PSTN Fallback

The PSTN Fallback feature monitors congestion in the IP network and redirects calls to the Public Switched Telephone Network (PSTN) or rejects calls on the basis of network congestion. This feature can also use the ICMP ping mechanism to detect loss of network connectivity and then reroute calls. The fallback subsystem has a network traffic cache that maintains the Calculated Planning Impairment Factor (ICPIF) or delay/loss values for various destinations. Performance is improved because each new call to a well-known destination does not have to wait on a probe to be admitted and the value is usually cached from a previous call.

ICPIF calculates an impairment factor for every piece of equipment along the voice path and then adds them up to get the total impairment value. Refer to International Telecommunication Union (ITU) standard G.113 for more information. The ITU assigns a value to the types of impairment, such as noise, delay, and echo.

Feature Information

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Information About PSTN Fallback

The VoIP Alternate Path Fallback SNMP Trap feature adds a Simple Network Management Protocol (SNMP) trap generation capability. This feature is built on top of the fallback subsystem to provide an SNMP notification trap when the fallback subsystem redirects or rejects a call because a network condition has failed to meet the configured threshold. The SNMP trap provides VoIP management status MIB information without flooding management systems with unnecessary messages about call status by triggering only when a call has been redirected to the public switched telephone network (PSTN) or the alternative IP port. A call can be rejected because of a network problem such as loss of WAN connection, delay, packet loss, or jitter. This feature supports only VoIP signaling protocol with H.323 in this release. This feature has to be configured on the originating gateway and the terminating gateway.

The **call fallback map** command option provides a target network summary/consolidation mode. For example, if there are four individual voice gateway routers connected together on a remote LAN via a separate LAN-to-WAN access router, the map option allows a single probe to be sent to the single remote WAN access router (instead of having to maintain separate probes for each of the four voice gateway routers' IP addresses). Because the remote access and voice gateway routers are connected together on the same remote LAN, the probes to the access router returns similar results to probes to the individual voice gateway routers.

Service Assurance Agent

Service Assurance Agent (SAA) is a network congestion analysis mechanism that provides delay, jitter, and packet loss information for the configured IP addresses. SAA is based on a client/server protocol defined on the User Datagram Protocol (UDP). UDP is a connectionless transport layer protocol in the 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. The SAA probe packets go out on randomly selected ports from the top end of the audio UDP port range.

The information that the SAA probes gather is used to calculate the ICPIF or delay/loss values that 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 user configurable.

With this feature enhancement, you can also configure codes that indicate the cause of the network rejection; for example, packets that are lost or that take too long to be transmitted. A default cause code of 49 displays the message **qos-unavail**, which means Quality of Service is unavailable.

Note The Cisco SAA functionality in Cisco IOS software was formerly known as Response Time Reporter (RTR). In the How to Configure PSTN Fallback, on page 3 section, note that the command-line interface still uses the keyword **rtr** for configuring RTR probes, which are now actually the SAA probes.

Application of PSTN Fallback

The PSTN Fallback feature and enhancement provide the following benefits:

- Automatically re-routes calls when the data network is congested at the time of the call setup.
- Enables the service provider to give a reasonable guarantee about the quality of the conversation to its Voice over IP (VoIP) users at the time of call admission.
- Provides delay, jitter, and packet loss information for the configured IP addresses.
- Caches call values from previous calls. New calls do not have to wait for probe results before they are admitted.
- Enables a user-configurable cause code display that indicates the type of call rejection.

Restrictions for PSTN Fallback

The PSTN Fallback feature has the following restrictions:

- When detecting network congestion, the PSTN fallback feature does nothing to the existing call. It affects only subsequent calls.
- Only a single ICPIF/delay-loss value is allowed per system.
- A small additional call setup delay can be expected for the first call to a new IP destination.

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.

How to Configure PSTN Fallback

Configuring Call Fallback to Use MD5 Authentication for SAA Probes

To configure call fallback to use MD5 authentication for SAA probes, use the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call fallback active**
4. **call fallback key-chain** *name-of-chain*

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`	Enables the PSTN fallback feature to alternate dial peers in case of network congestion.
Step 4	**call fallback key-chain** *name-of-chain* **Example:** `Router(config)# call fallback key-chain sample`	Specifies the use of message digest algorithm 5 (MD5) authentication for sending and receiving Service Assurance Agents (SAA) probes.

Configuring Destination Monitoring without Fallback to Alternate Dial Peers

To configure destination monitoring without fallback to alternate dial peers, use the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call fallback monitor**

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	**call fallback monitor** **Example:** `Router(config)# call fallback monitor`	Enables the monitoring of destinations without fallback to alternate dial peers.

Configuring Call Fallback Cache Parameters

To configure the call fallback cache parameters, use the following commands.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **call fallback cache-size** *number*
4. **call fallback cache-timeout** *seconds*
5. **clear call fallback cache** [*ip-address*]

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	**call fallback cache-size** *number* **Example:** `Router(config)# call fallback cache-size 5`	Specifies the call fallback cache size.
Step 4	**call fallback cache-timeout** *seconds* **Example:** `Router(config)# call fallback cache-timeout 300`	Specifies the time after which the cache entry is purged, in seconds. Default: 600.
Step 5	**clear call fallback cache** [*ip-address*] **Example:** `Router(config)# clear call fallback cache 10.1.1.1`	Clears the current ICPIF estimates for all IP addresses or a specific IP address in the cache.

Configuring Call Fallback Jitter-Probe Parameters

To configure call fallback jitter-probe parameters, use the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call fallback jitter-probe num-packets** *number-of-packets*
4. **call fallback jitter-probe precedence** *precedence*
5. **call fallback jitter-probe priority-queue**

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	**call fallback jitter-probe num-packets** *number-of-packets* **Example:** `Router(config)# call fallback jitter-probe num-packets 10`	Specifies the number of packets for jitter. Default: 15.

Step 4	**call fallback jitter-probe precedence** *precedence*
	Example:
	`or`
	Example:
	`call fallback jitter-probe dscp` *`dscp-number`*
	Example:
	`Router(config)# call fallback jitter-probe precedence 2`
	Example:
	`or`
	Example:
	`Router(config)# call fallback jitter-probe dscp 2`
		Specifies the treatment of the jitter-probe transmission. Default: 2.
		Specifies the differentiated services code point (dscp) packet of the jitter-probe transmission.
		Note The **call fallback jitter-probe precedence** command is mutually exclusive with the **call fallback jitter-probe dscp** command. Only one of these command can be enabled on the router. Usually, the **call fallback jitter-probe precedence** command is enabled. When the **call fallback jitter-probe dscp** 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 **no call fallback jitter-probe dscp**command.

Step 5	**call fallback jitter-probe priority-queue** **Example:** `Router(config)# call fallback jitter-probe priority-queue`	Assigns a priority to the queue for jitter probes.

Configuring Call Fallback Probe-Timeout and Weight Parameters

To configure call fallback probe-timeout and weight parameters, use the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call fallback probe-timeout** *seconds*
4. **call fallback instantaneous-value-weight** *percent*

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	**call fallback probe-timeout** *seconds* **Example:** `Router(config)# call fallback probe-timeout 20`	Sets the timeout for an SAA probe, in seconds. Default: 30.
Step 4	**call fallback instantaneous-value-weight** *percent* **Example:** `Router(config)# call fallback instantaneous-value-weight 50`	Configures the call fallback subsystem to take an average from the last two probes registered in the cache for call requests: • *percent* --Instantaneous value weight, expressed as a percentage. Range: 0 to 100. Default: 66.

Configuring Call Fallback Threshold Parameters

To configure call fallback threshold parameters, use the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call fallback threshold delay** *delay-value* **loss** *loss-value*

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	**call fallback threshold delay** *delay-value* **loss** *loss-value*
	Example:
	`or`
	Example:
	`call fallback threshold icpif` *`threshold-value`*
	Example:
	`Router(config)# call fallback threshold delay 100 loss 150`
	Example:
	`or`
	Example:
	`Router(config)# call fallback threshold icpif 100`
		Specifies fallback threshold to use packet delay and loss values. No defaults.
		Note The amount of delay set by the **call fallback threshold delay loss** command should not be more than half the amount of the time-to-wait value set by the **call fallback wait-timeout** command; otherwise the threshold delay will not work correctly. Because the default value of the **call fallback wait-timeout** command is set to 300 milliseconds, you can configure a delay of up to 150 milliseconds for the **call fallback threshold delay loss**command. If you want to configure a higher threshold, the time-to-wait delay has to be increased from its default (300 milliseconds) using the **call fallback wait-timeout** command.
		Specifies fallback threshold to use the Calculated Planning Impairment Factor (ICPIF) threshold for network traffic.

Configuring Call Fallback Wait-Timeout

To configure the call fallback wait-timeout parameters, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call fallback wait-timeout** *milliseconds*

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	**call fallback wait-timeout** *milliseconds* **Example:** `Router(config)# call fallback wait-timeout 200`	Configures the waiting timeout interval for a response to a probe in milliseconds. Default: 300 milliseconds. **Note** The time-to-wait period set by the **call fallback wait-timeout** command should always be greater than or equal to twice the amount of the threshold delay time set by the **call fallback threshold delay loss**command; otherwise the probe will fail. The delay configured by the **call fallback threshold delay loss** command corresponds to a one-way delay, whereas the time-to-wait period configured by the **call fallback wait-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.

Configuring VoIP Alternate Path Fallback SNMP Trap

To configure the SNMP trap parameters, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call fallback active**
4. **snmp-server enable traps voice fallback**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**call fallback active** **Example:** `Router(config)# call fallback active`	Enables the PSTN fallback feature to alternate dial peers in case of network congestion.
Step 4	**snmp-server enable traps voice fallback** **Example:** `Router(config)# snmp-server enable traps voice fallback`	Configures the SNMP trap parameters.

What to Do Next

Configure the **rtr responder** command on the terminating voice gateway. If the **rtr responder** is enabled on the terminating gateway, the terminating gateway responds to the probe request when the originating gateway sends an Response Time Report (RTR) probe to the terminating gateway to check the network conditions.

Configuring Call Fallback Map Parameters

To configure call fallback map parameters, use the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **call fallback map** *map* **target** *ip-address* **address-list** *ip-address1 ip-address2 ... ip-address7*
   -
   - **call fallback map** *map* **target** *ip-address* *subnet ip-network netmask*

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:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	Do one of the following: - **call fallback map** *map* **target** *ip-address* **address-list** *ip-address1 ip-address2 ... ip-address7* - - **call fallback map** *map* **target** *ip-address* *subnet ip-network netmask*	Specifies the call fallback router to keep a cache table (by IP addresses) of distances for several destination peers sitting behind the router. - *map* --Fallback map. Range is from 1 to 16. There is no default. - **target** *ip-address* --Target IP address. - *ip-address1 ip-address2 ... ip-address7* --Lists the IP addresses that are kept in the cache table. The maximum number of IP addresses is seven. Specifies the call fallback router to keep a cache table (by subnet addresses) of distances for several destination peers sitting behind the router.

Configuring ICMP Pings to Monitor IP Destinations

This capability to monitor ICMP pings is enabled to monitor the IP destinations in a VoIP network, which may not support RTR. This monitoring is referred to as ICMP pinging. Based on the RTR or ICMP pinging, results change the operational state of the dial-peer. The configurations described in this section also provide support for monitoring the following session targets configured under a VoIP dial-peer:

- DNS
- IP version 4
- SIP-server
- enum

To configure call-fallback monitor probes to ping IP destinations, complete one of the following tasks:

Dial Peer Configuration of the call fallback icmp-ping and monitor probe Commands

To configure dial-peer parameters to use ICMP pings to monitor IP destinations, complete this task. This configuration applies only to VoIP dial peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **call fallback** [**icmp-ping** | **rtr**]
5. **monitor probe** {**icmp-ping** | **rtr**} [*ip address*]

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	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 10 voip`	Enters dial peer configuration mode, specifies the method of voice encapsulation, and defines a particular dial peer: *tag* --Digits that define a particular dial peer. Range is from 1 to 2147483647.
Step 4	**call fallback** [**icmp-ping** | **rtr**] **Example:** `Router(config-dial-peer)# call fallback icmp-ping`	Configures dial-peer parameters for pings to IP destinations: • **icmp-ping** --Uses ICMP pings to monitor the IP destinations. • **rtr** --Uses RTR probes to monitor the session target and update the status of the dial peer. RTR probes are the default. **Note** If this **call fallback icmp-ping**command is not entered, the **call fallback active**command in global configuration is used for measurements. If this **call fallback icmp-ping** command is entered, these values override the global configuration. One of these two commands must be in effect before the **monitor probe icmp-ping**command can be used. If neither of **call fallback** commands is in effect, the **monitor probe icmp-ping** command will not work properly.
Step 5	**monitor probe** {**icmp-ping** | **rtr**} [*ip address*] **Example:** `Router(config-dial-peer)# monitor probe icmp-ping`	Enables dial-peer status changes based on the result of the probe: • **icmp-ping** --Uses ICMP ping as the method for the probe. • **rtr** --Uses RTR as the method for the probe. • *ip address* --IP address of the destination to be probed. If no IP address is specified, the IP address is read from the session target.

Global Configuration of the call fallback icmp-ping Command

To configure global parameters to use ICMP pings to monitor IP destinations, complete this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call fallback active** [**icmp-ping** | **rtr**]
4. **call fallback icmp-ping** [**count** *number*] [**codec** *type*] | **size** *bytes*] **interval** *seconds* [**loss** *number*] [**timeout** *milliseconds*]

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	**call fallback active** [**icmp-ping** | **rtr**] **Example:** `Router(config)# call fallback active icmp-ping`	Configures global parameters for pings to IP destinations: • **icmp-ping** --Uses ICMP pings to monitor the IP destinations. • **rtr** --Uses RTR probes to monitor the IP destinations. RTR probes are the default. **Note** The **call fallback active icmp-ping** command must be entered before the **call fallback icmp-ping** command can be used. If you do not enter this command first, the **call fallback icmp ping** command will not work properly.
Step 4	**call fallback icmp-ping** [**count** *number*] [**codec** *type*] | **size** *bytes*] **interval** *seconds* [**loss** *number*] [**timeout** *milliseconds*] **Example:** `Router(config)# call fallback icmp ping codec g729 interval 10 loss 10`	Configures the parameters for ICMP pings: • **count** --Number of ping packets to be sent to the destination IP address. Default is 5. • **codec** --Codec type for deciding the ping packet size. • *type* --Acceptable codec types are **g711a**, **g711u**, **g729**, and **g729b**. • **size** --Size (in bytes) of the ping packet. Default is 32.

	Command or Action	Purpose
		• **interval** --Time (in seconds) between ping packet sets. Default is 5. This value should be more than the **timeout** value. • **loss** --Threshold packet loss, expressed as a percentage. Default is 20. • **timeout** --Timeout (in milliseconds) for the echo packets. Default is 500.

Voice Port Configuration of the busyout monitor probe icmp-ping Command

To configure voice-port parameters to use ICMP pings to monitor IP destinations, complete this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-port** *slot* / *port*
4. **busyout monitor probe icmp-ping** *ip address* [**codec** *type* | **size** *bytes*][**loss** *percent*]

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	**voice-port** *slot* / *port* **Example:** `Router(config)# voice-port 1/0`	Enters voice-port configuration mode and identifies the slot and port where the configuration parameters take effect. **Note** The syntax for this command varies by platform. For more information, see the Cisco IOS Voice Command Reference.
Step 4	**busyout monitor probe icmp-ping** *ip address* [**codec** *type* | **size** *bytes*][**loss** *percent*] **Example:** `Router(config-voiceport)# busyout monitor probe 10.1.1.1 g711u loss 10 delay 2000`	Specifies the parameters for ICMP pings for monitoring under voice-port configuration: • *ip address* --IP address of the destination to which the ping is sent. • **codec** --(Optional) Codec type for deciding the ping packet size.

	Command or Action	Purpose
		• *type* --Acceptable codec types are **g711a**, **g711u**, **g729**, and **g729b**. • **size** --(Optional) Size (in bytes) of the ping packet. Default is 32. • **loss** --(Optional) Threshold packet loss, expressed as a percentage. Default is 20.

Voice Class Configuration of the busyout monitor probe icmp-ping Command

To configure voice-class parameters to use ICMP pings to monitor IP destinations, complete this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class busyout** *tag*
4. **busyout monitor probe icmp-ping** *ip address* [**codec** *type* | **size** *bytes*][**loss** *percent*]

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	**voice class busyout** *tag* **Example:** `Router(config)# voice class busyout 10`	Creates a voice class for local voice busyout functions: *tag* --Unique identification number assigned to one voice class. Range is 1 to 10000.
Step 4	**busyout monitor probe icmp-ping** *ip address* [**codec** *type* | **size** *bytes*][**loss** *percent*] **Example:** `Router(config-class)# busyout monitor probe icmp-ping 10.1.1.1 codec g729b size 32`	Configures the parameters for ICMP pings for monitoring under voice-port: • *ip address* --IP address of the destination to which the ping is sent. • **codec** --(Optional) Codec type for deciding the ping packet size. • *type* --Acceptable codec types are **g711a**, **g711u**, **g729**, and **g729b**.

	Command or Action	Purpose
		• **size** --(Optional) Size (in bytes) of the ping packet. Default is 32. • **loss** --(Optional) Threshold packet loss, expressed as a percentage. Default is 20.

How to Verify and Monitor the PSTN Fallback Feature

Verifying PSTN Fallback Configuration

The **show** commands in this section can be used to display statistics and configuration parameters to verify the operation of the PSTN Callback feature:

- **show running-config** --Displays the contents of the currently running configuration file to see if the new feature is configured.
- **show call history voice** --Displays the call history table for voice calls and verify call fallback, call delay, and call loss parameters.
- **show call fallback cache** --Displays the current Calculated Planning Impairment Factor (ICPIF) estimates for all IP addresses in the call fallback cache.
- **show call fallback config** --Displays the current configuration.
- **show call fallback stats** --Displays the call fallback statistics.

Monitoring and Maintaining PSTN Fallback

Use the following commands to monitor and maintain the PSTN Fallback feature:

- **clear call fallback cache** --Clears the current ICPIF estimates for all IP addresses in the cache.
- **clear call fallback stats** --Clears the call fallback statistics.
- **debug call fallback detail** --Displays details of VoIP call fallback.
- **debug call fallback probes** --Displays details of voice fallback probes.
- **test call fallback probe** *ip-address* --Tests a probe to a particular IP address and displays the ICPIF SAA values.
- **debug snmp packets** --Displays information about every Simple Network Management Protocol (SNMP) packet sent or received by the router.

What To Do Next

The Configuring ICMP Pings to Monitor IP Destinations, on page 11 describes the mechanism whereby a dial-peer becomes temporarily disabled because of poor SAA/RTR probe results (for example, ICPIF, jitter, or loss), or because of failure of the ICMP ping test. When this occurs, the normal alternate dial-peer selection process (hunting) is triggered to search for an alternate dial-peer that represents an alternate route.

The global configuration **voice hunt** command controls whether hunting (continue to look or "hunt" for an alternate dial-peer match) occurs, based on the specific cause code that describes why the initial dial-peer path failed. Hunting is usually appropriate if the cause code indicates network congestion, but usually inappropriate if the failure cause code indicates that the called user is actually busy. Even if an alternate path is taken to reach the called user, and if the user is actually busy, the user will be busy regardless of which path is used.

For more information about the **voice hunt** command, see the Cisco IOS Voice Command Reference.