Cisco IOS Voice Command Reference - K through R

First Published: 2015-08-04

Last Modified: 2023-12-08

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

K

keepalive retries

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

To set the number of keepalive retries from Skinny Client Control Protocol (SCCP) to Cisco Unified CallManager, use the **keepalive retries**command in SCCP Cisco CallManager configuration mode. To reset this number to the default value, use the **no** form of this command.

keepalive retries *number*
no keepalive retries

Syntax Description

number	Number of keepalive attempts. Range is 1 to 32. Default is 3.

Command Default

3 keepalive attempts

Command Modes

SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Use this command to control the number of keepalive retries before SCCP confirms that the Cisco Unified CallManager link is down. When SCCP confirms that the Cisco Unified CallManager link is down (if the number of keepalive messages sent without receiving an Ack reaches the keepalive retries value), Cisco Unified CallManager switchover is initiated.

Note The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the keepalive retries to meet your needs.

Examples

The following example sets the number of times that a Cisco Unified CallManager retries before confirming that the link is down to seven:

Router(conf-sccp-ccm) # **keepalive retries 7**

Related Commands

Command	Description
keepalive timeout	Sets the length of time between keepalive messages from SCCP to Cisco Unified CallManager.
sccp ccm group	Creates a Cisco CallManger group and enters the SCCP Cisco CallManager configuration mode.

keepalive target

To identify Session Initiation Protocol (SIP) servers that will receive keepalive packets from the SIP gateway, use the **keepalive target** command in SIP user-agent configuration mode. To disable the **keepalive target**command behavior, use the **no** form of this command.

keepalive target {{{**ipv4:***address* | **ipv6:***address*}[{:*port*}] | **dns:***host*} | [{**tcp** [{**tls**}]}] | [{**udp**}] | [{**secondary**}]}
no keepalive target [**secondary**]

Syntax Description

ipv4: *address*	IP address (in IP version 4 format) of the primary or secondary SIP server to monitor.
ipv6: *address*	IPv6 address of the primary or secondary SIP server to monitor.
: *port*	(Optional) SIP port number. Default SIP port number is 5060.
dns: *hostname*	DNS hostname of the primary or secondary SIP server to monitor.
tcp	(Optional) Sends keepalive packets over TCP.
tls	(Optional) Sends keepalive packets over Transport Layer Security (TLS).
udp	(Optional) Sends keepalive packets over User Datagram Protocol (UDP).
secondary	(Optional) Associates the IP version 4 address or the domain name system (DNS) hostname to a secondary SIP server to monitor.

Command Default

No keepalives are sent by default from SIP gateway to SIP gateway. The SIP port number is 5060 by default.

Command Modes

SIP user-agent configuration (config-sip-ua)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

The primary or secondary SIP server addresses are in the following forms: dns:example.sip.com or ipv4:172.16.0.10.

Examples

The following example sets the primary SIP server address and defaults to the UDP transport:

```
sip-ua
 keepalive target ipv4:172.16.0.10
```

The following example sets the primary SIP server address and the transport to UDP:

```
sip-ua
 keepalive target ipv4:172.16.0.10 udp
```

The following example sets both the primary and secondary SIP server address and the transport to UDP:

```
sip-ua
 keepalive target ipv4:172.16.0.10 udp
 keepalive target ipv4:172.16.0.20 udp secondary
```

The following example sets both the primary and secondary SIP server addresses and defaults to the UDP transport:

```
sip-ua
 keepalive target ipv4:172.16.0.10
 keepalive target ipv4:172.16.0.20 secondary
```

The following example sets the primary SIP server address and the transport to TCP:

```
sip-ua
 keepalive target ipv4:172.16.0.10 tcp
```

The following example sets both the primary and secondary SIP server addresses and the transport to TCP:

```
sip-ua
 keepalive target ipv4:172.16.0.10 tcp
 keepalive target ipv4:172.16.0.20 tcp secondary
```

The following example sets the primary SIP server address and the transport to TCP and sets security to TLS mode:

```
sip-ua
 keepalive target ipv4:172.16.0.10 tcp tls
```

The following example sets both the primary and secondary SIP server addresses and the transport to TCP and sets security to the TLS mode:

```
sip-ua
 keepalive target ipv4:172.16.0.10 tcp tls
 keepalive target ipv4:172.16.0.20 tcp tls secondary
```

Related Commands

Command	Description
busyout monitor keepalive	Selects a voice port or ports to be busied out in cases of a keepalive failure.
keepalive trigger	Sets the trigger count to the number of Options message requests that must consecutively receive responses from the SIP servers in order to unbusy the voice ports when in the down state.
retry keepalive	Sets the retry keepalive count for retransmission.
timers keepalive	Sets the timers keepalive interval between sending Options message requests when the SIP server is active or down.

keepalive timeout

To set the length of time between keepalive messages from Skinny Client Control Protocol (SCCP) to Cisco Unified CallManager, use the **keepalive timeout**command in SCCP Cisco CallManager configuration mode. To reset the length of time to the default value, use the **no** form of this command.

keepalive timeout *seconds*
no keepalive timeout

Syntax Description

seconds	Time between keepalive messages. Range is 1 to 180. Default is 30.

Command Default

30 seconds

Command Modes

SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Whenever SCCP sends the keepalive message to the Cisco Unified CallManager, it initiates this timer. Once the timeout occurs, it sends the next keepalive message unless the number of keepalive (messages without an Ack) reaches the number set by the **keepalive retries** command. As of now, the SCCP protocol uses the value provided by the Cisco Unified CallManager.

Note The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the keepalive timeout value to meet your needs.

Examples

The following example sets the length of time between Cisco Unified CallManager keepalive messages to 120 seconds (2 minutes):

Router(config-sccp-ccm)# **k eepalive timeout 120**

Related Commands

Command	Description
keepalive retries	Sets the number of keepalive retries from SCCP to Cisco Unified CallManager.
sccp ccm group	Creates a Cisco CallManger group and enters SCCP Cisco CallManager configuration mode.

keepalive trigger

The trigger count represents the number of Options message requests that must consecutively receive responses from the SIP servers when in the down state in order to unbusy the voice ports, use the **keepalive trigger** command in SIP user agent configuration mode. To restore to the default value of 3 seconds, use the **no** form of this command.

keepalive trigger *count*
no keepalive trigger *count*

Syntax Description

count	Keepalive trigger value in the range from 1 to 10. The default value is 3.

Command Default

The default value for the keepalive trigger is 3.

Command Modes

SIP user agent configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Sets the count to represent the number of Options message requests that must be consecutively receive responses from the SIP servers in order to unbusy the voice ports when in the down state. The default is 3.

Examples

The following example sets a time interval after the number of Options message requests that must consecutively receive responses from the SIP servers in order to unbusy the voice ports when in the down state. The trigger interval is set to 8 in the following example:

```
sip-ua
 keepalive trigger 8
```

Related Commands

Command	Description
busyout monitor keepalive	Selects a voice port or ports to be busied out in cases of a keepalive failure.
keepalive target	Identifies a SIP server that will receive keepalive packets from the SIP gateway.
retry keepalive	Sets the retry keepalive for retransmission.
timers keepalive	Sets the time interval between sending Options message requests when the SIP server is active or down.

L

link (RLM)

To enable a Redundant Link Manager (RLM) link, use the **link** command in RLM configuration mode. To disable this function, use the **no** form of this command.

link {**hostname** *name* | **address** *ip-address*} **source** *loopback-source* **weight** *factor*
no link {**hostname** *name* | **address** *ip-address*} **source** *loopback-source* **weight** *factor*

Syntax Description

hostname name	RLM host name. If host name is used, RLM looks up the DNS server periodically for the host name configured until lookup is successful or the configuration is removed.
address *ip -address*	IP address of the link.
source *loopback -source*	Loopback interface source. We recommend that you use the loopback interface as the source, so that it is independent of the hardware condition. Also, the source interface should be different in every link to avoid falling back to the same routing path. If you intend to use the same routing path for the failover, a single link is sufficient to implement it.
weight *factor*	An arbitrary number that sets link preference. The higher the weighting factor number assigned, the higher priority it gets to become the active link. If all entries have the same weighting factor assigned, all links are treated equally. There is no preference among servers according to the assumption that only one server accepts the connection requests at any given time. Otherwise, preferences are extended across all servers.

Command Default

Disabled

Command Modes

RLM configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Usage Guidelines

This command is a preference-weighted multiple entries command. Within the same server, the link preference is specified in weighting.

Examples

The following example specifies the RLM group (network access server), device name, and link addresses and their weighting preferences:

```
rlm group 1
 server r1-server
  link address 10.1.4.1 source Loopback1 weight 4
  link address 10.1.4.2 source Loopback2 weight 3
```

listen-port (SIP)

To configure the listen ports used for SIP protocols, use the **listen-port** command in **voice service voip/sip** configuration mode. To reset port use to its default value, use the **no** form of this command.

listen-port [**non-secure** | **secure**] *port-number*
no listen-port [**non-secure** | **secure**]

Syntax Description

secure	Specifies the TLS port value.
non-secure	Specifies the TCP/UDP port value.
port-number	Port number. Range: 1–65535. The default for UDP/TCP is 5060; the default for TLS is 5061.

Command Default

The port number is set to the default value based on the transport layer protocol used.

Command Modes

SIP configuration mode (config-serv-sip)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **listen-port** command is configurable on incoming SIP calls, and is applicable for both TDM-IP gateway and CUBE (IPIPGW). The CUBE gateway port number defined in global configuration will be used for In leg . Before configuring the SIP listen port for TCP/UDP/TLS, SIP service should be shut down using the **shutdown** in SIP configuration mode. If SIP service is not shut down, the **listen-port** command flashes an error message saying "shutdown SIP service before changing SIP listen port". This ensures that there are no active calls when the SIP listen port is changed. The **non-secure** keyword is supported on images, and both the **secure** and **non-secure** keywords are supported on Crypto images.

The following restrictions apply:

- Configuring the SIP listen port on a dial-peer basis is not supported.
- Configuring same listening port for both UDP/TCP and TLS is not allowed.
- Configuring the SIP listen port to a port that is already in use is not supported and results in an error message.
- Changing SIP listen port when Transport services (TCP/UDP/TLS) are shut down, will not close or reopen the port. The result is that only the new port number is updated. The new port will be bound when Transport services (TCP/UDP/TLS) is enabled.

Examples

The following example shows the port number on a Crypto image being changed to port 2000:

```
Router(config-serv-sip)# listen-port secure 2000
```

The following example shows the port number being reset to the TLS default port:

```
Router(config-serv-sip)# no listen-port
```

Related Commands

Command	Description
shutdown	Disables the port.

listen-port (tenant)

To set a specific SIP listen port in a tenant configuration, use the **listen-port** command in voice class tenant configuration mode. By default, tenant level listen port is not set and global level SIP listen port is used. To disable tenant level listen port, use the **no** form of this command.

listen-port { **secure** *port-number* | **non-secure** *port-number* }
no listen-port { **secure** *port-number* | **non-secure** *port-number* }

Syntax Description

secure	Specifies the TLS port value.
non-secure	Specified the TCP/UDP port value.
port-number	• Secure port number range: 1—65535. • Non-secure port number range: 5000—5500. **Note** Port range is restricted to avoid conflicts with RTP media ports that also use UDP transport.

Command Default

The port number will not be set to any default value.

Command Modes

Voice Class Tenant configuration mode

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1a	This command is introduced.

Usage Guidelines

Before the introduction of this feature, it was only possible to configure the listen port for SIP signaling at the global level (see listen-port (SIP)) and this value could only be changed if the call processing service was shut down first. It is now possible to specify a listen port for both secure and non-secure traffic within a tenant configuration, allowing SIP trunks to be selected more flexibly. Tenant listen ports may be changed without shutting down the call processing service, provided that there are no active calls on the associated trunk. If the listen port configuration is removed, all active connections associated with the port are closed.

For reliable call processing, ensure that signaling and media interface binding is configured for all tenants that include a listen port and also that interface binding (for VRF and IP address) and listen port combinations are unique across all tenants and global configurations.

Examples

The following is a configuration example for **listen-port***secure*:

```
Router(config)#voice class tenant 1
VOICECLASS configuration commands:
  aaa                    sip-ua AAA related configuration
  authentication         Digest Authentication Configuration
  credentials            User credentials for registration
  ...
  ...
  listen-port           Configure UDP/TCP/TLS SIP listen port (have bind
                        configured under this tenant for the config to take
                        effect)
```

```
  ...

Router(config-class)#listen-port ?
  non-secure  Change UDP/TCP SIP listen port (have bind configured under this
              tenant for the config to take effect)
  secure      Change TLS SIP listen port (have bind configured under this
              tenant for the config to take effect)

Router(config-class)#listen-port secure ?
  <0-65535>  Port-number

Router(config-class)#listen-port secure 5062
```

The following is a configuration example for **listen-port***non-secure*:

```
Router(config)#voice class tenant 1
VOICECLASS configuration commands:
  aaa                   sip-ua AAA related configuration
  authentication        Digest Authentication Configuration
  credentials           User credentials for registration
  ...
  ...
  listen-port          Configure UDP/TCP/TLS SIP listen port (have bind
                       configured under this tenant for the config to take
                       effect)
 ...

Router(config-class)#listen-port ?
  non-secure  Change UDP/TCP SIP listen port (have bind configured under this
              tenant for the config to take effect)
  secure      Change TLS SIP listen port (have bind configured under this
              tenant for the config to take effect)

Router(config-class)#listen-port non-secure ?
  <5000-5500>  Port-number

Router(config-class)#listen-port non-secure 5404
```

The following is a configuration example for **no listen-port**:

```
Router(config-class)# no listen-port ?
  non-secure  Change UDP/TCP SIP listen port (have bind configured under this
              tenant for the config to take effect)
  secure      Change TLS SIP listen port (have bind configured under this
              tenant for the config to take effect)

Router(config-class)#no listen-port secure ?
  <0-65535>  Port-number

Router(config-class)#no listen-port secure
```

Related Commands

Command	Description
call service stop	Shutdown SIP service on CUBE.
bind	Binds the source address for signaling and media packets to the IPv4 or IPv6 address of a specific interface.

lmr duplex half

To have the voice path for a voice port operate in half duplex mode, use the **lmr duplex half** command in voice-port configuration mode. To return to the default, use the **no** form of this command.

lmr duplex half
no lmr duplex half

Syntax Description

This command has no arguments or keywords.

Command Default

Full duplex mode

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

When a radio system is receiving voice traffic from the radio, operating the voice path in half duplex mode prevents the speaker from being interrupted and prevents the voice stream from being fed back to itself.

Examples

In the following example, the voice path for voice port 1/0/0 on a Cisco 3700 series router is set to operate in half duplex mode:

```
voice-port 1/0/0
 lmr duplex half
```

lmr e-lead

To define the use of the E-lead in signaling between the ear and mouth (E&M) voice port on the router and the attached Land Mobile Radio (LMR) device, use the **lmr e-lead**command in voice-port configuration mode. To return to the default use of the E-lead, use the **no** form of this command.

lmr e-lead {**inactive** | **seize** | **voice**}
no lmr e-lead {**inactive** | **seize** | **voice**}

Syntax Description

inactive	Specifies that the router never sends a seize signal on the E-lead to the LMR device. The router sends voice packets to LMR devices.
seize	Specifies that for PLAR and multicast connections, the router sends a seize signal on the E-lead when the LMR port is connected and removes the seize signal from the E-lead when the LMR port is not involved in a VoIP connection. This is the default. Specifies that for connection trunk connections, the router does not send a seize signal when the LMR port is connected. Instead, if the trunk connection is up, the M-lead signal from the far-end router is passed through as the E-lead on the near-end router. When the M-lead is dropped on the far-end router and the trunk connection is still up, the E-lead is dropped on the near-end router.
voice	Specifies that the router sends a seize signal on the E-lead only when it receives voice packets from the network. When no packets are detected on the network, the seize signal is removed from the E-lead.

Command Default

seize

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **lmr e-lead** command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is LMR. The **lmr e-lead** command is effective only if the attached LMR device operates under E-lead control. Use the **lmr e-lead** command to configure the voice port when using private line, automatic ringdown (PLAR) connections. The E-lead connects to the Push To Talk (PTT) of the LMR system.

Examples

In the following example, packet transmission from the E&M voice port on a Cisco 3745 to an attached LMR radio system is disabled:

```
lmr e-lead inactive
```

Related Commands

Command	Description
lmr m-lead	Defines the use of the M-lead in signaling between the E&M voice port on the router and the attached LMR device.

lmr ip-vad

To configure the Land Mobile Radio (LMR) digital signal processor (DSP) on a Cisco 2800 series integrated services router to report a voice packet arrival event only if the packet contains voice energy, use the **lmr ip-vad** command in voice-port configuration mode. To disable this feature, use the **no** form of this command.

lmr ip-vad
no lmr ip-vad

Syntax Description

This command has no arguments or keywords.

Command Default

Any voice packet received from the IP network side triggers the DSP to report a voice packet arrival event to the Cisco IOS software.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **lmr ip-vad** command applies to a voice interface card (VIC) in a Cisco 2800 series integrated services router if the VIC is one of the following types of ear and mouth (E&M) interfaces:

- VIC2-2E/M with signal type LMR
- ds0-group created with signal type e&m-lmr under an E1 or T1 controller

The **lmr ip-vad** command configures the LMR DSP to report voice activity detection (VAD) status change events (rather than voice packet arrival events) for a supported voice interface in a Cisco 2800 series integrated services router.

Examples

The following example shows a sequence of commands that can be used to configure a voice port so that a voice packet arrival event is reported to the Cisco IOS software on the router only if the packet contains voice energy.

```
Router(config)# voice-port 1/1/0

Router(config-voiceport)# signal lmr

Router(config-voiceport)# lmr ip-vad
```

Related Commands

Command	Description
signal	Configures the type of signaling to be used for a voice port.
voice-port	Enters voice-port configuration mode.

lmr led-on

To use the ear and mouth (E&M) LED to indicate the E-lead and M-lead status, use the **lmr led-on** command in voice-port configuration mode. To return to the default use of the E&M LED, use the **no** form of this command.

lmr led-on
no lmr led-on

Syntax Description

This command has no arguments or keywords.

Command Default

The E&M LED indicates voice port activity only.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **lmr e-lead** command is available on an E&M voice port only if the signal type for that port is Land Mobile Radio (LMR). This command enables the use of the E&M LED to indicate the E-lead and M-lead status as follows:

- Red--E-lead active
- Green--M-lead active
- Yellow--Both E-lead and M-lead active

The default behavior of the E&M LED is to light up when there is activity on the voice port and to turn off when there is no activity.

Examples

The following example specifies that the E&M LED is used to indicate the E-lead and M-lead status:

```
voice-port 1/0/0
 lmr led-on
```

lmr m-lead

To define the use of the M-lead in signaling between the ear and mouth (E&M) voice port on the router and the attached Land Mobile Radio (LMR) device, use the **lmr m-lead**command in voice-port configuration mode. To return to the default use of the M-lead, use the **no** form of this command.

lmr m-lead {**inactive** | **audio-gate-in** | **dialin**}
no lmr m-lead {**inactive** | **audio-gate-in** | **dialin**}

Syntax Description

inactive	The router ignores signals sent by voice on the M-lead. The flow of voice packets is determined by voice activity detection (VAD). The router sends voice received from the LMR device. This is the default.
audio-gate-in	The router generates VoIP packets when a seize signal is detected on the M-lead. The router stops generating VoIP packets when the seize signal is removed from the M-lead.
dialin	When the LMR device is not involved in a VoIP connection, the first seize signal detected on the M-lead triggers the router to set up a VoIP connection. Once the connection is made, the router behaves as in the **audio-gate-in** option.

Command Default

inactive

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **lmr m-lead** command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is LMR. The **lmr e-lead** command is effective only if the attached LMR device operates under M-lead control. The M-lead corresponds to the Carrier Operated Relay (COR) of the LMR system, which indicates receive activity on the LMR system.

Examples

In the following example, an LMR radio system attached to the E&M voice port on a Cisco 3745 is allowed to transmit audio by first raising the E-lead, then transmitting:

```
lmr m-lead dialin
```

Related Commands

Command	Description
lmr e-lead	Defines the use of the E-lead in signaling between the E&M voice port on the router and the attached LMR device.

load-balance

To configure load balancing, use the **load-balance**command ingatekeeper configuration mode. To disable load balancing, use the **no** form of this command.

load-balance [**endpoints** *max-endpoints*] [**calls** *max-calls*] [**cpu** *max-cpu*] [**memory** *max-em-used*]
no load-balance [**endpoints** *max-endpoint* **s**] [**calls** *max-calls*] [**cpu** *max-cpu*] [**memory** *max-mem-used*]

Syntax Description

endpoints *max -endpoints*	(Optional) Maximum number of endpoints.
calls *max-calls*	(Optional) Maximum number of calls.
cpu *max -cpu*	(Optional) Maximum percentage of CPU utilization.
memory *max -mem-used*	(Optional) Maximum percentage of memory used.

Command Default

Load balancing is performed by the gatekeeper.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(2)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Usage Guidelines

Load balancing occurs when one gatekeeper reaches the default or the configured load level. Upon reaching the load-level threshold, the gatekeeper begins sending alternate gatekeeper information in Registration, Admission, and Status (RAS) messages, and the gateways then attempt to migrate from the loaded gatekeeper to its least busy alternate. The move is permanent; endpoints are not actively moved back to the original gatekeeper if it stabilizes. However, they may return to that gatekeeper if the new gatekeeper reaches a load threshold and transfers them again. The gatekeepers share the load, but they may not have equal shares. The process of load balancing allows for more effective zone management.

Examples

The following example configures load balancing:

```
load-balance endpoints 200 calls 100 cpu 75 memory 80
```

Related Commands

Command	Description
zone cluster local	Configures alternate gatekeepers for each zone.

local

To define the local domain, including the IP address and port that the border element (BE) should use for interacting with remote BEs, use the **local** command in Annex G configuration mode. To reset to the default, use the no form of this command.

local ip *ip-address* [**port** *local-port*]
no local ip

Syntax Description

ip *ip -address*	IP address of the local border element.
port *local -port*	(Optional) Port number of the local border element, which is used for exchanging Annex G messages. Default is 2099.

Command Default

Port number: 2099

Command Modes

Annex G configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The local IP address can be a virtual Hot Standby Routing Protocol (HSRP) address for high reliability and availability. You can configure multiple gatekeepers and BEs identically and use HSRP to designate a primary BE and other standby BEs. If the primary BE is down, a standby BE operates in its place.

Examples

The following example sets the IP address and port that the BE should use. (Note that this example uses a nonstandard port number. If you do not want to use a nonstandard port number, use the default value of 2099.)

```
Router(config)# call-router h323-annexg be20
Router(config-annexg)# local ip 121.90.10.80 port 2010
```

Related Commands

Command	Description
call -router	Enables the Annex G border element configuration commands.
show call -router status	Displays the Annex G BE status.

localhost

To globally configure Cisco IOS voice gateways, Cisco Unified Border Elements (Cisco UBEs), or Cisco Unified Communications Manager Express (Cisco Unified CME) to substitute a Domain Name System (DNS) hostname or domain as the localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers in outgoing messages, use the **localhost** command in voice service SIP configuration mode or voice class tenant configuration mode. To remove a DNS localhost name and disable substitution for the physical IP address, use the **no** form of this command.

localhost dns: [{*hostname.*}] *domain* [{**preferred**}]
no localhost

Syntax Description

dns: [*hostname.*]*domain*	Alphanumeric value representing the DNS domain (consisting of the domain name with or without a specific hostname) in place of the physical IP address that is used in the host portion of the From, Call-ID, and Remote-Party-ID headers in outgoing messages. This value can be the hostname and the domain separated by a period (**dns:** *hostname.domain*) or just the domain name (**dns:** *domain*). In both case, the **dns:** delimiter must be included as the first four characters.
preferred	(Optional) Designates the specified DNS hostname as preferred.

Command Default

The physical IP address of the outgoing dial peer is sent in the host portion of the From, Call-ID, and Remote-Party-ID headers in outgoing messages.

Command Modes

Voice service SIP configuration (conf-serv-sip).

Voice class tenant configuration (config-class).

Command History

Release	Modification
12.4(2)T	This command was introduced.
15.0(1)XA	This command was modified. The **preferred** keyword was added to specify the preferred localhost if multiple registrars are configured on a SIP trunk.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(1)T	This command was integrated into Cisco IOS Release 5.1(1)T.
15.6(2)T and IOS XE Denali 16.3.1	This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the **localhost** command in voice service SIP configuration mode to globally configure a DNS localhost name to be used in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages on Cisco IOS voice gateways, Cisco UBEs, or Cisco Unified CME. When multiple registrars are configured you can then use the **localhost preferred** command to specify which host is preferred.

To override the global configuration and specify DNS localhost name substitution settings for a specific dial peer, use the **voice-class sip localhost** command in dial peer voice configuration mode. To remove a globally configured DNS localhost name and use the physical IP address in the From, Call-ID, and Remote-Party-ID headers in outgoing messages, use the **no localhost** command.

Examples

The following example shows how to globally configure a preferred DNS localhost name using only the domain for use in place of the physical IP address in outgoing messages on all dial peers:

```
Router> enable
Router# configure
 terminal
Router(config)# voice
 service
 voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# localhost dns:example.com preferred
```

The following example shows how to globally configure a preferred DNS localhost name by specifying the hostname along with the domain for use in place of the physical IP address in outgoing messages on all dial peers:

```
Router> enable
Router# configure
 terminal
Router(config)# voice
 service
 voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# localhost dns:MyHostname.example.com preferred
```

Related Commands

Command	Description
authentication (dial peer)	Enables SIP digest authentication on an individual dial peer.
authentication (SIP UA)	Enables SIP digest authentication.
credentials (SIP UA)	Configures a Cisco UBE to send a SIP registration message when in the UP state.
registrar	Enables Cisco IOS SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar.
voice-class sip localhost	Configures settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages on an individual dial peer, overriding the global setting.

loopback (controller)

To set the loopback method for testing a T1 or E1 interface, use the **loopback** command in controller configuration mode. To reset to the default, use the **no** form of this command.

loopback {**diagnostic** | **local** {**payload** | **line**} | **remote** {**v54** **channel-group** *channel-number* | **iboc** | **esf** {**payload** | **line**}}}
no **loopback**

Syntax Description

diagnostic	Loops the outgoing transmit signal back to the receive signal.
local	Places the interface into local loopback mode.
payload	Places the interface into external loopback mode at the payload level.
line	Places the interface into external loopback mode at the line level.
remote	Keeps the local end of the connection in remote loopback mode.
v54 channel -group	Activates a V.54 channel-group loopback at the remote end. Available for both T1 and E1 facilities.
channel -number	Channel number for the V.54 channel-group loopback. Range is from 0 to 1.
iboc	Sends an inband bit-oriented code to the far end to cause it to go into line loopback.
esf	T1 or E1 frame type of Extended Super Frame (ESF). Only available under T1 or E1 controllers when ESF is configured on the controller. The following are keywords: • **payload** --Activates remote payload loopback by sending Facility Data Link (FDL) code. FDL is a 4-kbps out-of-band signaling channel in ESF. • **line** --Activates remote line loopback by sending FDL code.

Command Default

No loopback is configured.

Command Modes

Controller configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced as a controller configuration command for the Cisco MC3810.
12.0(5)T and 12.0(5)XK	This command was introduced as an ATM interface configuration command for the Cisco 2600 series and Cisco 3600 series.
12.0(5)XE	This command was introduced as an ATM interface configuration command for the Cisco 7200 series and Cisco 7500 series.

Release	Modification
12.0(5)XK and 12.0(7)T	This command was introduced as a controller configuration command for the Cisco 2600 series and Cisco 3600 series.
12.1(1)T	This command was modified as a controller configuration command for the Cisco 2600 series.

Usage Guidelines

You can use a loopback test on lines to detect and distinguish equipment malfunctions caused either by the line and channel service unit/digital service unit (CSU/DSU) or by the interface. If correct data transmission is not possible when an interface is in loopback mode, the interface is the source of the problem.

Examples

The following example sets the diagnostic loopback method on controller T1 0/0:

```
controller t1 0/0
 loopback diagnostic
```

The following example sets the payload loopback method on controller E1 0/0:

```
controller e1 0/0
 loopback local payload
```

loop-detect

To enable loop detection for T1, use the **loop-detect** command in controller configuration mode. To cancel loop detection, use the no form of this command.

loop-detect
no loop-detect

Syntax Description

This command has no arguments or keywords.

Command Default

Loop detection is disabled.

Command Modes

Controller configuration

Command History

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

Usage Guidelines

This command applies to Voice over Frame Relay and Voice over ATM.

Examples

The following example configures loop detection for controller T1 0:

```
controller t1 0
 loop-detect
```

Related Commands

Command	Description
loopback (interface)	Diagnoses equipment malfunctions between an interface and a device.

loss-plan

To specify the analog-to-digital gain offset for an analog Foreign Exchange Office (FXO) or Foreign Exchange Station (FXS) voice port, use the **loss-plan**command in voice-port configuration mode. To reset to the default, use the **no**form of this command.

loss-plan {**plan1** | **plan2** | **plan3** | **plan4** | **plan5** | **plan6** | **plan7** | **plan8** | **plan9**}
no **loss-plan**

Syntax Description

plan1	FXO: A-D gain = 0 dB, D-A gain = 0 dB. FXS: A-D gain = -3 dB, D-A gain = -3 dB.
plan2	FXO: A-D gain = 3 dB, D-A gain = 0 dB. FXS: A-D gain = 0 dB, D-A gain = -3 dB.
plan3	FXO: A-D gain = -3 dB, D-A gain = 0 dB. FXS: Not applicable.
plan4	FXO: A-D gain = -3 dB, D-A gain = -3 dB. FXS: Not applicable.
plan5	FXO: Not applicable. FXS: A-D gain = -3 dB, D-A gain = -10 dB.
plan6	FXO: Not applicable. FXS: A-D gain = 0 dB, D-A gain = -7 dB.
plan7	FXO: A-D gain = 7 dB, D-A gain = 0 dB. FXS: A-D gain = 0 dB, D-A gain = -6 dB.
plan8	FXO: A-D gain = 5 dB, D-A gain = -2 dB. FXS: Not applicable.
plan9	FXO: A-D gain = 6 dB, D-A gain = 0 dB. FXS: Not applicable.

Command Default

FXO: A-D gain = 0 dB, D-A gain = 0 dB (loss plan 1) FXS: A-D gain = -3 dB, D-A gain = -3 dB (loss plan 1)

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	The following additional signal level choices were added: plan 3, plan 4, plan 8, and plan 9.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command sets the analog signal level difference (offset) between the analog voice port and the digital signal processor (DSP). Each loss plan specifies a level offset in both directions--from the analog voice port to the DSP (A-D) and from the DSP to the analog voice port (D-A).

Use this command to obtain the required levels of analog voice signals to and from the DSP.

Examples

The following example configures FXO voice port 1/6 for a -3 dB offset from the voice port to the DSP and for a 0 dB offset from the DSP to the voice port:

```
voice-port 1/6
 loss-plan plan3
```

The following example configures FXS voice port 1/1 for a 0 dB offset from the voice port to the DSP and for a -7 dB offset from the DSP to the voice port:

```
voice-port 1/1
 loss-plan plan6
```

Related Commands

Command	Description
impedance	Specifies the terminating impedance of a voice port interface.
input gain	Specifies the gain applied by a voice port to the input signal from the PBX or other customer premises equipment.
output attenuation	Specifies the attenuation applied by a voice port to the output signal toward the PBX or other customer premises equipment.

lrq e164 early-lookup

To start the E.164 registered endpoint matching before via-zone routing is processed in the location request (LRQ) routing process, use the lrq e164 early-lookup command in gatekeeper configuration mode. To return to the default behavior, use the **no** form of this command.

lrq e164 early-lookup
no lrq e164 early-lookup

Syntax Description

This command has no arguments or keywords.

Command Default

The E.164 endpoint matching is done at the last stage of LRQ routing.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The default gatekeeper algorithm for IP-to-IP gateway selection is based on the via-zone prefix and tech-prefix match. Use the **lrq e164 early-lookup**command to start the E.164 matching process before via-zone routing to block nonregistered endpoints.

Examples

The following example causes the gatekeeper to notify the sending gatekeeper on receipt of an LRQ message that no terminating endpoints are available:

```
Router(config)#
gatekeeper
Router(config-gk)# lrq e164 early-lookup
```

lrq forward-queries

To enable a gatekeeper to forward location request (LRQ) messages that contain E.164 addresses that match zone prefixes controlled by remote gatekeepers, use the **lrq forward-queries** command in gatekeeper configuration mode. To disable this function, use the **no** form of this command.

lrq forward-queries
no lrq forward-queries

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the following platforms: Cisco 2500 series, Cisco 3600 series, and Cisco MC3810.

Usage Guidelines

LRQ forwarding is dependent on a Cisco nonstandard field that first appeared in Cisco IOS Release 12.0(3)T. This means that any LRQ message received from a non-Cisco gatekeeper or any gatekeeper running a Cisco IOS software image prior to Cisco IOS Release 12.0(3)T is not forwarded.

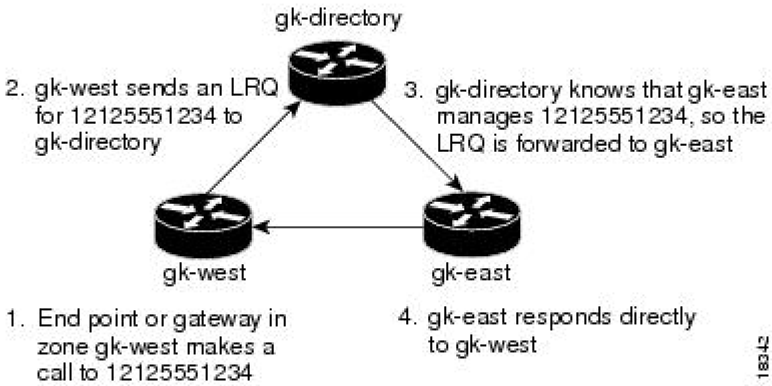
The routing of E.164-addressed calls is dependent on the configuration of zone prefix tables (for example, area code definitions) on each gatekeeper. Each gatekeeper is configured with a list of prefixes controlled by itself and by other remote gatekeepers. Calls are routed to the zone that manages the matching prefix. Thus, in the absence of a directory service for such prefix tables, you, the network administrator, may have to define extensive lists of prefixes on all the gatekeepers in your administrative domain.

To simplify this task, you can select one of your gatekeepers as the "directory" gatekeeper and configure that gatekeeper with the complete list of prefixes and the **lrq forward-queries** command. You can then simply configure all the other gatekeepers with their own prefixes and the wildcard prefix "*" for your directory gatekeeper.

This command affects only the forwarding of LRQ messages for E.164 addresses. LRQ messages for H.323-ID addresses are never forwarded.

Examples

The following example selects one gatekeeper as the directory gatekeeper. See the following figure:



Configuration on gk-directory

On the directory gatekeeper called gk-directory, identify all the prefixes for all the gatekeepers in your administrative domain:

```
zone local gk-directory cisco.com
zone remote gk-west cisco.com 172.16.1.1
zone remote gk-east cisco.com 172.16.2.1
zone prefix gk-west 1408.......
zone prefix gk-west 1415.......
zone prefix gk-west 1213.......
zone prefix gk-west 1650.......
zone prefix gk-east 1212.......
zone prefix gk-east 1617.......
lrq forward-queries
```

Configuration on gk-west

On the gatekeeper called gk-west, configure all the locally managed prefixes for that gatekeeper:

```
zone local gk-west cisco.com
zone remote gk-directory cisco.com 172.16.2.3
zone prefix gk-west 1408.......
zone prefix gk-west 1415.......
zone prefix gk-west 1213.......
zone prefix gk-west 1650.......
zone prefix gk-directory *
```

Configuration on gk-east

On the gatekeeper called gk-east, configure all the locally managed prefixes for that gatekeeper:

```
zone local gk-east cisco.com
zone remote gk-directory cisco.com 172.16.2.3
zone prefix gk-east 1212.......
zone prefix gk-east 1617.......
zone prefix gk-directory *
```

When an endpoint or gateway in zone gk-west makes a call to 12125551234, gk-west sends an LRQ message for that E.164 address to gk-directory, which forwards the message to gk-east. Gatekeeper gk-east responds directly to gk-west.

Related Commands

Command	Description
lrq reject -unknown-prefix	Enables the gatekeeper to reject all LRQ messages for zone prefixes that are not configured.

lrq lrj immediate-advance

To enable the Cisco IOS gatekeeper to immediately send a sequential location request (LRQ) message to the next zone after it receives a location reject (LRJ) message from a gatekeeper in the current zone, use the **lrq lrj immediate-advance** command in gatekeeper configuration mode. To disable this function, use the **no** form of this command.

lrq lrj immediate-advance
no lrq lrj immediate-advance

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(4)T	This command was introduced. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series in this release.

Usage Guidelines

In a network in which LRQ messages are forwarded through multiple gatekeepers along a single path, a single LRQ message sent from a gatekeeper could solicit multiple LRJ and location confirmation (LCF) responses. If an LRJ response is received first, a potentially unnecessary LRQ message could be sent to the next zone, increasing traffic.

To avoid this problem, perform the following:

- Configure the zone prefix to send sequential LRQ messages rather than to use the **blast** option, using the **zone prefix** command.
- Configure the sequential timer on each gatekeeper along the path, using the **timer lrq seq delay** command.

Examples

The following example enables the gatekeeper to immediately send a sequential LRQ message to the next zone after it receives an LRJ message from a gatekeeper in the current zone.

```
lrq lrj immediate-advance
```

Related Commands

Command	Description
timer lrq seq delay	Defines the time interval between successive sequential LRQ messages.
timer lrq window	Defines the time window during which the gatekeeper collects responses to one or more outstanding LRQ messages.
zone prefix	Adds a prefix to the gatekeeper zone list.

lrq reject-resource-low

To configure a gatekeeper to notify a sending gatekeeper on receipt of a location request (LRQ) message that no terminating endpoints are available, use the **lrq reject-resource-low** command in gatekeeper configuration mode. To disable this function, use the **no** form of this command.

lrq reject-resource-low
no lrq reject-resource-low

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco 7400 series.

Examples

The following example causes the gatekeeper to notify the sending gatekeeper on receipt of an LRQ message that no terminating endpoints are available:

```
Router(config)#
gatekeeper
Router(config-gk)# lrq reject-resource-low
```

lrq reject-unknown-circuit

To enable the gatekeeper to reject a location request (LRQ) message that contains an unknown destination circuit, use the **lrq reject-unknown-circuit**command in gatekeeper configuration mode. To disable the rejection, use the **no** form of this command.

lrq reject-unknown-circuit
no lrq reject-unknown-circuit

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The gatekeeper checks the destination circuit field in each LRQ message. If the field contains a circuit unknown to the gatekeeper and thiscommandis entered, the gatekeeper rejects the LRQ request. If thiscommand is disabled, the gatekeeper tries to resolve the alias without considering the circuit.

Examples

The following example causes the gatekeeper to reject unknown carriers in an LRQ request:

```
Router(config)# gatekeeper
Router(config-gk)# lrq reject-unknown-circuit
```

Related Commands

Command	Description
endpoint circuit-id h323id	Assigns a circuit to a non-Cisco endpoint.
show gatekeeper endpoint circuits	Displays the information of all registered endpoints for a gatekeeper.

lrq reject-unknown-prefix

To enable the gatekeeper to reject all location request (LRQ) messages for zone prefixes that are not configured, use the **lrq reject-unknown-prefix** command in gatekeeper configuration mode. To reenable the gatekeeper to accept and process all incoming LRQ messages, use the **no** form of this command.

lrq reject-unknown-prefix
no lrq reject-unknown-prefix

Syntax Description

This command has no arguments or keywords.

Command Default

The gatekeeper accepts and processes all incoming LRQ messages.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the Cisco 2500 series and Cisco 3600 series.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

Use this command to configure the gatekeeper to reject any incoming LRQ messages for a destination E.164 address that does not match any of the configured zone prefixes.

Whether or not you use this command, the following is true when the E.164 address matches a zone prefix:

- If the matching zone prefix is local (that is, controlled by this gatekeeper), the LRQ message is serviced.
- If the matching zone prefix is remote (that is, controlled by some other gatekeeper), the LRQ message is rejected.

If you do not use this command and the target address does not match any known local or remote prefix, the default behavior is to attempt to service the call using one of the local zones. If this default behavior is not suitable for your site, use this command on your router to force the gatekeeper to reject such requests.

Examples

Consider the following gatekeeper configuration:

```
zone local gk408 cisco.com
zone local gk415 cisco.com
zone prefix gk408 1408.......
zone prefix gk415 1415.......
lrq reject-unknown-prefix
```

In this sample configuration, the gatekeeper is configured to manage two zones. One zone contains gateways with interfaces in the 408 area code, and the second zone contains gateways in the 415 area code. Then using the **zone prefix** command, the gatekeeper is configured with the appropriate prefixes so that calls to those area codes hop off in the optimal zone.

Now say some other zone has been erroneously configured to route calls to the 212 area code to this gatekeeper. When the LRQ message for a number in the 212 area code arrives at this gatekeeper, the gatekeeper fails to match the area code, and the message is rejected.

If this was your only site that had any gateways in it and you wanted your other sites to route all calls that require gateways to this gatekeeper, you can undo the **lrq reject-unknown-prefix command** by simply using the **no lrq reject-unknown-prefix command.**Now when the gatekeeper receives an LRQ message for the address 12125551234, it attempts to find an appropriate gateway in either one of the zones gk408 or gk415 to service the call.

Related Commands

Command	Description
lrq forward-queries	Enables a gatekeeper to forward LRQ messages that contain E.164 addresses that match zone prefixes controlled by remote gatekeepers.

lrq timeout blast window

To configure the timeout window for use when sending multiple location request (LRQ) messages (either sequentially or simultaneously), use the lrq timeout blast window command in gatekeeper configuration mode. To reset to the default, use the no form of this command.

lrq timeout blast window seconds
no lrq timeout blast window

Syntax Description

seconds	Duration of the window, in seconds. Range is from 1 to 10. Default is 6.

Command Default

6 seconds

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.

Examples

The following example sets the window to 3 seconds:

```
lrq timeout blast window 3
```

Related Commands

Command	Description
gatekeeper gw -type-prefix	Sets the gatekeepers responsible for each technology prefix.
zone prefix	Adds a prefix to a gatekeeper’s zone list.

lrq timeout seq delay

To configure the delay for use when sending location request (LRQ) messages sequentially, use the lrq timeout seq delay command in gatekeeper configuration mode. To reset to the default, use the no form of this command.

lrq timeout seq delay value
no lrq timeout seq delay

Syntax Description

value	Duration of the delay, in 100-millisecond units.Range is from 1 to 10. The default is 5 (500 ms or 0.5 seconds).

Command Default

Five 100-millisecond units (500 ms or 0.5 seconds)

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.

Examples

The following example sets the delay to 300 milliseconds:

```
lrq timeout seq delay 3
```

Related Commands

Command	Description
gatekeeper gw-type-prefix	Sets the gatekeepers responsible for each technology prefix.
zone prefix	Adds a prefix to a gatekeeper’s zone list.

map q850-cause through mgcp package-capability

map q850-cause

To play a customized tone to PSTN callers if a call disconnects with a specific Q.850 call-disconnect cause code and release source, use the **map q850-cause** command in voice-service configuration mode. To disable the code-to-tone mapping, use the **no** form of this command.

map q850-cause *code-id* **release-source** {**local** | **remote** | **all**} **tone** *tone-id*
no map q850-cause *code-id* **release-source** {**local** | **remote** | **all**} **tone** *tone-id*

Syntax Description

code-id	Q.850 call-disconnect cause code. Range: 1 to 15, 17 to 127 (16 is not allowed).
release-source	Source from which the cause code is generated. Choices are the following: • **local** --Originating gateway or gatekeeper • **remote** --Terminating gateway or gatekeeper • **all** --Any gateway or gatekeeper
tone *tone-id*	Tone to play for this cause code. Choices are the following: • **1** --Busy tone • **2** --Congestion tone • **3** --Special-information tone (a three-tone sequence at 950, 1400, and 1800 MHz) (not supported on IP phones)

Command Default

No mapping occurs.

Command Modes

Voice-service

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use this command to cause a particular tone to play when a call disconnects for a particular reason.

The tone plays to callers only if the call-disconnect and wait-to-release timers are set to values greater than 0 by entering the **timeouts call-disconnect** and **timeouts wait-release** commands.

Examples

The following example maps Q.850 call-disconnect cause code 21 to tone 3 on the local gateway and to tone 2 on the remote gateway:

```
Router(config)# voice service pots
Router(conf-voi-serv)# map q850-cause 21 release-source local tone 3
Router(conf-voi-serv)# map q850-cause 21 release-source remote tone 2
```

Related Commands

Command	Description
progress_ind	Sets a specific PI in call setup, progress, or connect messages from an H.323 VoIP gateway.
q850-cause	Maps a Q.850 call-disconnect cause code to a different Q.850 call-disconnect cause code.
scenario-cause	Configures new Q.850 call-disconnect cause codes for use if an H.323 call fails.
timeouts call-disconnect	Configures the delay timeout before an FXO voice port disconnects an incoming call after disconnect tones are detected.
timeouts wait-release	Configures the delay timeout before the system starts the process for releasing voice ports.

map resp-code

To globally configure a Cisco Unified Border Element (CUBE) to map specific received Session Initiation Protocol (SIP) provisional response messages to a different SIP provisional response message on the outgoing SIP dial peer, use the **map resp-code** command in voice service SIP configuration mode or voice class tenant configuration mode. To disable mapping of received SIP provisional response messages, use the **no** form of this command.

map resp-code 181 to 183
no map resp-code 181

Syntax Description

181	The code representing the specific incoming SIP provisional response messages to be mapped and replaced.
to	The designator for specifying that the specified incoming SIP provisional response message should be mapped to and replaced with a different SIP provisional response message on the outgoing SIP dial peer.
183	The code representing the specific SIP provisional response message on the outgoing dial peer to which incoming SIP message responses should be mapped.

Command Default

Incoming SIP provisional response messages are passed, as is to the outgoing SIP leg.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
15.0(1)XA	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 5.1(1)T.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.6(2)T and IOS XE Denali 16.3.1	This command is now available under voice class tenants.

Usage Guidelines

Use the **map resp-code** command in voice service SIP configuration mode to globally enable a Cisco UBE to map incoming SIP 181 provisional response messages to SIP 183 provisional response messages on the outgoing SIP dial peer.

Note If the **block** command is configured for incoming SIP 181 messages, either globally or at the dial-peer level, the messages may be dropped before they can be passed or mapped to a different message--even when the **map resp-code** command is enabled. To globally configure whether and when incoming SIP 181 messages are dropped, use the **block** command in voice service SIP configuration mode (or use the **voice-class sip block** command in dial peer voice configuration mode to configure drop settings on individual dial peers).

To configure mapping of SIP provisional response messages for an individual dial peer on a CUBE, use the **voice-class sip map resp-code** command in dial peer voice configuration mode. To disable mapping of SIP 181 message globally on a CUBE, use the **no map resp-code** command in voice service SIP configuration mode.

As an example, to enable interworking of SIP endpoints that do not support the handling of SIP 181 provisional response messages, you could use the **block** command to configure a CUBE to drop SIP 181 provisional response messages received on the SIP trunk or you can use the **map resp-code** command to configure the CUBE to map the incoming messages to and send out, instead, SIP 183 provisional response messages to the SIP line in Cisco Unified Communications Manager Express (Unified CME).

Note This command is supported only for SIP-to-SIP calls and will have no effect on H.323-to-SIP or time-division multiplexing (TDM)-to-SIP calls.

Examples

The following example shows how to configure mapping of incoming SIP 181 provisional response messages on the CUBE to SIP 183 provisional response messages on the outbound dial peer:

```
Router> enable
Router# configure
 terminal
Router(config)# voice
 service
 voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# map resp-code 181 to 183
```

Related Commands

Command	Description
block	Configures global settings for dropping specific SIP provisional response messages on a Cisco IOS voice gateway or CUBE.
voice-class sip block	Configures an individual dial peer on a Cisco IOS voice gateway or CUBE to drop specified SIP provisional response messages.
voice-class sip map resp-code	Configures a specific dial peer on a CUBE to map specific incoming SIP provisional response messages to a different SIP response message.

max1 lookup

To enable Domain Name System (DNS) lookup for a new call-agent address when the suspicion threshold value is reached, use the **max1 lookup**command inMGCP profile configuration mode. To disable lookup, use the **no** form of this command.

max1 lookup
no max1 lookup

Syntax Description

This command has no arguments or keywords.

Command Default

Lookup is enabled.

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

Call-agent redundancy can be provided when call agents are identified by DNS name rather than by IP address in the **call-agent** command, because each DNS name can have more than one IP address associated with it.

When the active call agent does not respond to a message from the media gateway, the gateway tests to determine whether the call agent is out of service. The gateway retransmits the message to the call agent for the number of times specified in the **max1 retries** command; this is known as the *suspicion threshold* . If there is no response and the **max1 lookup** command is enabled, the gateway examines the DNS lookup table to find the IP address of another call agent. If a second call agent is listed, the gateway retransmits the message to the second call agent until a response is received or the number of retries specified in the **max1 retries** command is reached.

This process is repeated for each IP address in the DNS table until the final address is reached. For the final address, the number of retries is specified by the **max2 retries**command;this number is known as the *disconnect threshold* . If the number of retries specified in the **max2 retries**command is reached and there is still no response and the **max2 lookup**command is enabled, the gateway performs one final DNS lookup. If any new IP addresses have been added, the gateway starts the retransmission process again. Otherwise, the gateway places the endpoint in a disconnected state.

Examples

The following example enables DNS lookup and sets the suspicion retransmission counter to 7:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# call-agent igloo.northpole.net
Router(config-mgcp-profile)# max1 lookup
Router(config-mgcp-profile)# max1 retries 7
```

Related Commands

Command	Description
call -agent	Specifies a call-agent address and protocol for an MGCP profile.
max1 retries	Sets the MGCP suspicion threshold value.
max2 lookup	Enables DNS lookup for an MGCP call agent when the disconnect threshold is reached.
max2 retries	Sets the MGCP disconnect threshold value.
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

max1 retries

To set the Media Gateway Control Protocol (MGCP) suspicion threshold value (the number of attempts to retransmit messages to a call agent address before performing a new lookup for retransmission), use the **max1 retries**command inMGCP profile configuration mode. To reset to the default, use the **no** form of this command.

max1 retries *number*
no max1 retries

Syntax Description

number	Number of times to attempt to resend messages. Range is from 3 to 30. The default is 5.

Command Default

5 attempts

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced and replaces the **mgcp request retries**command, which is no longer supported.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850 platforms. The maximum number of retries was increased to 30.

Usage Guidelines

This command is used when configuring values for an MGCP profile.

Call-agent redundancy can be provided when call agents are identified by Domain Name System (DNS) name rather than by IP address in the **call-agent** command, because each DNS name can have more than one IP address associated with it.

When the active call agent does not respond to a message from the media gateway, the gateway tests to determine whether the call agent is out of service. The gateway retransmits the message to the call agent for the number of times specified in the **max1 retries**command; this is known as the *suspicion threshold* . If there is no response and the **max1 lookup** command is enabled, the gateway examines the DNS lookup table to find the IP address of another call agent.

If a second call agent is listed, the gateway retransmits the message to the second call agent until a response is received or the number of retries specified in the **max1 retries** command is reached. This process is repeated for each IP address in the DNS table until the final address is reached. For the final address, the number of retries is specified by the **max2 retries**command;this is known as the *disconnect threshold* . If the number of retries specified in the **max2 retries** command is reached and there is still no response and the **max2 lookup** command is enabled, the gateway performs one final DNS lookup. If any new IP addresses have been added, the gateway starts the retransmission process again. Otherwise, the gateway places the endpoint in a disconnected state.

Examples

The following example enables DNS lookup and sets the suspicion retransmission counter to 7:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# call-agent igloo.northpole.net
Router(config-mgcp-profile)# max1 lookup
Router(config-mgcp-profile)# max1 retries 7
```

Related Commands

Command	Description
call -agent	Specifies a call-agent address and protocol for an MGCP profile.
max1 lookup	Enables DNS lookup for an MGCP call agent when the suspicion threshold is reached.
max2 lookup	Enables DNS lookup for an MGCP call agent when the disconnect threshold is reached.
max2 retries	Sets the MGCP disconnect threshold value.
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints, or to configure the default profile.

max2 lookup

To enable Domain Name System (DNS) lookup for a new call-agent address after the disconnect threshold timeout value is reached, use the **max2 lookup**command inMGCP profile configuration mode. To disable DNS lookup, use the **no** form of this command.

max2 lookup
no max2 lookup

Syntax Description

This command has no arguments or keywords.

Command Default

Lookup is enabled.

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

Call-agent redundancy can be provided when call agents are identified by DNS name rather than by IP address in the **call-agent** command, because each DNS name can have more than one IP address associated with it.

When the active call agent does not respond to a message from the media gateway, the gateway tests to determine whether the call agent is out of service. The gateway retransmits the message to the call agent for the number of times specified in the **max1 retries** command; this is known as the suspicion threshold. If there is no response and the **max1 lookup** command is enabled, the gateway examines the DNS lookup table to find the IP address of another call agent. If a second call agent is listed, the gateway retransmits the message to the second call agent until a response is received or the number of retries specified in the **max1 retries** command is reached.

This process is repeated for each IP address in the DNS table until the final address is reached. For the final address, the number of retries is specified by the **max2 retries** command; this is known as the disconnect threshold. If the number of retries specified in the **max2 retries** command is reached and there is still no response and the **max2 lookup** command is enabled, the gateway performs one final DNS lookup. If any new IP addresses have been added, the gateway starts the retransmission process again. Otherwise, the gateway places the endpoint in a disconnected state.

Examples

The following example enables DNS lookup and sets the disconnect retransmission counter to 9:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# call-agent ca1@exp.example.com
Router(config-mgcp-profile)# max2 lookup
Router(config-mgcp-profile)# max2 retries 9
```

Related Commands

Command	Description
call -agent	Specifies a call-agent address and protocol for an MGCP profile.
max1 lookup	Enables DNS lookup for an MGCP call agent when the suspicion threshold is reached.
max1 retries	Sets the MGCP suspicion threshold value.
max2 retries	Sets the MGCP disconnect threshold value.
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints, or to configure the default profile.

max2 retries

To set the Media Gateway Control Protocol (MGCP) disconnect threshold value (the number of attempts to retransmit messages to a call agent address before performing a new lookup for further retransmission), use the **max2 retries**command inMGCP profile configuration mode. To disable the disconnect threshold or to return the number of retries to the default, use the **no** form of this command.

max2 retries *number*
no max2 retries

Syntax Description

number	Number of times to attempt to resend messages. Range is from 3 to 30. The default is 7.

Command Default

7 attempts

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced and replaced the **mgcp request retries**command, which is no longer supported.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850. The maximum number of retries was increased to 30.

Usage Guidelines

This command is used when configuring values for an MGCP profile.

Call-agent redundancy can be provided when call agents are identified by Domain Name System (DNS) name rather than by IP address in the **call-agent**command, because each DNS name can have more than one IP address associated with it.

When the active call agent does not respond to a message from the media gateway, the gateway tests to determine whether the call agent is out of service. The gateway retransmits the message to the call agent for the number of times specified in the **max1 retries** command; this is known as the *suspicion threshold* . If there is no response and the **max1 lookup** command is enabled, the gateway examines the DNS lookup table to find the IP address of another call agent. If a second call agent is listed, the gateway retransmits the message to the second call agent until a response is received or the number of retries specified in the **max1 retries** command is reached.

This process is repeated for each IP address in the DNS table until the final address is reached. For the final address, the number of retries is specified by the **max2 retries**command;this is known as the *disconnect threshold* . If the number of retries specified in the **max2 retries** command is reached and there is still no response and the **max2 lookup** command is enabled, the gateway performs one final DNS lookup. If any new IP addresses have been added, the gateway starts the retransmission process again. Otherwise, the gateway places the endpoint in a disconnected state.

Examples

The following example sets the disconnect retransmission counter to 9:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# call-agent igloo.northpole.net
Router(config-mgcp-profile)# max2 retries 9
```

Related Commands

Command	Description
call -agent	Specifies a call-agent address and protocol for an MGCP profile.
max1 lookup	Enables DNS lookup for an MGCP call agent after the suspicion threshold value is reached.
max1 retries	Sets the MGCP suspicion threshold value.
max2 lookup	Enables DNS lookup for an MGCP call agent after the disconnect threshold value is reached.
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints, or to configure the default profile.

max-bandwidth

To configure the bandwidth threshold for VoIP media traffic, use the **max-bandwidth** command in dial peer configuration mode. To disable the configuration, use the **no** form of this command.

max-bandwidth *bandwidth-value* [{**midcall-exceed**}]
no max-bandwidth

Syntax Description

bandwidth-value	Aggregate bandwidth in kbps (Kilobits per second). The range is from 8 to 2000000.
midcall-exceed	(Optional) Allows exceeding the bandwidth threshold during a midcall media renegotiation.

Command Default

By default the bandwidth threshold is not configured for VoIP media traffic.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use the **max-bandwidth** command to configure the Bandwidth-Based Call Admission Control feature at the dial peer level and reject SIP calls when the aggregate bandwidth threshold is exceeded.

Examples

The following example shows how to configure a bandwidth threshold of 24 kbps for VoIP media traffic:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2000 voip
Router(config-dial-peer)# session protocol sipv2
Router(config-dial-peer)# max-bandwidth 24 midcall-exceed
```

Related Commands

Command	Description
session protocol sipv2	Specifies the SIP Version 2 protocol for calls between local and remote routers using the packet network.

max-calls

To set the maximum number of calls that a trunk group can handle, use the **max-calls** command in trunk group configuration mode. To reset to the default, use the **no** form of this command.

max-calls {**any** | **data** | **voice**} *number* [**direction** [{**in** | **out**}]]
no max-calls {**any** | **data** | **voice**} *number* [**direction** [{**in** | **out**}]]

Syntax Description

any	Assigns the maximum number of calls that the trunk group can handle, regardless of the type of call.
data	Assigns the maximum number of data calls to the trunk group.
voice	Assigns the maximum number of voice calls to the trunk group.
number	Range is from 0 to 1000.
direction	(Optional) Specifies direction of calls.
in	(Optional) Allows only incoming calls.
out	(Optional) Allows only outgoing calls.

Command Default

No limit when the command is not set.

Command Modes

Trunk group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use this command to set the maximum number of calls to be handled by the trunk group. If the command is not set the maximum is infinite.

If the maximum is reached, the trunk group becomes unavailable for more calls. When the number of calls falls below the maximum, the trunk group will accept more calls.

Examples

The following example assigns a maximum number of 500 calls of any type to trunk group gw15:

```
Router(config)# trunk group gw15
Router(config-trunk-group)# max-calls any 500
```

The following example assigns a maximum of 200 data calls and 750 voice calls to trunk group 32:

```
Router(config)# trunk group 32
Router(config-trunk-group)# max-calls data 200
Router(config-trunk-group)# max-calls voice 750
```

Related Commands

Command	Description
show trunk group	Displays the configuration of one or more trunk groups.
trunk group	Initiates a trunk group definition.

max-conn (dial peer)

To specify the maximum number of incoming or outgoing connections for a particular Multimedia Mail over IP (MMoIP), plain old telephone service (POTS), Voice over Frame Relay (VoFR), or Voice over IP (VoIP) dial peer, use the **max-conn** command in dial peer configuration mode. To set an unlimited number of connections for this dial peer, use the **no** form of this command.

max-conn *number*
no max-conn

Syntax Description

number	Maximum number of connections for this dial peer. Range is 1–2147483647. Default is an unlimited number of connections.

Command Default

The **no** form of this command is the default, meaning an unlimited number of connections

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to define the maximum number of connections used simultaneously to send or receive fax-mail. This command applies to off-ramp store-and-forward fax functions.

Examples

The following example configures a maximum of 5 connections for VoIP dial peer 10:

```
dial-peer voice 10 voip
 max-conn 5
```

Related Commands

Command	Description
mta receive maximum -recipients	Specifies the maximum number of recipients for all SMTP connections.

max-concurrent-sessions

To specify the maximum number of concurrent TFTP sessions for the specific phone proxy, use the **max-concurrent-sessions** command in phone proxy configuration mode. To remove the maximum number of concurrent TFTP sessions, use the **no** form of the command.

max-concurrent-sessions *number-of-sessions*
no max-concurrent-sessions

Syntax Description

number-of-sessions	Maximum number of concurrent TFTP sessions. The range is 0 to 500. The default is 200.

Command Default

200 concurrent TFTP sessions are configured.

Command Modes

Phone proxy configuration mode (config-phone-proxy)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Example

The following example shows how to specify a maximum of 400 concurrent TFTP sessions:

```
Device(config)# voice-phone-proxy first-pp
Device(config-phone-proxy)# max-concurrent-sessions 300
```

max-connection

To set the maximum number of simultaneous connections to be used for communication with a settlement provider, use the **max-connection** command in settlement configuration mode. To reset to the default, use the **no** form of this command.

max-connection *number*
no max-connection *number*

Syntax Description

number	Maximum number of HTTP connections to a settlement provider.

Command Default

10 connections

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples

The following command sets the maximum number of simultaneous connections to 10:

```
settlement 0
 max-connection 10
```

Related Commands

Command	Description
connection -timeout	Configures the time that a connection is maintained after completing a communication exchange.
customer -id	Sets the customer identification.
device -id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
response -timeout	Configures the maximum time to wait for a response from a server.
retry -delay	Sets the time between attempts to connect with the settlement provider.
retry -limit	Sets the maximum number of connection attempts to the provider.
session -timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.

Command	Description
shutdown	Brings up the settlement provider.
type	Configures an SAA-RTR operation type.
url	Configures the ISP address.

max-forwards

To globally set the maximum number of hops, that is, proxy or redirect servers that can forward the Session Initiation Protocol (SIP) request, use the **max-forwards** command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset the default number of hops, use the no form of this command.

max-forwards *number-of-hops* **[system]**
no max-forwards *number-of-hops* **[system]**

Syntax Description

number-of-hops	Number of hops. Range is from 1 to 70. Default is 70.
system	Specifies that the hops use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations

Command Default

70 hops

Command Modes

SIP user-agent configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.1(3)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on Cisco AS5350 and AS5400 platforms.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(8)T	This command was implemented on Cisco 7200 series routers. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.3(8)T	This command was enhanced with a greater configurable range and a higher default value (compliant with RFC 3261).
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

To reset this command to the default value, you can also use the default command.

Examples

The following example sets the number of forwarding requests to 65:

```
sip-ua
 max-forwards 65
```

The following example sets the number of forwarding requests in the voice class tenant configuration mode:

```
Router(config-class)# max-forwards system
```

Related Commands

Command	Description
max -redirects	Sets the maximum number of redirects that the user agent allows.

max-redirects

To set the maximum number of redirect servers that the user agent allows, use the **max-redirects** command in dial-peer configuration mode. To reset to the default, use the no form of this command.

max-redirects *number*
no max-redirects

Syntax Description

number	Maximum number of redirect servers that a call can traverse. Range is from 1 to 10. The default is 1.

Command Default

1 redirect

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5400 and Cisco AS5350 platforms.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco 7200 series. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following is an example of setting the maximum number of redirect servers that the user agent allows:

```
dial-peer voice 102 voip
 max-redirects 2
```

Related Commands

Command	Description
dial -peer voice	Enters dial-peer configuration mode and specifies the method of voice-related encapsulation.

max-subscription

To set the maximum number of concurrent watch sessions that are allowed, use the **max-subscription** command in presence configuration mode. To return to the default, use the **no** form of this command.

max-subscription *number*
no max-subscription

Syntax Description

number	Maximum watch sessions. Range: 100 to 500. Default: 100.

Command Default

Maximum subscriptions is 100.

Command Modes

Presence configuration (config-presence)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command sets the maximum number of concurrent presence subscriptions for both internal and external subscribe requests.

Examples

The following example shows the maximum subscriptions set to 150:

```
Router(config)# presence
Router(config-presence)# max-subscription 150
```

Related Commands

Command	Description
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
allow subscribe	Allows internal watchers to monitor external presence entities (directory numbers).
presence enable	Allows incoming presence requests from SIP trunks.
server	Specifies the IP address of a presence server for sending presence requests from internal watchers to external presence entities.
watcher all	Allows external watchers to monitor internal presence entities (directory numbers).

maximum buffer-size

To set the maximum size of the file accounting buffer, use the **maximum buffer-size**command in gateway accounting file configuration mode. To reset to the default, use the **no** form of this command.

maximum buffer-size *kbytes*
no maximum buffer-size

Syntax Description

kbytes	Maximum buffer size, in kilobytes. Range: 6 to 40. Default: 20.

Command Default

Maximum buffer size is 20 kilobytes.

Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The file accounting process writes call detail records (CDRs) to a memory buffer instead of writing each record independently to the accounting file. Two buffers are allocated for file accounting and their size is set by this command. After the accounting records in the buffer reach the size limit set by this command, the system flushes the first buffer and writes the records to the accounting file. While the first buffer is busy being flushed, the system uses the second buffer to hold new data. After the flush process, the buffer is available again.

The buffer size must be large enough to accommodate incoming CDRs without the system filling up both buffers completely.

Examples

The following example sets the maximum buffer size to 25 kilobytes:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary ifs flash:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 maximum fileclose-timer 720
 cdr-format compact
```

Related Commands

Command	Description
cdr-format	Selects the format of the CDRs generated for file accounting.
file-acct flush	Manually flushes the CDRs from the buffer to the accounting file.
maximum fileclose-timer	Sets the maximum time for saving records to an accounting file before closing the file and creating a new one.

Command	Description
primary	Sets the primary location for storing the CDRs generated for file accounting.
secondary	Sets the backup location for storing CDRs if the primary location becomes unavailable.

maximum cdrflush-timer

To set the maximum time to hold call records in the buffer before appending the records to the accounting file, use the **maximum cdrflush-timer** command in gateway accounting configuration mode. To reset to the default, use the **no** form of this command.

maximum cdrflush-timer *minutes*
no maximum cdrflush-timer

Syntax Description

minutes	Maximum time, in minutes, to hold call records in the accounting buffer. Range: 1 to 1,435. Default: 60 (1 hour).

Command Default

Records are held in the buffer for 60 minutes (1 hour).

Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

After the time period set with this command expires, the router flushes the buffer and writes the call detail records (CDRs) to the accounting file.

The file accounting process sends CDRs to a memory buffer instead of writing each record independently to the accounting file. The system flushes the buffer automatically either after this timer expires or when the records in the buffer reach the size set by the **maximum buffer-size** command.

Set this flush timer to at least five minutes less than the file close timer set with the **maximum fileclose-timer** command.

To manually flush the CDRs from the buffer to the accounting file, use the **file-acct flush** command.

Examples

The following example shows that call records are held in the accounting file for three hours, after which the records are appended to the accounting file:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary ifs flash:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 maximum fileclose-timer 720
 cdr-format compact
```

Related Commands

Command	Description
file-acct flush	Manually flushes the CDRs from the buffer to the accounting file.

Command	Description
maximum buffer-size	Sets the maximum size of the file accounting buffer.
maximum fileclose-timer	Sets the maximum time for saving records to an accounting file before closing the file and creating a new one.
primary	Sets the primary location for storing the CDRs generated for file accounting.
secondary	Sets the backup location for storing CDRs if the primary location becomes unavailable.

maximum conference-participants

To configure the maximum number of conference participants allowed in each meet-me conference, use the **maximum conference-participants** command in DSP farm profile configuration mode. To reset the maximum to the default number, use the **no** form of this command.

maximum conference-participants *max-participants* [**video-cap-class** *number*]
no maximum conference-participants *max-participants* [**video-cap-class** *number*]

Syntax Description

max-participants	Maximum number of participants allowed in each meet-me conference session. One DSP can support the following maximums: • G.711--32 participants • G.729--16 participants • Video (H.263 or H.264)--4, 8, or 16 participants
video-cap-class *number*	(Optional) Reserves the DSP resources needed to support a video participant requiring video format conversion. The range for video port number is from 2 to 4. The default is 2.

Command Default

The default maximum number of participants for a video conference is 4. The default maximum number of participants for an audio conference is 8.

Command Modes

DSP farm profile configuration (config-dspfarm-profile)

Command History

Release	Modification
12.4(11)XJ2	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
15.1(4)M	This command was modified. The **video-cap-class** keyword was added.

Usage Guidelines

The maximum number of participants allowed for hardware conferencing is dependent on the codec used in the DSP farm profile. Use the **codec** command in DSP farm profile configuration mode to specify the codecs supported by the DSP farm profile. Use the **show dspfarm profile**command to display the DSP farm profile.

Examples

The following example configures a DSP farm profile that has a maximum of 16 participants for hardware conferences using the G.711 codec:

```
Router(config)# dspfarm profile conference 1
Router(config-dspfarm-profile)# maximum conference-participants 16
Router(config-dspfarm-profile)# codec g711alaw
```

Related Commands

Command	Description
codec (DSP Farm profile)	Specifies the codecs supported by a DSP farm profile.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
maximum sessions	Specifies the maximum number of sessions that are supported by the profile.
show dspfarm profile	Displays configured DSP farm profile information.

maximum fileclose-timer

To set the maximum time for writing call detail records (CDRs) to an accounting file before closing the file and creating a new one, use the **maximum fileclose-timer**command in gateway accounting configuration mode. To reset to the default, use the **no** form of this command.

maximum fileclose-timer *minutes*
no maximum fileclose-timer

Syntax Description

minutes	Maximum time, in minutes, to write records to an accounting file. Range: 60 (1 hour) to 1,440 (24 hours). Default: 1,440.

Command Default

Records are saved to an accounting file for 1,440 minutes (24 hours).

Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

After the timer set with this command expires, the current accounting file is closed and a new file with a new time stamp is opened to write CDRs. The name and location of the accounting file is set by the **primary** command, or the **secondary** command if in failover mode.

Set this file close timer to at least five minutes longer than the flush timer set with the **maximum cdrflush-timer** command.

To manually flush the CDRs from the buffer to the accounting file, use the **file-acct flush** command.

Examples

The following example shows that call records are saved to the currently open accounting file for 12 hours, after which a new accounting file is created:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary ifs flash:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 maximum fileclose-timer 720
 cdr-format compact
```

Related Commands

Command	Description
file-acct flush	Manually flushes the CDRs from the buffer to the accounting file.
maximum buffer-size	Sets the maximum size of the file accounting buffer.

Command	Description
maximum cdrflush-timer	Sets the maximum time to hold call records in the buffer before appending the records to the accounting file.
primary	Sets the primary location for storing the CDRs generated for file accounting.
secondary	Sets the backup location for storing CDRs if the primary location becomes unavailable.

maximum retry-count

To set the maximum number of times the router attempts to connect to the primary file device before switching to the secondary device, use the **maximum retry-count**command in gateway accounting file configuration mode. To reset to the default value, use the **no** form of this command.

maximum retry-count *number*
no maximum retry-count

Syntax Description

number	Number of connection attempts. Range: 1 to 5. Default: 2.

Command Default

Maximum connection attempts is 2.

Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command specifies the number of times that the router attempts to connect to the primary file device defined in the **primary** command before it attempts to connect to the backup file device specified with the **secondary** command.

Examples

The following example shows the maximum retries set to 3:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary ifs flash:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 cdr-format compact
```

Related Commands

Command	Description
file-acct reset	Manually switches back to the primary device for file-based accounting.
primary	Sets the primary location for storing the call detail records generated for file accounting.
secondary	Sets the backup location for storing CDRs if the primary location becomes unavailable.

maximum sessions (DSP farm profile)

To specify the maximum number of sessions that are supported by the profile, use the **maximum sessions** command in DSP farm profile configuration mode. To reset to the default, use the **no** form of this command.

Command Syntax When Conferencing or Transcoding Is Configured
maximum sessions *number*
no maximum sessions

Command Syntax When MTP Is Configured
maximum sessions {**hardware** | **software**} *number*
no maximum sessions

Syntax Description

number	Number of session supported by the profile. Range is 0 to *x* . Default is 0. The *x* value is determined at run time depending on the number of resources available with the resource provider.
hardware	Number of sessions that media termination points (MTP) hardware resources will support.
software	Number of sessions that MTP software resources will support.

Command Default

The maximum number of supported sessions is 0.

Command Modes

DSP farm profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

When using the MTP service type, you must specify the number of sessions separately for software MTP and hardware MTP. The hardware MTP needs digital signal processor (DSP) resources. Use hardware MTP when the codecs are the same and the packetization period is different.

Active profiles must be shut down before any parameters can be changed.

Note The syntax of the command will vary based on the type of profile that you are configuring. The keywords work only when MTP is configured.

Examples

The following example shows that four sessions are supported by the DSP farm profile:

```
Router(config-dspfarm-profile)#
maximum sessions
```

Related Commands

Command	Description
associate application	Associates the SCCP protocol to the DSP farm profile.
codec (dspfarm-profile)	Specifies the codecs supported by a DSP farm profile.
description (dspfarm-profile)	Includes a specific description about the DSP farm profile.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
shutdown (dspfarm-profile)	Allocates DSP farm resources and associates with the application.
voice-card	Enters voice-card configuration mode.

mdn

To request that a message disposition notification (MDN) be generated when a message is processed (opened), use the **mdn** command in dial-peer configuration mode. To disable generation of an MDN, use the **no** form of this command.

mdn
no mdn

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750 access router.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Message disposition notification is an e-mail message that is generated and sent to the sender when the message is opened by the receiver. Use this command to request that an e-mail response message be sent to the sender when the e-mail that contains the fax TIFF image has been opened.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example requests that a message disposition notification be generated by the recipient:

```
dial-peer voice 10 mmoip
 mdn
```

Related Commands

Command	Description
mta receive generate -mdn	Specifies that the off-ramp gateway process a response MDN from an SMTP server.
mta send return -receipt-to	Specifies the address to which MDNs are sent.

media

To enable media packets to pass directly between the endpoints, without the intervention of the Cisco Unified Border Element (Cisco UBE) and to enable signaling services, enter the **media** command in dial peer voice, voice class, or voice service configuration mode. To return to the default behavior, use the **no** form of this command.

media [{**bulk-stats** | **flow-around** | **flow-through** | **forking** | **monitoring [video]** [*max-calls*] | **statistics** | **transcoder high-density** | **anti-trombone** | **sync-streams**}]
no media [{**bulk-stats** | **flow-around** | **flow-through** | **forking** | **monitoring [video]** [*max-calls*] | **statistics** | **transcoder high-density** | **anti-trombone** | **sync-streams**}]

Syntax Description

bulk-stats	(Optional) Enables a periodic process to retrieve bulk call statistics.
flow-around	(Optional) Enables media packets to pass directly between the endpoints, without the intervention of the Cisco UBE. The media packet is to flow around the gateway.
flow-through	(Optional) Enables media packets to pass through the endpoints, without the intervention of the Cisco UBE.
forking	(Optional) Enables the media forking feature for all calls.
monitoring	(Optional) Monitors the media voice stream quality for all calls or a maximum number of calls.
video	(Optional) Specifies video quality monitoring.
max-calls	(Optional) Maximum number of calls that are monitored.
statistics	(Optional) Enables media monitoring.
transcoder high-density	(Optional) Converts media codecs from one voice standard to another to facilitate the interoperability of devices using different media standards.
anti-trombone	(Optional) Enables media anti-trombone for all calls. Media trombones are media loops in SIP entity due to call transfer or call forward.
sync-streams	(Optional) Specifies that both audio and video streams go through the DSP farms on Cisco UBE and Cisco Unified CME.

Command Default

The default behavior of the Cisco UBE is to receive media packets from the inbound call leg, terminate them, and then reoriginate the media stream on an outbound call leg.

Command Modes

Dial peer voice configuration (config-dial-peer)
Voice class configuration (config-class)
Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(1)T	This command was introduced.
12.4(11)XJ2	This command was modified. The **statistics** keyword was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.4(20)T	This command was modified. The **transcoder**and **high-density** keywords were introduced.
15.0(1)M	This command was modified. The **forking**and **monitoring** keywords and the *max-calls* argument were introduced.
15.1(3)T	This command was modified. The **anti-trombone** keyword was introduced.
15.1(4)M	This command was modified. The **sync-stream** keyword was added.
15.2(1)T	This command was modified. The **video** keyword was added.
Cisco IOS XE Release 15.0(1)S	The **bulk-stats** keyword was added.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Note **media bulk-stats** and **media statistics** are only supported.

With the default configuration, the Cisco UBE receives media packets from the inbound call leg, terminates them, and then reoriginates the media stream on an outbound call leg. Media flow-around enables media packets to be passed directly between the endpoints, without the intervention of the Cisco UBE. The Cisco UBE continues to handle routing and billing functions. Media flow-around for SIP-to-SIP calls is not supported.

Note The Cisco UBE must be running Cisco IOS Release 12.3(1) or a later release to support media flow-around.

You can specify media flow-around for a voice class, all VoIP calls, or individual dial peers.

The **transcoder high-density** keyword can be enabled in any of the configuration modes with the same command format. If you are configuring the **transcoder high-density** keyword for dial peers, make sure that the **media transcoder high-density** command is configured on both the in and out-legs.

The software does not support configuring the **transcoder high-density** keyword on any dial peer that is to handle video calls. The following scenarios are not supported:

- Dial peers used for video at any time. Configuring the **media transcoder high-density**command directly under the dial-peer or a voice-class media configuration mode is not supported.
- Dial peers configured on a Cisco UBE used for video calls at any time. The global configuration of the **media transcoder high-density** command under voice service configuration mode is not supported.

> **Note** The**media bulk-stats** command may impact performance when there are a large number of active calls. For networks where performance is crucial in customer's applications, it is recommended that the **media bulk-stats** command not be configured.

To enable the **media** command on a Cisco 2900 or Cisco 3900 series Unified Border Element voice gateway, you must first enter the **mode border-element** command. This enables the **media forking** and **media monitoring** commands. Do not configure the **mode border-element** command on the Cisco 2800 or Cisco 3800 series platform.

You can specify media anti-trombone for a voice class, all VoIP calls, or individual dial peers.

The **anti-trombone** keyword can be enabled only when no media interworking is required in both the out-legs. The anti-trombone will not work if call leg is flow-through and another call leg is flow-around.

Examples

Media Bulk-Stats Examples

The following example shows media bulk-stats being configured for all VoIP calls:

```
Device(config)# voice service voip
Device(config-voi-serv)# allow-connections sip to sip
Device(config-voi-serv)# media statistics
```

Media Flow-around Examples

The following example shows media flow-around configured on a dial peer:

```
Device(config)# dial-peer voice 2 voip
Device(config-dial-peer)# media flow-around
```

The following example shows media flow-around configured for all VoIP calls:

```
Device(config)# voice service voip
Device(config-voi-serv)# media flow-around
```

The following example shows media flow-around configured for voice class calls:

```
Device(config)# voice class media 1
Device(config-class)# media flow-around
```

Media Flow-through Examples

The following example shows media flow-through configured on a dial peer:

```
Device(config)# dial-peer voice 2 voip
Device(config-dial-peer)# media flow-through
```

The following example shows media flow-through configured for all VoIP calls:

```
Device(config)# voice service voip
Device(config-voi-serv)# media flow-through
```

The following example shows media flow-through configured for voice class calls:

```
Device(config)# voice class media 2
Device(config-class)# media flow-through
```

Media Statistics Examples

The following example shows media monitoring configured for all VoIP calls:

```
Device(config)# voice service voip

Device(config-voi-serv)# media statistics
```

The following example shows media monitoring configured for voice class calls:

```
Device(config)# voice class media 1
Device(config-class)# media
 statistics
```

Media Transcoder High-density Examples

The following example shows the **media transcoder** command configured for all VoIP calls:

```
Device(config)# voice service voip

Device(conf-voi-serv)# media transcoder high-density
```

The following example shows the **media transcoder**command configured for voice class calls:

```
Device(config)# voice class media 1
Device(config-voice-class)# media transcoder high-density
```

The following example shows the **media transcoder**command configured on a dial peer:

```
Device(config)# dial-peer voice 36 voip
Device(config-dial-peer)# media transcoder high-density
```

Media Monitoring on a Cisco UBE Platform

The following example shows how to configure audio call scoring for a maximum of 100 calls:

```
mode border-element
media monitoring 100
```

Media Antitrombone Examples

The following example shows the **media anti-trombone**command configured for all VoIP calls:

```
Device(config)# voice service voip
Device(conf-voi-serv)# media anti-trombone
```

The following example shows the **media anti-trombone**command configured for voice class calls:

```
Device(config)# voice class media 1
Device(config-voice-class)# media anti-trombone
```

The following example shows the **media anti-trombone**command configured on a dial peer:

```
Device(config)# dial-peer voice 36 voip
Device(config-dial-peer)# media anti-trombone
```

Media Transcoder Examples

The following example specifies that both audio and video RTP streams go through the DSP farms when either audio or video transcoding is needed:

```
Device(config)# voice service voip
Device(config-voi-serv)# media transcoder sync-streams
```

The following example specifies that both audio and video RTP streams go through the DSP farms when either audio or video transcoding is needed and the RTP streams flow around Cisco Unified Border Element.

```
Device(config)# voice service voip
Device(config-voi-serv)# media transcoder high-density sync-streams
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer voice configuration mode.
mode border-element	Enables the media monitoring capability of the **media** command.
voice class	Enters voice class configuration mode.
voice service	Enters voice service configuration mode.

media-address voice-vrf

To associate RTP port-range with VRF, use the **media-adderss voice-vrf** command in voice-service-voip configuration mode. To disable use **no** form of this command.

media-adderss voice-vrf *vrf name* **port-range**{*min max*}

no media-adderss voice-vrf *vrf name* **port-range**{*min max*}

Syntax Description

vrf name	Specifies the VRF name.
port-range	Specifies RTP port-range.
min-max	Specifies the minimum and maximum RTP port range.

Command Default

No media-address range is associated with VRF.

Command Modes

voice-serv-voip

Command History

Release	Modification
Cisco IOS 15.6(2)T	This command was introduced.
Cisco IOS XE Denali 16.3.1	This command was integrated with Cisco IOS XE Denali 16.3.1
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to associate RTP port-range with VRF.

Examples

Port-range configured on the same line as the media address:

```
Device(conf-voi-serv)# media-address voice-vrf VRF1 6000 7000
```

Multiple port-range lines are configured under the media address:

```
Device(conf-voi-serv)# media-address voice-vrf VRF1
Device(cfg-media-addr-vrf)# port-range 6000 7000
Device(cfg-media-addr-vrf)# port-range 8000 10000
Device(cfg-media-addr-vrf)# port-range 11000 20000
```

mediacard

To enter mediacard configuration mode and configure a Communications Media Module (CMM) media card, use the **mediacard** command in global configuration mode.

mediacard *slot*

Syntax Description

slot	Specifies the slot number for the media card to be configured. Valid values are from 1 to 4.

Command Default

No default behavior or values

Command Modes

Global configuration mode

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.4(3)	This command was integrated into Cisco IOS Release 12.4(3).

Usage Guidelines

Mediacard configuration mode is used to configure parameters related to the selected media card, such as digital signal processor (DSP) resource pools.

Examples

The following example shows how you configure DSP resources on the media card in slot 1:

```
mediacard 1
```

Related Commands

Command	Description
debug mediacard	Displays debugging information for Digital Signal Processor Resource Manager (DSPRM).
show mediacard	Displays information about the selected media card.

media class

To configure a media class and to enter media class configuration mode, use the **media class** command in global configuration mode. To disable the configuration, use the **no** form of this command.

media class *tag*
no media class *tag*

Syntax Description

tag	Media class tag. The range is 1–10000.

Command Default

No media class is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Bengaluru 17.6.1a	This command was modified to add **stream-service** as a sub-command.

Usage Guidelines

Use the **media class** command to combine different profiles, such as media forking, and apply the profile to a dial peer if required.

Examples

The following example shows how to configure a media class for tag 100:

```
Router(config)# media class 100
```

Related Commands

Command	Description
recorder profile	Configures the media profile recorder.

media-inactivity-criteria

To specify the mechanism for detecting media inactivity (silence) on a voice call, use the **media-inactivity-criteria** command in a gateway configuration mode. To disable detection, use the **no** form of this command.

media-inactivity-criteria {**rtp** | [**receive**] | **rtcp** | **all** | [**receive**] | **rtplib**}
no media-inactivity-criteria

Syntax Description

rtp	Real-Time Transport Protocol (RTP) (default)
rtcp	RTP Control Protocol (RTCP)
all	Both RTP and RTCP
receive	(Optional) Changes the media inactivity criteria to check for received packets only.
rtplib	RTP (comfort noise is considered as an activity)

Command Default

Media-inactivity detection is performed by RTP.

Command Modes

Global configuration mode.

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.4(03)M	This command was modified. The **receive** keyword was added.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to specify the mechanism for detecting silence on a voice call. After doing so, you can configure silent calls to disconnect by entering the related commands listed below.

Use this command, with the **application**, **package callfeature**, **param**, and **paramspace** commands, to configure callfeature parameters at the package level and to override them as needed for specific applications or dial peers.

The mechanism that you explicitly specify with this command takes precedence over any mechanism that you might implicitly have specified with the **ip rtcp report interval** command with the **timer media-inactive** or **timer receive-rtcp** command.

For SIP-to-SIP IPv4 calls, if the CLI command **media-inactivity-criteria rtp** is configured under a gateway configuration mode, then call is cleared due to media inactivity although two way RTP and RTCP are present. As a workaround, it is mandatory that you configure **media-inactivity-criteria** as **rtplib** or **rtcp**or **all**. For a sample configuration, see example.

Examples

The following example shows a **media-inactivity-criteria** configuration to ensure that call is not cleared due to media inactivity although RTP and RTCP are present.

```
Router(config)#gateway
Router(config-gateway)#media-inactivity-criteria rtcp|rtplib|all
```

The following example specifies the use of RTCP for silence detection:

```
Router(config)# gateway
Router(config-gateway)# media-inactivity-criteria rtcp
```

The following example shows a configuration that might result from the use of this and related commands:

```
voice service pots
map q850-cause 44 release-source local tone 3
application
 package callfeature
  param med-inact-disc-cause 44
  param med-inact-det enable
  param med-inact-action disconnect
ip rtcp report interval 9000
dial-peer voice 5 voip
destination-pattern .T
 progress_ind disconnect enable 8
 session target ras
 codec g711ulaw
gateway
 media-inactivity-criteria rtcp
 timer media-inactive 5
```

Related Commands

Command	Description
application	Enables a specific application on a dial peer.
ip rtcp report interval	Configures the average reporting interval between subsequent RTCP report transmissions.
package callfeature	Enters application-parameter configuration mode.
param	Loads and configures parameters in a package or a service (application) on the gateway.
paramspace	Enables an application to use parameters from the local parameter space of another application.
timer media-inactive	Sets the media-inactivity disconnect timer.
timer receive-rtcp	Sets the RTCP timer and configures a multiplication factor for the RTCP timer interval for SIP or H.323 calls.

media disable-detailed-stats

To disable detailed statistics collection about the calls present.

media disable-detailed-stats
no media disable-detailed-stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration mode

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

media profile asp

To create a media profile to configure acoustic shock protection parameters, use the **media profile asp** command in global configuration mode. To disable the configuration, use the **no** form of this command.

media profile asp *tag*
no media profile asp *tag*

Syntax Description

tag	Media profile tag. The range is from 1 to 10000.

Command Default

Media profile for acoustic shock protection is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.2(3)T	This command was modified. Support for the Cisco Unified Border Element (Cisco UBE) was added.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the **media profile asp** command to configure media profile for acoustic shock protection parameters. You can configure acoustic shock protection parameters after creating a media profile.

Examples

The following example shows how to create a media profile to configure acoustic shock protection parameters:

```
Device> enable
Device# configure terminal
Device(config)# media profile asp 200
Device(config)# end
```

Related Commands

Command	Description
media profile nr	Creates a media profile to configure noise reduction parameters.

media profile nr

To create a media profile to configure noise reduction parameters, use the **media profile nr** command in global configuration mode. To disable the configuration, use the **no** form of this command.

media profile nr *tag*
no media profile nr *tag*

Syntax Description

tag	Media profile tag. The range is from 1 to 10000.

Command Default

Media profile for noise reduction is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.2(3)T	This command was modified. Support for the Cisco Unified Border Element (Cisco UBE) was added.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the **media profile nr** command to configure media profile for noise reduction parameters. You can configure noise reduction parameters after creating a media profile.

Examples

The following example shows how to create a media profile to configure noise reduction parameters:

```
Device> enable
Device# configure terminal
Device(config)# media profile nr 200
Device(config)# end
```

Related Commands

Command	Description
media profile asp	Creates a media profile to configure acoustic shock protection parameters.

media profile video

To create a media profile video, use the **media profile video** command in dial-peer voice configuration mode.

media profile video *tag*
no media profile video *tag*

Syntax Description

tag	Media profile video tag. The range is from 1 to 10000.

Command Modes

Dial-peer configuration (config).

Release	Modification
15.2(2)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Related Commands

Command	Description
media profile nr	Creates a media profile to configure noise reduction parameters.
media profile asp	Creates a media profile to configure acoustic shock protection parameters.

media profile police

To configure the media policing profile, use the **media profile police** command in global configuration mode. To disable the configuration, use the **no** form of this command.

media profile police *tag*
no media profile police *tag*

Syntax Description

tag	Media profile tag. The range is from 1 to 10000.

Command Default

Media policing profiles are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use the **media profile police** command to configure a media policing profile. You must apply the profile to a dial peer or globally after configuring the media policing profile.

Examples

The following example shows how to configure the media policing profile:

```
Router> enable
Router# configure terminal
Router(config)# media profile police 1
```

Related Commands

Command	Description
media police-profile	Applies the media policing profile at the global level.
media-class	Applies the media policing profile at the dial peer level.
police profile	Applies the media bandwidth policing profile to a media class.

media profile recorder

To configure the media recorder profile, use the **media profile recorder** command in global configuration mode. To disable the configuration, use the **no** form of this command.

media profile recorder *profile-tag*
no media profile recorder *profile-tag*

Syntax Description

profile-tag	Media profile tag. The range is from 1 to 10000.

Command Default

Media profile recorder is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

You can use the **media profile recorder** command to configure the recorder profile. Here, you will be saving the dial peer tag that points to the recording server on the Cisco Unified Border Element (Cisco UBE).

Configuring the **media profile recorder** command is a method to define media recording globally. This configuration provides a profile for the recorder to define media recording.

Examples

The following example shows how to configure the media profile recorder:

```
Router# configure terminal
Router(config)# media profile recorder 100
```

Related Commands

Command	Description
media-recording	Sets voice class recording parameters.
show voip recmsp session	Displays active recording MSP session information.

media profile stream-service

To enable stream-service on CUBE, use the **media profile stream-service** *tag* command in global configuration mode. To disable stream-service, use the **no** form of this command.

media profile stream-service *tag*
no media profile stream-service *tag*

Syntax Description

tag	The media profile stream-service tag. Range is 1–10000.

Command Default

Stream service isn't enabled by default.

Command Modes

Global configuration mode (config)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was introduced on Cisco Unified Border Element.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

When you configure **media profile stream-service** *tag* , the media profile configuration mode is enabled.

```
router(config)#media profile stream-service <tag>
router(cfg-mediaprofile)#?
MEDIAPROFILE configuration commands:
connection stream service connection
description Mediaprofile specific description
exit Exit from media profile configuration mode
help Description of the interactive help system
no Negate a command or set its defaults
proxy Websocket Proxy Server
source-ip local source-ip for the websocket connection
```

Configure the required stream-service profile within the corresponding **media-class** to enable stream-service functionality using the **media profile stream-service** *tag* command on CUBE. Further, you must associate the **media-class** with the dial-peer pointing towards CVP. If **media-class** isn't associated with the dial-peer pointing towards CVP, CUBE rejects the forking request and sends an INFO message to CVP to inform that it's an unsupported flow.

CUBE uses the local IP address configured under source-interface for establishing WebSocket connection. When proxy is configured with host name instead of IP address, CUBE performs DNS resolution for proxy before sending the WebSocket request. However, when proxy is configured and json from CVP contains host name for speech server, DNS resolution isn't performed.

Examples

The following is a sample configuration for enabling stream-service functionality in CUBE:

```
media profile stream-service 99
connection idle-timeout 1(This can be 1-60 mins)

media class 9
stream-service profile 99

dial-peer voice 42 voip
```

```
destination-pattern 5678
session protocol sipv2
session target ipv4:8.41.17.71:8001
session transport udp
voice-class codec 40
voice-class sip bind control source-interface GigabitEthernet1
voice-class sip bind media source-interface GigabitEthernet1
media-class 9
```

Related Commands

Command	Description
connection (media-profile)	Configures idle timeout and call threshold for a media profile.
proxy (media-profile)	Configures IP address or hostname of proxy in media profile.
source-ip (media-profile)	Configures local source IP address of a WebSocket connection.
media class	Applies the media class at the dial peer level.
stream-service profile	Associates a stream service profile with media class.

media-recording

To configure voice class recording parameters, use the **media-recording** command in media profile or media class recorder parameter configuration mode. To disable the configuration, use the **no** form of this command.

media-recording *dial-peer-tag* [*dial-peer-tag2* ... *dial-peer-tag5*]
no media-recording *dial-peer-tag* [*dial-peer-tag2* ... *dial-peer-tag5*]

Syntax Description

dial-peer-tag	Dial peer tag to be matched on the forked leg. The range is from 1 to 1073741823. • You can specify a maximum of five dial peers.

Command Default

No voice class recording parameter is configured.

Command Modes

Media profile configuration (cfg-mediaprofile)
Media class recorder parameter configuration (cfg-mediaclass-recorder)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Use the **media-recording** command to define a dial peer tag for recording. This command configures the dial peer that points to the recording server.

Examples

The following example shows how to configure voice class recording parameters:

```
Router# configure terminal
Router(config)# media profile recorder 100
Router(cfg-mediaprofile)# media-recording 1000 1001 1002 1003 1004
```

Related Commands

Command	Description
media profile recorder	Configures the media recorder profile.
show voip recmsp session	Displays active recording MSP session information.

media recording proxy

Configures the dial-peers for forking.

Note You can specify maximum of five dial peer tags.

media-recording proxy [*dial-peer-tag1 dial-peer-tag2 dial-peer-tag3 dial-peer-tag4 dial-peer-tag5*]

media-recording proxy secure [*dial-peer-tag1 dial-peer-tag2 dial-peer-tag3 dial-peer-tag4 dial-peer-tag5*]

Syntax Description

media-recording proxy [*dial-peer-tag1 dial-peer-tag2 dial-peer-tag3 dial-peer-tag4 dial-peer-tag5*]	The proxy configures the first dial-peer of the sequence for establishing a back-to-back (B2B) call, and the remaining dial-peers for media forking.
media-recording proxy secure [*dial-peer-tag1 dial-peer-tag2 dial-peer-tag3 dial-peer-tag4 dial-peer-tag5*]	You can configure dial-peers for either secure or nonsecure forking. You may configure up to five secure or nonsecure dial-peers. The first available secure target is used for establishing a back-to-back call. Earlier behaviour remains unchanged if there are no secure dial peers configured. Configure all secure dial peers with the same voice class srtp-crypto profile.

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1a	This command was introduced.
Cisco IOS XE Bengaluru 17.5.1a	Introduced support for secure forking.

Examples

```
Device(cfg-mediaprofile)# media-recording proxy 8000 8001 8002
```

```
Device(cfg-mediaprofile)# media-recording proxy secure 8003 8004
```

media service

To apply a media class for noise reduction (NR) or acoustic shock protection (ASP) at a global level, use the **media service** command in global configuration mode. To disable the configuration, use the **no** form of this command.

media service
no media service

Syntax Description

This command has no arguments or keywords.

Command Default

Media service is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.2(3)T	This command was modified. Support for the Cisco Unified Border Element (Cisco UBE) was added.

Usage Guidelines

Use the **media service** command to apply a media class for NR or ASP at a global level. You can configure a media service after creating a media profile and applying the profile to a media class.

Examples

The following example shows how to apply a media class for NR or ASP at a global level:

```
Device> enable
Device# configure terminal
Device(config)# media service
Device(config)# end
```

Related Commands

Command	Description
media class	Creates a media class to configure noise reduction parameters.

meetme-conference

To define a feature code for a Feature Access Code (FAC) to initiate an SCCP Meet-Me Conference, use the **meetme-conference**command in STC application feature access-code configuration mode. To return the feature code to its default, use the **no** form of this command.

meetme-conference *keypad-character*
no meetme-conference

Syntax Description

keypad-character	Character string that can be dialed on a telephone keypad (0-9, *, #). Default: 5. The string can be any of the following: • A single character (0-9, *, #) • Two digits (00-99) • Two to four characters (0-9, *, #) and the leading or ending character must be an asterisk (*) or number sign (#)

Command Default

The default value of the feature code is 5.

Command Modes

STC application feature access-code configuration (config-stcapp-fac)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command changes the value of the feature code for SCCP Meet-Me Conference from the default (5) to the specified value.

If the length of the *keypad-character* argument is at least two characters and the leading or ending character of the string is an asterisk (*) or a number sign (#), phone users are not required to dial a prefix to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 55#, the phone user dials only 55#, without the FAC prefix, to access the corresponding feature.

If you attempt to configure this command with a value that is already configured for another FAC, speed-dial code, or the Redial FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

If you attempt to configure this command with a value that precludes or is precluded by another FAC, speed-dial code, or the Redial FSD, you receive a message. If you configure a feature code to a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable phone user access to that feature.

To display a list of all FACs, use the **show stcapp feature codes** command.

Examples

The following example shows how to change the value of the feature code for SCCP Meet-Me Conference from the default (5). This configuration also changes the value of the prefix for all FACs from the default (**) to ##. With this configuration, a phone user must press ##9 on the phone keypad to cancel all-call forwarding.

```
Router(config)# stcapp feature access-code
Router(config-stcapp-fac)# prefix ##
Router(config-stcapp-fac)# meetme-conference 9
Router(config-stcapp-fac)# exit
```

Related Commands

Command	Description
prefix (stcapp-fac)	Defines the prefix for feature access codes (FACs).
show stcapp feature codes	Displays all feature access codes (FACs).
stcapp feature access-code	Enables feature access codes (FACs) and enters STC application feature access-code configuration mode for changing values of the prefix and features codes from the default.

member (dial peer cor list)

To add a member to a dial peer class of restrictions (COR) list, use the **member** command in dial peer COR list configuration mode. To remove a member from a list, use the **no** form of this command.

member *class-name*
no **member** *class-name*

Syntax Description

class-name	Class name previously defined in dial peer COR custom configuration mode by using of the **name** command.

Command Default

No default behavior or values.

Command Modes

Dial peer COR list configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

The following example adds three members to the COR list named list3:

```
dial-peer cor list list3
 member 900_call
 member 800_call
 member catchall
```

Related Commands

Command	Description
dial-peer cor list	Defines a COR list name.

memory-limit (trace)

To define the memory limit for storing VoIP Trace information, use the **memory-limit** command in trace configuration mode. To reset to the default memory limit, use the **no** form of this command.

memory-limit { **platform** | **memory** }
no memory-limit { **platform** | **memory** }

Syntax Description

memory-limit	Defines the memory limit for storing VoIP Trace information.
memory	Defines a custom memory limit for VoIP Trace. Range is 10–1000 MB.
platform	Configures 10% of available platform memory at the time of configuration of the command as memory limit for VoIP Trace.

Command Default

A limit equivalent to 10% of available platform memory is enabled by default. (**memory-limit platform**)

Command Modes

Trace configuration mode (conf-serv-trace)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2 Cisco IOS XE Bengaluru 17.4.1a	This command was introduced on Cisco Unified Border Element.

Usage Guidelines

Configure **memory-limit** to define a custom memory limit for VoIP Trace information storage within the range of 10 MB to 1000 MB. If **platform** is configured, 10% of the total memory available to the IOS processor at the time of configuring is allocated to the storage of VoIP Trace information.

```
router(conf-voi-serv)#trace
router(conf-serv-trace)#?
memory-limit  Set limit on the usage of resources
router(conf-serv-trace)#memory-limit 10
```

Configuration of custom memory-limit more than the available platform memory is not allowed. Configuration fails with an error message:

```
router(config)#voice service voip
router(conf-voi-serv)#trace
router(conf-serv-trace)#memory-limit 800
Error: Setting memory-limit more than available platform memory (732 MB) is not allowed.
```

Configuration of memory-limit more than the 10% of the available platform memory affects the system performance. Configuration is successful with a warning message:

```
router(config)#voice service voip
router(conf-voi-serv)#trace
router(conf-serv-trace)#memory-limit 100
Warning: Setting memory limit more than 10% of available platform memory (73 MB) will affect
 system performance.
```

Reducing the memory-limit from an existing limit **resets** the VoIP Trace data. Take copy of the **show voip trace statistics detail** and **show voip trace all** output data before reducing the memory-limit.

A confirmation message is displayed when you reduce the memory-limit from an existing limit:

```
Reducing the memory-limit clears all VoIP Trace statistics and data.
If you wish to copy this data first, enter ‘no’ to cancel,
otherwise enter ‘yes’ to proceed.
```

Increasing the memory-limit does not impact the VoIP Trace data.

Note If the memory-limit is exhausted by active calls, incoming calls are not traced.

Examples

The following is a sample of CLI command **memory-limit** configured under trace configuration sub-mode:

```
router(conf-voi-serv)#trace
router(conf-serv-trace)#?
Voip Trace submode commands:
default       Set a command to its defaults
exit          Exit from voice service voip trace mode
no            Negate a command or set its defaults
shutdown      Shut Voip Trace debugging
memory-limit  Set limit based on memory used
router(conf-serv-trace)#memory-limit ?
<10-1000>     Specify maximum memory limit in MB
  platform    Use 10 percent of available memory
CSR(conf-serv-trace)#memory-limit 10
```

Related Commands

Command	Description
trace	Enables the VoIP Trace serviceability framework in CUBE.
shutdown (trace)	Disables the VoIP Trace serviceability framework in CUBE.
show voip trace	Displays the VoIP Trace information for SIP legs on a call that is received on CUBE.

message-exchange max-failures

To configure the maximum number of failed message that is exchanged between the application and the provider before the provider stops sending messages to the application, use the **message-exchange max-failures** command. To reset the maximum to the default number, use the **no** form of this command.

message-exchange max-failures *number*
no message-exchange max-failures *number*

Syntax Description

number	Maximum number of messages allowed before the service provider stops sending messages to the application. Range is from 1 to 3. Default is 1.

Command Default

The default is 1.

Command Modes

uc wsapi mode configuration mode

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use this command to set the maximum number of messages that can fail before the system determines that the application is unreachable and the service provider stops sending messages to the application.

Examples

The following example sets the maximum number of failed messages to 2.

```
Router(config)# uc wsapi
Router(config-uc-wsapi)# message-exchange max-failures 2
```

Related Commands

Command	Description
probing interval	Sets the time interval between probing messages.
probing max-failure	Sets the number of messages that the system will send without receiving a reply before the system unregisters the application.

method

To set a specific accounting method list, use the **method** command in gateway accounting AAA configuration mode.

method *acctMethListName*

Syntax Description

acctMethListName	Name of the accounting method list.

Command Default

H.323 is the default accounting method list.

Command Modes

Gateway accounting AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

- For information on setting AAA network security for your network, including setting method lists, refer to the *Authentication, Authorization, and Accounting Cisco IOS Security Configuration Guide* , Release 12.2.
- The **method** command sets the accounting method globally (not for a dial peer). To initially define the AAA method list name for accounting, use the **aaa accounting** command.
- The method list name used is the same name used to define the method list name under the **aaa accounting** command.

Examples

The following example uses the method list named "klz_aaa6" that was previously defined using the AAA commands.

```
aaa new-model
!
aaa group server radius sg6
server 1.6.30.70 auth-port 1708 acct-port 1709
!
aaa authentication login klz_aaa6 group sg6
! klz_aaa6 is defined as the method list name.
aaa authorization exec klz_aaa6 group sg6
aaa accounting connection klz_aaa6 start-stop group sg6
!
gw-accounting aaa
method klz_aaa6
! The same method list named klz_aaa6 is used.
```

Related Commands

Command	Description
aaa accounting	Enables accounting of requested services for billing or security purposes.

Command	Description
gw-accounting aaa	Enables VoIP gateway accounting.

mgcp

To allocate resources for the Media Gateway Control Protocol (MGCP) and start the MGCP daemon, use the **mgcp**command in global configuration mode. To terminate all calls, release all allocated resources, and stop the MGCP daemon, use the **no** form of this command.

mgcp [*port*]
no mgcp

Syntax Description

port	(Optional) User Datagram Protocol (UDP) port for the MGCP gateway. Range is from 1025 to 65535. The default is UDP port 2427.

Command Default

UDP port 2427

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 3660, Cisco uBR924, and Cisco 2600 series.
12.1(5)XM	This command was added to Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

Once you start the MGCP daemon using the **mgcp**command, you can suspend it (for example, for maintenance) by using the **mgcp block-newcalls** command. When you are ready to resume normal MGCP operations, use the **no mgcp block-newcalls** command. Use the **no mgcp** command only if you intend to terminate all MGCP applications and protocols.

W hen the MGCP daemon is not active, all MGCP messages are ignored.

If you want to change the UDP port while MGCP is running, you must stop the MGCP daemon using the **no mgcp** command, and then restart it with the new port number using the **mgcp** *port* command.

Examples

The following example initiates the MGCP daemon:

```
Router(config)# mgcp
```

The following example enables the MGCP daemon on port 4204:

```
Router(config)# mgcp
4204
```

Related Commands

Command	Description
application	Enables debugging on MGCP.
debug mgcp	Enables debugging on MGCP.
mgcp block -newcalls	Gracefully terminates all MGCP activity.
mgcp ip -tos	Enables or disables the IP ToS for MGCP connections.
mgcp request retries	Specifies the number of times to retry sending the **mgcp** command.
show mgcp	Displays the MGCP parameter settings.

mgcp behavior

To configure a gateway to alter the Media Gateway Control Protocol (MGCP) behavior, use the **mgcp behavior**command in global configuration mode. To resume using the standard protocol version behavior that is specified in the configuration, use the **no** form of this command.

mgcp behavior *category version*
no mgcp behavior *category version*

Syntax Description

category	MGCP behavior category. For valid values, see the first table below.
version	MGCP version for the behavior category. For valid values, see the second table below.

Command Default

The gateway follows the rules and guidelines that are specified by the configured MGCP protocol version.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T1	This command was introduced.
12.3(4)T	This command was modified. The **signals v0.1** keyword was added.
12.3(8)T	This command was modified. The **dlcx-clear-signals** keyword was added.
12.3(11)T	This command was modified. The **ack-init-rsip disable** and **init-rsip-per-insvc legacy**keywords were added.
12.3(14)T	This command was modified. The **q-mode-enduring legacy** keyword was added.
12.3(16)	This command was modified. The **mdcx-sdp ack-with-sdp**keyword was added.
12.4(4)T	This command was modified. The **rsip-range** keyword was added.
12.4(24)T	This command was modified. The default behavor of the mode parameter in the SDP was given higher preference to the mode present in the M: line of the MGCP message. The **digit-collect-stuck play-reorder**, **fxs-gs emulate-ls-disconnect**, **mode-attrb-in-sdp disable, private-localhost**, **and transient-state-response enable**keywords were added.
15.1(1)T	This command was modified. The **dynamically-change-codec-pt disable** keyword was added**.**
15.1(3)T	This command was modified. The **negotiate-nse enable** keyword was added.

Usage Guidelines

The table below describes the MGCP behavior category keywords.

Table 1: MGCP Behavior Category Keywords

Keywords	Description
ack-init-rsip disable	Forces the gateway to accept commands from the call agent before its initial ReStart In Progress (RSIP) messages are acknowledged; that is, 405 error codes do not occur. The gateway also behaves in this way if it is configured for MGCP Version 1.0 and earlier versions. By default, or when the **no** form of this command is issued, if the gateway is configured for MGCP Version RFC 3435-1.0 or later versions, it responds to call agent commands with a 405 error code until its initial RSIPs are acknowledged by the call agent.
digit-collect-stuck play-reorder	Forces the gateway to play a reorder tone to the user when 60 seconds have passed and when MGCP is in the process of collecting the digits. By default, or when the **no** form of this command is issued, if the MGCP application does not get a connection or gets disconnected within a specific time when the endpoint is in the off-hook state, then the endpoint may be busy in the digit collection state.
dlcx-clear-signals all	Forces the gateway to turn off or clear all signals when it receives a Delete Connection (DLCX) message from the call agent even if there is no S: line in the message. By default, and as specified by RFC 3435, the gateway maintains current endpoint signals if a DLCX has no S: line. The MGCP gateway clears signals only when the call agent explicitly turns off each signal or sends an empty S: line to clear all signals.
dynamically-change-codec-pt disable	Forces the gateway not to change the codec payload type when it is dynamically changed in the incoming Session Description Protocol (SDP). By default, or when **no** form of this command is issued, MGCP dynamically changes the payload, if the incoming SDP has a different codec.
fxs-gs emulate-ls-disconnect	Forces the gateway not to disconnect the call even when the gateway receives a DLCX for a ground-start enabled endpoint. The gateway plays the busy tone as the call does not get disconnected. By default, or when **no** form of thiscommand is issued, MGCP disconnects the call when it receives a DLCX.

<table>
<tr><th>Keywords</th><th>Description</th></tr>
<tr><td>init-rsip-per-insvc legacy</td><td>
Forces the gateway to always use the restart method of Restart for its initial RSIP messages, regardless of the service state of the endpoints. Wildcard demotion may occur as needed, based on configuration.
By default, or when the no form of this command is issued, if the MGCP gateway is running Version RFC 3435-1.0, the default restart method for initial RSIPs depends on the service state of the endpoint. For in-service endpoints, the restart method is Restart. For out-of-service endpoints, the restart method is Forced.
Additionally, regardless of the protocol version, the gateway always attempts to use a wildcard RSIP * message to minimize the number of messages that are sent to the call agent. The gateway sends the fully wildcarded RSIP * message as long as the following requirements are met:

MGCP is configured for a single profile (or the default profile) only.
A single DS0 group is configured for each DS1.
The single DS0 group includes all the possible DS0s.
All endpoints are in the same service state (when the MGCP call agent is configured for Version RFC 3435-1.0 and the no form of this command is issued).

If any one of these requirements is not met, the initial RSIP * message is demoted and sent as multiple RSIP messages to the call agent. When demoting, the gateway continues to attempt to minimize the number of RSIP messages.
</td></tr>
<tr><td>mdcx-sdp ack-with-sdp</td><td>
Forces the gateway to generate a SDP in response to a modify connection (MDCX) message that contains an SDP. The response contains the SDP only if the MDCX is responded to with a positive (200) acknowledgment.
By default, or when the no form of this command is issued, the positive acknowledgment reply generates an SDP only if any of the parameters have changed from the previous SDP that was generated by the gateway. With this command, even if all the parameters are the same as the previous SDP, the SDP is still generated. This enables operation with a SIP gateway that expects an SDP response to every CRCX or MDCX message.
</td></tr>
<tr><td>mode-attrb-in-sdp disable</td><td>
Forces the gateway to take connection mode M in Create Connection (CRCX).
By default, or when no form of this command is issued, preference is given to the connection mode present in SDP. This is only when the mode is present in SDP.
</td></tr>
<tr><td>negotiate-nse enable</td><td>
Makes MGCP gateway aware of the remote side’s Named Signaling Event (NSE) capabilities by examining the remote SDP for NSE capabilities.
By default, or when the no form of thiscommand is issued, NSE is disabled on the gateway.
Cisco Unified Call Manager (UCM) does not support modem or fax passthrough. This feature should not be enabled when Cisco UCM is the call agent.
</td></tr>
</table>

<table>
<tr><th>Keywords</th><th>Description</th></tr>
<tr><td>private-localhost</td><td>Requires the outgoing messages from the gateway, like Notify (NTFY), RSIP, DLCX, have the private-localhost appended to the endpoint ID.

By default, or when the no form of this command is issued, the outgoing messages from the gateway have the global router name appended to the endpoint ID.

This is applicable for MGCP 0.1 and MGCP 1.0 versions.</td></tr>
<tr><td>q-mode-enduring legacy</td><td>Allows the gateway to keep the current quarantine mode when a request notification (RQNT) does not contain a Q: line. Operation reverts to legacy behavior, which is the following:

Note Only the first bulleted item results in modified behavior.

• No Q: line--Makes no changes to the quarantine mode (whatever mode was set in the previous command persists).
• Empty Q: line--Resets the quarantine mode to the default.
• Valid Q: line--Sets the quarantine mode per command.
• Invalid Q: line--Generates an error.

Note The quarantine mode is set with the mgcp quarantine mode command, and the default is discarded. This is the configuration mode used if the quarantine mode is not specified in the RQNT or embedded request for events.

By default, or when the no form of this command is issued, MGCP behaves according to both MGCP Version 0.1 and MGCP Version 1.0 specifications--that is, the MGCP gateway resets the quarantine mode to the default in the running configuration if no Q: line is present.</td></tr>
<tr><td>rsip-range</td><td>Determines whether the gateway can generate RSIP messages with endpoint ranges for versions other than Trunking Gateway Control Protocol (TGCP). By default, endpoint ranges are generated in RSIP messages for TGCP only. The following category and version values can be configured:

• rsip-range all --Allows the gateway to generate endpoint ranges in RSIP messages for all MGCP versions.
• rsip-range none --Prevents the gateway from generating endpoint ranges for all MGCP versions, including TGCP.
• rsip-range tgcp-only --Allows the gateway to generate endpoint ranges in RSIP messages only if the configured protocol is TGCP. This is the default value.

TGCP specifications require support for endpoint ranges in RSIP messages. Not all call agents may support this functionality however. In such cases, selecting none allows the gateway to interoperate with these call agents. Conversely, if a non-TGCP call agent supports endpoint ranges, selecting all allows the gateway to take advantage of this functionality.</td></tr>
</table>

Keywords	Description
transient-state-response enable	Forces the gateway to send 400 responses for an MGCP message even if the endpoint is in a transient state. By default, or when **no** form of thiscommand is issued, the gateway does not respond to MGCP messages even if the endpoint is in a transient or disconnecting state.

The table below describes the MGCP behavior version keywords.

Table 2: MGCP Behavior Version Keywords

Keywords	Description
auep v0.1	Forces the gateway to reply to an Audit Endpoint (AUEP) command according to the MGCP Version 0.1 specification. This behavior applies specifically to the case in which the endpoint being audited is out of service. If this command is used, an AUEP command on an out-of-service endpoint returns error code of 501. By default, or when the **no** form of this command is issued, MGCP Version 1.0 behavior occurs--that is, response code 200 is sent for all valid endpoints, regardless of their service state, and requested audit information follows. In either case, the configured MGCP version is ignored.
signals v0.1	Forces the gateway to handle call signaling tones such as ringback, network congestion, reorder, busy, and off-hook warning tones according to the MGCP Version 0.1 specification. The MGCP Version 0.1 specification treats some call signaling tones as on-off tones, which terminate only after a specific MGCP message has been received to stop the signal. By default, or when the **no** form of this command is issued, RFC 3660 is followed, which treats the call signaling tones as timeout tones that terminate when the appropriate timeout expires. In either case, the configured MGCP version is ignored.

Examples

The following example shows how the gateway sends MGCP 0.1 responses to AUEP commands:

```
Router(config)# mgcp behavior auep v0.1
```

The following example shows how the gateway provides MGCP 0.1 treatment of call signaling tones:

```
Router(config)# mgcp behavior signals v0.1
```

The following example shows how to disable the requirement that the RSIP be acknowledged before a call agent command is accepted:

```
Router(config)# mgcp behavior ack-init-rsip disable
```

The following example show how to configure the gateway to not demote initial RSIPs based on the service state of the endpoints:

```
Router(config)# mgcp behavior init-rsip-per-insvc legacy
```

The following example shows how to configure the gateway to turn off all signals on receipt of a DLCX:

```
Router(config)# mgcp behavior dlcx-clear-signals all
```

The following examples show how to set quarantine mode to legacy:

```
Router(config)# mgcp behavior q-mode-enduring legacy
```

The following example shows how to force the gateway to generate an SDP in the response to an MDCX with SDP:

```
Router(config)# mgcp behavior mdcx-sdp ack-with-sdp
```

The following example shows how to force the gateway to generate endpoint ranges for all MGCP versions:

```
Router(config)# mgcp behavior rsip-range all
```

The following example shows how to force the gateway not to change the codec payload type when it is dynamically changed in the incoming SDP for all MGCP versions:

```
Router(config)# mgcp behavior dynamically-change-codec-pt disable
```

The following example shows how to force the gateway not to disconnect when it receives DLCX:

```
Router(config)# mgcp behavior fxs-gs emulate-ls-disconnect
```

The following example shows how forces the gateway to send responses for MGCP messages even if the endpoint is in a transient state:

```
Router(config)# mgcp behavior transient-state-response enable
```

The following example shows how to force the gateway to take connection mode M in CRCX:

```
Router(config)# mgcp behavior mode-attrb-in-sdp disable
```

The following example shows how to force the outgoing messages to have the configured private-localhost appended to the endpoint ID for MGCP 0.1 and MGCP 1.0 versions:

```
Router(config)# mgcp behavior private-localhost cisco.com
```

The following example shows how to force the gateway to play a reorder tone when MGCP is still stuck trying to collect digits:

```
Router(config)# mgcp behavior digit-collect-stuck play-reorder
```

The following example shows how to allow the gateway to be aware of NSE capabilities:

```
Router(config)# mccp behavior negotiate-nse enable
```

Use the following commands to display the MGCP behavior and versions settings:

```
Router# show running-config | include behavior
mgcp behavior auep v0.1
mgcp behavior signals v0.1
mgcp behavior ack-init-rsip disable
mgcp behavior init-rsip-per-insvc legacy
mgcp behavior q_mode-enduring legacy
```

```
mgcp behavior dlcx-clear-signals all
mgcp behavior mdcx-sdp ack-with-sdp
mgcp behavior rsip-range all
mgcp behaviour dynamically-change-codec-pt disable
mgcp behavior fxs-gs emulate-ls-disconnect
mgcp behavior transient-state-response enable
mgcp behavior mode-attrb-in-sdp-disable
mgcp behavior private-localhost cisco.com
mgcp behavior digit-collect-stuck- play-reorder
mgcp behavior negotiate-nse enable
Router# show running-config | include call-agent
mgcp call-agent ca123.example.net 4040 service-type mgcp version rfc3435-1.0
```

Related Commands

Command	Description
mgcp	Allocates resources for MGCP and starts the MGCP daemon.
mgcp call-agent	Specifies the address and protocol for the MGCP call agent.
mgcp quarantine mode	Configures the mode for MGCP quarantined events.
show mgcp	Displays values for MGCP parameters.
show running-config	Displays the contents of the currently running configuration file.

mgcp behavior comedia-check-media-src

To force IP address and port detection from the first RTP packet received for the entire Media Gateway Control Protocol (MGCP) gateway and enable the callback function selected by MGCP, use the **mgcp behavior comedia-check-media-src** command in global configuration mode.

mgcp behavior comedia-check-media-src {**enable** | **disable**}

Syntax Description

enable	Forces ip address and port detection.
disable	Disables ip address and port detection.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **mgcp behavior comedia-check-media-src** command to force IP address and port detection from the first rtp packet received for the entire MGCP gateway. This command also enables the callback function selected by MGCP, and with the configuration of the **mgcp behavior comedia-role** command contributes to the determination of whether to populate the SDP direction attribute.

Examples

The following example shows IP address and port detection being enabled for the entire MGCP gateway:

```
Router(config)# mgcp behavior comedia-check-media-src enable
```

Related Commands

Field	Description
mgcp	Allocates resources for the MGCP and starts the daemon.
mgcp behavior comedia-role	Specifies the location of the configured MGCP gateway.
mgcp behavior comedia-sdp-force	Forces the SDP to place the direction attribute in the SDP using the command as a reference.
show mgcp connection	Displays information for active MGCP-controlled connections.

mgcp behavior comedia-role

To specify the location of the configured Media Gateway Control Protocol (MGCP) gateway, use the **mgcp behavior comedia-role** command in global configuration mode.

mgcp behavior comedia-role {**active** | **passive** | **none**}

Syntax Description

active	Specifies MGCP gateways located inside NAT.
passive	Specifies MGCP gateways located outside of NAT.
none	Specifies gateway behavior be as in releases prior to Cisco IOS Release 12.4(11)T.

Command Default

none

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command will specify the location of the configured MGCP gateway and its role in solving the NAT media traversal. A comedia role of **active** is configured for MGCP gateways inside NAT. For gateways located outside of NAT a comedia role of **passive** is configured. Configuring the **none** keyword specifies gateway behavior before the **mgcp behavior comedia-role**command was introduced.

The **mgcp behavior comedia-role**and **mgcp behavior comedia-check-media-src** commands are used to determine when to populate the sdp direction attribute.

Examples

The following example shows the location of the MGCP gateway configured for MGCP gateways inside NAT:

```
Router(config)# mgcp behavior comedia-role active
```

Related Commands

Field	Description
mgcp behavior comedia-check-media-src	Enables ip address and port detection from the first rtp packet received for the entire MGCP gateway.
mgcp behavior comedia-sdp-force	Forces the SDP to place the direction attribute in the SDP using the command as a reference.
mgcp	Allocates resources for the MGCP and starts the daemon.
show mgcp	Displays the entire mgcp configuration.
show mgcp connection	Displays information for active MGCP-controlled connections.

mgcp behavior comedia-sdp-force

To force MGCP to place the direction attribute in the Session Description Protocol (SDP), use the **mgcp behavior comedia-sdp-force**command in global configuration mode.

mgcp behavior comedia-sdp-force {**enable** | **disable**}

Syntax Description

enable	Forces MGCP to place the direction attribute in the SDP.
disable	Allows the **mgcp behavior comedia-role**, and **mgcp behavior comedia-check-media-src** commands and the remote descriptor to determine if the direction attribute is added to the SDP.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command will force the MGCP to always place the direction attribute in the SDP using the **mgcp behavior comedia-sdp-force** command as a reference. When the **mgcp behavior comedia-sdp-force** command is configured with the **disable** keyword, the **mgcp behavior comedia-role** and **mgcp behavior comedia-check-media-src** commands and the remote descriptor determine if the direction is added to the SDP. If the role is not configured, this command has no effect.

Examples

The following example configuration forces the direction attribute to be placed in the SDP:

```
Router(config)# mgcp behavior comedia-sdp-force enable
```

Related Commands

Field	Description
mgcp	Allocates resources for the MGCP and starts the daemon.
mgcp behavior comedia-check-media-src	Enables ip address and port detection from the first rtp packet received for the entire MGCP gateway.
mgcp behavior comedia-role	Specifies the location of the configured MGCP gateway.
show mgcp connection	Displays information for active MGCP-controlled connections.

mgcp behavior g729-variants static-pt

To change the default from dynamic to static Real-time Transport Protocol (RTP) payload type on G.729 voice codecs, use the **mgcp behavior g729-variants static-pt** command in global configuration mode. To return the default to dynamic, use the **no** form of this command.

mgcp behavior g729-variants static-pt
no mgcp behavior g729-variants static-pt

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default, so the RTP payload type on G.729 voice codecs is static.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.4(22)T2 12.4(24)T1	This command was modified to be enabled by default.

Usage Guidelines

Prior to Cisco IOS Releases 12.4(22)T2 and 12.4(24)T1, the negotiated value (dynamic) payload type was not set in RTP packets. If you upgraded the Cisco IOS software on your network voice gateways (with existing Cisco Unified Communications Manager) and calls were going between Skinny Client Control Protocol (SCCP) phones controlled by Cisco Unified Communications Manager and public switched telephone network (PSTN) phones connected to a Cisco gateway, a condition of "no audio" could occur. The **mgcp behavior g729-variants static-pt**commandchanges the default from dynamic to static RTP payload type on G.729 voice codecs and eliminates the "no audio" condition.

Examples

The following example shows how to set the RTP payload type to static for G.729 voice codecs:

```
Router(config)# mgcp behavior g729-variants static-pt
```

Related Commands

Command	Description
mgcp codec	Selects the default codec type and its optional packetization period value.
mgcp rtp payload-type	Specifies use of the correct RTP payload type for backward compatibility in MGCP networks.

mgcp bind

To configure the source address for signaling and media packets to the IP address of a specific interface, use the **mgcp bind**command in global configuration mode. To disable binding, use the **no** form of this command.

mgcp bind {**control** | **media**} **source-interface** *interface-id*
no mgcp bind {**control** | **media**}

Syntax Description

control	Binds only Media Gateway Control Protocol (MGCP) control packets.
media	Binds only media packets.
source -interface	Specifies an interface as the source address of MGCP or Session Initiation Protocol (SIP) packets. **Note** The MGCP Gateway Support for the mgcp bind Command feature does not support SIP.
interface-id	Specifies the interface for source address of MGCP packets. The following are valid source addresses: • **Async** --Async interface • **BVI** --Bridge-Group Virtual Interface • **CTunnel** --CTunnel interface • **Dialer** --Dialer interface • **FastEthernet** --Fast Ethernet IEEE 802.3 • **Lex** --Lex interface • **Loopback** --Loopback interface • **MFR** --Multilink Frame Relay bundle interface • **Multilink** --Multilink-group interface • **Null** --Null interface • **Serial** --Serial • **Tunnel** --Tunnel interface • **Vif** --PGM Multicast Host interface • **Virtual -Template**--Virtual Template interface • **Virtual -TokenRin**g--Virtual Token Ring

Command Default

Binding is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced for MGCP on the Cisco 2400 series, Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5850, Cisco IAD2421, Cisco MC3810, and Cisco VG200.

Usage Guidelines

If the **mgcp bind** command is not enabled, the IP layer still provides the best local address.

A warning message is displayed if any of the following situations occur:

- When there are active MGCP calls on the gateway, the mgcp bind command is rejected for both control and media.
- If the bind interface is not up, the command is accepted but does not take effect until the interface comes up.
- If the IP address is not assigned on the bind interface, the mgcp bind command is accepted but takes effect only after a valid IP address is assigned. During this time, if MGCP calls are up, the mgcp bind command is rejected.
- When the bound interface goes down, either because of a manual shutdown on the interface or because of operational failure, the bind activity is disabled on that interface.
- When bind is not configured on the media gateway controller (MGC), the IP address used for sourcing MGCP control and media is the best available IP address.

Examples

The following example shows how the configuration of bind interfaces is shown when show running-config information is viewed:

```
.
.
.
mgcp bind control source-interface FastEthernet0
mgcp bind media source-interface FastEthernet0
.
.
.
```

Related Commands

Command	Description
show mgcp	Displays values for MGCP parameters.

mgcp block-newcalls

To block new calls while maintaining existing calls, use the **mgcp block-newcalls** command in global configuration mode. To resume media gateway control protocol (MGCP) operation, use the **no** form of this command.

mgcp block-newcalls
no mgcp block-newcalls

Syntax Description

This command has no arguments or keywords.

Command Default

New call are not blocked.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

This command is valid only if the **mgcp** command is enabled.

Once you issue this command, all requests for new connections (CreateConnection requests) are denied. All existing calls are maintained until participants terminate them or you use the **no mgcp** command. When the last active call is terminated, the MGCP daemon is terminated and all resources that are allocated to it are released. The **no mgcp block-newcalls** command returns the router to normal MGCP operations.

Examples

The following example prevents the gateway from receiving new calls:

```
Router(config)# mgcp block-newcalls
```

Related Commands

Command	Description
mgcp	Allocates resources for the MGCP and starts the daemon.

mgcp call-agent

To configure the address and protocol of the call agent for Media Gateway Control Protocol (MGCP) endpoints on a media gateway, use the **mgcp call-agent** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp call-agent {*host-nameip-address*} [*port*] [**service-type** *type* [**version** *protocol-version*]]
no mgcp call-agent

Syntax Description

host -name	Fully qualified domain name (including host portion) for the call agent; for example, ca123.example.net.
ip -address	IP address for the call agent.
port	(Optional) User Datagram Protocol (UDP) port over which the gateway sends messages to the call agent. Range is from 1025 to 65535.
service -type *type*	(Optional) Type of Gateway control service protocol. It can be one of the following values: • **mgcp** --Media Gateway Control Protocol • **ncs** --Network Communication Server • **sgcp** --Simple Gateway Control Protocol • **tgcp** --Trunking Gateway Control Protocol

version *protocol -version*	(Optional) Version of gateway control service protocol. It can be one of the following values:
	• For service-type mgcp: 0.1, 1.0, rfc3435-1.0
	  • 0.1--Version 0.1 of MGCP (Internet Draft)
	  • 1.0--Version 1.0 of MGCP (RFC2705 Version 1.0)
	  • rfc3435-1.0--Version 1.0 of MGCP (RFC3435 Version 1.0)
	Note This configuration value is used to allow the router to tailor the MGCP application behavior to be compatible based on the RFC2705 or RFC3435 definitions.
	• For service-type ncs: 1.0
	• For service-type sgcp: 1.1, 1.5
	• For service-type tgcp: 1.0

Command Default

Call-agent UDP port: 2727 for MGCP 1.0, NCS 1.0, and TGCP 1.0 Call-agent UDP port: 2427 for MGCP 0.1 and SGCP Call-agent UDP port: 2427 for Cisco CallManager Service type and version: mgcp 0.1 Service type for Cisco CallManager: mgcp

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	The service-type type keyword and argument were added.
12.1(5)XM	The **version***protocol-version* keyword and argument were added.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	New service types (ncs and tgcp) and appropriate versions were added. Version 1.0 was added for the mgcp service type. This command was implemented on Cisco 2600 series and Cisco 3600 series routers.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XN	This command was implemented to provide enhanced MGCP voice gateway interoperability on Cisco CallManager Version 3.1 for the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2 and implemented on the Cisco IAD2420 series and Cisco AS5850.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.3(8)T 1	This command was modified by adding the RFC3435-1.0 option to the command.

Usage Guidelines

Global call-agent configuration (with this command) and call-agent configuration for an MGCP profile (with the **mgcp profile call-agent** command) are mutually exclusive; the first to be configured on an endpoint blocks configuration of the other on the same endpoint.

Identifying call agents by Domain Name System (DNS) name rather than by IP address in the **mgcp call-agent**and **mgcp profile call-agent** commands provides call-agent redundancy, because a DNS name can have more than one IP address associated with it. If a call agent is identified by DNS name and a message from the gateway fails to reach the call agent, the **max1 lookup** and **max2 lookup** commands enable a search from the DNS lookup table for a backup call agent at a different IP address.

The *port* argument configures the call-agent port number (the UDP port over which the gateway sends messages to the call agent). The reverse (the gateway port number, or the UDP port over which the gateway receives messages from the call agent) is configured by specifying a port number in the **mgcp** command.

When the service type is set to mgcp, the call agent processes the restart in progress (RSIP) error messages sent by the gateway if the mgcp sgcp restart notify command is enabled. When the service type is set to sgcp, the call agent ignores the RSIP messages.

Use this command on any platform and media gateway.

The **mgcp**service type supports the RSIP error messages sent by the gateway if the **mgcp sgcp restart notify** command is enabled.

Examples

The following examples illustrate several formats for specifying the call agent (use any one of these formats):

```
Router(config)# mgcp call-agent 209.165.200.225 service-type mgcp version 1.0
Router(config)# mgcp call-agent 10.0.0.1 2427 service-type mgcp version rfc3435-1.0
Router(config)# mgcp call-agent igloo.northpole.net service-type ncs
Router(config)# mgcp call-agent igloo.northpole.net 2009 service-type sgcp version 1.5
Router(config)# mgcp call-agent 209.165.200.225 5530 service-type tgcp
```

Related Commands

Command	Description
call -agent	Specifies a call-agent address and protocol for an MGCP profile.
debug mgcp events	Displays debug messages for MGCP events.
max1 lookup	Enables DNS lookup of the MGCP call agent address when the suspicion threshold is reached.
max2 lookup	Enables DNS lookup of the MGCP call agent address when the disconnect threshold is reached.
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure an MGCP profile associated with one or more endpoints, or to configure the default profile.
mgcp sgcp restart notify	Starts RSIP message processing in the MGCP application.mgcp
sgcp restart notify	Enables the MGCP application to process SGCP-type RSIP messages.

mgcp codec

To select the codec type and its optional packetization period value, use the **mgcp codec** command in global configuration mode. To set the codec to its default value of G711 u-law, use the **no** form of this command.

mgcp codec *type* [**packetization-period** *value*]
no mgcp codec

Syntax Description

type	Type of codec supported. Valid codecs include the following: G711alaw, G711ulaw, G723ar53, G723ar63, G723r53, G723r63, G729ar8, G729br8, and G729r8.
packetization -period*value*	(Optional) Packetization period. This value is useful when the preferred compression algorithm and packetization period parameter is not provided by the media gateway controller. The range depends on the type of codec selected: • Range for **G729** is 10 to 220 in increments of 10. • Range for **G711** is 10 to 20 in increments of 10. • Range for **G723**is 30 to 330 in increments of 10.

Command Default

G711 u -law codec

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.1(5)XM	This command was implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5850.

Examples

The following example specifies the codec type:

```
Router(config)# mgcp codec g711alaw
```

The following example sets the codec type and packetization period:

```
Router(config)# mgcp codec g729r8 packetization-period 150
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp codec gsmamr-nb

To specify the Global System for Mobile Adaptive Multi-Rate Narrow Band (GSMAMR-NB) codec for an MGCP dial peer, use the **mgcp codec gsmamr-nb**command in dial peer voice configuration mode. To disable the GSMAMR-NB codec, use the **no** form of this command.

mgcp codec gsmamr-nb [**packetization-period 20**] [**encap rfc3267**] [**frame-format** {**bandwidth-efficient** | **octet-aligned** [{**crc** | **no-crc**}]}] [**modes** *modes-value*]
no mgcp codec gsmamr-nb

Syntax Description

packetization-period 20	(Optional) Sets the packetization period at 20 ms.
encap rfc3267	(Optional) Sets the encapsulation value to comply with RFC 3267.
frame-format	**(Optional) Specifies a frame format. Supported values are octet-aligned and bandwidth-efficient. The default is octet-aligned.**
crc | no-crc	**(Optional) CRC is applicable only for octet-aligned frame format. If you enter bandwidth-efficient frame format, the crc | no-crc options are not available because they are inapplicable.**
modes	(Optional) The eight speech-encoding modes (bit rates between 4.75 and 12.2 kbps) available in the GSMAMR-NB codec.
modes-value	(Optional) Valid values are from 0 to 7. You can specify modes as a range (for example, 0-2), or individual modes separated by commas (for example, 2,4,6), or a combination of the two (for example, 0-2,4,6-7).

Command Default

Packetization period is **20** ms. Encapsulation is **rfc3267**. Frame format is **octet-aligned**. CRC is **no-crc**. Modes value is **0-7**.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(11)XW	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use the **mgcp codec gsmamr-nb** command to configure the GSMAMR-NB codec and its parameters on the Cisco AS5350XM and Cisco AS5400XM platforms.

Examples

The following example shows how to set the codec to **gsmamr-nb** and set the parameters:

```
Router(config-dial-peer)# mgcp codec gsmamr-nb packetization-period 20 encap rfc3267
frame-format octet-aligned crc
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp codec ilbc

To specify the internet Low Bandwidth Codec (iLBC) for an MGCP dial peer, use the **mgcp codec ilbc**command in dial peer voice configuration mode. To disable the iLBC, use the **no** form of this command.

mgcp codec ilbc mode *frame_size* [**packetization-period** *value*]
no mgcp codec ilbc

Syntax Description

mode *frame_size*	Specifies the iLBC operating frame mode that is encapsulated in each packet in milliseconds (ms). Valid entries are the following: • 20--20, 40, 60, 80, 100 or 120 ms frames for 15.2 kbps bit rate. Default is 20. • 30--30, 60, 90, or 120 ms frames for 13.33 kbps bit rate. Default is 30.
packetization -period*value*	(Optional) Packetization period. This value is useful when the preferred compression algorithm and packetization period parameter are not provided by the media gateway controller. The range is 20 to120 in increments of 10.

Command Default

20ms frames for a 15.2 kbps bit rate.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(11)XW	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The iLBC is only supported on Cisco AS5350XM and Cisco AS5400XM Universal Gateways with Voice Feature Cards (VFCs) and IP-to-IP gateways with no transcoding and conferencing.

Examples

The following example shows how to set the MGCP codec to **ilbc** and set the parameters:

```
Router(config-dial-peer)# mgcp codec ilbc mode 20 packetization-period 60
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp crypto rfc-preferred

To enable support for the media-level Session Description Protocol (SDP) a=crypto attribute on Cisco IOS Media Gateway Control Protocol (MGCP) gateways, use the **mgcp crypto rfc-preferred** command in global configuration mode. To disable support for the a=crypto attribute, use the **no** form of this command.

mgcp crypto rfc-preferred
no mgcp crypto rfc-preferred

Syntax Description

This command has no arguments or keywords.

Command Default

Support for the a=crypto attribute is not enabled on Cisco IOS MGCP gateways.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)XA	This command was introduced.

Usage Guidelines

Cryptographic parameters for Secure RTP (SRTP) media sessions are signalled and negotiated using the crypto attribute in the SDP. Some versions of the crytpo attribute syntax set the crypto attribute name to the X-crypto keyword (a=X-crypto). RFC 4568 Session Description Protocol (SDP) Security Descriptions for Media Streams, defines the crypto attribute syntax, where the attribute name is set to the crypto keyword (a=crypto). You use the **mgcp crypto rfc-preferred** command to enable support for the a=crypto attribute on Cisco MGCP gateways.

When support for a=crypto is enabled, the system can choose to use the a=crypto or a=X-crypto notation, depending on the SDP received. By default, if a remote SDP is not present, all SDPs generated by the gateway use the a=crypto notation.

If the command is disabled, the gateway can understand both a=crypto or a=X-crypto in any SDP it receives. However, all SDPs generated by the gateway use the a=X-crypto notation.

You must configure the command based on the notation used by the call agent. For example, the Cisco public switched telephone network (PSTN) gateway (PGW) uses the a=crypto notation and Cisco Unified Call Manager uses the a=X-crypto notation.

Examples

The following example enables support for the SDP a=crypto attribute on the Cisco IOS MGCP gateway:

```
Router(config)# mgcp crypto rfc-preferred
```

The following is sample output from the **show mgcp** command when support for the SDP a=crypto attribute is enabled on the Cisco IOS MGCP gateway:

```
Router(config)# show mgcp
MGCP rsip-range is enabled for TGCP only.
MGCP Comedia role is NONE
MGCP Comedia check media source is DISABLED
MGCP Comedia SDP force is DISABLED
```

```
MGCP Guaranteed scheduler time is DISABLED
MGCP Disconnect delay error recovery DISABLED
MGCP support for a:crypto RFC notation is ENABLED
MGCP DNS stale threshold is 30 seconds
```

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, parser, and CAC.
max1 retries	Sets the MGCP suspicion threshold value (the number of attempts to retransmit messages to a call agent address before performing a new lookup for retransmission).
max2 retries	Set the MGCP disconnect threshold value (the number of attempts to retransmit messages to a call agent address before performing a new lookup for further retransmission).
mgcp	Allocates resources for the MGCP and starts the MGCP daemon.
mgcp block -newcalls	Blocks new calls while maintaining existing calls.
mgcp ip -tos	Enables or disables the IP ToS for MGCP connections.
mgcp profile	Creates and configures an MGCP profile to be associated with one or more MGCP endpoints or configures the default MGCP profile.
show mgcp	Displays values for MGCP parameters.

mgcp dns stale threshold

To configure the Media Gateway Control Protocol (MGCP) Domain Name System (DNS) stale threshold, use the **mgcp dns stale threshold** command in global configuration mode. To disable the stale threshold configuration, use the **no** form of this command.

mgcp dns stale threshold *seconds*
no mgcp dns stale threshold

Syntax Description

seconds	The threshold time in seconds, that MGCP DNS values are considered stale. The range is from 0 to 600. The default is 300.

Command Default

The MGCP DNS threshold value is set to 300 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.

Examples

The following example shows how to set the threshold stale time to 44 seconds:

```
Router(config)# mgcp dns stale threshold 44
```

Related Commands

Command	Description
show mgcp	Displays MGCP parameter details.

mgcp debug-header

To enable the display of Media Gateway Control Protocol (MGCP) module-dependent information in the debug header, use the **mgcp debug-header** command in global configuration mode. To disable the MGCP module-dependent information, use the **no** form of this command.

mgcp debug-header
no mgcp debug-header

Syntax Description

This command has no arguments or keywords.

Command Default

MGCP module-dependent information in the debug header is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

This command determines whether MGCP module-dependent information is displayed in the standard header for debug output.

Examples

The following example enables MGCP module-dependent information in debug headers:

```
Router(config)# mgcp debug-header
```

Related Commands

Command	Description
debug mgcp all	Enables all debug traces for MGCP.
debug mgcp endpoint	Enables debug traces for a specific MGCP endpoint.
mgcp	Starts the MGCP daemon.
show debugging	Displays the types of debugging that are enabled.
show mgcp	Displays the MGCP parameter settings.
voice call debug	Specifies the format of the debug header.

mgcp default-package

To configure the default package capability type for the media gateway, use the **mgcp default-package** command in global configuration mode. This command does not have a **no** form. To change the default package, use the **mgcp default-package** command with a different, actively supported package.

Residential Gateways
mgcp default-package {**dt-package** | **dtmf-package** | **fxr-package** | **gm-package** | **hs-package** | **line-package** | **ms-package** | **rtp-package**}

Business Gateways
mgcp default-package {**atm-package** | **dt-package** | **dtmf-package** | **fxr-package** | **gm-package** | **hs-package** | **line-package** | **ms-package** | **rtp-package** | **trunk-package**}

Trunking Gateways
mgcp default-package {**as-package** | **atm-package** | **dt-package** | **dtmf-package** | **gm-package** | **hs-package** | **md-package** | **mo-package** | **ms-package** | **nas-package** | **rtp-package** | **script-package** | **trunk-package**}

Syntax Description

as -package	Announcement server package.
atm -package	ATM package.
dtmf -package	DTMF package.
dt -package	DTMF trunk package (for Channel Associated Signaling (CAS) endpoints).
fxr-package	FXR package for fax transmissions.
gm -package	Generic media package.
hs -package	Handset package.
line -package	Line package.
md-package	MD package for Feature Group D (FGD) Exchange Access North American (EANA) signaling.
mo -package	MF operator services package (for CAS endpoints).
ms -package	MF wink/immediate start package (for CAS endpoints).
nas -package	Network access server package.
rtp -package	RTP package.
script -package	Script package.
trunk -package	Trunk package.

Command Default

For residential gateways: **line-package** For trunking gateways: **trunk-package**

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	The **line-package** keyword and a distinction between residential and trunking gateways were added.
12.1(5)XM	This command was implemented on the Cisco MC3810 and Cisco 3600 series. The **atm-package**, **hs-package**, **ms-package**, **dt-package**, and **mo-package** keywords were added.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
12.3(1)	The **fxr-package** keyword was added.
12.4(4)T	The **md-package** keyword was added.

Usage Guidelines

This command is helpful when the Media Gateway Controller does not provide the package capability to be used for the specific connection.

Before selecting a package as the default, use the **show mgcp** command to ensure that the package is actively supported. If the package you want does not appear in the display, use the **mgcp package-capability** command to add the package to the supported list.

Note The CAS packages (**dt-package**, **md-package**, **mo-package**, and **ms-package**) are available only as default package options. They do not appear as options in the **mgcp package-capability** command. This is because the non-CAS packages are configured on a per-gateway basis, whereas the CAS packages are defined on a per-trunk basis. Each trunk is defined using the **ds0-group** command.

If only one package is actively supported, it becomes the default package.

When the FXR package is the default, the call agent omits the "fxr/" prefix on two types of requests in CRCX, MDCX, DLCX, and RQNT messages: requests to detect events ("R:<pkg>/<evt>") and requests to generate events ("S:<pkg>/<evt>"). For example, to ask for T.38 detection, the call agent sends "R:t38" in an RQNT message rather than "R:fxr/t38." Note that the "fxr/fx:" parameter to the Local Connection Options is not affected by selection of FXR as the default package and always needs the "fxr/" prefix.

Examples

The following example sets the default package:

```
Router(config)# mgcp default-package as-package
! The announcement server package type will be the new default package type.
```

Related Commands

Command	Description
ds0-group	Specifies the DS0 time slots that make up a logical voice port

Command	Description
mgcp	Starts the MGCP daemon.
mgcp package -capability	Includes a specific MGCP package that is supported by the gateway.
show mgcp	Displays values for MGCP parameters.

mgcp disconnect-delay

To configure the MGCP disconnect delay error recovery mechanism, use the **mgcp disconnect-delay** command in global configuration mode. To disable error recovery, use the **no** form of this command.

mgcp disconnect-delay [**timeout** *seconds*]
no mgcp disconnect-delay

Syntax Description

timeout	(Optional) User defined timeout before the error recovery procedure is initiated.
seconds	Length of timeout, in seconds before the error recovery procedure is initiated. The range is from 2 to 15. There is no default.

Command Default

Disconnect delay error recovery is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T8, 12.4(20)T2	This command was introduced.
12.4(22)T1	This command was integrated into Cisco IOS Release 12.4(22)T1.

Usage Guidelines

When the FXS telephony endpoint disconnect request exceeds the configured timeout value for completion, the call agent continues to send MGCP messages, which cause the FXS endpoint to eventually block or unregister the gateway. To avoid this situation, configure the gateway with the **mgcp disconnect-delay**command so that the MGCP application initiates the disconnect delay error recovery procedure when the disconnect request takes too long to complete.

When the **mgcp disconnect-delay timeout** command is configured without the optional **timeout**keyword the disconnect delay error recovery mechanism is set to 7 seconds.

Examples

The following example shows the disconnect delay error recovery mechanism set to the default timeout of 7 seconds:

```
Router(config)# mgcp disconnect-delay
```

The following example shows the disconnect delay error recovery mechanism set with a user-defined 15 seconds:

```
Router(config)# mgcp disconnect-delay timeout 15
```

mgcp dtmf-relay

To ensure accurate forwarding of digits on compressed codecs, use the **mgcp dtmf-relay** command in global configuration mode. To disable this process for uncompressed codecs, use the **no** form of this command.

Voice over IP (VoIP)
mgcp dtmf-relay voip codec {**all** | **low-bit-rate**} **mode** {**cisco** | **disabled** | **nse** | **out-of-band** | **nte-gw** | **nte-ca**}
no mgcp dtmf-relay voip

Voice over AAL2 (VoAAL2)
mgcp dtmf-relay voaal2 codec [{**all** | **low-bit-rate**}]
no mgcp dtmf-relay voaal2

Syntax Description

voip	Specifies VoIP calls.
voaal2	Specifies voice over AAL2 (VoAAL2) calls (using Annex K type 3 packets).
codec	Specifies the MGCP DTMF relay codec configuration.
all	Specifies that dual-tone multifrequency (DTMF) relay is to be used with all voice codecs.
low -bit-rate	Specifies that the DTMF relay is to be used with only low-bit-rate voice codecs, such as G.729.
mode	Sets MGCP DTMF relay mode.
cisco	Specifies that Real-time Transport Protocol (RTP) digit events are encoded using a proprietary format similar to Frame Relay as described in the FRF.11 specification. The events are transmitted in the same RTP stream as nondigit voice samples, using payload type 121.
disabled	Sets MGCP DTMF relay mode to be disabled. This keyword is available only for the **all** keyword.
nse	Specifies that named signaling event (NSE) RTP digit events are encoded using the format specified in RFC 2833, Section 3.0, and are transmitted in the same RTP stream as nondigit voice samples, using the payload type that is configured using the **mgcp tse payload** command.
out -of-band	Specifies that Media Gateway Control Protocol (MGCP) digit events are sent using Notify (NTFY) messages to the call agent, which plays them on the remote gateway using Request Notification (RQNT) messages with **S:** (signal playout request).
nte-gw	Specifies that RTP digit events are encoded using the named telephony event (NTE) format specified in RFC 2833, Section 3.0, and are transmitted in the same RTP stream as nondigit voice samples. The payload type is negotiated by the gateways before use. The configured value for payload type is presented as the preferred choice at the beginning of the negotiation.
nte-ca	Behaves similar to the **nte-gw** keyword except that the call agent’s local connection options **a:** line is used to enable or disable DTMF relay.

Command Default

For the Cisco 7200 series router, the command is disabled. For all other platforms, noncompressed codecs are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.1(5)XM	This command was integrated into Cisco IOS Release 12.1(5)XM and implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series. The voaal2 keyword was added.
12.2(2)XB	This command was modified. The **nte-gw** and **nte-ca** keywords were added to this command.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(2)XN	This command was integrated into Cisco IOS Release 12.2(2)XN and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco Voice Gateway 200 (Cisco VG200).
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 2.0. This command was implemented on the following platforms: Cisco AS5300, Cisco AS5400, Cisco AS5850, and Cisco IAD2420.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T and implemented on the Cisco 1751 and Cisco 1760.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **disabled** keyword was added.

Usage Guidelines

Use this command to access an announcement server or a voice-mail server that cannot decode RTP packets containing DTMF digits. When the **mgcp dtmf-relay** command is active, the DTMF digits are removed from the voice stream and carried so that the server can decode the digits.

Only VoIP supports the **mode** keyword for forwarding digits on codecs.

Examples

The following example shows how to remove the DTMF tone from the voice stream and send FRF.11 with a special payload for the DTMF digits:

```
Router(config)# mgcp dtmf-relay codec mode cisco
```

The following example shows how to configure a low-bit-rate codec using VoIP in NSE mode:

```
Router(config)# mgcp dtmf-relay voip codec low-bit-rate mode nse
```

The following example shows how to configurev a codec for VoAAL2:

```
Router(config)# mgcp dtmf-relay voaal2 codec all
```

The following example shows how to configure a low-bit-rate codec using VoIP in NSE mode:

```
Router(config)# mgcp dtmf-relay voip codec low-bit-rate mode nse
```

The following example shows how to set the DTMF relay codec and mode to gateway:

```
Router(config)# mgcp dtmf-relay codec mode nte-gw
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp endpoint offset

To enable incrementing of the POTS or DS0 portion of an endpoint name when using the Network-based Call Signaling (NCS) 1.0 profile of Media Gateway Control Protocol (MGCP), use the **mgcp endpoint offset** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp endpoint offset
no mgcp endpoint offset

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used with NCS 1.0 to increment the POTS or DS0 portion of an endpoint name by 1 to minimize potential interoperability problems with call agents (media gateway controllers).

NCS 1.0 mandates that the port number of an endpoint be based on 1, and port numbering on some gateway platforms is based on 0.

When this command is configured, it offsets all endpoint names on the gateway. For example, an endpoint with a port number of aaln/0 is offset to aaln/1, and a DS0 group number of 0/0:0 is offset to 0/0:1.

Examples

The following example enables incrementing the port number portion of an endpoint name:

```
Router(config)# mgcp endpoint offset
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.

mgcp explicit hookstate

To enable detection of explicit hookstates, use the **mgcp explicit hookstate** command in global configuration mode. To disable hookstate detection, use the **no** form of this command.

mgcp explicit hookstate
no mgcp explicit hookstate

Syntax Description

This command has no arguments or keywords.

Command Default

Hookstate detection is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Explicit hookstate detection is enabled by default. In this state, the gateway returns a "401 endpoint already off hook" or "402 endpoint already on hook" NACK (Not Acknowledged) response to R:hu or R:hd event requests.

If you turn hookstate detection off with the **no**form of the **mgcp explicit hookstate** command, the hookstate is not checked when the gateway receives R:hu or R:hd event requests. The gateway acknowledges (ACK) these event requests.

Examples

The following example enables hookstate detection:

```
Router(config)# mgcp explicit hookstate
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp fax rate

To establish the maximum fax rate for Media Gateway Control Protocol (MGCP) T.38 sessions, use the **mgcp fax rate** command in global configuration mode. To reset MGCP endpoints to their default fax rate, use the **no** form of this command.

mgcp fax rate {**2400** | **4800** | **7200** | **9600** | **12000** | **14400** | **voice**}
no mgcp fax rate

Syntax Description

2400	Maximum fax transmission speed of 2400 bits per second (bps).
4800	Maximum fax transmission speed of 4800 bps.
7200	Maximum fax transmission speed of 7200 bps.
9600	Maximum fax transmission speed of 9600 bps.
12000	Maximum fax transmission speed of 12,000 bps.
14400	Maximum fax transmission speed of 14,400 bps.
voice	Highest possible transmission speed allowed by the voice codec. This is the default.

Command Default

MGCP fax rate is set to the highest possible transmission speed allowed by the voice codec (**mgcp fax rate voice**).

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use this command to specify the maximum fax transmission rate for all MGCP endpoints in the gateway.

The values for this command apply only to the fax transmission speed and do not affect the quality of the fax itself. The higher transmission speed values (14,400 bps) provide a faster transmission speed but use a significantly large portion of the available bandwidth. A lower transmission speed value (2400 bps, for example) provides a slower transmission speed but uses a smaller portion of the available bandwidth.

Note MGCP fax rate does not support call admission and control or bandwidth allocation.

When the MGCP fax rate is set to the highest possible transmission speed allowed by the voice codec (**mgcp fax rate voice**), all MGCP endpoints limit T.38 fax calls to this speed. For example, if the voice codec is G.711, fax transmission may occur up to 14,400 bps because 14,400 bps is less than the 64-kbps voice rate. If the voice codec is G.729 (8 kbps), the fax transmission speed is limited to the nearest fax rate of 7200 bps.

Tip

If the fax rate transmission speed is set higher than the codec rate in the same dial peer, the data sent over the network for fax transmission will be greater than the bandwidth reserved for Resource Reservation Protocol (RSVP). The **mgcp fax rate** command sets a maximum fax rate for T.30 negotiation (DIS/DCS). Fax machines can negotiate a lower rate, but not a higher rate.

Only values other than the default value appear in the saved gateway configuration.

Examples

The following example configures a maximum fax rate transmission speed of 9600 bps for MGCP T.38 fax relay sessions:

```
Router(config)# mgcp fax rate 9600
```

The following example configures the maximum fax rate transmission speed to 12,000 bps for MGCP T.38 fax relay sessions:

```
Router(config)# mgcp fax rate 12000
```

Related Commands

Command	Description
show call active fax	Displays the maximum fax rate for the current T.38 fax session.
show mgcp	Displays the current configuration for the MGCP fax rate.

mgcp fax-relay

To allow for the suppression of tones from the fax machine side so that Super Group 3 (SG3) fax machines can negotiate down to G3 speeds for Media Gateway Control Protocol (MGCP) fax relay, use the **mgcp fax-relay**commandinglobal configuration mode. To disable this function, use the **no** form of this command.

mgcp fax-relay {**ans-disable** | **sg3-to-g3**}
no mgcp fax-relay {**ans-disable** | **sg3-to-g3**}

Syntax Description

ans-disable	Suppresses ANS tones from originating SG3 fax machines so that these machines can operate at G3 speeds using fax relay.
sg3-to-g3	Allows SG3 machines to negotiate down to G3 speeds using fax relay.

Command Default

If this command is not enabled, modem upspeed can occur when ANS tones are detected and SG3-to-SG3 fax relay communication is not supported and probably will fail.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced as the **mgcp fax-relay sg3-to-g3** command.
12.4(6)T	This feature was implemented on the Cisco 1700 series and Cisco 2800 series.
12.4(20)T1	The **ans-disable** keyword was added.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

When the **mgcp fax-relay ans-disable** command is entered, modem upspeed does not occur when an ANS tone is detected. When the **ans-disable** keyword is entered, the modem-related sessions will fail because the ANS tones are squelched at the digital signal processor (DSP) level by the TI C5510 DSP.

When the **mgcp fax-relay sg3-to-g3** command is entered, the DSP fax-relay firmware suppresses the V.8 CM tone and the fax machines negotiate down to G3 speeds for the fax stream.

Examples

The following global configuration output shows V.8 fax CM message suppression being enabled on the voice dial peer for MGCP signaling types:

```
Router(config)# mgcp fax-relay sg3-to-g3
```

Related Commands

Command	Description
fax-relay (voice-service)	Allows ANS tones to be disabled for SG3 machines to operate at G3 speeds using fax relay and to enable the fax stream between two SG3 fax machines to negotiate down to G3 speeds on a VoIP dial peer.

Command	Description
mgcp fax t38	Specifies MGCP fax T.38 parameters.

mgcp fax t38

To configure MGCP fax T.38 parameters, use the **mgcp fax t38**command in global configuration mode. return a parameter to its default, use the **no** form of this command.

mgcp fax t38 {**ecm** | **gateway force** | **hs_redundancy** *factor* | **inhibit** | **ls_redundancy** *factor* | **nsf** *hexcode*}
no mgcp fax t38 {**ecm** | **gateway force** | **hs_redundancy** | **inhibit** | **ls_redundancy** | **nsf**}

Syntax Description

ecm	Enables error correction mode (ECM) for the gateway. By default, ECM is not enabled.
gateway force	Forces gateway-controlled T.38 fax relay using Cisco-proprietary named signaling events (NSEs) even if the capability to use T.38 and NSEs cannot be negotiated by the MGCP call agent at call setup time. The default is that force is not enabled.
hs_redundancy *factor*	Sends redundant T.38 fax packets. Refers to data redundancy in the high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. For the **hs_redundancy** parameter, the *factor* range is from 0 through 2. The default is 0 (no redundancy). **Note** Setting the **hs_redundancy** parameter to a value greater than 0 causes a significant increase in the network bandwidth consumed by the fax call.
inhibit	Disables use of T.38 for the gateway. By default, T.38 is enabled. **Note** If the MGCP gateway uses the auto-configuration function, the **mgcp fax t38 inhibit**command is automatically configured on the gateway each time a new configuration is downloaded. Beginning with Cisco IOS Software Release 12.4T, the auto-configuration of this command is removed. For MGCP gateways using auto-cofiguration and running Cisco IOS version 12.4T or later, you must manually configure the **mgcp fax t38 inhibit**command to use T.38 fax relay.
ls_redundancy *factor*	Sends redundant T.38 fax packets. The **ls_redundancy** parameter refers to data redundancy in the low-speed V.21-based T.30 fax machine protocol. For the **ls_redundancy** parameter, the *factor* range is from 0 through 2. Default is 0 (no redundancy).
nsf *hexcode*	Overrides the nonstandard facilities (NSF) code with the code provided using the *hexcode* argument. The *word* argument is a two-digit hexadecimal country code and a four-digit hexadecimal manufacturer code. By default, the NSF code is not overridden.

Command Default

ecm --disabled**gateway force**--disabled**hs_redundancy**--0**inhibit**--disabled (T.38 is enabled. See note in above table.)**ls_redundancy**--0**nsf**--not overridden

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was applicable to the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 in this release.
12.2(11)T2	This command was modified. The **gateway force** keyword pair was introduced.
12.2(15)T	This command was implemented on the Cisco 1751 and Cisco 1760.
12.4T	This command was modified. The **mgcp fax t38 inhibit**command was no longer configured by default for MGCP gateways that use the auto-configuration function.

Usage Guidelines

Nonstandard facilities (NSF) are capabilities a particular fax manufacturer has built into a fax machine to distinguish products from each other.

To disable T.38 fax relay, use the **mgcp fax t38 inhibit** command.

Some MGCP call agents do not properly pass those portions of Session Description Protocol (SDP) messages that advertise T.38 and NSE capabilities. As a result, gateways that are controlled by these call agents are unable to use NSEs to signal T.38 fax relay to other gateways that use NSEs. The **mgcp fax t38 gateway force** command provides a way to ensure gateway-controlled T.38 fax relay and use of NSEs between an MGCP gateway and another gateway. The other gateway can be an H.323, Session Initiation Protocol (SIP), or MGCP gateway. Both gateways must be configured to use NSEs to signal T.38 fax relay mode switchover. On H.323 and SIP gateways, use the **fax protocol t38 nse force**command to specify the use of NSEs for T.38 fax relay. On MGCP gateways, use the **mgcp fax t38 gateway force** command.

Examples

The following example configures the gateway to use NSEs for gateway-controlled T.38 fax relay signaling:

```
Router(config)# mgcp fax t38 gateway force
```

The following example shows that MGCP T.38 fax relay and ECM are enabled, NSF override is disabled, and low- and high-speed redundancy are set to the default value of 0:

```
Router(config)# mgcp fax t38 ecm

Router(config)# exit

Router# show mgcp

MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 172.18.195.147 2436 Initial protocol service is MGCP 0.1
MGCP block-newcalls DISABLED
MGCP send RSIP for SGCP is DISABLED
MGCP quarantine mode discard/step
MGCP quarantine of persistent events is ENABLED
MGCP dtmf-relay for VoIP disabled for all codec types
MGCP dtmf-relay for VoAAL2 disabled for all codec types
MGCP voip modem passthrough mode: CA, codec: g711ulaw, redundancy: DISABLED,
MGCP voaal2 modem passthrough mode: NSE, codec: g711ulaw
MGCP TSE payload: 119
MGCP T.38 Named Signalling Event (NSE) response timer: 200
```

```
MGCP Network (IP/AAL2) Continuity Test timer: 200
MGCP 'RTP stream loss' timer disabled
MGCP request timeout 500
MGCP maximum exponential request timeout 4000
MGCP gateway port: 2427, MGCP maximum waiting delay 3000
MGCP restart delay 0, MGCP vad DISABLED
MGCP rtrcac DISABLED
MGCP system resource check DISABLED
MGCP xpc-codec: DISABLED, MGCP persistent hookflash: DISABLED
MGCP persistent offhook: ENABLED, MGCP persistent onhook: DISABLED
MGCP piggyback msg ENABLED, MGCP endpoint offset DISABLED
MGCP simple-sdp DISABLED
MGCP undotted-notation DISABLED
MGCP codec type g729r8, MGCP packetization period 10
MGCP JB threshold lwm 30, MGCP JB threshold hwm 150
MGCP LAT threshold lmw 150, MGCP LAT threshold hwm 300
MGCP PL threshold lwm 1000, MGCP PL threshold hwm 10000
MGCP CL threshold lwm 1000, MGCP CL threshold hwm 10000
MGCP playout mode is adaptive 60, 4, 200 in msec
MGCP IP ToS low delay disabled, MGCP IP ToS high throughput disabled
MGCP IP ToS high reliability disabled, MGCP IP ToS low cost disabled
MGCP IP RTP precedence 5, MGCP signaling precedence: 3
MGCP default package: dt-package
MGCP supported packages: gm-package dtmf-package trunk-package line-package
                         hs-package rtp-package as-package atm-package ms-package
                         dt-package mo-package res-package mt-package
                         dt-package mo-package res-package mt-package
MGCP Digit Map matching order: shortest match
SGCP Digit Map matching order: always left-to-right
MGCP VoAAL2 ignore-lco-codec DISABLED
MGCP T.38 Fax is ENABLED
MGCP T.38 Fax ECM is ENABLED
MGCP T.38 Fax NSF Override is DISABLED
MGCP T.38 Fax Low Speed Redundancy: 0
MGCP T.38 Fax High Speed Redundancy: 0
```

The following example shows that NSF is overridden:

```
MGCP T.38 Fax NSF Override is ENABLED: AC04D3
```

Related Commands

Command	Description
fax protocol	Specifies fax protocol parameters on H.323 and SIP gateways.

mgcp ip qos dscp

To configure Differentiated Services Code Point (DSCP) for Media Gateway Control Protocol (MGCP) packets, use the **mgcp ip qos dscp** command in global configuration mode. To disable the configuration, use the **no** form of this command.

mgcp ip qos dscp {*dscp-valueaf-numbercs-number* | **default** | **ef**} {**media** | **signaling**}
no mgcp ip qos dscp {*dscp-valueaf-numbercs-number* | **default** | **ef**} {**media** | **signaling**}

Syntax Description

dscp-value	DSCP value. The range is from 0 to 63.
af-number	Assured forwarding bit pattern. The assure forwarding bit patterns are as follows: • **af11** • **af12** • **af13** • **af21** • **af22** • **af23** • **af31** • **af32** • **af33** • **af41** • **af42** • **af43** For more information, use the question mark (?) online help function.
cs-number	Class selector code point. The class selector code points are as follows: • **cs1** • **cs2** • **cs3** • **cs4** • **cs5** • **cs6** • **cs7** For more information, use the question mark (?) online help function.

default	Sets the DSCP to the default bit pattern. For more information, use the question mark (?) online help function.
ef	Sets the DSCP to the expedited forwarding bit pattern. For more information, use the question mark (?) online help function.
media	Applies DSCP to media payload packets.
signaling	Applies DSCP to signaling packets.

Command Default

DSCP is applied to media payload packets and signaling packets.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **mgcp ip qos dscp** command is used to set the DSCP for the quality of service. This command provides voice and signaling traffic priorities.

Examples

The following example shows how to configure DSCP for MGCP packets:

```
Router# configure terminal
Router(config)# mgcp ip qos dscp af31 signaling
```

Related Commands

Command	Description
show mgcp	Displays values for MGCP parameters.

mgcp ip-tos

To enable or disable the IP type of service (ToS) for media gateway control protocol (MGCP) connections, use the **mgcp ip-tos** command in global configuration mode. To restore the default, use the **no** form of this command.

mgcp ip-tos {**high-reliability** | **high-throughput** | **low-cost** | **low-delay** | **rtp precedence** *value* | **signaling precedence** *value*}
no mgcp ip-tos {**high-reliability** | **high-throughput** | **low-cost** | **low-delay** | **rtp precedence** *value* | **signaling precedence** *value*}

Syntax Description

high -reliability	High-reliability ToS.
high -throughput	High-throughput ToS.
low -cost	Low-cost ToS.
low -delay	Low-delay ToS.
rtp precedence *value*	Value of the Real-Time Transport Protocol (RTP) IP precedence bit. Range is from 0 to 7. The default is 3. **Note** In Cisco IOS Release 12.1(3)T, this parameter was **precedence** *value*.
signaling precedence *value*	IP precedence value for MGCP User Datagram Protocol (UDP) and Real-Time Transport Protocol Control Protocol (RTCP) signaling packets. Range is from 0 to 7. The default is 3.

Command Default

Services are disabled. RTP precedence: 3 Signaling precedence: 3

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.1(5)XM	This command was implemented on the Cisco MC3810. The **precedence**parameter was changed to **rtp precedence** and the **signaling precedence** parameter was added.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Only one of the keywords in the group **high-reliability**, **high-throughput**, **low-cost**, and **low-delay** can be enabled at any given time. Enabling one keyword disables any other that was active. Enabling one of these keywords has no effect on the **precedence** value.

The **no** form of the **mgcp ip-tos** command disables the first four keywords and sets **the precedence value**back to 3.

When you configure a new value for **precedence**, the old value is erased.

Examples

The following example activates the **low-delay** keyword and disables the previous three keywords:

```
Router(config)# mgcp ip-tos high-rel
Router(config)# mgcp ip-tos high-throughput
Router(config)# mgcp ip-tos low-cost
Router(config)# mgcp ip-tos low-delay
Router(config)# mgcp ip-tos rtp precedence 4
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp lawful-intercept

To enable the lawful-intercept feature for the Media Gateway Control Protocol (MGCP), use the **mgcp lawful-intercept**command in global configuration mode. To disable the feature in mgcp, use the **no** form of this command.

mgcp lawful-intercept
no mgcp lawful-intercept

Syntax Description

This command has no arguments or keywords.

Command Default

Lawful Intercept feature is enabled in mgcp.

Command Modes

Global configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The Lawful Intercept feature is the process law enforcement agencies conduct electronic surveillance of circuit and packet-mode communications as authorized by judicial or administrative order. By default the **lawful-intercept** feature is enabled in mgcp. The **no mgcp lawful-intercept** command is used to disable the lawful-intercept feature in mgcp.

Examples

The following example shows the electronic surveillance being disabled:

```
Router(config)# no mgcp lawful-intercept
```

Related Commands

Command	Description
debug mgcp	Enables debugging on MGCP.
show mgcp	Displays the MGCP parameter settings.

mgcp max-waiting-delay

To specify the media gateway control protocol (MGCP) maximum waiting delay (MWD), use the **mgcp max-waiting-delay** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp max-waiting-delay *milliseconds*
no mgcp max-waiting-delay

Syntax Description

milliseconds	Time, in milliseconds, to wait after restart. Range is from 0 to 600000 (600 seconds). The default is 3000 (3 seconds).

Command Default

3000 ms

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

Use this command to send out an Restart in Progress (RSIP) message to the call agent with the restart method. This command helps prevent traffic bottlenecks caused by MGCP gateways all trying to connect at the same time after a restart.

Examples

The following example sets the MGCP maximum waiting delay to 600 ms:

```
Router(config)# mgcp max-waiting-delay 600
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp restart -delay	Configures the graceful teardown method sent in the RSIP message.

mgcp modem passthrough codec

To select the codec that enables the gateway to send and receive modem and fax data in VoIP and VoATM adaptation layer 2 (VoAAL2) configurations, use the **mgcp modem passthrough codec**command in global configuration mode. To disable support for modem and fax data, use the **no** form of this command.

mgcp modem passthrough {**voip** | **voaal2**} **codec** {**g711alaw** | **g711ulaw**}
no mgcp modem passthrough {**voip** | **voaal2**}

Syntax Description

voip	VoIP voice protocol.
voaal2	VoAAL2 voice protocol.
g711alaw	G.711 a-law codec for changing speeds during modem and fax switchover.
g711ulaw	G.711 u-law codec for changing speeds during modem and fax switchover.

Command Default

The g711 u-law codec for both VOIP and VOAAL2

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.1(5)XM	This command was implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Use this command for fax pass-through because the answer tone can come from either modem or fax transmissions. Selecting a codec dynamically changes the codec type and speed to meet network conditions.

Examples

The following example enables a gateway to send and receive VoAAL2 modem or fax data using the G711 a-law codec:

```
Router(config)# mgcp modem passthrough voaal2 codec g711alaw
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp modem passthrough mode	Sets the method for changing speeds for modem and fax transmissions on the gateway.
mgcp quarantine persistent -events disable	Enables redundancy for VoIP modem and fax transmissions.

Command	Description
mgcp tse payload	Enables the TSE payload for modem and fax operation.

mgcp modem passthrough mode

To set the method for changing speeds that enables the gateway to send and receive modem and fax data in VoIP and VoATM adaptation layer 2 (VoAAL2) configurations, use the **mgcp modem passthrough mode**command in global configuration mode. To disable support for modem and fax data, use the **no** form of this command.

mgcp modem passthrough {**voip** | **voaal2**} **mode** {**cisco** | **nse**}
no mgcp modem passthrough {**voip** | **voaal2**}

Syntax Description

voip	VoIP.
voaal2	Voice over AAL2 calls using Annex K type 3 packets.
cisco	Cisco-proprietary method for changing modem speeds, based on the protocol.
nse	Named signaling event (NSE)-based method for changing modem speeds. For VoAAL2 configurations, AAL2 Annex K (type 3) is used.

Command Default

NSE-based method

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.1(5)XM	This command was implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series router.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Use this command for fax pass-through because the answer tone can come from either modem or fax transmissions.

Upspeed is the method used to change the codec type and speed dynamically to meet network conditions.

If you use the **nse** keyword, you must also use the **mgcp tse payload** command.

If you use the default **nse** keyword and the **voip** or **voaal2** keyword, the **show run** command does *not* display the **mgcp modem passthrough mode** command in the configuration output, although the command is displayed for the **cisco**keyword. The **show mgcp** command displays settings for both the **nse** and **cisco** keywords.

Examples

The following example enables a gateway to send and receive VoIP modem or fax data using the NSE modem-speed-changing method:

```
Router(config)# mgcp modem passthrough voip mode nse
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp modem passthrough codec	Selects the codec to use for modem and fax transmissions on the gateway.
mgcp quarantine persistent -events disable	Enables redundancy for VoIP modem and fax transmissions.
mgcp tse payload	Enables the TSE payload for modem and fax operation.

mgcp modem passthrough voip redundancy

To enable redundancy on a gateway that sends and receives modem and fax data in VoIP configurations, use the **mgcp modem passthrough voip redundancy**command in global configuration mode. To disable redundancy, use the **no** form of this command.

mgcp modem passthrough voip redundancy [**sample-duration** [{**10** | **20**}]] [**maximum-sessions** *number*]
no mgcp modem passthrough voip redundancy [**sample-duration** [{**10** | **20**}]] [**maximum-sessions** *number*]

Syntax Description

sample-duration	(Optional) Specifies the time length of the largest Real-time Transport Protocol (RTP) packet when packet redundancy is active, in milliseconds (ms).
10 | 20	(Optional) Specifies the redundancy sample duration in milliseconds (ms). The default sample duration is 10.
maximum-sessions	(Optional) Specifies the maximum number of redundant sessions that can run simultaneously on each subsystem.
number	Number of maximum modem passthrough sessions on each module. The range is from 1 to 30.

Command Default

The default redundancy sample duration is 10 milliseconds (ms).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco AS5300 and Cisco AS5850.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The *number*argument and the following keywords were added: • **sample-duration** • **10 | 20** • **maximum-sessions**

Usage Guidelines

Use the **modem passthrough voip redundancy**command for fax pass-through because the answer tone can come from either modem or fax transmissions. This command enables a single repetition of packets (using

RFC 2198) to improve reliability by protecting against packet loss. When redundancy is on, all calls on the gateway are affected.

Upspeed is the method used to dynamically change the codec type and speed to meet network conditions.

Examples

The following example shows how to enable redundancy for VoIP modem and fax transmissions on a gateway:

```
Router(config)# mgcp modem passthrough voip redundancy sample-duration 20
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp modem passthrough codec	Selects the codec for modem and fax transmissions.
mgcp modem passthrough mode	Sets the method for changing speeds for modem and fax transmissions on the gateway.
mgcp tse payload	Enables the TSE payload for modem and fax operation.

mgcp modem passthru

To enable the gateway to send and receive modem and fax data, use the **mgcp modem passthru** command in global configuration mode. To disable support for modem and fax data, use the **no** form of this command.

mgcp modem passthru {**cisco** | **ca**}
no mgcp modem passthru

Syntax Description

cisco	When the gateway detects a modem/fax tone, it switches the codec to G.711 to allow the analog data to pass through.
ca	When the gateway detects a modem/fax tone, it alerts the call agent to switch the codec to G.711 to allow the analog data to pass through.

Command Default

ca

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was added to MGCP.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

When the **cisco** keyword is activated and the gateway detects a modem/fax tone, the gateway switches the codec to G.711 then sends the analog data to a remote gateway. The remote gateway also switches the codec on its side of the call to G.711 to allow the analog data to pass through.

When the **ca**keyword is activated and the gateway detects a modem/fax tone, the gateway alerts the call agent to switch the codec to G.711 to allow the analog data to pass through. The call agent must send an MDCX signal to the G.711 codec for successful data pass-through.

Examples

The following example configures a gateway to send and receive modem or fax data:

```
Router(config)# mgcp modem passthru cisco
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp modem relay voip gateway-xid

To enable in-band negotiation of compression parameters between two VoIP gateways using Media Gateway Control Protocol (MGCP), use the **mgcp modem relay voip gateway-xid** command in global configuration mode. To disable this function, use the **no** form of this command.

mgcp modem relay voip gateway-xid [**compress** {**backward** | **both** | **forward** | **no**}] [**dictionary** *value*] [**string-length** *value*]
no mgcp modem relay voip gateway-xid

Syntax Description

compress	(Optional) Direction in which data flow is compressed. For normal dialup, compression should be enabled in both directions. You may want to disable compression in one or more directions. This is normally done during testing and perhaps for gaming applications, but not for normal dialup when compression is enabled in both directions. • **backward** --Enables compression only in the backward direction. • **both** --Enables compression in both directions. For normal dialup, this is the preferred setting. This is the default. • **forward** --Enables compression only in the forward direction. • no--Disables compression in both directions.
dictionary *value*	(Optional) V.42*bis* parameter that specifies characteristics of the compression algorithm. Range is from 512 to 2048. Default is 1024. **Note** Your modem may support values higher than this range. A value acceptable to both sides is negotiated during modem call setup.
string -length*value*	(Optional) V.42*bis* parameter that specifies characteristics of the compression algorithm. Range is from 16 to 32. Default is 32. **Note** Your modem may support values higher than this range. A value acceptable to both sides is negotiated during modem call setup.

Command Default

Command: enabled Compress: both Dictionary: 1024 String length: 32

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.

Usage Guidelines

This command enables XID negotiation for modem relay. By default it is enabled.

This command affects only VoIP calls and not Voice over ATM adaption layer 2 (VoAAL2) calls. This is because MGCP supports VoAAL2 calls for voice and fax/modem, but not for modem relay.

If this command is enabled on both VoIP gateways of a network, the gateways determine whether they need to engage in in-band negotiation of various compression parameters. The remaining keywords in this command specify the negotiation posture of this gateway in the subsequent in-band negotiation (assuming that in-band negotiation is agreed on by the two gateways).

The **compress**, **dictionary**, and **string-length** keywords are digital-signal-processor (DSP)-specific and related to xid negotiation. If this command is disabled, they are all irrelevant. The application (MGCP or H.323) just passes these configured values to the DSPs, and it is the DSP that requires them.

Examples

The following example enables in-band negotiation of compression parameters on the VoIP gateway, with compression in both directions, dictionary size of 1024, and string length of 32 for the compression algorithm:

```
mgcp modem relay voip gateway-xid compress both dictionary 1024 string-length 32
```

Related Commands

Command	Description
mgcp modem relay voip mode	Enables modem relay mode support in a gateway for MGCP VoIP calls.
mgcp modem relay voip sprt retries	Sets the maximum number of times that the SPRT protocol tries to send a packet before disconnecting.
modem relay gateway-xid	Enables in-band negotiation of compression parameters between two VoIP gateways that use MBCP.
mgcp tse payload	Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP.

mgcp modem relay voip latency

To optimize the Modem Relay Transport Protocol and the estimated one-way delay across the IP network using Media Gateway Control Protocol (MGCP), use the **mgcp modem relay voip latency** command in global configuration mode. To disable this function, use the **no** form of this command.

mgcp modem relay voip latency *value*
no mgcp modem relay voip latency

Syntax Description

value	Estimated one-way delay across the IP network, in milliseconds. Range is from 100 to 1000. Default is 200.

Command Default

200 ms

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.

Usage Guidelines

Use this command to adjust the retransmission timer of the Simple Packet Relay Transport (SPRT) protocol, if required, by setting the value to the estimated one-way delay (in milliseconds) across the IP network. Changing this value may affect the throughput or delay characteristics of the modem relay call. The default value of 200 does not need to be changed for most networks.

Examples

The following example sets the estimated one-way delay across the IP network to 100 ms.

```
mgcp modem relay voip latency 100
```

Related Commands

Command	Description
mgcp modem relay voip mode	Enables modem relay mode support in a gateway for MGCP VoIP calls.
mgcp modem relay voip sprt retries	Sets the maximum number of times that the SPRT protocol tries to send a packet before disconnecting.
mgcp tse payload	Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP.
modem relay gateway-xid	Enables in-band negotiation of compression parameters between two VoIP gateways that use MBCP.
modem relay latency	Optimizes the Modem Relay Transport Protocol and the estimated one-way delay across the IP network.

mgcp modem relay voip mode

To enable named signaling event (NSE) based modem relay mode for VoIP calls on a Media Gateway Control Protocol (MGCP) gateway, use the **mgcp modem relay voip mode** command in global configuration mode. To disable this function, use the **no** form of this command.

mgcp modem relay voip mode [**nse**] **codec** [{**g711alaw** | **g711ulaw**}] [**redundancy**] **gw-controlled**
no mgcp modem relay voip mode

Syntax Description

nse	(Optional) Instructs the gateway to use NSE mode for upspeeding.
codec	(Optional) Specifies a codec to use for upspeeding: • **g711alaw** --G.711 a-law 64,000 bits per second (bps) for E1. • **g711ulaw** --G.711 mu-law 64,000 bps for T1. This is the default.
redundancy	(Optional) Specifies packet redundancy for modem traffic during modem pass-through. By default, redundancy is disabled.
gw-controlled	Specifies the gateway-configured method for establishing modem relay parameters.

Command Default

Modem relay in NSE mode is disabled. All modem calls go through as pass-through calls, which are less reliable and use more bandwidth than modem relay calls, provided that pass-through is enabled. The G.711 mu-law codec is used for upspeeding. Redundancy is disabled and no duplicate data packets are sent while the gateway is in modem/fax pass-through mode.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.
12.4(2)T	Usage guidelines were added for the **nse** keyword.
12.4(4)T	The **gw-controlled** keyword was added.
12.4(6)T	This feature was implemented on the Cisco 1700 series and Cisco 2800 series.

Usage Guidelines

The **mgcp modem relay voip mode**command enables non secure modem relay mode for MGCP VoIP calls. By default, NSE modem relay mode is disabled. This command configures upspeeding, which is needed because modem pass-through is an intermediate step while the gateway switches from handling voice calls to handling modem relay calls.

The **mgcp modem relay voip mode nse** command is not supported on the TI C2510 digital signal processor (DSP), formerly known as the TI C5510 DSP; only the TI C549 DSP supports negotiation of NSE parameters. If Cisco CallManager is used as the call agent, the **mgcp modem relay voip mode nse** command is not supported.

Redundancy causes the gateway to generate duplicate (redundant) data packets for fax/modem pass-through calls as per RFC 2198. For these calls to be more reliable, redundant packets transmission is needed to make up for excessive loss of packets in VoIP networks. Even if one of the gateways is configured with redundancy, calls go through. Gateways can handle asymmetric (one-way) redundancy.

To enable secure voice and data calls between Secure Telephone Equipment (STE) and IP-STE endpoints using the state signaling events (SSE) protocol, use the **mgcp modem relay voip mode sse** command. Before configuring SSE parameters, you must use the **mgcp package-capability mdste** command to enable modem relay capabilities and SSE protocol support.

The **gw-controlled** keyword specifies that modem transport parameters are configured directly on the gateway instead of being negotiated by the call agent.

Examples

The following example enables MGCP modem relay and specifies the following: NSE mode for upspeeding, G.711 mu-law codec, packet redundancy, and gateway-controlled for modem traffic during modem pass-through:

```
Router(config)# mgcp modem relay voip mode nse codec g711ulaw redundancy gw-controlled
```

Related Commands

Command	Description
mgcp modem relay voip gateway-xid	Optimizes the modem relay transport protocol and the estimated one-way delay across the IP network.
mgcp modem relay voip mode sse	Enables SSE-based modem relay.
mgcp package-capability mdste	Enables MGCP gateway support for processing events and signals for modem connections over a secure communication path between IP-STE and STE.
mgcp tse payload	Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP.

mgcp modem relay voip mode sse

To enable State Signaling Event (SSE) based modem relay mode and to configure SSE parameters on the MGCP gateway, use the **mgcp modem relay voip mode sse** command in global configuration mode. To disable this function, use the **no** form of this command.

mgcp modem relay voip mode sse [**redundancy** [{**interval** *number* | **packet** *number*}]] [**retries** *value*] [**t1** *time*]
no mgcp modem relay voip mode sse

Syntax Description

redundancy	(Optional) Packet redundancy for modem traffic during modem pass-through. By default redundancy is disabled.
interval *milliseconds*	(Optional) Specifies the timer in milliseconds (ms) for redundant transmission of SSEs. Range is 5 - 50 ms. Default is 20 ms.
packet *number*	(Optional) Specifies the SSE packet retransmission count before disconnecting. Range is 1- 5 packets. Default is 3 packets.
retries *value*	(Optional) Specifies the number of SSE packet retries, repeated every **t1** interval, before disconnecting. Range is 0 - 5 retries. Default is 5 retries.
t1 *milliseconds*	(Optional) Specifies the repeat interval, in milliseconds, for initial audio SSEs used for resetting the SSE protocol state machine (clearing the call) following error recovery. Range is 500 - 3000 ms. Default is 1000 ms.

Command Default

SSE mode is enabled by default, using default parameter values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced

Usage Guidelines

Use the **mgcp modem relay voip mode sse**command to configure state signaling events (SSE) parameters for secure MGCP voice and data calls between Secure Telephone Equipment (STE) and IP STE endpoints using the SSE protocol, a subset of the V.150.1 standard for modem relay. SSEs, which are Real-Time Transport Protocol (RTP) encoded event messages, are used to coordinate transitions between the different media states, secure and nonsecure. Before configuring SSE parameters, you must use the **mgcp package-capability mdste**command to enable modem relay capabilities and SSE protocol support.

Examples

The following examples configure SSE parameters for redundancy interval redindancy packet count, number of retries and the **t1**timer interval:

```
Router(config)# mgcp modem relay voip mode sse redundancy interval 20
Router(config)# mgcp modem relay voip mode sse redundancy packet 4
Router(config)# mgcp modem relay voip mode sse retries 5
Router(config)# mgcp modem relay voip mode sse t1 1000
```

Related Commands

Command	Description
mgcp package-capability mdste	Enables MGCP gateway support for processing events and signals for modem connections over a secure communication path between IP Secure Telephone Equipment (IP-STE) and STE.

mgcp modem relay voip sprt retries

To set the maximum number of times that the Simple Packet Relay Transport (SPRT) protocol tries to send a packet before disconnecting, use the mgcp modem relay voip sprt retries command in global configuration mode. To disable this function, use the **no** form of this command.

mgcp modem relay voip sprt retries *value*
no mgcp modem relay voip sprt retries

Syntax Description

value	Maximum number of times that the SPRT protocol tries to send a packet before disconnecting. Range is from 6 to 30. The default is 12.

Command Default

12 times

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.

Examples

The following example sets 15 as the maximum number of times that the SPRT protocol tries to send a packet before disconnecting:

```
mgcp modem relay voip sprt retries 15
```

Related Commands

Command	Description
mgcp modem relay voip gateway-xid	Optimizes the Modem Relay Transport Protocol and the estimated one-way delay across the IP network.
mgcp modem relay voip mode	Enables modem relay mode support in a gateway for MGCP VoIP calls.
mgcp tse payload	Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP.
modem relay gateway-xid	Enables in-band negotiation of compression parameters between two VoIP gateways that use MBCP.

mgcp modem relay voip sprt v14

To configure V.14 modem relay parameters for packets sent by the Simple Packet Relay Transport (SPRT) protocol, use the **mgcp modem relay voip sprt v14** command in global configuration mode. To disable this function, use the **no** form of this command.

mgcp modem relay voip sprt v14 [{**receive playback hold-time** *milliseconds* | **transmit hold-time** *milliseconds* | **transmit maximum hold-count** *characters*}]
no mgcp modem relay voip sprt v14

Syntax Description

receive playback hold-time *milliseconds*	Configures the time in milliseconds (ms) to hold incoming data in the V.14 receive queue. Range is 20 to 250 ms. Default is 50 ms.
transmit hold-time *milliseconds*	Configures the time to wait, in ms, after the first character is ready before sending the SPRT packet. Range is 10 to 30 ms. Default is 20 ms.
transmit maximum hold-count *characters*	Configures the number of V.14 characters to be received on the ISDN public switched telephone network (PSTN) interface that will trigger sending the SPRT packet. Range is 8 to 128. Default is 16.

Command Default

V.14 modem relay parameters are enabled by default, using default parameter values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

The maximum size of receive buffers is set at 500 characters, a nonprovisionable limit. Use the **mgcp modem relay voip sprt v14 receive playback hold-time** *milliseconds*command to configure the minimum holding time before characters can be removed from the receive queue. Characters received on the PSTN or ISDN interface may be collected for a configurable collection period before being sent out on SPRT channel 3, potentially resulting in variable size SPRT packets. To configure V.14 transmit parameters for SPRT packets, use the **mgcp modem relay voip sprt v14 transmit hold-time** *milliseconds and*the **mgcp modem relay voip sprt v14 transmit maximum hold-count** *characters*commands.

Parameter changes do not take effect during existing calls; they affect new calls only.

SPRT transport channel 1 is not supported.

Examples

The following example sets 200 ms as the receive playback hold time, 25 ms as the transmit hold time, and 10 characters as the transmit hold count parameters:

```
Router(config)# mgcp modem relay voip sprt v14 receive playback hold-time 200
Router(config)# mgcp modem relay voip sprt v14 transmit hold-time 25
Router(config)# mgcp modem relay voip sprt v14 transmit maximum hold-count 10
```

Related Commands

Command	Description
debug voip ccapi inout	Traces the execution path through the call control API.
debug vtsp all	Displays all VTSP debugging except statistics, tone, and event.
mgcp package-capability mdste-package	Enables MGCP gateway support for processing events and signals for modem connections over a secure communication path between IP-STE and STE.
mgcp modem relay voip mode sse	Enables MGCP gateway SSE based modem relay mode support for VoIP calls.

mgcp package-capability

To specify the MGCP package capability type for a media gateway, use the **mgcp package-capability**command in global configuration mode. To remove a specific MGCP package capability from the list of capabilities, use the **no** form of this command.

mgcp package-capability *package*
no mgcp package-capability *package*

Syntax Description

package	One of the following package capabilities (available choices vary according to platform and release version; check the CLI help for a list): • **as -package**--Announcement server package. • **atm -package**--ATM package. MGCP for VoATM using ATM adaptation layer 2 (AAL2) permanent virtual circuit (PVC) and a subset of ATM extensions specified by Cisco is supported. Switched virtual circuit (SVC)-based VoAAL2 is not supported. • **dt -package**--Dual Tone(DT) package. Events and signals for immediate-start and basic dual tone multifrequency (DTMF) and dial-pulse trunks. • **dtmf -package**--DTMF package. Events and signals for DTMF relay. • **fxr -package**--Fax Transmission (FXR) package for fax transmissions. • **fm -package**--Media Format (FM) Parameter Package. This package provides support for the media format parameter Local Connection Option (LCO) and is used for easy DTMF over MGCP-to-SIP configuration. • **gm -package**--Generic media package. Events and signals for several types of endpoints, such as trunking gateways, access gateways, or residential gateways. • **hs -package**--Handset package. An extension of the line package, to be used when the gateway can emulate a handset. • **it -package**--PacketCable Trunking Gateway Control Protocol (TGCP) ISDN User Part (ISUP) trunk package. • **lcs -package**--MGCP Line Control Signaling (LCS) package. • **line -package**--Line package. Events and signals for residential lines. This is the default for residential gateways. • **md -package**--MD package. Provides support for Feature Group D (FGD) Exchange Access North American (EANA) protocol signaling. • **mdste -package--**Modem relay Secure Telephone Equipment (STE) package. Events and signals for modem connections enabling a secure communication path between IP-STE and STE. • **mf -package**--Multifrequency (MF) tone package. Events and signals for MF relay. • **mo -package**--Multifrequency Operations (MO) package. Events and signals for Operator Service Signaling protocol for FGD.

	• **ms -package**--MS package. Events and signals for MF single-stage dialing trunks, including wink-start and immediate-start PBX Direct Inward Dialing (DID) and Direct Outward Dialing (DOD), basic R1, and FGD Terminating Protocol. • **nas -package**--Network Access Server (NAS) Package. Accepts NAS requests from the call agent. **Note** For Cisco IOS Release 12.4(4)T and later releases, the **nas-package** is not enabled by default. • **script -package**--Script package. Events and signals for script loading. • **srtp -package**--Secure RTP (SRTP) package. Enables the MGCP gateway to process SRTP packages. The default is disabled. • **tone-package --Tone package. Disabled by default. Enables the MGCP gateway to play secure call tone during midcall.** • **trunk -package**--Trunk package. Events and signals for trunk lines. This is the default for trunking gateways.

Command Default

The **line-package** is configured by default for residential gateways and the **trunk package** is configured by default for trunk gateways.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR2	This command was introduced on the Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(3)T	This command was implemented on the following platforms: Cisco uBR924, Cisco 2600 series, and Cisco 3660. The **line-package**, **rtp-package**, and **script-package** keywords were added and a distinction was made between residential and trunking gateways.
12.1(5)XM	This command was implemented on the Cisco 3600 series and Cisco MC3810. The **atm-package**, **dt-package, hs-package**, **mo-package, and ms-package** keywords were added.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(2)XB	This command was modified. The **nat-package and res-package** keywords were added.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.3(1)	This command was modified. The **fxr-package** keyword was added.
12.3(8)T	This command was modified. The **lcs-package** keyword was added.

Release	Modification
12.3(8)XY	This command was modified. The **pre-package** keyword was added.
12.3(11)T	This command was modified. The **srtp-package** keyword was added.
12.4(2)T	This command was modified. The **mdste-package** keyword was added.
12.4(4)T	This command was modified. The **md-package** keyword was added. The **nas-package** keyword was not enabled by default.
15.1(4)M	This command was modified. The **tone-package** keyword was added.

Usage Guidelines

Events specified in the MGCP messages from the call agent must belong to one of the supported packages. Otherwise, connection requests are refused by the gateway.

By default, certain packages are configured as supported on each platform type. Using the **mgcp-package capability** command, you can configure additional package capability only for packages that are supported by your call agent. You can also disable support for a package with the **no** form of this command. Enter each package you want to add as a separate command.

Note Beginning in Cisco IOS Release12.4(4)T the **nas-package** keyword is not enabled by default.

The **md-package** keyword is enabled automatically when a T1 interface is configured to use FGD EANA signaling with the **ds0-group** command.

Use the **show mgcp** command to display the packages that are supported on the gateway.

Use this command before specifying a default package with the **mgcp default-package** command. Specify at least one default package.

Packages that are available to be configured with this command vary by platform and type of gateway. Use the CLI help to ascertain the packages available on your gateway. This example shows the CLI help output for a Cisco 3660:

```
Router# mgcp package-capability ?
as-package     Select the Announcement Server Package
atm-package    Select the ATM Package
dtmf-package   Select the DTMF Package
fm-package      Select the FM Package
gm-package     Select the Generic Media Package
hs-package     Select the Handset Package
line-package   Select the Line Package
mf-package     Select the MF Package
res-package    Select the RES Package
rtp-package    Select the RTP Package
trunk-package  Select the Trunk Package
tone-package     Select the Tone Package
```

Note The Channel Associated Signaling (CAS) packages configured using the **dt-package**, **md-package**, **mo-package**, and **ms-package** keywords are available only as default packages using the **mgcp default-package** command. They do not appear as keywords in the **mgcp package-capability** command because all the other packages are configured on a per-gateway basis, whereas the CAS packages are defined on a per-trunk basis. The per-trunk specification is made when the trunk is configured using the **ds0-group** command.

When the **lcs-package** keyword is used on the Cisco Integrated Access Device (IAD), the named telephony events (NTEs) associated with the line control signaling (LCS) package are enabled automatically. NTEs are used by a media gateway to transport telephony tones and trunk events across a packet network. See RFC 2833.

Note Using NTE in the LCS package requires a successful MGCP/Session Definition Protocol (SDP) negotiation during call setup. The call agent must use the Line Connection Option's FMTP parameter keyword, **telephone-event**, to indicate which LCS NTEs will be used. If the IAD has been configured to use the LCS package, the IAD will answer with an SDP containing the requested LCS NTE events.

Examples

The following example enables the modem relay STE package, trunk package, DTMF package, script package, and tone package on the gateway, and then names the trunk package as the default package for the gateway:

```
Router(config)# mgcp package-capability mdste-package
Router(config)# mgcp package-capability trunk-package
Router(config)# mgcp package-capability dtmf-package
Router(config)# mgcp package-capability script-package
Router(config)# mgcp package-capability tone-package
Router(config)# mgcp default-package trunk-package
```

Related Commands

Command	Description
ds0-group	Specifies the DS0 time slots that make up a logical voice port
mgcp	Starts the MGCP daemon.
mgcp default-package	Configures the default package capability type for the media gateway.
show mgcp	Displays the supported MGCP packages.

mgcp persistent through mmoip aaa send-id secondary

mgcp persistent

To configure the sending of persistent events from the Media Gateway Control Protocol (MGCP) gateway to the call agent, use the **mgcp persistent**command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp persistent {**hookflash** | **offhook** | **onhook**}
no mgcp persistent {**hookflash** | **offhook** | **onhook**}

Syntax Description

hookflash	Sends persistent hookflash events to the call agent.
offhook	Sends persistent off-hook events to the call agent.
onhook	Sends persistent on-hook events to the call agent.

Command Default

The **hookflash** keyword is disabled for persistence. The **offhook** keyword is enabled for persistence. The **onhook** keyword is disabled for persistence.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Persistent events are those events that, once they are detected, are defined as reportable to the call agent whether or not the call agent has explicitly requested to be notified of their occurrence; that is, even if they are not included in the list of RequestedEvents that the gateway is asked to detect and report. Such events can include fax tones, continuity tones, and on-hook transition. Each event has an associated action for the gateway to take.

Use this command for each type of persistent event that should override the default behavior.

Examples

The following example configures the gateway to send persistent on-hook events to the call agent:

```
Router(config)# mgcp persistent onhook
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.

mgcp piggyback message

To enable piggyback messages, use the **mgcp piggyback message**command in global configuration mode. To disable piggyback messages, use the **no** form of this command.

mgcp piggyback message
no mgcp piggyback message

Syntax Description

This command has no arguments or keywords.

Command Default

Piggyback messages are enabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

If the network gateway cannot handle piggyback messages, us e the no form of this command to disable the piggyback messages and to enable Media Gateway Control Protocol (MGCP) 1.0, Network-based Call Signaling (NCS), and Trunking Gateway Control Protocol (TGCP). Piggyback messaging is not available to Simple Gateway Control Protocol (SGCP) and MGCP 0.1.

The term piggyback message refers to a situation in which a gateway or a call agent sends more than one MGCP message in the same User Datagram Protocol (UDP) packets. The recipient processes the messages individually, in the order received. However, if a message must be retransmitted, the entire datagram is resent. The recipient must be capable of sorting out the messages and keeping track of which messages have been handled or acknowledged.

Piggybacking is used during retransmission of a message to send previously unacknowledged messages to the call agent. This maintains the order of events the call agent receives and makes sure that RestartInProgress (RSIP) messages are always received first by a call agent.

Examples

The following example disables piggyback messages:

```
Router(config)# no
mgcp piggyback message
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.

mgcp playout

To tune the jitter-buffer packet size attempted for MGCP-controlled connections, use the **mgcp playout** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp playout {**adaptive** *init-milliseconds min-milliseconds max-milliseconds* | **fax** *milliseconds* | **fixed** *milliseconds* [**no-timestamps**]}
no mgcp playout {**adaptive** | **fax** | **fixed**}

Syntax Description

adaptive *init -milliseconds min-milliseconds max-milliseconds*	Sets the range, in milliseconds (ms), for the jitter-buffer packet size. Range for each value is 4 to 250. Note that *init-milliseconds* must be between *min-milliseconds* and *max-milliseconds*. Default: 60 4 200.
fax *milliseconds*	Sets the value for the fax playout buffer size. Range: 1 to 700. Default: 300. **Note** The range and default value might vary with different platforms. See the platform digital signal processor (DSP) specifications before setting this value.
fixed *milliseconds*	Sets the fixed size, in milliseconds, for the jitter-buffer packet size. Range: 4 to 1000. There is no default value.
no-timestamps	(Optional) Fixes the jitter buffer at a constant delay without time stamps.

Command Default

The MGCP jitter playout-delay buffer is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.2(11)T	This command was implemented on the Cisco AS5850.
12.2(13)T	This command was modified. The **fax** keyword was added.
15.1(1.8)T	This command was modified. The **no-timestamps** keyword was added and the fixed range value was increased from 250 to 1000.

Examples

The following example configures a jitter buffer to an initial playout of 100 ms, minimum buffer size of 50 ms, and maximum buffer size of 150 ms:

```
Router(config)# mgcp playout adaptive 100 50 150
```

The following example configures a fax playout buffer size of 200 ms.

```
Router(config)# mgcp playout fax 200
```

The following example configures a jitter buffer to a fixed playout of 120 ms:

```
Router(config)# mgcp playout fixed 120
```

The following example configures a jitter buffer to a fixed playout of 65 ms delay without time stamps:

```
Router(config)# mgcp playout fixed 65 no-timestamps
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
playout-delay	Tunes the playout buffer on DSPs to accommodate packet jitter caused by switches in the WAN.
playout-delay mode	Selects fixed or adaptive mode for playout delay from the jitter buffer on DSPs.

mgcp profile

To create and configure a Media Gateway Control Protocol (MGCP) profile to be associated with one or more MGCP endpoints or to configure the default MGCP profile, use the **mgcp profile** command in global configuration mode. To delete the profile, use the **no**form of this command.

mgcp profile {*profile-name* | **default**}
no mgcp profile {*profile-name* | **default**}

Syntax Description

profile-name	Identifying name for the user-defined profile to be configured. The name can be a maximum of 32 characters.
default	The default profile is to be configured.

Command Default

If this command is not used, there are no MGCP profiles created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
12.4(24)T3	The maximum number of MGCP profiles that can be configured was increased from 13 (12 plus 1 default) to 29 (28 plus 1 default).

Usage Guidelines

An MGCP profile is a subset of endpoints on a media gateway. More than one MGCP profile can be configured on a gateway at the same time. Prior to Cisco IOS Release 12.2(24)T3, the maximum number of MGCP profiles was 13 (12 plus 1 default). Beginning in Cisco IOS Release 12.2(24)T3, the maximum number of MGCP profiles is 29 (28 plus 1 default). The **voice-port** command in MGCP profile configuration mode associates endpoints with the profile.

There are two types of MGCP parameters: global and profile-related. The parameters that are configured in MGCP profile configuration mode are the profile-related parameters. However, endpoints do not need to belong to an MGCP profile. When endpoints are not associated with any MGCP profile, values for the profile-related MGCP parameters are provided by a *default profile* . Although all of the parameters for the default profile have default values, they can also be configured in the same way that an MGCP profile is configured by simply using the **default** keyword instead of a profile name. The main difference between a default profile and a user-defined profile is that there is no voice-port or call-agent association in the default profile, but they are required in user-defined profiles. When configuring the default profile, do not use the **call-agent** command or the **voice-port** command.

This command initiates MGCP profile configuration mode, in which you create an MGCP profile for an endpoint or a set of endpoints on a media gateway, and you set parameters for that profile or for the default profile.

Examples

The following example shows the definition of the MGCP profile named newyork:

```
Router(config)# mgcp profile newyork

Router(config-mgcp-profile)# call-agent 10.14.2.200 4000 service-type mgcp version 1.0
Router(config-mgcp-profile)# voice-port 0:1
Router(config-mgcp-profile)# package persistent mt-package
Router(config-mgcp-profile)# timeout tsmax 100
Router(config-mgcp-profile)# timeout tdinit 30
Router(config-mgcp-profile)# timeout tcrit 600
Router(config-mgcp-profile)# timeout tpar 600
Router(config-mgcp-profile)# timeout thist 60
Router(config-mgcp-profile)# timeout tone mwi 600
Router(config-mgcp-profile)# timeout tone ringback 600
Router(config-mgcp-profile)# timeout tone ringback connection 600
Router(config-mgcp-profile)# timeout tone network congestion 600
Router(config-mgcp-profile)# timeout tone busy 600
Router(config-mgcp-profile)# timeout tone dial 600
Router(config-mgcp-profile)# timeout tone dial stutter 600
Router(config-mgcp-profile)# timeout tone ringing 600
Router(config-mgcp-profile)# timeout tone ringing distinctive 600
Router(config-mgcp-profile)# timeout tone reorder 600
Router(config-mgcp-profile)# timeout tone cot1 600
Router(config-mgcp-profile)# timeout tone cot2 600
Router(config-mgcp-profile)# max1 retries 10
Router(config-mgcp-profile)# no max2 lookup
Router(config-mgcp-profile)# max2 retries 10
Router(config-mgcp-profile)# exit
```

Related Commands

Command	Description
call-agent	Defines the call agent for an MGCP profile.
mgcp	Starts and allocates resources for the MGCP daemon.
voice-port	Enters voice-port configuration mode.

mgcp quality-threshold

To set the jitter buffer size threshold, latency threshold, and packet-loss threshold parameters, use the **mgcp quality-threshold** command in global configuration mode. To reset to the defaults, use the **no** form of this command.

mgcp quality-threshold {**hwm-cell-loss** *value* | **hwm-jitter-buffer** *value* | **hwm-latency** *value* | **hwm-packet-loss** *value* | **lwm-cell-loss** *value* | **lwm-jitter-buffer** *value* | **lwm-latency** *value* | **lwm-packet-loss** *value*}
no mgcp quality-threshold {**hwm-cell-loss** *value* | **hwm-jitter-buffer** *value* | **hwm-latency** *value* | **hwm-packet-loss** *value* | **lwm-cell-loss** *value* | **lwm-jitter-buffer** *value* | **lwm-latency** *value* | **lwm-packet-loss** *value*}

Syntax Description

hwm -cell-loss *value*	High-water-mark cell loss count, when the ATM package is enabled. Range is from 5000 to 25000. Default is 10000.
hwm -jitter-buffer*value*	High-water-mark jitter buffer size, in milliseconds. Range is from 100 to 200. Default is 150.
hwm -latency*value*	High-water-mark latency value, in milliseconds. Range is from 250 to 400. Default is 300.
hwm -packet-loss *value*	High-water-mark packet loss value, in milliseconds. Range is from 5000 to 25,000. Default is 10000.
lwm -cell-loss *value*	Low-water-mark cell loss count, when the ATM package is enabled. Range is from 1 to 3000. Default is 1000.
lwm -jitter-buffer *value*	Low-water-mark jitter buffer size, in milliseconds. Range is from 4 to 60. Default is 30.
lwm -latency *value*	Low-water-mark latency value, in milliseconds. Range is from 125 to 200. Default is 150.
lwm -packet-loss *value*	Low-water-mark packet-loss value, in milliseconds. Range is from 1 to 3000. Default is 1000.

Command Default

High-water-mark cell loss count: 10000 cells High-water-mark jitter buffer size: 150 ms High-water-mark latency value: 300 ms High-water-mark packet loss value: 10000 ms Low-water-mark cell loss count:1000 cells Low-water-mark jitter buffer size: 30 ms Low-water-mark latency value: 150 ms Low-water-mark packet-loss value:1000 ms

Command Modes

Global configuration

Command History

Release	Modification
11.3(3)T	The default was changed to 100 milliseconds.
12.1(1)T	This command was implemented on the Cisco AS5300.

Release	Modification
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.1(5)XM	This command was implemented on the Cisco MC3810. The **hwm-cell-loss** and **lwm-cell-loss**keywords were added.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

The following impact the quality of voice calls:

- **Cell loss** (the number of ATM cells lost during transmission)
- **Jitter buffer** (storage area containing active call voice packets that have been received from the network and are waiting to be decoded and played)
- **Latency** (network delay in sending and receiving packets)
- **Packet loss** (number of packets lost per 100,000 packets for a given call)

For good voice quality, the system should perform below the low water mark values. As the values go higher, voice quality degrades. The system generates a report when the values go above the high water marks levels. Set the high water marksand low water marks values sufficiently apart so that you receive reports on poor performance, but not so close together that you receive too much feedback.

Enter each parameter as a separate command.

Examples

The following example sets various keywords to new values:

```
Router(config)# mgcp quality-threshold hwm-jitter-buffer 100
Router(config)# mgcp quality-threshold hwm-latency 250
Router(config)# mgcp quality-threshold hwm-packet-loss 5000
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp package -capability	Activates various packages on the gateway.
mgcp playout	Tunes the jitter buffer packet size.

mgcp quarantine mode

To configure the mode for Media Gateway Control Protocol (MGCP) quarantined events, use the **mgcp quarantine mode**command inglobal configuration mode. To reset to the default, use the **no**form of this command.

mgcp quarantine mode [{**discard** | **process**}] [{**loop** | **step**}]
no mgcp quarantine mode

Syntax Description

discard	Enables discarding of quarantined events instead of processing. Observed events are not reported to the call agent, even if the call agent is ready to receive them.
loop	Enables loop mode for quarantined events instead of stepping. After receiving a request from the call agent, the gateway reports the observed events to the call agent in multiples without waiting for subsequent requests.
process	Enables processing of quarantined events instead of discarding. Observed events are reported to the call agent when the call agent is ready to receive them.
step	Enables step mode for quarantined events instead of looping. After receiving a request from the call agent, the gateway reports observed events individually to the call agent, one for each request.

Command Default

If no event is specified the default is **step**.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200.
12.2(2)XA	This command was modified to support MGCP.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Quarantine events are defined as events that have been detected by the gateway before the arrival of the MGCP NotificationRequest command but that have not yet been notified to the call agent. They are held in the quarantine buffer until receipt of the MGCP NotificationRequest command, when the gateway is expected to generate either one notification (step by step) or multiple notifications (loop) in response to this request (the default is exactly one), based on the configuration of **the mgcp quarantine mode** command.

This command supports backward compatibility with SGCP implementations running under the MGCP application. SGCP does not have a way to allow the call agent to control the quarantine mode. MGCP has this functionality.

When the gateway is in the notification state, the interdigit timer (Tcrit) is not started.

When the gateway receives an unsuccessful NotificationRequest, the current RequestEventList and SignalEventList are emptied. The ObservedEventList and quarantine buffer are also emptied.

Changes to the quarantine mode only take effect when the gateway is rebooted or the MGCP application is restarted.

Examples

The following example starts the MGCP application:

```
Router(config)# mgcp
```

The following example stops the MGCP application:

```
Router(config)# no mgcp
```

The following example turns on processing of quarantined events and sends observed events to the call agent:

```
Router(config)# mgcp quarantine mode process
```

The following example turns off processing of quarantined events:

```
Router(config)# no mgcp quarantine mode discard
```

The following example sends observed events to the call agent in loop mode:

```
Router(config)# mgcp quarantine mode process loop
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp quarantine persistent -event disable	Disables handling of persistent call events in the quarantine buffer.

mgcp quarantine persistent-event disable

To disable handling of persistent call events in the Media Gateway Control Protocol (MGCP) quarantine buffer, use the **mgcp quarantine persistent-events disable** command in global configuration mode. To reset to the default state, use the **no** form of this command.

mgcp quarantine persistent-event disable
no mgcp quarantine persistent-event disable

Syntax Description

This command has no arguments or keywords.

Command Default

Persistent events are held in the events buffer.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200.
12.2(2)XA	This command was modified to support MGCP.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command enables the reporting of persistent events immediately to the call agent rather than holding the events in quarantine. Persistent events are events defined as reportable whether or not the call agent explicitly has requested to be notified of their occurrence. Quarantining means that the gateway observes events but does not report them to the call agent until the call agent indicates readiness to receive notifications. By default, all events, including persistent events, are quarantined when they are detected, even when the gateway is in a notification state. When the **mgcp quarantine persistent-event disable** command is configured, however, persistent events are reported to the call agent immediately by an MGCP Notify command.

Examples

The following example disables quarantine buffer handling of persistent events:

```
Router(config)# mgcp quarantine persistent-event disable
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp quarantine mode	Configures MGCP event quarantine buffer handling mode.

mgcp request retries

This command was added in Cisco IOS Release 12.1(1)T. Beginning in Cisco IOS Release 12.2(2)XA and Cisco IOS Release 12.2(4)T, this command is supported no longer. It has been replaced by the MGCP profile **max1 retries** and **max2 retries** commands.

mgcp request timeout

To specify how long a Media Gateway Control Protocol (MGCP) gateway waits for a call-agent response to a request before retransmitting the request, use the **mgcp request timeout** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp request timeout {*timeout-value* | **max** *maxtimeout-value*}
no mgcp request timeout [**max**]

Syntax Description

timeout -value	Time, in milliseconds, to wait for a response to a request. Range is 1 to 10000. Default is 500.
max *maxtimeout -value*	Maximum timeout, in milliseconds. Default is 4000.

Command Default

timeout-value: 500 ms maxtimeout-value: 4000 ms

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.1(5)XM	This command was implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(2)XA	The **max** keyword was added to this command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T and implemented on the Cisco uBR925.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

The request timeout value sets the initial time period that an MGCP gateway waits for a response from the call agent before retransmitting the message. The interval doubles with each retransmission. The request timeout maximum value sets an upper limit on the timeout interval.

Examples

The following example sets a router to wait 40 ms for a reply to the first request before retransmitting and limits subsequent interval maximums to 10,000 ms (10 seconds):

```
Router(config)# mgcp request timeout 40
Router(config)# mgcp request timeout max 10000
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp request retries	Specifies the number of times to retry sending the mgcp command.

mgcp restart-delay

To select the delay value sent in the Restart in Progress (RSIP) graceful teardown, use the **mgcp restart-delay** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp restart-delay *value*
no mgcp restart-delay

Syntax Description

value	Restart delay value, in seconds. Range is 0 to 600. The default is 0.

Command Default

0 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.1(5)XM	This command was implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Use this command to send an RSIP message indicating when the connection in the gateway is to be torn down.

Examples

The following example sets the restart delay to 30 seconds:

```
Router(config)# mgcp restart-delay 30
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp max -waiting-delay	Specifies the MGCP maximum waiting delay after a restart.

mgcp rtp payload-type

To specify use of the correct Real-time Transport Protocol (RTP) payload type for backward compatibility in Media Gateway Control Protocol (MGCP) networks, use the **mgcp rtp payload-type** command in global configuration mode. To restore default values for payload types, use the **no** form of this command.

Fax and Modem Codecs
mgcp rtp payload-type {**cisco-codec-fax-ack** | **cisco-codec-fax-ind** | **cisco-pcm-switch-over-alaw127** | **cisco-pcm-switch-over-ulaw 126**}
no mgcp rtp payload-type {**cisco-codec-fax-ack** | **cisco-codec-fax-ind** | **cisco-pcm-switch-over-alaw127** | **cisco-pcm-switch-over-ulaw 126**}

Named Signaling and Telephony Events
mgcp rtp payload-type {**nse** | **nte**} *number*
no mgcp rtp payload-type {**nse** | **nte**}

Voice Codecs
mgcp rtp payload-type {**clear-channel** | **g726r16** | **g726r24**} **static**
no mgcp rtp payload-type {**clear-channel** | **g726r16** | **g726r24**}

Syntax Description

cisco-codec-fax-ack	Payload type for Cisco codec fax acknowledgment.
cisco-codec-fax-ind	Payload type for Cisco codec fax indication.
cisco -pcm-switch-over-alaw 127	Payload type for upspeed to the G.711 a-law codec.
cisco -pcm-switch-over-ulaw 126	Payload type for upspeed to the G.711 mu-law codec.
nse	Payload type for named signaling events (NSE).
nte	Payload type for named telephony events (NTE).
number	Indicates the payload-type value. The valid range for NSE and NTE payload is from 96 to127. Default for NSE is 100. Default for NTE is 99.
clear -channel	Payload type for clear channel codec.
g726r16	Payload type for the G.726 codec at a bit rate of 16 kbps.
g726r24	Payload type for the G.726 codec at a bit rate of 24 kbps.
static	Static payload type.

Command Default

Fax and modem codecs: static RTP payload type Voice codecs: dynamic RTP payload range from 96 to 127 (default for NSE is 100; default for NTE is 99)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5400HPX, and Cisco AS5850.
12.4(6)T	The **nse** and **nte**named signalling and telephony events keywords were added.
12.4(15)T5	The **cisco-codec-fax-ack**and **cisco-codec-fax-ind**keywords were added.
12.4(18a)	The **cisco-codec-fax-ack**and **cisco-codec-fax-ind**keywords were added.
12.4(13f)	The **cisco-codec-fax-ack**and **cisco-codec-fax-ind**keywords were added.

Usage Guidelines

Cisco IOS Release 12.2(11)T introduced an RTP payload type negotiation for MGCP VoIP calls different from previous Cisco IOS images. To ensure interoperability between gateways using different Cisco IOS images, follow these guidelines:

- For fax and modem codecs--If either the originating or terminating MGCP gateway is running Cisco IOS Release 12.2(11)T or a later release and the other gateway is running a release earlier than Cisco IOS Release 12.2(11)T, use the **mgcp rtp payload-type** command on the gateway with the later release.
- For voice codecs--If you are using a Clear Channel, G.726R16, or G.726R24 codec, and either the originating or terminating MGCP gateway is running Cisco IOS Release 12.2(11)T or a later release and the other gateway is running a release earlier than Cisco IOS Release 12.2(11)T, use the **mgcp rtp payload-type**command on the gateway with the later release.

If both the originating and terminating gateways are using Cisco IOS Release 12.2(11)T or a later release, this command is not required.

The **cisco-codec-fax-ack**and **cisco-codec-fax-ind**keywords are used to change the default dynamic payload type for the Cisco fax relay feature to a different dynamic payload type.

Note NSE and NTE cannot be configured to use the same value. An error message will be generated by the command parser if the same value is entered.

Examples

The following example specifies use of dynamic RTP payload type for fax and modem calls for mu-law pulse code modulation (PCM) calls in an MGCP network in which the other gateway is running a release of Cisco IOS software that is earlier than Release 12.2(11)T:

```
Router# mgcp rtp payload-type cisco-pcm-switch-over-ulaw 126
```

The following example specifies use of a static RTP payload type for a G.726R16 codec in an MGCP network in which the other gateway is running a release of Cisco IOS software that is earlier than Release 12.2(11)T:

```
Router# mgcp rtp payload-type g726r16 static
```

The following examples configure the gateway to use RTP payload 104 for NSE events and payload 108 for NTE events. These payload types are used when the gateway is advertising capabilities via the Session Definition Protocol (SDP). If the gateway is recieving the SDP, the payload types configured in the remote SDP will be used instead.

```
Router# mgcp rtp payload-type nse 104
Router# mgcp rtp payload-type nte 108
```

Related Commands

Command	Description
mgcp codec	Selects the default codec type and its optional packetization period value.

mgcp rtp unreachable timeout

To enable detection of an unreachable remote VoIP endpoint, use the **mgcp rtp unreachable timeout**command in global configuration mode. To disable detection, use the **no**form of this command.

mgcp rtp unreachable timeout *timer-value*
no mgcp rtp unreachable timeout

Syntax Description

timer -value	Time, in milliseconds, that the system waits for voice packets from the unreachable endpoint. Range is 500 to 10000.

Command Default

Detection is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Note This command replaces the previously hidden **mgcp rtp icmp timeout** command .

Thiscommand is useful for preventing calls from remaining open when the remote endpoint is no longer available.

For example, suppose an IP phone makes a call through a gateway to another IP phone. During the call, the call agent goes down and the remote IP phone hangs up. Normally, the call agent would tell the gateway to tear down the call. In this case, the gateway continues to treat the call as active and sends more voice packets to the remote IP phone. The remote IP phone returns Internet Control Message Protocol (ICMP) port unreachable messages to the gateway. If the **mgcp rtp unreachable timeout** command is enabled, the gateway tears down the call. If the command is disabled, the call is left open.

The *timer-value* argument tells the gateway how long to wait before tearing down the call. After receiving the ICMP the unreachable message, the gateway starts a timer. If the gateway does not receive any voice packets by the end of the timer-value period, the gateway tears down the call. If some voice packets arrive before the end of the timer-value period, the gateway resets the timer and leaves the call in active state.

Examples

The following example sets the Real-Time Transport Protocol (RTP) unreachable timer to 1500 ms:

```
Router(config)# mgcp rtp unreachable timeout 1500
```

Related Commands

Command	Description
mgcp	Initiates the MGCP daemon.
mgcp timer	Configures RTP stream host detection.

mgcp rtrcac

To enable Media Control Gateway Protocol (MGCP) Service Assurance (SA) Agent Call Admission Control (CAC) on an MGCP gateway supporting VoIP, use the **mgcp rtrcac** command in global configuration mode. To disable SA Agent checking on the gateway, use the **no** form of this command.

mgcp rtrcac
no mgcp rtrcac

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

Use thiscommandto initiate or disable MGCP SA Agent CAC on the MGCP gateway.

Examples

The following example enables MGCP SA Agent CAC:

```
Router(config)# mgcp rtrcac
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
mgcp	Starts and allocates resources for the MGCP daemon.
rtr responder	Enables the SA Agent Responder feature.

mgcp sched-time

To configure the scheduled timer value for Media Gateway Control Protocol (MGCP), use the **mgcp sched-time** command in global configuration mode. To disable the configuration, use the **no** form of this command.

mgcp sched-time *milliseconds*
no mgcp sched-time

Syntax Description

milliseconds	Schedule timer value, in milliseconds (ms). The range is from 12 to 40.

Command Default

The scheduled timer value for MGCP is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **mgcp sched-time** command is used to configure the MGCP process a specified time to run before it yields to a process of a lower or the same priority. The schedule timer value must be from 12 to 40 ms, the minimum and maximum time, respectively, a process can run. This ensures that the MGCP process is not suspending too often.

Examples

The following example shows how to configure the scheduled timer value for MGCP:

```
Router# configure terminal
Router(config)# mgcp sched-time 15
```

Related Commands

Command	Description
show mgcp	Displays values for MGCP parameters.

mgcp sdp

To specify parameters for Session Definition Protocol (SDP) operation in Media Gateway Control Protocol (MGCP), use the **mgcp sdp**command inglobal configuration mode. To disable the parameters, use the **no** form of this command.

mgcp sdp {**notation undotted** | **simple** | **xpc-codec**}
no mgcp sdp {**notation undotted** | **simple** | **xpc-codec**}

Syntax Description

notation undotted	Enables undotted SDP notation for the codec string in SDP.
simple	Enables simple mode of SDP operation for MGCP.
xpc -codec	Enables initial generation of the X-pc-codec field, which is used during codec negotiation in SDP for Network-based Call Signaling (NCS) and Trunking Gateway Control Protocol (TGCP).

Command Default

notation undotted: disabled**simple:**disabled**xpc-codec:**disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XA	The **notation undotted** and **xpc-codec** keywords were added.
12.2(2)T	This command was implemented on the Cisco 7200.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command allows you to configure SDP fields to meet the requirements of your call agent.

The **notation undotted**keyword is for the G.726-16 and G.729 codecs. The codec strings G.726-16 and G.729 are dotted notation. The codec notation format is selected dynamically in the following order of preference:

1. The notation used in SDP for MGCP packets from the call agent.
2. The notation used in the a: parameter of the Local connection option for MGCP packets from the call agent.
3. The notation set by the **mgcp sdp notation undotted** command.

The **simple** keyword**, w**hen enabled, causes the gateway not to generate the following SDP fields: o (origin and session identifier), s (session name), and t (session start time and stop time). Certain call agents require this modified SDP to send data through the network.

The **xpc-codec** keyword, in TGCP and NCS, defines a new field (X-pc-codec) in the SDP for codec negotiation. To be backward compatible with nonpacket-cable SDPs, the initial generation of the X-pc-codec field is suppressed by default. However, if a received SDP contains this field, the X-pc-codec field is read and generated in response to continue with the codec negotiation.

Examples

The following example configures simple mode for SDP:

```
Router(config)# mgcp sdp simple
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp sgcp disconnect notify

To enable enhanced endpoint synchronization after a disconnected procedure in a Simple Gateway Control Protocol (SGCP) version 1.5 network, use the **mgcp sgcp disconnect notify** command in global configuration mode. To disable this feature, use the **no** form of this command.

mgcp sgcp disconnect notify
no mgcp sgcp disconnect notify

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

This command is used with SGCP version 1.5 to provide enhanced messaging capability for an endpoint that undergoes the disconnected procedure. It does not apply to gateways that run Media Control Gateway Protocol (MGCP) or other versions of SGCP.

An SGCP endpoint may lose communication with its call agent because the call agent is temporarily off line or because of faults in the network. When a gateway recognizes that an endpoint has lost its communication with the call agent (has become disconnected), it attempts to restore contact. If contact is not established before the disconnected timer expires, the disconnected procedure is initiated.

The disconnected procedure consists of the endpoint sending a Restart In Progress (RSIP) message to the call agent, stating that the endpoint was disconnected and is now trying to reestablish connectivity. If the **mgcp sgcp disconnect notify** command has been configured on the gateway, a special disconnected RSIP message is sent. When contact is reestablished, the call agent may decide to audit the endpoint using an Audit Endpoint (AUEP) command with additional I, ES, and RM parameters, which are defined as follows:

- I--List of connection identifiers for current connections on the endpoint
- ES--Event state of the endpoint (off-hook or on-hook)
- RM--Restart method reason for the last RSIP (graceful, forced, restart, or disconnected)

Endpoint synchronization with the call agent is achieved by the exchange of the disconnected RSIP message and the endpoint audit.

Examples

The following example enables disconnected RSIP messaging between SGCP endpoints and a call agent:

```
Router(config)# mgcp sgcp disconnect notify
```

Related Commands

Command	Description
mgcp sgcp restart notify	Enables the MGCP application to process SGCP-type RSIP messages.
show mgcp	Displays information for MGCP and SGCP parameters.

mgcp sgcp restart notify

To trigger the Media Gateway Control Protocol (MGCP) application to process Simple Gateway Control Protocol (SGCP)-type restart in progress (RSIP) messages, use the **mgcp sgcp restart notify**command in global configuration mode. To cancel the trigger, use the **no**form of this command.

mgcp sgcp restart notify
no mgcp sgcp restart notify

Syntax Description

This command has no arguments or keywords.

Command Default

SGCP does not send any RSIP messages when the protocol type is configured as SGCP.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 3600 series.
12.1(5)XM	This command was modified for MGCP and implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

This command is used to send RSIP messages from the router to the SGCP call agent. The RSIP messages are used to indicate whether the T1 controller is up or down so that the call agent can synchronize with the router. RSIP messages are also sent when the **mgcp** command is entered, enabling the MGCP daemon.

Examples

The following example specifies that the system sends an RSIP notification to the SGCP call agent when the T1 controller state changes:

```
Router(config)# mgcp sgcp restart notify
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp src-cac

To enable System Resource Check (SRC) Call Admission Control (CAC) on a Media Gateway Control Protocol (MGCP) gateway supporting VoIP, use the **mgcp src-cac** command in global configuration mode. To disable system resource checking on the gateway, use the **no** form of this command.

mgcp src-cac
no mgcp src-cac

Syntax Description

This command has no arguments or keywords.

Command Default

System resource checking is disabled.

Command Modes

Global configuration

Command History

Releases	Modification
12.2(2)XB	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

When this command is entered, all system-resource checks of CPU utilization, memory utilization, and maximum number of calls are performed for every call setup or modification request received from the call agent.

Examples

The following example enables MGCP VoIP SRC CAC:

```
Router(config)# mgcp src-cac
```

Related Commands

Command	Description
call threshold global	Sets threshold values for SRC CAC parameters.
mgcp	Starts and allocates resources for the MGCP daemon.

mgcp timer

To configure how a gateway detects the Real-Time Transport Protocol (RTP) stream host, use the **mgcp timer** command in global configuration mode. To reset to the defaults, use the **no** form of this command.

mgcp timer {**receive-rtcp** *timer* | **net-cont-test** *timer* | **nse-response t38** *timer* | **toh-time** *timer*}
no mgcp timer {**receive-rtcp** | **net-cont-test** | **toh-time**}

Syntax Description

receive -rtcp *timer*	Multiples of the RTCP report transmission interval, in milliseconds. Range is 1 to 100. Default is 5.
net -cont-test *timer*	Continuity-test timeout interval for VoIP and VoATM adaptation layer 2 (VoAAL2) calls, in milliseconds. Range is from 100 to 3000. The default is 200. **Note** This keyword was previously called **rtp-nse**.
nse -response t38 *timer*	Timeout period, in milliseconds, for awaiting T.38 named signaling event (NSE) responses from a peer gateway. Range is from 100 to 3000. The default is 200.
toh-time *timer*	Tone on hold in milliseconds, for specifying the duration of silence between 3 beep groupings. Range is from 1 to 65500. The default is 10.

Command Default

receive-rtcp *timer* : 5 ms**net-cont-test** *timer*: 200 ms **nse-response t38** *timer*: 200 ms **toh-time** *timer*: 10 ms

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced for Simple Gateway Control Protocol (SGCP) on the Cisco AS5300.
12.0(7)XK	This command was implemented on the Cisco MC3810 and Cisco 3600 series (except for the Cisco 3620).
12.1(5)XM	This command was modified to support Media Gateway Control Protocol (MGCP). The **rtp-nse** keyword was changed to the **net-cont-test**keywordwithout change of functionality.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200.
12.2(2)XB	This command was modified. The **nse-response t38** option was added to support MGCP T.38.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5400, and Cisco AS5850.
12.2(15)T	This command was implemented on the Cisco 1751 and Cisco 1760.

Release	Modification
12.3(10)T	This command was modified. The **toh-time** keyword was added to adjust the duration of silence between the 3 beep groupings used for tone on hold.

Usage Guidelines

Use this command to specify the RTP Control Protocol (RTCP) transmission interval for VoIP calls and the continuity-test timeout interval for VoIP and VoATM adaptation layer 2 (VoAAL2) calls.

The **receive-rtcp**keyword is the timer used by a gateway to disconnect a VoIP call when IP connectivity is lost with the remote gateway. After receiving each RTP or RTCP packet from the remote gateway, the receiving gateway starts a timer. The period of the timer is determined by multiplying the value configured using the **mgcp timer receive-rtcp**command with the value configured using **ip rtcp report interval** command. If the timer expires before the next packet is received from the remote gateway, the receiving gateway disconnects the call and notifies the call agent.

The net -cont-test keyword uses the terminating gateway to verify the network connectivity with the originating gateway before ringing the called party. To do this, the terminating gateway sends a command packet to the originating gateway and starts a timed for the *timer*period. If the timer expires before any acknowledgement from the originating gateway is received, the terminating gateway does not ring the called party, but instead disconnects the call and alerts the call agent.

The **nse-response t38**option sets the timer for awaiting T.38 NSE responses. This timer is configured to tell the terminating gateway how long to wait for an NSE from a peer gateway. The NSE from the peer gateway can either acknowledge the switch and its readiness to accept packets or indicate that it cannot accept T.38 packets.

The **toh-time** *timer* option sets the duration of silence between the 3 beep groupings used for tone on hold.

Examples

The following example sets the multiplication factor to 10 (or x*10, where x is the interval that is set with the ip rtcp report interval command):

```
Router(config)# mgcp timer receive-rtcp 10
```

The following example sets the net-cont-test timer to 1500 ms (1.5 seconds):

```
Router(config)#
mgcp timer net-cont-test 1500
```

The following example enables MGCP fax relay and sets the gateway wait time to 300 ms for an NSE from a peer gateway:

```
Router(config)# mgcp timer nse-response t38 300
```

The following example enables tone on hold timer and set the duration of silence between the 3 beep groupings to 200 ms:

```
Router(config)# mgcp timer toh-time 200
```

Related Commands

Command	Description
ip rtcp report interval	Configures the minimum interval for RTCP report transmissions.
mgcp	Starts the MGCP daemon.

Command	Description
mgcp modem passthrough mode	Sets the method for changing speeds for modem and fax transmissions on the gateway.
mgcp tse payload	Sets the TSE payload for fax and modem calls.

mgcp tse payload

Note This command is no longer supported. It has been replaced by the **mgcp rtp payload-type** command.

To enable inband telephony signaling events (TSEs) and specify the payload value to be used during fax and modem pass-through and network continuity tests, use the **mgcp tse payload** command in global configuration mode. To disable these signaling events, use the **no**form of this command.

mgcp tse payload *value*
no mgcp tse payload

Syntax Description

value	TSE payload value. Range is from 98 to 119. The default is 100.

Command Default

100

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced for Simple Gateway Control Protocol (SGCP) on the Cisco MC3810 and on the Cisco 3600 series (except the Cisco 3620).
12.1(5)XM	This command was modified to support Media Gateway Control Protocol (MGCP).
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series router.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3620, and Cisco AS5300.
12.4(3rd)T	This command was replaced by the **mgcp rtp payload-type** command.

Usage Guidelines

Because this command is disabled by default, you must specify a TSE payload value. Both gateways must have the same payload value.

If you configure the **mgcp modem passthrough mode**command using the **nse** keyword, you must configure this command.

Examples

The following example sets NSE mode for VoIP modem pass-through and sets the TSE payload:

```
Router(config)# mgcp modem passthrough voip mode nse
Router(config)# mgcp tse payload 100
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp modem passthrough mode	Sets the method for changing speeds for modem and fax transmissions on the gateway.

mgcp vad

To enable voice activity detection (VAD) silence suppression for Media Gateway Control Protocol (MGCP), use the **mgcp vad** command in global configuration mode. To disable VAD silence suppression, use the **no** form of this command.

mgcp vad
no mgcp vad

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.1(5)XM	This command was implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Use this command to tell the MGCP gateway to turn VAD silence suppression on or off.

If VAD silence suppression is turned on, silence is not sent over the network, only audible speech. Sound quality is slightly degraded but the connection monopolizes much less bandwidth.

Examples

The following example turns VAD silence suppression on:

```
Router(config)# mgcp vad
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp validate call-agent source-ipaddr

To enable the Media Gateway Control Protocol (MGCP) application to validate that packets are received from a configured call agent, use the mgcp validate **call-agent**source-ipaddr command in global configuration mode. To disable the validation feature, use the **no** form of this command.

mgcp validate call-agent source-ipaddr
no mgcp validate call-agent source-ipaddr

Syntax Description

This command has no arguments or keywords.

Command Default

No validation occurs.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

This command verifies that incoming packets are received from MGCP or Cisco CallManager configured call agents only. When the command is enabled, all MGCP messages received from call agents that are not configured in MGCP or Cisco CallManager are dropped. Use the mgcp validate call-agent source-ipaddr command in place of access lists to filter out packets from unconfigured call agents. Use the **mgcp bind control source-interface** *interface*command to restrict the MGCP application from responding to unconfigured call agent requests on nonsecure interfaces. Use the **ccm-manager config server** *server address* command to configure the Cisco CallManager address to be used when verifying incoming packets.

Examples

The following example shows that MGCP call-agent validation is enabled:

```
Router(config)# mgcp validate call-agent source-ipaddr
```

Related Commands

Command	Description
ccm-manager config server	Configures the Cisco CallManager address used in verifying incoming packets.
mgcp bind control source-interface	Restricts the MGCP application from responding to unconfigured call agent requests on nonsecure interfaces.
mgcp call-agent	Configures the IP address for the primary or default Cisco CallManager server and designates the optional destination UDP port number for the specified Cisco CallManager server.
show mgcp srtp	Displays active MGCP SRTP calls.

mgcp validate domain-name

To enable validation of a hostname and domain (or a specific IP address) received as part of the endpoint name in MGCP messages against those configured on the gateway, use the **mgcp validate domain-name** command in global configuration mode. To disable Media Gateway Control Protocol (MGCP) endpoint validation, use the **no** form of this command.

mgcp validate domain-name
no mgcp validate domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

Hostname and domain (or IP address) validation is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(17)	The default state of this command was changed to disabled.
12.3(11)T8; 12.3(14)T5	The default state of this command was changed to disabled.
12.4(1c); 12.4(3b); 12.4(5)	The default state of this command was changed to disabled.
12.4(2)T2; 12.4(4)T1; 12.4(6)T	The default state of this command was changed to disabled.

Usage Guidelines

The **mgcp validate domain-name** command enables validation of a hostname and domain (or specific IP address) received as part of the endpoint name sent from the call agent (CA) or Cisco CallManager against those configured on the gateway. If the hostname or domain (or IP address) is not valid, the system returns a 500 error with appropriate comment.

Use the **mgcp validate domain-name** command before configuring MGCP globally in a VoIP network. (See the Cisco Unified CallManager and Cisco IOS Interoperability Guide for global MGCP configuration information.)

Note Only MGCP messages received from the CA or Cisco CallManager are validated .

You can display the current setting for MGCP domain name validation using the **show running-config** command. To show only MGCP information, limit the display output to the section on MGCP (see the "Examples" section).

Note When MGCP domain name validation is disabled, the output of the **show running-config** command does not include this command--it displays only when domain name validation is enabled. However, if your system is running a software image released before the default for this feature was changed, MGCP domain name validation is turned on by default and will appear in the **show running-config** command output only if validation is disabled.

Once you enable the MGCP validate domain name feature, you should verify that the appropriate endpoint name is included as part of incoming MGCP messages. Performing this verification helps to ensure that incoming messages with invalid hostnames, domain names, and IP addresses are rejected while valid incoming messages are still allowed to reach their target endpoint (host). Enabling this validation feature without verifying this information can cause all incoming messages, even those using valid names or addresses, to be rejected (see the "Examples" section).

Examples

The following examples show how to enable MGCP domain name validation, how to verify that validation is enabled in the running configuration, and how to verify and match the hostname, domain name, or IP address specified in incoming MGCP messages to the gateway configuration.

Use the following command to enable MGCP domain name validation:

```
Router(config)# mgcp validate domain-name
```

Use the following command to verify that MGCP domain name validation is enabled:

```
Router(config)# show running-config | section mgcp
```

or

```
Router(config)# show running-config | include mgcp validate
mgcp validate domain-name
Router(config)#
```

Use the following commands and processes to verify that hostname and domain name are configured so that all and only valid incoming messages are accepted by the gateway.

After enabling domain name validation, enable debug tracing for MGCP packets:

```
Router# debug mgcp packets
Media Gateway Control Protocol packets debugging for all endpoints is on
Router#
```

Generate a call to the gateway from a CA or Cisco CallManager. That call will generate debug messages on the gateway so that you can view the endpoint information included in the incoming MGCP message and the response from the gateway to the CA (or Cisco CallManager):

```
Router#
*Mar 14 02:29:11.512: MGCP Packet received from 192.0.2.135:2427--->
RQNT 3 aaln/S2/SU0/0@Router2821.example.com MGCP 0.1
R: L/hd(N)
X:1
<---
*Mar 14 02:29:11.512: MGCP Packet sent to 192.0.2.135:2427--->
500 3 Endpoint name contains an invalid host or domain
<---
```

Because the hostname in the incoming message (aaln/S2/SU0/0@Router2821.example.com) does not match the hostname of the gateway (Router), the message was rejected (replied to with a NACK). To resolve this, change the hostname of the gateway:

```
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname Router2821
Router2821(config)# end
Router2821#
```

Generate another call to the gateway from the CA or Cisco CallManager. That call will generate more debug messages so that you can view the endpoint information included in the incoming MGCP message and the response from the gateway to the CA (or Cisco CallManager):

```
*Mar 14 03:01:12.480: MGCP Packet received from 192.0.2.135:2427--->
RQNT 3 aaln/S2/SU0/0@Router2821.example.com MGCP 0.1
R: L/hd(N)
X:1
<---
*Mar 14 03:01:12.480: MGCP Packet sent to 192.0.2.135:2427--->
200 3 OK
<---
```

The validation is successful and an ACK (positive response) is sent back to the CA or Cisco CallManager because the hostname now matches. This same process also applies to validation for the domain name. Use the following commands to set the domain name for the gateway and to view current configuration for domain name and hostname:

```
Router2821# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router2821(config)# ip domain-name example.com
Router2821(config)# end
Router2821# show running-config
Building configuration...
.
.
.
hostname Router2821
.
.
.
ip domain name example.com
.
.
.
.
Router2821#
```

Use the following commands and processes to verify that the IP address for the gateway is configured so that all and only valid incoming messages are accepted by the gateway:

```
Router2821# show ip interface brief
Interface                 IP-Address       OK?    Method    Status    Protocol
GigabitEthernet0/0        192.0.2.189    YES    NVRAM     up        up
Router2821#
```

Generate a call to the gateway from the CA or Cisco CallManager. That call will generate debug messages so that you can view the endpoint information included in the incoming MGCP message and the response from the gateway to the CA (or Cisco CallManager). If the MGCP message is directed to a specific IP address instead of a domain or hostname, you will see debug messages similar to the following:

```
*Mar 14 03:16:52.356: MGCP Packet received from 192.0.2.135:2427--->
RQNT 3 aaln/S2/SU0/0@[192.0.2.190] MGCP 0.1
R: L/hd(N)
X:1
<---
*Mar 14 03:16:52.356: MGCP Packet sent to 192.0.2.135:2427--->
500 3 Endpoint name contains an invalid host or domain
<---
```

Because the IP address specified in the incoming message (aaln/S2/SU0/0@192.0.2.190) does not match the IP address of the GigE 0/0 interface (192.0.2.189), the message was rejected (replied to with a NACK). To resolve this, change the IP address specified by the CA or Cisco CallManager for this gateway and generate another call to this gateway. If the IP addresses match, you will see debug messages similar to the following:

```
*Mar 14 03:16:10.360: MGCP Packet received from 192.0.2.135:2427--->
RQNT 3 aaln/S2/SU0/0@[192.0.2.189] MGCP 0.1
R: L/hd(N)
X:1
<---
*Mar 14 03:16:10.364: MGCP Packet sent to 192.0.2.135:2427--->
200 3 OK
<---
```

Because the IP address now specified in the incoming MGCP message matches the IP address of the gateway, the message was accepted and replied to with an ACK (positive response).

Related Commands

Command	Description
mgcp call-agent	Configures the IP address for the primary or default Cisco CallManager server and designates the optional destination UDP port number for the specified Cisco CallManager server.
show ccm-manager	Displays a list of Cisco CallManager servers and their current status and availability.

mgcp voice-quality-stats

To enable voice-quality statistics reporting for the Media Gateway Control Protocol (MGCP), use the **mgcp voice-quality-stats** command in global configuration mode. To turn off voice-quality statistics reporting, use the no form of this command.

mgcp voice-quality-stats [{**priority** *variable* | **all**}]
no mgcp voice-quality-stats [{**priority** *variable* | **all**}]

Syntax Description

priority <*value*>	Selects numeric parameters 1 or 2 to indicate priority.
all	Selects all VQ parameters.

Command Default

Voice-quality statistics reporting is turned off.

Command Modes

Global configuration

Command History

Release	Modification
12.3(3)	This command was introduced.
12.4(4)T	**The priority** and **all** keywords were introduced.

Usage Guidelines

- The request for digital signal processor (DSP) statistics is controlled by the RTP Control Protocol (RTCP) statistics polling interval. The polling interval is configurable by entering the **ip rtcp report interval** command. Statistics are polled every 5 seconds by default.

Note The Cisco PGW 2200 must have a patch the supports DSP statistics in order to collect data in the call detail records (CDRs).

- This command does not generate any output on the console; it adds additional quality statistics parameters in the MGCP Delete Connection (DLCX) ACK message that is sent to the call agent.

Cisco IOS Release 12.4(4)T supports only priority levels 1 and 2.

- The keyword **priority** uses a value of 1 or 2 to indicate the priority of the parameters.

Note Choosing priority 2 is similar to using the keyword **all** where all the paramters are selected.

The corresponding set of VQ parameters are sent in the MGCP DLCX message based on the priority selected.

Examples

The following example enables voice-quality statistics reporting for MGCP:

```
Router> enable
Router# configure terminal
Router(config)# mgcp voice-quality-stats
Router(config)# end
```

The following example shows the VQ parameters selected for priority 1:

```
mgcp voice-quality-stats priority 1
16:38:20.461771 10.0.5.130:2427 10.0.5.133:2427 MGCP...... -> 250 1133 OK
P: PS=0, OS=0, PR=0, OR=0, PL=0, JI=65, LA=0
DSP/TX: PK=118, SG=0, NS=1, DU=28860, VO=2350
DSP/RX: PK=0, SG=0, CF=0, RX=28860, VO=0, BS=0, LP=0, BP=0
DSP/PD: CU=65, MI=65, MA=65, CO=0, IJ=0
DSP/LE: TP=0, RP=0, TM=0, RM=0, BN=0, ER=0, AC=0
DSP/IN: CI=0, FM=0, FP =0, VS=0, GT=0, GR=0, JD=0, JN=0, JM=0,
DSP/CR: CR=0, MN=0, CT=0, TT=0,
DSP/DC: DC=0,
DSP/CS: CS=0, SC=0, TS=0,
DSP/UC: U1=0, U2=0, T1=0, T2=0
```

The following example shows all the VQ parameters selected for the keyword **all**:

```
mgcp voice-quality-stats all

16:38:20.461771 10.0.5.130:2427 10.0.5.133:2427 MGCP...... -> 250 1133 OK
P: PS=0, OS=0, PR=0, OR=0, PL=0, JI=65, LA=0
DSP/TX: PK=118, SG=0, NS=1, DU=28860, VO=2350
DSP/RX: PK=0, SG=0, CF=0, RX=28860, VO=0, BS=0, LP=0, BP=0
DSP/PD: CU=65, MI=65, MA=65, CO=0, IJ=0
DSP/PE: PC=0, IC=0, SC=0, RM=0, BO=0, EE=0
DSP/LE: TP=0, RP=0, TM=0, RM=0, BN=0, ER=0, AC=0
DSP/ER: RD=0, TD=0, RC=0, TC=0
DSP/IC: IC=0
DSP/EC: CI=0, FM=0, FP =0, VS=0, GT=0, GR=0, JD=0, JN=0, JM=0, JX=0,
DSP/KF: KF=0, AV=0, MI=0, BS=0, NB=0, FL=0,
DSP/CS: CR=0, AV=0, MN=0, MX=0, CS=0, SC=0, TS=0, DC=0,
DSP/RF: ML=0, MC=0, R1=0, R2=0, IF=0, ID=0, IE=0, BL=0, R0=0,
DSP/UC: U1=0, U2=0, T1=0, T2=0,
DSP/DL: RT=0, ED=0
```

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, parser, and CAC.
ip rtcp report interval	Configures the RTCP statistics polling interval.

microcode reload controller

To reload the firmware and field programmable gate array (FPGA) without reloading the Cisco IOS image, use the **microcode reload controller** command in privileged EXEC mode.

microcode reload controller {**t1** | **e1** | **j1**} *x/y*

Syntax Description

t1	T1
e1	E1
j1	J1 controller.
x / y	Controller slot and unit numbers. The slash must be typed.

Command Default

No microcode reload activity is initiated.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(2)XH	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(8)T	The **j1** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Loopbacks in the running configuration are restored after this command is entered. If the controller is in a looped state before this command is issued, the looped condition is dropped. You have to reinitiate the loopbacks from the remote end by entering the **no loop**command from the controller configuration.

Examples

The following example shows how to start the microcode reload activity:

```
Router# microcode reload controller j1 3/0
TDM-connections and network traffic will be briefly disrupted.
Proceed with reload microcode?[confirm]
Router#
*Mar  3 209.165.200.225: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.226: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.227: %CONTROLLER-5-UPDOWN: Controller J1 3/0, changed state to)
*Mar  3 209.165.200.227: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.228: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.229: %CONTROLLER-5-UPDOWN: Controller J1 3/0, changed state top
*Mar  3 209.165.200.229: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.229: clk_src_link_up_down: Status of this CLK does not matter
```

midcall-signaling

To configure the method that is used for signaling messages, use the **midcall-signaling** command in SIP configuration mode, or voice class tenant configuration mode, or dial peer configuration mode. To disable the mid-call signaling feature, use the **no** form of this command.

midcall-signaling {**passthru media-change** | **block** | **preserve-codec**} **[system]**
no midcall-signaling

Syntax Description

passthru media-change	Passes SIP messages that involve media-change from one IP leg to another IP leg.
block	Blocks all SIP messages during mid-call.
preserve-codec	Preserves codec that is negotiated during call initialization. Mid-call codec change is disabled.
system	Specifies that the mid-call signaling feature uses the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

Midcall-signaling is disabled. Codec negotiation in the middle of a call is enabled.

Command Modes

SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T. The **media-change** and **block** keywords were added.
15.3(2)S, 15.3(1)T	This command was modified. The **preserve-codec** keyword was added.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

The **midcall-signaling** command distinguishes between the way Cisco Unified Communications Express and Cisco Unified Border Element handle signaling messages. Most SIP-to-SIP video and SIP-to-SIP reinvite based supplementary services require the **midcall-signaling** command to be configured before configuring other supplementary services. Supplementary service features that are functional without configuring **midcall-signaling** include: session refresh, fax, and refer-based supplementary services. The **midcall-signaling** command is for SIP-to-SIP calls only. All other calls (H323-to-SIP, and H323-to-H323) do not require the

midcall-signaling command be configured. The **allow-connections sip-to-sip** command must be configured before the **midcall-signaling** command.

Configuring the Session Refresh with Reinvites feature on a dial-peer basis is not supported.

Examples

The following example shows SIP messages that are configured to passthrough from one IP leg to another IP leg:

```
Router(config)#voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# midcall-signaling passthru
```

The following example shows SIP messages that are configured to media passthru from one IP leg to another IP leg:

```
Router(config)#voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# midcall-signaling passthru media-change
```

The following example shows how to block SIP messages.

```
Router(config)#voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# midcall-signaling block
```

The following example shows how to disable codec negotiation in the middle of a call and retains the codec that is negotiated at the start of the call.

```
Router(config)#voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# midcall-signaling preserve-codec
```

The following example shows SIP messages that are configured to pass thru from one IP leg to another IP leg in the voice class tenant configuration mode:

```
Router(config-class)# midcall-signaling passthru system
```

Related Commands

Command	Description
allow-connections	Allows connections between specific types of endpoints in a Cisco Unified BE.

min-se (SIP)

To change the minimum session expiration (Min-SE) header value for all calls that use the Session Initiation Protocol (SIP) session timer, use the **min-se**command in SIP configuration mode. To reset to the default, use the **no** form of this command.

min-se *time* **session-expires** *interval*
no min-se

Syntax Description

time	Length of time, in seconds. Range: 90–86400 (1 day). Default: 1800.
session-expires *interval*	Indicates that the session expires time interval. Range is 90–86400. Default: 1800.

Command Default

1800 seconds (30 minutes)

Command Modes

SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(9)T	This command was modified. The default time was changed 90–1800 seconds.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(2)T	This command was modified. The **session-expires**keyword was added.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

A proxy, user-agent client, and user-agent server can all have a configured minimum value indicating the smallest session interval that they accept. If they all happen to have a different configured minimum value, the highest minimum value is used. This command sets the minimum timer that is conveyed in the Min-SE header in the initial INVITE request.

The recommended value for this command is 1800 seconds (30 minutes), which is the default value. The value cannot be set below 90 seconds because excessive INVITEs create problems for routers. Once set, the value affects all calls that are originated by the router.

If you do not configure the session expires interval and configure only the min-se value, then the session expires interval takes the value that is configured for the min-se.

Examples

The following example sets the expiration timer to 90 seconds:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# min-se 90 session-expires 1800
```

Related Commands

Command	Description
show sip -ua min-se	Shows the current value of the Min-SE header.

mmoip aaa global-password

To define a password to be used with CiscoSecure for Microsoft Windows NT when using store and forward fax, use the **mmoip aaa global-password**command in global configuration mode. To reset to the default, use the **no** form of this command.

mmoip aaa global-password *password*
no mmoip aaa global-password *password*

Syntax Description

password	Password for CiscoSecure for Windows NT to be used with store and forward fax. The maximum length is 64 alphanumeric characters.

Command Default

No password is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

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

This command applies to on-ramp store and forward fax functions when using a modem card. It is not used with voice feature cards.

Examples

The following example specifies a password (password) when CiscoSecure for Microsoft Windows NT is used with store and forward fax:

```
mmoip aaa global-password password
```

mmoip aaa method fax accounting

To define the name of the method list to be used for authentication, authorization, and accounting (AAA) accounting with store-and-forward fax, use the **mmoip aaa method fax accounting**command in global configuration mode. To reset to the undefined state, use the **no** form of this command.

mmoip aaa method fax accounting *method-list-name*
no mmoip aaa method fax accounting *method-list-name*

Syntax Description

method -list-name	List of accounting methods to be used with store-and-forward fax.

Command Default

No AAA accounting method list is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

This command defines the name of the AAA accounting method list to be used with store-and-forward fax. The method list itself, which defines the type of accounting services provided for store-and-forward fax, is defined using the **aaa accounting** command in global configuration mode. Unlike standard AAA (in which 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.

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

This command applies to both on-ramp and off-ramp store-and-forward fax functions when a modem card is used. It is not used with voice feature cards.

Examples

The following example specifies a AAA accounting method list (called "list3") to be used with store-and-forward fax:

```
aaa new-model
mmoip aaa method fax accounting list3
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when RADIUS or TACACS+ is used.

Command	Description
mmoip aaa receive-accounting enable	Enables on-ramp store-and-forward fax for AAA accounting services.

mmoip aaa method fax authentication

To define the name of the method list to be used for authentication, authorization, and accounting (AAA) authentication with store and forward fax, use the **mmoip aaa method fax authentication** command inglobal configuration mode. To reset to the default, use the **no** form of this command.

mmoip aaa method fax authentication *method-list-name*
no mmoip aaa method fax authentication *method-list-name*

Syntax Description

method -list-name	List of authentication methods to be used with store and forward fax.

Command Default

No AAA authentication method list is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

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

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

This command applies to both on-ramp and off-ramp store and forward fax functions.

Examples

The following example specifies a AAA authentication method list (called xyz) to be used with store and forward fax:

```
aaa new-model
mmoip aaa method fax authentication xyz
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa receive -authentication enable	Enables on-ramp store and forward fax AAA authentication services.

mmoip aaa receive-accounting enable

To enable on-ramp authentication, authorization, and accounting (AAA) services, use the **mmoip aaa receive-accounting enable**command in global configuration mode. To disable on-ramp AAA services, use the **no** form of this command.

mmoip aaa receive-accounting enable
no mmoip aaa receive-accounting enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was introduced on the Cisco 1750.

Usage Guidelines

This command enables AAA services if an accounting method list has been defined using both the **aaa accounting** command and the **mmoip aaa method fax accounting** command.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example specifies an AAA method list (called xyz) to be used with inbound store-and-forward fax. In this example, store-and-forward fax is configured to track start and stop connection accounting records.

```
aaa new-model
mmoip aaa method fax accounting xyz
aaa accounting connection sherman stop-only radius
mmoip aaa receive-accounting enable
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa method fax accounting	Defines the name of the method list to be used for AAA accounting with store-and-forward fax.

mmoip aaa receive-authentication enable

To enable on-ramp authentication, authorization, and accounting (AAA) services, use the **mmoip aaa receive-authentication enable**command in global configuration mode. To disable on-ramp AAA services, use the **no** form of this command.

mmoip aaa receive-authentication enable
no mmoip aaa receive-authentication enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was introduced on the Cisco 1750.

Usage Guidelines

This command enables AAA services if an AAA method list has been defined using both the **aaa authentication** command and the **mmoip aaa method fax authentication** command.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example specifies an AAA method list (called xyz) to be used with inbound store-and-forward fax. In this example, RADIUS authentication (and if the RADIUS server fails, then local authentication) is configured for store-and-forward fax.

```
aaa new-model
mmoip aaa method fax authentication xyz
aaa authentication login peabody radius local
mmoip aaa receive-authentication enable
```

Related Commands

Command	Description
aaa authentication	Enables AAA of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa method fax authentication	Defines the name of the method list to be used for AAA authentication with store-and-forward fax.

mmoip aaa receive-id primary

To specify the primary location from which the authentication, authorization, and accounting (AAA) protocol retrieves its account identification information for on-ramp faxing, use the **mmoip aaa receive-id primary** command in global configuration mode. To remove the definition of the account identification source, use the no form of this command.

mmoip aaa receive-id primary {**ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}
no mmoip aaa receive-id primary {**ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}

Syntax Description

ani	AAA uses the calling party telephone number (automatic number identification [ANI]) as the AAA account identifier.
dnis	AAA uses the called party telephone number (dialed number identification service [DNIS]) as the AAA account identifier.
gateway	AAA uses the router-specific name derived from the hostname and domain name as the AAA account identifier, displayed in the following format: *router-name.domain-name*.
redialer -id	AAA uses the account string returned by the external redialer device as the AAA account identifier. In this case, the redialer ID is either the redialer serial number or the redialer account number.
redialer -dnis	AAA uses the called party telephone number (dialed number identification service [DNIS]) as the AAA account identifier that is captured by the redialer if a redialer device is present.

Command Default

No account identification source is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store-and-forward fax, you can specify that the ANI, DNIS, gateway ID, redialer ID, or redialer DNIS be used to identify the user for authentication. This command defines what AAA uses for the primary identifier for inbound or on-ramp user authentication with store-and-forward fax.

Store-and-forward fax allows you to define either a primary or a secondary identifier. You configure the secondary identifier using the **mmoip aaa receive-id secondary** command.

AAA does not use these methods sequentially. If the primary identifier is defined and AAA cannot authenticate the primary identifier information, it does not use the secondary identifier for authentication. Authentication simply fails.

Defining only the secondary identifier enables you to service two different scenarios simultaneously--for example, if you are offering fax services to two different companies, one of which uses redialers and the other does not. In this case, configure the **mmoip aaa receive-id primary** command to use the redialer DNIS, and configure the **mmoip aaa receive-id secondary** command to use ANI. With this configuration, when a user dials in and the redialer DNIS is not null, the redialer DNIS is used as the authentication identifier. If a user dials in and the redialer DNIS is null, ANI is used as the authentication identifier.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example defines the DNIS captured by the redialer as the primary AAA authentication identifier for store-and-forward fax:

```
aaa new-model
mmoip aaa receive-id primary redialer-dnis
```

Related Commands

Command	Description
mmoip aaa receive -id secondary	Specifies the secondary location from which AAA retrieves its account identification information for on-ramp faxing if the primary identifier has not been defined.

mmoip aaa receive-id secondary

To specify the secondary location where the authentication, authorization, and accounting (AAA) protocol retrieves its account identification information for on-ramp faxing if the primary identifier has not been defined, use the **mmoip aaa receive-id secondary** command in global configuration mode. To remove the definition of the account identification source, use the no form of this command.

mmoip aaa receive-id secondary {**ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}
no mmoip aaa receive-id secondary {**ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}

Syntax Description

ani	AAA uses the calling party telephone number (automatic number identification or ANI) as the AAA account identifier.
dnis	AAA uses the called party telephone number (dialed number identification service or DNIS) as the AAA account identifier.
gateway	AAA uses the router-specific name derived from the host name and domain name as the AAA account identifier, displayed in the following format: *router-name.domain-name*.
redialer -id	AAA uses the account string returned by the external redialer device as the AAA account identifier. In this case, the redialer ID is either the redialer serial number or the redialer account number.
redialer -dnis	AAA uses the called party telephone number (dialed number identification service or DNIS) as the AAA account identifier that is captured by the redialer if a redialer device is present.

Command Default

No account identification source is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was introduced on the Cisco 1750.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store-and-forward fax, you can specify that the ANI, DNIS, gateway ID, redialer DNIS, or redialer ID be used to identify the user for authentication. This command defines what AAA uses for the secondary identifier for inbound or on-ramp user authentication with store-and-forward fax if the primary identifier has not been defined.

Store-and-forward fax allows you to define either a primary or a secondary identifier. You configure the primary identifier using the **mmoip aaa receive-id primary** command.

AAA does not use these methods sequentially--meaning that if the primary identifier is defined and AAA cannot match the primary identifier information, it does not use the secondary identifier for authentication. Authentication simply fails.

Defining only the secondary identifier enables you to service two different scenarios simultaneously--for example, if you are offering fax services to two different companies, one of which uses redialers and the other does not. In this case, configure the **mmoip aaa receive-id primary** command to use the redialer DNIS, and configure the **mmoip aaa receive-id secondary** command to use ANI. With this configuration, when a user dials in and the redialer DNIS is not null, the redialer DNIS is used as the authentication identifier. If a user dials in and the redialer DNIS is null, ANI is used as the authentication identifier.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example defines the DNIS captured by the redialer as the secondary AAA authentication identifier for store-and-forward fax:

```
aaa new-model
mmoip aaa receive-id secondary redialer-dnis
```

Related Commands

Command	Description
mmoip aaa receive -id primary	Specifies the primary location where AAA retrieves its account identification information for on-ramp faxing.

mmoip aaa send-accounting enable

To enable off-ramp authentication, authorization, and accounting (AAA) services, use the **mmoip aaa send-accounting enable**command in global configuration mode. To reset to the default, use the **no** form of this command.

mmoip aaa send-accounting enable
no mmoip aaa send-accounting enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.

Usage Guidelines

This command enables AAA services if an AAA method list has been defined using both the **aaa accounting** command and the **mmoip aaa method fax accounting** command.

This command applies to off-ramp store-and-forward fax functions when using a modem card. It is not used with voice feature cards.

Examples

The following example specifies an AAA method list (called xyz) to be used with outbound store-and-forward fax. In this example, store-and-forward fax is configured to track start and stop connection accounting records.

```
aaa new-model
mmoip aaa method fax accounting xyz
aaa accounting connection sherman stop-only radius
mmoip aaa send-accounting enable
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa method fax accounting	Defines the name of the method list to be used for AAA accounting with store-and-forward fax.

mmoip aaa send-authentication enable

To enable off-ramp authentication, authorization, and accounting (AAA) services, use the **mmoip aaa send-authentication enable**command in global configuration mode. To disable off-ramp AAA services, use the **no** form of this command.

mmoip aaa send-authentication enable
no mmoip aaa send-authentication enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.

Usage Guidelines

This command enables AAA services if an AAA method list has been defined using both the **aaa authentication** command and the **mmoip aaa method fax authentication** command.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example specifies an AAA method list (called xyz) to be used with outbound store-and-forward fax. In this example, RADIUS authentication (and if the RADIUS server fails, then local authentication) is configured for store-and-forward fax.

```
aaa new-model
mmoip aaa method fax authentication xyz
aaa authentication login peabody radius local
mmoip aaa send-authentication enable
```

Related Commands

Command	Description
aaa authentication	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa method fax authentication	Defines the name of the method list to be used for AAA authentication with store-and-forward fax.

mmoip aaa send-id primary

To specify the primary location where the authentication, authorization, and accounting (AAA) protocol retrieves its account identification information for off-ramp faxing, use the **mmoip aaa send-id primary** command in global configuration mode. To remove the definition of the account identification source, use the no form of this command.

mmoip aaa send-id primary {**account-id** | **envelope-from** | **envelope-to** | **gateway**}
no mmoip aaa send-id primary {**account-id** | **envelope-from** | **envelope-to** | **gateway**}

Syntax Description

account -id	AAA uses the account username from the originating fax-mail system as the AAA account identifier. This means that the off-ramp gateway uses the account identifier in the X-account ID field of the e-mail header. Using this attribute offers end-to-end authentication and accounting tracking.
envelope -from	AAA uses the account username from the fax-mail header as the AAA account identifier.
envelope -to	AAA uses the recipient derived from the fax-mail header as the AAA account identifier.
gateway	AAA uses the router-specific name derived from the host name and domain name as the AAA account identifier, displayed in the following format: *router-name.domain-name*.

Command Default

No account identification source is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store-and-forward fax, you can specify that the account ID, username, or recipient name from the e-mail header information be used to identify the user for authentication. This command defines what AAA uses for the primary identifier for outbound or off-ramp user authentication with store-and-forward fax.

Store-and-forward fax allows you to define either a primary or a secondary identifier. You configure the secondary identifier using the **mmoip aaa send-id secondary** command. AAA extracts the authentication identifier information from the defined sources. If the field is blank (meaning undefined), AAA uses the secondary identifier source if configured. The secondary identifier is used only when the primary identifier is null. In this case, when AAA sees that the primary identifier is null, it checks to see if a secondary identifier has been defined and use that value for user authentication.

AAA does not use these methods sequentially--meaning that if the primary identifier is defined and AAA cannot authenticate the primary identifier information, it does not use the secondary identifier for authentication. Authentication simply fails.

When you enable authentication, the on-ramp gateway inserts whatever value you configure for the **mmoip aaa receive-id primary** command in the X-account ID field of the e-mail header. This X-account ID field contains the value that is used for authentication and accounting by the on-ramp gateway. For example, if the **mmoip aaa receive-id primary** command is set to **gateway**, the on-ramp gateway name (for example, hostname.domain-name) is inserted in the X-account ID field of the e-mail header of the fax-mail message.

If you want to use this configured gateway value in the X-account ID field, you must configure the **mmoip aaa send-id primary** command with the **account-id** keyword. This particular keyword enables store-and-forward fax to generate end-to-end authentication and accounting tracking records. If you do not enable authentication on the on-ramp gateway, the X-account ID field is left blank.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example specifies the recipient name as defined in the envelope-to field of the e-mail header to be used as the AAA authentication identifier for store-and-forward fax:

```
aaa new-model
mmoip aaa send-id primary envelope-to
```

Related Commands

Command	Description
mmoip aaa receive -id primary	Specifies the primary location where AAA retrieves its account identification information for off-ramp faxing.
mmoip aaa send -id secondary	Specifies the secondary location where AAA retrieves its account identification information for off-ramp faxing.

mmoip aaa send-id secondary

To specify the secondary location where the authentication, authorization, and accounting (AAA) protocol retrieves its account identification information for off-ramp faxing, use the **mmoip aaa send-id secondary** command in global configuration mode. To remove the definition of the account identification source, use the no form of this command.

mmoip aaa send-id secondary {**account-id** | **envelope-from** | **envelope-to** | **gateway**}
no mmoip aaa send-id secondary {**account-id** | **envelope-from** | **envelope-to** | **gateway**}

Syntax Description

account -id	AAA uses the account username from the originating fax-mail system as the AAA account identifier. This means that the off-ramp gateway uses the account identifier in the X-account ID field of the e-mail header. Using this attribute offers end-to-end authentication and accounting tracking.
envelope -from	AAA uses the account username from the fax-mail header as the AAA account identifier.
envelope -to	AAA uses the recipient derived from the fax-mail header as the AAA account identifier.
gateway	AAA uses the router-specific name derived from the host name and domain name as the AAA account identifier, displayed in the following format: *router-name.domain-name*.

Command Default

No account identification source is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store-and-forward fax, you can specify that the account ID, username, or recipient name from the e-mail header information be used to identify the user for authentication. This command defines what AAA uses for the secondary identifier for outbound or off-ramp user authentication with store-and-forward fax.

Store-and-forward fax allows you to define either a primary or a secondary identifier. You configure the primary identifier using the **mmoip aaa send-id primary** command. AAA extracts the authentication identifier information from the defined sources. If the field is blank (meaning undefined), AAA uses the secondary identifier source if configured. The secondary identifier is used only when the primary identifier is null. In this case, when AAA sees that the primary identifier is null, it checks to see if a secondary identifier has been defined and use that value for user authentication.

AAA does not use these methods sequentially--meaning that if the primary identifier is defined and AAA cannot match the primary identifier information, it does not use the secondary identifier for authentication. Authentication simply fails.

When you enable authentication, the on-ramp gateway inserts whatever value you configure for the **mmoip aaa receive-id secondary** command in the X-account ID field of the e-mail header (if store-and-forward fax uses the defined secondary identifier). This X-account ID field contains the value that is used for authentication and accounting by the on-ramp gateway. For example, if the **mmoip aaa receive-id secondary** command is set to **gateway**, the on-ramp gateway name (for example, hostname.domain-name) is inserted in the X-account ID field of the e-mail header of the fax-mail message.

If you want to use this configured gateway value in the X-account ID field, you must configure the **mmoip aaa send-id secondary** command with the **account-id** keyword. This particular keyword enables store-and-forward fax to generate end-to-end authentication and accounting tracking records. If you do not enable authentication on the on-ramp gateway, the X-account ID field is left blank.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example specifies the recipient name as defined in the envelope-to field of the e-mail header to be used as the AAA authentication identifier for store-and-forward fax:

```
aaa new-model
mmoip aaa send-id secondary envelope-to
```

Related Commands

Command	Description
mmoip aaa receive -id secondary	Specifies the secondary location where AAA retrieves its account identification information for off-ramp faxing.
mmoip aaa send -id primary	Specifies the primary location where AAA retrieves its account identification information for off-ramp faxing.

mode (ATM/T1/E1 controller) through mwi-server

mode (ATM T1 E1 controller)

To set the DSL controller into ATM mode and create an ATM interface or to set the T1 or E1 controller into T1 or E1 mode and create a logical T1/E1 controller, use the **mode** command in controller configuration mode. To disable the current mode and prepare to change modes, use the **no** form of this command.

Cisco 1800, Cisco 2800, Cisco 3700, Cisco 3800 Series
mode atm
no mode atm

Cisco 1700 Series, Cisco 2600XM
mode {**atm** | **t1** | **e1**}
no mode {**atm** | **t1** | **e1**}

Cisco IAD2430
mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}
no mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}

Syntax Description

atm	Sets the controller into ATM mode and creates an ATM interface (ATM 0). When ATM mode is enabled, no channel groups, DS0 groups, PRI groups, or time-division multiplexing (TDM) groups are allowed, because ATM occupies all the DS0s on the T1/E1 trunk. When you set the controller to ATM mode, the controller framing is automatically set to extended super frame (ESF) for T1 or cyclic redundancy check type 4 (CRC4) for E1. The line code is automatically set to binary 8-zero substitution (B8ZS) for T1 or high-density bipolar C (HDBC) for E1. When you remove ATM mode by entering the **no mode atm** command, ATM interface 0 is deleted. **Note** The **mode atm** command without the **aim** keyword uses software to perform ATM segmentation and reassembly (SAR). This is supported on Cisco 2600 series WIC slots only; it is not supported on network module slots.
aim	(Optional) The configuration on this controller uses the Advanced Integration Module (AIM) in the specified slot for ATM SAR. The **aim** keyword does not apply to the Cisco IAD2430 series IAD.
aim-slot	(Optional) AIM slot number on the router chassis: • Cisco 2600 series--0. • Cisco 3660--0 or 1.
cas	(Cisco 2600 series WIC slots only) Channel-associated signaling (CAS) mode. The T1 or E1 in this WIC slot is mapped to support T1 or E1 voice (that is, it is configured in a DS0 group or a PRI group). CAS mode is supported on both controller 0 and controller 1. On the Cisco IAD2430 series IAD, CAS mode is not supported.

t1	Sets the controller into T1 mode and creates a T1 interface. When you set the controller to T1 mode, the controller framing is automatically set to ESF for T1. The line code is automatically set to B8ZS for T1.
e1	Sets the controller into E1 mode and creates an E1 interface. When you set the controller to E1 mode, the controller framing is automatically set to CRC4 for E1. The line code is automatically set to HDB3 for E1.

Command Default

The controller mode is disabled.

Command Modes

Controller configuration

Command History

Release	Modification
11.3 MA	This command was introduced on the Cisco MC3810.
12.1(5)XM	Support for this command was extended to the merged SGCP/MGCP software.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T for the Cisco IAD2420.
12.2(2)XB	Support was extended to the Cisco 2600 series and Cisco 3660. The keyword **aim** and the argument *aim-slot* were added. The parenthetical modifier for the command was changed from "Voice over ATM" to "T1/E1 controller."
12.2(15)T	This command was implemented on the Cisco 2691 and the Cisco 3700 series.
12.3(4)XD	This command was integrated into Cisco IOS Release 12.3(4)XD on Cisco 2600 series and Cisco 3700 series routers to configure DSL Frame mode and to add T1/E1 Framed support.
12.3(4)XG	This command was integrated into Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 2600 series and Cisco 3700 series routers.
12.3(11)T	This command was implemented on Cisco 2800 and Cisco 3800 series routers.
12.3(14)T	This command was implemented on Cisco 1800 series routers.

Usage Guidelines

When a DSL controller is configured in ATM mode, the mode must be configured identically on both the CO and CPE sides. Both sides must be set to ATM mode.

Note If using the **no mode atm** command to leave ATM mode, the router must be rebooted immediately to clear the mode.

When configuring a DSL controller in T1 or E1 mode, the mode must be configured identically on the CPE and CO sides.

Examples

ATM Mode Example

The following example configures ATM mode on the DSL controller.

```
Router(config)# controller
 dsl
 3/0
Router(config-controller)# mode atm
```

T1 Mode Example

The following example configures T1 mode on the DSL controller.

```
Router(config)# controller
 dsl
 3/0
Router(config-controller)# mode t1
```

Related Commands

Command	Description
channel-group	Configures a list of time slots for voice channels on controller T1 0 or E1 0.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for time-division multiplexing (TDM) cross-connect.

mode (T1 E1 controller)

To set the T1 or E1 controller into asynchronous transfer mode (ATM) and create an ATM interface, to set the T1 or E1 controller into T1 or E1 mode and create a logical T1 or E1 controller, or to set the T1 or E1 controller into channel-associated signaling (CAS) mode, use the **mode** command in controller configuration mode. To disable the current mode and prepare to change modes, use the **no**form of this command.

mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}
no mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}

Syntax Description

atm	Sets the controller into ATM mode and creates an ATM interface (ATM 0). When ATM mode is enabled, no channel groups, DS0 groups, PRI groups, or time-division multiplexing (TDM) groups are allowed, because ATM occupies all the DS0s on the T1/E1 trunk. When you set the controller to ATM mode, the controller framing is automatically set to extended super frame (ESF) for T1 or cyclic redundancy check type 4 (CRC4) for E1. The line code is automatically set to binary 8-zero substitution (B8ZS) for T1 or high-density bipolar C (HDB3) for E1. When you remove ATM mode by entering the **no mode atm** command, ATM interface 0 is deleted. On the Cisco MC3810, ATM mode is supported only on controller 0 (T1 or E1 0). **Note** The **mode atm** command without the **aim** keyword uses software to perform ATM segmentation and reassembly (SAR). This is supported on Cisco 2600 series WIC slots only and is not supported on network module slots.
aim	(Optional) The configuration on this controller uses the Advanced Integration Module (AIM) in the specified slot for ATM SAR. The **aim** keyword does not apply to the Cisco MC3810 and the Cisco IAD2420 series IAD.
aim-slot	(Optional) AIM slot number on the router chassis. For the Cisco 2600 series, the AIM slot number is 0; for the Cisco 3660, the AIM slot number is 0 or 1.
cas	(CAS mode on Cisco 2600 series WIC slots only) The T1 or E1 in this WIC slot is mapped to support T1 or E1 voice (it is configured in a DS0 group or a PRI group). CAS mode is supported on both controller 0 and controller 1.
t1	(Cisco 2600XM series using the G.SHDSL WIC only) Sets the controller into T1 mode and creates a T1 interface. When you set the controller to T1 mode, the controller framing is automatically set to ESF for T1. The line code is automatically set to B8ZS for T1.
e1	(Cisco 2600XM series using the G.SHDSL WIC only) Sets the controller into E1 mode and creates an E1 interface. When you set the controller to E1 mode, the controller framing is automatically set to CRC4 for E1. The line code is automatically set to HDB3 for E1.

Command Default

No controller mode is configured.

Command Modes

Controller configuration

Command History

Release	Modification
11.3 MA	This command was introduced on the Cisco MC3810.
12.1(5)XM	Support for this command was extended to Simple Gateway Control Protocol (SGCP) and Media Gateway Control Protocol (MGCP).
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(2)XB	Support was extended to the Cisco 2600 series and Cisco 3660. The **aim**keyword and the *aim-slot* argument were added. The parenthetical modifier for the command was changed from "Voice over ATM" to "T1/E1 controller."
12.2(8)T	This command was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
12.2(15)T	This command was implemented on the Cisco 2691 and the Cisco 3700 series.
12.3(4)XD	Support was extended on Cisco 2600 series and Cisco 3700 series routers to configure DSL Frame mode and to add T1/E1 Framed support.
12.3(7)T	The support that was added in Cisco IOS Release 12.3(4)XD was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

This command has the following platform-specific usage guidelines:

- Cisco 2600 series, Cisco 3660 routers, or Cisco 3700 series that use an AIM for ATM processing must use the **mode atm aim***aim-slot* command.
- Cisco 2600 series routers that use an AIM for DSP processing and specify DS0 groups must use the **mode cas** command if they are using WIC slots for voice. This command does not apply if network modules are being used.
- Cisco 3660 routers or Cisco 3700 series that use an AIM only for DSP resources should not use this command.
- On Cisco 2600 series routers that use WIC slots for voice, the **mode atm** command without the **aim** keyword specifies software ATM segmentation and reassembly. When the **aim** keyword is used with the **mode atm** command, the AIM performs ATM segmentation and reassembly.
- Cisco MC3810 routers cannot use the **aim** keyword.
- Cisco MC3810 routers with digital voice modules (DVMs) use some DS0s exclusively for different signaling modes. The DS0 channels have the following limitations when mixing different applications (such as voice and data) on the same network trunk:
  - On E1 controllers, DS0 16 is used exclusively for either CAS or common channel signaling (CCS), depending on which mode is configured.
  - On T1 controllers, DS0 24 is used exclusively for CCS.

- Cisco MC3810--When no mode is selected, channel groups and clear channels (data mode) can be created using the **channel group** and **tdm-group** commands, respectively.
- Cisco MC3810 is not supported in the AIM-ATM, AIM-VOICE-30, and AIM-ATM-VOICE-30 on the Cisco 2600 Series, Cisco 3660, and Cisco 3700 Series feature.
- On Cisco 2600 series and Cisco 3700 series routers when configuring a DSL controller in ATM mode, the mode must be set to the same mode on both the CO and CPE sides. Both sides must be set to ATM mode.
    - If the **no mode atm** command is used to leave ATM mode, the router must be rebooted immediately to clear the mode.
- On Cisco 2600 series and Cisco 3700 series routers when configuring a DSL controller in T1 or E1 mode, the mode must be configured identically on the CO and CPE sides.

Examples

The following example configures ATM mode on controller T1 0. This step is required for Voice over ATM.

```
Router(config)# controller
 T1 0
Router(config-controller)# mode atm
```

The following example configures ATM mode on controller T1 1/ 0 on a Cisco 2600 series router using an AIM in slot 0 for ATM segmentation and reassembly:

```
Router(config)# controller
 t1 1/0
Router(config-controller)# mode atm aim 0
```

The following example configures CAS mode on controller T1 1 on a Cisco 2600 series router:

```
Router(config)# controller
 T1 1
Router(config-controller)# mode cas
```

The following example configures ATM mode on the DSL controller.

```
Router(config)# controller
 dsl 3/0
Router(config-controller)# mode atm
```

The following example configures T1 mode on the DSL controller.

```
Router(config)# controller
 dsl
 3/0
Router(config-controller)# mode t1
```

Related Commands

Command	Description
channel-group	Defines the time slots for voice channels on controller T1 0 or E1 0.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for TDM cross-connect.

mode border-element

To enable the set of commands used in the border-element configuration, use the **mode border-element** command in voice service voip configuration mode. To disable the set of commands used in border-element configuration, use the **no** form of this command.

mode border-element license [**capacity** *sessions* | **periodicity** {**mins** *value* | **hours** *value* | **days** *value*}]
no mode border-element

Syntax Description

license capacity	(Optional) Configures the license capacity for the Cisco Unified Border Element (UBE).
sessions	(Optional) Number of licenses enabled for the border-element configuration. The range is from 0 through 999999.
periodicity	(Optional) Configures periodicity interval for license entitlement requests for Cisco Unified Border Element (UBE). Default is 7 days.
mins	(Optional) Number of minutes for which the license periodicity configuration is applicable. The range is from 1 through 59.
hours	(Optional) Number of hours for which the license periodicity configuration is applicable. The range is from 1 through 23.
days	(Optional) Number of days for which the license periodicity configuration is applicable. The range is from 1 through 30.

Command Modes

voice service voip configuration (conf-voi-serv)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1r	• Introduced support for YANG models. • The **capacity** keyword and *sessions* argument were deprecated. • The **periodocity** keyword and corresponding arguments were introduced.
15.2(1)T	The command was modified. The **license capacity** keyword and the *sessions* argument were added.
15.0(1)M	This command was introduced.

Usage Guidelines

Effective from Cisco IOS XE Amsterdam 17.2.1r, the **capacity** keyword and *sessions* argument are deprecated. However, the keyword and argument are available in the Command Line Interface (CLI). If you try to configure license capacity using CLI, the following error message is displayed:

```
Error: CUBE SIP trunk licensing is now based on dynamic session counting. Static
 license capacity configuration has been deprecated.
```

If you have configured license capacity in your current release, then while upgrading to Cisco IOS XE Amsterdam 17.2.1r or later releases, license capacity count is ignored and only **mode border-element** command is configured.

For releases before Cisco IOS XE Amsterdam 17.2.1r, the Cisco UBE status display is enabled only if the license capacity has been configured with **mode border-element** command. Without the license capacity configuration, the **show cube status** command does not display any output. This dependency is removed from Cisco IOS XE Amsterdam 17.2.1r and later releases.

You can configure the license entitlement interval in minutes, hours, or days. The default value of the license entitlement interval is 7 days.

We recommend you to configure interval in days. Configuring interval in minutes or hours increases the frequency of entitlement requests and thereby increases the processing load on Cisco Smart Software Manager (CSSM). License periodicity configuration of minutes or hours is recommended to be used only with Cisco Smart Software Manager On-Prem (formerly known as Cisco Smart Software Manager satellite) mode.

The following warning is displayed when you try to configure the interval in minutes or hours:

```
Warning: Periodicity interval of mins/hours would result in frequent licensing
requests and should be used with satellite mode of license manager, continue?
[confirm]
```

For **mode border-element** or **no mode border-element** command to take effect, you must save the running-config file and reload the router after you enter the command. The CLI displays the following notification after the command is entered:

```
You need to save and reload the router for this configuration change to be
effective.
```

If you do not reload the router, the **mode border-element** or **no mode border-element** command does not take effect, and the availability of the commands used in the border-element configuration is not affected.

Note The **show running-config** command displays the **mode border-element** or **no mode border-element** command in its output, even if a reload has not been done and either command is not in effect.

Examples

The following example shows how to configure the license capacity in releases before Cisco IOS XE Amsterdam 17.2.1r with the **mode border-element** command for enabling the Cisco UBE status display:

```
Router(config)# voice service voip
Router(conf-voi-serv)# mode border-element license capacity 100
```

The following example shows how to configure license periodicity for releases Cisco IOS XE Amsterdam 17.2.1r and later.

```
Router(config)# voice service voip
Router(conf-voi-serv)# mode border-element license periodicity days 15
```

The following alert message is displayed if you configure periodicity in minutes or hours:

```
Router(config)# voice service voip
Router(conf-voi-serv)# mode border-element license periodicity mins 30
```

```
Warning: Periodicity interval of mins/hours would result in frequent licensing requests and
 should be used with satellite mode of license manager, continue? [confirm]
```

Related Commands

Command	Description
codec (voice port)	Specifies voice compression.
codec complexity	Specifies the call density and codec complexity based on the codec used.
media	Enables media packets to pass directly between the endpoints without the intervention of the IP-to-IP gateway and enables the incoming and outgoing IP-IP call gain/loss feature for audio call scoring on either the incoming dial peer or the outgoing dial peer.
show cube status	Displays the Cisco UBE status, the software version, the license capacity, the image version, and the platform name of the router.
show dial peer voice	Displays the codec setting for dial peers.
show running-config	Displays the contents of the currently running configuration file on the router.

mode ccs

To configure the T1/E1 controller to support common channel signaling (CCS) cross-connect or CCS frame forwarding, use the mode ccs command in global configuration mode. To disable support for CCS cross-connect or CCS frame forwarding on the controller, use the no form of this command.

mode ccs {**cross-connect** | **frame-forwarding**}
no mode ccs {**cross-connect** | **frame-forwarding**}

Syntax Description

cross -connect	Enables CCS cross-connect on the controller.
frame -forwarding	Enables CCS frame forwarding on the controller.

Command Default

No CCS mode is configured

Command Modes

Global configuration

Command History

Release	Modification
12.0(2)T	This command was introduced on the Cisco MC3810.
12.1(2)XH	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

On Cisco 2600 series routers and Cisco 2600XM series routers with the AIM-ATM, AIM-VOICE-30 or AIM-ATM-VOICE-30 module installed, the channel group configuration must be removed before the **no mode ccs frame-forwarding** command is entered. This restriction does not apply to the Cisco 3600 series routers or the Cisco 3700 series routers.

Examples

To enable CCS cross-connect on controller T1 1, enter the following commands:

```
controller T1 1
 mode ccs cross-connect
```

To enable CCS frame forwarding on controller T1 1, enter the following commands:

```
controller T1 1
 mode ccs frame-forwarding
```

Related Commands

Command	Description
ccs connect	Configures a CCS connection on an interface configured to support CCS frame forwarding.

modem passthrough (dial peer)

To enable modem pass-through over VoIP for a specific dial peer, use the **modem passthrough** command in dial peer configuration mode. To disable modem pass-through for a specific dial peer, use the **no**form of this command.

modem passthrough {**system** | **nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy**]}
no modem passthrough

Syntax Description

system	Defaults to the global configuration.
nse	Specifies that named signaling events (NSEs) are used to communicate codec switchover between gateways.
payload -type *number*	(Optional) NSE payload type. Range varies by platform, but is from 96 to 119 on most platforms. For details, refer to command-line interface (CLI) help. Default is 100.
codec	Codec selections for upspeeding.
g711ulaw	Codec G.711 u-law 64000 bits per second for T1.
g711alaw	Codec G.711 a-law 64000 bits per second for E1.
redundancy	(Optional) Enables a single repetition of packets (using RFC 2198) to improve reliability by protecting against packet loss.

Command Default

payload -type *number*:100

Command Modes

Dial peer configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

Use this command to enable fax pass-through over VoIP individually for a single dial peer. Use the same values for all options on originating and terminating gateways.

Fax pass-through occurs when incoming T.30 fax data is not demodulated or compressed for its transit through the packet network. On detection of a fax tone on an established VoIP call, the gateways switch into fax pass-through mode by suspending the voice codec and configuration and loading the pass-through parameters for the duration of the fax session. The switchover of codec is known as upspeeding, and it changes the bandwidth needed for the call to the equivalent of G.711.

The **system** keyword overrides the configuration for the dial peer and directs that the values from the global configuration are to be used for this dial peer. When the **system** keyword is used, the following parameters are not available: **nse**, **payload-type**, **codec**, and **redundancy**.

The **modem passthrough (voice service)** command can be used to set pass-through options globally on all dial peers at one time. If the **modem passthrough (voice service)**command is used to set pass-through options for all dial peers and the **modem passthrough (dial peer)**command is used on a specific dial peer, the dial peer configuration takes precedence over the global configuration for that dial peer.

Examples

The following example configures fax pass-through over VoIP for a specific dial peer:

```
dial-peer voice 25 voip
 modem passthrough nse codec g711ulaw redundancy
```

Related Commands

Command	Description
dial -peer voice	Enters dial-peer configuration mode.
modem passthrough (voice service)	Enables fax or modem pass-through over VoIP globally for all dial peers.

modem passthrough (voice-service)

To enable fax or modem pass-through over VoIP globally for all dial peers, use the **modem passthrough**command in voice-service configuration mode. To disable fax or modem pass-through, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, Cisco 3700 Series, Cisco AS5300
modem passthrough nse [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy** [**maximum-sessions** *sessions*]]
no modem passthrough

Cisco AS5350, Cisco AS5400, Cisco AS5850, Cisco AS5350XM, Cisco AS5400XM, Cisco VGD 1T3
modem passthrough {**nse** | **protocol**} [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy** [**maximum-sessions** *sessions*] [**sample-duration** [{**10** | **20**}]]]
no modem passthrough

Syntax Description

nse	Specifies the named signaling events (NSEs) used to communicate codec switchover between gateways.
payload -type *number*	(Optional) Specifies NSE payload type. The range varies for this keyword, but is from 96 to 119 on most platforms. For details, see the command-line interface (CLI) help. Default value is 100.
codec	Configures codec selections for upspeed.
g711ulaw	Configures Codec G.711 mu-law, 64000 bits per second for T1.
g711alaw	Configures Codec G.711 A-law, 64000 bits per second for E1.
redundancy	(Optional) Specifies the single repetition of packets (using RFC 2198) to improve reliability by protecting against packet loss.
maximum-sessions *sessions*	(Optional) Specifies the maximum number of simultaneous pass-through sessions. Ranges and defaults vary by platform. For details, see the CLI help.
protocol	Configures the Session Initiation Protocol (SIP)/H.323 protocol used for signal modem pass-through.
sample -duration	(Optional) Specifies the Time, in milliseconds, of the largest Real-time Transport Protocol (RTP) packet when packet redundancy is active. Keywords vary by platform, but are either **10** or **20**. Default is **10**.

Command Default

The command is disabled, so no fax or modem pass-through occurs.

Command Modes

Voice-service configuration (conf-voi-serv)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.

Release	Modification
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco AS5350, Cisco AS5400, and Cisco AS5850. The **sample-duration** keyword was added.
12.4(24)T	This command was implemented on the following platforms: Cisco AS5350XM, Cisco AS5400XM, and Cisco VGD 1T3. The **protocol** keyword was added.

Usage Guidelines

Use this command to enable fax or modem pass-through over VoIP globally for all dial peers. Use the same values for all options on originating and terminating gateways.

In Cisco IOS Release 12.4(24)T, the **modem passthrough protocol** command is supported only on SIP signaling.

Note The **modem passthrough protocol** and **fax protocol** commands cannot be configured at the same time. If you enter either one of these commands when the other is already configured, the command-line interface returns an error message. The error message serves as a confirmation notice because the **modem passthrough protocol** command is internally treated the same as the **fax protocol passthrough** command by the Cisco IOS software. For example, no other mode of fax protocol (for example, fax protocol T.38) can operate if the **modem passthrough protocol** command is configured.

Note Cisco does not support the following protocols for the **modem pass through protocol codec g711alaw** command for inter-operating third-party vendors using voice modems:

- ITU-T V.152
- A set standard for modem passthrough
- Protocol based modem passthrough up-speeds based on the sdp attribute "a=silenceSupp:off -"

Note Even though the **modem passthrough protocol** and **fax protocol passthrough** commands are treated the same internally, be aware that if you change the configuration from the **modem passthrough protocol** command to the **modem passthrough ns e** command, the configured **fax protocol passthrough** command is not automatically reset to the default. If default settings are required for the **fax protocol** command, you have to specifically configure the **fax protocol** command.

Fax pass-through occurs when incoming T.30 fax data is not demodulated or compressed for its transit through the packet network. On detection of a fax tone on an established VoIP call, the gateways switch into fax pass-through mode by suspending the voice codec and configuration and loading the pass-through parameters for the duration of the fax session. The switchover of codec is known as upspeeding, and it changes the bandwidth needed for the call to the equivalent of G.711.

When using the **voice service voip** and **modem passthrough nse** commands on a terminating gateway to globally set up fax or modem pass-through with NSEs, you must also ensure that each incoming call will be associated with a VoIP dial peer to retrieve the global fax or modem configuration. You can associate calls with dial peers by using the **incoming called-number** command to specify a sequence of digits that the incoming calls can match. You can ensure that all calls will match at least one dial peer by using the following commands:

```
Device(config)# dial-peer voice
 tag
 voip
Device(config-dial-peer)# incoming called-number
```

The **modem passthrough (dial peer)** command can be used to set pass-through options on individual dial peers. If the **modem passthrough (voice-service)**command is used to set pass-through options for all dial peers and the **modem passthrough (dial peer)** command is used on a specific dial peer, the dial-peer configuration takes precedence over the global configuration for that specific dial peer.

Examples

The following example shows how to configure modem pass-through for NSE payload type 101 using the G.711 mu-law codec:

```
voice service voip
 modem passthrough nse payload-type 101 codec g711ulaw redundancy maximum-sessions 1
```

Related Commands

Command	Description
fax protocol (voice-service)	Specifies the global default fax protocol to be used for all VoIP dial peers.
incoming called-number	Defines an incoming called number to match a specific dial peer.
modem passthrough (dial peer)	Enables fax or modem pass-through over VoIP for a specific dial peer.
voice service voip	Enters voice-service configuration mode and specifies the voice encapsulation type.

modem relay (dial peer)

To configure modem relay over VoIP for a specific dial peer, use the **modem relay** command in dial peer configuration mode. To disable modem relay over VoIP for a specific dial peer, use the **no**form of this command.

modem relay {**nse** [**payload-type** *number*] **codec** {**g711alaw** | **g711ulaw**} [**redundancy**] | **system**} **gw-controlled**
no modem relay {**nse** | **system**}

Syntax Description

nse	Named signaling event (NSE).
payload -type *number*	(Optional) NSE payload type. Range is from 98 to 119. Default is 100.
codec	Sets the upspeed voice compression selection for speech or audio signals. The upspeed method is used to dynamically change the codec type and speed to meet network conditions. A faster codec speed may be required to support both voice and data calls and a slower speed for only voice traffic.
g711ulaw	Codec G.711 mu-law 64,000 bits per second (bps) for T1.
g711alaw	Codec G.711 a-law 64,000 bps for E1.
redundancy	(Optional) Packet redundancy (RFC 2198) for modem traffic. Sends redundant packets for modem traffic during pass-through.
system	This default setting uses the global configuration parameters set with the **modem relay** command in voice-service configuration mode for VoIP.
gw -controlled	Specfies the gateway-configured method for establishing modem relay parameters.

Command Default

Cisco modem relay is disabled. Payload type: 100

Command Modes

Dial peer configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.
12.4(4)T	The **gw-controlled** keyword was added.
12.4(6)T	This feature was implemented on the Cisco 1700 series and Cisco 2800 series.

Usage Guidelines

This command applies to VoIP dial peers. Use this command to configure modem relay over VoIP for a specific dial peer.

Use the same codec typefor the originating and terminating gateway, as follows:

- T1 requires the G.711 mu-law codec.

- E1 requires the G.711 a-law codec.

The **system** keyword overrides the configuration for the dial peer, and the values from the **modem-relay** command in voice-service configuration mode for VoIP are used.

When using the **voice service voip** and **modem relay nse** commands on a terminating gateway to globally set up modem relay with NSEs, you must also ensure that each incoming call will be associated with a VoIP dial peer to retrieve the global fax or modem configuration. You associate calls with dial peers by using the **incoming called-number** command to specify a sequence of digits that incoming calls can match. You can ensure that all calls will match at least one dial peer by using the following commands:

```
Router(config)# dial-peer voice tag voip
Router(config-dial-peer)# incoming called-number .
```

Examples

The following example shows Cisco modem relay configured for a specific dial peer using the G.711 mu-law codec and enabling redundancy and gateway-controlled negotiation parameters:

```
Router(config-dial-peer)# modem relay nse codec g711ulaw redundancy gw-controlled
```

Related Commands

Command	Description
incoming called-number	Defines an incoming called number to match a specific dial peer.
modem passsthrough (voice service)	Enables fax or modem pass-through over VoIP globally for all dial peers.
modem relay (voice-service)	Enables fax or modem pass-through over VoIP globally for all dial peers.
voice service voip	Enters voice-service configuration mode and specifies the voice encapsulation type.

modem relay (voice-service)

To configure modem relay over VoIP for all connections, use the **modem relay**command in voice-service configuration mode. To disable modem relay over VoIP for all connections, use the **no** form of this command.

modem relay nse [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy** [**maximum-sessions** *value*]] **gw-controlled**
no modem relay nse

Syntax Description

nse	Named signaling event (NSE).
payload -type *number*	(Optional) NSE payload type. Range is from 98 to 119. Default is 100.
codec	Sets the upspeed voice compression selection for speech or audio signals. The upspeed method is used to dynamically change the codec type and speed to meet network conditions. A faster codec speed may be required to support both voice and data calls and a slower speed for only voice traffic.
g711ulaw	Codec G.711m u-law 64,000 bits per second (bps) for T1.
g711alaw	Codec G.711 a-law 64,000 bps for E1.
redundancy	(Optional) Packet redundancy (RFC 2198) for modem traffic. Sends redundant packets for modem traffic during pass-through.
maximum -sessions *value*	(Optional) Maximum redundant, simultaneous modem-relay pass-through sessions. Range is from 1 to 10000. Default is 16. Recommended value for the Cisco AS5300 is 26.
gw-controlled	Specfies the gateway-configured method for establishing modem relay parameters.

Command Default

Cisco modem relay is disabled. Payload type: 100.

Command Modes

Voice-service configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.
12.4(4)T	The **gw-controlled** keyword was added.
12.4(6)T	This feature was implemented on the Cisco 1700 series and Cisco 2800 series.

Usage Guidelines

Use this command to configure modem relay over VoIP. The default behavior for this command is **no modem relay**. Configuration of modem relay for VoIP dial peers via the **modem relay**dial-peer configuration command overrides this voice-service command for the specific VoIP dial peer on which the dial-peer command is configured.

Use the same payload-type number for both the originating and terminating gateways.

Use the same codec typefor the originating and terminating gateway, as follows:

- T1 requires the G.711 mu-law codec.
- E1 requires the G.711 a-law codec.

The **maximum-sessions** keyword is an optional parameter for the **modem relay** command. This parameter determines the maximum number of redundant, simultaneous modem relay sessions. The recommended *value* for the **maximum-sessions** keyword is 16. The value can be set from 1 to 10000. The **maximum-sessions** keyword applies only if the **redundancy** keyword is used.

When using the **voice service voip** and **modem relay nse** commands on a terminating gateway to globally set up modem relay with NSEs, you must also ensure that each incoming call will be associated with a VoIP dial peer to retrieve the global fax or modem configuration. You associate calls with dial peers by using the **incoming called-number** command to specify a sequence of digits that incoming calls can match. You can ensure that all calls will match at least one dial peer by using the following commands:

```
Router(config)# dial-peer voice
 tag
 voip
Router(config-dial-peer)# incoming called-number .
```

Examples

The following example shows Cisco modem relay enabled with NSE payload type 101 using the G.711 mu-law codec, enabling redundancy and gateway-controlled negotiation parameters:

```
Router(conf-voi-serv)# modem relay nse payload-type 101 codec g711ulaw redundancy
maximum-sessions 1 gw-controlled
```

Related Commands

Command	Description
incoming called-number	Defines an incoming called number to match a specific dial peer.
modem relay (dial-peer)	Configures modem relay on a specific VoIP dial peer.

modem relay gateway-xid

To enable in-band negotiation of compression parameters between two VoIP gateways, use the **modem relay gateway-xid** command in dial-peer or voice-service configuration mode. To disable this function, use the **no** form of this command.

modem relay gateway-xid [{**compress** {**backward** | **both** | **forward** | **no**}}] [{[**dictionary** *value*]}] [{[**string-length** *value*]}]
no modem relay gateway-xid

Syntax Description

compress	(Optional) Direction in which data flow is compressed. For normal dialup, compression should be enabled on both directions. You may want to disable compression in one or more directions. This is normally done during testing and perhaps for gaming applications, but not for normal dialup when compression is enabled in both directions. • **backward** --Enables compression only in the backward direction. • **both** --Enables compression in both directions. For normal dialup, this is the preferred setting. This is the default. • **forward** --Enables compression only in the forward direction. • no--Disables compression in both directions. **Note** The compress, dictionary, and string-length arguments can be entered in any order.
dictionary *value*	(Optional) V.42 *bis* parameter that specifies characteristics of the compression algorithm. Range is from 512 to 2048. Default is 1024. **Note** Your modem may support values higher than this range. A value acceptable to both sides is negotiated during modem call setup.
string-length *value*	(Optional) V.42 *bis* parameter that specifies characteristics of the compression algorithm. Range is from 16 to 32. Default is 32. **Note** Your modem may support values higher than this range. A value acceptable to both sides is negotiated during modem call setup.

Command Default

Command: enabled Compress: both Dictionary: 1024 String length: 32

Command Modes

Dial-peer configuration
Voice-service configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.

Usage Guidelines

This command enables XID negotiation for modem relay. By default it is enabled.

If this command is enabled on both VoIP gateways of a network, the gateways determine whether they need to engage in in-band negotiation of various compression parameters. The remaining keywords in this command specify the negotiation posture of this gateway in the subsequent in-band negotiation (assuming that in-band negotiation is agreed on by the two gateways).

The remaining parameters specify the negotiation posture of this gateway in the subsequent inband negotiation step (assuming inband negotiation was agreed on by the two gateways).

The **compress**, **dictionary**, and **string-length** keywords are digital-signal-processor (DSP)-specific and related to xid negotiation. If this command is disabled, they are all irrelevant. The application (MGCP or H.323) just passes these configured values to the DSPs, and it is the DSP that requires them.

Examples

The following example enables in-band negotiation of compression parameters on the VoIP gateway, with compression in both directions, dictionary size of 1024, and string length of 32 for the compression algorithm:

```
modem relay gateway-xid compress both dictionary 1024 string-length 32
```

Related Commands

Command	Description
mgcp modem relay voip gateway-xid	Optimizes the modem relay transport protocol and the estimated one-way delay across the IP network.
mgcp modem relay voip mode	Enables modem relay mode support in a gateway for MGCP VoIP calls.
mgcp modem relay voip sprt retries	Sets the maximum number of times that the SPRT protocol tries to send a packet before disconnecting.
mgcp tse payload	Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP.

modem relay latency

To optimize the Modem Relay Transport Protocol and the estimated one-way delay across the IP network, use the **modem relay latency** command in dial-peer or voice-service configuration mode. To disable this function, use the **no** form of this command.

modem relay latency *value*
no modem relay latency

Syntax Description

value	Estimated one-way delay across the IP network, in milliseconds. Range is from 100 to 1000. Default is 200.

Command Default

200 ms

Command Modes

Dial-peer configuration
Voice-service configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.

Usage Guidelines

Use this command to adjust the retransmission timer of the Simple Packet Relay Transport (SPRT) protocol, if required, by setting the value to the estimated one-way delay (in milliseconds) across the IP network. Changing this value may affect the throughput or delay characteristics of the modem relay call. The default value of 200 does not need to be changed for most networks.

Examples

The following example sets the estimated one-way delay across the IP network to 100 ms.

```
Router(config-dial-peer)# modem relay latency 100
```

Related Commands

Command	Description
mgcp modem relay voip latency	Optimizes the Modem Relay Transport Protocol and the estimated one-way delay across the IP network using MGCP.
mgcp modem relay voip mode	Enables modem relay mode support in a gateway for MGCP VoIP calls.
mgcp modem relay voip sprt retries	Sets the maximum number of times that the SPRT protocol tries to send a packet before disconnecting.
mgcp tse payload	Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP.
modem relay gateway-xid	Enables in-band negotiation of compression parameters between two VoIP gateways that use MBCP.

modem relay sprt retries

To set the maximum number of times that the Simple Packet Relay Transport (SPRT) protocol tries to send a packet before disconnecting, use the modem relay sprt retries command in dial-peer or voice-service configuration mode. To disable this function, use the **no** form of this command.

modem relay sprt retries *value*
no modem relay sprt retries

Syntax Description

value	Maximum number of times that the SPRT protocol tries to send a packet before disconnecting. Range is from 6 to 30. The default is 12.

Command Default

12 times

Command Modes

Dial-peer configuration
Voice-service configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.

Examples

The following example sets 15 as the maximum number of times that the SPRT protocol tries to send a packet before disconnecting.

```
modem relay sprt retries 15
```

Related Commands

Command	Description
mgcp modem relay voip mode	Enables modem relay mode support in a gateway for MGCP VoIP calls.
mgcp tse payload	Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP.
modem relay gateway-xid	Enables in-band negotiation of compression parameters between two VoIP gateways that use MBCP.
modem relay latency	Optimizes the Modem Relay Transport Protocol and the estimated one-way delay across the IP network.

modem relay sprt v14

To configure V.14 modem-relay parameters for packets sent by the Simple Packet Relay Transport (SPRT) protocol, use the **modem relay sprt v14**command in voice service configuration mode. To disable this function, use the **no** form of this command.

modem relay sprt v14 [{**receive playback hold-time** *milliseconds* | **transmit hold-time** *milliseconds* | **transmit maximum hold-count** *characters*}]
no modem relay sprt v14

Syntax Description

receive playback hold-time *milliseconds*	(Optional) Configures the time in milliseconds (ms) to hold incoming data in the V.14 receive queue. Range is 20 to 250 ms. Default is 50 ms.
transmit hold-time *milliseconds*	(Optional) Configures the time to wait, in ms, after the first character is ready before sending the SPRT packet. Range is 10 to 30 ms. Default is 20 ms.
transmit maximum hold-count *characters*	(Optional) Configures the number of V.14 characters to be received on the ISDN public switched telephone network (PSTN) interface that will trigger sending the SPRT packet. Range is 8 to 128. Default is 16.

Command Default

V.14 modem-relay parameters are enabled by default, using default parameter values.

Command Modes

Voice service configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

SPRT packets are used to reliably transport modem signals between gateways. Use the **modem relay sprt v14** command under the **voice service voip** command to configure parameters for SPRT packet transport. The maximum size of the receive buffers is set at 500 characters, a nonprovisionable limit. Use the **modem relay sprt v14 receive playback hold-time**command to configure the minimum holding time before characters can be removed from the receive queue. Characters received on the PSTN or ISDN interface may be collected for a configurable collection period before being sent out on SPRT channel 3, potentially resulting in variable size SPRT packets. To configure V.14 transmit parameters for SPRT packets, use the **modem relay sprt v14 transmit hold-time** *milliseconds and the* **modem relay sprt v14 transmit maximum hold-count** *characters*commands.

Parameter changes do not take effect during existing calls; they affect new calls only.

SPRT transport channel 1 is not supported.

Use the **stcapp register capability** *voice-port* **modem-relay** command to specify modem relay as the transport method for a specific device.

Examples

The following example shows the receive playback hold time, transmit hold time, and transmit hold count parameters:

```
Router(conf-voi-serv)
# modem relay sprt v14 receive playback hold-time 200
Router(conf-voi-serv)
# modem relay sprt v14 transmit hold-time 25
Router(conf-voi-serv)
# modem relay sprt v14 transmit maximum hold-count 10
```

Related Commands

Command	Description
debug voip ccapi inout	Traces the execution path through the call control API.
debug vtsp all	Displays all VTSP debugging except statistics, tone, and event.
stcapp register capability	Configures the modem transport method for a specified device registered with Cisco CallManager.
voice service voip	Enters voice service configuration mode for VoIP encapsulation.

modem relay sse

To enable V.150.1 modem-relay secure calls and configure state signaling events (SSE) parameters, use the **modem relay sse** command in voice service configuration mode. To disable this function, use the **no** form of this command.

modem relay sse [**redundancy**] [**interval** *milliseconds*] [**packet** *number*] [**retries** *value*] [**t1** *milliseconds*][**v150mer**]
no modem relay sse

Syntax Description

redundancy	(Optional) Specifies packet redundancy for modem traffic during modem pass-through. By default redundancy is disabled.
interval *milliseconds*	(Optional) Specifies the timer in milliseconds (ms) for redundant transmission of SSEs. Range is 5 to 50 ms. Default is 20 ms.
packet *number*	(Optional) Specifies the SSE packet retransmission count before disconnecting. Range is one to five packets. Default is three packets.
retries *value*	(Optional) Specifies the number of SSE packet retries, repeated every **t1** interval, before disconnecting. Range is zero to five retries. Default is five retries.
t1 *milliseconds*	(Optional) Specifies the repeat interval, in milliseconds, for initial audio SSEs used for resetting the SSE protocol state machine (clearing the call) following error recovery. Range is 500 to 3000 ms. Default is 1000 ms.
v150mer	Configures the V150.1 MER modem relay support for SIP trunks.

Command Default

Modem relay mode of operation, using the SSE protocol, is enabled by default using default parameter values.

Command Modes

Voice service configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
15.5(3)M	This command was modified. The **v150mer** keyword was added.

Usage Guidelines

Use the **modem relay sse** command under the **voice service voip** command to configure SSE parameters used to negotiate the transition from voice mode to V.150.1 modem-relay mode on the digital signal processor (DSP). Secure voice and data calls through the SCCP Telephony Control Application (STCAPP) gateway connect Secure Telephone Equipment (STE) and IP-STE endpoints using the SSE protocol, a subset of the V.150.1 standard for modem relay. SSEs, which are Real-Time Transport Protocol (RTP) encoded event messages that use payload 118, are used to coordinate transitions between secure and non-secure media states.

Use the **stcapp register capability** command to specify modem transport method for secure calls.

Use the **modem relay sprt v14 receive playback hold-time** command to configure V.14 receive parameters for Simple Packet Relay Transport (SPRT) protocol packets in V.150.1 modem relay mode.

Use the **modem relay sprt v14 transmit hold-time** and **modem relay sprt v14 transmit maximum hold-count** commands to configure SPRT transmit parameters in V.150.1 modem relay mode.

Use the **mgcp modem relay voip mode sse** command to enable secure V.150.1 modem relay calls on trunk-side or non-STCAPP-enabled gateways. Use the **mgcp modem relay voip mode nse** command to enable non-secure modem-relay mode; by default, NSE modem-relay mode is disabled.

Examples

The following example shows SSE parameters configured to support secure calls between IP-STE and STE endpoints:

```
Router(config-voi-serv)
# modem relay sse redundancy interval 20
Router(config-voi-serv)
# modem relay sse redundancy packet 4
Router(config-voi-serv)
# modem relay sse retries 5
Router(config-voi-serv)
# modem relay sse t1 1000
Router(config-voi-serv)
# modem relay sse v150mer
```

Related Commands

Command	Description
mgcp package-capability mdste	Enables MGCP gateway support for processing events and signals for modem connections over a secure communication path between IP-STE and STE.
modem relay sprt v14 receive playback hold-time	Configures SPRT parameters.
modem relay sprt v14 transmit hold-time	Configures SPRT transmit parameters.
modem relay sprt v14 transmit maximum hold-count	Configures SPRT transmit parameters.
modem relay sprt v14 transmit maximum hold-count	Configures SPRT transmit parameters.
stcapp register capability	Configures the modem transport method for a specified device registered with Cisco CallManager.
voice service voip	Enters voice service configuration mode for VoIP encapsulation.

monitor call application event-log

To display the event log for an active application instance in real-time, use the **monitor call application event-log**command in privileged EXEC mode.

monitor call application event-log [{**app-tag** *application-name* {**last** | **next**} | **session-id** *session-id* [{**stop**}] | **stop**}]

Syntax Description

app-tag *application-name*	Displays event log for the specified application.
last	Displays event log for the most recent active instance.
next	Displays event log for the next active instance.
session-id *session-id*	Displays event log for specific application instance.
stop	(Optional) Stops the monitoring session.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command enables dynamic event logging so that you can view events as they happen for active application instances. You can view the most recent active instance or the next new instance of a specified application, or the specified active application instance, or it stops the display. To display event logs with this command, you must enable either the **call application event-log** command or the**call application voice event-log** command.

Examples

The following example displays the event log for the next active session of the application named sample_app:

```
Router# monitor call application event-log app-tag generic last

5:1057278146:172:INFO: Prompt playing finished successfully.
5:1057278151:173:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057278151:174:INFO: Script received event = "noinput"
5:1057278151:175:INFO: Playing prompt #1: tftp://172.19.139.145/audio/ch_welcome.au
5:1057278158:177:INFO: Prompt playing finished successfully.
5:1057278163:178:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057278163:179:INFO: Script received event = "noinput"
5:1057278163:180:INFO: Playing prompt #1: tftp://172.19.139.145/audio/ch_welcome.au
5:1057278170:182:INFO: Prompt playing finished successfully.
5:1057278175:183:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057278175:184:INFO: Script received event = "noinput"
5:1057278175:185:INFO: Playing prompt #1: tftp://172.19.139.145/audio/ch_welcome.au
5:1057278181:187:INFO: Prompt playing finished successfully.
5:1057278186:188:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057278186:189:INFO: Script received event = "noinput"
5:1057278186:190:INFO: Playing prompt #1: tftp://172.19.139.145/audio/ch_welcome.au
```

Related Commands

Command	Description
call application event-log	Enables event logging for voice application instances.
call application voice event-log	Enables event logging for a specific voice application.

monitor call leg event-log

To display the event log for an active call leg in real-time, use the **monitor call leg event-log**command in privileged EXEC mode.

monitor call leg event-log {**leg-id** *leg-id* [**stop**] | **next** | **stop**}

Syntax Description

leg-id *leg-id*	Displays the event log for the identified call leg.
next	Displays the event log for the next active call leg.
stop	(Optional) Stops the monitoring session.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command enables dynamic event logging so that you can view events as they happen for active voice call legs. You can view the event log for the next new call leg, or the specified active call leg, or it stops the display. To display event logs with this command, you must enable the **call leg event-log** command.

Examples

The following is sample output from the **monitor call leg event-log next** command showing the event log for the next active call leg after a PSTN incoming call was made to the gateway:

```
Router# monitor call leg event-log next
2B:1058571679:992:INFO: Call setup indication received, called = 4085550198,  calling =
52927, echo canceller = enable, direct inward dialing
2B:1058571679:993:INFO: Dialpeer = 1
2B:1058571679:998:INFO: Digit collection
2B:1058571679:999:INFO: Call connected using codec None
2B:1058571688:1007:INFO: Call disconnected (cause = normal call clearing (16))
2B:1058571688:1008:INFO: Call released
```

Related Commands

Command	Description
call leg event-log	Enables event logging for voice, fax, and modem call legs.

monitor event-trace voip ccsip

To configure event tracing for Voice over IP (VoIP) Session Initiation Protocol (SIP) events, use the **monitor event-trace voip ccsip** command in global configuration mode. To disable event tracing, use the **no** form of this command.

monitor event-trace voip ccsip *trace-type*
size *number*
no monitor event-trace voip ccsip *trace-type*

Syntax Description

trace-type	The type of trace.
size *number*	(Optional) The number of events of the specific types that are stored for a specific instance. The range is from 1 to 1000000. The default value depends on the trace-type setting.

Command Default

Event tracing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Use the **monitor event-trace voip ccsip** command to enable or disable event tracing. The table below shows the valid values for *trace-type* argument.

Trace Type	Description
api	Use this keyword to configure event tracing for the VoIP CCSIP subsystem API events. These events are interactions between the SIP subsystem and other subsystems.
fsm	Use this keyword to configure event tracing for VoIP CCSIP Finite State Machine (FSM) and CNFSM events. These messages provide information on the status of various state transitions.
global	Use this keyword to configure event tracing for VoIP CCSIP global events. Global events are all events that occur outside of a call context.
misc	Use this keyword to configure event tracing for VoIP CCSIP miscellaneous events. These messages provide information about invoked features.

Trace Type	Description
msg	Use this keyword to configure event tracing for VoIP CCSIP message events. These messages provide information about the SIP messages that are sent and received by the Cisco Unified Border Element (Cisco UBE).

Use the **size** keyword to set the number of events of the specific types that are stored for this instance. If the number of events increases beyond this size earlier events are overwritten. If you do not set a value for size, the system uses the default value for the specified trace-type, as follows:

- **api**—50
- **fsm**—100
- **global**—100
- **misc**—50
- **msg**—50

Note The amount of data collected from the trace depends on the trace buffer size configured using the **monitor event-trace voip ccsip** command for each instance of a trace.

Example

The following example shows how to enable event tracing for different event types in the VoIP CCSIP subsystem component in Cisco IOS software:

```
Device# configure terminal
Device(config)# monitor event-trace voip ccsip api size 50
Device(config)# monitor event-trace voip ccsip fsm size 100
Device(config)# monitor event-trace voip ccsip global size 100
Device(config)# monitor event-trace voip ccsip misc size 50
Device(config)# monitor event-trace voip ccsip msg size 50
```

monitor event-trace voip ccsip (EXEC)

To monitor and control the event trace function for Voice Over IP (VoIP) Call-Control Session Initiation Protocol (CCSIP), use the **monitor event-trace voip ccsip** command is privileged EXEC mode.

monitor event-trace voip ccsip {**all** | **api** | **fsm** | **global** | **history** | **misc** | **msg**} {**clear** | **disable** | **dump** [**filter** {**call-id** | **called-num** | **calling-num** | **sip-call-id**} *filter-value*] [**pretty**] | **enable**}

Syntax Description

all	Event tracing for API, Finite State Machine (FSM) and Communicating Nested FSM (CNFSM), miscellaneous and message VoIP CCSIP events.
api	Event tracing for VoIP CCSIP API events.
fsm	Event tracing for VoIP CCSIP FSM and CNFSM events.
global	Event tracing for VoIP CCSIP global events.
history	Specifies that event traces are not deleted until the maximum limit is reached. When the maximum limit is reached, the oldest history trace is deleted to capture event-trace for new call.
misc	Event tracing for VoIP CCSIP miscellaneous events.
msg	Event tracing for VoIP CCSIP message events.
clear	Clears all captured VoIP CCSIP event traces.
disable	Turns off VoIP CCSIP event tracing.
dump	Writes the event trace results to the file configured with the global configuration **monitor event-trace voip ccsip dump-file** command. The traces are saved in binary format.
filter	(Optional) Filters the traces written to the file configured with the global configuration **monitor event-trace voip ccsip dump-file** command.
call-id *filter-value*	Filters the traces written to the file configured with the global configuration **monitor event-trace voip ccsip dump-file** command based on the specified call ID.
called-num *filter-value*	Filters the traces written to the file configured with the global configuration **monitor event-trace voip ccsip dump-file** command based on the specified called number.
calling-num *filter-value*	Filters the traces written to the file configured with the global configuration **monitor event-trace voip ccsip dump-file** command based on the specified calling number.

sip-call-id *filter-value*	Filters the traces written to the file configured with the global configuration **monitor event-trace voip ccsip dump-file** command based on the specified SIP call ID.
pretty	(Optional) Dumps the event trace message in ASCII format.
enable	Turns on VoIP CCSIP event tracing, if it has been configured in global configuration mode.

Command Default

Event tracing is disabled, except for history.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Use the **monitor event-trace voip ccsip** command to control what, when, and how event trace data is collected. Use this command after you have configured the event trace functionality on the networking device using the **monitor event-trace voip ccsip** command in global configuration mode.

Note The amount of data collected from the trace depends on the trace buffer size configured using the **monitor event-trace voip ccsip dump-file** command in global configuration mode for each instance of a trace.

Use the **show monitor event-trace voip ccsip** command to display traces. Use the **monitor event-trace voip ccsip dump filter** command to save trace message information for specific events.

By default, trace information is saved in binary format. If you want to save traces in ASCII format, possibly for additional application processing, use the **monitor event-trace voip ccsip dump pretty** command.

To write the event traces that are in the buffer to a file (secondary storage), enter the **monitor event-trace voip ccsip** *trace-type* **dump** command. To configure the file where you want to save trace information, use the **monitor event-trace voip ccsip dump-file** command in global configuration mode. By default, the event traces are saved in a binary format.

Example

The following example shows the command for writing traces for an event in ASCII format:

```
Device# monitor event-trace voip ccsip all dump pretty
```

The following shows how to stop event tracing, clear the current contents of memory, and re-enable the trace function for the VoIP CCSIP component. The **all** keyword indicates that these instructions apply to API, FSM, CNFSM, miscellaneous and message events. This example assumes that the tracing function is configured and enabled on the networking device:

```
Device# monitor event-trace voip ccsip all disable
Device# monitor event-trace voip ccsip all clear
Device# monitor event-trace voip ccsip all enable
```

monitor event-trace voip ccsip api

To configure event tracing for Voice over IP (VoIP) application programming interface (API) events, use the **monitor event-trace voip ccsip api** command in global configuration mode. To disable API event tracing, use the **no** form of the command.

monitor event-trace voip ccsip api [**size** *number*]
no monitor event-trace voip ccsip api [**size** *number*]

Syntax Description

size *number*	(Optional) The number of API events that are stored for a specific connection (call leg). The range is from 1 to 1000000. The default value is 50.

Command Default

API event tracing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.
15.3(3)S	This command was integrated into Cisco IOS Release 15.3(3)S.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Usage Guidelines

This command configures event tracing for the VoIP CCSIP subsystem API events. These events are interactions between the Session Initiation Protocol (SIP) subsystem and other subsystems.

Use the **size** keyword to set the number of events that are stored for this instance. If the number of events increases beyond this size, earlier events are overwritten. If you do not set a value for size, the system uses the default value.

Example

The following example shows how to enable event tracing for API events in the VoIP CCSIP subsystem component in Cisco IOS software:

```
Device(config)# monitor event-trace voip ccsip api size 50
```

monitor event-trace voip ccsip dump

To specify the options to automatically dump or store event tracing messages for Voice over IP (VoIP) Session Initiation Protocol (SIP) events, use the **monitor event-trace voip ccsip dump** command in global configuration mode. To stop event tracing messages being written to the dump file, use the **no** form of this command.

monitor event-trace voip ccsip dump {**all** | **marked** | **none**}
no monitor event-trace voip ccsip dump

Syntax Description

all	Specifies that all event trace messages are written to the specified location upon completion of the call or call-leg.
marked	Cisco Unified Border Element (Cisco UBE) has identified specific internal errors, and the traces are dumped only if any of these errors occur.
none	Specifies that event trace messages are not to be automatically written to the specified location.

Command Default

Event trace messages are not automatically dumped.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Use this command to specify an automatic policy based on which VoIP CCSIP event tracing messages are written to the dump file.

Note Use the **monitor event-trace voip ccsip dump-file** command to set the dump location. Without a valid dump-file configuration, neither manual dumps nor automatic dumps will function.

Example

The following examples show how to specify that only marked event trace messages are written to the dump file:

```
Device(config)# monitor event-trace voip ccsip
dump-file slot0:ccsip-dump-file
```

```
Device(config)# monitor event-trace voip ccsip dump-file
ftp://username:password@server_ip//path/ccsip-dump-file
Device(config)# monitor event-trace voip ccsip dump-file
tftp://server_ip//path/ccsip-dump-file
```

monitor event-trace voip ccsip dump-file

To specify the file where event trace messages are written from memory on the networking device, use the **monitor event-trace voip ccsip dump-file** command in global configuration mode.

monitor event-trace voip ccsip dump-file *file-name*
no monitor event-trace voip ccsip dump-file

Syntax Description

file-name	The name of the file where event trace messages are written.

Command Default

Dump file is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Use this command to specify the file to which event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters, and the path can point to flash memory on the networking device or to a TFTP or FTP server.

To make the filename unique for different calls a unique identifier is added after a file-name for each dump. If there is a filename length restriction on the storage device you must ensure that the length of the filename you specify plus the unique identifier string does not exceed the allowable filename length.

Note Without a valid dump-file configuration, neither manual dumps nor automatic dumps will function.

Example

The following example shows how to set the trace messages file to ccsip-dump-file in slot0 (flash memory) and to remote servers:

```
Device(config)# monitor event-trace voip ccsip dump-file slot0:ccsip-dump-file
Or
Device(config)# monitor event-trace voip ccsip dump-file
ftp://username:password@server_ip//path/ccsip-dump-file
Or
Device(config)# monitor event-trace voip ccsip dump-file
tftp://server_ip//path/ccsip-dump-file.txt
```

monitor event-trace voip ccsip fsm

To configure event tracing for Voice over IP (VoIP) CCSIP Finite State Machine (FSM) and communicating nested FSM (CNFSM) events, use the **monitor event-trace voip ccsip fsm** command in global configuration mode. To disable FSM and CNFSM event tracing, use the **no** form of the command.

monitor event-trace voip ccsip fsm [**size** *number*]
no monitor event-trace voip ccsip fsm [**size** *number*]

Syntax Description

size *number*	(Optional) The number of FSM events that are stored for a specific connection (call leg). The range is from 1 to 1000000. The default value is 100.

Command Default

FSM event tracing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.
15.3(3)S	This command was integrated into Cisco IOS Release 15.3(3)S.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Usage Guidelines

Event messages for VoIP CCSIP FSM and CNFSM events provide information on the status of various state transitions.

Use the **size** keyword to set the number of events that are stored for this instance. If the number of events increases beyond this size, earlier events are overwritten. If you do not set a value for size, the system uses the default value.

Example

The following example shows how to enable event tracing for FSM and CNFSM events in the VoIP CCSIP subsystem component in Cisco IOS software:

```
Device(config)# monitor event-trace voip ccsip fsm size 100
```

monitor event-trace voip ccsip global

To configure event tracing for Voice over IP (VoIP) global events, use the **monitor event-trace voip ccsip global** command in global configuration mode. To disable global event tracing, use the **no** form of the command.

monitor event-trace voip ccsip global [**size** *number*]
no monitor event-trace voip ccsip global [**size** *number*]

Syntax Description

size *number*	(Optional) The number of global events that are stored. The range is from 1 to 1000000. The default value is 100.

Command Default

Global event tracing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.
15.3(3)S	This command was integrated into Cisco IOS Release 15.3(3)S.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Usage Guidelines

Global events are all events that occur outside of a call context.

Use the **size** keyword to set the number of events that are stored. If the number of events increases beyond this size, earlier events are overwritten. If you do not set a value for size, the system uses the default value.

Example

The following example shows how to enable event tracing for global events in the VoIP CCSIP subsystem component in Cisco IOS software:

```
Device(config)# monitor event-trace voip ccsip global size 100
```

monitor event-trace voip ccsip limit

To limit the resources used by the event tracing mechanism, use the **monitor event-trace voip ccsip limit** command in global configuration mode. To remove any resource limits, use the **no** form of this command.

monitor event-trace voip ccsip limit {**connections** *max-connections* | **memory** *size*}
no monitor event-trace voip ccsip limit

Syntax Description

connections *max-connections*	Specifies the maximum number of calls that can be traced. The range is from 1 to 1000. The default is 1000 simultaneous call-legs.
memory *size*	Specifies the maximum memory that can be used by the event tracing mechanism. The range is from 1 to 1000 MB.

Command Default

The maximum number of call-legs that can be traced is 1000.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Use this command to control the amount of resources used by the event tracing mechanism. The limits can be applied based on the maximum call-leg allowed or the maximum memory that can be used by the event tracing mechanism. The event tracing mechanism will operate within the set limits. If the limit is reached, the system will first try to reuse memory reclaimed from the history. If this is not possible, then subsequent event traces are not captured.

Note If the **no** form of this command is configured, it can impact the resources available for calls, and can also impact the call density on the device.

Example

The following examples shows how to configure a maximum connections limit of 500 connections:

```
Device(config)# monitor event-trace voip ccsip limit connections 500
```

monitor event-trace voip ccsip misc

To configure event tracing for Voice over IP (VoIP) CCSIP miscellaneous events, use the **monitor event-trace voip ccsip misc** command in global configuration mode. To disable miscellaneous-event tracing, use the **no** form of the command.

monitor event-trace voip ccsip misc [**size** *number*]
no monitor event-trace voip ccsip misc [**size** *number*]

Syntax Description

size *number*	(Optional) The number of miscellaneous events that are stored for a specific connection (call leg). The range is from 1 to 1000000. The default value is 50.

Command Default

Miscellaneous event tracing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.
15.3(3)S	This command was integrated into Cisco IOS Release 15.3(3)S.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Usage Guidelines

Miscellaneous event messages provide information about invoked features.

Use the **size** keyword to set the number of events that are stored for this instance. If the number of events increases beyond this size, earlier events are overwritten. If you do not set a value for size, the system uses the default value.

Example

The following example shows how to enable event tracing for miscellaneous events in the VoIP CCSIP subsystem component in Cisco IOS software:

```
Device(config)# monitor event-trace voip ccsip misc size 50
```

monitor event-trace voip ccsip msg

Use this keyword to configure event tracing for VoIP CCSIP message events. These messages provide information about theSession Initiation Protocol (SIP) messages that are sent and received by the Cisco Unified Border Element (Cisco UBE).

To configure event tracing for Voice over IP (VoIP) CCSIP message events, use the **monitor event-trace voip ccsip msg** command in global configuration mode. To disable message-event tracing, use the **no** form of the command.

monitor event-trace voip ccsip msg [**size** *number*]
no monitor event-trace voip ccsip msg [**size** *number*]

Syntax Description

size *number*	(Optional) The number of message events that are stored for a specific connection (call leg). The range is from 1 to 1000000. The default value is 50.

Command Default

Message event tracing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.
15.3(3)S	This command was integrated into Cisco IOS Release 15.3(3)S.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Usage Guidelines

VoIP CCSIP message events provide information about the SIP messages that are sent and received by the Cisco Unified Border Element (Cisco UBE).

Use the **size** keyword to set the number of events that are stored for this instance. If the number of events increases beyond this size, earlier events are overwritten. If you do not set a value for size, the system uses the default value.

Example

The following example shows how to enable event tracing for message events in the VoIP CCSIP subsystem component in Cisco IOS software:

```
Device(config)# monitor event-trace voip ccsip msg size 50
```

monitor event-trace voip ccsip stacktrace

To enable stack traces at trace points, and to specify the depth of the stack trace stored, use the **monitor event-trace voip ccsip stacktrace** command in global configuration mode. To stop stack traces at trace points, use the **no** form of this command.

monitor event-trace voip ccsip stacktrace *number*
no monitor event-trace voip ccsip stacktrace

Syntax Description

number	The depth of the stack trace stored. Valid values are from 1 to 12.

Command Default

Stack trace at trace points is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Use this command to enable stack trace at tracepoint and to configure the stack trace depth.

Example

The following example shows how to enable stack traces at trace points and to specify a stack trace depth of 9:

```
Device(config)# monitor event-trace voip ccsip stacktrace 9
```

monitor probe icmp-ping

To enable dial-peer status changes based on the results of probes from Internet Control Message Protocol (ICMP) pings, use the **monitor probe icmp-ping** command in dial-peer configuration mode. To disable this capability, use the **no** form of this command.

monitor probe [{**icmp-ping** | **rtr**}] [*ip-address*]
no monitor probe [{**icmp-ping** | **rtr**}] [*ip-address*]

Syntax Description

icmp-ping	(Optional) Specifies ICMP ping as the method for monitoring the destination target and updating the status of the dial peer.
rtr	(Optional) Specifies that the Response Time Reporter (RTR) probe is the method for monitoring the destination target and updating the status of the dial peer.
ip -address	(Optional) The destination IP address of a target interface for the probe signal.

Command Default

If this command is not entered, no ICMP or RTR probes are sent.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(11)T	This command was introduced in a release earlier than Cisco IOS Release 12.2(11)T.

Usage Guidelines

The principal use of this command is to specify ICMP ping as the probe method, even though the option for selecting RTR is also available.

In order for the **monitor probe icmp-ping** command to work properly, the **call fallback icmp-ping** command or the **call fallback active** command must be configured. One of these two commands must be in effect before the **monitor probe icmp-ping** command can be used.

If the **call fallback icmp-ping** command is not entered, the **call fallback active** command in global configuration is used for measurements. If the **call fallback icmp-ping** command is entered, these values override the global configuration.

Examples

The following example shows how to configure a probe to use ICMP pings to monitor the connection to IP address 10.1.1.1:

```
dial-peer voice tag voip
 call fallback icmp-ping
 monitor probe icmp-ping 10.1.1.1
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion and specifies the type of probe for pings to IP destinations.

Command	Description
call fallback icmp-ping	Specifies ICMP ping as the method for network traffic probe entries to IP destinations and configures parameters for the ping packets.
show voice busyout	Displays information about the voice busyout state.
voice class busyout	Creates a voice class for local voice busyout functions.

mrcp client accept-charset-compliance

To set the format of the Media Resource Control Protocol (MRCP) client as per RFC 2616, use the **mrcp client accept-charset-compliance** command in global configuration mode.

mrcp client accept-charset-compliance

Syntax Description

This command has no arguments or keywords.

Command Default

The default character set is **Accept-charset: charset: utf-8**.

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS XE Fuji Release 16.8.1	This command was introduced.

Usage Guidelines

In a Cisco Voice Portal (CVP), the VXML gateway communicates with Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) servers using MRCP. Communication between the gateway and the ASR servers fails when the character set negotiation is incorrect.

The current character set, **Accept-Charset: charset: utf-8**, results in MRCP error on the VXML gateway. To resolve the MRCP error, use the command **mrcp client accept-charset-compliance** on the VXML gateway in global configuration mode. This command resets the character set as **Accept-charset: utf-8**, which is as per RFC 2616.

Examples

The following example sets the character set as per RFC 2616.

```
Router (config)# mrcp client accept-charset-compliance
```

mrcp client codec

To set the codec for communication between MRCP (Media Resource Control Protocol) client and the media processing resources such as Automatic Speech-Recognition (ASR) engines and Text-To-Speech (TTS) engines, use the **mrcp client codec** command in global configuration mode. To set the MRCP codec to the default g711ulaw, use the **no** form of this command.

mrcp client codec g711alaw
no mrcp client codec g711alaw

Syntax Description

g711alaw	Sets the audio codec for the MRCP client.

Command Default

Audio codec g711ulaw

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS XE Fuji Release 16.8.1	This command was introduced.

Usage Guidelines

Audio codecs determine VoIP call quality.The default MRCP client codec is g711ulaw. Use this command to set the audio codec g711alaw for the MRCP client.

Examples

The following example sets the audio codec g711alaw for the MRCP client.

```
Router (config)# mrcp client codec g711alaw
```

mrcp client rtpsettup enable

To enable the sending of an IP address in the Real Time Streaming Protocol (RTSP) SETUP message, use the **mrcp client rtpsettup enable** command in global configuration mode. To disable sending of the IP address, use the **no** form of this command.

mrcp client rtpsettup enable
no mrcp client rtpsettup enable

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to enable the sending of IP address in the RTSP SETUP message:

```
Router# configure terminal
Router(config)# mrcp client rtpsetup enable
```

Related Commands

Command	Description
show mgcp	Displays values for MGCP parameters.

mrcp client session history duration

To set the maximum number of seconds for which history records for Media Resource Control Protocol (MRCP) sessions are stored on the gateway, use the **mrcp client session history duration**command in global configuration mode. To reset to the default, use the **no** form of this command.

mrcp client session history duration *seconds*
no mrcp client session history duration

Syntax Description

seconds	Maximum time, in seconds, for which MRCP history records are stored. Range is from 0 to 99999999. The default is 3600 (1 hour). If 0 is configured, no MRCP records are stored on the gateway.

Command Default

3600 seconds (1 hour)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	This command was modified to support MRCP version 2 (MRCP v2).

Usage Guidelines

This command affects the number of records that are displayed when the **show mrcp client session history** command is used.

Active MRCP sessions are not affected by this command.

Examples

The following example sets the maximum amount of time for which MRCP history records are stored to 2 hours (7200 seconds):

```
Router(config)# mrcp client session history duration 7200
```

Related Commands

Command	Description
show mrcp client session history	Displays information about past MRCP client sessions that are stored on the gateway.

mrcp client session history records

To set the maximum number of records of Media Resource Control Protocol (MRCP) client history that the gateway can store, use the **mrcp client session history records** command in global configuration mode. To reset to the default, use the **no** form of this command.

mrcp client session history records *number*
no mrcp client session history records

Syntax Description

number	Maximum number of MRCP history records to save. The maximum value is platform-specific. The default is 50. If 0 is configured, no MRCP records are stored on the gateway.

Command Default

50 records

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	This command was modified to support MRCP version 2 (MRCP v2).

Usage Guidelines

This command affects the number of records that are displayed when the **show mrcp client session history** command is used.

Active MRCP sessions are not affected by this command.

Examples

The following example sets the maximum number of MRCP records to 30:

```
Router(config)# mrcp client history records 30
```

Related Commands

Command	Description
show mrcp client session history	Displays information about past MRCP client sessions that are stored on the gateway.

mrcp client session nooffailures

To configure the maximum number of consecutive failures before disconnecting calls, use the **mrcp client session nooffailures** command in global configuration mode. To disable the number of consecutive failures before disconnecting calls, use the **no** form of this command.

mrcp client session nooffailures *number*
no mrcp client session nooffailures

Syntax Description

number	Maximum number of consecutive failures before disconnecting calls. The range is from 1 to 50. The default is 20.

Command Default

The maximum number is set to 20.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure the maximum number of consecutive failures before disconnecting calls:

```
Router# configure terminal
Router(config)# mrcp client session nooffailures 20
```

Related Commands

Command	Description
show mgcp	Displays values for MGCP parameters.

mrcp client statistics enable

To enable Media Resource Control Protocol (MRCP) client statistics to be displayed, use the **mrcp client statistics enable**command in global configuration mode. To disable display, use the **no** form of this command.

mrcp client statistics enable
no mrcp client statistics enable

Syntax Description

This command has no arguments or keywords.

Command Default

MRCP client statistics are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	This command was modified to support MRCP version 2 (MRCP v2).

Usage Guidelines

This command enables MRCP client statistics to be displayed when the **show mrcp client statistics hostname** command is used. If this command is not enabled, client statistics cannot be displayed for any host when the **show mrcp client statistics hostname** command is used.

Examples

The following example enables MRCP statistics to be displayed:

```
Router(config)# mrcp client statistics enable
```

Related Commands

Command	Description
show mrcp client statistics hostname	Displays statistics about MRCP sessions for a specific MRCP host.

mrcp client timeout connect

To set the number of seconds allowed for the router to establish a TCP connection to a Media Resource Control Protocol (MRCP) server, use the **mrcp client timeout connect**command in global configuration mode. To reset to the default, use the **no** form of this command.

mrcp client timeout connect *seconds*
no mrcp client timeout connect

Syntax Description

seconds	Amount of time, in seconds, the router waits to connect to the server before timing out. Range is 1 to 20.

Command Default

3 seconds

Command Modes

Global configuration (global)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(15)T	This command was modified to support MRCP version 2 (MRCP v2).

Usage Guidelines

This command determines when the router abandons its attempt to connect to an MRCP server and declares a timeout error, if a connection cannot be established after the specified number of seconds.

Examples

The following example sets the connection timeout to 10 seconds:

```
Router(config)# mrcp client timeout connect 10
```

mrcp client timeout message

To set the number of seconds that the router waits for a response from a Media Resource Control Protocol (MRCP) server, use the **mrcp client timeout message**command in global configuration mode. To reset to the default, use the **no** form of this command.

mrcp client timeout message *seconds*
no mrcp client timeout message

Syntax Description

seconds	Amount of time, in seconds, the router waits for a response from the server after making a request. Range is 1 to 20.

Command Default

3 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(15)T	This command was modified to support MRCP version 2 (MRCP v2).

Usage Guidelines

This command sets the amount of time the router waits for the MRCP server to respond to a request before declaring a timeout error.

Examples

The following example sets the request timeout to 10 seconds:

```
Router(config)# mrcp client timeout message 10
```

mta receive aliases

To specify a hostname accepted as a Simple Mail Transfer Protocol (SMTP) alias for off-ramp faxing, use the **mta receive aliases**command in global configuration mode. To disable the alias, use the **no** form of this command.

mta receive aliases *string*
no mta receive aliases *string*

Syntax Description

string	Hostname or IP address to be used as an alias for the SMTP server. If you specify an IP address to be used as an alias, you must enclose the IP address in brackets as follows: [xxx.xxx.xxx.xxx]. Default is the domain name of the gateway.

Command Default

Enabled with an empty string

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

This command creates an accept or reject alias list. The first alias is used by the mailer to identify itself in SMTP banners and when generating its own RFC 822 Received: header.

Note This command does not automatically include reception for a domain IP address; the address must be explicitly added. To explicitly add a domain IP address, use the following format: **mta receive aliases** [*ip-address*] . Use the IP address of the Ethernet or the FastEthernet interface of the off-ramp gateway.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example specifies the host name "seattle-fax-offramp.example.com" as the alias for the SMTP server:

```
mta receive aliases seattle-fax-offramp.example.com
```

The following example specifies IP address 172.16.0.0 as the alias for the SMTP server:

```
mta receive aliases [172.16.0.0]
```

Related Commands

Command	Description
mta receive generate -mdn	Specifies that the off-ramp gateway process a response MDN from an SMTP server.
mta receive maximum -recipients	Specifies the maximum number of recipients for all SMTP connections.

mta receive disable-dsn

To stop the generation and delivery of a Delivery Status Notification (DSN) every time a failure occurs in a T.37 offramp call from a Cisco IOS gateway, use the **mta receive disable-dsn** command in global configuration mode. To restart the generation and delivery of DSNs when failures occur, use the **no** form of this command.

mta receive disable-dsn
no mta receive disable-dsn

Syntax Description

This command has no arguments or keywords.

Command Default

By default, this command is not enabled, and a DSN message is generated from the gateway each time a T.37 offramp call fails.

Command Modes

Global configuration

Command History

Release	Modification
12.4(13)	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The T.37 offramp gateway generates DSN messages when calls are successful and when calls fail. The **mta receive disable-dsn** command disables the generation and delivery of DSN messages for successful calls and for failed calls.

A DSN message confirming a successful call is a useful notification tool with no negative impact on processing. However, when a T.37 offramp call is made from a Cisco IOS gateway, and the call fails (ring but no answer), the gateway automatically generates a DSN for each failure. The DSN is based on the Simple Mail Transport Protocol (SMTP) error (which is temporary), so the SMTP client tries to resend the fax every 5 minutes for up to 24 hours. These multiple DSNs eventually overload the sender's inbox.

Examples

The following example shows how to disable the generation and sending of DSNs from the offramp gateway:

```
mta receive disable-dsn
```

Related Commands

Command	Description
debug fax mta	Troubleshoots the fax mail transfer agent.
mta receive generate	Specifies the type of fax delivery response message that a T.37 fax off-ramp gateway should return.

mta receive generate

Note The **mta receive generate** command replaces the **mta receive generate-mdn** command.

To specify the type of fax delivery response message that a T.37 fax off-ramp gateway should return, use the **mta receive generate** command in global configuration mode. To return to the default, use the **no** form of this command.

mta receive generate [{**mdn** | **permanent-error**}]
no mta receive generate [{**mdn** | **permanent-error**}]

Syntax Description

mdn	Optional. Directs the T.37 off-ramp gateway to process response message disposition notifications (MDNs) from an Simple Mail Transfer Protocol (SMTP) server.
permanent-error	Optional. Directs the T.37 off-ramp fax gateway to classify all fax delivery errors as permanent so that they are forwarded in DSN messages with descriptive error codes to an mail transfer agent (MTA).

Command Default

MDNs are not generated and standard SMTP status messages are returned to the SMTP client with error classifications of permanent or transient.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced as **mta receive generate-mdn**.
12.0(4)T	The **mta receive generate-mdn** command was integrated into Cisco IOS Release 12.0(4)T.
12.3(7)T	The **mta receive generate-mdn** command was replaced by the **mta receive generate** command, which uses the **mdn** and **permanent-error**keywords.

Usage Guidelines

When the **mdn** keyword is used to enable MDN on a sending device, a flag is inserted in the off-ramp message e-mail header, requesting that the receiving device generate an MDN. The MDN is then returned to the sender when the e-mail message that contains the fax image is opened. Use this command to enable the receiving device--the off-ramp gateway--to process the response MDN.

Depending on the configuration, usage, and features of the mailers used at a site, it might be desirable to enable or disable MDN generation. Specifications for MDN are described in RFC 2298. Delivery status notification (DSN) generation cannot be disabled.

The **permanent-error** keyword directs the T.37 off-ramp fax gateway to classify all fax delivery errors as permanent so that they are forwarded in a DSN with descriptive error codes to the originating MTA. The descriptive error codes allow the MTA to control fax operations directly because the MTA can examine the error codes and make decisions about how to proceed with each fax (whether to retry or cancel, for example).

If this command is not used, the default is to return standard SMTP status messages to SMTP clients using both permanent and transient error classifications.

Examples

The following example allows a T.37 off-ramp gateway to process response MDNs:

```
Router(config)# mta receive generate mdn
```

The following example directs a T.37 off-ramp gateway to classify all fax delivery errors as permanent and forward the errors and descriptive text using SMTP DSNs to the MTA:

```
Router(config)# mta receive generate permanent-error
```

Related Commands

Command	Description
mdn	Requests that a message disposition notification be generated when a fax-mail message is processed (opened).
mta receive aliases	Specifies a host name that is accepted as an SMTP alias for off-ramp faxing.
mta receive generate-mdn	Specifies that the off-ramp gateway process a response MDN from an SMTP server.
mta receive maximum-recipients	Specifies the maximum number of recipients for all SMTP connections.

mta receive generate-mdn

> **Note** The **mta receive generate-mdn** command was replaced by the **mta receive generate** command in Cisco IOS Release 12.3(7)T.

To specify that the off-ramp gateway process a response message disposition notification (MDN) from a Simple Mail Transfer Protocol (SMTP) server, use the **mta receive generate-mdn**command in global configuration mode. To disable MDN generation, use the **no** form of this command.

mta receive generate-mdn
no mta receive generate-mdn

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

When MDN is enabled on a sending device, a flag is inserted in the off-ramp message e-mail header, requesting that the receiving device generate the MDN and return that message to the sender when the e-mail message that contains the fax image is opened. Use this command to enable the receiving device--the off-ramp gateway--to process the response MDN.

Depending on the configuration, usage, and features of the mailers used at a site, it might be desirable to enable or disable MDN generation. Specifications for MDN are described in RFC 2298. Delivery status notification (DSN) generation cannot be disabled.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example enables the receiving device to generate MDNs:

```
mta receive generate-mdn
```

Related Commands

Command	Description
mdn	Requests that a message disposition notification be generated when the fax-mail message is processed (opened).
mta receive aliases	Specifies a host name accepted as an SMTP alias for off-ramp faxing.
mta receive maximum -recipients	Specifies the maximum number of recipients for all SMTP connections.

mta receive maximum-recipients

To specify the maximum number of simultaneous recipients for all Simple Mail Transfer Protocol (SMTP) connections, use the **mta receive maximum-recipients**command in global configuration mode. To reset to the default, use the **no** form of this command.

mta receive maximum-recipients *number*
no mta receive maximum-recipients

Syntax Description

number	Maximum number of simultaneously recipients for all SMTP connections. Range is from 0 to 1024. The default is 0.

Command Default

0 recipients

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Use thiscommand to configure the maximum number of resources that you want to allocate for fax usage at any one time. You can use this command to limit the resource usage on the gateway. When the value for the *number*argument is set to 0, no new connections can be established. Which is particularly useful when one is preparing to shut down the system.

This command applies to off-ramp store-and-forward fax functions.

The default of 0 recipients means that incoming mail messages are not accepted; therefore, no faxes are sent by the off-ramp gateway.

Note Unless the transmitting mailer supports the X-SESSION SMTP service extension, each incoming SMTP connection is allowed to send to only one recipient and thus consume only one outgoing voice feature card (VFC).

Examples

The following example sets the maximum number of simultaneous recipients for all SMTP connections to 10:

```
mta receive maximum-recipients 10
```

Related Commands

Command	Description
mta receive aliases	Specifies a host name accepted as an SMTP alias for off-ramp faxing.
mta receive generate -mdn	Specifies that the off-ramp gateway process a response MDN from an SMTP server.

mta send filename

To specify a filename for a TIFF file attached to an e-mail, use the mta send filename command in global configuration mode. To disable the configuration after the command has been used, use the **no** form of this command.

mta send filename [*string*] [**date**]
no mta send filename

Syntax Description

string	(Optional) Name of the TIFF file attached to an e-mail. If this text string does not contain an extension for the filename, ".tif" is added to the formatted filename.
date	(Optional) Adds today's date in the format yyyymmdd to the filename of the TIFF attachment.

Command Default

The formatted filename for TIFF attachments is "Cisco_fax.tif"

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use this command to specify the filename for a TIFF file attached to an e-mail.

Examples

The following example specifies a formatted filename of "abcd.tif" for the TIFF attachment:

```
Router(config)# mta send filename abcd
```

The following example specifies a formatted filename and extension of "abcd.123" for the TIFF attachment:

```
Router(config)# mta send filename abcd.123
```

The following example specifies a formatted filename "abcd_today's date" (so, for July 4, 2002, the filename would be "abcd_20020704.tif") for the TIFF attachment:

```
Router(config)# mta send filename abcd date
```

The following example specifies a formatted filename and extension of "abcd_today's date.123" (so, for July 4, 2002, the filename would be "abcd_20020704.123") for the TIFF attachment:

```
Router(config)# mta send filename abcd.123 date
```

Related Commands

Command	Description
mta send origin-prefix	Adds information to an e-mail prefix header.

Command	Description
mta send postmaster	To which an e-mail message should be delivered. Specifies the mail server postmaster account to which if it cannot be delivered to the intended destination.
mta send return-receipt-to	Specifies the address to which MDNs are sent.
mta send server	Specifies a destination mail server or servers.
mta send subject	Specifies the subject header of an e-mail message.

mta send mail-from

To specify a mail-from address (also called the RFC 821 envelope-from address or the return-path address), use the **mta send mail-from**command in global configuration mode. To remove this return-path information, use the **no** form of this command.

mta send mail-from {**hostname** *string* | **username** *string* | **username s**}
no mta send mail-from {**hostname** *string* | **username** *string* | **username s**}

Syntax Description

hostname *string*	Simple Mail Transfer Protocol (SMTP) host name or IP address. If you specify an IP address, you must enclose the IP address in brackets as follows: [xxx.xxx.xxx.xxx].
username *string*	Sender username.
username s	Wildcard that specifies that the username is derived from the calling number.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Use this command to designate the sender of the fax TIFF attachment, which is equivalent to the return path in an e-mail message. If the mail-from address is blank, the postmaster address, configured with the **mta send postmaster** command, is used.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example specifies that the mail-from username information is derived from the calling number of the sender:

```
mta send mail-from username $s$
```

Related Commands

Command	Description
mta send origin-prefix	Adds information to an e-mail prefix header.
mta send postmaster	To which an e-mail message should be delivered. Specifies the mail server postmaster account to which if it cannot be delivered to the intended destination.
mta send return-receipt-to	Specifies the address to which MDNs are sent.
mta send server	Specifies a destination mail server or servers.
mta send subject	Specifies the subject header of an e-mail message.

mta send origin-prefix

To add information to an e-mail prefix header, use the **mta send origin-prefix**command in global configuration mode. To remove the defined string, use the **no** form of this command.

mta send origin-prefix *string*
no mta send origin-prefix *string*

Syntax Description

string	Text string to add comments to the e-mail prefix header. If this string contains more than one word, the string value should be enclosed within quotation marks ("abc xyz").

Command Default

Null string

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Store-and-forward fax provides the slot and port number from which an e-mail comes. In the e-mail prefix header information, use this command to define a text string to be added to the front of the e-mail prefix header information. This text string is a prefix string that is added with the modem port and slot number and passed in the originator_comment field of the esmtp_client_engine_open() call. Eventually, this text ends up in the received header field of the fax-mail message; for example:

```
Received (test onramp Santa Cruz slot1 port15) by router-5300.cisco.com for
<test-test@cisco.com> (with Cisco NetWorks); Fri, 25 Dec 1998 001500 -0800
```

Using the command **mta send origin-prefix dog** causes the received header to contain the following information:

```
Received (dog, slot 3 modem 8) by as5300-sj.example.com ....
```

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example adds information to the e-mail prefix header:

```
mta send origin-prefix "Cisco-Powered Fax System"
```

Related Commands

Command	Description
mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
mta send postmaster	To which an e-mail message should be delivered. Specifies the mail server postmaster account to which if it cannot be delivered to the intended destination.
mta send return-receipt-to	Specifies the address to which MDNs are sent.
mta send server	Specifies a destination mail server or servers.
mta send subject	Specifies the subject header of an e-mail message.

mta send postmaster

To specify the mail server postmaster account to which an e-mail message should be delivered if it cannot be delivered to the intended destination, use the **mta send postmaster**command in global configuration mode. To remove the specification, use the **no** form of this command.

mta send postmaster *e-mail-address*
no mta send postmaster *e-mail-address*

Syntax Description

e -mail-address	Address of the mail server postmaster account to which an e-mail message should be delivered if it cannot be delivered to its intended destination.

Command Default

No e-mail destination is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

If you have configured a router to generate delivery status notifications (DSNs) and message disposition notifications (MDNs), but you have not configured the sender information (using the **mta send mail-from** command) or the Simple Mail Transfer Protocol (SMTP) server, DSNs and MDNs are delivered to the e-mail address determined by this command.

It is recommended that an address such as "fax-administrator@example.com" be used to indicate fax responsibility. In this example, fax-administrator is aliased to the responsible person. At some sites, this could be the same person as the e-mail postmaster, but most likely is a different person with a different e-mail address.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example configures the e-mail address "fax-admin@example.com" as the sender for all incoming faxes. Thus, any returned DSNs are delivered to "fax-admin@example.com" if the mail-from field is blank.

```
mta send postmaster fax-admin@example.com
```

Related Commands

Command	Description
mta send mail -from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
mta send origin -prefix	Adds information to an e-mail prefix header.
mta send return -receipt-to	Specifies the address to which where MDNs are sent.
mta send server	Specifies a destination mail server or servers.
mta send subject	Specifies the subject header of an e-mail message.

mta send return-receipt-to

To specify the address to which message disposition notifications (MDNs) are sent, use the **mta send return-receipt-to**command in global configuration mode. To remove the address, use the **no** form of this command.

mta send return-receipt-to {**hostname** *string* | **username** *string* | **s**}
no mta send return-receipt-to {**hostname** *string* | **username** *string* | **s**}

Syntax Description

hostname *string*	Simple Mail Transfer Protocol (SMTP) host name or IP address where MDNs are sent. If you specify an IP address, you must enclose the IP address in brackets as follows: [xxx.xxx.xxx.xxx].
username *string*	Username of the sender to which MDNs are to be sent.
s	Wildcard that specifies that the calling number (ANI) generates the disposition-notification-to e-mail address.

Command Default

No address is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Use this command to specify where you want MDNs to be sent after a fax-mail is opened.

Note Store-and-forward fax supports the Eudora proprietary format, meaning that the header that store-and-forward fax generates is in compliance with RFC 2298 (MDN).

Note Multimedia Mail over IP (MMoIP) dial peers must have MDN enabled in order to generate return receipts in off-ramp fax-mail messages.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example configures "xyz" as the user and "server.com" as the SMTP mail server to which MDNs are sent:

```
mta send return-receipt-to hostname server.com
mta send return-receipt-to username xyz
```

Related Commands

Command	Description
mta send mail -from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
mta send origin -prefix	Adds information to the e-mail prefix header.
mta send postmaster	To which an e-mail message should be delivered. Specifies the mail server postmaster account to which if it cannot be delivered to the intended destination.
mta send server	Specifies a destination mail server or servers.
mta send subject	Specifies the subject header of an e-mail message.

mta send server

To specify a destination mail server or servers, use the **mta send server**command in global configuration mode. To remove the specification, use the **no** form of this command.

mta send server {*host nameip-address*}
no mta send server {*host nameip-address*}

Syntax Description

hostname	Hostname of the destination mail server.
ip -address	IP address of the destination mail server.

Command Default

IP address defined as 0.0.0.0

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Use this command to provide a backup destination server in case the first configured mail server is unavailable. This command is not intended to be used for load distribution.

You can configure up to ten different destination mail servers using this command. If you configure more than one destination mail server, the router attempts to contact the first mail server configured. If that mail server is unavailable, it contacts the next configured destination mail server.

DNS mail exchange (MX) records are not used to look up host names provided to this command.

Note When you use thiscommand, configure the router to perform name lookups using the **ip name-server** command.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example defines the mail servers "xyz.example.com" and "abc.example.com" as the destination mail servers:

```
mta send server xyz.example.com
mta send server abc.example.com
```

Related Commands

Command	Description
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
mta send origin-prefix	Adds information to the e-mail prefix header.
mta send postmaster	Specifies the mail-server postmaster account to which an e-mail message should be delivered if it cannot be delivered to the intended destination.
mta send return-receipt-to	Specifies the address to which MDNs are sent.
mta send subject	Specifies the subject header of an e-mail message.

mta send success-fax-only

To configure the router to send only successful fax messages and drop failed fax messages, use the **mta send success-fax-only** command in global configuration mode. To disable this functionality, use the **no** form of this command.

mta send success-fax-only
no mta send success-fax-only

Syntax Description

This command has no arguments or keywords.

Command Default

The router is configured to send all fax messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure the router to send only successful fax messages drop failed fax messages:

```
Router# configure terminal
Router(config)# mta send success-fax-only
```

Related Commands

Command	Description
mta send origin-prefix	Adds information to an e-mail prefix header.
mta send postmaster	Specifies the mail server postmaster account to which an e-mail message should be delivered if it cannot be delivered to the intended destination.

mta send subject

To specify the subject header of an e-mail message, use the **mta send subject**command in global configuration mode. To remove the string, use the **no** form of this command.

mta send subject *string*
no mta send subject *string*

Syntax Description

string	Subject header of an e-mail message.

Command Default

Null string

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

This command applies to on-ramp store-and-forward fax functions.

Note The string does not have to be enclosed in quotation marks.

Examples

The following example defines the subject header of an e-mail message as "fax attachment":

```
mta send subject fax attachment
```

Related Commands

Command	Description
mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
mta send origin-prefix	Adds information to an e-mail prefix header.

Command	Description
mta send postmaster	To which an e-mail message should be delivered. Specifies the mail server postmaster account to which if it cannot be delivered to the intended destination.
mta send return-receipt-to	Specifies the address to which MDNs are sent.
mta send server	Specifies a destination mail server or servers.

mta send with-subject

To configure the subject attached with called or calling numbers, use the **mta send with-subject** command in global configuration mode. To disable the subject attached with called or calling numbers, use the **no** form of this command.

mta send with-subject {**d** | **s** | **both**}
no mta send with-subject

Syntax Description

d	Configures the subject attached with called number.
s	Configures the subject attached with calling number.
both	Configures the subject attached with both called and calling numbers.

Command Default

The subject is not attached with the calling or called numbers.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **mta send with-subject both** command instructs the router to include the calling and called party number in the "Subject:" line of the e-mail. This helps to route the fax e-mail to the appropriate mailbox.

Examples

The following example shows how to include the calling and the called party number in the "Subject:" line of the e-mail:

```
Router# configure terminal
Router(config)# mta send with-subject both
```

Related Commands

Command	Description
mta send origin-prefix	Adds information to an e-mail prefix header.
mta send postmaster	Specifies the mail server postmaster account to which an e-mail message should be delivered if it cannot be delivered to the intended destination.
mta send server	Specifies a destination mail server or servers.

music-threshold

To specify the threshold for on-hold music for a specified voice port, use the **music-threshold**command in voice-port configuration mode. To disable this feature, use the **no** form of this command.

music-threshold *decibels*
no music-threshold *decibels*

Syntax Description

decibels	On-hold music threshold, in decibels (dB). Range is from -70 to -10 (integers only). The default is -38 dB.

Command Default

-38 dB

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(4)T	This command was implemented on the Cisco MC3810.
12.3(4)XD	The range of values for the *decibels*argument was increased.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.

Usage Guidelines

Use thiscommand to specify the decibel level of music played when calls are put on hold. This command tells the firmware to pass steady data above the specified level. It affects the operation of voice activity detection (VAD) only when the voice port is receiving voice.

If the value for this command is set too high, VAD interprets music-on-hold as silence, and the remote end does not hear the music. If the value for this command is set too low, VAD compresses and passes silence when the background is noisy, creating unnecessary voice traffic.

Examples

The following example sets the decibel threshold to -35 for the music played when calls are put on hold:

```
voice port 0:D
 music-threshold -35
```

The following example sets the decibel threshold to -35 for the music played when calls are put on hold on a Cisco 3600 series router:

```
voice-port 1/0/0
```

music-threshold -35

mwi

To enable message-waiting indication (MWI) for a specified voice port, use the **mwi**command in voice-port configuration mode. To disable MWI for a specified voice port, use the **no** form of this command.

mwi
no mwi

Syntax Description

This command has no arguments or keywords.

Command Default

MWI is disabled by default.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **mwi** command to enable MWI functionality on the voice port and the **mwi-server** command to configure the voice-mail server to send MWI notifications. If the voice port does not have MWI enabled, the voice gateway returns a 481 Call Leg/Transaction Does Not Exist message to the voice-mail server. If there are multiple dial peers associated with the same FXS voice port, multiple subscriptions are sent to the voice-mail server.

Examples

The following example shows MWI set on a voice port.

```
voice-port 2/2
 cptone us
 mwi
```

Related Commands

Command	Description
mwi-server	Specifies voice-mail server settings on a voice gateway or UA.

mwi (supplementary-service)

To set the type of message waiting indication (MWI) when a voicemail is available, use the **mwi** command in supplementary-service configuration mode. To return to the default setting, use the **no** form of this command.

mwi {**audible** | **visible** | **both**}
no mwi

Syntax Description

audible	Audible message waiting indication (AMWI) is enabled.
visible	Visible message waiting indication (VMWI) is enabled.
both	Default configuration. Both AMWI and VMWI are enabled.

Command Default

Both AMWI and VMWI are enabled by default.

Command Modes

Supplementary-service configuration (config-stcapp-suppl-serv)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **mwi** command to enable MWI as audible only (AMVI), visible only (VMWI), or both (AMVI/VMWI).

When a voicemail is available, you go offhook to hear a special AMWI tone or you go onhook to see an MWI light (when the phone is equipped with one).

Examples

The following example shows how to set the type of MWI on voice ports 2/1, 2/2, and 2/3:

```
Router(config)# stcapp supplementary-services
Router(config-stcapp-suppl-serv)# port 2/1
Router(config-stcapp-suppl-serv-port)# fallback-dn 3001
Router(config-stcapp-suppl-serv)# port 2/2
Router(config-stcapp-suppl-serv-port)# fallback-dn 3102
Router(config-stcapp-suppl-serv-port)# mwi visible
Router(config-stcapp-suppl-serv)# port 2/3
Router(config-stcapp-suppl-serv-port)# fallback-dn 3203
Router(config-stcapp-suppl-serv-port)# mwi audible
```

Related Commands

Command	Description
stcapp supplementary-services	Enters supplementary-service configuration mode for configuring STCAPP supplementary-service features on an FXS port.

mwi-server

To specify voice-mail server settings on a voice gateway or user agent (UA), use the **mwi-server** command in SIP user-agent configuration mode. To reset to the default, use the **no** form of this command.

mwi-server {**ipv4:***destination-address* | **dns:***host-name*} [{**expires** *seconds*}] [{**port** *port*}] [{**transport** {**tcp** | **udp**}}] [{**unsolicited**}]
no mwi-server

Syntax Description

ipv4: *destination -address*	IP address of the voice-mail server.
dns: *host -name*	Host device housing the domain name server that resolves the name of the voice-mail server. • *host -name* --String that contains the complete host name to be associated with the target address; for example, **dns:test.cisco.com**.
expires *seconds*	(Optional) Subscription expiration time, in seconds. The range is 1 to 999999. The default is 3600.
port *port*	(Optional) Defines the port number on the voice-mail server. The default is 5060.
transport {**tcp** | **udp**	(Optional) Defines the transport protocol to the voice-mail server. Choices are **tcp** or **udp**. UDP is the default.
unsolicited	(Optional) Requires the voice-mail server to send a SIP notification message to the voice gateway or UA if the mailbox status changes. Removes the requirement that the voice gateway subscribe for MWI service.

Command Default

Voice-mail server settings are disabled by default.

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Using the **mwi-server** command a user can request that the UA subscribe to a voice-mail server requesting notification of mailbox status. When there is a status change, the voice-mail server notifies the UA. The UA then indicates to the user that there is a change in mailbox status with an MWI tone when the user takes the phone off-hook.

Only one voice-mail server can be configured per voice gateway. Use the **mwi-server** command with the **mwi** command to enable MWI functionality on the voice port. If the voice port does not have MWI enabled, the voice gateway returns a 481 Call Leg/Transaction Does Not Exist message to the voice-mail server. MWI status is always reset after a router reload.

Examples

The following example specifies voice-mail server settings on a voice gateway. The example includes the **unsolicited** keyword, enabling the voice-mail server to send a SIP notification message to the voice gateway or UA if the mailbox status changes.

```
sip-ua
 mwi-server dns:test.cisco.com expires 60 port 5060 transport udp unsolicited
```

For unsolicited Notify, the Contact header derives the voice-mail server address. If the unsolicited MWI message does not contain a Contact header, configure the voice-mail server on the gateway with the following special syntax to accept MWI Notify messages.

```
sip-ua
 mwi-server ipv4:255.255.255.255 unsolicited
```

Related Commands

Command	Description
mwi	Enables MWI for a specified voice port.
sip-us	Enables SIP user-agent configuration mode.
voice-port	Enters voice-port configuration mode.

N

name (dial peer cor custom)

To specify the name for a custom class of restrictions (COR), use the **name** command in dial peer COR custom configuration mode. To remove a specified COR, use the **no** form of this command.

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

Syntax Description

class-name	Name that describes the specific COR.

Command Default

No default behavior or values.

Command Modes

Dial peer COR custom configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

The **dial-peer cor custom** and **name** commands define the names of capabilities on which to apply COR operation. Examples of names might include any of the following: call1900, call527, call9, or call 911. You must define the capabilities before you specify the COR rules.

You can define a maximum of 64 COR names.

Examples

The following example defines three COR names:

```
dial-peer cor custom
 name 900_call
 name 800_call
 name catchall
```

Related Commands

Command	Description
dial-peer cor custom	Specifies that named CORs apply to dial peers.
name	Assigns a name to the internal adapter.

nat (sip-ua)

To use the SIP Network Address Translation (NAT) global configuration, use the **nat** command in SIP user agent configuration mode. To disable the **nat** configuration, use the **no** or **default** form of this command.

nat auto { **force-on** | **force-off** }
no nat

auto	Sets the symmetric NAT endpoint role to auto. Autodetect subscriber in a remote subnet when located behind a NAT.
force-on	Sets the symmetric NAT endpoint role to force-on. Assume that all remote subscribers are behind the NAT device.

Command Modes

SIP user agent configuration (sip-ua)

Voice class tenant configuration (config-class)

Voice service SIP configuration (conf-serv-sip)

Release	Modification
12.2(13)T	This command was introduced.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Examples

The following example shows how to set the endpoint role in connection setup to active:

```
Router(config)# sip-ua
Router(config-sip-ua)# nat auto
```

```
Router(config)# sip-ua
Router(config-sip-ua)# nat force-on
```

Related Commands

Command	Description
nat symmetric check-media-src	Enables source media checking for symmetric NAT.

nat media-keepalive

To enable media keepalive packets transmission for the specified interval of time (in seconds) at tenant or global level, use the **nat media-keepalive** command in voice class tenant configuration (config-class) or voice service SIP configuration (conf-serv-sip) mode. To disable the **nat** configuration, use the **no** or **default** form of this command.

nat { **auto** | **force-on** | **media-keepalive** [*interval*] }
no nat
default nat

Syntax Description

media-keepalive	Specifies media keepalive to subscriber if it's located behind NAT.
interval	Specifies keepalive interval configured in seconds. Range is 1—50. Default is 10.

Command Default

If no value is specified, default interval value is set to 10.

Command Modes

Voice class tenant configuration (config-class)

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
Cisco IOS XE 17.13.1a Cisco IOS XE Dublin 17.12.2	This command was introduced.

Examples

The following example shows how to configure media keepalive at global level:

```
Device(config)# voice service voip
Device(config-voi-serv)# sip
Device(config-serv-sip)# nat media-keepalive 20
```

The following example shows how to configure media keepalive at tenant level:

```
Device(config)# voice class tenant 1
Device(config-class)# nat media-keepalive 35
```

nat symmetric check-media-src

To enable the gateway, to check the media source of incoming Real-time Transport Protocol (RTP) packets in symmetric Network Address Translation (NAT) environments, use the **nat symmetric check-media-src** command in SIP user agent configuration mode. To disable media source checking, use the **no** form of this command.

nat symmetric check-media-src
no nat symmetric check-media-src

Syntax Description

This command has no arguments or keywords.

Command Default

Media source checking is disabled.

Command Modes

SIP user agent configuration (sip-ua)

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command provides the ability to enable or disable symmetric NAT settings for the Session Initiation Protocol (SIP) user agent. Use the **nat symmetric check-media-src command to configure the gateway to check the media source address and port of the first incoming**RTP **packet. Checking for media packets is automatically enabled if the gateway receives the direction role "active or both".**

Examples

The following example enables checking the media source:

```
Router(config)# sip-ua
Router(config-sip-ua)# nat symmetric check-media-src
```

Related Commands

Command	Description
nat symmetric role	Defines endpoint settings to initiate or accept a connection for symmetric.

nat symmetric role

To define endpoint settings to initiate or accept a connection for symmetric Network Address Translation (NAT) configuration, use the **nat symmetric role** command in SIP user agent configuration mode. To disable the **nat symmetric role**configuration, use the **no** form of this command.

nat symmetric role {**active** | **passive**}
no nat symmetric role {**active** | **passive**}

Syntax Description

active	Sets the symmetric NAT endpoint role to active, originating an outgoing connection.
passive	Sets the symmetric NAT endpoint role to passive, accepting an incoming connection to the port number on the m=line of the Session Description Protocol (SDP) body sent from the SDP body to the other endpoint.

Command Default

The endpoint settings to initiate or accept connections for NAT configuration are not defined..

Command Modes

SIP user agent configuration (sip-ua)

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command provides the ability to specify symmetric NAT endpoint settings for the SIP user agent. If the gateway does not receive the direction role, use the nat symmetric role command to define endpoint settings to initiate or accept a connection for symmetric NAT configuration. This is achieved by setting the symmetric NAT endpoint role to active or passive , respectively. Cisco recommends that you use the nat symmetric role command under the following conditions:

- Endpoints are aware of their presence inside or outside of NAT
- Endpoints parse and process direction:<role> in SDP

If the endpoints conditions are not satisfied, you may not achieve the desired results when you configure the **nat symmetric role command.**

Examples

The following example shows how to set the endpoint role in connection setup to active:

```
Router(config)# sip-ua
Router(config-sip-ua)# nat symmetric role active
```

Related Commands

Command	Description
nat symmetric check-media-src	Enables source media checking for symmetric NAT.

neighbor (annex g)

To configure the neighboring border elements (BEs) that interact with the local BE for the purpose of obtaining addressing information and aiding in address resolution, enter the **neighbor** command in Annex G configuration mode. To reset the default value, use the no form of this command.

neighbor *ip-address*
no neighbor

Syntax Description

ip -address	IP address of the neighbor that is used for exchanging Annex G messages.

Command Default

No default behavior or values

Command Modes

Annex G configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Examples

The following example configures a neighboring BE that has an IP address and border element ID:

```
Router(config)# call-router h323-annexg be20
Router(config-annexg)# neighbor 121.90.10.42
Router(config-annexg-neigh)# id be30
Router(config-annexg-neigh)# exit
```

Related Commands

Command	Description
advertise	Controls the types of descriptors that the BE advertises to its neighbors.
call -router	Enables the Annex G border element configuration commands.
id	Configures the local ID for the neighboring BE.
port	Configures the port number of the neighbor that is used for exchanging Annex G messages.
query -interval	Configures the interval at which the local BE will query the neighboring BE.

neighbor (tgrep)

To create a TGREP session with another device, use the neighbor command in TGREP configuration mode. To disable a TRIP connection, use the **no** form of this command.

neighbor ip_address
no neighbor ip_address

Syntax Description

ip_address	IP address of a peer device with which TGREP information will be exchanged.

Command Default

No neighboring devices are defined

Command Modes

TGREP configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example shows that the gateway with the IP address 192.116.56.10 is defined as a neighbor for ITAD 1234:

```
Router(config)# tgrep local-itad 1234
Router(config-tgrep)# neighbor 192.116.56.10
```

Related Commands

Command	Description
tgrep local - itad	Enters TGREP configuration mode and defines an ITAD.

network-clock base-rate

To configure the network clock base rate for universal I/O serial ports 0 and 1, use the **network-clock base-rate** command in global configuration mode. To disable the current network clock base rate, use the no form of this command.

network-clock base-rate {**56k** | **64k**}
no network-clock base-rate {**56k** | **64k**}

Syntax Description

56k	Sets the network clock base rate to 56 kbps.
64k	Sets the network clock base rate to 64 kbps.

Command Default

56 kbps

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command applies to Voice over Frame Relay and Voice over ATM.

Examples

The following example sets the network clock base rate to 64 kbps:

```
network-clock base-rate 64k
```

Related Commands

Command	Description
network -clock-select	Uses the network clock source to provide timing to the system backplane PCM bus.
network -clock-switch	Configures the switch delay time to the next priority network clock source when the current network clock source fails.

network-clock-participate

To allow the ports on a specified network module or voice/WAN interface card (VWIC) to use the network clock for timing, use the **network-clock-participate** command in global configuration mode. To restrict the device to use only its own clock signals, use the **no** form of this command.

network-clock-participate [{**slot** *slot-number* | **wic** *wic-slot* | **aim** *aim-slot-number*}]
no network-clock-participate [{**nm** *slot* | **wic** *wic-slot*}]

Syntax Description

slot *slot -number*	(Optional) Network module slot number on the router chassis. Valid values are from 1 to 6.
wic *wic -slot*	Configures the WAN interface card (WIC) slot number on the router chassis. Valid values are 0 or 1.
aim *aim -slot-number*	Configures the Advanced Integration Module (AIM) in the specified slot. The aim-slot-number values are 0 or 1 for the Cisco 3660 and 0 or 1 for the Cisco 3725, and Cisco 3745.

Command Default

No network clocking is enabled, and interfaces are restricted to using the clocking generated on their own modules.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 3660.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	The **slot** keyword was replaced by the **nm** keyword and the **wic** keyword and the *wic-slot*argument were added.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T with support for the Cisco 3660, Cisco 3725, and Cisco 3745. Clocks can be synchronized on two ports. The **aim** keyword was added. The **nm** keyword was replaced by the **slot** keyword.
12.4(15)T9	This command was integrated into Cisco IOS Release 12.4(15)T9, and support was added for the NM-CEM-4SER modules.

Usage Guidelines

This command is used for ATM segmentation and reassembly or digital signal processing and Cisco 3660, Cisco 3725, and Cisco 3745 routers.

This command applies to any network module with T1/E1 controllers to provide clocks from a central source (MIX module for the Cisco 3660) to the network module and to the port on the network module. Then that port can be selected as the clock source with the **network-clock-select** command to supply clock to other ports or network modules that choose to participate in network clocking with the **network-clock-participate** command. This command synchronizes the clocks for two ports.

On the Cisco 3700 series, you must use the **network-clock-participate** command and either the **wic** *wic-slot*keyword and argument or the **slot** *slot-number* keyword and argument.

Note If the AIM takes its clock signals from a T1 or E1 controller, it is mandatory to use the **network-clock-select** and **network-clock-participate** commands for ATM. The clocks for the ATM and voice interfaces do not need to be synchronous, but improved voice quality may result if they are.

Note The only VWICs that can participate in network clocking are digital T1/E1 packet voice trunk network modules (NM-HDV), and Fast Ethernet network modules (NM-2W, NM-1FE. and NM-2FE).

Note Beginning with Cisco IOS Release 12.4(15)T9, the **network-clock-participate** command can also be used for the NM-CEM-4SER modules. When the **network-clock-participate** command is configured, the clock is derived from the backplane. When the **no network-clock-participate** command is configured, the local oscillator clock is used.

Examples

The following example configures the network module in slot 5 to participate in network clocking on a Cisco 3660 with a MIX module:

```
network-clock-participate slot 5
network-clock-select 1 e1
```

The following example on a Cisco 3700 series router specifies that the AIM participates in network clocking and selects port E1 0/1 to provide the clock signals.

```
Router(config)# network-clock-participate wic 0
Router(config)# network-clock-participate aim 0
Router(config)# network-clock-select 2 E1 0/1
```

The following example on a Cisco 3660 specifies the slot number that participates in network clocking and selects port E1 5/0:

```
Router(config)# network-clock-participate slot 5
Router(config)# network-clock-select 1 E1 5/0
```

Related Commands

Command	Description
network-clock-select	Specifies selection priority for the clock sources.
network-clock-source	Selects the port to be the clock source to supply clock resources to other ports or network modules.

network-clock select

To name a source to provide timing for the network clock and to specify the selection priority for this clock source, use the **network-clock select** command in global configuration mode. To cancel the network clock selection, use the **no** form of this command.

Cisco ASR 1000 Series

network-clock select {*priority* [{**bits** [{**R0** | **R1**}] {**e1** [{**crc4** | **no-crc4** | **unframed**}] | **t1** [{**esf** | **sf** | **unframed**}]} | **controller** *type number* | **global** | **interface** *type number* | **local** | **system**}] | **option** {**1** | **2**}}

no network-clock select *priority* [{**global** | **local**}]

Cisco 7600 Series and Cisco 10000 Series

network-clock select *priority* {**controller** *type number* | **interface** *type number* | **slot** *number* | **system**} [{**global** | **local**}]

no network-clock select *priority* [{**global** | **local**}]

Syntax Description

priority	Selection priority for the clock source (1 is the highest priority). The range is 1 to 6. The clock with the highest priority is selected to drive the system time division multiplexing (TDM) clocks. When the higher-priority clock source fails, the next-higher-priority clock source is selected.
bits	(Optional) Derives network timing from the central office (CO) Building Integrated Timing Supply (BITS) clock.
R0	(Optional) Specifies Route Processor 0 BITS as the source slot.
R1	(Optional) Specifies Route Processor 1 BITS as the source slot.
e1	(Optional) Configures the BITS interface to use an E1 connection.
crc4	(Optional) Configures the E1 BITS interface framing with Cyclic Redundancy Check 4 (CRC4).
no-crc4	(Optional) Configures the E1 BITS interface framing with no CRC4.
unframed	(Optional) Configures the BITS interface with clear channel.
t1	(Optional) Configures the BITS interface to use a T1 connection.
esf	(Optional) Configures the T1 BITS interface with the Extended Super Frame (ESF) framing standard.
sf	(Optional) Configures the T1 BITS interface with the Super Frame (SF) framing standard.
controller *type number*	Specifies the controller to be the clock source.
interface *type number*	Specifies the interface to be the clock source.

slot *number*	Specifies the slot to be the clock source. The range is 1 to 6.
global	(Optional) Configures the source as global.
local	(Optional) Configures the source as local.
system	Specifies the system clock as the clock source.
option	Specifies the standards for the network option. The applicable values are as follows: • 1—Network option I is the ITU G-813 standard. • 2—Network option II (Gen1) is the Bellcore GR-1244/GR-253 (stratum 3) and ITU G-813 standard. This is the default value. **Note** The network options are available only in the RP2 platform.

Command Default

The router uses the system clock (also called free-running mode).

Note Because default clock values are derived from an external source, they can fall outside the configurable range.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3 MA	This command was introduced on the Cisco MC3810.
12.0(3)XG	The BVM as a possible network clock source was added.
12.1(5)XM	This command was implemented on the Cisco 3660. The keywords **t1** and **e1** were introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	This command was implemented on the Cisco 2600 series and Cisco 3660 with AIMs installed.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)T	This command was implemented on the Cisco 2600XM, Cisco 2691, Cisco 3725, and Cisco 3745.
12.3(8)T4	This command was integrated into Cisco IOS Release 12.3(8)T4 and the **bri**keyword was added. Support was also added for the Cisco 2800 series.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and the **atm**keyword was added. Support was also added for the Cisco 3800 series.
Cisco IOS XE Release 2.1	This command was introduced in a release earlier than Cisco IOS Release 2.1.
15.0(1)S	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)S.

Release	Modification
Cisco IOS XE Release 3.1	This command was modified. This command was implemented on the Cisco ASR 1000 platform. The **option** keyword was added.

Usage Guidelines

When an active clock source fails, the system chooses the next-lower-priority clock source that is specified by this command. When a higher-priority clock source becomes available, the system automatically reselects it.

You can specify up to five clock priorities. The highest-priority active interface in the router supplies the primary reference source to all other interfaces that require network clock synchronization services.

For timing sources, the Route Processor can receive timing information through its BITS interface or through a TDM-based Shared Port Adapter (SPA). For some telecommunications deployments, BITS clocking is required to provide global clocking synchronization of network equipment in the end-to-end data path. A BITS clock can be supplied to the network clock module using a T1 or E1 connection.

If a controller is specified in the clock source hierarchy, you must configure that controller for line timing (by using the appropriate **clock source line** command for the controller). Any controller that is not currently acting as the clock source will automatically operate in loop timing mode. Both controllers can be given different clock source priority values. For more information, see the Cisco IOS Interface and Hardware Component Command Reference .

Note To minimize backplane clock shifts, the **no network-clock select** command does not take effect until you return to EXEC mode by entering **exit** or **end**. This process minimizes the number of times that clock sources are configured.

Use the **show network-clocks** command to display clock priorities that are configured on the router.

Examples

The following example shows how to configure the network clock as revertive and assign clock sources to two priorities:

```
Router> enable
Router# configure terminal
Router(config)# network-clock revertive
Router(config)# network-clock select 1 bits R0 e1
Router(config)# network-clock select 2 interface GigabitEthernet 0/0/1
```

The following example shows how to configure the network option for network clock.

Router(config)# **network-clock select option 1**

Related Commands

Command	Description
network-clock-participate	Configures a network module to participate in network clocking.
network-clock-switch	Configures the switch delay time to the next-priority network clock source when the current network clock source fails or a higher-priority clock source is up and available.
show network-clocks	Displays the network clock configuration and current primary clock source.

network-clock-switch

To configure the switch delay time to the next priority network clock source when the current network clock source fails, use the **network-clock-switch** command in global configuration mode. To cancel the network clock delay time selection, use the no form of this command.

network-clock-switch [{*switch-delay* | **never**}] [{*restore-delay* | **never**}]
no network-clock-switch

Syntax Description

switch -delay	(Optional) Delay time, in seconds, before the next-priority network clock source is used when the current network clock source fails. Range is from 0 to 99. Default is 10.
never	(Optional) No delay time before the current network clock source recovers.
restore -delay	(Optional) Delay time, in seconds, before the current network clock source recovers. Range is from 0 to 99.
never	(Optional) No delay time before the next-priority network clock source is used when the current network clock source fails.

Command Default

10 seconds

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command applies to Voice over Frame Relay and Voice over ATM.

Examples

The following example switches the network clock source after 20 seconds and sets the delay time before the current network clock source recovers to 20 seconds:

```
network-clock-switch 20 20
```

Related Commands

Command	Description
network -clock-select	Uses the network clock source to provide timing to the system backplane PCM bus.

noisefloor

To configure the noise level, in dBm, above which noise reduction (NR) will operate, use the **noisefloor** command in media profile configuration mode. To disable the configuration, use the **no** form of this command.

noisefloor *level*
no noisefloor *level*

Syntax Description

level	Minimum noise level in dBm. The range is from -58 to -20.

Command Default

The default value is -48 dBm.

Command Modes

Media profile configuration (cfg-mediaprofile)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.2(3)T	This command was modified. Support for the Cisco Unified Border Element (Cisco UBE) was added.

Usage Guidelines

Use the **noisefloor** command to configure the noise level, in dBm, above which noise reduction (NR) will operate. NR will allow noises quieter than this level to pass without processing. You must create a media profile for noise reduction and then configure the noise level. Signal levels start at 0 dBm (extremely loud) and quieter levels are more negative. The default value of -48 dBm is very quiet.

Examples

The following example shows how to create a media profile to configure noise reduction parameters:

```
Device> enable
Device# configure terminal
Device(config)# media profile nr 200
Device(cfg-mediaprofile)# noisefloor -50
Device(cfg-mediaprofile)# end
```

Related Commands

Command	Description
intensity	The intensity or depth of the noise reduction process.
media profile nr	Creates a media profile to configure noise reduction parameters.

non-linear

To enable nonlinear processing (NLP) in the echo canceller and set its threshold or comfort-noise attenuation, use the **non-linear** command in voice-port configuration mode. To disable nonlinear processing, use the **no** form of this command.

non-linear [{**comfort-noise attenuation** {**0db** | **3db** | **6db** | **9db**} | **threshold** *dB*}]
no non-linear [{**comfort-noise attenuation** | **threshold**}]

Syntax Description

0db | **3db** | **6db** | **9db**	(Optional) Attenuation level of the comfort noise in dB. Default is **0db**, which means that comfort noise is not attenuated.
threshold *dB*	(Optional) Sets the threshold in dB. Range is -15 to -45. Default is -21. **Note** This keyword is not supported when using the extended G.168 echo canceller.

Command Default

NLP is enabled; comfort-noise attenuation is disabled; threshold is -21 dB.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced.
12.2(11)T	The **threshold** keyword was added.
12.2(13)T	This command was implemented on routers that support the extended G.168 echo canceller.
12.3(6)	The **comfort-noise** keyword was added.
12.4	The default setting for comfort-noise attenuation was changed from 0db to 6db.

Usage Guidelines

This command enables functionality that is also generally known as residual echo suppression. Use this command to shut off any signal if no near-end speech is detected. Enabling this command normally improves performance, although some users might perceive truncation of consonants at the end of sentences when this command is enabled.

Use the **comfort-noise** keyword if the comfort noise generated by the NLP sounds like hissing. Using this keyword makes the hissing sound less audible. The default setting for comfort-noise attenuation is 6db to achieve the highest satisfaction in voice quality.

Note The **echo-cancel enable** command must be enabled for this command to take effect.

Examples

The following example enables nonlinear call processing on a Cisco 3600 series router:

```
voice-port 1/0/0
 non-linear
```

The following example sets the attenuation level to 9 dB on a Cisco 3600 series router:

```
voice-port 1/0/0
 non-linear comfort-noise attenuation 9db
```

Related Commands

Command	Description
echo -cancel enable	Enables echo cancellation for voice that is sent and received on the same interface.

notify (MGCP profile)

To specify the order in which automatic number identification (ANI) and dialed number identification service (DNIS) digits are reported to the Media Gateway Control Protocol (MGCP) call agent, use the **notify**command in MGCP profile configuration mode. To revert to the default, use the **no** form of this command.

notify {**ani-dnis** | **dnis-ani**}
no notify {**ani-dnis** | **dnis-ani**}

Syntax Description

ani-dnis	ANI digits are sent in the first notify message, followed by DNIS. This is the default.
dnis-ani	DNIS digits are sent in the first notify message, followed by ANI.

Command Default

The default order is ANI first and DNIS second.

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

This command controls the order of ANI and DNIS when using the Feature Group D (FGD) Exchange Access North American (EANA) protocol on a T1 interface. Selecting the **ani-dnis** keyword causes the ANI digits to be sent in the first NTFY message to the MGCP call agent and the DNIS digits to be sent in a second NTFY message. Selecting the **dnis-ani** keyword causes the DNIS digits to be sent in the first NTFY message to the MGCP call agent and the ANI digits to be sent in a second NTFY message.

Examples

The following example sets the digit order to DNIS first and ANI second for the default MGCP profile:

```
Router(config)# mgcp profile default
Router(config-mgcp-profile)# notify dnis-ani
```

Related Commands

Command	Description
mgcp package-capability	Specifies an MGCP package capability type for a media gateway.
mgcp profile	Defines an MGCP profile to be associated with one or more MGCP endpoints
show mgcp	Displays MGCP configuration information.
show mgcp profile	Displays information for MGCP profiles.

notify redirect

To enable application handling of redirect requests for all VoIP dial peers on a Cisco IOS voice gateway, use the **notify redirect**command in voice service VoIP configuration mode. To disable application handling of redirect requests on the gateway, use the **no** form of this command. To return the gateway to the default **notify redirect** command settings, use the **default** form of this command.

notify redirect {**ip2ip** | **ip2pots**}
no notify redirect {**ip2ip** | **ip2pots**}
default notify redirect {**ip2ip** | **ip2pots**}

Syntax Description

ip2ip	Enables notify redirection for IP-to-IP calls.
ip2pots	Enables notify redirection for IP-to-IP calls for IP-to-POTS calls.

Command Default

Notify redirection for IP-to-IP calls is enabled.

Notify redirection for IP-to-POTS calls is disabled.

Notify redirection for Session Initiation Protocol (SIP) phones registered to Cisco Unified Communications Manager Express (Cisco Unified CME) is enabled.

Command Modes

Voice service VoIP configuration (conf-voi-serv)

Command History

Release	Modification
12.4(4)T	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T. The following default behavior was added: Notify redirection for SIP phones registered to Cisco Unified CME is enabled.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to enable notify redirection globally on a gateway. Use the **notify redirect** command in dial peer voice configuration mode to configure notify redirection settings for IP-to-IPand IP-to-POTS calls on a specific inbound dial peer on a gateway.

Note This command is supported on Cisco Unified Communications Manager Express (Cisco Unified CME), release 3.4 and later releases and on Cisco Unified Session Initiation Protocol (SIP) Survivable Remote Site Telephony (SRST) release 3.4 and later releases. However, to use the **notify redirect** command in voice service VoIP configuration mode on compatible Cisco Unified SIP SRST devices, you must first use the **allow-connections** command to enable the corresponding call flows on the SRST gateway.

Examples

The following is partial sample output from the **show running-config** command showing that notify redirection has been set up globally for both IP-to-IP and IP-to-POTS calling (because support of IP-to-IP calls is enabled by default, the ip2ip setting does not appear in the output).

```
voice service voip
 notify redirect ip2pots
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to sip
 no supplementary-service h450.2
 no supplementary-service h450.3
 sip
 registrar server expires max 600 min 60
```

Related Commands

Command	Description
allow-connections	Allows connections between specific endpoint types in a VoIP network.
notify redirect (dial peer)	Enables application handling of redirect requests on a specific VoIP dial peer on a Cisco IOS voice gateway.

notify redirect (dial peer)

To enable application handling of redirect requests on a specific VoIP dial peer on a Cisco IOS voice gateway, use the **notify redirect** command in dial peer voice configuration mode. To disable notify redirection on the gateway, use the **no** form of this command. To return the gateway to the default notify redirection settings, use the **default** form of this command.

notify redirect {**ip2ip** | **ip2pots**}
no notify redirect {**ip2ip** | **ip2pots**}
default notify redirect {**ip2ip** | **ip2pots**}

Syntax Description

ip2ip	Specifies that the notify redirect command is applied to IP-to-IP calls.
ip2pots	Specifies that the notify redirect command is applied to IP-to-POTS calls.

Command Default

Notify redirection for IP-to-IP is enabled. Notify redirection for IP-to-POTS is disabled.

Notify redirection for Session Initiation Protocol (SIP) phones registered to Cisco Unified Communications Manager Express (Cisco Unified CME) is enabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(4)T	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T. The following default behavior was added: Notify redirection for SIP phones registered to Cisco Unified CME is enabled.

Usage Guidelines

Use this command in dial peer configuration mode to configure IP-to-IP and IP-to-POTS calls on an inbound dial peer on a Cisco IOS voice gateway. This command configures notify redirection settings on a per-dial-peer basis.

When notify redirect is enabled in dial peer voice configuration mode, the configuration for the specific dial peer is activated only if the dial peer is an inbound dial peer. To enable notify redirect globally on a Cisco IOS voice gateway, use the **notify redirect** command in voice service VoIP configuration mode.

Note This command is supported on Cisco Unified Communications Manager Express (Cisco Unified CME), release 3.4 and later releases and Cisco Unified Session Initiation Protocol (SIP) Survivable Remote Site Telephony (SRST) release 3.4 and later releases. However, to use the **notify redirect** command in voice service VoIP configuration mode on compatible Cisco Unified SIP SRST devices, you must first use the **allow-connections** command to enable the corresponding call flows on the SRST gateway.

Examples

The following is partial sample output from the **show running-config** command showing that notify redirection is enabled for both IP-to-IP and IP-to-POTS calls on VoIP dial peer 8000 (because support of IP-to-IP calls is enabled by default, the ip2ip setting does not appear in the output):

```
dial-peer voice 8000 voip
 destination-pattern 80..
 notify redirect ip2pots
 session protocol sipv2
 session target ipv4:209.165.201.15
 dtmf-relay rtp-nte
 codec g711ulaw
!
```

Related Commands

Command	Description
allow-connections	Allows connections between specific endpoint types in a VoIP network.
notify redirect	Enables application handling of redirect requests for all VoIP dial peers on a Cisco IOS voice gateway.

notify telephone-event

To configure the maximum interval between two consecutive NOTIFY messages for a particular telephone event, use the **notify telephone-event** command in SIP UA configuration mode or voice class tenant configuration mode. To reset the interval to the default value, use the **no** form of this command.

notify telephone-event max-duration *milliseconds* **[system]**
no notify telephone-event

Syntax Description

max-duration *milliseconds*	Time interval between consecutive NOTIFY messages for a single DTMF event, in milliseconds. Range is from 40 to 3000. Default is 2000.
system	Specifies that the NOTIFY messages for a particular telephone event use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations

Command Default

2000 milliseconds

Command Modes

SIP UA configuration (config-sip-ua)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was modified. The acceptable value range for the *milliseconds* argument was expanded (the lower end of the range was changed from 500 to 40).
12.4(24)T3	This command was modified. The acceptable value range for the *milliseconds* argument was expanded (the lower end of the range was changed from 500 to 40).
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

The **notify telephone-event** command works with the **dtmf-relay sip-notify** command. The **dtmf-relay sip-notify** command forwards out-of-band DTMF tones by using SIP NOTIFY messages. The **notify telephone-event** command sets the maximum time interval between consecutive NOTIFY messages for a single DTMF event. The maximum time is negotiated between two SIP endpoints and the lowest duration value is the one selected. This duration is negotiated during call establishment as part of negotiating the SIP-NOTIFY DTMF relay.

The originating gateway sends an indication of DTMF relay in an Invite message using the SIP Call-Info header. The terminating gateway acknowledges the message with an 18x/200 Response message, also using the Call-Info header. The set duration appears in the Call-Info header in the following way:

```
Call-Info: <sip: address>; method="Notify;Event=telephone-event;Duration=msec"
```

For example, if the maximum duration of gateway A is set to 1000 ms, and gateway B is set to 700 ms, the resulting negotiated duration would be 700 ms. Both A and B would use the value 700 in all of their NOTIFY messages for DTMF events.

Examples

The following example sets the maximum duration for a DTMF event to 40 ms.

```
Router(config)# sip-ua
Router(config-sip-ua)# notify telephone-event max-duration 40
```

The following example sets the maximum duration for a DTMF event in the voice class tenant configuration mode:

```
Router(config-class)# notify telephone-event max-duration system
```

Related Commands

Command	Description
dtmf-relay sip-notify	Forwards DTMF tones using SIP NOTIFY messages.

notify ignore substate

To ignore the Subscription-State header, use the **notify ignore substae** command in SIP UA configuration mode or voice class tenant configuration mode. To reset the interval to the default value, use the **no** form of this command.

notify ignore substate
no notify ignore substate

Command Modes

SIP UA configuration (config-sip-ua)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Examples

The following is an example:

```
Router(config)# sip-ua
Router(config-sip-ua)# notify ignore substate
```

nsap

To specify the network service access point (NSAP) address for a local video dial peer, use the **nsap**command in dial-peer configuration mode. To remove any configured NSAP address from the dial peer, use the **no** form of this command.

nsap *nsap-address*
no nsap

Syntax Description

nsap -address	A 40-digit hexadecimal number; the number must be unique on the device.

Command Default

No NSAP address for a video dial peer is configured

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced for ATM video dial-peer configuration on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(9)T.

Usage Guidelines

The address must be unique on the router.

Examples

The following example sets up an NSAP address for the local video dial peer designated as 10:

```
dial-peer video 10 videocodec
 nsap 47.0091810000000002F26D4901.333333333332.02
```

Related Commands

Command	Description
dial -peer video	Defines a video ATM dial peer for a local or remote video codec, specifies video-related encapsulation, and enters dial-peer configuration mode.
show dial -peer video	Displays dial-peer configuration.

null-called-number

To substitute a user-defined number as the called number IE when an incoming H.323 setup message does not contain a called number IE, use the **null-called-number** command in voice service H.323 configuration mode. To disable the addition of the number used as the called number IE, use the **no** form of this command.

null-called-number override *string*
no null-called-number

Syntax Description

override *string*	Specifies the user-defined series of digits for the E.164 or private dialing plan telephone number when the called number IE is missing from the H.323 setup message. Valid entries are the digits 0 through 9.

Command Default

The command behavior is disabled. H.323 setup messages missing the called number IE are disconnected.

Command Modes

Voice service h323 configuration (conf-serv-h323)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

For a call connection to be completed the incoming H.323 setup messages must include the called number IE and the E.164 destination address. Calls lacking called number IE are disconnected. The null-called-number is a user-defined number used when the called number IE is missing to complete the call.

Examples

The following example shows the number 4567 configured as the user-defined number used to complete a call when the H.323 setup message is missing the called number IE:

```
Router(conf-serv-h323)# null-called-number override 4567
```

numbering-type

To match on a number type for a dial-peer call leg, use the **numbering-type**command in dial-peer configurationmode. To remove the numbering type for a dial-peer call leg, use the **no** form of this command.

numbering-type {**international** | **abbreviated** | **national** | **network** | **reserved** | **subscriber** | **unknown**}
no numbering-type {**international** | **abbreviated** | **national** | **network** | **reserved** | **subscriber** | **unknown**}

Syntax Description

international	International numbering type.
abbreviated	Abbreviated numbering type.
national	National numbering type.
network	Network numbering type.
reserved	Reserved numbering type.
subscriber	Subscriber numbering type.
unknown	Numbering type unknown.

Command Default

No default behaviors or values

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced on the Cisco AS5300.
12.0(7)XK	This command was implemented as follows: • VoIP: Cisco 2600 series, Cisco 3600 series, Cisco MC3810 • VoFR: Cisco 2600 series, Cisco 3600 series, Cisco MC3810 • VoATM: Cisco 3600 series, Cisco MC3810
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T and implemented as follows: • VoIP: Cisco 1750, Cisco 2600 series, Cisco 3600 series, Cisco AS5300, Cisco 7200 series, Cisco 7500 series
12.1(2)T	This command was implemented as follows: • VoIP: Cisco MC3810 • VoFR: Cisco 2600 series, Cisco 3600 series, Cisco MC3810 • VoATM: Cisco 3600 series, Cisco MC3810

Release	Modification
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Thiscommand is supported for POTS, VoIP, VoFR, and VoATM dial peers. The numbering type options are implemented as defined by the ITU Q.931 specification.

Examples

The following example shows how to configure a POTS dial peer for network usage:

```
dial-peer voice 100 pots
 numbering-type network
```

The following example shows how to configure a VoIP dial peer for subscriber usage:

```
dial-peer voice 200 voip
 numbering-type subscriber
```

Related Commands

Command	Description
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
show translation -rule	Displays the contents of all the rules that have been configured for a specific translation name.
test translation -rule	Tests the execution of the translation rules on a specific name-tag.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translate -outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
translation -rule	Creates a translation name and enters translation-rule configuration mode.
voip -incoming translation-rule	Captures calls that originate from H.323-compatible clients.

num-exp

To define how to expand a telephone extension number into a particular destination pattern, use the **num-exp**command in global configuration mode. To remove the configured number expansion, use the no form of this command.

num-exp *extension-number* *expanded-number*
no **num-exp** *extension-number*

Syntax Description

extension -number	One or more digits that define an extension number for a particular dial peer.
expanded -number	One or more digits that define the expanded telephone number or destination pattern for the extension number listed.

Command Default

No number expansion is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(3)T	This command was implemented on the Cisco AS5300.
12.0(4)XL	This command was implemented on the Cisco AS5800.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(2)T	This command was modified. It was integrated into Cisco IOS Release 12.1(2)T.
Cisco IOS XE Bengaluru 17.6.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to define how to expand a particular set of numbers (for example, a telephone extension number) into a particular destination pattern. With this command, you can bind specific extensions and expanded numbers together by explicitly defining each number, or you can define extensions and expanded numbers using variables. You can also use this command to convert seven-digit numbers to numbers containing fewer than seven digits.

You can configure a maximum of 250 number extensions before the router sends an error message stating that the limit has been reached.

Use a period (.) as a variable or wildcard, representing a single number. Use a separate period for each number that you want to represent with a wildcard--for example, if you want to replace four numbers in an extension with wildcards, type in four periods.

Translation of a number in +E.164 format is not supported if you use the CLI command **num-exp** , although the plus symbol (+) is displayed as a configurable option for the command. As a workaround, it is recommended that you use translation rule to support the +E.164 dial pattern that contains the plus (+) symbol. For a sample of the configuration, see Example.

Examples

The following is a sample configuration for support of +E.164 number on the Voice Gateway:

```
router(config)#show num-exp
Dest Digit Pattern = '1001'     Translation =
                                '+4001'
router(config)#num-exp 1001 ?
  WORD  Substitution Pattern to Translate Dialed Pat
        to E.164
```

The following example expands the extension number 50145 to the number 14085550145:

```
num-exp 50145 14085550145
```

The following example expands all five-digit extensions beginning with 5 such that the 5 is replaced with the digits 1408555 at the beginning of the extension number:

```
num-exp 5.... 1408555....
```

Related Commands

Command	Description
dial -peer terminator	Designates a special character to be used as a terminator for variable length dialed numbers.
forward -digits	Specifies which digits to forward for voice calls.
prefix	Specifies a prefix for a dial peer.

O

offer call-hold

To specify globally how the POTS-SIP gateway should initiate call-hold requests, use the **offer call-hold** command in SIP user-agent configuration mode or voice class tenant configuration mode. To disable a method of initiating call hold, use the **no** form of this command.

offer call-hold {**conn-addr** | **direction-attr** | **system**}
no offer call-hold {**conn-addr** | **direction-attr** | **system**}

Syntax Description

conn-addr	Specifies the RFC 2543 method of using the connection address for initiating call-hold requests. The RFC 2543 method uses 0.0.0.0.
direction-attr	Specifies the current RFC 3264 method of using the direction attribute (a=sendonly) for initiating call-hold requests.
system	Specifies how the call-hold requests use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations

Command Default

direction-attr

Command Modes

SIP user-agent configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.3(8)T	This command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**.

Usage Guidelines

Cisco POTS-SIP gateways support receiving call-hold requests in either of the two formats, but the direction attribute is recommended. Specifying a call-hold format is only available globally with the **offer call-hold** command; configuration is not available at the dial-peer level.

Examples

The following example initiates call hold by configuring the gateway to send a=sendonly in the Session Description Protocol (SDP). Using the **direction-attr**keyword is the current and preferred method to initiate call hold.

```
sip-ua
 retry invite 3
 offer call-hold direction-attr
```

The following example initiates call hold by configuring the gateway to send 0.0.0.0 as the IP address in the c=line.

```
sip-ua
 retry invite 3
 offer call-hold conn-addr
```

The following example initiates call hold by configuring the gateway in the voice class tenant configuration mode:

```
Router(config-class)# offer call-hold system
```

Related Commands

Command	Description
show sip-ua status	Displays status for the SIP UA.
suspend-resume	Enables SIP Suspend and Resume functionality.

operation

To select a specific cabling scheme for E&M ports, use the **operation**command in voice-port configuration mode. To restore the default, use the **no** form of this command.

operation {**2-wire** | **4-wire**}
no operation {**2-wire** | **4-wire**}

Syntax Description

2 -wire	Two-wire E&M cabling scheme.
4 -wire	Four-wire E&M cabling scheme.

Command Default

2-wire E&M cabling scheme

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810.

Usage Guidelines

This command affects only voice traffic. Signaling is independent of 2-wire versus 4-wire settings. If the wrong cable scheme is specified, the user might get voice traffic in only one direction.

Using this command on a voice port changes the operation of both voice ports on a VPM card. The voice port must be shut down and then opened again for the new value to take effect.

This command is not applicable to FXS or FXO interfaces because they are, by definition, 2-wire interfaces.

Examples

The following example specifies that an E&M port uses a 4-wire cabling scheme:

```
voice-port 1/0/0
 operation 4-wire
```

The following example specifies that an E&M port uses a 2-wire cabling scheme:

```
voice-port 1/1
 operation 2-wire
```

options-ping

To enable in-dialog OPTIONS, use the **options-ping** command in global configuration mode or voice class tenant configuration mode. To disable, use the **no** form of this command.

options-ping *seconds* **[system]**
no options-ping *seconds* **[system]**

Syntax Description

seconds	Intervals, in seconds OPTIONS transactions are sent. Range is 60-1200, there is no default.
system	Specifies that the in-dialog OPTIONS, use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations

Command Default

This command is disabled by default.

Command Modes

Global

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(11)T	This command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

The in-dialog OPTIONS refresh command eanbles an alterante refresh mechanism to RTP/RTCP media inactivity timer and session timer can be used on SIP-to-SIP and SIP-to-H.323 calls. The refresh with in-dialog OPTIONS method is meant to only be hop-to-hop, and not end-to-end. Since session timer achieves similar results, the OPTIONs refresh/ping will not take affect when session timer is negotiated. The behavior on the H.323 endpoint is as if it was a TDM-SIP call. The generating in-dialog OPTIONS is enabled at the global level or dialpeer level. The system default setting is disabled. This feature can be use by both a TDM voice gateway and an IP-to-IP gateway.

Examples

The following example sets the in-dialog refresh time to 60 seconds:

```
Router(conf-serv-sip)# options-ping
```

The following example sets the in-dialog refresh time in the voice class tenant configuration mode:

```
Router(conf-class)# options-ping system
```

Related Commands

Command	Description
options-ping	Enables in-dialog OPTIONS at the global level.
options-ping (dial peer)	Enables in-dialog OPTIONS on a dial-peer.

options-ping (dial-peer)

To enable in-dialog OPTIONS, use the **options-ping** command in global configuration mode. To disable, use the **no** form of this command.

options-ping *seconds*
no options-ping *seconds*

Syntax Description

seconds	Intervals, in seconds OPTIONS transactions are sent. Range is 60-1200, there is no default.

Command Default

This command is disabled by default.

Command Modes

dial peer configuration mode

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The in-dialog OPTIONS refresh command eanbles an alterante refresh mechanism to RTP/RTCP media inactivity timer and session timer can be used on SIP-to-SIP and SIP-to-H.323 calls. The refresh with in-dialog OPTIONS method is meant to only be hop-to-hop, and not end-to-end. Since session timer achieves similar results, the OPTIONs refresh/ping will not take affect when session timer is negotiated. The behavior on the H.323 endpoint is as if it was a TDM-SIP call. The generating in-dialog OPTIONS is enabled at the global level or dialpeer level. The system default setting is disabled. This feature can be use by both a TDM voice gateway and an IP-to-IP gateway.

Examples

The following example sets the in-dialog refresh time to 60 seconds:

```
Router(conf-serv-sip)# options-ping 60
```

Related Commands

Command	Description
options-ping	Enables in-dialog OPTIONS at the global level.
options-ping (dial peer)	Enables in-dialog OPTIONS on a dial-peer.

outbound-proxy

To configure a Session Initiation Protocol (SIP) outbound proxy for outgoing SIP messages globally on a Cisco IOS voice gateway, use the **outbound-proxy** command in voice service SIP configuration mode or voice class tenant configuration mode. To globally disable forwarding of SIP messages to a SIP outbound proxy globally, use the **no** form of this command.

outbound-proxy {**dhcp** | **ipv4:***ip-address*[{**:***port-number* | **dns:***host***:***domain* [{**reuse**}]}]} **[system]**
no outbound-proxy

Syntax Description

dhcp	Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway; all SIP dialog-initiating requests are sent to the SIP server obtained via DHCP.
ipv4 : *ip-address*	Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway; all SIP dialog-initiating requests are sent to this IP address. The colon is required.
: *port-number*	(Optional) The port to which all SIP dialog-initiating requests are sent at the specified IP address. Port number ranges from 0 to 65535. The default is 5060. The colon is required.
dns : *host* **:** *domain*	Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway; all initiating requests are sent to the specified destination domain. The colon is required.
reuse	(Optional) Reuses the outbound proxy address established during registration for all subsequent registration refreshes and calls.
system	Specifies that the outbound proxy for outgoing SIP messages use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations

Command Default

The Cisco IOS voice gateway does not forward outbound SIP messages to a proxy.

Command Modes

Voice service VoIP SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.
12.4(22)YB	This command was modifed. The **dhcp** keyword was added.
15.0(1)M	This command was integrated in Cisco IOS Release 15.0(1)M.
15.1(2)T	This command was modified. The **reuse** keyword was added.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**.

Release	Modification
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

You can use the **outbound-proxy** command in voice service SIP configuration mode to specify outbound proxy settings globally for a Cisco IOS voice gateway. You can also use the **voice-class sip outbound-proxy** command in dial peer voice configuration mode to configure settings for an individual dial peer that override or defer to the global settings for the gateway. However, if both a Cisco Unified Communications Manager Express (CME) and a SIP gateway are configured on the same router, then there is a scenario that can cause incoming SIP messages from line-side phones to be confused with SIP messages coming from the network side. To avoid failed calls caused by this scenario, disable the SIP outbound proxy setting for all line-side phones on a dial peer using the **outbound-proxy system** command in voice register global configuration mode.

Examples

The following example shows how to specify the SIP outbound proxy globally for a Cisco IOS voice gateway using an IP address:

```
Router> enable
Router# configure
 terminal
Router(config)# voice
 service
 voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# outbound
-proxy
 ipv4
:10.1.1.1
```

The following example shows how to specify the SIP outbound proxy globally for a Cisco IOS voice gateway using a destination hostname and domain:

```
Router> enable
Router# configure
 terminal
Router(config)# voice
 service
 voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# outbound
-proxy
 dns:sipproxy:example.com
```

The following example shows how to specify the SIP outbound proxy globally for a Cisco IOS voice gateway using the DHCP protocol:

```
Router> enable
Router# configure
 terminal
Router(config)# voice
 service
 voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# outbound
-proxy
 dhcp
```

The following example shows how to specify the SIP outbound proxy globally in the voice class tenant configuration mode:

```
Router(config-class)# outbound-proxy system
```

Related Commands

Command	Description
outbound-proxy system	Specifies whether Cisco Unified CME line-side SIP phones use the outbound proxy settings configured globally for a Cisco IOS voice gateway.
voice-class sip outbound-proxy	Configures SIP outbound proxy settings for an individual dial peer that override global settings for the Cisco IOS voice gateway.

outbound retry-interval

To define the retry period for attempting to establish the outbound relationship between border elements, use the **outbound retry-interval** command in Annex G neighbor service configuration mode. To disable the command, use the **no** form of this command.

outbound retry-interval *interval*
no outbound retry-interval

Syntax Description

interval	Amount of time, in seconds, to establish the outbound relationship. Range is from 1 to 2147483. The default is 30.

Command Default

30 seconds

Command Modes

Annex G neighbor service configuration (config-nxg-neigh-svc)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Service relationships are defined to be unidirectional. When a service relationship is established between border element A and border element B, A is entitled to send requests to B and expect responses. For B to send requests to A and expect responses, a second service relationship must be established. From A's perspective, the service relationship it establishes with B is designated as the "outbound" service relationship.

Use this command to set the retry period for attempting to bring up the outbound relationship between border elements.

Examples

The following example shows how to set the retry interval to 300 seconds (5 minutes):

```
Router(config-nxg-neigh-svc)
#
outbound retry-interval 300
```

Related Commands

Command	Description
access -policy	Requires that a neighbor be explicitly configured.
inbound ttl	Sets the inbound time-to-live value.
retry interval	Defines the time between delivery attempts.
retry window	Defines the total time that a border element will attempt delivery.
service -relationship	Establishes a service relationship between two border elements.
shutdown	Enables or disables the border element.

outgoing called-number

To configure debug filtering for outgoing called numbers, use the outgoing called-number command in call filter match list configuration mode. To disable, use the **no** form of this command.

outgoing called-number *string*
no outgoing called-number *string*

Syntax Description

string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 to 9, the letters A to D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touchtone dial pads. On the Cisco 3600 series routers only, these characters cannot be used as leading characters in a string (for example, *650). • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). On the Cisco 3600 series routers, the period cannot be used as a leading character in a string (for example, .650). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used in front of a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character; matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters 0 to 9 are allowed in the range. • Parentheses ( ), which indicate a pattern and are the same as the regular expression rule.

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The outgoing called number goes out after number translation and expansion.

Examples

The following example shows the voice call debug filter set to match outgoing called number 8288807:

```
call filter match-list 1 voice
 outgoing called-number 8288807
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming called-number (call filter match list)	Configure debug filtering for incoming called numbers.
incoming calling-number	Configure debug filtering for incoming calling numbers.
incoming dialpeer	Configure debug filtering for the incoming dial peer.
incoming secondary-called-number	Configure debug filtering for incoming called numbers from the second stage of a two-stage scenario.
outgoing calling-number	Configure debug filtering for outgoing calling numbers.
outgoing dialpeer	Configure debug filtering for the outgoing dial peer.
show call filter match-list	Display call filter match lists.

outgoing calling-number

To configure debug filtering for outgoing calling numbers, use the outgoing calling-number command in call filter match list configuration mode. To disable, use the **no** form of this command.

outgoing calling-number *string*
no outgoing calling-number *string*

Syntax Description

<table>
<tr><td>string</td><td>Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 to 9, the letters A to D, and the following special characters:
• The asterisk (*) and pound sign (#) that appear on standard touchtone dial pads. On the Cisco 3600 series routers only, these characters cannot be used as leading characters in a string (for example, *650).
• Comma (,), which inserts a pause between digits.
• Period (.), which matches any entered digit (this character is used as a wildcard). On the Cisco 3600 series routers, the period cannot be used as a leading character in a string (for example, .650).
• Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage.
• Plus sign (+), which indicates that the preceding digit occurred one or more times.
Note The plus sign used as part of a digit string is different from the plus sign that can be used in front of a digit string to indicate that the string is an E.164 standard number.
• Circumflex (^), which indicates a match to the beginning of the string.
• Dollar sign ($), which matches the null string at the end of the input string.
• Backslash symbol (\), which is followed by a single character; matches that character. Can be used with a single character with no other significance (matching that character).
• Question mark (?), which indicates that the preceding digit occurred zero or one time.
• Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters 0 to 9 are allowed in the range.
• Parentheses ( ), which indicate a pattern and are the same as the regular expression rule.</td></tr>
</table>

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The outgoing calling number goes out after number translation and expansion.

Examples

The following example shows the voice call debug filter set to match outgoing calling number 5550124:

```
call filter match-list 1 voice
 outgoing calling-number 5550124
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming called-number (call filter match list)	Configure debug filtering for incoming called numbers.
incoming calling-number	Configure debug filtering for incoming calling numbers.
incoming dialpeer	Configure debug filtering for the incoming dial peer.
incoming secondary-called-number	Configure debug filtering for incoming called numbers from the second stage of a two-stage scenario.
outgoing called-number	Configure debug filtering for outgoing called numbers.
outgoing dialpeer	Configure debug filtering for the outgoing dial peer.
show call filter match-list	Display call filter match lists.

outgoing dialpeer

To configure debug filtering for the outgoing dial peer, use the **outgoing dialpeer** command in call filter match list configuration mode. To disable, use the **no** form of this command.

outgoing dialpeer *tag*
no outgoing dialpeer *tag*

Syntax Description

tag	Digits that identify a specific dial peer. Valid entries are 1 to 2,147,483,647.

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match outgoing dial peer 12:

```
call filter match-list 1 voice
 outgoing dialpeer 12
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming called-number (call filter match list)	Configure debug filtering for incoming called numbers.
incoming calling-number	Configure debug filtering for incoming calling numbers.
incoming dialpeer	Configure debug filtering for the incoming dial peer.
incoming port	Configure debug filtering for the incoming port.
outgoing called-number	Configure debug filtering for outgoing called numbers.
outgoing calling-number	Configure debug filtering for outgoing calling numbers.
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

outgoing media local ipv4

To configure debug filtering for the outgoing media local IPv4 addresses for the voice gateway receiving the media stream, use the outgoing media local ipv4 command in call filter match list configuration mode. To disable, use the **no** form of this command.

outgoing media local ipv4 *ip_address*
no outgoing media local ipv4 *ip_address*

Syntax Description

ip_address	IP address of the local voice gateway

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match outgoing media on the local voice gateway, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 outgoing media local ipv4 192.168.10.255
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming media local ipv4	Configure debug filtering for the incoming media IPv4 addresses for calls to the IP side from the local voice gateway.
incoming media remote ipv4	Configure debug filtering for the incoming media IPv4 addresses for calls to the IP side from the remote IP device.
incoming port	Configure debug filtering for the incoming port.
outgoing media remote ipv4	Configure debug filtering for the outgoing media IPv4 addresses for calls to the IP side from the remote IP device.
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

outgoing media remote ipv4

To configure debug filtering for the outgoing media remote IPv4 addresses for the voice gateway receiving the media stream, use the outgoing media remote ipv4 command in call filter match list configuration mode. To disable, use the **no** form of this command.

outgoing media remote ipv4 *ip_address*
no outgoing media remote ipv4 *ip_address*

Syntax Description

ip_address	IP address of the remote IP device

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match outgoing media on the remote IP device, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 outgoing media remote ipv4 192.168.10.255
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming media local ipv4	Configure debug filtering for the incoming media IPv4 addresses for calls to the IP side from the local voice gateway.
incoming media remote ipv4	Configure debug filtering for the incoming media IPv4 addresses for calls to the IP side from the remote IP device.
incoming port	Configure debug filtering for the incoming port.
outgoing media local ipv4	Configure debug filtering for the outgoing media IPv4 addresses for calls to the IP side from the local voice gateway
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

outgoing port

To configure debug filtering for the outgoing port, use the outgoing port command in call filter match list configuration mode. To disable, use the **no** form of this command.

Cisco 2600, Cisco 3600, and Cisco 3700 Series
outgoing port {*slot-number*/*subunit-number*/*port* | *slot*/*port*:*ds0-group-no*}
no outgoing port {*slot-number*/*subunit-number*/*port* | *slot*/*port*:*ds0-group-no*}

Cisco 2600 and Cisco 3600 Series with a High-Density Analog Network Module (NM-HDA)
outgoing port {*slot-number*/*subunit-number*/*port*}
no outgoing port {*slot-number*/*subunit-number*/*port*}

Cisco AS5300
outgoing port *controller-number***:D**
no outgoing port *controller-number***:D**

Cisco AS5400
outgoing port *card*/*port***:D**
no outgoing port *card*/*port***:D**

Cisco AS5800
outgoing port {*shelf*/*slot*/*port***:D** | *shelf*/*slot*/*parent*:*port***:D**}
no outgoing port {*shelf*/*slot*/*port***:D** | *shelf*/*slot*/*parent*:*port***:D**}

Cisco MC3810
outgoing port *slot*/*port*
no outgoing port *slot*/*port*

Syntax Description

slot-number	Number of the slot in the router in which the VIC is installed. Valid entries are 0 to 3, depending on the slot in which it has been installed.
subunit-number	Subunit on the VIC in which the voice port is located. Valid entries are 0 or 1.
port	Voice port number. Valid entries are 0 and 1.
slot	The router location in which the voice port adapter is installed. Valid entries are 0 to 3.
port:	Indicates the voice interface card location. Valid entries are 0 and 3.
ds0-group-no	Indicates the defined DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.

controller-number	T1 or E1 controller.
:D	D channel associated with ISDN PRI.

card	Specifies the T1 or E1 card. Valid entries for the *card* argument are 1 to 7.

port	Specifies the voice port number. Valid entries are 0 to 7.
:D	Indicates the D channel associated with ISDN PRI.

shelf	Specifies the T1 or E1 controller on the T1 card, or the T1 controller on the T3 card. Valid entries for the *shelf* argument are 0 to 9999.
slot	Specifies the T1 or E1 controller on the T1 card, or the T1 controller on the T3 card. Valid entries for the *slot* argument are 0 to 11.
port	Specifies the voice port number. • T1 or E1 controller on the T1 card --Valid entries are 0 to 11. • T1 controller on the T3 card--Valid entries are 1 to 28
:*port*	Specifies the value for the *parent* argument. The only valid entry is 0.
:D	Indicates the D channel associated with ISDN PRI.

slot	The slot argument specifies the number slot in the router in which the VIC is installed. The only valid entry is 1.
port	The port variable specifies the voice port number. Valid interface ranges are as follows: • T1--ANSI T1.403 (1989), Telcordia TR-54016. • E1-- ITU G.703. • Analog voice--Up to six ports (FXS, FXO, E & M). • Digital voice-- Single T1/E1 with cross-connect drop and insert, CAS and CCS signaling, PRI QSIG. • Ethernet--Single 10BASE-T. • Serial--Two five-in-one synchronous serial (ANSI EIA/TIA-530, EIA/TIA-232, EIA/TIA-449; ITU V.35, X.21, Bisync, Polled async).

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match outgoing port 1/1/1 on a Cisco 3660 voice gateway:

```
call filter match-list 1 voice
 outgoing port 1/1/1
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming port	Configure debug filtering for the incoming port.
show call filter match-list	Display call filter match lists.

outgoing signaling local ipv4

To configure debug filtering for the outgoing signaling local IPv4 addresses for the gatekeeper managing the signaling, use the outgoing signaling local ipv4 command in call filter match list configuration mode. To disable, use the **no** form of this command.

outgoing signaling local ipv4 *ip_address*
no outgoing signaling local ipv4 *ip_address*

Syntax Description

ip_address	IP address of the local voice gateway

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match outgoing signaling on the local voice gateway, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 outgoing signaling local ipv4 192.168.10.255
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming port	Configure debug filtering for the incoming port.
incoming signaling local ipv4	Configure debug filtering for the incoming signaling IPv4 addresses for calls to the IP side from the local voice gateway.
incoming signaling remote ipv4	Configure debug filtering for the incoming signaling IPv4 addresses for calls to the IP side from the remote IP device.
outgoing port	Configure debug filtering for the outgoing port.
outgoing signaling remote ipv4	Configure debug filtering for the outgoing signaling IPv4 addresses for calls to the IP side from the remote IP device.
show call filter match-list	Display call filter match lists.

outgoing signaling remote ipv4

To configure debug filtering for the outgoing signaling remote IPv4 addresses for the gatekeeper managing the signaling, use the outgoing signaling remote ipv4 command in call filter match list configuration mode. To disable, use the **no** form of this command.

outgoing signaling remote ipv4 *ip_address*
no outgoing signaling remote ipv4 *ip_address*

Syntax Description

ip_address	IP address of the remote IP device

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match outgoing signaling on the remote IP device, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 outgoing signaling remote ipv4 192.168.10.255
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming port	Configure debug filtering for the incoming port.
incoming signaling local ipv4	Configure debug filtering for the incoming signaling IPv4 addresses for calls to the IP side from the local voice gateway.
incoming signaling remote ipv4	Configure debug filtering for the incoming signaling IPv4 addresses for calls to the IP side from the remote IP device.
outgoing port	Configure debug filtering for the outgoing port.
outgoing signaling local ipv4	Configure debug filtering for the outgoing signaling IPv4 addresses for calls to the IP side from the local voice gateway.
show call filter match-list	Display call filter match lists.

output attenuation

To configure a specific output attenuation value or enable automatic gain control, use the **output attenuation**command in voice-port configuration mode. To disable the selected output attenuation value, use the **no** form of this command.

output attenuation {*decibels* | **auto-control** [*auto-dbm*]}
no output attenuation {*decibels* | **auto-control** [*auto-dbm*]}

Syntax Description

decibels	Attenuation, in decibels (dB), at the transmit side of the interface. Range is integers from -6 to 14. The default is 3.
auto-control	Enable automatic gain control.
auto-dbm	(Optional) Target speech level, in decibels per milliwatt (dBm), to be achieved at the transmit side of the interface. Range is integers from -30 to 3. The default is -9.

Command Default

For Foreign Exchange Office (FXO), Foreign Exchange Station (FXS), and ear and mouth (E&M) ports: *decibels*: 3 decibels*auto-dbm*: -9 dBm

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810.
12.3(4)XD	The range of values for the *decibels* argument was increased.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(2)T	The **auto-control** keyword and *auto-dbm* argument were added.

Usage Guidelines

A system-wide loss plan must be implemented using both the **input gain** and **output attenuation** commands. You must consider other equipment (including PBXs) in the system when creating a loss plan. The default value for this command assumes that a standard transmission loss plan is in effect, meaning that there must be an attenuation of -6 dB between phones. Connections are implemented to provide -6 dB of attenuation when the **input gain** and **output attenuation** commands are configured with the default value of 3 dB.

You cannot increase the gain of a signal to the public switched telephone network (PSTN), but you can decrease it. If the voice level is too high, you can decrease the volume by either decreasing the input gain or increasing the output attenuation.

You can increase the gain of a signal coming into the router. If the voice level is too low, you can increase the input gain by using the **input gain** command.

The **auto-control**keyword and *auto-dbm* argument are available on an ear and mouth (E&M) voice port only if the signal type for that port is Land Mobile Radio (LMR). The **auto-control**keyword enables automatic gain control, which is performed by the digital signal processor (DSP). Automatic gain control adjusts speech to a comfortable volume when it becomes too loud or too soft. Because of radio network loss and other environmental factors, the speech level arriving at a router from an LMR system could be very low. You can use automatic gain control to ensure that the speech is played back at a more comfortable level. Because the gain is inserted digitally, the background noise can also be amplified. Automatic gain control is implemented as follows:

- Output level: -9 dB
- Gain range: -12 dB to 20 dB
- Attack time (low to high): 30 milliseconds
- Attack time (high to low): 8 seconds

Examples

On the Cisco 3600 series router, the following example configures a 3-dB loss to be inserted at the transmit side of the interface:

```
voice-port 1/0/0
 output attenuation 3
```

On the Cisco 3600 series router, the following example configures a 3-dB gain to be inserted at the transmit side of the interface:

```
voice-port 1/0/0
 output attenuation -3
```

On the Cisco AS5300, the following example configures a 3-dB loss to be inserted at the transmit side of the interface:

```
voice-port 0:D
 output attenuation 3
```

Related Commands

Command	Description
comfort-noise	Generates background noise to fill silent gaps during calls if VAD is activated.
echo-cancel enable	Enables the cancellation of voice that is sent out the interface and received back on the same interface.
input gain	Configures a specific input gain value or enables automatic gain control for a voice port.

overhead

To configure the overhead negotiated bandwidth percentage, use the **overhead** command in media profile configuration mode. To disable the configuration, use the **no** form of the command.

overhead {**audio** | **video**} *percentage*
no overhead {**audio** | **video**}

Syntax Description

audio	Configures the audio overhead percentage.
video	Configures the video overhead percentage.
percentage	Overhead percentage. The range is from 0 to 50.

Command Default

Overhead negotiated bandwidth is not configured.

Command Modes

Media profile configuration (cfg-mediaprofile)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

The overhead bandwidth is the extra bandwidth apart from the negotiated bandwidth for audio and video calls. Hence, the total policing bandwidth is:

Policing bandwidth = negotiated bandwidth + (1 + % overhead bandwidth)

Examples

The following example shows how to configure an overhead bandwidth of 10 percent for audio codecs and 20 percent for video codecs:

```
Router> enable
Router# configure terminal
Router(config)# media profile police 1
Router(cfg-mediaprofile)# overhead audio 10
Router(cfg-mediaprofile)# overhead video 20
```

Related Commands

Command	Description
media profile police	Configures the media policing profile.

package through pattern

package

To enter application-parameter configuration mode to load and configure a package, use the **package** command in application configuration mode. There is no **no** form of this command.

package *package-name* *location*
no **package** *package-name*

Syntax Description

package-name	Name that identifies the package.
location	Directory and filename of the package in URL format. For example, flash memory (flash:filename), a TFTP (tftp://../filename) or an HTTP server (http://../filename) are valid locations.

Command Default

No default behavior or values

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command to enter application parameter configuration mode to load and configure a package. A package is a linkable set of C or Tcl functions that provide functionality invoked by applications or other packages. They are not standalone. For example, a debit card application may use multiple language translation packages, such as English and French. These language translation packages can also be used by other applications without having to modify the package for each application using it.

The packages available on your system depend on the scripts, applications, and packages that you have installed. Your software comes with a set of built-in packages, and additional packages can be loaded using the Tcl **package** command. You can then use the **package** command in application configuration mode to access the parameters contained in those packages.

Examples

The following example shows that a French language translation package is loaded:

```
Router(config-app)# package frlang http://server-1/language_translate.tcl
```

Related Commands

Command	Description
call application voice	Defines the name of a voice application and specify the location of the Tcl or VoiceXML document to load for this application.
package appcommon	Configures parameters in the built-in common voice application package.
package callsetup	Configures parameters in the built-in call setup package.
package language	Loads an external Tcl language module for use with an IVR application.

Command	Description
package session_xwork	Configure parameters in the built-in session_xwork package.

package appcommon

To configure parameters in the built-in common voice application package, use the **package appcommon** command in application configuration mode. There is no **no** form of this command.

package appcommon

Syntax Description

No arguments or keywords

Command Default

No default behavior or values

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command to configure common voice-application-package parameters. After you enter this command, use the **param** command to configure individual parameters.

Examples

The following example shows using the **param security trusted** command to set the security level of a VoiceXML application to "trusted" so that automatic number identification (ANI) is not blocked.

```
application
package appcommon
param security trusted
```

Related Commands

Command	Description
package	Enters application parameter configuration mode to load and configure a package.
package callsetup	Configures parameters in the built-in call setup package.
package language	Loads an external Tcl language module for use with an IVR application.
package session_xwork	Configures parameters in the built-in session_xwork package.

package callsetup

To configure parameters in the built-in call setup package, use the **package callsetup**command in application configuration mode. There is no **no** form of this command.

package callsetup

Command Default

No arguments or keywords

Command Default

No default behavior or values

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command to configure parameters in the built-in call setup package. The callsetup package is used by applications and other packages to place outbound call legs and interwork them with incoming call legs. call setup After you enter this command, use the **param** command to configure individual parameters.

Examples

```
The following example shows the call transfer mode set to redirect:
application
package callsetup
param mode redirect
```

Related Commands

Command	Description
package	Enters application parameter configuration mode to load and configure a package.
package appcommon	Configures parameters in the built-in common voice application package.
package language	Loads an external Tcl language module for use with an IVR application.
package session_xwork	Configure parameters in the built-in session_xwork package.

package language

To load an external Tool Command Language (Tcl) language module for use with an interactive voice response (IVR) application, use the **package language command in**application configuration mode. There is no **no** form of the command.

package language *prefix url*

Syntax Description

prefix	Two-character prefix for the language; for example, "*en*" for English or "*ru*" for Russian.
url	Location of the module.

Command Default

No default behavior or values

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call language voice** command.

Usage Guidelines

Use this command to load language packages for use by applications or other packages. The built-in languages are English *(en)* , Chinese *(ch)* , and Spanish *(sp)* . If you specify "*en*" , "*ch*" , or "*sp*" , the new Tcl module replaces the built-in language functionality. When you add a new Tcl module, you create your own prefix to identify the language. When you configure and load the new languages, any upper-layer application (Tcl IVR) can use the language.

After loading language packages, you can configure an application or other package to use the new language package using the **param language** or **paramspace language location**command.

Examples

The following example adds Russian (*ru*) as a Tcl module and configures the debitcard application to use Russian for prompts:

```
application
package language ru tftp://box/unix/scripts/multi-lang/ru_translate.tcl
service debitcard tftp://server-1/tftpboot/scripts/app_debitcard.2.0.2.8.tcl
param language ru
```

Related Commands

Command	Description
package	Enters application parameter configuration mode to load and configure a package.
package appcommon	Configures parameters in the built-in common voice application package.
package callsetup	Configures parameters in the built-in call setup package.
package session_xwork	Configures parameters in the built-in session_xwork package.

Command	Description
param language	Configures the language parameter in a service or package on the gateway.
paramspace language location	Defines the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML).

package persistent

To configure the package type used when reporting persistent events for a multifrequency (MF) tone channel-associated signaling (CAS) endpoint type using a specific Media Gateway Control Protocol (MGCP) profile, use the **package persistent** command in MGCP profile configuration mode. To disable the persistent status, use the **no** form of this command.

package persistent *package-name*
no package persistent *package-name*

Syntax Description

package -name	Package name. Valid names are ms-package and mt-package.

Command Default

ms-package

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a MGCP profile.

This command is used only with MF trunks (gateway voice ports configured with the **dial-type mf** command in voice-port configuration mode). Because the same persistent event can be defined in different MGCP packages, you may need to use this command to tell the gateway which package to use when reporting persistent events to the call agent for the endpoints in this MGCP profile. For example, a T1 may be configured as an MF trunk, but there is more than one MGCP package that applies to an MF trunk. An *ans* (call answer) event must be mapped to the appropriate package for call-agent notification. This command allows different T1s to be configured for different CAS protocols.

The MS package is used with certain PBX direct inward dial (DID) and direct outward dial (DOD) trunks with wink-start or ground-start signaling as indicated in RFC 3064 (*MGCP CAS Packages*).

The MT package is a subset of the MS package, and it is used with certain operator services on terminating MF trunks on trunking gateway endpoints, as described in *PacketCable PSTN Gateway Call Signaling Protocol Specification* (TGCP) PKT-SP-TGCP-D02-991028, December 1, 1999.

Examples

The following example enables event persistence for the MT package:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# package persistent mt-package
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure an MGCP profile associated with one or more endpoints or to configure the default profile.

package session_xwork

To configure parameters in the built-in session_xwork package, use the **package session_xwork**command in application configuration mode.

package session_xwork

Syntax Description

No arguments or keywords

Command Default

No default behavior or values

Command Default

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command to configure parameters in the built-in session x_work package. After you enter this command, use the **param** command to configure individual parameters.

For example, use this command with the **param default disc-prog-ind-at-connect** command to convert a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.

Examples

The following example shows how to configure the system to convert a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state:

```
application
package session_xwork
param default disc-prog-ind-at-connect
```

Related Commands

Command	Description
package	Enters application parameter configuration mode to load and configure a package.
package appcommon	Configures parameters in the built-in common voice application package.
package callsetup	Configures parameters in the built-in call setup package.
package language	Loads an external Tool Command Language (Tcl) language module for use with an interactive voice response (IVR) application.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.

param

To load and configure parameters in a package or a service (application) on the gateway, use the **param** command in application configuration mode. To reset a parameter to its default value, use the **no** form of this command.

param *param-name* [{**param max-retries** | **param passwd** | **param passwd-prompt filename** | **param user-prompt filename** | **param term-digit** | **param abort-digit** | **param max-digits**}]
no param *param-name*

Syntax Description

param-name	Name of the parameter.
param max-retries	(Optional) Number of attempts to re-enter account or password. Value ranges from 0-10, default value is 0.
param passwd	(Optional) Character string that defines a predefined password for authorization.
param passwd-prompt filename	(Optional) Announcement URL to request password input. filename defines the name and location of the audio filename to be used for playing the password prompt.
param user-prompt filename	(Optional) Announcement URL to request authorization code username. filename defines the name and location of the audio filename to be used for playing the username prompt.
param term-digit	Digit for terminating username or password digit input.
param abort-digit	Digit for aborting username or password digit input. Default value is *.
param max-digits	Maximum number of digits in a username or password. Range of valid value: 1 - 32. Default value is 32.

Command Default

No default behavior or value.

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
15.1(3)T	This command was modified. The following keywords and arguments were added: param max-retries, param passwd, param passwd-prompt filename, param user-prompt filename, param term-digit, param max-digit.

Usage Guidelines

Use this command in application parameter configuration mode to configure parameters in a package or service. A package is a linkable set of C or Tcl functions that provide functionality invoked by applications or other packages. A service is a standalone application.

The parameters available for configuration differ depending on the package or service that is loaded on the gateway. The **param register** Tcl command in a service or package registers a parameter and provides a description and default values which allow the parameter to be configured using the CLI. The **param register** command is executed when the service or package is loaded or defined, along with commands such as **package provide**, which register the capability of the configured module and its associated scripts. You must configure and load the Tcl scripts for your service or package and load the package in order to configure its parameters. See the *Tcl IVR API Version 2.0 Programming Guide* for more information.

When a package or service is defined on the gateway, the parameters in that package or service become available for configuration when you use this command. Additional arguments and keywords are available for different parameters. To see a list of available parameters, enter **param** ?.

To avoid problems with applications or packages using the same parameter names, the *parameter namespace,* or *parameterspace* concept is introduced. When a service or a package is defined on the gateway, its parameter namespace is automatically defined. This is known as the service or package's local parameterspace, or "myparameterspace." When you use this command to configure a service or package's parameters, the parameters available for configuration are those contained in the local parameterspace. If you want to use parameter definitions found in different parameterspace, you can use the **paramspace***parameter-namespace* command to map the package's parameters to a different parameterspace. This allows that package to use the parameter definitions found in the new parameterspace, in addition to its local parameterspace.

Use this command in Cisco Unified Communication Manager Express 8.5 and later versions to define the username and password parameters to authenticate packages for Forced Authorization Code (FAC)

When a predefined password is entered using the param passwd keyword, callers are not requested to enter a password. You must define a filename for user-prompt to play an audio prompt requesting the caller to enter a valid username (in digits) for authorization. Similarly, you must define a filename for passwd-prompt to play an audio prompt requesting the caller to enter a valid password (in digits) for authorization.

Examples

The following example shows how to configure a parameter in the httpios package:

```
application
package httpios
param paramA value4
```

Related Commands

Command	Description
call application voice	Defines the name of a voice application and specify the location of the Tcl or VoiceXML document to load for this application.
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.

Command	Description
param pin-len	Defines the number of characters in the personal identification number (PIN) for an application.
param redirect-number	Defines the telephone number to which a call is redirected--for example, the operator telephone number of the service provider--for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param 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.
param security	Configures security for linkable Tcl functions (packages).
paramspace	Enables an application to use parameters from the local parameter space of another application.
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param access-method

To specify the access method for two-stage dialing for the designated application, use the **param access-method**command in application parameter configuration mode. To restore default values for this command, use the **no** form of this command.

param access-method {**prompt-user** | **redialer**}
no param access-method

Syntax Description

prompt-user	Specifies that no DID is set in the incoming POTS dial peer and that a Tcl script in the incoming POTS dial peer is used for two-stage dialing.
redialer	Specifies that no DID is set in the incoming POTS dial peer and that the redialer device are used for two-stage dialing.

Command Default

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

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice access-method** command.

Usage Guidelines

Use the **param 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:

```
application
service app_libretto_onramp9 tftp://server-1/tftpboot/scripts
param access-method prompt-user
```

Related Commands

Command	Description
call application voice access-method	Specifies the access method for two-stage dialing for the designated application.

param account-id-method

To configure an application to use a particular method to assign the account identifier, use the **param account id method**command in application parameter configuration mode. To remove configuration of this account identifier, use the **no** form of this command.

param account-id-method {**none** | **ani** | **dnis** | **gateway**}
no param account-id-method {**none** | **ani** | **dnis** | **gateway**}

Syntax Description

none	Account identifier is blank. This is the default.
ani	Account identifier is the calling party telephone number (automatic number identification, or ANI).
dnis	Account identifier is the dialed party telephone number (dialed number identification service, or DNIS).
gateway	Account identifier is a router-specific name derived from the hostname and domain name, displayed in the following format: router-name.domain-name.

Command Default

No default behavior or values

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice account-id-method** command.

Usage Guidelines

When an on-ramp application converts a fax into an e-mail, the e-mail contains a field called x-account-id, which can be used for accounting or authentication. The x-account-id field can contain information supplied as a result of this command, such as the calling party's telephone number (**ani**), the called party's telephone number (**dnis**), or the name of the gateway (**gateway**).

Examples

The following example sets the fax detection IVR application account identifier to the router-specific name derived from the hostname and domain name:

```
application
service fax_detect flash:app_fax_detect.2.1.2.2.tcl
param account-id-method gateway
```

Related Commands

Command	Description
call application voice account-id-method	Configures the fax detection IVR application to use a particular method to assign the account identifier.
param	Loads and configures parameters in a package or a service (application).

Command	Description
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected--for example, the operator telephone number of the service provider--for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param 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.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param accounting enable

To enable authentication, authorization, and accounting (AAA) accounting for a Tool Command Language (TCL) application, use the **param accounting enable**command in application configuration mode. To disable accounting for a TCL application, use the **no** form of this command.

param accounting enable
no param accounting enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice accounting enable**command.

Usage Guidelines

This command enables AAA accounting services if a AAA accounting method list has been defined using both the **aaa accounting** command and the **mmoip aaa method fax accounting** command.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example enables AAA accounting to be used with outbound store-and-forward fax:

```
application
service app_libretto_onramp9 tftp://server-1/tftpboot/scripts/
param accounting enable
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services when you use RADIUS or TACACS+.
mmoip aaa method fax accounting	Defines the name of the method list to be used for AAA accounting with store-and-forward fax.

param accounting-list

To define the name of the accounting method list to be used for authentication, authorization, and accounting (AAA) with store-and-forward fax on a voice feature card (VFC), use the **param accounting list** command in application configuration mode. To undefine the accounting method list, use the **no** form of this command.

param accounting-list *method-list-name*
no param accounting-list *method-list-name*

Syntax Description

method-list-name	Character string used to name a list of accounting methods to be used with store-and-forward fax.

Command Default

No AAA accounting method list is defined

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	The **param accounting-list command** was introduced to replace the **call application voice accounting-list**command.

Usage Guidelines

This command defines the name of the AAA accounting method list to be used with store-and-forward fax. The method list itself, which defines the type of accounting services provided for store-and-forward fax, is defined using the **aaa accounting** command. Unlike standard AAA (in which each defined method list can be applied to specific interfaces and lines), the AAA accounting method lists that are used in store-and-forward fax are applied globally.

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 VFCs. The command is not used on modem cards.

Examples

The following example defines a AAA accounting method list "smith" to be used with store-and-forward fax:

```
aaa new-model
application
service app_libretto_onramp9 tftp://server-1/tftpboot/scripts/
param accounting-list smith
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services when you use RADIUS or TACACS+.
param accounting enable	Enables AAA accounting for a TCL application.

Command	Description
mmoip aaa receive-accounting enable	Enables on-ramp AAA accounting services.

param authen-list

To specify the name of an authentication method list for a Tool Command Language (TCL) application, use the **param authen list**command in global configuration mode. To disable the authentication method list for a TCL application, use the **no** form of this command.

param authen-list *method-list-name*
no param authen-list *method-list-name*

Syntax Description

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.

Command Default

No default behavior or values

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice param authen-list** command.

Usage Guidelines

This command defines the name of the authentication, authorization, and accounting (AAA) 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** command. Unlike standard AAA (in which each defined method list can be applied to specific interfaces and lines), AAA method lists that are used with fax applications are applied globally.

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

Examples

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

```
application
service app_libretto_onramp9 tftp://server-1/tftpboot/scripts/
param authen-list fax
param authentication enable
```

Related Commands

Command	Description
aaa authentication	Enable AAA accounting of requested services for billing or security purposes.
param authen-method	Specifies the authentication method for a TCL application.
param authentication enable	Enables AAA authentication services for a TCL application.

param authen-method

To specify an authentication, authorization, and accounting (AAA) authentication method for a Tool Command Language (Tcl) application, use the **param authen-method**command in application configuration mode. To disable the authentication method for a Tcl application, use the **no** form of this command.

param authen-method {**prompt-user** | **ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}
no param authen-method {**prompt-user** | **ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}

Syntax Description

prompt user	User is prompted for the Tcl application account identifier.
ani	Calling party telephone number (automatic number identification or ANI) is used as the Tcl application account identifier.
dnis	Called party telephone number (dialed number identification service or DNIS) is used as the Tcl application account identifier.
gateway	Router-specific name derived from the host name and domain name is used as the Tcl application account identifier, displayed in the following format: *router-name.domain-name*.
redialer id	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	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.

Command Default

No default behavior or values

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice authen-method** command in application configuration mode.

Usage Guidelines

Normally, when AAA is 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 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 configures 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:

```
application
service app_libretto_onramp9 tftp://server-1/tftpboot/scripts/
param authen-method gateway
```

Related Commands

Command	Description
param authentication enable	Enables AAA authentication services for a Tcl application.

param authentication enable

To enable authentication, authorization, and accounting (AAA) services for a Tool Command Language (TCL) application, use the **param authentication enable**command in application configuration mode. To disable authentication for a TCL application, use the **no** form of this command.

param authentication enable
no param authentication enable

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice authentication enable**command.

Usage Guidelines

This command enables AAA authentication services for a TCL application if a AAA authentication method list has been defined using the **aaa authentication** command and the **param authen-list** command.

Examples

The following example enables AAA authentication for an authentication method list (called "fax") with outbound store-and-forward fax.

```
application
service app_libretto_onramp9 tftp://server-1/tftpboot/scripts/
param authen-list fax
param authentication enable
```

Related Commands

Command	Description
aaa authentication	Enables AAA accounting of requested services when you use RADIUS or TACACS+.
param authen-list	Specifies the name of an authentication method list for a Tool Command Language (TCL) application.
param authen-method	Specifies the authentication method for a TCL application.

param convert-discpi-after-connect

To enable or disable conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state, use the **param convert-discpi-after-connect**command in application parameter configuration mode. To restore this parameter to the default value, use the **no** form of this command.

param convert-discpi-after-connect {**enable** | **disable**}
no param convert-discpi-after-connect {**enable** | **disable**}

Syntax Description

enable	Convert a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
disable	Revert to a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) when the call is in the active state.

Command Default

Enabled

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice default disc-prog-ind-at-connect** command.

Usage Guidelines

This command has no effect if the call is not in the active state. This command is available for the session_xwork package. If you are configuring this parameter for a package, you must first use the command **package session x_work**.

If you are configuring this parameter for a service, use the following commands:

service *name url*

paramspace session_xwork convert-discpi-after-connect

Examples

The following example shows conversion enabled for a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8):

```
application
package session_xwork
param convert-discpi-after-connect enable
```

Related Commands

Command	Description
call application voice default disc-prog-ind-at-connect	Converts a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.

Command	Description
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the personal identification number (PIN) for an application.
param redirect-number	Defines the telephone number to which a call is redirected--for example, the operator telephone number of the service provider--for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param 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.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param dsn-script

To specify the VoiceXML application to which the off-ramp mail application hands off calls for off-ramp delivery status notification (DSN) and message disposition notification (MDN) e-mail messages, use the **param dsn script**command in application parameter configuration mode. To remove the application, use the **no** form of this command.

param dsn-script *application-name*
no param dsn-script *application-name*

Syntax Description

application-name	Name of the VoiceXML application to which the off-ramp mail application hands off the call when the destination answers.

Command Default

No default behavior or values

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice dsn-script** command.

Usage Guidelines

When the off-ramp gateway receives a DSN or MDN e-mail message, it handles it in the same way as a voice e-mail trigger message. The dial peer is selected on the basis of dialed number identification service (DNIS), and the mail application hands off the call to the VoiceXML application that is configured with this command.

Examples

The following example shows how to define the DSN application and how to apply it to a dial peer:

```
application
service offramp-mapp tftp://sample/tftp-users/tcl/app_voicemail_offramp.tcl
param dsn-script dsn-mapp-test
!
dial-peer voice 1000 mmoip
 application offramp-mapp
 incoming called-number 555....
 information-type voice
```

Related Commands

Command	Description
call application voice dsn-script	Specifies the VoiceXML application to which the off-ramp mail application hands off calls for off-ramp DSN and MDN e-mail messages.

param event-log

To enable or disable logging for linkable Tcl functions (packages), use the **param event-log** command in application parameter configuration mode. To restore this parameter to the default value, use the **no** form of this command.

param event-log {**enable** | **disable**}
no param event-log {**enable** | **disable**}

Syntax Description

enable	Event logging is enabled.
disable	Event logging is disabled.

Command Default

No default behavior or values

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice event-log** command.

Usage Guidelines

This command is available for the built-in common voice application package. If you are configuring this parameter for that package, you must first use the command **package appcommon**.

If you are configuring this parameter for a service, use the following commands:

service *name url*

paramspace appcommon event-log

If you are configuring event logging for all voice applications, use the **event-log** command in application configuration monitor mode.

Note To prevent event logging from adversely impacting system resources for production traffic, the gateway uses a throttling mechanism. When free processor memory drops below 20%, the gateway automatically disables all event logging. It resumes event logging when free memory rises above 30%. While throttling is occurring, the gateway does not capture any new event logs even if event logging is enabled. You should monitor free memory and enable event logging only when necessary for isolating faults.

Examples

The following example shows event-logging disabled for the built-in common voice application package:

```
application
package appcommon
param event-log disable
```

Related Commands

Command	Description
call application voice event-log	Enables event logging for a specific voice application.
event-log	Enables event logging for applications.
package appcommon	Configures parameters in the built-in common voice application package.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected--for example, the operator telephone number of the service provider--for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param 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.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param fax-dtmf

To direct the fax detection interactive voice response (IVR) application to recognize a specified digit to indicate a fax call in default-voice and default-fax modes, use the **param fax-dtmf** command in application parameter configuration mode. To remove configuration of this digit, use the **no** form of this command.

param fax-dtmf {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | ***** | **#**}
no param fax-dtmf {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | ***** | **#**}

Syntax Description

0 | 1| 2| 3| 4| 5| 6| 7| 8| 9| *| #	The telephone keypad digit processed by the calling party to indicate a fax call, in response to the audio prompt that plays during the default-voice or default-fax mode of the fax detection IVR application.

Command Default

2

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command is introduced to replace the **call application voice fax-dtmf** command.

Usage Guidelines

This command is useful only when the fax detection IVR application is being configured in default-voice mode or default-fax mode as defined by the **param mode** command.

If you also configure voice DTMF using the **param voice-dtmf** command, you must use different numbers for the voice and fax DTMF digits.

Examples

The following example selects DTMF digit 1 to indicate a fax call:

```
application
service faxdetect tftp://sample/tftp-users/tcl/app_fax_detect.2.x.x.tcl
param fax-dtmf 1
```

Related Commands

Command	Description
call application voice fax-dtmf	Directs the fax detection IVR application to recognize a specified digit to indicate a fax call in default-voice and default-fax modes.
param mode	Configures the call transfer mode for a package.
param voice-dtmf	Directs an application to recognize a specified digit to indicate a voice call in default-voice and default-fax modes.

param 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 **param global password** command in application parameter configuration mode. To restore the default value, use the **no** form of this command.

param global-password *password*
no param global-password *password*

Syntax Description

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.

Command Default

No password is defined

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command is introduced to replace the **call application voice global-password** command.

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:

```
application
service onramp tftp://sample/tftp-users/tcl/app_libretto_onramp9.tcl
param global-password abercrombie
```

Related Commands

Command	Description
call application voice global-password	Defines a password to be used with CiscoSecure for Windows NT when using store-and-forward fax on a voice feature card.

param language

To configure the language parameter in a service or package on the gateway, use the **param language**command in application parameter configuration mode. There is no **no** form of this command.

param language *prefix*

Syntax Description

prefix	Two-character prefix for the language; for example, "*en*" for English or "*ru*" for Russian.

Command Default

No default behavior or values

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call language voice** command.

Usage Guidelines

Before you configure the language parameter, you must load the language package using the **package language** command in application configuration mode.

If you are configuring this parameter for a service, use the following commands:

service *name url*

param language *prefix*

Examples

The following example adds Russian (*ru*) as a Tcl module and configures the debitcard application to use Russian for prompts:

```
application
package language ru tftp://box/unix/scripts/multi-lang/ru_translate.tcl
service debitcard tftp://server-1/tftpboot/scripts/app_debitcard.2.0.2.8.tcl
param language ru
```

Related Commands

Command	Description
call application voice set-location	Defines the category and location of audio files that are used for dynamic prompts by the specified IVR application (Tcl or VoiceXML).
call language voice	Configures an external Tcl module for use with an IVR application.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.

Command	Description
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected--for example, the operator telephone number of the service provider--for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param 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.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param mail-script

To specify the VoiceXML application to which the off-ramp mail application hands off a call when the destination telephone answers, use the **param mail-script**command in application parameter configuration mode. To remove the application, use the **no** form of this command.

param mail-script *application-name*
no param mail-script *application-name*

Syntax Description

application-name	Name of the VoiceXML application to which the off-ramp mail application hands off the call when the destination answers.

Command Default

No default behavior or values

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command is introduced to replace the **call application voice mail-script** command.

Usage Guidelines

- To configure the mail application onto the gateway, use the **application** command.
- The off-ramp mail application must be configured in the Multimedia Mail over Internet Protocol (MMoIP) dial peer that matches the telephone number contained in the header of the incoming e-mail message.
- The off-ramp mail application must use the Tool Command Language (Tcl) script named "app_voicemail_offramp.tcl" that is provided by Cisco. You can download this Tcl script from the Cisco website by following this path:

Cisco.com > Technical Support & Documentation > Tools & Resources > Software Downloads > Access Software > TclWare

Examples

The following example shows that the off-ramp mail application named "offramp-mapp" hands calls to the application named "mapp-test" if the telephone number in the e-mail header is seven digits beginning with 555 :

```
application
service offramp-mapp tftp://sample/tftp-users/tcl/app_voicemail_offramp.tcl
param mail-script mapp-test
!
dial-peer voice 1001 mmoip
 application offramp-mapp
 incoming called-number 555....
 information-type voice
```

Related Commands

Command	Description
call application voice mail-script	Specifies the VoiceXML application to which the off-ramp mail application hands off a call when the destination telephone answers.

param mode

To configure the call transfer mode for a package, use the **param mode** command in application parameter configuration mode. To reset to the default, use the **no** form of this command.

param mode {**redirect** | **redirect-at-alert** | **redirect-at-connect** | **redirect-rotary** | **rotary**}
no param mode

Syntax Description

redirect	Gateway redirects the call leg to the redirected destination number.
redirect-at-alert	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the alert state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports Two B-Channel Transfer (TBCT).
redirect-at-connect	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the connect state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports TBCT.
redirect-rotary	Gateway redirects the call leg to the redirected destination number. If redirection fails, the gateway places a rotary call to the redirected destination number and hairpins the two call legs. For TBCT, this mode is the same as **redirect-at-connect**.
rotary	Gateway places a rotary call for the outgoing call leg and hairpins the two call legs. Call redirection is not invoked. This is the default.

Command Default

Rotary method; call redirection is not invoked.

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is used to configure call transfer mode for a package only. You can then configure one or more services to use that package. Alternatively, you can use the **paramspace callsetup mode**command to configure call transfer mode for a service, or standalone application.

Examples

The following example shows the call transfer method set to redirect for the call setup package:

```
application
package callsetup
param mode redirect
```

Related Commands

Command	Description
call application voice mode	Directs the fax detection IVR application to operate in one of its four connection modes.
call application voice transfer mode	Specifies the call-transfer method for Tcl)or VoiceXML applications.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param pin-len	Defines the number of characters in the personal identification number (PIN) for an application.
param redirect-number	Defines the telephone number to which a call is redirected--for example, the operator telephone number of the service provider--for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param 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.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param pin-len

To define the number of characters in the personal identification number (PIN) for an application, use the **param pin len**command in application parameter configuration mode. To disable the PIN for the designated application, use the no form of this command.

param pin-len *number*
no param pin-len *number*

Syntax Description

number	Number of allowable characters in PINs associated with the specified application. Range is from 0 to 10. The default is 4.

Command Default

No default behavior or values

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice pin-len** command.

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 PIN for the specified application and to pass that information to the specified application.

To configure the PIN length for a package, load the package using the **package** command before using the **param pin-len** command. To configure the PIN length for a service, use the **service** command before using the **param pin-len** command.

Examples

The following example shows how to define a PIN length of 8 characters for a Tcl digit collection package:

```
application
package digcl.tcl
param pin-len 8
```

The following example shows how to define a PIN length of 8 characters for a debit card application:

```
application
service debitcard tftp://tftp-server/dc/app_debitcard.tcl
param pin-len 8
```

Related Commands

Command	Description
call application voice pin-len	Defines the number of characters in the PIN for the designated application.
param	Loads and configures parameters in a package or a service (application).

Command	Description
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param redirect-number	Defines the telephone number to which a call is redirected--for example, the operator telephone number of the service provider--for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param 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.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param prompt

To direct the fax detection interactive voice response (IVR) application to use the specified audio file as a user prompt, use the **param prompt** command in application parameter configuration mode. To disable use of this audio file, use the **no** form of this command.

param prompt *prompt-url*
no param prompt *prompt-url*

Syntax Description

prompt-url	The URL or Cisco IOS file system (IFS) location on the TFTP server for the audio file containing the prompt for the application.

Command Default

The prompt space is empty and no prompt is played.

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command is introduced to replace the **call application voice prompt** command.

Usage Guidelines

This command is useful only in the listen-first, default-voice, and default-fax modes of the fax detection application.

Audio files should be a minimum of 9 seconds long so that callers do not hear silence during the initial CNG detection period. Any .au file can be used; formats are described in the Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.4.

Examples

The following example associates the audio file" promptfile.au" with the application file "fax_detect", and the application with the inbound POTS dial peer:

```
application
service fax_detect tftp://users/scripts/app_fax_detect.2.x.x.tcl
param mode default-voice
param prompt promptfile.au
dial-peer voice 302 pots
 application fax_detect
```

Related Commands

Command	Description
call application voice prompt	Directs the fax detection interactive voice response (IVR) application to use the specified audio file as a user prompt.

param redirect-number

To define the telephone number to which a call is redirected--for example, the operator telephone number of the service provider--for an application, use the **param redirect number** command in application parameter configuration mode. To cancel the redirect telephone number, use the **no** form of this command.

param redirect-number *number*
no param redirect-number *number*

Syntax Description

number	Designated operator telephone number of the service provider (or any other number designated by the customer). This is the number where calls are terminated when, for example, allowed debit time has run out or the debit amount is exceeded.

Command Default

No default behavior or values

Command Modes

Application parameter configuration

Command History

Cisco IOS Release	Cisco Product	Modification
12.3(14)T	Cisco CME 3.3	This command was introduced to replace the **call application voice redirect-number** command.

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 is redirected.

To configure the redirect number for a package, load the package using the **package** command before using the **param redirect-number**command. To configure the redirect number for a service, use the **service** command before using the **param redirect-number**command.

Examples

The following example shows how to define a redirect number for the application named "prepaid":

```
application
service prepaid tftp://tftp-server/scripts/prepaid.tcl
param redirect-number 5550111
```

Related Commands

Command	Description
call application voice redirect-number	Defines the telephone number to which a call is redirected--for example, the operator telephone number of the service provider--for the designated application.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.

Command	Description
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the personal identification number (PIN) for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param 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.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.
service	Loads and configures a specific, standalone application on a dial peer.

param reroutemode

To configure the call transfer reroutemode (call forwarding) for a package, use the **param reroutemode** command in application parameter configuration mode. To reset to the default, use the **no** form of this command.

param reroutemode {**redirect** | **redirect-at-alert** | **redirect-at-connect** | **redirect-rotary** | **rotary**}
no param reroutemode

Syntax Description

redirect	Two call legs are directly connected. Supports RTPvt.
redirect-at-alert	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the alert state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports Two B-Channel Transfer (TBCT).
redirect-at-connect	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the connect state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports TBCT.
redirect-rotary	Two call legs are directly connected (redirect). If that fails, the two call legs are hairpinned on the gateway (rotary).
rotary	Gateway places a rotary call for the outgoing call leg and hairpins the two calls together. Release-to-Pivot (RTPvt) is not invoked. This is the default.

Command Default

Rotary method; RTPvt is not invoked.

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is used to configure call forwarding for a package only. You can then configure one or more services to use that package. Alternatively, you can use the **paramspace callsetup reroutemode**command to configure call forwarding for a service, or standalone application.

Redirect-rotary is the preferred transfer method because it ensures that a call-redirect method is always selected, provided that the call leg is capable of it.

Examples

The following example shows the call forwarding method set to redirect for the call setup package:

```
application
package callsetup
param reroutemode redirect
```

Related Commands

Command	Description
call application voice transfer reroute-mode	Specifies the call-forwarding behavior of a Tcl application.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected--for example, the operator telephone number of the service provider--for an application.
param 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.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param retry-count

To define the number of times that a caller is permitted to reenter the personal identification number (PIN) for a package, use the **param retry count** command in application parameter configuration mode. To cancel the configured retry count, use the **no** form of this command.

param retry-count *number*
no param retry-count *number*

Syntax Description

number	Number of times the caller is permitted to reenter PIN digits. Range is 1 to 5. The default is 3.

Command Default

3

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)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 how many times a user can reenter a PIN.

To configure the PIN retry count for a package, load the package using the **package** command before using the **param retry-count** command. To configure the PIN retry count for a service, use the **service** command before using the **param retry-count**command.

Examples

The following example shows how to configure the PIN retry count in a package so that a user can reenter a PIN two times before being disconnected.

```
application
package sample1.tcl
param retry-count 2
```

The following example shows how to configure the PIN retry count in a debit card application so that a user can reenter a PIN two times before being disconnected.

```
application
service debitcard tftp://tftp-server/dc/app_debitcard.tcl
param retry-count 2
```

Related Commands

Command	Description
call application voice retry-count	Defines the number of times that a caller is permitted to reenter the PIN for the designated application.
param	Loads and configures parameters in a package or a service (application).

Command	Description
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected--for example, the operator telephone number of the service provider--for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param security

To configure security for linkable Tcl functions (packages), use the **param security** command in application parameter configuration mode. To restore this parameter to the default value, use the **no** form of this command.

param security {**trusted** | **untrusted**}
no param security {**trusted** | **untrusted**}

Syntax Description

trusted	Automatic number identification (ANI) is not blocked.
untrusted	ANI is blocked.

Command Default

No default behavior or values

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice security** command.

Usage Guidelines

This command is available for the built-in common voice application package. If you are configuring this parameter for that package, you must first use the command **package appcommon**.

If you are configuring this parameter for a service, use the following commands:

service *name url*

paramspace appcommon security {**trusted** | **untrusted**}

If an application is configured as a trusted application, it is trusted not to provide the calling number to the destination party, so ANI is always provided if available. Normally, the voice gateway does not provide the calling number (ANI) to a VoiceXML application if the caller ID is blocked. Caller ID is blocked if a call that comes into the voice gateway has the presentation indication field set to "presentation restricted". The session.telephone.ani variable is set to "blocked". When the **param security trusted** command is configured, the gateway does not block caller ID; it provides the calling number to the VoiceXML application. If the keyword of this command is set to untrusted, caller ID is blocked.

To enable GTD (Generic Transparency Descriptor) parameters in call signaling messages to map to VoiceXML and Tcl session variables, the **param securit y trusted** command must be configured. If this command is not configured, the VoiceXML variables that correspond to GTD parameters are marked as not available. For a detailed description of the VoiceXML and Tcl session variables, see the Cisco VoiceXML Programmer's Guide and the Tcl IVR API Version 2.0 Programmer's Guide, respectively.

Examples

The following example shows using the **param security trusted** command to set the security level of the common application package to "trusted" so that automatic number identification (ANI) is not blocked.

```
application
package appcommon
param security trusted
```

Related Commands

Command	Description
call application voice security trusted	Sets the security level of a VoiceXML application to "trusted" so that ANI is not blocked.
package appcommon	Configures parameters in the built-in common voice application package.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected--for example, the operator telephone number of the service provider--for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param 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.
paramspace appcommon security	Configures security for a service (application).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.
service	Loads and configures a specific, standalone application on a dial peer.

param uid-len

To define the number of characters in the user identification number (UID) for a package, use the **param uid-len**command in application parameter configuration mode. To restore the default setting for this command, use the **no** form of this command.

param uid-len *number*
no param uid-len *number*

Syntax Description

number	Number of allowable characters in UIDs that are associated with the specified application. Range is from 1 to 20. Default is 10.

Command Default

10 characters

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice uid-length** command.

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.

This command is available for the built-in common voice application package. If you are configuring this parameter for that package, you must first use the command **package appcommon**. If you are configuring this parameter for a service, you must first use the **service** command

Examples

The following example configures the UID length to 20 in a package.

```
application
package sample1.tcl
param uid-len 20
```

The following example configures the UID length to 20 in a debit-card application.

```
application
service debitcard tftp://tftp-server/dc/app_debitcard.tcl
param uid-len 20
```

Related Commands

Command	Description
call application voice uid-length	Defines the number of characters in the UID for the designated application and to pass that information to the specified application.
package appcommon	Configures parameters in the built-in common voice application package.

Command	Description
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected--for example, the operator telephone number of the service provider--for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param 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.
param security	Configures security for linkable Tcl functions (packages).
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param voice-dtmf

To direct the fax detection interactive voice response (IVR) application to recognize a specified digit to indicate a voice call, use the **param voice dtmf** command in application parameter configuration mode. To remove configuration of this digit, use the **no** form of this command.

param voice-dtmf {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | ***** | **#**}
no param voice-dtmf {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | ***** | **#**}

Syntax Description

0 | 1| 2| 3| 4| 5| 6| 7| 8| 9| *| #	The telephone keypad button pressed by the calling party to indicate a voice call, in response to the audio prompt configured in default-voice and default-fax mode of the fax detection IVR application.

Command Default

1

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command is introduced to replace the **call application voice voice-dtmf**command.

Usage Guidelines

This command is useful only when the fax detection IVR application is being configured in default-voice mode or default-fax mode, as defined by the **param mode** command.

If you also configure voice DTMF using the **param voice-dtmf** command, you must use different numbers for the voice and fax DTMF digits.

Examples

The following example selects digit 2 Dual tone multifrequency (DTMF) to indicate a voice call:

```
application
service faxdetect tftp://sample/tftp-users/tcl/app_fax_detect.2.x.x.tcl
param voice-dtmf 2
dial-peer voice 302 pots
 application fax_detect
```

Related Commands

Command	Description
call application voice voice-dtmf	Directs the fax detection IVR application to recognize a specified digit to indicate a voice call.
param mode	Configures the call transfer mode for a package.
param fax-dtmf	Directs an application to recognize a specified digit to indicate a fax call in default-voice and default-fax modes.

param warning-time

To define the number of seconds of warning that a user receives before the allowed calling time expires use the **param warning time** command in application parameter configuration mode. To remove the configured warning period, use the **no** form of this command.

param warning-time *number*
no param warning-time *number*

Syntax Description

number	Length of the warning period, in seconds, before the allowed calling time expires. Range is from 10 to 600. This argument has no default value.

Command Default

No default behavior or values

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice warning-time** command.

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 seconds in the warning period before the allowed calling time expires.

This command is available for the built-in common voice application package. If you are configuring this parameter for that package, you must first use the command **package appcommon**. If you are configuring this parameter for a service, you must first use the **service** command

Examples

The following example configures the warning time parameter to 30 seconds in a package.

```
application
package sample1.tcl
param warning-time 30
```

The following example configures the warning time parameter to 30 seconds in a debit-card application.

```
application
service debitcard tftp://tftp-server/dc/app_debitcard.tcl
param warning-time 30
```

Related Commands

Command	Description
call application voice warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.
package appcommon	Configures parameters in the built-in common voice application package.

Command	Description
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected--for example, the operator telephone number of the service provider--for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param 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.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in theUID for a package.
service	Loads and configures a specific, standalone application on a dial peer.

paramspace

To enable an application to use parameters from the local parameter space of another application, use the **paramspace** command in application service configuration mode. To return to the default parameter namespace for this parameter, use the **no** form of this command.

paramspace *parameter-namespace* *parameter-name* *parameter-value*
no **paramspace** *parameter-namespace* *parameter-name* *parameter-value*

Syntax Description

parameter-namespace	Namespace of the parameter from which you want to use parameters.
parameter-name	Parameter to use.
parameter-value	Value of the parameter.

Command Default

No default behavior or values

Command Modes

Application service configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

To avoid problems with applications using the same parameter names, the *parameter namespace,* or *parameterspace* concept is provided. When an application is defined on the gateway, its parameter namespace is automatically defined. This is known as the application's s local parameterspace. When you use the **param** command to configure an application's parameters, the parameters available for configuration are those contained in the local parameterspace.

If you want to use parameter definitions found in different parameterspace, you can use the **paramspace***parameter-namespaceparameter-name parameter-value*command to map the application's parameters to a different parameterspace. This allows that application to use the parameter definitions found in the new parameterspace, in addition to its local parameterspace.

Examples

The following example shows a debit card service configured to use parameters from an English language translation package:

```
application
service debitcard tftp://server-1//tftpboot/scripts/app_debitcard.2.0.2.8.tcl
paramspace english language en
  paramspace english index 1
  paramspace english prefix en
  paramspace english location tftp://server-1//tftpboot/scripts/au/en/
```

Related Commands

Command	Description
param	Loads and configures parameters in a package or a service (application) on the gateway.

Command	Description
paramspace appcommon event-log	Enables or disables logging for a service (application).
paramspace appcommon security	Configures security for a service (application).
paramspace callsetup mode	Configures the call transfer mode for an application.
paramspace callsetup reroutemode	Configures the call reroute mode (call forwarding) for an application.
paramspace language	Defines the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML).

paramspace appcommon event-log

To enable or disable logging for a service (application), use the **paramspace appcommon event-log** command in application service configuration mode. There is no **no** form of this command.

paramspace appcommon event-log {**enable** | **disable**}

Syntax Description

enable	Event logging is enabled.
disable	Event logging is disabled.

Command Default

No default behavior or values

Command Modes

Application service configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice event-log** command.

Usage Guidelines

Use this command to configure event logging for a service (application).

If you are configuring event logging for a package only, use the **package appcommon** command in application-parameter configuration mode.

If you are configuring event logging for all voice applications, use the **event-log** command in application-configuration monitor mode.

Note To prevent event logging from adversely impacting system resources for production traffic, the gateway uses a throttling mechanism. When free processor memory drops below 20%, the gateway automatically disables all event logging. It resumes event logging when free memory rises above 30%. While throttling is occurring, the gateway does not capture any new event logs even if event logging is enabled. You should monitor free memory and enable event logging only when necessary for isolating faults.

Examples

The following example shows event-logging disabled for a debit-card application.

```
application
service debitcard tftp://tftp-server/dc/app_debitcard.tcl
paramspace appcommon event-log disable
```

Related Commands

Command	Description
call application voice event-log	Enables event logging for a specific voice application.
paramspace	Enables an application to use parameters from the local parameter space of another application.

Command	Description
paramspace appcommon security	Configures security for a service (application).
paramspace callsetup mode	Configures the call transfer mode for an application.
paramspace callsetup reroutemode	Configures the call reroute mode (call forwarding) for an application.
paramspace language	Defines the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML).

paramspace appcommon security

To configure security for a service (application), use the **paramspace appcommon security** command in application service configuration mode. To return to the default parameter namespace for this parameter, use the **no** form of this command.

paramspace appcommon security {**trusted** | **untrusted**}
no paramspace appcommon security {**trusted** | **untrusted**}

Syntax Description

trusted	Automatic number identification (ANI) is not blocked.
untrusted	ANI is blocked.

Command Default

No default behavior or values

Command Modes

Application service configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice security** command.

Usage Guidelines

This command is available for the built-in common voice application package. If you are configuring this parameter for the built-in common voice application package, use the command **param security** command.

If an application is configured as a trusted application, it is trusted not to provide the calling number to the destination party, so ANI is always provided if available. Normally, the voice gateway does not provide the calling number (ANI) to a VoiceXML application if the caller ID is blocked. Caller ID is blocked if a call that comes into the voice gateway has the presentation indication field set to "presentation restricted". The session.telephone.ani variable is set to "blocked". When the **paramspace appcommon security trusted**command is configured, the gateway does not block caller ID; it provides the calling number to the VoiceXML application. If the keyword of this command is set to untrusted, caller ID is blocked.

To enable GTD (Generic Transparency Descriptor) parameters in call signaling messages to map to VoiceXML and Tcl session variables, the **paramspace appcommon security trusted** command must be configured. If this command is not configured, the VoiceXML variables that correspond to GTD parameters are marked as not available. For a detailed description of the VoiceXML and Tcl session variables, see the Cisco VoiceXML Programmer's Guide and the Tcl IVR API Version 2.0 Programmer's Guide, respectively.

Examples

The following example shows security configured for a debit card application. The security level of the application is set to "trusted" so that automatic number identification (ANI) is not blocked.

```
application
service debitcard tftp://tftp-server/dc/app_debitcard.tcl
paramspace appcommon security trusted
```

Related Commands

Command	Description
call application voice security trusted	Sets the security level of a VoiceXML application to "trusted" so that ANI is not blocked.
paramspace	Enables an application to use parameters from the local parameter space of another application.
paramspace appcommon event-log	Enables or disables logging for a service (application).
paramspace callsetup mode	Configures the call transfer mode for an application.
paramspace callsetup reroutemode	Configures the call reroute mode (call forwarding) for an application.
paramspace language	Defines the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML).

paramspace callsetup mode

To configure the call transfer mode for an application, use the **paramspace callsetup mode** command in application service configuration mode. To reset to the default, use the **no** form of this command.

paramspace callsetup mode {**redirect** | **redirect-at-alert** | **redirect-at-connect** | **redirect-rotary** | **rotary**}
no paramspace callsetup mode

Syntax Description

redirect	Gateway redirects the call leg to the redirected destination number.
redirect-at-alert	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the alert state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports Two B-Channel Transfer (TBCT).
redirect-at-connect	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the connect state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports TBCT.
redirect-rotary	Gateway redirects the call leg to the redirected destination number. If redirection fails, the gateway places a rotary call to the redirected destination number and hairpins the two call legs. For TBCT, this mode is the same as **redirect-at-connect**.
rotary	Gateway places a rotary call for the outgoing call leg and hairpins the two call legs. Call redirection is not invoked. This is the default.

Command Default

Rotary method; call redirection is not invoked.

Command Modes

Application service configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice transfer mode** command.

Usage Guidelines

Use this command to configure the call transfer mode for a service, or standalone application. Alternatively, you can use the **package callsetup**and **param mode** commands to configure call transfer mode for a package only, and then configure one or more services to use that package.

This command determines whether a voice application can invoke TBCT or RTPvt.

Redirect-rotary is the preferred transfer method because it ensures that a call-redirect method is always selected if the call leg is capable of it.

Examples

The following example shows the call method set to redirect for a debit-card application:

```
application
service debitcard tftp://tftp-server/dc/app_debitcard.tcl
paramspace callsetup mode redirect
```

Related Commands

Command	Description
call application voice transfer mode	Specifies the call-transfer method for Tcl)or VoiceXML applications.
package callsetup	Configures parameters in the built-in call-setup package.
param mode	Configures the call-transfer mode for a package.
paramspace	Enables an application to use parameters from the local parameter space of another application.
paramspace appcommon event-log	Enables or disables logging for a service (application).
paramspace appcommon security	Configures security for a service (application).
paramspace callsetup reroutemode	Configures the call reroute mode (call forwarding) for an application.
paramspace language	Defines the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML).

paramspace callsetup reroutemode

To configure the call reroute mode (call forwarding) for an application, use the **paramspace callsetup reroutemode** command in application service configuration mode. To reset to the default, use the **no** form of this command.

paramspace callsetup reroutemode {**redirect** | **redirect-at-alert** | **redirect-at-connect** | **redirect-rotary** | **rotary**}
no paramspace callsetup reroutemode

Syntax Description

redirect	Gateway redirects the call leg to the redirected destination number.
redirect-at-alert	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the alert state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports Two B-Channel Transfer (TBCT).
redirect-at-connect	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the connect state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports TBCT.
redirect-rotary	Gateway redirects the call leg to the redirected destination number. If redirection fails, the gateway places a rotary call to the redirected destination number and hairpins the two call legs. For TBCT, this mode is the same as **redirect-at-connect**.
rotary	Gateway places a rotary call for the outgoing call leg and hairpins the two call legs. Call redirection is not invoked. This is the default.

Command Default

Rotary method; call redirection is not invoked.

Command Modes

Application service configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice transfer reroute-mode**command.

Usage Guidelines

This command is used to configure the call forward mode for a service, or standalone application. Alternatively, you can use the **package callsetup param reroutemode** command to configure call forward mode for a package only, and then configure one or more services to use that package.

This command determines whether a voice application can invoke TBCT or RTPvt.

Redirect-rotary is the preferred transfer method because it ensures that a call-redirect method is always selected if the call leg is capable of it.

Examples

The following example shows the call forward method set to redirect for a debitcard application:

```
application
service debitcard tftp://tftp-server/dc/app_debitcard.tcl
paramspace callsetup reroutemode redirect
```

Related Commands

Command	Description
call application voice transfer reroute-mode	Specifies the call-forwarding behavior of a Tcl application.
paramspace	Enables an application to use parameters from the local parameter space of another application.
paramspace appcommon event-log	Enables or disables logging for a service (application).
paramspace appcommon security	Configures security for a service (application).
paramspace callsetup mode	Configures the call transfer mode for an application.
paramspace language	Defines the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML).

paramspace language

To define the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML), use the **paramspace language**command in application service configuration mode. To remove these definitions, use the **no** form of this command.

To configure the language parameter in a service or package on the gateway, use the **param language** command in application service configuration mode.

paramspace *language* {**location** *location* | **index** *number* | **language** *prefix*}

Syntax Description

language	Name of the language package. Cisco IOS software includes some built-in language packages, such as English.
location *location*	URL of the audio files. Valid URLs refer to TFTP, FTP, HTTP, or RTSP servers, flash memory, or the removable disks on the Cisco 3600 series.
index *number*	Category group of the audio files (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, and audio files representing units of time--seconds, minutes, and hours--can be category 3. Range is from 0 to 4; 0 means all categories.
language *prefix*	Two-character code that identifies the language associated with the audio files. Valid entries are as follows: • **en** --English • **sp** --Spanish • **ch** --Mandarin • **aa** --all

Command Default

No location, index, or category is set.

Command Modes

Application service configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice language** and the **call application voice set-location** commands.

Usage Guidelines

Tcl scripts and VoiceXML documents can be stored in any of the following locations: On TFTP, FTP, or HTTP servers, in the flash memory on the gateway, or on the removable disks of the Cisco 3600 series. The audio files that they use can be stored in any of these locations, and on RTSP servers.

You can configure multiple set-location lines for a single application.

With the Pre-Paid Debitcard Multi-Language feature, you can create Tcl scripts and a two-character code for any language. See the Cisco Pre-Paid Debitcard Multi-Language Programmer's Reference.

With the multilanguage support for Cisco IOS IVR, you can create a Tcl language module for any language and any set of Text-to-Speech (TTS) notations for use with Tcl and VoiceXML applications. See the Enhanced Multi-Language Support for Cisco IOS Interactive Voice Response document.

Examples

The following example shows how to configure the **paramspace language**command for a debitcard application.

```
application
service debitcard tftp://server-1//tftpboot/scripts/app_debitcard.2.0.2.8.tcl
paramspace english language en
  paramspace english index 1
  paramspace english prefix en
  paramspace english location tftp://server-1//tftpboot/scripts/au/en/
```

Related Commands

Command	Description
call application voice language	Specifies the language for dynamic prompts used by an IVR application (Tcl or VoiceXML).
call application voice set-location	Defines the category and location of audio files that are used for dynamic prompts by the specified IVR application (Tcl or VoiceXML).
paramspace	Enables an application to use parameters from the local parameter space of another application.
paramspace appcommon event-log	Enables or disables logging for a service (application).
paramspace appcommon security	Configures security for a service (application).
paramspace callsetup mode	Configures the call transfer mode for an application.
paramspace callsetup reroutemode	Configures the call reroute mode (call forwarding) for an application.

paramspace session_xwork convert-discpi-after-connect

To enable or disable conversion of a DISCONNECT message with progress indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state, use the **paramspace session_xwork convert-discpi-after-connect** command in application-service configuration mode. To return to the default parameter namespace for this parameter, use the **no** form of this command.

paramspace session_xwork convert-discpi-after-connect {**enable** | **disable**}
no paramspace session_xwork convert-discpi-after-connect {**enable** | **disable**}

Syntax Description

enable	Convert a DISCONNECT message with progress indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
disable	Revert to a DISCONNECT message with progress indicator set to PROG_INBAND (PI=8) when the call is in the active state.

Command Default

Enabled

Command Modes

Application-service configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice default disc-prog-ind-at-connect** command.

Usage Guidelines

This command has no effect if the call is not in the active state. If you are configuring this parameter for a package, use the **package session xwork** command.

Examples

The following example shows conversion enabled for a DISCONNECT message with progress indicator set to PROG_INBAND (PI=8):

```
application
service callappl.tcl tftp://tftp-server/callappl.tcl
paramspace session_xwork convert-discpi-after-connect enable
```

Related Commands

Command	Description
call application voice default disc-prog-ind-at-connect	Converts a DISCONNECT message with progress indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
package session xwork	Configures parameters in the built-in session_xwork package.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with progress indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.

Command	Description
paramspace	Enables an application to use parameters from the local parameter space of another application.

pass-thru content

To enable the pass-through of Session Description Protocol (SDP) from in-leg to the out-leg, use the **pass-thru content** command either in global VoIP SIP configuration mode or dial-peer configuration mode. To remove a SDP header from a configured pass-through list, use the **no** form of the command.

pass-thru content[custom-sdp | sdp {mode | system}| unsupp]
no pass-thru content[custom-sdp | sdp {mode | system}| unsupp]

Syntax Description

custom-sdp	Enables the pass-through of custom SDP using SIP Profiles.
sdp	Enables the pass-through of SDP content.
mode	Enables the pass-through SDP mode.
system	Specifies that the pass-through configuration use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.
unsupp	Enables the pass-through of all unsupported content in a SIP message or request.

Command Default

Disabled

Command Modes

SIP configuration (conf-serv-sip)

Dial peer configuration (config-dial-peer)

Voice class tenant configuration (config-class)

Command History

Release	Modification
Cisco IOS 15.6(1)T, Cisco IOS XE 3.17S	This command was modified to add keyword: **custom-sdp**.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Examples

The following example shows how to configure pass-through of custom SDP using SIP Profiles peer rules in global VoIP SIP configuration mode:

```
Router(conf-serv-sip)# pass-thru content custom-sdp
```

The following example shows how to configure pass-through of custom SDP using SIP Profiles in dial-peer configuration mode:

```
Router(config-dial-peer)# voice-class sip pass-thru content custom-sdp
```

The following example shows how to configure pass-through of SDP in global VoIP SIP configuration mode:

```
Router(conf-serv-sip)# pass-thru content sdp
```

The following example shows how to configure pass-through of SDP in voice class tenant configuration mode:

```
Router(config-class)# pass-thru content sdp system
```

The following example shows how to configure pass-through of unsupported content types in dial-peer configuration mode:

```
Router(config-dial-peer)# voice-class sip pass-thru content unsupp
```

pass-thru headers

To enable the pass-through of a list of headers from a globally configured list, use the **pass-thru headers** command either in global VoIP SIP configuration mode or dial peer configuration mode. To remove a header from a configured pass-through list, use the **no** form of the command.

pass-thru headers [*number* **| unsupp]**
no pass-thru headers [*number* **| unsupp]**

Syntax Description

number	Specifies the sip-hdr-pass-thru list tag number to be linked as global value. Range is from 1 to 10000.
unsupp	Enables the pass-through of all unsupported headers.

Command Default

Disabled

Command Modes

SIP configuration (conf-serv-sip)

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
Cisco IOS 15.6(1)T, Cisco IOS XE 3.17S	This command was modified to add keyword: **system** in the dial-peer configuration mode.
Cisco IOS XE Bengaluru 17.4.1a	Introduced support for YANG models.

Examples

The following example shows how to configure pass-through of unsupported headers in global VoIP SIP configuration mode:

```
Router(conf-serv-sip)# pass-thru headers unsupp
```

The following example shows how to configure pass-through of unsupported headers in dial-peer configuration mode:

```
Router(config-dial-peer)# voice-class sip pass-thru headers unsupp
```

Related Commands

Command	Description
pass-thru	Passes the Session Description Protocol (SDP) transparently from in-leg to the out-leg with no media negotiation.
passthru-hdr-unsupp	Enables the pass-thru of all unsupported headers.
voice class sip-hdr-passthrulist	Configures list of headers to be passed through.

passthru-hdr

To add a header name to a configured pass-through list, use the **passthru-hdr** command in voice class configuration mode. To remove a header name from a configured pass-through list, use the **no** form of the command.

passthru-hdr *header-name*
no passthru-hdr [*header-name*]

Syntax Description

header-name	Header name of header to be added in the configured pass-through list.

Command Default

No header name is added to the configured pass-through list.

Command Modes

Voice class configuration mode (config-class)

Command History

Release	Modification
15.4(1)T	This command was introduced.
Cisco IOS XE Bengaluru 17.4.1a	Introduced support for YANG models.

Usage Guidelines

A pass-through list using the **voice class sip-hdr-passthrulist** command must be configured before adding a header name to the list.

You can configure a list of headers to be passed through. The list can contain any header except the mandatory headers shown in the table below:

Table 3: Mandatory Headers List

Mandtory Headers List		
ALSO	AUTHORIZATION	CALLID
CC_DIVERSION	CC_REDIRECT	CONTACT
CONTENT_DISP	CONTENT_ENCODING	CONTENT_LENGTH
CONTENT_TYPE	CISCO_GCID	CISCO_GUID
CSEQ	DATE	FROM
MAX_FORWARDS	MIME_VER	MIME_VER_VAL
PRIVACY	PRIVACY_ASSERTED_ID	PRIVACY_PREFERRED_ID
PROXY_AUTH	PROXY_AUTHENTICATE	RECORD_ROUTE
ROUTE	RTP_STAT	SESSION_EXPIRES
TIMESTAMP	TO	USER_AGENT
VIA	WWW_AUTHENTICATE	

Example

The following example shows how to configure a pass-through list using the **voice class sip-hdr-passthrulist** command and add the header name 'Resource-priority' to the list using the **passthru-hdr** command:

```
Device> enable
Device# configure terminal
Device(config)# voice class sip-hdr-passthrulist 101
Device(config-class)# passthru-hdr Resource-Priority
Device(config-class)# end
```

Related Commands

Command	Description
pass-thru	Passes the Session Description Protocol (SDP) transparently from in-leg to the out-leg with no media negotiation.
passthru-hdr-unsupp	Enables the pass-thru of all unsupported headers.
voice class sip-hdr-passthrulist	Configures list of headers to be passed through.
voice-classsip pass-thru	Passes the Session Description Protocol (SDP) transparently from in-leg to the out-leg with no media negotiation.

passthru-hdr-unsupp

To add the unsupported headers to a configured pass-through list and enable the pass-thru of all unsupported headers in the list, use the **passthru-hdr-unsupp** command in voice class configuration mode. To remove the unsupported headers from a configured pass-through list, use the **no** form of the command.

passthru-hdr-unsupp
no passthru-hdr-unsupp

Syntax Description

This command has no arguments or keywords.

Command Default

Unsupported headers are not included in the configured pass-through list.

Command Modes

Voice class configuration mode (config-class)

Command History

Release	Modification
15.4(1)T	This command was introduced.
Cisco IOS XE Bengaluru 17.4.1a	Introduced support for YANG models.

Usage Guidelines

A pass-through list using the **voice class sip-hdr-passthrulist** command must be configured before adding the unsupported headers to the list.

Example

The following example shows how to configure a pass-through list using the **voice class sip-hdr-passthrulist** command and add the unsupported headers to the list using the **passthru-hdr-unsupp** command:

```
Device> enable
Device# configure terminal
Device(config)# voice class sip-hdr-passthrulist 100
Device(config-class)# passthru-hdr-unsupp
Device(config-class)# end
```

Related Commands

Command	Description
pass-thru	Passes the Session Description Protocol (SDP) transparently from in-leg to the out-leg with no media negotiation.
passthru-hdr	Adds a header name to a configured pass-through list.
voice class sip-hdr-passthrulist	Configures list of headers to be passed through.
voice-classsip pass-thru	Passes the Session Description Protocol (SDP) transparently from in-leg to the out-leg with no media negotiation.

pattern

To match a call based on the entire Session Initiation Protocol (SIP) or telephone (TEL) uniform resource identifier (URI), use the **pattern**command in voice URI class configuration mode. To remove the match, use the **no** form of this command.

pattern *uri-pattern*
no pattern

Syntax Description

uri-pattern	Cisco IOS regular expression (regex) pattern that matches the entire URI. Can be up to 128 characters.

Command Default

No default behavior or values

Command Modes

Voice URI class configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- This command matches a regular expression pattern to the entire URI.
- When you use this command in a URI voice class, you cannot use any other pattern-matching command such as the **host**, **phone context**, **phone number**, or **user-id** commands.

Examples

The following example configures the voice class to match the entire SIP URI:

```
voice class uri r100 sip
 pattern elmo@cisco.com
```

Related Commands

Command	Description
destination uri	Specifies the voice class to use for matching the destination URI that is supplied by a voice application.
host	Matches a call based on the host field in a SIP URI.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the URI of an incoming call.
phone context	Filters out URIs that do not contain a phone-context field that matches the configured pattern.
phone number	Matches a call based on the phone number field in a TEL URI.
show dialplan incall uri	Displays which dial peer is matched for a specific URI in an incoming voice call.

Command	Description
show dialplan uri	Displays which outbound dial peer is matched for a specific destination URI.
user-id	Matches a call based on the user-id field in the SIP URI.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.

periodic-report interval through pulse-digit-detection

periodic-report interval

To configure periodic reporting parameters for gateway resource entities, use the **periodic-report interval**command in voice-class configuration mode. To disable the periodic reporting parameters configuration, use the **no** form of this command.

periodic-report interval *seconds*
no periodic-report interval *seconds*

Syntax Description

seconds	Periodic interval, in seconds. The range is from 30 to 21600.

Command Default

The periodic interval report parameters are disabled.

Command Modes

Voice-class configuration mode (config-class)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use the **periodic-report interval** command to periodically report the status of the monitoring resources to the external entity. The triggering takes place based on the preconfigured interval value. You can use the statistics collected by this method of reporting to collect information on resource usage.

Examples

The following example shows how to configure a resource group to trigger reporting every 180 seconds:

```
Router> enable
Router# configure terminal
Router(config)# voice class resource-group 1
Router(config-class)# periodic-report interval 180
```

Related Commands

Command	Description
debug rai	Enables debugging for Resource Allocation Indication (RAI).
rai target	Configures the SIP RAI mechanism.
resource (voice)	Configures parameters for monitoring resources, use the resource command in voice-class configuration mode.
show voice class resource-group	Displays the resource group configuration information for a specific resource group or all resource groups.
voice class resource-group	Enters voice-class configuration mode and assigns an identification tag number for a resource group.

permit hostname (SIP)

To store hostnames used during validation of initial incoming INVITE messages, use the **permit hostname** command in SIP-UA configuration mode or voice class tenant configuration mode. To remove a stored hostname, use the **no** form of this command.

permit hostname dns: *domain-name*
no permit hostname

Syntax Description

dns: *domain-name*	Domain name in DNS format. Domain names can be up to 30 characters in length; domain names exceeding 30 characters will be truncated.

Command Modes

SIP-UA configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

The **permit hostname** command allows you to specify hostnames in FQDN (fully qualified domain name) format used during validation of incoming initial INVITE messages. The length of the hostname can be up to 30 characters; hostnames exceeding 30 characters will be truncated. You can store up to 10 hostnames by repeating the **permit hostname** command.

Once configured, initial INVITEs with a hostname in the requested Universal Resource Identifier (URI) are compared to the configured list of hostnames. If there is a match, the INVITE is processed; if there is a mismatch, a "400 Bad Request - Invalid Host" is sent, and the call is rejected.

Note Before Software Release 12.4(9)T, hostnames in incoming INVITE-request messages were only validated when they were in IPv4 format; now you can specify hostnames in fully qualified domain name (FQDN) format.

Examples

The following example show you how to set the hostname to sip.example.com:

```
Router(config)# sip-ua
Router(conf-sip-ua)# permit hostname dns:sip.example.com
```

phone context

To filter out uniform resource identifiers (URIs) that do not contain a phone-context field that matches the configured pattern, use the **phone context** command in voice URI class configuration mode. To remove the pattern, use the **no** form of this command.

phone context *phone-context-pattern*
no phone context

Syntax Description

phone-context-pattern	Cisco IOS regular expression pattern to match against the phone context field in a SIP or TEL URI. Can be up to 32 characters.

Command Default

No default behavior or values

Command Modes

Voice URI class configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- Use this command with at least one other pattern-matching command, such as **host**, **phone number**, or **user-id**; using it alone does not result in any matches on the voice class.
- You cannot use this command if you use the **pattern** command in the voice class. The **pattern** command matches on the entire URI, whereas this command matches only a specific field.

Examples

The following example sets a match on the phone context in the URI voice class:

```
voice class uri 10 tel
 phone number ^408
 phone context 555
```

Related Commands

Command	Description
destination uri	Specifies the voice class to use for matching the destination URI that is supplied by a voice application.
host	Matches a call based on the host field in a SIP URI.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the URI of an incoming call.
pattern	Matches a call based on the entire SIP or TEL URI.
phone number	Matches a call based on the phone number field in a TEL URI.

Command	Description
show dialplan incall uri	Displays which dial peer is matched for a specific URI in an incoming voice call.
show dialplan uri	Displays which outbound dial peer is matched for a specific destination URI.
user-id	Matches a call based on the user-id field in the SIP URI.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.

phone number

To match a call based on the phone-number field in a telephone (TEL) uniform resource identifier (URI), use the **phone number** command in voice URI class configuration mode. To remove the pattern, use the **no** form of this command.

phone number *phone-number-pattern*
no phone number

Syntax Description

phone-number-pattern	Cisco IOS regular expression pattern to match against the phone-number field in a TEL URI. Can be up to 32 characters.

Command Default

No default behavior or values

Command Modes

Voice URI class configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- Use this command only in a voice class for TEL URIs.
- You cannot use this command if you use the **pattern** command in the voice class. The **pattern** command matches on the entire URI, whereas this command matches only a specific field.

Examples

The following example defines a voice class that matches on the phone number field in a TEL URI:

```
voice class uri r101 tel
 phone number ^408
```

Related Commands

Command	Description
debug voice uri	Displays debugging messages related to URI voice classes.
destination uri	Specifies the voice class to use for matching the destination URI that is supplied by a voice application.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the URI of an incoming call.
pattern	Matches a call based on the entire SIP or TEL URI.
phone context	Filters out URIs that do not contain a phone-context field that matches the configured pattern.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.

phone-proxy (dial peer)

To configure the phone proxy for the related dial peer, use the **phone-proxy** command in dial peer configuration mode. To remove the phone proxy for the related dial peer use the **no** form of the command.

phone-proxy *phone-proxy-name* **signal-addr ipv4** *ipv4-address* **cucm ipv4** *ipv4-address*

Syntax Description

phone-proxy-name	Name of the specific phone proxy.
signal-addr ipv4 *ipv4-address*	Specifies the SIP signal IPv4 address of the access side.
cucm ipv4 *ipv4-address*	Specifies the call manager server IPv4 address.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Example

The following example shows how to configure a phone proxy for the related dial peer:

```
Device(config)# dial-peer voice 1 voip
Device(config-dial-peer)# phone-proxy pp signal-addr ipv4 10.0.0.8 cucm ipv4 198.51.100.1
```

pickup direct

To define a feature code for a Feature Access Code (FAC) to access Pickup Direct on an analog phone, use the **pickup direct**command in STC application feature access-code configuration mode. To return the code to its default, use the **no** form of this command.

pickup direct *keypad-character*
no pickup direct

Syntax Description

keypad-character	Character string that can be dialed on a telephone keypad (0-9, *, #). Default: 6. Before Cisco IOS Release 12.4(20)YA, this is a single character. In Cisco IOS Release 12.4(20)YA and later releases, the string can be any of the following: • A single character (0-9, *, #) • Two digits (00-99) • Two to four characters (0-9, *, #) and the leading or ending character must be an asterisk (*) or number sign (#)

Command Default

The default value is 6.

Command Modes

STC application feature access-code configuration (config-stcapp-fac)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(20)YA	The length of the *keypad-character* argument was changed to 1 to 4 characters.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command changes the value of the feature code for Pickup Direct from the default (6) to the specified value.

In Cisco IOS Release 12.4(20)YA and later releases, if the length of the *keypad-character* argument is at least two characters and the leading or ending character of the string is an asterisk (*) or a number sign (#), phone users are not required to dial a prefix to access this feature. Typically, phone users dial a feature access code (FAC) consisting of a prefix plus a feature code, for example **6. If the feature code is 78#, the phone user dials only 78#, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that is already configured for another feature code, a speed-dial code, or the Redial FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that precludes or is precluded by another FAC, a speed-dial code, or the Redial FSD, you receive a message. If you configure a feature code to a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable phone user access to that feature.

To display a list of all FACs, use the **show stcapp feature codes** command.

Note This FAC is not supported by Cisco Unified Communications Manager.

Examples

The following example shows how to change the value of the feature code for Pickup Direct from the default (6). This configuration also changes the value of the prefix for all FACs from the default (**) to ##. With this configuration, a phone user must press ##3 on the keypad and then the ringing extension number to pick up an incoming call.

```
Router(config)# stcapp feature access-code
Router(config-stcapp-fac)# prefix ##
Router(config-stcapp-fac)# pickup direct 3
Router(config-stcapp-fac)# exit
```

Related Commands

Command	Description
pickup group	Defines a feature code for a feature access code (FAC) to Group Call Pickup from another group.
pickup local	Defines a feature code for a feature access code (FAC) to Group Call Pickup from the local group.
prefix (stcapp-fac)	Defines the prefix for feature access codes (FACs).
show stcapp feature codes	Displays all feature access codes (FACs).
stcapp feature access-code	Enables feature access codes (FACs) in STC application and enters STC application feature access-code configuration mode for changing values of the prefix and features codes from the default.

pickup group

To define a feature code for a feature access code (FAC) to access Group Call Pickup on an analog phone, use the **pickup group** command in STC application feature access-code configuration mode. To return the code to its default, use the **no** form of this command.

pickup group *keypad-character*
no pickup group

Syntax Description

keypad-character	Character string that can be dialed on a telephone keypad (0-9, *, #). Default: 4. Before Cisco IOS Release 12.4(20)YA, this is a single character. In Cisco IOS Release 12.4(20)YA and later releases, the string can be any of the following: • A single character (0-9, *, #) • Two digits (00-99) • Two to four characters (0-9, *, #) and the leading or ending character must be an asterisk (*) or number sign (#)

Command Default

The default value is 4.

Command Modes

STC application feature access-code configuration (config-stcapp-fac)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(20)YA	The length of the *keypad-character* argument was changed to 1 to 4 characters.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command changes the value of the feature code for Pickup Direct from the default (4) to the specified value.

In Cisco IOS Release 12.4(20)YA and later releases, if the length of the *keypad-character* argument is at least two characters and the leading or ending character of the string is an asterisk (*) or a number sign (#), phone users are not required to dial a prefix to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **4. If the feature code is 78#, the phone user dials only 78#, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that is already configured for another feature code, a speed-dial code, or the Redial FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that precludes or is precluded by another feature code, a speed-dial code, or the Redial FSD, you receive a message. If you configure a feature code to a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable phone user access to that feature.

To display a list of all FACs, use the **show stcapp feature codes** command.

Examples

The following example shows how to change the value of the feature code for Pickup Direct from the default (4). This configuration also changes the value of the prefix for all FACs from the default (**) to ##. After these values are configured, a phone user must press ##3 on the keypad, then the pickup-group number for the ringing extension number to pick up the incoming call.

```
Router(config)# stcapp feature access-code
Router(config-stcapp-fac)# prefix ##
Router(config-stcapp-fac)# pickup direct 3
Router(config-stcapp-fac)# exit
```

Related Commands

Command	Description
pickup direct	Defines a feature code for a feature access code (FAC) for Direct Call Pickup of a ringing extension number.
pickup local	Defines a feature code for a feature access code (FAC) for Group Call Pickup to pick up an incoming call from the local group.
prefix (stcapp-fac)	Defines the prefix for feature access codes (FACs).
show stcapp feature codes	Displays all feature access codes (FACs).
stcapp feature access-code	Enables feature access codes (FACs) and enters STC application feature access-code configuration mode for changing values of the prefix and features codes from the default.

pickup local

To define a a feature code for a Feature Access Code (FAC) to access Group Call Pickup for a local group on an analog phone, use the **pickup local** command in STC application feature access-code configuration mode. To return the code to its default, use the **no** form of this command.

pickup local *keypad-character*
no pickup local

Syntax Description

keypad-character	Character string that can be dialed on a telephone keypad. Default: 3. Before Cisco IOS Release 12.4(20)YA, this is a single character. In Cisco IOS Release 12.5(20)YA and later releases, the string can be any o the following: • A single character (0-9, *, #) • Two digits (00-99) • Two to four characters (0-9, *, #) and the leading or ending character must be an asterisk (*) or number sign (#)

Command Default

The default value is 3.

Command Modes

STC application feature access-code configuration (config-stcapp-fac)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(20)YA	The length of the *keypad-character* argument was changed to 1 to 4 characters.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command changes the value of the feature code for Local Group Pickup from the default (3) to the specified value.

In Cisco IOS Release 12.4(20)YA and later releases, if the length of the *keypad-character* argument is at least two characters and the leading or ending character of the string is an asterisk (*) or a number sign (#), phone users are not required to dial a prefix to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **3. If the feature code is 78#, the phone user dials only 78#, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that is already configured for another feature code or speed-dial code, or for the Redial FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that precludes or is precluded by another feature code or speed-dial code, or by the Redial FSD, you receive a message. If you configure a feature code to a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable phone user access to that feature.

To display a list of all FACs, use the **show stcapp feature codes** command.

Examples

The following example shows how to change the value of the feature code for Pickup Direct from the default (3). This configuration also changes the value of the prefix for all FACs from the default (**) to ##. With this configuration, a phone user must press ##9 on the keypad to pick up an incoming call in the same group as this extension number.

```
Router(config)# stcapp feature access-code
Router(config-stcapp-fac)# prefix ##
Router(config-stcapp-fac)# pickup local 9
Router(config-stcapp-fac)# exit
```

Related Commands

Command	Description
pickup direct	Defines a feature code for a feature access code (FAC) for Direct Call Pickup of a ringing extension number.
pickup group	Defines a feature code for a feature access code (FAC) for Group Call Pickup to pick up an incoming call from another group.
prefix (stcapp-fac)	Defines the prefix for feature access codes (FACs).
show stcapp feature codes	Displays all feature access codes (FACs).
stcapp feature access-code	Enables feature access codes (FACs) in STC application and enters STC application feature access-code configuration mode for changing values of the prefix and features codes from the default.

playout-delay (dial peer)

To tune the playout buffer on digital signal processors (DSPs) to accommodate packet jitter caused by switches in the WAN, use the **playout-delay** command in dial peer configuration mode. To reset the playout buffer to the default, use the **no** form of this command.

playout-delay {**fax** *milliseconds* | **maximum** *milliseconds* | **minimum** {**default** | **low** | **high**} | **nominal** *milliseconds*}
no playout-delay {**fax** | **maximum** | **minimum** | **nominal**}

Syntax Description

fax *milliseconds*	Amount of playout delay that the jitter buffer should apply to fax calls, in milliseconds. Range is from 0 to 700. Default is 300.
maximum *milliseconds*	(Adaptive mode only) Upper limit of the jitter buffer, or the highest value to which the adaptive delay is set, in milliseconds. Range is from 40 to 1700, although this value depends on the type of DSP and how the voice card is configured for codec complexity. (See **the codec complexity** command.) Default is 200. If the voice card is configured for high codec complexity, the highest value that can be configured for **maximum** for compressed codecs is 250 ms. For medium-complexity codec configurations, the highest **maximum** value is 150 ms. Voice hardware that does not support the voice card complexity configuration (such as analog voice modules for the Cisco 3600 series router) has an upper limit of 200 ms.
minimum	(Adaptive mode only) Lower limit of the jitter buffer, or the lowest value to which the adaptive delay is set, in milliseconds. Values are as follows: • **default** -- 40 ms. Use when there are normal jitter conditions in the network. This is the default. • **low** -- 10 ms. Use when there are low jitter conditions in the network. • **high** -- 40 ms. Use when there are high jitter conditions in the network.
nominal *milliseconds*	Amount of playout delay applied at the beginning of a call by the jitter buffer in the gateway, in milliseconds. In fixed mode, this is also the maximum size of the jitter buffer throughout the call. Range is from 0 to 1500, although this value depends on the type of DSP and how the voice card is configured for codec complexity. Default is 60. For non-conference calls when you are using DSPware version 4.1.33 or a later version, the following values are allowed. • If the voice card is configured for high codec complexity, the highest value that can be configured for the **nominal** keyword for compressed codecs is 200 ms. • For medium-complexity codec configurations, the highest nominal value is 150 ms.

nominal *milliseconds* (continued)	For conference calls when you are using DSPware version 4.1.33 or a later version, the following values are allowed: • The first decoder stream can be assigned a nominal value as high as 200 ms (high-complexity codec) or 150 ms (medium-complexity codec). • Subsequent decoder streams are limited to the highest nominal value of 150 ms (high-complexity) or 80 ms (medium-complexity). When the playout-delay mode is configured for fixed operation and setting the expected jitter buffer size with the nominal value, the minimum effective value for the playout delay will depend on the codec in use and the configured minimum value. • When the **playout-delay minimum low** is configured the minimum actual jitter buffer size will be 30ms even when setting the nominal to a value lower than 30msec. • When the **playout-delay minimum default**, the minimum jitter buffer size when running in fixed mode will be 60ms. When fixed mode is configured, there is a 10msec added to the nominal value when setting the jitter buffer when configured for G.729 and a 5ms added using G.711 Voice hardware that does not support the voice-card complexity configuration (such as analog voice modules for the Cisco 3600 series router) has an upper limit of 200 ms for the first decoder stream and 150 ms for subsequent decoder streams. **Note** With DSPware versions earlier than 4.1.33, the highest nominal value that can be configured is 150 ms for high-complexity codec configurations and analog modules. The highest nominal value for medium-complexity codec configurations is 80 ms.

Command Default

fax --300 milliseconds**maximum**--200 milliseconds**minimum**--default (40 milliseconds)**nominal**--60 milliseconds

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)XI	This command was implemented on the Cisco ICS7750.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T. Support for dial peer configuration mode was added on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco MC3810, Cisco AS5200, Cisco AS5300, Cisco AS5400, and Cisco AS5800. The **minimum** keyword was introduced.
12.2(13)T	The **fax** keyword was introduced.

Release	Modification
12.2(13)T8	DSPware version 4.1.33 was implemented.

Usage Guidelines

Before Cisco IOS Release 12.1(5)T, this command was used in voice-port configuration mode. For Cisco IOS Release 12.1(5)T and later releases, in most cases playout delay should be configured in dial-peer configuration mode on the Voice over IP (VoIP) dial peer that is on the receiving end of the voice traffic that is to be buffered. This dial peer senses network conditions and relays them to the DSPs, which adjust the jitter buffer as necessary. When multiple applications are configured on the gateway, playout delay should be configured in dial-peer configuration mode. When there are numerous dial peers to configure, it might be simpler to configure playout delay on a voice port. If conflicting playout-delay values have been configured on a voice port and on a dial peer, the dial-peer configuration takes precedence.

Playout delay is the amount of time that elapses between the time at which a voice packet is received at the jitter buffer on the DSP and the time at which it is played out to the codec. In most networks with normal jitter conditions, the defaults are adequate and you will not need to configure this command.

In situations in which you want to improve voice quality by reducing jitter or you want to reduce network delay, you can configure playout-delay parameters. The parameters are slightly different for each of the two playout-delay modes, adaptive and fixed (see the **playout-delay mode** command).

In adaptive mode, the average delay for voice packets varies depending on the amount of interarrival variation that packets have as the call progresses. The jitter buffer grows and shrinks to compensate for jitter and to keep voice packets playing out smoothly, within the maximum and minimum limits that have been configured. The maximum limit establishes the highest value to which the adaptive delay is set. The minimum limit is the low-end threshold for the delay of incoming packets by the adaptive jitter buffer. Algorithms in the DSPs that control the growth and shrinkage of the jitter buffer are weighted toward the improvement of voice quality at the expense of network delay: jitter buffer size increases rapidly in response to spikes in network transmissions and decreases slowly in response to reduced congestion.

In fixed mode, the nominal value is the amount of playout delay applied at the beginning of a call by the jitter buffer in the gateway and is also the maximum size of the jitter buffer throughout the call.

As a general rule, if there is excessive breakup of voice due to jitter with the default playout-delay settings, increase playout delay times. If your network is small and jitter is minimal, decrease playout-delay times for a smaller overall delay.

When there is bursty jitter in the network, voice quality can be degraded even though the jitter buffer is actually adjusting the playout delay correctly. The constant readjustment of playout delay to erratic network conditions causes voice quality problems that are usually alleviated by increasing the minimum playout delay-value in adaptive mode or by increasing the nominal delay for fixed mode.

Use the **show call active voice** command to display the current delay, as well as high- and low-water marks for delay during a call. Other fields that can help determine the size of a jitter problem are ReceiveDelay, GapFillWith..., LostPackets, EarlyPackets, and LatePackets. The following is sample output from the **show call active voice** command:

```
VOIP:
 ConnectionId[0xECDE2E7B 0xF46A003F 0x0 0x47070A4]
 IncomingConnectionId[0xECDE2E7B 0xF46A003F 0x0 0x47070A4]
 RemoteIPAddress=192.168.100.101
 RemoteUDPPort=18834
 RoundTripDelay=26 ms
 SelectedQoS=best-effort
 tx_DtmfRelay=inband-voice
 FastConnect=TRUE
```

```
 Separate H245 Connection=FALSE
 H245 Tunneling=FALSE
 SessionProtocol=cisco
 SessionTarget=
 OnTimeRvPlayout=417000
 GapFillWithSilence=850 ms
 GapFillWithPrediction=2590 ms
 GapFillWithInterpolation=0 ms
 GapFillWithRedundancy=0 ms
 HiWaterPlayoutDelay=70 ms
 LoWaterPlayoutDelay=29 ms
 ReceiveDelay=39 ms
 LostPackets=0
 EarlyPackets=0
 LatePackets=86
```

Examples

The following example uses default adaptive mode with a minimum playout delay of 10 ms and a maximum playout delay of 60 ms on VoIP dial peer 80. The size of the jitter buffer is adjusted up and down on the basis of the amount of jitter that the DSP finds, but is never smaller than 10 ms and never larger than 60 ms.

```
dial-peer 80 voip
 playout-delay minimum low
 playout-delay maximum 60
```

Related Commands

Command	Description
codec complexity	Specifies call density and codec complexity based on the codec standard you are using.
playout-delay (voice-port)	Tunes the playout buffer to accommodate packet jitter caused by switches in the WAN.
playout -delay mode	Selects fixed or adaptive mode for the jitter buffer on DSPs.
show call active voice	Displays active call information for voice calls.

playout-delay (voice-port)

To tune the playout buffer to accommodate packet jitter caused by switches in the WAN, use the **playout-delay** command in voice-port configuration mode. To reset the playout buffer to the default, use the **no** form of this command.

playout-delay {**fax** | **maximum** | **nominal**} *milliseconds*
no playout-delay {**fax** | **maximum** | **nominal**}

Syntax Description

fax *milliseconds*	Amount of playout delay that the jitter buffer should apply to fax calls, in milliseconds. Range is from 0 to 700. Default is 300.
maximum *milliseconds*	Delay time that the digital signal processor (DSP) allows before starting to discard voice packets, in milliseconds. Range is from 40 to 320. Default is 160.
nominal *milliseconds*	Initial (and minimum allowed) delay time that the DSP inserts before playing out voice packets, in milliseconds. Range is from 40 to 200. Default is 80.

Command Default

fax --300 milliseconds**maximum**--160 milliseconds**nominal**--80 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(13)T	The **fax** keyword was added.

Usage Guidelines

If there is excessive breakup of voice due to jitter with the default playout delay settings, increase the delay times. If your network is small and jitter is minimal, decrease the delay times to reduce delay.

Before Cisco IOS Release 12.1(5)T, the **playout-delay** command was configured in voice-port configuration mode. For Cisco IOS Release 12.1(5)T and later releases, in most cases playout delay should be configured in dial-peer configuration mode on the Voice over IP (VoIP) dial peer that is on the receiving end of the voice traffic that is to be buffered. This dial peer senses network conditions and relays them to the DSPs, which adjust the jitter buffer as necessary. When multiple applications are configured on the gateway, playout delay should be configured in dial-peer configuration mode. When there are numerous dial peers to configure, it might be simpler to configure playout delay on a voice port. If conflicting playout-delay values have been configured on a voice port and on a dial peer, the dial-peer configuration takes precedence.

Playout delay is the amount of time that elapses between the time at which a voice packet is received at the jitter buffer on the DSP and the time at which it is played out to the codec. In most networks with normal jitter conditions, the defaults are adequate and you will not need to configure the **playout-delay** command.

In situations in which you want to improve voice quality by reducing jitter or you want to reduce network delay, you can configure playout-delay parameters. The parameters are slightly different for each of the two playout-delay modes, adaptive and fixed (see the **playout-delay mode** command).

In adaptive mode, the average delay for voice packets varies depending on the amount of interarrival variation that packets have as the call progresses. The jitter buffer grows and shrinks to compensate for jitter and to keep voice packets playing out smoothly, within the maximum and minimum limits that have been configured. The maximum limit establishes the highest value to which the adaptive delay will be set. The minimum limit is the low-end threshold for incoming packet delay that is created by the adaptive jitter buffer. Algorithms in the DSPs that control the growth and shrinkage of the jitter buffer are weighted toward the improvement of voice quality at the expense of network delay: jitter buffer size increases rapidly in response to spikes in network transmissions and decreases slowly in response to reduced congestion.

In fixed mode, the nominal value is the amount of playout delay applied at the beginning of a call by the jitter buffer in the gateway and is also the maximum size of the jitter buffer throughout the call.

As a general rule, if there is excessive breakup of voice due to jitter with the default playout-delay settings, increase playout-delay times. If your network is small and jitter is minimal, decrease playout-delay times for a smaller overall delay.

When there is bursty jitter in the network, voice quality can be degraded even though the jitter buffer is actually adjusting the playout delay correctly. The constant readjustment of playout delay to erratic network conditions causes voice quality problems that are usually alleviated by increasing the minimum playout-delay value in adaptive mode or by increasing the nominal delay for fixed mode.

Note The minimum limit for playout delay is configured using the **playout-delay** (dial peer) command.

Use the **show call active voice** command to display the current delay, as well as high- and low-water marks for delay during a call. Other fields that can help determine the size of a jitter problem are GapFillWith..., ReceiveDelay, LostPackets, EarlyPackets, and LatePackets. The following is sample output from the **show call active voice** command:

```
VOIP:
 ConnectionId[0xECDE2E7B 0xF46A003F 0x0 0x47070A4]
 IncomingConnectionId[0xECDE2E7B 0xF46A003F 0x0 0x47070A4]
 RemoteIPAddress=192.168.100.101
 RemoteUDPPort=18834
 RoundTripDelay=26 ms
 SelectedQoS=best-effort
 tx_DtmfRelay=inband-voice
 FastConnect=TRUE
 Separate H245 Connection=FALSE
 H245 Tunneling=FALSE
 SessionProtocol=cisco
 SessionTarget=
 OnTimeRvPlayout=417000
 GapFillWithSilence=850 ms
 GapFillWithPrediction=2590 ms
 GapFillWithInterpolation=0 ms
 GapFillWithRedundancy=0 ms
 HiWaterPlayoutDelay=70 ms
 LoWaterPlayoutDelay=29 ms
 ReceiveDelay=39 ms
 LostPackets=0
 EarlyPackets=0
 LatePackets=86
```

Examples

The following example sets nominal playout delay to 80 ms and maximum playout delay to 160 ms on voice port 1/0/0:

```
voice-port 1/0/0

playout-delay nominal 80
 playout-delay maximum 160
```

Related Commands

Command	Description
playout -delay (dial peer)	Tunes the playout buffer on DSPs to accommodate packet jitter caused by switches in the WAN.
playout -delay mode	Selects fixed or adaptive mode for playout delay from the jitter buffer on digital signal processors.
show call active	Shows active call information for voice calls or fax transmissions in progress.
vad	Enables voice activity detection.

playout-delay mode (dial-peer)

To select fixed or adaptive mode for playout delay from the jitter buffer on digital signal processors (DSPs), use the **playout-delay mode** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

playout-delay mode {**adaptive** | **fixed**}
no playout-delay mode

Syntax Description

adaptive	Jitter buffer size and amount of playout delay are adjusted during a call, on the basis of current network conditions.
fixed	Jitter buffer size does not adjust during a call; a constant playout delay is added.

Command Default

Adaptive jitter buffer size

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.1(5)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco MC3810, and Cisco ICS 7750. The **no-timestamps** keyword was removed.

Usage Guidelines

Before Cisco IOS Release 12.1(5)T, this command was used only in voice-port configuration mode. For Cisco IOS Release 12.1(5)T and later releases, in most cases playout delay should be configured in dial-peer configuration mode on the VoIP dial peer that is on the receiving end of the voice traffic that is to be buffered. This dial peer senses network conditions and relays them to the DSPs, which adjust the jitter buffer as necessary. When multiple applications are configured on the gateway, playout delay should be configured in dial-peer configuration mode.

Tip When there are numerous dial peers to configure, it might be simpler to configure playout delay on a voice port. If conflicting playout delay values have been configured on a voice port and on a dial peer, the dial-peer configuration takes precedence.

In most networks with normal jitter conditions, the default is adequate and you do not need to configure this command.

The default is adaptive mode, in which the average delay for voice packets varies depending on the amount of interarrival variation that packets have as the call progresses. The jitter buffer grows and shrinks to compensate for jitter and to keep voice packets playing out smoothly, within the maximum and minimum limits that have been configured.

Select fixed mode only when you understand your network conditions well, and when you have a network with very poor quality of service (QoS) or when you are interworking with a media server or similar transmission source that tends to create a lot of jitter at the transmission source. In most situations it is better to configure adaptive mode and let the DSP size the jitter buffer according to current conditions.

Examples

The following example sets adaptive playout-delay mode with a high (80 ms) minimum delay on a VoIP dial peer 80:

```
dial-peer 80 voip
 playout-delay mode adaptive
 playout-delay minimum high
```

Related Commands

Command	Description
playout -delay	Tunes the jitter buffer on DSPs for playout delay of voice packets.
show call active voice	Displays active call information for voice calls.

playout-delay mode (voice-port)

To select fixed or adaptive mode for playout delay from the jitter buffer on digital signal processors (DSPs), use the **playout-delay mode** command in voice port configuration mode. To reset to the default, use the **no** form of this command.

playout-delay mode {**adaptive** | **fixed**}
no playout-delay mode

Syntax Description

adaptive	Jitter buffer size and amount of playout delay are adjusted during a call, on the basis of current network conditions.
fixed	Jitter buffer size does not adjust during a call; a constant playout delay is added.

Command Default

Adaptive jitter buffer size

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)XI	Thiscommand was implemented on the Cisco ICS 7750. The keyword **mode** was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T and the **no-timestamps** keyword was removed.

Usage Guidelines

Before Cisco IOS Release 12.1(5)T, this command was used only in voice-port configuration mode. For Cisco IOS Release 12.1(5)T and later releases, in most cases playout delay should be used in dial-peer configuration mode on the VoIP dial peer that is on the receiving end of the voice traffic that is to be buffered. This dial peer senses network conditions and relays them to the DSPs, which adjust the jitter buffer as necessary. When multiple applications are configured on the gateway, playout delay should be configured in dial-peer configuration mode.

Tip When there are numerous dial peers to configure, it might be simpler to configure playout delay on a voice port. If conflicting playout delay values have been configured on a voice port and on a dial peer, the dial-peer configuration takes precedence.

In most networks with normal jitter conditions, the default is adequate and you do not need to configure the **playout-delay mode** command.

The default is adaptive mode, in which the average delay for voice packets varies depending on the amount of interarrival variation that packets have as the call progresses. The jitter buffer grows and shrinks to compensate for jitter and to keep voice packets playing out smoothly, within the maximum and minimum limits that have been configured.

Select fixed mode only when you understand your network conditions well, and when you have a network with very poor quality of service (QoS) or when you are interworking with a media server or similar transmission source that tends to create a lot of jitter at the transmission source. In most situations it is better to configure adaptive mode and let the DSP size the jitter buffer according to current conditions.

Examples

The following example sets fixed mode on a Cisco 3640 voice port with a nominal delay of 80 ms.

```
voice-port 1/1/0
 playout-delay mode fixed
 playout-delay nominal 80
```

Related Commands

Command	Description
playout -delay	Tunes the jitter buffer on DSPs for playout delay of voice packets.
show call active voice	Displays active call information for voice calls.

police profile

To apply the media bandwidth policing profile to a media class, use the **police profile** command in media class configuration mode. To disable the configuration, use the **no** form of this command.

police profile *tag*
no police profile

Syntax Description

tag	Media profile police tag. The range is from 1 to 10000.

Command Default

The media bandwidth policing profile is not applied to a media class.

Command Modes

Media class configuration (cfg-mediaclass)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Applying the media bandwidth policing profile at the dial peer level involves two actions; applying the profile for a media class and then applying the corresponding media class to a dial peer. Use the **police profile** command to apply the media bandwidth policing profile to a media class.

Examples

The following example shows how to apply the media bandwidth policing profile to a media class:

```
Router> enable
Router# configure terminal
Router(config)# media class 1
Router(cfg-mediaclass)# police profile 1
```

Related Commands

Command	Description
media-class	Applies the media class at the dial peer level.
snmp-server enable traps voice media-policy	Enables SNMP media policy voice traps at the global level.
snmp enable peer-trap media-policy	Enables SNMP media policy voice traps at the dial peer level.

port (Annex G neighbor BE)

To configure the port number of the neighbor that is used for exchanging Annex G messages, use the **port** command in Annex G Neighbor BE configuration mode. To remove the port number, use the **no** form of this command.

port *neighbor-port*
no port

Syntax Description

neighbor -port	Port number of the neighbor. This number is used for exchanging Annex G messages. The default port number is 2099.

Command Default

2099

Command Modes

Annex G Neighbor BE configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Usage Guidelines

When cofiguring the **no port** command the *neighbor-port*argument is not used.

Examples

The following example sets a neighbor BE to port number 2010.

```
Router(config-annexg-neigh)# port 2010
```

Related Commands

Command	Description
advertise (annex g)	Controls the types of descriptors that the BE advertises to its neighbors.
cache	Configures the local BE to cache the descriptors received from its neighbors.
id	Configures the local ID of the neighboring BE.
query -interval	Configures the interval at which the local BE will query the neighboring BE.

port (dial peer)

To associate a dial peer with a specific voice port, use the **port** command in dial peer configuration mode. To cancel this association, use the **no** form of this command.

Cisco 1750 and Cisco 3700 Series
port *slot-number*/*port*
no port *slot-number*/*port*

Cisco 2600 Series, Cisco 3600 Series, and Cisco 7200 Series
port {*slot-number*/*subunit-number*/*port* | *slot*/*port***:***ds0-group-number*}
no port {*slot-number*/*subunit-number*/*port* | *slot*/*port***:***ds0-group-number*}

Cisco AS5300 and Cisco AS5800
port *controller-number***:D**
no port *controller-number***:D**

Cisco uBR92x Series
port *slot*/*subunit*/*port*
no port *slot*/*subunit*/*port*

Syntax Description

slot -number	Number of the slot in the router in which the voice interface card (VIC) is installed. Valid entries are from 0 to 2, depending on the slot in which the VIC has been installed.
port	Voice port number. Valid entries are 0 and 1.

slot -number	Number of the slot in the router in which the VIC is installed. Valid entries are from 0 to 3, depending on the slot in which it has been installed.
subunit -number	Subunit on the VIC in which the voice port is located. Valid entries are 0 and 1.
port	Voice port number. Valid entries are 0 and 1.
slot	Router location in which the voice port adapter is installed. Valid entries are 0 and 3.
port	Voice interface card location. Valid entries are 0 and 3.
ds0 -group-number	The DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.

controller -number	The T1 or E1 controller.
:D	Indicates the D channel associated with the ISDN PRI.

slot/subunit/port	The analog voice port. Valid entries for the *slot/subunit/port* are as follows: • *slot* -- A router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • *subunit* -- A VIC in which the voice port is located. Valid entries are 0 and 1. (The VIC fits into the voice network module.) • *port*-- An analog voice port number. Valid entries are 0 and 1.

Command Default

No port is configured.

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(3)T	This command was implemented on the Cisco 2600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco AS5300.
12.0(4)T	This command was implemented on the Cisco uBR924.
12.0(7)T	This command was implemented on the Cisco AS5800.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 3725, and Cisco 3745.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. This command does not support the extended echo canceller (EC) feature on the Cisco AS5300 or the Cisco AS5800.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

This command enables calls that come from a telephony interface to select an incoming dial peer and for calls that come from the VoIP network to match a port with the selected outgoing dial peer.

This command applies only to POTS peers.

Note This command does not support the extended EC feature on the Cisco AS5300.

Examples

The following example associates POTS dial peer 10 with voice port 1, which is located on subunit 0 and accessed through port 0:

```
dial-peer voice 10 pots
 port 1/0/0
```

The following example associates POTS dial peer 10 with voice port 0:D:

```
dial-peer voice 10 pots
 port 0:D
```

The following example associates POTS dial peer 10 with voice port 1/0/0:D (T1 card):

```
dial-peer voice 10 pots
 port 1/0/0:D
```

Related Commands

Command	Description
prefix	Specifies the prefix of the dialed digits for a dial peer.

port (MGCP profile)

To associate a voice port with the Media Gateway Control Protocol (MGCP) profile that is being configured, use the **port**command inMGCP profile configuration mode. To disassociate the voice port from the profile, use the **no** form of this command.

port *port-number*
no port *port-number*

Syntax Description

port -number	Voice port or DS0-group number to be used as an MGCP endpoint associated with an MGCP profile.

Command Default

No default behavior or values

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced as the **voice-port** (MGCP profile) command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was renamed the **port** (MGCP profile) command.

Usage Guidelines

This command is used when values for an MGCP profile are configured.

This command associates a voice port with the MGCP profile that is being defined. To associate multiple voice ports with a profile, repeat this command with different voice port arguments.

This command is not used when the default MGCP profile is configured because the values in the default profile configuration apply to all parameters that have not been otherwise configured for a user-defined MGCP profile.

Examples

The following example associates an analog voice port with an MGCP profile on a Cisco uBR925 platform:

```
Router(config)# mgcp profile ny110ca
Router(config-mgcp-profile)# port 0
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

port (supplementary-service)

To enter the supplementary-service voice-port configuration mode for associating a voice port with STC application supplementary-service features, use the **port** command in supplementary-service configuration mode. To cancel the association, use the **no** form of this command.

port *port*
no port *port*

Syntax Description

port	Location of port in Cisco ISR or Cisco VG224 Analog Phone Gateway. Syntax is platform-dependent; type **?** to determine.

Command Default

This command has no default behavior or values.

Command Modes

Supplementary-service configuration (config-stcapp-suppl-serv)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command associates an analog FXS port to STC application supplementary-service features being configured.

Examples

The following example shows how to enable Hold/Resume on analog endpoints connected to port 2/0 of a Cisco VG224.

```
Router(config)# stcapp supplementary-services
Router(config-stcapp-suppl-serv)# port 2/0
Router(config-stcapp-suppl-serv-port)# hold-resume
Router(config-stcapp-suppl-serv-port)# end
```

Related Commands

Command	Description
hold-resume	Enables Hold/Resume in Feature mode on the port being configured.

port media

To specify the serial interface to which the local video codec is connected for a local video dial peer, use the port media command in video dial-peer configuration mode. To remove any configured locations from the dial peer, use the **no** form of this command.

port media *interface*
no port media

Syntax Description

interface	Serial interface to which the local codec is connected. Valid entries are 0 and 1.

Command Default

No interface is specified

Command Modes

Video dial-peer configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced for ATM video dial-peer configuration on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Examples

The following example specifies serial interface 0 as the specified interface for the codec local video dial peer 10:

```
dial-peer video 10 videocodec
 port media Serial0
```

Related Commands

Command	Description
port signal	Specifies the slot location of the VDM and the port location of the EIA/TIA-366 interface for signaling.
show dial-peer video	Displays dial-peer configuration.

port-range

To specify a port range for the TFTP server, use the **port-range** command in phone-proxy configuration mode. To remove the port-range, use the **no** form of the command.

port-range *min-port* *max-port*
no port-range *min-port* *max-port*

Syntax Description

min-port	First port number of the port range.
max-port	Last port number of the port range.

Command Default

No port range is specified.

Command Modes

Phone-proxy configuration mode (config-pp-pr)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Example

The following example shows how to configure a port range for the TFTP server. The first port number is 30000 and the last port number is 40000:

```
Device(config-pp-pr)# port-range 30000 40000
```

port signal

To specify the slot location of the video dialing module (VDM) and the port location of the EIA/TIA-366 interface for signaling for a local video dial peer, use the port signal command in video dial-peer configuration mode. To remove any configured locations from the dial peer, use the **no** form of this command.

port signal *slot/port*
no port signal

Syntax Description

slot/	Slot location of the VDM. Valid values are 1 and 2.
port	Port location of the EIA/TIA-366 interface.

Command Default

No locations are specified

Command Modes

Video dial-peer configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced for ATM video dial-peer configuration on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Examples

The following example sets up the VDM and EIA/TIA-366 interface locations for the local video dial peer designated as 10:

```
dial-peer video 10 videocodec
 port signal 1/0
```

Related Commands

Command	Description
port media	Specifies the serial interface to which the local video codec is connected.
show dial-peer video	Displays dial-peer configuration.

pots call-waiting

To enable the local call-waiting feature, use the global configuration **pots call-waiting** command in global configuration mode. To disable the local call-waiting feature, use the no form of this command.

pots call-waiting {**local** | **remote**}
no pots call-waiting {**local** | **remote**}

Syntax Description

local	Enable call waiting on a local basis for the routers.
remote	Rely on the network provider service instead of the router to hold calls.

Command Default

Remote, in which case the call- holding pattern follows the settings of the service provider rather than those of the router.

Command Modes

Global configuration

Command History

Release	Modification
12.1.(2)XF	This command was introduced on the Cisco 800 series.

Usage Guidelines

To display the call-waiting setting, use the show running-config or show pots status command. The ISDN call waiting service is used if it is available on the ISDN line connected to the router even if local call waiting is configured on the router. That is, if the ISDN line supports call waiting, the local call waiting configuration on the router is ignored.

Examples

The following example enables local call waiting on a router:

```
pots call-waiting local
```

Related Commands

Command	Description
call-waiting	Configures call waiting for a specific dial peer.
show pots status	Displays the settings of the physical characteristics and other information on the telephone interfaces of a Cisco 800 series router.

pots country

To configure your connected telephones, fax machines, or modems to use country-specific default settings for each physical characteristic, use the **pots country**command in global configuration mode. To disable the use of country-specific default settings, use the **no** form of this command.

pots country *country*
no pots country *country*

Syntax Description

country	Country in which your router is located.

Command Default

A default country is not defined.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command applies to the Cisco 800 series routers.

If you need to change a country-specific default setting of a physical characteristic, you can use the associated command listed in the "Related Commands" section. Enter the **pots country ?** command to get a list of supported countries and the code you must enter to indicate a particular country.

Examples

The following example specifies that the devices connected to the telephone ports use default settings specific to Germany for the physical characteristics:

```
pots country de
```

Related Commands

Command	Description
pots dialing -method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect -supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect -time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots distinctive -ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.

Command	Description
pots line -type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing -freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence -time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone -source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots dialing-method

To specify how the router collects and sends digits dialed on your connected telephones, fax machines, or modems, use the **pots dialing-method**command in global configuration mode. To disable the specified dialing method, use the **no** form of this command.

pots dialing-method {**overlap** | **enblock**}
no pots dialing-method {**overlap** | **enblock**}

Syntax Description

overlap	The router sends each digit dialed in a separate message.
enblock	The router collects all digits dialed and sends the digits in one message.

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command applies to Cisco 800 series routers.

To interrupt the collection and transmission of dialed digits, enter a pound sign (#), or stop dialing digits until the interdigit timer runs out (10 seconds).

Examples

The following example specifies that the router uses the enblock dialing method:

```
pots dialing-method enblock
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots disconnect -supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect -time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots distinctive -ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).

Command	Description
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line -type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing -freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence -time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone -source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots disconnect-supervision

To specify how a router notifies the connected telephones, fax machines, or modems when the calling party has disconnected, use the **pots disconnect-supervision**command in global configuration mode. To disable the specified disconnect method, use the **no** form of this command.

pots disconnect-supervision {**osi** | **reversal**}
no pots disconnect-supervision {**osi** | **reversal**}

Syntax Description

osi	Open switching interval (OSI) is the duration for which DC voltage applied between tip and ring conductors of a telephone port is removed.
reversal	Polarity reversal of tip and ring conductors of a telephone port.

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command applies to Cisco 800 series routers.

Most countries except Japan typically use the **osi** option. Japan typically uses the **reversal** option.

Examples

The following example specifies that the router uses the OSI disconnect method:

```
pots disconnect-supervision osi
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing -method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect -time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots distinctive -ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).

Command	Description
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line -type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing -freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence -time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone -source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots disconnect-time

To specify the interval in which the disconnect method is applied if your connected telephones, fax machines, or modems fail to detect that a calling party has disconnected, use the **pots disconnect-time**command in global configuration mode. To disable the specified disconnect interval, use the **no** form of this command.

pots disconnect-time *interval*
no pots disconnect-time *interval*

Syntax Description

interval	Interval, in milliseconds. Range is from 50 to 2000.

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command applies to Cisco 800 series routers.

The **pots disconnect-supervision** command configures the disconnect method.

Examples

The following example specifies that the connected devices apply the configured disconnect method for 100 ms after a calling party disconnects:

```
pots disconnect-time 100
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing -method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect -supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots distinctive -ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.

Command	Description
pots line -type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing -freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence -time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone -source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots distinctive-ring-guard-time

To specify the delay in which a telephone port can be rung after a previous call is disconnected, use the **pots distinctive-ring-guard-time**command in global configuration mode. To disable the specified delay, use the **no** form of this command.

pots distinctive-ring-guard-time *milliseconds*
no pots distinctive-ring-guard-time *milliseconds*

Syntax Description

milliseconds	Delay, in milliseconds. Range is from 0 to 1000.

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command applies to Cisco 800 series routers.

Examples

The following example specifies that a telephone port can be rung 100 ms after a previous call is disconnected:

```
pots distinctive-ring-guard-time 100
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing -method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect -supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect -time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.

Command	Description
pots line -type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing -freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence -time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone -source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
ring	Sets up a distinctive ring for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots encoding

To specify the pulse code modulation (PCM) encoding scheme for your connected telephones, fax machines, or modems, use the **pots encoding** command in global configuration mode. To disable the specified scheme, use the **no** form of this command.

pots encoding {**alaw** | **ulaw**}
no pots encoding {**alaw** | **ulaw**}

Syntax Description

alaw	A-law. International Telecommunication Union Telecommunication Standardization Section (ITU-T) PCM encoding scheme used to represent analog voice samples as digital values.
ulaw	Mu-law. North American PCM encoding scheme used to represent analog voice samples as digital values.

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command applies to Cisco 800 series routers.

Europe typically uses a-law. North America typically uses u-law.

Examples

The following example specifies a-law as the PCM encoding scheme:

```
pots encoding alaw
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing -method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect -supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect -time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.

Command	Description
pots distinctive -ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots line -type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing -freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence -time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone -source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots forwarding-method

To configure the type of call-forwarding method to be used for Euro-ISDN (formerly NET3) switches, use the **pots forwarding-method** command in global configuration mode. To turn forwarding off, use the **no** form of this command.

pots forwarding-method {**keypad** | **functional**}
no pots forwarding-method {**keypad** | **functional**}

Syntax Description

keypad	Gives forwarding control to the Euro-ISDN switch.
functional	Gives forwarding control to the router. If you select this method, use the dual-tone multifrequency (DTMF) keypad commands listed in the table below to configure call-forwarding service.

Command Default

Forwarding is off

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

Use this command to select the type of forwarding method to be used for Euro-ISDN switches. This command does not affect any other switch types.

You can select one or more call-forwarding services at a time, but keep the following Euro-ISDN switch characteristics in mind:

- Call forward unconditional (CFU) redirects a call without restriction and takes precedence over other call-forwarding service types.
- Call forward busy (CFB) redirects a call to another number if the dialed number is busy.
- Call forward no reply (CFNR) forwards a call to another number if the dialed number does not answer within a specified period of time.

If all three call-forwarding services are enabled, CFU overrides CFB and CFNR. The default is that no call-forwarding service is selected.

If you select thefunctional forwarding method, use the DTMF keypad commands in the table below to configure the call-forwarding service.

Table 4: DTMF Keypad Commands for Call-Forwarding Service

Task	DTMF Keypad Command[1]
Activate CFU	****21*** *number* **#**
Deactivate CFU	**#21#**

Task	DTMF Keypad Command[1]
Activate CFNR	****61*** *number* #
Deactivate CFNR	**#61#**
Activate CFB	****67*** *number* #
Deactivate CFB	**#67#**

1 Where number is the telephone number to which your calls are forwarded.

When you enable or disable the call-forwarding service, it is enabled or disabled for four basic services: speech, audio at 3.1 kilohertz (kHz), telephony at 3.1 kHz, and telephony at 7 kHz. You should hear a dial tone after you enter the DTMF keypad command when the call-forwarding service is successfully enabled for at least one of the four basic services. If you hear a busy tone, the command is invalid or the switch does not support that service.

Examples

The following example gives forwarding control to the router:

```
pots forwarding-method functional
```

Related Commands

Command	Description
pots prefix filter	Sets a filter that prevents a dial prefix from being added to a dialed number when the digits in the dialed number match the filter.
pots prefix number	Sets a prefix to be added to a called telephone number for analog or modem calls.

pots line-type

To specify the impedance of your connected telephones, fax machines, or modems, use the **pots line-type**command in global configuration mode. To disable the specified line type, use the **no** form of this command.

pots line-type {**type1** | **type2** | **type3**}
no pots line-type {**type1** | **type2** | **type3**}

Syntax Description

type1	Runs at 600 ohms.
type2	Runs at 900 ohms.
type3	Runs at 300 or 400 ohms.

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command applies to Cisco 800 series routers.

Examples

The following example sets the line type to type1:

```
pots line-type type1
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing -method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect -supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect -time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.

Command	Description
pots distinctive -ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing -freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence -time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone -source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots prefix filter

To set a filter that prevents a dial prefix from being added to a dialed number when the digits in the dialed number match the filter, use the **pots prefix filter** command in global configuration mode. To remove the filter, use the **no** form of this command.

pots prefix filter *number*
no pots prefix filter *number*

Syntax Description

number	Prefix filter numbers, up to a maximum of eight characters.

Command Default

No default filter is set.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced on the Cisco 803 and Cisco 804.

Usage Guidelines

The **pots prefix filter** command is used to set a filter for prefix dialing. A maximum of ten filters can be set. Once the maximum number of filters have been configured, an additional filter is not accepted nor does it overwrite any of the existing filters.

To configure a new filter, remove at least one filter using the **no pots prefix filter** command.

You can set matching criteria for the filter using the * wildcard character. For example, if you configure the filter 1* and a dialed number starts with 1, the called number is not prefixed. Prefix filters can be of variable length. All configured prefix filters are compared to the number dialed, up to the length of the prefix filter. If there is a match, no prefix is added to the dialed number.

Examples

The following example configures five filters that prevent dial prefixes from being added to dialed numbers:

```
pots prefix filter 192
pots prefix filter 1
pots prefix filter 9
pots prefix filter 0800
pots prefix filter 08456
```

With these filters configured, a prefix is *not* added to the following dialed numbers:

192 Directory calls

100 Operator services

999 Emergency services

0800... Toll-free calls

08456... Calls on an Energis network information controller

Related Commands

Command	Description
pots forwarding -method	Configures the type of forwarding method to be used for Euro-ISDN (formerly NET3) switches.
pots prefix number	Sets a prefix to be added to a called telephone number for analog or modem calls.

pots prefix number

To set a prefix to be added to a called telephone number for analog or modem calls, use the **pots prefix number** command in global configuration mode. To remove the prefix, use the **no** form of this command.

pots prefix number *number*
no pots prefix number *number*

Syntax Description

number	Prefix, up to a maximum of five digits.

Command Default

No prefix is associated with the called number for analog or modem calls

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced on the Cisco 803 and Cisco 804.

Usage Guidelines

Only one prefix can be configured using this command. If a prefix already exists, the next prefix configured with this command overwrites the old prefix. Prefixes can be of variable length, up to five digits. The **no pots prefix number** command removes the prefix.

As numbers are dialed on the keypad, a comparison is made to the configured prefix filter. When a match is determined, the number is dialed without adding the prefix. In the unlikely event that the prefix filter has more digits than the dialed number, and the dialed number matches the first digits of the prefix filter, the prefix is not added to the dialed number. For example, if the prefix filter is 5554000 and you dial 555 and stop, the router considers the called number to be 555 and does not add a prefix to the number. This event is unlikely to occur because the number of digits in dialed numbers is typically greater than the number of digits in prefix filters.

Examples

The following example sets the prefix to 12345:

```
pots prefix number 12345
```

This prefix is added to any number dialed for analog or modem calls that do not match the prefix filter.

Related Commands

Command	Description
pots prefix filter	Sets a filter that prevents a dial prefix from being added to a dialed number when the digits in the dialed number match the filter.

pots ringing-freq

To specify the frequency on the Cisco 800 series router at which connected telephones, fax machines, or modems ring, use the **pots ringing-freq**command in global configuration mode. To disable the specified frequency, use the **no** form of this command.

pots ringing-freq {**20Hz** | **25Hz** | **50Hz**}
no pots ringing-freq {**20Hz** | **25Hz** | **50Hz**}

Syntax Description

20Hz	Connected devices ring at 20 Hz.
25Hz	Connected devices ring at 25 Hz.
50Hz	Connected devices ring at 50 Hz.

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command applies to Cisco 800 series routers.

Examples

The following example sets the ringing frequency to 50 Hz:

```
pots ringing-freq 50Hz
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing -method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect -supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect -time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.

Command	Description
pots distinctive -ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line -type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots silence -time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone -source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots silence-time

To specify the interval of silence after a calling party disconnects, use the **pots silence-time**command in global configuration mode. To disable the specified silence time, use the **no** form of this command.

pots silence-time *interval*
no pots silence-time *interval*

Syntax Description

interval	Number from 0 to 10 (seconds).

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command applies to Cisco 800 series routers.

Examples

The following example sets the interval of silence to 10 seconds:

```
pots silence-time 10
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing -method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect -supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect -time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots distinctive -ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.

Command	Description
pots line -type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing -freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots tone -source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots tone-source

To specify the source of dial, ringback, and busy tones for your connected telephones, fax machines, or modems, use the **pots tone-source**command in global configuration mode. To disable the specified source, use the **no** form of this command.

pots tone-source {**local** | **remote**}
no pots tone-source {**local** | **remote**}

Syntax Description

local	Router supplies the tones.
remote	Telephone switch supplies the tones.

Command Default

Local (router supplies the tones)

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command applies to Cisco 800 series routers.

This command applies only to ISDN lines connected to a EURO-ISDN (NET3) switch.

Examples

The following example sets the tone source to remote:

```
pots tone-source remote
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic
pots dialing -method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect -supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect -time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots distinctive -ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).

Command	Description
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line -type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing -freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence -time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pre-dial delay

To configure a delay on an Foreign Exchange Office (FXO) interface between the beginning of the off-hook state and the initiation of dual-tone multifrequency (DTMF) signaling, use the **pre-dial delay** command in voice-port configuration mode. To reset to the default, use the **no** form of the command.

pre-dial delay *seconds*
no pre-dial delay

Syntax Description

seconds	Delay, in seconds, before signaling begins. Range is from 0 to 10. Default is 1.

Command Default

1 second

Command Modes

Voice-port configuration

Command History

Release	Modification
11.(7)T	This command was introduced on the Cisco 3600 series.
12.0(2)T	This command was integrated into Cisco IOS Release 12.0(2)T.

Usage Guidelines

To disable the command, set the delay to 0. When an FXO interface begins to draw loop current (off-hook state), a delay is required between the initial flow of loop current and the beginning of signaling. Some devices initiate signaling too quickly, resulting in redial attempts. This command allows a signaling delay.

Examples

The following example sets a predial delay value of 3 seconds on the FXO port:

```
voice-port 1/0/0
 pre-dial delay 3
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timing delay -duration	Configures delay dial signal duration for a specified voice port.

preference (dial-peer)

To indicate the preferred order of an outbound dial peer within a hunt group, use the **preference** command in dial-peer configuration mode. To remove the preference, use the **no** form of this command.

preference **value**
no **preference**

Syntax Description

value	An integer from 0 to 10. A lower number indicates a higher preference. The default is 0, which is the highest preference.

Command Default

The longest matching dial peer supersedes the preference value.

Command Modes

Dial-peer configuration (dial-peer)

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco 2600 series and Cisco 3600 series routers.
12.0(4)T	This command was modified to support Voice over Frame Relay(VoFR) dial peers on the Cisco 2600 series and Cisco 3600 series routers.
15.1(3)T	This command was modified. Support for matching different pattern types was modified.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

This command applies to Plain Old Telephone Service(POTS), VoIP, VoFR, and Voice over ATM(VoATM) dial peers.

Use this command to indicate the preferred order for matching dial peers in a hunt group. Setting a preference enables the desired dial peer to be selected when multiple dial peers within a hunt group are matched for a dial string.

Note If POTS and voice-network peers are mixed in the same hunt group, the POTS dial peers must have priority over the voice-network dial peers.

The hunting algorithm preference is configurable. For example, to specify that a call processing sequence go to destination A, then to destination B, and finally to destination C, you would assign preferences (0 being the highest preference) to the destinations in the following order:

- Preference 0 to A
- Preference 1 to B

- Preference 2 to C

Use this command only on the same pattern type. For example, destination uri and destination-pattern are two different pattern types. By default, destination uri has higher preference than destination-pattern.

Examples

The following example shows how to set POTS dial peer 10 to a preference of 1, POTS dial peer 20 to a preference of 2, and VoFR dial peer 30 to a preference of 3:

```
dial-peer voice 10 pots
 destination-pattern 5550150
 preference 1
 exit
dial-peer voice 20 pots
 destination-pattern 5550150
 preference 2
 exit
dial-peer voice 30 vofr
 destination-pattern 5550150
 preference 3
 exit
```

The following examples shows different dial peer configurations:

```
Dialpeer        destpat         preference              session-target
1               4085550148      0 (highest)             jmmurphy-voip
2               408555          0                       sj-voip
3               408555          1 (lower)               backup-sj-voip
4               ..........      1                       0:D     (interface)
5               ..........      0                       anywhere-voip
```

If the destination number is 4085550148, the order of attempts is 1, 2, 3, 5, 4:

```
Dialpeer        destpat         preference
1               408555          0
2               4085550148      1
3               4085550         0
4     4085550    0
```

The following example shows how to set POTS dial peer 10 for the destination-pattern to a preference of 0, POTS dial peer 20 for the destination uri to a preference of 1. Though destination-pattern has higher preference than destination uri, destination uri takes preference:

```
dial-peer voice 10 pots
 destination-pattern 5550158
 preference 0
 exit
dial-peer voice 20 pots
 destination uri 5550158
 preference 1
```

exit

Related Commands

Command	Description
called-number (dial-peer)	Enables an incoming VoFR call leg to get bridged to the correct POTS call leg when using a static FRF.11 trunk connection.

Command	Description
codec (dial-peer)	Specifies the voice coder rate of speech for a Voice over Frame Relay dial peer.
cptone	Specifies a regional analog voice interface-related tone, ring, and cadence setting.
destination-pattern	Specifies the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
destination uri	Specifies the voice class used to match a dial peer to the destination uniform resource identifier (URI).
dtmf-relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
session protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

preemption enable

To enable preemption capability on a trunk group, use the **preemption enable** command in trunk group configuration mode. To disable preemption capabilities, use the **no** form of this command.

preemption enable
no preemption enable

Syntax Description

This command has no arguments or keywords.

Command Default

Preemption is disabled on the trunk group.

Command Modes

Trunk group configuration

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Examples

The following command example enables preemption capabilities on trunk group test:

```
Router(config)# trunk group test
Router(config-trunk-group)# preemption enable
```

Related Commands

Command	Description
isdn integrate all	Enables integrated mode on an ISDN PRI interface.
max-calls	Sets the maximum number of calls that a trunk group can handle.
preemption guard timer	Defines time for a DDR call and allows time to clear the last call from the channel.
preemption level	Sets the preemption level of the selected outbound dial peer. Voice calls can be preempted by a DDR call with higher preemption level.
preemption tone timer	Defines the expiry time for the preemption tone for the outgoing call being preempted by a DDR backup call.

preemption guard timer

To define the time for a DDR call and to allow time to clear the last call from the channel, use the **preemption guard timer** command in trunk group configuration mode. To disable the preemption guard time, use the **no** form of this command.

preemption guard timer *value*
no preemption guard timer

Syntax Description

value	Number, in milliseconds for the preemption guard timer. The range is 60 to 500. The default is 60.

Command Default

No preemption guard timer is configured.

Command Modes

Trunk group configuration

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Examples

The following set of commands configures a 60-millisecond preemption guard timer on the trunk group dial2.

```
Router(config)# trunk group dial2
Router(config-trunk-group)# preemption enable
Router(config-trunk-group)# preemption guard timer 60
```

Related Commands

Command	Description
isdn integrate all	Enables integrated mode on an ISDN PRI interface.
max-calls	Sets the maximum number of calls that a trunk group can handle.
preemption enable	Enables preemption capabilities on a trunk group.
preemption level	Sets the preemption level of the selected outbound dial-peer. Voice calls can be preempted by a DDR call with higher preemption level.
preemption tone timer	Sets the expiry time for the preemption tone for the outgoing call being preempted by a DDR backup call.

preemption level

To set the precedence for voice calls to be preempted by a dial-on demand routing (DDR) call for the trunk group, use the **preemption level** command in dial-peer configuration mode. To restore the default preemption level setting, use the **no** form of this command

preemption level {**flash-override** | **flash** | **immediate** | **priority** | **routine**}
no preemption level

Syntax Description

flash-override	Sets the precedence for voice calls to preemption level 0 (highest).
flash	Sets the precedence for voice calls to preemption level 1.
immediate	Sets the precedence for voice calls to preemption level 2.
priority	Sets the precedence for voice calls to preemption level 3.
routine	Sets the precedence for voice calls to preemption level 4 (lowest). This is the default.

Command Default

The preemption level default is **routine** (lowest).

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Examples

The following command example sets a preemption level of flash (level 1) on POTS dial-peer 20:

```
Router(config)# dial-peer voice 20 pots
Router(config-dial-peer)# preemption level flash
```

Related Commands

Command	Description
dialer preemption level	Sets the precedence for voice calls to be preempted by a DDR call for the dialer map.
isdn integrate all	Enables integrated mode on an ISDN PRI interface.
max-calls	Sets the maximum number of calls that a trunk group can handle.
preemption enable	Enables preemption capabilities on a trunk group.
preemption guard timer	Defines time for a DDR call and allows time to clear the last call from the channel.

Command	Description
preemption tone timer	Defines the expiry time for the preemption tone for the outgoing call being preempted by a DDR backup call.

preemption tone timer

To set the expiry time for the preemption tone for the outgoing call being preempted by a DDR backup call, use the **preemption tone timer** command in trunk group configuration mode. To clear the expiry time, use the **no** form of this command.

preemption tone timer *seconds*
no preemption tone timer

Syntax Description

seconds	Length of preemption tone, in seconds. Range: 4 to 30. Default: 10.

Command Default

No preemption tone timer is configured.

Command Modes

Trunk group configuration

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Examples

The following set of commands configures a 20-second preemption tone timer on trunk group dial2.

```
Router(config)# trunk group dial2
Router(config-trunk-group)# preemption enable
Router(config-trunk-group)# preemption tone timer 20
```

Related Commands

Command	Description
isdn integrate all	Enables integrated mode on an ISDN PRI interface.
max-calls	Sets the maximum number of calls that a trunk group can handle.
preemption enable	Enables preemption capabilities on a trunk group.
preemption level	Sets the preemption level of the selected outbound dial peer. Voice calls can be preempted by a DDR call with higher preemption level.

prefix

To specify the prefix of the dialed digits for a dial peer, use the **prefix** command in dial-peer configuration mode. To disable this feature, use the **no** form of this command.

prefix *string*
no prefix

Syntax Description

string	Integers that represent the prefix of the telephone number associated with the specified dial peer. Valid values are 0 through 9 and a comma (,). Use a comma to include a pause in the prefix.

Command Default

Null string

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(4)XJ	This command was implemented on the Cisco AS5300. It and modified for store-and-forward fax.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(13)T	This command was supported in Cisco IOS Release 12.2(13)T and implemented on the Cisco 2600XM, Cisco ICS7750, and Cisco VG200.

Usage Guidelines

Use this command to specify a prefix for a specific dial peer. When an outgoing call is initiated to this dial peer, the **prefix** *string* value is sent to the telephony interface first, before the telephone number associated with the dial peer.

If you want to configure different prefixes for dialed numbers on the same interface, you need to configure different dial peers.

This command is applicable only to plain old telephone service (POTS) dial peers. This command applies to off-ramp store-and-forward fax functions.

Examples

The following example specifies a prefix of 9 and then a pause:

```
dial-peer voice 10 pots
 prefix 9,
```

The following example specifies a prefix of 5120002:

```
Router(config-dial-peer)# prefix 5120002
```

Related Commands

Command	Description
answer -address	Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call.
destination -pattern	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer.

prefix (Annex G)

To restrict the prefixes for which the gatekeeper should query the Annex G border element (BE), use the **prefix** command in gatekeeper border element configuration mode.

prefix *prefix** [{**seq** | **blast**}]

Syntax Description

prefix *****	Prefix for which BEs should be queried.
seq	(Optional) Queries are sent out to the neighboring BEs sequentially.
blast	(Optional) Queries are sent out to the neighboring BEs simultaneously.

Command Default

Any time a remote zone query occurs, the BE is also queried.

Command Modes

Gatekeeper border element configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

By default, the gatekeeper sends all remote zone requests to the BE. Use this command only if you want to restrict the queries to the BE to a specific prefix or set of prefixes.

Examples

The following example directs the gatekeeper to query the BE using a prefix of 408.

```
Router(config-gk-annexg)# prefix 408* seq
```

Related Commands

Command	Description
h323 -annexg	Enables the BE on the gatekeeper and enters border element configuration mode.

prefix (stcapp-fac)

To define a prefix for feature access codes (FACs) used with the SCCP telephony control (STC) application, use the **prefix**command in STC application feature access-code configuration mode. To return the prefix to its default, use the **no** form of this command.

prefix *prefix-string*
no prefix

Syntax Description

prefix-string	String of one to five characters that can be dialed on a telephone keypad. String must start with an asterisk (*) or a number sign (#). Default is **.

Command Default

The default value is **.

Command Modes

STC application feature access-code configuration (stcapp-fac)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

This command modifies the FAC prefix from the default (**) to the specified character string.

Use the **show stcapp feature codes** command to display a list of all FACs.

Examples

The following example shows how to change the prefix for FACs from the default value (**) to two number signs (##).

```
Router(config)# stcapp feature access-code
Router(stcapp-fac)# prefix ##
Router(stcapp-fac)#
```

Related Commands

Command	Description
call forward all	Defines the feature code in the feature access code (FAC) for forwarding all calls.
call forward cancel	Defines the feature code in the feature access code (FAC) for cancelling Call Forward All.
pickup direct	Defines the feature code in the feature access code (FAC) for Directed Call Pickup.
pickup group	Defines the feature code in the feature access code (FAC) for call pickup from another group.
pickup local	Defines the feature code in the feature access code (FAC) for call pickup from the local group.

Command	Description
show stcapp feature codes	Displays all feature access codes (FACs) and all feature speed-dials (FSDs).
stcapp feature access-code	Enables feature access codes (FACs) in STC application and enters STC application feature access-code configuration mode for changing values of the prefix and features codes from the default.

prefix (stcapp-fsd)

To define a prefix for feature speed dials (FSDs) used with the SCCP telephony control (STC) application, use the **prefix** command in STC application feature speed-dial configuration mode. To return the prefix to its default, use the **no** form of this command.

prefix *prefix-string*
no prefix

Syntax Description

prefix-string	String of one to five characters (0-9, *, #) that can be dialed on a telephone keypad. String must begin with asterisk (*) or number sign(#). Default is *.

Command Default

The default value is *.

Command Modes

STC application feature speed-dial configuration (stcapp-fsd)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

This command is used with the STC application, which enables certain features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control. Phone users must dial the feature speed-dial (FSD) prefix string before dialing an FSD speed-dial that dials a telephone number. For example, to dial the telephone number that is stored in speed-dial position 3, a phone user dials *2.

Use this command only if you want to change the prefix from its default (*).

The **show stcapp feature codes** command displays the FSD prefix and all FSD speed-dials.

The following example shows how to change the prefix for FSDs from the default value (*) to three asterisks (***). After this value is configured, a phone user must press***2 on the keypad to dial speed-dial number 2.

```
Router(config)# stcapp feature speed-dial
Router(stcapp-fsd)# prefix ***
Router(stcapp-fsd)# speed dial from 2 to 7
Router(stcapp-fsd)# redial 9
Router(stcapp-fsd)# voicemail 8
Router(stcapp-fsd)# exit
```

Related Commands

Command	Description
redial	Defines an speed-dial code to dial again the most-recently dialed number on this phone line.
show stcapp feature codes	Displays all feature access codes (FACs) and all feature speed-dials (FSDs).
speed dial	Designates a range of feature speed-dials (FSDs) in STC application.

Command	Description
stcapp feature access-code	Enables feature speed-dials (FSDs) in STC application and enters STC application feature speed-dial configuration mode for changing values of the prefix and speed-dial codes from the default.
voicemail (stcapp-fsd)	Defines an speed-dial code to dial the voice-mail number.

preloaded-route

To enable preloaded route support for VoIP Session Initiation Protocol (SIP) calls, use the **preloaded-route**command in SIP configuration mode or voice class tenant configuration mode. To reset to the default, use the **no** form of this command.

preloaded-route [**sip-server**] **service-route system**
no preloaded-route

Syntax Description

sip-server	(Optional) Adds SIP server information to the Route header.
service-route	Adds the Service-Route information to the Route header.
system	Specifies that the preloaded route support for VoIP Session Initiation Protocol (SIP) calls use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

Route support is not enabled.

Command Modes

SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**.

Usage Guidelines

The **voice-class preloaded-route**command, in dial-peer configuration mode, takes precedence over the **preloaded-route** command in SIP configuration mode. However, if the **voice-class preloaded-route** command is configured with the **system** keyword, the gateway uses the global settings configured by the **preloaded-route**command.

Enter SIP configuration mode after entering voice-service VoIP configuration mode, as shown in the "Examples" section.

Examples

The following example shows how to configure the system to include SIP server and Service-Route information in the Route header:

```
voice service voip
sip
 preloaded-route sip-server service-route
```

The following example shows how to configure the system to include only Service-Route information in the Route header:

```
voice service voip
```

```
sip
 preloaded-route service-route
```

The following example shows how to configure the system to include only Service-Route information in the Route header in voice class tenant configuration mode:

```
Router(config-class)# preloaded-route service-route system
```

Related Commands

Command	Description
sip	Enters SIP configuration mode from voice-service VoIP configuration mode.
voice -class preloaded-route	Enables preloaded route support for dial-peer SIP calls.

presence

To enable presence service and enter presence configuration mode, use the **presence** command in global configuration mode. To disable presence service, use the **no** form of this command.

presence
no presence

Syntax Description

This command has no arguments or keywords.

Command Default

Presence service is disabled.

Command Modes

Global configuration (config)

Command History

Release	Cisco Product	Modification
12.4(11)XJ	Cisco Unified CME 4.1	This command was introduced.
12.4(15)T	Cisco Unified CME 4.1	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command enables the router to perform the following presence functions:

- Process presence requests from internal lines to internal lines. Notify internal subscribers of any status change.
- Process incoming presence requests from a SIP trunk for internal lines. Notify external subscribers of any status change.
- Send presence requests to external presentities on behalf of internal lines. Relay status responses to internal lines.

Examples

The following example shows how to enable presence and enter presence configuration mode to set the maximum subscriptions to 150:

```
Router(config)# presence
Router(config-presence)# max-subscription 150
```

Related Commands

Command	Description
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
debug presence	Displays debugging information about the presence service.
max-subscription	Sets the maximum number of concurrent watch sessions that are allowed.
presence enable	Allows the router to accept incoming presence requests.

Command	Description
server	Specifies the IP address of a presence server for sending presence requests from internal watchers to external presence entities.
show presence global	Displays configuration information about the presence service.
show presence subscription	Displays information about active presence subscriptions.

presence call-list

To enable Busy Lamp Field (BLF) monitoring for call lists and directories on phones registered to the Cisco Unified CME router, use the **presence call-list**command in ephone, presence, or voice register pool configuration mode. To disable BLF indicators for call lists, use the **no** form of this command.

presence call-list
no presence call-list

Syntax Description

This command has no arguments or keywords.

Command Default

BLF monitoring for call lists is disabled.

Command Modes

Ephone configuration (config-ephone)
Presence configuration (config-presence)
Voice register pool configuration (config-register pool)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command enables a phone to monitor the line status of directory numbers listed in a directory or call list, such as a missed calls, placed calls, or received calls list. Using this command in presence mode enables the BLF call-list feature for all phones. To enable the feature for an individual SCCP phone, use this command in ephone configuration mode. To enable the feature for an individual SIP phone, use this command in voice register pool configuration mode.

If this command is disabled globally and enabled in voice register pool or ephone configuration mode, the feature is enabled for that voice register pool or ephone.

If this command is enabled globally, the feature is enabled for all voice register pools and ephones regardless of whether it is enabled or disabled on a specific voice register pool or ephone.

To display a BLF status indicator, the directory number associated with a telephone number or extension must have presence enabled with the **allow watch** command.

For information on the BLF status indicators that display on specific types of phones, see the Cisco Unified IP Phone documentation for your phone model.

Examples

The following example shows the BLF call-list feature enabled for ephone 1. The line status of a directory number that appears in a call list or directory is displayed on phone 1 if the directory number has presence enabled.

```
Router(config)# ephone 1
Router(config-ephone)# presence call-list
```

Related Commands

Command	Description
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
blf-speed-dial	Enables BLF monitoring for a speed-dial number on a phone registered to Cisco Unified CME.
presence	Enables presence service and enters presence configuration mode.
show presence global	Displays configuration information about the presence service.

presence enable

To allow incoming presence requests, use the **presence enable** command in SIP user-agent configuration mode. To block incoming requests, use the **no** form of this command.

presence enable
no presence enable

Syntax Description

This command has no arguments or keywords.

Command Default

Incoming presence requests are blocked.

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command allows the router to accept incoming presence requests (SUBSCRIBE messages) from internal watchers and SIP trunks. It does not impact outgoing presence requests.

Examples

The following example shows how to allow incoming presence requests:

```
Router(config)# sip-ua
Router(config-sip-ua)# presence enable
```

Related Commands

Command	Description
allow subscribe	Allows internal watchers to monitor external presence entities (directory numbers).
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
max-subscription	Sets the maximum number of concurrent watch sessions that are allowed.
show presence global	Displays configuration information about the presence service.
show presence subscription	Displays information about active presence subscriptions.
watcher all	Allows external watchers to monitor internal presence entities (directory numbers).

pri-group (pri-slt)

To specify an ISDN PRI on a channelized T1 or E1 controller, use the **pri-group (pri-slt)**command in controller configuration mode. To remove the ISDN PRI configuration, use the **no** form of this command.

pri-group [**timeslots** *timeslot-range* [**nfas_d** [{**backup** | **none** | **primary** [**nfas_int** *number*]}] [**nfas-group** *number* [**iua** *as-name*]]]]
no pri-group

Syntax Description

timeslots *timeslot -range*	Specifies a single range of timeslot values in the PRI goup. For T1, the allowable range is from 1 to 23. For E1, the allowable range is from 1 to 31.
nfas_d	Specifies the operation of the D channel timeslot.
backup	(Optional) Specifes that the operation of the D channel timeslot on this controller is the NFAS D backup.
none	(Optional) Specifes that the D channel timeslot is used as an additional B channel.
primary	Specifies that the D channel timeslot on this controller in NFAS D.
nfas_int *range*	Specifies the provisioned NFAS interface value. Valid values range from 0 to 32.
nfas-group *number*	Specifies the NFAS group and the NFAS group number. Valid values range from 0 to 31.
iua *as -name*	Binds the Non-Facility Associated Signaling (NFAS) group to the IDSN User Adaptation Layer (IUA) application server (AS).

Command Default

No ISDN-PRI group is configured.

Command Modes

Controller configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(15)T	This command was integrated on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

Usage Guidelines

The pri-group (pri-slt) command provides another way to bind a D channel to a specific IUA AS. This option allows the RLM group to be configured at the pri-group level instead of in the D channel configuration. For example, a typical configuration would look like the following:

```
controller t1 1/0/0
 pri-group timeslots 1-24 nfas_d pri nfas_int 0 nfas_group 1 iua asname
```

Before you enter the **pri-group** command, you must specify an ISDN-PRI switch type and an E1 or T1 controller.

When configuring NFAS, you use an extended version of the pri-group command to specify the following values for the associated channelized T1 controllers configured for ISDN:

- The range of PRI timeslots to be under the control of the D channel (timeslot 24).
- The function to be performed by timeslot 24 (primary D channel, backup, or none); the latter specifies its use as a B channel.
- The group identifier number for the interface under the control of a particular D channel.

The iua keyword is used to bind an NFAS group to the IUA AS.

When binding the D channel to an IUA AS, the *as-name* must match the name of an AS set up during IUA configuration.

Before you can modify a PRI group on a Media Gateway Controller (MGC), you must first shut down the D channel.

The following shows how to shut down the D channel:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface Dchannel3/0:1
Router(config-if)# shutdown
```

Examples

The following example configures the NFAS primary D channel on one channelized T1 controller, and binds the D channel to an IUA AS. This example uses the Cisco AS5400 and applies to T1, which has 24 timeslots and is used mainly in North America and Japan:

```
Router(config-controller)# pri-group timeslots 1-23 nfas-d primary nfas-int 0 nfas-group 1
 iua as5400-4-1
```

The following example applies to E1, which has 32 timeslots and is used by the rest of the world:

```
Router(config-controller)# pri-group timeslots 1-31 nfas-d primary nfas-int 0 nfas-group 1
 iua as5400-4-1
```

The following example configures ISDN-PRI on all time slots of controller E1:

```
Router(config)# controller E1 4/1
Router(config-controller)# pri-group timeslots 1-7,16
```

In the following example, the **rlm-timeslot** keyword automatically creates interface serial 4/7:11 (4/7:0:11 if you are using the CT3 card) for the D channel object on a Cisco AS5350. You can choose any timeslot other than 24 to be the virtual container for the D channel parameters for ISDN.

```
Router(config-controller)# pri-group timeslots 1-23 nfas-d primary nfas-int 0 nfas-group 0
 rlm-timeslot 3
```

Related Commands

Command	Description
isdn switch -type	Configures the Cisco 2600 series router PRI interface to support QSIG signaling.

pri-group nec-fusion

To configure your NEC PBX to support Fusion Call Control Signaling (FCCS), use the **pri-group nec-fusion** command in controller configuration mode. To disable FCCS, use the **no** form of this command.

pri-group nec-fusion {*pbx-ip-addresspbx-ip-host-name*} **pbx-port** *number*
no pri-group nec-fusion {*pbx-ip-addresspbx-ip-host-name*} **pbx-port** *number*

Syntax Description

pbx -ip-address	IP address of the NEC PBX.
pbx -ip-host-name	Host name of the NEC PBX.
pbx -port *number*	Port number for the PBX. Range is from 49152 to 65535. Default is 55000. If this value is already in use, the next greater value is used.

Command Default

PBX port number: 55000

Command Modes

Controller configuration

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5300.
12.2(1)	This command was modified to add support for setup messages from a POTS dial peer.

Usage Guidelines

This command is used only if the PBX in your configuration is an NEC PBX, and if you are configuring it to run FCCS and not QSIG signaling.

Examples

The following example directs this NEC PBX to use FCCS:

```
pri-group nec-fusion 172.31.255.255 pbx-port 60000
```

Related Commands

Command	Description
isdn protocol-emulate	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality.
isdn switch type	Configures the Cisco AS5300 universal access server PRI interface to support QSIG signaling.
show cdapi	Displays the CDAPI.
show rawmsg	Displays the raw messages owned by the required component.

pri-group timeslots

To specify an ISDN PRI group on a channelized T1 or E1 controller, and to release the ISDN PRI signaling time slot, use the **pri-group timeslots**command in controller configuration mode. To remove or change the ISDN PRI configuration, use the **no** form of this command.

pri-group timeslots *timeslot-range* [{**nfas_d** {**backup nfas_int** *number* **nfas_group** *number* [**service mgcp**] | **none nfas_int** *number* **nfas_group** *number* [**service mgcp**] | **primary nfas_int** *number* **nfas_group** *number* [{**iua** *as-name* | **rlm-group** *number* | **service mgcp**}]} | **service mgcp**}] [**voice-dsp**]
no pri-group timeslots *timeslot-range* [{**nfas_d** {**backup nfas_int** *number* **nfas_group** *number* [**service mgcp**] | **none nfas_int** *number* **nfas_group** *number* [**service mgcp**] | **primary nfas_int** *number* **nfas_group** *number* [{**iua** *as-name* | **rlm-group** *number* | **service mgcp**}]} | **service mgcp**}] [**voice-dsp**]

Syntax Description

timeslot-range	A value or range of values for time slots on a T1 or E1 controller that consists of an ISDN PRI group. Use a hyphen to indicate a range. **Note** Groups of time slot ranges separated by commas (1-4,8-23 for example) are also accepted.
nfas_d	(Optional) Configures the operation of the ISDN PRI D channel.
backup	The D-channel time slot is used as the Non-Facility Associated Signaling (NFAS) D backup.
service mgcp	(Optional) Configures the service type as Media Gateway Control Protocol (MGCP) service.
none	The D-channel time slot is used as an additional B channel.
primary	The D-channel time slot is used as the NFAS D primary.
nfas_int *number*	Specifies the provisioned NFAS interface as a value. The NFAS interface range is from 0 to 44.
nfas_group *number*	Specifies the NFAS group. The NFAS group number range is from 0 to 31.
iua *as-name*	(Optional) Configures the ISDN User Adaptation Layer (IUA) application server (AS) name.
rlm-group *number*	(Optional) Specifies the Redundant Link Manager (RLM) group and releases the ISDN PRI signaling channel. The RLM group number range is from 0 to 255.
voice-dsp	(Optional) Configures an ISDN PRI group for voice applications by using the Digital Signal Processor (DSP).

Command Default

No ISDN PRI group is configured. The switch type is automatically set to the National ISDN switch type (**primary-ni** keyword)when the **pri-group timeslots**command is configured with the **rlm-group** keyword.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
11.0	This command was introduced.
11.3	This command was enhanced to support NFAS.
12.0(2)T	This command was implemented on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	This command was implemented on the Cisco 2600 and Cisco 3600 series routers.
12.1(2)T	The modifications in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.
12.2(8)B	This command was modified with the **rlm-group** subkeyword to support the release of the ISDN PRI signaling channels.
12.2(15)T	The modifications in Cisco IOS Release 12.2(8)B were integrated into Cisco IOS Release 12.2(15)T.
12.4(16)b	This command was modified to ensure that the NFAS primary interface is configured before the NFAS backup or NFAS none interfaces are configured.
12.4(24)T	Support was extended to provide backup functionality for the NFAS interface in MGCP backhaul mode. With this support, if the primary interface fails, the backup can become active and calls can be maintained.
15.1(3)T	This command was modified. The **voice-dsp** keywordwas added.

Usage Guidelines

The **pri-group** command supports the use of DS0 time slots for Signaling System 7 (SS7) links, and, therefore, enables the coexistence of SS7 links and PRI voice and data bearer channels on the same T1 or E1 span. In these configurations, the command applies to voice applications.

In SS7-enabled Voice over IP (VoIP) configurations when an RLM group is configured, High-Level Data Link Control (HDLC) resources allocated for ISDN signaling on a digital subscriber line (DSL) interface are released and the signaling slot is converted to a bearer channel (B24). The D channel will be running on IP. The chosen D-channel time slot can still be used by a B channel by using the **isdn rlm-group** interface configuration command to configure the NFAS groups.

NFAS allows a single D channel to control multiple PRI interfaces. Use of a single D channel to control multiple PRI interfaces frees one B channel on each interface to carry other traffic. A backup D channel can also be configured for use when the primary NFAS D channel fails. When a backup D channel is configured, any hard system failure causes a switchover to the backup D channel and currently connected calls remain connected.

NFAS is supported only with a channelized T1 controller and, as a result, must be ISDN PRI capable. When the channelized T1 controllers are configured for ISDN PRI, only the NFAS primary D channel must be configured; its configuration is distributed to all members of the associated NFAS group. Any configuration changes made to the primary D channel will be propagated to all NFAS group members. The primary D-channel interface is the only interface shown after the configuration is written to memory.

The channelized T1 controllers on the router must also be configured for ISDN. The router must connect to either an AT&T 4ESS, Northern Telecom DMS-100 or DMS-250 switch type, or a National ISDN switch type.

The ISDN switch must be provisioned for NFAS. The primary and backup D channels should be configured on separate T1 controllers. The primary, backup, and B-channel members on the respective controllers should have the same configuration as that of the router and ISDN switch. The interface ID assigned to the controllers must match that of the ISDN switch.

You can disable a specified channel or an entire PRI interface, thereby taking it out of service or placing it into one of the other states that is passed in to the switch using the **isdn service** command.

In the event that a controller belonging to an NFAS group is shut down, all active calls on the controller that is shut down will be cleared (regardless of whether the controller is set to primary, backup, or none), and one of the following events will occur:

- If the controller that is shut down is configured as the primary and no backup is configured, all active calls on the group are cleared.
- If the controller that is shut down is configured as the primary, and the active (In service) D channel is the primary and a backup is configured, then the active D channel changes to the backup controller.
- If the controller that is shut down is configured as the primary, and the active D channel is the backup, then the active D channel remains as the backup controller.
- If the controller that is shut down is configured as the backup, and the active D channel is the backup, then the active D channel changes to the primary controller.

The expected behavior in NFAS when an ISDN D channel (serial interface) is shut down is that ISDN Layer 2 should go down but keep ISDN Layer 1 up, and that the entire interface will go down after the amount of seconds specified for timer T309.

Note The active D -channel changeover between primary and backup controllers happens only when one of the link fails and not when the link comes up. The T309 timer is triggered when the changeover takes place.

Note You must first configure the NFAS primary D channel before configuring the NFAS backup or NFAS none interfaces. If this order is not followed, this message is displayed: NFAS backup and NFAS none interfaces are not allowed to be configured without primary. First configure primary D channel. To remove the NFAS primary D channel after the NFAS backup or NFAS none interfaces are configured, you must remove the NFAS backup or NFAS none interfaces first, and then remove the NFAS primary D channel.

The **voice-dsp**keyword is available only on 1-Port and 2-Port HWIC on ISR-G2 (Cisco 2911, Cisco 2921, Cisco 2951, Cisco 3925, Cisco 3925E, Cisco 3945, and Cisco 3945E). This keyword is not available on controller T1 0/1/0 on Voice/WAN(VWIC) interface card.

Examples

The following example shows how to configure a T1 controller 1/0 for PRI and for the NFAS primary D channel. This primary D channel controls all the B channels in NFAS group 1.

```
controller t1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 1
```

The following example shows how to configure an ISDN PRI on T1 slot 1, port 0, and configure voice and data bearer capability on time slots 2 through 6:

```
isdn switch-type primary-4ess
controller t1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 2-6
```

The following example shows how to configure a standard ISDN PRI interface:

```
! Standard PRI configuration:
controller t1 1
 pri-group timeslots 1-23 nfas_d primary nfas_int 0 nfas_group 0
 exit
! Standard ISDN serial configuration:
interface serial1:23
! Set ISDN parameters:
 isdn T309 4000
 exit
```

The following example shows how to configure a dedicated T1 link for SS7-enabled VoIP:

```
controller T1 1
 pri-group timeslots 1-23 nfas_d primary nfas_int 0 nfas_group 0
 exit
! In a dedicated configuration, we assume the 24th timeslot will be used by ISDN.
! Serial interface 0:23 is created for configuring ISDN parameters.
interface Serial:24
! The D channel is on the RLM.
 isdn rlm 0
 isdn  T309 4000
 exit
```

The following example shows how to configure a shared T1 link for SS7-enabled VoIP. The **rlm-group 0** portion of the **pri-group timeslots** command releases the ISDN PRI signaling channel.

```
controller T1 1
 pri-group timeslots 1-3 nfas_d primary nfas_int 0 nfas_group 0 rlm-group 0
 channel group 23 timeslot 24
 end
! D-channel interface is created for configuration of ISDN parameters:
interface Dchannel1
 isdn T309 4000
 end
```

The following example shows how to configure T1 controller 0/2/1 for a PRI with the voice applications option:

```
Router(config)#controller T1 0/2/1
Router(config-controller)#pri-group timeslots 1-24
Router(config-controller)#pri-group timeslots 1-24 voice-dsp
```

Related Commands

Command	Description
controller	Configures a T1 or E1 controller and enters controller configuration mode.

Command	Description
interface Dchannel	Specifies an ISDN D-channel interface for VoIP applications that require release of the ISDN PRI signaling time slot for RLM configurations.
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI signaling.
isdn rlm-group	Specifies the RLM group number that ISDN will start using.
isdn switch-type	Specifies the central office switch type on the ISDN PRI interface.
isdn timer t309	Changes the value of the T309 timer to clear network connections and releases the B channels when there is no active signaling channel.
show isdn nfas group	Displays all the members of a specified NFAS group or all NFAS groups.

primary (gateway accounting file)

To set the primary location for storing the call detail records (CDRs) generated for file accounting, use the **primary**command in gateway accounting file configuration mode. To reset to the default, use the **no** form of this command.

primary {**ftp** *path/filename* **username** *username* **password** *password* | **ifs** *device***:***filename*}
no primary {**ftp** | **ifs**}

Syntax Description

ftp *path /filename*	Name and location of the file on an external FTP server. Filename is limited to 25 characters.
ifs *device* **:** *filename*	Name and location of the file in flash memory or other internal file system on this router. Values depend on storage devices available on the router, for example flash or slot0. Filename is limited to 25 characters.
username *username*	User ID for authentication.
password *password*	Password user enters for authentication.

Command Default

Call records are saved to **flash:cdr**.

Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command specifies the name and location of the primary file where CDRs are stored during the file accounting process. The filename you assign is appended with the gateway hostname and time stamp at the time the file is created to make the filename unique.

For example, if you specify the filename cdrtest1 on a router with the hostname cme-2821, a file is created with the name cdrtest1.cme-2821.2007_10_28T22_21_41.000, where 2007_10_28T22_21_41.000 is the time that the file was created.

Limit the filename you assign with this command to 25 characters, otherwise it could be truncated when the accounting file is created because the full filename, including the appended hostname and timestamp, is limited to 63 characters.

If the file transfer to this primary device fails, the file accounting process retries the primary device up to the number of times defined by the **maximum retry-count** command and then switches over to the secondary device defined with the **secondary** command.

To manually switch back to the primary device when it becomes available, use the **file-acct reset** command. The system does not automatically switch back to the primary device.

A syslog warning message is generated when flash becomes full.

Examples

The following example shows the primary location of the accounting file is set to an external FTP server and the filename is cdrtest1:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary flash ifs:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 maximum fileclose-timer 720
 cdr-format compact
```

The following examples show how the accounting file is named when it is created. The router hostname and time stamp are appended to the filename that you assign with this command:

```
cme-2821(config)# primary ftp server1/cdrtest1 username bob password temp
```

The name of the accounting file that is created has the following format:

cdrtest1.cme-2821.06_04_2007_18_44_51.785

Related Commands

Command	Description
file-acct flush	Manually flushes the CDRs from the buffer to the accounting file.
file-acct reset	Manually switches back to the primary device for file accounting.
maximum retry-count	Sets the maximum number of times the router attempts to connect to the primary file device before switching to the secondary device.
secondary	Sets the backup location for storing CDRs if the primary location becomes unavailable.

privacy

To set privacy support at the global level as defined in RFC 3323, use the **privacy** command in voice service voip sip configuration mode or voice class tenant configuration mode. To remove privacy support as defined in RFC 3323, use the **no** form of this command.

privacy {**pstn** | *privacy-option* [**critical**]} **[system]**
no privacy

Syntax Description

pstn	Requests that the privacy service implements a privacy header using the default Public Switched Telephone Network (PSTN) rules for privacy (based on information in Octet 3a). When selected, this becomes the only valid option.
privacy-option	The privacy support options to be set at the global level. The following keywords can be specified for the *privacy-option* argument: • **header** -- Requests that privacy be enforced for all headers in the Session Initiation Protocol (SIP) message that might identify information about the subscriber. • **history** -- Requests that the information held in the history-info header is hidden outside the trust domain. • **id** -- Requests that the Network Asserted Identity that authenticated the user be kept private with respect to SIP entities outside the trusted domain. • **session** -- Requests that the information held in the session description is hidden outside the trust domain. • **user** -- Requests that privacy services provide a user-level privacy function. **Note** The keywords can be used alone, altogether, or in any combination with each other, but each keyword can be used only once.
critical	(Optional) Requests that the privacy service performs the specified service or fail the request. **Note** This optional keyword is only available after at least one of the *privacy-option* keywords (**header**, **history**, **id**, **session**, or **user**) has been specified and can be used only once per command.
system	Specifies that the privacy support use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

Privacy support is disabled.

Command Modes

Voice service voip sip configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Release	Modification
12.4(22)T	The **history** keyword was added to provide support for the history-info header information.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the **privacy** command to instruct the gateway to add a Proxy-Require header set to a value supported by RFC 3323 in outgoing SIP request messages.

Use the **privacy critical** command to instruct the gateway to add a Proxy-Require header with the value set to critical. If a user agent sends a request to an intermediary that does not support privacy extensions, the request fails.

Examples

The following example shows how to set the privacy to PSTN:

```
Router> enable

Router# configure
 terminal
Router(config)# voice
 service
 voip

Router(conf-voi-serv)# sip
Router(conf-serv-sip)# privacy
 pstn
```

The following example shows how to set privacy in the voice class tenant configuration mode:

```
Router(config-class)# privacy system
```

Related Commands

Command	Description
asserted-id	Sets the privacy level and enables either PAI or PPI privacy headers in outgoing SIP requests or response messages.
calling-info pstn-to-sip	Specifies calling information treatment for PSTN-to-SIP calls.
clid (voice-service-voip)	Passes the network-provided ISDN numbers in an ISDN calling party information element screening indicator field, removes the calling party name and number from the calling-line identifier in voice service voip configuration mode, or allows a presentation of the calling number by substituting for the missing Display Name field in the Remote-Party-ID and From headers.
voice-class sip privacy	Sets privacy support at the dial-peer configuration level as defined in RFC 3323.

privacy (supplementary-service)

To prevent phones on a shared line from joining active calls, use the **privacy** command in supplementary-service voice-port configuration mode. To return to the default behavior, use the **no** form of this command.

privacy {**on** | **off**}
no privacy

Syntax Description

on	Prevents other phones on the shared line to join active calls.
off	Allows other phones on the shared line to join active calls.

Command Default

The **no privacy** command implies that a port does not decide on its privacy status. It is not the gateway but the Cisco Unified CM that decides on the privacy status of a port.

Command Modes

Supplementary-service voice-port configuration mode (config-stcapp-suppl-serv-port)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

The **privacy** command enables privacy support on analog endpoints that are connected to Foreign Exchange Station (FXS) ports on a Cisco IOS Voice Gateway, such as a Cisco Integrated Services Router (ISR) or Cisco VG224 Analog Phone Gateway.

Use the **privacy** command to prevent other phones on the shared line to join active calls.

Examples

The following example shows how to turn on privacy support on port 2/4 on a Cisco VG224:

```
Router(config)# stcapp supplementary-services
Router(config-stcapp-suppl-serv)# port 2/4
Router(config-stcapp-suppl-serv-port)# privacy on
Router(config-stcapp-suppl-serv-port)# end
```

Related Commands

Command	Description
stcapp supplementary-services	Enters supplementary-service configuration mode for configuring STCAPP supplementary-service features on an FXS port.

privacy-policy

To configure the privacy header policy options at the global level, use the **privacy-policy** command in voice service VoIP SIP configuration mode or voice class tenant configuration mode. To disable privacy header policy options, use the **no** form of this command.

privacy-policy {**passthru** | **send-always** | **strip** {**diversion** | **history-info**} **[system]**}
no privacy-policy {**passthru** | **send-always** | **strip** {**diversion** | **history-info**} **[system]**}

Syntax Description

passthru	Passes the privacy values from the received message to the next call leg.
send-always	Passes a privacy header with a value of None to the next call leg, if the received message does not contain privacy values but a privacy header is required.
strip	Strips the diversion or history-info headers received from the next call leg.
diversion	Strips the diversion headers received from the next call leg.
history-info	Strips the history-info headers received from the next call leg.
system	Specifies that the privacy header policy options use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

No privacy-policy settings are configured.

Command Modes

Voice service VoIP SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(2)T	This command was modified. The **strip**, **diversion**, and **history-info** keywords were added.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

If a received message contains privacy values, use the **privacy-policy passthru** command to ensure that the privacy values are passed from one call leg to the next. If the received message does not contain privacy values but the privacy header is required, use the **privacy-policy send-always** command to set the privacy header to None and forward the message to the next call leg. If you want to strip the diversion and history-info from the headers received from the next call leg, use the **privacy-policy strip** command. You can configure the system to support all the options at the same time.

Examples

The following example shows how to enable the pass-through privacy policy:

```
Router> enable

Router# configure
 terminal
Router(config)# voice
 service
 voip

Router(conf-voi-serv)# sip
Router(conf-serv-sip)# privacy-policy passthru
```

The following example shows how to enable the send-always privacy policy:

```
Router(config-class)# privacy-policy send-always system
```

The following example shows how to enable the strip privacy policy:

```
Router> enable

Router# configure
 terminal
Router(config)# voice
 service
 voip

Router(conf-voi-serv)# sip
Router(conf-serv-sip)# privacy-policy strip diversion
Router(conf-serv-sip)# privacy-policy strip history-info
```

The following example shows how to enable the pass-through, send-always privacy, and strip policies:

```
Router> enable

Router# configure
 terminal
Router(config)# voice
 service
 voip

Router(conf-voi-serv)# sip
Router(conf-serv-sip)# privacy-policy passthru
Router(conf-serv-sip)# privacy-policy send-always
Router(conf-serv-sip)# privacy-policy strip diversion
Router(conf-serv-sip)# privacy-policy strip history-info
```

The following example shows how to enable the send-always privacy policy in the voice class tenant configuration mode:

Related Commands

Command	Description
asserted-id	Sets the privacy level and enables either PAID or PPID privacy headers in outgoing SIP requests or response messages.
voice-class sip privacy-policy	Configures the privacy header policy options at the dial-peer configuration level.

probing interval

To configure the time interval between probing messages sent by the router, use the **probing interval** command. To reset the time interval to the default number, use the **no** form of this command.

probing interval[{**keepalive** | **negative**}] *seconds*

Syntax Description

keepalive	(optional) Configures the time interval between probing messages when the session is in a keepalive state. Range is from 1 to 255 seconds. Default is 5 seconds.
negative	(optional) Configures the time interval between probing messages when the session is in a negative state. Range is from 1 to 20 seconds. Default is 5 seconds.
seconds	Number of seconds between probing message.

Command Default

The default is 120 seconds between probing messages when the session is in a normal state and 5 seconds between probing messages when the session is in a negative state.

Command Modes

uc wsapi configuration mode.

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use this command to configure the time interval between probing messages sent by the router.

Examples

The following example sets an interval of 180 seconds for a normal session and 10 seconds when the session is in a negative state.

```
Router(config)# uc wsapi
Router(config-uc-wsapi)# probing interval keepalive 180
Router(config-uc-wsapi)# probing interval negative 10
```

Related Commands

Command	Description
message-exchange	Sets the maximum number of failed message responses before the provider stops sending messages.
probing max-failure	Sets the number of messages that the system will send without receiving a reply before the system unregisters the application.

probing max-failures

To configure the maximum number of probing messages that the system attempts to send to the application, and the application does not respond to before the system stops the session and unregisters the application, use the **probing max-failures** command. To reset the maximum to the default number, use the **no** form of this command.

probing max-failures *number*
no probing max-failures *number*

Syntax Description

number	Maximum number of messages allowed before the system stops the session and unregisters the application. Range is from 1 to 5. Default is 3.

Command Default

The default is 3.

Command Modes

uc wsapi configuration mode

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use this command to set the maximum number of probing messages sent by the system that the application does not respond to before the system stops the session and unregisters the application session.

Examples

The following example sets the maximum number of failed messages to 5.

```
Router(config)# uc wsapi
Router(config-uc-wsapi)# probing max-failures 5
```

Related Commands

Command	Description
message-exchange	Sets the maximum number of failed message attempts before the provider stops sending messages.
probing interval	Sets the time interval between probing messages.

progress_ind

To configure an outbound dial peer on a Cisco IOS voice gateway or Cisco Unified Border Element to override and remove or replace the default progress indicator (PI) in specified call messages, use the **progress_ind** command in dial peer voice configuration mode. To disable removal or replacement of the default PI in specific call messages, use the **no** form of this command.

progress_ind {{**alert** | **callproc**} {**enable** *pi-number* | **disable** | **strip** [*strip-pi-number*]} | {**connect** | **disconnect** | **progress** | **setup**} {**enable** *pi-number* | **disable**}}
no progress_ind {**alert** | **callproc** | **connect** | **disconnect** | **progress** | **setup**}

Syntax Description

alert	Specifies that the configuration applies to call Alert messages.
callproc	Specifies that the configuration applies to Session Initiation Protocol (SIP) 183 Session In Progress (Call_Proceeding) messages.
connect	Specifies that the configuration applies to call Connect messages.
disconnect	Specifies that the configuration applies to call Disconnect messages.
progress	Specifies that the configuration applies to call progress messages.
setup	Specifies that the configuration applies to call setup messages.
enable	Enables user-specified configuration of the progress indicator on the specified call message type.
pi -number	Specifies the PI to be used in place of the default PI. The following are acceptable PI values according to the call message type: • Alert, Connect, Progress, and SIP 183 Session In Progress messages: 1, 2, or 8. • Disconnect messages: 8. • Setup messages: 0, 1, or 3.
disable	Disables user-specified configuration of the progress indicator on the specified call message type.
strip	Configures the dial peer to remove all or specific progress indicators in the specified call message type. **Note** This option applies only to call Alert message on POTS dial peers or to call Proceeding messages on VoIP dial peers.
strip-pi -number	(optional) Specifies that only a specific PI is to be removed from the specified call message. The value can be 1, 2, or 8.

Command Default

This command is disabled on the outbound dial peer and the default progress indicator that is received in the incoming call message is passed intact (it is not intercepted, modified, or removed).

Command Modes

Dial peer voice configuration (conf-dial-peer)

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco 7500 series, Cisco MC3810, Cisco AS5300, and Cisco AS5800.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(1)	This command was modified. Support was added for setup messages from a POTS dial peer.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
15.0(1)XA	This command was modified. Support was added for stripping of PIs in call Alert and SIP 183 Session In Progress (Call_Proceeding) messages.
15.1(1)T	This command was integrated into Cisco IOS Release 5.1(1)T.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Before configuring the **progress_ind** command on an outbound dial peer, you must configure a destination pattern on the dial peer. To configure a destination pattern for an outbound dial peer, use the **destination-pattern** command in a dial peer voice configuration mode. Once you have set a destination pattern on the dial peer, you can then use the **progress_ind** command, also in dial peer voice configuration mode, to override and replace or remove the default PI in specific call message types.

You can use the **progress_ind** command to configure replacement behavior on outbound dial peers on a Cisco IOS voice gateway or CUBEto ensure proper end-to-end signaling of VoIP calls. You can also use this command to configure removal (stripping) of PIs on outbound dial peers on Cisco IOS voice gateways or CUBEs, such as when configuring a Cisco IOS SIP gateway (or SIP-SIPCUBE) to not generate another SIP 183 Session In Progress messages.

For messages that contain multiple PIs, behavior that is configured using the **progress_ind** command overrides only the first PI in the message. Also, configuring a replacement PI will not result in an override of the default PI in call progress messages if the Progress message is sent after a backward cut-through event, such as when an Alert message with a PI of 8 was sent before the Progress message.

Use the **no progress_ind** command in dial peer voice configuration mode to disable PI override configurations on a dial peer on a Cisco IOS voice gateway or CUBE.

Examples

The following example shows how to configure POTS dial peer 3 to override default PIs in call progress and Connect messages and replace them with a PI of 1:

```
Router(config)# dial-peer voice 3 pots
Router(config-dial-peer)# destination-pattern 555
```

```
Router(config-dial-peer)# progress_ind progress enable 1
Router(config-dial-peer)# progress_ind connect enable 1
```

The following example configures outbound VoIP dial peer 1 to override SIP 183 Session In Progress messages and to strip out any PIs with a value of 8:

```
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# destination-pattern 777
Router(config-dial-peer)# progress_ind callproc strip 8
```

Related Commands

Command	Description
destination-pattern	Specifies the destination pattern (prefix or full E.164 phone number) to be used on an outbound dial peer.

protocol mode

To configure the Cisco IOS Session Initiation Protocol (SIP) stack, use the **protocol mode**command in SIP user-agent configuration mode. To disable the configuration, use the **no** form of this command.

protocol mode {**ipv4** | **ipv6** | **dual-stack** [**preference** {**ipv4** | **ipv6**}]}
no protocol mode

Syntax Description

ipv4	Specifies the IPv4-only mode.
ipv6	Specifies the IPv6-only mode.
dual-stack	Specifies the dual-stack (that is, IPv4 and IPv6) mode.
preference {**ipv4** | **ipv6**	(Optional) Specifies the preferred dual-stack mode, which can be either IPv4 (the default preferred dual-stack mode) or IPv6.

Command Default

No protocol mode is configured. The Cisco IOS SIP stack operates in IPv4 mode when the **no protocol mode** or **protocol mode ipv4** command is configured.

Command Modes

SIP user-agent configuration (config-sip-ua)

Command History

Release	Modification
12.4(22)T	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

The **protocol mode** command is used to configure the Cisco IOS SIP stack in IPv4-only, IPv6-only, or dual-stack mode. For dual-stack mode, the user can (optionally) configure the preferred family, IPv4, or IPv6.

For a particular mode (for example, IPv6-only), the user can configure any address (for example, both IPv4 and IPv6 addresses) and the system will not hide or restrict any commands on the router. SIP chooses the right address for communication based on the configured mode on a per-call basis.

For example, if the domain name system (DNS) reply has both IPv4 and IPv6 addresses and the configured mode is IPv6-only (or IPv4-only), the system discards all IPv4 (or IPv6) addresses and tries the IPv6 (or IPv4) addresses in the order they were received in the DNS reply. If the configured mode is dual-stack, the system first tries the addresses of the preferred family in the order they were received in the DNS reply. If all the addresses fail, the system tries addresses of the other family.

Examples

The following example configures dual-stack as the protocol mode:

```
Router(config-sip-ua)# protocol mode dual-stack
```

The following example configures IPv6 only as the protocol mode:

```
Router(config-sip-ua)# protocol mode ipv6
```

The following example configures IPv4 only as the protocol mode:

```
Router(config-sip-ua)# protocol mode ipv4
```

The following example configures no protocol mode:

```
Router(config-sip-ua)# no protocol mode
```

Related Commands

Command	Description
sip ua	Enters SIP user-agent configuration mode.

protocol rlm port

To configure the RLM port number, use the **protocol rlm port** RLM configuration command. To disable this function, use the **no** form of this command.

protocol rlm port *port-number*
no protocol rlm port *port-number*

Syntax Description

port -number	RLM port number. See the table below for the port number choices.

Command Default

3000

Command Modes

RLM configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Usage Guidelines

The port number for the basic RLM connection can be reconfigured for the entire RLM group. The table below lists the default RLM port numbers.

Table 5: Default RLM Port Number

Protocol	Port Number
RLM	3000
ISDN	Port[RLM]+1

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.

Command	Description
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

provider

To configure and enable a service provider, use the **provider** command. To remove the provider, use the **no** form of this command.

provider [{**xcc** | **xsvc** | **xcdr** | **xmf**}]
no provider [{**xcc** | **xsvc** | **xcdr** | **xmf**}]

Syntax Description

xcc	(optional) Enables the XCC service provider.
xsvc	(optional) Enables the XSVC service provider.
xcdr	(optional) Enables the XCDR service provider.
xmf	(optional) Enables the XMF service provider.

Command Default

No default behavior or values.

Command Modes

uc wsapi configuration mode

uc secure-wsapi

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.3(2)T	**xmf** keyword was added.
Cisco IOS XE Everest 16.6.1	Added support for **xcc** and **xsvc** service providers in secure mode.

Usage Guidelines

Use this command to enable a service provider.

Note You can enable only **xcc** and **xsvc** service providers in secure mode.

Examples

The following example enables the XCC service provider in nonsecure mode.

```
Router(config)# uc wsapi
Router(config-uc-wsapi)# provider xcc
Router(config-uc-wsapi-xcc)# no shutdown
```

Examples

The following example enables the XCC service provider in secure mode.

```
Router(config)# uc secure-wsapi
Router(config-uc-wsapi)# provider xcc
Router(config-uc-wsapi-xcc)# no shutdown
```

Related Commands

Command	Description
remote-url	Specifies the URL of the application.
source-address	Specifies the IP address of the provider.
uc wsapi	Enters nonsecure Cisco Unified Communication IOS services configuration mode.
uc secure-wsapi	Enters secure Cisco Unified Communication IOS services configuration mode.

proxy h323

To enable the proxy feature on your router, use the **proxy h323** command in global configuration mode. To disable the proxy feature, use the **no** form of this command.

proxy h323
no proxy h323

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 series and Cisco 3600 series.

Usage Guidelines

If the multimedia interface is not enabled using this command or if no gatekeeper is available, starting the proxy allows it to attempt to locate these resources. No calls are accepted until the multimedia interface and the gatekeeper are found.

Examples

The following example turns on the proxy feature:

```
proxy h323
```

proxy (media-profile)

To configure IP address or hostname of a WebSocket proxy server in CUBE, use the **proxy** command in media profile configuration mode. To remove the configuration, use the **no** form of this command.

proxy { **host** *host* **port** *port* | **ipv4** *ip-address* **port** *port* }
no proxy { **host** *host* **port** *port* | **ipv4** *ip-address* **port** *port* }

Syntax Description

host	WebSocket proxy server hostname.
ipv4 *ip-address*	Host IP address of the WebSocket proxy server.
port *port*	WebSocket proxy server port.

Command Default

Disabled by default.

Command Modes

Media Profile configuration mode (cfg-mediaprofile)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was introduced on Cisco Unified Border Element.

Usage Guidelines

If there's a proxy between the WebSocket speech server and CUBE, the IP address or hostname of the proxy must be configured in media-profile. The **proxy** command configures the host IP address of the proxy server or the hostname in media profile configuration mode.

If a proxy server is configured, the WebSocket connection must be established with the proxy server itself. It is not possible to establish a direct connection with the speech server.

Note **port** *port* is an optional configuration parameter.

Examples

The following is a sample configuration for **proxy (media-profile)** in CUBE:

```
router(cfg-mediaprofile)#proxy ?
host WebSocket proxy server hostname
ip WebSocket proxy server IP address

router(cfg-mediaprofile)#proxy host
router(cfg-mediaprofile)#proxy host abc.com ?
port WebSocket proxy server port
<cr> <cr>

router(cfg-mediaprofile)#proxy host abc.com port ?
<0-65535> proxy server port

router(cfg-mediaprofile)#proxy host abc.com port 3578


router(cfg-mediaprofile)#proxy ipv4 ?
```

```
A.B.C.D Specify IP address of proxy server

router(cfg-mediaprofile)#proxy ip 1.1.1.1 ?
port WebSocket proxy server port
<cr> <cr>

router(cfg-mediaprofile)#proxy ip 1.1.1.1 port ?
<0-65535> proxy server port

router(cfg-mediaprofile)#proxy ip 1.1.1.1 port 3456
```

Related Commands

Command	Description
media profile stream-service	Enables stream service on CUBE.
connection (media-profile)	Configures idle timeout and call threshold for a media profile.
source-ip (media-profile)	Configures local source IP address of a WebSocket connection.
media class	Applies the media class at the dial peer level.

pulse-digit-detection

To enable pulse digit detection at the beginning of a call, use the **pulse-digit-detection** command in voice-port configuration mode. To disable pulse digit detection, use the **no** form of this command.

pulse-digit-detection
no pulse-digit-detection

Syntax Description

This command has no arguments or keywords.

Command Default

Pulse digit detection is enabled.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Pulse digit detection is disabled at the beginning of a call for any Foreign Exchange Station (FXS) voice port not configured with the **no pulse-digit-detection** command. By default, pulse digit detection is enabled.

Note Users should configure the **no pulse-digit-detection** command only if their equipment generates pulse digits in error when initiating an outbound call.

Examples

The following example shows how to disable pulse digit detection on voice port 2/0/0:

```
Device> enable
Device# configure terminal
Device(config)# voice-port 2/0/0
Device(config-voiceport)# no pulse-digit-detection
Device(config-voiceport)# end
```

Related Commands

Command	Description
timing pulse	Specifies the pulse dialing rate for a specified voice port.

Q

q850-cause

To map a Q.850 call-disconnect cause code to a different Q.850 call-disconnect cause code, use the **q850-cause** command in application-map configuration mode. To disable the code-to-code mapping, use the **no** form of this command.

q850-cause *code-id* **q850-cause** *code-id*
no q850-cause *code-id* **q850-cause** *code-id*

Syntax Description

code-id	Q.850 call-disconnect cause code to be mapped. Range: 1 to 127.

Command Default

No mapping occurs.

Command Modes

Application-map

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use this command to map a Q.850 call-disconnect cause code to any different Q.850 call-disconnect cause code.

Use this command in conjunction with the **application** and **map** commands.

This command operates only on incoming H.323 call legs that are disconnected by a call-control application.

Examples

The following example maps cause code 34 to cause code 17:

```
Router(config)# application
Router(config-app)# map
Router(config-app-map)# q850-cause 34 q850-cause 17
```

Related Commands

Command	Description
application	Enables a specific application on a dial peer.
map	Enables mapping.
map q850-cause	Maps a Q.850 call-disconnect cause code to a tone.
progress_ind	Sets a specific progress indicator in Call Setup, Progress, or Connect messages from an H.323 VoIP gateway.

qsig decode

To enable decoding for QSIG supplementary services, use the **qsig decode**command in voice service configuration mode. To reset to the default, use the **no** form of this command.

qsig decode
no qsig decode

Syntax Description

This command has no keywords or arguments.

Command Default

QSIG decoding is disabled.

Command Modes

Voice service configuration

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

This command decodes application protocol data units (APDUs) for supplementary services. If this command is not enabled, data units are not interpreted and are tunneled through the router.

Examples

The following example enables QSIG decoding:

```
Router(config)# voice service voip
Router(conf-voi-serv)# qsig decode
```

Related Commands

Command	Description
supplementary-service h450.7	Globally enables H.450.7 supplementary services capabilities exchange.

query-interval

To configure the interval at which the local border element (BE) queries the neighboring BE, use the **query-interval** command in Annex G Neighbor BE Configuration mode. To remove the interval, use the **no** form of this command.

query-interval *query-interval*
no query-interval

Syntax Description

query -interval	Frequency, in minutes, at which this BE should query the specified neighbor BE for descriptors. Default is 30. A value of 0 disables periodic querying.

Command Default

30 minutes

Command Modes

Annex G Neighbor BE configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Use this command to configure the interval at which the local BE queries the neighboring BE. Use this command only if you want a query interval other than 30 minutes.

Examples

The following example sets the query interval to 45 minutes:

```
Router(config-annexg-neigh)# query-interval 45
```

Related Commands

Command	Description
emulate	Configures the local BE to cache the descriptors received from its neighbors. If caching is enabled, the neighbors are queried at the specified interval for their descriptors.
local	Configures the identifier for the neighbor BE.
session transport	Configures the neighbor’s port number that is used for exchanging Annex G messages.

R

radius-server attribute 6

To provide for the presence of the Service-Type attribute (attribute 6) in RADIUS Access-Accept messages, use the **radius-server attribute 6**command in global configuration mode. To make the presence of the Service-Type attribute optional in Access-Accept messages, use the **no** form of this command.

radius-server attribute 6 {**mandatory** | **on-for-login-auth** | **support-multiple** | **voice** *value*}
no radius-server attribute 6 {**mandatory** | **on-for-login-auth** | **support-multiple** | **voice** *value*}

Syntax Description

mandatory	Makes the presence of the Service-Type attribute mandatory in RADIUS Access-Accept messages.
on-for-login-auth	Sends the Service-Type attribute in the authentication packets. **Note** The Service-Type attribute is sent by default in RADIUS Accept-Request messages. Therefore, RADIUS tunnel profiles should include "Service-Type=Outbound" as a check item, not just as a reply item. Failure to include Service-Type=Outbound as a check item can result in a security hole.
support-multiple	Supports multiple Service-Type values for each RADIUS profile.
voice *value*	Selects the Service-Type value for voice calls. The only value that can be entered is 1. The default is 12.

Command Default

If this command is not configured, the absence of the Service-Type attribute is ignored, and the authentication or authorization does not fail. The default for the **voice** keyword is 12.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(13)T	The **mandatory** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If this command is configured and the Service-Type attribute is absent in the Access-Accept message packets, the authentication or authorization fails.

The **support-multiple** keyword allows for multiple instances of the Service-Type attribute to be present in an Access-Accept packet. The default behavior is to disallow multiple instances, which results in an Access-Accept packet containing multiple instances being treated as though an Access-Reject was received.

Examples

The following example shows that the presence of the Service-Type attribute is mandatory in RADIUS Access-Accept messages:

```
Router(config)# radius-server attribute 6 mandatory
```

The following example shows that attribute 6 is to be sent in authentication packets:

```
Router(config)# radius-server attribute 6 on-for-login-auth
```

The following example shows that multiple Service-Type values are to be supported for each RADIUS profile:

```
Router(config)# radius-server attribute 6 support-multiple
```

The following example shows that Service-Type values are to be sent in voice calls:

```
Router(config)# radius-server attribute 6 voice 1
```

rai target

To configure the Session Initiation Protocol (SIP) Resource Allocation Indication (RAI) mechanism, use the **rai target** command in SIP UA configuration mode. To disable SIP RAI configuration, use the **no** form of this command.

rai target *target-address* **resource-group** *group-index* [**transport** [{**tcp** [**tls** [**scheme** {**sip** | **sips**}]] | **udp**}]]
no rai target *target-address*

Syntax Description

target-address	IPv4, IPv6, or Domain Name Server (DNS) target address to which the status of the gateway resources are reported. The format of the target address can be one of the following: • **ipv4:** *ipv4-address* • **ipv6:** *ipv6-address* • **dns:** *domain-name*
resource-group	Maps the target address with the resource group index.
group-index	Resource group index. The range is from 1 to 5.
transport	(Optional) Specifies the mechanism to transport the RAI information.
tcp	(Optional) Transports the RAI information through Transmission Control Protocol (TCP).
tls	(Optional) Transports the RAI information through Transport Layer Security (TLS).
scheme	(Optional) Specifies the URL scheme for outgoing messages.
sip	(Optional) Selects SIP URL in outgoing OPTIONS message.
sips	(Optional) Selects Secure SIP (SIPS) URL in outgoing OPTIONS message.
udp	(Optional) Transports the RAI information through Unified Datagram Protocol (UDP).

Command Default

The SIP RAI mechanism is disabled.

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use the **rai target** command to provide the details of SIP along with the index of the resource group that needs to be monitored for reporting over SIP trunk. A maximum of five RAI configurations can be applied for other destination targets or monitoring entities. However, only one RAI configuration is possible for one target address.

Examples

The following example shows how to enable reporting of SIP RAI information over TCP to a target address of example.com:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# rai target dns:example.com resource-group 1
```

Related Commands

Command	Description
debug rai	Enables debugging for Resource Allocation Indication (RAI).
periodic-report interval	Configures periodic reporting parameters for gateway resource entities.
resource (voice)	Configures parameters for monitoring resources, use the resource command in voice-class configuration mode.
show voice class resource-group	Displays the resource group configuration information for a specific resource group or all resource groups.
voice class resource-group	Enters voice-class configuration mode and assigns an identification tag number for a resource group.

random-contact

To populate an outgoing INVITE message with random-contact information (instead of clear-contact information), use the **random-contact** command in voice service VoIP SIP configuration mode or voice class tenant configuration mode. To disable random-contact information, use the **no** form of this command.

random-contact system
no random-contact

Syntax Description

system	Specifies that the random-contact information use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

Outgoing INVITE messages are populated with clear-contact information.

Command Modes

Voice service VoIP SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

To populate outbound INVITE messages from the Cisco Unified Border Element with random-contact information instead of clear-contact information, use the **random-contact** command. This functionality will work only when the Cisco Unified Border Element is configured for Session Initiation Protocol (SIP) registration with random contact using the **credentials** and **registrar** commands.

Examples

The following example shows how to populate outbound INVITE messages with random-contact information:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# random-contact
```

The following example shows how to populate outbound INVITE messages with random-contact information:

```
Router(config-class)# random-contact system
```

Related Commands

Command	Description
credentials (sip ua)	Sends a SIP registration message from a Cisco Unified Border Element in the UP state.
registrar	Enables SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar.
voice-class sip random-contact	Populates the outgoing INVITE message with random-contact information at the dial-peer level.

random-request-uri validate

To enable the validation of the called number based on the random value generated during the registration of the number, use the **random-request-uri validate** command in voice service VoIP SIP configuration mode or voice class tenant configuration mode. To disable validation, use the **no** form of this command.

random-request-uri validate system
no random-request-uri validate

Syntax Description

system	Specifies that the validated called number use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

Validation is disabled.

Command Modes

Voice service voip sip configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.

Usage Guidelines

The system generates a random string when registering a new number. An INVITE message with the P-Called-Party-ID value can have the Request-URI set to this random number. To enable the system to identify the called-number from the random number in the Request-URI, use the **random-request-uri validate** command.

If the P-Called-Party-ID is not set in the INVITE message, the Request URI for that message must contain the called party information (and cannot contain a random number). Therefore validation is performed only on INVITE messages with a P-Called-Party-ID.

Examples

The following example shows how to enable called-number validation at the global configuration level:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# random-request-uri validate
```

The following example shows how to enable called-number validation in the voice class tenant configuration mode:

```
Router(config-class)# random-request-uri validate system
```

Related Commands

Command	Description
credentials (sip ua)	Sends a SIP registration message from a Cisco Unified Border Element in the UP state.
register	Enables SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar.
voice-class sip random-request-uri validate	Validates the called number based on the random value generated during the registration of the number at the dial-peer configuration level.

ras retry

To configure the H.323 Registration, Admission, and Status (RAS) message retry counters, use the ras retry command in voice service h323 configuration mode. To set the counters to the default values, use the **no** form of this command.

ras retry {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**} *value*
no ras retry {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**}

Syntax Description

all	Configures all RAS message counters that do not have explicit values configured individually. If **no ras retry all** is entered, all values are set to the default except for the individual values that were configured separately.
arq	Configures the admission request (ARQ) message counter.
brq	Configures the bandwidth request (BRQ) message counter.
drq	Configures the disengage request (DRQ) message counter.
grq	Configures the gatekeeper request (GRQ) message counter.
rai	Configures the resource availability indication (RAI) message counter.
rrq	Configures the registration request (RRQ) message counter.
value	Number of times for the gateway to resend messages to the gatekeeper after the timeout period. The timeout period is the period in which a message has not been received by the gateway from the gatekeeper and is configured using the **ras timeout** command. Valid values are 1 through 30.

Command Default

arq: 2 retries brq: 2 retries drq: 9 retries grq: 2 retries rai: 9 retries rrq: 2 retries

Command Modes

Voice service h323 configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command in conjunction with the **ras timeout** command. The **ras timeout** command configures the number of seconds for the gateway to wait before resending a RAS message to a gatekeeper. The **ras retry** command configures the number of times to resend the RAS message after the timeout period expires. The default values for timeouts and retries are acceptable in most networks. You can use these commands if you are experiencing problems in RAS message transmission between gateways and gatekeepers. For example, if you have gatekeepers that are slow to respond to a type of RAS request, increasing the timeout value and the number of retries increases the call success rate, preventing lost billing information and unnecessary switchover to an alternate gatekeeper.

Examples

The following example shows the GRQ message counter set to 5 and all other RAS message counters set to 10:

```
Router(conf-serv-h323)# ras retry all 10
Router(conf-serv-h323)# ras retry grq 5
```

Related Commands

Command	Description
ras timeout	Configures the H.323 RAS message timeout values.

ras retry lrq

To configure the gatekeeper Registration, Admission, and Status (RAS) message retry counters, use the ras retry lrq command in gatekeeper configuration mode. To set the counters to the default values, use the **no** form of this command.

ras retry lrq *value*
no ras retry lrq

Syntax Description

lrq	Configures the location request (LRQ) message counter.
value	Number of times for the zone gatekeeper (ZGK) to resend messages to the directory gatekeeper (DGK) after the timeout period. The timeout period is the period in which a message has not been received by the ZKG from the DGK and is configured using the **ras timeout lrq** command. Valid values are 1 through 30.

Command Default

The retry counter is set to1.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Use this command in conjunction with the **ras timeout lrq** command. The **ras timeout lrq** command configures the number of seconds for the gateway to wait before resending a RAS message to a gatekeeper. The **ras retry lrq**command configures the number of times to resend the RAS message after the timeout period expires. The default values for timeouts and retries are acceptable in most networks. You can use these commands if you are experiencing problems in RAS message transmission between gateways and gatekeepers. For example, if you have gatekeepers that are slow to respond to a type of RAS request, increasing the timeout value and the number of retries increases the call success rate, preventing lost billing information and unnecessary switchover to an alternate gatekeeper.

Examples

The following example shows the LRQ message counter set to 5:

```
Router(conf-gk)# ras retry lrq 5
```

Related Commands

Command	Description
ras timeout lrq	Configures the gatekeeper RAS message timeout values.

ras rrq dynamic prefixes

To enable advertisement of dynamic prefixes in additive registration request (RRQ) RAS messages on the gateway, use the **ras rrq dynamic prefixes** command in voice service h323 configuration mode. To disable advertisement of dynamic prefixes in additive RRQ messages, use the **no** form of this command.

ras rrq dynamic prefixes
no ras rrq dynamic prefixes

Syntax Description

This command has no arguments or keywords.

Command Default

In Cisco IOS Release 12.2(15)T, the default was set to enabled. In Cisco IOS Release 12.3(3), the default is set to disabled.

Command Modes

Voice service h323 configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(3)	The default is modified to be disabled by default.
12.3(4)T	The default change implemented in Cisco IOS Release 12.3(3) was integrated in Cisco IOS Release 12.3(4)T.

Usage Guidelines

In Cisco IOS Release 12.2(15)T, the default for the **ras rrq dynamic prefixes** command was set to enabled so that the gateway automatically sent dynamic prefixes in additive RRQ messages to the gatekeeper. Beginning in Cisco IOS Release 12.3(3), the default is set to disabled, and you must specify the command to enable the functionality.

Examples

The following example allows the gateway to send advertisements of dynamic prefixes in additive RRQ **messages**to the gatekeeper:

```
Router(conf-serv-h323)# ras rrq dynamic prefixes
```

Related Commands

Command	Description
rrq dynamic -prefixes-accept	Enables processing of additive RRQ messages and dynamic prefixes on the gatekeeper.

ras rrq ttl

To configure the H.323 Registration, Admission, and Status (RAS) registration request (RRQ) time-to-live value, use the ras rrq ttl command in voice service h323 configuration mode. To set the RAS RRQ time-to-live value to the default value, use the **no** form of this command.

ras rrq ttl time-to-live *seconds* [**margin** *seconds*]
no ras rrq ttl

Syntax Description

time-to-live *seconds*	Number of seconds that the gatekeeper should consider the gateway active. Valid values are 15 through 4000. The time-to-live seconds value must be greater than the margin seconds value.
margin *seconds*	(Optional) The number of seconds that an RRQ message can be transmitted from the gateway before the time-to-live seconds value advertised to the gatekeeper. Valid values are 1 through 60. The margin time value times two must be less than or equal to the time-to-live seconds value.

Command Default

time-to-live seconds : 60 seconds margin seconds: 15 seconds

Command Modes

Voice service h323 configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.3(6)	The maximum time-to-live value was changed from 300 to 4000 seconds.
12.3(4)T2	The maximum time-to-live value was changed from 300 to 4000 seconds.
12.3(7)T	The maximum time-to-live value was changed from 300 to 4000 seconds.

Usage Guidelines

Use this command to configure the number of seconds that the gateway should be considered active by the gatekeeper. The gateway transmits this value in the RRQ message to the gatekeeper. The margin time keyword and argument allow the gateway to transmit an early RRQ to the gatekeeper before the time-to-live value advertised to the gatekeeper.

Examples

The following example shows the *time-to-live seconds* value configured to 300 seconds and the **margin** *seconds* value configured to 60 seconds:

```
Router(conf-serv-h323)# ras rrq ttl 300 margin 60
```

ras timeout

To configure the H.323 Registration, Admission, and Status (RAS) message timeout values, use the ras timeout command in voice service h323 configuration mode. To set the timers to the default values, use the **no** form of this command.

ras timeout {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**} *seconds*
no ras timeout {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**}

Syntax Description

all	Configures message timeout values for all RAS messages that do not have explicit values configured individually. If no ras timeout all is entered, all values are set to the default except for the individual values that were configured separately.
arq	Configures the admission request (ARQ) message timer.
brq	Configures the bandwidth request (BRQ) message timer.
drq	Configures the disengage request (DRQ) message timer.
grq	Configures the gatekeeper request (GRQ) message timer.
rai	Configures the resource availability indication (RAI) message timer.
rrq	Configures the registration request (RRQ) message timer.
seconds	Number of seconds for the gateway to wait for a message from the gatekeeper before timing out. Valid values are 1 through 45.

Command Default

arq : 3 seconds**brq**: 3 seconds**drq**: 3 seconds**grq**: 5 seconds**rai**: 3 seconds**rrq**: 5 seconds

Command Modes

Voice service h323 configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command in conjunction with the **ras retry** command. The **ras timeout** command configures the number of seconds for the gateway to wait before resending a RAS message to a gatekeeper. The **ras retry** command configures the number of times to resend the RAS message after the timeout period expires. The default values for timeouts and retries are acceptable in most networks. You can use these commands if you are experiencing problems in RAS message transmission between gateways and gatekeepers. For example, if you have gatekeepers that are slow to respond to a type of RAS request, increasing the timeout value and the number of retries increases the call success rate, preventing lost billing information and unnecessary switchover to an alternate gatekeeper.

Examples

The following example shows the GRQ message timeout value set to 10 seconds and all other RAS message timeout values set to 7 seconds:

```
Router(conf-serv-h323)# ras timeout grq 10
Router(conf-serv-h323)# ras timeout all 7
```

Related Commands

Command	Description
ras retry	Configures the H.323 RAS message retry counters.

ras timeout decisec

To configure the H.323 Registration, Admission, and Status (RAS) message timeout values in deciseconds, use the **ras timeout decisec** command in voice service h323 configuration mode. To set the timers to the default values, use the **no** form of this command.

ras timeout {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**} **decisec** *decisecond*
no ras timeout {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**} **decisec**

Syntax Description

all	Configures message timeout values for all RAS messages that do not have explicit values configured individually. If no ras timeout all is entered, all values are set to the default except for the individual values that were configured separately.
arq	Configures the admission request (ARQ) message timer. Default: 3.
brq	Configures the bandwidth request (BRQ) message timer. Default: 3.
drq	Configures the disengage request (DRQ) message timer.Default: 3.
grq	Configures the gatekeeper request (GRQ) message timer. Default: 5.
rai	Configures the resource availability indication (RAI) message timer. Default: 3.
rrq	Configures the registration request (RRQ) message timer. Default: 5.
decisecond	Number of deciseconds for the gateway to wait for a message from the gatekeeper before timing out. Valid values are 1 through 45.

Command Default

Timers are set to their default values.

Command Modes

Voice service h323 configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Use this command in conjunction with the **ras retry** command. The **ras timeout decisec** command configures the number of deciseconds for the gateway to wait before resending a RAS message to a gatekeeper. The **ras retr**y command configures the number of times to resend the RAS message after the timeout period expires. The default values for timeouts and retries are acceptable in most networks. You can use these commands if you are experiencing problems in RAS message transmission between gateways and gatekeepers. For example, if you have gatekeepers that are slow to respond to a type of RAS request, increasing the timeout value and the number of retries increases the call success rate, preventing lost billing information and unnecessary switchover to an alternate gatekeeper.

Examples

The following example shows the ARQ message timeout value set to 25 deciseconds and all other RAS message timeout values set to 30 deciseconds:

```
Router(conf-serv-h323)# ras timeout arq decisec 25
Router(conf-serv-h323)# ras timeout all decisec 30
```

Related Commands

Command	Description
ras retry	Configures the H.323 RAS message retry counters.
ras timeout	Configures the H.323 RAS message timeout values in seconds.

ras timeout lrq

To configure the Gatekeeper Registration, Admission, and Status (RAS) message timeout values, use the ras timeout lrq command in gatekeeper configuration mode. To set the timers to the default values, use the **no** form of this command.

ras timeout lrq *seconds*
no ras timeout lrq

Syntax Description

lrq	Configures the location request (LRQ) message timer.
seconds	Number of seconds for the zone gatekeeper (ZGK) to wait for a message from the directory gatekeeper (DGK) before timing out. Valid values are 1 through 45. The default is 2.

Command Default

Timers are set to their default value

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Use this command in conjunction with the **ras retry lrq** command. The **ras timeout lrq** command configures the number of seconds for the zone gatekeeper (ZGK) to wait before resending a RAS message to a directory gatekeeper (DGK). The **ras retry lrq** command configures the number of times to resend the RAS message after the timeout period expires. The default values for timeouts and retries are acceptable in most networks. You can use these commands if you are experiencing problems in RAS message transmission between gatekeepers. For example, if you have gatekeepers that are slow to respond to a LRQ RAS request, increasing the timeout value and the number of retries increases the call success rate, preventing lost billing information and unnecessary switchover to an alternate gatekeeper.

Examples

The following example shows the LRQ message timeout value set to 4 seconds:

```
Router(conf-gk)# ras timeout lrq 4
```

Related Commands

Command	Description
ras retry lrq	Configures the gatekeeper RAS message retry counters.

rbs-zero

To enable 1AESS switch support for T1 lines on the primary serial interface of an access server, use the **rbs-zero**command in serial interface configuration mode. To disable IAESS switch support, use the **no** form of this command.

rbs-zero [**nfas-int** *nfas-int-range*]
no rbs-zero [**nfas-int** *nfas-int-range*]

Syntax Description

nfas-int *nfas-int-range*	(Optional) Non-Facility Associated Signaling (NFAS) interface number. Range is from 0 to 32.

Command Default

1AESS switch support is disabled.

Command Modes

Serial interface configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command supports the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.

Usage Guidelines

Use this command to configure the primary serial interface of an access server connected to T1 lines to support 1AESS switches for dial-in and dial-out calls. Modem calls of 56K or a lower rate are accepted; 64K calls are rejected.

In IAESS mode, the following occurs:

- Modem calls are accepted and digital calls are rejected.
- The ABCD bit of the 8 bits in the incoming calls is ignored. The ABCD bit of the 8 bits in the outgoing modem calls is set to 0.

In non-1AESS mode, modem and digital calls are accepted.

Examples

The following example enables 1AESS switching support on T1 channel 0:

```
Router(config)# controller t1 1/0
Router(config-controller)# framing esf
Router(config-controller)# linecode b8zs
Router(config-controller)# pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 1
Router(config)# interface serial 1/0:23
Router(config-if)# no ip address
Router(config-if)# isdn switch-type primary-ni
Router(config-if)# rbs-zero nfas-int 0
```

Related Commands

Command	Description
interface serial	Enters serial interface configuration mode.
isdn switch -type	Sets the switch type.
pri -group timeslots	Configures the PRI trunk for a designated operation.
show controllers t1	Displays information about the T1 links and the hardware and software driver information for the T1 controller.
show isdn nfas group	Displays all the members of a specified NFAS group or all NFAS groups.

reason-header override

To enable cause code passing from one SIP leg to another, use the **reason-header override** command in SIP UA configuration mode or voice class tenant configuration mode. To disable reason-header override, use the **no** form of this command.

reason-header override system
no reason-header override system

Syntax Description

system	Specifies that the override header use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

No default behavior or values.

Command Modes

SIP UA configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(9)T	Usage guidelines were updated to include configuration requirements for SIP-to-SIP configurations.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG entry.

Usage Guidelines

In an SIP-to-SIP configuration the **reason-header override**command must be configured to ensure cause code passing from the incoming SIP leg to the outgoing SIP leg.

Examples

The following example, shows the SIP user agent with reason-header override being configured.

```
Router(config)# sip-ua
Router(config-sip-ua)# reason-header override
```

The following example, shows the SIP user agent with reason-header override being configured in the voice class tenant configuration mode:

```
Router(config-class)# reason-header override system
```

Related Commands

Command	Description
sip-ua	Enables SIP UA configuration commands.

record-entry

To specify the trustpoints to be used for the creation of the Cisco Certificate Trust List (CTL) file, use the **record-entry** command in CTL file configuration mode. To remove a record entry from a CTL, use the **no** form of the command.

record-entry {**capf** | **cucm-tftp** | **selfsigned**} **trustpoint** *trustpoint-name*
no record-entry {**capf** | **cucm-tftp** | **selfsigned**} **trustpoint** *trustpoint-name*

Syntax Description

capf	Specifies that the trustpoint is created using the CAPF certificate imported from Cisco Unified Communications Manager to the device.
cucm-tftp	Specifies the role of this trustpoint to be Cisco Unified Call Manager and TFTP.
selfsigned	Specifies that the trustpoint is self-signed by the router.
trustpoint*trustpoint-name*	Specifies the name of the trustpoint.

Command Default

No trustpoints are specified for the CTL file.

Command Modes

CTL file configuration mode (config-ctl-file)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Example

The following example shows how to specify that the trustpoint is created using the CAPF certificate imported from CUCM. The trustpoint is called “trustpoint_1”:

```
Device(config)# voice-ctl-file myctl
Device(config-ctl-file)# record-entry capf trustpoint trustpoint_1
```

recorder profile

To configure a media profile recorder, use the **recorder profile** command in media class configuration mode. To disable the configuration, use the **no** form of this command.

recorder profile *tag*
no recorder

Syntax Description

tag	Media profile recorder tag. The range is from 1 to 10000.

Command Default

A media profile recorder is not configured.

Command Modes

Media class configuration (cfg-mediaclass)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use the **recorder profile** command to associate a recorder profile with a media class. The configured recorder profile specifies the recorder profile that is used by the media class. You can configure any number of recorder profiles.

Examples

The following example shows how to configure a media profile recorder:

```
Router# configure terminal
Router(config) media class 200
Router(cfg-mediaclass)# recorder profile 100
```

Related Commands

Command	Description
media class	Enters media class configuration mode.

redial

To define speed-dial code for a Feature Speed-dial (FSD) to redial the last number dialed, use the **redial** command in STC application feature speed-dial configuration mode. To return the code to its default, use the **no** form of this command.

redial *keypad-character*
no redial

Syntax Description

keypad-character	Character string that can be dialed on a telephone keypad (0-9, *, #). Default: #. Before Cisco IOS Release 12.4(20)YA, this is a single character. In Cisco IOS Release 12.5(20)YA and later releases, the string can be any of the following: • A single character (0-9, *, #) • Two digits (00-99) • Two to four characters (0-9, *, #) and the leading or ending character must be an asterisk (*) or number sign (#)

Command Default

The default value is # (number sign).

Command Modes

STC application feature speed-dial configuration (config-stcapp-fsd)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(20)YA	The length of the *keypad-character* argument was changed to 1 to 4 characters.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command changes the value of the speed-dial code for Redial from the default (#) to the specified value.

In Cisco IOS Release 12.4(20)YA and later releases, if the length of the *keypad-character* argument is at least two characters and the leading or ending character of the string is an asterisk (*) or a number sign (#), phone users are not required to dial a prefix to access this speed dial. Typically, phone users dial a Feature Speed-dial (FSD) consisting of a prefix plus a speed-dial code, for example *#. If the feature code is 78#, the phone user dials only 78#, without the FSD prefix, to access the corresponding feature.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that is already being used for a feature access code (FAC) or another FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that precludes or is precluded by a feature code for a FAC or another FSD, you receive a message. If you configure this command with a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable access to that feature.

To display a list of all FACs and FSDs, use the **show stcapp feature codes** command.

Examples

The following example shows how to change the value of the speed-dial code for Redial from the default (#). In this configuration, a phone user must press ** on the keypad to redial the number that was most recently dialed on this line, regardless of what value is configured for the FSD prefix.

```
Router(config)# stcapp feature speed-dial
Router(config-stcapp-fsd)# redial **
Router(config-stcapp-fsd)# exit
```

Related Commands

Command	Description
digit	Designates the number of digits for feature speed-dial codes (FSDs).
prefix (stcapp-fsd)	Defines the prefix for feature speed-dials (FSDs).
show stcapp feature codes	Displays all feature access codes (FACs) and feature access codes (FSDs) that are available for the STC application.
speed dial	Designates a range of speed-dial codes for the STC application.
stcapp feature speed-dial	Enables feature speed-dials (FSDs) in STC application and enters STC application feature speed-dial configuration mode for changing values of the prefix and speed-dial codes from the default.

redirect contact order

To set the order of contacts in the 300 Multiple Choice message, use the **redirect contact order** command in SIP configuration mode. To reset the order of contacts to the default, use the **no** form of this command.

redirect contact order [{**best-match** | **longest-match**}]
no redirect contact order

Syntax Description

best-match	(Optional) Uses the current system configuration.
longest-match	(Optional) Uses the destination pattern longest match first, and then the second longest match, the third longest match, and so on. This is the default.

Command Default

longest-match

Command Modes

SIP configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

This command applies when a 300 Multiple Choice message is sent by a SIP gateway indicating that a call has been redirected and that there are multiple routes to the destination.

Enter SIP configuration mode after entering voice service VoIP configuration mode as shown in the following example.

Examples

The following example uses the current system configuration to set the order of contact:

```
Router(config)# voice service voip
Router(config-voi-srv)# sip

Router(conf-serv-sip)# redirect contact order best-match
```

Related Commands

Command	Description
sip	Enters SIP configuration mode.

redirect ip2ip (dial peer)

To redirect SIP phone calls to SIP phone calls on a specific VoIP dial peer using the Cisco IOS Voice Gateway, use the **redirect ip2ip** command in dial peer configuration mode. To disable redirection, use the **no** form of this command.

redirect ip2ip
no redirect ip2ip

Syntax Description

This command has no arguments or keywords.

Command Default

Redirection is disabled.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The **redirect ip2ip**command must be configured on the inbound dial peer of the gateway. This command enables, on a per dial peer basis, IP-to-IP call redirection for the gateway.

To enable global IP-to-IP call redirection for all VoIP dial peers, use voice service configuration mode. To specify IP-to-IP call redirection for a specific VoIP dial peer, configure the dial peer in dial-peer configuration mode.

Note When IP-to-IP redirection is configured in dial-peer configuration mode, the configuration for the specific dial peer is activated only if the dial peer is an inbound dial peer. To enable IP-to-IP redirection globally, use **redirect ip2ip** (voice service)command.

Examples

The following example specifies that on VoIP dial peer 99, IP-to-IP redirection is set:

```
dial-peer voice 99 voip
 redirect ip2ip
```

Related Commands

Command	Description
redirect ip2ip (voice service)	Redirects SIP phone calls to SIP phone calls globally on a gateway using the Cisco IOS voice gateway.

redirect ip2ip (voice service)

To redirect SIP phone calls to SIP phone calls globally on a gateway using the Cisco IOS Voice Gateway, use the **redirect ip2ip**command in voice service configuration mode. To disable redirection, use the **no** form of this command.

redirect ip2ip
no redirect ip2ip

Syntax Description

This command has no arguments or keywords.

Command Default

Redirection is disabled.

Command Modes

Voice service configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to enable IP-to-IP call redirection globally on a gateway. Use the **redirect ip2ip**(dial-peer) command to configure IP-to-IP redirection on a specific inbound dial peer.

Examples

The following example specifies that all VoIP dial peers use IP-to-IP redirection:

```
voice service voip
 redirect ip2ip
```

Related Commands

Command	Description
redirect ip2ip (dial peer)	Redirects SIP phone calls to SIP phone calls on a specific VoIP dial peer using the Cisco IOS voice gateway.

redirection (SIP)

To enable the handling of 3*xx* redirect messages, use the **redirection** command in SIP UA configuration mode or voice class tenant configuration mode. To disable the handling of 3*xx* redirect messages, use the **no** form of this command.

redirection system
no redirection system

Syntax Description

system	Specifies that the SIP redirection messages use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

Redirection is enabled.

Command Modes

SIP UA configuration

Voice class tenant configuration (config-class).

Command History

Release	Modification
12.2(13)T	This command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

The **redirection** command applies to all Session Initiation Protocol (SIP) VoIP dial peers configured on the gateway.

The default mode of SIP gateways is to process incoming 3*xx* redirect messages according to RFC 2543. However if redirect handling is disabled with the **no redirection**command, the gateway treats the incoming 3*xx* responses as 4*xx* error class responses. To reset the default processing of 3*xx* messages, use the **redirection** command.

Examples

The following example disables processing of incoming 3*xx* redirection messages:

```
Router(config)# sip-ua
Router(config-sip-ua)# no redirection
```

The following example enables processing of incoming 3*xx* redirection messages in the voice class tenant configuration mode:

```
Router(config-class)# redirection system
```

Related Commands

Command	Description
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP UA status.

redundancy-reload

To reload control when the redundancy group (RG) fails, use the **redundancy-reload** command in global VoIP configuration mode. To enable the device to transition into PROTECTED mode (high availability), use the **no** form of this command.

redundancy-reload
no redundancy-reload

Syntax Description

This command has no arguments or keywords.

Command Default

The PROTECTED mode for voice high availability is not enabled.

Command Modes

Global VoIP configuration (conf-voi-serv)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

Use the **no redundancy-reload** command to enable the device to transition into PROTECTED mode. The default form of this command is **redundancy-reload**.

In the PROTECTED mode:

- Bulk synchronization request, call checkpointing, and incoming call processing are disabled.
- The device needs to be manually reloaded to exit from this state.

Examples

The following example enables the PROTECTED mode for the device:

```
Device(config)# voice service voip
Device(conf-voi-serv)#no redundancy-reload
```

redundancy group

To associate the interface with the redundancy group created, use the **redundancy group** command in interface mode. To dissociate the interface, use the **no** form of this command.

redundancy group *group-number* { **ipv4** | **ipv6** } *ip address* **exclusive**
no redundancy group *group-number* { **ipv4** | **ipv6** } *ip address* **exclusive**

Syntax Description

group-number	Specifies the redundancy group number.
ip address	Specifies IPv4 or IPv6 address.
exclusive	Associates the redundancy group to the interface.

Command Default

No default behavior or values

Command Modes

Interface configuration mode (config-if)

Command History

Release	Modification
Cisco IOS XE Dublin 17.12.1a	This command was introduced.

Usage Guidelines

You can configure a maximum of two redundancy groups. Hence, there can be only two Active and Standby pairs within the same network.

Examples

The following example configuration shows how to associate the IPv4 interface with the redundancy group:

```
Router(config-if)# redundancy group 1 ip 10.64.86.126 exclusive
```

The following example configuration shows how to associate the IPv6 interface with the redundancy group:

```
Router(config-if)# redundancy group 1 ipv6 2001:10:64:86::126/119 exclusive
```

Related Commands

Command	Description
ipv6 address *ip-address*	Physical IPv6 address configuration of the device.

refer-delay-disconnect

To delay the disconnect on transferor leg after successful transfer completion, use the **refer-delay-disconnect** command. If the call leg is not disconnected within the specified timeout, CUBE disconnects the call leg with BYE message.

refer-delay-disconnect *<1-5>*
no refer-delay-disconnect

<1-5>	Specifies that CUBE delays the disconnect message (sending BYE) on the transferor leg for the configured timeout.

Command Default

Refer-delay-disconnect is disabled.

Command Modes

Voice service voip SIP configuration (conf-serv-sip)
Voice class tenant configuration (config-class)
Dial peer configuration

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command is introduced.

Usage Guidelines

When this command is configured, CUBE delays the disconnect message on transferor leg for the configured time. Default value is not enabled. Hence without this config, CUBE disconnects the call immediately after REFER transaction completion.

Examples

The following example shows how to enable refer-delay-disconnect on the CUBE in voice service configuration mode:

```
Router(config)# voice service voip
 Router(conf-voi-serv)#sip
Router(conf-serv-sip)#refer-delay-disconnect 3
```

Examples

The following example shows how to enable refer-delay-disconnect on the CUBE in the voice class tenant configuration mode:

```
Router(config)# voice class tenant 10
 Router(config-class)#refer-delay-disconnect 3
```

Examples

The following example shows how to enable refer-delay-disconnect on the CUBE in dial-peer configuration mode:

```
Router(config)#dial-peer voice 22 voip
Router(config-dial-peer)#voice-class sip refer-delay-disconnect 3
```

Related Commands

Command	Description
refer-delay-disconnect (dial peer)	Delays the disconnect message on a transferor leg with a BYE message on a specific VoIP dial peer using CUBE .

refer-ood enable

To enable out-of-dialog refer (OOD-R) processing, use the **refer-ood enable** command in SIP user-agent configuration mode or voice class tenant configuration mode. To disable OOD-R, use the **no** form of this command.

refer-ood enable [*request-limit*] **[system]**
no refer-ood enable

Syntax Description

request-limit	(Optional) Maximum number of concurrent incoming OOD-R requests that the router can process. Range: 1 to 500. Default: 500.
system	Specifies that the out-of-dialog refer (OOD-R) processing use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

OOD-R processing is disabled.

Command Modes

SIP UA configuration (config-sip-ua)

Voice class tenant configuration (config-class)

Command History

Release	Cisco product	Modification
12.4(11)XJ	Cisco Unified CME 4.1	This command was introduced.
12.4(15)T	Cisco Unified CME 4.1	This command was integrated into Cisco IOS Release 12.4(15)T.
15.6(2)T and IOS XE Denali 16.3.1	CUBE	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.

Usage Guidelines

Out of dialog Refer allows applications to establish calls using the SIP gateway or Cisco Unified CME. The application sets up the call and the user does not dial out from their own phone.

Examples

The following example shows how to enable OOD-R:

```
Router(config)# sip-ua
Router(config-sip-ua)# refer-ood enable
```

The following example shows how to enable OOD-R in the voice class tenant configuration mode:

```
Router(config-class)# refer-ood enable system
```

Related Commands

Command	Description
authenticate (voice register global)	Defines the authenticate mode for SIP phones in a Cisco Unified CME or Cisco Unified SRST system.
credential load	Reloads a credential file into flash memory.
debug voip application	Displays all application debug messages.

referto-passing

To disable dial peer lookup and modification of the Refer-To header when the Cisco Unified Border Element (UBE) passes across a REFER message during a call transfer, use the **referto-passing** command in voice service voip SIP configuration mode or voice class tenant configuration mode. To enable dial peer lookup and the Refer-To header modification, use the **no** form of this command.

referto-passing system
no referto-passing system

Syntax Description

system	Specifies that the enable dial peer lookup and the Refer-To header modification use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

Dial peer lookup is performed. The Refer-To header is modified to include the address of the CUBE if address hiding is enabled or to include the address of the call target if a dial peer match is found.

Command Modes

Voice service voip SIP configuration (conf-serv-sip).

Voice class tenant configuration (config-class).

Command History

Release	Modification
15.2(1)T	This command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

By default, while passing across the REFER message, the CUBE replaces the host portion of the Refer-To header with the address of the CUBE if the **address-hiding** command is enabled or with the address of the call target if a dial peer match is found. You can use the **referto-passing** command to disable the CUBE from overwriting the Refer-To header even if address hiding is enabled. This command also disables dial peer lookup when the CUBE passes across the REFER message.

Examples

The following example shows how to enable REFER message pass-through on the CUBE and disable the modification of the Refer-To header:

```
Router(config)# voice service voip
Router(conf-voi-serv)# supplementary-service sip refer
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# referto-passing
```

The following example shows how to enable REFER message pass-through on the CUBE in the voice class tenant configuration mode:

```
Router(config-class)# referto-passing system
```

Related Commands

Command	Description
address-hiding	Hides signaling and media peer addresses from endpoints other than the gateway.
sip	Enters SIP configuration mode from voice service voip configuration mode.
supplementary-service sip refer	Enables REFER message pass-through on the CUBE.

register e164

To configure a gateway to register or deregister a fully-qualified dial-peer E.164 address with a gatekeeper, use the **register e164**command in dial peer configuration mode. To deregister the E.164 address, use the **no** form of this command.

register e164
no register e164

Syntax Description

This command has no arguments or keywords.

Command Default

No E.164 addresses are registered until you enter this command.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(5)XM2	The command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400, and the Cisco AS5850 in this release.

Usage Guidelines

Use this command to register the E.164 address of an analog telephone line attached to a foreign exchange station (FXS) port on a router. The gateway automatically registers fully qualified E.164 addresses. Use the **no register e164**command to deregister an address. Use the **register e164**command to register a deregistered address.

Before you automatically or manually register an E.164 address with a gatekeeper, you must create a dial peer (using the **dial-peer** command), assign an FXS port to the peer (using the **port** command), and assign an E.164 address using the **destination-pattern** command. The E.164 address must be a fully qualified address. For example, +5550112, 5550112, and 4085550112 are fully qualified addresses; 408555.... is not. E.164 addresses are registered only for active interfaces, which are those that are not shut down. If an FXS port or its interface is shut down, the corresponding E.164 address is deregistered.

Tip You can use the **show gateway** command to find out whether the gateway is connected to a gatekeeper and whether a fully qualified E.164 address is assigned to the gateway. Use the **zone-prefix** command to define prefix patterns on the gatekeeper, such as 408555...., that apply to one or more gateways.

Examples

The following command sequence places the gateway in dial peer configuration mode, assigns an E.164 address to the interface, and registers that address with the gatekeeper.

```
gateway1(config)# dial-peer voice 111 pots
gateway1(config-dial-peer)# port 1/0/0
gateway1(config-dial-peer)# destination-pattern 5550112
gateway1(config-dial-peer)# register e164
```

The following commands deregister an address with the gatekeeper.

```
gateway1(config)# dial-peer voice 111 pots
gateway1(config-dial-peer)# no register e164
```

The following example shows that you must have a connection to a gatekeeper and must define a unique E.164 address before you can register an address.

```
gateway1(config)# dial-peer voice 222 pots
gateway1(config-dial-peer)# port 1/0/0
gateway1(config-dial-peer)# destination 919555....
gateway1(config-dial-peer)# register e164
ERROR-register-e164:Dial-peer destination-pattern is not a full E.164 number
gateway1(config-dial-peer)# no gateway
gateway1(config-dial-peer)# dial-peer voice 111 pots
gateway1(config-dial-peer)# register e164
ERROR-register-e164:No gatekeeper
```

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.
dial -peer (voice)	Enters dial peer configuration mode and specifies the method of voice encapsulation.
port (dial peer)	Associates a dial peer with a specific voice port.
show gateway	Displays the current gateway status.
zone prefix	Adds a prefix to the gatekeeper zone list.

registered-caller ring

To configure the Nariwake service registered caller ring cadence, use the registered-caller ring command in dial peer configuration mode.

registered-caller ring *cadence*

Syntax Description

cadence	A value of 0, 1, or 2. The default ring cadence for registered callers is 1 and for unregistered callers is 0. The on and off periods of ring 0 (normal ringing signals) and ring 1 (ringing signals for the Nariwake service) are defined in the NTT user manual.

Command Default

The default Nariwake service registered caller ring cadence is ring 1.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.1.(2)XF	This command was introduced on the Cisco 800 series.

Usage Guidelines

If your ISDN line is provisioned for the I Number or dial-in services, you must also configure a dial peer by using the destination-pattern not-provided command. Either port 1 or port 2 can be configured under this dial peer. The router then forwards the incoming call to voice port 1. (See the "Examples" section below.

If more than one dial peer is configured with the destination-pattern not-provided command, the router uses the first configured dial peer for the incoming calls. To display the Nariwake ring cadence setting, use the show run command.

Examples

The following example sets the ring cadence for registered callers to 2.

```
pots country jp
dial-peer voice 1 pots
 registered-caller ring 2
```

Related Commands

Command	Description
destination-pattern not-provided	Specifies the port to receive the incoming calls that have no called-party number.

registrar

To enable Session Initiation Protocol (SIP) gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and Skinny Client Control Protocol (SCCP) phones with an external SIP proxy or SIP registrar, use the **registrar** command in SIP UA configuration mode. To disable registration of E.164 numbers, use the **no** form of this command.

registrar {**dhcp** | [*registrar-index*] *registrar-server-address* [**:** *port*]} [**auth-realm** **realm**] [**expires** *seconds*] [**random-contact**] [**refresh-ratio** *ratio-percentage*] [**scheme** {**sip** | **sips**}] [**tcp**] [*type*] [**secondary**]
server | {**expires** | **system**}
no **registrar** [{*registrar-index* | **secondary**}]

Syntax Description

dhcp	(Optional) Specifies that the domain name of the primary registrar server is retrieved from a DHCP server (cannot be used to configure secondary or multiple registrars).
registrar-index	(Optional) A specific registrar to be configured, allowing configuration of multiple registrars (maximum of six). Range is 1–6.
registrar-server-address	The SIP registrar server address to be used for endpoint registration. This value can be entered in one of three formats: • **dns:** *address* --the Domain Name System (DNS) address of the primary SIP registrar server (the **dns:** delimiter must be included as the first four characters). • **ipv4:** *address* --the IP address of the SIP registrar server (the **ipv4:** delimiter must be included as the first five characters). • **ipv6:[** *address*]--the IPv6 address of the SIP registrar server (the **ipv6:** delimiter must be included as the first five characters and the address itself must include opening and closing square brackets).
: *port*]	(Optional) The SIP port number (the colon delimiter is required).
auth-realm	(Optional) Specifies the realm for preloaded authorization.
realm	The realm name.
expires *seconds*	(Optional) Specifies the default registration time, in seconds. Range is 60–65535 . Default is 3600.
random-contact	(Optional) Specifies the Random String Contact header that is used to identify the registration session.
refresh-ratio *ratio-percentage*	(Optional) Specifies the registration refresh ratio, in percentage. Range is 1–100 . Default is 80.
scheme {**sip** | **sips**}	(Optional) Specifies the URL scheme. The options are SIP (**sip**) or secure SIP (**sips**), depending on your software installation**.** The default is **sip**.

tcp	(Optional) Specifies TCP. If not specified, the default is UDP UDP.
type	(Optional) The registration type. **Note** The *type* argument cannot be used with the **dhcp** option.
secondary	(Optional) Specifies a secondary SIP registrar for redundancy if the primary registrar fails. This option is not valid if DHCP is specified. When there are two registrars, REGISTER message is sent to both the registrar servers, even if the primary registrar sends a 200 OK and the trunk is registered to the primary registrar. If you want to send the registration to the secondary registrar, only when the primary fails, then use DNS SRV. **Note** You cannot configure any other optional settings once you enter the **secondary** keyword--specify all other settings first.
expires	(Optional) Specifies the registration expiration time
system	(Optional) Specifies the usage of global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

Registration is disabled.

Command Modes

SIP UA configuration (config-sip-ua)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(6)T	This command was modified. The **tls** keyword and the **scheme** keyword with the *string* argument were added.
12.4(22)T	This command was modified. Support for IPv6 addresses was added.
12.4(22)YB	This command was modified. The **dhcp**, **random-contact and refresh-ratio** keywords were added. Also, the **aor-domain** keyword and the **tls** option for the tcp keyword were removed.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.0(1)XA	This command was modified. The *registrar-index* argument for support of multiple registrars on SIP trunks was added.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(2)T	This command was modified. The **auth-realm** keyword was added.

Release	Modification
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the **registrar dhcp** or **registrar** *registrar-server-address* command to enable the gateway to register E.164 phone numbers with primary and secondary external SIP registrars. In Cisco IOS Release 15.0(1)XA and later releases, endpoints on Cisco IOS SIP time-division multiplexing (TDM) gateways, Cisco Unified Border Elements (CUBEs), and Cisco Unified Communications Manager Express (Cisco Unified CME) can be registered to multiple registrars using the **registrar** *registrar-index* command.

By default, Cisco IOS SIP gateways do not generate SIP register messages.

Note When entering an IPv6 address, you must include square brackets around the address value.

Examples

The following example shows how to configure registration with a primary and secondary registrar:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# retry invite 3
Router(config-sip-ua)# retry register 3
Router(config-sip-ua)# timers register 150
Router(config-sip-ua)# registrar ipv4:209.165.201.1 expires 14400 secondary
```

The following example shows how to configure a device to register with the SIP server address received from the DHCP server. The **dhcp** keyword is available only for configuration by the primary registrar and cannot be used if configuring multiple registrars.

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar dhcp expires 14400
```

The following example shows how to configure a primary registrar using an IP address with TCP:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# retry invite 3
Router(config-sip-ua)# retry register 3
Router(config-sip-ua)# timers register 150
Router(config-sip-ua)# registrar ipv4:209.165.201.3 tcp
```

The following example shows how to configure a URL scheme with SIP security:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# retry invite 3
Router(config-sip-ua)# retry register 3
```

```
Router(config-sip-ua)# timers register 150
Router(config-sip-ua)# registrar ipv4:209.165.201.7 scheme sips
```

The following example shows how to configure a secondary registrar using an IPv6 address:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar ipv6:[3FFE:501:FFFF:5:20F:F7FF:FE0B:2972] expires 14400
secondary
```

The following example shows how to configure all POTS endpoints to two registrars using DNS addresses:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar 1 dns:example1.com expires 180
Router(config-sip-ua)# registrar 2 dns:example2.com expires 360
```

The following example shows how to configure the realm for preloaded authorization using the registrar server address:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar 2 192.168.140.3:8080 auth-realm example.com expires 180
```

The following example shows how to configure registrar in the voice class tenant configuration mode:

```
Router(config-class)# registrar server system
```

Related Commands

Command	Description
authentication (dial peer)	Enables SIP digest authentication on an individual dial peer.
authentication (SIP UA)	Enables SIP digest authentication.
credentials (SIP UA)	Configures a Cisco UBE to send a SIP registration message when in the UP state.
localhost	Configures global settings for substituting a DNS local host name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages.
retry register	Sets the total number of SIP register messages to send.
show sip-ua register status	Displays the status of E.164 numbers that a SIP gateway has registered with an external primary or secondary SIP registrar.
timers register	Sets how long the SIP UA waits before sending register requests.
voice-class sip localhost	Configures settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages on an individual dial peer, overriding the global setting.

registrar server

To enable the local Session Initiation Protocol (SIP) registrar, use the **registrar server** command in service SIP configuration mode. To disable the configuration, use the **no** form of this command.

registrar server [**expires** [**max** *value*] [**min** *value*]]
no registrar server

Syntax Description

expires	(Optional) Configures the registration expiry time.
max *value*	(Optional) Configures the maximum registration expiry time, in seconds. The range is from 120 to 86400. The default is 3600.
min *value*	(Optional) Configures the minimum registration expiry time, in seconds. The range is from 60 to 3600. The default is 60.

Command Default

The local SIP registrar is disabled.

Command Modes

Service SIP configuration (conf-serv-sip)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

You must enable the local SIP registrar by using the **registrar server** command before configuring the SIP registration on Cisco Unified Border Element (UBE).

Examples

The following example shows how to enable the local SIP registrar and set the maximum and minimum expiry values to 4000 and 100 seconds respectively:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# registrar server expires max 4000 min 100
```

Related Commands

Command	Description
registration passthrough	Configures SIP registration pass-through options at the global level.
voice-class sip registration passthrough	Configures SIP registration pass-through options on a dial peer.

registration retries

To set the number of times that Skinny Client Control Protocol (SCCP) tries to register with a Cisco Unified CallManager, use the **registration retries**command in SCCP Cisco CallManager configuration mode. To reset this number to the default value, use the **no** form of this command.

registration retries *retry-attempts*
no registration retries

Syntax Description

retry-attempts	Number of registration attempts. Range is 1 to 32. Default is 3.

Command Default

3 registration attempts

Command Modes

SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use this command to control the number of registration retries before SCCP confirms that it cannot register with the Cisco Unified CallManager. When SCCP confirms that it cannot register to the current Cisco Unified CallManager (if the number of registration requests sent without an Ack reaches the registration retries value), SCCP tries to register with the next Cisco Unified CallManager.

Note The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the registration retry attempts to meet your needs.

Examples

The following example sets the number of registration retries to 15:

```
Router(config-sccp-ccm)# registration retries 15
```

Related Commands

Command	Description
ccm group	Creates a Cisco Unified CallManger group and enters SCCP Cisco CallManager configuration mode.
registration timeout	Sets the length of time between registration messages sent from SCCP to the Cisco CallManager.

registration timeout

To set the length of time between registration messages sent from Skinny Client Control Protocol (SCCP) to the Cisco Unified CallManager, use the **registration timeout**command in SCCP Cisco CallManager configuration mode. To reset the length of time to the default value, use the **no** form of this command.

registration timeout *seconds*
no registration timeout

Syntax Description

seconds	Time, in seconds, between registration messages. Range is 1 to 180. Default is 3.

Command Default

3 seconds

Command Modes

SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Whenever SCCP sends the registration message to the Cisco Unified CallManager, it initiates this timer. Once the timeout occurs, it sends the next registration message unless the number of messages without an Ack reaches the number set by the **registration retries**command. Use this command to set the Cisco Unified CallManager registration timeout parameter value.

Note The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the registration timeout value to meet your needs.

Examples

The following example sets the length of time between registration messages sent from SCCP to the Cisco Unified CallManager to 12 seconds:

```
Router
(config-sccp-ccm)#
 registration timeout 12
```

Related Commands

Command	Description
ccm group	Creates a Cisco CallManger group and enters SCCP Cisco CallManager configuration mode.
registration retries	Sets the number of times that SCCP tries to register with the Cisco Unified CallManager.

registration passthrough

To configure the Session Initiation Protocol (SIP) registration pass-through options, use the **registration passthrough** command in service SIP configuration mode or voice class tenant configuration mode. To disable the configuration, use the **no** form of this command.

registration passthrough [**static**] [**rate-limit** [**expires** *value*] [**fail-count** *value*]] [**registrar-index** [*index*]]**[system]**
no registration passthrough

Syntax Description

static	(Optional) Configures Cisco Unified Border Element (UBE) to use static registrar details for SIP registration. Cisco UBE works in point-to-point mode when the **static** keyword is used.
rate-limit	(Optional) Configures SIP registration pass-through rate limit options.
expires *value*	(Optional) Sets the expiry value for rate limiting, in seconds. The range is from 60 to 65535. The default value is 3600.
fail-count *value*	(Optional) Sets the fail count value for rate limiting. The range is from 2 to 20. The default value is 0.
registrar-index	(Optional) Configures the registrar index that is to be used for registration pass-through.
index	(Optional) Registration index value. The range is from 1 to 6.
system	Specifies that the registration pass-through options use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

SIP registration pass-through options are not configured.

Command Modes

Service SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
15.1(3)T	This command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.

Usage Guidelines

You can use the **registration passthrough** command to configure the following SIP pass-through functionalities:

- Back-to-back registration facility to register phones for call routing.
- Options to configure the rate-limiting values, such as the expiry time, fail-count, and a list of registrars to be used for registration.

Examples

The following example shows how to set the registrar index as 2 for the SIP registration pass-through rate-limiting:

```
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# registration passthrough static rate-limit registrar-index 2
```

The following example shows how SIP registration pass-through is configured in the voice class tenant configuration mode:

```
Router(config-class)# registration passthrough system
```

Related Commands

Command	Description
voice-class sip registration passthrough static rate-limit	Sets the SIP registration pass-through rate limiting options on a dial peer.

rel1xx

To enable all Session Initiation Protocol (SIP) provisional responses (other than 100 Trying) to be sent reliably to the remote SIP endpoint, use the **rel1xx** command in SIP configuration mode or voice class tenant configuration mode. To reset to the default, use the **no** form of this command.

rel1xx {**supported** *value* | **require** *value* | **disable** | **system**}
no rel1xx

Syntax Description

supported *value*	Supports reliable provisional responses. The *value* argument may have any value, as long as both the user-agent client (UAC) and user-agent server (UAS) configure it the same. This keyword, with *value* of 100rel, is the default.
require *value*	Requires reliable provisional responses. The *value* argument may have any value, as long as both the UAC and UAS configure it the same.
disable	Disables the use of reliable provisional responses.
system	Use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

supported with the 100rel value

Command Modes

SIP configuration mode (conf-voi-serv)

Voice class tenant configuration (config-class)

Dial-peer configuration mode

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(11)T	This command was supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

The use of resource reservation with SIP requires that the reliable provisional feature for SIP be enabled either at the VoIP dial-peer level or globally on the router.

There are two ways to configure reliable provisional responses:

- Dial-peer configuration mode. You can configure reliable provisional responses for the specific dial peer only by using the **voice-class sip rel1xx**command.
- SIP configuration mode. You can configure reliable provisional responses globally by using the **rel1xx**command.

The **voice-class sip rel1xx** command in dial-peer configuration mode takes precedence over the **rel1xx**command in global configuration mode with one exception: If the **voice-class sip rel1xx** command is used with the **system**keyword, the gateway uses what was configured under the **rel1xx** command in global configuration mode.

Enter SIP configuration mode from voice-service VoIP configuration mode as shown in the following example.

Examples

The following example shows use of the **rel1xx** command with the value 100rel:

```
Router(config)# voice service voip
Router(config-voi-srv)# sip
Router(conf-serv-sip)# rel1xx supported 100rel
```

The following example shows use of the **rel1xx** command in the voice class tenant configuration mode:

```
Router(config-class)# rel1xx system
```

Related Commands

Command	Description
sip	Enters SIP configuration mode from voice-service VoIP configuration mode.
voice-class sip rel1xx	Provides provisional responses for calls on a dial peer basis.

remote-party-id

To enable translation of the SIP header Remote-Party-ID, use the **remote-party-id** command in SIP UA configuration mode or voice class tenant configuration mode. To disable Remote-Party-ID translation, use the no form of this command.

remote-party-id system
no remote-party-id

Syntax Description

system	Specifies that the SIP header Remote-Party-ID use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

Remote-Party-ID translation is enabled.

Command Modes

SIP UA configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.2(13)T	This command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

When the **remote-party-id** command is enabled, one of the following calling information treatments occurs:

- If a Remote-Party-ID header is present in the incoming INVITE message, the calling name and number that is extracted from the Remote-Party-ID header are sent as the calling name and number in the outgoing Setup message. This is the default behavior. Use the remote-party-id command to enable this option.
- When no Remote-Party-ID header is available, no translation occurs so the calling name and number are extracted from the From header and are sent as the calling name and number in the outgoing Setup message. This treatment also occurs when the feature is disabled.

Examples

The following example shows the Remote-Party-ID translation being enabled:

```
Router(config-sip-ua)#
remote-party-id
```

The following example shows the Remote-Party-ID translation being enabled in the voice class tenant configuration mode:

```
Router(config-class)# remote-party-id system
```

Related Commands

Command	Description
debug ccsip events	Enables tracing of SIP SPI events.
debug ccsip messages	Enables SIP SPI message tracing.
debug isdn q931	Displays call setup and teardown of ISDN connections.
debug voice ccapi in out	Enables tracing the execution path through the call control API.

remote-url

To configure the url the application that will be used by the service provider, use the **remote-url** command. The provider uses this url to authenticate and communicate with the application. To delete the configured url, use the **no** form of this command.

remote-url [{*url-number*}] *url*

Syntax Description

url-number	(optional) URL number. Range is from 1 to 8. **Note** You can configure only one URL for XSVC service provider in secure mode.
url	Specifies the URL that the service provider will be using in the messages. In secure mode, only HTTPS URL can be configured. **Note** In secure mode, only IPv4 address can be configured. IPv6 address and domain name cannot be configured.

Command Default

No default behavior or values.

Command Modes

uc wsapi mode

uc secure-wsapi mode

Command History

Release	Modification
15.2(2)T	This command was introduced.
Cisco IOS XE Everest 16.6.1	This command extended support for configuring Cisco Unified Communication IOS services environment using HTTPS connection.

Usage Guidelines

Use this command to configure the remote URL (application) that the service provider uses in messages.

Examples

The following example configures the remote url that the the xcc service provider will use in messages while in nonsecure mode.

```
Router(config)# uc wsapi
Router(config-uc-wsapi)# provider xcc
Router(config-uc-wsapi-xcc)# no shutdown
Router(config-uc-wsapi-xcc)# remote-url 1 http://192.0.2.0:24/my_route_control
```

The following example configures the remote url that the the xcc service provider will use in messages while in secure mode.

```
Router(config)# uc secure-wsapi
Router(config-uc-wsapi)# provider xcc
Router(config-uc-wsapi-xcc)# no shutdown
Router(config-uc-wsapi-xcc)# remote-url 1 https://192.0.2.0:24/my_route_control
```

Examples

Related Commands

Command	Description
provider	Enables a provider service.
source-address	Specifies the IP address of the provider.
uc wsapi	Enters nonsecure Cisco Unified Communication IOS services configuration mode.
uc secure-wsapi	Enters secure Cisco Unified Communication IOS services configuration mode.

ren

To configure Ring Equivalent Number of the ringer device connected to analog FXS voice port. Use the ren <1-5> command in voice-port configuration mode. To reset to default, use no form of this command or ren 1.

This command is only applicable to analog FXS voice port.

ren [{ *number* }]
no **ren**

Command History

Syntax Description

Syntax Description

number	REN value 1-5 for short loop analog FXS voice port. Default is 1 number REN value 1-2 for long loop analog FXS voice port. Default is 1.

Command Default

no ren or ren 1

Command Modes

Voice-port configuration

req-qos

To specify the desired quality of service to be used in reaching a specified dial peer, use the **req-qos** command in dial peer configuration mode. To restore the default value for this command, use the **no** form of this command.

req-qos {**best-effort** | **controlled-load** | **guaranteed-delay**} [{{**audio bandwidth** | **video bandwidth**} **default** | **max** *bandwidth-value*}]
no req-qos

Syntax Description

best-effort	Indicates that Resource Reservation Protocol (RSVP) makes no bandwidth reservation.
controlled-load	Indicates that RSVP guarantees a single level of preferential service, presumed to correlate to a delay boundary. The controlled load service uses admission (or capacity) control to assure that preferential service is received even when the bandwidth is overloaded.
guaranteed-delay	Indicates that RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded.
audio bandwidth	(Optional) Specifies amount of bandwidth to be requested for audio streams.
default	Sets the default bandwidth to be requested for audio or video streams. • Audio streams--Range is 1 to 64 kbps; default value is 64 kbps. • Video streams--Range is 1 to 5000 kbps; default value is no maximum
max *bandwidth-value*	Sets the maximum bandwidth to be requested for audio streams. Range is 1 to 64 kbps; default value is no maximum.
video bandwidth	(Optional) Specifies the amount of bandwidth to be requested for video streams.
default *bandwidth-value*	Sets the default bandwidth to be requested for video streams. Range is 1 to 5000 kbps; default value is 384 kbps.
max *bandwidth-value*	(Optional) Sets the maximum bandwidth to be requested for video streams. .

Command Default

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.
12.3(4)T	Keywords added to support audio and video streams.

Usage Guidelines

Use the **req-qos**command to request a specific quality of service to be used in reaching a dial peer. Like **acc-qos**, when you issue this command, the Cisco IOS software reserves a certain amount of bandwidth so that the selected quality of service can be provided. Cisco IOS software uses Resource Reservation Protocol (RSVP) to request quality of service guarantees from the network.

This command is applicable only to VoIP dial peers.

Examples

The following example configures **guaranteed-delay** as the requested quality of service to a dial peer:

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

The following example configures **guaranteed-delay**andrequests a default bandwidth level of 768 kbps for video streams:

```
dial-peer voice 20 voip
 req-qos guaranteed-delay video bandwidth default 768
```

Related Commands

Command	Description
acc-qos	Defines the acceptable QoS for any inbound and outbound call on a VoIP dial peer.

request

To use SIP profiles to add, copy, modify, or remove Session Initiation Protocol (SIP) or Session Description Protocol (SDP) header value in a SIP request message, use the **request**command in voice class configuration mode. To disable the configuration, use the **no** form of this command.

request *method* {**sdp-header** | **sip-header**} *header-name* {**add** | **copy** | **modify** | **remove**} *string*
no request *method* {**sdp-header** | **sip-header**} *header-name* {**add** | **copy** | **modify** | **remove**} *string*

Syntax Description

method	Type of message to be added, modified, or removed. It can be one of the following values: • **ack** --SIP acknowledgment message. • **any** --Any SIP message. • **bye** --SIP BYE message. • **cancel** --SIP CANCEL message. • **comet** --SIP COMET message. • **info** --SIP INFO message. • **invite** --The first SIP INVITE message. • **notify** --SIP NOTIFY message. • **options** --SIP OPTIONS message. • **prack** --SIP PRACK message. • **publish** --SIP PUBLISH message. • **refer** --SIP REFER message. • **register** --SIP REGISTER message. • **reinvite** --SIP REINVITE message. • **subscribe** --SIP SUBSCRIBE message. • **update** --SIP UPDATE message.
sdp-header	Specifies an SDP header.
sip-header	Specifies a SIP header.
header-name	SDP or SIP header name.
add	Adds a header.
copy	Copies a header.
modify	Modifies a header.

remove	Removes a header.
string	String to be added, copied, modified, or removed as a header. **Note** If you use the **copy** keyword, you must provide a matching pattern followed by the variable name for the *string* argument.

Command Default

SIP profiles are not modified to add, copy, modify, or remove SIP or SDP header values.

Command Modes

Voice class configuration (config-class)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

If there are interoperability issues with Cisco UBE, the Cisco UBE will not work with the default SIP signaling. Hence, you must modify the SIP profiles to add, copy, modify, or remove SIP or SDP header values, and therefore enable Cisco UBE to work with SIP signaling.

Use the **request**command to modify SIP profiles for a request message. You can add, copy, modify, or remove SIP or SDP header values in an outgoing SIP request message.

Examples

The following example shows how to copy a SIP header value in a SIP request message:

```
Router(config)# voice class sip-profiles 10
Router(config-class)# request invite sip-header contact copy "(.*)" u01
```

Related Commands

Command	Description
response	Modifies a SIP profile to add, copy, modify, or remove a SIP or SDP header value from a SIP response message.

request peer-header

To use SIP profiles to copy a peer header from an outgoing Session Initiation Protocol (SIP) request message, use the **request peer-header** command in voice class configuration mode. To disable the configuration, use the **no** form of this command.

request *method* **peer-header sip** {**sip-req-uri***header-name*} **copy** *pattern variable*
no request *method* **peer-header sip** {**sip-req-uri***header-name*} **copy** *pattern variable*

Syntax Description

method	Type of message to be copied. You can specify any of the following values: • **ack** --SIP acknowledgment message. • **any** --SIP message. • **bye** --SIP BYE message. • **cancel** --SIP CANCEL message. • **comet** --SIP COMET message. • **info** --SIP INFO message. • **invite** --First SIP INVITE message. • **notify** --Specifies SIP NOTIFY message. • **options** --SIP OPTIONS message. • **prack** --SIP PRACK message. • **publish** --SIP PUBLISH message. • **refer** --SIP REFER message. • **register** --SIP REGISTER message. • **reinvite** --SIP REINVITE message. • **subscribe** --SIP SUBSCRIBE message. • **update** --SIP UPDATE message.
sip	Specifies that the SIP header must be copied from the peer call leg.
sip-req-uri	Specifies the SIP request Uniform Resource Identifier (URI) to be copied from the peer call leg.
header-name	Header name from which the values must be copied.
copy	Copies a header.
pattern	Match pattern.
variable	Variable to which the pattern value must be copied. The range is from u01 to u99.

Command Default

No SIP profiles are modified to copy a peer header in an outgoing SIP request message.

Command Modes

Voice class configuration (config-class)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

If there are interoperability issues with Cisco UBE, then the Cisco UBE will not be able to work with the default SIP signaling. Hence, you must modify the SIP profiles to add, copy, modify, or remove SIP or SDP header values, and therefore enable Cisco UBE to work with SIP signaling.

Configure the **request peer-header**command to use SIP profiles to copy a peer header from an outgoing SIP request message.

Examples

The following example shows how to copy a peer header in an outgoing SIP request message:

```
Router(config)# voice class sip-profiles 10
Router(config-class)# request invite peer-header sip contact copy "(.*)" u01
```

Related Commands

Command	Description
response peer-header	Uses SIP profiles to copy a peer header from an outgoing SIP response message.

request (XML transport)

To set the XML transport mode request handling parameters, use the **request** command in XML transport configuration mode. To disable the XML transport request parameter setting, use the **no** form of this command

request {**outstanding** *number* | **timeout** *seconds*}
no request

Syntax Description

outstanding	Maximum number of outstanding requests.
number	The valid range for the number of outstanding requests is from 1 to 10. The default is 1.
timeout	Response timeout at the transport level.
seconds	Specifies the number of seconds a request is active before it times out. Valid rangeis from 0 to 60 seconds. The default value is 0 (no timeout).

Command Default

The default for **outstanding** is 1 and the default for **timeout** is 0 (no timeout).

Command Modes

XML transport configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Use this command to set the request timeout. A value of 0 seconds specifies no timeout. This timeout applies to the request being processed and not outstanding requests as described below. The specified timeout limits the amount of time between the request being dequeued by the application and the completion of the processing of that request.

Use this command to specify the number of outstanding requests allowed per application for the specified transport mode. The outstanding requests are those requests that are queued at the application for processing but have not yet been processed.

Examples

The following example shows how to enter XML transport configuration mode, set the XML transport request timeout to 10 seconds, and exit XML transport configuration mode:

```
Router(config)# ixi transport http
Router(conf-xml-trans)# request timeout 10
```

Related Commands

Command	Description
ixi transport http	Enters XML transport configuration mode.
ixi application mib	Enters XML application configuration mode.
response size (XML transport)	Set the XML transport fragment size.

requri-passing

To enable pass through of the host part of the Request-URI and To SIP headers, use the **requri-passing** command in the Session Initiation Protocol (SIP) configuration mode. To disable this configuration, use the **no** form of the command.

requri-passing
no requri-passing

Syntax Description

This command has no keywords or arguments.

Command Default

The outbound Request-URI is set to session target.

Command Modes

Session Initiation Protocol (SIP) configuration mode (conf-voi-serv).

Voice class tenant configuration (config-class).

Command History

Release	Modification
15.4(1)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

By default, Cisco Unified Border Element sets the host part of the URI to the value configured under the session target of the outbound dial peer.

Example

The following example shows how to enable pass through of the host part of the Request-URI and To SIP headers using the **requri-passing** command:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# requri-passing
Device(conf-serv-sip)# end
```

Related Commands

Command	Description
contact-passing	Configures pass-through of the contact header from one leg to the other leg for 302 pass-through.
session target sip-uri	Derives session target from incoming URI.
voice-class sip requri-passing	Enables the pass through of SIP URI headers.

reset

To reset a set of digital signal processors (DSPs), use the **reset** command in global configuration mode.

reset *number*

Syntax Description

number	Number of DSPs to be reset. Range is from 0 to 30.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

12.0(5)XE	This command was introduced on the Cisco 7200 series.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Examples

The following example displays the reset command configuration for DSP 1:

```
reset 1
01:24:54:%DSPRM-5-UPDOWN: DSP 1 in slot 1, changed state to up
```

reset timer expires

To globally configure Cisco Unified Communications Manager Express (Cisco Unified CME), a Cisco IOS voice gateway, or a Cisco Unified Border Element (Cisco UBE) to reset the expires timer upon receipt of a Session Initiation Protocol (SIP) 183 Session In Progress message, use the **reset timer expires** command in voice service SIP configuration mode or voice class tenant configuration mode. To globally disable resetting of the expires timer upon receipt of SIP 183 messages, use the **no** form of this command.

reset timer expires 183 system
no reset timer expires 183 system

Syntax Description

183	Specifies resetting of the expires timer upon receipt of SIP 183 Session In Progress messages.
system	Specifies that the expires timer requests use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

The expires timer is not reset after receipt of SIP 183 Session In Progress messages and a session or call that is not connected within the default expiration time (three minutes) is dropped.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
15.0(1)XA	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.

Usage Guidelines

In some scenarios, early media cut-through calls (such as emergency calls) rely on SIP 183 with session description protocol (SDP) Session In Progress messages to keep the session or call alive until receiving a FINAL SIP 200 OK message, which indicates that the call is connected. In these scenarios, the call can time out and be dropped if it does not get connected within the default expiration time (three minutes).

Note The expires timer default is three minutes. However, you can configure the expiration time to a maximum of 30 minutes using the **timers expires** command in SIP user agent (UA) configuration mode.

To prevent early media cut-through calls from being dropped because they reach the expires timer limit, use the **reset timer expires** command in voice service SIP configuration mode to globally enable all dial peers on Cisco Unified CME, Cisco IOS voice gateways, or Cisco UBEs to reset the expires timer upon receipt of any SIP 183 message.

To configure the reset timer expiration setting for an individual dial peer, use the **voice-class sip reset timer expires** command in dial peer voice configuration mode. To disable the expires timer reset on receipt of SIP 183 messages function, use the **no reset timer expires** command in voice service SIP configuration mode.

Examples

The following example shows how to globally configure all dial peers on Cisco Unified CME, a Cisco IOS voice gateway, or a Cisco UBE to reset the expires timer each time a SIP 183 message is received:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# reset timer expires 183
```

The following example shows how to reset the expire timer each time a SIP 183 message is received in the voice class tenant configuration mode:

```
Router(config-class)# reset timer expires 183 system
```

Related Commands

Command	Description
timers expires	Specifies how long a SIP INVITE request remains valid before it times out if no appropriate response is received for keeping the session alive.
voice-class sip reset timer expires	Configures an individual dial peer on Cisco Unified CME, a Cisco IOS voice gateway, or a Cisco UBE to reset the expires timer upon receipt of a SIP 183 message.

resource (voice)

To configure parameters for monitoring resources, use the **resource** command in voice-class configuration mode. To disable the configuration for monitoring resources, use the **no** form of this command.

resource {**cpu** {**1-min-avg** | **5-sec-avg**} | **ds0** | **dsp** | **mem** {**io-mem** | **proc-mem** | **total-mem**}} [**threshold high** *threshold-value* **low** *threshold-value*]
no resource {**cpu** | **ds0** | **dsp** | **mem**}

Syntax Description

cpu	Reports the CPU utilization information.
1-min-avg	Collects the CPU data for an average of one minute.
5-sec-avg	Collects the CPU data for an average of five seconds.
ds0	Reports utilization information for the DS0 port.
dsp	Reports utilization information for the digital signal processor (DSP) channel.
mem	Reports the memory utilization information.
io-mem	Reports the input/output memory utilization information.
proc-mem	Reports the process memory utilization information.
total-mem	Reports the complete memory utilization information.
threshold	Configures the high and low threshold values for the critical resources.
high	(Optional) Configures the resource high watermark value.
low	(Optional) Configures the resource low watermark value.
threshold-value	Threshold value, in percentage.

Command Default

Critical gateway resources are not monitored.

Command Modes

Voice-class configuration mode (config-class)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use the **resource** command to configure parameters for critical resources such as CPU, memory, DS0, and DSP to report the utilization status to external entities using the gateway resources for call handling. You can use the **voice class resource-group** command to enter voice-class configuration mode and configure resource groups. Each resource group has a unique number that identifies a group of resources to be monitored.

When you configure the high watermark values for any of the monitoring resources, be sure not to use more resources than available on the gateway. The high and low watermark values for threshold only indicate that the gateway might run out of resources soon. However, the gateway must still be able to trigger threshold-based reporting to the routing/monitoring entity.

When you configure the low watermark value for the threshold, be sure not to underutilize the gateway resources.

Examples

The following example shows how to configure CPU to report the utilization information to the external entities:

```
Router> enable
Router# configure terminal
Router(config)# voice class resource-group 1
Router(config-class)# resource cpu 1-min-avg threshold high 10 low 2
```

Related Commands

Command	Description
debug rai	Enables debugging for Resource Allocation Indication (RAI).
periodic-report interval	Configures periodic reporting parameters for gateway resource entities.
rai target	Configures the SIP RAI mechanism.
show voice class resource-group	Displays the resource group configuration information for a specific resource group or all resource groups.
voice class resource-group	Enters voice-class configuration mode and assigns an identification tag number for a resource group.

resource threshold

To configure a gateway to report H.323 resource availability to its gatekeeper, use the **resource threshold**command in gateway configuration mode. To disable gateway resource-level reporting, use the **no** form of this command.

resource threshold [**all**] [**high** *percentage-value*] [**low** *percentage-value*]
no resource threshold

Syntax Description

all	(Optional) High- and low-parameter settings are applied to all monitored H.323 resources. This is the default condition.
high *percentage -value*	(Optional) Resource utilization level that triggers a Resource Availability Indicator (RAI) message that indicates that H.323 resource use is high. Enter a number between 1 and 100 that represents the high-resource utilization percentage. A value of 100 specifies high-resource usage when any H.323 resource is unavailable. Default is 90 percent.
low *percentage-value*	(Optional) Resource utilization level that triggers an RAI message that indicates H.323 resource usage has dropped below the high-usage level. Enter a number between 1 and 100 that represents the acceptable resource utilization percentage. After the gateway sends a high-utilization message, it waits to send the resource recovery message until the resource use drops below the value defined by the **low** parameter. Default is 90 percent.

Command Default

Reports low resources when 90 percent of resources are in use and reports resource availability when resource use drops below 90 percent.

Command Modes

Gateway configuration

Command History

Release	Modification
12.0(5)T	This command was introduced on the Cisco AS5300.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release

Usage Guidelines

This command defines the resource load levels that trigger RAI messages. To view the monitored resources, enter the **show gateway** command.

The monitored H.323 resources include digital signal processor (DSP) channels and DS0s. Use the **show call resource voice stats** command to see the total amount of resources available for H.323 calls.

> **Note** The DS0 resources that are monitored for H.323 calls are limited to the ones that are associated with a voice POTS dial peer.

See the dial-peer configuration commands for details on how to associate a dial peer with a PRI or channel-associated signaling (CAS) group.

When any monitored H.323 resources exceed the threshold level defined by the **high** parameter, the gateway sends an RAI message to the gatekeeper with the AlmostOutOfResources field flagged. This message reports high resource usage.

When all gateway H.323 resources drop below the level defined by the **low** parameter, the gateway sends the RAI message to the gatekeeper with the AlmostOutOfResources field cleared.

When a gatekeeper can choose between multiple gateways for call completion, the gatekeeper uses internal priority settings and gateway resource statistics to determine which gateway to use. When all other factors are equal, a gateway that has available resources is chosen over a gateway that has reported limited resources.

Examples

The following example defines the H.323 resource limits for a gateway.

```
gateway1(config-gateway)# resource threshold high 70 low 60
```

Related Commands

Command	Description
show call resource voice stats	Displays resource statistics for an H.323 gateway.
show call resource voice threshold	Displays the threshold configuration settings and status for an H.323 gateway.
show gateway	Displays the current gateway status.

resource-pool (mediacard)

To create a Digital Signal Processor (DSP) resource pool on ad-hoc conferencing and transcoding port adapters, use the **resource-pool**command in mediacard configuration mode. To remove the DSP resource pool and release the associated DSP resources, use the **no** form of this command.

resource-pool *identifier* **dsps** *number*
no resource-pool *identifier* **dsps** *number*

Syntax Description

identifier	Identifies the DSP resource to be configured. Valid values consist of alphanumeric characters, plus "_" and "-".
dsps	Digital signal processor.
number	Specifies the number of DSPs to be allocated for the specified resource pool. Valid values are from 1 to 4.

Command Default

No default behavior or values

Command Modes

Mediacard configuration

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.4(3)	This command was integrated into Cisco IOS Release 12.4(3).

Usage Guidelines

The DSP resource pool identifier should be unique across the same Communication Media Module (CMM). Removing a resource pool may cause the profile using that resource pool to be disabled if it is the last resource pool in the profile.

Examples

The following example shows how to create a DSP resource pool:

```
resource-pool headquarters_location1 dsps 2
```

Related Commands

Command	Description
debug mediacard	Displays debugging information for DSPRM.
show mediacard	Displays information about the selected media card.

response (voice)

To use SIP profiles to add, copy, modify, or remove Session Initiation Protocol (SIP) or Session Description Protocol (SDP) header value in a SIP response message, use the **response**command in voice class configuration mode. To disable the configuration, use the **no** form of this command.

response *option* {**sdp-header** | **sip-header**} *header-name* {**add** | **copy** | **modify** | **remove**} *string*
no response *option* {**sdp-header** | **sip-header**} *header-name* {**add** | **copy** | **modify** | **remove**} *string*

Syntax Description

option	Response code to be added, copied, modified, or removed.
	You can specify one of the following values:
	• *code* --Response code value. It can be one of the following values:
	  • **100**
	  • **180** to **183**
	  • **200**
	  • **102**
	  • **300** to **302**
	  • **305**
	  • **380**
	  • **400** to **423**
	  • **480** to **489**
	  • **491**
	  • **493**
	  • **500** to **505**
	  • **515**
	  • **580**
	  • **600**
	  • **603**
	  • **604**
	  • **606**
	• **any** --Adds, copies, modifies, or removes any response message.

sdp-header	Specifies SDP header.
sip-header	Specifies SIP header.
header-name	SDP or SIP header name.
add	Adds a header.
copy	Copies a header.
modify	Modifies a header.
remove	Removes a header.

string	String to be added as a header.

Command Default

No SIP profile is modified to add, copy, modify, or remove a SIP header value.

Command Modes

Voice class configuration (config-class)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

If there are interoperability issues with Cisco UBE, the Cisco UBE will not be able to work with the default SIP signaling. Hence, you must modify the SIP profiles to add, copy, modify, or remove SIP header values, to enable Cisco UBE to work with SIP signaling.

Use the **response** command to modify SIP profiles for a response message. You can add, copy, modify, or remove SIP or SDP header values in an outgoing SIP response message.

Examples

The following example shows how to copy a SIP header value in a SIP response message:

```
Router(config)# voice class sip-profiles 10
Router(config-class)# response 409 sip-header to copy string1
```

Related Commands

Command	Description
request	Modifies a SIP profile to add, copy, modify, or remove a SIP or SDP header value from an outgoing SIP request message.

response (XML application)

To set XML application response parameters, use the **response** command in XML application configuration mode. To disable response parameter settings, use the **no** form of this command.

response {**formatted** | **timeout** {**-1***seconds*}}
no response {**formatted** | **timeout** {**-1***seconds*}}

Syntax Description

formatted	Response parameters in formatted human readable XML.
timeout	Application specified response timeout.
-1	Enter -1 to indicate no application specified timeout. This is the default timeout setting.
seconds	Number of seconds a response is active before it times out. Valid range includes 0 to 60 seconds.

Command Default

The default for the **timeout** keyword is **-1** indicating not application specified timeout.

Command Modes

XML application configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The response timeout specified in this command, if other than -1 which is the default, overwrites the timeout value specified in the request (XML transport) command that sets the timeout at the transport level.

The same http transport layer could have multiple applications active at the same time. You can set the timeout for each application individually or have all of the applications to use the same timeout value set at transport layer using the request (XML transport) command in XML transport configuration mode.

Examples

The following example shows how to enter XML application configuration mode, set XML response parameters in formatted human readable XML, and exit XML application configuration mode:

```
Router(config)# ixi application mib
Router(conf-xml-app)# response formatted
```

Related Commands

Command	Description
ixi application mib	Enters XML application configuration mode.
request (XML transport)	Set the XML transport mode request handling parameters.

response peer-header

To use SIP profiles to copy a peer header value in a SIP response message, use the **response peer-header** command in voice class configuration mode. To disable the configuration, use the **no** form of this command.

response {*code* | **any**} **peer-header** **sip** {**sip-req-uri***header-name*} **copy** *pattern* *variable*
no **response** *option* **peer-header** **sip** {**sip-req-uri***header-name*} **copy** *pattern* *variable*

Syntax Description

code	Response code to be copied. You can specify one of the following values: • • **100** • **180** to **183** • **200** • **102** • **300** to **302** • **305** • **380** • **400** to **423** • **480** to **489** • **491** • **493** • **500** to **505** • **515** • **580** • **600** • **603** • **604** • **606** • **any** --Adds, copies, modifies, or removes any response message.
any	Adds, copies, modifies, or removes any response message.
sip	Specifies that the SIP header must be copied from the peer call leg.
sip-req-uri	Specifies the SIP request Uniform Resource Identifier (URI) to be copied from the peer call leg.
header-name	Header name from which the peer header values must be copied.
copy	Copies a header.
pattern	Match pattern.
variable	The destination variable name. The range is from u01 to u99.

Command Default

No SIP profile is modified.

Command Modes

Voice class configuration (config-class)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

If there are interoperability issues with Cisco UBE, the Cisco UBE will not be able to work with the default SIP signaling. Hence, you must modify the SIP profiles to add, copy, modify, or remove SIP or SDP header values, to enable Cisco UBE to work with SIP signaling.

Use the **response peer-header** command to copy a peer header value in a SIP response message.

Examples

The following example shows how to copy a peer header value in a SIP response message:

```
Router(config)# voice class sip-profiles 10
Router(config-class)# response 200 peer-header sip contact copy "(.*)" u01
```

Related Commands

Command	Description
request peer-header	Uses SIP profiles to copy a peer header value in a SIP request message.

response size (XML transport)

To set the response transport fragment size, use the **response size** command in XML transport configuration mode. To disable the response transport fragment size setting, use the **no** form of this command.

response size *kBps*
no response size

Syntax Description

kBps	Size of the fragment in the response buffer in kilobytes. Valid range is 1 to 64 kB. The default is 4 kB.

Command Modes

XML transport configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The fragment size is constrained by the transport type. The CLI help provides input guidelines.

Examples

The following example shows how to enter XML transport configuration mode, set XML transport fragment size to 32 Kbytes, and exit XML transport configuration mode:

```
Router(config)# ixi transport http
Router(conf-xml-trans)# response size 32
```

Related Commands

Command	Description
ixi transport http	Enters XML transport configuration mode.
ixi application mib	Enter XML application configuration mode.
request (XML transport)	Sets XML transport request handling parameters.

response-timeout

To configure the maximum time to wait for a response from a server, use the **response-timeout**command in settlement configuration mode. To reset to the default, use the **no** form of this command.

response-timeout *seconds*
no response-timeout *seconds*

Syntax Description

seconds	Response waiting time, in seconds. Default is 1.

Command Default

1 second

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

If no response is received within the response-timeout time limit, the current connection ends, and the router attempts to contact the next service point.

Examples

The following example sets response timeout to 1 second.

```
settlement 0
 response-timeout 1
```

Related Commands

Command	Description
connection -timeout	Configures the time for which a connection is maintained after completion of a communication exchange.
customer -id	Identifies a carrier or ISP with a settlement provider.
device -id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max -connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
retry -delay	Sets the time between attempts to connect with the settlement provider.
retry -limit	Sets the maximum number of attempts to connect to the provider.

Command	Description
session -timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement mode and specifies the attributes specific to a settlement provider.
show settlement	Displays the configuration for all settlement server transactions.
shutdown/no shutdown	Deactivates the settlement provider/activates the settlement provider.
type	Configures an SAA-RTR operation type.
url	Specifies the Internet service provider address.

retries (auto-config application)

To set the number of download retry attempts for an auto-configuration application, use the **retries** command in auto-config application configuration mode. To reset to the default, use the **no** form of this command.

retries *number*
no retries

Syntax Description

number	Specifies the download retry attempts. Valid range is 1 to 3.

Command Default

The default value is 2.

Command Modes

Auto-config application configuration

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Examples

The following example shows the **retries** command used to set the number of retries for an auto-configuration application to 3:

```
Router(auto-config-app)# retries 3
```

Related Commands

Command	Description
auto-config	Enables auto-configuration or enters auto-config application configuration mode for the SCCP application.
show auto-config	Displays the current status of auto-configuration applications.

retry bye

To configure the number of times that a BYE request is retransmitted to the other user agent, use the **retry bye** command in SIP UA configuration mode voice class tenant configuration mode. To reset to the default, use the no form of this command.

retry bye *number* **system**
no retry bye *number* **system**

Syntax Description

number	Number of BYE retries. Range is from 1 to 10. The default is 10.
system	Specifies that the requests use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

10 retries

Command Modes

SIP UA configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400 and Cisco AS5850 in this release.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models under voice class tenant configuration.

Usage Guidelines

To reset this command to the default value, you can also use the **default** command.

Examples

```
The following example sets the number of BYE retries to 5.
```

```
sip-ua
 retry bye 5
```

```
Router(config-class)# retry bye system
```

Related Commands

Command	Description
default	Resets the value of a command to its default.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
sip-ua	Enables the SIP user-agent configuration commands, with which you configure the user agent.

retry cancel

To configure the number of times that a CANCEL request is retransmitted to the other user agent, use the **retry cancel** command in SIP UA configuration mode or voice class tenant configuration mode. To reset to the default, use the **no** form of this command.

retry cancel *number* **system**
no retry cancel *number* **system**

Syntax Description

number	Number of CANCEL retries. Range is from 1 to 10. Default is 10.
system	Specifies that the cancel requests use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

10 retries

Command Modes

SIP UA configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400 and Cisco AS5850 in this release.
15.6(2)T	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models under voice class tenant configuration.

Usage Guidelines

To reset this command to the default value, you can also use the **default** command.

Examples

```
The following example sets the number of cancel retries to 5.
sip-ua
 retry cancel 5
```

The following example sets the number of cancel retries in the voice class tenant configuration mode:

```
Router(config-class)# retry cancel system
```

Related Commands

Command	Description
default	Resets the value of a command to its default.
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
sip-ua	Enables the sip ua configuration commands, with which you configure the user agent.

retry comet

To configure the number of times that a COMET request is retransmitted to the other user agent, use the **retry comet**command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

retry comet *number*
no retry comet

Syntax Description

number	Number of COMET retries. Range is from 1 to 10. Default is 10.

Command Default

10 retries

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Usage Guidelines

COMET, or conditions met, indicates if preconditions for a given call or session have been met. This command is applicable only with calls (other than best-effort) that involve quality of service (QoS).

Use the default number of 10 retries, when possible. Lower values, such as 1, can lead to an increased chance of the message not being received by the other user agent.

Examples

The following example configures aCOMET request to be retransmitted 8 times:

```
Router(config)# sip-ua
Router(config-sip-ua)# retry comet 8
```

Related Commands

Command	Description
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry invite	Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.

Command	Description
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
show sip -ua retry	Displays the SIP retry attempts.
show sip -ua statistics	Displays response, traffic, timer, and retry statistics.

retry info

To configure the number of times, that an INFO request is retransmitted to the other user agent, use **retry info** command in SIP UA configuration mode or voice class tenant configuration mode.

retry info *number* **[system]**

no retry update

Syntax Description

number	Number of INFO retries. Range is from 1 to 10. Default is 6.
system	Specifies that the INFO requests use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

6 retries

Command Modes

SIP UA configuration

Voice class tenant configuration

Command History

Release	Modification
Cisco IOS 15.6(2)T and Cisco IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models under voice class tenant configuration.

Usage Guidelines

Configures the number of times, that an INFO request is retransmitted to the other user agent.

Example

In sip-ua mode:

```
Device> enable
Device# configure terminal
Device(config)# sip-ua
Device(config-sip-ua)# retry info 8
```

In voice class tenant mode:

```
Device> enable
Device# configure terminal
Device(config)# voice class tenant 1
Device(config-class)# retry info 8
```

retry interval

To define the time between border element attempts delivery of unacknowledged call-detail-record (CDR) information, use the **retry interval**command in Annex G neighbor usage configuration mode. To reset to the default, use the **no** form of this command.

retry interval *seconds*
no retry interval

Syntax Description

seconds	Retry interval between delivery attempts, in seconds. Range is from 1 to 3600 (1 hour). The default is 900.

Command Default

900 seconds

Command Modes

Annex G neighbor usage configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use this command to set the interval during which the border element attempts delivery of unacknowledged call-detail-record (CDR) information.

Examples

The following example sets the retry interval to 2700 seconds (45 minutes):

```
Router(config-nxg-neigh-usg)#
retry interval 2700
```

Related Commands

Command	Description
access-policy	Requires that a neighbor be explicitly configured.
inbound ttl	Sets the inbound time-to-live value.
outbound retry-interval	Defines the retry period for attempting to establish the outbound relationship between border elements.
retry window	Defines the total time for which a border element attempts delivery.
service-relationship	Establishes a service relationship between two border elements.
shutdown	Enables or disables the border element.
usage-indication	Enters the mode used to configure optional usage indicators.

retry invite

To configure the number of times that a Session Initiation Protocol (SIP) INVITE request is retransmitted to the other user agent, use the **retry invite** command in SIP UA configuration mode or voice class tenant configuration mode. To reset to the default, use the **no** form of this command.

retry invite *number* **system**
no retry invite *number* **system**

Syntax Description

number	Number of INVITE retries. Range is from 1 to 10. Default is 6.
system	Specifies that the INVITE requests use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

6 retries

Command Modes

SIP UA configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

To reset this command to the default value, you can also use the **default** command.

When using the dial-peer rotary function, ensure that the **retry invite** command value is set to 4 or less.

Note CUBE uses the exponential backoff series algorithm (1, 2, 4, 8, 16, 32, 64, 128, ... seconds) to retry the invites. The invites are resent after each exponential delay. For example, if the retry-invite value is 6 (default), then the CUBE uses 6 exponential backoff elements and resend invite after each exponential delay (that is, re-sends invite after 1, 2, 4, 8, 16, 32, seconds). In this case, the final invite is sent after 64 seconds (1+2+4+8+16+32=64). If you reset the retry value to 2, then the CUBE uses 2 exponential backoff elements (that is, re-sends invite after 1, 2 seconds). In this case, the final invite is sent after 3 seconds (1+2=3).

Examples

The following example sets the number of invite retries to 5.

```
sip-ua
 retry invite 5
```

The following example sets the number of invite retries to 2 for tenant 1 in the voice class tenant configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# voice class tenant 1
Router(config-class)# retry invite 2
```

Related Commands

Command	Description
default	Resets the value of a command to its default.
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
sip-ua	Enables the UA configuration commands, with which you configure the user agent.

retry keepalive (SIP)

To set the retry count for keepalive retransmission, use the **retry keepalive** command in SIP UA configuration mode. To restore the retry count to the default value for keepalive retransmission, use the **no** form of this command.

retry keepalive *count*
no retry keepalive *count*

Syntax Description

count	Retry keepalive retransmission value in the range from 1 to 10. The default value is 6.

Command Default

The default value for the retry keepalive retransmission is 6.

Command Modes

SIP UA configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Sets the keepalive retransmissions retry count.

Examples

The following example sets the retry for the keepalive retransmissions to 8:

```
sip-ua
 retry keepalive 8
```

Related Commands

Command	Description
busyout monitor keepalive	Selects a voice port or ports to be busied out in cases of a keepalive failure.
keepalive target	Identifies a SIP server that will receive keepalive packets from the SIP gateway.
keepalive trigger	Sets the trigger to the number of Options message requests that must consecutively receive responses from the SIP servers in order to unbusy the voice ports when in the down state.
timers keepalive	Sets the time interval between sending Options message requests when the SIP server is active or down.

retry notify

To configure the number of times that the notify message is retransmitted to the user agent that initiated the transfer or Refer request, use the **retry notify** command in SIP UA configuration mode or voice class tenant configuration mode. To reset to the default, use the **no** form of this command.

retry notify *number* **system**
no retry notify system

Syntax Description

number	Number of notify message retries. Range is from 1 to 10. Default is 10.
system	Specifies that the notify messages use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

10 retries

Command Modes

SIP UA configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB2	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models under voice class tenant configuration.

Usage Guidelines

A notify message informs the user agent that initiated the transfer or refer request of the outcome of the Session Initiation Protocol (SIP) transaction.

Use the default number of 10 when possible. Lower values such as 1 can lead to an increased chance of the message not being received by the other user agent.

Examples

The following example configures a notify message to be retransmitted 10 times:

```
Router(config)# sip-ua
Router(config-sip-ua)# retry notify 10
```

The following example configures a notify message to be retransmitted in the voice class tenant configuration mode:

```
Router(config-class)# retry notify system
```

Related Commands

Command	Description
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a Session Initiation Protocol (SIP) INVITE request is retransmitted to the other user agent.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
show sip-ua retry	Displays the SIP retry attempts.
show sip-ua statistics	Displays response, traffic, timer, and retry statistics.
timers notify	Sets the amount of time that the user agent should wait before retransmitting the Notify message.

retry options

To configure the number of times, that an OPTIONS request is retransmitted to the other user agent, use **retry options** command in SIP UA configuration mode or voice class tenant configuration mode.

retry options *number* **[system]**

no retry options

Syntax Description

number	Number of OPTIONS retries. Range is from 1 to 10. Default is 6.
system	Specifies that the OPTIONS requests use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

6 retries

Command Modes

SIP UA configuration

Voice class tenant configuration

Command History

Release	Modification
Cisco IOS 15.6(2)T and Cisco IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models under voice class tenant configuration.

Usage Guidelines

Configures the number of times, that an OPTIONS request is retransmitted to the other user agent.

Example

In sip-ua mode:

```
Device> enable
Device# configure terminal
Device(config)# sip-ua
Device(config-sip-ua)# retry options 8
```

In voice class tenant mode:

```
Device> enable
Device# configure terminal
Device(config)# voice class tenant 1
Device(config-class)# retry options 8
```

retry prack

To configure the number of times that the PRACK request is retransmitted to the other user agent, use the **retry prack** command in SIP UA configuration mode or voice class tenant configuration mode. To reset to the default, use the **no** form of this command.

retry prack *number* **system**
no retry prack system

Syntax Description

number	Number of PRACK retries. Range is from 1 to 10. Default is 10.
system	Specifies that the prack requests use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

10 retries

Command Modes

SIP UA configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models under voice class tenant configuration.

Usage Guidelines

PRACK allows reliable exchanges of Session Initiation Protocol (SIP) provisional responses between SIP endpoints. Use the default number of 10 when possible. Lower values such as 1 can lead to an increased chance of the message not being received by the other user agent.

Examples

The following example configures a PRACK request to be retransmitted 9 times:

```
Router(config)# sip-ua
Router(config-sip-ua)# retry prack 9
```

The following example configures a PRACK request to be retransmitted in the voice class tenant configuration mode:

```
Router(config-class)# retry prack system
```

Related Commands

Command	Description
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
show sip-ua retry	Displays the SIP retry attempts.
show sip-ua statistics	Displays response, traffic, timer, and retry statistics.

retry refer

To configure the number of times that the Refer request is retransmitted, use the **retry refer** command in SIP UA configuration mode or voice class tenant configuration mode. To reset to the default, use the **no** form of this command.

retry refer *number* **system**
no retry refer system

Syntax Description

number	Number of Refer request retries. Range is from 1 to 10. Default is 10.
system	Specifies that the REFER requests use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

10 retries

Command Modes

SIP UA configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.2(11)YT	This command was introduced.
12.2(15)T	This command is supported on the Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and the Cisco 7200 series routers in this release.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models under voice class tenant configuration.

Usage Guidelines

A Session Initiation Protocol (SIP) Refer request is sent by the originating gateway to the receiving gateway and initiates call forward and call transfer capabilities.

When configuring the **retry refer** command, use the default number of 10 when possible. Lower values such as 1 can lead to an increased chance of the message not being received by the receiving gateway.

Examples

The following example configures a Refer request to be retransmitted 10 times:

```
Router(config)# sip-ua
Router(config-sip-ua)# retry refer 10
```

The following example configures a Refer request to be retransmitted in the voice class tenant configuration mode:

```
Router(config-class)# retry refer system
```

Related Commands

Command	Description
show sip-ua retry	Displays the SIP retry attempts.
show sip-ua statistics	Displays response, traffic, timer, and retry statistics.

retry register

To set the total number of Session Initiation Protocol (SIP) register messages that the gateway should send, use the **retry register** command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset this number to the default, use the **no** form of this command.

retry register *retries* **system**[**exhausted-random-interval minimum** *minutes* **maximum** *minutes*]
no retry register

Syntax Description

retries	Total number of register messages that the gateway should send. The range is from 1 to 10. The default is 6 retries.
exhausted-random-interval	Specifies the register request to be generated within the defined range of time intervals.
minimum *minutes*	Specifies the minimum time interval range, in minutes, that will be used as the interval before the next registration is sent.
maximum *minutes*	Specifies the maximum time interval range, in minutes, that will be used as the interval before the next registration is sent.
system	Specifies that the register messages use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

The gateway sends 6 retries.

Command Modes

SIP UA configuration (config-sip-ua)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(22)T	This command was modified. Support for IPv6 was added.
12.4(22)YB	This command was modified. The **exhausted-random-interval** keyword was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models under voice class tenant configuration.

Usage Guidelines

Use the default number when possible. Lower values such as 1 may lead to the message not being received by the other user agent.

Examples

The following example shows how to configure the gateway to send 9 register messages:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# retry register 9
```

The following example shows how to configure the gateway to send 6 register messages and choose a random number between 2 and 5 as the interval before sending the next registration message:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# retry register 6 exhausted-random-interval minimum 2 maximum 5
```

The following example configures the gateway to register messages in the voice class tenant configuration mode:

```
Router(config-class)# retry register system
```

Related Commands

Command	Description
registrar	Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar.
timers register	Sets how long the SIP user agent waits before sending register requests.

retry rel1xx

To configure the number of times that the reliable 1*xx* response is retransmitted to the other user agent, use the **retry rel1xx** command in SIP UA configuration mode or voice class tenant configuration mode. To reset to the default, use the **no** form of this command.

retry rel1xx *number* **system**
no retry rel1xx system

Syntax Description

number	Number of reliable 1*xx* retries. Range is from 1 to 10. Default is 6.
system	Specifies that the reliable 1*xx* response is retransmitted use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

6 retries

Command Modes

SIP UA configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models under voice class tenant configuration.

Usage Guidelines

Use the default number of 6 when possible. Lower values such as 1 can lead to an increased chance of the message not being received by the other user agent.

Examples

The following example configures the reliable 1*xx* response to be retransmitted 7 times:

```
Router(config)# sip-ua
Router(config-sip-ua)# retry rel1xx 7
```

The following example configures the reliable 1*xx* response to be retransmitted in the voice class tenant configuration mode:

```
Router(config-class)# retry rel1xx system
```

Related Commands

Command	Description
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times the PRACK request is retransmitted.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
show sip-ua retry	Displays the SIP retry attempts.
show sip-ua statistics	Displays response, traffic, timer, and retry statistics.

retry response

To configure the number of times that the response message is retransmitted to the other user agent, use the **retry response** command in SIP UA configuration mode or voice class tenant configuration mode. To reset to the default, use the no form of this command.

retry response *number* **system**
no retry response system

Syntax Description

number	Number of response retries. Range is from 1 to 10. Default is 6.
system	Specifies that the response messages use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

6 retries

Command Modes

SIP UA configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models under voice class tenant configuration.

Usage Guidelines

To reset this command to the default value, you can also use the **default** command.

Examples

The following example sets the number of response retries to 5.

```
sip-ua
 retry response 5
```

The following example sets the number of response retries in the voice class tenant configuration mode:

```
Router(config-class)# retry response system
```

Related Commands

Command	Description
default	Resets the value of a command to its default.
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times the PRACK request is retransmitted.
retry rel1xx	Configures the number of times that the reliable 1*xx* response is retransmitted to the other user agent.
sip-ua	Enables the sip-ua configuration commands, with which you configure the user agent.

retry subscribe

To configure the number of times that a SIP SUBSCRIBE message is retransmitted to the other user agent, use the **retry subscribe** command in SIP UA configuration mode or voice class tenant configuration mode. To reset to the default, use the no form of this command.

retry subscribe *number* **system**
no retry subscribe *number* **system**

Syntax Description

number	Number of SUBSCRIBE retries. Range is 1 to 10. Default is 10.
system	Specifies that the SIP SUBSCRIBE message retransmitted use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

10 retries

Command Modes

SIP UA configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.3(4)T	This command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models under voice class tenant configuration.

Usage Guidelines

Use the **retry timer** command to configure retry intervals for this command. The default value for **retry timer** is 1000 ms, and the range is 10 to 100. Setting the timer to lower values can cause the application to get a failure response more quickly.

Examples

The following example sets the number of subscribe retries to 5:

```
sip-ua
 retry subscribe 5
```

The following example sets the number of subscribe retries in the voice class tenant configuration mode:

```
Router(config-class)# retry subscribe system
```

Related Commands

Command	Description
retry notify	Configures the number of times that the Notify message is resent to the user agent that initiated the Invite request.
retry timer	Configures the retry interval for resending SIP messages.
show sip-ua retry	Displays SIP user agent retry statistics.

retry update

To configure the number of times, that an UPDATE request is retransmitted to the other user agent, use **retry update** command in SIP UA configuration mode or voice class tenant configuration mode.

retry update *number* **[system]**

no retry update

Syntax Description

number	Number of UPDATE retries. Range is from 1 to 10. Default is 6.
system	Specifies that the UPDATE requests use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

6 retries

Command Modes

SIP UA configuration

Voice class tenant configuration

Command History

Release	Modification
Cisco IOS 15.6(2)T and Cisco IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models under voice class tenant configuration.

Usage Guidelines

Configures the number of times, that an UPDATE request is retransmitted to the other user agent.

Example

In sip-ua mode:

```
Device> enable
Device# configure terminal
Device(config)# sip-ua
Device(config-sip-ua)# retry update 8
```

In voice class tenant mode:

```
Device> enable
Device# configure terminal
Device(config)# voice class tenant 1
Device(config-class)# retry update 8
```

retry window

To define the total time for which a border element attempts delivery, use the **retry window**command in Annex G neighbor usage configuration mode. To reset to the default, use the **no** form of this command.

retry window *window-value*
no retry window

Syntax Description

window -value	Window value, in minutes. Range is from 1 to 65535. Default is 1440 minutes (24 hours).

Command Default

1440 minutes (24 hours)

Command Modes

Annex G neighbor usage configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use this command to set the total time during which a border element attempts delivery of unacknowledged call-detail-record (CDR) information.

Examples

The following example sets the retry window to 15 minutes:

```
Router(config-nxg-neigh-usg)# retry window 15
```

Related Commands

Command	Description
access-policy	Requires that a neighbor be explicitly configured.
inbound ttl	Sets the inbound time-to-live value.
outbound retry-interval	Defines the retry period for attempting to establish the outbound relationship between border elements.
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.

Command	Description
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
service-relationship	Establishes a service relationship between two border elements.
shutdown	Enables or disables the border element.
usage-indication	Enters the submode used to configure optional usage indicators.

retry-delay

To set the time between attempts to connect with the settlement provider, use the **retry-delay** command in settlement configuration mode. To reset to the default, use the **no** form of this command.

retry-delay *seconds*
no retry-delay

Syntax Description

seconds	Interval, in seconds, between attempts to connect with the settlement provider. Range is from 1 to 600.

Command Default

2 seconds

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

After exhausting all service points for the provider, the router is delayed for the specified length of time before resuming connection attempts.

Examples

The following example sets a retry value of 15 seconds:

```
settlement 0
 relay-delay 15
```

Related Commands

Command	Description
connection -timeout	Configures the time for which a connection is maintained after completion of a communication exchange.
customer -id	Identifies a carrier or ISP with a settlement provider.
device -id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max -connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response -timeout	Configures the maximum time to wait for a response from a server.
retry -limit	Sets the maximum number of attempts to connect to the provider.

Command	Description
session -timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.
show settlement	Displays the configuration for all settlement server transactions.
shutdown/no shutdown	Deactivates the settlement provider/activates the settlement provider.
type	Configures an SAA-RTR operation type.

retry-limit

To set the maximum number of attempts to connect to the provider, use the **retry-limit** command in settlement configuration mode. To reset to the default, use the **no** form of this command.

retry-limit *number*
no retry-limit *number*

Syntax Description

number	Maximum number of connection attempts in addition to the first attempt. Default is 1.

Command Default

1 retry

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

If no connection is established after the configured number of retries has been attempted, the router ceases connection attempts. The retry limit number does not count the initial connection attempt. A retry limit of one (default) results in a total of two connection attempts to every service point.

Examples

The following example sets the number of retries to 1:

```
settlement 0
 retry-limit 1
```

Related Commands

Command	Description
connection -timeout	Configures the time for which a connection is maintained after a communication exchange is complete.
customer -id	Identifies a carrier or ISP with a settlement provider.
device -id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max -connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response -timeout	Configures the maximum time to wait for a response from a server.
retry -delay	Sets the time between attempts to connect with the settlement provider.

Command	Description
session -timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement mode and specifies the attributes specific to a settlement provider.
show settlement	Displays the configuration for all settlement server transactions.
shutdown	Brings up the settlement provider.
type	Configures an SAA-RTR operation type.

ring

To set up a distinctive ring for your connected telephones, fax machines, or modems, use the **ring**command in interface configuration mode. To disable the ring, use the **no** form of this command.

ring *cadence-number*
no ring *cadence-number*

Syntax Description

cadence -number	Number that determines the ringing cadence. Range is from 0 to 2: • Type 0 is a primary ringing cadence--default ringing cadence for the country your router is in. • Type 1 is a distinctive ring--0.8 seconds on, 0.4 seconds off, 0.8 seconds on, 0.4 seconds off. • Type 2 is a distinctive ring--0.4 seconds on, 0.2 seconds off, 0.4 seconds on, 0.2 seconds off, 0.8 seconds on, 4 seconds off.

Command Default

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 applies to Cisco 800 series routers.

You can specify this command when creating a dial peer. This command does not work if it is not specified within the context of a dial peer. For information on creating a dial peer, see to the *Cisco 800 Series Routers Software Configuration Guide*.

Examples

The following example specifies the type 1 distinctive ring :

```
ring 1
```

Related Commands

Command	Description
destination -pattern	Specifies the prefix, the full E.164 telephone number, or an ISDN directory number to be used for a dial peer.
dial -peer voice	Enters dial-peer configuration mode, defines the type of dial peer, and defines the tag number associated with a dial peer.
no call -waiting	Disables call waiting.
port (dial -peer)	Enables an interface on a PA-4R-DTR port adapter to operate as a concentrator port.

Command	Description
pots distinctive -ring-guard-time	Specifies a delay during which a telephone port can be rung after a previous call is disconnected (for Cisco 800 series routers).
show dial -peer voice	Displays configuration information and call statistics for dial peers.

ring cadence

To specify the ring cadence for a Foreign Exchange Station (FXS) voice port, use the **ring cadence** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

ring cadence {*pattern-number* | **define** *pulse interval*}
no ring cadence
{**ring cadence external** *patternXX* | **define**}
{**ring cadence** *patternXX* | **define**}

Syntax Description

pattern -number	Predefined ring cadence patterns. Each pattern specifies a ring-pulse time and a ring-interval time. • **pattern01** -- 2 seconds on, 4 seconds off • **pattern02** -- 1 second on, 4 seconds off • **pattern03** -- 1.5 seconds on, 3.5 seconds off • **pattern04** -- 1 second on, 2 seconds off • **pattern05** -- 1 second on, 5 seconds off • **pattern06** -- 1 second on, 3 seconds off • **pattern07** -- 0.8 second on, 3.2 seconds off • **pattern08** -- 1.5 seconds on, 3 seconds off • **pattern09** -- 1.2 seconds on, 3.7 seconds off • **pattern09** -- 1.2 seconds on, 4.7 seconds off • **pattern11** -- 0.4 second on, 0.2 second off, 0.4 second on, 2 seconds off • **pattern12** -- 0.4 second on, 0.2 second off, 0.4 second on, 2.6 seconds off
define	User-definable ring cadence pattern. Each number pair specifies one ring-pulse time and one ring-interval time. You must enter numbers in pairs, and you can enter from 1 to 6 pairs. The second number in the last pair that you enter specifies the interval between rings.
pulse	Number (1 or 2 digits) specifying ring-pulse (on) time in hundreds of milliseconds. Range is from 1 to 50, for pulses of 100 to 5000 ms. For example: 1 = 100 ms; 10 = 1 s, 40 = 4 s.
interval	Number (1 or 2 digits) specifying ring-interval (off) time in hundreds of milliseconds. Range is from 1 to 50, for pulses of 100 to 5000 ms. For example: 1 = 100 ms; 10 = 1 s, 40 = 4 s.

Command Default

Ring cadence defaults to the pattern that you specify with the **cptone** command.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series. The **patternXX** keyword was added.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
15.0(1)M	This command was modified. The **external** keyword was added to specify the ring pattern of external calls.

Usage Guidelines

To specify the ring pattern for external calls, use the **ring cadence external** command. It is supported only in STCAPP. To specify the ring cadence for internal calls, use the existing **ring cadence** command. The syntax for the ring cadence external command is the same as for the **ring cadence** command.

The **patternXX** keyword provides preset ring cadence patterns for use on any platform. The **define** keyword allows you to create a custom ring cadence. On the Cisco 2600 and Cisco 3600 series routers, only one or two pairs of digits can be entered under the **define** keyword.

Examples

The following example sets the ring cadence to 1 second on and 2 seconds off on voice port 1/0/0:

```
voice-port 1/0/0
 ring cadence pattern04
```

Related Commands

Command	Description
cptone	Specifies the default tone, ring, and cadence settings according to country.
ring frequency	Specifies the ring frequency for a specified FXS voice port.

ring dc-offset

To configure ring voltage threshold to prevent the ringer devices from sounding so as to ignore the lower voltages that can be produced when dialing. An increase in the ring voltage threshold value can overcome this. Use the ring dc-offset command in voice-port configuration mode. To reset to default, use the no form of this command.

This command is only applicable to analog FXS voice port with loop-length long configured.

ring dc-offset *volt-value*
no ring dc-offset

Syntax Description

volt-value	volt-value 10-volts - Ring DC offset 10 volts 20-volts - Ring DC offset 20 volts 24-volts - Ring DC offset 24 volts 30-volts - Ring DC offset 30 volts 35-volts - Ring DC offset 35 volts

Command Default

no ring dc-offset

Command Modes

Voice-port configuration

ring frequency

To specify the ring frequency for a specified Foreign Exchange Station (FXS) voice port, use the **ring frequency**command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

ring frequency *hertz*
no ring frequency *hertz*

Syntax Description

hertz	Ring frequency, in hertz, used in the FXS interface. Valid entries are as follows: • Cisco 3600 series: 25 and 50. Default is 25.

Command Default

Cisco 3600 series routers: 25 Hz

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco MC3810.

Usage Guidelines

Use this command to select a specific ring frequency for an FXS voice port. Use the **no** form of this command to reset the default value. The ring frequency you select must match the connected equipment. If set incorrectly, the attached phone might not ring or might buzz. In addition, the ring frequency is usually country-dependent. You should take into account the appropriate ring frequency for your area before configuring this command.

This command does not affect ringback, which is the ringing a user hears when placing a remote call.

Examples

The following example sets the ring frequency on the voice port to 25 Hz:

```
voice-port 1/0/0
 ring frequency 25
```

Related Commands

Command	Description
ring cadence	Specifies the ring cadence for an FXS voice port.
ring number	Specifies the number of rings for a specified FXO voice port.

ring number

To specify the number of rings for a specified Foreign Exchange Office (FXO) voice port, use the **ring number**command in voice port configuration mode. To reset to the default, use the **no** form of this command.

ring number *number*
no ring number *number*

Syntax Description

number	Number of rings detected before answering the call. Range is from 1 to 10. The default is 1.

Command Default

1 ring

Command Modes

Voice port configuration

Command History

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

Usage Guidelines

Use this command to set the maximum number of rings to be detected before answering a call over an FXO voice port. Use the **no** form of this command to reset the default value, which is one ring.

Normally, this command should be set to the default so that incoming calls are answered quickly. If you have other equipment available on the line to answer incoming calls, you might want to set the value higher to give the equipment sufficient time to respond. In that case, the FXO interface would answer if the equipment online did not answer the incoming call in the configured number of rings.

This command is not applicable to Foreign Exchange Station (FXS) or E&M interfaces because they do not receive ringing on incoming calls.

Examples

The following example sets 5 as the maximum number of rings to be detected before closing a connection over this voice port:

```
voice-port 1/0/0
 ring number 5
```

Related Commands

Command	Description
ring frequency	Specifies the ring frequency for a specified FXS voice port.

ringing-timeout

To define the timeout period for the SCCP telephony control (STC) application feature call back, use the **ringing-timeout**command in STC application feature callback configuration mode. To return to the default timeout period, use the **no** form of this command.

ringing-timeout *seconds*
no ringing-timeout

Syntax Description

seconds	Period of time in seconds. Range: 5 to 60. Default: 30.

Command Default

The default is 30 seconds.

Command Modes

STC application feature callback configuration (config-stcapp-callback)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command changes the timeout period of the ringing timer from the default of 30 seconds to the specified value.

The ringing timer specifies the number of seconds during which the calling device that is in a Callback on Busy condition can receive a Callback Ringing and after which, if the calling device does not answer, the CallBack on Busy condition is cancelled.

Examples

The following example shows how to change the timeout period of the ringing timer for CallBack on Busy from the default (30) to a new value (45).

```
Router(config)# stcapp feature callback
Router(config-stcapp-callback)# ringing-timer 45
Router(config-stcapp-callback)#
```

Related Commands

Command	Description
activation-code	Defines the callback activation key sequence for CallBack on Busy.

roaming (dial peer)

To enable roaming capability for a dial peer, use the **roaming** command in dial-peer configuration mode. To disable roaming capability, use the **no** form of this command.

roaming
no roaming

Syntax Description

This command has no arguments or keywords.

Command Default

No roaming

Command Modes

Dial peer configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines

Use this command to enable roaming capability of a dial peer if that dial peer can terminate roaming calls. If a dial peer is dedicated to local calls only, disable roaming capability.

The roaming dial peer must work with a roaming service provider. If the dial peer allows a roaming user to go through and the service provider is not roaming-enabled, the call fails.

Examples

The following example enables roaming capability for a dial peer:

```
dial-peer voice 10 voip
roaming
```

Related Commands

Command	Description
roaming (settlement)	Enables the roaming capability for a settlement provider.
settle-call	Limits the dial peer to using only the specific clearinghouse identified by the specified >*provider* ->*number* .
settlement roam-pattern	Configures a pattern to match against when determining roaming.

roaming (settlement)

To enable roaming capability for a settlement provider, use the **roaming** command in settlement configuration mode. To disable roaming capability, use the **no** form of this command.

roaming
no roaming

Syntax Description

This command has no arguments or keywords.

Command Default

No roaming

Command Modes

Settlement configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines

Enable roaming capability of a settlement provider if that provider can authenticate a roaming user and route roaming calls.

A roaming call is successful only if both the settlement provider and the outbound dial peer for that call are roaming-enabled.

Examples

The following example enables roaming capability for a settlement provider:

```
settlement 0
roaming
```

Related Commands

Command	Description
roaming (dial-peer mode)	Enables the roaming capability for the dial peer.
settle-call	Limits the dial peer to using only the specific clearinghouse identified by the specified >*provider* ->*number* .
settlement roam-pattern	Configures a pattern to match against when determining roaming.

rrq dynamic-prefixes-accept

To enable processing of additive registration request (RRQ) RAS messages and dynamic prefixes on the gatekeeper, use the **rrq dynamic-prefixes-accept** command in gatekeeper configuration mode. To disable processing of additive RRQ messages and dynamic prefixes, use the **no** form of this command.

rrq dynamic-prefixes-accept
no rrq dynamic-prefixes-accept

Syntax Description

This command has no arguments or keywords.

Command Default

In Cisco IOS Release 12.2(15)T, the default was set to enabled. In Cisco IOS Release 12.3(3), the default is set to disabled.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(3)	The default is modified to be disabled by default.
12.3(4)T	The default change implemented in Cisco IOS Release 12.3(3) was integrated in Cisco IOS Release 12.3(4)T.

Usage Guidelines

In Cisco IOS Release 12.2(15)T, the default for the **rrq dynamic-prefixes-accept** command was set to enabled so that the gatekeeper automatically received dynamic prefixes in additive RRQ messages from the gateway. Beginning in Cisco IOS Release 12.3(3), the default is set to disabled, and you must specify the command to enable the functionality.

Examples

The following example allows the gatekeeper to process additive RRQmessages and dynamic prefixes from the gateway:

```
Router(config-gk)# rrq dynamic-prefixes-accept
```

Related Commands

Command	Description
ras rrq dynamic prefixes	Enables advertisement of dynamic prefixes in additive RRQ messages on the gateway.

rsvp

To enable RSVP support on a transcoding or MTP device, use the **rsvp** command in DSP farm profile configuration mode. To disable RSVP support, use the **no** form of this command.

rsvp
no rsvp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

DSP farm profile configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command enables a transcoder or MTP device to register as RSVP-capable with Cisco Unified CallManager. The SCCP device acts as an RSVP agent under the control of Cisco Unified CallManager. To support RSVP, you must also enable the **codec pass-through** command.

Note This command is not supported in conferencing profiles.

Note When RSVP is not configured for call signaling on the Cisco UBE, use the **show dial-peer voice** command to verify the QoS settings that the signaling and media packets will be marked with. Fields corresponding to QoS negotiation in the output produced by the **show sip-ua calls** command should be ignored.

```
Local QoS Strength : BestEffort
Negotiated QoS Strength : BestEffort
Negotiated QoS Direction : None
```

Examples

The following example enables RSVP support on the transcoding device defined by profile 200:

```
Router(config)# dspfarm profile 200 transcode
Router(config-dspfarm-profile)# rsvp
Router(config-dspfarm-profile)# codec pass-through
```

Related Commands

Command	Description
codec (DSP Farm profile)	Specifies the codecs supported by a DSP farm profile.
debug call rsvp-sync events	Displays events that occur during RSVP setup.

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
show sccp connections rsvp	Displays information about active SCCP connections that use RSVP.

rtcp keepalive

To configure RTP Control Protocol (RTCP) keepalive report generation and generate RTCP keepalive packets, use the **rtcp keepalive**command in voice service configuration mode. To disable the configuration, use the **no** form of this command.

rtcp keepalive
no rtcp keepalive

Syntax Description

This command has no arguments or keywords.

Command Default

The command is disabled by default.

Command Modes

Voice service configuration (config)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to configure RTCP keepalive report generation and generate RTCP keepalive packets. The **no** form of the command restores the default behavior.

Examples

The following example shows how to configure RTCP keepalive report generation and generate RTCP keepalive packets:

```
Router> enable
Router# configure terminal
Router(config) voice service voip
Router(conf-voi-serv)# rtcp keepalive
```

Related Commands

Command	Description
debug voip rtcp	Enables debugging for RTCP packets.
debug voip rtp	Enables debugging for RTP packets.
debug ip rtp protocol	Enables debugging for RTP protocol.
ip rtcp report interval	Configures the average reporting interval between subsequent RTCP report transmissions.

rtcp all-pass-through

To pass through all the RTCP packets in datapath. To disable the configuration, use the **no** form of this command.

rtcp all-pass-through
no rtcp all-passthrough

Syntax Description

This command has no arguments or keywords.

Command Default

The command is disabled by default.

Command Modes

Voice service configuration (config)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

```
Device(conf-voi-serv)# rtcp all-pass-through
```

rtp-media-loop count

To configure the number of media loops before Real-Time Transport Protocol (RTP) voice and video media packets are dropped, use the **rtp-media-loop count** command in voice service configuration mode. To remove this configuration, use the **no** form of this command.

rtp-media-loop count *number*
no rtp-media-loop count

Syntax Description

number	Number of media loops. The range is from 6 to 21.

Command Default

The number of media loops is not configured, and a default value of 6 is applied.

Command Modes

Voice service configuration (conf-voi-serv)

Command History

Release	Modification
15.2(2)T3	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the **rtp-media-loop count** command when you want to control the maximum number of media loops before the RTP media packets are dropped for IP-to-IP calls. The recommended configuration is to use the default loop count of 6.

Example

The following example shows how to configure the loop count before RTP media packets are dropped:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# rtp-media-loop count 10
```

rtp payload-type

To identify the payload type of a Real-Time Transport Protocol (RTP) packet, use the **rtp payload-type** command in dial peer voice configuration mode. To remove the RTP payload type, use the **no** form of this command.

rtp payload-type {**cisco-cas-payload** *number* | **cisco-clear-channel** *number* | **cisco-codec-aacld** *number* | **cisco-codec-fax-ack** *number* | **cisco-codec-fax-ind** *number* | **cisco-codec-gsmamrnb** *number* | **cisco-codec-ilbc** *number* | **cisco-codec-isac** *number* | **cisco-codec-video-h263**+ *number* | **cisco-codec-video-h264** *number* | **cisco-fax-relay** *number* | **cisco-pcm-switch-over-alaw** *number* | **cisco-pcm-switch-over-ulaw** *number* | **cisco-rtp-dtmf-relay** *number* | **lmr-tone** *number* | **nse** *number* | **nte** *number* | **nte-tone** *number* | **opus** *number* } [**comfort-noise** {**13** | **19**}]
no rtp payload-type {**cisco-cas-payload** *number* | **cisco-clear-channel** *number* | **cisco-codec-fax-ack** *number* | **cisco-codec-fax-ind** *number* | **cisco-codec-gsmamrnb** *number* | **cisco-codec-ilbc** *number* | **cisco-codec-video-h263**+ *number* | **cisco-codec-video-h264** *number* | **cisco-fax-relay** *number* | **cisco-pcm-switch-over-alaw** *number* | **cisco-pcm-switch-over-ulaw** *number* | **cisco-rtp-dtmf-relay** *number* | **lmr-tone** *number* | **nse** *number* | **nte** *number* | **nte-tone** *number* | **opus** *number* } [**comfort-noise** {**13** | **19**}]

Syntax Description

cisco-cas-payload *number*	Cisco channel-associated signaling (CAS) RTP payload. Range: 96–127. Default: 123.
cisco-clear-channel *number*	Cisco clear-channel RTP payload. Range: 96–127. Default: 125.
cisco-codec-aacld *number*	Cisco MPEG-4 Advanced Audio Codec - Low Delay (AAC-LD) codec. Range: 96–127. Default: 114.
cisco-codec-fax-ack *number*	Cisco codec fax acknowledge. Range: 96–127. Default: 97.
cisco-codec-fax-ind *number*	Cisco codec fax indication. Range: 96–127. Default: 96.
cisco-codec-gsmamrnb *number*	Cisco Global System for Mobile Adaptive Multi-Rate narrowband (GSMAMR-NB) codec. Range: 96–127. Default: 117.
cisco-codec-ilbc *number*	Cisco Internet Low Bitrate Codec (iLBC) codec. Range: 96–127. Default: 116.
cisco-codec-isac *number*	Cisco internet Speech Audio Codec (iSAC) codec. Range: 96–127. Default: 124.
cisco -codec-video-h263+ *number*	RTP video codec H.263+ payload type. Range: 96–127. Default: 118.
cisco -codec-video-h264 *number*	RTP video codec H.264 payload type. Range: 96–127. Default: 119.
cisco-fax-relay *number*	Cisco fax relay. Range: 96–127. Default: 122.
cisco-pcm-switch-over-alaw *number*	Cisco RTP pulse code modulation (PCM) codec switch over indication (a-law). Default: 8.
cisco-pcm-switch-over-ulaw *number*	Cisco RTP PCM codec switch over indication (mu-law). Default: 0.

cisco-rtp-dtmf-relay *number*	Cisco RTP dual-tone multifrequency (DTMF) relay. Range: 96–127. Default: 121.
lmr-tone *number*	LMR payload type. Range: 96–127. Default: 0. The default value is set by the **no rtp payload-type lmr-tone** command.
nse *number*	A Named Signaling Event (NSE). Range: 96–117. Default: 100.
nte *number*	A named phone event (NTE). Range: 96–127. Default: 101.
nte-tone *number*	RFC-2833 tone payload type. Range 96–127. Default: 101.
comfort-noise 13 19	(Optional) RTP payload type of comfort noise. The July 2001 draft entitled *RTP Payload for Comfort Noise,* from the IETF (IETF) Audio or Video Transport (AVT) working group, designates 13 as the payload type for comfort noise. If you are connecting to a gateway that complies with the *RTP Payload for Comfort Noise* draft, use 13. Use 19 only if you are connecting to older Cisco gateways that use DSPware before version 3.4.32. **Note** This command option is not available on the Cisco AS5400 running NextPort digital signal processors (DSPs). This command option is available on the Cisco AS5400 only if the platform has a high-density packet voice/fax feature card (AS5X-FC) with one or more AS5X-PVDM2-64 DSP modules installed. This support was added in Cisco IOS Release 12.4(4)XC, and integrated into Release 12.4(9)T, and later 12.4T releases.
opus *number*	Interactive speech and audio codec (opus). Range: 96–127. Default: 114.

Command Default

No RTP payload type is configured.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(2)XB	This command was modified. The **nte** and **comfort - noise** keywords were added.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4(4)XC	This command was modified. The **cisco-codec-gsmamrnb** keyword was added.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Release	Modification
12.4(11)T	This command was modified. The **cisco-codec-ilbc**, **cisco-codec-video-h263+**, and **cisco-codec-video-h264** keywords were added.
12.4(15)XY	This command was modified. The **lmr-tone** and **nte-tone** keywords were added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(1)T	This command was modified. The **cisco-codec-isac** keyword was added.
Cisco IOS XE Amsterdam 17.3.1a	This command was modified. The **opus** keyword was added.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Note **rtp payload** YANG configuration is supported for audio and video codecs. Other configurations that are related to fax, NSE, pcm-switchover are not supported. For example, **cisco fax-relay**,**cisco-pcm-switch-over-alaw**,**cisco-codec-fax-ack/ind**, **nse**, and**g726r16**.

Use this command to identify the payload type of an RTP. Use this command after the **dtmf-relay**command is used to choose the NTE method of DTMF relay for a Session Initiation Protocol (SIP) call.

Configured payload types of NSE and NTE exclude certain values that have been previously hardcoded with Cisco proprietary meanings. Do not use the following numbers, which have preassigned values: 96, 97, 100, 117, 121–123, and 125–127.

Use of these values results in an error message when the command is entered. You must first reassign the value in use to a different unassigned number, for example:

```
rtp payload-type cisco-codec-ilbc 100
ERROR: value 100 in use!
rtp payload-type nse 105
rtp payload-type cisco-codec-ilbc 100
```

Examples

The following example shows how to identify the RTP payload type as GSMAMR-NB115:

```
Router(config-dial-peer)# rtp payload-type cisco-codec-gsmamrnb 115
```

The following example shows how to identify the RTP payload type as NTE 99:

```
Router(config-dial-peer)# rtp payload-type nte 99
```

The following example shows how to identify the RTP payload type for the iLBC as 100:

```
Router(config-dial-peer)# rtp payload-type cisco-codec-ilbc 100
```

The following example shows how to identify the RTP payload type as Opus:

```
Router(config-dial-peer)# rtp payload-type opus 126
```

Related Commands

Command	Description
dtmf-relay	Specifies how an H.323 or SIP gateway relays DTMF tones between telephony interfaces and an IP network.

rtp-port

To configure real-time protocol range.

rtp-port range *min-port max-port*

Syntax Description

min port	Minimum port number.
max port	Maximum port number.

Command Default

Default range of 8000–48189 is configured by default.

Command Modes

Global configuration voice service VoIP (conf-voi-serv).

Command History

Release	Modification
Cisco IOS XE 3.11S	The command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Configure rtp-port range to restrict the RTP ports that are used for setting up the VOIP calls on CUBE. The default global RTP port range is 8000–48189. With extended keyword, the range can be 5500–65498.

Examples

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#voice service voip
Router(conf-voi-serv)#rtp-port
Router(conf-voi-serv)#rtp-port ?
  range  port range

Router(conf-voi-serv)#rtp-port ran
Router(conf-voi-serv)#rtp-port range ?
  <8000-48198>  minimum port number
  extended      extended ports

Router(conf-voi-serv)#rtp-port range 8000 ?
  <8000-48198>  maximum port number

Router(conf-voi-serv)#rtp-port range 8000 8012 ?
  <cr>  <cr>

Router(conf-voi-serv)#rtp-port range 8000 8012
Router(conf-voi-serv)#rtp-port range exte
Router(conf-voi-serv)#rtp-port range extended ?
  <5500-65498>  minimum port number extended range

Router(conf-voi-serv)#rtp-port range extended 5510 5512
Warning: Using extended port range of 5510 to 5512 could result in some tcp/udp services
not working properly due to port usage conflicts. Use caution in choosing range.
Router(conf-voi-serv)#
```

Related Commands

Command	Description
allow-connections sip to sip	To allow sip-to-sip connections under voice service VoIP configuration mode for CUBE.
media-address range	To configure the media-address range, which enables the media gateway to allocate the available free port for a given IP address within the address range.

rtp send-recv

To configure a Cisco IOS Session Initiation Protocol (SIP) gateway to establish a bidirectional voice path as soon as it receives a SIP 183 PROGRESS message with Session Description Protocol (SDP), use the **rtp send-recv** command in voice service SIP configuration mode. To configure the gateway to establish a backward-only media cut-through voice path upon receipt of a 183 PROGRESS message with SDP that persists until the call progresses to the connect state, use the **no** form of this command.

rtp send-recv
no rtp send-recv

Syntax Description

This command has no arguments or keywords.

Command Default

A bidirectional voice path is established upon receipt of a 183 PROGRESS message with SDP.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The default behavior on a Cisco IOS SIP gateway is to establish a bidirectional voice path from the moment it receives a SIP 183 PROGRESS message with SDP. However, this can result in clipping on some voice platforms if both parties send audio at the same time, such as during a call setup process when interactive voice response (IVR) and a caller both speak simultaneously. To establish the voice path in the backward direction only until the call is connected, use the **no rtp send-recv** command in voice service SIP configuration mode.

A backward-only voice path operates only during the connection attempt--once a call is connected, the voice path automatically converts to bidirectional sending and receiving of Real-Time Transport Protocol (RTP) packets and RTP control packets (RTCPs). However, if the **no rtp send-recv**command is configured on a SIP gateway, no inband or RFC 2833-based dual tone multifrequency (DTMF) digits can be sent in the forward direction until after the call is connected and the bidirectional voice path is established.

Examples

The following example enables RTP backward-only media cut-through on a Cisco IOS SIP gateway:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# no rtp send-recv
```

rtp-ssrc multiplex

To multiplex Real-Time Transport Control Protocol (RTCP) packets with RTP packets and to send multiple synchronization source in RTP headers (SSRCs) in a RTP session, use the **rtp-ssrc multiplex**command in voice service or dial peer voice configuration mode. To disable the configuration, use the **no** form of this command.

Syntax Available Under Voice Service Configuration Mode
rtp-ssrc multiplex
no rtp-ssrc multiplex

Syntax Available Under Dial Peer Voice Configuration Mode
rtp-ssrc multiplex [**system**]
no rtp-ssrc multiplex [**system**]

Syntax Description

system	Uses the system value. This is the default value.

Command Default

Under voice service configuration mode, the **rtp-ssrc multiplex** command is not enabled and hence there is no interoperation with Cisco TelePresence System (CTS).

At the dial-peer level, the **rtp-ssrc multiplex** command uses the global configuration level settings.

Command Modes

Voice service configuration (conf-voi-serv)

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

The **rtc-ssrc multiplex** command is used for the interoperation with CTS.

Examples

The following example shows how to multiplex RTCP packets with RTP packets and send multiple SSRCs in a RTP session:

```
Router# configure terminal
Router(config)# dial-peer voice 234 voip
Router(config-dial-peer)# rtp-ssrc multiplex system
```

rtsp client session history duration

To specify how long to keep Real Time Streaming Protocol (RTSP) client history records in memory, use the **rtsp client session history duration** command in global configuration mode. To reset to the default, use the **no** form of this command.

rtsp client session history duration *minutes*
no rtsp client session history duration

Syntax Description

minutes	Duration, in minutes, to keep the record. Range is from 1 to 10000. Default is 10.

Command Default

10 minutes

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. This release does not support any other Cisco platforms.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Examples

The following example sets the duration for the RTSP session history to 500 minutes:

```
rtsp client session history duration 500
```

Related Commands

Command	Description
call application voice load	Allows reload of an application that was loaded via the MGCP scripting package.
rtsp client session history records	Specifies the number of RTSP client session history records kept during the session.
show call application voice	Displays all TCL or MGCP scripts that are loaded.

Command	Description
show rtsp client session	Displays cumulative information about the RTSP session records.

rtsp client rtpsetup enable

To configure a router to send the IP address in a Real Time Streaming Protocol (RTSP) setup message, use the **rtsp client rtpsetup enable** command in global configuration mode. To disable the configuration, use the **no** form of this command.

rtsp client rtpsetup enable
no rtsp client rtpsetup enable

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure a router to send the IP address in an RTSP setup message:

```
Router# configure terminal
Router(config)# rtsp client rtpsetup enable
```

Related Commands

Command	Description
rtsp client session history duration	Specifies how long to keep RTSP client history records in memory.
rtsp client timeout connect	Sets the number of seconds allowed for the router to establish a TCP connection to an RTSP server.

rtsp client session history records

To configure the number of records to keep in the Real Time Streaming Protocol (RTSP) client session history, use the **rtsp client session history records** command in global configuration mode. To reset to the default, use the **no** form of this command.

rtsp client session history records *number*
no rtsp client session history records *number*

Syntax Description

number	Number of records to retain in a session history. Range is from 1 to 100000. Default is 50.

Command Default

50 records

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. This release does not support any other Cisco platforms.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Examples

The following example specifies that a total of 500 records are to be kept in the RTSP client history:

```
rtsp client session history records 500
```

Related Commands

Command	Description
call application voice load	Allows reload of an application that was loaded via the MGCP scripting package.
rtsp client session history duration	Specifies the how long the RTSP is kept during the session.
show call application voice	Displays all Tcl or MGCP scripts that are loaded.

rtsp client timeout connect

To set the number of seconds allowed for the router to establish a TCP connection to a Real -Time Streaming Protocol (RTSP) server, use the **rtsp client timeout connect**command in global configuration mode. To reset to the default, use the **no** form of this command.

rtsp client timeout connect *seconds*
no rtsp client timeout connect

Syntax Description

seconds	How long, in seconds, the router waits to connect to the server before timing out. Range is 1 to 20.

Command Default

3 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

This command determines when the router abandons its attempt to connect to an RTSP server and declares a timeout error, if a connection cannot be established after the specified number of seconds.

Examples

The following example sets the connection timeout to 10 seconds:

```
rtsp client timeout connect 10
```

Related Commands

Command	Description
rtsp client session history records	Sets the maximum number of records to store in the RTSP client session history.
rtsp client timeout message	Sets the number of seconds that the router waits for a response from an RTSP server.

rtsp client timeout message

To set the number of seconds that the router waits for a response from a Real -Time Streaming Protocol (RTSP) server, use the **rtsp client timeout message**command in global configuration mode. To reset to the default, use the **no** form of this command.

rtsp client timeout message *seconds*
no rtsp client timeout message

Syntax Description

seconds	How long, in seconds, the router waits for a response from the server after making a request. Range is 1 to 20.

Command Default

3 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

This command sets how long the router waits for the RTSP server to respond to a request before declaring a timeout error.

Examples

The following example sets the request timeout to 10 seconds:

```
rtsp client timeout message 10
```

Related Commands

Command	Description
rtsp client session history records	Sets the maximum number of records to store in the RTSP client session history.
rtsp client timeout connect	Sets the number of seconds allowed for the router to establish a TCP connection to an RTSP server.

rule (ENUM configuration)

To define a rule for an ENUM match table, use the **rule** command in ENUM configuration mode. To delete the rule, use the **no**form of this command.

rule *rule-number preference /match-pattern /replacement-rule /domain-name*
rule *rule-number preference /match-pattern /replacement-rule /domain-name*

Syntax Description

rule -number	Assigns an identification number to the rule. Range is from 1 to 2147483647.
preference	Assigns a preference value to the rule. Range is from 1 to 2147483647. Lower values have higher preference.
/ *match -pattern*	Stream editor (SED) expression used to match incoming call information. The slash "/" is a delimiter in the pattern.
/ *replacement -rule*	SED expression used to repla ce match-pattern in the call information. The slash "/" is a delimiter in the pattern.
/ *domain -name*	Domain name to be used while the query to the DNS server is sent.

Command Default

No default behavior or values

Command Modes

ENUM configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The table below shows examples of match patterns, input strings, and result strings for the rule (voice translation-rule) command.

Table 6: Match Patterns, Input Strings and Result Strings

Match Pattern	Replacement Pattern	Input String	Result String	Description
/^.*/	//	4085550100	--	Any string to null string.
/^456\(.*\)/	/555\1/	5550100	5550100	Match from the beginning of the input string.
/\(^...\)456\(...\)/	/\1555\2/	408555010	4085550100	Match from the middle of the input string.
/\(.*\)0100/	/\0199/	4085550100	4085550199	Match from the end of the input string.
/^1#\(.*\)/	/\1/	1#2345	2345	Replace match string with null string.
/^408...\(8333\)/	/555\1/	4085550100	5550100	Match multiple patterns.

Rules are entered in any order, but their preference number determines the sequence in which they are used for matching against the input string, which is a called number. A lower preference number is used before a higher preference number.

If a match is found, the input string is modified according to the replacement rule, and the E.164 domain name is attached to the modified number. This longer number is sent to a Domain Name System (DNS) server to determine a destination for the call. The server returns one or more URLs as possible destinations. The originating gateway tries to place the call using each URL in order of preference. If a call cannot be completed using any of the URLs, the call is disconnected.

Examples

The following example defines ENUM rule number 3 with preference 2. The beginning of the call string is checked for digits 9011; when a match is found, 9011 is replaced with 1408 and the call is sent out as an e164.arpa number.

```
Router(config)# voice enum-match-table number
 Router(config-enum)# rule 3 2 /^9011\(.*\)//+1408\1/ arpa
```

Related Commands

Command	Description
show voice enum-match-table	Displays the configuration of a voice ENUM match table.
test enum	Tests the ENUM rule.
voice enum-match-table	Initiates the definition of a voice ENUM match table.

rule (SIP Profile Configuration)

To tag rules in SIP profile configurations, use **rule** command in voice class sip-profiles configuration mode. To remove a rule from a SIP profile configuration, use **no** form this command.

rule before *tag* **request** *method* {**sdp-header** | **sip-header**} *header-name* {**add** | **copy** | **modify** | **remove**} *string*
rule before *tag* **response** *method* {**sdp-header** | **sip-header**} *header-name* {**add** | **copy** | **modify** | **remove**} *string*
no rule *tag*

Syntax Description

tag	Specifies the rule number. Range is 1 to 1073741823.
before	(Optional) Specifies the position of the new rule in the SIP profile configuration.
request	Modifies a SIP profile to add, copy, modify, or remove a SIP or SDP header value from a SIP request message.
response	Modifies a SIP profile to add, copy, modify, or remove a SIP or SDP header value from a SIP response message.
method	Type of message to be added, modified, or removed. It can be one of the following values: • **ack** --SIP acknowledgment message. • **any** --Any SIP message. • **bye** --SIP BYE message. • **cancel** --SIP CANCEL message. • **comet** --SIP COMET message. • **info** --SIP INFO message. • **invite** --The first SIP INVITE message. • **notify** --SIP NOTIFY message. • **options** --SIP OPTIONS message. • **prack** --SIP PRACK message. • **publish** --SIP PUBLISH message. • **refer** --SIP REFER message. • **register** --SIP REGISTER message. • **reinvite** --SIP REINVITE message. • **subscribe** --SIP SUBSCRIBE message. • **update** --SIP UPDATE message.

sdp-header	Specifies an SDP header.
sip-header	Specifies a SIP header.
header-name	SDP or SIP header name.
add	Adds a header.
copy	Copies a header.
modify	Modifies a header.
remove	Removes a header.
string	String to be added, copied, modified, or removed as a header. **Note** If you use the **copy** keyword, you must provide a matching pattern followed by the variable name for the *string* argument.

Command Default

SIP profile configurations are in non-rule format.

Command Modes

Voice class configuration (config-class)

Command History

Release	Modification
15.5(2)T, Cisco IOS XE Release 3.15S	This command was introduced.

Usage Guidelines

This command tags the rules in a SIP profile configuration. The **before** keyword is used to introduce a new command at any position in the existing set of rules in a SIP profile configuration.

Example

Example for tagging a SIP profile rule

```
Device(config)# voice class sip-profiles 10
Device(config-class)# rule 1 request invite sip-header contact copy "(.*)" u01
```

Example for inserting a rule in an existing SIP profile

```
Device(config)# voice class sip-profiles 10
Device(config-class)# rule before 1 request invite sip-header contact copy "(.*)" u01
```

Related Commands

Command	Description
request	Modifies a SIP profile to add, copy, modify, or remove a SIP or SDP header value from a SIP request message.
response	Modifies a SIP profile to add, copy, modify, or remove a SIP or SDP header value from a SIP response message.

rule (voice translation-rule)

To define a translation rule, use the **rule** command in voice translation-rule configuration mode. To delete the translation rule, use the **no**form of this command.

Match and Replace Rule
rule *precedence* */match-pattern/* */replace-pattern/* [{**type** *match-type* *replace-type*[{**plan** {*match-type* *replace-type*}}]}]
no rule *precedence*

Reject Rule
rule *precedence* **reject** */match-pattern/* {**type** *match-type* [{**plan** *match-type*}]}
no rule *precedence*

Syntax Description

precedence	Priority of the translation rule. Range is from 1 to 15.
/ *match -pattern* /	Stream editor (SED) expression used to match incoming call information. The slash '/' is a delimiter in the pattern.
/ *replace -pattern* /	SED expression used to replace the match pattern in the call information. The slash '/' is a delimiter in the pattern.
type *match -type* *replace-type*	(Optional) Number type of the call. Valid values for the *match-type* argument are as follows: • **abbreviated** --Abbreviated representation of the complete number as supported by this network. • **any** --Any type of called number. • **international** --Number called to reach a subscriber in another country. • **national** --Number called to reach a subscriber in the same country, but outside the local network. • **network** --Administrative or service number specific to the serving network. • **reserved** --Reserved for extension.**subscriber**--Number called to reach a subscriber in the same local network. • **unknown** --Number of a type that is unknown by the network. Valid values for the *replace-type* argument are as follows: • **abbreviated** --Abbreviated representation of the complete number as supported by this network. • **international** --Number called to reach a subscriber in another country. • **national** --Number called to reach a subscriber in the same country, but outside the local network.

type *match -type replace-type*(continued)	• **network** --Administrative or service number specific to the serving network. • **reserved** --Reserved for extension. • **subscriber** --Number called to reach a subscriber in the same local network. • **unknown** --Number of a type that is unknown by the network.
plan *match -type replace-type*	(Optional) Numbering plan of the call. Valid values for the *match-type* argument are as follows: • **any** --Any type of dialed number. • **data** • **ermes** • **isdn** • **national** --Number called to reach a subscriber in the same country, but outside the local network. • **private** • **reserved** --Reserved for extension. • **telex** • **unknown** --Number of a type that is unknown by the network. Valid values for the *replace-type* argument are as follows: • **data** • **ermes** • **isdn** • **national** --Number called to reach a subscriber in the same country, but outside the local network. • **private** • **reserved** --Reserved for extension. • **telex** • **unknown** --Number of a type that is unknown by the network.
reject	The match pattern of a translation rule is used for call-reject purposes.

Command Default

No default behavior or values

Command Modes

Voice translation-rule configuration

Command History

Release	Modification
12.2(11)T	This command was introduced with a new syntax in voice-translation-rule configuration mode.
15.1(4)M	This command was introduced with an increase in the maximum value of the precidence variable from 15 to 100.

Usage Guidelines

Note Use this command in conjunction after the **voice translation-rule** command. An earlier version of this command uses the same name but is used after the **translation-rule** command and has a slightly different command syntax. In the older version, you cannot use the square brackets when you are entering command syntax. They appear in the syntax only to indicate optional parameters, but are not accepted as delimiters in actual command entries. In the newer version, you can use the square brackets as delimiters. Going forward, we recommend that you use this newer version to define rules for call matching. Eventually, the **translation-rule**command will not be supported.

A translation rule applies to a calling party number (automatic number identification [ANI]) or a called party number (dialed number identification service [DNIS]) for incoming, outgoing, and redirected calls within Cisco H.323 voice-enabled gateways.

Number translation occurs several times during the call routing process. In both the originating and terminating gateways, the incoming call is translated before an inbound dial peer is matched, before an outbound dial peer is matched, and before a call request is set up. Your dial plan should account for these translation steps when translation rules are defined.

The table below shows examples of match patterns, input strings, and result strings for the rule (voice translation-rule) command.

Table 7: Match Patterns, Input Strings and Result Strings

Match Pattern	Replacement Pattern	Input String	Result String	Description
/^.*/	//	4085550100		Any string to null string.
//	//	4085550100	4085550100	Match any string but no replacement. Use this to manipulate the call plan or call type.
/\(^...\)456\(...\)/	/\1555\2/	4084560177	4085550177	Match from the middle of the input string.
/\(.*\)0120/	/\10155/	4081110120	4081110155	Match from the end of the input string.
/^1#\(.*\)/	/\1/	1#2345	2345	Replace match string with null string.
/^408...\(8333\)/	/555\1/	4087770100	5550100	Match multiple patterns.
/1234/	/00&00/	5550100	55500010000	Match the substring.
/1234/	/00\000/	5550100	55500010000	Match the substring (same as &).

The software verifies that a replacement pattern is in a valid E.164 format that can include the permitted special characters. If the format is not valid, the expression is treated as an unrecognized command.

The number type and calling plan are optional parameters for matching a call. If either parameter is defined, the call is checked against the match pattern and the selected type or plan value. If the call matches all the conditions, the call is accepted for additional processing, such as number translation.

Several rules may be grouped together into a translation rule, which gives a name to the rule set. A translation rule may contain up to 15 rules. All calls that refer to this translation rule are translated against this set of criteria.

The precedence value of each rule may be used in a different order than that in which they were typed into the set. Each rule’s precedence value specifies the priority order in which the rules are to be used. For example, rule 3 may be entered before rule 1, but the software uses rule 1 before rule 3.

The software supports up to 128 translation rules. A translation profile collects and identifies a set of these translation rules for translating called, calling, and redirected numbers. A translation profile is referenced by trunk groups, source IP groups, voice ports, dial peers, and interfaces for handling call translation.

Examples

The following example applies a translation rule. If a called number starts with 5550105 or 70105, translation rule 21 uses the rule command to forward the number to 14085550105 instead.

```
Router(config)# voice translation-rule 21
 Router(cfg-translation-rule)# rule 1 /^5550105/ /14085550105/
 Router(cfg-translation-rule)# rule 2 /^70105/ /14085550105/
```

In the next example, if a called number is either 14085550105 or 014085550105, after the execution of translation rule 345, the forwarding digits are 50105. If the match type is configured and the type is not "unknown," dial-peer matching is required to match the input string numbering type.

```
Router(config)# voice translation-rule 345
 Router(cfg-translation-rule)# rule 1 /^14085550105/ /50105/ plan any national
 Router(cfg-translation-rule)# rule 2 /^014085550105/ /50105/ plan any national
```

Related Commands

Command	Description
show voice translation-rule	Displays the parameters of a translation rule.
voice translation-rule	Initiates the voice translation-rule definition.