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. To disable random-contact information, use the **no** form of this command.

random-contact

no random-contact

Syntax Description

This command has no arguments or keywords.

Command Default

Outgoing INVITE messages are populated with clear-contact information.

Command Modes

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

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

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
```

Related Commands

Command	Description
credentials (sip ua)	Sends a SIP registration message from a Cisco Unified Border Element in the UP state.

Command	Description
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. To disable validation, use the **no** form of this command.

random-request-uri validate

no random-request-uri validate

Syntax Description

This command has no keywords or arguments.

Command Default

Validation is disabled.

Command Modes

Voice service voip sip configuration (conf-serv-sip)

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

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
```

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. To disable reason-header override, use the **no** form of this command.

reason-header override

no reason-header override

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

SIP UA configuration

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.

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
```

Related Commands

Command	Description
sip-ua	Enables SIP UA configuration commands.

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.

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. To disable the handling of 3*xx* redirect messages, use the **no** form of this command.

redirection

no redirection

Syntax Description

This command has no arguments or keywords.

Command Default

Redirection is enabled.

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

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
```

Related Commands

Command	Description
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP UA status.

refer-ood enable

To enable out-of-dialog refer (OOD-R) processing, use the **refer-ood enable** command in SIP user-agent configuration mode. To disable OOD-R, use the **no** form of this command.

refer-ood enable [*request-limit*]

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.

Command Default

OOD-R processing is disabled.

Command Modes

SIP UA configuration (config-sip-ua)

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

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
```

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.

Command	Description
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. To enable dial peer lookup and the Refer-To header modification, use the **no** form of this command.

referto-passing

no referto-passing

Syntax Description

This command has no arguments or keywords.

Command Default

Dial peer lookup is performed. The Refer-To header is modified to include the address of the Cisco UBE 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)

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

By default, while passing across the REFER message, the Cisco UBE replaces the host portion of the Refer-To header with the address of the Cisco UBE 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 Cisco UBE from overwriting the Refer-To header even if address hiding is enabled. This command also disables dial peer lookup when the Cisco UBE passes across the REFER message.

Examples

The following example shows how to enable REFER message pass-through on the Cisco UBE 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
```

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.

Command	Description
supplementary-service sip refer	Enables REFER message pass-through on the Cisco UBE.

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]**

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 to 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 to 65535. Default is 3600.
random-contact	(Optional) Specifies the Random String Contact header used to identify the registration session.
refresh-ratio *ratio-percentage*	(Optional) Specifies the registration refresh ratio, in percentage. Range is 1 to 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 User Datagram Protocol 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 specifying DHCP or if configuring multiple registrars. **Note** You cannot configure any other optional settings once you enter the **secondary** keyword--specify all other settings first.

Command Default

Registration is disabled.

Command Modes

SIP UA configuration (config-sip-ua)

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. Additionally, the **aor-domain** keyword and the **tls** option for the tcp keyword were removed.

Release	Modification
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.

Usage Guidelines

Use the **registrar dhcp** or **registrar** *registrar-server-address* command to enable the gateway to register E.164 telephone 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 (Cisco UBEs), 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
```

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 localhost 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.

Command	Description
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.

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.

Command	Description
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. To disable the configuration, use the **no** form of this command.

registration passthrough [static] [**rate-limit** [**expires** *value*] [**fail-count** *value*]] [**registrar-index** [*index*]]

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.

Command Default

SIP registration pass-through options are not configured.

Command Modes

Service SIP configuration (conf-serv-sip)

Command History

Release	Modification
15.1(3)T	This command was introduced.

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
```

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. To reset to the default, use the **no** form of this command.

rel1xx {**supported** *value*| **require** *value*| **disable**}

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.

Command Default

supported with the 100rel value

Command Modes

SIP 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 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.

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
```

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. To disable Remote-Party-ID translation, use the no form of this command.

remote-party-id

no remote-party-id

Syntax Description

This command has no arguments or keywords.

Command Default

Remote-Party-ID translation is enabled

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

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 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
```

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.

Command	Description
debug voice ccapi in out	Enables tracing the execution path through the call control API.

remote-url

To configure the url the application that wil be used by the service provider, use the **remote-url** command. The provider will use this url to authenticate and commnunicate 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.
url	Specifies the URL that the service provider will be using in the messages.

Command Default

No default behavior or values.

Command Modes

uc wsapi mode

Command History

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

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.

```
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://209.133.85.47:8090/my_route_control
```

Related Commands

Command	Description
provider	Enables a provider service.
source-address	Specifies the IP address of the provider.
uc wsapi	Enters Cisco Unified Communication IOS services configuration mode.

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.

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. 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

no reset timer expires 183

Syntax Description

183	Specifies resetting of the expires timer upon receipt of SIP 183 Session In Progress messages.

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)

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.

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
```

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.

Release	Modification
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.

Command	Description
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.
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. To reset to the default, use the no form of this command.

retry bye *number*

no retry bye *number*

Syntax Description

number	Number of BYE retries. Range is from 1 to 10. The default is 10.

Command Default

10 retries

Command Modes

SIP UA 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 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.

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
```

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. To reset to the default, use the **no** form of this command.

retry cancel *number*

no retry cancel *number*

Syntax Description

number	Number of CANCEL retries. Range is from 1 to 10. Default is 10.

Command Default

10 retries

Command Modes

SIP UA 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 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.

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
```

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.
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 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.

Command	Description
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. To reset to the default, use the **no** form of this command.

retry invite *number*

no retry invite *number*

Syntax Description

number	Number of INVITE retries. Range is from 1 to 10. Default is 6.

Command Default

6 retries

Command Modes

SIP UA 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 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.

Usage Guidelines

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

When configuring SIP using SIP user-agent configuration commands such as the **retry invite** command, the use of the default values for the commands causes the rotary function to not take effect. The rotary function is when you set up more than one VoIP dial peer for the same destination pattern, and the dial peers are assigned to different targets. Assign different targets so that if the call cannot be set up with the first dial peer (preference one), the next dial peer can be tried.

To use the rotary function within SIP, set the retry value for the SIP **retry invite**command to 4 or less.

Examples

The following example sets the number of invite retries to 5.

```
sip-ua
 retry invite 5
```

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.

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.

Command	Description
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. To reset to the default, use the **no** form of this command.

retry notify *number*

no retry notify

Syntax Description

number	Number of notify message 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)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.

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 anotify message to be retransmitted 10 times:

```
Router(config)# sip-ua
Router(config-sip-ua)# retry notify 10
```

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 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. To reset to the default, use the **no** form of this command.

retry prack *number*

no retry prack

Syntax Description

number	Number of PRACK 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. 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.

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 aPRACK request to be retransmitted 9 times:

```
Router(config)# sip-ua
Router(config-sip-ua)# retry prack 9
```

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. To reset to the default, use the **no** form of this command.

retry refer *number*

no retry refer

Syntax Description

number	Number of Refer request 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(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.

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 aRefer request to be retransmitted 10 times:

```
Router(config)# sip-ua
Router(config-sip-ua)# retry refer 10
```

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. To reset this number to the default, use the **no** form of this command.

retry register *retries* [**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.

Command Default

The gateway sends 6 retries.

Command Modes

SIP UA configuration (config-sip-ua)

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.

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
```

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. To reset to the default, use the **no** form of this command.

retry rel1xx *number*

no retry rel1xx

Syntax Description

number	Number of reliable 1*xx* retries. Range is from 1 to 10. Default is 6.

Command Default

6 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. 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

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
```

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. To reset to the default, use the no form of this command.

retry response *number*

no retry response

Syntax Description

number	Number of response retries. Range is from 1 to 10. Default is 6.

Command Default

6 retries

Command Modes

SIP UA 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 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.

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
```

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. To reset to the default, use the no form of this command.

retry subscribe *number*

no retry subscribe *number*

Syntax Description

number	Number of SUBSCRIBE retries. Range is 1 to 10. Default is 10.

Command Default

10 retries

Command Modes

SIP UA configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

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
```

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 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.

Command	Description
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.
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.

Command	Description
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.
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.

Command	Description
device -id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max -connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response -timeout	Configures the maximum time to wait for a response from a server.
retry -delay	Sets the time between attempts to connect with the settlement provider.
session -timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement 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.
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 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.
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.

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.

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*} [**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*} [**comfort-noise** {**13**| **19**}]

Syntax Description

cisco-cas-payload *number*	Cisco channel-associated signaling (CAS) RTP payload. Range: 96 to 127. Default: 123.
cisco-clear-channel *number*	Cisco clear-channel RTP payload. Range: 96 to 127. Default: 125.
cisco-codec-aacld *number*	Cisco MPEG-4 Advanced Audio Codec - Low Delay (AAC_LD) codec. Range: 96 to 127. Default: 114.
cisco-codec-fax-ack *number*	Cisco codec fax acknowledge. Range: 96 to 127. Default: 97.
cisco-codec-fax-ind *number*	Cisco codec fax indication. Range: 96 to 127. Default: 96.
cisco-codec-gsmamrnb *number*	Cisco Global System for Mobile Adaptive Multi-Rate Narrow Band (GSMAMR-NB) codec. Range: 96 to 127. Default: 117.
cisco-codec-ilbc *number*	Cisco internet Low Bitrate Codec (iLBC) codec. Range: 96 to 127. Default: 116.
cisco-codec-isac *number*	Cisco internet Speech Audio Codec (iSAC) codec. Range: 96 to 127. Default: 124.
cisco -codec-video-h263+ *number*	RTP video codec H.263+ payload type. Range: 96 to 127. Default: 118.

cisco -codec-video-h264 *number*	RTP video codec H.264 payload type. Range: 96 to 127. Default: 119.
cisco-fax-relay *number*	Cisco fax relay. Range: 96 to 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 to 127. Default: 121.
lmr-tone *number*	LMR payload type. Range: 96 to 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 to 117. Default: 100.
nte *number*	A named telephone event (NTE). Range: 96 to 127. Default: 101.
nte-tone *number*	RFC-2833 tone payload type. Range 96 to 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 Internet Engineering Task Force (IETF) Audio/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.

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.
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.

Usage Guidelines

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 hard-coded with Cisco-proprietary meanings. Do not use the following numbers, which have preassigned values: 96, 97, 100, 117, 121 to 123, and 125 to 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
```

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 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.

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.
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 1: 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.

Command	Description
voice enum-match-table	Initiates the definition of a voice ENUM match table.

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 2: 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.

Match Pattern	Replacement Pattern	Input String	Result String	Description
/\(.*\)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.