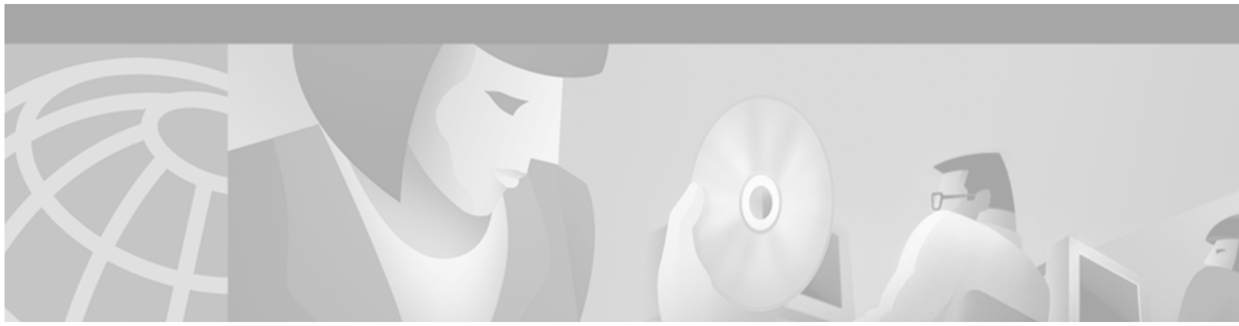


Cisco IOS Voice, Video, and Fax Commands: A Through C

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).
ds0-group-list	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

ip-signaling-addr	IP address of the H.323 node, used as the address to signal when establishing a call.
port	(Optional) Port number other than the endpoint Call Signaling well-known port number (1720).
gkid *gatekeeper-name*	Name of the local gatekeeper of whose zone this node is a member.
ras *ip-ras-addr*	(Optional) Node remote access server (RAS) signaling address. If omitted, the *ip-signaling-addr* parameter is used in conjunction with the RAS well-known port.
port	(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 *e164-address*	(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 *h323-id*	(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

string	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.
string	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

application-name	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 mmoip
 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

as-name	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-iua)# 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

asp-name	Names the current ASP.
as	The application server to which the ASP belongs.
as-name	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 alives

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-iua)# 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-iua)# 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:

```
interface atm0
 atm scramble-enable
```

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).
esi-address	(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

name	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 TFP) 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 stastistics 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.
zone-name	Names the particular zone.
bandwidth-size	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 specifiy 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

bandwidth-size	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:

```
gatekeeper
 bandwidth remote 100000
```

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.
interface-number	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 *interface number* 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

ip-address	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.
codec-type	(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.
number	(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.
percent	(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.
milliseconds	(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

cadence-id	A tag to identify this cadence list. The range is from 1 to 10.
cycle-1-on-time	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.
cycle-1-off-time	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.
cycle-2-on-time	(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.
cycle-2-off-time	(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.
cycle-3-on-time	(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.
cycle-3-off-time	(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.
cycle-4-on-time	(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.
cycle-4-off-time	(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

time	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

time	The minimum on time of a tone that can be detected, in 10-millisecond increments. The range is from 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 *off* 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

time	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 3
```

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

bg-minutes	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:

```
call application cache reload time 30
```

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

application-name	Character string that defines the name of the application.
location	Location of the TCL file in URL format. Valid storage locations are TFTP, FTP, and Flash.
word	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 *word* 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

application-name	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

application-name	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:

```
configure terminal
  call application voice app_libretto_onramp9 accounting enable
```

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

application-name	The name of the application.
method-list-name	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

application-name	The name of the application.
method-list-name	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

application-name	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: *router-name.domain-name*.
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

application-name	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

application-name	The name of the application.
password	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

application-name	The name of the application to which the language parameters are being passed.
number	Tag that uniquely identifies an audio file. Valid entries are from 0 to 9.
language	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

name	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

application-name	The name of the application to which the redirect telephone number parameter is being passed.
number	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

application-name	The name of the application to which the **set-location** parameters are being passed.
language	Defines the language associated with the audio files. Possible values for this parameter are as follows: • **en** = English • **ch** = Mandarin • **sp** = Spanish
category	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).
location	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

application-name	The name of the application to which the UID length parameter is being passed.
number	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

application-name	The name of the application to which the warning time parameter is being passed.
number	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

number	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:

```
call fallback cache-size 120
```

When call fallback is already configured, the output is as follows:

```
call fall cache-size 128
Cache size left unchanged (can be changed only when Fallback is OFF (use no call fallback)
```

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

seconds	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

weight	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

number-of-packets	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:

```
call fallback jitter-probe num-packets 20
```

If the **call fallback** command has been enabled before configuring the number of jitter-probe packets, the output is as follows:

```
call fallback jitter-probe num-packets 20
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

precedence-value	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 *precedence* 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

name-of-chain	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:

```
call fallback key-chain secret
```

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

map	Specifies the fall back map. The valid range is from 1 to 16.
target *ip-address*	Specifies the target IP address.
ip-address1 ... ip-address7	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.

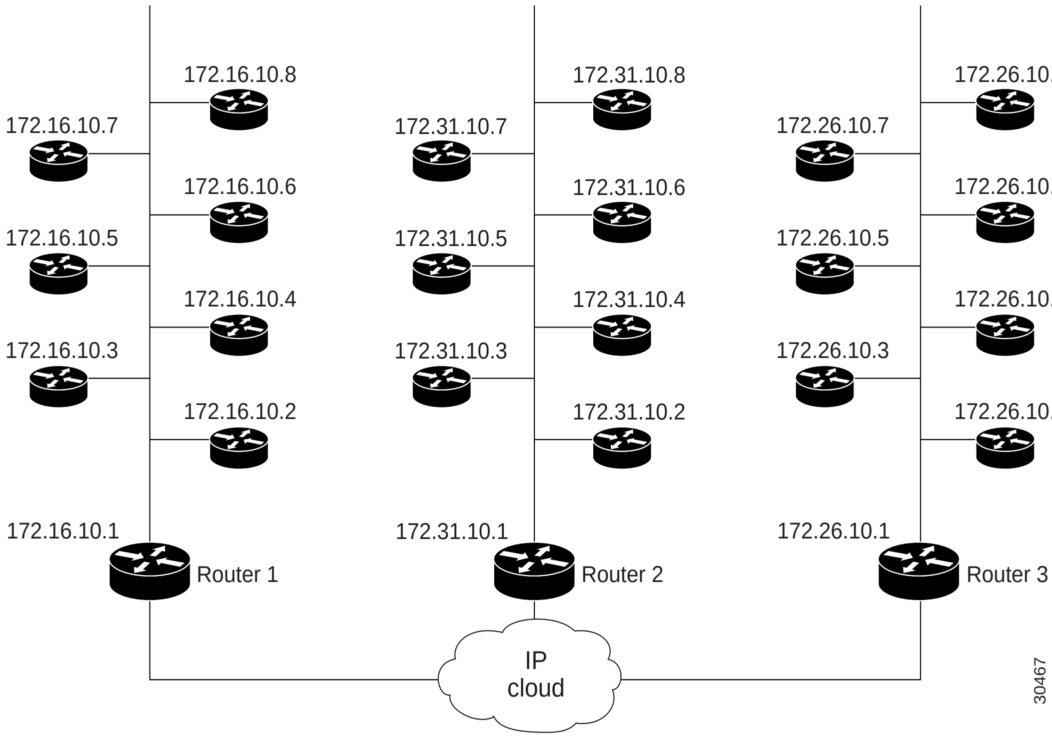
Usage Guidelines

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



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

map	Specifies the fall back map. The valid range is from 1 to 16.
target *ip-address*	Specifies the target IP address.
subnet *ip-network*	Specifies the subnet IP address.
netmask	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.

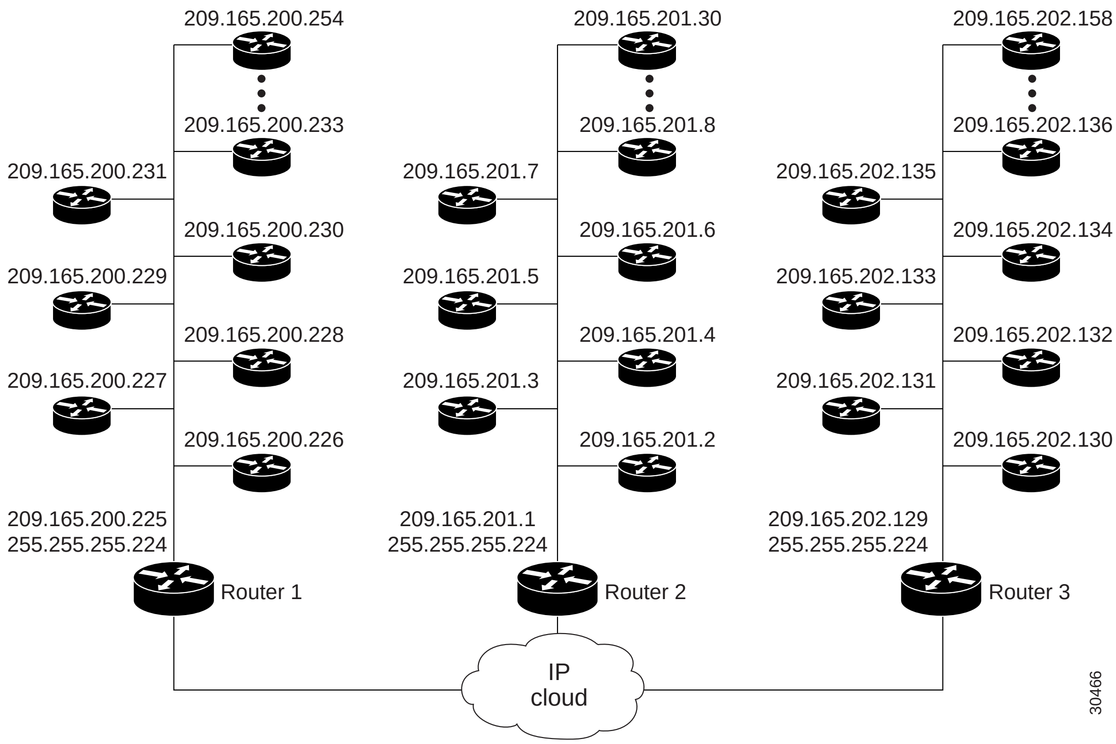
Usage Guidelines

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 fall back, use the **no** form of this command.

call fallback monitor

no call fallback monitor

Syntax Description

This command has no arguments or keywords.

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

seconds	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 (*seconds*). 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:

```
call fallback probe-timeout 120
```

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

delay-value	Sets the delay value. The valid range is from 1 to 2,147,483,647 milliseconds.
loss-value	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

threshold-value	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

seconds	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 *Cisco 800 Series Routers Software Configuration Guide*.

Examples

The following example disables call waiting:

```
no call-waiting
```

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

string	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

attenuation	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 (*string1* to *string2*).
sequence	Configures a sequence of discrete strings (*string1... string5*) 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.
string# ...	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

filename	Identifies the codec file stored in voice feature card (VFC) Flash memory.
slot-number	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 *filename*) 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.
slot	Slot number of the interface.
bay	(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

number	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 **ccc-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

ip-address	Internet protocol address of the backup Cisco CallManager.
DNS-name	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 *DNS-name* 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 *hh:mm*	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 *minutes*	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.
dlci	(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.
cidnumber	(Optional) If you have executed the **ccs encap frf11** command, the *cidnumber* 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.
dlci	(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.
cidnumber	(Optional) If you have executed the **ccs encap frf11** command, the *cidnumber* 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

period	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:

```
interface serial 0
 ces cell-loss-integration-period 1056
```

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

atm-interface	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.
name	The name of the ATM PVC.
vpi/	(Optional) The virtual path identifier value.
vci	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

bytes	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	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 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 stastistics 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 *group-name*	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

ip-address	(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:

```
clear call fallback cache 209.165.200.225
```

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 *number*. In this case, the additional options of **system-hwm** or **all** will not be available.
number	Clears an individual controller. Select the shelf (for Cisco ASRouters) /slot/port number in the following format: *shelf*/*slot*/*port*.
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 *all* 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
```

```
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       00:01:58
     23       pri           1       00:02:27
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       00:02:14
     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
```

```
      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
```

```
      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:
```

```
  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

slot/*port*	(Optional) Identifies the location (and thereby the identity) of a specific modem.
modem-group-number	(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*/*dspm*/*dsp*/*dsp-channel*]

Syntax Description

slot/dspm/dsp/dsp-channel	(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 *slot/dspm/dsp/dsp-channel* 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.
local-callID	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 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

slot/*port*	(Optional) The voice port slot number and port number. If you do not specify a voice port, all calls on all voice ports are cleared.

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:

```
Router# clear voice port 1/2
```

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

priority-number	Priority of the clock source. Values are 1 (high priority) to 4 (low priority).
interface	Specifies the interface to supply the clock source.
slot/port	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.
codec	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**—G729 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.
payload_size	(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.
codec	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**—G729 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.
payload_size	(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.
codec	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**—G729 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 13,200 bps.
bytes	(Optional) Specifies the number of bytes in the voice payload of each frame.
payload_size	(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 *codec* choices and other options were added.
12.0(5)XK	The **g729br8** and **pre-ietf** *codec* 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** *codec* choices were added for the Cisco MC3810 multiservice concentrator, and the keyword **pre-ietf** was deleted.
12.1(1)T	The codec 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** codec 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 **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

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 *profile-number* as an ITU-T type.
atmf	Specifies the *profile-number* as an ATMF type.
custom	Specifies the *profile-number* as a custom type.
profile-number	The available *profile-number* 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
codec	Enter one codec for the DSP. The possible *codec* entries depend on the *profile-number*. 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**—G726 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

value	Specifies the order of preference, with 1 being the most preferred and 14 being the least preferred.
codec_type	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.
payload-size	(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

id	A name for this connection.
atm	Specifies the ATM interface.
slot/port-1	The location of the ATM controller to be connected.
name of PVC/SVC	Specifies the permanent or switched virtual circuit.
vpi/vci	Specifies a virtual path identifier (VPI) and virtual channel identifier (VCI).
T1	Specifies a T1 port.
E1	Specifies an E1 port.
slot/port-2	The location of the T1 or E1 controller to be connected.
TDM-group-number	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

id	A name for this connection.
t1	Specifies a T1 port.
e1	Specifies an E1 port.
slot/port-1	The location of the first T1 or E1 controller to be connected. Valid values for *slot* and *port* are 0 and 1.
tdm-group-no-1	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.
slot/port-2	The location of the second T1 or E1 controller port to be connected. Valid values for *slot* are from 0 to 5, depending on the platform. Valid values for *port* are 0 to 3, depending on the platform and the presence of a network module.
tdm-group-no-2	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.

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.
digits	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.

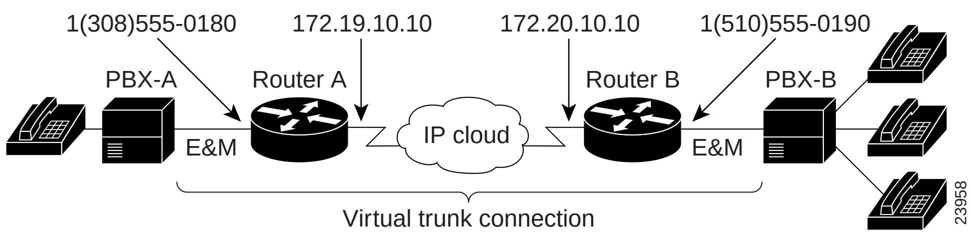
Release	Modification
12.0(3)XG	The **trunk** keyword was made available on the Cisco MC3810 multiservice concentrator. The **trunk answer-mode** option was added.
12.0(4)T	The **trunk** and **trunk answer-mode** additions were integrated in Cisco IOS Release 12.0(4)T.
12.0(7)XK	This command was unified 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

number	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

slot-number	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

slot-number	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

locale	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 *locale* are contained in Table 14. Keywords for ISDN PRI signaling are contained in 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 Eqypt, 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

id	Unique identification (ID) assigned to this cross-connection. The valid range is from 0 to 31.
controller-1	Type of the first controller (T1 0, T1 1, or E1)
tdm-group-no-1	Time-division multiplexing (TDM) group number assigned to the first controller.
controller-2	Type of the second controller (T1, E1 0, or E1 1).
tdm-group-no-2	TDM group number assigned to the second controller.

Pass-Through Traffic from a UIO Serial Port to a Trunk Controller

id	Unique ID assigned to this cross connection.
interface-serial	Number of the serial port, either 0 or 1.
controller	Type of the controller. Enter one of the following: T1 0, T1 1, E1 0, or E1 1.
tdm-group-no	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

number	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.