SIP: Measurement-Based Call Admission Control for SIP

The Measurement-Based Call Admission Control for Session Initiation Protocol (SIP) feature implements support within SIP to monitor IP network capacity and reject or redirect calls based on congestion detection. This feature does the following:

- Verifies that adequate resources are available to carry a successful VoIP session.
- Implements a mechanism to prevent calls arriving from the IP network from entering the gateway when required resources are not available to process the call.
- Supports measurement-based call admission control (CAC) processes.

Feature Specifications for the Measurement-Based Call Admission Control for SIP Feature

Feature History	
Release	**Modification**
12.2(15)T	This feature was introduced.
Supported Platforms	
Cisco 2610, Cisco 2611, Cisco 2612, Cisco 2613, Cisco 2620, Cisco 2621, Cisco 2650, Cisco 2651, Cisco 2691, Cisco 3620, Cisco 3631, Cisco 3640, Cisco 3725, Cisco 3745, Cisco 7200, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco CVA 120, and Cisco uBR945	

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- Prerequisites for Measurement-Based Call Admission Control for SIP, page 2
- Restrictions for Measurement-Based Call Admission Control for SIP, page 2
- Information About Measurement-Based Call Admission Control for SIP, page 3
- How to Configure Measurement-Based Call Admission Control for SIP, page 7
- Configuration Examples for Measurement-Based Call Admission Control for SIP, page 18

- Additional References, page 19
- Command Reference, page 19
- Glossary, page 22

Prerequisites for Measurement-Based Call Admission Control for SIP

- Before this feature can be operational, a basic VoIP network must be configured. For more information about configuring VoIP, refer to:

  Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2.
- By default, gateways support reliable provisional responses. That is, no additional configuration tasks are necessary to enable reliable provisional responses. For more information about configuring reliable provisional responses including reenabling the feature if it was disabled, refer to:

  SIP Gateway Support of RSVP and TEL URL
- Enable Service Assurance Agent (SAA) Responder on the originating and terminating gateway. For more information about configuring Service Assurance Agent, refer to:

  Network Monitoring Using Cisco Service Assurance Agent

Restrictions for Measurement-Based Call Admission Control for SIP

- When detecting network congestion, the PSTN fallback feature does not affect an existing call; it affects only subsequent calls.
- Only a single calculated planning impairment factor (ICPIF) delay or loss value is allowed per system.
- A small additional call setup delay can be expected for the first call to a new IP destination.
- The Service Assurance Agent Responder feature, a network congestion analysis mechanism, cannot be configured for non-Cisco devices.

Information About Measurement-Based Call Admission Control for SIP

To configure Measurement-Based Call Admission Control for SIP, you need to understand the following concepts:

- Benefits of Measurement-Based Call Admission Control for SIP, page 3
- Feature Design of Measurement-Based Call Admission Control for SIP, page 3

Benefits of Measurement-Based Call Admission Control for SIP

PSTN Fallback

- Automatically routes a call to an alternate destination when the data network is congested at the time of call setup, thereby enabling higher call completion rates.
- Enables the service provider to give a reasonable guarantee about the quality of the conversation to VoIP users at the time of call admission.
- PSTN fallback provides network congestion measurement, including delay, jitter, and packet loss information for the configured IP addresses.
- A new call need not wait for probe results before being admitted, thereby minimizing delays.

Call Admission Control

- Configurable call treatment allows the Internet service provider (ISP) the flexibility to configure how the call will be treated when local resources to process the call are not available.
- Resource unavailable signaling allows you to automatically busy out channels when local resources are not available to handle the call.
- User-selected thresholds allow you the flexibility to configure thresholds to determine resource availability.

Feature Design of Measurement-Based Call Admission Control for SIP

Before the CAC feature was developed, gateways did not have a mechanism to check for IP network congestion and resource unavailability. Although quality of service (QoS) mechanisms provide a level of low latency and guaranteed delivery that is required for voice traffic, CAC mechanisms are intended to extend the capabilities of QoS to protect voice traffic from being negatively affected by other voice traffic. CAC is used to gracefully deny network access under congestion conditions and provide alternative call rerouting to prevent dropped or delayed calls. There are a variety of CAC mechanisms, including the following:

- Measurement-based CAC, which uses probes to look ahead into the packet network to gauge the state of the network to determine whether to allow a new call.
- Resource-based CAC, which calculates resources needed for the call, determines their availability, and reserves those resources.

The Measurement-Based Call Admission Control for SIP feature provides an alternative to Resource Reservation Protocol (RSVP) for VoIP service providers that do not deploy RSVP.

The new feature implements measurement-based CAC using the mechanisms described in the following sections:

- Service Assurance Agents
- Calculated Planning Impairment Factor
- PSTN Fallback
- Call Admission Thresholds
- Call Treatment Options
- Resource Unavailable Signaling

Service Assurance Agents

Service Assurance Agents (SAA) is a generic network management feature that provides a mechanism for network congestion analysis. SAA determine latency, delay, and jitter and provides real-time ICPIF calculations before establishing a call across an IP infrastructure. The SAA Responder feature uses SAA probes to traverse the network to a given IP destination and measure the loss and delay characteristics of the network along the path traveled. These values are returned to the outgoing gateway to use in making a decision on the condition of the network and its ability to carry a call. Threshold values for rejecting a call are configured at the outgoing gateway. See the "PSTN Fallback" section.

Each probe consists of multiple packets, a configurable parameter of this feature. SAA packets emulate voice packets and receive the same priority as voice throughout the entire network. The delay, loss, and ICPIF values entered into the cache for the IP destination are averaged from all the responses. If the call uses G.729 and G.711 codecs, the probe packet sizes mimic those of a voice packet for that codec. Other codecs use G.711-like probes. In Cisco IOS software releases later than Release 12.1(3)T, other codec choices may also be supported with their own specific probes.

The IP precedence of the probe packets can also be configured to simulate the priority of a voice packet more closely. This parameter should be set equal to the IP precedence used for other voice media packets in the network.

SAA probes used for CAC go out randomly on ports selected from within the top end of the audio User Datagram Protocol (UDP) defined port range (16384 to 32767). Probes use a packet size based on the codec the call will use. IP precedence can be set if desired, and a full Realtime Transport Protocol (RTP), UDP, or IP header is used just as a real voice packet would carry. The SAA Responder feature was called Response Time Reporter (RTR) in earlier releases of Cisco IOS software.

The SAA Responder feature can not be configured for non-Cisco devices. For a complete description of SAA configuration, refer to the "Network Monitoring Using Cisco Service Assurance Agent" chapter of the Release 12.1 *Cisco IOS Configuration Fundamentals Configuration Guide.*

Calculated Planning Impairment Factor

The Measurement-Based Call Admission Control for SIP feature supports the determination of ICPIF, as specified by International Telecommunications Union (ITU) standard G.113. The SIP subsystem calculates an impairment factor for network conditions to a particular IP address. ICPIF checks for end-to-end resource availability by calculating a Total Impairment Value, which is a function of codecs used and loss or delay of packets. You can configure router resources to make call admission decisions, using either the ICPIF threshold, or by setting delay and loss thresholds.

Configurable ICPIF values that represent the ITU specification for quality of voice as described in G.113 are the following:

- 5—Very good
- 10—Good

- 20—Adequate
- 30—Limiting case
- 45—Exceptional limiting case
- 55—Customers likely to react strongly

The default value is 20. SAA probe delay and loss information is used in calculating an ICPIF value, which is then used as a threshold for CAC decisions. You can base such decisions on either the ITU interpretation described or on the requirements of an individual customer network.

PSTN Fallback

The Measurement-Based Call Admission Control for SIP feature supports PSTN Fallback, which monitors congestion in the IP network and either redirects calls to the public switched telephone network (PSTN) or rejects calls based on network congestion. Calls can be rerouted to an alternate IP destination or to the PSTN if the IP network is found unsuitable for voice traffic at that time. You can define congestion thresholds based on the configured network. This functionality allows the service provider to give a reasonable guarantee about the quality of the conversation to VoIP users at the time of call admission.

Note PSTN Fallback does not provide assurances that a VoIP call that proceeds over the IP network is protected from the effects of congestion. This is the function of the other QoS mechanisms, such as IP Real-Time Transport Protocol (RTP) priority or low latency queueing (LLQ).

PSTN Fallback includes the following capabilities:

- Provides the ability to define the congestion thresholds based on the network.
  - Defines a threshold based on ICPIF, which is derived as part of ITU G.113. See the "Service Assurance Agents" section.
  - Defines a threshold based solely on packet delay and loss measurements.
- Uses SAA probes to provide packet delay, jitter, and loss information for the relevant IP addresses. Based on the packet loss, delay, and jitter encountered by these probes, an ICPIF or delay or loss value is calculated.
- Supports calls of any codec. Only G.729 and G.711 have accurately simulated probes. Calls of all other codecs are emulated by a G.711 probe.

Caution Configuring **call fallback active** in a gateway creates an SAA jitter probe against other (target) gateways to which the calls are sent. In order for the **call fallback active** to work properly, the target gateways must have the **rtr responder** command (in Cisco IOS releases prior to 12.3(14)T) or the **ip sla monitor responder** command (in Cisco IOS Release 12.3(14)T or later) in their configurations. If one of these commands is not included in the configuration of each target gateway, calls to the target gateway will fail.

The call fallback subsystem has a network traffic cache that maintains the ICPIF or delay or loss values for various destinations. This capability helps performance, because each new call to a well-known destination need not wait for a probe to be admitted because the value is usually cached from a previous call.

Once the ICPIF or delay or loss value is calculated, they are stored in a fallback cache where they remain until the cache ages out or overflows. Until an entry ages out, probes are sent periodically for that particular destination. This time interval is configurable.

Media Information for Fallback Services

SIP reliable provisional responses ensure that media information is exchanged and that resource and network checks can take place prior to connecting the call. The following SIP methods have been implemented to support fallback services:

- INVITE with Session Description Protocol (SDP) body. The PSTN Fallback feature provides support for a new attribute line, a=rtr, in the SDP message body. The rtr attribute enables support for invoking fallback services. The INVITE message with SDP body provides media connection information, including IP address and negotiated codec.
- Provisional Acknowledgment (PRACK). PRACK allows reliable exchanges of SIP provisional responses between SIP endpoints. When the INVITE message has no SDP body, that is, no delayed media, the terminating gateway sends media information in the 183 Session Progress message and expects the SDP from the originating gateway in the PRACK message.
- Conditions Met (COMET), which indicates if the preconditions for a given call have been met.

Call Admission Thresholds

User-selected thresholds allow you to configure call admission thresholds for local resources and end-to-end memory and CPU resources. You can configure two thresholds, high and low, for each global or interface-related resource. The specified call treatment is triggered when the current value of a resource goes beyond the configured high, and remains in effect until the current resource value falls below the configured low.

Call Treatment Options

You can select how the call should be treated when local resources are not available to handle the call. For example, when the current resource value for any one of the configured triggers for call threshold exceeds the configured threshold, you have the following the call treatment choices:

- TDM hairpinning—Hairpins the calls through the POTS dial peer.
- Reject—Disconnects the call.
- Play message or tone—Plays a configured message or tone to the user.

Resource Unavailable Signaling

The Resource Unavailable Signaling feature supports autobusyout capability, which busies out channels when local resources are not available to handle the call. Autobusyout is supported on both channel-associated signaling (CAS) and primary rate interface (PRI) channels:

- CAS—Uses busyout to signal local resources are unavailable.
- PRI—Uses either service messages or disconnect with correct cause-code to signal resources are unavailable.

How to Configure Measurement-Based Call Admission Control for SIP

This section contains the following procedures:

- Configuring SAA Responder, page 7 (required)
- Configuring PSTN Fallback, page 8 (required)
- Configuring Resource Availability Check, page 10 (required)
- Configuring SIP Reliable Provisional Response, page 14 (required)

Configuring SAA Responder

Perform this task to enable SAA Responder functionality on the destination node.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **rtr responder**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**rtr responder** **Example:** `Router(config)# rtr responder`	Enables SAA Responder functionality on a device.
Step 4	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Configuring PSTN Fallback

PSTN fallback configuration applies to both inbound and outbound gateways. In most networks, gateways generate calls to each other, so that every gateway is both an outgoing gateway and a terminating gateway.

Prerequisites

The destination node, which is often but not necessarily the terminating gateway, should be configured with the SAA Responder feature.

Restrictions

PSTN fallback configuration is done at the global level and therefore applies to all calls attempted by the gateway. You cannot selectively apply PSTN fallback only to calls initiated by specific PSTN or PBX interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call fallback active**
4. **call fallback cache size** *number*
5. **call fallback instantaneous-value-weight** *weight*
6. **call fallback jitter-probe num-packets** *number-of-packets*
7. **call fallback jitter-probe precedence**
8. **call fallback jitter-probe priority-queue**
9. **call fallback threshold delay** *value* **loss** *value*
10. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	**`call fallback active`** **Example:** `Router(config) # call fallback active`	(Required) Enables a call request to fall back to alternate dial peers in case of network congestion. • The **active** keyword enables a call request to fall back to alternate dial peers in case of network congestion. • Configuring **call fallback active** in a gateway creates an SAA jitter probe against other (target) gateways to which the calls are sent. In order for the **call fallback active** to work properly, the target gateways must have the **rtr responder** command (in Cisco IOS releases prior to 12.3(14)T) or the **ip sla monitor responder** command (in Cisco IOS Release 12.3(14)T or later) in their configurations. If one of these commands is not included in the configuration of each target gateway, calls to the target gateway will fail.
Step 4	**`call fallback cache size`** *`number`* **Example:** `Router(config) # call fallback cache size 128`	Specifies the call fallback cache size for network traffic probe entries. • Specifies the cache size in number of entries. The valid range is from 1 to 256. Default is 128 entries.
Step 5	**`call fallback instantaneous-value-weight`** *`weight`* **Example:** `Router(config) # call fallback instantaneous-value-weight 50`	Configures the call fallback subsystem to determine an average value based on the last two probes registered in the cache for call requests. • This command allows the call fallback subsystem to recover gradually from network congestion conditions. When a new probe is received, the subsystem calculates in percent how much to rely upon the new probe, and how much to rely upon the previous cache entry. The configured weight applies to the new probe first. Range is from 0 to 100 percent. Default is 66 percent.
Step 6	**`call fallback jitter-probe num-packets`** *`number-of-packets`* **Example:** `Router(config) # call fallback jitter-probe num-packets 15`	Specifies the number of packets in a jitter probe used to determine network conditions. • The *number-of-packets* argument specifies the number of packets value. Range is from 2 to 50. Default is 15.
Step 7	**`call fallback jitter-probe precedence`** ***`precedence-value`*** **Example:** `Router(config) # call fallback jitter-probe precedence 2`	Specifies the priority of the jitter-probe transmission by setting the IP precedence of IP packets. • The *precedence-value* argument specifies the jitter-probe precedence. Range is from 0 to 6. Default is 2.
Step 8	**`call fallback jitter-probe priority-queue`** **Example:** `Router(config) # call fallback jitter-probe priority-queue 32767`	Assign a priority-queue for jitter-probe transmissions. • IP priority queueing must be set for UDP voice ports 16384 to 32767.

	Command or Action	Purpose
Step 9	**call fallback threshold delay** *value* **loss** *value* **Example:** `Router(config) # call fallback threshold delay 36000 loss 50`	Configures the call fallback threshold to use only specified packet delay and loss values.
Step 10	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Configuring Resource Availability Check

To enable resource availability checking, perform the tasks in the following sections:

- Configuring Global Resources
- Configuring Interface Resources

Configuring Global Resources

To configure resource availability checking for global resources, perform the following task:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call threshold global** *trigger-name* **low** *value* **high** *value* [**busyout** | **treatment**]
4. **call treatment** {**on** | **action** *action* [*value*] | **cause-code** *cause-code* | **isdn-reject** *value*}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 3	`Router(config)# call threshold global trigger-name low value high value [busyout][treatment]`
	
	Example:
	`Router(config)# call threshold global total-calls low 5 high 1000 busyout`
		Enables a trigger and defines associated parameters to allow or disallow new calls on the router. Action is enabled when the trigger value exceeds the value specified by the **high** keyword and is disabled when the trigger value drops below the value specified by the **low** keyword.
		• The *trigger-name* argument specifies the global resources on the gateway to be used as call admission or utilization triggers. 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**—IO memory utilization.
		– **proc-mem**—processor memory utilization.
		– **total-calls**— total number of calls.
		– **total-mem**— total memory utilization.
		• **low** *value*— Value of low threshold: Range is from 1 to 100 percent for utilization triggers, and from 1 to 10000 for **total-calls**.
		• **high** *value*— Value of high threshold: Range is from 1 to 100 percent for utilization triggers, and from 1 to 10000 for **total-calls**.
		• **busyout**— (Optional) Busies out the T1 or E1 channels if the resource is not available.
		• **treatment**— (Optional) Applies call treatment from the session application if the resource is not available.

	Command or Action	Purpose

Step 4	`Router(config)# call treatment {on | action action [value]| cause-code cause-code | isdn-reject value}`
	
	Example:
	`Router(config)# call treatment action cause-code 17`
		Configures how calls should be processed when local resources are unavailable.
		• The **on** keyword enables call treatment from the default session application
		• The **action** keyword specifies the action to be taken when call treatment is triggered. The *action* argument can be one of the following:
		– The *hairpin* argument specifies hairpinning action.
		– The *playmsg* argument specifies that the gateway play the selected message. The optional *value* argument specifies the audio file to play in URL format.
		– The *reject* argument specifies whether the call should be disconnected and the ISDN cause code passed.
		• The **cause-code** keyword specifies the reason for disconnection to the caller, where the *cause-code* argument can be one of the following:
		– The *busy* argument indicates that the gateway is busy.
		– The *no-QoS* indicates that the gateway cannot provide quality of service (QOS).
		– The *no-resource* argument indicates that the gateway has no resources available.
		• The **isdn-reject** keyword applies to ISDN interfaces only and specifies the ISDN reject cause code. Range for the *value* argument is 34 to 47 (ISDN cause code for rejection).
		Note The **isdn-reject** keyword takes effect only when all ISDN trunks are busied out and the switch ignores the busyout trunks and still sends ISDN calls into the gateway. Otherwise the keyword has no effect.

Step 5	`end`
	
	Example:
	`Router(config)# end`
		Exits to privileged EXEC mode.

Configuring Interface Resources

To configure resource availability checking for interface resources, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **call threshold interface** *interface-name interface-number* **int-calls low** *value* **high** *value*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)#` **call threshold interface** *interface-name interface number* **int-calls low** *value* **high** *value* **Example:** `Router(config)# call threshold interface ethernet 0 int-calls low 5 high 2500`	Allows threshold values to be configured for total numbers of voice calls placed through a particular interface. This command is used to allow or disallow admission for new calls on the router. • The *interface-name* argument *s*pecifies the interface used in making call admission decisions. Types of interfaces and their numbers will depend upon the configured interfaces. • The *interface-number* argument specifies the number of calls through the interface that triggers a call admission decision. • The **int-calls** keyword configures the gateway to use the number of calls through the interface as a threshold. • The **low** keyword enables the specified **call treatment** until the number of calls through the interface drops below the configured **low** *value.* – The *value* argument specifies the number of calls used to make call admission decisions. Range is from 1 to 10000 calls. • The **high** keyword enables the specified **call treatment** until the number of calls through the interface exceeds the configured **high** *value.* – The *value* argument specifies the number of calls used to make call admission decisions. Range is from 1 to 10000 calls.
Step 4	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Configuring SIP Reliable Provisional Response

By default, gateways support reliable provisional responses. That is, no additional configuration tasks are necessary to enable reliable provisional responses. For more details, refer to the document *SIP Gateway Support of RSVP and TEL URL.*

This task enables reliable provisional response if it was disabled using the **no rel1xx** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **rel1xx** {**default** | **supported** *value* | **require** *value* | disable
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)#` **voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode.
Step 4	`Router(config-voi-serv)#` **sip** **Example:** `Router (config-voi-serv)# sip`	Enters SIP configuration mode.

	Command or Action	Purpose

Step 5	`Router(sip-ua)# rel1xx {default | supported value | require value |disable}`
	
	Example:
	`Router(conf-serv-sip)# rel1xx supported 100rel`
		Enables reliable provisional responses on VoIP calls.
		• Default is **supported** with the 100rel value.

Step 6	`Router(conf-serv-sip)# exit` **Example:** `Router(conf-serv-sip)# exit`	Exits SIP configuration mode.

Verifying Measurement-Based Call Admission Control for SIP

This task verifies that the Measurement-Based Call Admission Control for SIP feature is working.

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **show sip-ua statistics**
4. **show call fallback cache**
5. **show call fallback config**
6. **show call fallback stats**
7. **test call fallback probe** *ip-address codec*

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`show running-config`
	
	Example:
	`Router# show running-config`
		Displays running configuration.

Step 3	`Router(config)# show sip-ua statistics`
	
	Example:
	`Router# show sip-ua statistics`
		Displays SIP user agent statistics, including reliable provisional response information.

	Command or Action	Purpose
Step 4	`Router# show call fallback cache` **Example:** `Router# show call fallback cache`	Displays the current ICPIF estimates for all IP addresses in the cache.
Step 5	`Router# show call fallback config` **Example:** `Router# show call fallback config`	Displays the call fallback configuration.
Step 6	`Router# show call fallback stats` **Example:** `Router# show call fallback stats`	Displays call fallback statistics.

Step 7	`Router# test call fallback probe ip-address`
	
	Example:
	`Router# test call fallback probe 10.1.1.1 codec g711ulaw`
		Tests a probe to a specific IP address and displays ICPIF RTR values.

Troubleshooting Tips

- Make sure VoIP is working before call fallback is configured.
- Use the **debug call fallback detail** command to display details of the VoIP call fallback.
- Use the **debug call fallback probe** command to verify that probes are being sent correctly.
- Use the **debug sip messages** command to enable CCSIP SPI messages debugging trace.
- Use the **debug sip error** command to enable SIP error debugging trace.
- Use the **debug sip all** command to enable all SIP debugging traces.

Examples

This section provides sample debugging output for the following commands:

- Configuration output for the debug rtr trace Command
- Configuration output for the debug call fallback probe Command

Configuration output for the debug rtr trace Command

```
Router# debug rtr trace

Router#
*Mar  1 00:11:42.439: RTR 1: Starting An Echo Operation - IP RTR Probe 1
*Mar  1 00:11:42.439: rtt hash insert : 10.1.1.63 32117
*Mar  1 00:11:42.439:    source=10.1.1.63(32117)  dest-ip=10.1.1.67(32057) vrf tableid = 0
*Mar  1 00:11:42.439: sending control enable:
*Mar  1 00:11:42.439: cmd: command: , ip: 10.1.1.67, port: 32057, duration: 1200
*Mar  1 00:11:42.439: sending control msg:
*Mar  1 00:11:42.439:  Ver: 1 ID: 20 Len: 52
*Mar  1 00:11:42.443: receiving reply
*Mar  1 00:11:42.443:  Ver: 1 ID: 20 Len: 8
*Mar  1 00:11:42.459: sdTime: -1989906017 dsTime: 2076306018
```

```
*Mar  1 00:11:42.459:  responseTime (1): 1
*Mar  1 00:11:42.479: sdTime: -1989906017 dsTime: 2076306017
*Mar  1 00:11:42.479: jitterOut: 0
*Mar  1 00:11:42.479: jitterIn: -1
*Mar  1 00:11:42.479:  responseTime (2): 1
*Mar  1 00:11:42.499: sdTime: -1989906017 dsTime: 2076306017
*Mar  1 00:11:42.499: jitterOut: 0
*Mar  1 00:11:42.499: jitterIn: 0
*Mar  1 00:11:42.499:  responseTime (3): 1
*Mar  1 00:11:42.519: sdTime: -1989906017 dsTime: 2076306017
*Mar  1 00:11:42.519: jitterOut: 0
*Mar  1 00:11:42.519: jitterIn: 0
*Mar  1 00:11:42.519:  responseTime (4): 1
*Mar  1 00:11:42.539: sdTime: -1989906017 dsTime: 2076306017
*Mar  1 00:11:42.539: jitterOut: 0
*Mar  1 00:11:42.539: jitterIn: 0
*Mar  1 00:11:42.539:  responseTime (5): 1
*Mar  1 00:11:42.559: sdTime: -1989906017 dsTime: 2076306017
*Mar  1 00:11:42.559: jitterOut: 0
*Mar  1 00:11:42.559: jitterIn: 0
*Mar  1 00:11:42.559:  responseTime (6): 1
*Mar  1 00:11:42.579: sdTime: -1989906017 dsTime: 2076306017
*Mar  1 00:11:42.579: jitterOut: 0
*Mar  1 00:11:42.579: jitterIn: 0
*Mar  1 00:11:42.579:  responseTime (7): 1
*Mar  1 00:11:42.599: sdTime: -1989906017 dsTime: 2076306017
*Mar  1 00:11:42.599: jitterOut: 0
*Mar  1 00:11:42.599: jitterIn: 0
*Mar  1 00:11:42.599:  responseTime (8): 1
*Mar  1 00:11:42.619: sdTime: -1989906017 dsTime: 2076306017
*Mar  1 00:11:42.619: jitterOut: 0
*Mar  1 00:11:42.619: jitterIn: 0
*Mar  1 00:11:42.619:  responseTime (9): 1
*Mar  1 00:11:42.639: sdTime: -1989906017 dsTime: 2076306017
*Mar  1 00:11:42.639: jitterOut: 0
*Mar  1 00:11:42.639: jitterIn: 0
*Mar  1 00:11:42.639:  responseTime (10): 1
*Mar  1 00:11:42.639: rtt hash remove: 10.1.1.63 32117

Router# debug rtr trace

Router#
*Mar  1 00:14:12.439: RTR 1: Starting An Echo Operation - IP RTR Probe 1
*Mar  1 00:14:12.439: rtt hash insert : 10.1.1.63 32117
*Mar  1 00:14:12.439:    source=10.1.1.63(32117)  dest-ip=10.1.1.67(32057) vrf tableid = 0
*Mar  1 00:14:12.439: sending control enable:
*Mar  1 00:14:12.439: cmd: command: , ip: 10.1.1.67, port: 32057, duration: 1200
*Mar  1 00:14:12.439: sending control msg:
*Mar  1 00:14:12.439:  Ver: 1 ID: 27 Len: 52
*Mar  1 00:14:13.439: control message timeout
*Mar  1 00:14:13.439: sending control msg:
*Mar  1 00:14:13.439:  Ver: 1 ID: 28 Len: 52
*Mar  1 00:14:14.439: control message timeout
*Mar  1 00:14:14.439:    control message failure: 1
*Mar  1 00:14:14.439: rtt hash remove: 10.1.1.63 32117
*Mar  1 00:14:42.439: RTR 1: Starting An Echo Operation - IP RTR Probe 1
*Mar  1 00:14:42.439: rtt hash insert : 10.1.1.63 32117
*Mar  1 00:14:42.439:    source=10.1.1.63(32117)  dest-ip=10.1.1.67(32057) vrf tableid = 0
```

Configuration output for the debug call fallback probe Command

```
Router# debug call fallback probe
```

```
Router#
*Mar  1 00:10:12.439: fb_main: Probe timer expired, 10.1.1.67, codec:g711ulaw
*Mar  1 00:10:12.639: fb_main:NumOfRTT=10, RTTSum=10, loss=0, jitter in=0, jitter out=0->
10.1.1.67, codec:g711ulaw, delay = 28
*Mar  1 00:10:12.639:  g113_calc_icpif: loss=0, expect_factor=10, delay (w/codec
delay)=28, Icpif=0
*Mar  1 00:10:12.639: fb_main: New smoothed values: inst_weight=100, ICPIF=0, Delay=28,
Loss=0 -> 10.1.1.67, codec:g711ulaw
3640SDP#
r  1 00:13:12.439: fb_main: Probe timer expired, 10.1.1.67, codec:g711ulaw
*Mar  1 00:13:14.439: %FALLBACK-3-PROBE_FAILURE: A probe error to 10.1.1.67 occured -
control message failure
*Mar  1 00:13:14.439: fb_main:NumOfRTT=0, RTTSum=0, loss=100, jitter in=0, jitter out=0->
10.1.1.67, codec:g711ulaw, delay is N/A (since loss is 100 percent)
*Mar  1 00:13:14.439:  g113_calc_icpif: loss=100, expect_factor=10, delay is N/A (since
loss is 100 percent), Icpif=64
*Mar  1 00:13:14.439: fb_main: New unsmoothed values: inst_weight=100, ICPIF=64,
Delay=N/A, Loss=100 -> 10.1.1.67, codec:g711ulaw
3/0:23(1) is in busyout state

*Mar  1 00:13:22.435: %LINK-3-UPDOWN: Interface ISDN-VOICE 3/0:23(1), changed state to
Administrative Shutdown
*Mar  1 00:13:22.439: %ISDN-6-LAYER2DOWN: Layer 2 for Interface Se3/0:23, TEI 0 changed to
down
```

Configuration Examples for Measurement-Based Call Admission Control for SIP

- Configuring SAA Responder Example, page 18
- Configuring PSTN Fallback Example, page 18
- Configuring Resource Availability Example, page 19
- Configuring Reliable Provisional Response Example, page 19

Configuring SAA Responder Example

The following example enables SAA Responder functionality.

```
Router(config)# rtr responder
```

Configuring PSTN Fallback Example

The following example configures fallback to alternate dial peers in case of network congestion.

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

Caution Configuring **call fallback active** in a gateway creates an SAA jitter probe against other (target) gateways to which the calls are sent. In order for the **call fallback active** to work properly, the target gateways must have the **rtr responder** command (in Cisco IOS releases prior to 12.3(14)T) or the **ip sla monitor**

responder command (in Cisco IOS Release 12.3(14)T or later) in their configurations. If one of these commands is not included in the configuration of each target gateway, calls to the target gateway will fail.

Configuring Resource Availability Example

The following example will busy out the total-calls resource if a low of 5 or a high of 5000 is received:

```
Router (config)# call threshold global total-calls low 5 high 5000 busyout
```

The following example will busy out the average CPU utilization if a low of 5 percent or if a high of 65 percent is received:

```
Router(config)# call threshold global cpu-avg low 5 high 65 busyout
```

The following example enables the call treatment feature with a hairpin action:

```
Router(config)# call treatment on
Router(config)# call treatment action hairpin
```

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

```
Router(config)# call treatment on
Router(config)# call treatment cause-code no-Qos
```

The following example enables thresholds of 5 for a low and 2500 as a high value for interface calls on Ethernet interface 0:

```
Router(config)# call threshold interface Ethernet 0 int-calls low 5 high 2500
```

Configuring Reliable Provisional Response Example

The following example shows how to enable SIP provisional responses (other than 100 Trying) to be sent reliably to the remote SIP endpoint by setting the **rel1xx** command to the value 100rel:

```
Router(config)# voice service voip
Router(config-voi-serv)# sip
Router(conf-serv-sip)# rel1xx supported 100rel
```

Additional References

For additional information related to the Measurement-Based Call Admission Control for SIP feature, see the following sections:

- Related Documents
- Standards
- MIBs
- RFCs
- Technical Assistance

Related Documents

Related Topic	Document Title
Call fallback	*PSTN Fallback*
Reliable provisional responses	*SIP Gateway Support of RSVP and TEL URL*
Service assurance agents	*Network Monitoring Using Cisco Service Assurance Agent* *Configuring Cisco Service Assurance Agent*
Service assurance agents	*Network Monitoring Using Cisco Service Assurance Agent*
IP configuration tasks	*Cisco IOS IP Configuration Guide*, Release 12.2
IP configuration commands	*Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2
VoIP configuration tasks	*Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2
VoIP configuration	*Voice over IP for the Cisco AS5300*
VoIP configuration	*Voice over IP for the Cisco AS5800*
VoIP configuration	*Voice over IP for the Cisco 2600/3600 Series*
Calculated planning impairment factor	*Managing Voice Quality with Cisco Voice Manager (CVM) and Telemate*
Call Admission Control	*VoIP Call Admission Control,* "Advanced Voice Busyout" chapter

Standards

Standards[1]	Title

1. Not all supported standards are listed.

MIBs

MIBs[1]	MIBs Link
•	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

1. Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Command Reference

This feature uses no new or modified commands. All commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

Glossary

CAS—channel-associated signaling. The transmission of signaling information within the voice channel.

cause codes—Code that indicates the reason for PSTN call failure or completion.

CLI—command-line interface.

codec—coder-decoder. Integrated circuit device that typically uses pulse code modulation to transform analog signals into a digital bit stream and digital signals back into analog signals. In Voice over IP, Voice over Frame Relay, and Voice over ATM, a DSP software algorithm used to compress/decompress speech or audio signals.

COMET—conditions met. A SIP method that indicates if the preconditions for a given call or session have been met.

dial peer—An addressable call endpoint that contains configuration information including voice protocol, a codec type, and a telephone number associated with the call endpoint. There are four kinds of dial peers: POTS, VoIP, VoFR, and VoATM.

endpoint—A terminal or gateway that acts as a source or sink of voice data. An endpoint can call or be called, and it generates or terminates the information stream.

hairpinning—A call routing capability in which an incoming call on a specific gateway is signaled through the IP network and back out the same gateway.

INVITE—A message that initiates a session. It indicates that a user is invited to participate, provides a session description, indicates the type of media, and provides insight regarding the capabilities of the called and calling parties.

IP— Internet Protocol. A connectionless protocol that operates at the network layer (Layer 3) of the OSI model. IP provides features for addressing, type-of-service specification, fragmentation and reassemble, and security. Defined in RFC 791. This protocol works with TCP and is usually identified as TCP/IP. See TCP/IP.

ICPIF—Calculated Planning Impairment Factor. Calculated and used as per the ITU G.113 specification. The ICPIF numbers represent predefined combinations of loss and delay. Packet loss and delay determine the threshold for initiating the busyout state.

ISDN—Integrated Services Digital Network. Communication protocol offered by telephone companies that permits telephone networks to carry data, voice, and other source traffic.

ITSP—Internet telephony service provider.

LLQ—low latency queueing. LLQ brings strict priority queueing to class-based weighted fair queueing (CBWFQ). Strict priority queueing allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.

OGW—originating VoIP gateway.

PBX—private branch exchange. A privately owned central switching office.

POTS dial peer—Dial peer connected by a traditional telephony network. POTS peers point to a particular voice port on a voice network device.

PRACK—Provisional Acknowledgment. Allows reliable exchanges of SIP provisional responses between SIP endpoints.

provisional responses—Informational responses that are often used for responding to an INVITE and provide information on call progress. Reliability is not guaranteed when delivered over UDP.

PSTN—Public Switched Telephone Network. PSTN refers to the global network, made up of many local and long distance companies, and various categories in between.

QoS—quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability. QoS refers to the ability of a network to provide better service to selected network traffic over various underlying technologies. QoS is not inherent in a network infrastructure. Rather, you must institute QoS by strategically deploying features that implement it throughout the network.

reliable provisional responses—Provisional responses that guarantee reliability.

RSVP—Resource Reservation Protocol.

RTP—Real-Time Transport Protocol. The protocol provides end-to-end network transport functions for applications sending real-time data and services such as payload type identification, sequence numbering, time-stamping, and delivery monitoring. A network protocol used to carry packetized audio and video traffic over an IP network.

RTR—Response Time Reporter. Works with TCP to carry streaming data over the network. RTP uses packet headers that contain sequencing information, time stamps required to time the output (for example, display of frames) and synchronize different data streams (for example, audio and video), and information on the packet payload, for example, MPEG versus H.261 encoding. This payload descriptor allows RTP to support multiple compression types

SDP—Session Description Protocol. Messages containing capabilities information that are exchanged between gateways.

session—A SIP session is a set of multimedia senders and receivers and the data streams flowing between the senders and receivers. A SIP multimedia conference is an example of a session. The called party can be invited several times by different calls to the same session.

SIP—Session Initiation Protocol. An application-layer protocol originally developed by the Multiparty Multimedia Session Control (MMUSIC) working group of the Internet Engineering Task Force (IETF). Their goal was to equip platforms to signal the setup of voice and multimedia calls over IP networks. SIP features are compliant with IETF RFC 2543, published in March 1999.

TCP—Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmissions. TCP is part of the TCP/IP protocol stack. See also TCP/IP and IP.

TCP/IP—Transmission Control Protocol/Internet Protocol. Common name for the suite of protocols developed by the U.S. Department of Defense in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best known protocols in the suite. See also TCP and IP.

TDM—time-division multiplexing. Technique in which information from multiple channels can be allocated bandwidth on a single wire, based on preassigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to send.

TGW—terminating VoIP gateway.

UA—user agent. A combination of UAS and UAC that initiates and receives calls.

UDP— User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC-768.

URL—uniform resource locator. Standard address of any resource on the Internet that is part of the World Wide Web (WWW).

Voice over IP—Voice over IP enables a router to carry voice traffic, for example, telephone calls and faxes) over an IP network. In Voice over IP, the DSP segments the voice signal into frames, which are then coupled in groups and stored in voice packets that are transported by using IP. The number of samples in a packet depends on the codec and the configuration settings.

Note .Refer to the *Internetworking Terms and Acronyms* for terms not included in this glossary.