

call fallback through called-number (dial peer)

- call fallback, on page 3
- call fallback active, on page 5
- call fallback cache-size, on page 7
- call fallback cache-timeout, on page 9
- call fallback expect-factor, on page 11
- call fallback icmp-ping, on page 13
- call fallback icmp-ping (dial peer), on page 15
- call fallback instantaneous-value-weight, on page 17
- call fallback jitter-probe dscp, on page 19
- call fallback jitter-probe num-packets, on page 21
- call fallback jitter-probe precedence, on page 22
- call fallback jitter-probe priority-queue, on page 24
- call fallback key-chain, on page 26
- call fallback map address-list, on page 28
- call fallback map subnet, on page 30
- call fallback monitor, on page 32
- call fallback probe-timeout, on page 34
- call fallback reject-cause-code, on page 36
- call fallback threshold delay loss, on page 43
- call fallback threshold icpif, on page 45
- call fallback wait-timeout, on page 47
- call filter match-list, on page 48
- call forward all, on page 49
- call forward cancel, on page 52
- call history max, on page 54
- call-history-mib, on page 55
- call-progress-analysis, on page 57
- call language voice, on page 58
- call language voice load, on page 59
- call leg dump event-log, on page 60
- call leg event-log, on page 61
- call leg event-log dump ftp, on page 63
- call leg event-log errors-only, on page 66

- call leg event-log max-buffer-size, on page 67
- call leg history event-log save-exception-only, on page 68
- callmonitor, on page 69
- call preserve, on page 70
- call-route, on page 73
- call-router h323-annexg, on page 75
- call-routing hunt-scheme, on page 76
- call rscmon update-timer, on page 77
- call rsvp-sync, on page 78
- call rsvp-sync resv-timer, on page 79
- call service stop, on page 81
- call spike, on page 83
- call start, on page 85
- call threshold global, on page 88
- call threshold interface, on page 90
- call threshold poll-interval, on page 93
- call treatment action, on page 95
- call treatment cause-code, on page 97
- call treatment isdn-reject, on page 99
- call treatment on, on page 101
- call-waiting, on page 103
- called-number (dial peer), on page 104

call fallback

To enable a call request to fall back to a specific dial peer in case of network congestion, use the **callfallback** command in dial peer configuration mode. To disable PSTN fallback for a specific dial peer, use the **no** form of this command.

call fallback
no call fallback

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default if the **callfallbackactive** command is enabled in global configuration mode

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The PSTN Fallback feature and enhancements were introduced on Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.

Usage Guidelines

Disabling the **callfallback** command for a dial peer causes the call fallback subsystem not to fall back to the specified dial peer. Disabling the command is useful when internetworking fallback capable H.323 gateways with the Cisco CallManager or third-party equipment that does not run fallback. Connected calls are not affected by this feature.

Examples

The following example disables a PSTN fallback for a specific dial peer:

```
no call fallback
```

Related Commands

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

Command	Description
call fallback jitter-probe num-packets	Specifies the number of packets in a jitter probe that are used to determine network conditions.
call fallback jitter-probe precedence	Specifies the priority of the jitter-probe transmission.
call fallback jitter-probe priority-queue	Assigns a priority queue for jitter-probe transmissions.
call fallback key-chain	Specifies use of MD5 authentication for sending and receiving SAA probes.
call fallback map address-list	Specifies that the call fallback router keep a cache table by IP addresses of distances for several destination peers that are sitting behind the router.
call fallback map subnet	Specifies that the call fallback router keep a cache table by subnet addresses of distances for several destination peers that are sitting behind the router.
call fallback probe-timeout	Sets the timeout for an SAA probe for call fallback purposes.
call fallback threshold delay loss	Specifies that the call fallback threshold use only packet delay and loss values.
call fallback threshold icpif	Specifies that call fallback use the ICPIF threshold.
dial-peer voice number	Enters dial peer configuration mode.
show call fallback config	Displays the call fallback configuration.

call fallback active

To enable the Internet Control Message Protocol (ICMP)-ping or Service Assurance Agent (SAA) (formerly Response Time Reporter [RTR]) probe mechanism for use with the dial-peer **monitorprobe** or voice-port **busyoutmonitorprobe** commands, use the **callfallbackactive** command in global configuration mode. To disable these probe mechanisms, use the **no** form of this command.

call fallback active [**icmp-ping** | **rtr**]
no call fallback active [**icmp-ping** | **rtr**]

Syntax Description

icmp-ping	Uses ICMP pings to monitor the IP destinations.
rtr	Uses SAA (formerly RTR) probes to monitor the IP destinations. SAA (RTR) probes are the default.

Command Default

This command is disabled by default. If the command is entered without an optional keyword, the default is RTR.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented for Cisco 7500 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The **callfallbackactive** command creates and maintains a consolidated cache of probe results for use by the dial-peer **monitorprobe** or voice-port **busyoutmonitorprobe** commands.

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

Use the**callfallbackthresholddelayloss** or **callfallbackthresholdicpif** command to set the threshold parameters.

Connected calls are not affected by this command.



Caution The **callfallbackactiveicmp-ping** command must be entered before the **callfallbackicmp-ping** command can be used. If you do not enter this command first, the **callfallbackicmpping** command will not work properly.

Note The Cisco SAA functionality in Cisco IOS software was formerly known as Response Time Reporter (RTR). The command-line interface still uses the keyword **rtr** for configuring RTR probes, which are now actually SAA probes.

Examples

The following example enables the **callfallbackactive**command and globally enables ICMP pinging to probe target destinations. The second command specifies values for the ping packets:

```
Router(config)# call fallback active icmp-ping
Router(config)# call fallback icmp-ping codec g729 interval 10 loss 10
```

Related Commands

Command	Description
call fallback cache-size	Specifies the call fallback cache size for network traffic probe entries.
call fallback cache-timeout	Specifies the time after which the cache entries of network conditions are purged.
call fallback instantaneous-value-weight	Specifies the call fallback subsystem to take an average from the last two cache entries for call requests.
call fallback jitter-probe num-packets	Specifies the number of packets in a jitter probe that are used to determine network conditions.
call fallback jitter-probe precedence	Specifies the priority of the jitter-probe transmission.
call fallback jitter-probe priority-queue	Assigns a priority queue for jitter-probe transmissions.
call fallback key-chain	Specifies use of MD5 authentication for sending and receiving SAA probes.
call fallback map address-list	Specifies that the call fallback router keep a cache table by IP addresses of distances for several destination peers that are sitting behind the router.
call fallback map subnet	Specifies that the call fallback router keep a cache table by subnet addresses of distances for several destination peers that are sitting behind the router.
call fallback probe-timeout	Sets the timeout for an SAA probe for call fallback purposes.
call fallback threshold delay loss	Specifies that the call fallback threshold use only packet delay and loss values.
call fallback threshold icpif	Specifies that call fallback use the ICPIF threshold.
dial-peer voice number	Enters dial peer configuration mode.

call fallback cache-size

To specify the call fallback cache size for network traffic probe entries, use the **callfallbackcachesize** command in global configuration mode. To restore the default value, use the **no** form of this command.

call fallback cache-size *number*
no call fallback cache-size

Syntax Description

number	Cache size, in number of entries. Range is from 1 to 256. The default is 128.

Command Default

128 entries

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced..
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were introduced on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The cache size can be changed only when the **callfallbackactive** command is not enabled.

The overflow process deletes up to one-fourth of the cache entries to allow for additional calls beyond the specified cache size. The cache entries chosen for deletion are the oldest entries in the cache.

If the cache size is left unchanged, it can be changed only when fallback is off. Use the **no** form of the **callfallback** command to turn fallback off.

Examples

The following example specifies 120 cache entries:

```
Router(config)#
call fallback cache-size 120
```

Related Commands

Command	Description
call fallback	Enables a call request to fall back to a specific dial peer in case of network congestion
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.

Command	Description
call fallback cache-timeout	Specifies the time after which the cache entries of network conditions are purged.
show call fallback cache	Displays the current ICPIF estimates for all IP addresses in the cache.
show call fallback config	Displays the call fallback configuration.

call fallback cache-timeout

To specify the time after which the cache entries of network conditions are purged, use the **callfallbackcachetimeout** command in global configuration mode. To disable the **callfallbackcache-timeout** command, use the **no** form of this command.

call fallback cache-timeout *seconds*
no call fallback cache-timeout

Syntax Description

seconds	Cache timeout value, in seconds. Range is from 1 to 2147483. The default is 600.

Command Default

600 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Enabling the **callfallbackcachetimeout** command sends a Service Assurance Agent (SAA) probe out to the network to determine the amount of congestion in terms of configured thresholds. The network condition is based upon delay and loss, or Calculated Planning Impairment Factor (ICPIF) thresholds. Use the**callfallbackthresholddelayloss** or **callfallbackthresholdicpif** command to set the threshold parameters.

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

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

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

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

Examples

The following example specifies an elapsed time of 1200 seconds before the cache times out:

```
Router(config)# call fallback cache-timeout 1200
```

Related Commands

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

call fallback expect-factor

To set a configurable value by which the call fallback expect factor feature will be activated, use the **callfallbackexpect-factor**command in global configuration mode. To disable the expect factor, use the **no** form of this command.

call fallback expect-factor *value*
no call fallback expect-factor

Syntax Description

value	Configures the expect-factor A. Range: 0 to 20. Default: 10.

Command Default

No value for the expect-factor is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(3)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The expect-factor is the level of expected voice quality that the user may have during a call. For example, you expect higher voice quality from a call on your home than on your cell phone. The expect-factor is a subjective value determined by the local administrators.

Call fallback is used by the software to generate a series of probes across an IP network to help make a Impairment/Calculated Impairment Planning Factor (ICPIF) calculation. The value calculated by the probes, ICPIF, is modified by the configured expect factor using the following formula:

ICPIF = Idd + Ie-A

Idd represents the impairment due to end-end delay, Ie, represents the impairment due to packet loss and the impact of the codec being used on the call, and A represents the expect-factor value. The expect-factor is the value to be subtracted from the calculated ICPIF value. This expect factor is known as the Advantage Factor (A) as specified in G.107 and takes into account the user's expected level of voice quality based upon the type of call being made.

Examples

The following example shows the **callfallbackexpect-factor**command and the **callfallbackthresholdicpicf** command being configured. A calculated ICPIF value of 20 based on Idd and Ie from the probes set on a IP network would not activate the call fallback feature in this configuration. Even though the calculated ICPIF value of 20 exceeds the configured threshold of 10, subtraction of the expect-value of 15 would leave a value of 5, which is below the threshold value.

```
Router(config)# call fallback expect-factor 15
Router(config)# call fallback threshold icpif 10
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers.
call fallback cache-size	Specifies the call fallback cache size for network traffic probe entries.
call fallback cache-timeout	Specifies the time after which the cache entries of network conditions are purged.
call fallback instantaneous-value-weight	Configures the call fallback subsystem to take an average from the last two cache entries for call requests.
call fallback jitter-probe num-packets	Specifies the number of packets in a jitter probe that are used to determine network conditions.
call fallback jitter-probe precedence	Specifies the priority of the jitter-probe transmission.
call fallback jitter-probe priority-queue	Assigns a priority queue for jitter-probe transmissions.
call fallback key-chain	Specifies use of MD5 authentication for sending and receiving SAA probes.
call fallback map address-list	Specifies that the call fallback router keep a cache table by IP addresses of distances for several destination peers that are sitting behind the router.
call fallback map subnet	Specifies that the call fallback router keep a cache table by subnet addresses of distances for several destination peers that are sitting behind the router.
call fallback probe-timeout	Sets the timeout for an SAA probe for call fallback purposes.
call fallback threshold delay loss	Specifies that the call fallback threshold use only packet delay and loss values.
call fallback threshold icpif	Specifies that call fallback use the ICPIF threshold.
dial-peer voice number	Enters dial peer configuration mode.
show call fallback config	Displays the call fallback configuration.

call fallback icmp-ping

To specify Internet Control Message Protocol (ICMP) ping as the method for network traffic probe entries to IP destinations and configure parameters for the ping packets, use the **callfallbackicmp-ping** command in global configuration mode. To restore the default value, use the **no** form of this command.

call fallback icmp-ping[**count** *packets* | **size***bytes*]**interval***seconds*[[**loss** [*percent*]]]**timeout***milliseconds*
no call fallback icmp-ping[**count** *packets* | **size***bytes*]**interval***seconds*[[**loss** [*percent*]]]**timeout***milliseconds*

Syntax Description

count *packets*	(Optional) Number of ping packets that are sent to the destination address.
codec	(Optional) Configures the profile of the SAA probe signal to mimic the packet size and interval of a specific codec type.
codec -type	(Optional) The codec type for the SAA probe signal. Available options are as follows: • **g711a** --G.711 a-law • **g711u** --G.711 mu-law • **g729** --G.729 (the default) • **g729b** --G.729 Annex B
size *bytes*	(Optional) Size (in bytes) of the ping packet. Default is 32.
interval *seconds*	Time (in seconds) between ping packet sets. Default is 5. This number should be higher than the **timeout***milliseconds* value.
loss *percent*	(Optional) Configures the percentage-of-packets-lost threshold for initiating a busyout condition.
timeout *milliseconds*	(Optional) Timeout (in milliseconds) for echo packets. Default is 500.

Command Default

If this command is not configured, Response Time Reporter (RTR) is the probe method used.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(2)T.

Usage Guidelines

The values configured by the global configuration version of the **callfallbackicmp-ping** command are appllied globally for measurements on probes and pings. If the **callfallbackicmp-ping** is configured in dial-peer configuration mode, these values override the global configuration for the specific dial peer.

One of these two commands must be in effect before the **monitorprobeicmp-ping** command can be used. If neither of the **callfallback** commands is in effect, the **monitorprobeicmp-ping** command will not work properly.

Examples

The following example shows how to configure an ICMP ping probe with a G.729 profile to probe the link with an interval value of 10 seconds and a packet-loss threshold of 10 percent:

```
call fallback active icmp-ping
call fallback icmp-ping codec g729 interval 10 loss 10
```

Related Commands

Command	Description
call fallback active	Forces a voice port into the busyout state.
call fallback icmp-ping (dial peer)	Specifies Internet Control Message Protocol (ICMP) ping as the method for network traffic probe entries to IP destinations.
monitor probe icmp-ping	Enables dial-peer status changes based on the results of probes.

call fallback icmp-ping (dial peer)

To specify Internet Control Message Protocol (ICMP) ping as the method for network traffic probe entries to IP destinations, use the **callfallbackicmp-ping** command in dial-peer configuration mode. To restore the default value, use the **no** form of this command.

call fallback [**icmp-ping** | **rtr**]
no call fallback [**icmp-ping** | **rtr**]

Syntax Description

icmp-ping	(Optional) Specifies ICMP ping as the method for monitoring the session target and updating the status of the dial peer.
rtr	(Optional) Specifies that the Response Time Reporter (RTR) probe is the method for monitoring the session target and updating the status of the dial peer.

Command Default

If this command is not entered, the globally configured method is used for measurements.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(11)T	This command was introduced in a release earlier than Cisco IOS Release 12.2(11)T.

Usage Guidelines

The principal use of this command is to specify ICMP ping as the probe method, even though the option for selecting RTR is also available.

If the **callfallbackicmp-ping** command is not entered, the **callfallbackactive** command in global configuration is used for measurements. If the **callfallbackicmp-ping** command is entered, these values override the global configuration.

One of these two commands must be in effect before the **monitorprobeicmp-ping** command can be used. If neither of the **callfallback** commands is in effect, the **monitorprobeicmp-ping** command will not work properly.

Note The Cisco Service Assurance Agent (SAA) functionality in Cisco IOS software was formerly known as Response Time Reporter (RTR). The command-line interface still uses the keyword **rtr** for configuring RTR probes, which are now actually the SAA probes.

Examples

The following example specifies that ICMP ping is used for monitoring the session target IP address and for updating the status of the dial peer:

```
Router(config)#
dial-peer voice 10 voip
Router(config-dial-peer)#
call fallback icmp-ping
```

Related Commands

Command	Description
call fallback	Enables a call request to fall back to a specific dial peer in case of network congestion
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
monitor probe icmp-ping	Specifies that ICMP ping is the method used for probes.
show call fallback config	Displays the call fallback configuration.

call fallback instantaneous-value-weight

To configure the call fallback subsystem to take an average from the last two probes registered in the cache for call requests, use the **callfallbackinstantaneousvalueweight** command in global configuration mode. To return to the default before the average was calculated, use the **no** form of this command.

call fallback instantaneous-value-weight *percent*
no call fallback instantaneous-value-weight

Syntax Description

percent	Instantaneous value weight, in expressed as a percentage. Range is from 0 to 100. The default is 66.

Command Default

66 percent

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

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

Use the **callfallbackinstantaneousvalueweight**command to gradually recover from heavy traffic network conditions. While the system waits for a call, probes update the cache. When a new probe is received, the *percentage* is set and indicates how much the system is to rely upon the new probe and the previous cache entry. If the *percentage*is set to 50 percent, the system enters a cache entry based upon an average from the new probe and the most recent entry in the cache. Call requests use this blended entry to determine acceptance. This allows the call fallback subsystem to keep conservative measures of network congestion.

The configured *percentate*applies to the new probe first. If the **callfallbackinstantaneousvalueweight**command is configured with the default *percentage*of 66 percent, the new probe is given a higher value to calculate the average for the new cache entry.

Examples

The following example specifies a fallback value weight of 50 percent:

```
Router(config)# call fallback instantaneous-value-weight 50
```

Related Commands

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

call fallback jitter-probe dscp

To specify the differentiated services code point (DSCP) of the jitter-probe transmission, use the **callfallbackjitter-probedscp**command in global configuration mode. To disable this feature and restore the default value of jitter-probe precedence, use the **no** form of this command.

call fallback jitter-probe dscp *dscp-number*
no call fallback jitter-probe dscp

Syntax Description

dscp-number	DSCP value. Range is from 0 to 63.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(9)	This command was implemented in Cisco IOS Release 12.3(9).

Usage Guidelines

Network devices that support differentiated services (DiffServ) use a DSCP in the IP header to select a per-hop behavior (PHB) for a packet. Cisco implements queuing techniques that can base their PHB on the IP precedence or DSCP value in the IP header of a packet. On the basic of DSCP or IP precedence, traffic can be put into a particular service class. Packets within a service class are treated alike.

The **callfallbackjitter-probedscp** command allows you to set a DSCP for jitter-probe packets. The specified DSCP is stored, displayed, and passed in probing packets to the Service Assurance Agent (SAA). This command enables the router to reserve some bandwidth so that during network congestion some of the jitter-probe packets do not get dropped. This command avoids the conflict that occurs with traditional precedence bits.

The **callfallbackjitter-probedscp** command is mutually exclusive with the **callfallbackjitter-probeprecedence** command. Only one of these command can be enabled on the router. When the **callfallbackjitter-probedscp** command is configured, the precedence value is replaced with the DSCP value. The **nocallfallbackjitter-probedscp** command restores the default value for precedence.

Examples

The following example specifies the jitter-probe DSCP as 10. DSCP configuration replaces the set jitter-probe precedence value with the DSCP value.

```
call fallback jitter-probe dscp 10
```

The following configuration disables the DSCP value and restores the default value for precedence, which is set to 2:

```
no call fallback jitter-probe dscp
```

Related Commands

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

call fallback jitter-probe num-packets

To specify the number of packets in a jitter probe used to determine network conditions, use the **callfallbackjitterprobenumpackets** command in global configuration mode. To restore the default number of packets, use the **no** form of this command.

call fallback jitter-probe num-packets *number-of-packets*
no call fallback jitter-probe num-packets

Syntax Description

number-of-packets	Number of packets. Range is from 2 to 50. The default is 15.

Command Default

15 packets

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

A jitter probe, consisting of 2 to 50 packets, details the conditions of the network. More than one packet is used by the probe to calculate an average of delay/loss or Calculated Planning Impairment Factor (ICPIF). After the packets return to the probe, the probe delivers the traffic information to the cache where it is logged for call acceptance/denial. Use the**callfallbackthresholddelayloss** or **callfallbackthresholdicpif** command to set the threshold parameters. The newly specified number of packets take effect only for new probes.

To get a more realistic estimate on the network congestion, increase the number of packets. If more probing packets are sent, better estimates of network conditions are obtained, but the bandwidth for other network operations is negatively affected. Use fewer packets when you need to maximize bandwidth.

Examples

The following example specifies 20 packets in a jitter probe:

```
Router(config)# call fallback jitter-probe num-packets 20
```

Related Commands

Command	Description
call fallback threshold icpif	Specifies the ICPIF threshold.
call fallback threshold delay loss	Specifies the call fallback threshold delay and loss values.

call fallback jitter-probe precedence

To specify the priority of the jitter-probe transmission, use the **callfallbackjitter-probeprecedencecommanding**global configuration mode. To restore the default priority, use the **no** form of this command.

call fallback jitter-probe precedence *precedence-value*
no call fallback jitter-probe precedence

Syntax Description

precedence-value	Jitter-probe precedence. Range is from 0 to 6. The default is 2.

Command Default

Enabled Value set to 2

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

Every IP packet has a precedence header. Precedence is used by various queueing mechanisms in routers to determine the priority of traffic passing through the system.

Use the **callfallbackjitter-probeprecedence**command if there are different queueing mechanisms in your network. Enabling the **callfallbackjitter-probeprecedence**command sets the precedence for jitter probes to pass through your network.

If you require your probes to be sent and returned quickly, set the *precedence* to a low number (0 or 1): the lower the precedence, the higher the priority given.

The **callfallbackjitter-probeprecedence** command is mutually exclusive with the **callfallbackjitter-probedscp** command. Only one of these commands can be enabled on the router. Usually the **callfallbackjitter-probeprecedence** command is enabled. When the **callfallbackjitter-probedscp** command is configured, the precedence value is replaced by the DSCP value. To disable DSCP and restore the default jitter probe precedence value, use the **nocallfallbackjitter-probedscp** command.

Examples

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

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

The following configuration restores the default value for precedence:

```
no call fallback jitter-probe precedence
```

Related Commands

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

call fallback jitter-probe priority-queue

To assign a priority queue for jitter-probe transmissions, use the**callfallbackjitter-probepriority-queuecommandin**global configuration mode. To return to the default state, use the **no** form of this command.

call fallback jitter-probe priority-queue
no call fallback jitter-probe priority-queue

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

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

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

Examples

The following example specifies that a probe be sent to an SAA port:

```
Router(config)# call fallback jitter-probe priority-queue
```

Note In order for this command to have any effect on the probes, the IP priority queueing must be set for UDP voice ports numbered from 16384 to 32767.

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback jitter-probe num-packets	Specifies the number of packets in a jitter probe that are used to determine network conditions.
call fallback jitter-probe precedence	Specifies the jitter-probe precedence.
ip rtp priority	Provides a strict priority queueing scheme for delay-sensitive data.
show call fallback config	Displays the call fallback configuration.

call fallback key-chain

To specify the use of message digest algorithm 5 (MD5) authentication for sending and receiving Service Assurance Agents (SAA) probes, use the **callfallbackkeychain** command in global configuration mode. To disable MD5, use the **no** form of this command.

call fallback key-chain *name-of-chain*
no call fallback key-chain *name-of-chain*

Syntax Description

name-of-chain	Name of the chain. This name is alphanumeric and case-sensitive text. There is no default value.

Command Default

MD5 authentication is not used.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

This command is used to enable the SAA probe authentication using MD5. If MD5 authentication is used, the keys on the sender and receiver routers must match.

Examples

The following example specifies "sample" as the fallback key chain:

```
Router(config)# call fallback key-chain sample
```

Related Commands

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

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

call fallback map address-list

To specify that the call fallback router keep a cache table by IP addresses of distances for several destination peers, use the **callfallbackmapaddresslist** command in global configuration mode. To restore the default values, use the **no** form of this command.

call fallback map *map* **target** *ip-address* **address-list** *ip-address1 . . . ip-address7*
no call fallback map *map* **target** *ip-address* **address-list** *ip-address1 . . . ip-address7*

Syntax Description

map	Fallback map. Range is from 1 to 16. There is no default.
target *ip address*	Target IP address.
ip address1 ... ip-address7	Lists the IP addresses that are kept in the cache table. The maximum number of IP addresses is seven.

Command Default

No call fallback maps are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

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

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

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

Examples

The following example specifies call fallback map address-list configurations for 172.32.10.1 and 172.46.10.1:

```
Router(config)# call fallback map 1 target 172.32.10.1 address-list 172.32.10.2 172.32.10.3
 172.32.10.4 172.32.10.5 172.32.10.6 172.32.10.7 172.32.10.8
Router(config)# call fallback map 2 target 172.46.10.1 address-list 172.46.10.2 172.46.10.3
 172.46.10.4 172.46.10.5 172.46.10.6 172.46.10.7 172.46.10.8
```

Related Commands

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

call fallback map subnet

To specify that the call fallback router keep a cache table by subnet addresses of distances for several destination peers, use the **callfallbackmapsubnet** command in global configuration mode. To restore the default values, use the **no** form of this command.

call fallback map *map* **target** *ip-address* **subnet** *ip-network netmask*
no call fallback map *map* **target** *ip-address* **subnet** *ip-network netmask*

Syntax Description

map	Fallback map. Range is from 1 to 16. There is no default.
target *ip address*	Target IP address.
subnet *ip network*	Subnet IP address.
netmask	Network mask number.

Command Default

No call fallback maps are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5850 in this release.

Usage Guidelines

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

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

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

Examples

The following examples specify the **callfallbackmapsubnet** configuration for two different IP addresses:

```
Router(config)#
call fallback map 1 target 209.165.201.225 subnet
209.165.201.224 255.255.255.224
Router(config)#
call fallback map 2 target 209.165.202.225 subnet
209.165.202.224 255.255.255.224
```

Related Commands

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

call fallback monitor

To enable the monitoring of destinations without call fallback to alternate dial peers, use the **callfallbackmonitor**commandinglobal configuration mode. To disable monitoring without fallback, use the **no** form of this command.

call fallback monitor
no call fallback monitor

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were introduced on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

The **callfallbackmonitor**command is used as a statistics collector of network conditions based upon probes (detailing network traffic) and connected calls. There is no H.323 call checking/rejecting as with the **callfallbackactive** command. All call requests are granted regardless of network traffic conditions.

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

Examples

The following example enables the **callfallbackmonitor**command:

```
Router(config)#
call fallback monitor
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.

Command	Description
call fallback threshold delay loss	Specifies that the call fallback threshold use only packet delay and loss values.
call fallback threshold icpif	Specifies that call fallback use the ICPIF threshold.
show call fallback config	Displays the call fallback configuration.

call fallback probe-timeout

To set the timeout for a Service Assurance Agent (SAA) probe for call fallback purposes, use the **callfallbackprobetimeoutcommand** in global configuration mode. To restore the default value, use the**no**form of this command.

call fallback probe-timeout *seconds*
no call fallback probe-timeout

Syntax Description

seconds	Interval, in seconds. Range is from 1 to 2147483. The default is 30.

Command Default

30 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

SAA probes collect network traffic information based upon configured delay and loss or Calculated Planning Impairment Factor (ICPIF) values and report this information to the cache for call request determination. Use the**callfallbackthresholddelayloss** or **callfallbackthresholdicpif** command to set the threshold parameters.

When the probe timeout expires, a new probe is sent to collect network statistics. To reduce the bandwidth taken up by the probes, increase the probe - timeout interval (*seconds*). Probes do not have a great effect upon bandwidth unless several thousand destinations are involved. If this is the case in your network, use a longer timeout. If you need more network traffic information, and bandwidth is not an issue, use a lower timeout. The default interval, 30 seconds, is a low timeout.

When the **callfallbackcachetimeout** command is configured or expires, new probes are initiated for data collection.

Examples

The following example configures a 120-second interval:

```
Router(config)# call fallback probe-timeout 120
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback cache-timeout	Specifies the time after which the cache entries of network conditions are purged.
call fallback threshold delay loss	Specifies that the call fallback threshold use only packet delay and loss values.
call fallback threshold icpif	Specifies that call fallback use the ICPIF threshold.
show call fallback config	Displays the call fallback configuration.

call fallback reject-cause-code

To enable a specific call fallback reject cause code in case of network congestion, use the **callfallbackrejectcausecode**command in global configuration mode. To reset the code to the default of 49, use the **no** form of this command.

call fallback reject-cause-code *number*
no call fallback reject-cause-code

Syntax Description

number	Specifies the cause code as defined in the International Telecommunication Union (ITU) standard Q.850 except the code for normal call clearing, which is code 16. The default is 49. See the table below for ITU cause-code numbers.

Command Default

49 (quality of service is unavailable)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.

Usage Guidelines

Enabling the **callfallbackrejectcausecode**commanddetermines the code to display when calls are rejected because of probing of network conditions.

Note Connected calls are not affected by this command.

Table 1: ITU cause codes and their associated display message and meanings.

Cause Code	Displayed Message	Meaning
1	Unallocated (unassigned) number	Indicates that the called party cannot be reached because, although the called party number is in a valid format, it is not currently allocated (assigned).
2	No route to specified transit network (national use)	Indicates that the equipment that is sending this code has received a request to route the call through a particular transit network that it does not recognize. The equipment that is sending this code does not recognize the transit network either because the transit network does not exist or because that particular transit network, although it does exist, does not serve the equipment that is sending this cause. This code is supported on a network-dependent basis.

Cause Code	Displayed Message	Meaning
3	No route to destination	Indicates that the called party cannot be reached because the network through which the call has been routed does not serve the destination desired. This code is supported on a network-dependent basis.
4	Send special information tone	Indicates that the called party cannot be reached for reasons that are of a long-term nature and that the special information tone should be returned to the calling party.
5	Misdialed trunk prefix (national use)	Indicates the erroneous inclusion of a trunk prefix in the called party number.
6	Channel unacceptable	Indicates that the channel most recently identified is not acceptable to the sending entity for use in this call.
7	Call awarded and being delivered in an established channel	Indicates that the user has been awarded the incoming call and that the incoming call is being connected to a channel that is already established to that user for similar calls (for example, packet-mode X.25 virtual calls).
8	Preemption	Indicates that the call is being preempted.
9	Preemption - circuit reserved for reuse	Indicates that the call is being preempted and that the circuit is reserved for reuse by the preempting exchange.
16	Normal call clearing	Indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared. Under normal situations, the source of this code is not the network.
17	User busy	Indicates that the called party is unable to accept another call. The user busy code may be generated by the called user or by the network. If the called user generates the user busy code, it is noted that the user equipment is compatible with the call.
18	No user responding	Indicates when a called party does not respond to a call establishment message with either an alerting or a connect indication within the prescribed period of time allocated.
19	No answer from user (user alerted)	Indicates when the called party has been alerted but does not respond with a connect indication within a prescribed period of time. **Note** This code is not necessarily generated by ITU standard Q.931 procedures but may be generated by internal network timers.
20	Subscriber absent	Indicates when a mobile station has logged off, when radio contact is not obtained with a mobile station, or when a personal telecommunication user is temporarily not addressable at any user-network interface.
21	Call rejected	Indicates that the equipment that is sending this code does not want to accept this call although it could have accepted the call because the equipment that is sending this code is neither busy nor incompatible. The network may also generate this code, indicating that the call was cleared because of a supplementary service constraint. The diagnostic field may contain additional information about the supplementary service and reason for rejection.

Cause Code	Displayed Message	Meaning
22	Number changed	Indicates when the called-party number indicated by the calling party is no longer assigned. The new called-party number may be included in the diagnostic field. If a network does not support this code, codeNo. 1, an unallocated (unassigned) number, shall be used.
26	Non-selected user clearing	Indicates that the user has not been sent the incoming call.
27	Destination out of order	Indicates that the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term "not functioning correctly" indicates that a signaling message was unable to be delivered to the remote party; for example, a physical layer or data link layer failure at the remote party, or the equipment of the user is offline.
28	Invalid number format (address incomplete)	Indicates that the called party cannot be reached because the called party number is not in a valid format or is not complete.
29	Facility rejected	Indicates when a supplementary service requested by the user cannot be provided by the network.
30	Response to STATUS ENQUIRY	Indicates when the reason for generating the STATUS message was the prior receipt of a STATUS ENQUIRY message.
31	Normal, unspecified	Reports a normal event only when no other code in the normal class applies.
34	No circuit/channel available	Indicates that no appropriate circuit or channel is available to handle the call.
38	Network out of order	Indicates that the network is not functioning correctly and that the condition is likely to last a relatively long period of time; for example, immediately reattempting the call is not likely to be successful.
39	Permanent frame mode connection out-of-service	Indicates in a STATUS message that a permanently established frame mode connection is out-of-service (for example, due to equipment or section failure) (see the ITU standard, Annex A/Q.933).
40	Permanent frame mode connection operational	Indicates in a STATUS message to indicate that a permanently established frame mode connection is operational and capable of carrying user information (see the ITU standard, Annex A/Q.933).
41	Temporary failure	Indicates that the network is not functioning correctly and that the condition is not likely to last a long period of time; for example, the user may want to try another call attempt almost immediately.
42	Switching equipment congestion	Indicates that the switching equipment that is generating this code is experiencing a period of high traffic.
43	Access information discarded	Indicates that the network could not deliver access information to the remote user as requested, that is, user-to-user information, low layer compatibility, high layer compatibility, or subaddress, as indicated in the diagnostic. It is noted that the particular type of access information discarded is optionally included in the diagnostic.

Cause Code	Displayed Message	Meaning
44	Requested circuit/channel not available	Indicates when the circuit or channel indicated by the requesting entity cannot be provided by the other side of the interface.
46	Precedence call blocked	Indicates that there are no preemptable circuits or that the called user is busy with a call of an equal or higher preemptable level.
47	Resource unavailable, unspecified	Reports a resource-unavailable event only when no other cause in the resource-unavailable class applies.
49	Quality of service not available	Reports that the requested quality of service, as defined in ITU recommendation X.213, cannot be provided (for example, throughput or transit delay cannot be supported).
50	Requested facility not subscribed	Indicates that the user has requested a supplementary service that is implemented by the equipment that generated this cause but that the user is not authorized to use this service.
53	Outgoing calls barred within CUG	Indicates that, although the calling party is a member of the closed user group (CUG) for the outgoing CUG call, outgoing calls are not allowed for this member of the CUG.
55	Incoming calls barred within CUG	Indicates that, although the called party is a member of the CUG for the incoming CUG call, incoming calls are not allowed for this member of the CUG.
57	Bearer capability not authorized	Indicates that the user has requested a bearer capability that is implemented by the equipment that generated this cause but that the user is not authorized to use this capability.
58	Bearer capability not presently available	Indicates that the user has requested a bearer capability that is implemented by the equipment that generated this cause but that is not available at this time.
62	Inconsistency in designated outgoing access information and subscriber class	Indicates that there is an inconsistency in the designated outgoing access information and subscriber class.
63	Service or option not available, unspecified	Reports a service or option not available event only when no other cause in the service or option not available class applies.
65	Bearer capability not implemented	Indicates that the equipment that is sending this code does not support the bearer capability requested.
66	Channel type not implemented	Indicates that the equipment that is sending this code does not support the channel type requested.
69	Requested facility not implemented	Indicates that the equipment that is sending this code does not support the requested supplementary service.
70	Only restricted digital information bearer capability is available (national use)	Indicates that the calling party has requested an unrestricted bearer service but that the equipment that is sending this cause supports only the restricted version of the requested bearer capability.

Cause Code	Displayed Message	Meaning
79	Service or option not implemented, unspecified	Reports a service or option not implemented event only when no other code in the service or option not implemented class applies.
81	Invalid call reference value	Indicates that the equipment that is sending this code has received a message with a call reference that is not currently in use on the user-network interface.
82	Identified channel does not exist	Indicates that the equipment that is sending this code has received a request to use a channel not activated on the interface for a call. For example, if a user has subscribed to those channels on a PRI numbered from 1 to 12 and the user equipment or the network attempts to use channels 13 through 23, this cause is generated.
83	A suspended call exists, but this call identity does not	Indicates that a call resume has been attempted with a call identity that differs from that in use for any suspended calls.
84	Call identity in use	Indicates that the network has received a call suspended request that contains a call identity (including the null call identity) that is already in use for a suspended call within the domain of interfaces over which the call might be resumed.
85	No call suspended	Indicates that the network has received a call resume request that contains a call identity information element that does not indicate any suspended call within the domain of interfaces over which calls may be resumed.
86	Call having the requested call identity has been cleared	Indicates that the network has received a call resume request that contains a call identity information element that indicates a suspended call that has in the meantime been cleared while suspended (either by network timeout or by the remote user).
87	User not member of CUG	Indicates that the called user for the incoming CUG call is not a member of the specified CUG or that the calling user is an ordinary subscriber that is calling a CUG subscriber.
88	Incompatible destination	Indicates that the equipment that is sending this code has received a request to establish a call that has low layer compatibility, high layer compatibility, or other compatibility attributes (for example, data rate) that cannot be accommodated.
90	Non-existent CUG	Indicates that the specified CUG does not exist.
91	Invalid transit network selection (national use)	Indicates that a transit network identification was received that is of an incorrect format as defined in ITU standard Annex C/Q.931.
95	Invalid message, unspecified	Reports an invalid message event only when no other code in the invalid message class applies.
96	Mandatory information element is missing	Indicates that the equipment that is sending this code has received a message that is missing an information element that must be present in the message before that message can be processed.
97	Message type non-existent or not implemented	Indicates that the equipment that is sending this code has received a message with a message type that it does not recognize because this is a message not defined or defined but not implemented by the equipment that is sending this cause.

Cause Code	Displayed Message	Meaning
98	Message not compatible with call state or message type non-existent or not implemented	Indicates that the equipment that is sending this code has received a message that the procedures do not indicate as a permissible message to receive while in the call state, or that a STATUS message that indicates an incompatible call state was received.
99	Information element/parameter non-existent or not implemented	Indicates that the equipment that is sending this code has received a message that includes information elements or parameters not recognized because the information element identifiers or parameter names are not defined or are defined but not implemented by the equipment sending the code. This code indicates that the information elements or parameters were discarded. However, the information element is not required to be present in the message for the equipment that is sending the code to process the message.
100	Invalid information element contents	Indicates that the equipment that is sending this code has received an information element that it has implemented; however, one or more fields in the information element are coded in a way that has not been implemented by the equipment that is sending this code.
101	Message not compatible with call state	Indicates that a message has been received that is incompatible with the call state.
102	Recovery on timer expired	Indicates that a procedure has been initiated by the expiration of a timer in association with error-handling procedures.
103	Parameter non-existent or not implemented - passed on	Indicates that the equipment that is sending this code has received a message that includes parameters not recognized because the parameters are not defined or are defined but not implemented by the equipment that is sending the code. The code indicates that the parameters were ignored. In addition, if the equipment that is sending this code is an intermediate point, this code indicates that the parameters were passed on unchanged.
110	Message with unrecognized parameter discarded	Indicates that the equipment that is sending this code has discarded a received message that includes a parameter that is not recognized.
111	Protocol error, unspecified	Reports a protocol error event only when no other code in the protocol error class applies.
127	Interworking, unspecified	Indicates that there has been interworking with a network that does not provide codes for actions it takes. Thus, the precise code for a message that is being sent cannot be ascertained.

Examples

The following example enables the **callfallbackrejectcausecode**command and specifies cause code 34:

```
call fallback reject-cause-code 34
```

Related Commands

Command	Description
call fallback cache-size	Specifies the call fallback cache size for network traffic probe entries.
call fallback cache-timeout	Specifies the time after which the cache entries of network conditions are purged.
call fallback instantaneous-value-weight	Specifies that the call fallback subsystem take an average from the last two cache entries for call requests.
call fallback jitter-probe num-packets	Specifies the number of packets in a jitter probe that are used to determine network conditions.
call fallback jitter-probe precedence	Specifies the priority of the jitter - probe transmission.
call fallback jitter-probe priority-queue	Assigns a priority queue for jitter-probe transmissions.
call fallback key-chain	Specifies MD5 authentication for sending and receiving SAA probes.
call fallback map address-list	Specifies that the call fallback router keep a cache table by IP addresses of distances for several destination peers that are sitting behind the router.
call fallback map subnet	Specifies that the call fallback router keep a cache table by subnet addresses of distances for several destination peers that are sitting behind the router.
call fallback probe-timeout	Sets the timeout for an SAA probe for call fallback purposes.
call fallback threshold delay loss	Specifies that the call fallback threshold use only packet delay and loss values.
call fallback threshold icpif	Specifies that call fallback use the ICPIF threshold.
show call fallback config	Displays the call fallback configuration.

call fallback threshold delay loss

To specify that the call fallback threshold use only packet delay and loss values, use the **callfallbackthresholddelaylosscommandin**global configuration mode. To restore the default value, use the **no** form of this command.

call fallback threshold delay *milliseconds* **loss** *percent*
no call fallback threshold delay *milliseconds* **loss** *percent*

Syntax Description

milliseconds	The delay value, in milliseconds (ms). Range is from 1 to 2147483647. There is no default value.
percent	The loss value, expressed as a percentage. The valid range is from 0 to 100. There is no default value.

Command Default

None

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

Use the **callfallbackthresholddelayloss**command to configure parameters for voice quality. Lower values of delay and loss allow higher quality of voice. Call requests match the network information in the cache with the configured thresholds of delay and loss.

The amount of delay set by the **callfallbackthresholddelayloss** command should not be more than half the amount of the time-to-wait value set by the **callfallbackwait-timeout** command; otherwise the threshold delay will not work correctly. Because the default value of the **callfallbackwait-timeout** command is set to 300 ms, the user can configure a delay of up to 150 ms for the **callfallbackthresholddelayloss** command. If the user wants to configure a higher threshold, the time-to-wait delay has to be increased from its default (300 ms) using the **callfallbackwait-timeout**command.



Note The delay configured by the **callfallbackthresholddelayloss** command corresponds to a one-way delay, whereas the time-to-wait period configured by the **callfallbackwait-timeout** command corresponds to a round-trip delay.

If you enable the **callfallbackactive**command, the call fallback subsystem uses the last cache entry compared with the configured delay/loss threshold to determine whether the call is connected or denied. If you enable the **callfallbackmonitor**command, all calls are connected, regardless of the configured threshold or voice quality. In this case, configuring the **callfallbackthresholddelayloss**command allows you to collect network statistics for further tracking.

Note The **callfallbackthresholddelayloss**command differs from the call fallback threshold icpif command because the**callfallbackthresholddelayloss**commanduses only packet delay and loss parameters, and the call fallback threshold icpif command uses packet delay and loss parameters plus other International Telecommunication Union (ITU) G.113 factors to gather impairment information.

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

Examples

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

```
Router(config)#

call fallback threshold delay 20 loss 50
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback monitor	Enable the monitoring of destinations without call fallback to alternate dial peers.
call fallback threshold icpif	Specifies the ICPIF threshold.
call fallback wait-timeout	Specifies the time to wait for a response to a probe.
show call fallback config	Displays the call fallback configuration.

call fallback threshold icpif

To specify that call fallback use the Calculated Planning Impairment Factor (ICPIF) threshold, use the **callfallbackthresholdicpif**command in global configuration mode. To restore the default value, use the **no** form of this command.

call fallback threshold icpif *threshold-value*
no call fallback threshold icpif

Syntax Description

threshold-value	Threshold value. Range is from 0 to 34. The default is 5.

Command Default

5

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were introduced on the Cisco 7200 series routers and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

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

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

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

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

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

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

Examples

The following example sets the **ICPIFthreshold**to 20:

```
Router(config)#
call fallback threshold icpif 20
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback monitor	Enables the monitoring of destinations without call fallback to alternate dial peers.
call fallback threshold delay loss	Specifies the call fallback threshold delay and loss values.
show call fallback config	Displays the call fallback configuration.

call fallback wait-timeout

To modify the time to wait for a response to a probe, use the **callfallbackwait-timeout**command in global configuration mode. To return to the default value, use the **no** form of this command.

call fallback wait-timeout *milliseconds*
no call fallback wait-timeout *milliseconds*

Syntax Description

milliseconds	The time-to-wait value in milliseconds (ms). The range is 100 to 3000 milliseconds.

Command Default

300 milliseconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T9	This command was introduced.

Usage Guidelines

This command is enabled by default. The time to wait for a response to a probe is set to 300 ms. This command allows the user to modify the amount of time to wait for a response to a probe. The *milliseconds* argument allows the user to configure a time-to-wait value from 100 ms and 3000 ms. A user that has a higher-latency network may want to increase the value of the default timer.

The time-to-wait period set by the **callfallbackwait-timeout** command should always be greater than or equal to twice the amount of the threshold delay time set by the **callfallbackthreshold delayloss** command; otherwise the probe will fail.

Note The delay configured by the **callfallbackthreshold delayloss** command corresponds to a one-way delay, whereas the time-to-wait period configured by **callfallbackwait-timeout** command corresponds to a round-trip delay. The threshold delay time should be set at half the value of the time-to-wait value.

Examples

The following example sets the amount of time to wait for a response to a probe to 200 ms:

```
call fallback wait-timeout 200
```

Related Commands

Command	Description
call fallback threshold delay loss	Specifies the call fallback threshold delay and loss values.

call filter match-list

To enter the call filter match list configuration mode and create a call filter match list for debugging voice calls, use the **callfiltermatch-list**command in global configuration mode. To remove the filter, use the **no** form of this command.

call filter match-list *number* {**voice** | **gatekeeper**}
no call filter match-list *number* {**voice** | **gatekeeper**}

Syntax Description

number	Numeric label that uniquely identifies the match list. The range is 1 to 16.
voice	Sets the conditions for filtering voice call debugging.
gatekeeper	Defines the conditions on the gatekeeper. The **gatekeeper** keyword is available only if the Cisco IOS image contains the gatekeeper debug filter functionality or a combination of gateway and gatekeeper debug filter functionality.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **gatekeeper** keyword was added.

Usage Guidelines

After the conditions are set with this command, use the **debugconditionmatch-list** command in privileged EXEC mode to get the filtered debug output and debug voice calls.

Examples

The following example shows that the call filter match list designated as list 1 filters the debug output for an incoming calling number matching 8288807, an incoming called number matching 6560729, and on incoming port 7/0:D:

```
call filter match-list 1 voice
 incoming calling-number 8288807
 incoming called-number 6560729
 incoming port 7/0:D
```

Related Commands

Command	Description
debug condition match-list	Runs a filtered debug on a voice call.
show call filter match-list	Displays call filter match lists.

call forward all

To define a a feature code for a Feature Access Code (FAC) to access Call Forward All (CFA) on an analog phone, use the **callforwardall**command in STC application feature access-code configuration mode. To return the code to its default, use the **no** form of this command.

call forward all *keypad-character*
no call forward all

Syntax Description

keypad-character	Character string that can be dialed on a telephone keypad (0-9, *, #). Default: 1. 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 (#) In Cisco IOS Release 15.0(1)M and later releases, the string can also be any of the following: • Three digits (000-999) • Four digits (0000-9999)

Command Default

The default value of the feature code for CFA is 1.

Command Modes

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

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(20)YA	This command was modified. 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.
15.0(1)M	This command was modified.

Usage Guidelines

This command changes the value of the feature code for Call Forward All from the default (1) to the specified value.

In Cisco IOS Release 12.4(20)YA and later releases, if the length of the *keypad-character* argument is at least two characters and the leading or ending character of the string is an asterisk (*) or a number sign (#), phone users are not required to dial a prefix to access this feature. Typically, phone users dial a special feature access

code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 78#, the phone user dials only 78#, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 15.0(1)M and later releases, if the length of the keypad-character argument is three or four digits, phone users are not required to dial a prefix or any special characters to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 788, the phone user dials only 788, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that is already configured for another FAC, for a speed-dial code, or for the Redial FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **showstcappfeaturecodes** command.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that precludes or is precluded by another FAC, by a speed-dial code, or by the Redial FSD, you receive a message. If you configure a feature code to a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable phone user access to that feature.

To display a list of all FACs, use the **showstcappfeaturecodes** command.

Examples

The following example shows how to change the value of the feature code for Call Forward All from the default (1). This configuration also changes the value of the prefix for all FACs from the default (**) to ##. With this configuration, a phone user must press ##3 on the keypad and then dial a target number, to forward all incoming calls to the target number.

```
Router(config)# stcapp feature access-code
Router(config-stcapp-fac)# prefix ##
Router(config-stcapp-fac)# call forward all 3
Router(config-stcapp-fac)# exit
```

The following example shows how to configure all-numeric three or four digit flexible feature access codes so that users are not required to dial a prefix or special characters:

```
VG224(config-stcapp-fac)# call forward all 111
do not use prefix. call forward all is 111
```

Related Commands

Command	Description
call-forward all	Configures call forwarding so that all incoming calls to a particular directory number are forwarded to another directory number.
call forward cancel	Defines a feature code for a feature access code (FAC) to cancel the call-forward-all condition.
call forward to voicemail	Configures call forwarding to voicemail so that all incoming calls are forwarded to voicemail.
prefix (stcapp-fac)	Defines the prefix for feature access codes (FACs).
show stcapp feature codes	Displays all feature access codes (FACs).

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

call forward cancel

To define a a feature code for a Feature Access Code (FAC) to access Call Forward All Cancel, use the **callforwardcancel**command in STC application feature access-code configuration mode. To return the feature code to its default, use the **no** form of this command.

call forward cancel *keypad-character*
no call forward cancel

Syntax Description

keypad-character	Character string that can be dialed on a telephone keypad (0-9, *, #). Default: 2. Before Cisco IOS Release 12.4(20)YA, this is a single character. In Cisco IOS Release 12.4(20)YA and later releases, the string can be any of the following: • A single character (0-9, *, #) • Two digits (00-99) • Two to four characters (0-9, *, #) and the leading or ending character must be an asterisk (*) or number sign (#) In Cisco IOS Release 15.0(1)M and later releases, the string can also be any of the following: • Three digits (000-999) • Four digits (0000-9999)

Command Default

The default value of the feature code is 2.

Command Modes

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

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(20)YA	The length of the *keypad-character* argument was changed to 1 to 4 characters.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.
15.0(1)M	This command was modified.

Usage Guidelines

This command changes the value of the feature code for Call Forward All Cancel from the default (2) to the specified value.

In Cisco IOS Release 12.4(20)YA and later releases, if the length of the *keypad-character* argument is at least two characters and the leading or ending character of the string is an asterisk (*) or a number sign (#), phone users are not required to dial a prefix to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 78#, the phone user dials only 78#, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 15.0(1)M and later releases, if the length of the keypad-character argument is three or four digits, phone users are not required to dial a prefix or any special characters to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 788, the phone user dials only 788, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that is already configured for another FAC, for a speed-dial code, or for the Redial FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **showstcappfeaturecodes** command.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that precludes or is precluded by another FAC, by a speed-dial code, or by the Redial FSD, you receive a message. If you configure a feature code to a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable phone user access to that feature.

To display a list of all FACs, use the **showstcappfeaturecodes** command.

Note To disable call-forward-all on a particular directory number associated with SCCP endpoints connected to Cisco Unified CME through an analog voice gateway, use the **nocall-forwardall**command in ephone-dn or ephone-dn-template configuration mode.

Examples

The following example shows how to change the value of the feature code for Call Forward Cancel from the default (2). This configuration also changes the value of the prefix for all FACs from the default (**) to ##. With this configuration, a phone user must press ##3 on the phone keypad to cancel all-call forwarding.

```
Router(config)# stcapp feature access-code
Router(config-stcapp-fac)# prefix ##
Router(config-stcapp-fac)# call forward cancel 3
Router(config-stcapp-fac)# exit
```

Related Commands

Command	Description
call forward all	Defines the feature code in the feature access code (FAC) for forwarding all calls.
call-forward all	Configures call forwarding so that all incoming calls to a particular directory number are forwarded to another directory number.
prefix (stcapp-fac)	Defines the prefix for feature access codes (FACs).
show stcapp feature codes	Displays all feature access codes (FACs).
stcapp feature access-code	Enables feature access codes (FACs) and enters STC application feature access-code configuration mode for changing values of the prefix and features codes from the default.

call history max

To retain call history information and to specify the number of call records to be retained, use the **callhistorymax** command in global configuration mode.

call history max *number*

Syntax Description

number	The maximum number of call history records to be retained in the history table. Values are from 0 to 1200. The default is 15.

Command Default

If this command is not configured, no call history is maintained for disconnected calls. If the command is configured, the default value for number of records is 15.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

The number of disconnected calls displayed is the number specified in the number argument. This maximum number helps to reduce CPU usage in the storage and reporting of this information.

Examples

The following example configures the history table on the gatekeeper to retain 25 records:

```
Router# call history max 25
```

Related Commands

Command	Description
show call history voice	Displays historical information on disconnected calls.

call-history-mib

To define the history MIB parameters, use the **call-history-mib**command in global configuration mode. To disable the configured parameters, use the **no** form of this command.

call-history-mib {**max-size** *num-of-entries* | **retain-timer** *seconds*}
no call-history-mib {**max-size** *num-of-entries* | **retain-timer** *seconds*}

Syntax Description

max-size	Specifies the maximum size of the call history MIB table.
number-of-entries	Number of entries in the call history MIB table. The valid range is from 0 to 500. The default value is 100.
retain-timer	Specifies the timer for entries in the call history MIB table.
seconds	Time in minutes, for removing an entry. The valid range is from 0 to 500. The default time is 15 minutes.

Command Default

The default values are set if the command is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

CISCO-CALL-HISTORY-MIB describes the objects defined and used for storing the call information for all calls. The MIB contains a table that stores the past call information. The call information will include the destination number, the call connect time, the call disconnect time and the disconnection cause. These calls could be circuit switched or they could be virtual circuits. The history of each call will be stored. An entry will be created when a call gets disconnected. At the time of creation, the entry will contain the connect time and the disconnect time and other call information.

The history table is characterized by two values, the maximum number (*number-of-entries*) of entries that could be stored in a period of time (*seconds*).

The **max-size** value specifies the maximum size of the call history MIB table.

The**retain-timer** value specifies the length of time, in minutes, that entries will remain in the call history MIB table. Setting the value to 0 prevents any call history from being retained.

Examples

The following examples shows how to set call history MIB parameters:

```
Router# configure terminal
Router(config)# call-history-mib max-size 250
Router# configure terminal
Router(config)# call-history-mib retain-timer 250
```

Related Commands

Command	Description
show startup-config	Displays the contents of the startup configuration file.

call-progress-analysis

To activate call progress analysis (CPA) for a digital signal processor (DSP) farm profile on the Cisco Unified Border Element (Cisco UBE), use the **call-progress-analysis** command in DSP farm profile configuration mode. To disable this command from your configuration, use the **no** form of this command.

call-progress-analysis
no call-progress-analysis

Syntax Description

This command has no arguments or keywords.

Command Default

Call progress analysis is disabled.

Command Modes

DSP farm profile configuration (config-dspfarm-profile)

Command History

Release	Modification
15.3(2)T	This command was introduced.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

Use the **call-progress-analysis** command to activate CPA on Cisco UBE. This command is applicable only for local transcoding interface (LTI)-based DSP farm profiles, which has associate application CUBE applied on the respective DSP farm profiles. This command is not available on Skinny Call Control Protocol (SCCP)-based DSP farm profiles. If CPA is not activated on the DSP farm profile, you cannot configure the CPA timing and threshold parameters for VoIP calls.

Examples

The following example shows how to activate CPA on a DSP farm profile:

```
Device> enable
Device# configure terminal
Device(config)# dspfarm profile 15 transcode universal
Device(config-dspfarm-profile)# call-progress-analysis
```

Related Commands

Command	Description
cpa	Enables the CPA algorithm for outbound VoIP calls and sets the CPA parameters.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.

call language voice

To configure an external Tool Command Language (Tcl) module for use with an interactive voice response (IVR) application, use the **calllanguagevoicecommandin**global configuration mode.

call language voice *language url*

Syntax Description

language	Two-character abbreviation for the language; for example, "**en**" for English or "**ru**" for Russian.
url	URL that points to the Tcl module.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.3(14)T	This is obsolete in Cisco IOS Release 12.3(14)T. Use the **paramlanguage**command in application parameter configuration mode.

Usage Guidelines

The built-in languages are English (*en)* , Chinese (*ch)* , and Spanish (*sp)* . If you specify "**en**" , "**ch**" , or **sp**" , the new Tcl module replaces the built-in language functionality. When you add a new Tcl module, you create your own prefix to identify the language. When you configure and load the new languages, any upper-layer application (Tcl IVR) can use the language.

You can use the language abbreviation in the *language* argument of any **callapplicationvoice** command. The language and the text-to-speech (TTS) notations are available for the IVR application to use after they are defined by the Tcl module.

Examples

The following example adds Russian (**ru**) as a Tcl module:

```
call language voice ru tftp://box/unix/scripts/multi-lang/ru_translate.tcl
```

Related Commands

Command	Description
call application voice	Configures an application.
debug voip ivr	Specifies the type of VoIP IVR debug output that you want to view.
param language	Configures the language parameter in a service or package on the gateway.
show language voice	Displays information about configured languages and applications.

call language voice load

To load or reload a Tool Command Language (Tcl) module from the configured URL location, use the **calllanguagevoiceload** command in EXEC mode.

call language voice load *language*

Syntax Description

language	The two-character prefix configured with the **calllanguagevoice** command in global configuration mode; for example, "en" for English or "ru" for Russian.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

You cannot use this command if the interactive voice response (IVR) application using the language that you want to configure has an active call. A language that is configured under an IVR application is not necessarily in use. To determine if a call is active, use the **showcallapplicationvoice** command.

Examples

The following example loads French (fr) into memory:

```
call language voice load fr
```

Related Commands

Command	Description
call application voice load	Loads an application.
debug voip ivr	Specifies the type of VoIP IVR debug output that you want to view.
show language voice	Displays information about configured languages and applications.

call leg dump event-log

To flush the event log buffer for call legs to an external file, use the **call leg dump event-log** command in privileged EXEC mode.

call leg dump event-log

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command immediately writes the event log buffer to the external file whose location is defined with the **call leg event-log dump ftp** command in global configuration mode.

Note The **call leg dump event-log** command and the **call leg event-log dump ftp** command are two different commands.

Examples

The following example writes the event log buffer to an external file named leg_elogs:

```
Router(config)# call leg event-log dump ftp ftp-server/elogs/leg_elogs.log username myname
 password 0 mypass
Router(config)# exit
Router# call leg dump event-log
```

Related Commands

Command	Description
call leg event-log	Enables event logging for voice, fax, and modem call legs.
call leg event-log dump ftp	Enables the voice gateway to write the contents of the call-leg event log buffer to an external file.
call leg event-log max-buffer-size	Sets the maximum size of the event log buffer for each call leg.
monitor call leg event-log	Displays the event log for an active call leg in real-time.
show call leg	Displays event logs and statistics for voice call legs.

call leg event-log

To enable event logging for voice, fax, and modem call legs, use the **calllegevent-log** command in global configuration mode. To reset to the default, use the **no** form of this command.

call leg event-log
no call leg event-log

Syntax Description

This command has no arguments or keywords.

Command Default

Event logging for call legs is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command enables event logging for telephony call legs. IP call legs are not supported.

Note To prevent event logging from adversely impacting system performance for production traffic, the system includes a throttling mechanism. When free processor memory drops below 20%, the gateway automatically disables all event logging. It resumes event logging when free memory rises above 30%. While throttling is occurring, the gateway does not capture any new event logs even if event logging is enabled. You should monitor free memory on the gateway and enable event logging only when necessary to isolate faults.

Examples

The following example enables event logging for all telephony call legs:

```
call leg event-log
```

Related Commands

Command	Description
call leg dump event-log	Flushes the event log buffer for call legs to an external file.
call leg event-log dump ftp	Enables the voice gateway to write the contents of the call-leg event log buffer to an external file.
call leg event-log error-only	Restricts event logging to error events only for voice call legs.
call leg event-log max-buffer-size	Sets the maximum size of the event log buffer for each call leg.
call leg history event-log save-exception-only	Saves to history only event logs for call legs that had at least one error.
monitor call leg event-log	Displays the event log for an active call leg in real-time.

Command	Description
show call leg	Displays event logs and statistics for voice call legs.

call leg event-log dump ftp

To enable the gateway to write the contents of the call-leg event log buffer to an external file, use the **call leg event-log dump ftp** command in global configuration mode. To reset to the default, use the **no** form of this command.

call leg event-log dump ftp *server* [*:port*] */path* **username** *username* **password** { **0** | **6** | **7** } *password*
no call leg event-log dump ftp

Syntax Description

server	Name or IP address of FTP server where the file is located.
: *port*	(Optional) Specific port number on the server.
/ *file*	Name and path of the file.
username *username*	Username required for accessing the file.
password *encryption-type*	(Optional) The Cisco proprietary algorithm used to encrypt the password. Values are **0** or **7**. **0** disables encryption; **7** enables encryption. If you specify **7**, you must enter an encrypted password (a password already encrypted by a Cisco router).
password {*0* | *6* | *7*}	Following are the password encryption types– • **0**– Specifies that the subsequent password is in plain text. Type **0** disables encryption. • **6**– Specifies that the subsequent password is encrypted using the AES algorithm. Ensure to provide a string in AES-encrypted format. • **7**– Specifies that the subsequent password is hidden. You must enter a Cisco-proprietary encrypted password string. • **LINE**– The cleartext password.
password	Password required for accessing the file.

Command Default

Event logs are not written to an external file.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
Cisco IOS XE 26.2.1	This command was modified for the following: • To support Type 6 encryption. • To display warning message for insecure protocol usage.

Usage Guidelines

This command enables the gateway to automatically write the event log buffer to the named file either after an active call leg terminates or when the event log buffer becomes full. The default buffer size is 4 KB. To modify the size of the buffer, use the **call leg event-log max-buffer-size** command. To manually flush the event log buffer, use the **call leg dump event-log** command in privileged EXEC mode.

Starting from Cisco IOS XE 26.2.1 release, it is recommended to use Type 6 (AES) for all credential provisioning to comply with security standards. Usage of Type 0, or 7 triggers a syslog warning. Ensure **password encryption aes** and **key config-key password-encrypt** are enabled to support auto-conversion of Type 0, or 7 to Type 6 reversible encryption. If the encryption commands are not enabled, 0 and 7 password types are not converted to type 6; they remain saved as type 0 and 7.



Warning Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used, as they do not provide encryption or authentication. Use secure alternatives such as HTTPS, SFTP, or SCP instead.



Note The **call leg dump event-log** command and the **call leg event-log dump ftp** command are two different commands.

Enabling the gateway to write event logs to FTP could adversely impact gateway memory resources in some scenarios, for example, when:

- The gateway is consuming high processor resources and FTP does not have enough processor resources to flush the logged buffers to the FTP server.
- The designated FTP server is not powerful enough to perform FTP transfers quickly.
- Bandwidth on the link between the gateway and the FTP server is not large enough.
- The gateway is receiving a high volume of short-duration calls or calls that are failing.

You should enable FTP dumping only when necessary and not enable it in situations where it might adversely impact system performance.

The following example enables type 6 auto-conversion:

```
Router(config)# password encryption aes
Router(config)# key config-key password-encrypt
New Key :
Confirm Key :
Router(config)# call leg event-log dump ftp 10.10.10.101/elogs/leg_elogs.log username myname
 password 0 mypass
SECURITY WARNING - Module: CALL_LEG, Command: call leg event-log dump ftp
10.10.10.101/elogs/leg_elogs.log username myname password 0 *,
Reason: No encryption is configured, Description: Call leg event log dump configured with
insecure FTP protocol -
vulnerable to log tampering, Remediation: Transition to secure file transfer methods using
 SCP, SFTP, HTTPS protocols
Router(config)# end

Router#show run | sec call leg
call leg event-log dump ftp 10.10.10.101/elogs/leg_elogs.log username myname password 6
```

```
EMSefGVigEAMP][YVUF\ZPDbCD^PJQ
call leg event-log
```

The following example shows the warning being displayed for the usage of insecure FTP protocol:

```
Device(config)#call leg event-log dump ftp 10.10.10.101/elogs/leg_elogs.log username myname
 password 0 password
SECURITY WARNING - Module: CALL_LEG, Command: call leg event-log dump ftp
10.10.10.101/elogs/leg_elogs.log username myname password 0 *,
Reason: No encryption is configured, Description: Call leg event log dump configured with
insecure FTP protocol - vulnerable to log tampering,
Remediation: Transition to secure file transfer methods using SCP, SFTP, HTTPS protocols
```

Examples

The following example enables the gateway to write call leg event logs to an external file named leg_elogs.log on a server named ftp-server:

```
call leg event-log dump ftp ftp-server/elogs/leg_elogs.log username myname password 0 mypass
```

Examples

The following example specifies that call leg event logs are written to an external file named leg_elogs.log on a server with the IP address 10.10.10.101:

```
call leg event-log dump ftp 10.10.10.101/elogs/leg_elogs.log username myname password 0
mypass
```

Related Commands

Command	Description
call leg dump event-log	Flushes the event log buffer for call legs to an external file.
call leg event-log	Enables event logging for voice, fax, and modem call legs.
call leg event-log error-only	Restricts event logging to error events only for voice call legs.
call leg event-log max-buffer-size	Sets the maximum size of the event log buffer for each call leg.
call leg history event-log save-exception-only	Saves to history only event logs for call legs that had at least one error.
monitor call leg event-log	Displays the event log for an active call leg in real-time.
show call leg	Displays event logs and statistics for voice call legs.

call leg event-log errors-only

To restrict event logging to error events only for voice call legs, use the **calllegevent-logerrors-only**command in global configuration mode. To reset to the default, use the **no** form of this command.

call leg event-log errors-only
no call leg event-log errors-only

Syntax Description

This command has no arguments or keywords.

Command Default

All call leg events are logged.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command limits the severity level of the events that are logged; it does not enable logging. You must use this command with the **calllegevent-log** command, which enables event logging for call legs.

Examples

The following example shows how to capture event logs only for call legs with errors:

```
Router(config)# call leg event-log
Router(config)# call leg event-log errors-only
```

Related Commands

Command	Description
call leg event-log	Enables event logging for voice, fax, and modem call legs.
call leg event-log dump ftp	Enables the gateway to write the contents of the call-leg event log buffer to an external file.
call leg event-log max-buffer-size	Sets the maximum size of the event log buffer for each call leg.
call leg history event-log save-exception-only	Saves to history only event logs for call legs that had at least one error.
monitor call leg event-log	Displays the event log for an active call leg in real-time.
show call leg	Displays event logs and statistics for voice call legs.

call leg event-log max-buffer-size

To set the maximum size of the event log buffer for each call leg, use the **calllegevent-logmax-buffer-size**command in global configuration mode. To reset to the default, use the **no** form of this command.

call leg event-log max-buffer-size *kbytes*
no call leg event-log max-buffer-size

Syntax Description

kbytes	Maximum buffer size, in kilobytes (KB). Range is 1 to 20. Default is 4.

Command Default

4 KB

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

If the event log buffer reaches the limit set by this command, the gateway allocates a second buffer of equal size. The contents of both buffers is displayed when you use the **showcallleg** command. When the first event log buffer becomes full, the gateway automatically appends its contents to an external FTP location if the **calllegevent-logdumpftp**command is used.

A maximum of two buffers are allocated for an event log. If both buffers are filled, the first buffer is deleted and another buffer is allocated for new events (buffer wraps around). If the **calllegevent-logdumpftp** command is configured and the second buffer becomes full before the first buffer is dumped, event messages are dropped and are not recorded in the buffer.

Examples

The following example sets the maximum buffer size to 8 KB:

```
call leg event-log max-buffer-size 8
```

Related Commands

Command	Description
call leg dump event-log	Flushes the event log buffer for call legs to an external file.
call leg event-log dump ftp	Enables the voice gateway to write the contents of the call-leg event log buffer to an external file.
monitor call leg event-log	Displays the event log for an active call leg in real-time.
show call leg	Displays event logs and statistics for voice call legs.

call leg history event-log save-exception-only

To save to history only event logs for call legs that had at least one error, use the **callleghistoryevent-logsave-exception-only** command in global configuration mode. To reset to the default, use the **no** form of this command.

call leg history event-log save-exception-only
no call leg history event-log save-exception-only

Syntax Description

This command has no arguments or keywords.

Command Default

By default all the events will be logged.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Call leg event logs move from the active to the history table after the call leg terminates. If you use this command, event logs are saved only for those legs that had errors. Event logs for normal legs that do not contain any errors are not saved.

Note This command does not affect records saved to an FTP server by using the **calllegdumpevent-log** command.

Examples

The following example saves to history only call leg records that have errors:

```
call leg history event-log save-exception-only
```

Related Commands

Command	Description
call leg dump event-log	Flushes the event log buffer for call legs to an external file.
call leg event-log	Enables event logging for voice, fax, and modem call legs.
call leg event-log error-only	Restricts event logging to error events only for voice call legs.
call leg event-log max-buffer-size	Sets the maximum size of the event log buffer for each call leg.
show call leg	Displays event logs and statistics for voice call legs.

callmonitor

To enable call monitoring messaging functionality on a SIP endpoint in a VoIP network, use the **callmonitor** command in voice-service configuration mode. To return to the default, use the **no** form of this command.

callmonitor
no callmonitor

Syntax Description

This command has no arguments or keywords.

Command Default

Monitoring service is disabled.

Command Modes

Voice service VoIP configuration (config-voi-serv).

Voice class tenant configuration.

Command History

Cisco IOS Release	Modification
12.4(11)XW2	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command in voice service configuration mode to allow a SIP endpoint, such as an external feature server, to watch call activity on a VoIP network.

To view call activity, use the **showcallmon**command.

Examples

The following example enables call monitoring messaging functionality on a SIP endpoint:

```
Router(config-voi-serv)# callmonitor
```

Related Commands

Command	Description
show callmon	Displays call-monitor information.

call preserve

To enable the preservation of H.323 VoIP calls, use the**callpreserve** command in h323, voice-class, and voice-service configuration modes. To reset to the default, use the **no** form of this command.

call preserve [**limit-media-detection**]
no call preserve [**limit-media-detection**]

Syntax Description

limit-media-detection	Limits RTP and RTCP inactivity detection and bidirectional silence detection (if configured) to H.323 VoIP preserved calls only.

Command Default

H.323 VoIP call preservation is disabled.

Command Modes

h323
Voice-class configuration (config-voice-class)
Voice-service configuration (config-voi-serv)

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

The **callpreserve**command activates H.323 VoIP call preservation for following types of failures and connections:

Failure Types

- WAN failures that include WAN links flapping or degraded WAN links
- Cisco Unified CallManager software failure, such as when the ccm.exe service crashes on a Cisco Unified CallManager server.
- LAN connectivity failure, except when a failure occurs at the local branch

Connection Types

- Calls between two Cisco Unified CallManager controlled endpoints
  - During Cisco Unified CallManager reloads
  - When a Transmission Control Protocol (TCP) connection between one or both endpoints and Cisco Unified CallManager used for signaling H.225.0 or H.245 messages is lost or flapping
  - Between endpoints that are registered to different Cisco Unified CallManagers in a cluster and the TCP connection between the two Cisco Unified CallManagers is lost
  - Between IP phones and the PSTN at the same site
- Calls between Cisco IOS gateway and an endpoint controlled by a softswitch where the signaling (H.225.0, H.245 or both) flows between the gateway and the softswitch and media flows between the gateway and the endpoint.
  - When the softswitch reloads.

- When the H.225.0 or H.245 TCP connection between the gateway and the softswitch is lost, and the softswitch does not clear the call on the endpoint
- When the H.225.0 or H.245 TCP connection between softswitch and the endpoint is lost, and the soft-switch does not clear the call on the gateway

- Call flows that involve a Cisco IP in IP (IPIP) gateway running in media flow-around mode that reload or lose connection with the rest of the network

When bidirectional silence and RTP and RTCP inactivity detection are configured, they are enabled for all calls by default. To enable them for H.323 VoIP preserved calls only, you must use the **callpreserve**command's **limit-media-detection** keyword.

H.323 VoIP call preservation can be applied globally to all calls and to a dial peer.

Examples

The following example enables H.323 VoIP call preservation for all calls.

```
voice service voip
 h323
  call preserve
```

The following configuration example enables H.323 VoIP call preservation for dial peer 1.

```
voice-class h323 4
 call preserve
dial-peer voice 1 voip
 voice-class h323 4
```

The following example enables H.323 VoIP call preservation and enables RTP and RTCP inactivity detection and bidirectional silence detection for preserved calls only:

```
voice service voip
 h323
  call preserve limit-media-detection
```

The following example enables RTP and RTCP inactivity detection. Note that for H.323 VoIP call preservation VAD must be set to off (**novad** command).

```
dial-peer voice 10 voip
 no vad
gateway
 timer receive-rtcp
ip rtcp report-interval
```

The following configuration example enables bidirectional silence detection:

```
gateway
 timer media-inactive
ip rtcp report interval
```

Related Commands

Command	Description
h323	Enables the H.323 voice service configuration commands.
show h323 calls preserved	Displays data about active H.323 VoIP preserved calls.

Command	Description
voice-class h323	Assigns an H.323 voice class to a VoIP dial peer.
voice service voip	Enters voice-service configuration mode.

call-route

To enable Header-Based routing, at the global configuration level, use the **call-route** command in voice service VoIP SIP configuration mode or voice class tenant configuration mode. To disable Header-Based routing, use the **no** form of this command.

call-route {**dest-route-string** | **p-called-party-id** | **history-info** | **url**} `[system]`
no call-route {**dest-route-string** | **p-called-party-id** | **history-info** | **url**}

Syntax Description

dest-route-string	Enables call routing based on the Destination-Route-String header.
p-called-party-id	Enables call routing based on the P-Called-Party-Id header.
history-info	Enables call routing based on the History-Info header.
url	Enables call routing based on the URL.
system	Use the global value of the header. This keyword is available only for the tenant configuration mode.

Command Default

Support for call routing based on the header in a received INVITE message is disabled.

Command Modes

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

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(2)T	This command was modified. The **history-info** keyword was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(1)T	This command was modified. The **url** keyword was added.
15.3(3)M	This command was modified. The **dest-route-string** keyword was added.
Cisco IOS XE Release 3.10S	This command was modified. The **dest-route-string** keyword was added.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the **call-route** command to enable the Cisco Unified Border Element to route calls based on the Destination-Route-String, P-Called-Party-ID or History-Info header in a received INVITE message. If multiple

call routes are configured, call routing enabled based on destination route string takes precedence over other header configurations. Destination route string configuration is applicable only for outbound dial-peer matching.

Examples

The following example shows how to enable call routing based on the header value:

```
Router> enable

Router# configure terminal
Router(config)# voiceservicevoip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# call-route dest-route-string
Router(conf-serv-sip)# call-route p-called-party-id
Router(conf-serv-sip)# call-route history-info
Router(conf-serv-sip)# call-route url
```

The following example shows how to route a call based on the History-Info header in the voice class tenant configuration mode:

```
Router(config-class)# call-route history-info system
```

Related Commands

Command	Description
voice-class sip call-route	Enables call routing based on the Destination-Route-String, P-called-party-id and History-Info header values at the dial-peer configuration level.

call-router h323-annexg

To enable the Annex G border element (BE) configuration commands by invoking H.323 Annex G configuration mode, use the **call-router** command in global configuration mode. To remove the definition of a BE, use the no form of this command.

call-router h323-annexg *border-element-id*
no call-router h323-annexg

Syntax Description

border -element-id	Identifier of the BE that you are provisioning. Possible values are any International Alphabet 5 (IA5) string, without spaces and up to 20 characters in length. This value must match the value that you specified for the BE ID in the **border-element** command.

Command Default

No default behaviors or values

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use this command to enter Annex G configuration mode and to identify BEs.

Examples

The following example shows that Annex G configuration mode is being entered for a BE named "be20":

```
Router(config)# call-router h323-annexg be20
```

Related Commands

Command	Description
show call history	Displays the fax call history table for a fax transmission.
show call-router status	Displays the Annex G BE status.

call-routing hunt-scheme

To enable capacity based load-balancing, use the **call-routing hunt-scheme** command in gatekeeper configuration mode. To disable this function, use the **no** form of this command.

call-routing hunt-scheme percentage-capacity-util
no call-routing hunt-scheme

Syntax Description

percentage -capacity -util	Selects the one with least percentage capacity utilized among the gateways.

Command Default

This command is disabled.

Command Modes

Gatekeeper configuration (config-gk)

Command History

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

Usage Guidelines

Use the **call-routing hunt-scheme** command to turn on load balancing based on capacity of gateway and verify that the gateway capacity reporting is enabled.

Examples

The following example shows the gateway with the with least percentage capacity being selected:

```
Router(config-gk)# call-routing hunt-scheme percentage-capacity-util
```

Related Commands

Command	Description
timer cluster-element	Sets the time between resource update messages to gatekeepers in local cluster.

call rscmon update-timer

To change the value of the resource monitor throttle timer, use the **callrscmonupdate-timer** command in privileged EXEC mode. To revert to the default value, use the **no** form of this command.

call rscmon update-timer *milliseconds*
no call rscmon update-timer

Syntax Description

milliseconds	Duration of the resource monitor throttle timer, in milliseconds (ms). Range is from 20 to 3500. The default is 2000.

Command Default

2000 ms

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command specifies the duration of the resource monitor throttle timer. When events are delivered to the resource monitor process, the throttle timer is started and the event is processed after the timer expires (unless the event is a high-priority event). The timer ultimately affects the time it takes the gateway to send Resource Availability Indicator (RAI) messages to the gatekeeper. This command allows you to vary the timer according to your needs.

Examples

The following example shows how the timer is to be configured:

```
Router(config)# call rscmon update-timer 1000
```

Related Commands

Command	Description
resource threshold	Configures a gateway to report H.323 resource availability to its gatekeeper.

call rsvp-sync

To enable synchronization between Resource Reservation Protocol (RSVP) signaling and the voice signaling protocol, use the **callrsvp-sync** command in global configuration mode. To disable synchronization, use the **no** form of this command.

call rsvp-sync
no call rsvp-sync

Syntax Description

This command has no keywords or arguments.

Command Default

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

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco 2600 series, 3600 series, 7200 series, Cisco AS5300, Cisco AS5800, and Cisco MC3810.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The **callrsvp-sync** command is enabled by default.

Examples

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

```
call rsvp-sync
```

Related Commands

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

call rsvp-sync resv-timer

To set the timer on the terminating VoIP gateway for completing RSVP reservation setups, use the **callrsvp-syncresv-timer** command in global configuration mode. To restore the default value, use the **no** form of this command.

call rsvp-sync resv-timer *seconds*
no call rsvp-sync resv-timer

Syntax Description

seconds	Number of seconds in which the reservation setup must be completed, in both directions. Range is from 1 to 60. The default is 10.

Command Default

10 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)XI	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco AS5800, and Cisco MC3810.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

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

Examples

The following example sets the reservation timer to 30 seconds:

```
call rsvp-sync resv-timer 30
```

Related Commands

Command	Description
call rsvp -sync	Enables synchronization of RSVP and the H.323 voice signaling protocol.
debug call rsvp -syncevents	Displays the events that occur during RSVP synchronization.
show call rsvp -syncconf	Displays the RSVP synchronization configuration.

Command	Description
show call rsvp -syncstats	Displays statistics for calls that have attempted RSVP reservation.

call service stop

To shut down VoIP call service on a gateway, use the **call service stop** command in voice service SIP or voice service H.323 configuration mode. To enable VoIP call service, use the **no** form of this command. To set the command to its defaults, use the **default call service stop** command.

call service stop [**forced**] [**maintain-registration**]
no call service stop
default call service stop

Syntax Description

forced	(Optional) Forces the gateway to immediately terminate all in-progress calls.
maintain -registration	(Optional) Forces the gateway to remain registered with the gatekeeper.

Command Default

VoIP call service is enabled.

Command Modes

Voice service SIP configuration (conf-serv-sip)
Voice service H.323 configuration (conf-serv-h323)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.4(22)T	Support for IPv6 was added.
12.4(23.08)T01	The default behavior was clarified for SIP and H.323 protocols.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Use the **call service stop** command to shut down the SIP or H.323 services regardless of whether the **shutdown** or **no shutdown** command was configured in voice service configuration mode.

Use the **no call service stop** command to enable SIP or H.323 services regardless of whether the **shutdown** or **no shutdown** command was configured in voice service configuration mode.

Use the **default call service stop** command to set the command to its defaults. The defaults are as follows:

- Shut down SIP or H.323 service, if the **shutdown** command was configured in voice service configuration mode.
- Enable SIP or H.323 service, if the **no shutdown** command was configured in voice service configuration mode.

Examples

The following example shows SIP call service being shut down on a Cisco gateway:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
```

```
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# call service stop
```

The following example shows H.323 call service being enabled on a Cisco gateway:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# no call service stop
```

The following example shows SIP call service being enabled on a Cisco gateway because the **no shutdown** command was configured in voice service configuration mode:

```
Router> enable
Router# configure terminal
Router(config)#voice service voip
Router(conf-voi-serv)# no shutdown
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# default call service stop
```

The following example shows H.323 call service being shut down on a Cisco gateway because the **shutdown** command was configured in voice configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# shutdown
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# default call service stop
```

Related Commands

Command	Description
bandwidth audio as-modifier	Allows SIP SDP bandwidth-related options.
billing b-channel	Enables the H.323 gateway to access B-channel information for all H.323 calls.
outbound-proxy	Configures an outbound proxy server.
telephony-service ccm-compatible	Enables the detection of a Cisco Unified Communications Manager system in the network and allows the exchange of calls.

call spike

To configure the limit on the number of incoming calls received in a short period of time (a call spike), use the **callspike** command in global or dial peer voice configuration mode. To disable this command, use the**no** form of this command.

call spike *call-number* [**steps** *number-of-steps* **size** *milliseconds*]
no call spike

Dial Peer Voice Configuration Mode
call spike *threshold* [**steps** *number-of-steps* **size** *milliseconds*]

Syntax Description

call -number	Incoming call count for the spiking threshold. Range is 1 to 2147483647.
steps *number -of-steps*	(Optional) Specifies the number of steps for the spiking sliding window. Range is from 3 to 10. The default is 5.steps for the spiking sliding window.
size *milliseconds*	(Optional) Specifies step size in milliseconds. Range is from 100 to 250. The default is 200.
threshold	Threshold for the incoming call count for spiking. Range is 1 to 2147483647.

Command Default

The limit on the number of incoming calls received during a specified period is not configured.

Command Modes

Global configuration (config)
Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. This release does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on Cisco 1750 and Cisco 1751 routers. Support for other Cisco platforms was not included in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
15.1(3)T	This command was modified. Support for this command was added in the dial peer level.

Release	Modification
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

A call spike occurs when a large number of incoming calls arrive from the Public Switched Telephone Network (PSTN) in a short period of time (for example, 100 incoming calls in 10 milliseconds). Setting this command allows you to control the number of call requests that can be received in a configured time period. The sliding window buffers the number of calls that get through. The counter resets according to the specified step size.

The period of the sliding window is calculated by multiplying the number of steps by the size. If an incoming call exceeds the configured call number during the period of the sliding window the call is rejected.

If the **callspike** is configured at both the global and dial-peer levels, the dial-peer level takes precedence and the call spike is calculated. If the call spike threshold is exceeded the call gets rejected, and the call spike calculation is done at the global level.

Examples

The following example shows how to configure the **callspike** command with a call-number and the of 1, a sliding window of 10 steps, and a step size of 200 milliseconds. The period of the sliding window is 2 seconds. If the gateway receives more than 1 call within 2 seconds the call is rejected.

```
Router(config)# call spike 1 steps 10 size 200
```

The following example shows how to configure the **callspike** command with a call number of 30, a sliding window of 10 steps, and a step size of 2000 milliseconds:

```
Router(config)# call spike 30 steps 10 size 2000
```

The following example shows how to configure the **callspike** command in dial peer voice mode with threshold of 20, a sliding window of 7, and a step size of 2000 milliseconds:

```
Router(config)# dial-peer voice 400 voip
Router(config-dial-peer)# call spike 20 steps 7 size 2000
```

Related Commands

Command	Description
dtmf-relay (Voice over IP)	Specifies how an H.323 gateway relays DTMF tones between telephony interfaces and an IP network.
show call spike status	Displays the configuration of the threshold for incoming calls.

call start

To force an H.323 Version 2 gateway to use either fast connect or slow connect procedures for a dial peer, use the **callstart** command in H.323 voice-service configuration mode. To restore the default setting, use the **no** form of this command.

call start {**fast** | **slow** | **system** | **interwork**} [**sync-rsvp slow-start**]
no call start

Syntax Description

fast	Gateway uses H.323 Version 2 (fast connect) procedures.
slow	Gateway uses H.323 Version 1 (slow connect) procedures.
system	Gateway defaults to voice-service configuration mode.
interwork	Gateway interoperates between fast-connect and slow-connect procedures. **Note** The **interwork** keyword is applicable to IP-to-IP gateways only and supports basic audio calls Dual-tone multi-frequency (DTMF), fax, and audio transcoding calls are not supported).
sync-rsvp slow-start	(Optional) Gateway uses Resource Reservation Protocol (RSVP) synchronization for slow-start calls.

Command Default

The gateway defaults to voice-service configuration mode.

Command Modes

H.323 voice-service configuration (conf-serv-h323)

Command History

Release	Modification
12.1(3)XI	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco AS5800, and Cisco MC3810.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XA	This command was changed to use the H.323 voice-service configuration mode from the voice-class configuration mode.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Release	Modification
12.3(4)T	The **synch-rsvpslow-start**keywords were added.
12.3(8)T	The **interwork** keyword was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

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

The **callstart** command is configured as part of the voice class assigned to an individual VoIP dial peer. It takes precedence over the**h323callstart**command that is enabled globally to all VoIP calls, unless the **system** keyword is used, in which case the gateway defaults to Version 2.

The **sync-rsvpslow-start**keyword, when used in H.323 voice-class configuration mode, controls RSVP synchronization for all slow-start calls handled by the gateway. When the **sync-rsvpslow-start**keyword is used in an H.323 voice-class definition, the behavior can be specified for individual dial peers by invoking the voice class in dial-peer voice configuration mode. This command is enabled by default in some Cisco IOS images, and in this situation the **showrunning-config** command displays this information only when the **no**form of the command is used.

Note The **callstart** command supports only H.323 to H.323 calls.

The **interwork** keyword is only used with IP-to-IP gateways connecting fast connect from one side to slow connect on the other for basic audio calls. Configure the **interwork** keyword in voice-class H.323 configuration mode or on both the incoming and outgoing dial peers. Codecs must be specified on both dial peers for interworking to function. When the **interwork** keyword is configured, codecs need to be specified on both dial-peers and the **codectransparent** command should not be configured.

Examples

The following example shows slow connect for the voice class 1000 being selected:

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

The following example shows the gateway configured to use the H.323 Version 1 (slow connect) procedures:

```
h323
 call start slow
```

Related Commands

Command	Description
acc-qos	Selects the acceptable quality of service for a dial peer.

Command	Description
call rsvp-sync	Enables synchronization between RSVP and the H.323 voice signaling protocol.
call rsvp-sync resv-timer	Sets the timer for RSVP reservation setup.
codec transparent	Enables codec capabilities to be passed transparently between endpoints in a Cisco IPIPGW.
debug call rsvp-sync events	Displays the events that occur during RSVP synchronization.
h323	Enables H.323 voice service configuration commands.
req-qos	Selects the desired quality of service to use in reaching a dial peer.
show call rsvp-sync conf	Displays the RSVP synchronization configuration.
show call rsvp-sync stats	Displays statistics for calls that attempted RSVP reservation.
show running-config	Displays the contents of the currently running configuration file.
voice class h323	Enters voice-class configuration mode and creates a voice class for H.323 attributes.

call threshold global

To enable the global resources of a gateway, use the **callthresholdglobal**command in global configuration mode. To disable the global resources of the gateway, use the **no** form of this command.

call threshold global *trigger-name* **low** *percent* **high** *percent* [**busyout**] [**treatment**]
no call threshold global *trigger-name*

Syntax Description

trigger -name	Specifies the global resources on the gateway. The *trigger-name*argument can be one of the following: • **cpu-5sec** --CPU utilization in the last 5 seconds. • **cpu-avg** --Average CPU utilization. • **io-mem** --I/O memory utilization. • **proc-mem** --Processor memory utilization. • **total-calls** --Total number of calls. • **total-mem** --Total memory utilization.
low *percent*	Value of low threshold: Range is 1–100% for the utilization triggers; 1–10000 calls for the total-calls.
high *percent*	Value of high threshold: Range is 1–100% for the utilization triggers; 1–10000 calls for the total-calls.
busyout	(Optional) Busy out the T1/E1 channels if the resource is not available.
treatment	(Optional) Applies call treatment from the session application if the resource is not available.

Command Default

The default is **busyout**and **treatment** for global resource triggers.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The 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(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751 routers. Support for other Cisco platforms is not included in this release

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 in this release.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines



Note YANG model for bandwidth-based CAC configuration is not available.

For example:

call threshold interface type number int-bandwidth class-map name [l2-overhead percentage] | low low-threshold high high-threshold} [midcall-exceed]

Use this command to enable a trigger and define associated parameters to allow or disallow new calls on the router. Action is enabled when the trigger value goes above the value that is specified by the **high** keyword and is disabled when the trigger drops below the value that is specified by the **low**keyword.

You can configure these triggers to calculate Resource Availability Indicator (RAI) information. An RAI is forwarded to a gatekeeper so that it can make call admission decisions. You can configure a trigger that is global to a router or is specific to an interface.

Examples

The following example shows how to busy out the total calls when a low of 5 or a high of 5000 is reached:

```
call threshold global total-calls low 5 high 5000 busyout
```

The following example shows how to busy out the average CPU utilization if a low of 5 percent or a high of 65 percent is reached:

```
call threshold global cpu-avg low 5 high 65 busyout
```

Related Commands

Command	Description
call threshold (interface)	Enables interface resources of a gateway.
call threshold poll-interval	Enables a polling interval threshold for CPU or memory.
clear call threshold	Clears enabled triggers and their associated parameters.
show call threshold	Displays enabled triggers, current values for configured triggers, and number of API calls that were made to global and interface resources.

call threshold interface

To enable interface resources of a gateway, use the **call threshold interface** command in global configuration mode. To disable the interface resources of the gateway, use the **no** form of this command.

call threshold interface *type number* {**int-bandwidth** {**class-map** *name* [**l2-overhead** *percentage*] | **low** *low-threshold* **high** *high-threshold*} [**midcall-exceed**] | **int-calls low** *value* **high** *value*}
no call threshold interface *type number* {**int-bandwidth** | **int-calls**}

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
int-bandwidth	Configures the threshold bandwidth for VoIP media through an interface.
class-map *name*	Specifies a traffic class for the VoIP media traffic that is configured through Modular Quality of Service (MQS).
l2-overhead *percentage*	(Optional) Configures the Layer 2 overhead as the percentage of the configured bandwidth. This is the value by which the configured bandwidth will be deducted to obtain the IP bandwidth. The default value is 10 percent.
low *low-threshold*	Specifies the low threshold for the aggregate interface bandwidth value in Kbps. The range is from 8 to 2000000.
high *high-threshold*	Specifies the high threshold for the aggregate interface bandwidth value in Kbps. The range is from 8 to 2000000.
midcall-exceed	(Optional) Allows the bandwidth that exceeds the configured threshold during midcall media renegotiation.
int-calls	Specifies the number of calls that are transmitted through the interface.
low *value*	Specifies the low threshold for the number of calls allowed. The range is from 1 to 10000.
high *value*	Specifies the high threshold for the number of calls allowed. The range is from 1 to 10000.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The 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.

Release	Modification
12.2(4)XM	This command was implemented on Cisco 1750 and Cisco 1751 routers. This command does not support any other Cisco platforms in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. This command is not supported on Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 routers in this release.
15.2(2)T	This command was modified. The **int-bandwidth**, **class-map** *name*, **l2-overhead** *percentage*, **low** *low-threshold*, **high** *high-threshold*, and **midcall-exceed** keywords and arguments were added.

Usage Guidelines

Use this command to specify thresholds that allow or disallow new calls on the router.

The Bandwidth-Based Call Admission Control feature is supported on the following interfaces:

- ATM
- Ethernet (Fast Ethernet, Gigabit Ethernet)
- Loopback
- Serial

Examples

The following example shows how to enable thresholds as low as 5 and as high as 2500 for interface calls on Ethernet interface 0/1:

```
Router> enable
Router# configure terminal
Router(config)# call threshold interface Ethernet 0/1 int-calls low 5 high
2500
```

The following example shows how to configure the Cisco Unified Border Element (Cisco UBE) to reject new SIP calls when the VoIP media bandwidth on Gigabit Ethernet interface 0/0 exceeds 400 kbps and continues to have 100 Kbps:

```
Router> enable
Router# configure terminal
Router(config)# call threshold interface GigabitEthernet 0/0 int-bandwidth
low 100 high 400
```

The following example shows how to configure Cisco UBE to reject new SIP calls when the VoIP media bandwidth on Gigabit Ethernet interface 0/0 exceeds the configured bandwidth for priority traffic in the “voip-traffic” class:

```
Router> enable
Router# configure terminal
Router(config)# class-map match-all voip-traffic

Router(config-cmap)# policy-map voip-policy
Router(config-pmap)# class  voip-traffic
Router(config-pmap-c)# priority 440
Router(config-pmap-c)# end
```

```
Router# configure terminal
Router(config)# call threshold interface GigabitEthernet 0/0 int-bandwidth
class-map voip-traffic l2-overhead 10
```

Related Commands

Command	Description
call threshold (global)	Enables global resources of a gateway.
call threshold poll-interval	Enables a polling interval threshold for CPU or memory.
clear call threshold	Clears enabled triggers and their associated parameters.
show call threshold	Displays enabled triggers, current values for configured triggers, and the number of API calls that were made to global and interface resources.

call threshold poll-interval

To enable a polling interval threshold for assessing CPU or memory thresholds, use the **callthresholdpoll-interval** command in global configuration mode. To disable this command, use the **no** form of this command.

call threshold poll-interval {**cpu-average** | **memory**} *seconds*
no call threshold poll-interval {**cpu-average** | **memory**}

Syntax Description

cpu -average	The CPU average interval, in seconds. The default is 60.
memory	The average polling interval for the memory, in seconds. The default is 5.
seconds	Window of polling interval, in seconds. Range is from 10 to 300 for the CPU average interval, and from 1 to 60 for the memory average polling interval.

Command Default

cpu -average: 60 seconds**memory**: 5 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The 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(4)XM	This command was implemented on Cisco 1750 and Cisco 1751 routers. This release does not support any other Cisco platforms in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series routers. This release does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.

Examples

The following example shows how to specify that memory thresholds be polled every 10 seconds:

```
call threshold poll-interval memory 10
```

Related Commands

Command	Description
call threshold	Enables the global resources of the gateway.
clear call threshold	Clears enabled triggers and their associated parameters.

Command	Description
show call threshold	Displays enabled triggers, current values for configured triggers, and number of API calls that were made to global and interface resources.

call treatment action

To configure the action that the router takes when local resources are unavailable, use the **call treatment action** command in global configuration mode. To disable call treatment action, use the **no** form of this command.

call treatment action {**hairpin** | **playmsg** *url* | **reject**}
no call treatment action

Syntax Description

hairpin	Hairpins the calls through the POTS dial peer. **Note** The **hairpin** keyword is not available on Cisco 1750 and Cisco 1751 routers.
playmsg	Plays a specified message to the caller.
url	Specifies the URL of the audio file to play.
reject	Disconnects the call and pass-down cause code.

Command Default

No treatment is applied.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series routers. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751 routers. This command does not support any other Cisco platforms in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series in this release.
12.2(2)XA	This command was introduced.

Usage Guidelines

Use the **call treatment action** command to define parameters to disconnect (with cause code), or hairpin, or whether a message or busy tone is played to the user.



Warning Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used, as they do not provide encryption or authentication. Use secure alternatives such as HTTPS, SFTP, or SCP instead.

Examples

The following example shows the warning message displayed for the usage of insecure HTTP protocol:

```
Device(config)#call treatment action playmsg http://10.10.10.70//tftpboot/COLT-DE-CUCM.cfg
SECURITY WARNING - Module: DEFAULT_VOICE_CONFIG, Command: call treatment action playmsg
http://10.10.10.70//tftpboot/COLT-DE-CUCM.cfg,
Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: call treatment action playmsg configured with insecure FTP/HTTP/TFTP URL
protocol,
Remediation: Use secure protocols such as HTTPS, SFTP, or SCP instead of insecure HTTP,
FTP, or TFTP
Device(config)#
```

Examples

The following example shows how to enable the call treatment feature with a "hairpin" action:

```
call treatment on
call treatment action hairpin
```

The following example shows how to enable the call treatment feature with a "playmsg" action. The file "congestion.au" plays to the caller when local resources are not available to handle the call.

```
call treatment on
call treatment action playmsg tftp://keyer/prompts/conjestion.au
```

Related Commands

Command	Description
call threshold	Clears enabled triggers and their associated parameters.
call treatment on	Enables call treatment to process calls when local resources are unavailable.
clear call treatment stats	Clears the call treatment statistics.
show call treatment	Displays the call treatment configuration and statistics for handling calls on the basis of resource availability.

call treatment cause-code

To specify the reason for the disconnection to the caller when local resources are unavailable, use the **call treatment cause-code** command in global configuration mode. To disable the call treatment cause-code specification, use the **no** form of this command.

call treatment cause-code {**busy** | **no-QoS** | **no-resource**}
no call treatment cause-code

Syntax Description

busy	Indicates that the gateway is busy.
no-QoS	Indicates that the gateway cannot provide quality of service (QoS).
no-resource	Indicates that the gateway has no resources available.

Command Default

Disconnect reason is not specified to the caller.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series in this release.
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 routers. This command does not support any other Cisco platforms in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series routers. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to associate a cause-code with a disconnect event.

Examples

The following example shows how to configure a call treatment cause code to reply with "no-Qos" when local resources are unavailable to process a call:

```
call treatment on
call treatment cause-code no-Qos
```

Related Commands

Command	Description
call threshold	Clears enabled triggers and their associated parameters.
call treatment on	Enables call treatment to process calls when local resources are unavailable.
clear call treatment stats	Clears the call treatment statistics.
show call treatment	Displays the call treatment configuration and statistics for handling calls on the basis of resource availability.

call treatment isdn-reject

To specify the rejection cause code for ISDN calls when all ISDN trunks are busied out and the switch ignores the busyout trunks and still sends ISDN calls into the gateway, use the **call treatment isdn-reject** command in global configuration mode. To disable call treatment, use the **no** form of this command.

call treatment isdn-reject *cause-code*
no call treatment isdn-reject

Syntax Description

cause-code **34**	No circuit/channel available—The connection cannot be established because no appropriate channel is available to take the call.
cause-code **38**	Network out of order—The destination cannot be reached because the network is not functioning correctly, and the condition might last for an extended period of time. An immediate reconnect attempt will probably be unsuccessful.
cause-code **41**	Temporary failure—An error occurred because the network is not functioning correctly. The problem will be resolved shortly.
cause-code **42**	Switching equipment congestion—The destination cannot be reached because the network switching equipment is temporarily overloaded.
cause-code **43**	Access information discarded—Discarded information element identifier. The network cannot provide the requested access information.
cause-code **44**	Requested circuit/channel not available—The remote equipment cannot provide the requested channel for an unknown reason. This might be a temporary problem.
cause-code **47**	Resources unavailable, unspecified—The requested channel or service is unavailable for an unknown reason. This might be a temporary problem.

Command Default

No value is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series in this release.
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 routers. This command does not support any other Cisco platforms in this release.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series routers. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command only when all ISDN trunks are busied out and the switch ignores the busyout trunks and still sends ISDN calls into the gateway. The gateway should reject the call in the ISDN stack using the configured cause code.

Under any other conditions, the command has no effect.

Examples

The following example shows how to configure the call treatment to reply to an ISDN call with an ISDN rejection code for "temporary failure" when local resources are unavailable to process a call:

```
call treatment on
call treatment isdn-reject 41
```

Related Commands

Command	Description
call threshold	Clears enabled triggers and their associated parameters.
call treatment on	Enables call treatment to process calls when local resources are unavailable.
clear call treatment stats	Clears the call treatment statistics.
show call treatment	Displays the call treatment configuration and statistics for handling calls on the basis of resource availability.

call treatment on

To enable call treatment to process calls when local resources are unavailable, use the **call treatment on**command in global configuration mode. To disable call treatment, use the **no** form of this command.

call treatment on
no call treatment on

Syntax Description

This command has no arguments or keywords.

Command Default

Treatment is inactive.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series in this release.
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 routers. This command does not support any other Cisco platforms in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series routers. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to enable a trigger and define associated parameters to disconnect (with cause code), or hairpin, or whether a message or busy tone is played to the user.

Examples

The following example shows how to enable the call treatment feature with a "hairpin" action:

```
call treatment on
call treatment action hairpin
```

The following example shows how to enable the call treatment feature with a "playmsg" action. The file "congestion.au" plays to the caller when local resources are not available to handle the call.

```
call treatment on
call treatment action playmsg tftp://keyer/prompts/conjestion.au
```

The following example shows how to configure a call treatment cause code to reply with "no-QoS" when local resources are unavailable to process a call:

```
call treatment on
call treatment cause-code no-QoS
```

Related Commands

Command	Description
call threshold	Clears enabled triggers and their associated parameters.
call treatment action	Configures the action that the router takes when local resources are unavailable.
call treatment cause-code	Specifies the reason for the disconnection to the caller when local resources are unavailable.
call treatment isdn-reject	Specifies the rejection cause-code for ISDN calls when local resources are unavailable.
clear call treatment stats	Clears the call treatment statistics.
show call treatment	Displays the call treatment configuration and statistics for handling calls on the basis of resource availability.

call-waiting

To enable call waiting, use the **call-waiting**command in interface configuration mode. To disable call waiting, use the **no** form of this command.

call-waiting
no call-waiting

Syntax Description

This command has no arguments or keywords.

Command Default

Call waiting is enabled.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

This command is applicable to Cisco 800 series routers.

You must specify this command when creating a dial peer. This command does not work if it is not specified within the context of a dial peer. For information on creating a dial peer, refer to the *Cisco800SeriesRoutersSoftwareConfigurationGuide*.

Examples

The following example disables call waiting:

```
no call-waiting
```

Related Commands

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

called-number (dial peer)

To enable an incoming Voice over Frame Relay (VoFR) call leg to get bridged to the correct plain old telephone service (POTS) call leg when a static FRF.11 trunk connection is used, use the **callednumber**command in dial peer configuration mode. To disable a static trunk connection, use the **no** form of this command.

called-number *string*
no called-number

Syntax Description

string	A string of digits, including wildcards, that specifies the telephone number of the voice port dial peer.

Command Default

This command is disabled.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

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

Usage Guidelines

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

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

Examples

The following example shows how to configure a static FRF.11 trunk connection to a specific telephone number (555-0150), beginning in global configuration mode:

```
voice-port 1/0/0
 connection trunk 55Router0
 exit
dial-peer voice 100 pots
 destination pattern 5550150
 exit
dial-peer voice 200 vofr
 session protocol frf11-trunk
 called-number 5550150
 destination pattern 55Router0
```

Related Commands

Command	Description
codec (dial peer)	Specifies the voice coder rate of speech for a VoFR dial peer.
connection	Specifies a connection mode for a voice port.

Command	Description
destination pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dtmf relay (VoFR)	Enables the generation of FRF.11 Annex A frames for a dial peer.
fax rate	Establishes the rate at which a fax is sent to the specified dial peer.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.
session protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
signal type	Sets the signaling type to be used when connecting to a dial peer.
vad (dial peer)	Enables VAD for the calls using a particular dial peer.