service provider. If the dial peer allows a roaming user to go through, and the service provider is not roaming-enabled, the call fails.

Examples	The following example enables the roaming capability for the dial peer:

```
dial-peer voice 10 voip
roaming
```

Related Commands	Command	Description
	roaming (settlement)	Enables the roaming capability for a settlement provider.
	settle-call	Limits the dial peer to using only the specific clearinghouse identified by the specified <i>provider-number</i> .
	settlement roam-pattern	Configures a pattern to match against when determining roaming.

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.

Defaults	No roaming

Command Modes	Settlement configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.

Usage Guidelines	Enable roaming capability of a settlement provider if that provider can authenticate a roaming user and route roaming calls.
	A roaming call is successful only if both the settlement provider and the outbound dial peer for that call are roaming-enabled.

Examples	The following example enables the roaming capability for the settlement provider:
	<pre>settlement 0 roaming</pre>

Related Commands	Command	Description
	roaming (dial-peer mode)	Enables the roaming capability for the dial peer.
	settle-call	Limits the dial peer to using only the specific clearinghouse identified by the specified <i>provider-number</i> .
	settlement roam-pattern	Configures a pattern to match against when determining roaming.

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	<i>number</i>	Specifies how long, in minutes, to keep the record.
Defaults	10 minutes	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco AS5300 universal access server.
Examples	The following example sets the RTSP session history to 500 minutes: <pre>rtsp client session history duration 500</pre>	
Related Commands	Command	Description
	call application voice load	Allows reload of an application that was loaded via the MGCP scripting package.
	rtsp client session history records	Specifies the number of RTSP client session history records kept during the session.
	show call application voice	Displays all TCL or MGCP scripts that are loaded.
	show rtsp client session	Displays cumulative information about the RTSP session records.

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	<i>number</i>	Specifies the number of records to retain in a session history. Values range from 1 to 100000.

Defaults	50 records

Command Modes	Global configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco AS5300 universal access server.

Examples	The following example sets the RTSP client history to 500 records: rtsp client session history records 500

Related Commands	Command	Description
	call application voice load	Allows reload of an application that was loaded via the MGCP scripting package.
	rtsp client session history duration	Specifies the how long the RTSP is kept during the session.
	show call application voice	Displays all TCL or MGCP scripts that are loaded.

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 international , national , subscriber , abbreviated , unknown , and any , as defined by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) 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 international , national , subscriber , abbreviated and unknown , as defined by the ITU Q.931 specification.



Note

In the syntax description above, the square brackets indicate optional values. When using this command, do not include these square brackets as part of the syntax. They are not valid parameters in the **rule** command. The square brackets can only be used in actual syntax for such commands as the **destination-pattern** and **incoming called-number** commands, where the syntax specifically allows this delimiter.

Defaults

No default behavior or values.

Command Modes

Translation-rule configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced for Voice over IP on the Cisco AS5300 universal access server.
12.0(7)XKs	This command was first supported for Voice over IP on the following platforms: Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrators.

Release	Modification
12.1(1)T	This command was first supported on the T train for Voice over IP on the following platforms: Cisco 1750 routers, Cisco 2600 and 3600 series routers, Cisco AS5300 universal access servers, Cisco 7200 series routers, and Cisco 7500 series routers.
12.1(2)T	This command was first supported for Voice over IP on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

When configuring your dial peers, you are provided with an option called the *translation rule*. This option applies a translation rule to a calling party number (Automatic Number Identification [ANI]) or a called party number (Dial Number Information Service [DNIS]) for both incoming and outgoing calls within Cisco H.323 voice-enabled gateways. Also, the rule allows translation of the *type of number*.

Examples

The following example applies a translation rule. If a called number starts with 5552205 or 52205, then translation rule 21 will use the rule command to forward the number to 14085552205 instead.

```
translation-rule 21
rule 1 555.% 1408555 subscriber international
rule 2 7.% 1408555 abbreviated international
```

In the next example, if a called number is either 14085552205 or 014085552205, then after the execution of the translation rule 345, the forwarding digits will be 52205. If the match type is configured and the type is not “unknown,” then the dial peer matching will be required to match input string numbering type.

```
translation-rule 345
rule 1 .%555.% 7 any abbreviated
```

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
test translation-rule	Tests the execution of the translation rules on a specific name tag.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

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		
any		Uses the first alias of an incoming registration, admission, and status (RAS) protocol registration, regardless of its type, as the means of identifying the user to RADIUS/TACACS+.
h323-id		Uses the first H.323 ID type alias as the means of identifying the user to RADIUS/TACACS+.
e164		Uses the first E.164 address type alias as the means of identifying the user to RADIUS/TACACS+.
password default <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.
password separator <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.

Defaults No default

Command Modes Gatekeeper configuration

Command History	Release	Modification
	11.3(2)NA	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers.

Usage Guidelines Use the **security** command to enable identification of registered aliases by RADIUS/TACACS+. If the alias does not exist in RADIUS/TACACS+, the endpoint will not be allowed to register.

A RADIUS/TACACS+ server and encryption key must have been configured in Cisco IOS software for security to work.

Only the first alias of the proper type will be identified. If no alias of the proper type is found, the registration will be rejected.

This command does not allow you to define the password mechanism unless the security type (**h323-id** or **e164** or **any**) has been defined. Although the **no security password** command undefines the password mechanism, it leaves the security type unchanged, so security is still enabled. However, the **no security** command disables security entirely, including removing any existing password definitions.

Examples

The following example enables identification of registrations using the first H.323 ID found in any registration:

```
security h323id
```

The following example enables security, authenticating all users by using their H.323-IDs and a password of qwerty2x:

```
security h323-id  
security password qwerty2x
```

The next example enables security, authenticating all users by using their H.323-IDs and the password entered by the user in the H.323-ID alias he or she registers:

```
security h323-id  
security password separator !
```

Now if a user registers with an H.323-ID of joe!024aqx, the gatekeeper authenticates user joe with password 024aqx, and if that is successful, registers the user with the H.323-ID of joe. If the exclamation point is not found, the user is authenticated with the default password, or a null password if no default has been configured.

The following example enables security, authenticating all users by using their E.164 IDs and the password entered by the user in the H.323-ID alias he or she registers:

```
security e164  
security password separator !
```

Now if a user registers with an E.164 address of 5551212 and an H.323-ID of !hs8473q6, the gatekeeper authenticates user 5551212 and password hs8473q6. Because the H.323-ID string supplied by the user begins with the separator character, no H.323-ID is registered, and the user is known only by the E.164 address.

Related Commands

Command	Description
accounting (gatekeeper)	Enables the accounting security feature on the gatekeeper.
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

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.

Defaults

Disabled

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco 2600 and 3600 series routers and the Cisco MC3810 multiservice concentrator.
12.0(4)T	This command was integrated into the Cisco IOS Release 12.0(4)T.

Usage Guidelines

Sequence numbers on voice packets allow the digital signal processor (DSP) at the playout side to detect lost packets, duplicate packets, or out-of-sequence packets. This helps the DSP to mask out occasional drop-outs in voice transmission at the cost of one extra byte per packet. The benefit of using sequence numbers versus the cost in bandwidth of adding an extra byte to each voice packet on the Frame Relay network must be weighed to determine whether to disable this function for your application.

Another factor to consider is that this command does not affect codecs that require a sequence number, such as G.726. If you are using a codec that requires a sequence number, the DSP will generate one regardless of the configuration of this command.

Examples

The following example shows how to disable the generation of sequence numbers for VoFR frames on a Cisco 2600 series or 3600 series router or on a Cisco MC3810 multiservice concentrator for VoFR dial peer 200, starting from global configuration mode:

```
dial-peer voice 200 vofr
no sequence-numbers
```

Related Commands	Command	Description
	called-number (dial-peer)	Enables an incoming VoFR call leg to get bridged to the correct POTS call leg when using a static FRF.11 trunk connection.
	codec (dial-peer)	Specifies the voice coder rate of speech for a Voice over Frame Relay dial peer.
	cptone	Specifies a regional analog voice interface-related tone, ring, and cadence setting.
	destination-pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
	dtmf-relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
	session protocol (Voice over Frame Relay)	Establishes a session protocol for calls between the local and remote routers via the packet network.
	session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
	signal-type	Sets the signaling type to be used when connecting to a dial peer.

server (RLM)

To identify an RLM server, use the **server** RLM configuration command. To remove the identification, use the **no** form of this command

server *name-tag*

no server *name-tag*

Syntax Description	<i>name-tag</i>	Name to identify the server configuration so that multiple entries of server configuration can be entered.

Defaults	Disabled

Command Modes	RLM configuration

Command History	Release	Modification
	11.3(7)	This command was introduced.

Usage Guidelines	Each server can have multiple entries of IP addresses or aliases.

Examples	The following example identifies the RLM server and defines the associated IP addresses:

```
rlm group 1
  server rl-server
  link address 10.1.4.1 source Loopback1 weight 4
  link address 10.1.4.2 source Loopback2 weight 3
```

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

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.

server registration-port *port number*

no server registration-port *port number*

Syntax Description

<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.

Defaults

The registration port of the gatekeeper is not configured, so no external server can register with this gatekeeper.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

Use this command to configure a server registration port to poll for servers that want to establish connections with the gatekeeper on this router.



Note

The **no** form of this command forces the gatekeeper on this router to close the listen socket, so it cannot accept more registrations. However, existing connections between the gatekeeper and servers are left open.

Examples

The following example shows how a listener port for a server is established for connection with a gatekeeper:

```
server registration-port 20000
```

Related Commands

Command	Description
server trigger	Configure static server triggers for specific RAS messages to be forwarded to a specified server.

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
```

Syntax Description		
all		Specified to delete all command-line interface configured triggers.
arq, lcf, lrj, lrq, rrq, urq		Registration, admission, and status (RAS) protocol 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.

Defaults No server triggers are set.

Command Modes Gatekeeper configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced on the Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines Use this command to configure a static server trigger. There are six different server triggers—one for each of the RAS messages. To configure a trigger, go to its submode where a set of subcommands are used to trigger a condition. See the following examples.

In ARQ submode, enter the following syntax:

```
server trigger arq gkid priority server-id server-ipaddress server-port
```

In LCF submode, enter the following syntax:

```
server trigger lcf gkid priority server-id server-ipaddress server-port
```

In LRJ submode, enter the following syntax:

```
server trigger lrj gkid priority server-id server-ipaddress server-port
```

In LRQ submode, enter the following syntax:

```
server trigger lrq gkid priority server-id server-ipaddress server-port
```

In RRQ submode, enter the following syntax:

```
server trigger rrq gkid priority server-id server-ipaddress server-port
```

In URQ submode, enter the following syntax:

```
server trigger urq gkid priority server-id server-ipaddress server-port
```

The following options are available in all submodes:

<i>info-only</i>	Information only—no need to wait for acknowledgment.
<i>shutdown</i>	Enter this subcommand to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward.

The *destination-info* argument is under the ARQ, LRQ, LCF, and LRJ submode and has the following options:

<i>destination-info</i>	Configure <i>destination-info</i> to trigger one of the following conditions:
e164	Configure an E.164 pattern.
email-id	Configure an email ID.
h323-id	Configure an H.323 ID.
word	When configuring the e164 address option, the email-id option, or the h323-id option above, the E.164 address can end in a trailing '.', 's', or '*'.

The *redirect-reason* argument is under the ARQ and LRQ submodes and has the following options:

<i>redirect-reason</i>	Configure a <i>redirect-reason</i> to trigger on (range of 0 through 65535) with the following reserved values:
0	Unknown reason.
1	Call forwarding busy or called DTE busy.
2	Call forwarded no reply.
4	Call deflection.
9	Called DTE out of order.
10	Call forwarding by the call DTE.
15	Call forwarding unconditionally.

The *remote-ext-address* argument is under the LCF trigger submode and has the following options:

<i>remote-ext-address</i>	Configure remote extension addresses, with the following options:
e164	Configure an E.164 pattern.
word	When configuring the e164 address option, the email-id option, or the h323-id option above, the E.164 address can end in a trailing ‘., ‘s, or ‘*’.

The *endpoint-type* argument is under the RRQ and URQ trigger submodes and has the following options:

<i>endpoint-type</i>	Configure the type of endpoint to trigger, with the following options:
gatekeeper	The endpoint is an H.323 gatekeeper.
h320-gateway	The endpoint is an H.320 gateway.
mcu	The endpoint is a multipoint control unit (MCU).
other-gateway	The endpoint is another type of gateway not specified on this list.
proxy	The endpoint is a H.323 proxy.
terminal	The endpoint is an H.323 proxy.
voice-gateway	The endpoint is a voice gateway.

The **supported-prefix** keyword is under the RRQ and URQ submodes and has the following options:

supported-prefix	Configure the gateway technology prefix to trigger on.
word	Enter a word within the set of “0123456789#*” when configuring the E.164 pattern for a gateway technology prefix.

Entering the **no** form of the server trigger command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a server trigger on gatekeeper sj.xyz.com to notify external server “Server-123” of any call to an E.164 number that starts with 1800 followed by any 7 digits (1800551212, for example):

```
Gatekeeper
  server trigger arq sj.xyz.com 1 Server-123 1.14.93.130 1751
    destination-info e164 1800.....
  exit
```

Related Commands

Command	Description
server registration port	Configure a gatekeeper listening port to listen for external server connections.
show gatekeeper servers	Show a list of currently registered and statically configured triggers on this gatekeeper router.

session

To associate a transport session with a specified session-group, use the **session group** command in backhaul session manager configuration mode. It is assumed that the server is located on a remote machine. To delete the session, use the **no** form of this command.

session group *group-name remote_ip remote_port local_ip local_port priority*

no session group *group-name remote_ip remote_port local_ip local_port priority*

Syntax Description		
group		Specifies the session-group name.
<i>group-name</i>		Session-group name.
<i>remote_ip</i>		Remote IP address.
<i>remote_port</i>		Remote port number. Range is 1024 through 9999.
<i>local_ip</i>		Local IP address.
<i>local_port</i>		Local port number. Range is 1024 through 9999.
<i>priority</i>		Priority of the session-group. Range is 0 through 9999 and 0 is the highest priority.

Defaults	No default behavior or values.

Command Modes	Backhaul session manager configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced.
	12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.

Examples	To associate a transport session with the session-group Group5 and specify the parameters described above, see the following example: <pre>Router(config-bsm) # session group group5 161.44.2.72 5555 172.18.72.198 5555 1</pre>

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

cisco	Configure the dial peer to use proprietary Cisco VoIP session protocol.
sipv2	SIP users should use this option. This option configures the VoIP dial peer to use IETF SIP.
aal2-trunk	AAL2 nonswitched trunk session protocol.
smtp	Specifies Simple Mail Transfer Protocol (SMTP) session protocol.

Defaults

No default behaviors or values.

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series router.
12.0(4)XJ	This command was modified for store-and-forward fax on the Cisco AS5300 universal access server.
12.1(1)T	The sipv2 option was added.
12.1(1)XA	Support was added for VoATM dial peers on the Cisco MC3810 multiservice concentrator with the aal2-trunk keyword.
12.1(2)T	Modifications to this command in Cisco IOS Release 12.1(1)XA were integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The keyword **cisco** is applicable only to VoIP on the Cisco 3600 series routers. The keyword **aal2-trunk** is applicable only to VoATM on the Cisco MC3810 multiservice concentrator.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following is an example of configuring a VoIP dial peer for H.323 or SIP as the session protocol for VoIP call signaling:

```
dial-peer voice 102 voip
 session protocol sipv2
```

The following example selects AAL2 trunking as the session protocol on a Cisco MC3810 multiservice concentrator:

```
dial-peer voice 10 voatm
 session protocol aal2-trunk
```

The following example selects Cisco Session Protocol as the session protocol on a Cisco 3600 series router:

```
dial-peer voice 20 voip
 session protocol cisco
```

The following example selects SMTP as the session protocol:

```
dial-peer voice 10 mmoup
 session protocol smtp
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice-related encapsulation.
session target (VoIP)	Configures a network-specific address for a dial peer.

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

cisco-switched	Specifies proprietary Cisco VoFR session protocol. (This is the only valid session protocol for the Cisco 7200 series.)
frf11-trunk	Specifies FRF.11 session protocol.

Defaults

cisco-switched

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced for VoIP.
12.0(3)XG	This command was modified to support VoFR on the Cisco 2600, 3600, and 7200 series routers and the Cisco MC3810 multiservice concentrator.
12.0(4)T	The cisco-switched and frf11-trunk keywords were added for VoFR dial peers.

Usage Guidelines

For Cisco-to-Cisco dial peer connections, Cisco recommends that you use the default session protocol because of the advantages it offers over a pure FRF.11 implementation. When connecting to FRF.11-compliant equipment from other vendors, use the FRF.11 session protocol.



Note

When using the FRF.11 session protocol on Cisco 2600 series and 3600 series routers, you must also use the **called-number** command.

Examples

The following example shows how to configure the FRF.11 session protocol on a Cisco 2600 series or 3600 series router for VoFR dial peer 200:

```
dial-peer voice 200 vofr
  session protocol frf11-trunk
  called-number 5552150
```

The following example shows how to configure the FRF.11 session protocol on a Cisco MC3810 multiservice concentrator for VoFR dial peer 200:

```
dial-peer voice 200 vofr
  session protocol frf11-trunk
```

Related Commands	Command	Description
	called-number (dial-peer)	Enables an incoming VoFR call leg to get bridged to the correct POTS call leg when using a static FRF.11 trunk connection.
	codec (dial-peer)	Specifies the voice coder rate of speech for a Voice over Frame Relay dial peer.
	cptone	Specifies a regional analog voice interface-related tone, ring, and cadence setting.
	destination-pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
	dtmf-relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
	preference	Indicates the preferred order of a dial peer within a rotary hunt group.
	session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
	signal-type	Sets the signaling type to be used when connecting to a dial peer.

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 keywords or arguments.

Defaults	There is no default setting for this command.

Command Modes	Voice-service configuration

Command History	Release	Modification
	12.1(1)XA	This command was introduced on the Cisco MC3810 multiservice concentrator.
	12.1(2)T	This command was integrated into the 12.1(2)T release.

Usage Guidelines	This command applies to VoATM on the MC3810 multiservice concentrator. In the voice-service-session configuration mode for AAL2, you can configure only AAL2 features, such as call admission control and subcell multiplexing.

Examples	The following example shows how to access the voice-service-session configuration mode, beginning in global configuration mode: <pre>voice service voatm session protocol aal2</pre>

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

There are no keywords or arguments.

Defaults

When this command is not implemented, the default session protocol is **cisco**.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.1(2)XH	This command was introduced on Cisco 2600 and Cisco 3600 series routers for the Cisco Hoot and Holler over IP application.
12.1(3)T	This command was integrated into the Cisco IOS Release 12.1(3)T.

Usage Guidelines

Use the **session protocol multicast** dial-peer configuration command for voice conferencing in a Hoot and Holler networking implementation. This command allows more than two ports to join the same session simultaneously. It is supported on Cisco 2600 and Cisco 3600 series routers.

Examples

The following example shows the use of the **session protocol multicast** dial-peer configuration command in context with its accompanying commands:

```
dial-peer voice 111 voip
 destination-pattern 111
 session protocol multicast
 session target ipv4:237.111.0.111:2222
 ip precedence 5
 codec g711ulaw
```

Related Commands

Command	Description
session target ipv4	Assigns the session target for voice-multicasting dial peers.

session target (VoATM)

To specify a network-specific address for a specified VoATM 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.

Cisco 3600 Series 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

Syntax Description		
serial		Specifies the serial interface for the dial-peer address.
atm		Specifies the ATM interface. The only valid number is 0.
<i>interface</i>		Interface type and interface number on the router.
pvc		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>name</i>		The PVC name.
<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.

Defaults The default for this command is enabled with no IP address or domain name defined.

Command Modes Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(1)MA	Support was added for VoATM, VoHDL, and POTS dial peers on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	Support was added for VoATM dial peers on the Cisco 3600 series routers. Support for VoHDL on the Cisco MC3810 multiservice concentrator was removed.
12.1(2)T	Support was added for VoATM on Cisco MC3810 multiservice concentrators.

Usage Guidelines

Use the **session target** command to specify a network-specific address or domain name for a dial peer. Whether you select a network-specific address or a domain name depends on the session protocol you select. The syntax of this command complies with the simple syntax of mailto: as described in RFC 1738.

The **session target loopback** command is used for testing the voice transmission path of a call. The loopback point will depend on the call origin and the loopback type selected.

This command applies to on-ramp store-and-forward fax functions.

You must enter the **session protocol aal2-trunk** dial-peer configuration command before you can specify a *cid* for a dial peer for VoATM on the Cisco MC3810 multiservice concentrator.

**Note**

This command does not apply to plain old telephone service (POTS) dial peers.

Examples

The following example configures a session target for Voice over ATM on a Cisco MC3810 multiservice concentrator. The session target is sent to ATM interface 0, and for a PVC with a VCI of 20.

```
dial-peer voice 12 voatm
 destination-pattern 13102221111
 session target atm0 pvc 20
```

The following example delivers fax-mail to multiple recipients:

```
dial-peer voice 10 mmoip
 session target marketing-information@mailers.example.com
```

Assuming that mailers.example.com is running sendmail, you can put the following information into its /etc/aliases file:

```
marketing-information:
 john@example.com,
 fax=+14085551212@sj-offramp.example.com
```

The following example displays configuring a session target for Voice over ATM on the Cisco 3600 series. The session target is sent to ATM interface 0, and is for a PVC with a VPI/VCI of 1/100.

```
dial-peer voice 12 voatm
 destination-pattern 13102221111
 session target atm1/0 pvc 1/100
```

Related Commands

Command	Description
called-number	Enables an incoming VoFR call leg to be bridged to the correct POTS call leg.
codec (dial-peer)	Specifies the voice coder rate of speech for a dial peer.
cptone	Specifies a regional tone, ring, and cadence setting for an analog voice port.
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer.
dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred selection order of a dial peer within a hunt group.
session protocol	Establishes a VoFR protocol for calls between the local and the remote routers via the packet network.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

session target (VoFR)

To specify a network-specific address for a specified VoFR 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.

Cisco 2600 and 3600 Series Routers Voice over Frame Relay Dial Peers

session target *interface dlc* [*cid*]

no session target

Cisco MC3810 Multiservice Concentrator Voice over Frame Relay Dial Peers

session target *interface dlc* [*cid*]

no session target

Cisco 7200 Series Routers Voice over Frame Relay Dial Peers

session target *interface dlc*

no session target

Syntax Description	<i>interface</i>	Specifies the serial interface and interface number (slot number and port number) associated with this dial peer. For the range of valid interface numbers for the selected interface type, enter a ? character after the interface type.
	<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 frf11-trunk . When the session protocol is cisco-switched , 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.

Defaults The default for this command is enabled with no IP address or domain name defined.

Command Modes Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(1)MA	Support was added for VoFR, VoHDL, and POTS dial peers on the Cisco MC3810 multiservice concentrator.
12.0(3)XG	Support was added for VoFR dial peers on the Cisco 2600 series and 3600 series routers. The <i>cid</i> option was added.
12.0(4)T	Support was added for VoFR and POTS dial peers on the Cisco 7200 series routers and the support added in Cisco IOS Release 12.0(3)XG was integrated into Cisco IOS Release 12.0(4)T.

Usage Guidelines

Use the **session target** command to specify a network-specific address or domain name for a dial peer. Whether you select a network-specific address or a domain name depends on the session protocol you select. The syntax of this command complies with the simple syntax of mailto: as described in RFC 1738.

The **session target loopback** command is used for testing the voice transmission path of a call. The loopback point will depend on the call origin and the loopback type selected.

For VoFR dial peers, the *cid* option is not allowed when the **cisco-switched** option for the **session protocol** command is used.

Examples

The following example configures a session target for Voice over Frame Relay on a Cisco MC3810 multiservice concentrator with a session target on serial port1 and a DLCI of 200:

```
dial-peer voice 11 vofr
destination-pattern 13102221111
session target serial1 200
```

The following example shows how to configure serial interface 1/0, DLCI 100 as the session target for VoFR dial peer 200 (an FRF.11 dial peer) on a Cisco 2600 series or 3600 series router, starting from global configuration mode and using the FRF.11 session protocol:

```
dial-peer voice 200 vofr
destination-pattern 13102221111
called-number 5552150
session protocol frf11-trunk
session target serial 1/0 100 20
```

The following example delivers fax-mail to multiple recipients:

```
dial-peer voice 10 mmoip
session target marketing-information@mailers.example.com
```

Assuming that mailers.example.com is running sendmail, you can put the following information into its */etc/aliases* file:

```
marketing-information:
john@example.com,
fax=+14085551212@sj-offramp.example.com
```

Related Commands	Command	Description
	called-number	Enables an incoming VoFR call leg to be bridged to the correct POTS call leg.
	codec (dial-peer)	Specifies the voice coder rate of speech for a dial peer.
	cptone	Specifies a regional tone, ring, and cadence setting for an analog voice port.
	destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer.
	dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
	preference	Indicates the preferred selection order of a dial peer within a hunt group.
	session protocol	Establishes a VoFR protocol for calls between the local and the remote routers via the packet network.
	signal-type	Sets the signaling type to be used when connecting to a dial peer.

session target (VoIP)

To specify a network-specific address for a specified VoIP 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.

Cisco 2600 and Cisco 3600 Series Routers and Cisco MC8310 Multiservice Concentrator Voice over IP Dial Peers

```
session target { ipv4:destination-address | dns:[$s$. | $d$. | $e$. | $u$.] host-name | loopback:rtp
| loopback:compressed | loopback:uncompressed | ras | settlement }
```

```
no session target
```

Cisco AS5300 Universal Access Server Voice over IP Dial Peers

```
session target { ipv4:destination-address | dns:[$s$. | $d$. | $e$. | $u$.] host-name | loopback:rtp
| loopback:compressed | loopback:uncompressed | mailto: { name | $d$ } @domain-name |
ipv4:destination-address | dns:[$s$. | $d$. | $u$. | $e$.] host-name }
```

```
no session target
```

Cisco AS5800 Universal Access Server Voice over IP Dial Peers

```
session target { ipv4:destination-address | dns:[$s$. | $d$. | $e$. | $u$.] host-name | loopback:rtp
| loopback:compressed | loopback:uncompressed }
```

```
no session target
```

Syntax Description

ipv4:destination-address	IP address of the dial peer.
dns:[<i>\$s\$...</i>] host-name	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: <i>\$s\$</i>.—Indicates that the source destination pattern will be used as part of the domain name. <i>\$d\$</i>.—Indicates that the destination number will be used as part of the domain name. <i>\$e\$</i>.—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. <i>\$u\$</i>.—Indicates that the unmatched portion of the destination pattern (such as a defined extension number) will be used as part of the domain name.
loopback:rtp	Indicates that all voice data will be looped back to the source. This is applicable for VoIP peers.
loopback:compressed	Indicates that all voice data will be looped back in compressed mode to the source. This is applicable for POTS peers.

■ session target (VoIP)

loopback:uncompress d	Indicates that all voice data will be looped-back in uncompressed mode to the source. This is applicable for POTS peers.
ras	Indicates that the registration, admission, and status (RAS) signaling function protocol is being used, meaning that a gatekeeper will be consulted to translate the E.164 address into an IP address.
settlement <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.

Defaults

The default state for this command is enabled, with no IP address or domain name defined.

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers.
12.0(3)T	Support was added for VoIP and POTS dial peers on the Cisco AS5300 universal access server. The parameter was added for RAS.
12.0(4)XJ	Support was added for store-and-forward fax on the Cisco AS5300 universal access server platform.
12.1(1)T	Support was added for session target <i>type</i> of settlement .

Usage Guidelines

Use the **session target** command to specify a network-specific address or domain name for a dial peer. Whether you select a network-specific address or a domain name depends on the session protocol you select.

The **session target loopback** command is used for testing the voice transmission path of a call. The loopback point will depend on the call origin and the loopback type selected.

The **session target dns** command can be used with or without the specified wildcards. Using the optional wildcards can reduce the number of VoIP dial peer session targets you must configure if you have groups of numbers associated with a particular router.

Use the **session target ras** command to specify that the RAS protocol is being used to determine the IP address of the session target.

In Cisco IOS Release 12.1(1)T the **session target** command configuration cannot combine the target of RAS with the **settle-call** command. When configuring the VoIP dial peers for a settlement server, if **session target** *type* is **settlement**, the *provider-number* parameter in the **session target** and **settle-call** commands should be identical.

When the VoIP dial peers are configured for a settlement server, if the **session target** *type* is **settlement**, the *provider-number* parameter in the **session target** and **settle-call** commands should be identical.

Examples

The following example configures a session target using DNS for a host, “voice_router,” in the domain cisco.com:

```
dial-peer voice 10 voip
```

```
session target dns:voice_router.cisco.com
```

The following example configures a session target using DNS, with the optional **\$u\$**. wildcard. In this example, the destination pattern has been configured to allow for any four-digit extension, beginning with the numbers 1310222. The optional wildcard **\$u\$**. indicates that the router will use the unmatched portion of the dialed number—in this case, the four-digit extension—to identify the dial peer. As in the preceding example, the domain is “cisco.com.”

```
dial-peer voice 10 voip
 destination-pattern 1310222...
 session target dns:$u$.cisco.com
```

The following example configures a session target using DNS, with the optional **\$d\$**. wildcard. In this example, the destination pattern has been configured for 13102221111. The optional wildcard **\$d\$**. indicates that the router will use the destination pattern to identify the dial peer in the “cisco.com” domain.

```
dial-peer voice 10 voip
 destination-pattern 13102221111
 session target dns:$d$.cisco.com
```

The following example configures a session target using DNS, with the optional **\$e\$**. wildcard. In this example, the destination pattern has been configured for 12345. The optional wildcard **\$e\$**. indicates that the router will reverse the digits in the destination pattern, add periods between the digits, and then use this reverse-exploded destination pattern to identify the dial peer in the “cisco.com” domain.

```
dial-peer voice 10 voip
 destination-pattern 12345
 session target dns:$e$.cisco.com
```

The following example configures a session target using RAS:

```
dial-peer voice 11 voip
 destination-pattern 13102221111
 session target ras
```

The following example configures a session target using settlement:

```
session target settlement:0
```

Related Commands

Command	Description
called-number	Enables an incoming VoFR call leg to be bridged to the correct POTS call leg.
codec (dial-peer)	Specifies the voice coder rate of speech for a dial peer.
cptone	Specifies a regional tone, ring, and cadence setting for an analog voice port.
dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred selection order of a dial peer within a hunt group.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer.
session protocol	Establishes a session protocol for calls between the local and remote routers through the packet network in Voice over IP.
settle-call	Specifies that settlement is to be used for this dial peer, regardless of session target type.

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	Configure the SIP dial peer to use the UDP transport layer protocol. This is the default.
tcp	Configure the SIP dial peer to use the TCP transport layer protocol.

Defaults

The SIP dial peer uses UDP.



Note

The transport protocol specified with the **transport** command and the one specified with the **session transport** command must be the same.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.

Usage Guidelines

Use **show sip-ua status** to ensure that the transport protocol that you set using the **session transport** command matches the protocol set using the **transport** command.

Examples

The following example shows a VoIP dial peer configured to use UDP as the underlying transport layer protocol for SIP messages:

```
dial-peer voice 102 voip
  session transport udp
```

set

To create a fault-tolerant or non-fault-tolerant session-set with the client or server option, use the **set** command in backhaul session manager configuration mode. To delete the set, use the **no** form of this command.

```
set set-name { client | server } { ft | nft }
```

```
no set set-name { client | server } { ft | nft }
```

Syntax Description

<i>set-name</i>	Session-set name.
client	Client option. The session-set should only be configured as client for backhaul.
server	Server option.
ft	Fault-tolerant. Fault-tolerance is the level of ability within a system to operate properly even if a group in the set fails.
nft	Non-fault-tolerant. Only one group is allowed in a non-fault-tolerant set.

Defaults

No default behavior or values.

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

There can be multiple groups associated with a session-set.

The session-set should only be configured for the client for backhaul (not the server).

A set cannot be deleted unless the groups associated with the set are deleted first.

Examples

To specify the client set named Set1 to fault-tolerant, see the following example:

```
Router(config-bsm)# set set1 client ft
```

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.

Defaults

No default behavior or values.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.

Usage Guidelines

Using the **session target** command, a dial peer can determine the address of the terminating gateway through the **ipv4**, **dns**, **ras**, and **settlement** keywords.

If the session target is not **settlement**, and the **settle-call** *provider-number* argument is set, the gateway resolves the terminating gateway's address using the specified method and then requests the settlement server to authorize that address and create a settlement token for that particular address. If the server cannot authorize the terminating gateway address suggested by the gateway, the call fails.

Do not combine the session target types **ras** and **settle-call**. Combination of session target types is not supported in Cisco IOS Release 12.1(1)T.

Examples

The following example sets a call to be authorized with a settlement server that uses the address resolution method specified in the **session target**:

```
dial-peer voice 10 voip
 destination-pattern 1408.....
 session target ipv4:172.22.95.14
 settle-call 0
```

Related Commands

Command	Description
session target	Specifies a network-specific address for a specified dial peer.

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	<i>provider-number</i>	Specifies a digit that defines a particular settlement server. The only valid entry is 0.

Defaults	0

Command Modes	Global configuration

Command History	Release	Modification
	12.0(4)XH1	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines	The variable <i>provider-number</i> defines a particular settlement provider. For Cisco IOS Release 12.1, only one clearinghouse per system is allowed, and the only valid value for <i>provider-number</i> is 0.

Examples	This example shows how to enter settlement configuration mode: settlement 0

Related Commands	Command	Description
	connection-timeout	Configures the length of time for which a connection is maintained after a communication exchange is completed.
	customer-id	Identifies a carrier or ISP with a settlement provider.
	device-id	Specifies a gateway associated with a settlement provider.
	encryption	Sets the encryption method to be negotiated with the provider.
	max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
	response-timeout	Configures the maximum time to wait for a response from a server.
	retry-delay	Sets the time between attempts to connect with the settlement provider.
	retry-limit	Sets the connection retry limit.

Command	Description
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
show settlement	Displays the configuration for all settlement server transactions.
shutdown	Brings up the settlement provider.
type	Configures an SAA-RTR operation type.

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.
roaming no roaming	Determines whether a user is roaming.

Defaults

No default pattern

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.

Usage Guidelines

Multiple “roam patterns” could be entered on one gateway.

Examples

The following example will configure a pattern that determines if a user is roaming:

```
settlement 0 roam-pattern 1222 roam
settlement 0 roam-pattern 1333 noroam
settlement roam-pattern 1444 roam
settlement roam-pattern 1555 noroam
```

Related Commands

Command	Description
roaming (settlement)	Enables the roaming capability for a settlement provider.
settlement	Enters settlement configuration mode.

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.

Defaults

The SGCP daemon is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

When the SGCP daemon is not active, all SGCP messages are ignored.

When you enter the **no sgcp** command, the SGCP process is removed.



Note

After you enter the **no sgcp** command, you must save the configuration and reboot the router for the disabling of SGCP to take effect.

Examples

The following example shows the SGCP daemon being enabled:

```
sgcp
```

The following example shows the SGCP daemon being disabled:

```
no sgcp
```

Related Commands

Command	Description
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp call-agent

To define the IP address of the default Simple Gateway Control Protocol (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.

Defaults

No IP address is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

Setting this command defines the IP address of the default SGCP call agent to which the router sends an initial RSIP (Restart In Progress) packet when the router boots up. This is used for initial boot-up only before the SGCP call agent contacts the router acting as the gateway.

When you enter the **no sgcp call-agent** command, only the IP address of the default SGCP call agent is removed.

Examples

The following example shows SGCP being enabled and the IP address of the call agent being specified:

```
sgcp
sgcp call-agent 209.165.200.225
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

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.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
	12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
	12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines Once you issue this command, all requests for new connections (CreateConnection requests) are denied. All existing calls are maintained until users terminate them, or until you enter the **no sgcp** command. When the last active call is terminated, the SGCP daemon is terminated, and all resources allocated to it are released.

Examples The following example shows all new calls being blocked and existing calls being terminated:

```
sgcp graceful-shutdown
```

Related Commands	Command	Description
	sgcp	Starts and allocates resources for the SGCP daemon.
	sgcp call-agent	Defines the IP address of the default SGCP call agent.
	sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
	sgcp modem passthru	Enables SGCP modem or fax pass-through.

Command	Description
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband Tse for fax/modem operation.

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*

Syntax Description

<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.

Defaults

3,000 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only, and was not generally available.
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Examples

The following example shows the maximum wait delay value set to 40 milliseconds:

```
sgcp max-waiting-delay 40
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.

Command	Description
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband Tse for fax/modem operation.

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}
```

Syntax Description

ca	Uses the call agent controlled modem upspeed method violation message.
cisco	Uses a Cisco-proprietary upspeed method based on the protocol.
nse	Uses the NSE-based modem upspeed method.

Defaults

SGCP modem or fax pass-through is disabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 multiservice concentrator and Cisco 3600 series routers (except the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

You can use this command for fax pass-through because the answer tone can come from either modem or fax transmissions. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions.

If you use the **nse** option, you must also configure the **sgcp tse payload** command.

Examples

The following example shows SGCP modem pass-through configured using the call agent upspeed method:

```
sgcp modem passthru ca
```

The following example shows SGCP modem pass-through configured using the proprietary Cisco upspeed method:

```
sgcp modem passthru cisco
```

The following example shows SGCP modem pass-through configured using the NSE-based modem upspeed:

■ sgcp modem passthru

```
sgcp modem passthru nse
sgcp tse payload 110
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband Tse for fax/modem operation.

sgcp quarantine-buffer disable

To disable the Simple Gateway Control Protocol (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.

Defaults

The SGCP quarantine buffer is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

The SGCP quarantine buffer is the mechanism for buffering the SGCP events between two RQNT messages.

Examples

The following example shows the SGCP quarantine buffer being disabled:

```
sgcp quarantine-buffer disable
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.

Command	Description
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband Tse for fax/modem operation.

sgcp request retries

To specify the number of times to retry sending “notify” and “delete” messages to the Simple Gateway Control Protocol (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

Syntax Description

<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.

Defaults

The default for the number of times a “notify” and “delete” message is retransmitted to the SGCP call agent before it is dropped is 3

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

The actual retry count may be different from the value you enter for this command. The retry count is also limited by the call agent. If there is no response from the call agent after 30 seconds, the gateway will not retry anymore, even though the number set using the **sgcp request retries** command has not been reached.

The router will stop sending retries after 30 seconds, regardless of the setting for this command.

Examples

The following example shows the system configured to send the **sgcp** command 10 times before dropping the request:

```
sgcp request retries 10
```

Related Commands	Command	Description
	sgcp	Starts and allocates resources for the SGCP daemon.
	sgcp call-agent	Defines the IP address of the default SGCP call agent.
	sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
	sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
	sgcp modem passthru	Enables SGCP modem or fax pass-through.
	sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
	sgcp request timeout	Specifies how long the system should wait for a response to a request.
	sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
	sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
	sgcp timer	Configures how the gateway detects the RTP stream host.
	sgcp tse payload	Enables Inband Tse for fax/modem operation.

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

Syntax Description	<i>timeout</i>	Specifies the number of milliseconds to wait for a response to a request. Valid range is from 1 to 10,000.

Defaults	500 milliseconds

Command Modes	Global configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
	12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
	12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines	This command is used for “notify” and “delete” messages, which are sent to the SGCP call agent.

Examples	The following example shows the system configured to wait 40 milliseconds for a reply to a request: <pre>sgcp request timeout 40</pre>

Related Commands	Command	Description
	sgcp	Starts and allocates resources for the SGCP daemon.
	sgcp call-agent	Defines the IP address of the default SGCP call agent.
	sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
	sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
	sgcp modem passthru	Enables SGCP modem or fax pass-through.
	sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.

Command	Description
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband Tse for fax/modem operation.

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 <i>delay</i>	Specifies the restart delay timer value in milliseconds. The valid range is from 0 to 600, and the default value is 0.
	notify	Enables the restart notification upon the SGCP/digital interface state transition.

Defaults	Zero (0)

Command Modes	Global configuration

Command History	Release	Modification
	12.0(7)XK	This command was introduced on the Cisco MC3810 multiservice concentrator and Cisco 3600 series routers (except the Cisco 3620) in a private release that was not generally available.
	12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines	This command is used to send RSIP messages from the router to the SGCP call agent. The RSIP messages are used to synchronize the router and the call agent. RSIP messages are also sent when the sgcp command is entered to enable the SGCP daemon.
	You must enter the notify option to enable RSIP messages to be sent.

Examples	The following example shows the system configured to wait 40 milliseconds before restarting SGCP: <pre>sgcp restart delay 40</pre>
	The following example shows the system configured to send an RSIP notification to the SGCP call agent when the T1 controller state changes: <pre>sgcp restart notify</pre>

Related Commands	Command	Description
	sgcp	Starts and allocates resources for the SGCP daemon.
	sgcp call-agent	Defines the IP address of the default SGCP call agent.
	sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
	sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
	sgcp modem passthru	Enables SGCP modem or fax pass-through.
	sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
	sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
	sgcp request timeout	Specifies how long the system should wait for a response to a request.
	sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
	sgcp timer	Configures how the gateway detects the RTP stream host.
	sgcp tse payload	Enables Inband Tse for fax/modem operation.

sgcp retransmit timer

To configure the Simple Gateway Control Protocol (SGCP) retransmission timer to use a random algorithm, 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.

Defaults

The SGCP retransmission timer does not use the random algorithm.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco 3600 and Cisco MC3810 multiservice concentrator in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

Use this command to enable the random algorithm component of the retransmission timer. For example, if the retransmission timer is set to 200 milliseconds, the first retransmission timer is 200 milliseconds, but the second retransmission timer picks up a timer value randomly between either 200 or 400. The third retransmission timer picks up a timer value randomly of 200, 400, or 800 as shown below:

- First retransmission timer: 200
- Second retransmission timer: 200 or 400
- Third retransmission timer: 200, 400, or 800
- Fourth retransmission timer: 200, 400, 800, or 1600
- Fifth retransmission timer: 200, 400, 800, 1600, or 3200 and so on.

After 30 seconds, the retransmission timer no longer retries.

Examples

The following example shows the retransmission timer set to use the random algorithm:

```
sgcp retransmit timer random
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband Tse for fax/modem operation.

sgcp timer

To configure how the gateway detects the Real-Time Transport Protocol (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 <i>timer</i>	Sets the multiples of the RTP Control Protocol (RTCP) transmission interval in milliseconds. The valid range is from 1 to 100, and the default is 5.
rtp-nse <i>timer</i>	Sets the multiples of the RTP named signaling event (NSE) timeout in milliseconds. The valid range is from 100 to 3000, and the default is 200.

Defaults

Default for **receive-rtcp** *timer* is 5.

Default for **rtp-nse** *timer* is 200.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

The RTP NSE timer is used for proxy ringing (the ringback tone is provided at the originating gateway).

Examples

The following example shows the **receive-rtcp** *timer* set to 100 milliseconds:

```
sgcp timer receive-rtcp 100
```

The following example shows the **rtp-nse** *timer* set to 1000 milliseconds:

```
sgcp timer rtp-nse 1000
```

Related Commands	Command	Description
	sgcp	Starts and allocates resources for the SGCP daemon.
	sgcp call-agent	Defines the IP address of the default SGCP call agent.
	sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
	sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
	sgcp modem passthru	Enables SGCP modem or fax pass-through.
	sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
	sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
	sgcp request timeout	Specifies how long the system should wait for a response to a request.
	sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
	sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
	sgcp tse payload	Enables Inband TSE for fax/modem operation.

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*

Syntax Description

<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.

Defaults

Zero (0)

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 multiservice concentrator and Cisco 3600 series routers (except the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

Because this command is disabled by default, you must specify a TSE payload type.

If you configure the **sgcp modem passthru** command to the **nse** value, then you must configure this command.

Examples

The following example shows the Simple Gateway Control Protocol (SGCP) modem pass-through set using the NSE-based modem upspeed and the Inband Telephony Signaling Events payload value set to 110:

```
sgcp modem passthru nse
sgcp tse payload 110
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.

Command	Description
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.up or down so that the call agent can synchronize
sgcp timer	Configures how the gateway detects the RTP stream host.

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* }

Syntax Description		
all		Displays International Telecommunication Union Telecommunication Standardization Sector (ITU-T), ATM Forum, and custom AAL2 profiles configured on the system.
itut		Displays ITU-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: • 1 = G.711 u-law • 2 = G.711 u-law with silence insertion descriptor (SID) • 7 = G.711 u-law and G.729ar8 For ATMF: None. ATMF is not supported. For custom: • 100 = G.711 u-law and G.726r32 • 110 = G.711 u-law, G.726r32, and G.729ar8
custom		Displays custom profiles configured on the system.
atmf		Displays ATM Forum profiles configured on the system.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(1)XA	This command was introduced on the Cisco MC3810 multiservice concentrator.
	12.1(2)T	This command was integrated into the 12.1(2)T release.

Usage Guidelines

This command applies to AAL2 Voice over ATM (VoATM) applications on the Cisco MC3810 multiservice concentrator.

Use the **show aal2 profile** EXEC command to display the AAL2 profiles configured in the system.

Examples

The following is sample output from the **show aal2 profile** command for displaying all the profiles configured in the system:

```
Router# show aal2 profile all
```

■ **show aal2 profile**

Printing all the Profiles in the system

```

Profile Type: ITUT Profile Number: 1 SID Support: 0
Red enable: 1 Num entries: 1
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 15

Profile Type: ITUT Profile Number: 2 SID Support: 1
Red enable: 1 Num entries: 1
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 15

Profile Type: custom Profile Number: 100 SID Support: 1
Red enable: 1 Num entries: 2
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 7
Coding type: g726r32 Packet length: 40 UUI min: 8 UUI max: 15

Profile Type: ITUT Profile Number: 7 SID Support: 1
Red enable: 1 Num entries: 2
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 15
Coding type: g729ar8 Packet length: 10 UUI min: 0 UUI max: 15

Profile Type: custom Profile Number: 110 SID Support: 1
Red enable: 1 Num entries: 3
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 7
Coding type: g726r32 Packet length: 40 UUI min: 8 UUI max: 15
Coding type: g729ar8 Packet length: 30 UUI min: 8 UUI max: 15

```

Table 26 provides an alphabetical listing of the fields in this output and a description of each field.

Table 26 *show aal2 profile Field Descriptions*

Field	Description
Profile Type	Category of codec types configured on DSP. Possible types are ITU-T, ATMF, and custom.
ITUT Profile Number	Predefined combination of one or more codec types configured for a digital signal processor (DSP).
SID Support	Silence insertion descriptor.
Red enable	Redundancy enable for type3 packets.
Num entries	Number of profile elements.
Coding type	Voice compression algorithm.
Packet length	Sample size.
UUI min	Minimum sequence number on the voice packets.
UUI max	Maximum sequence number on the voice packets.

Related Commands

Command	Description
codec aal2-profile	Sets the codec profile for a DSP on a per-call basis.

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 keywords or arguments.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(5)XK	This command was introduced for the Cisco MC3810 multiservice concentrator.
	12.0(7)T	Cisco IOS Release 12.0(5)XK was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines	Enter this command to review ATM interface NSAP addresses that have been assigned with the atm video aesa command and to ensure that ATM management is confirmed for those addresses.

Examples	On a Cisco MC3810 multiservice concentrator, the following example displays ATM interface NSAP addresses:

Router# **show atm video-voice address**

nsap address	type	ilmi status
47.0091810000000002F26D4901.00107B4832E1.FE	VOICE_AAL5	Confirmed
47.0091810000000002F26D4901.00107B4832E1.C8	VIDEO_AAL1	Confirmed

Related Commands	Command	Description
	codec aal2-profile	Sets the codec profile for a DSP on a per-call basis.

show backhaul-session-manager group

To display status, statistics, or configuration information for all available session-groups, use the **show backhaul-session-manager group** command in privileged EXEC mode.

show backhaul-session-manager group { status | stats | cfg } { all | name *group-name* }

Syntax Description

status	Displays status information for session-groups.
stats	Displays statistics for session-groups.
cfg	Displays configuration information for session-groups.
all	Displays information for all available session-groups.
name <i>group-name</i>	Displays information for a specific session-group. The <i>group-name</i> argument specifies the name of the session-group.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

The following displays statistics for all session-groups:

```
Router# show backhaul-session-manager group stats all
Session-Group grp1 statistics
  Successful Fail-Overs      :0
  Un-Successful Fail-Over attempts:0
  Active Pkts receive count  :0
  Standby Pkts receive count :0
  Total PDUs dispatch err    :0
```

The following displays the current configuration for all session-groups:

```
Router# show backhaul-session-manager group cfg all
Session-Group
  Group Name :grp1
  Set Name   :set1
  Sessions   :3
  Dest:10.5.0.3 8304 Local:10.1.2.15 8304 Priority:0
  Dest:10.5.0.3 8300 Local:10.1.2.15 8300 Priority:2
  Dest:10.5.0.3 8303 Local:10.1.2.15 8303 Priority:2
  RUDP Options
    timer cumulative ack :100
    timer keepalive      :1000
    timer retransmit     :300
    timer transfer state :2000
    receive max          :32
```

```
cumulative ack max    :3
retrans max           :2
out-of-sequence max   :3
auto-reset max        :5
```

The following displays the current status of all session-groups. This group named grp1 belongs to the set named set1.

The Status will be either Group-OutOfService (no session in the group has been established) or Group-Inservice (at least one session in the group has been established).

The Status(use) will be either Group-Standby (the VSC connected to the other end of this group will go into standby mode), Group-Active (the VSC connected to the other end of this group will be the active VSC), or Group-None (the VSC has not declared its intent yet).

```
Router# show backhaul-session-manager group status all
Session-Group
Group Name      :grp1
Set Name        :set1
Status          :Group-OutOfService
Status (use)    :Group-None
```

Related Commands

Command	Description
show backhaul-session-manager session	Displays status, statistics, or configuration of sessions.
show backhaul-session-manager set	Displays session-groups associated with a specific or all session-sets.

show backhaul-session-manager session

To display various information for about a session or sessions, use the **show backhaul-session-manager session** command in privileged EXEC mode.

show backhaul-session-manager session { all | ip *ip_address* }

Syntax Description	all	All available sessions.
	ip <i>ip_address</i>	The IP address of the local or remote session.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced.

Examples To display information for all available sessions, see the following example.

The State will be OPEN (the connection is established), OPEN_WAIT (the connection is awaiting establishment), OPEN_XFER (session failover is in progress for this session, which is a transient state), or CLOSE (this session is down, also a transient state). The session will move to OPEN_WAIT after waiting a fixed amount of time.

The Use-status field indicates whether PRI signaling traffic is currently being transported over this session . The field will be either OOS (this session is not being used to transport signaling traffic) or IS (this session is being used currently to transport all PRI signaling traffic). OOS does not indicate if the connection is established and IS indicates that the connection is established.

```
Router# show backhaul-session-manager session all

Session information --
Session-id:35
  Group:grp1 /*this session belongs to the group named 'grp1' */
Configuration:
  Local:10.1.2.15      , port:8303
  Remote:10.5.0.3      , port:8303
  Priority:2
  RUDP Option:Client, Conn Id:0x2
State:
  Status:OPEN_WAIT, Use-status:OOS, /*see explanation below */
Statistics:
  # of resets:0
  # of auto_resets 0
  # of unexpected RUDP transitions (total) 0
  # of unexpected RUDP transitions (since last reset) 0
  Receive pkts - Total:0 , Since Last Reset:0
  Recieve failures - Total:0 ,Since Last Reset:0
  Transmit pkts - Total:0, Since Last Reset:0
```



```
Transmit Failures (PDU Only)
  Due to Blocking (Not an Error) - Total:0, Since Last Reset:0
  Due to causes other than Blocking - Total:0, Since Last
Reset:0
Transmit Failures (NON-PDU Only)
  Due to Blocking(Not an Error) - Total:0, Since Last Reset:0
  Due to causes other than Blocking - Total:0, Since Last
Reset:0
RUDP statistics
  Open failures:0
  Not ready failures:0
  Conn Not Open failures:0
  Send window full failures:0
  Resource unavailble failures:0
  Enqueue failures:0
```

Related Commands

Command	Description
show backhaul-session-manager group	Displays status, statistics, or configuration of a specified or all session-groups.
show backhaul-session-manager set	Displays session-groups associated with a specified or all session-sets.

show backhaul-session-manager set

To display session-groups associated with a specified session-set or all session-sets, use the **show backhaul-session-manager set** command in privileged EXEC mode.

show backhaul-session-manager set { all | name *session-set-name* }

Syntax Description	all	All available session-sets.
	name <i>session-set-name</i>	A specified session-set.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced.

Examples	To show session groups associated with all session-sets, see the following example:
	Router# show backhaul-session-manager set all

Related Commands	Command	Description
	show backhaul-session-manager group	Displays status, statistics, or configuration of a specified or all session-groups.
	show backhaul-session-manager session	Displays status, statistics, or configuration of a session or all sessions.

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]

Syntax Description	voice	Specifies that information be displayed for all active voice calls.
	fax	Specifies that information be displayed for all active fax calls.
	brief	(Optional) Displays a truncated version of the active call information.

Defaults	No default behavior or values.

Command Modes	User EXEC or Privileged EXEC

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 2600 series and 3600 series.
	12.0(3)XG	Support for VoFR was added.
	12.0(4)XJ	This command was modified for store-and-forward fax on the Cisco AS5300 universal access server.
	12.0(4)T	This command was first supported on the Cisco 7200 series.
	12.0(7)XK	This command was first supported on the Cisco MC3810 multiservice concentrator.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
	12.1(3)T	This command was modified for Modem Passthrough over VoIP on the Cisco AS5300 universal access server.

Usage Guidelines	Use the show call active command to display the contents of the active call table. This command displays information about call times, dial peers, connections, quality of service, and other status and statistical information. If you use the voice keyword, information is displayed about all voice calls currently connected through the router or access server. If you use the fax keyword, information is displayed about all fax calls currently connected.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

See Table 19 for a listing of the information types associated with this command.

Examples

The following is sample output from the **show call active voice** command:

```
Router# show call active voice

GENERIC:
SetupTime=104443 ms
Index=1
PeerAddress=50110
PeerSubAddress=
PeerId=100
PeerIfIndex=104
LogicalIfIndex=10
ConnectTime=104964
CallDuration=00:02:43
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=2
TransmitPackets=15720
TransmitBytes=2362904
ReceivePackets=15670
ReceiveBytes=2737904
TELE:
ConnectionId=[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
TxDuration=155310 ms
VoiceTxDuration=155310 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
NoiseLevel=-75
ACOMLevel=11
OutSignalLevel=-13
InSignalLevel=-22
InfoActivity=2
ERLLevel=27
SessionTarget=
ImgPages=0
GENERIC:
SetupTime=104648 ms
Index=1
PeerAddress=55240
PeerSubAddress=
PeerId=2
PeerIfIndex=105
LogicalIfIndex=0
ConnectTime=104964
CallDuration=00:02:47
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=2
TransmitPackets=16026
TransmitBytes=2608248
ReceivePackets=16075
ReceiveBytes=2609164
VOIP:
ConnectionId[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
RemoteIPAddress=1.14.82.14
RemoteUDPPort=18202
RoundTripDelay=2 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=TRUE

SessionProtocol=cisco
```

```

SessionTarget=ipv4:1.14.82.14
OnTimeRvPlayout=40
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=67 ms
LoWaterPlayoutDelay=67 ms
ReceiveDelay=67 ms
LostPackets=0 ms
EarlyPackets=0 ms
LatePackets=0 ms
VAD = enabled
CoderTypeRate=g729r8
CodecBytes=20
SignalingType=cas

Modem passthrough signaling method is nse:
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 157sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec

```

The following is sample output from the **show call active voice brief** command:

```

Router# show call active voice brief

<ID>: <start>hs.<index> +<connect> pid:<peer_id> <dir> <addr> <state>
dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes>
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
delay:<last>/<min>/<max>ms <codec>
MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
last <buf event time>s dur:<Min>/<Max>s
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
sig:<on/off> <codec> (payload size)
ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
sig:<on/off> <codec> (payload size)
Tele <int>: tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm

3      : 104443hs.1 +521 pid:100 Answer 50110 active
dur 00:03:28 tx:20151/3036404 rx:20102/3517936
Tele 0:D:1: tx:199630/199630/0ms g711ulaw noise:-75 acom:11 i/o:-22/-13 dBm

3      : 104648hs.1 +316 pid:2 Originate 55240 active
dur 00:03:28 tx:20102/3276712 rx:20151/3277628
IP 1.14.82.14:18202 rtt:3ms pl:40/0ms lost:0/0/0 delay:67/67/67ms g729r8
MODEMPASS nse buf:0/0 loss 0% 0/0 last 195s dur:0/0s

```

The following is sample output from the **show call active fax** command:

```

Router# show call active fax

GENERIC:
SetupTime=22021 ms
Index=1
PeerAddress=wook song
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=24284

```

```

CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=10
TransmitPackets=0
TransmitBytes=0
ReceivePackets=0
ReceiveBytes=41190

MMOIP:
ConnectionId[0x37EC7F41 0xB0110001 0x0 0x35C34]
RemoteIpAddress=0.0.0.0
SessionProtocol=SMTP
SessionTarget=
MessageId=
AccountId=
ImgEncodingType=MH
ImgResolution=fine
AcceptedMimeTypes=2
DiscardedMimeTypes=1
Notification=None

GENERIC:
SetupTime=23193 ms
Index=1
PeerAddress=527....
PeerSubAddress=
PeerId=3469
PeerIfIndex=157
LogicalIfIndex=30
ConnectTime=24284
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=10
TransmitPackets=5
TransmitBytes=6513
ReceivePackets=0
ReceiveBytes=0

TELE:
ConnectionId=[0x37EC7F41 0xB0110001 0x0 0x35C34]
TxDuration=24010 ms
FaxTxDuration=10910 ms
FaxRate=14400
NoiseLevel=-1
ACOMLevel=-1
OutSignalLevel=0
InSignalLevel=0
InfoActivity=0
ERLLevel=-1
SessionTarget=
ImgPages=0

```

The following is sample output from the **show call active fax brief** command:

Router# **show call active fax brief**

```

<ID>: <start>hs.<index> +<connect> pid:<peer_id> <dir> <addr> <state> \
  tx:<packets>/<bytes> rx:<packets>/<bytes> <state>
IP <ip>:<udp> rt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  sig:<on/off> <codec> (payload size)

```

```
Tele <int>: tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm
```

```
1      : 22021hs.1 +2263 pid:0 Answer wook song active
tx:0/0 rx:0/41190
IP 0.0.0.0 AcceptedMime:2 DiscardedMime:1
```

```
1      : 23193hs.1 +1091 pid:3469 Originate 527.... active
tx:10/13838 rx:0/0
Tele : tx:31200/10910/20290ms noise:-1 acom:-1 i/0:0/0 dBm
```

Table 27 provides an alphabetical listing of the fields displayed in the output from the **show call active** command and a description of each field.

Table 27 *show call active Field Descriptions*

Field	Description
ACOM Level	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceler, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
Buffer Drain Events	Total number of jitter buffer drain events.
Buffer Fill Events	Total number of jitter buffer fill events.
CallDuration	Length of the call in hours, minutes, and seconds, hh:mm:ss.
CallOrigin	Call origin: answer or originate.
CallState	Current state of the call.
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size in bytes for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time at which the call was connected.
Consecutive-packets-lost Events	Total number of consecutive (two or more) packet-loss events.
Corrected packet-loss Events	Total number of packet loss events that were corrected using the RFC 2198 method.
Dial-Peer	Tag of the dial peer sending this call.
ERLLevel	Current Echo Return Loss (ERL) level for this call.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.

Table 27 *show call active Field Descriptions (continued)*

Field	Description
GapFillWithPrediction	Duration of the voice signal played out with signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser or frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
HiWaterPayoutDelay	High-water mark Voice Payout FIFO Delay during this call.
Index	Dial peer identification number.
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call, for example, voice or fax.
InSignalLevel	Active input signal level from the telephony interface used by this call.
Last Buffer Drain/Fill Event	Time since the last jitter buffer drain or fill event, in seconds.
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPayoutDelay	Low water mark Voice Payout FIFO Delay during this call.
Modem passthrough signaling method in use	Indicates that this is a modem pass-through call and that named signaling events (NSEs)—also called <i>telephone-events</i> in RFC 2833—are used for signaling codec 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.
NoiseLevel	Active noise level for this call.
OnTimeRvPayout	Duration of voice payout from data received on time for this call. Derive the Total Voice Payout Duration for Active Voice by adding the OnTimeRvPayout value to the GapFill values.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
Percent Packet Loss	Total percent packet loss.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average Payout FIFO Delay plus the Decoder Delay during this voice call.
ReceivePackets	Number of packets received by this peer during this call.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system UDP listener port to which voice packets are sent.

Table 27 *show call active Field Descriptions (continued)*

Field	Description
RoundTripDelay	Voice packet round trip delay between the local and remote systems on the IP backbone for this call.
SelectedQoS	Selected RSVP quality of service (QoS) for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.
SetupTime	Value of the system UpTime when the call associated with this entry was started.
SignalingType	Signaling type for this call; for example, channel-associated signaling (CAS) or common-channel signaling (CCS).
Time between Buffer Drain/Fills	Minimum and maximum durations between jitter buffer drain or fill events, in seconds.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	Duration of transmit path open from this peer to the voice gateway for this call.
VAD	Whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

Related Commands

Command	Description
show call history	Displays the call history table.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in Voice over IP.
show voice port	Displays configuration information about a specific voice port.

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**]

Syntax Description	<i>name</i>	(Optional) The name of the desired IVR application.
	summary	(Optional) Displays a one-line summary. If the command is entered without the summary keyword, a complete detailed description is displayed of the application.

Defaults	No default behavior or values.

Command Modes	EXEC

Command History	Release	Modification
	11.3(6)NA2	This command was introduced on the Cisco 2500 series and Cisco 3600 series routers and the Cisco AS5300 universal access server.

Usage Guidelines

If the name of a specific application is entered, it will give information about that application.

If the **summary** keyword is entered, a one-line summary will be displayed about each application.

If the command is entered without the **summary**, a detailed description of the entered IVR application is displayed.

Examples

This example shows the output for the clid_authen_collect IVR script:

```
Router# show call application voice clid_authen_collect
```

```
Application clid_authen_collect has 10 states with 0 calls active
State start has 1 actions and 5 events
  Do Action IVR_ACT_AUTHENTICATE. accountName=ani, pinName=dnis
  If Event IVR_EV_DEFAULT goto state end
  If Event IVR_EV_CALL_DIGIT do nothing
  If Event IVR_EV_CALL_SETUP_IND do action IVR_ACT_CALL_SETUP_ACK
    and goto state start
  If Event IVR_EV_AAA_SUCCESS goto state collect_dest
  If Event IVR_EV_AAA_FAIL goto state get_account
State end has 1 actions and 3 events
  Do Action IVR_ACT_END.
  If Event IVR_EV_DEFAULT goto state end
  If Event IVR_EV_CALL_DIGIT do nothing
  If Event IVR_EV_CALL_DISCONNECT_DONE do action IVR_ACT_CALL_DESTROY
```

```

        and do nothing
State get_account has 4 actions and 7 events
  Do Action IVR_ACT_PLAY.
    URL: flash:enter_account.au
    allowInt=1, pContent=0x60E4C564
  Do Action IVR_ACT_ABORT_KEY. abortKey=*
  Do Action IVR_ACT_TERMINATION_KEY. terminationKey=#
  Do Action IVR_ACT_COLLECT_PATTERN. Pattern account is .+
  If Event IVR_EV_DEFAULT goto state end
  If Event IVR_EV_CALL_DIGIT do nothing
  If Event IVR_EV_PAT_COL_SUCCESS goto state get_pin
    patName=account
  If Event IVR_EV_ABORT goto state get_account
  If Event IVR_EV_PLAY_COMPLETE do nothing
  If Event IVR_EV_TIMEOUT goto state get_account count=0
  If Event IVR_EV_PAT_COL_FAIL goto state get_account
State get_pin has 4 actions and 7 events
  Do Action IVR_ACT_PLAY.
    URL: flash:enter_pin.au
    allowInt=1, pContent=0x0
  Do Action IVR_ACT_ABORT_KEY. abortKey=*
  Do Action IVR_ACT_TERMINATION_KEY. terminationKey=#
  Do Action IVR_ACT_COLLECT_PATTERN. Pattern pin is .+
  If Event IVR_EV_DEFAULT goto state end
  If Event IVR_EV_CALL_DIGIT do nothing
  If Event IVR_EV_PAT_COL_SUCCESS goto state authenticate
    patName=pin
  If Event IVR_EV_PLAY_COMPLETE do nothing
  If Event IVR_EV_ABORT goto state get_account
  If Event IVR_EV_TIMEOUT goto state get_pin count=0
  If Event IVR_EV_PAT_COL_FAIL goto state get_pin
State authenticate has 1 actions and 5 events
  Do Action IVR_ACT_AUTHENTICATE. accountName=account, pinName=pin
  If Event IVR_EV_DEFAULT goto state end
  If Event IVR_EV_CALL_DIGIT do nothing
  If Event IVR_EV_AAA_SUCCESS goto state collect_dest
  If Event IVR_EV_TIMEOUT do nothing count=0
  If Event IVR_EV_AAA_FAIL goto state authenticate_fail
State collect_dest has 4 actions and 8 events
  Do Action IVR_ACT_PLAY.
    URL: flash:enter_destination.au
    allowInt=1, pContent=0x0
  Do Action IVR_ACT_ABORT_KEY. abortKey=*
  Do Action IVR_ACT_TERMINATION_KEY. terminationKey=#
  Do Action IVR_ACT_COLLECT_DIALPLAN.
  If Event IVR_EV_DEFAULT goto state end
  If Event IVR_EV_CALL_DIGIT do nothing
  If Event IVR_EV_PLAY_COMPLETE do nothing
  If Event IVR_EV_ABORT goto state collect_dest
  If Event IVR_EV_TIMEOUT goto state collect_dest count=0
  If Event IVR_EV_DIAL_COL_SUCCESS goto state place_call
  If Event IVR_EV_DIAL_COL_FAIL goto state collect_dest
  If Event IVR_EV_TIMEOUT goto state collect_dest count=0
State place_call has 1 actions and 4 events
  Do Action IVR_ACT_PLACE_CALL.
    destination= called=
    calling= account=
  If Event IVR_EV_DEFAULT goto state end
  If Event IVR_EV_CALL_DIGIT do nothing
  If Event IVR_EV_CALL_UP goto state active
  If Event IVR_EV_CALL_FAIL goto state place_fail
State active has 0 actions and 2 events
  If Event IVR_EV_DEFAULT goto state end
  If Event IVR_EV_CALL_DIGIT do nothing

```

show call application voice

```

State authenticate_fail has 1 actions and 2 events
  Do Action IVR_ACT_PLAY.
    URL: flash:auth_failed.au
    allowInt=0, pContent=0x0
  If Event IVR_EV_DEFAULT goto state end
  If Event IVR_EV_CALL_DIGIT do nothing
State place_fail has 1 actions and 2 events
  Do Action IVR_ACT_PLAY_FAILURE_TONE.
  If Event IVR_EV_DEFAULT goto state end
  If Event IVR_EV_CALL_DIGIT do nothing

```

Router# **show call application voice clid_authen_collect**

```

Application clid_authen_collect has 10 states with 0 calls active
State start has 1 actions and 5 events
  Do Action IVR_ACT_AUTHENTICATE. accountName=ani, pinName=dnis
  If Event IVR_EV_DEFAULT goto state end
  If Event IVR_EV_CALL_DIGIT do nothing
  If Event IVR_EV_CALL_SETUP_IND do action IVR_ACT_CALL_SETUP_ACK
    and goto state start
  If Event IVR_EV_AAA_SUCCESS goto state collect_dest
  If Event IVR_EV_AAA_FAIL goto state get_account
State end has 1 actions and 3 events
  Do Action IVR_ACT_END.
  If Event IVR_EV_DEFAULT goto state end
  If Event IVR_EV_CALL_DIGIT do nothing
  If Event IVR_EV_CALL_DISCONNECT_DONE do action IVR_ACT_CALL_DESTROY
    and do nothing
State get_account has 4 actions and 7 events
  Do Action IVR_ACT_PLAY.
    URL: flash:enter_account.au
    allowInt=1, pContent=0x60E4C564
  Do Action IVR_ACT_ABORT_KEY. abortKey=*
  Do Action IVR_ACT_TERMINATION_KEY. terminationKey=#
  Do Action IVR_ACT_COLLECT_PATTERN. Pattern account is .+
  If Event IVR_EV_DEFAULT goto state end
  If Event IVR_EV_CALL_DIGIT do nothing
  If Event IVR_EV_PAT_COL_SUCCESS goto state get_pin
    patName=account
  If Event IVR_EV_ABORT goto state get_account
  If Event IVR_EV_PLAY_COMPLETE do nothing
  If Event IVR_EV_TIMEOUT goto state get_account count=0
  If Event IVR_EV_PAT_COL_FAIL goto state get_account
State get_pin has 4 actions and 7 events
  Do Action IVR_ACT_PLAY.
    URL: flash:enter_pin.au
    allowInt=1, pContent=0x0
  Do Action IVR_ACT_ABORT_KEY. abortKey=*
  Do Action IVR_ACT_TERMINATION_KEY. terminationKey=#
  Do Action IVR_ACT_COLLECT_PATTERN. Pattern pin is .+
  If Event IVR_EV_DEFAULT goto state end
  If Event IVR_EV_CALL_DIGIT do nothing
  If Event IVR_EV_PAT_COL_SUCCESS goto state authenticate
    patName=pin
  If Event IVR_EV_PLAY_COMPLETE do nothing
  If Event IVR_EV_ABORT goto state get_account
  If Event IVR_EV_TIMEOUT goto state get_pin count=0
  If Event IVR_EV_PAT_COL_FAIL goto state get_pin
State authenticate has 1 actions and 5 events
  Do Action IVR_ACT_AUTHENTICATE. accountName=account, pinName=pin
  If Event IVR_EV_DEFAULT goto state end
  If Event IVR_EV_CALL_DIGIT do nothing
  If Event IVR_EV_AAA_SUCCESS goto state collect_dest
  If Event IVR_EV_TIMEOUT do nothing count=0

```

```

    If Event IVR_EV_AAA_FAIL goto state authenticate_fail
State collect_dest has 4 actions and 8 events
    Do Action IVR_ACT_PLAY.
        URL: flash:enter_destination.au
        allowInt=1, pContent=0x0
    Do Action IVR_ACT_ABORT_KEY. abortKey=*
    Do Action IVR_ACT_TERMINATION_KEY. terminationKey=#
    Do Action IVR_ACT_COLLECT_DIALPLAN.
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
    If Event IVR_EV_PLAY_COMPLETE do nothing
    If Event IVR_EV_ABORT goto state collect_dest
    If Event IVR_EV_TIMEOUT goto state collect_dest count=0
    If Event IVR_EV_DIAL_COL_SUCCESS goto state place_call
    If Event IVR_EV_DIAL_COL_FAIL goto state collect_dest
    If Event IVR_EV_TIMEOUT goto state collect_dest count=0
State place_call has 1 actions and 4 events
    Do Action IVR_ACT_PLACE_CALL.
        destination= called=
        calling=         account=
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
    If Event IVR_EV_CALL_UP goto state active
    If Event IVR_EV_CALL_FAIL goto state place_fail
State active has 0 actions and 2 events
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
State authenticate_fail has 1 actions and 2 events
    Do Action IVR_ACT_PLAY.
        URL: flash:auth_failed.au
        allowInt=0, pContent=0x0
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
State place_fail has 1 actions and 2 events
    Do Action IVR_ACT_PLAY_FAILURE_TONE.
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing

```

Related Commands

Command	Description
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice load	Reloads the designated TCL script.

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*]

Syntax Description	<i>ip-address</i> (Optional) Specifies a specific IP address.

Defaults	This command is not configured by default.

Command Modes	EXEC

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines	To clear all entries in the cache, use the clear call fallback cache command.

Examples	The following example displays output from the show call fallback cache command:

Router# **show call fallback cache**

Probe	IP Address	Codec	Delay	Loss	ICPIF	Reject	Accept
----	-----	-----	-----	-----	-----	-----	-----
1	1.1.1.4	g729r8	40	00	0	9	
2	122.24.56.25	g729r8	14810	5	1	4	

2 active probes

Field	Description
-----	-----
Probe	Probe number
IP Address	IP Address to which the probe is sent
Codec	Codec Type of the probe
Delay	Delay in milliseconds that the probe incurred
Loss	Loss in % that the probe incurred
ICPIF	Computed ICPIF value for the probe
Reject	Number of times that calls of Codec Type <Codec> were rejected to the IP Address
Accept	Number of times that calls of Codec Type <Codec> were accepted to the IP Address
active probes	Number of destinations being probed

```
Router# show call fallback cache 10.14.115.53
```

Probe	IP Address	Codec	ICPIF	Reject	Accept
-----	-----	-----	-----	-----	-----
1	10.14.115.53	g729r8	0	0	2

```
1 active probes
```

Related Commands

Command	Description
show call fallback stats	Displays the call fallback statistics.

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.

Defaults	This command is not configured by default.

Command Modes	EXEC

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco MC3810 multiservice concentrator.

Examples	The following example displays output from the show call fallback config command:

```
Router# show call fallback config

VoIP fallback config:
Fallback is ON
Using ICPIF threshold:
    ICPIF value timeout:20 seconds
    ICPIF threshold:20
Number of packets in a probe:20
IP precedence of probe packets:2
Fallback cache size:2 entries
Fallback cache timeout:240 seconds
Instantaneous value weight:65
MD5 Keychain:secret
```

Related Commands	Command	Description
	call fallback monitor	Enables the monitoring of destinations without fallback to alternate dial peers.
	show voice trunk-conditioning signaling	Enables fallback to alternate dial peers in case of network congestion.

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.

Defaults	This command is not configured by default.

Command Modes	EXEC

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines	To remove all values, use the clear call fallback stats command.

Examples	The following example displays output from the show call fallback stats command:

```
Router# show call fallback stats
```

```
VOIP Fallback Stats:  
Total accepted calls:3  
Total rejected calls:1  
Total cache overflows:1
```

Field	Description
Total accepted calls	Number of times that calls were successful over IP.
Total rejected calls	Number of times that calls were rejected over IP.
Total cache overflows	Number of times that the fallback cache overflowed and required pruning.

Related Commands	Command	Description
	clear call fallback stats	Clears the call fallback statistics.
	show call fallback cache	Displays the current ICPIF estimates for all IP addresses in the cache.

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**]

Syntax Description	voice	Specifies that call history information be displayed for voice calls.
	fax	Specifies that call history information be displayed for fax calls.
	last <i>number</i>	(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.
	brief	(Optional) Displays a truncated version of the call history table.

Defaults No default behavior or values.

Command Modes

User EXEC

Privileged EXEC

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 series.
	12.0(3)XG	Support for Voice over Frame Relay (VoFR) was added on the Cisco 2600 and Cisco 3600 series.
	12.0(4)XJ	This command was modified for store-and-forward fax.
	12.0(4)T	The brief keyword was added and the command was first supported on the Cisco 7200 series.
	12.0(7)XK	Support for the brief keyword was added on the Cisco MC3810 multiservice concentrator.
	12.1(2)T	This command was integrated into Cisco IOS 12.1(2)T.

Usage Guidelines

The **show call history** command displays a call history table containing a list of voice or fax calls connected through the router in descending time order. The maximum number of calls contained in the table can be set to a number between 0 and 500 using the **dial-control-mib** command in global configuration mode. The default maximum number of table entries is 50. Each call record is aged out of the table after a configurable number of minutes has elapsed, also specified by the **dial-control-mib** command. The default timer value is 15 minutes.

You can display subsets of the call history table by using specific keywords. To display the last calls connected through this router, use the keyword **last**, and define the number of calls to be displayed with the *number* argument.

To display a truncated version of the call history table, use the **brief** keyword.

When using the **fax** keyword, this command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following is sample output from the **show call history voice** command:

```
Router# show call history voice

GENERIC:
SetupTime=104648 ms
Index=1
PeerAddress=55240
PeerSubAddress=
PeerId=2
PeerIfIndex=105
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing.
ConnectTime=104964
DisconnectTime=143329
CallDuration=00:06:23
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=37668
TransmitBytes=6157536
ReceivePackets=37717
ReceiveBytes=6158452
VOIP:
ConnectionId[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
RemoteIPAddress=1.14.82.14
RemoteUDPPort=18202
RoundTripDelay=2 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=TRUE

SessionProtocol=cisco
SessionTarget=ipv4:1.14.82.14
OnTimeRvPayout=40
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPayoutDelay=67 ms
LoWaterPayoutDelay=67 ms
ReceiveDelay=67 ms
LostPackets=0 ms
EarlyPackets=0 ms
LatePackets=0 ms
VAD = enabled
CoderTypeRate=g729r8
CodecBytes=20
cvVoIPCallHistoryIcpif=0
SignalingType=cas

Modem passthrough signaling method is nse
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
```

■ show call history

```
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 373sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec
```

```
GENERIC:
SetupTime=104443 ms
Index=2
PeerAddress=50110
PeerSubAddress=
PeerId=100
PeerIfIndex=104
LogicalIfIndex=10
DisconnectCause=10
DisconnectText=normal call clearing.
ConnectTime=104964
DisconectTime=143330
CallDuration=00:06:23
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=37717
TransmitBytes=5706436
ReceivePackets=37668
ReceiveBytes=6609552
TELE:
ConnectionId=[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
TxDuration=375300 ms
VoiceTxDuration=375300 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
NoiseLevel=-75
ACOMLevel=11
SessionTarget=
ImgPages=0
```

The following is sample output from the **show call history voice brief** command:

```
Router# show call history voice brief
```

```
<ID>: <start>hs.<index> +<connect> +<disc> pid:<peer_id> <direction> <addr>
dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>)
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
delay:<last>/<min>/<max>ms <codec>
MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
last <buf event time>s dur:<Min>/<Max>s
FR <protocol> [int dlcid cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
sig:<on/off> <codec> (payload size)
ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
sig:<on/off> <codec> (payload size)
Telephony <int>: tx:<tot>/<voice>/<fax>ms <codec> noise:<lvl>dBm acom:<lvl>dBm
```

The following is sample output from the **show call history fax** command:

```
Router# show call history fax
```

```
GENERIC:
SetupTime=23193 ms
Index=1
PeerAddress=527....
PeerSubAddress=
PeerId=3469
PeerIfIndex=157
LogicalIfIndex=30
DisconnectCause=10
```

```

DisconnectText=normal call clearing.: Normal connection
ConnectTime=24284
DisconnectTime=31288
CallOrigin=1
ChargedUnits=0
InfoType=fax
TransmitPackets=62
TransmitBytes=88047
ReceivePackets=0
ReceiveBytes=0

```

```

TELE:
ConnectionId=[0x37EC7F41 0xB0110001 0x0 0x35C34]
TxDuration=80950 ms
FaxTxDuration=10910 ms
FaxRate=14400
NoiseLevel=-1
ACOMLevel=-1
SessionTarget=
ImgPages=3

```

```

GENERIC:
SetupTime=22021 ms
Index=2
PeerAddress=wook song
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing.
ConnectTime=24284
DisconnectTime=31545
CallOrigin=2
ChargedUnits=0
InfoType=fax
TransmitPackets=0
TransmitBytes=0
ReceivePackets=0
ReceiveBytes=41190

```

```

MMOIP:
ConnectionId[0x37EC7F41 0xB0110001 0x0 0x35C34]
RemoteIPAddress=0.0.0.0
SessionProtocol=SMTP
SessionTarget=
MessageId=
AccountId=
ImgEncodingType=MH
ImgResolution=fine
AcceptedMimeTypes=2
DiscardedMimeTypes=1
Notification=None

```

The following is sample output from the **show call history fax brief** command:

Router# **show call history fax brief**

```

<ID>: <start>hs.<index> +<connect> +<disc> pid:<peer_id> <direction> <addr>
tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>)
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
delay:<last>/<min>/<max>ms <codec>
Telephony <int>: tx:<tot>/<voice>/<fax>ms <codec> noise:<lvl>dBm acom:<lvl>dBm

```

■ show call history

```

2      : 5996450hs.25 +-1 +3802 pid:100 Answer 408
tx:0/0 rx:0/0 1F (T30 T1 EOM timeout)
Telephony : tx:38020/38020/0ms g729r8 noise:0dBm acom:0dBm

2      : 5996752hs.26 +-1 +3500 pid:110 Originate uut1@linux2.allegro.com
tx:0/0 rx:0/0 3F (The e-mail was not sent correctly. Remote SMTP server said: 354 )
IP 14.0.0.1 AcceptedMime:0 DiscardedMime:0

3      : 6447851hs.27 +1111 +3616 pid:310 Originate 576341.
tx:11/14419 rx:0/0 10 (Normal connection)
Telephony : tx:36160/11110/25050ms g729r8 noise:115dBm acom:-14dBm

3      : 6447780hs.28 +1182 +4516 pid:0 Answer
tx:0/0 rx:0/0 10 (normal call clearing.)
IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

4      : 6464816hs.29 +1050 +3555 pid:310 Originate 576341.
tx:11/14413 rx:0/0 10 (Normal connection)
Telephony : tx:35550/10500/25050ms g729r8 noise:115dBm acom:-14dBm

4      : 6464748hs.30 +1118 +4517 pid:0 Answer
tx:0/0 rx:0/0 10 (normal call clearing.)
IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

5      : 6507900hs.31 +1158 +2392 pid:100 Answer 4085763413
tx:0/0 rx:3/3224 10 (Normal connection)
Telephony : tx:23920/11580/12340ms g729r8 noise:0dBm acom:0dBm

5      : 6508152hs.32 +1727 +2140 pid:110 Originate uut1@linux2.allegro.com
tx:0/2754 rx:0/0 3F (service or option not available, unspecified)
IP 14.0.0.4 AcceptedMime:0 DiscardedMime:0

6      : 6517176hs.33 +1079 +3571 pid:310 Originate 576341.
tx:11/14447 rx:0/0 10 (Normal connection)
Telephony : tx:35710/10790/24920ms g729r8 noise:115dBm acom:-14dBm

6      : 6517106hs.34 +1149 +4517 pid:0 Answer
tx:0/0 rx:0/0 10 (normal call clearing.)
IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

7      : 6567382hs.35 +1054 +3550 pid:310 Originate 576341.
tx:11/14411 rx:0/0 10 (Normal connection)
Telephony : tx:35500/10540/24960ms g729r8 noise:115dBm acom:-14dBm

7      : 6567308hs.36 +1128 +4517 pid:0 Answer
tx:0/0 rx:0/0 10 (normal call clearing.)
IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

```

[Table 28](#) provides an alphabetical listing of the fields displayed in the output from the **show call history** command and a description of each field.

Table 28 *show call history* Field Descriptions

Field	Description
ACOMLevel	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceler, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
Buffer Drain Events	Total number of jitter buffer drain events.
Buffer Fill Events	Total number of jitter buffer fill events.

Table 28 *show call history Field Descriptions (continued)*

Field	Description
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallOrigin	Call origin: answer or originate.
ChargedUnits	Total number of charging units applying to this peer since system startup. The unit of measure for this field is hundredths of a second.
CodecBytes	Payload size in bytes for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionID	Global call identifier for the gateway call.
ConnectTime	Time at which this call was connected.
Consecutive-packets-lost Events	Total number of consecutive (two or more) packet loss events.
Corrected packet-loss Events	Total number of packet-loss events that were corrected using the RFC 2198 method.
DisconnectCause	Description explaining why this call was disconnected.
DisconnectText	Descriptive text explaining the reason for the disconnect.
DisconnectTime	Time when this call was disconnected.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time, because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from redundancy parameters available because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GapFillWithPrediction	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call.
HiWaterPlayoutDelay	High-water mark Voice Playout FIFO Delay during this voice call.
Index	Dial peer identification number.
InfoType	Information type for this call; for example, voice or fax.
Last Buffer Drain/Fill Event	Time since the last jitter buffer drain or fill event, in seconds.
LogicalIfIndex	Index number of the logical voice port for this call.
LoWaterPlayoutDelay	Low-water mark Voice Playout FIFO Delay during this voice call.

Table 28 *show call history Field Descriptions (continued)*

Field	Description
Modem passthrough signaling method is nse	Indicates that this is a modem pass-through call and named signaling events (NSEs)—also called <i>telephone-events</i> in RFC 2833—are used for signaling codec 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.
NoiseLevel	Average noise level for this call.
OnTimeRvPayout	Duration of voice payout from data received on time for this call. Derive the Total Voice Payout Duration for Active Voice by adding the OnTimeRvPayout value to the GapFill values.
Percent Packet Loss	Total percent packet loss.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer entry table to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress where this call is connected.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average Playout FIFO Delay plus the Decoder Delay during this voice call.
ReceivePackets	Number of packets received by this peer during this call.
RemoteIPAddress	Remote system IP address for this call.
RemoteUDPPort	Remote system UDP listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay between the local and remote systems on the IP backbone for this call.
SelectedQoS	Selected RSVP QoS for this call.
Session Protocol	Session protocol used for an Internet call between the local and remote router through the IP backbone.
Session Target	Session target of the peer used for this call.
SetUpTime	Value of the system UpTime when the call associated with this entry was started.
SignalingType	Signaling type for this call, for example, channel-associated signaling (CAS) or common-channel signaling (CCS).
Time between Buffer Drain/Fills	Minimum and maximum durations between jitter buffer drain or fill events, in seconds.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	Duration of the transmit path open from this peer to the voice gateway for this call.

Table 28 *show call history Field Descriptions (continued)*

Field	Description
VAD	Specifies whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

Related Commands

Command	Description
show call active	Displays the active call information for voice calls or fax transmissions in progress.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in Voice over IP.
show voice port	Displays configuration information about a specific voice port.

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.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(5)XK	This command was introduced for the Cisco MC3810 multiservice concentrator.
	12.0(7)T	The command introduced in Cisco IOS Release 12.0(5)XK was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines	Use this command to review statistics about recent incoming and outgoing video calls.

Examples	On a Cisco MC3810 multiservice concentrator, the following example displays information about two video calls:

```
Router# show call history video record

CallId = 4
CalledNumber = 221
CallDuration = 39006 seconds
DisconnectText = remote hangup
SVC: call ID = 8598630
Remote NSAP = 47.0091810000000002F26D4901.00107B09C645.C8
Local NSAP = 47.0091810000000002F26D4901.00107B4832E1.C8
vcd = 414, vpi = 0, vci = 158
SerialPort = Serial0
VideoSlot = 1, VideoPort = 0
CallId = 3
CalledNumber = 221
CallDuration = 557 seconds
DisconnectText = local hangup
SVC: call ID = 8598581
Remote NSAP = 47.0091810000000002F26D4901.00107B09C645.C8
Local NSAP = 47.0091810000000002F26D4901.00107B4832E1.C8
vcd = 364, vpi = 0, vci = 108
SerialPort = Serial0
VideoSlot = 1, VideoPort = 0
```

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.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(5)XK	This command was introduced for the Cisco MC3810 multiservice concentrator.
	12.0(7)T	The command introduced in Cisco IOS Release 12.0(5)XK was integrated into Cisco IOS Release 12.0(7)T.

Examples	The following example displays a sample of voice call history records showing a local call between two telephones attached to the same Cisco MC3810 multiservice concentrator:

```
Router# show call history voice record

ConnectionId=[0x2C7AEFDC 0x59830001 0x0 0xB0AAA3]
Media=TELE, TxDuration= 1418 ms
CallingNumber=2001
SetupTime=1157801 x 10ms
ConnectTime=1158046 x 10ms
DisconnectTime=1158188 x 10ms
DisconnectText=local onhook

ConnectionId=[0x2C7AEFDC 0x59830001 0x0 0xB0AAA3]
Media=TELE, TxDuration= 1422 ms
CalledNumber=2002
SetupTime=1157802 x 10ms
ConnectTime=1158046 x 10ms
DisconnectTime=1158188 x 10ms
DisconnectText=remote onhook
```

[Table 29](#) describes the significant fields shown in the display.

Table 29 *show call history voice record Field Descriptions*

Field	Description
ConnectionID	Global call identifier for this voice call.
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry will be TELE. If the call is carried over the voice network side, the entry will be either ATM, FR (for Frame Relay), or HDLC.
LowerIFName	Physical lower interface information. Appears only if the medium is either ATM, FR, or HDLC.
TxDuration	The length of the call. Appears only if the medium is TELE.
CalledNumber	The called number.
CallingNumber	The calling number.
SetupTime	Time the call setup started.
ConnectTime	Time the call is connected.
DisconnectTime	Time the call is disconnected.
DisconnectText	Descriptive text explaining the reason for the disconnect.

Related Commands

Command	Description
show call active voice	Displays the Voice over IP active call table.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in Voice over IP.
show voice port	Displays configuration information about a specific voice port.

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.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines	This command displays the H.323 resources that are monitored when the resource threshold command is used to configure and enable resource threshold reporting.

Examples	The following example shows the resource statistics for an H.323 gateway:

```
Router# show call resource voice stats

Resource Monitor - Dial-up Resource Statistics Information:

DSP Statistics:

Utilization: 0 percent
Total channels: 48
Inuse channels: 0
Disabled channels 0:
Pending channels: 0
Free channels: 48

DS0 Statistics:

Total channels: 0
Addressable channels: 0
Inuse channels: 0
Disabled channels: 0
Free channels: 0
```

[Table 30](#) describes the significant fields shown in the display.

Table 30 *show call resource voice stats Field Descriptions*

Statistic	Definition
Total channels	Number of channels physically configured for the resource.
Addressable channels	Number of channels that can be used for a specific type of dialup service, such as H.323, which includes all the DS0 resources that have been associated with a voice plain old telephone service (POTS) dial plan profile.
Inuse channels	Number of addressable channels that are in use. This value includes all channels that either have active calls or have been reserved for testing.
Free channels	Number of addressable channels that are free.
Pending channels	Number of addressable channels that are pending in loadware download.
Disabled channels	Number of addressable channels that are physically down or that have been disabled administratively with the shutdown or busyout command.

Related Commands

Command	Description
resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.
show call resource voice threshold	Displays the threshold configuration settings and status for an H.323 gateway.

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.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines	This command displays the H.323 resource thresholds that are configured with the resource threshold command.

Examples	The following example shows the resource threshold settings and status for an H.323 gateway:

```
Router# show call resource voice threshold
```

```
Resource Monitor - Dial-up Resource Threshold Information:
```

```
DS0 Threshold:
```

```
Client Type: h323
High Water Mark: 70
Low Water Mark: 60
Threshold State: init
DSP Threshold:
```

```
Client Type: h323
High Water Mark: 70
Low Water Mark: 60
Threshold State: low_threshold_hit
```

Related Commands	Command	Description
	resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.
	show call resource voice stats	Displays resource statistics for an H.323 gateway.

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.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(3)XI1	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers, the Cisco MC3810 multiservice concentrator, and on the Cisco AS5300 and Cisco AS5800 universal access servers.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples The following example shows sample output from the **show call rsvp-sync conf** command:

```
Router# show call rsvp-sync conf
```

```
VoIP QoS: RSVP/Voice Signaling Synchronization config:
```

```
Overture Synchronization is ON
Reservation Timer is set to 10 seconds
```

[Table 31](#) describes the significant fields shown in the display

Table 31 *show call rsvp-sync conf Field Descriptions*

Field	Description
Overture Synchronization is ON	Indicates whether RSVP synchronization is enabled.
Reservation Timer is set to xx seconds	Number of seconds for which the RSVP reservation timer is configured.

Related Commands

Command	Description
call rsvp-sync	Enables synchronization between RSVP and the H.323 voice signaling protocol.
call rsvp-sync resv-timer	Sets the timer for RSVP reservation setup.
debug call rsvp-sync events	Displays the events that occur during RSVP synchronization.
show call rsvp-sync stats	Displays statistics for calls that attempted RSVP reservation.

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.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(3)XI1	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples The following example shows sample output from the **show call rsvp-sync stats** command:

```
Router# show call rsvp-sync stats
```

```
VoIP QoS:Statistics Information:
```

```
Number of calls for which QoS was initiated : 18478
```

```
Number of calls for which QoS was torn down : 18478
```

```
Number of calls for which Reservation Success was notified : 0
```

```
Total Number of PATH Errors encountered : 0
```

```
Total Number of RESV Errors encountered : 0
```

```
Total Number of Reservation Timeouts encountered : 0
```

[Table 32](#) describes the significant fields shown in the display.

Table 32 *show call rsvp-sync stats Field Descriptions*

Field	Description
Number of calls for which QoS was initiated	Number of calls for which RSVP setup was attempted.
Number of calls for which QoS was torn down	Number of calls for which an established RSVP reservation was released.
Number of calls for which Reservation Success was notified	Number of calls for which an RSVP reservation was successfully established.
Total Number of PATH Errors encountered	Number of path errors that occurred.
Total Number of RESV Errors encountered	Number of reservation errors that occurred.
Total Number of Reservation Timeouts encountered	Number of calls in which the reservation setup was not complete before the reservation timer expired.

Related Commands

Command	Description
call rsvp-sync	Enables synchronization between RSVP and the H.323 voice signaling protocol.
call rsvp-sync resv-timer	Sets the timer for RSVP reservation setup.
debug call rsvp-sync events	Displays the events that occur during RSVP synchronization.
show call rsvp-sync conf	Displays the RSVP synchronization configuration.

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.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(7)T	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines	CDAPI is the internal application programming interface (API) that provides an interface between signaling stacks and applications.

Examples	The following is output for the show cdapi command:

```
Router# show cdapi

Registered CDAPI Applications/Stacks
=====
Application TSP CDAPI Application
      Application Type(s)  Voice Facility Signaling
      Application Level    Tunnel
      Application Mode     Enbloc
Signaling Stack ISDN
      Interface Se023
Signaling Stack ISDN
      Interface Se123
Active CDAPI Calls
=====
Interface Se023
      No active calls.
Interface Se123
      Call ID = 0x39, Call Type = VOICE, Application = TSP CDAPI Application
CDAPI Message Buffers
=====
Used Msg Buffers 0, Free Msg Buffers 1600
Used Raw Buffers 1, Free Raw Buffers 799
Used Large-Raw Buffers 0, Free Large-Raw Buffers 80
scarlatt11#
```

Related Commands	Command	Description
	isdn protocol-emulate	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality.
	isdn switch type	Configures the Cisco AS5300 universal access server PRI interface to support Q.SIG signaling.
	pri-group nec-fusion	Configures your NEC PBX to support FCCS.
	show rawmsg	Displays the raw messages owned by the required component.

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

Syntax Description

<i>slot</i>	Backplane slot number.
<i>/port</i>	Interface port number. The slash must be entered.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(2)T	This command was introduced on the Cisco 3600 series router.

Examples

The following is sample output from the **show ces clock-select** command for slot 1, port 0:

```
Router# show ces 1/0 clock-select

Priority 1 clock source:not configured
Priority 2 clock source:not configured
Priority 3 clock source:ATM1/0 UP
Priority 4 clock source:Local oscillator
Current clock source:ATM1/0, priority:3
```

Related Commands

Command	Description
clock-select	Establishes the sources and priorities of the requisite clocking signals for the OC-3/STM-1 ATM Circuit Emulation Service network module.

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*}

Syntax Description		
all		Displays a table of all configured connections.
elements		Displays registered hardware or software interworking elements.
name		Displays a connection that has been named by using the connect global configuration command. The name you enter is case sensitive and must match the configured name exactly.
id		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 show connect all command displays these IDs.
port		Displays the status of a connection that you specify by indicating the type of controller (T1 or E1) and location of the interface.
T1		Specifies a T1 controller.
E1		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.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(5)XK	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers.
	12.0(7)T	The command introduced in Cisco IOS Release 12.0(5)XK was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines	This command shows drop-and-insert connections on the Cisco 2600 and 3600 series. The command displays different information in different formats, depending on the keyword that you use.

Examples

The following examples show how the same tabular information appears when you enter different keywords:

Router# **show connect all**

ID	Name	Segment 1	Segment 2	State
1	Test	-T1 1/0 01	-T1 1/1 02	ADMIN UP
2	Test2	-T1 1/0 03	-T1 1/1 04	ADMIN UP

Router# **show connect id 1-2**

ID	Name	Segment 1	Segment 2	State
1	Test	-T1 1/0 01	-T1 1/1 02	ADMIN UP
2	Test2	-T1 1/0 03	-T1 1/1 04	ADMIN UP

Router# **show connect port t1 1/1**

ID	Name	Segment 1	Segment 2	State
1	Test	-T1 1/0 01	-T1 1/1 02	ADMIN UP
2	Test2	-T1 1/0 03	-T1 1/1 04	ADMIN UP

The following examples show details about specific connections, including the number of time slots in use and the switching elements:

Router# **show connect id 2**

```

Connection: 2 - Test2
Current State: ADMIN UP
Segment 1: -T1 1/0 03
  TDM timeslots in use: 14-18 (5 total)
Segment 2: -T1 1/1 04
  TDM timeslots in use: 14-18
Internal Switching Elements: VIC TDM Switch

```

Router# **show connect name Test**

```

Connection: 1 - Test
Current State: ADMIN UP
Segment 1: -T1 1/0 01
  TDM timeslots in use: 1-13 (13 total)
Segment 2: -T1 1/1 02
  TDM timeslots in use: 1-13
Internal Switching Elements: VIC TDM Switch

```

Related Commands

Command	Description
connect	Defines connections between T1 or E1 controller ports for Drop and Insert.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for TDM cross-connect.

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.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(5)XK	This command was introduced for the Cisco MC3810 multiservice concentrator.
	12.0(7)T	The command introduced in Cisco IOS Release 12.0(5)XK was integrated into Cisco IOS Release 12.0(7)T.

Examples On a Cisco MC3810 multiservice concentrator, the following example displays information about the RS-366 controller:

```
Router# show controller rs366 0 1
```

```
RS366:driver is initialized in slot 1, port 0:
```

```
STATUS STATE LSR  LCR  ICSR EXT  T1      T2      T3      T4      T5
0x02   0x01  0x00 0x50 0xE0 0x00 5000   5000   5000  20000 10000
Dial string:
121C
```

[Table 33](#) describes the significant fields shown in the display.

Table 33 *show controllers Field Descriptions*

Field	Description
STATUS	Last interrupt status.
STATE	Current state of the state machine.
LSR	Line status register of the VDM.
LCR	Line control register of the VDM.

Table 33 *show controllers Field Descriptions (continued)*

Field	Description
ICSR	Interrupt control and status register of the VDM.
EXT	Extended register of the VDM.
T1 through T5	Timeouts 1 through 5 of the watchdog timer, in milliseconds.
Dial string	Most recently dialed number collected by the driver. 0xC at the end of the string indicates the EON (end of number) character.

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	tl/e1	Specifies the type of interface.
	<i>controller-number</i>	Specifies the controller number of CAS or ISDN PRI time slot. Range 0 through 7.
	timeslots	Displays DS0 information.
	<i>timeslot-range</i>	Specifies time slot range 1 through 31 for E1, 1 through 24 for T1.

Defaults No default

Command Modes Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.1(3)T	The timeslots keyword was added.
	12.1(5)T	Support for Cisco AS5400 universal access servers was added.

Usage Guidelines Use the **show controllers t1/e1 timeslots** command to display the CAS and ISDN PRI channel state in detail. This command shows whether the DS0 channels of a controller are in idle, in-service, maintenance, or busyout states. Enter the **show controllers t1/e1** command to display statistics about the T1 or E1 links.

Examples The following example shows that the CAS state is enabled on the Cisco AS5300 universal access server with a T1 PRI card:

```
Router# show controllers timeslots
```

```
T1 1 is up:
```

```
Loopback: NONE
```

DS0	Type	Modem	<->	Service State	Channel State	Rx A B C D				Tx A B C D			
1	cas-modem	1	in	insvc	connected	1	1	1	1	1	1	1	1
2	cas	-	-	insvc	idle	0	0	0	0	0	0	0	0
3	cas	-	-	insvc	idle	0	0	0	0	0	0	0	0
4	cas	-	-	insvc	idle	0	0	0	0	0	0	0	0
5	cas	-	-	insvc	idle	0	0	0	0	0	0	0	0
6	cas	-	-	insvc	idle	0	0	0	0	0	0	0	0
7	cas	-	-	insvc	idle	0	0	0	0	0	0	0	0
8	cas	-	-	insvc	idle	0	0	0	0	0	0	0	0
9	cas	-	-	insvc	idle	0	0	0	0	0	0	0	0

show controllers timeslots

```

10  cas      -      -      maint    static-bo    0  0  0  0    1  1  1  1
11  cas      -      -      maint    static-bo    0  0  0  0    1  1  1  1
12  cas      -      -      maint    static-bo    0  0  0  0    1  1  1  1
13  cas      -      -      maint    static-bo    0  0  0  0    1  1  1  1
14  cas      -      -      maint    static-bo    0  0  0  0    1  1  1  1
15  cas      -      -      maint    static-bo    0  0  0  0    1  1  1  1
16  cas      -      -      maint    static-bo    0  0  0  0    1  1  1  1
17  cas      -      -      maint    static-bo    0  0  0  0    1  1  1  1
18  cas      -      -      maint    static-bo    0  0  0  0    1  1  1  1
19  cas      -      -      maint    dynamic-bo   0  0  0  0    1  1  1  1
20  cas      -      -      maint    dynamic-bo   0  0  0  0    1  1  1  1
21  cas      -      -      maint    dynamic-bo   0  0  0  0    1  1  1  1
22  unused
23  unused
24  unused

```

The following example shows that the ISDN PRI state is enabled on the Cisco AS5300 universal access server with a T1 PRI card:

T1 2 is up:

Loopback: NONE

DS0	Type	Modem	<->	Service State	Channel State	Rx A B C D	Tx A B C D
1	pri	-	-	insvc	idle		
2	pri	-	-	insvc	idle		
3	pri	-	-	insvc	idle		
4	pri	-	-	insvc	idle		
5	pri	-	-	insvc	idle		
6	pri	-	-	insvc	idle		
7	pri	-	-	insvc	idle		
8	pri	-	-	insvc	idle		
9	pri	-	-	insvc	idle		
10	pri	-	-	insvc	idle		
11	pri	-	-	insvc	idle		
12	pri	-	-	insvc	idle		
13	pri	-	-	insvc	idle		
14	pri	-	-	insvc	idle		
15	pri	-	-	insvc	idle		
16	pri	-	-	insvc	idle		
17	pri	-	-	insvc	idle		
18	pri	-	-	insvc	idle		
19	pri	-	-	insvc	idle		
20	pri	-	-	insvc	idle		
21	pri-modem	2	in	insvc	busy		
22	pri-modem	1	out	insvc	busy		
23	pri-digi	-	in	insvc	busy		
24	pri-sig	-	-	outofsvc	reserved		

show controllers voice

To display information about voice-related hardware, use the **show controllers voice** command in privileged EXEC mode.

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(5)XQ	This command was introduced on the Cisco 1750.

Usage Guidelines This command displays interface status information that is specific to voice-related hardware, such as the registers of the TDM switch, the host port interface of the digital signal processor (DSP), and the DSP firmware versions. The information displayed is generally useful only for diagnostic tasks performed by technical support.

Examples The following is an example of the output from the **show controllers voice** command:

```
Router# show controllers voice
```

```
EPIC Switch registers:
STDA 0xFF STDB 0xFF SARA 0xAD SARB 0xFF SAXA 0xFF SAXB 0x0 STCR 0x3F
MFAIR 0x3F
STAR 0x65 OMDR 0xE2 VNSR 0x0 PMOD 0x4C PBNR 0xFF POFD 0xF0 POFU 0x18
PCSR 0x1 PICM 0x0 CMD1 0xA0 CMD2 0x70 CBNR 0xFF CTAR 0x2 CBSR 0x20 CSCR
0x0
```

```
DSP 0 Host Port Interface:
HPI Control Register 0x202
InterfaceStatus 0x2A MaxMessageSize 0x80
RxRingBufferSize 0x6 TxRingBufferSize 0x9
pInsertRx 0x4 pRemoveRx 0x4 pInsertTx 0x6 pRemoveTx 0x6
```

```
Rx Message 0:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000: 0000 4AC7 5F08 91D1 0000 0000 7DF1 69E5 63E1 63E2
0020: 6E7C ED67 DE5D DB5C DC60 EC7E 6BE1 58D3 50CD 4DCE
0040: 50D2 5AE5 7868 DA52 CE4A C746 C647 C94B D25A EAF4
0060: 5DD7 4FCD 4ACA 4ACC 4FD3 5DE8 F769 DC58 D352 D253
0080: D65B E573 6CDF 59D3 4ECF 4FD0
```

```
Rx Message 1:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000: 0000 1CDD 3E48 3B74 0000 0000 3437 3D4C F0C8 BBB5
0020: B2B3 B7BF D25B 4138 3331 3339 435F CFBD B6B2 B1B4
```

■ show controllers voice

```

0040:   BBC8 7E48 3B34 3131 363D 4FDE C3B9 B3B1 B3B8 C2DB
0060:   533F 3833 3235 3B48 71CC BDB7 B4B5 B8BF CF67 483D
0080:   3836 383C 455B DAC6 BDB9 B9BB

```

Rx Message 2:

```

packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 4AC8 5F08 9221 0000 0000 54DA 61F5 EF60 DA53
0020:   CF4F CD4E D256 DB63 FCEE 5FDA 55D1 50CF 4FD3 56D8
0040:   5DE1 6E7C EC60 DC59 D655 D456 D85D DF6A F4F4 69E2
0060:   5CDD 5BDC 5BDE 61E9 6DF1 FF76 F16D E96A E566 EA6A
0080:   EB6F F16D EF79 F776 F5F5 73F0

```

Rx Message 3:

```

packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 1CDE 3E48 3BC4 0000 0000 C0CC EC54 453E 3C3C
0020:   3F47 56F3 D1C7 C1BF C0C6 CEE1 6752 4A46 4648 4E59
0040:   6FE4 D6CF CDCE D2DA E57E 675E 5B5B 5E62 6B76 FCF6
0060:   F6FA 7D75 7373 7BF5 EAE1 DCDA DADD E6FE 6559 514D
0080:   4D4E 5563 EFD9 CDC8 C5C6 CAD1

```

Rx Message 4:

```

packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 4AC6 5F08 9181 0000 0000 DD5B DC5E E161 E468
0020:   FAFD 6CE1 5AD3 53D1 53D7 61EC EA59 CF4A C644 C344
0040:   CA4E D86C 60D0 48C2 3EBD 3CBD 3EC0 47CF 5976 DF4F
0060:   C945 C242 C146 C94E D668 73DB 54CE 4DCC 4DCE 53DB
0080:   64F9 ED63 DC59 DA58 DC5D E46C

```

Rx Message 5:

```

packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 1CDC 3E48 3B24 0000 0000 5B5B 5D62 6A76 FCF5
0020:   F5F9 7D78 7374 7CF5 EAE1 DDDA DBDD E7FE 6559 514E
0040:   4D4F 5663 EFD8 CDC8 C6C6 CAD1 E760 4E46 403F 4047
0060:   5173 D5C7 BFBC BCBE C5D4 6D4C 3F3B 3939 3D46 5ADB
0080:   C5BC B7B6 B8BD C8E8 4F3F 3835

```

Tx Message 0:

```

packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 4AC6 5F08 9181 0000 003C DD5B DC5E E161 E468
0020:   FAFD 6CE1 5AD3 53D1 53D7 61EC EA59 CF4A C644 C344
0040:   CA4E D86C 60D0 48C2 3EBD 3CBD 3EC0 47CF 5976 DF4F
0060:   C945 C242 C146 C94E D668 73DB 54CE 4DCC 4DCE 53DB
0080:   64F9 ED63 DC59 DA58 DC5D E46C

```

Tx Message 1:

```

packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDC 3E48 3B24 0000 003C 5B5B 5D62 6A76 FCF5
0020:   F5F9 7D78 7374 7CF5 EAE1 DDDA DBDD E7FE 6559 514E
0040:   4D4F 5663 EFD8 CDC8 C6C6 CAD1 E760 4E46 403F 4047
0060:   5173 D5C7 BFBC BCBE C5D4 6D4C 3F3B 3939 3D46 5ADB
0080:   C5BC B7B6 B8BD C8E8 4F3F 3835

```

Tx Message 2:

```

packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 4AC7 5F08 91D1 0000 003C 7DF1 69E5 63E1 63E2
0020:   6E7C ED67 DE5D DB5C DC60 EC7E 6BE1 58D3 50CD 4DCE
0040:   50D2 5AE5 7868 DA52 CE4A C746 C647 C94B D25A EAF4
0060:   5DD7 4FCD 4ACA 4ACC 4FD3 5DE8 F769 DC58 D352 D253
0080:   D65B E573 6CDF 59D3 4ECF 4FD0

```

Tx Message 3:

```

packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDD 3E48 3B74 0000 003C 3437 3D4C F0C8 BBB5
0020:   B2B3 B7BF D25B 4138 3331 3339 435F CFBD B6B2 B1B4

```

```

0040:  BBC8 7E48 3B34 3131 363D 4FDE C3B9 B3B1 B3B8 C2DB
0060:  533F 3833 3235 3B48 71CC BDB7 B4B5 B8BF CF67 483D
0080:  3836 383C 455B DAC6 BDB9 B9BB

```

Tx Message 4:

```

packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:  0000 4AC8 5F08 9221 0000 003C 54DA 61F5 EF60 DA53
0020:  CF4F CD4E D256 DB63 FCEE 5FDA 55D1 50CF 4FD3 56D8
0040:  5DE1 6E7C EC60 DC59 D655 D456 D85D DF6A F4F4 69E2
0060:  5CDD 5BDC 5BDE 61E9 6DF1 FF76 F16D E96A E566 EA6A
0080:  EB6F F16D EF79 F776 F5F5 73F0

```

Tx Message 5:

```

packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:  0000 1CDE 3E48 3BC4 0000 003C C0CC EC54 453E 3C3C
0020:  3F47 56F3 D1C7 C1BF C0C6 CEE1 6752 4A46 4648 4E59
0040:  6FE4 D6CF CDCE D2DA E57E 675E 5B5B 5E62 6B76 FCF6
0060:  F6FA 7D75 7373 7BF5 EAE1 DCDA DADD E6FE 6559 514D
0080:  4D4E 5563 EFD9 CDC8 C5C6 CAD1

```

Tx Message 6:

```

packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:  0000 1CDA 3E48 3A84 0000 003C E75F 4E46 403F 4147
0020:  5174 D5C7 BFBC BCBE C5D4 6C4C 3F3B 3939 3D46 5BDA
0040:  C5BC B7B6 B8BD C8E9 4F3F 3834 3437 3D4C EEC8 BBB5
0060:  B2B3 B8BF D35A 4138 3331 3339 435F CEBD B6B1 B1B4
0080:  BBC9 7C48 3B34 3131 363D 4FDE

```

Tx Message 7:

```

packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:  0000 4AC5 5F08 9131 0000 003C 66DE 66EB 67EE FE6E
0020:  F7E7 6B68 E068 EE6A DF5C DF62 EDF1 6FF2 7A78 67DC
0040:  5EDF 62E7 64E6 66E0 7071 EA69 F86E E260 DE5D E665
0060:  EB75 F0FB 6DE9 64E4 69E3 66EA 67E9 6DF9 F177 EC6E
0080:  EB6E F876 F875 7D6E E966 E05D

```

Tx Message 8:

```

packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:  0000 1CDB 3E48 3AD4 0000 003C C2B9 B3B1 B3B8 C2DC
0020:  523F 3733 3235 3C49 72CB BDB7 B4B5 B8BF CF67 483C
0040:  3836 373C 455C DAC6 BDB9 B9BB C0CC EE54 453E 3C3C
0060:  3F47 56F1 D1C7 C1BF C0C6 CEE1 6651 4A46 4648 4D59
0080:  70E3 D6CF CDCE D2D9 E67E 675E

```

Bootloader 1.8, Appn 3.1

Application firmware 3.1.8, Built by claux on Thu Jun 17 11:00:05 1999

```

VIC Interface Foreign Exchange Station 0/0, DSP instance (0x19543C0)
Singalling channel num 128 Signalling proxy 0x0 Signaling dsp 0x19543C0
tx outstanding 0, max tx outstanding 32
ptr 0x0, length 0x0, max length 0x0
dsp_number 0, Channel ID 1
received 0 packets, 0 bytes, 0 gaint packets
0 drops, 0 no buffers, 0 input errors 0 input overruns
650070 bytes output, 4976 frames output, 0 output errors, 0 output
underrun
0 unaligned frames

```

```

VIC Interface Foreign Exchange Station 0/1, DSP instance (0x1954604)
Singalling channel num 129 Signalling proxy 0x0 Signaling dsp 0x1954604
tx outstanding 0, max tx outstanding 32
ptr 0x0, length 0x0, max length 0x0
dsp_number 0, Channel ID 2
received 0 packets, 0 bytes, 0 gaint packets

```

■ **show controllers voice**

```
0 drops, 0 no buffers, 0 input errors 0 input overruns
393976 bytes output, 3982 frames output, 0 output errors, 0 output
underrun
0 unaligned frames
```

Related Commands

Command	Description
show dial-peer voice	Displays configuration information and call statistics for dial peers.
show interface dspfarm	Displays hardware informatio,n including DRAM, SRAM, and the revision-level information on the line card.
show voice dsp	Displays the current status of all DSP voice channels on the Cisco MC3810 multiservice concentrator.
show voice port	Displays configuration information about a specific voice port.

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/dsp/dsp-channel]}
```

Cisco AS5800 Universal Access Server

```
show csm voice [shelf/slot/port]
```

Syntax Description	modem	Specifies CSM call statistics for modems.
	voice	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/dsp/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.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	11.3 NA	This command was introduced.
	12.0(3)T	Port-specific values for the Cisco AS5300 universal access server were added.
	12.0(7)T	Port-specific values for the Cisco AS5800 were added.

Usage Guidelines	This command shows the information related to CSM, which includes the DSP channel, the start time of the call, the end time of the call, and the channel on the controller used by the call.

Use the **show csm modem** command to display the CSM call statistic information for a specific modem, for a group of modems, or for all modems. If a *slot/port* argument is specified, then CSM call statistics are displayed for the specified modem. If the *modem-group-number* argument is specified, the CSM call statistics for all of the modems associated with that modem group are displayed. If no keyword is specified, CSM call statistics for all modems on the Cisco AS5300 universal access server are displayed.

Use the **show csm voice** command to display CSM statistics for a particular DSP channel. If the *slot/dsp/dsp/dsp-channel* or *shelf/slot/port* argument is specified, the CSM call statistics for calls using the identified DSP channel will be displayed. If no argument is specified, all CSM call statistics for all DSP channels will be displayed.

Examples

The following is sample output from the Cisco AS5300 universal access server for the **show csm voice** command:

```
Router# show csm voice 2/4/4/0
```

```
slot 2, dspm 4, dsp 4, dsp channel 0,
slot 2, port 56, tone, device_status(0x0002): VDEV_STATUS_ACTIVE_CALL.
```

```
csm_state(0x0406)=CSM_OC6_CONNECTED, csm_event_proc=0x600E2678, current call thru PRI line
invalid_event_count=0, wdt_timeout_count=0
wdt_timestamp_started is not activated
wait_for_dialing:False, wait_for_bchan:False
pri_chnl=TDM_PRI_STREAM(s0, u0, c22), tdm_chnl=TDM_DSP_STREAM(s2, c27)
dchan_idb_start_index=0, dchan_idb_index=0, call_id=0xA003, bchan_num=22
csm_event=CSM_EVENT_ISDN_CONNECTED, cause=0x0000
ring_no_answer=0, ic_failure=0, ic_complete=0
dial_failure=0, oc_failure=0, oc_complete=3
oc_busy=0, oc_no_dial_tone=0, oc_dial_timeout=0
remote_link_disc=0, stat_busyout=0
oobp_failure=0
call_duration_started=00:06:53, call_duration_ended=00:00:00, total_call_duration=00:00:44
The calling party phone number = 408
The called party phone number = 5271086
total_free_rbs_timeslot = 0, total_busy_rbs_timeslot = 0, total_dynamic_busy_rbs_timeslot
= 0, total_static_busy_rbs_timeslot = 0,
total_sw56_rbs_timeslot = 0, total_sw56_rbs_static_bo_ts = 0,
total_free_isdn_channels = 21, total_busy_isdn_channels = 0, total_auto_busy_isdn_channels
= 0,
min_free_device_threshold = 0
```

The following is sample output from the Cisco AS5800 for the **show csm voice** command:

```
Router# show csm voice 1/8/19
```

```
shelf 1, slot 8, port 19
VDEV_INFO:slot 8, port 19
vdev_status(0x00000401):VDEV_STATUS_ACTIVE_CALL.VDEV_STATUS_HASLOCK.
csm_state(0x00000406)=CSM_OC6_CONNECTED, csm_event_proc=0x60868B8C, current
call thru PRI line
invalid_event_count=0, wdt_timeout_count=0
watchdog timer is not activated
wait_for_bchan:False
pri_chnl=(T1 1/0/0:22), vdev_chnl=(s8, c19)
start_chan_p=0, chan_p=62436D58, call_id=0x800D, bchan_num=22
The calling party phone number =
The called party phone number = 7511
ring_no_answer=0, ic_failure=0, ic_complete=0
dial_failure=0, oc_failure=0, oc_complete=1
oc_busy=0, oc_no_dial_tone=0, oc_dial_timeout=0
remote_link_disc=0, busyout=0, modem_reset=0
call_duration_started=3d16h, call_duration_ended=00:00:00,
total_call_duration=00:00:00
```

Table 34 describes the significant fields shown in the display.

Table 34 *show csm voice Field Descriptions*

Field	Description
slot	Slot where the VFC resides.
shelf/slot/port	Specifies the T1 or E1 controller.
dspm/dsp/dsp channel	Indicates which DSP channel is engaged in this call.
dsp	Indicates the DSP through which this call is established.
slot/port	Logical port number for the device. This is equivalent to the DSP channel number. The port number is derived as follows: • $(\text{max\_number\_of\_dsp\_channels per dspm}=12) * \text{the dspm \# (0-based)} +$ • $(\text{max\_number\_of\_dsp\_channels per dsp}=2) * \text{the dsp \# (0-based)} + \text{the dsp channel number (0-based)}.$
tone	Indicates which signaling tone is being used (DTMF, MF, R2). This only applies to CAS calls. Possible values are as follows: • mf • dtmf • r2-compelled • r2-semi-compelled • r2-non-compelled

Table 34 *show csm voice Field Descriptions (continued)*

Field	Description
device_status	The status of the device. Possible values are as follows: • VDEV_STATUS_UNLOCKED—Device is unlocked (meaning that it is available for new calls). • VDEV_STATUS_ACTIVE_WDT—Device is allocated for a call and the watchdog timer is set to time the connection response from the central office. • VDEV_STATUS_ACTIVE_CALL—Device is engaged in an active, connected call. • VDEV_STATUS_BUSYOUT_REQ—Device is requested to busyout; does not apply to voice devices. • VDEV_STATUS_BAD—Device is marked as bad and not usable for processing calls. • VDEV_STATUS_BACK2BACK_TEST—Modem is performing back-to-back testing (for modem calls only). • VDEV_STATUS_RESET—Modem needs to be reset (for modem only). • VDEV_STATUS_DOWNLOAD_FILE—Modem is downloading a file (for modem only). • VDEV_STATUS_DOWNLOAD_FAIL—Modem has failed during downloading a file (for modem only). • VDEV_STATUS_SHUTDOWN—Modem is not powered up (for modem only). • VDEV_STATUS_BUSY—Modem is busy (for modem only). • VDEV_STATUS_DOWNLOAD_REQ—Modem is requesting connection (for modem only).

Table 34 *show csm voice Field Descriptions (continued)*

Field	Description
csm_state	CSM call state of the current call (PRI line) associated with this device. Possible values are as follows: • CSM_IDLE_STATE—Device is idle. • CSM_IC_STATE—A device has been assigned to an incoming call. • CSM_IC1_COLLECT_ADDR_INFO—A device has been selected to perform ANI/DNIS address collection for this call. ANI/DNIS address information collection is in progress. The ANI/DNIS is used to decide whether the call should be processed by a modem or a voice DSP. • CSM_IC2_RINGING—The device assigned to this incoming call has been told to get ready for the call. • CSM_IC3_WAIT_FOR_SWITCH_OVER—A new device is selected to take over this incoming call from the device collecting the ANI/DNIS address information. • CSM_IC4_WAIT_FOR_CARRIER—This call is waiting for the CONNECT message from the carrier. • CSM_IC5_CONNECTED—This incoming call is connected to the central office. • CSM_IC6_DISCONNECTING—This incoming call is waiting for a DISCONNECT message from the VTSP module to complete the disconnect process. • CSM_OC_STATE —An outgoing call is initiated. • CSM_OC1_REQUEST_DIGIT—The device is requesting the first digit for the dial-out number. • CSM_OC2_COLLECT_1ST_DIGIT—The first digit for the dial-out number has been collected. • CSM_OC3_COLLECT_ALL_DIGIT—All the digits for the dial-out number have been collected. • CSM_OC4_DIALING—This call is waiting for a dsx0 (B channel) to be available for dialing out. • CSM_OC5_WAIT_FOR_CARRIER—This (outgoing) call is waiting for the central office to connect. • CSM_OC6_CONNECTED—This (outgoing) call is connected. • CSM_OC7_BUSY_ERROR—A busy tone has been sent to the device (for VoIP call, no busy tone is sent; just a DISCONNECT INDICATION message is sent to the VTSP module), and this call is waiting for a DISCONNECT message from the VTSP module (or ONHOOK message from the modem) to complete the disconnect process. • CSM_OC8_DISCONNECTING—The central office has disconnected this (outgoing) call, and the call is waiting for a DISCONNECT message from the VTSP module to complete the disconnect process.

Table 34 *show csm voice Field Descriptions (continued)*

Field	Description
csm_state: invalid_event_count=	Number of invalid events received by the CSM state machine.
wdt_timeout_count=	Number of times the watchdog timer is activated for this call.
wdt_timestamp_started	Indicates whether the watchdog timer is activated for this call.
wait_for_dialing:	Indicates whether this (outgoing) call is waiting for a free digit collector to become available to dial out the outgoing digits.
wait_for_bchan:	Indicates whether this (outgoing) call is waiting for a B channel to send the call out on.
pri_chnl=	Indicates which type of TDM stream is used for the PRI connection. For PRI and CAS calls, it will always be TDM_PRI_STREAM.
tdm_chnl=	Indicates which type of TDM stream is used for the connection to the device used to process this call. In the case of a VoIP call, this will always be set to TDM_DSP_STREAM.
dchan_idb_start_index=	First index to use when searching for the next IDB of a free D channel.
dchan_idb_index=	Index of the currently available IDB of a free D channel.
csm_event=	Event just passed to the CSM state machine.
cause	Event cause.
ring_no_answer=	Number of times a call failed because there was no response.
ic_failure=	Number of failed incoming calls.
ic_complete=	Number of successful incoming calls.
dial_failure=	Number of times a connection failed because there was no dial tone.
oc_failure=	Number of failed outgoing calls.
oc_complete=	Number of successful outgoing calls.
oc_busy=	Number of outgoing calls whose connection failed because there was a busy signal.
oc_no_dial_tone=	Number of outgoing calls whose connection failed because there was no dial tone.
oc_dial_timeout=	Number of outgoing calls whose connection failed because the timeout value was exceeded.
call_duration_started=	Indicates the start of this call.
call_duration_ended=	Indicates the end of this call.
total_call_duration=	Indicates the duration of this call.
The calling party phone number =	Calling party number as given to CSM by ISDN.
The called party phone number =	Called party number as given to CSM by ISDN.
total_free_rbs_time slot =	Total number of free RBS (CAS) time slots available for the whole system.

Table 34 *show csm voice Field Descriptions (continued)*

Field	Description
total_busy_rbs_time slot =	Total number of RBS (CAS) time slots that have been busied-out. This includes both dynamically and statically busied out RBS time slots.
total_dynamic_busy_rbs_time slot =	Total number of RBS (CAS) time slots that have been dynamically busied out.
total_static_busy_rbs_time slot =	Total number of RBS (CAS) time slots that have been statically busied out (that is, they are busied out using the CLI command).
total_free_isdn_channels =	Total number of free ISDN channels.
total_busy_isdn_channels =	Total number of busy ISDN channels.
total_auto_busy_isdn_channels =	Total number of ISDN channels that are automatically busied out.

Related Commands

Command	Description
show call active voice	Displays the contents of the active call table.
show call history voice	Displays the contents of the call history table.
show num-exp	Displays how number expansions are configured.
show voice port	Displays configuration information about a specific voice port.

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**]

Syntax Description	<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.
	summary	(Optional) Displays a summary of all video dial peer information.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(5)XK	This command was introduced for the Cisco MC3810 multiservice concentrator.
	12.0(7)T	The command introduced in Cisco IOS Release 12.0(5)XK was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines Use this command to review video dial peer configuration.

Examples On a Cisco MC3810 multiservice concentrator, the following example displays detailed information about all configured video dial peers:

```
Router# show dial-peer video
```

```
Video Dial-Peer 1
  type = videocodec, destination-pattern = 111
  port signal = 1/0, port media = Serial1
  nsap = 47.0091810000000050E201B101.00107B09C6F2.C8
Video Dial-Peer 2
  type = videoatm, destination-pattern = 222
  session-target = ATM0 svc nsap 47.0091810000000050E201B101.00E01E92ADC2.C8
Video Dial-Peer 3
  type = videoatm, destination-pattern = 333
  session-target = ATM0 pvc 70/70
```


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.
	<i>summary</i>	(Optional) Displays a summary of all voice dial peers.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	11.3(1)T	This command was introduced.
	11.3(1)MA	The summary keyword was added for the Cisco MC3810 multiservice concentrator.
	12.0(3)XG	This command was modified to support Voice over Frame Relay (VoFR) for the Cisco 2600 series and Cisco 3600 series routers.
	12.0(4)T	Support was added for VoFR for the Cisco 7200 series routers.
	12.1(3)T	This command was modified for Modem Passthrough over Voice over IP on the Cisco AS5300 universal access server.

Usage Guidelines	Use the show dial-peer voice privileged EXEC command to display the configuration for all Voice over IP (VoIP) and plain old telephone service (POTS) dial peers configured for the router. To show configuration information for only one specific dial peer, use the argument <i>number</i> to identify the dial peer.

Examples	The following is sample output from the show dial-peer voice command for a POTS dial peer:

```
Router# show dial-peer voice 1

VoiceEncapPeer1
  tag = 1, dest-pat = '+14085291000',
  answer-address = '',
  group = 0, Admin state is up, Operation state is down
  Permission is Both,
  type = pots, prefix = '',
  session-target = '', voice port =
  Connect Time = 0, Charged Units = 0
```

■ **show dial-peer voice**

```

Successful Calls = 0, Failed Calls = 0
Accepted Calls = 0, Refused Calls = 0
Last Disconnect Cause is ""
Last Disconnect Text is ""
Last Setup Time = 0

```

The following is sample output from the **show dial-peer voice** command for a VoIP dial peer:

Router# **show dial-peer voice 10**

```

VoiceOverIpPeer10
  tag = 10, dest-pat = '',
  incall-number = '+14087',
  group = 0, Admin state is up, Operation state is down
  Permission is Answer,
  type = voip, session-target = '',
  sess-proto = cisco, req-qos = bestEffort,
  acc-qos = bestEffort,
  fax-rate = voice, codec = g729r8,
  Expect factor = 10, Icpif = 30, VAD = disabled, Poor QOV Trap = disabled,
  Connect Time = 0, Charged Units = 0
  Successful Calls = 0, Failed Calls = 0
  Accepted Calls = 0, Refused Calls = 0
  Last Disconnect Cause is ""
  Last Disconnect Text is ""
  Last Setup Time = 0

```

[Table 35](#) provides an alphabetical listing of the **show dial-peer voice** output fields and a description of each field.

Table 35 *show dial-peer voice Field Descriptions*

Field	Description
Accepted Calls	Number of calls accepted from this peer since system startup.
acc-qos	Lowest acceptable quality of service configured for calls for this peer.
Admin state	Administrative state of this peer.
answer-address	Answer address configured for this dial peer.
Charged Units	Total number of charging units applying to this peer since system startup. The unit of measure for this field in hundredths of a second.
codec	Default voice coder rate of speech for this peer.
Connect Time	Accumulated connect time to the peer since system startup for both incoming and outgoing calls. The unit of measure for this field is in hundredths of a second.
dest-pat	Destination pattern (telephone number) for this peer.
DTMF Relay	Indicates whether or not dual-tone multifrequency (DTMF) relay has been enabled, by using the dtmf-relay command, for this dial peer.
Expect factor	User-requested Expectation Factor of voice quality for calls through this peer.
fax-rate	Fax transmission rate configured for this peer.
Failed Calls	Number of failed call attempts to this peer since system startup.
group	Group number associated with this peer.

Table 35 *show dial-peer voice Field Descriptions (continued)*

Field	Description
huntstop	Indicates whether dial-peer hunting has been turned on, by using the huntstop command, for this dial peer.
Icpif	Configured Calculated Planning Impairment Factor (ICPIF) value for calls sent by a dial peer.
incall-number	Full E.164 telephone number to be used to identify the dial peer.
incoming called-number	Indicates the incoming called number if it has been set by using the incoming-called number command.
information type	Information type for this call; for example, voice or fax.
Last Disconnect Cause	Encoded network cause associated with the last call. This value will be updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface.
Last Disconnect Text	ASCII text describing the reason for the last call termination.
Last Setup Time	Value of the System Up Time when the last call to this peer was started.
Modem passthrough	Modem pass-through signaling method is named signaling event (NSE).
Operation state	Operational state of this peer.
Payload type	NSE payload type.
Permission	Configured permission level for this peer.
Poor QOV Trap	Whether Poor Quality of Voice trap messages have been enabled or disabled.
Redundancy	Packet redundancy (RFC 2198) for modem traffic.
Refused Calls	Number of calls from this peer refused since system startup.
req-qos	Configured requested quality of service for calls for this dial peer.
session-target	Session target of this peer.
sess-proto	Session protocol to be used for Internet calls between local and remote routers through the IP backbone.
Successful Calls	Number of completed calls to this peer.
tag	Unique dial peer ID number.
VAD	Whether voice activation detection (VAD) is enabled for this dial peer.

Related Commands

Command	Description
show call active voice	Displays the Voice over IP active call table.
show call history voice	Displays the Voice over IP call history table.
show num-exp	Displays how the number expansions are configured in Voice over IP.
show voice port	Displays configuration information about a specific voice port.

show dialplan incall number

To show which plain old telephone service (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* [**timeout**]

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 voice-port global configuration command.
<i>calling-number</i>	Specifies the calling number or ANI of the incoming voice call.
timeout	(Optional) Allows matching for variable-length destination patterns.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series router.
12.2(8)T	The timeout keyword was added.

Usage Guidelines

Use the **show dialplan incall number** command as a troubleshooting tool to determine which POTS dial peer is matched for an incoming call, for the selected calling number and voice port. When using the **show dialplan incall number** command, the router attempts to match these items in the order listed:

1. Calling number with answer-address configured in dial peer
2. Calling number with destination-pattern configured in dial peer
3. Voice port with voice port configured in dial peer

The router first attempts to match a dial peer based on the calling number (ANI). If the router is unable to match a dial peer based on the calling number, it matches the call to a POTS dial peer based on the selected voice interface. If more than one dial peer uses the same voice port, the router selects the first matching dial peer. Use the **timeout** keyword to enable matching variable-length destination patterns associated with dial peers. This can increase your chances of finding a match for the dial peer number you specify.



Note

For actual voice calls coming into the router, the router attempts to match the called number (the dialed number identification service [DNIS] number) with the incoming called-number configured in a dial peer. The router, however, does not consider the called number when using the **show dialplan incall number** command.

Examples

The following example shows that an incoming call from interface 1/0/0:D with a calling number of 12345 is matched to POTS dial peer 10:

```
Router# show dialplan incall 1/0/0:D number 12345
```

```
Macro Exp.: 12345
```

```
VoiceEncapPeer10
  information type = voice,
  tag = 10, destination-pattern = `123..',
  answer-address = `', preference=0,
  numbering Type = `unknown'
  group = 10, Admin state is up, Operation state is up,
  incoming called-number = `', connections/maximum = 0/unlimited,
  DTMF Relay = disabled,
  huntstop = disabled,
  in bound application associated: DEFAULT
  out bound application associated:
  permission :both
  incoming COR list:maximum capability
  outgoing COR list:minimum requirement
  type = pots, prefix = `',
  forward-digits default
  session-target = `', voice-port = `1/0/0:D',
  direct-inward-dial = disabled,
  digit_strip = enabled,

  register E.164 number with GK = TRUE
  Connect Time = 0, Charged Units = 0,

  register E.164 number with GK = TRUE
  Connect Time = 0, Charged Units = 0,
  Successful Calls = 0, Failed Calls = 0,
  Accepted Calls = 0, Refused Calls = 0,
  Last Disconnect Cause is "",
  Last Disconnect Text is "",
  Last Setup Time = 0.
Matched: 12345   Digits: 3
Target:
```

The following example shows that if no dial peer has a destination pattern or answer address that matches the calling number of 888, the incoming call is matched to POTS dial peer 99, because the call comes in on voice port 1/0/1:D, which is the voice port configured for this dial peer:

```
Router# show dialplan incall 1/0/1:D number 888
```

```
Macro Exp.: 888
```

```
VoiceEncapPeer99
  information type = voice,
  tag = 99, destination-pattern = `99...',
  answer-address = `', preference=1,
  numbering Type = `national'
  group = 99, Admin state is up, Operation state is up,
  incoming called-number = `', connections/maximum = 0/unlimited,
  DTMF Relay = disabled,
  huntstop = disabled,
  in bound application associated: DEFAULT
  out bound application associated:
  permission :both
  incoming COR list:maximum capability
  outgoing COR list:minimum requirement
  type = pots, prefix = `5',
```

show dialplan incall number

```

forward-digits 4
session-target = '', voice-port = '1/0/1:D',
direct-inward-dial = enabled,
digit_strip = enabled,

register E.164 number with GK = TRUE
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0,
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
Matched:      Digits: 0
Target:

```

Table 36 describes the significant fields shown in the display.

Table 36 *show dialplan number Field Descriptions*

Field	Description
Macro Exp.	Expected destination pattern for this dial peer.
VoiceEncapPeer	Dial peer associated with the calling number entered.
tag	Unique number identifying the dial peer.
destination-pattern	Destination pattern (telephone number) configured for this dial peer.
answer-address	Answer address (calling number) configured for this dial peer.
preference	Hunt group preference order set for this dial peer.
Admin state	Describes the administrative state of this dial peer.
Operation state	Describes the operational state of this dial peer.
incoming called-number	Called number (DNIS) configured for this dial peer.
DTMF Relay	Whether the dtmf-relay command is enabled or disabled for this dial peer.
huntstop	Whether the huntstop command is enabled or disabled for this dial peer.
in bound application associated	The IVR application that is associated with this dial peer when this dial peer is used for an inbound call leg.
out bound application associated	The IVR application that is associated with this dial peer when this dial peer is used for an outbound call leg.
type	Type of dial peer (POTS or VoIP).
prefix	The prefix number that is added to the front of the dial string before it is forwarded to the telephony device.
forward-digits	Which digits are forwarded to the telephony interface as configured using the forward-digits command.
session-target	Displays the configured session target (IP address or host name) for this dial peer.
voice-port	The voice port through which calls come into this dial peer.
direct-inward-dial	Whether the direct-inward-dial command is enabled or disabled for this dial peer.

Table 36 *show dialplan number Field Descriptions (continued)*

Field	Description
digit_strip	Whether digit stripping is enabled or disabled in the dial peer. Enabled is the default.
session-protocol	Session protocol to be used for Internet calls between local and remote router via the IP backbone.
Connect Time	Unit of measure indicating the call connection time associated with this dial peer.
Charged Units	Number of call units charged to this dial peer.
Successful Calls	Number of completed calls to this peer since system startup.
Failed Calls	Number of uncompleted (failed) calls to this peer since system startup.
Accepted Calls	Number of calls from this peer accepted since system startup.
Refused Calls	Number of calls from this peer refused since system startup.
Last Disconnect Cause	Encoded network cause associated with the last call. This value will be updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface.
Last Disconnect Text	ASCII text describing the reason for the last call termination.
Last Setup Time	Value of the System Up Time when the last call to this peer was started.
Matched	Destination pattern matched for this dial peer.
Target	Matched session target (IP address or host name) for this dial peer.

Related Commands

Command	Description
show dial peer voice	Displays the configuration information for dial peers.
show dialplan number	Displays which dial peer is matched for a particular telephone number.

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* [**huntstop**] [**timeout**]

Syntax Description

<i>dial string</i>	Specifies a particular destination pattern (telephone number).
huntstop	(Optional) Terminates further dial-peer hunting upon encountering the first dial string match.
timeout	(Optional) Allows matching for variable-length destination patterns.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series router.
12.2(1)	The huntstop keyword was added.
12.2(8)T	The timeout keyword was added.

Usage Guidelines

The **show dialplan number** command is used to test whether the dial plan configuration is valid and working as expected. Use the **timeout** keyword to enable matching variable-length destination patterns associated with dial peers. This can increase your chances of finding a match for the dial peer number you specify.

Examples

The following example shows sample output from the **show dialplan number** command using the destination pattern of 1001:

```
Router# show dialplan number 1001
```

```
Macro Exp.: 1001
```

```
VoiceEncapPeer1003
  information type = voice,
  tag = 1003, destination-pattern = `1001',
  answer-address = `', preference=0,
  numbering Type = `unknown'
  group = 1003, Admin state is up, Operation state is up,
  incoming called-number = `', connections/maximum = 0/unlimited,
  DTMF Relay = disabled,
  huntstop = enabled,
  type = pots, prefix = `',
  forward-digits default
  session-target = `', voice-port = `1/1',
```



```

        direct-inward-dial = disabled,
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched: 1001   Digits: 4
Target:

VoiceEncapPeer1004
    information type = voice,
    tag = 1004, destination-pattern = `1001',
    answer-address = `', preference=0,
    numbering Type = `unknown'
    group = 1004, Admin state is up, Operation state is up,
...
Matched: 1001   Digits: 4
Target:

VoiceEncapPeer1002
    information type = voice,
    tag = 1002, destination-pattern = `1001',
    answer-address = `', preference=0,
    numbering Type = `unknown'
    group = 1002, Admin state is up, Operation state is up,
...
Matched: 1001   Digits: 4
Target:

VoiceEncapPeer1001
    information type = voice,
    tag = 1001, destination-pattern = `1001',
    answer-address = `', preference=0,
    numbering Type = `unknown'
    group = 1001, Admin state is up, Operation state is up,
...
Matched: 1001   Digits: 4
Target:

```

The following example shows sample output from the **show dialplan number** command using the destination pattern of 1001 and the **huntstop** keyword:

Router# **show dialplan number 1001 huntstop**

Macro Exp.: 1001

```

VoiceEncapPeer1003
    information type = voice,
    tag = 1003, destination-pattern = `1001',
    answer-address = `', preference=0,
    numbering Type = `unknown'
    group = 1003, Admin state is up, Operation state is up,
    incoming called-number = `', connections/maximum = 0/unlimited,
    DTMF Relay = disabled,
    huntstop = enabled,
    type = pots, prefix = `',
    forward-digits default
    session-target = `', voice-port = `1/1',
    direct-inward-dial = disabled,
    Connect Time = 0, Charged Units = 0,
    Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
    Accepted Calls = 0, Refused Calls = 0,
    Last Disconnect Cause is "",

```

show dialplan number

```

Last Disconnect Text is "",
Last Setup Time = 0.
Matched: 1001   Digits: 4
Target:

```

Table 37 explains the significant fields shown in this example.

Table 37 *show dialplan number Field Descriptions*

Field	Description
Macro Exp.	Expected destination pattern for this dial peer.
VoiceEncapPeer	Dial peer associated with the destination pattern entered.
type	Type of dial peer (POTS or VoIP).
tag	Unique dial peer identifying number.
destination-pattern	Destination pattern (telephone number) configured for this dial peer.
answer-address	Answer address configured for this dial peer.
Admin state	Administrative state of this dial peer.
Operation state	Operational state of the dial peer.
session-target	Configured session target (IP address or host name) for this dial peer.
Connect Time	Unit of measure indicating the call connection time associated with this dial peer.
Charged Units	Number of call units charged to this dial peer.
Successful Calls	Number of completed calls to this peer since system startup.
Failed Calls	Number of uncompleted (failed) calls to this peer since system startup.
Accepted Calls	Number of calls accepted from this peer since system startup.
Refused Calls	Number of calls refused from this peer since system startup.
Last Disconnect Cause	Encoded network cause associated with the last call. This value will be updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface.
Last Disconnect Text	ASCII text describing the reason for the last call termination.
Last Setup Time	Value of the System Up Time when the last call to this peer was started.
Matched	Destination pattern matched for this dial peer.
Target	Matched session target (IP address or host name) for this dial peer.

Related Commands

Command	Description
show dialplan incall number	Pairs different voice ports and telephone numbers together for troubleshooting Voice over IP.

show frame-relay vofr

To display information about the FRF.11 subchannels being used on Voice over Frame Relay (VoFR) data link connection identifiers (DLCIs), use the **show frame-relay vofr** command in privileged EXEC mode.

show frame-relay vofr [*interface* [*dlci* [*cid*]]]

Syntax Description	<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.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(4)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco MC3810 multiservice concentrator.
	12.0(4)T	This command was integrated in Cisco IOS Release 12.0(4)T.

Usage Guidelines If this command is entered without a specified interface, FRF.11 subchannel information will be displayed for all VoFR interfaces and DLCIs configured on the router.



Note

This command is currently not supported on the Cisco MC3810 multiservice concentrator for PVCs configured with the **vofr cisco** command or the **frame-relay interface-dlci voice-encap** command.

Examples The following is sample output from the **show frame-relay vofr** command when an interface is not specified:

Router# **show frame-relay vofr**

interface	vofr-type	dlci	cid	cid-type
Serial0/0.1	VoFR	16	4	data
Serial0/0.1	VoFR	16	5	call-control
Serial0/0.1	VoFR	16	10	voice
Serial0/1.1	VoFR cisco	17	4	data

■ **show frame-relay vofr**

The following is sample output from the **show frame-relay vofr** command when an interface is specified:

```
Router# show frame-relay vofr serial0

interface      vofr-type  dlci  cid  cid-type
Serial0        VoFR       16    4    data
Serial0        VoFR       16    5    call-control
Serial0        VoFR       16    10   voice
```

The following is sample output from the **show frame-relay vofr** command when an interface and a DLCI are specified:

```
Router# show frame-relay vofr serial0 16

VoFR Configuration for interface Serial0

dlci vofr-type  cid cid-type      input-pkts  output-pkts  dropped-pkts
16   VoFR       4   data          0           0            0
16   VoFR       5   call-control  85982       86099       0
16   VoFR       10  voice        2172293     6370815     0
```

The following is sample output from the **show frame-relay vofr** command when an interface, a DLCI, and a CID are specified:

```
Router# show frame-relay vofr serial0 16 10

VoFR Configuration for interface Serial0 dlci 16

      vofr-type VoFR      cid 10      cid-type voice
      input-pkts 2172293  output-pkts 6370815  dropped-pkts 0
```

[Table 38](#) describes the significant fields shown in the display.

Table 38 *show frame-relay vofr Field Descriptions*

Field	Description
interface	Number of the interface that has been selected for observation of FRF.11 subchannels.
vofr-type	Type of VoFR DLCI being observed.
cid	The portion of the specified DLCI that is carrying the designated traffic type. A DLCI can be subdivided into 255 subchannels.
cid-type	Type of traffic carried on this subchannel.
input-pkts	Number of packets received by this subchannel.
output-pkts	Number of packets sent on this subchannel.
dropped-pkts	Total number of packets discarded by this subchannel.

Related Commands

Command	Description
show call active voice	Displays the contents of the active call table.
show call history voice	Displays the contents of the call history table.
show dial-peer voice	Displays configuration information and call statistics for dial peers.
show frame-relay fragment	Displays Frame Relay fragmentation details.

Command	Description
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show voice-port	Displays configuration information about a specific voice port.

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.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.3(2)NA	This command was introduced.
	12.0(3)T	The command introduced in Cisco IOS Release 11.3(2)NA was integrated into Cisco IOS Release 12.0(3)T.
	12.0(5)T	The output for this command was changed.

Usage Guidelines Use the **show gatekeeper calls** command to show all active calls currently being handled by a particular MCM gatekeeper. If you have forced a disconnect for either a particular call or all calls associated with a particular MCM gatekeeper by using the **clear h323 gatekeeper call** command, the system will not display information about those calls.

Examples The following is sample output from the **show gatekeeper calls** command:

```
Router# show gatekeeper calls
```

```
Total number of active calls = 1.
```

```

                                GATEKEEPER CALL INFO
                                =====
LocalCallID                    Age (secs)    BW
12-3339                        94         768 (Kbps)
Endpt(s):Alias                  E.164Addr    CallSignalAddr  Port  RASSignalAddr  Port
src EP:epA                      90.0.0.11    1720  90.0.0.11      1700
dst EP:epB@zoneB.com
src PX:pxA                      90.0.0.01    1720  90.0.0.01      24999
dst PX:pxB                      172.21.139.90 1720  172.21.139.90  24999
```

Table 39 describes the significant fields shown in the display.

Table 39 *show gatekeeper calls Field Descriptions*

Field	Description
LocalCallID	Identification number of the call.
Age(secs)	The age of the call in seconds.
BW(Kbps)	The bandwidth in use, in kilobits per second.
Endpoint(s)	Lists the role of each endpoint (terminal, gateway, or proxy) in the call (originator, target, or proxy), and the call signaling and registration, admission, and status (RAS) protocol address.
Alias	H.323-ID or Email-ID of the endpoint.
E.164Addr	E.164 address of the endpoint.
CallSignalAddr	Call signaling IP address of the endpoint.
Port	Call signaling port number of the endpoint.
RASSignalAddr	RAS IP address of the endpoint.
Port	RAS port number of the endpoint.

Related Commands

Command	Description
clear h323 gateway call	Forces a specific call or all calls currently active on the gatekeeper to disconnect.

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.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	11.3(2)NA	This command was introduced.
	12.0(5)T	The display format was modified for H.323 Version 2.

Usage Guidelines Use this command to display the status of all registered endpoints for a gatekeeper.

Examples The following is sample output from the **show gatekeeper endpoints** command:

```
Router# show gatekeeper endpoints

CallSignalAddr  Port  RASignalAddr  Port  Zone Name  Type  F
-----
172.21.127.8    1720  172.21.127.8  24999 sj-gk      MCU
              H323-ID:joe@cisco.com
172.21.13.88    1720  172.21.13.88  1719  sj-gk      VOIP-GW  O    H323-ID:la-gw
```

[Table 40](#) describes the significant fields shown in the display.

Table 40 show gatekeeper endpoints Field Descriptions

Field	Description
CallSignalAddr	Call signaling IP address of the endpoint. If the endpoint is also registered with alias, a list of all aliases registered for that endpoint should be listed on the line below.
Port	Call signaling port number of the endpoint.
RASignalAddr	Registration, admission, and status (RAS) protocol IP address of the endpoint.
Port	RAS port number of the endpoint.
Zone Name	Zone name (gatekeeper ID) that this endpoint registered in.

Table 40 *show gatekeeper endpoints Field Descriptions (continued)*

Field	Description
Type	The endpoint type (for example, terminal, gateway, or MCU).
F	S—Indicates that the endpoint is statically entered from the alias command rather than being dynamically registered through RAS messages. O—Indicates that the endpoint, which is a gateway, has sent notification that it is nearly out of resources.

Related Commands

Command	Description
show gatekeeper gw-type-prefix	Displays the gateway technology prefix table.
show gatekeeper zone status	Displays the status of zones related to a gatekeeper.
show gateway	Displays the current gateway status.

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.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.3(2)NA	This command was introduced.
	12.0(5)T	The display format was modified for H.323 Version 2.

Usage Guidelines Use the **show gatekeeper gw-type-prefix** command to display the gateway technology prefix table.

Examples The following is sample output for a gatekeeper that is controlling two local zones, sj-gk and la-gk:

```
Router# show gatekeeper gw-type-prefix

GATEWAY TYPE PREFIX TABLE
=====
Prefix:12#*      (Default gateway-technology)
  Zone sj-gk master gateway list:
    172.21.13.11:1720 sj-gw1
    172.21.13.22:1720 sj-gw2 (out-of-resources)
    172.21.13.33:1720 sj-gw3
  Zone sj-gk prefix 408..... priority gateway list(s):
    Priority 10:
      172.21.13.11:1720 sj-gw1
    Priority 5:
      172.21.13.22:1720 sj-gw2 (out-of-resources)
      172.21.13.33:1720 sj-gw3
Prefix:7#*      (Hopoff zone la-gk)
  Statically-configured gateways (not necessarily currently registered):
    1.1.1.1:1720
    2.2.2.2:1720
  Zone la-gk master gateway list:
    171.69.127.11:1720 la-gw1
    171.69.127.22:1720 la-gw2
```

Table 41 describes the fields contained in the **show gatekeeper gw-type-prefix** sample output.

Table 41 *show gatekeeper gw-type-prefix Field Descriptions*

Field	Description
Prefix	The technology prefix defined with the gw-type-prefix command.
Zone sj-gk master gateway list	A list of all the gateways registered to zone sj-gk with the technology prefix, under which they are listed. (This display shows that gateways sj-gw1, sj-gw2, and sj-gw3 have registered in zone sj-gk with the technology prefix 12#.)
Zone sj-gk prefix 408..... priority gateway list(s)	A list of prioritized gateways to handle calls to area code 408.
Priority 10	Highest priority level. Gateways listed following “Priority 10” are given the highest priority when selecting a gateway to service calls to the specified area code. (In this display, gateway sj-gw1 is given the highest priority to handle calls to the 408 area code.)
Priority 5	Any gateway that does not have a priority level assigned to it defaults to priority 5.
(out-of-resources)	Indication that the displayed gateway has sent a “low-in-resources” notification.
(Hopoff zone la-gk)	Any call specifying this technology prefix should be directed to hop off in the la-gk zone, no matter what the area code of the called number is. (In this display, calls specifying technology prefix 7# are always routed to zone la-gk, regardless of the actual zone prefix in the destination address.)
Zone la-gk master gateway list	A list of all the gateways registered to la-gk with the technology prefix under which they are listed. (This display shows that gateways la-gw1 and la-gw2 have registered in zone la-gk with the technology prefix 7#. No priority lists are displayed here because none were defined for zone la-gk.)
(Default gateway-technology)	If no gateway-type prefix is specified in a called number, then gateways registering with 12# are the default type to be used for the call.
(Statically-configured gateways)	Lists all IP addresses and port numbers of gateways that are incapable of supplying technology-prefix information when they register. This display shows that when gateways 1.1.1.1:1720 and 2.2.2.2:1720 register, they will be considered to be of type 7#.

 **show gatekeeper gw-type-prefix**

Related Commands	Command	Description
	show gatekeeper calls	Displays the status of each ongoing call that a gatekeeper is aware of.
	show gatekeeper endpoints	Displays the status of all registered endpoints for a gatekeeper.
	show gateway	Displays the current gateway status.

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	<i>gkid</i> (Optional) The local gatekeeper name to which this trigger applies.

Command Modes	EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced on the Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines	Enter this command to show all server triggers (whether dynamically registered from the external servers or statically configured from the command line interface) on this gatekeeper. If <i>gkid</i> is specified, only triggers applied to the specified gatekeeper zone appear. If the <i>gkid</i> argument is not specified, server triggers for all local gatekeeper zones on this router appear.

Examples	This example shows the operating information of the specified gk102 server:

```
Router# show gatekeeper servers gk102

GATEKEEPER SERVERS STATUS
=====

Gatekeeper Server listening port:20000

Gatekeeper-ID:gk102
-----
RRQ  Priority:1
  Server-ID:sj-server
  Server IP address:1.14.93.28:42387
  Server type:dynamically registered
  Connection Status:active
  Trigger Information:
    Supported Prefix:10#
    Supported Prefix:3#
RRQ  Priority:2
  Server-ID:sf-server
  Server IP address:1.14.93.43:3820
  Server type:CLI-configured
  Connection Status:inactive
  Trigger Information:
    Endpoint-type:MCU
    Endpoint-type:VOIP-GW
    Supported Prefix:99#
```

show gatekeeper servers

```
ARQ  Priority:1
  Server-ID:sj-server
  Server IP address:1.14.93.28:42387
  Server type:dynamically registered
  Connection Status:active
  Trigger Information:
    Destination Info:M:nilkant@zone14.com
    Destination Info:E:1800.....
    Redirect Reason:Call forwarded no reply
    Redirect Reason:Call deflection
```

Related Commands

Command	Description
debug gatekeeper server	Traces all the message exchanges between the Cisco IOS gatekeeper and the external applications. Shows any errors that occur in sending messages to the external applications or in parsing messages from the external applications.

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.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	11.3(2)NA	This command was introduced.
	12.0(3)T	The command introduced in Cisco IOS Release 11.3(2)NA was integrated into Cisco IOS Release 12.0(3)T.

Examples The following is sample output from the **show gatekeeper status** command:

```
Router# show gatekeeper status
```

```
Gatekeeper State: UP  
Zone Name: gk-px4.cisco.com  
Accounting: DISABLED  
Security: DISABLED
```

[Table 42](#) describes the significant fields shown in the display.

Table 42 *show gatekeeper status Field Descriptions*

Field	Description
Gatekeeper State	Gatekeeper status has the following values: - UP is operational. - DOWN is administratively shut down. - INACTIVE is administratively enabled, that is, the no shutdown command has been issued, but no local zones have been configured. - HSRP STANDBY indicates that the gatekeeper is on hot standby and will take over when the currently active gatekeeper fails.
Zone Name	Zone name.
Accounting	Authorization and accounting status.
Security	Security status.

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.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Release	Modification
11.3(2)NA	This command was introduced.

Examples The following is an example of output from the **show gatekeeper zone prefix** command:

```
Router# show gatekeeper zone prefix
```

```

      ZONE PREFIX TABLE
      =====
GK-NAME      E164-PREFIX
-----
gk.zone13    212.....
gk.zone14    415.....
gk.zone14    408.....

```

[Table 43](#) describes the significant fields shown in the display.

Table 43 *show gatekeeper zone prefix Field Descriptions*

Field	Description
GK-NAME	Gatekeeper name.
E164-PREFIX	The E.164 prefix and a dot that acts as a wildcard for matching each remaining number in the telephone number.

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.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.3(2)NA	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers.
	12.0(5)T	This display format was modified for H.323 Version 2.

Usage Guidelines Use this command to display the status of all zones related to a gatekeeper.

Examples The following is an example of output from the **show gatekeeper zone status** command:

Router# **show gatekeeper zone status**

```

                                GATEKEEPER ZONES
                                =====
GK name      Domain Name    RAS Address    PORT  FLAGS  MAX-BW    CUR-BW
-----
sj.xyz.com   xyz.com      1.14.93.85     1719  LS           0
SUBNET ATTRIBUTES :
  All Other Subnets : (Enabled)
PROXY USAGE CONFIGURATION :
  inbound Calls from germany.xyz.com :
    to terminals in local zone sj.xyz.com :use proxy
    to gateways in local zone sj.xyz.com  :do not use proxy
  Outbound Calls to germany.xyz.com
    from terminals in local zone germany.xyz.com :use proxy
    from gateways in local zone germany.xyz.com  :do not use proxy
  Inbound Calls from all other zones :
    to terminals in local zone sj.xyz.com :use proxy
    to gateways in local zone sj.xyz.com  :do not use proxy
  Outbound Calls to all other zones :
    from terminals in local zone sj.xyz.com :do not use proxy
    from gateways in local zone sj.xyz.com  :do not use proxy
tokyo.xyz.co xyz.com      172.21.139.89   1719  RS           0
milan.xyz.co xyz.com      171.69.57.90    1719  RS           0

```

Table 44 describes the significant fields shown in the display.

Table 44 *show gatekeeper zone status Field Descriptions*

Field	Description
GK name	The gatekeeper name (also known as zone name), which is truncated after 12 characters in the display.
Domain Name	The domain with which the gatekeeper is associated.
RAS Address	The registration, admission, and status (RAS) protocol address of the gatekeeper.
FLAGS	Displays the following information: • S = static (CLI-configured, not DNS-discovered) • L = local • R = remote
MAX-BW	The maximum bandwidth for the zone, in kbps.
CUR-BW	The current bandwidth in use, in kbps.
SUBNET ATTRIBUTES	A list of subnets controlled by the local gatekeeper.
PROXY USAGE CONFIGURATION	Inbound and outbound proxy policies as configured for the local gatekeeper (or zone).

Related Commands

Command	Description
show gatekeeper calls	Displays the status of each ongoing call of which a gatekeeper is aware.
show gatekeeper endpoints	Displays the status of all registered endpoints for a gatekeeper.
show gateway	Displays the current gateway status.

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.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	11.3(6)NA2	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers.
	12.0(5)T	This display format was modified for H.323 V2.

Usage Guidelines	This command displays the current gateway status.

Examples	The following example shows the report that appears when the gateway is not registered with a gatekeeper:

```
Router# show gateway
```

```
Gateway gateway1 is not registered to any gatekeeper
Gateway alias list
H323-ID gateway1
H323 resource thresholding is Enabled but NOT Active
H323 resource threshold values:
    DSP: Low threshold 60, High threshold 70
    DS0: Low threshold 60, High threshold 70
```

This following example indicates that an E.164 address has been assigned to the gateway:

```
Router# show gate
```

```
Gateway gateway1 is registered to Gatekeeper gk1
Gateway alias list
E.164 Number 5551212
H323-ID gateway1
```

The following example shows the report that appears when the gateway is registered with a gatekeeper and H.323 resource threshold reporting is enabled with the **resource threshold** command:

```
Router# show gateway
```

```
Gateway gateway1 is registered to Gatekeeper gk1
Gateway alias list
```

 show gateway

```
H323-ID gateway1
H323 resource thresholding is Enabled and Active
H323 resource threshold values:
  DSP: Low threshold 60, High threshold 70
  DS0: Low threshold 60, High threshold 70
```

The following example shows the report that appears when the gateway is registered with a gatekeeper and H.323 resource threshold reporting is disabled with the **no resource threshold** command:

```
Router# show gateway
```

```
Gateway gateway1 is registered to Gatekeeper gk1
Gateway alias list
H323-ID gateway1
H323 resource thresholding is Disabled
```

Related Commands

Command	Description
resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.

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*]

Syntax Description	<i>slot</i>	(Optional) Slot location of the port adapter.
	<i>/port</i>	(Optional) Port number on the port adapter.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(5)XE	This command was introduced on the Cisco 7200 series router.
	12.1(1)T	This command was integrated into the Cisco IOS 12.1(1)T.

Usage Guidelines The local time-division multiplexing (TDM) cross-connect map can be displayed.

Examples The following example is sample output from the show interface dspfarm command for port adapter slot 0 of chassis slot 3, on the Cisco 7200 series router:

```
Router# show interface dspfarm 3/0

DSPfarm3/0 is up, line protocol is up
  Hardware is VXC-2T1/E1
  MTU 256 bytes, BW 12000 Kbit, DLY 0 usec,
    reliability 255/255, txload 4/255, rxload 1/255
  Encapsulation VOICE, loopback not set
  C549 DSP Firmware Version:MajorRelease.MinorRelease (BuildNumber)
    DSP Boot Loader:255.255 (255)
    DSP Application:4.0 (3)
    Medium Complexity Application:3.2 (5)
    High Complexity Application:3.2 (5)
  Total DSPs 30, DSP0-DSP29, Jukebox DSP id 30
  Down DSPs:none
  Total sig channels 120 used 24, total voice channels 120 used 0
    0 active calls, 0 max active calls, 0 total calls
    30887 rx packets, 0 rx drops, 30921 tx packets, 0 tx frags
    0 curr_dsp_tx_queued, 29 max_dsp_tx_queued
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 13000 bits/sec, 94 packets/sec
  5 minute output rate 193000 bits/sec, 94 packets/sec
```

show interface dspfarm

```

30887 packets input, 616516 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
30921 packets output, 7868892 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out

```

Table 45 describes the significant fields shown in the display.

Table 45 *show interface dspfarm Field Descriptions*

Field	Description
DSPfarm3/0 is up	DSPfarm interface is operating. The interface state can be up, down, or administratively down.
Line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Version number of the hardware.
MTU	256 bytes.
BW	12000 Kbit.
DLY	Delay of the interface in microseconds.
Reliability	Reliability of the interface as a fraction of 255 (255/255 is 100% reliability, calculated as an exponential average over 5 minutes).
Txload	Number of packets sent.
Rxload	Number of packets received.
Encapsulation	Encapsulation method assigned to the interface.
Loopback	Loopback conditions.
C549 DSP Firmware Version	The version of DSP firmware installed.
DSP Boot Loader	DSP boot loader version.
DSP Application	DSP application code version.
Medium Complexity Application	DSP Medium Complexity Application code version.
High Complexity Application	DSP High Complexity Application code version.
Total DSPs	Total DSPs that are equipped in the PA.
DSP0-DSP	DSP number range.
Jukebox DSP id	Jukebox DSP number.
Down DSPs	DSPs not in service.
Total sig channels...used...	Total number of signal channels used.
Total voice channels...used...	Total number of voice channels used.
Active calls	Number of active calls.
Max active calls	Maximum number of active calls.
Total calls	Total number of calls.
Rx packets	Number of received (rx) packets.
Rx drops	Number of rx packets dropped at PA.

Table 45 *show interface dspfarm Field Descriptions (continued)*

Field	Description
Tx packets	Number of transmit (tx) packets.
Tx frags	Number of tx packets that were fragmented.
Curr_dsp_tx_queued	Number of tx packets that are being queued at host DSP queues.
Max_dsp_tx_queued	The max total tx packets that were queued at host DSP queues.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process switched and not when packets are fast switched.
Output	Number of hours, minutes, and seconds since the last packet was successfully sent by the interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process switched and not when packets are fast switched.
Output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks (**) are printed.
Last clearing of “show interface” counters	Number of times the “show interface” counters were cleared.
queueing strategy	First-in, first-out queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue	Number of packets in output queue.
Drops	Number of packets dropped because of a full queue.
Input queue	Number of packets in input queue.
Minute input rate	Average number of bits and packets received per minute in the past 5 minutes.
Bits/sec	Average number of bits sent per second.
Packets/sec	Average number of packets sent per second.
Packets input	Total number of error-free packets received by the system.
Bytes	Total number of bytes, including data and MAC encapsulation, in the error free packets received by the system.
No buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no-input-buffer events.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
Runts	Number of packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.

Table 45 *show interface dspfarm Field Descriptions (continued)*

Field	Description
Giants	Number of packets that are discarded because they exceed the maximum packet size for the medium. For instance, any Ethernet packet that is greater than 1518 bytes is considered a giant.
Throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
Input errors	Number of packet input errors.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station sending bad data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
Frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
Overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the ability of the receiver to handle the data.
Ignore	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
Abort	Illegal sequence of one bits on the interface.
Packets output	Total number of messages sent by the system.
Bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
Underruns	Number of times that the far end transmitter has been running faster than the near-end router's receiver can handle.
Output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this value might not balance with the sum of the enumerated output errors; some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
Collisions	Number of messages re-sent because of an Ethernet collision. Collisions are usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.

Table 45 *show interface dspfarm Field Descriptions (continued)*

Field	Description
Interface resets	Number of times an interface has been completely reset. Resetting can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurs, or when an interface is looped back or shut down.
Output buffer failures	Number of failed buffers.
Output buffers swapped out	Number of buffers swapped out.

show mgcp

To display Media Gateway Control Protocol (MGCP) configuration information, use the **show mgcp** command in EXEC mode.

show mgcp

Defaults

No defaults

Command Modes

EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
12.1(3)T	Output was updated to show additional gateway and platform information.

Examples

The following displays an example of the command format and output for **show mgcp**.

```
Router# show mgcp

MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 192.168.10.10 2302 Initial protocol service is MGCP
mgcp block-newcalls DISABLED
MGCP dtmf-relay disabled for all codec types
MGCP modem passthru: CA
MGCP request timeout 500, MGCP request retries 3
MGCP gateway port: 2427, MGCP maximum waiting delay 3000
MGCP restart delay 5, MGCP vad DISABLED
MGCP sdp simple DISABLED, MGCP cisco fgdos DISABLED
MGCP codec type g711ulaw, MGCP packetization period 20
MGCP JB threshold lwm 30, MGCP JB threshold hwm 150
MGCP LAT threshold lwm 150, MGCP LAT threshold hwm 300
MGCP PL threshold lwm 1000, MGCP PL threshold hwm 10000
MGCP playout mode is adaptive 60, 4, 200 in msec
MGCP IP ToS low delay disabled, MGCP IP ToS high throughput disabled
MGCP IP ToS high reliability disabled, MGCP IP ToS low cost disabled
MGCP IP precedence 3, MGCP default package: trunk-package
MGCP supported packages: gm-package dtmf-package trunk-package rtp-package
as-packagescript-package
```

Table 46 describes the significant fields shown in the display.

Table 46 *show mgcp Field Descriptions*

MGCP Admin State...Oper State	The administrative and operational state of the MGCP daemon. The administrative state controls starting and stopping the application using the mgcp and mgcp block-newcalls commands. The operational state controls normal MGCP operations.
MGCP call-agent	The address of the call agent specified in the mgcp command.
Initial protocol service is...	Indicates the protocol initiated for this session.
MGCP block-newcalls enabled	The state of the mgcp block-newcalls command.
MGCP dtmf-relay	The setting for the mgcp dtmf-relay command.
MGCP modem passthru	Indicates whether a call agent will be involved in relaying modem data.
MGCP request timeout	The setting for the mgcp request timeout command.
MGCP request retries	The setting for the mgcp request retries command.
MGCP gateway port	The UDP port specification.
MGCP maximum waiting delay	The setting for the mgcp max-waiting-delay command.
MGCP restart delay	The setting for the mgcp restart-delay command.
MGCP vad	The setting for the mgcp vad command.
MGCP sdp simple	Indicates whether the simple sdp protocol is being used.
MGCP cisco fgdos	For Cisco use only.
MGCP codec type	The setting for the mgcp codec command.
MGCP packetization period	The packetization period parameter setting for the mgcp codec command.
MGCP JB threshold lwm	The jitter buffer minimum threshold parameter setting for the mgcp quality-threshold command.
MGCP JB threshold hwm	The jitter buffer maximum threshold parameter setting for the mgcp quality-threshold command.
MGCP LAT threshold lwm	The latency minimum threshold parameter setting for the mgcp quality-threshold command.
MGCP LAT threshold hwm	The latency maximum threshold parameter setting for the mgcp quality-threshold command.
MGCP PL threshold lwm	The packet loss minimum threshold parameter setting for the mgcp quality-threshold command.
MGCP PL threshold hwm	The packet loss maximum threshold parameter setting for the mgcp quality-threshold command.
MGCP playout mode	The jitter buffer packet size type and size.
MGCP IP ToS low delay	The low-delay parameter setting for the mgcp ip-tos command.
MGCP IP ToS high throughput	The high-throughput parameter setting for the mgcp ip-tos command.

Table 46 *show mgcp Field Descriptions (continued)*

MGCP IP ToS high reliability	The high-reliability parameter setting for the mgcp ip-tos command.
MGCP IP ToS low cost	The low-cost parameter setting for the mgcp ip-tos command.
MGCP IP precedence	The precedence parameter setting for the mgcp ip-tos command.
MGCP default package	The default-package parameter setting for the mgcp default-package command.
MGCP supported packages	The packages supported in this session.

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
show mgcp connection	Displays connection-related MGCP configuration information.
show mgcp endpoint	Displays endpoint-specific MGCP configuration information.
show mgcp statistics	Displays statistical MGCP configuration information.

show mgcp connection

To display Media Gateway Control Protocol (MGCP) configuration information, use the **show mgcp connection** command in EXEC mode.

show mgcp connection

Syntax Description	connection	Displays the active MGCP-controlled connections.

Defaults	No defaults

Command Modes	EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
	12.1(3)T	Output was updated to show additional gateway and platform information.

Examples Following is an example of an MGCP configuration displaying active MGCP-controlled connections.

```
Router# show mgcp connection
```

```
Endpoint  Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (C)odec (E)vent[SIFL] (R)esult[EAL]
1. S0/DS1-0/1 C=103,23,24 I=0x8 P=16586,16634 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
2. S0/DS1-0/2 C=103,25,26 I=0x9 P=16634,16586 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
3. S0/DS1-0/3 C=101,15,16 I=0x4 P=16506,16544 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
4. S0/DS1-0/4 C=101,17,18 I=0x5 P=16544,16506 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
5. S0/DS1-0/5 C=102,19,20 I=0,6 P=16572,16600 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
6. S0/DS1-0/6 C=102,21,22 I=0x7 P=16600,16572 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
```

```
Total number of active calls 6
```

[Table 47](#) describes the significant fields shown in the display.

Table 47 *show mgcp connection Field Descriptions*

Endpoint	The endpoint for each call shown in the digital endpoint naming convention of slot number (S0) and digital line (DS1-0) number (1).
Call_ID(C)	The MGCP call ID sent by the call agent, the internal Call Control Application Programming Interface (CCAPI) call ID for this endpoint, and the peer call legs CCAPI call ID. (CCAPI is an API that provides call control facilities to applications.)
Conn_ID(I)	The connection ID generated by the gateway and sent in the ACK message.

Table 47 *show mgcp connection Field Descriptions (continued)*

(P)ort	The ports used for this connection. The first port is the local UDP port. The second port is the remote UDP port.
(M)ode	The call mode, where: 0—An invalid value for mode. 1—The gateway should only send packets. 2—The gateway should only receive packets. 3—The gateway can send and receive packets. 4—The gateway should neither send nor receive packets. 5—The gateway should place the circuit in loopback mode. 6—The gateway should place the circuit in test mode. 7—The gateway should use the circuit for network access for data. 8—The gateway should place the connection in network loopback mode. 9—The gateway should place the connection in network continuity test mode. 10— The gateway should place the connection in conference mode. All other values are used for internal debugging.
(S)tate	The call state. The values are used for internal debugging purposes.
(C)odec	The codec identifier. The values are used for internal debugging purposes.
(E)vent [SIFL]	Used for internal debugging.
(R)esult [EA]	Used for internal debugging.

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
show mgcp	Displays general MGCP configuration information.
show mgcp endpoint	Displays endpoint-specific MGCP configuration information.
show mgcp statistics	Displays statistical MGCP configuration information.

show mgcp endpoint

To display Media Gateway Control Protocol (MGCP) configuration information, use the **show mgcp endpoint** command in EXEC mode.

show mgcp endpoint

Syntax Description	endpoint	Displays the MGCP-controlled endpoints.

Defaults	No defaults

Command Modes	EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
	12.1(3)T	Output was updated to show additional gateway and platform information.

Examples The following example shows how endpoints are configured:

```
Router# show mgcp endpoint
```

```
T1/0 ds0-group 0 timeslots 1-24 type none
T1/1 ds0-group 0 timeslots 1-24 type none
T1/2 ds0-group 0 timeslots 1-24 type none
T1/3 ds0-group 0 timeslots 1-24 type none
```

Related Commands	Command	Description
	mgcp	Starts the MGCP daemon.
	show mgcp	Displays general MGCP configuration information.
	show mgcp connection	Displays connection-related MGCP configuration information.
	show mgcp statistics	Displays statistical MGCP configuration information.

show mgcp statistics

To display Media Gateway Control Protocol (MGCP) configuration information, use the **show mgcp statistics** command in EXEC mode.

show mgcp statistics

Syntax Description	statistics	Displays MGCP statistics regarding network messages that have been received and sent.

Defaults	No defaults

Command Modes	EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
	12.1(3)T	Output was updated to show additional gateway and platform information.

Examples	Following is an example of an MGCP configuration displaying MGCP statistics of network messages that have been received and sent.

Router# **show mgcp statistics**

```
UDP pkts rx 8, tx 9
Unrecognized rx pkts 0, MGCP message parsing errors 0
Duplicate MGCP ack tx 0, Invalid versions count 0
CreateConn rx 4, successful 0, failed 0
DeleteConn rx 2, successful 2, failed 0
ModifyConn rx 4, successful 4, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 4, failed 0
AuditConnection rx 0, successful 0, failed 0
AuditEndpoint rx 0, successful 0, failed 0
RestartInProgress tx 1, successful 1, failed 0
Notify tx 0, successful 0, failed 0
ACK tx 8, NACK tx 0
ACK rx 0, NACK rx 0
IP address based Call Agents statistics:
IP address 10.24.167.3, Total msg rx 8, successful 8, failed 0
```


Table 48 describes the significant fields shown in the display.

Table 48 *show mgcp statistics Field Descriptions*

UDP pkts rx, tx	The number of UDP packets transmitted and received by the gateway's MGCP application from the Call Agent.
Unrecognized rx pkts	The number of unrecognized UDP packets received by the MGCP application.
MGCP message parsing errors	The number of MGCP messages received with parsing errors.
Duplicate MGCP ack tx messages	The number of duplicate MGCP acknowledgment messages transmitted to the Call Agent.
Invalid versions count	The number of MGCP messages received with invalid MGCP protocols version.
CreateConn rx	The number of Create Connection (CRCX) messages received by the gateway, the number that were successful, and the number that failed.
DeleteConn rx	The number of Delete Connection (DLCX) messages received by the gateway, the number that were successful, and the number that failed.
NotifyRequest rx	The number of Notify Request (RQNT) messages received by the gateway, the number that were successful, and the number that failed.
AuditConnection rx	The number of Audit Connection (AUCX) message received by the gateway, the number that were successful, and the number that failed.
AuditEndpoint rx	The number of Audit Endpoint (AUEP) messages received by the gateway, the number that were successful, and the number that failed.
RestartinProgress tx	The number of Restart in Progress (RSIP) messages transmitted by the gateway, the number that were successful, and the number that failed.
Notify tx	The number of Notify (NTFY) messages transmitted by the gateway, the number that were successful, and the number that failed.
ACK tx, NACK tx	The number of Acknowledgment and Negative Acknowledgment messages transmitted by the gateway.
ACK rx, NACK rx	The number of Acknowledgment and Negative Acknowledgment messages received by the gateway.
IP address based Call Agents statistics: IP address, Total msg rx	IP address of the Call Agent, the total number of MGCP messages received from that Call Agent, the number of messages that were successful, and the number of messages that failed.

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
show mgcp	Displays general MGCP configuration information.

■ show mgcp statistics

show mgcp connection	Displays connection-related MGCP configuration information.
show mgcp endpoint	Displays endpoint-specific MGCP configuration information.

show num-exp

To show the number expansions configured, use the **show num-exp** command in privileged EXEC mode.

show num-exp [*dialed-number*]

Syntax Description	<i>dialed-number</i> (Optional) Dialed number.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 platform.
	12.0(3)T	This command was supported on the Cisco AS5300 universal access server platform.
	12.0(4)XL	This command was supported on the Cisco AS5800 platform.
	12.0(7)XK	This command was supported on the Cisco MC3810 multiservice concentrator.
	12.1(2)T	This command was integrated into Cisco IOS 12.1(2)T.

Usage Guidelines	Use the show num-exp privileged EXEC command to display all the number expansions configured for this router. To display number expansion for only one number, specify that number by using the <i>dialed-number</i> argument.

Examples	The following is sample output from the show num-exp command:

Router# **show num-exp**

```
Dest Digit Pattern = '0...' Translation = '+14085270...'
Dest Digit Pattern = '1...' Translation = '+14085271...'
Dest Digit Pattern = '3...' Translation = '+140852703..'
Dest Digit Pattern = '4..' Translation = '+140852804..'
Dest Digit Pattern = '5..' Translation = '+140852805..'
Dest Digit Pattern = '6....' Translation = '+1408526....'
Dest Digit Pattern = '7....' Translation = '+1408527....'
Dest Digit Pattern = '8...' Translation = '+14085288...'

```

Table 49 describes the significant fields shown in the display.

Table 49 *show num-exp Field Descriptions*

Field	Description
Dest Digit Pattern	Index number identifying the destination telephone number digit pattern.
Translation	Expanded destination telephone number digit pattern.

Related Commands

Command	Description
show call active voice	Displays the Voice over IP active call table.
show call history voice	Displays the Voice over IP call history table.
show dial-peer voice	Displays configuration information for dial peers.
show voice port	Displays configuration information about a specific voice port.

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*

Syntax Description	<i>port</i>	Port number 1 or 2.

Command Modes	EXEC

Command History	Release	Modification
	12.1.1(2)XF	This command was introduced on the Cisco 800 series routers.

Examples The following is an example of **show pots csm** command output:

```
Router# show pots csm 1
```

```
POTS PORT: 1
```

```
CSM Finite State Machine:
```

```
Call 0 - State: idle, Call Id: 0x0
```

```
Active: no
```

```
Event: CSM_EVENT_NONE Cause: 0
```

```
Call 1 - State: idle, Call Id: 0x0
```

```
Active: no
```

```
Event: CSM_EVENT_NONE Cause: 0
```

```
Call 2 - State: idle, Call Id: 0x0
```

```
Active: no
```

```
Event: CSM_EVENT_NONE Cause: 0
```

Related Commands	Command	Description
	test pots dial	Dial a telephone number for the POTS port on the router by using a dial application on your workstation.
	test pots disconnect	Disconnect a telephone call for the POTS port on the router.

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.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(3)T	This command was introduced on the Cisco 800 series router.

Usage Guidelines The **show pots status** command displays the settings and information for both telephone ports.

Examples The following is sample output from the **show pots status** command.

```
Router# show pots status

POTS Global Configuration:
  Country: United States
  Dialing Method: Overlap, Tone Source: Remote, CallerId Support: YES
  Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
  Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
  Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
  TX Gain: 6dB, RX Loss: -6dB,
  Filter Mask: 6F
  Adaptive Cntrl Mask: 0
POTS PORT: 1
  Hook Switch Finite State Machine:
    State: On Hook, Event: 0
    Hook Switch Register: 10, Suspend Poll: 0
  CODEC Finite State Machine:
    State: Idle, Event: 0
    Connection: None, Call Type: Two Party, Direction: Rx only
    Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
    Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
    Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
    TX Gain: 6dB, RX Loss: -6dB,
    Filter Mask: 6F
    Adaptive Cntrl Mask: 0
```

```
CODEC Registers:
  SPI Addr: 2, DSLAC Revision: 4
  SLIC Cmd: 0D, TX TS: 00, RX TS: 00
  Op Fn: 6F, Op Fn2: 00, Op Cond: 00
  AISN: 6D, ELT: B5, EPG: 32 52 00 00
  SLIC Pin Direction: 1F
CODEC Coefficients:
  GX: A0 00
  GR: 3A A1
  Z: EA 23 2A 35 A5 9F C2 AD 3A AE 22 46 C2 F0
  B: 29 FA 8F 2A CB A9 23 92 2B 49 F5 37 1D 01
  X: AB 40 3B 9F A8 7E 22 97 36 A6 2A AE
  R: 01 11 01 90 01 90 01 90 01 90 01 90
  GZ: 60
  ADAPT B: 91 B2 8F 62 31
CSM Finite State Machine:
  Call 0 - State: idle, Call Id: 0x0
           Active: no
  Call 1 - State: idle, Call Id: 0x0
           Active: no
  Call 2 - State: idle, Call Id: 0x0
           Active: no
POTS PORT: 2
Hook Switch Finite State Machine:
  State: On Hook, Event: 0
  Hook Switch Register: 20, Suspend Poll: 0
CODEC Finite State Machine:
  State: Idle, Event: 0
  Connection: None, Call Type: Two Party, Direction: Rx only
  Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
  Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
  Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
  TX Gain: 6dB, RX Loss: -6dB,
  Filter Mask: 6F
  Adaptive Cntrl Mask: 0
CODEC Registers:
  SPI Addr: 3, DSLAC Revision: 4
  SLIC Cmd: 0D, TX TS: 00, RX TS: 00
  Op Fn: 6F, Op Fn2: 00, Op Cond: 00
  AISN: 6D, ELT: B5, EPG: 32 52 00 00
  SLIC Pin Direction: 1F
CODEC Coefficients:
  GX: A0 00
  GR: 3A A1
  Z: EA 23 2A 35 A5 9F C2 AD 3A AE 22 46 C2 F0
  B: 29 FA 8F 2A CB A9 23 92 2B 49 F5 37 1D 01
  X: AB 40 3B 9F A8 7E 22 97 36 A6 2A AE
  R: 01 11 01 90 01 90 01 90 01 90 01 90
  GZ: 60
  ADAPT B: 91 B2 8F 62 31
CSM Finite State Machine:
  Call 0 - State: idle, Call Id: 0x0
           Active: no
  Call 1 - State: idle, Call Id: 0x0
           Active: no
  Call 2 - State: idle, Call Id: 0x0
           Active: no
Time Slot Control: 0
```

Table 50 describes the significant fields shown in the display.

Table 50 *show pots status Field Descriptions*

Field	Descriptions
POTS Global Configuration	Displays the settings of the telephone port physical characteristic commands. Also displays the following: • TX GAIN—Current transmit gain of telephone ports. • RX LOSS—Current transmit loss of telephone ports. • Filter Mask—Value determines which filters are currently enabled or disabled in the telephone port hardware. • Adaptive Cntrl Mask—Value determines if telephone port adaptive line impedance hardware is enabled or disabled.
Hook Switch Finite State Machine	Device driver that tracks state of telephone port hook switch.
CODEC Finite State Machine	Device driver that controls telephone port codec hardware.
CODEC Registers	Register contents of telephone port codec hardware.
CODEC Coefficients	Codec coefficients selected by telephone port driver. Selected line type determines codec coefficients.
CSM Finite State Machine	State of call-switching module (CSM) software.
Time Slot Control	Register that determines if telephone port voice or data packets are sent to an ISDN B channel.

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots distinctive-ring-guard-time	Specifies a delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.

Command	Description
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.

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.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.3(2)NA	This command was introduced.
	12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and supported on the Cisco MC3810 multiservice concentrator.

Examples The following is sample output from the **show proxy h323 calls** command:

```
Router# show proxy h323 calls
```

```
Call unique key = 1
Conference ID = [277B87C0A283D111B63E00609704D8EA]
Calling endpoint call signalling address = 55.0.0.41
Calling endpoint aliases:
  H323_ID: ptel11@zone1.com
Call state = Media Streaming
Time call was initiated = 731146290 ms
```

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 show proxy h323 calls display.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	11.3(2)NA	This command was introduced.
	12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and supported on the Cisco MC3810 multiservice concentrator.

Usage Guidelines	The show proxy h323 detail-call command can be used with or without the proxy statistics enabled.

Examples	The following is sample output from the show proxy h323 detail-call command without the proxy statistics enabled:

```
Router# show proxy h323 detail-call 1

ConferenceID = [277B87C0A283D111B63E00609704D8EA]
Calling endpoint aliases:
  H323_ID: ptel11@zone1.com
Called endpoint aliases:
  H323_ID: ptel21@zone2.com
Peer proxy call signalling address = 55.0.0.41
Time call was initiated = 731146290 ms
Inbound CRV = 144
Outbound CRV = 70
Call state = Media Streaming
H245 logical channels for call leg ptel11@zone1.com<->px1@zone.com
  Channel number = 2
    Type = VIDEO
    State = OPEN
    Bandwidth = 374 kbps
    Time created = 731146317 ms
  Channel number = 1
    Type = AUDIO
    State = OPEN
    Bandwidth = 81 kbps
    Time created = 731146316 ms
  Channel number = 2
    Type = VIDEO
    State = OPEN
```

■ **show proxy h323 detail-call**

```

        Bandwidth = 374 kbps
        Time created = 731146318 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146317 ms
H245 logical channels for call leg pte111@zone1.com<->50.0.0.41:
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146317 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146316 ms
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146318 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146317 ms

```

The following is sample output from the **show proxy h323 detail-call** command with the proxy statistics enabled:

```

Router# show proxy h323 detail-call 1

ConferenceID = [677EB106BD0D111976200002424F832]
Calling endpoint call signalling address = 172.21.127.49
    Calling endpoint aliases:
        H323_ID: intel2
        E164_ID: 2134
Called endpoint aliases:
    H323_ID: mcs@sanjose.cisco.com
Peer proxy call signalling address = 171.68.183.199
Peer proxy aliases:
    H323_ID: proxy.sanjose.cisco.com
Time call was initiated = 730949651 ms
Inbound CRV = 2505
Outbound CRV = 67
Call state = H245 open logical channels
H245 logical channels for call leg intel2 <-> cisco7-pxy:
    Channel number = 259
        RTP stream from intel2 to cisco7-pxy
        Type = VIDEO
        State = OPEN
        Bandwidth = 225 kbps
        Time created = 730949676 ms
    Channel number = 257
        RTP stream from intel2 to cisco7-pxy
        Type = AUDIO
        State = OPEN
        Bandwidth = 18 kbps
        Time created = 730949658 ms
    Channel number = 2
        RTP stream from cisco7-pxy to intel2
        Type = VIDEO

```

```

State = OPEN
Bandwidth = 225 kbps
Time created = 730949664 ms
RTP Statistics:
  Packet Received Count = 3390
  Packet Dropped Count = 0
  Packet Out of Sequence Count = 0
  Number of initial packets used for Arrival-Spacing bin setup = 200
  min_arrival_spacing = 0(ms)  max_arrival_spacing = 856(ms)
  Average Arrival Rate = 86(ms)
  Arrival-Spacing(ms)  Packet-Count
    0                   2116
    26                  487
    52                   26
    78                   0
   104                   0
   130                    1
   156                   0
   182                    1
   208                   0
   234                    4
   260                   99
   286                  315
   312                  154
   338                    8
   364                   0
   390                    2
   416                   10
   442                   73
   468                   51
   494                   43
=====
Min Jitter = 34(ms)  Max Jitter = 408(ms)
Average Jitter Rate = 117
Jitter Rate(ms)  Packet-Count
    0              0
   41             514
   82             2117
Number of initial packets used for Arrival-Spacing bin setup = 200
min_arrival_spacing = 32(ms)  max_arrival_spacing = 96(ms)
Average Arrival Rate = 60(ms)
Arrival-Spacing(ms)  Packet-Count
    32              35
    34               0
    36             177
    38               0
    40              56
    42               0
    44              10
    46               0
    48              27
    50               0
    52             541
    54               0
    56            2642
    58               1
    60            1069
    62               0
    64             77 0
    68               6
    70             257
=====

```

■ show proxy h323 detail-call

```

Min Jitter = 0(ms)  Max Jitter = 28(ms)
Average Jitter Rate = 5
Jitter Rate(ms)    Packet-Count
0                  1069
3                  2720
6                  0
9                  804
12                 27
15                 10
18                 0
21                 56
24                 177
27                 35

H245 logical channels for call leg cisco7-pxy <->
proxy.sanjose.cisco.com:
Channel number = 259
RTP stream from cisco7-pxy to proxy.sanjose.cisco.com
Type = VIDEO
State = OPEN
Bandwidth = 225 kbps
Time created = 730949676 ms
RTP Statistics:
  Packet Received Count = 3398
  Packet Dropped Count = 1
  Packet Out of Sequence Count = 0
  Number of initial packets used for Arrival-Spacing bin setup = 200
  min_arrival_spacing = 0(ms)  max_arrival_spacing = 872(ms)
  Average Arrival Rate = 85(ms)
  Arrival-Spacing(ms)    Packet-Count
0                        2636
28                       0
56                       0
84                       0
112                      0
140                      1
168                      0
196                      0
224                      0
252                      0
280                      2
308                      425
336                      154
364                      5
392                      0
420                      0
448                      0
476                      114
504                      41
532                      20

=====
Min Jitter = 55(ms)  Max Jitter = 447(ms)
Average Jitter Rate = 127
Jitter Rate(ms)    Packet-Count
0                  0
45                 1
90                 2636
135                0
180                2
225                425
270                159
315                0
360                0
405                175

```

```

Channel number = 257
RTP stream from cisco7-pxy to proxy.sanjose.cisco.com
Type = AUDIO
State = OPEN
Bandwidth = 18 kbps
Time created = 730949658 ms
RTP Statistics:
  Packet Received Count = 2537
  Packet Dropped Count = 3
  Packet Out of Sequence Count = 0
  Number of initial packets used for Arrival-Spacing bin setup = 200
  min_arrival_spacing = 0(ms)  max_arrival_spacing = 32716(ms)
  Average Arrival Rate = 112(ms)
  Arrival-Spacing(ms)    Packet-Count
    0                     2191
    72                    253
    144                   31
    216                   7
    288                   3
    360                   4
    432                   4
    504                   2
    576                   1
    648                   3
    720                   2
    792                   1
    864                   2
    936                   1
    1008                  1
    1080                  1
    1152                  1
    1224                  1
    1296                  0
    1368                  28
  =====
  Min Jitter = 32(ms)  Max Jitter = 1256(ms)
  Average Jitter Rate = 121
  Jitter Rate(ms)      Packet-Count
    0                   284
    126                 2201
    252                 4
    378                 6
    504                 4
    630                 3
    756                 2
    882                 2
    1008                2
    1134                29
Channel number = 2
RTP stream from proxy.sanjose.cisco.com to cisco7-pxy
Type = VIDEO
State = OPEN
Bandwidth = 225 kbps
Time created = 730949664 ms
Channel number = 1
RTP stream from proxy.sanjose.cisco.com to cisco7-pxy
Type = AUDIO
State = OPEN
Bandwidth = 18 kbps
Time created = 730949661 ms

```

show proxy h323 detail-call

Related Commands

Command	Description
h323 qos	Enables QoS on the proxy.

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.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	11.3(2)NA	This command was introduced.
	12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and supported on the Cisco MC3810 multiservice concentrator.

Examples	The following is sample output from the show proxy h323 status command:

```
Router# show proxy h323 status

H.323 Proxy Status
=====
H.323 Proxy Mode: Enabled
Proxy interface = Serial1: UP
Application Specific Routing: Disabled
RAS Initialization: Complete
Proxy aliases configured:
  H323_ID: px2
Proxy aliases assigned by Gatekeeper:
  H323_ID: px2
Gatekeeper multicast discovery: Disabled
Gatekeeper:
  Gatekeeper ID: gk.zone2.com
  IP address: 70.0.0.31
Gatekeeper registration succeeded
T.120 Mode: BYPASS
RTP Statistics: OFF
Number of calls in progress: 1
```

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.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

The number displayed for **show rawmsg all** should be zero to indicate that there are no memory leaks.

Examples

The following example shows how to display memory leaks from the telephony service provider:

```
Router# show rawmsg tsp
```

Related Commands

Command	Description
isdn protocol-emulate	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality.
isdn switch type	Configures the Cisco AS5300 universal access server PRI interface to support Q.SIG signaling.
pri-group nec-fusion	Configures your NEC PBX to support FCCS.
show cdapi	Displays the CDAPI.

show rlm group statistics

To display the network latency of the Redundant Link Manager (RLM) group, use the **show rlm group statistics** command in privileged EXEC mode.

show rlm group *group-number* statistics

Syntax Description	<i>group-number</i> RLM group number (0 to 255).				
Command Modes	Privileged EXEC				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>11.3(7)</td><td>This command was introduced.</td></tr> </table>	Release	Modification	11.3(7)	This command was introduced.
Release	Modification				
11.3(7)	This command was introduced.				

Examples

The following is sample output from the **show rlm group *group-number* statistics** command:

```
Router# show rlm group 1 statistics
```

```
RLM Group 1 Statistics
```

```
Link_up:
```

```
  last time occurred at 02:45:48.724, total transition=1
  avg=00:00:00.000, max=00:00:00.000, min=00:00:00.000, latest=00:00:00.000
```

```
Link_down:
```

```
  last time occurred at 02:42:33.724, total transition=1
  avg=00:03:15.000, max=00:03:15.000, min=00:00:00.000, latest=00:03:15.000
```

```
Link_recovered:
```

```
  last time occurred at 00:00:00.000, success=0(0%), failure=0
  avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
```

```
Link_switched:
```

```
  last time occurred at 00:00:00.000, success=0(0%), failure=0
  avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
```

```
Server_changed:
```

```
  last time occurred at 00:00:00.000 for totally 0 times
```

```
Server Link Group[r1-server]:
```

```
Open the link [10.1.1.1(Loopback1), 10.1.4.1]:
```

```
  last time occurred at 02:43:03.724, success=1(100%), failure=0
  avg=162.000s, max=162.000s, min=0.000s, latest=162.000s
```

```
Echo over link [10.1.1.1(Loopback1), 10.1.4.1]:
```

```
  last time occurred at 02:47:15.724, success=91(62%), failure=54
  avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
```

```
Open the link [10.1.1.2(Loopback2), 10.1.4.2]:
```

```
  last time occurred at 02:43:03.724, success=1(100%), failure=0
  avg=162.000s, max=162.000s, min=0.000s, latest=162.000s
```

```
Echo over link [10.1.1.2(Loopback2), 10.1.4.2]:
```

```
  last time occurred at 02:47:19.724, success=95(63%), failure=54
  avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
```

show rlm group statistics

```

Server Link Group[r2-server]:
  Open the link [10.1.1.1(Loopback1), 10.1.5.1]:
    last time occurred at 02:46:06.724, success=0(0%), failure=1
    avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
  Echo over link [10.1.1.1(Loopback1), 10.1.5.1]:
    last time occurred at 02:47:18.724, success=0(0%), failure=85
    avg=0.000s, max=0.000s, min=0.000s, latest=0.000s

Open the link [10.1.1.2(Loopback2), 10.1.5.2]:
  last time occurred at 02:46:06.724, success=0(0%), failure=1
  avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
Echo over link [10.1.1.2(Loopback2), 10.1.5.2]:
  last time occurred at 02:47:18.724, success=0(0%), failure=85
  avg=0.000s, max=0.000s, min=0.000s, latest=0.000s

Router#

```

Table 51 describes the significant fields shown in the display.

Table 51 *show rlm group statistics Field Descriptions*

Field	Description
Link_up	Statistics collected when RLM group is in link up state.
total transition	Total number of transitions into a particular RLM group state.
avg	How long the average time interval lasts.
max	How long the maximum time interval lasts.
min	How long the minimum time interval lasts.
latest	How long the most recent time interval lasts.
Link_down	Statistics collected when RLM group is in the link down state.
Link_recovered	Statistics collected when RLM group is in the link recovery state.
Link_switched	Statistics collected when RLM group is in the link switching state.
Server_changed	Statistics collected for when and how many times RLM server failover happens.
Server Link Group[r1-server]	Statistics collected for those signaling links defined under a particular server link group, for example, r1-server.
Open the link	Statistics collected when a particular signaling link connection is open (broken).
Echo over link	Statistics collected when a particular signaling link connection is established.

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

show rlm group status

To display the status of the Redundant Link Manager (RLM) group, use the **show rlm group status** command in privileged EXEC mode.

show rlm group *group-number* status

Syntax Description	<i>group-number</i>	RLM group number (0 to 255).

Command Modes	Privileged EXEC

Command History	Release	Modification
	11.3(7)	This command was introduced.

Examples The following is sample output from the **show rlm group *group-number* status** command:

```
Router# show rlm group 1 status

RLM Group 1 Status
User/Port: RLM_MGR/3000
Link State: Up           Last Link Status Reported: Up
Next tx TID: 1           Last rx TID: 0
Server Link Group[r1-server]:
  link [10.1.1.1(Loopback1), 10.1.4.1] = socket[active]
  link [10.1.1.2(Loopback2), 10.1.4.2] = socket[standby]
Server Link Group[r2-server]:
  link [10.1.1.1(Loopback1), 10.1.5.1] = socket[opening]
  link [10.1.1.2(Loopback2), 10.1.5.2] = socket[opening]
```

[Table 52](#) describes the significant fields shown in the display.

Table 52 show rlm group status Field Descriptions

Field	Description
User/Port	A list of registered RLM users and the corresponding port numbers associated with them.
RLM_MGR	RLM management module.
Link State	The current RLM group’s link state for connecting to the remote end.
Last Link Status Reported	The most recent link status change is reported to RLM users.
Next tx TID	The next transaction ID for transmission.
Last rx TID	The most recent transaction ID has been received.
Server Link Group[r1-server]	The status of all signaling links configured under a particular RLM server link group r1-server.

Table 52 *show rlm group status Field Descriptions (continued)*

Field	Description
socket	The status of the individual signaling link.
Server Link Group[r2-server]	The status of all signaling links configured under a particular RLM server link group (r2-server).

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

show rlm group timer

To display the current timer values, use the **show rlm group timer** command in privileged EXEC mode.

show rlm group *group-number* **timer**

Syntax Description	<i>group-number</i>	RLM group number (0 to 255).

Command Modes	Privileged EXEC

Command History	Release	Modification
	11.3(7)	This command was introduced.

Examples The following is sample output from the **show rlm group** *group-number* **timer** command:

```
Router# show rlm group 1 timer
```

```
RLM Group 1 Timer Values
open_wait  = 3s           force-down  = 30s
recovery   = 12s          switch-link = 5s
minimum-up = 60s          retransmit  = 1s
keepalive  = 1s
```

Table 90 describes the significant fields shown in the display.

Table 53 *show rlm group timer Field Descriptions*

Field	Description
open_wait	Wait for the connection request to be acknowledged.
recovery	Time to allow the link to recover to backup link before declaring the link is down.
minimum-up	Minimum time to force RLM to stay in the down state to make sure the remote end detects the link state is down.
keepalive	A keepalive packet will be sent out from network access server to CSC periodically.
force-down	Minimum time to force RLM to stay in the down state to make sure that the remote end detects that the link state is down.
switch-link	The maximum transition period allows RLM to switch from a lower preference link to a higher preference link. If the switching link does not complete successfully before this timer expires, RLM will go into the recovery state.
retransmit	Because RLM is operating under UDP, it needs to resend the control packet if the packet is not acknowledged within this retransmit interval.

Related Commands	Command	Description
	clear interface	Resets the hardware logic on an interface.
	clear rlm group	Clears all RLM group time stamps to zero.
	interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
	link (RLM)	Specifies the link preference.
	protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
	retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
	server (RLM)	Defines the IP addresses of the server.
	show rlm group status	Displays the status of the RLM group.
	shutdown (RLM)	Shuts down all of the links under the RLM group.
	timer	Overwrites the default setting of timeout values.

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 detailed is not specified, the command displays the session information and stream information for the stream that is currently active.
detailed	(Optional) If the keyword detailed is specified, the command displays the session information and stream information in detail for all streams that are associated with the session.

Defaults

Active (current) stream information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

Use this command to display cumulative information about the session, packet statistics, and general call information such as call ID, session ID, and so on.



Note

Session refers to a session between the application and the RTSP client. Each call leg that is configured to use RTSP streaming has a session.

A call leg could play several prompts in a session; the “Play Time” refers to the play time associated with a stream or, in other words, a prompt; the cumulative play time is the sum total of all streams (or prompts) played out in a session.

The command output is a stream block that contains information about the stream (URL, packet statistics, current state of the stream, play duration, call ID, session ID, individual RTSP stream URLs, and packet statistics).

Examples

The following output is displayed when the **show rtsp client session active** command is used during an active session:

```
Router# show rtsp client session active

RTSP Session ID:0x8      Current Status:RTSP_STATUS_PLAYING
Associated CallID:0xF
Active Request:RTSP_API_REQ_PLAY
Control Protocol:TCP      Data Protocol:RTP

Total Packets Transmitted:0 (0 bytes)
Total Packets Received:708 (226560 bytes)

Cumulative Elapsed Play   Time:00:00:28.296
Cumulative Elapsed Record Time:00:00:00.000

      Session ID:0x8      State:ACTIVE
      Local  IP Address:1.13.79.45      Local  Port 16660
      Server IP Address:1.13.79.6      Server Port 11046
      Stream URL:rtsp://rtsp-cisco.cisco.com:554/chinna.au/streamid=0

      Packets Transmitted:0 (0 bytes)
      Packets Received:708 (226560 bytes)

      Elapsed Play   Time:00:00:28.296
      Elapsed Record Time:00:00:00.000
      ReceiveDelay:85      LostPackets:0
```

The following output is displayed when the **show rtsp client session history detailed** command is used:

```
Router# show rtsp client session history detailed

RTSP Session ID:0x8
Associated CallID:0xF
Control Protocol:TCP      Data Protocol:RTP

Total Packets Transmitted:0 (0 bytes)
Total Packets Received:2398 (767360 bytes)

Cumulative Elapsed Play   Time:00:01:35.916
Cumulative Elapsed Record Time:00:00:00.000

      Session ID:0x8      State:INACTIVE
      Local  IP Address:1.13.79.45      Local  Port 16660
      Server IP Address:1.13.79.6      Server Port 11046
      Stream URL:rtsp://rtsp-cisco.cisco.com:554/chinna.au/streamid=0

      Packets Transmitted:0 (0 bytes)
      Packets Received:2398 (767360 bytes)

      Play   Time:00:01:35.916
      Record Time:00:00:00.000
      OntimeRcvPayout:93650
      GapFillWithSilence:0
      GapFillWithPrediction:70
      GapFillWithInterpolation:0
      GapFillWithRedundancy:0
      HighWaterPayoutDelay:85
      LowWaterPayoutDelay:64
      ReceiveDelay:85      LostPackets:0
      EarlyPackets:2      LatePackets:12
```

 show rtsp client session

Related Commands	Command	Description
	rtsp client session history duration	Specifies the length of time the RTSP is kept during the session.
	rtsp client session history records	Specifies the number of RTSP client session history records during the session.

show rudpv0 failures

To show SS7 Reliable User Datagram Protocol (RUDP) failure statistics, enter the **show rudpv0 failures** command in privileged EXEC mode.

show rudpv0 failures

Syntax Description	There are no keywords or arguments.

Defaults	There are no default behaviors or values.

Command History	Release	Modification
	12.0(7)XR	This command was introduced.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples	The following example shows the display of RUDP failures. The fields are self-explanatory.

```
show rudpv0 failures

**** RUDP Failure Stats ****

CreateBufHdrsFailure      0
CreateConnRecsFailure    0
CreateEventsFailure      0

NotReadyFailures         0
OptionNotSupportedFailures 0
OptionRequiredFailures   0
GetConnRecFailures       0
InvalidConnFailures      0
EventUnavailFailures     0

EmptyBufferSendFailures  0
BufferTooLargeFailures   0
ConnNotOpenFailures      0
SendWindowFullFailures   0
GetBufHdrSendFailures    0

GetDataBufFailures       0
GetBufHdrFailures        0

SendEackFailures         0
SendAckFailures          0
SendSynFailures          0
SendRstFailures          0
SendNullFailures         0

TimerNullFailures        0
FailedRetransmits        0
IncomingPktsDropped      0
UnknownRudpEvents        0
```

 show rudpv0 failures

Related Commands	Command	Description
	clear rudpv0 statistics	Resets the counters for the statistics generated by show rudpv0 failures to 0.
	show rudpv0 statistics	Displays RUDP information about number of packets sent, received, and so forth. clear rudpv0 statistics resets the counters for these statistics to 0.

show rudpv0 statistics

To show SS7 Reliable User Datagram Protocol (RUDP) internal statistics, enter the **show rudpv0 statistics** privileged EXEC command.

show rudpv0 statistics

Syntax Description

There are no keywords or arguments.

Defaults

There are no default behaviors or values.

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Because the statistics counters are continually updated, the cumulative total may not be exactly equal to individual connection counters. After a connection is reset, previous statistics are lost, so the current connection statistics reflect only this instance of the RUDP connection—since the last reset.

Cumulative statistics reflect counts since the router was rebooted or since the last time the **clear rudpv0 statistics** command was issued.

Examples

The following example shows the display of RUDP statistics and states for two connections. The fields are self-explanatory.

```
show rudpv0 statistics

*** RUDP Internal Stats ***

Connection ID: 811641AC,    Current State: OPEN

RcvdInSeq                1
RcvdOutOfSeq             0

SoftResets                0
SoftResetsRcvd           0

TotalPacketsSent          4828
TotalPacketsReceived      4826
TotalDataBytesSent        0
TotalDataBytesReceived    4
TotalDataPacketsSent      0
TotalDataPacketsReceived  1
TotalPacketsRetrans       0
TotalPacketsDiscarded     0

Connection ID: 81163FD4,    Current State: OPEN

RcvdInSeq                2265
RcvdOutOfSeq             0
```

show rudpv0 statistics

```
SoftResets          0
SoftResetsRcvd      0

TotalPacketsSent    7863
TotalPacketsReceived 6755
TotalDataBytesSent  173690
TotalDataBytesReceived 56121
TotalDataPacketsSent 2695
TotalDataPacketsReceived 2265
TotalPacketsRetrans  0
TotalPacketsDiscarded 0

Cumulative RudpV0 Statistics

RcvdInSeq           2266
RcvdOutOfSeq        0

SoftResets          0
SoftResetsRcvd      0

TotalPacketsSent    12691
TotalPacketsReceived 11581
TotalDataBytesSent  173690
TotalDataBytesReceived 56125
TotalDataPacketsSent 2695
TotalDataPacketsReceived 2266
TotalPacketsRetrans  0
TotalPacketsDiscarded 0
```

Related Commands

Command	Description
clear rudpv0 statistics	Resets the counters for the statistics generated by show rudpv0 statistics to 0.
show rudpv0 failures	Displays RUDP information about failed connections and the reasons for them. clear rudpv0 statistics resets the counters for these statistics to 0.

show rudpv1

To display Reliable User Datagram Protocol (RUDP) information, use the **show rudpv1** command in privileged EXEC mode.

show rudpv1 { failures | parameters | statistics }

Syntax Description

failures	RUDP failure statistics.
parameters	RUDP connection parameters.
statistics	RUDP internal statistics.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

Because the statistics counters are continually updated, the cumulative total may not be exactly equal to individual connection counters. After a connection is reset, previous statistics are lost, so the current connection statistics reflect only this instance of the RUDP connection—since the last reset.

Cumulative statistics reflect counts since the router was rebooted or since the last time the **clear rudpv1 statistics** command was issued.

Examples

The following example shows sample output for **show rudpv1 failures**:

```
Router# show rudpv1 failures

**** RUDPV1 Failure Stats ****

CreateBufHdrsFailure      0
CreateConnRecsFailure     0
CreateEventQueueFailure   0
OsSpecificInitFailure     0

NotReadyFailures          0
OptionNotSupportedFailures 0
InvalidOptionFailures     0
OptionRequiredFailures    0
GetConnRecFailures        0
InvalidConnFailures       0
EventUnavailFailures      0

GetConnRecFailures        0
FindConnRecFailures       0
EmptyBufferSendFailures   0
```

■ show rudpv1

```

BufferTooLargeFailures      0
ConnNotOpenFailures        0
SendWindowFullFailures     0
GetBufHdrSendFailures      0

SendInProgressFailures     0

GetDataBufFailures         0
GetBufHdrFailures          0

SendFailures               0
SendEackFailures           0
SendAckFailures            0
SendSynFailures            0
SendRstFailures            0
SendTcsFailures            0
SendNullFailures           0

TimerFailures              0
ApplQueueFailures          0
FailedRetransmits          0
IncomingPktsDropped        0
CksumErrors                0
UnknownRudpv1Events        0
InvalidVersion              0
InvalidNegotiation         0

```

The following example shows sample output for **show rudpv1 parameters**:

```
Router# show rudpv1 parameters
```

```
*** RUDPV1 Connection Parameters ***
```

```
Next Connection Id:61F72B6C, Remote conn id 126000
```

```

Conn State      OPEN
Conn Type       ACTIVE
Accept Negot params? Yes
Receive Window  32
Send Window     32
Receive Seg Size 384
Send Seg Size   384

```

	Requested	Negotiated
Max Auto Reset	5	5
Max Cum Ack	3	3
Max Retrans	2	2
Max OutOfSeq	3	3
Cum Ack Timeout	100	100
Retrans Timeout	300	300
Null Seg Timeout	1000	1000
Trans State Timeout	2000	2000
Cksum type	Hdr	Hdr

```
Next Connection Id:61F72DAC, Remote conn id 126218
```

```

Conn State      OPEN
Conn Type       ACTIVE
Accept Negot params? Yes
Receive Window  32
Send Window     32
Receive Seg Size 384

```

Send Seg Size	384	
	Requested	Negotiated
Max Auto Reset	5	5
Max Cum Ack	3	3
Max Retrans	2	2
Max OutOfSeq	3	3
Cum Ack Timeout	100	100
Retrans Timeout	300	300
Null Seg Timeout	1000	1000
Trans State Timeout	2000	2000
Cksum type	Hdr	Hdr

The following example shows sample output for **show rudpv1** statistics:

Router# **show rudpv1 statistics**

*** RUDPV1 Internal Stats ***

Connection ID:61F72B6C, Current State:OPEN

RcvdInSeq	647
RcvdOutOfSeq	95
AutoResets	0
AutoResetsRcvd	0
TotalPacketsSent	1011
TotalPacketsReceived	958
TotalDataBytesSent	17808
TotalDataBytesReceived	17808
TotalDataPacketsSent	742
TotalDataPacketsReceived	742
TotalPacketsRetrans	117
TotalPacketsDiscarded	38

Connection ID:61F72DAC, Current State:OPEN

RcvdInSeq	0
RcvdOutOfSeq	0
AutoResets	0
AutoResetsRcvd	0
TotalPacketsSent	75
TotalPacketsReceived	75
TotalDataBytesSent	0
TotalDataBytesReceived	0
TotalDataPacketsSent	0
TotalDataPacketsReceived	0
TotalPacketsRetrans	0
TotalPacketsDiscarded	0

Cumulative RudpV1 Statistics

NumCurConnections	2
RcvdInSeq	652
RcvdOutOfSeq	95
AutoResets	0
AutoResetsRcvd	0
TotalPacketsSent	1102

■ show rudpv1

```
TotalPacketsReceived      1047
TotalDataBytesSent        18048
TotalDataBytesReceived    18048
TotalDataPacketsSent      752
TotalDataPacketsReceived  752
TotalPacketsRetrans       122
TotalPacketsDiscarded     38
```

Related Commands

Command	Description
clear rudpv1 statistics	Clears the RUDP statistics counters.
debug rudpv1	Displays debugging information for RUDP.

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.
	transactions	(Optional) Displays the transaction status of a specific provider.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(4)XH1	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples	The following example shows information about all settlement servers configured:

```
Router# show settlement
```

```
Settlement Provider 0
Type = osp
Address url = https://1.14.115.100:6556/
Encryption = all (default)
Max Concurrent Connections = 20 (default)
Connection Timeout = 3600 (s) (default)
Response Timeout = 1 (s) (default)
Retry Delay = 2 (s) (default)
Retry Limit = 1 (default)
Session Timeout = 86400 (s) (default)
Customer Id = 1000
Device Id = 1000
Roaming = Disabled (default)
Signed Token = on
```

```
Number of Connections = 0
Number of Transactions = 7
```

The following example shows transaction and state information about a specific settlement server:

```
Router# show settlement 0 transactions
```

```
Transaction ID=8796304133625270342
      state=OSPC_GET_DEST_SUCCESS, index=0
      callingNumber=5710868, calledNumber=15125551212
```

Table 54 describes the significant fields shown in the display. The provider attributes not configured are not shown.

Table 54 *show settlement Field Descriptions*

Field	Description
type	Settlement provider type.
address url	URL address of the provider.
encryption	SSL encryption method.
max-connections	Maximum number of concurrent connections to provider.
connection-timeout	Connection timeout with provider (in seconds).
response-timeout	Response timeout with provider (in seconds).
retry-delay	Delay time between retries (in seconds).
retry-limit	Number of retries.
session-timeout	SSL session timeout (in seconds).
customer-id	Customer ID, assigned by provider.
device-id	Device ID, assigned by provider.
roaming	Roaming enabled.
signed-token	Indicates if the settlement token is signed by the server.

Related Commands

Command	Description
connection-timeout	Configures the time that a connection is maintained after a communication exchange is completed.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response-timeout	Configures the maximum time to wait for a response from a server.
retry-delay	Sets the time between attempts to connect with the settlement provider.
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.
type	Configures an SAA-RTR operation type.

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	interface	(Optional) Specifies a DS1 interface.
	number	(Optional) Specifies the T1 interface (controller) number. Valid values on the Cisco MC3810 multiservice concentrator are from 0 to 1.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
	12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.

Usage Guidelines If you do not specify an interface, this command shows all the active SGCP connections on this host. If you specify an interface, this command shows only those active connections on the specified interface.

Examples The following example shows the active connections on this router being displayed:

```
Router# show sgcp connection
```

```
Endpoint          Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (E)vent[SIFL] (R)esult[EA]
1. ds1-0/1@r3810-5      C=1,1,2 I=0x1 P=16492,16476 M=3 S=4 E=3,0,0,3 R=0, 0
```

The following example shows the state of SGCP on the router being displayed:

```
Router# show sgcp connection
```

```
SGCP Admin State DOWN, Oper State DOWN
SGCP call-agent: 209.165.200.225 , SGCP graceful-shutdown enabled? FALSE
SGCP request timeout 40, SGCP request retries 10
```

[Table 55](#) describes the significant fields shown in the display.

Table 55 *show sgcp connection Field Descriptions*

Field	Description
SGCP Admin State	The administrative and operational state of the SGCP daemon.
SGCP call-agent	The address of the call agent specified in the sgcp command.
SGCP graceful-shutdown enabled	The state of the sgcp graceful-shutdown command.
SGCP request timeout	The setting for the sgcp request timeout command.
SGCP request retries	The setting for the sgcp request retries command.

Related Commands

Command	Description
show sgcp endpoint	Displays SGCP endpoint information.
show sgcp statistics	Displays global statistics for the SGCP packet count, success, and failure counts.

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	interface <i>ds1</i>	(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.

Defaults	No default behavior or values.

Command Modes	EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
	12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.

Usage Guidelines	You can use this command to see SGCP endpoint information for the whole router, or you can see SGCP endpoint information for a specific DS1 interface and, optionally, a specific DS0. If you enter a nonexistent combination of a DS1 and DS0, the following error message appears: “No matching connection found.”

Examples	The following command shows SGCP endpoint information being set for a matching connection between DS1 interface 1 and DS0 interface 10:

```
Router# show sgcp endpoint interface 1 10
```

 **show sgcp endpoint**

Related Commands	Command	Description
	show sgcp connection	Displays all the active connections on the host router.
	show sgcp statistics	Displays global statistics for the SGCP packet count, success, and failure counts.

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.

Defaults	No default behavior or values.

Command Modes	EXEC

Command History	Release	Modification
	12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
	12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.

Examples	The following example shows SGCP packet statistics being displayed:

```
Router# show sgcp statistics

UDP pkts rx 5, tx 13
Unrecognized rx pkts 0, SGCP message parsing errors 0
Duplicate SGCP ack tx 0
Failed to send SGCP messages 0
CreateConn rx 1, successful 1, failed 0
DeleteConn rx 0, successful 0, failed 0
ModifyConn rx 0, successful 0, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 3, successful 3, failed 0
Notify tx 3, successful 3, failed 0
ACK tx 4, NACK tx 0
ACK rx 1, NACK rx 0

IP address based Call Agents statistics:
IP address 1.4.63.100, Total msg rx 5,
                        successful 5, failed 2
```

The following examples show how you can filter the command return for specific information:

```
Router# show sgcp statistics | begin Failed

Failed to send SGCP messages 0
CreateConn rx 0, successful 0, failed 0
DeleteConn rx 0, successful 0, failed 0
```

■ **show sgcp statistics**

```

ModifyConn rx 0, successful 0, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 0, failed 0
Notify tx 0, successful 0, failed 0
ACK tx 0, NACK tx 0
ACK rx 0, NACK rx 0

Router# show sgcp statistics | exclude ACK

UDP pkts rx 0, tx 0
Unrecognized rx pkts 0, SGCP message parsing errors 0
Duplicate SGCP ack tx 0
Failed to send SGCP messages 0
CreateConn rx 0, successful 0, failed 0
DeleteConn rx 0, successful 0, failed 0
ModifyConn rx 0, successful 0, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 0, failed 0
Notify tx 0, successful 0, failed 0

Router# show sgcp statistics | include ACK

ACK tx 0, NACK tx 0
ACK rx 0, NACK rx 0

```

Related Commands	Command	Description
	show sgcp connection	Display all the active connections on the host Cisco AS5300 universal access server.
	show sgcp endpoint	Displays SGCP endpoint information.

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	retry	Displays SIP protocol retry counts.
	statistics	Displays SIP UA response, traffic, and retry statistics.
	status	Displays SIP UA listener status.
	timers	Displays current settings for the SIP UA protocol timers.

Defaults No default behaviors or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.
	12.1(3)T	The following changes were made: • The statistics keyword was added. • The statistics portion of the output from the status keyword was moved from the status keyword to the statistics keyword. • The output from the timers keyword was changed to reflect the changes in the timers command.

Examples The following example displays output for the **show sip-ua retry** command:

```
Router# show sip-ua retry
```

```
SIP UA Retry Values
invite retry count = 2
response retry count = 2
bye retry count    = 2
cancel retry count  = 1
```

The following example displays output for the **show sip-ua statistics** command:

```
Router# show sip-ua statistics
```

```
SIP Response Statistics (Inbound/Outbound)
Informational:
  Trying 0/0, Ringing 0/0,
  Forwarded 0/0, Queued 0/0,
  SessionProgress 0/0
Success:
```

■ **show sip-ua**

```

    OkInvite 0/0, OkBye 0/0,
    OkCancel 0/0, OkOptions 0/0
Redirection (Inbound only):
    MultipleChoice 0, MovedPermanently 0,
    MovedTemporarily 0, SeeOther 0,
    UseProxy 0, AlternateService 0
Client Error:
    BadRequest 0/0, Unauthorized 0/0,
    PaymentRequired 0/0, Forbidden 0/0,
    NotFound 0/0, MethodNotAllowed 0/0,
    NotAcceptable 0/0, ProxyAuthReqd 0/0,
    ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
    LengthRequired 0/0, ReqEntityTooLarge 0/0,
    ReqURITooLarge 0/0, UnsupportedMediaType 0/0,
    BadExtension 0/0, TempNotAvailable 0/0,
    CallLegNonExistent 0/0, LoopDetected 0/0,
    TooManyHops 0/0, AddrIncomplete 0/0,
    Ambiguous 0/0, BusyHere 0/0
Server Error:
    InternalError 0/0, NotImplemented 0/0,
    BadGateway 0/0, ServiceUnavail 0/0,
    GatewayTimeout 0/0, BadSipVer 0/0
Global Failure:
    BusyEverywhere 0/0, Decline 0/0,
    NoExistAnywhere 0/0, NotAcceptable 0/0

SIP Total Traffic Statistics (Inbound/Outbound)
    Invite 0/0, Ack 0/0, Bye 0/0,
    Cancel 0/0, Options 0/0

```

```

Retry Statistics
    Invite 0, Bye 0, Cancel 0, Response 0

```

The following example displays output for the **show sip-ua status** command:

```

Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP :ENABLED
SIP User Agent for TCP :ENABLED
SIP max-forwards :6

```

The following example displays output for the **show sip-ua timers** command:

```

Router# show sip-ua timers

SIP UA Timer Values (millisecs)
trying 500, expires 180000, connect 500, disconnect 500

```

Related Commands

Command	Description
sip-ua	Enables the SIP user-agent configuration commands, with which you configure the user agent.

show ss7 mtp2 ccb

To display SS7 MTP 2 Channel Control Block (CCB) information, use the **show ss7 mtp2 ccb** command in privileged EXEC mode.

show ss7 mtp2 ccb [*channel*]

Syntax Description

<i>channel</i>	Specifies a channel from 0 through 3.

Defaults

The default is set when you first configure the MTP 2 variant. The link must be out of service in order to change the MTP 2 variant.

If you do not specify a channel, the command shows Channel Control Block information for channel 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The application and meaning of the output is dependent on the MTP 2 variant. For example, NTT and TTC only support emergency alignment.

Examples

The following example shows the display of MTP 2 CCB information:

```
Router# show ss7 mtp2 ccb 0
SS7 MTP2 Internal Channel Control Block Info for channel 0
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
ModuloSeqNumber      = 128   (0x80 )
MaxSeqNumber         = 127   (0x7F )
Unacked-MSUs (MaxInRTB) = 40   (0x28 )
MaxProvingAttempts   = 5     (0x5  )
error_control        = Basic
LSSU_Len             = 1     (0x1  )
MSU_Len              = 272   (0x110 )

SUERM-threshold       = 64    (0x40 )
SUERM-number-octets   = 16    (0x10 )
SUERM-number-SUs     = 256   (0x100 )

Tie-AERM-Emergency    = 1     (0x1  )
Tin-AERM-Normal       = 1     (0x1  )

MSU_FISU_Accepted_flag = FALSE
LSSU_available        = TRUE
AbnormalBSN_flag      = FALSE
```

 show ss7 mtp2 ccb

```
AbnormalBSN_flag           = FALSE
UnreasonableBSN            = FALSE
UnreasonableFSN            = FALSE
Abnormal_FIBR_flag         = FALSE
congestionDiscard          = TRUE

ThisIsA_MSU                = FALSE
local_processor_outage     = FALSE
remote_processor_outage    = FALSE

provingEmergencyFlag       = FALSE
RemoteProvingEmergencyFlag = FALSE
further_proving_required   = FALSE
ForceRetransmitFlag        = FALSE
RetransmissionFlag         = FALSE

link_present               = FALSE
Debug Mask                 = 0x0
```


show ss7 mtp2 state

To display internal SS7 Message Transfer Part level 2 (MTP 2) state machine information, use the **show ss7 mtp2 state** command in privileged EXEC mode.

show ss7 mtp2 state [*channel*]

Syntax Description	<i>channel</i>	Specifies a channel from 0 to 3.

Defaults	If you do not specify a channel, the command shows state machine information for channel 0.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(7)XR	This command was introduced.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples	The following examples show the display of MTP 2 state machine information for two different channels. Table 56 explains the fields.

```
Router# show ss7 mtp2 state 0
SS7 MTP2 states for channel 0
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
  MTP2LSC_OOS           MTP2IAC_IDLE
  MTP2TXC_INSERVICE    MTP2RC_IDLE
  MTP2SUERM_IDLE        MTP2AERM_IDLE
  MTP2CONGESTION_IDLE
    Congestion Backhaul = Abate
  Remote Processor Outage = FALSE
```

```
Router# show ss7 mtp2 state 1
SS7 MTP2 states for channel 1
Protocol version for channel 1 is Japan NTT Q.703 Version 1-1
  MTP2LSC_OOS           MTP2IAC_IDLE
  MTP2TXC_INSERVICE    MTP2RC_IDLE
  MTP2SUERM_IDLE        MTP2AERM_IDLE
  MTP2CONGESTION_IDLE
    Congestion Backhaul = Abate
  Remote Processor Outage = FALSE
```

Table 56 SS7 MTP 2 State Information Fields

State	Description	Possible Values
MTP2LSC	Indicates the overall status of the link.	OOS—The link is Out-of-Service. INITIAL_ALIGNMENT—The link is in a transitional link alignment state. ALIGNED_READY—The link is in a transitional link alignment state. ALIGNED_NOT_READY—The link is in a transitional link alignment state. INSERVICE—The link is in service. PROCESSOR_OUTAGE—There is an outage in the local processor. This state implies that the link has been aligned. POWER_OFF—It is possible you don't have the I/O memory set to at least 40 percent. There may not be enough memory for the SS7 MTP2 signaling.
MTP2IAC	Indicates the status of the initial alignment control state machine.	IDLE—The state machine is idle. It is not aligning the link. NOT_ALIGNED—The state machine has begun the alignment process. ALIGNED—The link has exchanged the alignment handshake with the remote device. PROVING—The link alignment is being proven. This is a waiting period before the LSC state changes to INSERVICE.
MTP2TXC	Indicates the status of the transmission control state machine.	IDLE—The state machine is inactive. INSERVICE—The state machine is the active transmitter.
MTP2RC	Indicates the status of the receive control state machine.	IDLE—The state machine is inactive. INSERVICE—The state machine is the active receiver.
MTP2SUERM	Indicates the status of the signal unit error monitor (SUERM).	IDLE—The state machine is inactive. MONITORING—The SUERM is active. SUERM uses a leaky-bucket algorithm to track link errors while the link is in service. If the number of link errors reaches the threshold, the link is taken out of service.

Table 56 SS7 MTP 2 State Information Fields (continued)

State	Description	Possible Values
MTP2AERM	Indicates the status of the alignment error rate monitor state machine (AERM).	IDLE—The state machine is inactive. MONITORING—Alignment error monitor is active. This is part of the alignment process.
MTP2CONGESTION	Indicates the status of the congestion control state machine.	IDLE—The state machine is inactive. No congestion is detected; normal traffic flow. ACTIVE—Congestion has been declared. The Cisco 2600 series router is sending SIBs every T5, which indicates that the remote end should stop sending new MSUs until the local Cisco 2600 series router can catch up.
Congestion Backhaul	Indicates congestion status of the backhaul link between the Cisco SLT and the Media Gateway Controller.	Abate—The link between the Cisco 2600 series router and the Media Gateway Controller is not under congestion. Onset—The link between the Cisco 2600 series router and the Media Gateway Controller is under congestion. and the Media Gateway Controller should stop sending new MSUs until the local Cisco 2600 series router can catch up.
Remote Processor Outage	Indicates the processor outage status of the remote.	TRUE indicates that the remote is in processor outage. FALSE indicates that the remote has not declared processor outage.

show ss7 mtp2 stats

To display SS7 MTP 2 operational statistics, use the **show ss7 mtp2 stats** command in privileged EXEC mode.

```
show ss7 mtp2 stats [channel]
```

Syntax Description

channel Specifies a channel from 0 through 3.

Defaults

If you do not specify a channel, the command shows status information for channel 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples

The following example shows operations and maintenance (OM) statistics for MTP 2 channel 0. [Table 57](#) explains some of the fields.

```
Router# show ss7 mtp2 stats 0
SS7 MTP2 Statistics for channel 0
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
OMIACAlignAttemptCount = 0
OMIACAlignFailCount = 0
OMIACAlignCompleteCount = 0

OMMSU_TO_XMIT_Count = 0
OMMSU_XMIT_Count = 0
OMMSU_RE_XMIT_Count = 0
OMMSU_RCV_Count = 0
OMMSU_Posted_Count = 0
OMMSU_too_long = 0

OMFISU_XMIT_Count = 0
OMFISU_RCV_Count = 0

OMLSSU_XMIT_Count = 17
OMLSSU_XMIT_SINCount = 0
OMLSSU_XMIT_SIECount = 0
OMLSSU_XMIT_SIOCount = 0
OMLSSU_XMIT_SIOSCount = 17
OMLSSU_XMIT_SIPOCount = 0
OMLSSU_XMIT_SIBCount = 0
```

```

OMLSSU_RCV_Count          = 0
OMLSSU_RCV_SINCount       = 0
OMLSSU_RCV_SIECount       = 0
OMLSSU_RCV_SIOCount       = 0
OMLSSU_RCV_SIOSCount      = 0
OMLSSU_RCV_SIPOCount      = 0
OMLSSU_RCV_SIBCount       = 0
OMLSSU_RCV_InvalidCount   = 0

OMRemote_PO_Count         = 0
OMRemote_Congestion_Cnt   = 0

OMtimeINSV (secs)         = 0
OMtimeNotINSV (secs)      = 9550
OMMSUBytesTransmitted     = 0
OMMSUBytesReceived        = 0

OMTransmitReqCount        = 33
OMPDU_notAcceptedCount    = 0
OMPDU_NACK_Count          = 0
OMunreasonableFSN_rcvd    = 0
OMunreasonableBSN_rcvd    = 0

OMT1_TMO_Count            = 0
OMT2_TMO_Count            = 0
OMT3_TMO_Count            = 0
OMT4_TMO_Count            = 0
OMT5_TMO_Count            = 0
OMT6_TMO_Count            = 0
OMT7_TMO_Count            = 0
OMT8_TMO_Count            = 0
OMTA_TMO_Count            = 0
OMTF_TMO_Count            = 0
OMTO_TMO_Count            = 0
OMTS_TMO_Count            = 477218
OMLostTimerCount          = 0

OMOMLostBackHaulMsgs      = 0

OMAERMCount               = 0
OMAERMFailCount           = 0
OMSUERMCount              = 0
OMSUERMFailCount          = 0
OMCongestionCount         = 0
OMCongestionBackhaulCnt   = 0

```

Table 57 SS7 OM Information Fields

Field	Description
OMIACAlignAttemptCount OMIACAlignFailCount OMIACAlignCompleteCount	Counts for Initial Alignment Control (IAC) attempts.
OMMSU_TO_XMIT_Count	This count is related to the results of the show ss7 sm stats command's PDU_pkts_recieve_count statistic. The number shown in OMMSU_TO_XMIT_Count is less than the PDU_pkts_recieve_count because OMMSU_TO_XMIT_Count shows the number of PDUs going out on the link, while the PDU_pkts_recieve_count includes PDUs that are internal to MTP2.
OMMSU_RCV_Count	Related to the results of the show ss7 sm stats command's packets_send_count.
OMLSSU_XMIT_Count OMLSSU_XMIT_SINCount OMLSSU_XMIT_SIECount OMLSSU_XMIT_SIOCount OMLSSU_XMIT_SIOSCount OMLSSU_XMIT_SIPOCount OMLSSU_XMIT_SIBCount	These counters represent the number of times that MTP 2 has posted the specific Link Status Signal Unit (LSSU) to MTP 1. They do <i>not</i> show the number of LSSUs actually sent over the link.
OMLSSU_RCV_Count OMLSSU_RCV_SINCount OMLSSU_RCV_SIECount OMLSSU_RCV_SIOCount OMLSSU_RCV_SIOSCount OMLSSU_RCV_SIPOCount OMLSSU_RCV_SIBCount OMLSSU_RCV_InvalidCount	These counters represent the number of LSSUs received by MTP 2 from MTP 1. Because of MTP 1 filtering, this is <i>not</i> the same as the actual LSSUs sent over the link.

Table 57 SS7 OM Information Fields (continued)

Field	Description
OMT1_TMO_Count	These fields show information about timers in use.
OMT2_TMO_Count	
OMT3_TMO_Count	
OMT4_TMO_Count	
OMT5_TMO_Count	
OMT6_TMO_Count	
OMT7_TMO_Count	
OMT8_TMO_Count	
OMTA_TMO_Count	
OMTF_TMO_Count	
OMTO_TMO_Count	
OMTA_TMO_Count	
OMLostTimerCount	
OMLostBackhaulMsgs	This count is related to the results of the show ss7 sm stats command's PDU_pkts_recieve_count statistic. The counter indicates how many messages received from the Media Gateway Controller have been lost because of a lack of resources in the Cisco 2600 series router. For example, if the Media Gateway Controller sends 100 MSUs and the Cisco 2600 series router only has 65 free buffers, 35 MSUs might be lost.

show ss7 mtp2 timer

To display durations of the SS7 MTP 2 state machine timers, use the **show ss7 mtp2 timer** command in privileged EXEC mode.

show ss7 mtp2 timer [*channel*]



Note

The eight timers whose status is displayed using the **show ss7 mtp2 timer** command are set on the Media Gateway Controller using MML commands. The timers are then downloaded from the controller to the Cisco SLT.

Syntax Description

<i>channel</i>	Specifies a channel from 0 through 3.

Defaults

If you do not specify a channel, the command shows status information for channel 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

MTP 2 uses eight different timers on each link. Throughout the link state transitions, multiple timers are active. An in-service MTP 2 link requires timers that are constantly started, stopped, and restarted. Use this command to display the configured timer durations.



Note

All MTP 2 configuration parameters are set at the Cisco SLT command line interface. The Media Gateway Controller parameter data files are no longer used to configure the Cisco SLT.

Examples

The following example shows how to display timer information for channel 0:

```
Router# show ss7 mtp2 timer 0
SS7 MTP2 Timers for channel 0 in milliseconds
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
  T1 aligned/ready = 15000
    T2 not aligned = 5000
      T3 aligned = 3000
T4 Emergency Proving = 3000
  T4 Normal Proving = 3000
    T5 sending SIB = 200
      T6 remote cong = 3000
T7 excess ack delay = 2000
  T8 errored int mon = 0
TA SIE timer = 20
  TF FISU timer = 20
    TO SIO timer = 20
      TS SIOS timer = 20
```

show ss7 mtp2 variant

To display information about the SS7 MTP 2 protocol variant, use the **show ss7 mtp2 variant** command in privileged EXEC mode.

show ss7 mtp2 variant [*channel*]

Syntax Description	<i>channel</i>	Specifies a channel from 0 through 3.

Defaults	If you do not specify a channel, the command shows protocol information for channel 0.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(7)XR	This command was introduced.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines	Each country specifies its own variant of SS7, and the Cisco SLT supports several variants of the MTP 2 protocol. The selected variant can affect the MTP 2 statistics displayed by various commands. The Cisco SLT support the following variants:

- Telcordia Technologies (formerly Bellcore)
- ITU
- NTT (Japan)
- TTC (Japan Telecom)

Each channel can be configured to any one of the protocol variants. When you change from one variant to another, for example from Bellcore to NTT, the MTP 2 parameters default to those specified by NTT. You can then change the defaults as required.

Examples	The following example shows how to display protocol variant information for channel 1:

```
Router# show ss7 mtp2 variant 1
Protocol version for channel 1 is Bellcore GR-246-Core Issue 2, Dec 1997
```

show ss7 sm session

To display information about SS7 Session Manager session, use the **show ss7 sm session** command in privileged EXEC mode.

show ss7 sm session [*session*]

Syntax Description	<i>session</i>	Specifies a session, 0 or 1.

Defaults	If you do not specify a session, the command shows information for both sessions.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(7)XR	This command was introduced.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines	If no sessions are configured, the message “No Session is configured” appears.

Examples	The following example shows how to display session information for both sessions. Table 58 explains the fields.

```
Router# show ss7 sm session
Session[0]: Remote Host 255.255.251.254:8060, Local Host 255.255.255.254:8060
    retrans_t = 600
    cumack_t  = 300
    kp_t      = 2000
    m_retrans = 2
    m_cumack  = 3
    m_outseq  = 3
    m_rcvnum  = 32

Session[1]: Remote Host 255.255.251.255:8061, Local Host 255.255.255.254:8061
    retrans_t = 600
    cumack_t  = 300
    kp_t      = 2000
    m_retrans = 2
    m_cumack  = 3
    m_outseq  = 3
    m_rcvnum  = 32
```

```
show ss7 sm session
```

Table 58 Session Manager Session Information

Field	Description
Remote Host, Local Host	Shows the IP address and port number for the session.
retrans_t	Shows the retransmission timer value.
cumack_t	Shows the cumulative acknowledgment timer value.
m_cumack	Shows the maximum number of segments that can be received before the RUDP sends an acknowledgment.
m_outseq	Shows the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
m_rcvnum	Shows the maximum number of segments that the remote end can send before receiving an acknowledgment

Related Commands

Command	Description
ss7 session retrans_t	Sets the retransmission timer.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session	Establishes a session.

show ss7 sm set

To display information about the SS7 failover timer, use the **show ss7 sm set** command in privileged EXEC mode.

show ss7 sm set

Syntax Description	There are no arguments or keywords.

Defaults	There is no default.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(7)XR	This command was introduced.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples	The following example shows how to display failover timer information; the failover timer is set to the default of 3 seconds:

```
Router# show ss7 sm set
Session Manager Set
    failover timer = 3 seconds
```

Related Commands	Command	Description
	ss7 set failover timer	Specifies the amount of time that the Session Manager waits for the session to recover before declaring the session inactive.
	ss7 session	Establishes a session.

show ss7 sm stats

To display SS7 Session Manager session statistics, use the **show ss7 sm stats** command in privileged EXEC mode.

show ss7 sm stats

Syntax Description There are no arguments or keywords for this command.

Defaults The command shows information for both sessions.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(7)XR	This command was introduced.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines If no sessions are configured, the message “No Session is configured” appears.

Examples The following example shows how to display SS7 Session Manager statistics. The fields are self-explanatory and show information about the session state, protocol data units (PDUs) packets sent and received, and SS7 Reliable User Datagram Protocol (RUDP) performance:

```
Router# show ss7 sm stats

----- Session Manager -----

Session Manager state           = SESSION SET STATE-ACTIVE
Session Manager Up count       = 1
Session Manager Down count     = 0
    lost control packet count   = 0
        lost PDU count         = 0
    failover timer expire count = 0
    invalid_connection_id_count = 0

Session[0] statistics  SM SESSION STATE-STANDBY:
Session Down count      = 0
    Open Retry count    = 0

    Total Pkts receive count = 1
    Active Pkts receive count = 0
    Standby Pkts receive count = 1
    PDU Pkts receive count   = 0
    Unknown Pkts receive count = 0
```

```

Pkts send count                = 0
Pkts requeue count             = 0
-Pkts window full count       = 0
-Pkts resource unavail count   = 0
-Pkts enqueue fail count      = 0
PDUs dropped (Large)           = 0
PDUs dropped (Empty)           = 0

RUDP Not Ready Errs            = 0
RUDP Connection Not Open       = 0
RUDP Invalid Conn Handle       = 0
RUDP Unknown Errors            = 0
RUDP Unknown Signal            = 0
NonActive Receive count        = 0

Session[1] statistics  SM SESSION STATE-ACTIVE:
Session Down count            = 0
Open Retry count              = 0

Total Pkts receive count      = 2440
Active Pkts receive count     = 1
Standby Pkts receive count    = 0
PDU Pkts receive count        = 2439
Unknown Pkts receive count    = 0

Pkts send count                = 2905
Pkts requeue count             = 0
-Pkts window full count       = 0
-Pkts resource unavail count   = 0
-Pkts enqueue fail count      = 0
PDUs dropped (Large)           = 0
PDUs dropped (Empty)           = 0

RUDP Not Ready Errs            = 0
RUDP Connection Not Open       = 0
RUDP Invalid Conn Handle       = 0
RUDP Unknown Errors            = 0
RUDP Unknown Signal            = 0
NonActive Receive count        = 0

```

Related Commands

Command	Description
clear ss7 sm-stats	Clears the counters that track Session Manager statistics for the show ss7 sm stats command.
ss7 session	Establishes a session.

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.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR1	This command was introduced for Voice over IP on the Cisco AS5300 universal access server.
12.0(7)XK	This command was first supported for the following voice technologies on the following platforms: • Voice over IP (Cisco 2600 series, Cisco 3600 series, Cisco MC3810 multiservice concentrator) • Voice over Frame Relay (Cisco 2600 series, Cisco 3600 series, Cisco MC3810 multiservice concentrator) • Voice over ATM (Cisco 3600 series, Cisco MC3810 multiservice concentrator)
12.1(1)T	This command was first supported on the T train for the following voice technology on the following platforms: • Voice over IP (1750, Cisco 2600 series, Cisco 3600 series, Cisco AS5300 universal access server, Cisco 7200 series, and Cisco 7500 series)
12.1(2)T	This command was first supported on the T train for the following voice technologies on the following platforms: • Voice over IP (Cisco MC3810 multiservice concentrator) • Voice over Frame Relay (Cisco 2600 series, Cisco 3600 series, Cisco MC3810 multiservice concentrator) • Voice over ATM (Cisco 3600 series, Cisco MC3810 multiservice concentrator)

Usage Guidelines

This command gives detailed information about the configured rules under this rule name. If the name tag is not entered, a complete display of all the configured rules will be shown.

Examples

The following example shows output for the **show translation-rule** command:

```
Router# show translation-rule

Translation rule address:0x61AB94F8
Tag name:21
Translation rule in_used 1
**** Xrule rule table ****
    Rule :1
    in_used state:1
    Match pattern:555.%
    Sub pattern:1408555
    Match type:subscriber
    Sub type:international
**** Xrule rule table ****
    Rule :2
    in_used state:1
    Match pattern:8.%
    Sub pattern:1408555
    Match type:abbreviated
    Sub type:international
Translation rule address:0x61C2E6D4
Tag name:345
Translation rule in_used 1
**** Xrule rule table ****
    Rule :1
    in_used state:1
    Match pattern:.%555.%
    Sub pattern:7
    Match type:ANY
    Sub type:abbreviated
```

Table 59 describes the significant fields shown in the display.

Table 59 *show translation-rule Field Descriptions*

Translation rule address	The translation rule address in hex.
Tag name	The translation rule tag name.
Translation rule in_used	The translation rule in which the tag is used.
**** Xrule rule table ****	Specifies the beginning of the display for a specific rule.
Rule:x	The number of the rule.
in_used state:	The input-searched-pattern.
Match pattern:	The match pattern of the rule.
Sub pattern:	The substituted pattern.
Match type:	The match type.
Sub type:	The substituted pattern match type.

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
test translation-rule	Tests the execution of the translation rules on a specific name-tag.

Command	Description
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

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.
technology	(Optional) Displays the technology type of the VFC.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300 universal access server.
12.0(2)XH	The technology keyword was added.

Examples

The following example shows that the card in slot 1 is a C549 DSPM:

```
Router# show vfc 1 technology
```

```
Technology in VFC slot 1 is C549
```

Related Commands

Command	Description
voice-card	Configures a voice card and enters voice-card configuration mode.

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.

Defaults	No default behavior or values.

Command Modes	User EXEC

Command History	Release	Modification
	11.3 NA	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines	To identify the specific VFC, enter the number of the slot on the chassis where the VFC resides using the <i>slot</i> argument.

Examples	The following is sample output from the show vfc cap-list command:

```
Router# show vfc 1 cap-list
```

```
Capability List for VFC in slot 1:
```

```
1. fax-vfc-1.0.1.bin
2. bas-vfc-1.0.1.bin
3. cdc-g729-1.0.1.bin
4. cdc-g711-1.0.1.bin
5. cdc-g726-1.0.1.bin
6. cdc-g728-1.0.1.bin
7. cdc-gsmfr-1.0.1.bin
```

The first line in this output is a general description, stating that this is the capability list for the VFC residing in slot 1. Below this is a numbered list, each line of which identifies one currently installed in-service file.

Related Commands	Command	Description
	show vfc default-file	Displays the default files included in the default file list for this VFC.
	show vfc directory	Displays the list of all files residing on this VFC.
	show vfc version	Displays the version of the software residing on this VFC.

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

Syntax Description	<i>slot</i>	Identifies the slot where the VFC is installed. Valid entries are from 0 to 2.

Defaults	No default behavior or values.

Command Modes	User EXEC

Command History	Release	Modification
	11.3 NA	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines	Use the show vfc default-file user EXEC command to display a list of all default files for a particular voice feature card. To identify the specific VFC, enter the number of the slot on the chassis where the VFC resides using the <i>slot</i> argument.

Examples	The following is sample output from the show vfc default-file command:

```
Router# show vfc 1 default-file
```

```
Default List for VFC in slot 1:
```

```
1. btl-vfc-1.0.13.0.bin
2. cor-vfc-1.0.1.bin
3. bas-vfc-1.0.1.bin
4. cdc-g729-1.0.1.bin
5. fax-vfc-1.0.1.bin
6. jbc-vfc-1.0.13.0.bin
```

The first line in this output is a general description, stating that this is the default list for the VFC residing in slot 1. Below this is a numbered list, each line of which identifies one default file.

Related Commands	Command	Description
	show vfc cap-list	Displays the current list of files on the capability list for this VFC.
	show vfc directory	Displays the list of all files residing on this VFC.
	show vfc version	Displays the version of the software residing on this VFC.

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

Syntax Description	<i>slot</i>	Identifies the slot where the VFC is installed. Valid entries are from 0 to 2.

Defaults	No default behavior or values.

Command Modes	User EXEC

Command History	Release	Modification
	11.3 NA	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines	Use the show vfc directory user EXEC command to display a list of all of the files currently stored in Flash memory for a particular VFC. To identify the specific VFC, enter the number of the slot on the chassis where the VFC resides using the <i>slot</i> argument.

Examples	The following is sample output from the show vfc directory command:

Router# **show vfc 1 directory**

```
Files in slot 1 VFC flash:
      File Name                               Size (Bytes)
1 . vcw-vfc-mz.gsm.VCW                       292628
2 . btl-vfc-1.0.13.0.bin                      4174
3 . cor-vfc-1.0.1.bin                         54560
4 . jbc-vfc-1.0.13.0.bin                     16760
5 . fax-vfc-1.0.1.bin                         64290
6 . bas-vfc-1.0.1.bin                         54452
7 . cdc-g711-1.0.1.bin                        190
8 . cdc-g729-1.0.1.bin                       21002
9 . cdc-g726-1.0.1.bin                        190
10. cdc-g728-1.0.1.bin                       22270
11. cdc-gsmfr-1.0.1.bin                       190
```

[Table 60](#) describes the significant fields shown in the display.

Table 60 *show vfc directory Field Descriptions*

Field	Description
File Name	Name of the file stored in Flash memory.
Size (Bytes)	Size of the file in bytes.

Related Commands

Command	Description
show vfc cap-list	Displays the current list of files on the capability list for this VFC.
show vfc default-file	Displays the default files included in the default file list for this VFC.
show vfc version	Displays the version of the software residing on this VFC.

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 | vcware}

Syntax Description

<i>slot</i>	Identifies the slot where the VFC is installed. Valid values are 0, 1, and 2.
dspware	Defines which DSPWare software to display.
vcware	Defines which VCWare software to display.

Defaults

No default behavior or values.

Command Modes

User EXEC

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

Use the **show vfc version** user EXEC command to display the version of the software (running on either DSP or VFC) currently installed in Flash memory on the VFC.

Examples

The following is sample output from the **show vfc version** command:

```
Router# show vfc 0 version dspware
```

```
Version of Dspware in VFC slot 0 is 0.10
```

The output from this command is a simple declarative sentence stating the version number for the selected type of software (in this example, DSPWare) for the VFC residing in the selected slot number (in this example, slot 0).

Related Commands

Command	Description
show vfc cap-list	Displays the current list of files on the capability list for this VFC.
show vfc default-file	Displays the default files included in the default file list for this VFC.
show vfc directory	Displays the list of all files residing on this VFC.

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

Syntax Description	There are no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(5)XK	This command was introduced for the Cisco MC3810 multiservice concentrator.
	12.0(7)T	The command introduced in Cisco IOS Release 12.0(5)XK was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines	Use this command to look quickly at the status of current calls. In Cisco IOS Releases 12.0(5)XK and 12.0(7)T, there can be only one video call in progress.

Examples	On a Cisco MC3810 multiservice concentrator, the following example displays information about the ViCM when no call is in progress on the serial interface that connects to the local video codec:

```
Router# show video call summary
```

```
Serial0:ViCM = Idle, Codec Ready
```

When a call is starting, the output looks like this:

```
Router# show video call summary
```

```
Serial0:ViCM = Call Connected
```

When a call is disconnecting, the output looks like this:

```
Router# show video call summary
```

```
Serial0:ViCM = Idle
```

Related Commands	Command	Description
	show call history video record	Displays information about video calls.

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.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(3)T	This command was introduced on the Cisco MC3810 multiservice concentrator.
	12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series.
	12.1(2)T	This command was integrated into the 12.1(2)T release.

Usage Guidelines The **show voice busyout** command lists the following information:

- Interfaces that are being monitored for busyout events
- Voice ports currently in the busyout state and the reasons

Examples The following example displays the busyout information:

```
Router# show voice busyout
```

```
If following network interfaces are down, voice port will be put into busyout state
ATM0
```

```
Serial0
```

```
The following voice ports are in busyout state
```

```
1/1      is forced into busyout state
1/2      is in busyout state caused by network interfaces
1/3      is in busyout state caused by ATM0
1/4      is in busyout state caused by network interfaces
1/5      is in busyout state caused by Serial0
```

Related Commands

Command	Description
busyout forced	Forces a voice port into the busyout state.
busyout monitor	Places a voice port in the busyout monitor state.
busyout seize	Changes the busyout seize procedure from a voice port.
voice-port busyout	Places all voice ports associated with a serial or ATM interface in a busyout state.

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. <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. <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.) <i>port</i> specifies an analog voice port number. Valid entries are 0 and 1.
summary	(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. <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. <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.) <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.
summary	(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. <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. <i>port</i> specifies an analog voice port number. Valid entries are from 1 to 6.
summary	(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. <i>slot</i> specifies the module (and controller). Valid entries are 0 for the MFT (controller 0) and 1 for the DVM (controller 1). <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.
summary	(Optional) Displays a summary of all voice ports.

Command Modes	EXEC

Command History	Release	Modification
	11.3(1)MA	This command was introduced for the Cisco MC3810 multiservice concentrator.
	12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series.
	12.1(2)T	This command was integrated into the 12.1(2)T release.

Usage Guidelines

The **show voice call** command applies to Voice over Frame Relay, Voice over ATM, and Voice over IP. This command shows call-processing and protocol state-machine information for a voice port, if it is available. It also shows information on the DSP channel associated with the voice port, if it is available. All real-time information in the DSP channel, such as jitter and buffer overrun for example, is queried to the DSP channel, and asynchronous responses are returned to the host side.

If no call is active on a voice port, the **show voice call summary** command displays only the VPM (shutdown) state. If a call is active on a voice port, the VTSPS state is shown. For an on-net call or a local call without local-bypass (not cross-connected), the CODEC and VAD fields are displayed. For an off-net call or a local call with local-bypass, the CODEC and VAD fields are not displayed.

CODEC and VAD are not displayed by the **show voice call** command because this information is in the summary display.

The **show voice call** command provides the status at these levels of the call handling module:

- Tandem switch
- End-to-end call manager
- Call processing state machine
- Protocol state machine

Examples

The following is a sample display from the **show voice call summary** command for voice ports on a Cisco MC3810 multiservice concentrator, showing two local calls connected without local bypass:

PORT	CODEC	VAD	VTSP	STATE	VPM STATE
0:17.18					*shutdown*
0:18.19	g729ar8	n	S_CONNECT		FXOLS_OFFHOOK
0:19.20					FXOLS_ONHOOK
0:20.21					FXOLS_ONHOOK
0:21.22					FXOLS_ONHOOK
0:22.23					FXOLS_ONHOOK
0:23.24					EM_ONHOOK
1/1					FXSLS_ONHOOK
1/2					FXSLS_ONHOOK
1/3					EM_ONHOOK
1/4					EM_ONHOOK
1/5					FXOLS_ONHOOK
1/6	g729ar8	n	S_CONNECT		FXOLS_CONNECT

The following is a sample display from the **show voice call summary** command for voice ports on a Cisco MC3810 multiservice concentrator, showing two local calls connected with local bypass:

PORT	CODEC	VAD	VTSP	STATE	VPM STATE
0:17.18					*shutdown*
0:18.19			S_CONNECT		FXOLS_OFFHOOK
0:19.20					FXOLS_ONHOOK
0:20.21					FXOLS_ONHOOK
0:21.22					FXOLS_ONHOOK
0:22.23					FXOLS_ONHOOK
0:23.24					EM_ONHOOK
1/1					FXSLS_ONHOOK
1/2					FXSLS_ONHOOK
1/3					EM_ONHOOK
1/4					EM_ONHOOK
1/5					FXOLS_ONHOOK
1/6			S_CONNECT		FXOLS_CONNECT

The following is a sample display from the **show voice call** command for analog voice ports on a Cisco MC3810 multiservice concentrator:

```

1/1 vpm level 1 state = FXSLS_ONHOOK
vpm level 0 state = S_UP
1/2 vpm level 1 state = FXSLS_ONHOOK
vpm level 0 state = S_UP
1/3 is shutdown
1/4 vtsp level 0 state = S_CONNECT
vpm level 1 state = S_TRUNKED
vpm level 0 state = S_UP
1/5 vpm level 1 state = EM_ONHOOK
vpm level 0 state = S_UP
1/6 vpm level 1 state = EM_ONHOOK
vpm level 0 state = S_UP

```

```

sys252#show voice call 1/4
1/4 vtsp level 0 state = S_CONNECT
vpm level 1 state = S_TRUNKED
vpm level 0 state = S_UP
router#***DSP VOICE VP_DELAY STATISTICS***
Clk Offset(ms): 1445779863, Rx Delay Est(ms): 95
Rx Delay Lo Water Mark(ms): 95, Rx Delay Hi Water Mark(ms): 125
***DSP VOICE VP_ERROR STATISTICS***
Predict Conceal(ms): 10, Interpolate Conceal(ms): 0
Silence Conceal(ms): 0, Retroact Mem Update(ms): 0
Buf Overflow Discard(ms): 20, Talkspurt Endpoint Detect Err: 0
***DSP VOICE RX STATISTICS***
Rx Vox/Fax Pkts: 537, Rx Signal Pkts: 0, Rx Comfort Pkts: 0
Rx Dur(ms): 50304730, Rx Vox Dur(ms): 16090, Rx Fax Dur(ms): 0
Rx Non-seq Pkts: 0, Rx Bad Hdr Pkts: 0
Rx Early Pkts: 0, Rx Late Pkts: 0
***DSP VOICE TX STATISTICS***
Tx Vox/Fax Pkts: 567, Tx Sig Pkts: 0, Tx Comfort Pkts: 0
Tx Dur(ms): 50304730, Tx Vox Dur(ms): 17010, Tx Fax Dur(ms): 0
***DSP VOICE ERROR STATISTICS***
Rx Pkt Drops(Invalid Header): 0, Tx Pkt Drops(HPI SAM Overflow): 0
***DSP LEVELS***
TDM Bus Levels(dBm0): Rx -70.3 from PBX/Phone, Tx -68.0 to PBX/Phone
TDM ACOM Levels(dBm0): +2.0, TDM ERL Level(dBm0): +5.6
TDM Bgd Levels(dBm0): -71.4, with activity being voice

```

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all VoIP and POTS dial peers configured on the router.
show voice dsp	Displays the current status of all DSP voice channels.
show voice port	Displays configuration information about a specific voice port.

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.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.
	12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series routers, and the display format was modified.
	12.1(2)T	This command was integrated into the 12.1(2)T release.

Usage Guidelines Use this command when abnormal behavior in the DSP voice channels occurs.

Examples The following is sample output from the **show voice dsp** command on a Cisco MC3810 multiservice concentrator:

```
Router# show voice dsp

DSP# 0, channel# 0 G729A BUSY
DSP# 0, channel# 1 G729A BUSY
DSP# 1, channel# 2 FAX IDLE
DSP# 1, channel# 3 FAX IDLE
DSP# 2, channel# 4 NONE BAD
DSP# 2, channel# 5 NONE BAD
DSP# 3, channel# 6 NONE BAD
DSP# 3, channel# 7 NONE BAD
DSP# 4, channel# 8 NONE BAD
DSP# 4, channel# 9 NONE BAD
DSP# 5, channel# 10 NONE BAD
DSP# 5, channel# 11 NONE BAD
```

[Table 61](#) describes the significant fields shown in the display.

Table 61 *show voice dsp Field Descriptions*

Field	Description
DSP	Number of the DSP.
Channel	Number of the channel and its status.

The following is sample output from the **show voice dsp** command on a Cisco 1750 router:

Router# **show voice dsp**

```
DSP#0: state IN SERVICE, 2 channels allocated
channel#0: voice port 1/0, codec G711 ulaw, state UP
channel#1: voice port 1/1, codec G711 ulaw, state UP
DSP#1: state IN SERVICE, 2 channels allocated
channel#0: voice port 2/0, codec G711 ulaw, state UP
channel#1: voice port 2/1, codec G711 ulaw, state UP
DSP#2: state RESET, 0 channels allocated
```

[Table 62](#) describes the significant fields shown in the display.

Table 62 *show voice dsp Field Descriptions*

Field	Description
DSP	Number of the DSP.
Channel	Number of the channel and its status.

Related Commands

Command	Description
clear counters	Clears all the current interface counters from the interface.
show dial-peer voice	Displays configuration information for dial peers.
show voice call	Displays the call status for all voice ports.
show voice port	Displays configuration information about a specific voice port.

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.
summary	(Optional) Displays summary information about VoFR and VoATM ports used for permanent connections.

Defaults

No default behavior or values.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(4)T	The command introduced in Cisco IOS Release 12.0(3)XG was integrated into Cisco IOS Release 12.0(4)T.

Usage Guidelines

This command is available only on the Cisco MC3810 multiservice concentrator.

When no parameters are specified with this command, the output displays information for all ports containing permanent calls. When a specific interface is specified, information is displayed about the permanent calls for that interface only.

Examples

The following is sample output for the **show voice permanent-call** command:

```
Router# show voice permanent-call 1/1

1/1 state=connect coding=G729A payload size=30 vad=off
ec=8 (ms), cng=off fax=on digit_relay=on Seq num = off, VOFR Serial0,dlci = 550,cid = 6
TX INFO :slow-mode seq#= 25, sig pkt cnt= 19646, last-ABCD=1101
hardware-state ACTIVE signal type is CEPT/MELCAS
voice-gate CLOSED,network-path OPEN MASTER
 1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
 1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
 1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
RX INFO :slow-mode, sig pkt cnt= 19648, under-run = 0, over-run = 0
missing = 0, out of seq = 0, very late = 0
playout depth = 0 (ms), refill count = 1
  prev-seq#= 25, last-ABCD=1101, slave standby timeout 25000 (ms)
max inter-arrival time 0 (ms), current timer 384 (ms)
```

```

max timeout timer 5016 (ms), restart timeout is 0 (ms)
signaling packet fast-mode inter-arrival times (ms)
16 24 16 24 16 24 16 24 16 24 16 24 16 24
16 24 16 24 16 24 16 24 0 0 0 0 0 0 0

signaling playout history
1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
1101 1101 1101 1101 1101 1101 1101 1101 1101 1101

```

The following is sample output for the **show voice permanent-call summary** command:

Router# **show voice permanent-call summary**

```

1/1 state= connect, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 880,cid = 6
1/2 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 102
1/3 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 103
1/4 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 104
1/5 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 105
1/6 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 106
1/7 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 107
1/8 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 108
1/9 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 109
1/10 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 110
1/11 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 111
1/12 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 112
1/13 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 113
1/14 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 114
1/15 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 115
1/17 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 117
1/18 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 118
1/19 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 119
1/20 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 120
1/21 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 121
1/22 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 122
1/23 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 123
1/24 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 124
1/25 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 125

```

Table 63 describes the fields shown in these displays.

Table 63 *show voice permanent-call Field Descriptions*

Field	Description
state	Current status of the call on this voice port.
coding	Codec type used for this call.
payload size	Size in bytes of the voice payload.
vad	Indicates whether voice activity detection is turned on or off.
ec	Echo canceler length, in milliseconds.
cng	Indicates whether or not comfort noise generation is used.
fax	Indicates if fax-relay is enabled.
digit_relay	Indicates if FRF.11 Annex A DTMF digit-relay is enabled.
Seq num	Indicates whether sequence numbers are turned on or off.
VOFR	Interface used for this call.
dlci	DLCI for this call.
cid	DLCI subchannel for this call.
TX INFO:slow-mode	Indicates that FRF.11 Annex B packets are being sent at the slow rate defined by the signal timing keepalive period.
TX INFO:seq#	Sequence number of the last packet sent.
TX INFO:sig pkt cnt	Number of signaling packets sent by this dial peer.
TX INFO:last-ABCD	Last ABCD signaling state sent by this dial peer to the network.
hardware-state	Indicates the on-hook/off-hook state of the call when the signaling protocol in use is a supported protocol. Not valid when the signal type is “transparent.”
signal type	Indicates the type of call-control signaling used by this dial peer.
voice-gate	Indicates whether voice packets are being sent (OPEN) or not sent (CLOSED).
network-path	Indicates if any type of packet is being sent (OPEN) or not sent (CLOSED) to the network. This field will indicate CLOSED only if the port is configured as a slave using the connection trunk answer-mode command.
RX INFO:slow-mode	Indicates that FRF.11 Annex B packets are being received at the slow rate. Successive packets have the same sequence number.
RX INFO:sig pkt cnt	Number of slow-mode signaling packets received by this dial peer.
RX INFO:under-run	Valid for fast-mode only. Counts the number of times the signaling playout buffer became empty during FRF.11 Annex B fast-mode. In this mode, signaling packets are expected to be received every 20 milliseconds.
RX INFO:over-run	Valid for fast-mode only. Counts the number of times the signaling playout buffer became full during FRF.11 Annex B fast-mode. In this mode, signaling packets are expected to be received every 20 milliseconds.

Table 63 *show voice permanent-call Field Descriptions (continued)*

Field	Description
RX INFO:missing	Indicates the number of FRF.11 Annex B packets that were counted as missing based on checking Annex B sequence numbers.
RX INFO:out of seq	Number of FRF.11 Annex B packets that were counted as received in the wrong order based on checking Annex B sequence numbers.
RX INFO:very late	Number of FRF.11 Annex B packets that were received with a sequence number significantly different from the expected sequence number.
RX INFO:playout depth	Valid for fast-mode only. Shows the current FRF.11 Annex B signaling buffer playout depth in milliseconds.
RX INFO:refill count	Indicates the number of times the FRF.11 Annex B signaling playout buffer was refilled as a result of a slow-mode to fast-mode transition.
RX INFO:prev-seq#	Sequence number of the last FRF.11 Annex B signaling packet received.
RX INFO:last-ABCD	Last ABCD signaling bit pattern sent to the attached PBX (telephone network side). In the out-of-service condition, this will show the OOS pattern being sent to the PBX.
RX INFO:slave standby timeout	Value configured using the signal timing oos standby command for the applicable voice class permanent entry.
max inter-arrival time	Maximum interval between the arrival of fast-mode FRF.11 Annex B packets since the last time this parameter was displayed.
current timer	Time, in milliseconds, since the last signaling packet was received.
max timeout timer	Maximum value of the “current timer” parameter since the last time it was displayed.
restart timeout	Connection restart timeout value.
signaling packet fast-mode inter-arrival time	Shows the last several values of the fast-mode FRF.11 Annex B signaling packet inter-arrival time.
signaling playout history	Shows recent ABCD signaling bits received from the data network.

Related Commands

Command	Description
show frame-relay fragment	Displays Frame Relay fragmentation details.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show frame-relay vofr	Displays details about FRF.11 subchannels being used on Voice over Frame Relay DLCIs.

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:	
slot-number	Slot number in the router where the voice interface card (VIC) is installed. Valid entries are from 0 to 2, depending on the slot where it has been installed.
port	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. • <i>slot</i> specifies a router slot in which a voice network module (VNM) is installed. Valid entries are router slot numbers for the particular platform. • <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.) • <i>port</i> specifies an analog voice port number. Valid entries are 0 and 1.
summary	(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. • <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. • <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.) • <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.
summary	(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. • <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. • <i>port</i> specifies an analog voice port number. Valid entries are from 1 to 6.
summary	(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. <i>slot</i> specifies the module (and controller). Valid entries are 0 for the MFT (controller 0) and 1 for the DVM (controller 1). <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.
summary	(Optional) Displays a summary of all voice ports.

For the Cisco AS5300 Access Server :

<i>controller number</i>	Specifies the T1 or E1 controller.
:D	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.
:D	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.

Defaults

No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	11.3(1) T	This command was introduced on the Cisco 3600 series router.
	11.3(1)MA	Port-specific values for the Cisco MC3810 multiservice concentrator were added.
	12.0(3)T	Port-specific values for the Cisco MC3810 multiservice concentrator were added.
	12.0(5)XK	The <i>ds0-group</i> argument was added for the Cisco 2600 and Cisco 3600 series routers.
	12.0(5)XE	Additional syntax was created for digital voice to allow specification of the DS0 group. This command applies to VoIP on the Cisco 7200 series.
	12.0(7)T	The additions from Cisco IOS Release 12.0(5)XE were integrated into Cisco IOS Release 12.0(7)T.
	12.0(7)XK	The summary keyword was added for the Cisco 2600 and 3600 series routers. The <i>ds0-group</i> argument was added for the Cisco MC3810 multiservice concentrator.
	12.1(2)T	This command was integrated into the 12.1(2)T release.

Usage Guidelines

Use the **show voice port EXEC** command to display configuration and voice-interface-card-specific information about a specific port.

This command applies to Voice over IP, Voice over Frame Relay, and Voice over ATM.

The **ds0-group** command automatically creates a logical voice port that is numbered as follows on Cisco 7200 series routers and the Cisco 2600 and Cisco 3600 series routers: *slot/port:ds0-group-no*. Although only one voice port is created for each group, applicable calls are routed to any channel in the group.

Examples

The following is sample output from the **show voice port summary** command for all voice ports on a Cisco MC3810 multiservice concentrator with an analog voice module (AVM):

```

IN  OUT  ECHO
PORT SIG-TYPE  ADMIN OPER IN-STATUS OUT-STATUS GAIN ATTN CANCEL
1/1  fxs-ls      up   up   on-hook  idle      0    0    y
1/2  fxs-ls      up   up   on-hook  idle      0    0    y
1/3  e&m-wnk     up   up   idle     idle      0    0    y
1/4  e&m-wnk     up   up   idle     idle      0    0    y
1/5  fxo-ls      up   up   idle     on-hook   0    0    y
1/6  fxo-ls      up   up   idle     on-hook   0    0    y

```

The following is sample output from the **show voice port summary** command on a Cisco MC3810 multiservice concentrator with a digital voice module (DVM):

```

          IN      OUT
PORT  CH SIG-TYPE  ADMIN OPER STATUS STATUS  EC
=====
0:17  18 fxo-ls      down down idle  on-hook  y
0:18  19 fxo-ls      up   dorm idle  on-hook  y
0:19  20 fxo-ls      up   dorm idle  on-hook  y
0:20  21 fxo-ls      up   dorm idle  on-hook  y

```

■ show voice port

```

0:21 22 fxo-ls      up    dorm idle    on-hook y
0:22 23 fxo-ls      up    dorm idle    on-hook y
0:23 24 e&m-imd     up    dorm idle    idle      y
1/1  -- fxs-ls      up    dorm on-hook idle      y
1/2  -- fxs-ls      up    dorm on-hook idle      y
1/3  -- e&m-imd     up    dorm idle    idle      y
1/4  -- e&m-imd     up    dorm idle    idle      y
1/5  -- fxo-ls      up    dorm idle    on-hook y
1/6  -- fxo-ls      up    dorm idle    on-hook y
Elements :
sys/voip/ccvpm          vpm_htsp.c (107)
sys/voip/ccvtsp         vtsp_core.c (167)
sys/voip/cli            voiceport_action.c (58)

```

```

receiVe and transMit Slot is 1, Sub-unit is 0, Port is 1
Type of VoicePort is E&M
Operation State is DORMANT
Administrative State is UP
No Interface Down Failure
Description is not set
Noise Regeneration is enabled
Non Linear Processing is enabled
Music On Hold Threshold is Set to -38 dBm
In Gain is Set to 0 dB
Out Attenuation is Set to 0 dB
Echo Cancellation is enabled
Echo Cancel Coverage is set to 8 ms
Connection Mode is normal
Connection Number is not set
Initial Time Out is set to 10 s
Interdigit Time Out is set to 10 s
Region Tone is set for US

```

The following is sample output from the **show voice port** command for an E&M analog voice port on a Cisco 3600:

```

E&M Slot is 1, Sub-unit is 0, Port is 0
Type of VoicePort is E&M
Operation State is unknown
Administrative State is unknown
The Interface Down Failure Cause is 0
Alias is NULL
Noise Regeneration is disabled
Non Linear Processing is disabled
Music On Hold Threshold is Set to 0 dBm
In Gain is Set to 0 dB
Out Attenuation is Set to 0 dB
Echo Cancellation is disabled
Echo Cancel Coverage is set to 16ms
Connection Mode is Normal
Connection Number is
Initial Time Out is set to 0 s
Interdigit Time Out is set to 0 s
Analog Info Follows:
Region Tone is set for northamerica
Currently processing none
Maintenance Mode Set to None (not in mtc mode)
Number of signaling protocol errors are 0

Voice card specific Info Follows:
Signal Type is wink-start
Operation Type is 2-wire
Impedance is set to 600r Ohm
E&M Type is unknown

```

```
Dial Type is dtmf
In Seizure is inactive
Out Seizure is inactive
Digit Duration Timing is set to 0 ms
InterDigit Duration Timing is set to 0 ms
Pulse Rate Timing is set to 0 pulses/second
InterDigit Pulse Duration Timing is set to 0 ms
Clear Wait Duration Timing is set to 0 ms
Wink Wait Duration Timing is set to 0 ms
Wink Duration Timing is set to 0 ms
Delay Start Timing is set to 0 ms
Delay Duration Timing is set to 0 ms
```

The following is sample output from the **show voice port** command for a Foreign Exchange Station (FXS) analog voice port on a Cisco 3600:

```
Foreign Exchange Station 1/0/0 Slot is 1, Sub-unit is 0, Port is 0
Type of VoicePort is FXS
Operation State is DORMANT
Administrative State is UP
The Interface Down Failure Cause is 0
Alias is NULL
Noise Regeneration is enabled
Non Linear Processing is enabled
Music On Hold Threshold is Set to 0 dBm
In Gain is Set to 0 dB
Out Attenuation is Set to 0 dB
Echo Cancellation is enabled
Echo Cancel Coverage is set to 16ms
Connection Mode is Normal
Connection Number is
Initial Time Out is set to 10 s
Interdigit Time Out is set to 10 s
Analog Info Follows:
Region Tone is set for northamerica
Currently processing none
Maintenance Mode Set to None (not in mtc mode)
Number of signaling protocol errors are 0
Voice card specific Info Follows:
Signal Type is loopStart
Ring Frequency is 25 Hz
Hook Status is On Hook
Ring Active Status is inactive
Ring Ground Status is inactive
Tip Ground Status is inactive
Digit Duration Timing is set to 100 ms
InterDigit Duration Timing is set to 100 ms
Hook Flash Duration Timing is set to 600 ms
```

The following is sample output from the **show voice port** command for an FXS analog voice port on a Cisco MC3810 multiservice concentrator:

```
Voice port 1/2 Slot is 1, Port is 2
Type of VoicePort is FXS
Operation State is UP
Administrative State is UP
No Interface Down Failure
Description is not set
Noise Regeneration is enabled
Non Linear Processing is enabled
In Gain is Set to 0 dB
Out Attenuation is Set to 0 dB
Echo Cancellation is enabled
Echo Cancel Coverage is set to 8 ms
```

■ show voice port

```

Connection Mode is normal
Connection Number is not set
Initial Time Out is set to 10 s
Interdigit Time Out is set to 10 s
Coder Type is g729ar8
Companding Type is u-law
Voice Activity Detection is disabled
Ringing Time Out is 180 s
Wait Release Time Out is 30 s
Nominal Playout Delay is 80 milliseconds
Maximum Playout Delay is 160 milliseconds

Analog Info Follows:
Region Tone is set for northamerica
Currently processing Voice
Maintenance Mode Set to None (not in mtc mode)
Number of signaling protocol errors are 0
Impedance is set to 600r Ohm
Analog interface A-D gain offset = -3 dB
Analog interface D-A gain offset = -3 dB
Voice card specific Info Follows:
Signal Type is loopStart
Ring Frequency is 20 Hz
Hook Status is On Hook
Ring Active Status is inactive
Ring Ground Status is inactive
Tip Ground Status is active
Digit Duration Timing is set to 100 ms
InterDigit Duration Timing is set to 100 ms
Ring Cadence are [20 40] * 100 msec
InterDigit Pulse Duration Timing is set to 500 ms

```

The following is sample output from the **show voice port** command for an E&M digital voice port on a Cisco 3600:

```

receIve and transMit Slot is 1, Sub-unit is 0, Port is 1
Type of VoicePort is E&M
Operation State is DORMANT
Administrative State is UP
No Interface Down Failure
Description is not set
Noise Regeneration is enabled
Non Linear Processing is enabled
Music On Hold Threshold is Set to -38 dBm
In Gain is Set to 0 dB
Out Attenuation is Set to 0 dB
Echo Cancellation is enabled
Echo Cancel Coverage is set to 8 ms
Connection Mode is normal
Connection Number is not set
Initial Time Out is set to 10 s
Interdigit Time Out is set to 10 s
Region Tone is set for US

```

The following is sample output from the **show voice port summary** command for all voice ports on a Cisco MC3810 multiservice concentrator with an analog voice module (AVM):

```

IN  OUT  ECHO
PORT SIG-TYPE      ADMIN OPER IN-STATUS OUT-STATUS CODEC  VAD GAIN ATTN CANCEL
1/1  fxs-ls        up   up   on-hook  idle    729a  n   0   0   y
1/2  fxs-ls        up   up   on-hook  idle    729a  n   0   0   y
1/3  e&m-wnk       up   up   idle     idle    729a  n   0   0   y
1/4  e&m-wnk       up   up   idle     idle    729a  n   0   0   y
1/5  fxo-ls        up   up   idle     on-hook 729a  n   0   0   y
1/6  fxo-ls        up   up   idle     on-hook 729a  n   0   0   y

```

Table 64 explains the fields in the sample output

Table 64 *show voice port Field Descriptions*

Field	Description
Administrative State	Administrative state of the voice port.
Alias	User-supplied alias for the voice port.
Analog interface A-D gain offset	Offset of the gain for analog-to-digital conversion.
Analog interface D-A gain offset	Offset of the gain for digital-to-analog conversion.
Clear Wait Duration Timing	Time of inactive seizure signal to declare call cleared.
Coder Type	Voice compression mode used.
Companding Type	Companding standard used to convert between analog and digital signals in PCM systems.
Connection Mode	Connection mode of the interface.
Connection Number	Full E.164 telephone number used to establish a connection with the trunk or PLAR mode.
Currently Processing	Type of call currently being processed: none, voice, or fax.
Delay Duration Timing	Maximum delay signal duration for delay dial signaling.
Delay Start Timing	Timing of generation of delayed start signal from detection of incoming seizure.
Description	Description of the voice port.
Dial Type	Out-dialing type of the voice port.
Digit Duration Timing	DTMF digit duration in milliseconds.
E&M Type	Type of E&M interface.
Echo Cancel Coverage	Echo cancel coverage for this port.
Echo Cancellation	Whether or not echo cancellation is enabled for this port.
Hook Flash Duration Timing	Maximum length of hook flash signal.
Hook Status	Hook status of the FXO/FXS interface.
Impedance	Configured terminating impedance for the E&M interface.
In Gain	Amount of gain inserted at the receiver side of the interface.
In Seizure	Incoming seizure state of the E&M interface.
Initial Time Out	Amount of time the system waits for an initial input digit from the caller.
InterDigit Duration Timing	DTMF interdigit duration, in milliseconds.

Table 64 *show voice port Field Descriptions (continued)*

Field	Description
InterDigit Pulse Duration Timing	Pulse dialing interdigit timing, in milliseconds.
Interdigit Time Out	Amount of time the system waits for a subsequent input digit from the caller.
Maintenance Mode	Maintenance mode of the voice port.
Maximum Playout Delay	The amount of time before the Cisco MC3810 multiservice concentrator DSP starts to discard voice packets from the digital signal processor (DSP) buffer.
Music On Hold Threshold	Configured Music-On-Hold Threshold value for this interface.
Noise Regeneration	Whether or not background noise should be played to fill silent gaps if VAD is activated.
Nominal Playout Delay	The amount of time the Cisco MC3810 multiservice concentrator DSP waits before starting to play out the voice packets from the DSP buffer.
Non-Linear Processing	Whether or not nonlinear processing is enabled for this port.
Number of signaling protocol errors	Number of signaling protocol errors.
Operations State	Operation state of the port.
Operation Type	Operation of the E&M signal: two-wire or four-wire.
Out Attenuation	Amount of attenuation inserted at the transmit side of the interface.
Out Seizure	Outgoing seizure state of the E&M interface.
Port	Port number for this interface associated with the voice interface card.
Pulse Rate Timing	Pulse dialing rate, in pulses per second (pps).
Region Tone	Configured regional tone for this interface.
Ring Active Status	Ring active indication.
Ring Cadence	Configured ring cadence for this interface.
Ring Frequency	Configured ring frequency for this interface.
Ring Ground Status	Ring ground indication.
Ringing Time Out	Ringing timeout duration.
Signal Type	Type of signaling for a voice port: loop-start, ground-start, wink-start, immediate, and delay-dial.
Slot	Slot used in the voice interface card for this port.
Sub-unit	Subunit used in the voice interface card for this port.
Tip Ground Status	Tip ground indication.
Type of VoicePort	Type of voice port: FXO, FXS, or E&M.
The Interface Down Failure Cause	Text string describing why the interface is down,
Voice Activity Detection	Whether Voice Activity Detection is enabled or disabled.

Table 64 *show voice port Field Descriptions (continued)*

Field	Description
Wait Release Time Out	The length of time a voice port stays in the call-failure state while the Cisco MC3810 multiservice concentrator sends a busy tone, a reorder tone, or an out-of-service tone to the port.
Wink Duration Timing	Maximum wink duration for wink start signaling.
Wink Wait Duration Timing	Maximum wink wait duration for wink start signaling.

The following example displays voice port configuration information for the digital voice port 0 located in slot 1, DS0 group 1:

```

receEive and transMit Slot is 1, Sub-unit is 0, Port is 1
Type of VoicePort is E&M
Operation State is DORMANT
Administrative State is UP
No Interface Down Failure
Description is not set
Noise Regeneration is enabled
Non Linear Processing is enabled
Music On Hold Threshold is Set to -38 DBMS
In Gain is Set to 0 dBm
Out Attenuation is Set to 0 dB
Echo Cancellation is enabled
Echo Cancel Coverage is set to 8 ms
Connection Mode is normal
Connection Number is not set
Initial Time Out is set to 10 s
Interdigit Time Out is set to 10 s
Region Tone is set for US

```

The following is sample output from the Cisco AS5800 for the **show voice port** command:

```

ISDN 1/0/0:D
Type of VoicePort is ISDN
Operation State is DORMANT
Administrative State is UP
No Interface Down Failure
Description is ""
Noise Regeneration is enabled
Non Linear Processing is enabled
Music On Hold Threshold is Set to -38 dBm
In Gain is Set to 0 dB
Out Attenuation is Set to 0 dB
Echo Cancellation is enabled
Echo Cancel Coverage is set to 16 ms
Connection Mode is normal
Connection Number is not set
Initial Time Out is set to 10 s
Interdigit Time Out is set to 10 s
Region Tone is set for US

```

Table 65 describes the significant fields shown in the display.

Table 65 *show voice port Field Descriptions for the Cisco AS5800*

Field	Description
Type of VoicePort	Indicates the voice port type.
Operational State	Operational state of the voice port.
Administrative State	Administrative state of the voice port.
Clear Wait Duration Timing	Time of inactive seizure signal to declare call cleared.
Currently Processing	Type of call currently being processed: none, voice, or fax.
Operations State	Operation state of the port.
Operation Type	Operation of the E&M signal: two-wire or four-wire.
Noise Regeneration	Whether or not background noise should be played to fill silent gaps if VAD is activated.
Non-Linear Processing	Whether or not nonlinear processing is enabled for this port.
Music-On-Hold Threshold	Configured music-on-hold threshold value for this interface.
In Gain	Amount of gain inserted at the receiver side of the interface.
Out Attenuation	Amount of attenuation inserted at the transmit side of the interface.
Pulse Rate Timing	Pulse dialing rate, in pulses per second (pps).
Echo Cancellation	Whether or not echo cancellation is enabled for this port.
Echo Cancel Coverage	Echo cancel coverage for this port.
Connection Mode	Connection mode of the interface.
Connection Number	Full E.164 telephone number used to establish a connection with the trunk or PLAR mode.
Initial Time Out	Amount of time the system waits for an initial input digit from the caller.
Interdigit Time Out	Amount of time the system waits for a subsequent input digit from the caller.
Regional Tone	Configured regional tone for this interface.

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.

Command Modes	User EXEC
	Privileged EXEC

Command History	Release	Modification
	12.0(3)XG	This command was introduced on the Cisco MC3810 multiservice concentrator as show voice permanent-call .
	12.0(4)T	This command was integrated into the 12.0(4)T release.
	12.0(7)XK	This command was renamed show voice trunk-conditioning signaling .
	12.1(2)T	This command was integrated into the 12.1(2)T release.
	12.1(3)T	This command was first supported on the Cisco 2600 and 3600 series routers.

Usage Guidelines	The show voice trunk-conditioning signaling command displays the trunk signaling status for analog and digital voice ports on Cisco MC3810 multiservice concentrators and Cisco 2600 and 3600 series routers.

Examples	The following is a sample display from the show voice trunk-conditioning signaling summary command for voice ports on a Cisco MC3810 multiservice concentrator:

```
Router# show voice trunk-conditioning signaling summary
```

```
1/1 is shutdown
1/4 is shutdown
1/5 :
TX INFO :slow-mode seq#= 25, sig pkt cnt= 40, last-ABCD=0000
hardware-state ACTIVE signal type is NorthamericanCAS signal path is OPEN
RX INFO :slow-mode, sig pkt cnt= 36, prev-seq#= 25, last-ABCD=0000
```

The following is a sample display from the **show voice trunk-conditioning signaling** command for voice port 1/5 on a Cisco MC3810 multiservice concentrator:

```
Router# show voice trunk-conditioning signaling 1/5
```

```
1/5 :
```

■ show voice trunk-conditioning signaling

```
TX INFO :slow-mode seq#= 25, sig pkt cnt= 42, last-ABCD=0000
hardware-state ACTIVE signal type is NorthamericanCAS
signal path is OPEN
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
RX INFO :slow-mode, sig pkt cnt= 37
missing = 0, out of seq = 0, very late = 0
playout depth = 0 (ms), refill count = 1
prev-seq#= 25, last-ABCD=0000
trunk_down_timer = 4212 (ms), idle timer = 0 (sec),
tx_oos_timer = 0 (sec), rx_ais_duration = 0 (ms)
forced playout signal pattern = NONE
signaling playout history
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
```

The following is a sample display from the **show voice trunk-conditioning signaling summary** command for voice ports on a Cisco 3600 series router:

```
Router# show voice trunk-conditioning signaling summary
```

```
2/0/0 is shutdown
2/0/1 is shutdown
3/0:0 8 is shutdown
3/0:1 1 is shutdown
3/0:2 2 is shutdown
3/0:3 3 is shutdown
3/0:5 5 is shutdown
3/0:6(6) :
  status :
3/0:7 7 is shutdown
3/1:0 8 is shutdown
3/1:1 1 is shutdown
3/1:3 3 is shutdown
3/1:5 5 is shutdown
3/1:7 7 is shutdown
```

The following is a sample display from the **show voice trunk-conditioning signaling** command for voice port 3/0:6 on a Cisco 3600 series router:

```
Router# show voice trunk-conditioning signaling 3/0:6
```

```
hardware-state ACTIVE signal type is NorthamericanCAS
status :
forced playout pattern = STOPPED
trunk_down_timer = 0, rx_ais_duration = 0, idle_timer = 0
```

Table 66 describes the significant fields shown in the display.

Table 66 *show voice trunk-conditioning signaling Field Descriptions*

Field	Description
current timer	Time since last signaling packets were received.
forced playout pattern	Which forced playout pattern is sent to PBX: 0 = no forced playout pattern is sent 1 = receive IDLE playout pattern is sent 2 = receive OOS playout pattern is sent
hardware-state	Hardware state based on received IDLE pattern: IDLE = both sides are idle ACTIVE = at least one side is active
signal type	Signaling type used by lower level driver: northamerica, melcas, transparent, or external.
idle timer	Time the hardware on both sides has been in idle state.
last-ABCD	Last received or transmitted signal bit pattern.
max inter-arrival time	Maximum interval between received signaling packets.
missing	Number of missed signal packets.
mode	Signaling packet generation frequency: - fast mode = every 4 milliseconds - slow mode = same frequency as keepalive timer
out of seq	Number of out-of-sequence signal packets.
playout depth	Number of packets in playout buffer.
prev-seq#	Sequence number of previous signaling packet.
refill count	Number of packets created to maintain nominal length of playout packet buffer.
rx_ais_duration	Time since receipt of AIS indicator.
seq#	Sequence number of signaling packet.
sig pkt cnt	Number of transmitted or received signaling packets.
signal path	Status of signaling path.
signaling playout history	Signaling bits received in last 60 milliseconds.
trunk_down_timer	Time since last signaling packets were received.
tx_oos_timer	Time since PBX started sending OOS signaling pattern defined by signal pattern oos transmit .
very late	Number of very late signaling packets.

 **show voice trunk-conditioning signaling**

Related Commands	Command	Description
	show dial-peer voice	Displays the configuration for all VoIP and POTS dial peers configured on the router.
	show voice dsp	Shows the current status of all DSP voice channels.
	show voice port	Displays configuration information about a specific voice port.
	show voice trunk-conditioning supervisory	Displays the status of trunk supervision and configuration parameters for voice ports.

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.

Command Modes	User EXEC
	Privileged EXEC

Command History	Release	Modification
	12.0(7)XK	This command was introduced on the Cisco 2600 and 3600 series routers, and the MC3810 multiservice concentrator.
	12.1(2)T	This command was integrated into the 12.1(2)T release.
	12.1(3)T	This command was first supported on the Cisco 2600 and 3600 series routers.

Usage Guidelines	The show voice trunk-conditioning supervisory command displays the trunk supervision and configuration status for analog and digital voice ports.

Examples	The following is a sample display from the show voice trunk-conditioning supervisory summary command for voice ports on a Cisco MC3810 multiservice concentrator:

```
Router# show voice trunk-conditioning supervisory summary

1/1 is shutdown
1/4 is shutdown
1/5 : state : TRUNK_SC_CONNECT, voice : on , signal : on , slave
```

The following is a sample display from the **show voice trunk-conditioning supervisory** command for voice port 1/5 on a Cisco MC3810 multiservice concentrator:

```
Router# show voice trunk-conditioning supervisory 1/5

1/5 : state : TRUNK_SC_CONNECT, voice : on, signal : on, slave
status: trunk connected
sequence oos : idle and oos
pattern :rx_idle = 0x0 rx_oos = 0xF tx_oos = 0xF
timing : idle = 0, restart = 0, standby = 0, timeout = 40
supp_all = 50, supp_voice = 0, keep_alive = 5
timer: oos_ais_timer = 0, timer = 0
```

The following is a sample display from the **show voice trunk-conditioning supervisory summary** command for voice ports on a Cisco 3600 series router:

```
Router# show voice trunk-conditioning supervisory summary

2/0/0 is shutdown
2/0/1 is shutdown
3/0:0 8 is shutdown
3/0:1 1 is shutdown
3/0:2 2 is shutdown
3/0:3 3 is shutdown
3/0:5 5 is shutdown
3/0:6(6) : state : TRUNK_SC_CONNECT, voice : on , signal : on ,master
3/0:7(7) : state : TRUNK_SC_CONNECT, voice : on , signal : on ,master
3/1:0(8) : state : TRUNK_SC_CONNECT, voice : on , signal : on ,master
3/1:1(1) : state : TRUNK_SC_CONNECT, voice : on , signal : on ,master
3/1:3(3) : state : TRUNK_SC_CONNECT, voice : on , signal : on ,master
3/1:5(5) is shutdown
3/1:7(7) is shutdown
```

The following is a sample display from the **show voice trunk-conditioning supervisory** command for voice port 3/0:6 on a Cisco 3600 series router:

```
Router# show voice trunk-conditioning supervisory 3/0:6

3/0:6(6) : state : TRUNK_SC_CONNECT, voice : on, signal : on, master
status: trunk connected
sequence oos : idle and oos
pattern :rx_idle = 0x0 rx_oos = 0xF
timing : idle = 0, restart = 0, standby = 0, timeout = 40
supp_all = 0, supp_voice = 0, keep_alive = 5
timer: oos_ais_timer = 0, timer = 0
```

Table 67 describes the significant fields shown in the display.

Table 67 *show voice trunk-conditioning supervisory Field Descriptions*

Field	Description
keep_alive	Signaling packets periodically sent to the far end, even if there is no signal change. These signaling packets function as keep alive messages.
master	The voice port configured as “connect trunk xxxx.”
slave	The voice port configured as “connect trunk xxxx answer-mode.”
oos_ais_timer	Time since the signaling packet with AIS indicator was received.
pattern	4-bit signaling pattern.
restart	The restart timeout after far end is OOS.
rx-idle	The signaling bit pattern indicating that the far end is idle.
rx-oos	The signaling bit pattern sent to the PBX indicating that the network is OOS.
standby	The time before the slave side goes back to standby after the far end goes OOS.
supp_all	The timeout before suppressing transmission of voice and signaling packets to the far end after detection of PBX OOS.
supp_voice	The timeout before suppressing transmission of voice packet to the far end after detection of PBX oos.
timeout	The timeout for nonreceipt of keepalive packets before the far end is considered to be OOS.
TRUNK_SC_CONNECT	Trunk conditioning supervisory component status.

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all VoIP and POTS dial peers configured on the router.
show voice dsp	Displays the current status of all DSP voice channels.
show voice port	Displays configuration information about a specific voice port.
show voice trunk-conditioning signaling	Displays the status of trunk-conditioning signaling and timing parameters for a 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.
all	Lists all active calls for VFC slots.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5800 universal access server.

Usage Guidelines

Use the **show vrm active_calls** to display active-only voice calls either for a specific VFC or for all VFCs. Each active call occupies a block of information describing the call. This information provides basically the same information as the **show vrm vdevice** command.

Examples

The following is sample output from the **show vrm active_calls** command specifying dial shelf slot number:

```
Router# show vrm active_calls 6

slot = 6 virtual voice dev (tag) = 61 channel id = 2
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 241
Resource (vdev_common) status = 401 means :active others
tot ingress data = 24
tot ingress control = 1308
tot ingress data drops = 0
tot ingress control drops = 0
tot egress data = 22051
tot egress control = 1304
tot egress data drops = 0
tot egress control drops = 0

slot = 6 virtual voice dev (tag) = 40 channel id = 2
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 157
Resource (vdev_common) status = 401 means :active others
```


Table 68 describes the significant fields shown in the display.

Table 68 *show vrm active_calls Field Descriptions*

Field	Description
slot	Slot where voice card is installed.
virtual voice dev (tag)	Identification number of the virtual voice device.
channel id	Identification number of the channel associated with this virtual voice device.
capability list map	Bitmaps for the codec supported on that DSP channel. Available values are: CC_CAP_CODEC_G711U: 0x1 CC_CAP_CODEC_G711A: 0x2 CC_CAP_CODEC_G729IETF: 0x4 CC_CAP_CODEC_G729a: 0x8 CC_CAP_CODEC_G726r16: 0x10 CC_CAP_CODEC_G726r24: 0x20 CC_CAP_CODEC_G726r32: 0x40 CC_CAP_CODEC_G728: 0x80 CC_CAP_CODEC_G723r63: 0x100 CC_CAP_CODEC_G723r53: 0x200 CC_CAP_CODEC_GSM: 0x400 CC_CAP_CODEC_G729b: 0x800 CC_CAP_CODEC_G729ab: 0x1000 CC_CAP_CODEC_G723ar63: 0x2000 CC_CAP_CODEC_G723ar53: 0x4000 CC_CAP_CODEC_G729: 0x8000
last/current codec loaded/used	Indicates the last codec loaded or used.
TDM time slot	Time division multiplexing time slot.
Resource (vdev_common) status	Current status of the VFC.
tot ingress data	Total amount of data (number of packets) sent from the PSTN side of the connection to the VoIP side of the connection.
tot ingress control	Total number of control packets sent from the PSTN side of the connection to the Voice over IP (VoIP) side of the connection.
tot ingress data drops	Total number of data packets dropped from the PSTN side of the connection to the VoIP side of the connection.
tot ingress control drops	Total number of control packets dropped from the PSTN side of the connection to the VoIP side of the connection.
tot egress data	Total amount of data (number of packets) sent from the VoIP side of the connection to the PSTN side of the connection.

 `show vrm active_calls`**Table 68** *show vrm active_calls Field Descriptions (continued)*

Field	Description
tot egress control	Total number of control packets sent from the VoIP side of the connection to the PSTN side of the connection.
tot egress data drops	Total number of data packets dropped from the VoIP side of the connection to the PSTN side of the connection.
tot egress control drops	Total number of control packets dropped from the VoIP side of the connection to the PSTN side of the connection.

Related Commands

Command	Description
<code>show vrm vdevices</code>	Displays detailed information for a specific DSP or a brief summary display for all VFCs.

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.
	summary	List synopsis of voice feature card DSP mappings, capabilities, and resource states.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(7)T	This command was introduced on the Cisco AS5800 universal access server.

Usage Guidelines	Use the show vrm vdevices command to display detailed information for a specific DSP or a brief summary display for all VFCs. The display provides information on the number of channels, channels per DSP, bitmap of DSPMs, version numbers, and so on. This information is useful in monitoring the current state of your VFCs.

The display for a specific DSP provides information on the codec that each channel is using, if active, or last used and if the channel is not currently sending cells. It also displays the state of the resource. In most cases, if there is an active call on that channel, the resource should be marked active. If the resource is marked as reset or bad, this may be an indication of a response loss for the VFC on a reset request. If this condition persists, you might experience a problem with the communication link between the router shelf and the VFC.

Examples	The following is sample output from the show vrm vdevices command specifying dial shelf slot number and DSP number. In this particular example, the call is active so the statistics displayed are for this active call. If no calls are currently active on the device, the statistics would be for the previous (or last active) call.

```
Router# show vrm vdevices 6 1
```

```
slot = 6 virtual voice dev (tag) = 1 channel id = 1
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 0
Resource (vdev_common) status = 401 means :active others
tot ingress data = 101
```

show vrm vdevices

```

tot ingress control  = 1194
tot ingress data drops  = 0
tot ingress control drops  = 0
tot egress data  = 39722
tot egress control  = 1209
tot egress data drops  = 0
tot egress control drops  = 0

slot = 6 virtual voice dev (tag) = 1 channel id = 2
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 1
Resource (vdev_common) status = 401 means :active others
tot ingress data = 21
tot ingress control  = 1167
tot ingress data drops  = 0
tot ingress control drops  = 0
tot egress data  = 19476
tot egress control  = 1163
tot egress data drops  = 0
tot egress control drops  = 0

```

[Table 69](#) describes the significant fields shown in the display.

Table 69 *show vrm vdevices Field Descriptions*

Field	Description
slot	Slot where voice card is installed.
virtual voice dev (tag)	Identification number of the virtual voice device.
channel id	Identification number of the channel associated with this virtual voice device.

Table 69 *show vrm vdevices Field Descriptions (continued)*

Field	Description
capability list map	Bitmaps for the codec supported on that DSP channel. Available values are: • CC_CAP_CODEC_G711U: 0x1 • CC_CAP_CODEC_G711A: 0x2 • CC_CAP_CODEC_G729IETF: 0x4 • CC_CAP_CODEC_G729a: 0x8 • CC_CAP_CODEC_G726r16: 0x10 • CC_CAP_CODEC_G726r24: 0x20 • CC_CAP_CODEC_G726r32: 0x40 • CC_CAP_CODEC_G728: 0x80 • CC_CAP_CODEC_G723r63: 0x100 • CC_CAP_CODEC_G723r53: 0x200 • CC_CAP_CODEC_GSM: 0x400 • CC_CAP_CODEC_G729b: 0x800 • CC_CAP_CODEC_G729ab: 0x1000 • CC_CAP_CODEC_G723ar63: 0x2000 • CC_CAP_CODEC_G723ar53: 0x4000 • CC_CAP_CODEC_G729: 0x8000
last/current codec loaded/used	The last codec loaded or used.
TDM time slot	Time division multiplexing time slot.

Table 69 *show vrm vdevices Field Descriptions (continued)*

Field	Description
Resource (vdev_common) status	Current status of the VFC. Possible field values are: • FREE = 0x0000 • ACTIVE_CALL = 0x0001 • BUSYOUT_REQ = 0x0002 • BAD = 0x0004 • BACK2BACK_TEST = 0x0008 • RESET = 0x0010 • DOWNLOAD_FILE = 0x0020 • DOWNLOAD_FAIL = 0x0040 • SHUTDOWN = 0x0080 • BUSY = 0x0100 • OIR = 0x0200 • HASLOCK = 0x0400 /* vdev_pool has locked port */ • DOWNLOAD_REQ = 0x0800 • RECOVERY_REQ = 0x1000 • NEGOTIATED = 0x2000 • OOS = 0x4000
tot ingress data	Total amount of data (number of packets) sent from the PSTN side of the connection to the Voice over IP (VoIP) side of the connection.
tot ingress control	Total number of control packets sent from the PSTN side of the connection to the VoIP side of the connection.
tot ingress data drops	Total number of data packets dropped from the PSTN side of the connection to the VoIP side of the connection.
tot ingress control drops	Total number of control packets dropped from the PSTN side of the connection to the VoIP side of the connection.
tot egress data	Total amount of data (number of packets) sent from the VoIP side of the connection to the PSTN side of the connection.
tot egress control	Total number of control packets sent from the VoIP side of the connection to the PSTN side of the connection.
tot egress data drops	Total number of data packets dropped from the VoIP side of the connection to the PSTN side of the connection.
tot egress control drops	Total number of control packets dropped from the VoIP side of the connection to the PSTN side of the connection.

The following is sample output from the **show vrm devices** command specifying a summary list. In the “Voice Device Mapping” area, the “C_Ac” column indicates number of active calls for a specific DSP. If there are any nonzero numbers under the “C_Rst” and/or “C_Bad” column, this indicates that a reset request was sent but it was lost; this could mean a faulty DSP.

```
Router# show vrm vdevices summary
```

```

*****
*****summary of voice devices for all voice cards*****
*****

slot = 6 major ver = 0 minor ver = 1 core type used = 2
number of modules = 16 number of voice devices (DSPs) = 96
chans per vdevice = 2 tot chans = 192 tot active calls = 178
module presense bit map = FFFF tdm mode = 1 num_of_tdm_timeslots = 384
auto recovery is on

number of default voice file (core type images) = 2
file 0 maj ver = 0 min ver = 0 core_type = 1
trough size = 2880 slop value = 0 built-in codec bitmap = 0
loadable codec bitmap = 0 fax codec bitmap = 0

file 1 maj ver = 3 min ver = 1 core_type = 2
trough size = 2880 slop value = 1440 built-in codec bitmap = 40B
loadable codec bitmap = BFC fax codec bitmap = 7E

-----Voice Device Mapping-----
Logical Device (Tag)  Module#  DSP#  C_Ac  C_Busy  C_Rst  C_Bad
-----
1                    1        1    2      0       0      0
2                    1        2    2      0       0      0
3                    1        3    2      0       0      0
4                    1        4    2      0       0      0
5                    1        5    2      0       0      0
6                    1        6    2      0       0      0
+++++
7                    2        1    2      0       0      0
8                    2        2    2      0       0      0
9                    2        3    2      0       0      0
10                   2        4    1      0       0      0
11                   2        5    2      0       0      0
12                   2        6    1      0       0      0
+++++
<information deleted>
+++++
91                   16        1    2      0       0      0
92                   16        2    2      0       0      0
93                   16        3    1      0       0      0
94                   16        4    2      0       0      0
95                   16        5    2      0       0      0
96                   16        6    2      0       0      0
+++++

Total active call channels = 178
Total busied out channels = 0
Total channels in reset = 0
Total bad channels = 0
Note :Channels could be in multiple states

```

[Table 70](#) describes the significant fields shown in the display.

Table 70 *show vrm vdevices summary Field Descriptions*

Field	Description
slot	Slot number where VFC is installed.
major ver	Major version of firmware running on VFC.
minor ver	Minor version of firmware running on VFC.

Table 70 *show vrm vdevices summary Field Descriptions (continued)*

Field	Description
core type used	Type of DSPware in use. Possible field values are: • 1 = UBL (boot loader) • 2 = high complexity core • 3 = medium complexity core • 4 = low complexity core • 255 = invalid
number of modules	Number of modules on the VFC. Maximum is 16.
number of voice devices (DSP)s	Number of possible DSPs. Maximum number is 96.
chans per vdevice	Number of channels (meaning calls) each DSP can handle.
tot chans	Total number of channels.
tot active calls	Total number of active calls on this VFC.
module presense bit map	Indicates a 16-bit bitmap, each bit representing a module.
tdm mode	Time division multiplex bus mode. Possible field values are: • 0 = VFC is in classic mode. • 1 = VFC is in plus mode. This field should always be 1.
num_of_tdm_time slots	Total number of calls that can be handled by the VFC.
auto recovery	Indicates whether auto recovery is enabled. When autorecovery is enabled, the VRM will try to recover a DSP by resetting it if, for some reason, the DSP stops responding.
number of default voice file (core type images)	Number of DSPware files in use.
maj ver	Major version of the DSPware in use.
min ver	Minor version of the DSPware in use.
core type	Type of DSPware in use: Possible field values are: • 1 = boot loader • 2 = high complexity core • 3 = medium complexity core • 4 = low complexity core
trough size	This value indirectly represents the complexity of the DSPware in use.
slop value	This value indirectly represents the complexity of the DSPware in use.

Table 70 *show vrm vdevices summary Field Descriptions (continued)*

Field	Description
built-in codec bitmap	Represents the bitmap of the codec built into the DSP firmware. Possible field values are: • CC_CAP_CODEC_G711U 0x0001 • CC_CAP_CODEC_G711A 0x0002 • CC_CAP_CODEC_G729IETF 0x0004 • CC_CAP_CODEC_G729a 0x0008 • CC_CAP_CODEC_G726r16 0x0010 • CC_CAP_CODEC_G726r24 0x0020 • CC_CAP_CODEC_G726r32 0x0040 • CC_CAP_CODEC_G728 0x0080 • CC_CAP_CODEC_G723r63 0x0100 • CC_CAP_CODEC_G723r53 0x0200 • CC_CAP_CODEC_GSM 0x0400 • CC_CAP_CODEC_G729b 0x0800 • CC_CAP_CODEC_G729ab 0x1000 • CC_CAP_CODEC_G723ar63 0x2000 • CC_CAP_CODEC_G723ar53 0x4000 • CC_CAP_CODEC_G729 0x8000
loadable codec bitmap	Represents the loadable codec bitmap for the loadable codecs. Possible field values are: • CC_CAP_CODEC_G711U = 0x0001 • CC_CAP_CODEC_G711A = 0x0002 • CC_CAP_CODEC_G729IETF = 0x0004 • CC_CAP_CODEC_G729a = 0x0008 • CC_CAP_CODEC_G726r16 = 0x0010 • CC_CAP_CODEC_G726r24 = 0x0020 • CC_CAP_CODEC_G726r32 = 0x0040 • CC_CAP_CODEC_G728 = 0x0080 • CC_CAP_CODEC_G723r63 = 0x0100 • CC_CAP_CODEC_G723r53 = 0x0200 • CC_CAP_CODEC_GSM = 0x0400 • CC_CAP_CODEC_G729b = 0x0800 • CC_CAP_CODEC_G729ab = 0x1000 • CC_CAP_CODEC_G723ar63 = 0x2000 • CC_CAP_CODEC_G723ar53 = 0x4000 • CC_CAP_CODEC_G729 = 0x8000

Table 70 *show vrm vdevices summary Field Descriptions (continued)*

Field	Description
fax codec bitmap	Represents the fax codec bitmap. Possible field values are: • FAX_NONE = 0x1 • FAX_VOICE = 0x2 • FAX_144 = 0x4 • FAX_96 = 0x8 • FAX_72 = 0x10 • FAX_48 = 0x20 • FAX_24 = 0x40
Logical Device (Tag)	Tag number or DSP number on that VFC.
Module #	Number identifying the module associated with a specific logical device.
DSP#	Number identifying the DSP on the VFC.
C_Ac	Number of active calls on identified DSP.
C_Busy	Number of busied-out channels associated with identified DSP.
C_Rst	Number of channels in the reset state associated with identified DSP.
C_Bad	Number of defective (“bad”) channels associated with identified DSP.
Total active call channels	Total number of active calls.
Total busied out channels	Total number of busied-out channels.
Total channels in reset	Total number of channels in reset state.
Total bad channels	Total number of defective channels.

Related Commands

Command	Description
show vrm active_calls	Displays active-only voice calls for either a specific VFC or all VFCs.

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.

Defaults	no shut

Command Modes	DSP configuration

Command History	Release	Modification
	12.0(5)XE	This command was introduced on the Cisco 7200 series router.
	12.1(1)T	This command was modified to add information about DSP groups.

Usage Guidelines	This command applies to Voice over IP on the Cisco 7200 series routers.

Examples	The following example shuts down two sets of DSPs: shut 2

shutdown (dial-peer)

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.

Defaults **no shutdown**

Command Modes Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series router.
12.1(1)	This command was modified for store-and-forward fax.

Usage Guidelines

When a dial peer is shut down, you cannot initiate calls to that peer.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following example changes the administrative state of voice telephony (plain old telephone service [POTS]) dial peer 10 to down:

```
dial-peer voice 10 pots
shutdown
```

The following example changes the administrative state of voice telephony (POTS) dial peer 10 to up:

```
dial-peer voice 10 pots
no shutdown
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode, defines the type of dial peer, and defines the dial-peer tag number.

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.

Defaults	no shutdown

Command Modes	Controller configuration

Command History	Release	Modification
	11.3(1)MA	This command was introduced.

Usage Guidelines	This command applies to Voice over Frame Relay and Voice over ATM on the Cisco MC3810 multiservice concentrator.

Examples	The following example shuts down a DS1 link on controller T1 0:

```
controller T1 0
shutdown
```

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.

Defaults Disabled (shut down)

Command Modes gatekeeper configuration

Command History	Release	Modification
	11.3(2)NA	This command was introduced on the Cisco 2500 series and Cisco 3600 series routers.
	12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and supported on the Cisco MC3810 multiservice concentrator.

Usage Guidelines The gatekeeper does not have to be enabled before you can use the other gatekeeper configuration commands. In fact, it is recommended that you complete the gatekeeper configuration before bringing up the gatekeeper because some characteristics may be difficult to alter while the gatekeeper is running, as there may be active registrations or calls.

The **no shutdown** command enables the gatekeeper, but it does not make the gatekeeper operational. The two exceptions to this are as follows:

- If no local zones are configured, a **no shutdown** command places the gatekeeper in INACTIVE mode waiting for a local zone definition.
- If local zones are defined to use an HSRP virtual address, and the HSRP interface is in STANDBY mode, the gatekeeper goes into HSRP STANDBY mode. Only when the HSRP interface is ACTIVE will the gatekeeper go into the operational UP mode.

Examples The following command disables a gatekeeper:

```
shutdown
```

shutdown (RLM)

To shut down all of the links under the RLM group, use the **shutdown** command in RLM configuration mode. RLM will not try to reestablish those links until the command is negated. To disable this function, use the **no** form of this command.

shutdown

no shutdown

Syntax Description	This command has no arguments or keywords.

Defaults	Disabled

Command Modes	RLM configuration

Command History	Release	Modification
	11.3(7)	This command was introduced.

Related Commands	Command	Description
	clear rlm group	Clears all RLM group time stamps to zero.
	clear interface	Resets the hardware logic on an interface.
	interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
	link (RLM)	Specifies the link preference.
	protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
	retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
	server (RLM)	Defines the IP addresses of the server.
	show rlm group statistics	Displays the network latency of the RLM group.
	show rlm group status	Displays the status of the RLM group.
	show rlm group timer	Displays the current RLM group timer values.
	timer	Overwrites the default setting of timeout values.

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.

Defaults

The default status of a settlement provider is deactivated. The settlement provider is down.

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced the Cisco 2500 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Use the **no shutdown** command at the end of the configuration of a settlement server to bring up the provider. This command activates the provider. Otherwise, transactions will not go through the provider to be audited and charged. Use the **shutdown** command to deactivate the provider.

Examples

The following example enables a settlement server:

```
settlement 0
no shutdown
```

The following example disables a settlement server:

```
settlement 0
shutdown
```

Related Commands

Command	Description
connection-timeout	Configures the time that a connection is maintained after completing a communication exchange.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.

Command	Description
response-timeout	Configures the maximum time to wait for a response from a server.
retry-delay	Sets the time between attempts to connect with the settlement provider.
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.
type	Configures an SAA-RTR operation type.

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.

Defaults

shutdown

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series router.

Usage Guidelines

When you enter the **shutdown** command, all ports on the voice interface card are disabled. When you enter the **no shutdown** command, all ports on the voice interface card are enabled. A telephone connected to an interface will hear dead silence when a port is shut down.

Examples

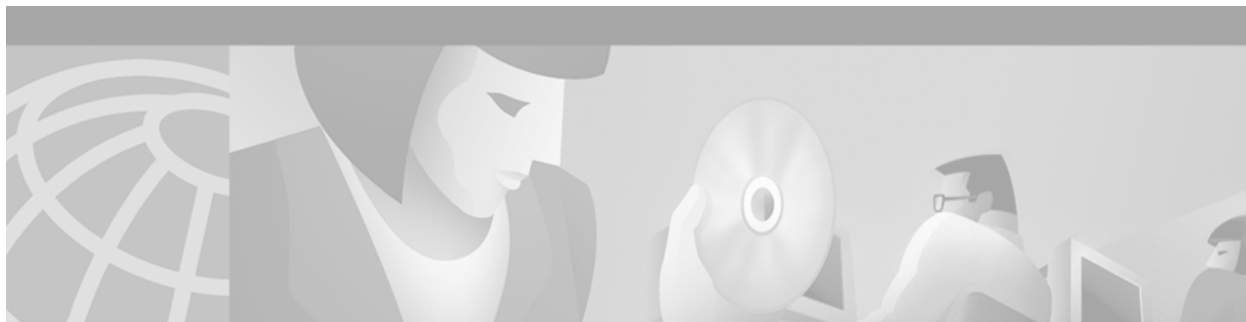
The following example takes voice port 1/1/0 on the Cisco 3600 series offline:

```
voice-port 1/1/0
shutdown
```



Note

The preceding configuration example shuts down both voice ports 1/1/0 and 1/1/1.



Cisco IOS Voice, Video, and Fax Commands: Si Through Z

This chapter presents the commands to configure and maintain Cisco IOS voice, video, and fax applications. The commands are presented in alphabetical order beginning with Si. Some commands required for configuring voice, video, and fax may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice, Video, and Fax Configuration Guide*.

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		
loop-start		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.
ground-start		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.
wink-start		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 dual tone multifrequency (DTMF) digits. Used for E&M tie trunk interfaces. This is the default setting for E&M voice ports.
immediate		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.
delay-dial		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.

Defaults	Loop-start for FXO and FXS interfaces; wink-start for E&M interfaces.

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 series routers.

Usage Guidelines

This command applies to analog voice ports only.

Configuring the **signal** command for an FXO or FXS voice port changes the signal value for both voice ports on a voice port module (VPM) card.

**Note**

If you change the signal type for an FXO voice port on Cisco 3600 series routers, you need to move the appropriate jumper in the voice interface card of the voice network module. For more information about the physical characteristics of the voice network module, refer to the installation documentation, *Voice Network Module and Voice Interface Card Configuration Note*, that came with your voice network module.

Configuring this command for an E&M voice port changes only the signal value for the selected voice port. In either case, the voice port must be shut down and then activated before the configured values will take effect.

Some PBXs will miss initial digits if the E&M voice port is configured for Immediate signaling. If this occurs, use Delay-Dial signaling instead. Some non-Cisco devices have a limited number of DTMF receivers. This type of equipment must delay the calling side until a DTMF receiver is available.

Examples

The following example configures ground start signaling on the Cisco 3600 series as the signaling type for a voice port, which means that both sides of a connection can place a call and hang up:

```
voice-port 1/1/1
 signal ground-start
```

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*

Syntax Description	<i>number</i>	Specifies the keepalive signaling packet interval, in seconds. The valid range is from 1 to 65,535.

Defaults	A keepalive packet is sent every 5 seconds.

Command Modes	Voice-class configuration

Command History	Release	Modification
	12.0(3)XG	This command was introduced on the Cisco MC3810 multiservice concentrator.
	12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
	12.1(3)T	This command was first supported on the Cisco 2600 and 3600 series routers.

Usage Guidelines	Before configuring the keepalive signaling interval, you must use the voice class permanent command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. The voice class must then be assigned to a dial peer.

Examples	The following example, beginning in global configuration mode, sets the keepalive signaling interval to 3 seconds for voice class 10. <pre>voice class permanent 10 signal keepalive 3 exit dial-peer voice 100 vofr voice-class permanent 10</pre>

Related Commands	Command	Description
	dial-peer voice	Enters dial-peer configuration mode and specifies a dial-peer type.
	signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.
	signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
	signal timing oos	Configures the signal timing parameter for the OOS state of a call.
	voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
	voice class permanent	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

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*

Syntax Description		
idle receive		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 signal sequence oos idle-only or signal sequence oos both command is configured.
idle transmit		Defines the signaling pattern for identifying an idle message from the PBX.
oos receive		Defines the OOS signaling pattern to be sent to the PBX if the network trunk is out of service and the signal sequence oos oos-only or signal sequence oos both command is configured.
oos transmit		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.

Defaults		
idle receive		For near-end E&M—0000 (for T1) or 0001 (for E1) For near-end FXO loop start—0101 For near-end FXO ground start—1111 For near-end FXS—0101 For near-end MELCAS—1101
idle transmit		For near-end E&M—0000 For near-end FXO—0101 For near-end FXS loop start—0101 For near-end FXS ground start—1111 For near-end MELCAS—1101
oos receive		For near-end E&M—1111 For near-end FXO loop start—1111 For near-end FXO ground start—0000 For near-end FXS loop start—1111 For near-end FXS ground start—0101 For near-end MELCAS—1111
oos transmit		No default signaling pattern is defined.

Command Modes	Voice-class configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(7)XK	Default signaling patterns were defined.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was first supported on the Cisco 2600 and 3600 series routers.

Usage Guidelines

Before configuring the signaling pattern, you must use the **voice-class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you define the voice class, you assign it to a dial peer.

Idle Patterns

An idle state is generated if the router detects an idle signaling pattern coming from either direction. If an idle pattern is configured for only one direction (transmit or receive), an idle state can be detected only in the configured direction. Therefore, you should normally enter both the **idle receive** and the **idle transmit** keywords.

To suppress voice packets whenever the transmit or receive trunk is in the idle state, use the **idle receive** and **idle transmit** keywords in conjunction with the **signal timing idle suppress-voice** command.

OOS Patterns

An OOS state is generated differently in each direction under the following conditions:

- If the router detects an **oos transmit** signaling pattern sent from the PBX, the router transmits the **oos transmit** signaling pattern to the network.
- If the **signal timing oos timeout** timer expires and the router receives no signaling packets from the network (network is OOS), the router sends an **oos receive** signaling pattern to the PBX. (The **oos receive** pattern is not matched against the signaling packets received from the network; the receive packets indicate an OOS condition directly by setting the AIS alarm indication bit in the packet.)

To suppress voice packets whenever the transmit or receive trunk is in the OOS state, use the **oos receive** and **oos transmit** keywords in conjunction with the **signal timing oos suppress-voice** command.

To suppress voice and signaling packets whenever the transmit or receive trunk is in the OOS state, use the **oos receive** and **oos transmit** keywords in conjunction with the **signal timing oos suppress-all** command.

PBX Busyout

To “busy out” a PBX if the network connection fails, set the **oos receive** pattern to match the seized state (busy), and set the **signal timing oos** timeout value. When the timeout value expires and no signaling packets have been received, the router will send the **oos receive** pattern to the PBX.

Use the busy seized pattern only if the PBX does not have a specified pattern for indicating an OOS state. If the PBX has a specific OOS pattern, use that pattern instead.

Examples

The following example, beginning in global configuration mode, configures the signaling bit pattern for the idle receive and transmit states:

```
voice class permanent 10
  signal keepalive 3
  signal pattern idle receive 0101
  signal pattern idle transmit 0101
exit
dial-peer voice 100 vofr
  voice-class permanent 10
```

The following example, beginning in global configuration mode, configures the signaling bit pattern for the out-of-service receive and transmit states:

```
voice class permanent 10
  signal keepalive 3
  signal pattern oos receive 0001
  signal pattern oos transmit 0001
exit
dial-peer voice 100 vofr
  voice-class permanent 10
```

The following example restores default signaling bit patterns for the receive and transmit idle states:

```
voice class permanent 10
  signal keepalive 3
  signal timing idle suppress-voice
  no signal pattern idle receive
  no signal pattern idle transmit
exit
dial-peer voice 100 vofr
  voice-class permanent 10
```

The following example configures non-default signaling bit patterns for the receive and transmit out-of-service states:

```
voice class permanent 10
  signal keepalive 3
  signal pattern oos receive 0001
  signal pattern oos transmit 0001
exit
dial-peer voice 100 vofr
  voice-class permanent 10
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies a dial-peer type.
signal timing idle suppress-voice	Specifies the length of time before voice traffic is stopped after a trunk goes into the idle state.
signal timing oos	Configures the signal timing parameter for the OOS call state.
signal timing oos slave-standby	Specifies that a slave port return to its initial standby state after the trunk has been OOS for a specified time.
signal timing oos suppress-all	Stops sending voice and signaling packets to the network if a transmit OOS signaling pattern id detected from the PBX for a specified time.
signal timing oos suppress-voice	Stops sending voice packets to the network if a transmit OOS signaling pattern is detected from the PBX for a specified time.

Command	Description
signal timing oos timeout	Changes the delay time between the loss of signaling packets from the network and the start time for the OOS state.
voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice class permanent	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal sequence oos

To specify which signaling pattern is sent to the PBX when the far-end keepalive message is lost or an alarm indication signal (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

no-action	No signaling pattern is sent.
idle-only	Only the idle signaling pattern is sent.
oos-only	Only the out-of-service (OOS) signaling pattern is sent.
both	Both idle and OOS signaling patterns are sent. This is the default value.

Defaults

Both idle and OOS signaling patterns are sent.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 multiservice concentrators.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was first supported on the Cisco 2600 and 3600 series routers.

Usage Guidelines

Before configuring the idle or OOS signaling patterns to be sent, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

Use the **signal sequence oos** command to specify which signaling pattern) to send. Use the **signal pattern idle receive** or the **signal pattern oos receive** command to define the bit patterns of the signaling patterns if other than the defaults.

Examples

The following example, beginning in global configuration mode, defines voice class 10, sets the **signal sequence oos** command to send only the idle signalin pattern to the PBX, and applies the voice class configuration to VoFR dial peer 100.

```
voice-class permanent 10
  signal-keepalive 3
  signal sequence oos idle-only
  signal timing idle suppress-voice
  exit
dial-peer voice 100 vofr
  voice-class permanent 10
  signal-type transparent
```

Related Commands	Command	Description
	dial-peer voice	Enters dial-peer configuration mode and specifies a dial-peer type.
	signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.
	signal timing idle suppress-voice	Specifies the length of time before the router stops sending voice packets after a trunk goes into the idle state.
	signal timing oos	Specifies that a permanent voice connection be torn down and restarted after the trunk has been OOS for a specified time.
	signal timing oos slave-standby	Specifies that a slave port return to its initial standby state after the trunk has been OOS for a specified time.
	signal timing oos suppress-all	Configures the router or concentrator to stop sending voice and signaling packets to the network if it detects an OOS signaling pattern from the PBX for a specified time.
	signal timing oos suppress-voice	Configures the router or concentrator to stop sending voice packets to the network if it detects a transmit OOS signaling pattern from the PBX for a specified time.
	signal timing oos timeout	Changes the delay time between the loss of signaling packets from the network and the start time for the OOS state.
	voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
	voice class permanent	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

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.

Defaults	No signal timing idle suppress-voice timer is configured.

Command Modes	Voice-class configuration

Command History	Release	Modification
	12.0(3)XG	This command was introduced on the Cisco MC3810 multiservice concentrator.
	12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
	12.0(7)XK	This command was modified to simplify the configuration process.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
	12.1(3)T	This command was first supported on the Cisco 2600 and 3600 series routers.

Usage Guidelines	Before configuring the signal timing idle suppress-voice timer, you must use the voice class permanent command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. The voice class must then be assigned to a dial peer.

The **signal timing idle suppress-voice** command is used when the **signal-type** command is set to **transparent** in the dial peer for the Cisco trunk or FRF.11 trunk connection. The router stops sending voice packets when the timer expires. Signaling packets are still sent.

To detect an idle trunk state, the router or concentrator monitors both transmit and receive signaling for the **idle transmit** and **idle receive** signaling patterns. These can be configured by the **signal pattern idle transmit** or **signal pattern idle receive** command, or they can be the defaults. The default **idle receive** pattern is the idle pattern of the local voice port. The default **idle transmit** pattern is the idle pattern of the far-end voice port.

Examples

The following example, beginning in global configuration mode, sets the signal timing idle suppress-voice timer to 5 seconds for the idle state on voice class 10.

```
voice class permanent 10
  signal keepalive 3
  signal pattern idle receive 0101
  signal pattern idle transmit 0101
  signal timing idle suppress-voice 5
exit
dial-peer voice 100 vofr
voice-class permanent 10
signal-type transparent
```

The following example defines voice class 10, sets the idle detection time to 5 seconds, configures the trunk to use the default transmit and receive idle signal patterns, and applies the voice class configuration to VoFR dial peer 100.

```
voice class permanent 10
  signal keepalive 3
  signal timing idle suppress-voice 5
exit
dial-peer voice 100 vofr
voice-class permanent 10
signal-type transparent
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing oos	Configures the signal timing parameter for the OOS state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice class permanent (dial peer)	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

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		
restart		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.
slave-standby		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 connection trunk number answer-mode command).
suppress-all		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.
suppress-voice		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).
timeout		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.

Defaults No signal timing OOS pattern parameters are configured.

Command Modes Voice-class configuration

Command History	Release	Modification
	12.0(4)T	This command was introduced.

Usage Guidelines Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. The voice class must then be assigned to a dial peer.

You can enter several values for this command. However, the **suppress-all** and **suppress-voice** options are mutually exclusive.

Examples

The following example, beginning in global configuration mode, configures the signal timeout parameter for the OOS state on voice class 10. The **signal timing oos timeout** command is set to 60 seconds.

```
voice-class permanent 10
  signal-keepalive 3
  signal pattern oos receive 0001
  signal pattern oos transmit 0001
  signal timing oos timeout 60
exit
dial-peer voice 100 vofr
  voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of the call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

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

Syntax Description	<i>seconds</i>	Delay duration, in seconds, for the restart attempt. There is no default duration. The range is from 0 to 65,535.

Defaults	No restart attempt is made if the trunk becomes OOS.

Command Modes	Voice-class configuration

Command History	Release	Modification
	12.0(3)XG	This command was introduced on the Cisco MC3810 series.
	12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
	12.1(3)T	This command was first supported on the Cisco 2600 and 3600 series routers.

Usage Guidelines	Before configuring signal timing OOS parameters, you must use the voice class permanent command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. You then assign the voice class to a dial peer.

The **signal timing oos restart** command is valid only if the **signal timing oos timeout** command is enabled, which controls the start time for the OOS state. The timer for the **signal timing oos restart** command does not start until the trunk is OOS.

Examples	The following example, beginning in global configuration mode, creates voice class 10, sets the OOS timeout time to 60 seconds and sets the restart time to 30 seconds:

```
voice-class permanent 10
  signal-keepalive 3
  signal pattern oos receive 0001
  signal pattern oos transmit 0001
  signal timing oos timeout 60
  signal timing oos restart 30
exit
dial-peer voice 100 vofr
  voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

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

Syntax Description	<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.

Defaults	The slave port does not return to its standby state if the trunk becomes OOS.

Command Modes	Voice-class configuration

Command History	Release	Modification
	12.0(3)XG	This command was introduced on the Cisco MC3810 series.
	12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
	12.1(3)T	This command was first supported on the Cisco 2600 and 3600 series routers.

Usage Guidelines	Before configuring signal timing OOS parameters, you must use the voice class permanent command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

If no signaling packets are received for the specified delay period, the slave port returns to its initial standby state. The **signal timing oos slave-standby** command is valid only if both of the following conditions are true:

- The **signal timing oos timeout** command is enabled, which controls the start time for the OOS state. The timer for the **signal timing oos slave-standby** command does not start until the trunk is OOS.
- The voice port is configured as a slave port with the **connection trunk digits answer-mode** command.

Examples

The following example, beginning in global configuration mode, creates a voice port as a slave voice port, creates voice class 10, sets the OOS timeout time to 60 seconds, and sets the return-to-slave-standby time to 120 seconds:

```
voice-port 1/0/0
connection trunk 5559262 answer-mode
exit
voice-class permanent 10
signal-keepalive 3
signal pattern oos receive 0001
signal pattern oos transmit 0001
signal timing oos timeout 60
signal timing oos slave-standby 120
exit
dial-peer voice 100 vofr
voice-class permanent 10
```

Command History

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

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

Syntax Description	<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.	
Defaults	The router or concentrator does not stop sending packets to the network if it detects a transmit OOS signaling pattern from the PBX.	
Command Modes	Voice-class configuration	
Command History	Release	Modification
	12.0(3)XG	This command was introduced on the Cisco MC3810 series.
	12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
	12.1(3)T	This command was first supported on the Cisco 2600 and 3600 series routers.
Usage Guidelines	Before configuring signal timing OOS parameters, you must use the voice class permanent command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer. The signal timing oos suppress-all command is valid only if you configure an OOS transmit signaling pattern with the signal pattern oos transmit command. (There is no default oos transmit signaling pattern.) The signal timing oos suppress-all command is valid whether or not the signal timing oos timeout command is enabled, which controls the start time for the OOS state. The timer for the signal timing oos suppress-all command starts immediately when the OOS transmit signaling pattern is matched.	

Examples

The following example, beginning in global configuration mode, creates voice class 10, sets the OOS **timeout** time to 60 seconds, and sets the packet suppression time to 60 seconds:

```
voice-class permanent 10
  signal-keepalive 3
  signal pattern oos receive 0001
  signal pattern oos transmit 0001
  signal timing oos timeout 60
  signal timing oos suppress-all 60
exit
dial-peer voice 100 vofr
  voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

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

Syntax Description	<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.	
Defaults	The router or concentrator does not stop sending voice packets to the network if it detects a transmit OOS signaling pattern from the PBX.	
Command Modes	Voice-class configuration	
Command History	Release	Modification
	12.0(3)XG	This command was introduced on the Cisco MC3810 series.
	12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
	12.1(3)T	This command was first supported on the Cisco 2600 and 3600 series routers.
Usage Guidelines	Before configuring signal timing OOS parameters, you must use the voice class permanent command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer. The signal timing oos suppress-voice command is valid only if you configure an OOS transmit signaling pattern with the signal pattern oos transmit command. (There is no default oos transmit signaling pattern.) The signal timing oos suppress-voice s command is valid whether or not the signal timing oos timeout command is enabled, which controls the start time for the OOS state. The timer for the signal timing oos suppress-voice command starts immediately when the OOS transmit signaling pattern is matched.	

Examples

The following example, beginning in global configuration mode, creates voice class 10, sets the OOS timeout time to 60 seconds, and sets the packet suppression time to 60 seconds:

```
voice-class permanent 10
  signal-keepalive 3
  signal pattern oos receive 0001
  signal pattern oos transmit 0001
  signal timing oos timeout 60
  signal timing oos suppress-voice 60
exit
dial-peer voice 100 vofr
  voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

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

Syntax Description	<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.
	disabled	(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.

Defaults No signal timing OOS pattern parameters are configured.

Command Modes Voice-class configuration

Command History	Release	Modification
	12.0(3)XG	This command was introduced on the Cisco MC3810 series.
	12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
	12.1(3)T	This command was first supported on the Cisco 2600 and 3600 series routers.

Usage Guidelines Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

You can use the **signal timing oos timeout** command to enable busyout to the PBX.

The **signal timing oos timeout** command controls the starting time for the **signal timing oos restart** and **signal timing oos slave-standby** commands. If this command is entered with the **disabled** keyword, the **signal timing oos restart** and **signal timing oos slave-standby** commands are ineffective.

Examples

The following example, beginning in global configuration mode, creates voice class 10 and sets the OOS timeout time to 60 seconds:

```
voice-class permanent 10
  signal-keepalive 3
  signal pattern oos receive 0001
  signal pattern oos transmit 0001
  signal timing oos timeout 60
exit
dial-peer voice 100 vofr
  voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

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		
cas		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.
cept		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.
ext-signal		External signaling. The digital signal processor (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.
transparent		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 cas .

Defaults	
	cas

Command Modes	
	Dial-peer configuration

Command History	Release	Modification
	12.0(3)XG	This command was introduced on Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrator.
	12.0(4)T	Support was added for the Cisco 7200 series router.
	12.0(7)XK	In previous releases, the cept and transparent keywords were supported only on the Cisco MC3810 multiservice concentrator. Beginning in this release, these keywords are supported on the Cisco 2600, 3600 and 7200 series routers.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command applies to Voice over Frame Relay (VoFR) and Voice over ATM (VoATM) dial peers. It is used with permanent connections only (Cisco trunks and FRF.11 trunks), not with switched calls.

This command is used to inform the local telephony interface of the type of signaling it should expect to receive from the far-end dial peer. To turn signaling off at this dial peer, select the **ext-signal** option. If signaling is turned off and there are no external signaling channels, a “hot” line exists, enabling this dial peer to connect to anything at the far end.

When you connect an FXS to another FXS, or if you have anything other than an FXS/FXO or E&M/E&M pair, the appropriate signaling type on Cisco 2600 series and 3600 series routers is **ext-signal** (disabled).

If you have a digital E1 connection at the remote end that is running cept/MELCAS signaling and you then trunk that across to an analog port, you should make sure that you configure both ends for the **cept** signal type.

If you have a T1 or E1 connection at both ends and the T1/E1 is running a signaling protocol that is neither EIA-464, or cept/MELCAS, you might want to configure the signal type for the transparent option in order to pass through the signaling.

Examples

The following example shows how to disable signaling on a Cisco 2600 or 3600 series router or on a Cisco MC3810 multiservice concentrator for VoFR dial peer 200, starting from global configuration mode:

```
dial-peer voice 200 vofr
  signal-type ext-signal
exit
```

Related Commands

Command	Description
codec (dial-peer)	Specifies the voice coder rate of speech for a dial peer.
connection	Specifies the connection mode for a voice port.
destination-pattern	Specifies the telephone number associated with a dial peer.
dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
preference	Enables the preferred dial peer to be selected when multiple dial peers within a hunt group are matched for a dial string.
sequence-numbers	Enables the generation of sequence numbers in each frame generated by the DSP.
session protocol	Establishes the VoFR protocol for calls between local and remote routers.
session target	Specifies a network-specific address for a dial peer.

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:ipaddr[:port-num]}
```

Syntax Description

dns:	Sets the global SIP server interface to a Domain Name System (DNS) host name. If you do not specify a host name, the default DNS defined by the ip name-server command is used.
<i>host-name</i>	(Optional) A valid DNS host name takes the following format: name.gateway.xyz.
ipv4:ip_addr	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.

Defaults

The default for this command is a null value.

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on Cisco 2600 and 3600 series routers and Cisco AS5300 universal access servers.

Usage Guidelines

If you use this command, you can then specify **session target sip-server** for each dial peer instead of repeatedly entering the SIP server interface address for each dial peer. To reset this command to a null value, use the **default** command.

Examples

The following example, beginning in global configuration mode, sets the global SIP server interface to the DNS host name of UA-1-f0.sip.com:

```
sip-ua
 sip-server dns:UA-1-f0.sip.com
```

Related Commands

Command	Description
sip-ua	Enters SIP user-agent configuration mode, in which you configure the SIP user agent.

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.

Defaults	No default behaviors or values.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced on Cisco 2600 and 3600 series routers and Cisco AS5300 universal access servers.

Usage Guidelines	Use the sip-ua command to enter the SIP user-agent configuration mode. Table 71 lists the SIP user-agent configuration mode commands:

Table 71 SIP User-Agent Configuration Mode Commands

Command	Description
exit	Exits SIP user-agent configuration mode.
inband-alerting	Specifies an inband-alerting SIP header.
retry	Configures the SIP signaling timers for retry attempts.
sip-server	Configures a SIP server interface.
timers	Configures the SIP signaling timers configuration.
transport	Enables or disables a SIP user agent transport for TCP or UDP, the protocol SIP user agents will be listening for on port 5060 (default).

Examples	The following example, beginning in global configuration mode, enters SIP user-agent configuration mode, configures the SIP user agent, then returns to global configuration mode:

```
sip-ua
retry invite 2
retry response 2
retry bye 2
retry cancel 2
sip-server ipv4:10.0.2.254
timers invite-wait-100 500
exit
```

Related Commands	Command	Description
	exit	Exits SIP user-agent configuration mode.
	inband-alerting	Specifies an inband-alerting SIP header.
	retry	Configures the retry attempts for SIP messages.
	show sip-ua	Displays statistics for SIP retries, timers, and current listener status.
	sip-server	Configures the SIP server interface.
	timers	Configures the SIP signaling timers.
	transport	Configures the SIP user agent (gateway) for SIP signaling messages on inbound calls through the SIP TCP or UDP socket.

snmp enable peer-trap poor-qov

To generate poor quality of voice notification for applicable calls associated with Voice over IP (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.

Defaults

Disabled

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series routers.

Usage Guidelines

Use the **snmp enable peer-trap poor-qov** command to generate poor quality of voice notifications for applicable calls associated with this dial peer. If you have a Simple Network Management Protocol (SNMP) manager that uses SNMP messages when voice quality drops, you might want to enable this command. Otherwise, you should disable this command to reduce unnecessary network traffic.

Examples

The following example enables poor quality of voice notifications for calls associated with VoIP dial peer 10:

```
dial-peer voice 10 voip
 snmp enable peer-trap poor-qov
```

Related Commands

Command	Description
snmp-server enable traps	Enables a router to send SNMP traps and information.
snmp trap link-status	Enables SNMP trap messages to be generated when a specific port is brought up or down.

ss7 mtp2-variant bellcore

To configure the router for Telcordia Technologies (formerly Bellcore) standards, use the **ss7 mtp2-variant bellcore** command in global configuration mode.

ss7 mtp2-variant bellcore [*channel*] [*parameters*]

Syntax Description

<i>channel</i>	Specifies the channel, 0 through 3.
<i>parameters</i>	See table below for timer descriptions, defaults, and ranges.

Defaults

Bellcore is the default variant if no other is configured.
See [Table 72](#) for default parameters.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

This MTP2 variant has timers and parameters that can be configured using the values listed in [Table 72](#). To restore the designated default, use the **no** or the **default** form of the command (see example below).



Note

Timer durations are converted to 10 millisecond units. For example, a T1 value of 1005 is converted to 100 which results in a actual timeout duration of 1000 milliseconds. This is true for all timers and all variants.

Table 72 Bellcore (Telcordia Technologies) Parameters and Values

Parameter	Description	Default	Range
T1	aligned/ready timer duration (milliseconds)	13000	1000 to 65535
T2	not aligned timer (milliseconds)	11500	1000 to 65535
T3	aligned timer (milliseconds)	11500	1000 to 65535
T4-Emergency-Proving	emergency proving timer (milliseconds)	600	1000 to 65535
T4-Normal-Proving	normal proving period (milliseconds)	2300	1000 to 65535
T5	sending SIB timer (milliseconds)	100	80 to 65535
T6	remote congestion timer (milliseconds)	6000	1000 to 65535
T7	excessive delay timer (milliseconds)	1000	500 to 65535

Table 72 *Belcore (Telcordia Technologies) Parameters and Values (continued)*

Parameter	Description	Default	Range
lssu-len	1 or 2 byte LSSU format	1	1 to 2
unacked-MSUs	Maximum number of MSUs waiting ACK	127	16 to 127
proving-attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM-threshold	SUERM error rate threshold	64	32 to 128
SUERM-number-octets	SUERM octet counting mode	16	8 to 32
SUERM-number-signal-units	signal units (good or bad) needed to dec ERM	256	128 to 512
Tie-AERM-Emergency	AERM emergency error rate threshold	1	1 to 8
Tie-AERM-Normal	AERM normal error rate threshold	4	1 to 8

Examples

The following example sets the aligned/ready timer duration on channel 0 to 30,000 milliseconds:

```
ss7 mtp2-variant Bellcore 0
T1 30000
```

The following example restores the aligned/ready timer default value of 13,000 milliseconds:

```
ss7 mtp2-variant Bellcore 0
no T1
```

Related Commands

Command	Description
ss7 mtp2-variant itu	Specifies the mtp2-variant as ITU.
ss7 mtp2-variant ntt	Specifies the mtp2-variant as NTT.
ss7 mtp2-variant ttc	Specifies the mtp2-variant as TTC.

ss7 mtp2-variant itu

To configure the router for ITU (International Telecom United) standards, use the **ss7 mtp2-variant itu** command in global configuration mode.

ss7 mtp2-variant itu [*channel*] [*parameters*]

Syntax Description

<i>channel</i>	Specifies the channel, 0 through 3.
<i>parameters</i>	See table below for timer descriptions, defaults, and ranges.

Defaults

Bellcore is the default variant if no other is configured.

See [Table 73](#) for ITU default parameters.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The ITU MTP2 variant has timers and parameters that can be configured using the values listed in [Table 73](#). To restore the designated default, use the **no** or the **default** form of the command (see the example below).

Table 73 ITU (White) Parameters and Values

Parameter	Description	Default	Range
T1	aligned/ready timer duration (milliseconds)	40000	1000 to 65535
T2	not aligned timer (milliseconds)	5000	1000 to 65535
T3	aligned timer (milliseconds)	1000	1000 to 65535
T4-Emergency-Proving	emergency proving timer (milliseconds)	500	1000 to 65535
T4-Normal-Proving	normal proving timer (milliseconds)	8200	1000 to 65535
T5	sending SIB timer (milliseconds)	100	80 to 65535
T6	remote congestion timer (milliseconds)	6000	1000 to 65535
T7	excessive delay timer (milliseconds)	1000	1000 to 65535
lssu-len	1 or 2 byte LSSU format	1	1 to 2
msu-len			

Table 73 ITU (White) Parameters and Values (continued)

Parameter	Description	Default	Range
unacked-MSUs	Maximum number of MSUs waiting ACK	127	16 to 127
proving-attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM-threshold	SUERM error rate threshold	64	32 to 128
SUERM-number-octets	SUERM octet counting mode	16	8 to 32
SUERM-number-signal-units	signal units (good or bad) needed to dec ERM	256	128 to 512
Tie-AERM-Emergency	AERM emergency error rate threshold	1	1 to 8
Tin-AERM-Normal	AERM normal error rate threshold	4	1 to 8

Examples

The following example sets the emergency proving period on channel 1 to 10,000 milliseconds:

```
ss7 mtp2-variant itu 1
t4-Emergency-Proving 10000
```

The following example restores the emergency proving period default value of 5,000 milliseconds:

```
ss7 mtp2-variant itu 1
default t4-Emergency-Proving
```

Related Commands

Command	Description
ss7 mtp2-variant bellcore	Specifies the mtp2-variant as Bellcore.
ss7 mtp2-variant ntt	Specifies the mtp2-variant as NTT.
ss7 mtp2-variant ttc	Specifies the mtp2-variant as TTC.

ss7 mtp2-variant ntt

To configure the router for NTT (Japan) standards, use the **ss7 mtp2-variant ntt** command in global configuration mode.

ss7 mtp2-variant ntt [*channel*] [*parameters*]

Syntax Description

<i>channel</i>	Specifies the channel, 0 through 3.
<i>parameters</i>	See table below for timer descriptions, defaults, and ranges.

Defaults

Bellcore is the default variant if no other is configured.

See [Table 74](#) for NTT default parameters.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The NTT MTP2 variant has timers and parameters that can be configured using the values listed in [Table 74](#). To restore the designated default, use the **no** or the **default** form of the command (see the example below).

Table 74 NTT Parameters and Values

Parameter	Description	Default	Range
T1	aligned/ready timer duration (milliseconds)	15000	1000 to 65535
T2	not aligned timer (milliseconds)	5000	1000 to 65535
T3	aligned timer (milliseconds)	3000	1000 to 65535
T4-Emergency-Proving	emergency proving timer (milliseconds)	3000	1000 to 65535
T5	sending SIB timer (milliseconds)	200	80 to 65535
T6	remote congestion timer (milliseconds)	2000	1000 to 65535
T7	excessive delay timer (milliseconds)	3000	1000 to 65535
TA	SIE interval timer (milliseconds)	20	10 to 500
TF	FISU interval timer (milliseconds)	20	10 to 500
TO	SIO interval timer (milliseconds)	20	10 to 500
TS	SIOS interval timer (milliseconds)	20	10 to 500

Table 74 *NTT Parameters and Values (continued)*

Parameter	Description	Default	Range
unacked-MSUs	Maximum number of MSUs waiting ACK	40	16 to 40
proving-attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM-threshold	SUERM error rate threshold	64	32 to 128
SUERM-number-octets	SUERM octet counting mode	16	8 to 32
SUERM-number-signal-units	signal units (good or bad) needed to dec ERM	256	128 to 512
Tie-AERM-Emergency	AERM emergency error rate threshold	1	1 to 8

Examples

The following example sets the SUERM error rate threshold on channel 2 to 100:

```
ss7 mtp2-variant ntt 2
  SUERM-threshold 100
```

The following example restores the SUERM error rate threshold default value of 64:

```
ss7 mtp2-variant ntt 2
  no SUERM-threshold
```

Related Commands

Command	Description
ss7 mtp2-variant bellcore	Specifies the mtp2-variant as Bellcore.
ss7 mtp2-variant itu	Specifies the mtp2-variant as ITU.
ss7 mtp2-variant ttc	Specifies the mtp2-variant as TTC.

ss7 mtp2-variant ttc

To configure the router for TTC (Japan Telecom) standards, use the **ss7 mtp2-variant ttc** command in global configuration mode.

ss7 mtp2-variant ttc [*channel*] [*parameters*]

Syntax Description

<i>channel</i>	Specifies the channel, 0 through 3.
<i>parameters</i>	See table below for timer descriptions, defaults, and ranges.

Defaults

Bellcore is the default variant if no other is configured.

See [Table 75](#) for TTC default parameters.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The TTC MTP2 variant has timers and parameters that can be configured using the values listed in [Table 75](#). To restore the designated default, use the **no** or the **default** form of the command (see the example below).

Table 75 TTC Parameters and Values

Parameter	Description	Default	Range
T1	aligned/ready timer duration (milliseconds)	15000	1000 to 65535
T2	not aligned timer (milliseconds)	5000	1000 to 65535
T3	aligned timer (milliseconds)	3000	1000 to 65535
T4-Emergency-Proving	emergency proving timer (milliseconds)	3000	1000 to 65535
T5	sending SIB timer (milliseconds)	200	80 to 65535
T6	remote congestion timer (milliseconds)	2000	1000 to 65535
T7	excessive delay timer (milliseconds)	3000	1000 to 65535
TA	SIE interval timer (milliseconds)	20	10 to 500
TF	FISU interval timer (milliseconds)	20	10 to 500
TO	SIO interval timer (milliseconds)	20	10 to 500
TS	SIOS interval timer (milliseconds)	20	10 to 500

Table 75 *TTC Parameters and Values (continued)*

Parameter	Description	Default	Range
unacked-MSUs	Maximum number of MSUs waiting ACK	40	16 to 40
proving-attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM-threshold	SUERM error rate threshold	64	32 to 128
SUERM-number-octets	SUERM octet counting mode	16	8 to 32
SUERM-number-signal-units	signal units (good or bad) needed to decrement	256	128 to 512
Tie-AERM-Emergency	AERM emergency error rate threshold	1	1 to 8

Examples

The following example sets the maximum number of proving attempts for channel 3 to 3:

```
ss7 mtp2-variant ttc 3
   proving-attempts 3
```

The following example restores the maximum number of proving attempts to the default value:

```
ss7 mtp2-variant ttc 3
   default proving-attempts
```

Related Commands

Command	Description
ss7 mtp2-variant bellcore	Specifies the mtp2-variant as Bellcore.
ss7 mtp2-variant itu	Specifies the mtp2-variant as ITU.
ss7 mtp2-variant ntt	Specifies the mtp2-variant as NTT.

ss7 session

To create a Reliable User Datagram Protocol (RUDP) session, use the **ss7 session** command in global configuration mode. To delete the session, use the **no** form of this command.

ss7 session-session number {address remote-address remote-port local-address local-port}

no ss7session-session number address

Syntax Description

<i>session-number</i>	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the session keyword.
<i>remote-address</i>	The remote IP address of the Media Gateway Controller in four-part dotted-decimal format.
<i>remote-port</i>	The number of the remote UDP port on which the Media Gateway Controller is configured to listen. This UDP port cannot be used by another protocol as defined in RFC 1700 and cannot be otherwise used in the network.
<i>local-address</i>	The local IP address of the router in four-part dotted-decimal format. The local IP address for both sessions, 0 and 1, must be the same.
<i>local-port</i>	The number of the local UDP port on which the router expects to receive messages from the Media Gateway Controller. Specify any UDP port that is not used by another protocol as defined in RFC 1700 and that is not otherwise used in your network. The local UDP port must be different for session-0 and session-1.

Defaults

No session is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

You can configure a maximum of two sessions, one for each signaling link. In a redundant Media Gateway Controller configuration, session-0 is configured to one MGC and session-1 is configured to the other.

The Media Gateway Controller must be configured to send messages to the local port, and it must be configured to listen on the remote port.

You must reload the router whenever you remove a session or change the parameters of a session.

Examples

The following example sets up two sessions on a Cisco 2611:

```
ss7 session-0 address 255.251.255.255 7000 255.255.255.254 7000
ss7 session-1 address 255.255.255.252 7002 255.255.255.254 7001
```



Note

The example above shows how the local IP addresses in session-0 and session-1 must be the same.

Related Commands

Command	Description
ss7 session retrans_t	Sets the retransmission timer.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.

ss7 session cumack_t

To set the Reliable User Datagram Protocol (RUDP) cumulative acknowledgment timer for a specific SS7 signaling link session, use the **ss7 session cumack_t** command in global configuration mode. To restore the default value, use the **no** form of this command.

ss7 session-session number cumack_t milliseconds

no ss7 session-session number cumack_t



Caution

Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Syntax Description

<i>session-number</i>	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the session keyword.
<i>milliseconds</i>	Use this parameter to specify the amount of time (in milliseconds) that the RUDP waits before it sends an acknowledgment after receiving a segment. Valid values are from 100 to 65535. This value should be less than the value configured for the retransmission timer by using the ss7 session-session number retrans_t command.

Defaults

The default value is 300 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The cumulative acknowledgment timer determines when the receiver sends an acknowledgment. If the timer is not already running, it is initialized when a valid data, null, or reset segment is received. When the cumulative acknowledgment timer expires, the last in-sequence segment is acknowledged. The RUDP typically tries to “piggyback” acknowledgments on data segments being sent. However, if no data segment is sent in this period of time, it sends a standalone acknowledgment.

Examples

The following example sets up two sessions and sets the cumulative acknowledgment timer to 320 milliseconds for each one:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7000
ss7 session-0 cumack_t 320
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7001
ss7 session-1 cumack_t 320
```

Related Commands

Command	Description
ss7 session retrans_t	Sets the retransmission timer.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session k_pt	Sets the null segment (keepalive) timer.
show ss7	Displays the SS7 configuration.

ss7 session kp_t

To set the null segment (keepalive) timer for a specific SS7 signaling link session, use the **ss7 session kp_t** command in global configuration mode. To restore the default value, use the **no** form of this command.

ss7 session-session number kp_t milliseconds

no ss7 session-session number kp_t



Caution

Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Syntax Description

<i>session-number</i>	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the session keyword.
<i>milliseconds</i>	Use this parameter to specify the amount of time (in milliseconds) that the Reliable User Datagram Protocol (RUDP) waits before sending a keepalive to verify that the connection is still active. Valid values are 0 and from 100 to 65535.

Defaults

The default value is 2000 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The null segment timer determines when a null segment (keepalive) is sent by the client Cisco 2600 series router. On the client, the timer starts when the connection is established and is reset each time a data segment is sent. If the null segment timer expires, the client sends a keepalive to the server to verify that the connection is still functional. On the server, the timer restarts each time a data or null segment is received from the client.

The value of the server's null segment timer is twice the value configured for the client. If no segments are received by the server in this period of time, the connection is no longer valid.

To disable keepalive, set this parameter to 0.

Examples

The following example sets up two sessions and sets a keepalive of 1,800 milliseconds for each one:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7000
ss7 session-0 kp_t 1800
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7001
ss7 session-1 kp_t 1800
```

Related Commands

Command	Description
ss7 session retrans_t	Sets the retransmission timer.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
show ss7	Displays the SS7 configuration.

ss7 session m_cumack

To set the maximum number of segments that can be received before the Reliable User Datagram Protocol (RUDP) sends an acknowledgment in a specific SS7 signaling link session, use the **ss7 session m_cumack** command in global configuration mode. To restore the default value, use the **no** form of this command.

ss7 session-session number m_cumack segments

no ss7 session-session number m_cumack



Caution

Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Syntax Description

<i>session-number</i>	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the session keyword.
<i>segments</i>	Use this parameter to specify maximum number of segments that can be received before the Reliable User Datagram Protocol (RUDP) sends an acknowledgment. Valid values are from 0 to 255.

Defaults

The default value is 3 segments.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The cumulative acknowledgment counter records the number of unacknowledged, in-sequence data, null, or reset segments received without a data, null, or reset segment being sent to the transmitter. If this counter reaches the configured maximum, the receiver sends a standalone acknowledgment (a standalone acknowledgment is a segment that contains only acknowledgment information). The standalone acknowledgment contains the sequence number of the last data, null, or reset segment received.

If you set this parameter to 0, an acknowledgment is sent immediately after a data, null, or reset segment is received.

Examples

The following example sets up two sessions and in each session sets a maximum of two segments for receipt before acknowledgment:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 m_cumack 2
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_cumack 2
```

Related Commands

Command	Description
ss7 session retrans_t	Sets the retransmission timer.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
show ss7	Displays the SS7 configuration.

ss7 session m_outseq

To set the maximum number of out-of-sequence segments that can be received before the Reliable User Datagram Protocol (RUDP) sends an extended acknowledgment in a specific SS7 signaling link session, use the **ss7 session m_outseq** command in global configuration mode. To restore the default value, use the **no** form of this command.

ss7 session-session number m_outseq segments

no ss7 session-session number m_outseq



Caution

Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Syntax Description

<i>session-number</i>	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the session keyword.
<i>segments</i>	Use this parameter to specify the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment. If the specified number of segments are received out of sequence, an Extended Acknowledgment segment is sent to inform the sender which segments are missing. Valid values are from 0 to 255.

Defaults

The default value is 3 segments.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The out-of-sequence acknowledgment counter records the number of data segments that have arrived out of sequence. If this counter reaches the configured maximum, the receiver sends an extended acknowledgment segment that contains the sequence numbers of the out-of-sequence data, null, and reset segments received. When the transmitter receives the extended acknowledgment segment, it retransmits the missing data segments.

If you set this parameter to 0, an acknowledgment is sent immediately after an out-of-sequence segment is received.

Examples

The following example sets up two sessions and sets a maximum number of four out-of-sequence segments for each session:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 m_outseq 4
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_outseq 4
```

Related Commands

Command	Description
ss7 session retrans_t	Sets the retransmission timer.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
show ss7	Displays the SS7 configuration.

ss7 session m_rcvnum

To set the maximum number of segments that the remote end can send before receiving an acknowledgment in a specific SS7 signaling link session, use the **ss7 session m_rcvnum** command in global configuration mode. To restore the default value, use the **no** form of this command.

ss7 session-session number m_rcvnum segments

no ss7 session-session number m_rcvnum



Caution

Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Syntax Description

<i>session-number</i>	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the session keyword.
<i>segments</i>	Use this parameter to specify the maximum number of segments that the remote (Cisco IOS software) end can send before receiving an acknowledgment. Valid values are from 1 to 64.

Defaults

The default value is 32 segments.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The outstanding segments counter is the maximum number of segments that the Cisco IOS software end of the connection can send without getting an acknowledgment from the receiver. The receiver uses the counter for flow control.

Examples

The following example sets up two sessions and for each session sets a maximum of 36 segments for receipt before an acknowledgment:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 m_rcvnum 36
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_rcvnum 36
```

Related Commands

Command	Description
ss7 session retrans_t	Sets the retransmission timer.
ss7 session m_retrans	Sets the maximum number of times that the Reliable User Datagram Protocol (RUDP) attempts to resend a segment before declaring the connection invalid.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
show ss7	Displays the SS7 configuration.

ss7 session m_retrans

To set the maximum number of times that the Reliable User Datagram Protocol (RUDP) attempts to resend a segment before declaring the connection invalid in a specific SS7 signaling link session, use the **ss7 session m_retrans** command in global configuration mode. To restore the default value, use the **no** form of this command.

ss7 session-session number m_retrans number

no ss7 session-session number m_retrans



Caution

Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Syntax Description

<i>session-number</i>	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the session keyword.
<i>number</i>	Use this parameter to specify the maximum number of times that the RUDP attempts to resend a segment before declaring the connection broken. Valid values are from 0 to 255.

Defaults

The default value is 2 times.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The retransmission counter is the number of times a segment has been retransmitted. If this counter reaches the configured maximum, the transmitter resets the connection and informs the upper-layer protocol.

If you set this parameter to 0, the RUDP attempts to resend the segment continuously.

Examples

The following example sets up two sessions and for each session sets a maximum number of three times to resend before a session becomes invalid:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 m_retrans 3
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_retrans 3
```

Related Commands

Command	Description
ss7 session retrans_t	Sets the retransmission timer.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
show ss7	Displays the SS7 configuration.

ss7 session retrans_t

To set the amount of time that the Reliable User Datagram Protocol (RUDP) waits to receive an acknowledgment for a segment in a specific SS7 signaling link session, use the **ss7 session retrans_t** command in global configuration mode. If the RUDP does not receive the acknowledgment in this time period, the RUDP retransmits the segment. To restore the default value, use the **no** form of this command.

ss7 session-session number retrans_t milliseconds

no ss7 session-session number retrans_t



Caution

Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Syntax Description

<i>session-number</i>	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the session keyword.
<i>milliseconds</i>	Use this parameter to specify the amount of time that the RUDP waits to receive an acknowledgment for a segment. Valid values are from 100 to 65535.

Defaults

The default value is 600 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The retransmission timer is used to determine whether a packet must be retransmitted and is initialized each time a data, null, or reset segment is sent. If an acknowledgment for the segment is not received by the time the retransmission timer expires, all segments that have been transmitted—but not acknowledged—are retransmitted.

This value should be greater than the value configured for the cumulative acknowledgment timer by using the **ss7 session cumack_t** command.

Examples

The following example sets up two sessions and specifies 550 milliseconds as the time to wait for an acknowledgment for each session:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 retrans_t 550
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 retrans_t 550
```

Related Commands

Command	Description
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
show ss7	Displays the SS7 configuration.

ss7 set failover-timer

To specify the amount of time that the SS7 Session Manager waits for the active session to recover or for the standby Media Gateway Controller to indicate that the SLT should switch traffic to the standby session, use the **ss7 set failover-timer** command in global configuration mode. To restore the default setting, use the **no** form of this command.

ss7 set failover-timer [*seconds*]

no ss7 set failover-timer

Syntax Description	<i>seconds</i>	Time in seconds that the Session Manager waits for a session to recover. Values from 1 through 10 are valid.

Defaults	The default is 3 seconds.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(7)XR	This command was introduced.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines	This command specifies the number of seconds that the Session Manager waits for the the active session to recover or for the standby Media Gateway Controller to indicate that the SLT should switch traffic to the standby session and to make that session the active session. If the timer expires without a recovery of the original session or an active message from the standby Media Gateway Controller, the signaling links are taken out of service.

Examples	The following example sets the failover timer to four seconds: <pre>ss7 set failover-timer 4</pre>

Related Commands	Command	Description
	show ss7 sm set	Displays the current failover timer setting.
	ss7 session	Establishes a session.

station-id

To specify the name or number that will be sent as Caller-ID information and enable Caller-ID, use the **station-id** voice-port configuration command 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 or number, use the **no** form of this command.

station-id [**name** *name* | **number** *number*]

no station-id [**name** *name* | **number** *number*]

Syntax Description

<i>name</i>	A string of 1 to 15 characters to represent the station name.
<i>number</i>	A string of from 1 to 15 characters to represent the station number.

Defaults

The default is no station name or number.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(2)XH	This command was implemented for Cisco MC3810 and for Cisco 2600 and 3600 series routers.
12.1(3)T	This command was first supported on the T Train.

Usage Guidelines

This optional command is configured on FXS voice ports that are used to originate on-net calls. The information entered is displayed by the telephone attached to the FXS port at the far end of the on-net call. It can also be configured on the FXO port of a router on which Caller ID information is expected to be received from the CO, to suit situations where a call is placed from the CO, then goes through the FXO interface, and continues to a far-end FXS port through an on-net call. In this case, if no Caller ID information is received from the CO telephone line, the far-end call recipient receives the information configured on the FXO port.



Note

This feature applies only to Caller ID name display provided by an FXS port connection to a telephone device. The station name will not be passed through telephone trunk connections supporting Automatic Number Identification (ANI) calls. ANI supplies calling number identification only and does not support calling number names.

Do not use this command when the Caller-ID standard is dual-tone multifrequency (DTMF). DTMF Caller ID can carry only the calling number.

If the **station-id** or **caller-id alerting** command is configured on the voice port, these automatically enable Caller-ID, and the **caller-id enable** command is not necessary.

This command applies to the Cisco MC3810 and to Cisco 2600 and 3600 series routers.

Examples

The following example configures a Cisco 2600 or 3600 series router voice port from which Caller-ID information is sent:

```
voice-port 1/0/1
  cptone US
  station-id name A. Person
  station-id number 4085551111
```

The following example configures a Cisco MC3810 voice port from which Caller-ID information is sent:

```
voice-port 1/0
  cptone northamerica
  station-id name A. Person
  station-id number 4085551111
  caller-id alerting ring 1
```

Related Commands

Command	Description
caller-id enable	Enables Caller-ID operation.

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

Syntax Description This command has no arguments or keywords.

Defaults Subcell multiplexing is not enabled.

Command Modes Voice-service configuration

Command History	Release	Modification
	12.1(1)XA	The command was introduced for the Cisco MC3810 multiservice concentrator.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines Use this command to enable ATM adaptation layer 2 (AAL2) common part sublayer (CPS) subcell multiplexing when the Cisco MC3810 interoperates with other equipment that uses subcell multiplexing.

Examples The following example enables AAL2 CPS subcell multiplexing on a Cisco MC3810 multiservice concentrator:

```
voice service voatm
  session protocol aal2
  subcell-mux
```

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

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Voice-port configuration

Command History	Release	Modification
	11.3(1)MA	This command was introduced on Cisco MC3810 multiservice concentrators.

Usage Guidelines This command indicates whether supervisory disconnect signaling is available on the FXO port. Supervisory disconnect signaling is a power denial from the switch lasting at least 350 milliseconds. When this condition is detected, the system interprets this as a disconnect indication from the switch and clears the call.

You should configure no supervisory disconnect on the voice port if there is no supervisory disconnect available from the switch.



Note

If there is no disconnect supervision on the voice port, the interface could be left active if the caller abandons the call before the far end answers. After the router collects the dialed digits but before the called party answers, the router starts a tone detector. Within this time window, the tone detector listens for signals (such as a fast busy signal) that occur if the originating caller hangs up. If this occurs, the router will interpret those tones as a disconnect indication and close the window.

Examples The following example configures supervisory disconnect on a Cisco 3600 series voice port:

```
voice-port 2/1/0
 supervisory disconnect
```

The following example configures supervisory disconnect on a Cisco MC3810 multiservice concentrator voice port:

```
voice-port 1/1
 supervisory disconnect
```

supervisory disconnect anytime

To configure an Foreign Exchange Office (FXO) voice port to go on-hook if the router detects any tone from a PBX or public switched telephone network (PSTN) before the call is answered, use the **supervisory disconnect anytime** command in voice-port configuration mode. To restore the default, use the **no** form of this command.

supervisory disconnect anytime

no supervisory disconnect anytime

Syntax Description

This command has no arguments or keywords.

Defaults

The supervisory disconnect function is not enabled on voice ports.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600, 3600, and MC3810 series.

Usage Guidelines

The **supervisory disconnect anytime** voice-port configuration command can be used to provide the disconnect function if the PBX or PSTN does not provide a supervisory tone. This function is enabled only during call setup (before the call is answered); examples of tones that trigger a disconnect include busy tone, fast busy tone, and dial tone. You must enable echo cancellation; otherwise, the router's own ringback tone can trigger a disconnect.

This command replaces the **no supervisory disconnect signal** command. If you enter the **no supervisory disconnect signal** command, the supervisory disconnect any-tone feature will be enabled, and "supervisory disconnect" anytime will be displayed when **show** commands are entered.

Examples

The following example configures voice ports 1/4 and 1/5 to go on-hook if any tone from the PBX or PSTN is detected before the call is answered:

```
voice-port 1/4
  supervisory disconnect anytime
exit
voice-port 1/5
  supervisory disconnect anytime
exit
```

The following example disables the disconnect function on voice port 1/5:

```
voice-port 1/5
  no supervisory disconnect anytime
exit
```

 supervisory disconnect anytime**Related Commands**

Command	Description
voice class dualtone	Creates a voice class for FXO tone detection parameters.

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

Syntax Description	mid-call	Configures tone detection to operate throughout the duration of the call.
	pre-connect	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 voice class dualtone global configuration command. The range is from 1 to 10,000.

Defaults	No voice class is assigned to a voice port.

Command Modes	Voice-port configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600, 3600, and MC3810 series.

Usage Guidelines	You can apply an FXO supervisory disconnect tone voice class to multiple voice ports. You can assign only one FXO supervisory disconnect tone voice class to a voice port. If a second voice class is assigned to a voice port, the second voice class replaces the one previously assigned. You cannot assign separate FXO supervisory disconnect tone commands directly to the voice port.

This feature is applicable to analog FXO voice ports with loop-start signaling.

Examples	The following example assigns voice class 70 to FXO voice port 1/5 of a Cisco MC3810 series concentrator and specifies tone detection during the entire call duration:

```
voice-port 1/5
no echo-cancel enable
supervisory disconnect dualtone mid-call voice-class 70
```

The following example assigns voice class 80 to FXO voice port 0/1/1 of a Cisco 3600 series router and specifies tone detection only during call setup:

```
voice-port 0/1/1
no echo-cancel enable
supervisory disconnect dualtone pre-connect voice-class 80
```

Related Commands	Command	Description
	channel-group	Defines the time slots of each T1 or E1 circuit.
	mode	Sets the mode of the T1/E1 controller and enters specific configuration commands for each mode type in VoATM.
	voice class dualtone	Creates a voice class for FXO tone detection parameters.

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**}]

Syntax Description	
<i>tdm-group-no</i>	TDM group number.
timeslot	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.
type	(Optional) (Valid only when the mode cas 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. Choose from one of the following options: • e&m—for E&M signaling • fxs—for Foreign Exchange Station signaling (optionally, you can also specify loop-start or ground-start) • fxo—for Foreign Exchange Office signaling (optionally, you can also specify loop-start or ground-start) • fxs-melcas—for Foreign Exchange Station MEL CAS • fxo-melcas—for Foreign Exchange Office MEL CAS • e&m-melcas—for E&M Mercury Exchange Limited Channel-Associated signaling (MEL CAS) The MELCAS options apply only to E1 lines and are used primarily in the United Kingdom.

Defaults	No TDM group is configured.

Command Modes	Controller configuration

Command History	Release	Modification
	11.3(1)MA	This command was introduced on Cisco MC38310 multiservice concentrators.

Release	Modification
12.1(1)T	This command was modified to include voice WAN interface cards (VWICs) for Cisco 2600 and Cisco 3600 series routers.
12.1(2)T	This command was modified for the OC-3/STM-1 ATM Circuit Emulation Service network module on the Cisco 2600 and 3600 series routers.

Usage Guidelines

The **tdm-group** command allows specific timeslots to switch from port 0 to port 1 and vice versa. This command is similar to the **channel-group** command, but it does not create a serial interface to terminate the specified channels.



Note

Channel groups, CAS voice groups, and TDM groups all use group numbers. All group numbers configured for channel groups, CAS voice groups, and TDM groups must be unique on the local router. For example, you cannot use the same group number for a channel group and for a TDM group.

Examples

The following example shows TDM group 1 being set up to include timeslots 13 through 20:

```
controller T1 1
 tdm-group 1 timeslots 13-20
```

The following example configures TDM group number 20 on controller T1 1 to support FXO ground-start:

```
controller T1 1
 tdm-group 20 timeslot 20 type fxs ground-start
```

Related Commands

Command	Description
connect	Starts passage of data between ports for cross-connect TDM.

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 (*).

Defaults

No technology prefix is defined.

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on Cisco 2500 and 3600 series routers.

Usage Guidelines

Technology prefixes are used to distinguish between gateways that have specific capabilities within a given zone. In the exchange between the gateway and the gatekeeper, the technology prefix is used to select a gateway after the zone has been selected. Use the **tech-prefix** command to define technology prefixes.

Technology prefixes can be used as a discriminator so that the gateway can tell the gatekeeper that a certain technology is associated with a particular call (for example, 15# could mean a fax transmission), or a technology prefix can be used like an area code for more generic routing. No standard defines what the numbers in a technology prefix mean; by convention, technology prefixes are designated by a pound (#) symbol as the last character.

In most cases, there is a dynamic protocol exchange between the gateway and the gatekeeper that enables the gateway to inform the gatekeeper about technology prefixes and where to forward calls. If, for some reason, that dynamic registry feature is not in effect, you can statically configure the gatekeeper to query the gateway for this information by configuring the **gw-type-prefix** command on the gatekeeper. Use the **show gatekeeper gw-type-prefix** command to display how the gatekeeper has mapped the technology prefixes to local gateways.



Note

Cisco gatekeepers use the asterisk (*) as a reserved character. If you are using Cisco gatekeepers, do not use the asterisk as part of the technology prefix.

Examples

The following example defines a technology prefix of 14# for the specified dial peer. In this example, the technology prefix means that the H.323 gateway will ask the RAS gatekeeper to direct calls using the technology prefix of 14#.

```
dial-peer voice 10 voip
 destination-pattern 14...
 tech-prefix 14#
```

Related Commands

Command	Description
gw-type-prefix	Configures a technology prefix in the gatekeeper.
show gatekeeper gw-type-prefix	Displays the gateway technology prefix table.

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.
	codec 711/729	(Optional) Specifies a specific codec type.

Defaults	This command is not configured by default.

Command Modes	EXEC

Command History	Release	Modification
	12.1(3)T	This command was introduced.

Examples	The following example demonstrates a test probe to IP address 10.1.1.4, and shows that the ICPIF value to 10.1.1.4 is 0:

```
Router# test call fallback probe 10.1.1.4
```

```
Running a test RTR probe....  
ICPIF value for the test probe is 0
```

Related Commands	Command	Description
	call fallback active	Enables fallback to alternate dial peers in case of network congestion.
	call fallback monitor	Enables the monitoring of destinations without fallback to alternate dial peers.

test pots dial

To dial a telephone number for the plain old telephone service (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.

Command Modes

EXEC

Command History

Release	Modification
12.1(2)XF	The command test pots <i>port</i> dial was introduced on the Cisco 800 series routers.

Usage Guidelines

If the telephone is on the hook when you issue the dial command, the router rings the telephone, waits until the telephone is taken off the hook, and then dials the requested number. If the telephone is off the hook and providing a dial tone when you issue the command, the router dials the requested number.

Examples

The following POTS dial command dials the telephone number 4085551234:

```
Router# test pots 1 dial 4085551234#
```

For an example of the **test pots *port* dial** command with debug output, see the **debug pots csm** command in the *Cisco IOS Debug Command Reference*, Release 12.2.

Related Commands

Command	Description
show pots csm	Displays the current state of calls and the most recent event received by the CSM on the router.
test pots disconnect	Disconnects a telephone call for the POTS port on the router.

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.

Command Modes	EXEC

Command History	Release	Modification
	12.1(2)XF	This command was introduced on the Cisco 800 series routers.

Examples	The following POTS disconnect command disconnects a telephone call from POTS port 1: Router# test pots 1 disconnect
	For an example of the test pots port disconnect command with debug output, see the debug pots csm command in the <i>Cisco IOS Debug Command Reference</i> , Release 12.2.

Related Commands	Command	Description
	show pots csm	Displays the current state of calls and the most recent event received by the CSM on the router.
	test pots dial	Dials a telephone number for the POTS port on the router by using a dial application on your workstation.

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 the test, 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 international , national , subscriber , abbreviated , unknown , and any .

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.0(7)XR1	This command was introduced for Voice over IP on the Cisco AS5300.
	12.0(7)XK	This command was first supported for the following voice technologies on the following platforms: - Voice over IP (Cisco 2600 series, Cisco 3600 series, Cisco MC3810 series) - Voice over Frame Relay (Cisco 2600 series, Cisco 3600 series, Cisco MC3810 multiservice concentrator) - Voice over ATM (Cisco 3600 series, Cisco MC3810 multiservice concentrator)
	12.1(1)T	This command was first supported on the T train for the following voice technology on the following platforms: Voice over IP (Cisco 1750, Cisco 2600 series, Cisco 3600 series, Cisco AS5300, Cisco 7200 series, and Cisco 7500 series)
	12.1(2)T	This command was first supported on the T train for the following voice technologies on the following platforms: - Voice over IP (Cisco MC3810 multiservice concentrator) - Voice over Frame Relay (Cisco 2600 series, Cisco 3600 series, Cisco MC3810 multiservice concentrator) - Voice over ATM (Cisco 3600 series, Cisco MC3810 multiservice concentrator)

Examples

The following example shows output from the **test translation-rule** command:

```
Router# translation-rule 21
Rule 1 555.% 1408555 subscriber international
Rule 2 8.% 1408555 abbreviated international

Router# test translation-rule 21 45678 abbreviated
*Jan 19 16:39:14.578:The replace number 45614085558
```

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
show translation-rule	Displays the contents of all the rules that have been configured for a specific translation name.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

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. <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. <i>subunit</i> specifies a voice interface card (VIC) in which the voice port is located. Valid entries are 0 and 1. <i>port</i> specifies an analog voice port number. Valid entries are 0 and 1.

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. <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. <i>port</i> specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1. <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.

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. <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. <i>port</i> specifies an analog voice port number. Valid entries are 1 to 6.

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. <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). <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.

For All Platforms:

m-lead	Forces the E&M m-lead detector to the specified state.
loop	Forces the FXO loop detector to the specified state.
battery-reversal	Forces the FXO battery-reversal detector to the specified state.
ring	Forces the FXO ringing detector to the specified state.
tip-ground	Forces the FXO tip-ground detector to the specified state.
ring-ground	Forces the FXS ring-ground detector to the specified state.
ring-trip	Forces the FXS ring-trip detector to the specified state.
on	Forces the selected item to the on state.
off	Forces the selected item to the off state.
disable	Ends the forced state for the selected item.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(7)XK	This command was introduced on Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrators.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use the **test voice port detector** privileged EXEC command to force a detector into specific states for testing. For each signaling type (E&M, FXO, FXS), only the applicable keywords are displayed. When you are finished testing, be sure to enter the command with the **disable** keyword to end the forced state. The **disable** keyword is available only if a test condition is already activated.

Examples

The following example forces the tip-ground detector to the off state on an FXO voice port (1/3) on a Cisco MC3810 and ends any call in progress:

```
Router# test voice port 1/3 detector tip-ground off
```

The following example ends the forced off state on an FXO voice port (1/3) on a Cisco MC3810:

```
Router# test voice port 1/3 detector tip-ground disable
```

The following example forces the ring-trip detector to the on state on an FXS port (0/0/1) on a Cisco 3600 series router and should start a call:

```
Router# test voice port 0/0/1 detector ring-trip on
```

The following example ends the forced on state on an FXS port (0/0/1) on a Cisco 3600 series router:

```
Router# test voice port 0/0/1 detector ring-trip disable
```

Related Commands

Command	Description
test voice port inject-tone	Injects a test tone into a voice port.
test voice port loopback	Performs loopback testing on a voice port.
test voice port relay	Tests relay-related functions on a voice port.
test voice port switch	Forces a voice port into fax or voice mode.

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. <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. <i>subunit</i> specifies a voice interface card (VIC) in which the voice port is located. Valid entries are 0 and 1. <i>port</i> specifies an analog voice port number. Valid entries are 0 and 1.

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. <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. <i>port</i> specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1. <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.

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.
	<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. <i>port</i> specifies an analog voice port number. Valid entries are 1 to 6.

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.
	<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). <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.

For All platforms:

local	Directs the injected tone toward the local interface (near end).
network	Directs the injected tone toward the network (far end).
1000hz	Injects a 1-kilohertz test tone.
2000hz	Injects a 2-kilohertz test tone.
200hz	Injects a 200-hertz test tone.
3000hz	Injects a 3-kilohertz test tone.
300hz	Injects a 300-hertz test tone.
3200hz	Injects a 3.2-kilohertz test tone.
3400hz	Injects a 3.4-kilohertz test tone.
500hz	Injects a 500-hertz test tone.
quiet	Injects a quiet tone.
disable	Ends the test tone.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XK	This command was introduced on Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrators.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use the **test voice port inject-tone** privileged EXEC command to inject a test tone or to end a test tone. A call must be established on the voice port under test. When you are finished testing, be sure to enter the **disable** keyword to end the test tone. The **disable** keyword is available only if a test condition is already activated.

When you enter the **disable** keyword, you must enter a direction (either **network** or **local**); however, you can enter either direction, regardless of which direction you entered to inject the test tone.

Examples

The following example injects a 1-kilohertz test tone into voice port 1/1, directed toward the network (far end), on a Cisco MC3810:

```
Router# test voice port 1/1 inject-tone network 1000hz
```

The following example removes the test tone from port 0/0/1 on a Cisco 3600 series router:

```
Router# test voice port 0/0/1 inject-tone network disable
```

or

```
Router# test voice port 0/0/1 inject-tone local disable
```

Related Commands

Command	Description
test voice port detector	Tests detector-related functions on a voice port.
test voice port loopback	Performs loopback testing on a voice port.
test voice port relay	Tests relay-related functions on a voice port.
test voice port switch	Forces a voice port into fax or voice mode.

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. <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. <i>subunit</i> specifies a voice interface card (VIC) in which the voice port is located. Valid entries are 0 and 1. <i>port</i> specifies an analog voice port number. Valid entries are 0 and 1.

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. <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. <i>port</i> specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1. <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.

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. <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. <i>port</i> specifies an analog voice port number. Valid entries are 1 to 6.

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. <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). <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.

All Platforms:

local	Forces a loopback at the voice port toward the customer premises equipment (CPE).
network	Forces a loopback at the voice port toward network.
disable	Ends the forced loopback.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(7)XK	This command was introduced on Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrators.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines Use the **test voice port loopback** privileged EXEC command to initiate or end a loopback at a voice port. A call must be established on the voice port under test. When you are finished testing, be sure to enter the **disable** keyword to end the forced loopback. The **disable** keyword is available only if a test condition is already activated.

Examples The following example forces a loopback toward the CPE on voice port 1/1 on a Cisco MC3810:

```
Router# test voice port 1/1 loopback local
```

The following example ends a forced loopback on port 0/0/1 on a Cisco 3600 series router:

```
Router# test voice port 0/0/1 loopback disable
```

Related Commands	Command	Description
	test voice port detector	Tests detector-related functions on a voice port.
	test voice port inject-tone	Injects a test tone into a voice port.
	test voice port relay	Tests relay-related functions on a voice port.
	test voice port switch	Forces a voice port into fax or voice mode.

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. <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. <i>subunit</i> specifies a voice interface card (VIC) in which the voice port is located. Valid entries are 0 and 1. <i>port</i> specifies an analog voice port number. Valid entries are 0 and 1.

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. <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. <i>port</i> specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1. <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.

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. <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. <i>port</i> specifies an analog voice port number. Valid entries are 1 to 6.

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. <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). <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.

All Platforms:

e-lead	Forces the E&M e-lead relay to the specified state.
loop	Forces the FXO loop relay to the specified state.
ring-ground	Forces the FXO ring-ground relay to the specified state.
battery-reversal	Forces the FXO battery-reversal relay to the specified state.
power-denial	Forces the FXS power-denial relay to the specified state.
ring	Forces the FXS ringing relay to the specified state.
tip-ground	Forces the FXS tip-ground relay to the specified state.
on	Forces the selected item to the on state.
off	Forces the selected item to the off state.
disable	Ends the forced state for the selected item.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(7)XK	This command was introduced on Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrators.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use the **test voice port relay** privileged EXEC command to force a relay into specific states for testing. For each signaling type (E&M, FXO, FXS), only the applicable keywords are displayed. When you are finished testing, be sure to enter the **disable** keyword to end the forced state. The **disable** keyword is available only if a test condition is already activated.

Examples

The following example forces the E&M e-lead relay to the on state on port 0/0/1 on a Cisco 3600 series router:

```
Router# test voice port 0/0/1 relay e-lead on
```

The following example ends a forced actuation of the battery-reversal relay on an FXS port (0/0/1) on a Cisco 3600 series router:

```
Router# test voice port 0/0/1 relay battery-reversal disable
```

Related Commands

Command	Description
test voice port detector	Tests detector-related functions on a voice port.
test voice port inject-tone	Injects a test tone into a voice port.
test voice port switch	Forces a voice port into fax or voice mode.

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. <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. <i>subunit</i> specifies a voice interface card (VIC) in which the voice port is located. Valid entries are 0 and 1. <i>port</i> specifies an analog voice port number. Valid entries are 0 and 1.

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. <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. <i>port</i> specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1. <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.

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. <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. <i>port</i> specifies an analog voice port number. Valid entries are 1 to 6.

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.
	<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). <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.

For All Platforms:

fax	Forces a switch to fax mode.
disable	Ends fax mode; switches back to voice mode.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XK	This command was introduced on Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrators.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use the **test voice port switch** privileged EXEC command to force a voice port into fax mode for testing. If no fax data is detected by the voice port, the voice port remains in fax mode for 30 seconds and then reverts automatically to voice mode. After you enter the **test voice port switch fax** command, you can use the **show voice call** or **show voice call summary** command to check whether the voice port is able to operate in fax mode.

The **disable** keyword ends the forced mode switch; however, the fax mode ends automatically after 30 seconds. The **disable** keyword is available only while the voice port is in fax mode.

Examples

The following example forces voice port 1/3 on a Cisco MC3810 into fax mode:

```
Router# test voice port 1/3 switch fax
```

The following example returns voice port 0/0/1 on a Cisco 3600 series router to voice mode:

```
Router# test voice port 0/0/1 switch disable
```

Related Commands

Command	Description
show voice call	Displays the call processing and protocol state-machine information for a voice port.
show voice call summary	Displays a summary of the call processing and protocol state-machine information for a voice port.

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 voice feature card (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.
	channel	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.
	all	Indicates that all 96 DSPs on the VFC installed in the defined slot will be busied out.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(7)T	This command was introduced on Cisco AS5800 universal access servers.

Usage Guidelines Use the **test vrm busyout** command to busy out either one specific DSP or a range of DSPs on a specific VFC. In addition, you can use this command to busy out a particular channel on a specified DSP or range of DSPs. To restore the activity of the busied-out DSPs, use the **test vrm unbusyout** command.

Examples The following example busies out all of the DSPs and associated channels for the VFC located in slot 4:

```
Router# test vrm busyout 4 all
```

The following example busies out all of the channels from DSP1 to DSP3 for the VFC located in slot 4:

```
Router# test vrm busyout 4 1 3
```

The following example busies out only channel 2 of DSP1 for the VFC located in slot 4:

```
Router# test vrm busyout 4 1 channel 2
```

 test vrm busyout**Related Commands**

Command	Description
test vrm unbusyout	Restores activity to a busied-out DSP or busied-out channels on a DSP.

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 voice feature card (VFC) is installed.
	<i>dsp-number</i>	Number that identifies the DSP to be reset.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.0(7)T	This command was introduced on the Cisco AS5300.

Usage Guidelines	Use the test vrm reset command to send a hard reset command to an identified DSP. When this command is used, any active calls on all channels associated with this DSP are dropped. Under most circumstances, you will never need to use this command.

Examples	The following example resets DSP 4 on the VFC installed in slot 2:

```
Router# test vrm reset 2 4
Resetting voice device may terminate active calls [confirm]
Reset command sent to voice card 4 for voice device 2.
```

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 voice feature card (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.
channel	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.
all	Indicates that all 96 DSPs on the VFC installed in the defined slot will be restored.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5300.

Usage Guidelines

Use the **test vrm unbusyout** command to restore either one specific DSP or a range of DSPs on a specific VFC. In addition, you can use this command to restore a particular channel on a specified DSP or range of DSPs. To busy out a DSP (or range of DSPs) or to busy out a particular channel, use the **test vrm busyout** command.

Examples

The following example restores the activity of all DSPs and associated channels for the VFC located in slot 4:

```
Router# test vrm unbusyout 4 all
```

The following example restores the activity of all channels on the DSP from DSP1 to DSP3 for the VFC located in slot 4:

```
Router# test vrm unbusyout 4 1 3
```

The following example restores the activity of only channel 2 of DSP1 for the VFC located in slot 4:

```
Router# test vrm unbusyout 4 1 channel 2
```

Related Commands

Command	Description
test vrm busyout	Busy outs a specific DSP or channels on a specific DSP.

threshold noise

To configure a noise threshold for incoming calls, use the **threshold noise** command in voice-port configuration mode. To restore the default, use the **no** form of this command.

threshold noise {*value*}

no threshold noise {*value*}

Syntax Description	<i>value</i>	Number that establishes a noise threshold. Valid values are from -30 to -90 decibels (dBs). The default value is -62 dB.

Defaults	-62dB

Command Modes	Voice-port configuration

Command History	Release	Modification
	12.2(16)	This command was introduced on the following platforms: Cisco 1700 Cisco 1751, Cisco 2600 (with and without the NM-HDA), Cisco 3600 (with and without the NM-HDA), Cisco 7200 (with and without the NM-HDA), Cisco AS5300, Cisco AS5800, and Cisco MC3810.

Usage Guidelines	Cisco voice activity detection (VAD) has two layers: application programming interface (API) layer and processing layer. There are 3 states that the processing layer classifies incoming signals: speech, unknown, and silence. The state of the incoming signals is determined by the noise threshold.
	In earlier Cisco IOS Releases, the noise threshold is fixed between -62dB and -78 dB. If the voice level is below the noise threshold, then the signal is classified as silence. If the incoming signal cannot be classified, the variable thresholds that are computed with the statistics of speech and noise that VAD gathers is used to make a determination. If the signal still cannot be classified, then it is marked as unknown. The final decision is made by the API. For applications such as hoot-n-holler, you could have the noise create unwanted spurious packets (for example, a voice stream) taking up bandwidth.
	With Cisco IOS Release 12.2(16), the noise threshold is configurable using the threshold noise command.

Examples	The following sample configuration shows a noise threshold level of -50 dB configured on a Cisco 3600:

```
voice-port 1/0/0
 threshold noise -50
```

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.

Defaults	60 seconds

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(9)T	This command was introduced on Cisco 3600 series routers.
	12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.

Usage Guidelines	This command applies to Cisco 3600 series routers. To disable the timeouts call-disconnect timer, set the seconds value to 0. Use the timeouts call-disconnect command to specify the number of seconds for which the originating end system waits after receiving disconnect before notifying the user to hang up by playing a fast busy tone. During this duration, the user just hears silence. If the command is disabled by setting the value to 0, the user hears silence indefinitely.

Examples	The following example sets a call-disconnect timeout value of 10 seconds on a Cisco 3600 series router voice port: voice-port 1/0/0 timeouts call-disconnect 10

Related Commands	Command	Description
	timeouts initial	Configures the initial digit timeout value for a specified voice port.
	timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
	timing delay-duration	Configures the delay dial signal duration for a specified voice port.

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*

Syntax Description	<i>seconds</i>	Initial timeout duration, in seconds. Valid entries are any integer from 0 to 120.

Defaults	10 seconds

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on Cisco 3600 series routers.

Usage Guidelines

Use the **timeouts initial** command to specify the number of seconds for which the system will wait for the caller to input the first digit of the dialed digits. The timeouts initial timer is activated when the call is accepted and is deactivated when the caller inputs the first digit. If the configured timeout value is exceeded, the caller is notified through the appropriate tone and the call is terminated.

To disable the timeouts initial timer, set the *seconds* value to 0.

Examples

The following example sets the initial digit timeout value on the Cisco 3600 series to 10 seconds:

```
voice-port 1/0/0
  timeouts initial 10
```

The following example sets the initial digit timeout value on the Cisco MC3810 multiservice concentrator to 10 seconds:

```
voice-port 1/1
  timeouts initial 10
```

Related Commands	Command	Description
	timeouts interdigit	Configures the interdigit timeout value for a specified voice port.

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*

Syntax Description	<i>seconds</i>	Interdigit timeout duration, in seconds. Valid entries are any integer from 0 to 120.

Defaults	10 seconds

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on Cisco 3600 series routers.

Usage Guidelines	This command applies to both the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator. Use the timeouts interdigit command to specify the number of seconds for which the system will wait (after the caller has input the initial digit) for the caller to input a subsequent digit of the dialed digits. The timeouts interdigit timer is activated when the caller inputs a digit and is restarted each time the caller inputs another digit until the destination address is identified. If the configured timeout value is exceeded before the destination address is identified, the caller is notified through the appropriate tone and the call is terminated. To disable the timeouts interdigit timer, set the <i>seconds</i> value to 0.

Examples	The following example sets the interdigit timeout value on the Cisco 3600 series for 10 seconds: <pre>voice-port 1/0/0 timeouts interdigit 10</pre> The following example sets the interdigit timeout value on the Cisco MC3810 multiservice concentrator for 10 seconds: <pre>voice-port 1/1 timeouts interdigit 10</pre>

■ timeouts interdigit**Related Commands**

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.

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

Syntax Description	<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.
	infinity	Ringing continues until the caller goes on-hook.

Defaults	180 seconds

Command Modes	Voice-port configuration

Command History	Release	Modification
	12.0(7)XK	This command was introduced on Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrators.
	12.1(2)T	This command was integrated into Cisco Release 12.1(2)T.

Usage Guidelines	The timeouts ringing command provides the capability to limit the length of time for which a caller can continue ringing a telephone when there is no answer.

Examples	The following example configures voice port 1/1 on a Cisco MC3810 to allow ringing for 600 seconds:

```
voice-port 1/1
  timeouts ringing 600
```

The following example configures voice port 0/0/1 on a Cisco 3600 series router to allow ringing for 600 seconds:

```
voice-port 0/0/1
  timeouts ringing 600
```

Related Commands	Command	Description
	timeouts initial	Configures the initial digit timeout value for a voice port.
	timeouts interdigit	Configures the interdigit timeout value for a voice port.

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.
infinity	The voice port is never released as long as the call-failure state remains.

Defaults

30 seconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1) MA	This command was introduced on the Cisco MC3810 series.
12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series routers.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use the **timeouts wait-release** command to limit the time a voice port can be held in a call failure state. After the timeout, the release sequence is enabled.

You can also use this command for voice ports with Foreign Exchange Station (FXS) loop-start signaling to specify the time allowed for a caller to hang up before the voice port goes into the parked state.

Examples

The following example configures voice port 1/1 on a Cisco MC3810 to stay in the call-failure state for 180 seconds while a busy tone, reorder tone, or out-of-service tone is sent to the voice port:

```
voice-port 1/1
  timeouts wait-release 180
```

The following example configures voice port 0/0/1 on a Cisco 3600 series router to stay in the call-failure state for 180 seconds while a busy tone, reorder tone, or out-of-service tone is sent to the voice port:

```
voice-port 0/0/1
  timeouts wait-release 180
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a voice port.
timeouts interdigit	Configures the interdigit timeout value for a voice port.

timers

To configure the Session Initiation Protocol (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*}

Syntax Description

trying <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.
connect <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.
disconnect <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.
expires <i>number</i>	Time (in milliseconds) for which an INVITE request is valid. Possible values are 60,000 through 300,000. The default is 180,000.

Defaults

The default for trying, connect, and disconnect is 500. The default for expires is 180,000.

Command Modes

SIP user agent configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on Cisco 2600 and 3600 series routers and Cisco AS5300 universal access servers.
12.1(3)T	This command was modified to change the names of the parameters. Two of the parameters (invite-wait-180 and invite-wait-200) were combined into one (trying).

Usage Guidelines

If you used the previous version of this command to configure timers, your previous timer settings will be maintained. The output of the **show running configuration** command will reflect both timers.

To reset this command to the default value, you can also use the **default** command.

Examples

The following example configures the SIP signaling timers to wait 500 milliseconds for a 100 response to an INVITE request:

```
sip-ua
 timers trying 500
```

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*

Syntax Description	<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.

Defaults	400 milliseconds

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on Cisco 2600 and 3600 series routers.

Examples	The following example configures the clear-wait duration on a Cisco 3600 series voice port to 300 milliseconds: voice-port 1/0/0 timing clear-wait 300
	The following example configures the clear-wait duration on a Cisco MC3810 multiservice concentrator voice port to 300 milliseconds: voice-port 1/1 timing clear-wait 300

Related Commands	Command	Description
	timeouts initial	Configures the initial digit timeout value for a specified voice port.
	timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
	timeouts wait-release	Configures the timeout value for releasing voice ports on the Cisco MC3810 multiservice concentrator.
	timing delay-duration	Specifies the delay signal duration for a specified voice port.
	timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
	timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
	timing digit	Specifies the DTMF digit signal duration for a specified voice port.
	timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
	timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing pulse	Specifies the pulse dialing rate for a specified voice port.
	timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
	timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
	timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

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*

Syntax Description	<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.

Defaults	2000 milliseconds

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on Cisco 3600 series routers.

Usage Guidelines	The call direction for the timing delay-duration command is out.

Examples	The following example configures the delay signal duration on a Cisco 3600 series voice port for 3000 milliseconds:

```
voice-port 1/0/0
 timing delay-duration 3000
```

The following example configures the delay signal duration on a Cisco MC3810 multiservice concentrator voice port for 3000 milliseconds:

```
voice-port 1/1
 timing delay-duration 3000
```

Related Commands	Command	Description
	timeouts initial	Configures the initial digit timeout value for a specified voice port.
	timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
	timeouts wait-release	Configures the timeout value for releasing voice ports on the Cisco MC3810 multiservice concentrator.
	timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
	timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
	timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
	timing digit	Specifies the DTMF digit signal duration for a specified voice port.
	timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
	timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing pulse	Specifies the pulse dialing rate for a specified voice port.
	timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
	timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
	timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing delay-start

To specify the minimum delay time from outgoing seizure to out-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*

Syntax Description	<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.

Defaults	300 milliseconds on the Cisco 3600 series. 150 milliseconds on the Cisco MC3810 multiservice concentrator.

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on Cisco 3600 series routers.

Usage Guidelines	The call direction for the timing delay-start command is out.

Examples	The following example configures the delay-start duration on a Cisco 3600 series voice port for 250 milliseconds: voice-port 1/0/0 timing delay-start 250
	The following example configures the delay-start duration on a Cisco MC3810 multiservice concentrator voice port for 250 milliseconds: voice-port 1/1 timing delay-start 250

Related Commands	Command	Description
	timeouts initial	Configures the initial digit timeout value for a specified voice port.
	timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
	timeouts wait-release	Configures the timeout value for releasing voice ports on the Cisco MC3810 multiservice concentrator.
	timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
	timing delay-duration	Specifies the delay signal duration for a specified voice port.
	timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
	timing digit	Specifies the DTMF digit signal duration for a specified voice port.
	timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
	timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing pulse	Specifies the pulse dialing rate for a specified voice port.
	timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
	timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
	timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

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*

Syntax Description	<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.

Defaults	Zero (0)

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)MA	This command was introduced on Cisco MC3810 multiservice concentrators.

Usage Guidelines	This command applies only to the Cisco MC3810 multiservice concentrator.

Examples	The following example configures the duration of the wink pulse for the delay dial on a Cisco MC3810 voice port for 10 milliseconds:

```
voice-port 1/1
 timing delay-with-integrity 10
```

Related Commands	Command	Description
	timeouts initial	Configures the initial digit timeout value for a specified voice port.
	timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
	timeouts wait-release	Configures the timeout value for releasing voice ports on the Cisco MC3810 multiservice concentrator.
	timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
	timing delay-duration	Specifies the delay signal duration for a specified voice port.
	timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
	timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
	timing digit	Specifies the DTMF digit signal duration for a specified voice port.
	timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
	timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing pulse	Specifies the pulse dialing rate for a specified voice port.
	timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
	timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
	timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

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*

Syntax Description	<i>milliseconds</i>	Time, in milliseconds, between the generation of wink-like pulses. Valid entries are integers from 0 to 5000.

Defaults	300 milliseconds

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on Cisco 3600 series routers.

Usage Guidelines	Use the timing dial-pulse min-delay command with PBXs that require a wink-like pulse, even though they have been configured for delay-dial signaling. If the value for this argument is set to 0, the router will not generate this wink-like pulse. The call signal direction for this command is in.

Examples	The following example configures the time between the generation of wink-like pulses on a Cisco 3600 series voice port for 350 milliseconds:

```
voice-port 1/0/0
 timing dial-pulse min-delay 350
```

Related Commands	Command	Description
	timeouts initial	Configures the initial digit timeout value for a specified voice port.
	timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
	timeouts wait-release	Configures the timeout value for releasing voice ports on the Cisco MC3810 multiservice concentrator.
	timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
	timing delay-duration	Specifies the delay signal duration for a specified voice port.
	timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
	timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing digit	Specifies the DTMF digit signal duration for a specified voice port.
	timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
	timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing pulse	Specifies the pulse dialing rate for a specified voice port.
	timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
	timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
	timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

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*

Syntax Description	<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.

Defaults	300 milliseconds

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)MA	This command was introduced on Cisco MC3810 multiservice concentrators.

Usage Guidelines	This command applies only to the Cisco MC3810 multiservice concentrator.

Examples	The following example configures the dial-out delay on a Cisco MC3810 multiservice concentrator voice port for 350 milliseconds:

```
voice-port 1/1
 timing dialout-delay 350
```

Related Commands	Command	Description
	timeouts initial	Configures the initial digit timeout value for a specified voice port.
	timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
	timeouts wait-release	Configures the timeout value for releasing voice ports on the Cisco MC3810 multiservice concentrator.
	timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
	timing delay-duration	Specifies the delay signal duration for a specified voice port.
	timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
	timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
	timing digit	Specifies the DTMF digit signal duration for a specified voice port.
	timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
	timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing pulse	Specifies the pulse dialing rate for a specified voice port.
	timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
	timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
	timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing digit

To specify the dual tone multifrequency (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*

Syntax Description	<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.	
Defaults	100 milliseconds	
Command Modes	Voice-port configuration	
Command History	Release	Modification
	11.3(1)T	This command was introduced on Cisco 3600 series routers.
Usage Guidelines	The call signal direction for the timing digit command is out.	
Examples	The following example configures the DTMF digit signal duration on a Cisco 3600 series voice port for 50 milliseconds:	
	<pre>voice-port 1/0/0 timing digit 50</pre>	
Examples	The following example configures the DTMF digit signal duration on a Cisco MC3810 multiservice concentrator voice port for 50 milliseconds:	
	<pre>voice-port 1/1 timing digit 50</pre>	

Related Commands	Command	Description
	timeouts initial	Configures the initial digit timeout value for a specified voice port.
	timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
	timeouts wait-release	Configures the timeout value for releasing voice ports on the Cisco MC3810 multiservice concentrator.
	timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
	timing delay-duration	Specifies the delay signal duration for a specified voice port.
	timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
	timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
	timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
	timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing pulse	Specifies the pulse dialing rate for a specified voice port.
	timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
	timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
	timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

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

Syntax Description	<i>milliseconds</i>	Duration, in milliseconds, of the guard-out period. The range is 300 to 3000. The default is 2000.

Defaults	2000 milliseconds

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator
	12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series routers.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines	The timing guard-out command applies to the Cisco 2600, 3600, and MC3810 multiservice concentrator. This command is supported on FXO voice ports only.

Examples	The following example configures the timing guard-out duration on a Cisco MC3810 multiservice concentrator voice port for 1000 milliseconds:

```
voice-port 1/1
 timing guard-out 1000
```

The following example configures the timing guard-out duration on a Cisco 2600 or 3600 series voice port for 1000 milliseconds:

```
voice-port 1/0/0
 timing guard-out 1000
```

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 voice-port configuration mode. To restore the default duration for hookflash timing, use the **no** form of this command.

timing hookflash-input *milliseconds*

no timing hookflash-input

Syntax Description	<i>milliseconds</i> Duration of the hookflash, in milliseconds. Possible values are 50 through 1550 milliseconds. Default is 600 milliseconds.					
Defaults	600 milliseconds					
Command Modes	Voice-port configuration					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.1(1)T</td><td>This command was introduced on the Cisco 3600 series.</td></tr></table>		Release	Modification	12.1(1)T	This command was introduced on the Cisco 3600 series.
Release	Modification					
12.1(1)T	This command was introduced on the Cisco 3600 series.					
Usage Guidelines	This command does <i>not</i> affect whether hookflash relay is enabled; hookflash relay is enabled only when the dtmf-relay h245-signal command is configured on the applicable VoIP dial peers. When the dtmf-relay h245-signal command is configured, the H.323 gateway relays hookflash by using an H.245 “signal” User Input Indication method. Hookflash is sent only when an h245 signal is available. Use the timing hookflash-input command on FXS interfaces to specify the maximum duration (in milliseconds) of a hookflash indication. If the hookflash lasts longer than the specified limit, the FXS interface processes the indication as an on-hook.					
Examples	The following example implements timing for the hookflash with a duration of 200 milliseconds: <pre>voice-port 1/0/0 timing hookflash-input 200</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>dtmf-relay (Voice over IP)</td><td>Specifies how an H.323 gateway relays DTMF tones between telephony interfaces and an IP network.</td></tr></table>		Command	Description	dtmf-relay (Voice over IP)	Specifies how an H.323 gateway relays DTMF tones between telephony interfaces and an IP network.
Command	Description					
dtmf-relay (Voice over IP)	Specifies how an H.323 gateway relays DTMF tones between telephony interfaces and an IP network.					

timing hookflash-out

To specify the duration of hookflash indications that the gateway generates on a Foreign Exchange Office (FXO) interface, use the **timing hookflash-out** command in voice-port configuration mode. To restore the default duration for hookflash timing, use the **no** form of this command.

timing hookflash-out *milliseconds*

no timing hookflash-out

Syntax Description	<i>milliseconds</i>	Duration of the hookflash, in milliseconds. Possible values are 50 through 1550 milliseconds.

Defaults	400 milliseconds

Command Modes	Voice-port configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced on Cisco 2500, Cisco 2600, Cisco 3600, and Cisco 7200 series routers and Cisco MC3810 multiservice concentrators.

Usage Guidelines	This command does <i>not</i> affect whether hookflash relay is enabled; hookflash relay is enabled only when the dtmf-relay h245-signal command is configured on the applicable Voice over IP (VoIP) dial peers. Hookflash is relayed by using an h245-signal indication and can be sent only when an h245 signal is available.
	Use the timing hookflash-out command on FXO interfaces to specify the duration (in milliseconds) of a hookflash indication. To set hookflash timing parameters for analog voice interfaces, use the voice-port timing subcommand.

Examples	The following example implements timing for the hookflash with a duration of 200 milliseconds:
	<pre>Router# voice-port 1/0/0 timing hookflash-out 200</pre>

Related Commands	Command	Description
	dtmf-relay (Voice over IP)	Specifies how an H.323 gateway relays DTMF tones between telephony interfaces and an IP network.
	voice-port	Enters voice-port configuration mode.

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*

Syntax Description	<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.

Defaults	100 milliseconds

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on Cisco 3600 series routers.
	11.3(1)MA	This command was supported on Cisco MC3810 multiservice concentrators.

Usage Guidelines	The call signal direction for the timing interdigit command is out.

Examples	The following example configures the DTMF interdigit duration on a Cisco 3600 series voice port for 150 milliseconds:

```
voice-port 1/0/0
 timing interdigit 150
```

The following example configures the DTMF interdigit duration on a Cisco MC3810 multiservice concentrator voice port for 150 milliseconds:

```
voice-port 1/1
 timing interdigit 150
```


Related Commands	Command	Description
	timeouts initial	Configures the initial digit timeout value for a specified voice port.
	timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
	timeouts wait-release	Configures the timeout value for releasing voice ports on the Cisco MC3810 multiservice concentrator.
	timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
	timing delay-duration	Specifies the delay signal duration for a specified voice port.
	timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
	timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
	timing digit	Specifies the DTMF digit signal duration for a specified voice port.
	timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing pulse	Specifies the pulse dialing rate for a specified voice port.
	timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
	timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
	timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

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

Syntax Description	<i>percent</i>	Percentage of the break period for dialing pulses. Valid entries are from 20 to 80. The default is 50.

Defaults	50 percent

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)MA4	This command was introduced on the Cisco MC3810 multiservice concentrator.
	12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series routers.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines	The timing percentbreak command is supported on Foreign Exchange Office (FXO) and ear and mouth (E&M) voice ports only.

Examples	The following example configures the break period percentage on a Cisco MC3810 multiservice concentrator voice port for 30 percent:
	<pre>voice-port 1/1 timing percentbreak 30</pre>
	The following example configures the break period percentage on a Cisco 2600 or 3600 voice port for 30 percent:
	<pre>voice-port 0/0/1 timing percentbreak 30</pre>

Related Commands	Command	Description
	timing pulse	Configures the pulse dialing rate for a voice port.
	timing pulse-interdigit	Configures the pulse interdigit timing for a voice port.

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*

Syntax Description	<i>pulses-per-second</i>	Pulse dialing rate, in pulses per second. Valid entries are numbers from 10 to 20. Supported on Foreign Exchange Office (FXO) and ear and mouth (E&M) ports only.

Defaults	20 pulses per seconds

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on Cisco 3600 series routers.
	11.3(1)MA	This command was supported on Cisco MC3810 multiservice concentrators.

Usage Guidelines	The call signal direction for the timing pulse command is out.

Examples	The following example configures the pulse dialing rate on a Cisco 3600 series voice port for 15 pulses per second:

```
voice-port 1/0/0
 timing pulse 15
```

The following example configures the pulse dialing rate on a Cisco MC3810 multiservice concentrator voice port for 15 pulses per second:

```
voice-port 1/1
 timing pulse 15
```

Related Commands	Command	Description
	timeouts initial	Configures the initial digit timeout value for a specified voice port.
	timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
	timeouts wait-release	Configures the timeout value for releasing voice ports on the Cisco MC3810 multiservice concentrator.

Command	Description
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port on the Cisco MC3810 multiservice concentrator.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port on the Cisco MC3810 multiservice concentrator.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port on the Cisco MC3810 multiservice concentrator.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

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	<i>milliseconds</i>	Pulse dialing interdigit timing, in milliseconds. Valid entries are integers from 100 to 1000. Supported on Foreign Exchange Office (FXO) and ear and mouth (E&M) ports only.
Defaults	500 milliseconds	
Command Modes	Voice-port configuration	
Command History	Release	Modification
	11.3(1)T	This command was introduced on Cisco 3600 series routers.
	11.3(1)MA	This command was supported on Cisco MC3810 multiservice concentrators.
Usage Guidelines	The call signal direction for the timing pulse-interdigit command is out.	
Examples	The following example configures the pulse-dialing interdigit timing on a Cisco 3600 series voice port for 300 milliseconds: <pre>voice-port 1/0/0 timing pulse-interdigit 300</pre> The following example configures the pulse-dialing interdigit timing on a Cisco MC3810 multiservice concentrator voice port for 300 milliseconds: <pre>voice-port 1/1 timing pulse-interdigit 300</pre>	

Related Commands	Command	Description
	timeouts initial	Configures the initial digit timeout value for a specified voice port.
	timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
	timeouts wait-release	Configures the timeout value for releasing voice ports on the Cisco MC3810 multiservice concentrator.
	timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
	timing delay-duration	Specifies the delay signal duration for a specified voice port.
	timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
	timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
	timing digit	Specifies the DTMF digit signal duration for a specified voice port.
	timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
	timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing pulse	Specifies the pulse dialing rate for a specified voice port.
	timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
	timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

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 ear and mouth (E&M) ports only.
Defaults	200 milliseconds	
Command Modes	Voice-port configuration	
Command History	Release	Modification
	11.3(1)T	This command was introduced on Cisco 3600 series routers.
	11.3(1)MA	This command was supported on Cisco MC3810 multiservice concentrators.
Usage Guidelines	The call signal direction for the timing wink-duration command is out.	
Examples	The following example configures the wink-signal duration on a Cisco 3600 series voice port for 300 milliseconds: <pre>voice-port 1/0/0 timing wink-duration 300</pre> The following example configures the wink-signal duration on a Cisco MC3810 multiservice concentrator voice port for 300 milliseconds: <pre>voice-port 1/1 timing wink-duration 300</pre>	

Related Commands	Command	Description
	timeouts initial	Configures the initial digit timeout value for a specified voice port.
	timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
	timeouts wait-release	Configures the timeout value for releasing voice ports on the Cisco MC3810 multiservice concentrator.
	timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
	timing delay-duration	Specifies the delay signal duration for a specified voice port.
	timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
	timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing delay-with-integrity	Specifies the time between wink-like pulses for a specified voice port.
	timing digit	Specifies the DTMF digit signal duration for a specified voice port.
	timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
	timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port on the Cisco MC3810 multiservice concentrator.
	timing pulse	Specifies the pulse dialing rate for a specified voice port.
	timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
	timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

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	<i>milliseconds</i>	Maximum wink-wait duration, in milliseconds, for a wink start signal. Valid entries are from 100 to 5000 milliseconds. Supported on ear and mouth (E&M) ports only.

Defaults	200 milliseconds

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on Cisco 3600 series routers.
	11.3(1)MA	This command was supported on Cisco MC3810 multiservice concentrators.

Usage Guidelines	The call signal direction for the timing wink-wait command is out.

Examples	The following example configures the wink-wait duration on a Cisco 3600 series voice port for 300 milliseconds: <pre>voice-port 1/0/0 timing wink-wait 300</pre>
	The following example configures the wink-wait duration on a Cisco MC3810 multiservice concentrator voice port for 300 milliseconds: <pre>voice-port 1/1 timing wink-wait 300</pre>

Related Commands	Command	Description
	timeouts initial	Configures the initial digit timeout value for a specified voice port.
	timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
	timeouts wait-release	Configures the timeout value for releasing voice ports on the Cisco MC3810 multiservice concentrator.
	timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.

Command	Description
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port on the Cisco MC3810 multiservice concentrator.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port on the Cisco MC3810 multiservice concentrator.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port on the Cisco MC3810 multiservice concentrator.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.

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 crypto ca identity <i>name</i> command or the crypto ca trusted-root <i>name</i> command.

Defaults

The terminating gateway uses the CA certificate to validate the settlement token.

Command Modes

Settlement configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on Cisco 2600 and 3600 series routers and Cisco AS5300 and AS5800 universal access servers.

Examples

The following example defines the **token-root-name** as sample:

```
token-root-name sample
```

The following example shows new output for the **show settlement** command to display the value of the **token-root-name** command:

```
Settlement Provider 0
  Operation Status = UP
  Type = osp
  Address url = https://1.14.115.100:8444/
  Encryption = all (default)
  Token Root Name = sample
  Max Concurrent Connections = 20 (default)
  Connection Timeout = 3600 (s) (default)
  Response Timeout = 1 (s) (default)
  Retry Delay = 2 (s) (default)
  Retry Limit = 1 (default)
  Session Timeout = 86400 (s) (default)
  Customer Id = 1000
  Device Id = 2000
  Roaming = Disabled (default)
  Signed Token = On

  Number of Connections = 1
  Number of Transactions = 0
```

■ token-root-name

Related Commands	Command	Description
	crypto ca identity	Declares the Certificate Authority that your router should use.
	crypto ca trusted-root	Configures the root certificate that the server uses to sign the settlement tokens.
	show settlement	Displays the configuration for all settlement server transactions.

tone ringback alert-no-PI

To generate automatic ringback for the caller when no Progress Indicator (PI) alert has been received over the H.323 network, use the **tone ringback alert-no-PI** command in dial-peer configuration mode. To disable automatic ringback, use the **no** form of this command.

tone ringback alert-no-PI

no tone ringback alert-no-PI

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values

Command Modes	Dial-peer configuration

Command History	Release	Modification
	12.2(1)	This command was introduced on Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, and Cisco 7200 series routers and on the Cisco AS5300 and Cisco AS5800 universal access servers.

Usage Guidelines	The tone ringback alert-no-PI command is used to generate ringback in an H.323 network when the attached device (for example, an ISDN device) cannot.

Examples	The following example activates ringback for a VoIP dial peer numbered 322:

```
router(config)# dial-peer voice 322 voip
router(config-dial-peer)# tone ringback alert-no-PI
```

Related Commands	Command	Description
	progress_ind	Sets a specific PI in call Setup, Progress, or Connect messages from an H.323 VoIP gateway.

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	calling-number	Applies the translation rule to the inbound calling party number.
	called-number	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.

Defaults No default behavior or values.

Command Modes Voice-port configuration

Command History	Release	Modification
	12.0(7)XR1	This command was introduced for Voice over IP on the Cisco AS5300.
	12.0(7)XK	This command was first supported for Voice over IP on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 multiservice concentrator.
	12.1(1)T	This command was first supported on the T train for Voice over IP on the Cisco 1750, Cisco 2600 series, Cisco 3600 series, Cisco AS5300, Cisco 7200 series, and Cisco 7500 series.
	12.1(2)T	This command was first supported on the T train for Voice over IP on the Cisco MC3810 multiservice concentrator.

Examples The following example applies translation rule 21 to the POTS inbound calling party number:

```
translation-rule 21
 rule 1 555.% 1408555 subscriber international
 rule 2 7.% 1408555 abbreviated international
voice-port 0:1
 translate calling-number 21
```

The following example applies translation rule 20 to the POTS inbound called party number:

```
translation-rule 20
 rule 1 .%555.% 7 any abbreviated
voice-port 0:1
 translate called-number 20
```

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
show translation-rule	Displays the contents of all the rules that have been configured for a specific translation name.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

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	calling-number	Applies the translation rule to the outbound calling party number.
	called-number	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.

Defaults No default behavior or values.

Command Modes Dial-peer configuration

Command History	Release	Modification
	12.0(7)XR1	This command was introduced for Voice over IP on the Cisco AS5300.
	12.0(7)XK	This command was first supported for Voice over IP on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 multiservice concentrator.
	12.1(1)T	This command was first supported on the T train for Voice over IP on the Cisco 1750, Cisco 2600 series, Cisco 3600 series, Cisco AS5300, Cisco 7200 series, and Cisco 7500 series.
	12.1(2)T	This command was first supported on the T train for Voice over IP on the Cisco MC3810 multiservice concentrator.

Examples The following example applies translation rule 21 to the VoIP outbound calling number:

```
Translation-rule 21
rule 1 555.% 1408555 subscriber international
rule 2 7.% 1408555 abbreviated international
dial-peer voice 100 voip
translate-outgoing calling-number 21
```


The following example applies translation rule 20 to the VoIP called number:

```
translation-rule 20
 rule 1 .%555.% 7 any abbreviated
dial-peer voice 100 voip
 translate-outgoing called-number 20
```

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
show translation-rule	Displays the contents of all the rules that have been configured for a specific translation name.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

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.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced for Voice over IP on the Cisco AS5300.
12.0(7)XK	This command was first supported for the following voice technologies on the following platforms: - Voice over IP (Cisco 2600 series, Cisco 3600 series, Cisco MC3810 multiservice concentrator) - Voice over Frame Relay (Cisco 2600 series, Cisco 3600 series, Cisco MC3810 multiservice concentrator) - Voice over ATM (Cisco 3600 series, Cisco MC3810 multiservice concentrator)
12.1(1)T	This command was first supported on the T train for the following voice technology on the following platforms: Voice over IP (Cisco 1750, Cisco 2600 series, Cisco 3600 series, Cisco AS5300, Cisco 7200 series, and Cisco 7500 series)
12.1(2)T	This command was first supported on the T train for the following voice technologies on the following platforms: - Voice over IP (Cisco MC3810 multiservice concentrator) - Voice over Frame Relay (Cisco 2600 series, Cisco 3600 series, Cisco MC3810 multiservice concentrator) - Voice over ATM (Cisco 3600 series, Cisco MC3810 multiservice concentrator)

Usage Guidelines

This command applies to all translation rules.

Examples

The following example creates translation rule 21 and applies a rule to it:

```
translation-rule 21
rule 1 555.% 1408555 subscriber international
```

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
test translation-rule	Tests the execution of the translation rules on a specific name tag.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

transport

To configure the Session Initiation Protocol (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

udp	Configures the SIP user agent to receive SIP messages on UDP port 5060.
tcp	Configures the SIP user agent to receive SIP messages on TCP port 5060.

Defaults

Both UDP and TCP transport protocols are enabled.

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on Cisco 2600 and 3600 series routers and Cisco AS5300 universal access servers.
12.1(3)T	Support for access platforms was added.

Usage Guidelines

This command controls whether messages reach the SIP service provider interface (SPI).

Examples

The following example configures the SIP user agent to block reception of SIP signaling messages on the TCP socket:

```
sip-ua
 no transport tcp
```

Related Commands

Command	Description
sip-ua	Enables the SIP user-agent configuration commands, with which you configure the user agent.

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	1	Indicates the following lead configuration: - E—Output, relay to ground. - M—Input, referenced to ground.
	2	Indicates the following lead configuration: - E—Output, relay to SG. - M—Input, referenced to ground. - SB—Feed for M, connected to –48V. - SG—Return for E, galvanically isolated from ground.
	3	Indicates the following lead configuration: - E—Output, relay to ground. - M—Input, referenced to ground. - SB—Connected to –48V. - SG—Connected to ground.
	5	Indicates the following lead configuration: - E—Output, relay to ground. - M—Input, referenced to –48V.

Defaults	Type 1

Command Modes	Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on Cisco 3600 series routers.
	11.3(1)MA	This command was first supported on Cisco MC3810 multiservice concentrators.

Usage Guidelines

Use the **type** command to specify the E&M interface for a particular voice port. With **1**, the tie-line equipment generates the E-signal to the PBX type grounding the E-lead. The tie-line equipment detects the M-signal by detecting current flow to ground. If you select **1**, a common ground must exist between the line equipment and the PBX.

With **2**, the interface requires no common ground between the equipment, thereby avoiding ground loop noise problems. The E-signal is generated toward the PBX by connecting it to SG. The M-signal is indicated by the PBX connecting it to SB. While Type 2 interfaces do not require a common ground, they do have the tendency to inject noise into the audio paths because they are asymmetrical with respect to the current flow between devices.

**Note**

E&M Type 4 is not a supported option. However, Type 4 operates similarly to Type 2 except for the M-lead operation. On Type 4, the M-lead states are open/ground, compared to Type 2, which is open/battery. Type 4 can interface with Type 2. To use Type 4 you can set the E&M voice port to Type 2 and perform the necessary M-lead rewiring.

With **3**, the interface operates the same as Type 1 interfaces with respect to the E-signal. The M-signal, however, is indicated by the PBX connecting it to SB on assertion and alternately connecting it to SG during inactivity. If you select **3**, a common ground must be shared between equipment.

With **5**, the Type 5 line equipment indicates E-signal to the PBX by grounding the E-lead. The PBX indicates M-signal by grounding the M-lead. A Type 5 interface is quasi-symmetrical in that while the line is up, current flow is more or less equal between the PBX and the line equipment, but noise injection is a problem.

Examples

The following example selects Type 3 as the interface type for the voice port on the Cisco 3600 series:

```
voice-port 1/0/0
type 3
```

The following example selects Type 3 as the interface type for the voice port on the Cisco MC3810 multiservice concentrator:

```
voice-port 1/1
type 3
```

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	osp	Enables the Open Settlement Protocol (OSP) server type.
	uni-osp	Enables authentication of Voice over IP (VoIP) calls to the Public Switched Telephone Network (PSTN) using a single settlement server.

Defaults	osp

Command Modes	Settlement configuration

Command History	Release	Modification
	12.0(4)XH1	This command was introduced on Cisco 2600 and 3600 series routers and Cisco AS5300 universal access servers.
	12.1(2)T	The uni-osp keyword was introduced.

Usage Guidelines	This command defines the settlement server that is doing the accounting and enables the server to do the accounting.

Examples	The following example enables authentication of VoIP calls to the PSTN using a single settlement server:

```
settlement 0
  type uni-osp
```

Related Commands	Command	Description
	connection-timeout	Sets the connection timeout.
	customer-id	Sets the customer identification.
	device-id	Sets the device identification.
	encryption	Specifies the encryption method.
	max-connection	Sets the maximum simultaneous connections.
	response-timeout	Sets the response timeout.
	retry-delay	Sets the retry delay.
	retry-limit	Sets the connection retry limit.

Command	Description
session-timeout	Sets the session timeout.
settlement	Enters settlement configuration mode.
show settlement	Displays the configuration for all settlement server transactions.
shutdown/no shutdown	Brings up the settlement provider and then shuts it down.
url	Specifies the Internet service provider (ISP) address.

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

high-complexity	(Optional) Unbundles the high-complexity firmware set.
medium-complexity	(Optional) Unbundles the medium-complexity firmware set.
<i>slot-number</i>	Indicates the voice feature card (VFC) slot number.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco AS5300 universal access servers.
12.0(2)XH	The high-complexity and medium-complexity keywords were added.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

VFCs come with a single bundled image, VCWare, stored in VFC Flash memory. Use the **unbundle vfc** command to unbundle this bundled image into separate files, which are then written to Flash memory. When VCWare is unbundled, it automatically adds DSPWare to Flash memory, creates both the capability and default file lists, and populates these lists with the default files for that version of VCWare. The default file list includes the files that will be used to boot up the system. The capability list defines the available voice codecs for H.323 capability negotiation. These files are used during initial card configuration and for subsequent firmware upgrades.

Before unbundling a VFC software image that you have just copied over to VFC Flash, use the **clear vfc** command. Unbundling a DSP firmware set rewrites the default-file and capabilities lists. After unbundling, you must reload the router for any changes to take effect.

Examples

The following example unbundles the high-complexity firmware set into slot 2:

```
Router# unbundle high-complexity vfc 2
```

Related Commands

Command	Description
copy flash vfc	Copies a new version of VCWare from the Cisco AS5300 motherboard to VFC Flash memory.
copy tftp vfc	Copies a new version of VCWare from a TFTP server to VFC Flash memory.

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>	Specifies the URL address. A valid URL address is as follows: <i>http://fully qualified domain name[:port]/[URL]</i>

Defaults

No default behavior or values.

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on Cisco 2600 and 3600 series routers and Cisco AS5300 universal access servers.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

You can configure the address type multiple times. If you configure multiple URLs for the settlement server, the gateway attempts to send the request to each URL in the order in which you configured these addresses.

Examples

The following example configures four URLs for the settlement server:

```
settlement 0
url http://1.2.3.4/
url http://1.2.3.4:80/
url https://1.2.3.4:4444/
url https://yourcompany.com:443/
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.

Command	Description
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters settlement configuration mode.
show settlement	Displays the configuration for all settlement server transactions.
shutdown/no shutdown	Brings up the settlement provider and then shuts it down.
type	Specifies the provider type.

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.
default	Defines the default proxy policy for all calls that are not defined by a use-proxy command with the remote-zone keyword.
remote-zone <i>remote-zone-name</i>	Defines a proxy policy for calls to or from a specific remote gatekeeper or zone.
inbound-to	Applies the proxy policy to calls that are inbound to the local zone from a remote zone. Each use-proxy command defines the policy for only one direction.
outbound-from	Applies the proxy policy to calls that are outbound from the local zone to a remote zone. Each use-proxy command defines the policy for only one direction.
gateway	Defines the type of local device to which the policy applies. The gateway option applies the policy only to local gateways.
terminal	Defines the type of local device to which the policy applies. The terminal option applies the policy only to local terminals.

Defaults

The local zone uses proxy for both inbound and outbound calls to and from the local H.323 terminals only. Proxy is not used for both inbound and outbound calls to and from local gateways.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.0(5)T	This command was introduced on Cisco AS5300 universal access servers.

Usage Guidelines

This command replaces the **zone access** command used in the previous versions of the gatekeeper. When a previous version of gatekeeper is upgraded, any **zone access** commands are translated to **use-proxy** commands. You can use the **show gatekeeper zone status** command to see the gatekeeper proxy configuration.

Examples

In the following example, the local zone sj.xyz.com is configured to use a proxy for inbound calls from remote zones tokyo.xyz.com and milan.xyz.com to gateways in its local zone. The sj.xyz.com zone is also configured to use a proxy for outbound calls from gateways in its local zone to remote zones tokyo.xyz.com and milan.xyz.com.

```
use-proxy sj.xyz.com remote-zone tokyo.xyz.com inbound-to gateway
use-proxy sj.xyz.com remote-zone tokyo.xyz.com outbound-from gateway
use-proxy sj.xyz.com remote-zone milan.xyz.com inbound-to gateway
use-proxy sj.xyz.com remote-zone milan.xyz.com outbound-from gateway
```

Because the default mode disables proxy communications for all gateway calls, only the gateway call scenarios listed above can use the proxy.

In the following example, the local zone sj.xyz.com uses a proxy for only those calls that are outbound from H.323 terminals in its local zone to the specified remote zone germany.xyz.com:

```
no use-proxy sj.xyz.com default outbound-from terminal
use-proxy sj.xyz.com remote-zone germany.xyz.com outbound-from terminal
```

**Note**

Any calls inbound to H.323 terminals in the local zone sj.xyz.com from the remote zone germany.xyz.com use the proxy because the default applies.

The following example shows how to remove one or more proxy statements for the remote zone germany.xyz.com from the proxy configuration list:

```
no use-proxy sj.xyz.com remote-zone germany.xyz.com
```

The command above removes all special proxy configurations for the remote zone germany.xyz.com. After you enter a command like this, all calls between the local zone (sj.xyz.com) and germany.xyz.com are processed according to the defaults defined by any **use-proxy** commands that use the **default** option.

To prohibit proxy use for inbound calls to H.323 terminals in a local zone from a specified remote zone, enter a command similar to the following :

```
no use-proxy sj.xyz.com remote-zone germany.xyz.com inbound-to terminal
```

This command overrides the default and disables proxy use for inbound calls from remote zone germany.xyz.com to all H.323 terminals in the local zone sj.xyz.com.

Related Commands

Command	Description
show gatekeeper zone status	Displays the status of zones related to a gatekeeper.

vad (dial peer)

To enable voice activity detection (VAD) for the calls using a particular dial peer, use the **vad** command in dial-peer configuration mode. To disable VAD, use the **no** form of this command.

vad [aggressive]

no vad [aggressive]

Syntax Description

aggressive	Reduces noise threshold from –78 to –62 dBm. Available only when session protocol multicast is configured.

Defaults

VAD is enabled

Aggressive VAD is enabled in multicast dial peers

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.
12.0(4)T	This command was implemented as a dial-peer command on Cisco MC3810 (in prior releases, the vad command was available only as a voice-port command).
12.2(10)	The aggressive keyword was added.

Usage Guidelines

Use this command to enable voice activity detection. With VAD, voice data packets fall into three categories: speech, silence, and unknown. Speech and unknown packets are sent over the network; silence packets are discarded. The sound quality is slightly degraded with VAD, but the connection monopolizes much less bandwidth. If you use the **no** form of this command, VAD is disabled and voice data is continuously sent to the IP backbone. When configuring voice gateways to handle fax calls, VAD should be disabled at both ends of the IP network because it can interfere with the successful reception of fax traffic.

When the **aggressive** keyword is used, the VAD noise threshold is reduced from –78 to –62 dBm. Noise that falls below the –62 dBm threshold is considered to be silence and is not sent over the network. Additionally, unknown packets are considered to be silence and are discarded.

On the Cisco MC3810, VAD can also be assigned to the voice port using the **vad (voice-port)** command. On the Cisco MC3810 multiservice concentrator, if you enable VAD on the dial peer for Voice over Frame Relay switched calls or permanent calls, the dial-peer setting overrides the VAD setting on the voice port.



Note

On the Cisco MC3810, the **vad (dial-peer)** command is enabled by default. The **vad (voice-port)** command is disabled by default.

Examples

The following example enables VAD for a Voice over IP (VoIP) dial peer, starting from global configuration mode:

```
dial-peer voice 200 voip
vad
```

Related Commands

Command	Description
comfort-noise	Generates background noise to fill silent gaps during calls if VAD is activated.
dial-peer voice	Enters dial-peer configuration mode, defines the type of dial peer, and defines the tag number associated with a dial peer.
vad (voice-port)	Enables VAD for the calls using a particular voice port.

vad (voice-port)

To enable voice activity detection (VAD) for the calls using a particular 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.

Defaults VAD is not enabled.

Command Modes Voice-port configuration

Command History	Release	Modification
	11.3(1)MA	This command was introduced as a voice-port command on Cisco MC3810 multiservice concentrators.

Usage Guidelines This command applies to Voice over Frame Relay and Voice over ATM on Cisco MC3810 multiservice concentrators.

Use the **vad** command to enable voice activity detection. With VAD, silence is not sent over the network; only audible speech is sent. If you enable VAD, the sound quality will be slightly degraded but the connection will monopolize much less bandwidth. If you use the **no** form of this command, VAD is disabled on the voice port.



Note

It is recommended that you use the **vad** command in dial-peer configuration mode.

Examples The following example enables VAD:

```
voice-port 1/1
vad
```

Related Commands	Command	Description
	comfort-noise	Generates background noise to fill silent gaps during calls if VAD is activated.
	vad (dial peer)	Enables VAD for the calls using a particular dial peer.

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.

Defaults

No vbr-rt settings are configured.

Command Modes

ATM virtual circuit configuration

Command History

Release	Modification
12.0	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	Support for this command was extended to the Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The **vbr-rt** command configures traffic shaping between voice and data permanent virtual circuits (PVCs). Traffic shaping is required so that the carrier does not discard calls. To configure voice and data traffic shaping, you must configure the peak, average, and burst options for voice traffic. Configure the burst value if the PVC will be carrying bursty traffic. The peak, average, and burst values are needed so that the PVC can effectively handle the bandwidth for the number of voice calls. To calculate the *minimum* peak, average, and burst values for the number of voice calls, use the following calculations:

- Peak value: (2 x the maximum number of calls) x 16 kbps
- Average value: (1 x the maximum number of calls) x 16 kbps
- Burst value: (4 x the maximum number of calls)



Note

When you configure data PVCs that will be traffic shaped with voice PVCs, use the **encapsulation aal5 snap** command and calculate the overhead as 1.13 times the voice rate.

Examples

The following example configures the traffic shaping rate for ATM PVC 20 on a Cisco 3600. In the example, the peak, average, and burst rates are calculated based on a maximum of 20 calls on the PVC.

```
pvc 20
 encapsulation aal5mux voice
 vbr-rt 640 56 80
```

Related Commands

Command	Description
encapsulation	Configures the ATM adaptation layer (AAL) and encapsulation type for an ATM PVC class.

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		
data		(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 data is specified, enter a valid CID.
call-control		(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.

cisco	(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.
cid	(Optional) Specifies the subchannel to be used for call-control signaling. Valid values are from 4 to 255; the default is 5. If call-control is specified and a CID is not entered, the default CID will be used.

Defaults

Disabled

Command Modes

Frame relay DLCI configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on Cisco 2600, 3600, and 7200 series routers and Cisco MC3810 multiservice concentrators.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(7)XK	The use of the cisco option was modified. Beginning in this release, use the cisco option only when configuring connections to Cisco MC3810 concentrators running Cisco IOS Releases before 12.0(7)XK and 12.1(2)T.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Table 76 lists the different options of the **vofr** command and which combination of options is used beginning in Cisco IOS Release 12.0(7)XK and 12.1(2)T.

Table 76 Combinations of the vofr Command

Type of Call	Command Combination to Use
Switched call (user dialed or auto-ringdown) to other routers supporting VoFR	vofr [data cid] [call-control [cid]] ¹
Switched call (user dialed or auto-ringdown) to a Cisco MC3810 running Cisco IOS Releases before 12.0(7)XK and 12.1(2)T	vofr cisco ²

Table 76 Combinations of the **vofr** Command (continued)

Type of Call	Command Combination to Use
Cisco-trunk permanent call (private-line) to other routers supporting VoFR	vofr data <i>cid</i> call-control <i>cid</i>
Cisco-trunk permanent call (private-line) to a Cisco MC3810 running Cisco IOS Releases before 12.0(7)XK and 12.1(2)T	vofr cisco
FRF.11 trunk call (private-line) to other routers supporting VoFR	vofr [data <i>cid</i>] [call-control <i>cid</i>] ³

1. The recommended form of this command to use is **vofr data 4 call-control 5**.
2. This command consumes data CID 4 and call-control CID 5.
3. For FRF.11 trunk calls, the call-control option is not required. It is required only if you mix FRF.11 trunk calls with other types of voice calls on the same PVC.

Usage Restrictions for Cisco IOS Releases Before 12.0(7)XK and 12.1(2)T

This section describes restrictions for using the **vofr** command in releases before Cisco IOS Release 12.0(7)XK and 12.1(2)T. Beginning in Cisco IOS Release 12.0(7)XK and 12.1(2)T, these restrictions no longer apply.

When you use the **vofr** command without the **cisco** option, all subchannels on the DLCI are configured for FRF.11 encapsulation. If you enter the **vofr** command without any keywords or arguments, the data subchannel is CID 4 and there is no call-control subchannel.

[Table 77](#) describes special conditions and restrictions for the use of the **vofr** command on the Cisco MC3810 running releases before 12.0(7)XK and 12.1(2)T.

Table 77 Using the **vofr** Command with the Cisco MC3810 Multiservice Concentrator

Type of Call	Conditions and Restrictions
FRF.11 trunks	1. Do <i>not</i> use the cisco option or the call-control option. 2. Use vofr or vofr data <i>cid</i> .
Cisco trunks	1. Must use vofr cisco .
switched-vofr	1. Must use vofr cisco .

If you select the “data” option, enter a numeric value to complete the command. If you select the **call-control** option, you do not enter a numeric value if you wish to accept the default call-control subchannel. See the following examples for clarification.

When you use the **vofr** command on a Cisco MC3810 multiservice concentrator without the “cisco” option, switched calls are not permitted. You can make only permanent FRF.11-trunk calls.

**Note**

It is not possible to configure the **call-control** option on a Cisco MC3810 multiservice concentrator. If you configure this option, the setting is ignored.

Examples

The following example, beginning in global configuration mode, shows how to enable VoFR on serial interface 1/1, DLCI 100 on a Cisco 2600 series, 3600 series, or 7200 series router or on a Cisco MC3810 multiservice concentrator. The example configures CID 4 for data; no call-control CID is defined.

```
interface serial 1/1
 frame-relay interface-dlci 100
 vofr
```

To configure CID 4 for data and CID 5 for call-control (both defaults), enter the following command:

```
vofr call-control
```

To configure CID 10 for data and CID 15 for call-control, enter the following command:

```
vofr data 10 call-control 15
```

To configure CID 4 for data and CID 15 for call-control, enter the following command:

```
vofr call-control 15
```

To configure CID 10 for data and CID 5 for call-control, enter the following command:

```
vofr data 10 call-control
```

To configure CID 10 for data with no call-control, enter the following command:

```
vofr data 10
```

To configure a Cisco router or MC3810 for a VoFR application with an older release of the Cisco MC3810 (before Release 12.0(3)XG), enter the following command:

```
vofr cisco
```

Related Commands

Command	Description
class	Assigns a VC class to a PVC.
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface.

voice call convert-discpi-to-prog

To convert a disconnect message with a progress indicator (PI) to a progress message, use the **voice call convert-discpi-to-prog** command in global configuration mode. To restore the default, use the **no** form of this command.

voice call convert-discpi-to-prog

no voice call convert-discpi-to-prog

Syntax Description

This command has no arguments or keywords.

Defaults

A disconnect message with a PI is not converted to a progress message.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)	This command was introduced.

Usage Guidelines

In Cisco IOS Release 12.2(1), a disconnect message with a PI is always converted to a progress message, even if the disconnect with PI is received after the connect message.

Examples

The following example changes a disconnect with PI to a progress message:

```
voice call convert-discpi-to-prog
```

Related Commands

Command	Description
disc_pi_off	Enables an H.323 gateway to disconnect a call when it receives a disconnect message with a PI.

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.

Defaults

The terminating gateway sends a progress message after it receives a call Setup message.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)XI4	This command was introduced.
12.1(5)T	This command was not supported in this release.
12.1(5.3)T	This command was integrated into Cisco IOS Release 12.1(5.3)T.
12.2(1)	This command was integrated into Cisco IOS Release 12.2.

Usage Guidelines

In Cisco IOS Release 12.1(3)XI and later, the terminating gateway sends a Progress message with a progress indicator (PI) after it receives a Setup message. Previously, the gateway responded with an Alert message after receiving a call. In some cases, if the terminating switch does not forward the progress message to the originating gateway, the originating gateway does not cut-through the voice path until a Connect is received and the caller will not hear a ringback tone. In these cases, you can use the **voice call send-alert** command to make the gateway backward compatible with releases earlier than Cisco IOS Release 12.1(3)XI. If you configure the **voice call send-alert** command, the terminating gateway sends an Alert message after it receives a Setup message from the originating gateway.

To complete calls from a PRI to an FXS interface, configure the **voice call send-alert** command on the FXS device.

Examples

The following example configures the gateway to send an Alert message:

```
voice call send-alert
```

Related Commands

Command	Description
progress_ind	Sets a specific PI in call Setup, Progress, or Connect messages from an H.323 VoIP gateway.

voice-card

To configure a voice card, use the **voice-card** command in global configuration mode.

voice-card *slot*

Syntax Description	<i>slot</i>	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 multiservice concentrators with one or two HCMs installed, enter 0 only; this applies to the entire chassis.

Defaults	No default behavior or values.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(5)XK	The command was introduced for the Cisco 2600 and 3600 series.
	12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
	12.0(7)XK	This command was first supported on the Cisco MC3810 series.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines	You can configure codec complexity only in voice-card configuration mode. On the Cisco 2600 and 3600 series, the slot corresponds to the physical slot in the chassis. On the Cisco MC3810 series, the slot is always 0, and all changes made in voice-card configuration mode apply to the entire Cisco MC3810. On Cisco MC3810 series concentrators, this command is available only if the chassis is equipped with one or two HCMs.

Examples	The following example enters voice-card configuration mode for the voice card in slot 1 on a Cisco 2600 or 3600 router:

```
voice-card 1
```

The following example enters voice-card configuration mode on a Cisco MC3810 concentrator:

```
voice-card 0
```

Related Commands	Command	Description
	codec complexity	Matches the DSP complexity packaging to the codecs to be supported. Codec complexity changes are made in the voice-card configuration mode.

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	<i>tag</i>	A unique identification number assigned to one voice class. The range is 1 to 10,000.

Defaults	No voice class is configured for busyout functions.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrators.

Usage Guidelines	You can apply a busyout voice class to multiple voice ports. You can assign only one busyout voice class to a voice port. If a second busyout voice class is assigned to a voice port, the second voice class replaces the one previously assigned.

If you assign a busyout voice class to a voice port, you may not assign separate busyout commands directly to the voice port, such as **busyout monitor serial**, **busyout monitor ethernet**, or **busyout monitor probe**.

Examples	The following example configures busyout voice class 20, in which the connections to two remote interfaces are monitored by a response time reporter (RTR) probe with a G.711ulaw profile, and voice ports are busied out whenever both links have a packet loss exceeding 10 percent and a packet delay time exceeding 2 seconds:

```
voice class busyout 20
  busyout monitor probe 171.165.202.128 g711u loss 10 delay 2000
  busyout monitor probe 171.165.202.129 g711u loss 10 delay 2000
```

The following example configures busyout voice class 30, in which voice ports are busied out when serial ports 0/0, 1/0, 2/0, and 3/0 go out of service.

```
voice class busyout 30
  busyout monitor serial 0/0
  busyout monitor serial 1/0
  busyout monitor serial 2/0
  busyout monitor serial 3/0
```

Related Commands

Command	Description
busyout monitor ethernet	Configures a voice port to monitor a local Ethernet interface for events that would trigger a voice-port busyout.
busyout monitor probe	Configures a voice port to enter the busyout state if an RTR probe signal returned from a remote, IP-addressable interface crosses a specified delay or loss threshold.
busyout monitor serial	Configures a voice port to monitor a serial interface for events that would trigger a voice-port busyout.
show voice busyout	Displays information about the voice busyout state.

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

<i>tag</i>	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.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(2)XH	This command was introduced on the Cisco AS5300.
12.0(7)T	This command was first supported on the Cisco 2600 and Cisco 3600 series routers.
12.0(7)XK	This command was first supported on the Cisco MC3810 multiservice concentrator.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command only creates the voice class for codec selection preference and assigns an identification tag. Use the **codec preference** command to specify the parameters of the voice class, and use the **voice-class codec** dial-peer command to apply the voice class to a Voice over IP (VoIP) dial peer.



Note

The **voice class codec** command in global configuration mode is entered without the hyphen. The **voice-class codec** command in dial-peer configuration mode is entered with the hyphen.

Examples

The following example shows how to enter voice-class configuration mode and assign a voice class tag number starting from global configuration mode:

```
voice class codec 10
```

After you enter voice-class configuration mode for codecs, use the **codec preference** command to specify the parameters of the voice class.

The following example creates preference list 99, which can be applied to any dial peer:

```
voice class codec 99
  codec preference 1 g711alaw
  codec preference 2 g711ulaw bytes 80
  codec preference 3 g723ar53
  codec preference 4 g723ar63 bytes 144
  codec preference 5 g723r53
  codec preference 6 g723r63 bytes 120
  codec preference 7 g726r16
  codec preference 8 g726r24
  codec preference 9 g726r32 bytes 80
  codec preference 10 g728
  codec preference 11 g729br8
  codec preference 12 g729r8 bytes 50
```

Related Commands

Command	Description
codec preference	Specifies a list of preferred codecs to use on a dial peer.
test voice port detector	Defines the order of preference in which network dial peers select codecs.
voice-class codec (dial peer)	Assigns a previously configured codec selection preference list to a dial peer.

voice-class codec (dial peer)

To assign a previously configured codec selection preference list (codec voice class) to a Voice over IP (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*

Syntax Description

<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 voice class codec global configuration command.

Defaults

Dial peers have no codec voice class assigned.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.0(2)XH	This command was introduced on the Cisco AS5300.
12.0(7)T	This command was supported on the Cisco 2600 and 3600 series routers.
12.0(7)XK	This command was supported on the Cisco MC3810 multiservice concentrator.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

You can assign one voice class to each VoIP dial peer. If you assign another voice class to a dial peer, the last voice class assigned replaces the previous voice class.



Note

The **voice-class codec** command in dial-peer configuration mode is entered with the hyphen. The **voice class codec** command in global configuration mode is entered without the hyphen.

Examples

The following example shows how to assign a previously configured codec voice class to a dial peer:

```
dial-peer voice 100 voip
  voice-class codec 10
```

Related Commands	Command	Description
	show dial-peer voice	Displays the configuration for all dial peers configured on the router.
	test voice port detector	Defines the order of preference in which network dial peers select codecs.
	voice class codec	Enters voice-class configuration mode and assigns an identification tag number for a codec voice class.

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*

Syntax Description

<i>tag</i>	A unique identification number assigned to one voice class. The range is from 1 to 10,000.

Defaults

No voice class is configured for tone detection parameters.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrators.

Usage Guidelines

Use this command first to create the voice class. Then use the **supervisory disconnect dualtone voice-class** command to assign the voice class to a voice port.

A voice class can define any number of tones to be detected. You need to define a matching tone for each supervisory disconnect tone expected from a PBX or from the public switched telephone network (PSTN).

Examples

The following example configures voice class dualtone 70, which defines one tone with two frequency components, and does not configure a cadence list:

```
voice class dualtone 100
  freq-pair 1 350 440
  freq-max-deviation 10
  freq-max-power 6
  freq-min-power 25
  freq-power-twist 15
  freq-max-delay 16
  cadence-min-on-time 50
  cadence-max-off-time 400
  cadence-variation 8
exit
```


The following example configures voice class dualtone 100, which defines one tone with two frequency components, and configures a cadence list:

```
voice class dualtone 100
  freq-pair 1 350 440
  freq-pair 2 480 850
  freq-max-deviation 10
  freq-max-power 6
  freq-min-power 25
  freq-power-twist 15
  freq-max-delay 16
  cadence-min-on-time 50
  cadence-max-off-time 400
  cadence-list 1 100 100 300 300
  cadence-variation 8
exit
```

The following example configures voice class dualtone 90, which defines three tones, each with two frequency components, and configures two cadence lists:

```
voice class dualtone 90
  freq-pair 1 350 440
  freq-pair 2 480 850
  freq-pair 3 1000 1250
  freq-max-deviation 10
  freq-max-power 6
  freq-min-power 25
  freq-power-twist 15
  freq-max-delay 16
  cadence-min-on-time 50
  cadence-max-off-time 500
  cadence-list 1 100 100 300 300 100 200
  cadence-list 2 100 200 100 400
  cadence-variation 8
exit
```

Related Commands

Command	Description
supervisory disconnect dualtone voice-class	Assigns a previously configured voice class for FXO supervisory disconnect tone to a voice port.

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

Syntax Description

<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.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on Cisco 1700 routers, Cisco 2600, 3600 and 7200 series routers, Cisco AS5300 universal access servers, and Cisco uBR910 and uBR924 cable access routers.

Usage Guidelines

The **voice class h323** command in global configuration mode does not include a hyphen. The **voice-class h323** command in dial-peer configuration mode uses a hyphen.

Examples

The following example creates an H.323 voice class labeled 1:

```
voice class h323 1
```

Related Commands

Command	Description
h225 timeout tcp establish	Sets the H.225 TCP timeout value.

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*

Syntax Description	<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.

Defaults	The dial peer does not use an H.323 voice class.

Command Modes	Dial-peer configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced.

Usage Guidelines	The voice class that you assign to the dial peer must be configured using the voice class h323 in global configuration mode. The voice-class h323 command in dial-peer configuration mode uses a hyphen and in global configuration mode does not include a hyphen.

You can assign one voice class to each VoIP dial peer. If you assign another voice class to a dial peer, the last voice class assigned replaces the previous voice class.

Examples	The following example shows how to create an H.323 voice class and then assign it to a dial peer:

```
voice class h323 10
dial-peer voice 100 voip
 voice-class h323 10
```

Related Commands	Command	Description
	show dial-peer voice	Displays the configuration for all dial peers configured on the router.
	voice class h323	Enters voice-class configuration mode and assigns an identification tag number for an H.323 voice class.

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*

Syntax Description

<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.

Defaults

No voice class is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 series.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was first supported on the Cisco 2600 and 3600 series routers.

Usage Guidelines

The **voice class permanent** command can be used for Voice over Frame Relay (VoFR), Voice over ATM (VoATM), and Voice over IP (VoIP) trunks.



Note

The **voice class permanent** command in global configuration mode is entered without the hyphen. The **voice-class permanent** command in dial-peer and voice-port configuration modes is entered with the hyphen.

Examples

The following example shows how to create a permanent voice class starting from global configuration mode:

```
voice class permanent 10
  signal keepalive 3
exit
```

Related Commands	Command	Description
	signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
	signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.
	signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
	signal timing oos	Configures the signal timing parameter for the OOS state of a call.
	signal-type	Sets the signaling type for a network dial peer.
	voice-class permanent	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a network dial peer.

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*

Syntax Description

<i>tag</i>	The unique number assigned to the voice class. The <i>tag</i> number maps to the tag number created using the voice class permanent global configuration command. The valid range is from 1 to 10,000.

Defaults

Network dial peers have no voice class assigned.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was first supported on the Cisco 2600 and 3600 series routers.

Usage Guidelines

You can assign one voice class to any given network dial peer. If you assign another voice class to a dial peer, the last voice class assigned replaces the previous voice class.



Note

You cannot assign a voice class to a plain old telephone service (POTS) dial peer.



Note

The **voice-class permanent** command in dial-peer configuration mode is entered with the hyphen. The **voice class permanent** command in global configuration mode is entered without the hyphen.

Examples

The following example assigns a previously configured voice class to a Voice over Frame Relay (VoFR) network dial peer:

```
dial-peer voice 100 vofr
voice-class permanent 10
```

Related Commands	Command	Description
	signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
	signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.
	signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
	signal timing oos	Configures the signal timing parameter for the OOS state of a call.
	signal-type	Sets the signaling type for a network dial peer.
	voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.

voice-class permanent (voice-port)

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*

Syntax Description

<i>tag</i>	The unique number assigned to the voice class. The <i>tag</i> number maps to the tag number created using the voice class permanent global configuration command. The valid range is from 1 to 10,000.

Defaults

Voice ports have no voice class assigned.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was first supported as a voice port configuration command and on Cisco 2600 and 3600 series routers.

Usage Guidelines

You can assign one voice class to any given voice port. If you assign another voice class to a voice port, the last voice class assigned replaces the previous voice class.



Note The **voice-class permanent** command in voice-port configuration mode is entered with a hyphen. The **voice class permanent** command in global configuration mode is entered without the hyphen.

Examples

The following example assigns a previously configured voice class to voice port 1/1 in a Cisco MC3810 series concentrator:

```
voice-port 1/1
 voice-class permanent 10
```

The following example assigns a previously configured voice class to voice port 1/1/0 in a Cisco 3600 series router:

```
voice-port 1/1/0
 voice-class permanent 10
```


Related Commands	Command	Description
	signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
	signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.
	signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
	signal timing oos	Configures the signal timing parameter for the OOS state of a call.
	signal-type	Sets the signaling type for a network dial peer.
	voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.

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

Syntax Description

This command has no arguments or keywords.

Defaults

The two-beep confirmation tone is heard on the PLAR or PLAR OPX connection.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on Cisco MC3810 multiservice concentrators.

Usage Guidelines

This command applies only to the Cisco MC3810 multiservice concentrator.

Use this command to disable the two-beep confirmation tone that a caller hears when picking up the handset for PLAR and PLAR OPX connections. This command is valid only if the voice-port **connection** command is set to PLAR or PLAR OPX.

Examples

The following example disables the two-beep confirmation tone on voice port 1/1 on the Cisco MC3810 multiservice concentrator:

```
voice-port 1/1
 connection plar-opx
 voice confirmation-tone
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.

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

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** 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** | **invalid-number** | **unassigned-number** }

no voice { **user-busy** | **invalid-number** | **unassigned-number** }

Syntax Description	user-busy	Router continues to dial-peer hunting if it receives a user-busy disconnect cause code from a destination router.
	invalid-number	Router stops dial-peer hunting if it receives an invalid-number disconnect cause code from a destination router.
	unassigned-number	Router stops dial-peer hunting if it receives an unassigned-number disconnect cause code from a destination router.

Defaults	The default depends on the disconnect cause code. By default, the router stops dial-peer hunting if it receives the user-busy disconnect cause code. By default, the router continues dial-peer hunting if it receives an invalid-number, or an unassigned-number disconnect cause code.

Command Modes	Global configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced on the Cisco 2600 series and 3600 series routers, and the Cisco MC3810 multiservice concentrator for Voice over Frame Relay (VoFR). It was also supported for Voice over IP (VoIP) on the 2600 series and 3600 series routers.
	12.0(7)T	This command was first supported on the Cisco AS5300 and Cisco AS5800 for VoIP.
	12.0(7)XK	This command was first used for VoIP on the Cisco MC3810 multiservice concentrator.
	12.1(2)T	The support for VoIP on the Cisco MC3810 multiservice concentrator was implemented in Cisco IOS Release 12.1(2)T.
	12.1(3)XI	The invalid-number and unassigned-number keywords were added, and the command name was changed to voice hunt .
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines	This command applies to routers that act as originating or tandem nodes in a Voice over IP, Voice over Frame Relay, or Voice over ATM environment.

This command is used for a configuration in which an originating or tandem router is configured with multiple dial peer entries that route a call to the same destination number, but on different destination routers. In this configuration, after all routes to the first router entry in the dial-peer list are active, a new call will not “roll over” to the next router in the dial-peer list.

This failure to route to the second destination router happens when the bandwidth on the voice interface is greater than the maximum capacity of the first destination router. This condition allows the originating or tandem router to attempt to place a new call to the first destination router because it has indications from the first destination router that there is more capacity based on the bandwidth setting. When the first destination router receives the call, if all of the ports are in use, the destination router returns a “user-busy” disconnect reason code to the originating or tandem router.

The originating or tandem router interprets the disconnect reason code as “unavailable destination” for the call and returns a busy tone to the initiating caller.

The originating or tandem router fails to try other routers in the dial-peer list after receiving a “user disconnect” reason code, and so it terminates the call attempt. By using this command, you can perform dial-peer hunting on multiple destination routers even if the originating or tandem router receives a “user-busy” disconnect reason code from one of the destination routers.

Examples

The following example displays configuring the originating or tandem router to continue dial-peer hunting if it receives a “user-busy” disconnect code from a destination router:

```
voice hunt user-busy
```

The following example displays configuring the originating or tandem router to continue dial-peer hunting if it receives an “invalid-number” disconnect code from a destination router:

```
voice hunt invalid-number
```

Related Commands

Command	Description
huntstop	Disables all further dial-peer hunting if a call fails when using hunt groups.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.

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.

Defaults

Local calls bypass the DSP.

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced.
12.0(7)XK	This command was implemented on the Cisco 2600 and 3600 series routers and the MC3810 multiservice concentrator.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Local calls (calls between voice ports on a router or concentrator) normally bypass the DSP to minimize use of system resources. Use the **no** form of the **voice local-bypass** command if you need to direct local calls through the DSP. Input gain and output attenuation can be configured only if calls are directed through the DSP.

Examples

The following example configures a Cisco MC3810 multiservice concentrator, 2600 or 3600 series routers to pass local calls through the DSP:

```
no voice local-bypass
```

Related Commands

Command	Description
input gain	Configures a specific input gain value.
output attenuation	Configures a specific output attenuation value.

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>dso-group-no</i>	Indicates the defined 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> argument specifies the slot number in the Cisco router in which the VIC 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 voice port: - 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.
:D	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.
:D	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 defined 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.

Defaults

No default behavior or values.

Command Modes

Global configuration

■ voice-port

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(3)T	Support for Cisco 2600 series routers was added.
12.0(3)T	Support for the Cisco AS5300 access server was added.
12.0(7)T	Support for the Cisco AS5800 universal access server, the Cisco 7200 series router, and the Cisco 1750 router was added. Arguments for the Cisco 2600 and Cisco 3600 series router were added.

Usage Guidelines

Use the **voice-port** global configuration command to switch to voice-port configuration mode from global configuration mode. Use the **exit** command to exit voice-port configuration mode and return to global configuration mode.

Examples

The following example accesses voice-port configuration mode for port 0, located on subunit 0 on a voice interface card installed in slot 1 for the Cisco 3600 series:

```
voice-port 1/0/0
```

The following example accesses the voice-port configuration mode for digital voice port 24 on a Cisco MC3810 with a digital voice module (DVM) installed:

```
voice-port 1/24
```

The following example accesses the voice-port configuration mode for the Cisco AS5300:

```
voice-port 1:D
```

The following example accesses the voice-port configuration mode for the Cisco AS5800 (T1 card):

```
voice-port 1/0/0:D
```

The following example accesses the voice-port configuration mode for the Cisco AS5800 (T3 card):

```
voice-port 1/0/0:1:D
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.

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.

Defaults

The voice ports on the interface are not in busyout state.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on Cisco MC3810 multiservice concentrators.

Usage Guidelines

This command busies out all voice ports associated with the interface, except any voice ports configured to busy out under specific conditions using the **busyout monitor** and **busyout seize** commands.

Examples

The following example places the voice ports associated with serial interface 1 into busyout state:

```
interface serial 1
 voice-port busyout
```

The following example places the voice ports associated with ATM interface 0 into busyout state:

```
interface atm 0
 voice-port busyout
```

■ voice-port busyout

Related Commands	Command	Description
	busyout forced	Forces a voice port on the Cisco MC3810 multiservice concentrator into the busyout state.
	busyout monitor	Places a voice port on the Cisco MC3810 multiservice concentrator into the busyout monitor state.
	busyout seize	Changes the busyout action for an FXO or FXS voice port.
	show voice busyout	Displays information about the voice busyout state on the Cisco MC3810 multiservice concentrator.

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.

Defaults

The voice path is cut-through in only the backward direction when the RTP channel is opened.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced on Cisco 2600, Cisco 3600, Cisco 7200, and Cisco 7500 series routers, Cisco AS5300 and Cisco AS5800 universal access servers, and Cisco MC3810 multiservice concentrators.

Usage Guidelines

The **voice rtp send-recv** command should be enabled only when the voice path must be cut-through (established) in both the backward and forward directions before a Connect message is received from the destination switch. The **voice rtp send-recv** command affects all Voice over IP (VoIP) calls when it is enabled.

Examples

The following example enables the voice path to cut-through in both directions when the RTP channel is opened:

```
voice rtp send-recv
```

voice service

To specify the voice encapsulation type, use the **voice service** command in global configuration mode.

voice service { voip | voatm }

Syntax Description

voip	Specifies Voice over IP (VoIP) parameters.
voatm	Specifies Voice over ATM (VoATM) parameters.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)XA	This command was introduced for VoATM for the Cisco MC3810 multiservice concentrators.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T for the Cisco MC3810 multiservice concentrators.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T for VoIP on the Cisco 2600 series routers, Cisco 3600 series routers, and Cisco MC3810 multiservice concentrators.

Usage Guidelines

Use the **voice service** command to switch to voice-service configuration mode from global configuration mode and to specify a voice encapsulation type. Use the **exit** command to exit the voice-service configuration mode and return to the global configuration mode.

Examples

The following example shows how to access voice-service configuration mode and specify VoIP parameters, beginning in global configuration mode:

```
voice service voip
```

Related Commands

Command	Description
fax protocol	Specifies the global default fax protocol for all the VoIP dial peers.
modem passthrough	Configures modem pass-through over VoIP.

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

Syntax Description	<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.

Defaults	250 milliseconds

Command Modes	Global configuration

Command History	Release	Modification
	12.0(7)XK	This command was introduced on the Cisco 2600, 3600, and MC3810 multiservice concentrator.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines	The voice vad-time command affects all voice ports on a router or concentrator, but it does not affect calls already in progress.
	You can use this command in transparent common channel signaling (CCS) applications in which you want VAD to activate when the voice channel is idle, but not during active calls. With a longer silence detection delay, VAD reacts to the silence of an idle voice channel, but not to pauses in conversation.
	The voice vad-time command does not affect voice codecs that have ITU-standardized built-in VAD features—for example, G.729B, G.729AB, G.723.1A. The VAD behavior and parameters of these codecs are defined exclusively by the applicable ITU standard.

Examples	The following example configures a 20-second delay before VAD silence detection is enabled:
	<pre>voice vad-time 20000</pre>

Related Commands	Command	Description
	vad (dial peer)	Enables voice activity detection on a network dial peer.

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**}

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.
calling-number	The automatic number identification (ANI) number or the number of the calling party.
called-number	The Dial Number Information Service (DNIS) number or the number of the called party.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced for Voice over IP on the Cisco AS5300.
12.0(7)XK	This command was first supported for Voice over IP on the Cisco 2600 series and Cisco 3600 series routers, and on the Cisco MC3810 multiservice concentrator.
12.1(1)T	This command was first supported on the T train for Voice over IP on the Cisco 1750, Cisco 2600 series, and Cisco 3600 series routers, the Cisco AS5300 universal access server, and the Cisco 7200 series and Cisco 7500 series routers.
12.1(2)T	This command was first supported on the T train for Voice over IP on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

With this command, all IP-based calls are captured and handled, depending on either the calling number or the called number to the specified tag name.

Examples

The following example identifies the rule set for calls that originate from H.323-compatible clients:

```
voip-incoming translation-rule 5 called-number
```


Related Commands

Command	Description
numbering-type	Matches one number type for a dial-peer call leg.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
show translation-rule	Displays the contents of all the rules that have been configured for a specific translation name.
test translation-rule	Tests the execution of the translation rules on a specific name-tag.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.

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*

Syntax Description		
	<i>local-zone-name</i>	Name of local zone (synonymous with local gatekeeper).
	default	Use with the direct or proxied keyword to define the mode of behavior for all remote zones that have not been specially named using the remote-zone <i>remote-zone-name</i> keyword and argument combination.
	remote-zone <i>remote-zone-name</i>	Name of remote zone (synonymous with remote gatekeeper) for which a special mode of behavior is defined.
	direct	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.
	proxied	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.

Defaults The local zone allows proxied access for all remote zones.

Command Modes Gatekeeper configuration

Command History	Release	Modification
	11.3(2)NA	This command was introduced on Cisco 2500 and 3600 series routers.

Usage Guidelines By default, a gatekeeper will offer a local proxy IP address when queried by a remote gatekeeper about a target local endpoint. This is considered proxied access. By using the **zone access** command, you can configure the local gatekeeper to offer the local endpoint address instead of the local proxy address. This is considered direct access.



Note

The **zone access** command, configured on your local gatekeeper, affects only the use of proxies for incoming calls (that is, it does not affect the use of local proxies for outbound calls). When originating a call, a gatekeeper will use a proxy only if the remote gatekeeper offers a proxy at the remote end. A call between two endpoints in the same zone will always be a direct (nonproxied) call.

You can define the accessibility behavior of a local zone relative to certain remote zones using the **remote-zone** *remote-zone-name* keyword and argument combination with the **direct** or **proxied** keyword. You can define the default behavior of a local zone relative to all other remote zones using the **default** keyword with the **direct** or **proxied** keywords. To remove an explicitly named remote zone so that it is governed by the default-behavior rule, use the **no zone access** command.

Examples

The following example allows direct access to the local zone eng.xyz.com from remote zones within xyz corporation. All other remote locations will have proxied access to eng.xzy.com.

```
zone local eng.xyz.com xyz.com
zone access eng.xyz.com remote-zone mfg.xyz.com direct
zone access eng.xyz.com remote-zone mktg.xyz.com direct
zone access eng.xyz.com remote-zone sales.xyz.com direct
zone access eng.xyz.com default proxied
```

The following example supposes that only local gatekeepers within xyz.com have direct access to each other because your corporation has firewalls or you do not advertise your gatekeepers externally. You have excellent Quality of Service (QoS) within your corporate network, except for a couple of foreign offices. In this case, use proxies with the foreign offices (in Milan and Tokyo) and nowhere else.

```
zone local sanjose.xyz.com xyz.com
zone access sanjose.xyz.com default direct
zone access sanjose.xyz.com remote-zone milan.xyz.com proxied
zone access sanjose.xyz.com remote-zone tokyo.xyz.com proxied
```

Related Commands

Command	Description
show proxy h323 calls	Displays a list of each active call on the proxy.
zone local	Specifies a zone controlled by a gatekeeper.

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*

Syntax Description

<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.

Defaults

Bandwidth is unlimited.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 and 3600 series routers.

Examples

The following example sets the maximum bandwidth to 1000 kbps for zone gk1:

```
zone bw gk1 1000
```

Related Commands

Command	Description
show proxy h323 calls	Displays a list of each active call on the proxy.

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 gatekeepers 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.

Defaults

No local zone is defined.



Note

The gatekeeper cannot operate without at least one local zone definition. Without local zones, the gatekeeper goes to an inactive state when the **no shutdown** command is issued.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 and 3600 series routers.

Usage Guidelines

Multiple local zones can be defined. The gatekeeper manages all configured local zones. Intrazone and interzone behavior remains the same (zones are controlled by the same or different gatekeepers).

Only one *ras-IP-address* argument can be defined for all local zones. You cannot configure each zone to use a different RAS IP address. If you define this in the first zone definition, you can omit it for all subsequent zones, which automatically pick up this address. If you set it in a subsequent **zone local** command, it changes the RAS address of all previously configured local zones as well. Once defined, you can change it by reissuing any **zone local** command with a different *ras-IP-address* argument.

If the *ras-IP-address* argument is a Hot Standby Router Protocol (HSRP) virtual address, it automatically puts the gatekeeper into HSRP mode. In this mode, the gatekeeper assumes STANDBY or ACTIVE status according to whether the HSRP interface is on STANDBY or ACTIVE status.

You cannot remove a local zone if there are endpoints or gateways registered in it. To remove the local zone, shut down the gatekeeper first, which forces unregistration.

Multiple zones are controlled by multiple logical gatekeepers on the same Cisco IOS platform.

The maximum number of local zones defined in a gatekeeper should not exceed 100.

This command can also be used to change the IP address used by the gatekeeper.

Examples

The following example creates a zone controlled by a gatekeeper in the domain called cisco.com:

```
zone local gk1.cisco.com cisco.com
```

Related Commands

Command	Description
show proxy h323 calls	Displays a list of each active call on the proxy.
zone subnet	Specifies a zone controlled by a gatekeeper.

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	
<i>gatekeeper-name</i>	The name of a local or remote gatekeeper, which must have been defined by using the zone local or zone remote command.
<i>e164-prefix</i>	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 <i>pri-0-to-10 gw-alias</i>	(Optional) Use the gw-priority option to define how the gatekeeper selects gateways in its local zone for calls to numbers beginning with prefix <i>e164-prefix</i>. Do not use this option to set priority levels for a prefix assigned to a remote gatekeeper. Use values from 0 to 10. A 0 value prevents the gatekeeper from using the gateway <i>gw-alias</i> for that prefix. Value 10 places the highest priority on gateway <i>gw-alias</i>. 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 <i>pri-0-to-10</i> value. The <i>gw-alias</i> 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.

Defaults

No knowledge of its own prefix or the prefix of any other zone is defined.

Command Modes Gatekeeper configuration

Command History	Release	Modification
	11.3(6)Q	This command was introduced.
	11.3(7)NA	This command was modified for H.323 Version 1.
	12.0(5)T	The display format was modified for H.323 Version 2.

Usage Guidelines A gatekeeper can handle more than one zone prefix, but a zone prefix cannot be shared by more than one gatekeeper. If you have defined a zone prefix as being handled by a gatekeeper and now define it as being handled by a second gatekeeper, the second assignment cancels the first.

If you need a gatekeeper to handle more than one prefix, but for cost reasons you want to be able to group its gateways by prefix usage, there are two ways to do it.

The first method is simpler, has less overhead, and is recommended if your gateways can be divided into distinct groups, in which each group is to be used for a different set of prefixes. For instance, if a group of gateways is used for calling area codes 408 and 650, and another group is used for calling area code 415, you can use this method. In this case, you define a local zone for each set of prefixes, and have the group of gateways to be used for that set of prefixes register with that specific local zone. Do not define any gateway priorities. All gateways in each local zone are treated equally in the selection process.

However, if your gateways cannot be cleanly divided into nonintersecting groups (for instance if one gateway is used for calls to 408 and 415 and another gateway is used for calls to 415 and 650, and so on), you can put all these gateways in the same local zone and use the **gw-priority** option to define which gateways will be used for which prefixes.

When choosing a gateway, the gatekeeper first looks for the longest zone prefix match; then it uses the priority and the gateway status to select from the gateways. If all gateways are available, the gatekeeper chooses the highest priority gateway. If all the highest priority gateways are busy (see the gateway **resource threshold** command), a lower priority gateway is selected.



Note

The **zone prefix** command matches a prefix to a gateway. It does not register the gateway. The gateway must register with the gatekeeper before calls can be completed through that gateway.

Examples The following example shows how you can define multiple local zones for separating your gateways:

```
zone local gk408or650 xyz.com
zone local gk415 xyz.com
zone prefix gk408or650 408.....
zone prefix gk408or650 650.....
zone prefix gk415 415.....
```

Now you need to configure all the gateways to be used for area codes 408 or 650 to register with gk408or650 and all gateways to be used for area code 415 to register with gk415. On Cisco voice gateways, you configure the gateways to register with the appropriate gatekeepers by using the **h323 voip id** command.

The following example shows how you can put all your gateways in the same zone but use the **gw-priority** keyword to determine which gateways will be used for calling different area codes:

```
zone local localgk xyz.com
```



```

zone prefix localgk 408.....
zone prefix localgk 415..... gw-priority 10 gw1 gw2
zone prefix localgk 650..... gw-priority 0 gw1

```

The commands shown accomplish the following tasks:

- Domain xyz.com is assigned to gatekeeper localgk.
- Prefix 408..... is assigned to gatekeeper localgk, and no gateway priorities are defined for it; therefore, all gateways registering to localgk can be used equally for calls to the 408 area code. No special gateway lists are built for the 408..... prefix; selection is made from the master list for the zone.
- The prefix 415..... is added to gatekeeper localgk, and priority 10 is assigned to gateways gw1 and gw2.
- Prefix 650..... is added to gatekeeper localgk, and priority 0 is assigned to gateway gw1.

A priority 0 is assigned to gateway gw1 to exclude it from the gateway pool for prefix 650..... When gateway gw2 registers with gatekeeper localgk, it is added to the gateway pool for each prefix as follows:

- For gateway pool for 415....., gateway gw2 is set to priority 10.
- For gateway pool for 650....., gateway gw2 is set to priority 5.

The following example changes gateway gw2 from priority 10 for zone 415..... to the default priority 5:

```
no zone prefix localgk 415..... gw-pri 10 gw2
```

The following example changes both gateways gw1 and gw2 from priority 10 for zone 415..... to the default priority 5:

```
no zone prefix localgk 415..... gw-pri 10 gw1 gw2
```

In the preceding example, the prefix 415..... remains assigned to gatekeeper localgk. All gateways that do not specify a priority level for this prefix are assigned a default priority of 5. The following example removes the prefix and all associated gateways and priorities from this gatekeeper:

```
no zone prefix localgk 415.....
```

Related Commands

Command	Description
register	Configures a gateway to register or deregister a fully qualified dial-peer E.164 address with a gatekeeper.
resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.
show call resource voice threshold	Displays the threshold configuration settings and status for an H.323 gateway.
show gateway	Displays the current gateway status.
zone local	Specifies a zone controlled by a gatekeeper.
zone remote	Statically specifies a remote zone if DNS is unavailable or undesirable.

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

<i>other-gatekeeper-name</i>	Name of the remote gatekeeper.
<i>other-domain-name</i>	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.

Defaults

No remote zone is defined. DNS will locate the remote zone.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 and 3600 series routers.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

All gatekeepers do not have to be in DNS. For those that are not, use the **zone remote** command so that the local gatekeeper knows how to access them. In addition, you may wish to improve call response time slightly for frequently accessed zones. If the **zone remote** command is configured for a particular zone, you do not need to make a DNS lookup transaction.

The maximum number of zones defined on a gatekeeper varies depending on the mode or the call model or both. For example, a directory gatekeeper may be in the mode of being responsible for forwarding location request (LRQ) messages and not handling any local registrations and calls; the call model might be E.164 addressed calls instead of H.323-ID addressed calls.

For a directory gatekeeper that does not handle local registrations and calls, the maximum remote zones defined should not exceed 10,000; an additional 4 MB of memory is required to store this maximum number of remote zones.

For a gatekeeper that handles local registrations and only E.164 addressed calls, the number of remote zones defined should not exceed 2000.

For a gatekeeper that handles H.323-ID calls, the number of remote zones defined should not exceed 200.

Examples

The following example configures the local gatekeeper to reach targets of the form *xxx.cisco.com* by sending queries to the gatekeeper named *sj3.cisco.com* at IP address 10.1.1.12:

```
zone remote sj3.cisco.com cisco.com 10.1.1.12
```

Related Commands

Command	Description
show proxy h323 calls	Displays a list of each active call on the proxy.
zone local	Specifies a zone controlled by a gatekeeper.

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.
default	Applies to all other subnets that are not specifically defined by the zone subnet 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.
enable	Gatekeeper accepts discovery and registration from the specified subnets.

Defaults The local gatekeeper accepts discovery and registration requests from all subnets. If the request specifies a gatekeeper name, it must match the local gatekeeper name or the request will not be accepted.

Command Modes Gatekeeper configuration

Command History	Release	Modification
	11.3(2)NA	This command was introduced on Cisco 2500 and 3600 series routers.
	12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines You can use the **zone subnet** command more than once to create a list of subnets controlled by a gatekeeper. The subnet masks do not have to match actual subnets in use at your site. For example, to specify a particular endpoint, you can supply its address with a 32-bit netmask.

Examples

The following example starts by disabling the gatekeeper, gk1.cisco.com, from accepting discovery and registration messages from all subnets. Next, gk1.cisco.com is configured to accept discovery and registration messages from all H.323 nodes on the subnet 172.21.127.0.

In addition, gk1.cisco.com is configured to accept discovery and registration messages from a particular endpoint with the IP address 172.21.128.56.

```
no zone subnet gk1.cisco.com default enable
zone subnet gk1.cisco.com 172.21.127.0/24 enable
zone subnet gk1.cisco.com 172.21.128.56/32 enable
```

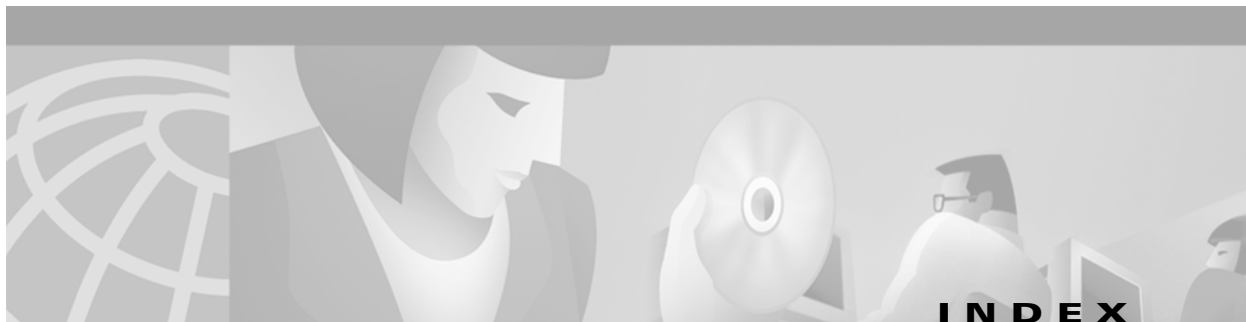
Related Commands

Command	Description
show gatekeeper zone status	Displays the status of zones related to a gatekeeper.
zone local	Specifies a zone controlled by a gatekeeper.

■ zone subnet

Index





Symbols

<cr> [xv](#)

? command [xiv](#)

A

AAA account identification

off-ramp fax location, specifying [VR-472, VR-474](#)

AAA accounting services

off-ramp fax service, enabling [VR-470 to VR-471](#)

on-ramp fax service, enabling [VR-464](#)

AAA authentication services

enabling on-ramp [VR-465](#)

aaa nas port voip command [VR-2](#)

ABCD signaling

OOS bit patterns, defining [VR-876](#)

accounting

overloaded Acct-Session-Id field [VR-353](#)

syslog messages [VR-356](#)

vendor-specific RADIUS attributes [VR-355](#)

acc-qos command [VR-3](#)

alarm-trigger command [VR-5](#)

aliases

SMTP off-ramp fax host name, specifying [VR-483](#)

alias static command [VR-7](#)

alt-dial command [VR-9](#)

answer-address command [VR-10](#)

application command [VR-12](#)

arq reject-unknown-prefix command [VR-14](#)

as command [VR-16](#)

asp command [VR-19](#)

ASR (application-specific routing)

proxy bandwidth maximum, specifying [VR-360](#)

ATM interface NSAP addresses, displaying [VR-649](#)

atm scramble-enable command [VR-22](#)

atm video aesa command [VR-23](#)

audio-prompt load command [VR-25](#)

auto-cut-through command [VR-26](#)

B

backhaul-session-manager command [VR-27](#)

bandwidth command [VR-29](#)

bandwidth remote command [VR-31](#)

battery-reversal command [VR-32](#)

block-caller command [VR-34](#)

Blue Alarm

See DS1 links, shutting down

busyout forced command [VR-36](#)

busyout monitor command [VR-38](#)

busyout monitor probe command [VR-41](#)

busyout seize command [VR-43](#)

C

cac master command [VR-46](#)

cadence-list command [VR-47](#)

cadence-max-off-time command [VR-49](#)

cadence-min-on-time command [VR-50](#)

cadence-variation command [VR-51](#)

call application cache reload time command [VR-52](#)

call application voice access-method command [VR-55](#)

call application voice accounting enable command [VR-57](#)

call application voice accounting-list command [VR-58](#)

call application voice authen-list command [VR-59](#)

- call application voice authen-method command [VR-61](#)
- call application voice authentication enable command [VR-63](#)
- call application voice command [VR-53](#)
- call application voice global-password command [VR-64](#)
- call application voice language command [VR-65](#)
- call application voice load command [VR-68](#)
- call application voice pin-len command [VR-69](#)
- call application voice redirect-number command [VR-72](#)
- call application voice retry-count command [VR-75](#)
- call application voice set-location command [VR-78](#)
- call application voice uid-len command [VR-81](#)
- call application voice uid-length command [VR-81](#)
- call application voice warning-time command [VR-84](#)
- call completion without M-lead response, enabling [VR-26](#)
- called-number dial-peer configuration command [VR-114](#)
- caller-id alerting dsp-pre-alloc command [VR-118](#)
- caller-id alerting line-reversal command [VR-120](#)
- caller-id alerting pre-ring command [VR-122](#)
- caller-id alerting ring command [VR-124](#)
- caller-id attenuation command [VR-126](#)
- caller-id block command [VR-127](#)
- Caller ID Call Blocking, configuring [VR-34](#)
- caller-id command [VR-116](#)
- caller-id enable command [VR-129](#)
- call fallback
 - configuration, displaying [VR-668](#)
 - statistics, displaying [VR-669](#)
- call fallback active command [VR-87](#)
- call fallback cache-size command [VR-89](#)
- call fallback instantaneous-value-weight command [VR-92](#)
- call fallback jitter-probe num-packets command [VR-94](#)
- call fallback jitter-probe precedence command [VR-96](#)
- call fallback jitter-probe priority-queue command [VR-97](#)
- call fallback key-chain command [VR-99](#)
- call fallback map target address-list command [VR-100](#)
- call fallback map target subnet command [VR-102](#)
- call fallback monitor command [VR-104](#)
- call fallback probe-timeout command [VR-105](#)
- call fallback threshold delay loss command [VR-106](#)
- call fallback threshold icpif command [VR-108](#)
- calling-number outbound command [VR-131](#)
- call rsvp-sync command [VR-110](#)
- call rsvp-sync resv-timer command [VR-111](#)
- calls
 - authorization, forcing [VR-618](#)
 - blocking new [VR-438](#)
 - called party number translation rules, applying [VR-588](#)
 - call history table attributes, specifying [VR-247](#)
 - calling party number translation rules, applying [VR-588](#)
 - Cisco 800 series router CSM status, displaying [VR-753](#)
 - country-specific defaults, configuring [VR-529](#)
 - digits to forward for voice, specifying [VR-324](#)
 - disconnecting [VR-941](#)
 - disconnect notification, configuring [VR-533](#)
 - H.323 connect procedures, forcing [VR-361](#)
 - H.323 proxy calls, displaying [VR-758](#), [VR-759](#)
 - idle state timing parameter, configuring [VR-882](#)
 - POTS dial peer call leg digits, stripping [VR-258](#)
 - session protocol on packet network, selecting [VR-601](#)
 - VoFR session protocol on packet network, selecting [VR-603](#)
 - voice and fax active call information, displaying [VR-655](#)
- calls, video
 - configuring [VR-252](#)
 - history, displaying [VR-679](#)
 - statistics, displaying [VR-678](#)
 - status summary, displaying [VR-821](#)
- call start command [VR-112](#)
- call-waiting command [VR-113](#)
- cap-list vfc command [VR-133](#)
- card type command [VR-134](#)
- carriage return (<cr>) [xv](#)
- CAs (certificate authorities)
 - root, specifying [VR-999](#)
- CAS (channel-associated signalling)
 - state, displaying [VR-695](#)

- cautions, usage in text [x](#)
- ccm-manager application redundant-link port command [VR-135](#)
- ccm-manager mgcp command [VR-136](#)
- ccm-manager redundant-host command [VR-137](#)
- ccm-manager switchback command [VR-138](#)
- ccs connect (controller) command [VR-139](#), [VR-141](#)
- ccs encap frf11 command [VR-143](#)
- CDAPI (Call Distributor Application Programming Interface)
 - registered applications, displaying [VR-688](#)
- CES (circuit emulation service)
 - ATM encapsulation, enabling [VR-294](#)
 - ATM PVC, mapping to [VR-148](#)
 - cell-loss integration period, setting [VR-144](#)
 - clock, setting [VR-146](#)
 - clocking signals, specifying [VR-187](#)
 - receive buffer, configuring [VR-150](#)
 - structured type, configuring [VR-154](#)
 - synchronous clock mode, setting [VR-147](#)
 - transmit buffer, configuring [VR-152](#)
- ces cell-loss-integration-period command [VR-144](#)
- ces-clock command [VR-146](#)
- ces clockmode synchronous command [VR-147](#)
- ces connect command [VR-148](#)
- ces initial-delay command [VR-150](#)
- ces max-buf-size command [VR-152](#)
- ces service command [VR-154](#)
- Cisco 800 series routers
 - telephone port characteristics, displaying [VR-754](#)
- Cisco IOS configuration changes, saving [xviii](#)
- Cisco MC3810 universal concentrator
 - ATM scrambling on E1, enabling [VR-22](#)
 - PCM signal companding standard, selecting [VR-206](#)
- CiscoSecure for Windows NT
 - password, defining [VR-459](#)
- clear backhaul-session-manager group command [VR-156](#)
- clear call fallback cache command [VR-157](#)
- clear call fallback stats command [VR-158](#)
- clear controllers call-counters command [VR-159](#)
- clear csm-statistics command [VR-174](#), [VR-175](#)
- clear h323 gatekeeper call command [VR-176](#)
- clear ip sctp statistics [VR-178](#)
- clear mgcp statistics command [VR-179](#)
- clear rlm group command [VR-180](#)
- clear rudpv0 statistics command [VR-182](#)
- clear rudpv1 statistics command [VR-183](#)
- clear sgcp statistics command [VR-184](#)
- clear ss7 sm stats command [VR-185](#)
- clear voice port command [VR-186](#)
- clock-select command [VR-187](#)
- codec (dial-peer) command [VR-188](#)
- codec (dsp) command [VR-195](#)
- codec (voice-port) command [VR-197](#)
 - See* codec (dial-peer) command
- codec aal2-profile command [VR-198](#)
- codec complexity command [VR-200](#)
- codec preference command [VR-202](#)
- codecs
 - configuring [VR-440](#)
 - digits on compressed, forwarding [VR-443](#)
 - list of preferred [VR-202](#)
 - local video serial interface location, specifying [VR-526](#)
 - pass-through analog data, enabling [VR-447](#)
 - selection preference list, assigning [VR-1034](#), [VR-1039](#)
 - video ATM dial peer, defining [VR-252](#)
 - voice coder rate of speech, specifying [VR-188](#)
- comfort-noise command [VR-205](#)
- command modes, understanding [xiii to xiv](#)
- commands
 - context-sensitive help for abbreviating [xiv](#)
 - default form, using [xvii](#)
 - no form, using [xvii](#)
- command syntax
 - conventions [ix](#)
 - displaying (example) [xv](#)
- compand-type command [VR-206](#)
- condition command [VR-207](#)

configurations, saving [xviii](#)
 connect (atm) command [VR-209](#)
 connect (drop-and-insert) command [VR-211](#)
 connect (global) command [VR-213](#)
 connect command [VR-211](#)
 connection command [VR-215](#)
 connections
 ATM T1 and E1, defining [VR-209](#)
 drop-and-insert statistics, displaying [VR-691](#)
 T1 and E1 TDM cross-connect
 configuring slots [VR-935](#)
 defining [VR-211](#)
 timeout, configuring [VR-219](#)
 voice port, specifying [VR-215](#)
 connection-timeout command [VR-219](#)
 connect voice command [VR-214](#)
 copy flash vfc command [VR-221](#)
 copy tftp vfc command [VR-222](#)
 cptone command [VR-223](#)
 cross-connect command [VR-228](#)
 CSI (called subscriber identifier)
 fax, defining [VR-308](#)
 CSM (call switching module)
 statistics
 clearing [VR-174 to VR-175](#)
 displaying [VR-701](#)
 customer-id command [VR-230](#)

D

default [VR-234](#)
 default command [VR-234](#)
 default-file vfc command [VR-235](#)
 define command [VR-236](#)
 delete vfc command [VR-238](#)
 description (dspfarm) command [VR-240](#)
 description command [VR-239](#)
 destination-pattern (interface) command [VR-244](#)
 destination-pattern (ISDN) command [VR-244](#)
 destination-pattern command [VR-241](#)
 detect v54 channel-group command [VR-245](#)
 device-id command [VR-246](#)
 dial-control-mib command [VR-247](#)
 dialing
 delayed, wink pulse duration [VR-977](#)
 dial-peer hunt command [VR-248](#)
 dial peers
 alternate dial-out string [VR-9](#)
 application, enabling [VR-12](#)
 association with telephone number, displaying [VR-716](#)
 ATM video NSAP address, specifying [VR-505](#)
 call leg numbering type, selecting [VR-508](#)
 configuration, displaying [VR-708](#)
 fax relay VoIP ECM, disabling [VR-309](#)
 fax transmission rate, establishing [VR-306](#)
 FRF.11 Annex A frames, generating [VR-283](#)
 hunting, disabling when call fails [VR-377](#)
 hunting after user-busy disconnect, configuring [VR-1049](#)
 hunt selection order, specifying [VR-248](#)
 information digits, specifying [VR-390](#)
 information type, selecting [VR-391](#)
 maximum connections, specifying [VR-431](#)
 maximum redirect servers, setting [VR-435](#)
 Modem Passthrough over VoIP, configuring [VR-479](#)
 network-specific address, specifying [VR-607, VR-610](#)
 packet priority (IP Precedence), setting [VR-396](#)
 roaming capability, enabling [VR-584](#)
 shutting down [VR-864](#)
 signal type, selecting [VR-896](#)
 technology prefix, specifying [VR-937](#)
 video configuration, displaying [VR-708](#)
 voice configuration, displaying [VR-709](#)
 VoIP fax protocol, specifying [VR-302, VR-304](#)
 VoIP H.225 TCP timeout value, setting [VR-359](#)
 VoIP network-specific address, specifying [VR-613](#)
 VoIP poor voice quality notifications,
 generating [VR-901](#)
 dial-peer terminator command [VR-250](#)

- dial-peer video command [VR-252](#)
- dial-peer voice command [VR-253](#)
- dial-type command [VR-256](#)
- DID (direct inward dial) call treatment, enabling [VR-261](#)
- digit-strip command [VR-258](#)
- direct-inward-dial command [VR-261](#)
- disc_pi_off command [VR-262](#)
- disconnect-ack command [VR-263](#)
- documentation
 - conventions [ix](#)
 - feedback, providing [xi](#)
 - modules [v to vii](#)
 - online, accessing [x](#)
 - ordering [xi](#)
- Documentation CD-ROM [x](#)
- documents and resources, supporting [viii](#)
- ds0 busyout command [VR-264](#)
- ds0-group command [VR-266](#), [VR-555](#)
- DS0 groups
 - cross connecting [VR-228](#)
 - DTMF inter-digit timer, configuring [VR-285](#)
- DS0 high water marks, clearing [VR-159](#)
- DS0 timeslot
 - busyout state, forcing [VR-264](#)
 - logical voice ports, specifying [VR-266](#)
- DS1 links, shutting down [VR-865](#)
- DSN (delivery status notice)
 - delivery options, configuring [VR-277](#)
- dsn command [VR-277](#)
- DSP (digital signal processor)
 - busy out test [VR-957](#)
 - enabling [VR-280](#)
 - interface, description [VR-239](#), [VR-240](#)
 - playout buffers, tuning [VR-513](#), [VR-517](#)
 - playout delay mode, selecting [VR-519](#), [VR-521](#)
 - reset test [VR-959](#)
 - resetting [VR-566](#)
 - restore activity test [VR-960](#), [VR-962](#)
 - shutting down [VR-863](#)

- statistics, displaying [VR-737](#)
- VFC summary, displaying [VR-852](#), [VR-855](#)
- VoFR frame sequence numbers, generating [VR-592](#)
- voice channel status, displaying [VR-824](#), [VR-828](#)
- dspint dspfarm command [VR-280](#)
- dtmf-relay (Voice over Frame Relay) command [VR-283](#)
- dtmf-relay (Voice over IP) command [VR-281](#)
- dtmf timer inter-digit command [VR-285](#)

E

- E&M interface type, specifying [VR-1009](#)
- E&M MELCAS (Mercury Exchange Limited Channel Associated Signaling) voice signaling
 - receive bits, ignoring [VR-381](#)
 - transmit and receive bits, defining [VR-236](#)
- E.164 addresses
 - gateway, registering to [VR-562](#)
- E.164 telephone numbers
 - destination pattern [VR-241](#)
 - incoming call, identifying to dial peer [VR-10](#)
- E1
 - CCS cross-connect, configuring [VR-478](#)
 - CCS frame-forwarding, configuring [VR-478](#)
 - contiguous bearer channel handling, configuring [VR-399](#)
 - controller interface mode, configuring [VR-476](#)
 - microcode images, reloading [VR-458](#)
 - out-of-service alarm, configuring [VR-5](#)
 - signal levels, attenuating [VR-287](#), [VR-288](#)
- echo-cancel comfort-noise command [VR-286](#)
- echo-cancel compensation command [VR-287](#)
- echo-cancel coverage command [VR-288](#)
- echo-cancel enable (controller) command [VR-292](#)
- echo-cancel enable command [VR-290](#)
- echo cancellation processor
 - loopback mode, configuring [VR-293](#)
- echo-cancel loopback command [VR-293](#)
- echo suppression, nonlinear processing [VR-504](#)

encapsulation atm-ces command [VR-294](#)
 encapsulation ftc-trunk command [VR-296](#)
 encapsulations
 voice types, specifying [VR-1058](#)
 encryption algorithm, setting [VR-297](#)
 encryption command [VR-297](#)
 erase vfc command [VR-299](#)
 EXEC commands
 show dialplan incall number [VR-712](#)
 expect-factor command [VR-300](#)
 external applications, triggering [VR-597](#)

F

fax cover sheet
 e-mail, generating from [VR-315](#), [VR-316](#)
 header data, specifying [VR-317](#), [VR-320](#)
 personalizing [VR-312](#)
 standard, generating [VR-313](#)
 fax header information, configuring [VR-310](#)
 fax image resolution, specifying [VR-385](#)
 fax images, encoding method [VR-383](#)
 fax protocol (dial-peer) command [VR-302](#)
 fax protocol (voice-service) command [VR-304](#)
 fax rate command [VR-306](#)
 fax receive called-subscriber [VR-308](#)
 fax receive called-subscriber command [VR-308](#)
 fax-relay ecm disable command [VR-309](#)
 fax send center-header [VR-310](#)
 fax send center-header command [VR-310](#)
 fax send coverage comment [VR-312](#)
 fax send coverage comment command [VR-312](#)
 fax send coverage e-mail-controllable [VR-313](#)
 fax send coverage e-mail-controllable command [VR-313](#)
 fax send coverage enable [VR-315](#)
 fax send coverage enable command [VR-315](#)
 fax send coverage show-detail [VR-316](#)
 fax send coverage show-detail command [VR-316](#)
 fax send left-header [VR-317](#)
 fax send left-header command [VR-317](#)
 fax send max-speed [VR-319](#)
 fax send max-speed command [VR-319](#)
 fax send right-header [VR-320](#)
 fax send right-header command [VR-320](#)
 fax send transmitting-subscriber command [VR-322](#)
 fax transmission rate, establishing [VR-319](#)
 Feature Navigator
 See platforms, supported
 filtering output, show and more commands [xviii](#)
 firmware, unbundling VFC [VR-1013](#)
 forward-alarms command [VR-323](#)
 forward-digits command [VR-324](#)
 frag-pre-queuing command [VR-328](#)
 frame-relay voice bandwidth command [VR-326](#)
 freq-max-power command [VR-331](#)
 freq-min-power command [VR-332](#)
 freq-pair command [VR-333](#)
 freq-power-twist command [VR-335](#)
 FRF.11 subchannel information, displaying [VR-719](#)
 FRF.11 trunk
 voice class, creating [VR-1040](#), [VR-1042](#), [VR-1044](#)
 ftc-trunk frame-relay-dlci command [VR-336](#)
 ftc-trunk management-dlci command [VR-337](#)
 ftc-trunk management-protocol command [VR-338](#)
 FXO (foreign exchange office)
 analog-to-digital gain offset, specifying [VR-422](#)
 battery polarity reversal, configuring [VR-32](#)
 guard-out durations, specifying [VR-985](#)
 FXO supervisory disconnect
 enabling [VR-930](#)
 tone, assigning [VR-933](#)
 tone detection parameters voice class, creating [VR-1036](#)
 voice port tone detection, configuring [VR-931](#)
 FXS (foreign exchange station)
 analog-to-digital gain offset, specifying [VR-422](#)
 battery polarity reversal, configuring [VR-32](#)
 disconnect signal acknowledgment,
 configuring [VR-263](#)

- hook flash duration, specifying [VR-986](#)
- idle port voltage, specifying [VR-379](#)
- voice port ring
 - cadence, specifying [VR-578](#)
 - frequency, specifying [VR-580](#)
 - specifying number of [VR-582](#)

G

- gatekeeper command [VR-340](#)
- gatekeepers
 - active calls, displaying [VR-722](#)
 - ARQ requests, rejecting [VR-14](#)
 - call disconnect, forcing [VR-176](#)
 - disabling [VR-866](#)
 - full status, displaying [VR-731](#)
 - H.323, specifying [VR-363](#)
 - listener port, configuring [VR-596](#)
 - local zone, configuring [VR-1065](#)
- LRQs
 - delay, configuring [VR-429](#)
 - forwarding [VR-424](#)
 - rejecting [VR-427](#)
 - sending multiple [VR-429](#)
 - sending sequential [VR-430](#)
- registered endpoint status, displaying [VR-724](#)
- registered server triggers, displaying [VR-729](#)
- remote zone, configuring [VR-1070](#)
- security, enabling [VR-590](#)
- static entry, creating [VR-7](#)
- technology prefix, configuring [VR-357](#)
- zone accessibility, configuring [VR-1062](#)
- zone bandwidth, configuring [VR-1064](#)
- zone prefix, configuring [VR-1067](#)
- zone prefix table, displaying [VR-732](#)
- zone status, displaying [VR-733](#)
- zone subnetworks, configuring [VR-1072](#)
- gateway command [VR-341](#)
- gateways

- alert message on terminating, enabling [VR-1028](#)
- H.323 resource availability, reporting [VR-567](#)
- Modem Passthrough over VoIP, configuring [VR-481](#)
- SMTP server response MDN, processing [VR-485](#)
- status, displaying [VR-735](#)
- technology prefix table, displaying [VR-726](#)
- global configuration mode, summary of [xiv](#)
- group auto-reset command [VR-343](#)
- group command [VR-342](#)
- group cumulative-ack command [VR-344](#)
- group out-of-sequence command [VR-345](#)
- group receive command [VR-346](#)
- group retransmit command [VR-347](#)
- group timer cumulative ack command [VR-348](#)
- group timer keepalive command [VR-349](#)
- group timer retransmit command [VR-350](#)
- group timer transfer command [VR-351](#)
- gw-accounting command [VR-352](#)
- gw-accounting h323 command [VR-352](#), [VR-354](#)
- gw-accounting h323 syslog command [VR-356](#)
- gw-type-prefix command [VR-357](#)

H

- H.323 accounting, enabling [VR-352](#)
- H.323 gateway
 - call disconnect, enabling [VR-262](#)
 - DTMF tones, relaying [VR-281](#)
 - gatekeeper ID name, defining [VR-366](#)
 - gatekeeper location, defining [VR-367](#)
 - interface, configuring [VR-369](#)
 - resource statistics, displaying [VR-681](#)
 - technology index, defining [VR-370](#)
 - threshold settings, displaying [VR-683](#)
- H.323 proxy
 - alias, registering [VR-372](#)
 - calls, displaying [VR-758](#), [VR-759](#)
 - local and remote zone communication, configuring [VR-1016](#)

- status, displaying [VR-765](#)
 - H.323 traffic
 - bandwidth maximum, specifying [VR-29](#)
 - bandwidth total, specifying [VR-31](#)
 - H.323 voice class, creating [VR-1038](#)
 - h225 timeout tcp establish command [VR-359](#)
 - h323 asr bandwidth command [VR-360](#)
 - h323 asr command [VR-360](#)
 - h323 call start command [VR-361](#)
 - h323 gatekeeper command [VR-363](#)
 - h323-gateway voip bind srcaddr command [VR-365](#)
 - h323-gateway voip h323-id command [VR-366](#)
 - h323-gateway voip id command [VR-367](#)
 - h323-gateway voip interface command [VR-369](#)
 - h323-gateway voip tech-prefix command [VR-370](#)
 - h323 h323-id command [VR-372](#)
 - h323 interface command [VR-373](#)
 - h323 qos command [VR-375](#)
 - h323 t120 command [VR-376](#)
 - hardware platforms
 - See* platforms, supported
 - HDLC interface
 - VoHDL segmentation size, defining [VR-1048](#)
 - help command [xiv](#)
 - huntstop command [VR-377](#)
-
- I**
- ICPIF (Impairment/Calculated Planning Impairment Factor)
 - estimates
 - clearing [VR-157](#)
 - displaying [VR-666](#)
 - RTR values, displaying [VR-939](#)
 - VoIP dial peers, specifying [VR-378](#)
 - icpif command [VR-378](#)
 - idle-voltage command [VR-379](#)
 - ignore command [VR-381](#)
 - image encoding command [VR-383](#)
 - image resolution command [VR-385](#)
 - imaging encoding command [VR-383](#)
 - impedance command [VR-387](#)
 - incoming called-number command [VR-388](#)
 - indexes, master [viii](#)
 - info-digits command [VR-390](#)
 - information-type command [VR-391](#)
 - input gain command [VR-392](#)
 - interface (RLM server) command [VR-394](#)
 - interface configuration mode, summary of [xiv](#)
 - IP
 - addresses
 - configuring [VR-394](#)
 - ip circuit command [VR-396](#)
 - ip precedence (dial-peer) command [VR-396](#)
 - ip udp checksum command [VR-397](#)
 - ISDN
 - subscriber line [VR-402](#)
 - telephone number destination pattern [VR-244](#)
 - isdn bind-l3 command [VR-398](#)
 - ISDN BRI
 - line power supply, configuring [VR-413](#)
 - state, displaying [VR-695](#)
 - isdn contiguous-bchan command [VR-399](#)
 - isdn global-disconnect command [VR-400](#)
 - isdn i-number command [VR-402](#)
 - isdn network-failure-cause command [VR-403](#)
 - ISP (Internet service provider) address,
 - configuring [VR-1014](#)
 - IVR (interactive voice response)
 - dynamic audio files [VR-411](#)
 - file autoload [VR-406, VR-408, VR-409](#)
 - script, displaying [VR-662](#)
 - ivr autoload command [VR-406](#)
 - ivr autoload mode command [VR-409](#)
 - ivr autoload retry command [VR-408](#)
 - ivr prompt memory command [VR-411](#)

K

keepalives

signaling packet interval, configuring [VR-874](#)

L

line-power command [VR-413](#)

link (RLM) command [VR-415](#)

loopback (T1 controller) command [VR-419](#)

loop-detect command [VR-421](#)

loss-plan command [VR-422](#)

lrq forward-queries command [VR-424](#)

lrq reject-unknown-prefix command [VR-427](#)

lrq timeout blast window command [VR-429](#)

lrq timeout seq delay command [VR-430](#)

M

max-conn command [VR-431](#)

max-connection command [VR-432](#)

max-forwards command [VR-434](#)

max-redirects command [VR-435](#)

MDN (message disposition notice)

address for, specifying [VR-495](#)

off-ramp gateway process, specifying [VR-485](#)

requesting [VR-436](#)

mdn command [VR-436](#)

media gateway

package capability, configuring [VR-441, VR-448](#)

messages

raw telephone equipment, displaying [VR-766](#)

MGCP (Media Gateway Control Protocol) statistical
counters, resetting [VR-179](#)

mgcp block-newcalls command [VR-438](#)

mgcp call-agent command [VR-439](#)

mgcp codec command [VR-440](#)

mgcp command [VR-437](#)

mgcp default-package command [VR-441](#)

mgcp dtmf-relay command [VR-443](#)

mgcp ip-tos command [VR-444](#)

mgcp max-waiting-delay command [VR-446](#)

mgcp modem passthru command [VR-447](#)

mgcp package-capability command [VR-448](#)

mgcp playout command [VR-450](#)

mgcp quality-threshold command [VR-451](#)

mgcp request retries command [VR-453](#)

mgcp request timeout command [VR-454](#)

mgcp restart-delay command [VR-455](#)

mgcp sdp simple command [VR-456](#)

mgcp vad command [VR-457](#)

MIB, descriptions online [viii](#)

microcode reload controller command [VR-458](#)

mmoip aaa global-password command [VR-459](#)

mmoip aaa method fax accounting command [VR-460](#)

mmoip aaa method fax authentication command [VR-462](#)

mmoip aaa receive-accounting enable command [VR-464](#)

mmoip aaa receive-authentication enable
command [VR-465](#)

mmoip aaa receive-id primary command [VR-466](#)

mmoip aaa receive-id secondary command [VR-468](#)

mmoip aaa send-accounting enable command [VR-470](#)

mmoip aaa send-authentication enable command [VR-471](#)

mmoip aaa send-id primary command [VR-472](#)

mmoip aaa send-id secondary command [VR-474](#)

mode (Voice over ATM) command [VR-476](#)

mode ccs command [VR-478](#)

modem passthrough (dial-peer) command [VR-479](#)

modem passthrough (voice-service) command [VR-481](#)

modes

See command modes

mta receive aliases command [VR-483](#)

mta receive generate-mdn command [VR-485](#)

mta receive maximum-recipients command [VR-487](#)

mta send mail-from command [VR-489](#)

mta send origin-prefix command [VR-491](#)

mta send postmaster command [VR-493](#)

mta send return-receipt-to command [VR-495](#)

mta send server command [VR-497](#)
 mta send subject command [VR-499](#)
 music-threshold command [VR-500](#)

N

Nariwake service registered caller ring cadence,
 configuring [VR-564](#)
 network-clock base-rate command [VR-502](#)
 network clocks
 base rate, configuring [VR-502](#)
 setings, displaying [VR-690](#)
 switch delay time, setting [VR-503](#)
 network-clock-switch command [VR-503](#)
 non-linear command [VR-504](#)
 notes, usage in text [x](#)
 nsap command [VR-505](#)
 numbering-type command [VR-508](#)
 num-exp command [VR-506](#)

O

OOS (out-of-service) signal
 connection restart timeout, specifying [VR-886](#)
 lost signal delay time, specifying [VR-894](#)
 pattern, specifying [VR-880](#), [VR-890](#), [VR-892](#)
 standby state, configuring [VR-888](#)
 timing parameters, specifying [VR-884](#)
 operation command [VR-510](#)
 output attenuation command [VR-511](#)

P

platforms, supported
 Feature Navigator, identify using [xix](#)
 release notes, identify using [xix](#)
 playout-delay (dial peer) command [VR-513](#)
 playout-delay (voice-port) command [VR-517](#)
 playout-delay command [VR-513](#), [VR-517](#)

playout-delay mode (dial-peer) command [VR-519](#)
 playout-delay mode (voice-port) command [VR-521](#)
 port (dial peer) command [VR-523](#)
 port (voice) command [VR-523](#)
 port media command [VR-526](#)
 port signal command [VR-527](#)
 pots call-waiting command [VR-528](#)
 pots country command [VR-529](#)
 pots dialing-method command [VR-531](#)
 pots disconnect-supervision command [VR-533](#)
 pots disconnect-time command [VR-535](#)
 pots distinctive-ring-guard-time command [VR-537](#)
 pots encoding command [VR-539](#)
 pots line-type command [VR-541](#)
 pots ringing-freq command [VR-543](#)
 pots silence-time [VR-545](#)
 pots silence-time command [VR-545](#)
 pots tone-source [VR-547](#)
 pots tone-source command [VR-547](#)
 pre-dial delay command [VR-549](#)
 preference command [VR-550](#)
 prefix command [VR-553](#)
 pri-group command [VR-555](#)
 pri-group nec-fusion command [VR-557](#)
 privileged EXEC mode, summary of [xiv](#)
 progress_ind command [VR-558](#)
 prompts, system [xiv](#)
 protocol rlm port command [VR-417](#)
 proxy h323 command [VR-560](#)

Q

QoS (quality of service)
 dial peer, specifying [VR-565](#)
 H.323 gateway, enabling on [VR-375](#)
 RSVP attempted call statistics, displaying [VR-686](#)
 RSVP synchronization, displaying [VR-684](#)
 VoIP dial peer, defining for [VR-3](#)
 question mark (?) command [xiv](#)

R

RADIUS accounting attributes

overloaded Acct-Session-Id field [VR-353](#)

vendor specific [VR-355](#)

register e164 command [VR-562](#)

registered-caller ring command [VR-564](#)

release notes

See platforms, supported

req-qos command [VR-565](#)

reset command [VR-566](#)

resource threshold command [VR-567](#)

response-timeout [VR-569](#)

response-timeout command [VR-569](#)

retry (SIP user-agent) command [VR-575](#)

retry-delay command [VR-571](#)

retry-limit command [VR-573](#)

RFC

full text, obtaining [viii](#)

RFC 821, envelope-from address or Return-Path address [VR-489](#)

ringback tone, enabling [VR-1001](#)

ring cadence command [VR-578](#)

ring command [VR-576](#)

ring frequency command [VR-580](#)

ringing

distinctive, configuring [VR-576](#)

timeout value, configuring [VR-967](#)

ring number command [VR-582](#)

RLM (Redundant Link Manager)

enabling [VR-415](#)

group

latency display [VR-767](#)

status [VR-770](#)

timer values [VR-772](#)

roaming

matching pattern, configuring [VR-622](#)

roaming (settlement) command [VR-585](#)

roaming command [VR-584](#)

ROM monitor mode, summary of [xiv](#)

RS-366 video interface

statistics, displaying [VR-693](#)

RTSP (Real Time Streaming Protocol)

session history, keeping [VR-586, VR-587](#)

session records, displaying [VR-774](#)

rtsp client session history duration command [VR-586](#)

rtsp client session history records command [VR-587](#)

rule [VR-588](#)

rule command [VR-588](#)

S

security command [VR-590](#)

sequence-numbers command [VR-592](#)

server (RLM) command [VR-594](#)

server registration-port command [VR-596](#)

server trigger command [VR-597](#)

session group command [VR-600](#)

session protocol (VoFR) command [VR-603](#)

session protocol aal2 command [VR-605](#)

session protocol command [VR-601](#)

session protocol multicast command [VR-606](#)

sessions

SIP transport layer protocol [VR-616](#)

session target (VoATM) command [VR-607](#)

session target (VoFR) command [VR-610](#)

session target (VoIP) command [VR-613](#)

session transport command [VR-616](#)

set command [VR-617](#)

settle-call command [VR-618](#)

settlement command [VR-620](#)

settlement providers

attributes

displaying [VR-785](#)

specifying [VR-620](#)

connection attempt maximum, setting [VR-573](#)

delay between connection attempts, setting [VR-571](#)

gateway associated with [VR-246](#)

- roaming capability, enabling [VR-585](#)
- type, selecting [VR-1011](#)
- settlement roam-pattern command [VR-622](#)
- SGCP (Simple Gateway Control Protocol)
 - active connections, listing [VR-787](#)
 - call agent, defining [VR-625](#)
 - calls, terminating [VR-627](#)
 - daemon, starting [VR-623](#)
 - fax and modem passthrough, enabling [VR-631](#)
 - management-eligible endpoints, displaying [VR-789](#)
 - notify and delete message retries, specifying [VR-635](#)
 - quarantine buffer, disabling [VR-633](#)
 - request response timeout, specifying [VR-637](#)
 - retransmission timer algorithm, configuring [VR-641](#)
 - RSIP message, triggering [VR-639](#)
 - RTP transmission interval, configuring [VR-643](#)
 - statistics, clearing [VR-184](#)
 - statistics, displaying [VR-791](#)
 - TSE payload type, enabling [VR-645](#)
 - waiting delay, setting [VR-629](#)
- sgcp call-agent command [VR-625](#)
- sgcp command [VR-623](#)
- sgcp graceful-shutdown [VR-627](#)
- sgcp max-waiting-delay command [VR-629](#)
- sgcp modem passthru command [VR-631](#)
- sgcp quarantine-buffer disable command [VR-633](#)
- sgcp request retries command [VR-635](#)
- sgcp request timeout command [VR-637](#)
- sgcp restart command [VR-639](#)
- sgcp retransmit timer command [VR-641](#)
- sgcp timer command [VR-643](#)
- sgcp tse payload command [VR-645](#)
- show aal2 profile command [VR-647](#)
- show atm video-voice address command [VR-649](#)
- show backhaul-session-manager group command [VR-650](#)
- show backhaul-session-manager session command [VR-652](#)
- show backhaul-session-manager set command [VR-654](#)
- show call active command [VR-655](#)
- show call application voice command [VR-662](#)
- show call fallback cache command [VR-666](#)
- show call fallback config command [VR-668](#)
- show call fallback stats command [VR-669](#)
- show call history [VR-670](#)
- show call history command [VR-670](#)
- show call history video record command [VR-678](#)
- show call history voice record command [VR-679](#)
- show call resource voice stats command [VR-681](#)
- show call resource voice threshold command [VR-683](#)
- show call rsvp-sync conf command [VR-684](#)
- show call rsvp-sync stats command [VR-686](#)
- show cdapi command [VR-688](#)
- show ces clock-select command [VR-690](#)
- show connect command [VR-691](#)
- show controllers rs366 command [VR-693](#)
- show controllers timeslots command [VR-695](#)
- show controllers voice command [VR-697](#)
- show csm command [VR-701](#)
- show dhcp command [VR-708](#)
- show dial-peer video command [VR-708](#)
- show dial-peer voice command [VR-709](#)
- show dialplan incall number command [VR-712](#)
- show frame-relay vofr command [VR-719](#)
- show gatekeeper calls command [VR-722](#)
- show gatekeeper endpoints command [VR-724](#)
- show gatekeeper gw-type-prefix command [VR-726](#)
- show gatekeeper servers command [VR-729](#)
- show gatekeeper status command [VR-731](#)
- show gatekeeper zone prefix [VR-732](#)
- show gatekeeper zone prefix command [VR-732](#)
- show gatekeeper zone status command [VR-733](#)
- show gateway command [VR-735](#)
- show interface dspfarm dsp command [VR-737](#)
- show mgcp command [VR-742](#)
- show mgcp connection command [VR-745](#)
- show mgcp endpoint command [VR-747](#)
- show mgcp statistics command [VR-748](#)
- show num-exp command [VR-751](#)

- show pots csm command [VR-753](#)
- show pots status command [VR-754](#)
- show proxy h323 calls command [VR-758](#)
- show proxy h323 detail-call command [VR-759](#)
- show proxy h323 status command [VR-765](#)
- show rawmsg command [VR-766](#)
- show rlm group statistics command [VR-767](#)
- show rlm group status command [VR-770](#)
- show rlm group timer command [VR-772](#)
- show rtsp client session command [VR-774](#)
- show rudpv1 command [VR-781](#)
- show settlement command [VR-785](#)
- show sgcp connection command [VR-787](#)
- show sgcp endpoint command [VR-789](#)
- show sgcp statistics command [VR-791](#)
- show sip-ua command [VR-793](#)
- show translation-rule command [VR-812](#)
- show vfc cap-list command [VR-816](#)
- show vfc command [VR-815](#)
- show vfc default-file command [VR-817](#)
- show vfc directory command [VR-818](#)
- show vfc version command [VR-820](#)
- show video call summary command [VR-821](#)
- show voice busyout command [VR-822](#)
- show voice call command [VR-824](#)
- show voice dsp command [VR-828](#)
- show voice permanent-call command [VR-830](#)
- show voice port command [VR-834](#)
- show voice trunk-conditioning signaling command [VR-845](#)
- show voice trunk-conditioning supervisory command [VR-849](#)
- show vrm active_calls command [VR-852](#)
- show vrm vdevices command [VR-855](#)
- shut command [VR-863](#)
- shutdown (DS 1 link) commands [VR-865](#)
- shutdown (gatekeeper) command [VR-866](#)
- shutdown (RLM) command [VR-867](#)
- shutdown (settlement) command [VR-868](#)
- shutdown (voice-port) command [VR-870](#)
- shutdown command
 - dial-peer configuration [VR-864](#)
- signal command [VR-872](#)
- signal keepalive command [VR-874](#)
- signal pattern command [VR-876](#)
- signal sequence oos command [VR-880](#)
- signal timing idle suppress-voice command [VR-882](#)
- signal timing oos command [VR-884](#)
- signal timing oos restart command [VR-886](#)
- signal timing oos slave-standby command [VR-888](#)
- signal timing oos suppress-all command [VR-890](#)
- signal timing oos suppress-voice command [VR-892](#)
- signal timing oos timeout command [VR-894](#)
- signal-type command [VR-896](#)
- SIP (Session Initiation Protocol)
 - enabling [VR-899](#)
 - UA, configuring [VR-1008](#)
 - UA settings, displaying [VR-793](#)
- sip-server command [VR-898](#)
- sip-ua command [VR-899](#)
- snmp enable peer-trap poor-qov command [VR-901](#)
- station-id command [VR-927](#)
- Store and Forward Fax
 - AAA accounting method, defining [VR-460](#)
 - AAA authentication method, defining [VR-462](#)
 - email prefix header, adding [VR-491](#)
 - SMTP maximum recipients, specifying [VR-487](#)
- subcell multiplexing, enabling [VR-929](#)
- subcell-mux command [VR-929](#)
- supervisory disconnect anytime command [VR-931](#)
- supervisory disconnect command [VR-930](#)
- supervisory disconnect dualtone voice-class command [VR-933](#)

T

- T.120 data channels
 - H.323 gateway, enabling capabilities on [VR-376](#)

T1

- CCS cross-connect, configuring [VR-478](#)
- CCS frame-forwarding, configuring [VR-478](#)
- controller interface mode, configuring [VR-476](#)
- loopback test mode, setting [VR-419](#)
- loop detection, enabling [VR-421](#)
- microcode images, reloading [VR-458](#)
- out-of-service alarm [VR-5](#)
- signal levels, attenuating [VR-287, VR-288](#)
- Tab key, command completion [xiv](#)
- tdm-group command [VR-935](#)
- tech-prefix command [VR-937](#)
- telephone numbers
 - destination pattern, expanding [VR-506](#)
 - expansions, displaying [VR-751](#)
 - incoming called, specifying [VR-388](#)
 - variable length terminator, changing [VR-250](#)
 - workstation dial application, using [VR-940](#)
- test call fallback probe command [VR-939](#)
- test pots dial command [VR-940](#)
- test pots disconnect command [VR-941](#)
- test translation-rule command [VR-942](#)
- test voice port detector command [VR-944](#)
- test voice port inject-tone command [VR-947](#)
- test voice port loopback command [VR-950](#)
- test voice port relay command [VR-952](#)
- test voice port switch command [VR-955](#)
- test vrm busyout command [VR-957](#)
- test vrm reset command [VR-959](#)
- test vrm unbusyout command [VR-960, VR-962](#)
- threshold noise command [VR-962](#)
- timeouts call-disconnect command [VR-963](#)
- timeouts initial command [VR-964](#)
- timeouts interdigit command [VR-965](#)
- timeouts ringing [VR-967](#)
- timeouts ringing command [VR-967](#)
- timeouts wait-release command [VR-968](#)
- timers command [VR-970](#)
- timing clear-wait command [VR-971](#)
- timing delay-duration command [VR-973](#)
- timing delay-start command [VR-975](#)
- timing delay-with-integrity command [VR-977](#)
- timing dialout-delay command [VR-981](#)
- timing dial-pulse min-delay command [VR-979](#)
- timing digit command [VR-983](#)
- timing guard-out command [VR-985](#)
- timing hookflash-input command [VR-986](#)
- timing hookflash-out [VR-987](#)
- timing interdigit command [VR-988](#)
- timing percentbreak command [VR-990](#)
- timing pulse command [VR-991](#)
- timing pulse-interdigit command [VR-993](#)
- timing wink-duration command [VR-995](#)
- timing wink-wait command [VR-997](#)
- token-root-name command [VR-999](#)
- tone ringback command [VR-1001](#)
- tones
 - analog voice, specifying [VR-223](#)
 - frequency component, specifying [VR-333](#)
- ToS (type of service)
 - MGCP-controlled connections, enabling [VR-444](#)
- translate command [VR-1002](#)
- translate-outgoing command [VR-1004](#)
- translation-rule command [VR-1006](#)
- translations
 - rules
 - applying [VR-1002, VR-1004](#)
 - testing [VR-942](#)
 - rule tag name, creating [VR-1006](#)
 - VoIP rules
 - displaying [VR-812](#)
 - setting [VR-1060](#)
- transport command [VR-1008](#)
- TSI (transmitting subscriber identifier)
 - fax, displaying [VR-322](#)
- type (voice) command [VR-1009](#)
- type command [VR-1011](#)

U

unbundle vfc [VR-1013](#)
 unbundle vfc command [VR-1013](#)
 unbundle vfc EXEC command [VR-1013](#)
 url command [VR-1014](#)
 use-proxy command [VR-1016](#)
 user EXEC mode, summary of [xiv](#)

V

V.54 loopback detection, enabling [VR-245](#)
 vad (dial peer) command [VR-1018](#)
 VAD (voice activity detection) gaps
 changing [VR-1059](#)
 comfort noise, generating [VR-205, VR-286](#)
 enabling [VR-1018, VR-1020](#)
 vad command [VR-1020](#)
 VBR (variable bit rate)
 VoATM, configuring [VR-1021](#)
 vbr-rt command [VR-1021](#)
 VFC (voice feature card)
 cache entries, displaying [VR-815](#)
 default files, listing [VR-817](#)
 file directory, listing [VR-818](#)
 Flash memory
 adding file to list [VR-235](#)
 copying VCWare to [VR-221 to VR-222](#)
 deleting file from [VR-238](#)
 erasing [VR-299](#)
 list capacity, displaying [VR-816](#)
 version, displaying [VR-820](#)
 ViCM (Video Call Manager)
 status, displaying [VR-821](#)
 VoFR (Voice over Frame Relay)
 on DLCI, configuring [VR-1023](#)
 vofr command [VR-1023](#)
 voice call convert-discipi-to-prog [VR-1027](#)
 voice call send-alert command [VR-1028](#)
 voice-card command [VR-1029](#)
 voice class busyout command [VR-1030](#)
 voice class codec command [VR-1032](#)
 voice-class codec command [VR-1034, VR-1039](#)
 voice class dualtone command [VR-1036](#)
 voice class h323 command [VR-1038](#)
 voice class permanent [VR-1040](#)
 voice-class permanent (dial-peer) [VR-1042](#)
 voice-class permanent (dial-peer) command [VR-1042](#)
 voice-class permanent (voice-port) [VR-1044](#)
 voice class permanent command [VR-1040](#)
 voice-class permanent command [VR-1044](#)
 voice conferencing
 multicast session protocol, setting [VR-606](#)
 voice confirmation-tone [VR-1046](#)
 voice confirmation-tone command [VR-1046](#)
 voice-encap [VR-1047](#)
 voice gateway
 IP address, designating source [VR-365](#)
 voice-group [VR-1048](#)
 voice hardware
 status, displaying [VR-697](#)
 voice hunt [VR-1049](#)
 voice hunt user-busy command [VR-1049](#)
 voice local-bypass [VR-1051](#)
 voice local-bypass command [VR-1051](#)
 voice network
 failure cause codes, specifying [VR-403](#)
 release messages over, enabling [VR-400](#)
 voice packets
 UDP checksum, calculating [VR-397](#)
 voice path
 two-way, establishing [VR-1057](#)
 voice-port [VR-1052](#)
 voice-port busyout command [VR-1055](#)
 voice-port command [VR-1052](#)
 voice ports
 busyout function voice class, creating [VR-1030](#)
 busyout state

- configuring monitor [VR-38](#)
- displaying [VR-822](#)
- forcing [VR-36](#)
- placing in [VR-1055](#)
- prompted by remote RTR probe signal [VR-41](#)
- calls in progress, clearing [VR-186](#)
- codec voice class ID tag, assigning [VR-1032](#)
- configuration and status, displaying [VR-834](#), [VR-845](#), [VR-849](#)
- delay dial wink pulse duration, specifying [VR-977](#)
- delay signal duration, specifying [VR-973](#)
- detector-related functions, testing [VR-944](#)
- dialing type, specifying [VR-256](#)
- dial-out delay, specifying [VR-981](#)
- dial peer, associating [VR-523](#)
- disabling [VR-870](#)
- disabling settlement [VR-868](#)
- disconnect timeout value, configuring [VR-963](#)
- DTMF digit signal duration, specifying [VR-983](#)
- fax mode, forcing [VR-955](#)
- inactive seizure signal minimum wait, specifying [VR-971](#)
- initial digit timeout value, configuring [VR-964](#)
- interdigit timeout value, configuring [VR-965](#)
- loopback test [VR-950](#)
- maximum wink-signal duration, specifying [VR-995](#)
- maximum wink-wait duration, specifying [VR-997](#)
- on-hold music threshold, specifying [VR-500](#)
- outgoing seizure signal minimum delay, specifying [VR-975](#)
- output attenuation, configuring [VR-511](#)
- permanent calls on, displaying [VR-830](#)
- pulse interdigit timing, configuring [VR-993](#)
- relay-related functions, testing [VR-952](#)
- release process delay timeout, configuring [VR-968](#)
- signal gain values, specifying [VR-392](#)
- signal type, specifying [VR-872](#)
- terminating impedance, specifying [VR-387](#)
- test tone, injecting [VR-947](#)
- wink-like pulses, configuring [VR-979](#)

- voice quality
 - echo cancel, configuring [VR-288](#), [VR-290](#), [VR-292](#)
 - quality drop alarm, generating [VR-300](#)
- voice rtp send-recv command [VR-1057](#)
- voice service [VR-1058](#)
- voice service command [VR-1058](#)
- voice traffic bandwidth allocation, specifying [VR-326](#)
- voice vad-time [VR-1059](#)
- voice vad-time command [VR-1059](#)
- voip-incoming translation-rule [VR-1060](#)
- voip-incoming translation-rule command [VR-1060](#)

Z

- zone access command [VR-1062](#)
- zone bw [VR-1064](#)
- zone bw command [VR-1064](#)
- zone local [VR-1065](#)
- zone local command [VR-1065](#)
- zone prefix [VR-1067](#)
- zone prefix command [VR-1067](#)
- zone remote [VR-1070](#)
- zone remote command [VR-1070](#)
- zone subnet [VR-1072](#)
- zone subnet command [VR-1072](#)