



Cisco VoIP Internal Error Codes

The Cisco VoIP Internal Error Codes feature generates internal error codes (IECs) for gateway-detected errors that cause the gateway to release or refuse a call. IECs enhance troubleshooting for VoIP networks by helping to determine the source and reason for call termination.

- [Prerequisites for Cisco VoIP Internal Error Codes, page 1](#)
- [Restrictions for Cisco VoIP Internal Error Codes, page 1](#)
- [Information About Cisco VoIP Internal Error Codes, page 1](#)
- [How to Configure IEC Options, page 38](#)
- [Configuration Examples for Cisco VoIP Internal Error Codes, page 43](#)
- [Troubleshooting VoIP Networks Using Cisco VoIP Internal Error Codes, page 49](#)

Prerequisites for Cisco VoIP Internal Error Codes

Before this feature can be operational, a basic VoIP network must be configured.

Restrictions for Cisco VoIP Internal Error Codes

- Memory usage increases slightly when this feature is implemented, depending upon the number of subsystems that support IECs and upon the number of error codes defined for each subsystem.
- IECs are reported only in RADIUS accounting records. They are not supported in syslog accounting.

Information About Cisco VoIP Internal Error Codes

To configure the Cisco VoIP Internal Error Codes feature, you should understand the following concepts:

- [Benefits of Cisco VoIP Internal Error Codes, page 2](#)
- [Feature Design of Cisco VoIP Internal Error Codes, page 2](#)
- [IEC Reporting, page 2](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Internal Error Code Notation, page 7](#)

Benefits of Cisco VoIP Internal Error Codes

- Allows the service provider to see the cause of call disconnect in the accounting record.
- Provides enhanced diagnostic and troubleshooting capability for VoIP networks.
- Supports the development of enhanced analysis tools that can determine if patterns of call failures exist.
- Improves network reliability by enabling more effective monitoring and call management.
- Internal Error Code (IEC) reporting has been enhanced in Cisco IOS Release 12.4(4)T to provide better tracking and diagnostic capability for networks, and specifically for gatekeepers.

Feature Design of Cisco VoIP Internal Error Codes

Prior to the implementation of IECs, Q.850-based disconnect cause codes were used to track and diagnose network problems. These cause codes, defined by ITU Recommendation Q.850, were more applicable to traditional PSTN networks than to packet networks and were too generic to be useful for diagnosing and isolating faulty VoIP network components.

The Cisco VoIP Internal Error Codes feature allows an error code to be generated for a gateway-detected error that causes the gateway to release or refuse a call or call attempt. The error may not actually cause the call to fail; for example, in the case of rotary attempts, a subsequent attempt may result in the call completing. The error does not necessarily indicate a problem on the gateway itself, but may be due, for example, to a protocol error detected in a message, or to a timeout while communicating with a nonresponding party. IECs are not generated for normal calls that are released without an error; for example, no answer, busy, and user hangs up.

Each internal error in the voice signaling path that leads to the release of a call is assigned an IEC value. Fields within the IEC identify which network entity and subsystem originated the error, and specify the error code within the subsystem. The IEC mechanism maintains error counters and allows you to use command-line interface (CLI) commands to collect, display, and offload error counters. The CLI also allows you to clear counters. The IEC mechanism also generates a CLI-enabled syslog message and a new RADIUS vendor-specific attribute (VSA) whenever an IEC is generated.

The IEC feature supports a mechanism for enforcing disconnect cause code consistency for internal errors by providing a configurable mapping table to translate the IEC error category to an appropriate disconnect cause code.

In addition to generating IECs, this feature set makes use of enhanced release source indicators (RSIs) to report gatekeeper-released and route server-released calls. For more information on RSIs, refer to [Call Release Source Reporting in Gateway-Generated Accounting Records](#).

**Note**

IECs are not generated for the following types of calls: VoiceXML, fax, MGCP or SGCP, and SS7 continuity (COT).

IEC Reporting

Cisco implements IEC reporting by logging IEC values into the following records:

- VSAs in RADIUS accounting records
- Call history records
- Dial Control MIB
- Syslog messages

The gateway sends VSAs in RADIUS accounting stop records. Because each IEC is associated with a call leg, an IEC is reported only in the stop record for one of the legs in a call. VSAs are also sent by the gatekeeper. The gateway collects IECs for all call legs involved in a call and reports them to the gatekeeper, which inserts the IECs in its accounting stop record. In some scenarios, multiple errors may be encountered for a particular call leg; for example, multiple attempts to connect to an alternate endpoint. Up to five IECs may be generated per call.

Because IECs are reported through accounting records, if there is no voice call association or context, no IEC is generated. This scenario occurs, for example, if the gateway receives an ISDN setup message and the ISDN layer fails to allocate resources to process the setup message. In this instance there is no indication to the Voice Telephony Service Provider (VTSP) layer and no creation of a call-leg or call-history record, so no IEC is generated.

Gatekeeper Behavior and Cisco VoIP Internal Error Codes

Gatekeeper behavior for RADIUS accounting for start and stop records changes with the introduction of VoIP internal error codes. Prior to the Cisco VoIP Internal Error Codes feature, the gatekeeper generated two records for intrazone calls: one start record, based on the originating admission reject (ARJ) message, and one stop record, based on the first incoming disengage request (DRQ) message. This limitation resulted in data from the DRQ of the other gateway not being included in the accounting.

For intrazone calls the Cisco VoIP Internal Error Codes feature allows the gatekeeper to generate start and stop records based on each ARQ and DRQ; that is, two start and stop records are generated for each call.

Gatekeeper IEC Logging

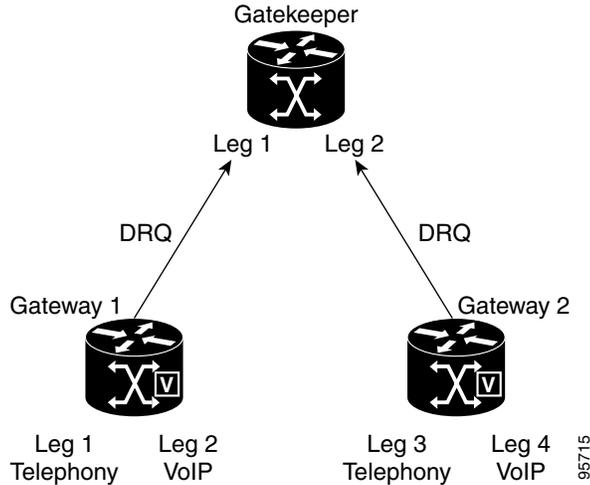
The gateway collects IECs for all call legs involved in a call and reports them to the gatekeeper in a DRQ message during call release. The gateway also sends RSI information in the DRQ message. The gatekeeper then logs the RSI and IEC information in RADIUS accounting stop records.

IEC Differences in Gateway and Gatekeeper Accounting

On the gateway an IEC is logged in to a stop accounting record for the call leg that encountered the error. If an error occurred in the VTSP call leg, an IEC is logged in the telephony stop record; no IEC is recorded in the VoIP stop record, and vice versa.

[Figure 9](#) shows the differences between gateway and gatekeeper accounting. On the gatekeeper, the two call legs, telephony and VoIP, are treated as one call leg, with IEC information merged from both originating gateway (Gateway 1) call legs. The DRQ message to the gatekeeper therefore contains IECs combined from both the telephony and VoIP call legs for a particular call. From the gatekeeper perspective, the second call leg is the terminating gateway (Gateway 2) call leg. This call leg records accounting information received as well.

Figure 9 Differences in Gateway and Gatekeeper Accounting



IEC and RSI Format in DRQ

IEC and RSI information is communicated in the RasnonStdUsageInformation field in the usageInformation information element (IE) of the DRQ message. The following example shows a partial DRQ message:

```
value RasnonStdUsageInformation ::=
{
  rasMessageSpecificData drqRasnonStdUsageData :
  {
    callReleaseSource internalReleaseInVoipLeg :NULL
    iecInfo
    {
      '10105480022C0000'H
    }
  }
}
```

The 64-bit IECs are communicated as an array of eight characters (of size eight bits). The callReleaseSource is communicated as an enumerated value.

Gatekeeper-Initiated Release Scenario

Prior to Cisco IOS Release 12.4(4)T, if the gatekeeper forcefully initiates a release for an active call by sending a DRQ message, then no IEC is generated. The IEC feature does not support gatekeeper-generated IECs. The ReleaseSource VSA for this scenario indicates a value of gatekeeper; however, there is no InternalErrorCode VSA.

Starting with Cisco IOS Release 12.4(4)T, the capability was expanded so that gatekeeper-detected errors that cause the gateway to release or refuse a call are covered. The IEC generated at the gatekeeper is sent in the ARJ/DRQ RAS message to the gateway. The gateway then sends the IEC in a RADIUS accounting record. The gatekeeper IEC clearly identifies:

- Physical network entity that encountered the error
- Type of error (category or class)
- Subsystem within that entity
- Subsystem-defined error code
- Private diagnostic code to allow developers to better pinpoint the software point of failure

Release Source Extension

Prior to Cisco IOS Release 12.3(2)T, both gatekeeper and Gatekeeper Transaction Message Protocol (GKTMP) server-released calls were treated as gatekeeper-released calls, and were indicated by an RSI value of external call control agent. The Cisco IOS Release 12.3(2)T version provides extended release source values for GKTMP server and gatekeeper. RSI information is passed in the NonStandardUsageData parameter field of the ARJ and DRQ messages from the gatekeeper to gateway during call tear down.

There is no change in the GKTMP interface; instead the context of the release scenario is used to determine the RSI value at the gatekeeper. For example, the receipt of a RESPONSE.ARJ message from the route server results in an RSI value of external gktmp server. Similarly, a forced release from gatekeeper using the **clear h323 gatekeeper call** command results in the RSI value of gatekeeper.

Release Source Values

With respect to a single network, the following release sources are possible:

- Calling party located in the PSTN
- Calling party located in the VoIP network
- Called party located in the PSTN
- Called party located in the VoIP network
- Internal release in a POTS leg
- Internal release in a VoIP leg
- Internal call-control application (for example, Tool Command Language (Tcl) or Voice eXtensible Markup Language (VXML) script)
- Internal release in VoIP authentication, authorization, and accounting (AAA)
- CLI or Man Machine Language (MML)
- External RADIUS server
- External network management application
- External call control agent
- Gatekeeper
- External GKTMP server

Obtaining IECs

Choose one or more of the following options to obtain IEC information:

- Display IECs as they are encountered in real time by enabling syslog messages. The IEC is not included in syslog-accounting records. For more information on enabling syslog messages, refer to the chapter “Task 2. Enabling Syslog” of *Enabling Management Protocols: NTP, SNMP, and Syslog*.
- Display running and interval IEC counters, and IEC descriptor strings using CLI commands.
- Export IEC counts to a specified server. For more information, refer to *Voice Call Performance Statistics on Cisco Gateways*.
- Retrieve IEC and RSI information using Tcl IVR 2.0 scripts. For more information on using Tcl scripts with the IEC feature, refer to *Supplemental Tcl IVR API Version 2.0 Programmer's Guide*.

If you use call detail recording (CDR) templates to filter VSAs that are included in accounting records to the RADIUS server, you must add the IEC VSA to the CDR template if you want to display IEC VSAs.

Sample IEC Syslog Message

The following example shows an IEC-generated syslog message:

```
Oct 14 17:13:21.534:%VOICE_IEC-3-GW:CCAPI:Internal Error (Trunk-group select
fail):IEC=1.1.182.1.23.8 on callID 62 GUID=11C79B82DECF11D68044C61A8D4F75E3
```

Sample IEC Syslog Message for Gatekeeper

The following example shows an IEC-generated system logging (syslog) message for gatekeeper:

```
Oct 14 17:13:21.534:%VOICE_IEC-3-GK:Internal Error ("DRQ in progress"):IEC=1.2.182.1.23.0
on ConfID 243 GUID=123a2b0912345678
```

If there is no call leg context, the ConfID is -1, and the GUID field is blank.

Sample RADIUS VSA Internal Error Code

The following example shows a partial RADIUS stop accounting record for an IEC:

```
[Vendor 9/1] cisco-avpair = "internal-error-code=1.1.179.2.37.0"
```

Sample Call History Record

The **show call history voice** command displays VSA information in the following format:

```
InternalErrorCode=1.1.128.7.47.0
```

Sample Dial Control MIB Entry

The IEC entry is controlled by the following indexes:

- `cCallHistoryIndex`, which indicates IECs related to a specific call history record.
- `cCallHistoryIecIndex`, which is used if there is more than one IEC for a call history record.

The following example shows a partial Dial Control MIB table entry for an IEC:

```
CCallHistoryIecEntry ::=
    SEQUENCE {
        cCallHistoryIecIndex      Unsigned32,
        cCallHistoryIec          SnmpAdminString
    }
```

The following example shows the use of the management tool command **getmany** to obtain the IEC:

```
getmany 10.7.102.32 cCallHistoryIec
cCallHistoryIec.5.1 = 1.1.180.1.26.0

getmany 10.7.102.32 cCallHistory
cCallHistorySetupTime.5 = 8540739
cCallHistoryPeerAddress.5 = 4085550190
cCallHistoryPeerSubAddress.5 =
cCallHistoryPeerId.5 = 1112224
cCallHistoryPeerIfIndex.5 = 213
cCallHistoryLogicalIfIndex.5 = 108
cCallHistoryDisconnectCause.5 = 3F
cCallHistoryDisconnectText.5 = service or option not available, unspecified (63)
cCallHistoryConnectTime.5 = 0
cCallHistoryDisconnectTime.5 = 8540740
cCallHistoryCallOrigin.5 = answer(2)
cCallHistoryChargedUnits.5 = 0
cCallHistoryInfoType.5 = speech(2)
cCallHistoryTransmitPackets.5 = 0
cCallHistoryTransmitBytes.5 = 0
```

```

cCallHistoryReceivePackets.5 = 0
cCallHistoryReceiveBytes.5 = 0
cCallHistoryReleaseSrc.5 = calledPartyInVoip(4)
cCallHistoryIec.5.1 = 1.1.180.1.26.0

```

In the preceding example, 5 is the index of the call history record and 1 is the index of the IEC for that record.

The following example shows the use of the indexes and the management tool command **getone** to obtain the IEC directly:

```

getone 10.7.102.32 cCallHistoryIec.5.1
cCallHistoryIec.5.1 = 1.1.180.1.26.0

```

Internal Error Code Notation

The IEC value takes the form of a dotted string of decimal numbers:
version.entity.category.subsystem.errorcode.diagnosticcode.

[Table 11](#) describes the six fields that identify the components of the IEC.

Table 11 IEC Fields

IEC Field	Field Definition
version	Indicates the IEC version. The value 1 indicates the current version.
entity	Indicates the network physical entity (hardware system) that generated the IEC. The value 1 is assigned to the gateway.
category	Indicates an error category, defined in terms of ITU-based Q.850 cause codes and VoIP network errors.
subsystem	Indicates the specific subsystem within the physical entity where the IEC was generated.
error code	Identifies the error code within the subsystem.
diagnostic code	Indicates a Cisco internal diagnostic value. Report this value to Cisco Technical Assistance Center (TAC).

Entity

The entity field indicates the network signaling entity that generated the IEC. A value of 1 in this field indicates the IEC is generated by the gateway.

Category Codes

Cisco VoIP IEC category codes

Cisco VoIP IEC categories range from 1 to 278, allowing an exact category of error to be specified in the category field of an IEC. With the Cisco VoIP Internal Error Codes feature, the concept of error categories combines and extends the existing Q.850 cause codes to handle VoIP-specific errors as well.

IEC category codes are specified as follows:

- The value range 1 to 127 is equivalent to ITU-based Q.850 cause codes defined for PSTN networks.
- The value range 128 to 278 is defined based on VoIP network errors. A mapping is maintained between these error categories to corresponding Q.850 codes (1 to 127 range).



Note

Only the H.323 and Session Initiation Protocol (SIP) subsystems implement an approach to generate disconnect cause codes or Q.850 PSTN cause codes based on error categories. The disconnect cause is chosen based on the mapping from the corresponding error category. You can configure this mapping using CLI. This correspondence of IEC error category and Q.850 disconnect cause is implemented only for SIP and H.323 internal errors, and is not implemented for other subsystems in this release. For more information on SIP and H.323 cause codes, refer to [Internal Cause Code Consistency Between SIP and H.323](#).

Table 12 shows the category codes outside the Q.850 range, their descriptions, and the default Q.850 cause code used for each error category. The Q.850 cause codes for these categories can be changed using CLI.

Table 12 VoIP Error Category Codes

Category	Description	Default Q.850 code
128	Destination address resolution failure	3
129	Call setup timeout	102
178	Internal communication error	41
179	External communication Error	41
180	Software error	47
181	Software resources unavailable	47
182	Hardware resources unavailable	47
183	Capability exchange failure	41
184	QoS error	49
185	RTP/RTCP receive timer expired or bearer layer failure	41
186	Signaling socket failure	38
187	Gateway or signaling interface taken out of service	38
228	User denied access to this service	50
278	Media negotiation failure due to nonexisting codec	65

Gatekeeper Category Codes

Cisco gatekeeper IEC categories range from 1 to 24, allowing an exact category of error to be specified in the category field of an IEC. [Table 13](#) shows the category codes for gatekeeper IECs.

Table 13 *Gatekeeper IEC Category Codes*

Category	Description
1	Called party not registered
2	Invalid permission
3	Request denied
4	Undefined reason
5	Caller not registered
6	Route call to gatekeeper
7	Invalid endpoint ID
8	Resource unavailable
9	Security denial
10	QoS control not supported
11	Incomplete address
12	Alias inconsistent
13	Route call to SCN
14	Exceeds capacity
15	Error while collecting destination
16	Error while collecting PIN
17	Generic data reason
18	Needed feature unsupported
19	Software resource unavailable
20	External communication error
21	Software error
22	Socket failure
23	Normal disconnect
24	Force disconnect

Subsystem Codes

Together the subsystem and error codes pinpoint the exact error that cause the call to be released. IECs are reported for the subsystems defined in [Table 14](#).

Table 14 **Subsystem Codes**

Subsystem Code	Subsystem	Description
1	CCAPI	Call control messaging layer that sits between the session applications and the signaling-protocol legs.
2	Tcl IVR	Session applications that are scripted in Tcl IVR 2.0.
3	Application Framework (AFW)	Library that implements Tcl verbs and VXML tags. Executes functionality such as placing a call, collecting digits, playing prompts, and so on.
4	Default Session Application (SSAPP)	Formerly the default session application that controls the call when an inbound-matched dial peer is not configured with any application or with application default.
5	H.323	Subsystem that performs call signaling for the H.323 VoIP leg.
7	SIP	Subsystem that performs call signaling for the SIP VoIP leg.
9	VTSP	Subsystem that performs call signaling for the telephony leg.
10	Application Framework Session Application (AFSAPP)	Default session application that controls the call when an inbound-matched dial peer is not configured with any application or with application default.

Error Codes

The Error Code field of the IEC dotted-decimal string value indicates the subsystem-defined error code. Codes 1 through 20 are common to all subsystems and may occur in several places within a subsystem; for these errors, the point of failure can be further isolated by referring to the unique diagnostic code field. Subsystem-specific error codes begin at 21.



Note

The diagnostic code field is a Cisco internal code. Report this code to Cisco TAC for troubleshooting assistance.

The following tables, [Table 15](#) through [Table 22](#), are organized by subsystem and show error code values, descriptors, associated explanation, and category codes.

Table 15 **Error Codes for Subsystem 1 (CCAPI)**

Code	Descriptor	Explanation	Category
1	No memory	Dynamically allocated memory on the gateway is exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181
2	No buffers	Packet or buffer memory is exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181

Table 15 *Error Codes for Subsystem 1 (CCAPI) (continued)*

Code	Descriptor	Explanation	Category
3	CPU high	Call is rejected because default or configured CPU usage threshold has been exceeded.	181
4	Low memory	Call is rejected because default or configured memory usage threshold has been exceeded.	181
5	No dial peer match	No dial peer satisfied the match criteria for accepting or handling the call. This condition usually indicates a dial peer misconfiguration.	128
6	No DSP resource	There were insufficient DSP resources to handle the call.	182
7	Socket error	An error occurred on a socket interface.	179
8	RTP inactivity error	Media (RTP/RTCP) inactivity timer expired for the call.	185
9	Invalid arguments	Invalid arguments passed to a function. This condition usually indicates an internal software error.	180
10	Invalid State	Some unexpected event was received while in a state that was inappropriate for processing such an event.	180
11	Timeout	The software timed out waiting for some response or event to happen.	179
12	Inter-process communication	An internal process communication error occurred. This condition usually indicates some software error, but may also mean that some process was not running because of misconfiguration.	178
13	Software error	An internal software error occurred. Report the entire IEC string, including the diagnostic code field, to customer support.	180
14	Gateway or interface OOS	The gateway or signaling interfaces are being taken out of service (forcefully or gracefully). A possible cause may be the signaling interface required to support the call has already been administratively shut down.	187
21	Dial peer connections exceeded	An outbound dial peer could not be used because the configured maximum number of connections for the dial peer had been reached.	181
22	Incompatible number type	An outbound dial peer could not be used because the configured numbering type did not match the type specified in the call.	28
23	Trunk-group select fail	The system failed to select an available interface among the trunk group specified for use by a matching dial peer.	182
24	Caller-ID processing failure	An error occurred in processing caller ID information.	180

Table 15 **Error Codes for Subsystem 1 (CCAPI) (continued)**

Code	Descriptor	Explanation	Category
25	Resource busy	A resource needed to service the call was busy.	181
26	No application	The system could not find an application to take the incoming call. Check your call application and dial peer configurations.	180
27	Application no longer exists	The event points to a session application that no longer exists and is being discarded.	180
28	Incoming loop	An incoming call setup indication was received, bearing the same globally unique identifier (GUID) as a call in existence. The call is being rejected because a loop is suspected.	180
29	Call spike threshold	An incoming call was rejected because configured call spike thresholds were exceeded.	181
30	Inbound dial peer blocked	A matched dial peer could not be used to find an inbound application because the permission setting on it blocked its use as an inbound dial peer. As a result, no application could be found to handle the call.	181
31	Outbound dial peer blocked	A matched dial peer could not be used to place the call because the configured permission on it contradicted its use as an outbound dial peer.	181
32	Handoff depth reached	The maximum number of handoffs between applications for a single call has been exceeded. Check your application scripts to make sure there is no infinite loop within the applications.	180
33	Incompatible apps for handoff	A call handoff attempt between applications failed because the applications were incompatible. Tcl IVR 1.0 applications are incompatible with Tcl IVR 2.0 or VXML applications.	180
34	No dial peer interface	A matched dial peer could not be used for the outbound leg because there was no appropriate interface for the dial peer type. This condition may be a software or configuration error. The tag identifier for the problematic dial peer is provided in the diagnostic field (the last component) of the six-part IEC string. Check your dial peer configuration.	180
35	System init error	Some data structure or process that should have been created at system initialization is missing. Report the IEC to customer support.	180

Table 16 *Error Codes for Subsystem 2 (Tcl IVR)*

Code	Descriptor	Explanation	Category
1	No Memory	Dynamically allocated memory on the gateway is exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181
2	No buffers	Packet or buffer memory is exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181
3	CPU high	Call is rejected because default or configured CPU usage threshold has been exceeded.	181
4	Low memory	Call is rejected because default or configured memory usage threshold has been exceeded.	181
5	No dial peer match	No dial peer satisfied the match criteria for accepting or handling the call. This condition usually indicates a dial peer misconfiguration.	128
6	No DSP resource	There were insufficient DSP resources to handle the call.	182
7	Socket error	An error occurred on a socket interface.	179
8	RTP inactivity error	Media (RTP/RTCP) inactivity timer expired for the call. This is logged by the script when it specifies <code>media_inactivity_err</code> as the IEC to be used for the disconnect.	185
9	Invalid arguments	Invalid arguments were passed to a function. This condition usually indicates an internal software error.	180
10	Invalid state	An unexpected event was received while in a state that was inappropriate for processing such an event.	180
11	Timeout	The software timed out waiting for some response or event to happen.	179
12	Inter-process communication	An internal process communication error occurred. This usually indicates some software error, but may also mean that some process was not running because of misconfiguration.	178
13	Software error	An internal software error occurred. Please report the entire IEC string, including the diagnostic code field, to customer support.	180
14	Gateway or interface OOS	The gateway or signaling interfaces are being taken out of service (forcefully or gracefully). A possible cause may be the signaling interface required to support the call has already been administratively shut down.	187

Table 16 Error Codes for Subsystem 2 (Tcl IVR) (continued)

Code	Descriptor	Explanation	Category
21	Script syntax	An error was detected while parsing a Tcl script. Enable the debug voip ivr error command for more detailed information.	180
22	Bad FSM event	A Tcl IVR script specified an unrecognized event in the definition of the finite state machine (FSM). Enable the debug voip ivr error command for more detailed information.	180
23	Invalid args in script	A Tcl IVR script specified invalid arguments when invoking a Tcl command procedure. Enable the debug voip ivr error command for more detailed information.	180
24	Unsupported infotag	A Tcl script tried to access an unrecognized infotag, or it may have tried to use a recognized infotag in an unsupported mode (for example, issues a get command on a set-only infotag or vice versa). Enable the debug voip ivr error command for more detailed information.	180
25	Invalid action in script	A Tcl script tried to execute an action or command that was invalid, or invalid given the state it was in. Enable the debug voip ivr error command for more detailed information.	180
26	Call blocked by CLI	This call was rejected because it matched the profile defined for calls to be blocked.	228
27	Settlement check failure	An inbound call was rejected because it failed OSP settlement checking, due to one of the following conditions: <ul style="list-style-type: none"> An OSP token was required and no valid one was found. An OSP token was included in the SETUP indication when none was expected. 	228
28	vxmldialog failed	The Tcl IVR application failed to initiate the VXML dialog. Turn on VXML debugging for more detailed information.	180
29	Can't set up prompt	A Tcl script terminated execution on failure of the media play command because the prompt initialization failed. Possible causes: <ul style="list-style-type: none"> A syntax error in the specification of prompt tokens Misconfiguration of language prompt-file locations. Enable the debug voip ivr dynamic and debug voip ivr error commands for more detailed information.	47

Table 16 *Error Codes for Subsystem 2 (Tcl IVR) (continued)*

Code	Descriptor	Explanation	Category
30	Wrong state for media	A Tcl script requested a media operation, for example, play, stop, or seek, on one or more legs that were in a conferenced state, or where there was a VXML dialog active.	180
31	Get infotag failed	A Tcl script terminated because an infotag retrieval failed. Enable the debug voip ivr error command for more information.	180
32	Set infotag failed	A Tcl script terminated because an infotag set operation failed. Enable the debug voip ivr error command for more information.	180
33	TCL script error	An error was encountered while interpreting a 180 Tcl script. Enable the debug voip ivr error command for more information.	180
34	Bad callinfo params	The application was unable to use one of the callinfo parameters for setup; for example, the octet 3 or octet 3a fields, redirect IE, and GUID. Enable the debug voip ivr error command for more information.	180
35	Version mismatch	The application could not run because it required an incompatible version of Tcl IVR.	180
36	Media request failed	A Tcl script terminated a call because an error status was reported by the media layer in the ev_media_done event. This indicates a failure in the execution of media play or some other media operation requested by the script. The script may choose to ignore the error, or it can opt to terminate the call, specifying this IEC, media_done_err, as the reason for the disconnect.	181
37	Digit collect failed	The error is logged by the Tcl script when it fails to collect digits in response to a prompt and decides to terminate the call because of the failure. The failure may be normal, that is, the caller did not enter any digits, or it may be due to an actual error in software or hardware. This IEC is logged by the script when it specifies collectdigits_done_err as the IEC associated with the disconnect.	179
38	Accounting conn err	The error code is set by the Tcl script when it terminates the call because it has received an indication that connectivity to the accounting server is lost. This IEC is logged when the script specifies accounting_conn_err as the IEC associated with the disconnect.	179

Table 16 *Error Codes for Subsystem 2 (Tcl IVR) (continued)*

Code	Descriptor	Explanation	Category
39	Authentication err	The error code is set by the Tcl script when it terminates a call because of error status reported on an ev_authenticate_done event. The script logs this error by specifying authenticate_done_err as the IEC associated with the disconnect.	179
40	Authorization err	The error code is set by the Tcl script when it terminates a call because of error status reported on an ev_authorize_done event. The script logs this error by specifying authorize_done_err as the IEC associated with the disconnect.	179
41	AAA invalid attribute type	The error is logged by the Tcl script when the attribute type in the AAA av pair specified in the script is not supported.	180

Table 17 *Error Codes for Subsystem 3 (Application Framework)*

Code	Descriptor	Explanation	Category
1	No Memory	Dynamically allocated memory on the gateway is exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181
2	No buffers	Packet or buffer memory is exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181
3	CPU high	Call was rejected because default or configured CPU usage threshold has been exceeded.	181
4	Low memory	Call was rejected because default or configured memory usage threshold has been exceeded.	181
5	No dial peer match	No dial peer satisfied the match criteria for accepting or handling the call. This condition usually indicates a dial peer misconfiguration.	128
6	No DSP resource	There were insufficient DSP resources to handle the call.	182
7	Socket error	An error occurred on a socket interface.	179
8	RTP inactivity error	Media (RTP/RTCP) inactivity timer expired for the call.	185
9	Invalid arguments	Invalid arguments passed to a function. This condition usually indicates an internal software error.	180

Table 17 *Error Codes for Subsystem 3 (Application Framework) (continued)*

Code	Descriptor	Explanation	Category
10	Invalid State	An unexpected event was received while in a state that was inappropriate for processing such an event.	180
11	Timeout	The software timed out waiting for some response or event to happen.	179
12	Inter-process communication	An internal process communication error occurred. This condition usually indicates some software error, but may also mean that some process was not running because of misconfiguration.	178
13	Software error	An internal software error occurred. Report the entire IEC string, including the diagnostic code field, to customer support.	180
14	Gateway or interface OOS	The gateway or signaling interfaces are being taken out of service (forcefully or gracefully). A possible cause may be the signaling interface required to support the call has already been administratively shut down.	187
21	Leg connections maxed	The maximum number of connections for the leg has been exceeded. An attempt to bridge yet another connection on the leg failed.	180
22	Handoff app not found	The specified target application for a call handoff was not found on the gateway.	180
23	Incompatible protocols	A matched dial peer could not be used for the outbound leg because the gateway cannot translate between the inbound and outbound protocols.	47
24	OSP Fail	OSP settlement checking failed for an outbound call.	228
25	dial peer deleted	A dial peer that was being used for a call setup was deleted (through CLI) before the call could be initiated.	47
26	Interface busy	An outbound dial peer matching this call's parameters specified an interface that was in use and unavailable.	182
27	App can't handoff	An application tried to place an outbound call using a dial peer configured with an outbound application. However, the first application does not support call handoff, so cannot pass the call to the second application.	180
28	Illegal "setup continue"	A Tcl script tried to issue a leg setup continue command when a previous setup continue command was still outstanding.	180
29	Call blocked by CLI	The call was rejected because it matched the profile defined for calls to be blocked.	228

Table 18 **Error Codes for Subsystem 4 (Default Session Application)**

Code	Descriptor	Explanation	Category
1	No Memory	Dynamically allocated memory on the gateway is exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181
2	No buffers	Packet or buffer memory is exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181
3	CPU high	Call rejected because default or configured CPU usage threshold has been exceeded.	181
4	Low memory	Call rejected because default or configured memory usage threshold has been exceeded.	181
5	No dial peer match	No dial peer satisfied the match criteria for accepting or handling the call. This condition usually indicates a dial peer misconfiguration.	128
6	No DSP resource	Insufficient DSP resources to handle the call.	182
7	Socket error	An error occurred on a socket interface.	179
8	RTP inactivity error	Media (RTP/RTCP) inactivity timer expired for the call.	185
9	Invalid arguments	Invalid arguments were passed to a function. This condition usually indicates an internal software error.	180
10	Invalid State	An unexpected event was received while in a state that was inappropriate for processing such an event.	180
11	Timeout	The software timed out waiting for some response or event to happen.	179
12	Inter-process communication	An internal process communication error occurred. This condition usually indicates some software error, but may also mean that some process was not running because of misconfiguration.	178
13	Software error	An internal software error occurred. Report the entire IEC string, including the diagnostic code field, to customer support.	180
14	Gateway or interface OOS	The gateway or signaling interfaces are being taken out of service (forcefully or gracefully). A possible cause may be the signaling interface required to support the call has already been administratively shut down.	187
21	Leg connections maxed	A loop was detected while processing a redirected call. The new destination matches a previously seen redirect address.	128

Table 18 Error Codes for Subsystem 4 (Default Session Application) (continued)

Code	Descriptor	Explanation	Category
22	Handoff app not found	Either an OSP token was detected in the setup message, or the dial peer configuration specified that settlement is to be used for this call. However, the default or session application configured to handle this call does not support the OSP protocol. Check the dial peer configuration and ensure that an OSP-capable application is defined.	47
23	Incompatible protocols	The call was rejected because it matched the profile defined for incoming calls to be blocked.	228
24	OSP Fail	An outbound dial peer matching this call's parameters specified an interface that was in use and unavailable.	182
25	dial peer deleted	Either the default application timed out waiting for the user to enter digits for the called number, or an INFO message arrived with zero-length called number.	28
26	Interface busy	The user entered an excessive number of digits for the called number.	28
27	App can't handoff	Digit collection is not supported on the interface or protocol that originated this call.	79
28	Illegal "setup continue"	The number of calls serviced by this gateway has exceeded the total number permitted, as defined by the call threshold global total-calls command.	181
29	Call blocked by CLI	The maximum number of redirects (call forwarding) allowed for a call has been exceeded.	128

Table 19 Error Codes for Subsystem 5 (H.323)

Code	Descriptor	Explanation	Category
1	No memory	Dynamically allocated memory on the gateway is exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181
2	No buffers	Packet or buffer memory is exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181
3	CPU high	Call rejected because default or configured CPU usage threshold has been exceeded.	181
4	Low memory	Call rejected because default or configured memory usage threshold has been exceeded.	181

Table 19 **Error Codes for Subsystem 5 (H.323) (continued)**

Code	Descriptor	Explanation	Category
5	No dial peer match	No dial peer satisfied the match criteria for accepting or handling the call. This condition usually indicates a dial peer misconfiguration.	128
6	No DSP resource	There were insufficient DSP resources to handle the call.	182
7	Socket error	An error occurred on a socket interface.	179
8	RTP inactivity error	Media (RTP/RTCP) inactivity timer expired for the call.	185
9	Invalid arguments	Invalid arguments passed to a function. This condition usually indicates an internal software error.	180
10	Invalid state	An unexpected event was received while in a state that was inappropriate for processing such an event.	180
11	Timeout	The software timed out waiting for some response or event to happen.	179
12	Inter-process communication	An internal process communication error occurred. This condition usually indicates some software error, but may also mean that some process was not running because of misconfiguration.	178
13	Software error	An internal software error occurred. Report the entire IEC string, including the diagnostic code field, to customer support.	180
14	Gateway or interface OOS	The gateway or signaling interfaces are being taken out of service (forcefully or gracefully). A possible cause may be the signaling interface required to support the call has already been administratively shut down.	187
21	H323 interworking error	The H.323 subsystem routinely provides specific IEC information, depending upon the source of an error. This IEC indicates that the exact source of an error is not available in this instance.	127
22	No usr responding, H225 timeout	Timeout occurred waiting for the callproc or alerting messages. The calling party is given the response "No user responding," and the called party is given the response "Recovery on timer expiry" as specified by Q931.	18
23	No answer from user	Setup was sent; callproc, alert, or progress messages were already received; and timeout occurred waiting for connect message.	19
24	ARQ wait timeout	A timeout occurred while waiting for response for admission request sent to the gatekeeper.	41

Table 19 **Error Codes for Subsystem 5 (H.323) (continued)**

Code	Descriptor	Explanation	Category
25	BRQ wait timeout	A timeout occurred while waiting for response for bandwidth request sent to the gatekeeper.	41
26	ANNEX E restart remote	The system received an Annex E RESTART message from the remote end. All calls with CRVs corresponding with destination address were cleared.	41
27	H225 invalid msg	The H.225 message was received with one of the following: <ul style="list-style-type: none"> • An invalid CRV • Parse error • Mandatory IE missing • Message out of sequence • Wrong IE length • Wrong IEC content 	95
28	Setup no called no	Received H.225 setup message and the mandatory field, called number, was not present.	96
29	H225 ASN error	The H.225 message received on parsing the H.225 message found an ASN decode error.	100
30	Wait RAS Cfm msg bad	The system received an unexpected message in a state waiting for RAS CFM message.	101
31	ACF, call redirected	In response to the ARQ, the gatekeeper returned 0.0.0.0 as the destination IP address in the Admission confirm (ACF). This is an attempt to redirect the call by the gatekeeper.	128
32	Setup, DNS fail	During an originating call attempt, the DNS/Enum resolution fails.	128
33	Setup no alternate	During call setup attempt using an alternate endpoint, the gatekeeper found that there are no alternate endpoints to try.	128
34	Setup, GW not registered	A new call is not allowed due to RAS not ready, that is, the gateway is not registered to the gatekeeper.	179
35	SETUP, next CRV invalid	Received setup message at terminating endpoint, failed to get a valid unique CRV value.	180
36	TCS encode send	Encoding and sending of terminal capability request failed.	180
37	End session ack send	Encoding and sending of end session acknowledgement PDU failed.	180
38	End session send	Encoding and sending of end session PDU failed.	180

Table 19 Error Codes for Subsystem 5 (H.323) (continued)

Code	Descriptor	Explanation	Category
39	Userinput send	Encoding and sending of user input signal PDU failed.	180
40	Userinput upd send	Encoding and sending of user input signal update PDU failed.	180
41	Userinput alpha send	Encoding and sending of user input alpha signal PDU failed.	180
42	TCS ack fail	The H.245 capability state machine failed to send TCS acknowledgement for the received TCS request.	180
43	TCS rej send fail	The H.245 capability state machine failed to send TCS reject for the received TCS request.	180
44	TCS rel sent	The H.245 capability state machine received a TCS request, and received an internal event to send the TCS release request.	180
45	SETUP send resource fail	During H.225 PDU send operation, an error occurred in memory allocation or socket queue was full.	180
46	ALERT send failed	Encoding and sending of ALERT PDU failed.	180
47	CallProc send failed	Encoding and sending of Call Proceeding PDU failed.	180
48	PROGRESS send failed	Encoding and sending of PROGRESS PDU failed.	180
49	NOTIFY send failed	Encoding and sending of NOTIFY PDU failed.	180
50	INFO send failed	Encoding and sending of INFO PDU failed.	180
51	USER INFO send failed	Encoding and sending of USER INFO PDU failed.	180
52	FACILITY send failed	Encoding and sending of FACILITY PDU failed.	180
53	SUSPEND send failed	Encoding and sending of SUSPEND PDU failed.	180
54	SUSPEND REJ send failed	Encoding and sending of SUSPEND REJECT PDU failed.	180
55	RESUME send failed	Encoding and sending of RESUME PDU failed.	180
56	PASSTHRU send failed	Encoding and sending of PASSTHRU PDU failed.	180
57	CONNECT send failed	Encoding and sending of CONNECT PDU failed.	180
58	SETUP ACK send failed	Encoding and sending of SETUP ACK PDU failed.	180
59	RSCMSM interface unavail	RSCMSM call admission control (CAC) interface unavailable due to resource failure.	181

Table 19 *Error Codes for Subsystem 5 (H.323) (continued)*

Code	Descriptor	Explanation	Category
60	H245 sock start fail	H.245 listening socket failed to start.	181
61	Call entry no mem	During the outgoing call, a resource failure occurred for call entry data structure.	181
62	Timeout h245 conn	H.245 connection wait timeout occurred.	183
63	TCS ack wait timeout	In the capability state machine, timer expiry occurred waiting for the TCS ACK message.	183
64	MS status indetermine	In the MSD state machine, the MSD request is received from remote, and the result of master slave status is indeterminate. This status occurs if sent and received random numbers are the same, or if both the local and remote terminal types are same.	183
65	MSD result disagreement	In the MSD state machine, MSD ACK is received from remote end but there is a disagreement in the MSD result.	183
66	MSD/MSD ACK Timeout	The gateway sent the MSD request, but neither the incoming MSD or MSD ACK message was received.	183
67	MSD ACK timeout	The gateway sent the MSD request, the incoming MSD was received from the remote end, and MSD ACK was sent to the remote end in response. The expected MSD ACK message was not received from the remote.	183
68	MSD rej received	In the MSD state machine, the MSD request was sent and the MSD reject was received from the remote end. MSD requests are sent for a fixed maximum number of retries before release.	183
69	MSD rel received	In the MSD state machine, the MSD request was sent, and the MSD release indication was received from the remote end.	183
70	OLC ACK T103 timeout	In the OLC state machine, T103 timer expired waiting for the OLC ACK message in response to the sent OLC message.	183
71	IPIP QoS Failure	Received QoS failure for non sync RSVP on IP-IP gateway, indicating minimum QoS was provided, not best effort.	184
72	BW > config, min QoS not best	The bandwidth in bearer capability exceeds the maximum configured, and minimum QoS was provided, not best effort. This error occurs during build of nonstandard QoS IE for setup or call processing messages.	184

Table 19 Error Codes for Subsystem 5 (H.323) (continued)

Code	Descriptor	Explanation	Category
73	NonStd min QoS not best	Received setup or call processing message with QoS in nonstandard parameter; the remote end did not have enough bandwidth to support RSVP. The acceptable QoS for audio was not best effort, and remote minimum QoS was provided, not best effort.	184
74	RSVP fail treat abort	Received RSVP failure and QoS treatment specifies that the gateway abort the call, because the minimum QoS was not best effort.	184
75	Fast QoS mismatch	Received fast start setup for QoS and remote minimum QoS was not best effort, but desired QoS was best effort.	184
76	Slow QoS mismatch	The H.225 state machine received a slow start H.225 Setup, with no H.245 address in Setup; that was not a sigonly call and remote minimum QoS was not best effort.	184
77	H225, QoS release	Received external QoS release from QoS resource manager for either the outgoing or incoming H.225 QoS call setup request.	184
78	Fallback chk fail	In the H.225 state machine, the fallback check failed.	184
79	H225 chn, sock fail	During H.225 connection establishment, the channel connection failed due to TCP socket error. The session target in the dial peer directly points to the remote VoIP endpoint.	186
80	Alt h225 chn sock fail	During H.225 connection establishment, in a call attempt to an alternate endpoint, the channel connection failed due to TCP socket error.	186
81	H225 chn, sock fail in RAS	During H.225 connection establishment (new connection), the channel connection failed due to TCP socket error. The dial peer has a session target of RAS.	186
82	H245, chn sock fail	During H.245 connection establishment, the channel connection failed due to TCP socket error.	186
83	SETUP send sock fail	An error occurred during the setup PDU send operation on socket connection for H..225. This error occurs under the following conditions: <ul style="list-style-type: none"> • If the remote IP is a reachable address for pinging, but is not a valid H.323 endpoint. • If there is an ASN.1 encoding error for setup PDU. 	186
84	Preauth fail	Preauthentication attempt failed.	228

Table 19 *Error Codes for Subsystem 5 (H.323) (continued)*

Code	Descriptor	Explanation	Category
85	OLC bandwidth exceeded	Received an OLC with bandwidth requirement that exceeds the configured value for acc-QoS for that media type.	278
86	OLC ind asymmetric codec	Received OLC indication when waiting for OLC ACK; the codecs in OLC did not match. Also the connection attempt was an asymmetric codec retry.	278
87	Received OLC rej	The H.245 state machine received an OLC reject message.	278
88	Fast codec mismatch	The H.225 state machine received an H.225 fast SETUP message during build of an OLC ACK and found that there was no matching codec.	278
89	OLC m/c, rcvd bw rej	The OLC state machine received a bandwidth reject message.	278
90	TCS ACK neg codec none	Received TCS ACK, but the negotiated codec result was none when call type was not passthrough.	278
91	Cap not supported	In the capability state machine, codec capabilities received from the remote end in the incoming TCS are not supported.	278
92	TCS rej received	In the capability state machine, after sending a TCS request, a TCS reject was received from the remote end.	278
93	Negotiated codec/T-man none	There was no negotiated codec or DTMF relayed mode based on the local or remote capabilities.	278
94	MSD send fail	Encoding and sending of Master Slave Request failed.	180

Table 20 *Error Codes for Subsystem 7 (SIP)*

Code	Descriptor	Explanation	Category
1	No memory	Dynamically allocated memory on the gateway is exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181
2	No buffers	Packet or buffer memory is exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181
3	CPU high	Call rejected because default or configured CPU usage threshold has been exceeded.	181
4	Low memory	Call rejected because default or configured memory usage threshold has been exceeded.	181

Table 20 Error Codes for Subsystem 7 (SIP) (continued)

Code	Descriptor	Explanation	Category
5	No dial peer match	No dial peer satisfied the match criteria for accepting or handling the call. This condition usually indicates a dial peer misconfiguration.	128
6	No DSP resource	Insufficient DSP resources to handle the call.	182
7	Socket error	An error occurred on a socket interface.	179
8	RTP inactivity error	Media (RTP/RTCP) inactivity timer expired for the call.	185
9	Invalid arguments	Invalid arguments passed to a function. This condition usually indicates an internal software error.	180
10	Invalid state	An unexpected event was received while in a state that was inappropriate for processing such an event.	180
11	Timeout	The software timed out waiting for some response or event to happen.	179
12	Inter-process communication	An internal process communication error occurred. This condition usually indicates some software error, but may also mean that some process was not running because of misconfiguration.	178
13	Software error	An internal software error occurred. Report the entire IEC string, including the diagnostic code field, to customer support.	180
14	Gateway or interface OOS	The gateway or signaling interfaces are being taken out of service (forcefully or gracefully). A possible cause may be the signaling interface required to support the call has already been administratively shut down.	187
21	SIP interworking error	The CCSIP subsystem provides IEC information depending upon the source of an error. This IEC indicates that specific information was not available. Use SIP debug tools to help in troubleshooting.	127
22	Hold/Retrieve Timeout	A call was placed on hold with a configurable timer started, and a timeout occurred for the retrieve operation.	41
23	Request, CallID unused	An incoming request message was received with a CallID that is not currently in use; that is, there was a mismatch in associating CallID with the current call control block.	95
24	2xx, dest SDP null	An INVITE was sent, a 2xx response was received but the destination Session Description Protocol (SDP) body was unavailable.	96

Table 20 *Error Codes for Subsystem 7 (SIP) (continued)*

Code	Descriptor	Explanation	Category
25	ACK, dest SDP null	An ACK request was received but the destination SDP body was unavailable for the delayed media call.	96
26	2xx, dest SDP null	A mid-call INVITE was sent, a 2xx response was received, but the destination SDP body was unavailable.	96
27	Redirect contact null	The SIP contact header was missing in incoming SIP redirect (3xx) or 485 messages.	96
28	Request, missing From/To	An incoming request message was received with the following conditions: <ul style="list-style-type: none"> • From, to, or both mandatory fields were missing • There was an error in parsing the from and to fields 	96
29	Request, missing Via	An incoming request message was received, and the mandatory field Via was missing.	96
30	Request, missing CSeq	An incoming request message was received, and the mandatory field CSeq was missing.	96
31	Request, missing Contact	An incoming request message was received, and the mandatory field Contact was missing.	96
32	Request, unknown method	An incoming request message was received with an unknown or invalid SIP method.	97
33	Request, Version bad	An incoming request message was received with a SIP version that was not supported on the user agent.	97
34	18x, invalid disptype	Invalid or unsupported Content-Disposition with mandatory handling was received in an 18x session progress message.	100
35	INVITE, invalid IE content	INVITE with either invalid header contents, SDP, or VIA parameters was received.	100
36	Request, parse Via	An incoming request message was received and encountered an error in parsing the Via field.	100
37	Request, parse CSeq	An incoming request message was received that generated an error in parsing the CSeq field.	100
38	Request, parse Contact	An incoming request message was received that generated an error in parsing the Contact field.	100
39	Request, extension bad	An incoming request message was received with a Require header field containing an option tag with an unsupported extension.	100

Table 20 Error Codes for Subsystem 7 (SIP) (continued)

Code	Descriptor	Explanation	Category
40	Request, Record-Route bad	An incoming request message was received with a Record-Route header field in a malformed format.	100
41	Request, Diversion bad	An incoming request message was received with a Diversion header field in a malformed format.	100
42	Sent INVITE, bad msg	An unknown SIP response message was received while the system was waiting for an INVITE response.	101
43	Bad msg for state	During an outgoing resource reservation state, an unexpected SIP response message was received for the current call state.	101
44	Session trgt null	During an outgoing call, a session target found null.	128
45	Session trgt parse	During an outgoing call, a session target parse failed.	128
46	Session trgt invalid	During an outgoing call, an invalid session target type occurred.	128
47	DNS query fail	For an outgoing call, a DNS lookup of session target failed.	128
48	INVITE, DNS qry fail	A failure response, rcvd target addr null, was received for the DNS query that was sent to resolve the contact in the received invite/FQDN in SDP.	128
49	ACK, DNS qry fail	A failure response, rcvd target addr null, was received for the DNS query that was sent to resolve the contact in the received FQDN message in SDP after the 200 OK message was sent	128
50	MID-INVITE, dns qry fail	A failure response, rcvd target addr null, was received for the DNS query that was sent to resolve the contact or SDP FQDN message in the received mid-INVITE request.	128
51	100, DNS qry fail	DNS lookup failure for the Contact header/FQDN message that was received in the SIP response message.	128
52	DNS qry fail	A failure response, rcvd target addr null, was received for the DNS query that was sent for contact resolution, after a QoS progress message has been sent.	128
53	3xx, redirect loop	Upon the system receiving a 3xx response on an outbound call during redirect procedure, a redirect loop was encountered.	128

Table 20 *Error Codes for Subsystem 7 (SIP) (continued)*

Code	Descriptor	Explanation	Category
54	3xx, redirect max	Upon the system receiving a 3xx response on an outbound call during redirect procedure, the maximum number of redirects was exceeded.	128
55	3xx, redirect exhaust	Upon the system receiving a 3xx response on an outbound call during redirect procedure, all contact choices were exhausted.	128
56	Enum resolution fail	A failure response, rcvd contact list null, was received for the query that was sent for enum resolution.	128
57	Contact not resolved	The INVITE Contact or Record Route was not resolved to an IP address and port due to one of the following: <ul style="list-style-type: none"> • The user answered the call. • A loopback event was received from the session application during the connection attempt. 	128
58	Setup conn timeout	No response was received for the socket connection request.	129
59	1xx wait timeout	Retries were exhausted for sending INVITEs while waiting for 1xx response, and no redirect information was available.	129
60	200 wait timeout	Retries were exhausted for PRACK retransmission.	129
61	200 wait timeout	Retries were exhausted for COMET retransmission.	129
62	PRACK wait timeout	Retries were exhausted for sending rel1xx messages and waiting for PRACK.	129
63	PRACK wait timeout & state bad	This condition occurs when the system tries to resend the rel1xx while waiting for a PRACK message, but the call state is wrong.	129
64	Session app rsp timeout	An INVITE request was received and timeout occurred while the system waited for a response to the SETUP sent from the session application.	129
65	1xx wait timeout	Retries were exhausted for sending midcall INVITE, while waiting for 1xx response and not trying DNS.	129
66	ACK wait timeout	Retries were exhausted after sending 200 OK message and waiting for ACK.	129
67	ACK wait timeout	Error occurs if the connection attempt is in an active state and ACK is not received after retries were exhausted sending 200 OK for the initial incoming INVITE.	129

Table 20 **Error Codes for Subsystem 7 (SIP) (continued)**

Code	Descriptor	Explanation	Category
68	200 wait timeout	Retries were exhausted sending INVITE and waiting for the 200 OK.	129
69	Xfer 2xx wait timeout	Failed call transfer, system timed out while waiting response for NOTIFY request.	129
70	Connect wait timeout	A timeout occurred after receiving a 200 OK in response to an INVITE and trying to request a UDP/TCP connection to the endpoint specified in the Contact or Record Route headers in order to send the ACK.	129
71	Info Req wait timeout	Timeout occurred while waiting for the Info request on a UDP/ TCP connection. Can occur for user agent client (UAC) or user agent server (UAS).	129
72	Send 200, rsrc fail	Received invite request, resource error in sending 200 OK response.	180
73	Send 200, rsrc fail	Received PRACK message, resource error in sending 200 OK response.	180
74	Send PRACK, rsrc fail	Sending PRACK message failed.	180
75	Send COMET, rsrc fail	Sending COMET message failed during retransmission.	180
76	Send 183, rsrc fail	Sending 183 (progress) response message failed during transmission.	180
77	Send 180, rsrc fail	Sending of 180 response message failed during transmission.	180
78	Rcvd 3xx, contact parse	Internal error or malformed Contact header encountered during SIP redirect (3xx) response processing.	180
79	Rsrc process media	Resource failure during processing of the media changes.	180
80	Err launch dns	Encountered a resource error in launching a DNS query.	180
81	Err reinserting ccb	Resource error in reinserting the associated call control block into table.	180
82	INVITE send fail	A send operation for invite request failed.	180
83	NOTIFY send fail	A send operation for notify request failed.	180
84	ACK send fail	A send operation for ACK request failed.	180
85	REFER send fail	A send operation for refer request failed.	180
86	REFER response send fail	A send operation for refer response failed.	180
87	Call Hold fail	A hold operation failed on an active call while resending the invite to the peer.	180

Table 20 *Error Codes for Subsystem 7 (SIP) (continued)*

Code	Descriptor	Explanation	Category
88	RSCMSM interface unavail	The voice CPU and memory resource monitor, RSCMSM CAC interface, is unavailable due to resource failure.	181
89	Call entry no mem	While creating a call entry, a resource failure occurred during call origination.	181
90	Redirect info no mem	Memory allocation failure for a redirect info structure creation during a SIP redirect (3xx) message process.	181
91	Setup, QoS mismatch	During an outgoing call, a mismatch occurred in QoS or invalid reliable provisional response and QoS configuration.	184
92	1xx, QoS mismatch	After 1xx Session progress receipt, QoS failure in negotiation occurred while the system checked the configured req and acc QoS values against values in incoming message.	184
93	RSVP failure outgoing	Resource allocation failure occurred at RSVP layer for outgoing call.	184
94	QoS retries crossed	Retries were exhausted for sending QoS PROGRESS or resource reservation requests.	184
95	RSVP failure incoming	Resource allocation failure occurred at RSVP layer for incoming call.	184
96	INVITE, QoS mismatch	During handling of INVITE, QoS failure in negotiation occurred while checking the configured req and acc QoS values against values in incoming message.	184
97	PRACK, QoS mismatch	During handling of PRACK, QoS failure in negotiation occurred while the system checked the configured req and acc QoS values against values in incoming message.	184
98	COMET, QoS mismatch	During handling of COMET, QoS failure in negotiation occurred while the system checked the local QoS values with those in received a=QoS:line in COMET.	184
99	Fback chk fail	Fallback check failure for IP network quality occurred at either the originating or terminating gateway.	184
100	ACK send sock err	The success response for INVITE send has been received; the socket returned an error for sending ACK.	186
101	Connection to contact fail	Sent INVITE and received 200 OK; TCP/UDP connection to the endpoint specified in the contact or record route failed.	186
102	Socket conn refused	A connection refused error occurred during a send operation with error 146.	186

Table 20 Error Codes for Subsystem 7 (SIP) (continued)

Code	Descriptor	Explanation	Category
103	INVITE, Preauth fail	Received INVITE; preauthentication attempt failed.	228
104	180, codec mismatch	Media negotiation failure occurred for incoming 180 Alerting responses.	278
105	183, codec mismatch	Media negotiation failure occurred for incoming 183 Session Progress responses.	278
106	200, codec mismatch	Media negotiation failure occurred for incoming 200 OK responses.	278
107	RE-INVITE, codec mismatch	A media information mismatch occurred for the media information received in re-INVITE with the media information previously received in INVITE.	278
108	ACK, codec mismatch	During processing of the ACK message in response to 200 OK, media negotiation failed due to a codec mismatch in delayed media processing.	278
109	2xx, codec mismatch	Sent mid-INVITE; received 2xx response and the media negotiation failed due to a codec mismatch.	278
110	INVITE, codec mismatch	Media negotiation failure occurred for an incoming INVITE request.	278
111	PRACK, codec mismatch	Media negotiation failure occurred for an incoming PRACK message.	278

Table 21 Error Codes for Subsystem 9 (VTSP)

Code	Descriptor	Explanation	Category
1	No Memory	Dynamically allocated memory on the gateway was exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181
2	No buffers	Packet or buffer memory is exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181
3	CPU high	Call rejected because the default or configured CPU usage threshold has been exceeded.	181
4	Low memory	Call rejected because the default or configured memory usage threshold has been exceeded.	181
5	No dial peer match	No dial peer satisfied the match criteria for accepting or handling the call. This condition usually indicates a dial peer misconfiguration.	128
6	No DSP resource	There were insufficient DSP resources to handle the call.	182

Table 21 *Error Codes for Subsystem 9 (VTSP) (continued)*

Code	Descriptor	Explanation	Category
7	Socket error	An error occurred on a socket interface.	179
8	RTP inactivity error	Media (RTP/RTCP) inactivity timer expired for the call.	185
9	Invalid arguments	Invalid arguments passed to a function. This condition usually indicates an internal software error.	180
10	Invalid state	An unexpected event was received while in a state that was inappropriate for processing such an event.	180
11	Timeout	The software timed out waiting for some response or event to happen.	179
12	Inter-process communication	An internal process communication error occurred. This usually indicates some software error, but may also mean that some process was not running because of misconfiguration.	178
13	Software error	An internal software error occurred. Report the entire IEC string, including the diagnostic code field, to customer support.	180
14	Gateway or interface OOS	The gateway or signaling interfaces are being taken out of service (forcefully or gracefully). A possible cause may be the signaling interface required to support the call has already been administratively shut down.	187
21	DSP mode change	An attempt to change the DSP mode failed.	182
22	DSP unknown failure	An unspecified failure occurred in DSP interaction.	182
23	No DSP memory available	DSP could not allocate chunk memory, indicating a temporary overload or a memory leak caused by faulty software.	182
24	No DSP resource available	The call was disconnected because no DSP resources were available.	182
25	Bad DSP parameters	The call was disconnected because of some code error path.	182
26	Codec incompatible	The call failed because of incompatible codec types.	182
27	DSP alarm	DSP sent an alarm. Possible causes are: <ul style="list-style-type: none"> • Receiving a bad packet • Receiving a wrong message • A software problem 	182
28	No voice cut through	The call failed because the voice path could not be cut through.	182

Table 21 *Error Codes for Subsystem 9 (VTSP) (continued)*

Code	Descriptor	Explanation	Category
29	Tie line misconfiguration	A tie-line call failed because of a misconfiguration of the tie line on the voice port. Check the tie-line string.	180
30	Invalid call mode	An unknown call mode was specified to set up a call. This condition usually indicates an internal software error.	180
31	Interface deleted	Failure to set up a call occurred on a deleted interface. This condition may happen if a call comes on an interface while the interface is being hot-swapped.	182
32	TDM hairpinning failed	TDM hairpinning failed. This condition may occur because of data structure allocation failure or because of actual hairpinning failure.	182
33	Set digit mode failed	Attempt to set the DSP to the specific digit mode failed. This condition also occurs when memory is exhausted.	182
34	Setup indication failed	This condition occurs when memory is exhausted.	180
35	DSP timeout	Call failed because of a time out on waiting for DSP action.	182

Table 22 *Error Codes for Subsystem 10 (AFSAPP)*

Code	Descriptor	Explanation	Category
1	No memory	Dynamically allocated memory on the gateway was exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181
2	No buffers	Packet or buffer memory was exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	181
3	CPU high	Call rejected because default or configured CPU usage threshold has been exceeded.	181
4	Low memory	Call rejected because default or configured memory usage threshold has been exceeded.	181
5	No dial peer match	No dial peer satisfied the match criteria for accepting or handling the call. This condition usually indicates a dial peer misconfiguration.	128
6	No DSP resource	There were insufficient DSP resources to handle the call.	182
7	Socket error	An error occurred on a socket interface.	179
8	RTP Inactivity Error	Media (RTP/RTCP) inactivity timer expired for the call.	185

Table 22 **Error Codes for Subsystem 10 (AFSAPP)**

Code	Descriptor	Explanation	Category
9	Invalid arguments	Invalid arguments were passed to a function. This condition usually indicates an internal software error.	180
10	Invalid State	Some unexpected event was received while the system was in a state that was inappropriate for processing such an event.	180
11	Timeout	The software timed out waiting for some response or event to happen.	179
12	Inter-process communication	An internal process communication error occurred. This condition usually indicates some software error, but may also mean that some process was not running because of misconfiguration.	178
13	Software Error	An internal software error occurred. Report the entire IEC string, including the diagnostic code field, to customer support.	180
14	Gateway or Interface OOS	The gateway or signaling interfaces are being taken out of service (forcefully or gracefully). A possible cause may be the signaling interface required to support the call has already been administratively shut down.	187
21	OSP Fail	OSP settlement checking failed for an outbound call.	228
22	Call blocked by CLI	The call was rejected because it matched the profile defined for calls to be blocked. Diagnostic codes are the following: <ul style="list-style-type: none"> • 1—unassigned number • 17—user-busy • 21—call reject • 28—invalid number 	228
23	Media request failed	Indicates a failure in media play or some other media operation.	181
24	Digit collect failed	The error occurred due to the session application failure to collect digits. The failure may be normal; that is, the caller did not enter any digits, or it may be due to an actual error in software or hardware. To interpret the diagnostic code, see Tcl IVR cd_XXX status codes in the “Events and Status Codes” chapter in the <i>Tcl IVR API Version 2.0 Programming Guide</i> .	179

Table 22 Error Codes for Subsystem 10 (AFSAPP)

Code	Descriptor	Explanation	Category
25	Call setup failed	Call setup was not successful. To interpret the diagnostic code, see Tcl IVR ls_xxx status codes in the “Events and Status Codes” chapter in the <i>Tcl IVR API Version 2.0 Programming Guide</i> .	179
26	Credit time has expired	OSP settlement allocated a limited time for call usage. The total time of the call has exceeded that usage.	228

Table 23 shows the standard internal error codes (numbered 1 through 14) and the new gatekeeper-specific error codes (numbered 21 through 45) added in Release 12.4(4)T.

Table 23 Error Codes for the Gatekeeper Subsystem

Code	Descriptor	Explanation	Category
1	No memory	Dynamically allocated memory on the gateway was exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	19
2	No buffers	Packet or buffer memory was exhausted. This condition may indicate a temporary overload or a memory leak caused by faulty software.	19
3	Timeout	Call rejected because the default or configured CPU usage threshold has been exceeded.	20
4	Software error	An internal software error occurred. Report the entire IEC string, including the diagnostic code field, to customer support.	21
5	Code not assigned, reserved for future use	Error code not assigned—reserved for future use.	0
6	Code not assigned, reserved for future use	Error code not assigned—reserved for future use.	0
7	Code not assigned, reserved for future use	Error code not assigned—reserved for future use.	0
8	Code not assigned, reserved for future use	Error code not assigned—reserved for future use.	0
9	Code not assigned, reserved for future use	Error code not assigned—reserved for future use.	0
10	Code not assigned, reserved for future use	Error code not assigned—reserved for future use.	0
11	Code not assigned, reserved for future use	Error code not assigned—reserved for future use.	0
12	Code not assigned, reserved for future use	Error code not assigned—reserved for future use.	0

Table 23 *Error Codes for the Gatekeeper Subsystem (continued)*

Code	Descriptor	Explanation	Category
13	Code not assigned, reserved for future use	Error code not assigned—reserved for future use.	0
14	Call threshold exceeded	ARQ came, but because the call threshold is exceeded, this ARQ cannot be processed.	8
21	GK server error	Error in processing the GKTMP message. Server is trying to modify a field that should not be modified.	20
22	GW out of resource	Gateway is out of resources, so no more calls can be routed.	14
23	Could not find an available GW for routing	Address resolution was not successful. Could not find the GW to route.	8
24	LRQ fail	LRQ/LRQs were sent to the remote GK, but the GK could not resolve.	20
25	Invalid endpoint ID	Mandatory endpoint identifier field in the incoming ARQ is invalid or not present.	7
26	Bad message from server	Badly formatted server message. GK/GKAPI could not process.	20
27	Proxy selection failed	Proxy selection failed.	8
28	No session bandwidth	There is no session bandwidth to process the incoming ARQ.	3
29	No total bandwidth	There is no total bandwidth to process incoming ARQ.	3
30	Invalid CAT token present	Incoming ARQ did not have a valid CAT to authenticate.	9
31	Endpoint killed	GK had sent a request AAA/Route server/OSP server. When the response came, the endpoint was deleted.	8
32	DRQ in progress	GK had sent a request AAA/Route server/OSP server. When the response came, DRQ is in progress.	8
33	No server responded	GK sent a request to the route server, but no server responded.	20
34	Dest proxy not found	Proxy session failed, so admission is denied.	8
35	Incomplete address	No destination Info alias and no destination IP address, and no pointers to remote zones or carriers.	11
36	Bandwidth not available	Remote or interzone bandwidth is not available.	3
37	Unable to send ACF	ACF was prepared, but could not be sent. ASN or socket error.	22
38	Duplicate CRV	Answer ARQ came with a CRV that is already being processed at the GK.	21

Table 23 Error Codes for the Gatekeeper Subsystem (continued)

Code	Descriptor	Explanation	Category
39	IZCT acc list denied	IZCT access list denied.	9
40	No bandwidth	Bandwidth not available at the terminating GK.	3
41	No bandwidth during update request	When a call is using a proxy or the call is intrazone, the call failed trying to update the bandwidth information in the call record.	3
42	Forced disengage	call delete CLI was used to forcefully delete the call.	24
43	GK shutdown	Call was deleted because the GK was shut down.	24
44	Aged call	Call was deleted because of aging.	24
45	Acc list denied	Access list denied.	9

How to Configure IEC Options

This section contains the following procedures:

- [Configuring IEC Options, page 38](#) (optional)
- [Verifying IEC Options, page 41](#) (optional)

Configuring IEC Options

No configuration is required to enable the Cisco VoIP Internal Error Codes feature. Select the following optional configuration tasks:

- [Enabling IEC Syslog Reporting, page 38](#)
- [Configuring Cause Code Mapping, page 39](#)
- [Troubleshooting Tips, page 40](#)

Enabling IEC Syslog Reporting

This task enables IEC syslog reporting.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice iec syslog**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	voice iec syslog Example: Router(config)# voice iec syslog	(Optional) Enables syslog messages as IECs occur.

Configuring Cause Code Mapping

This task enables cause code mapping.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice cause-code**
4. error-category *number* q850-cause *number*
5. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Router# configure terminal	Enters global configuration mode.
Step 3	voice cause-code Example: Router(config)# voice cause-code	(Optional) Enters voice cause-code configuration mode.

	Command or Action	Purpose
Step 4	<pre>error-category number q850-cause number</pre> <p>Example: <pre>Router(conf-voice-cause)# error-category 128 q850-cause 27</pre></p>	(Optional) Specifies the values to be mapped. <ul style="list-style-type: none"> • Values for error-category range from 128 to 278. • Values for the Q.850 cause code range from 1 to 127.
Step 5	<pre>exit</pre> <p>Example: <pre>Router(conf-voice-cause)# exit</pre></p>	Exits voice cause-code configuration mode.

Troubleshooting Tips

The IEC feature is itself a troubleshooting tool. By enabling the **voice iec syslog command** you can display IECs logged in real time, which allows you to isolate a failure cause without turning on debugging. Then, based on the IEC reported, you can selectively enable the appropriate debug tool to gather additional information.

The IEC feature also provides a Cisco.com diagnostic tool that allows you to enter an IEC dotted string and receive an explanation of the component fields. The explanation includes a description of the problem, and depending upon the error type, a recommended course of action. Use the IEC lookup tool at <http://www.cisco.com/univercd/cc/td/doc/product/voice/vtgemd.htm>.

To troubleshoot specific subsystems that do not generate corresponding IECs, use the following **debug** and **show** commands:

- To learn whether the ISDN link is up or down, use the **show isdn status** command.
- To display information about whether the ISDN link is receiving SETUP, CALLPRO, ALERT, CONNECT, and RELEASE COMPLETE messages, use the **debug isdn q931** command.
- To display information about H.225 and RAS messages exchanged between a gateway and gatekeeper, use the **debug h225 asn1** command. H.225 debug output for the terminating side, in the initial stage when a setup message is being received, provides an indication if messages are being received from the IP side and if H.323 service is operational. If the H.225 connection is not established from the incoming side, then no IECs are generated.

What to Do Next

Proceed to the section “[Verifying IEC Options, page 41.](#)”

New and Modified Configuration Commands for Gatekeeper IECs in Cisco IOS Release 12.4(4)T

To enable the enhanced capabilities of the gatekeeper-specific IECs in Release 12.4(4)T, there is one new command and one modified command. This section describes only the new information. For complete information on the commands for voice gateways and gatekeepers, refer to the *Cisco IOS Voice Configuration Library* on Cisco.com.

This release introduces a new command for the gatekeeper configuration that causes retention of call history and enables you to specify the number of records to be kept in the history table.

In gatekeeper configuration mode, enter:

```
gatekeeper(config)# call-history max-size number
```

The *number* argument in this syntax can be any number from 0 to 1200. The default is 15. This represents the maximum number of records of old calls to be stored and available for display.

To display the historical information, enter the following command on the gatekeeper:

```
gatekeeper# show gatekeeper calls history
```

This command has been modified with the addition of the **history** keyword. This keyword was added to display call history information along with internal error codes at the gatekeeper. The number of disconnected calls displayed in response to this command is the *number* value specified in the **call-history max-size *number*** command. Use of this **max-size** number helps to reduce excessive CPU usage in the storage and reporting of this information.

Verifying IEC Options

You can use **show** command output to display IEC option configuration, to verify that the feature is working, and to display IEC counter information.

Prerequisites

Before you can display IEC counter information, you must configure voice statistics settings.

SUMMARY STEPS

1. **enable**
2. **voice statistics type iec**
3. **voice statistics max-storage-duration {day *number-of-days* | hour *number-of-hours* | minute *number-of-minutes* }**
4. **voice statistics time-range periodic *interval-length* [start *hh:mm*] [end *hh:mm*] [days-of-week *days*]**
5. **voice statistics time-range since-reset**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example: Router> enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<pre>voice statistics type iec</pre> <p>Example: Router# voice statistics type iec</p>	(Optional) Configures the collection of IEC statistics.

Command or Action	Purpose
<p>Step 3</p> <pre>voice statistics max-storage-duration {day number-of-days hour number-of-hours minute number-of-minutes}</pre> <p>Example: Router# voice statistics max-storage-duration day 1</p>	<p>(Optional) Configures how long interval counters are kept for display.</p> <ul style="list-style-type: none"> If you want to display counters for past intervals, you must configure a storage duration for expired counters. Otherwise, once the interval has expired, the counters are no longer available.
<p>Step 4</p> <pre>voice statistics time-range periodic interval-length [start hh:mm] [end hh:mm] [days-of-week days]</pre> <p>Example: Router# voice statistics time-range periodic 30minutes</p>	<p>(Optional) Specifies IEC collection intervals.</p> <ul style="list-style-type: none"> The <i>interval-length</i> argument takes one of the following values: <ul style="list-style-type: none"> 5minutes 15minutes 30minutes 60minutes 1day The range for <i>hh:mm</i> is 00:00 to 23:59. The default for the start keyword is 00:00. The default for the end keyword is 00:00. The <i>days</i> argument takes one of the following values: <ul style="list-style-type: none"> friday—Friday monday—Monday saturday—Saturday sunday—Sunday thursday—Thursday tuesday—Tuesday wednesday—Wednesday daily—Every day of the week weekdays—Monday thru Friday weekend—Saturday and Sunday <p>The default is daily.</p>
<p>Step 5</p> <pre>voice statistics time-range since-reset</pre> <p>Example: Router# voice statistics time-range since-reset</p>	<p>(Optional) Enables the collection of call statistics information accumulated since the last resetting of IEC counters.</p>

Displaying IEC Options

Perform this task to verify that the Cisco VoIP Internal Error Codes feature is working.

SUMMARY STEPS

- enable

2. **show running-config**
3. `show voice cause-code category-q850`
4. **show voice iec description *string***
5. `show voice statistics iec {interval number | since-reboot | since-reset}`
6. `clear voice statistics iec`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show running-config Example: Router# show running-config	(Optional) Displays the configuration information currently running on the router.
Step 3	<code>show voice cause-code category-q850</code> Example: Router# show voice cause-code category-q850	(Optional) Displays Q.850 cause code mapping.
Step 4	<code>show voice iec description <i>string</i></code> Example: Router# show voice iec description 1.1.128.1.5.0	(Optional) Displays an IEC description.
Step 5	<code>show voice statistics iec {interval <i>number</i> since-reboot since-reset}</code> Example: Router# show voice statistics iec interval 15	(Optional) Displays IEC statistics. <ul style="list-style-type: none"> • Specify the following displays: statistics by selected time interval, or statistics since the last router reboot, or statistics since the last instance when counters were cleared.
Step 6	<code>clear voice statistics iec</code> Example: Router# clear voice statistics iec	(Optional) Resets IEC counters.

Configuration Examples for Cisco VoIP Internal Error Codes

This section provides configuration examples for the tasks identified in the previous section.

- [Enabling IEC Syslog Reporting and Configuring Cause Code Mapping: Example, page 44](#)
- [Verifying IEC Configuration: Example, page 44](#)

Enabling IEC Syslog Reporting and Configuring Cause Code Mapping: Example

In the following example, IEC syslog reporting and cause-code mapping are enabled:

```
enable
configure terminal
  voice iec syslog
  voice cause-code
    error-category 128 q850-cause 27
```

Verifying IEC Configuration: Example

In the following examples, the output is displayed for each command used to verify IEC configuration:

Sample Output from the show running-config Command: Example

```
Router# show running-config

Building configuration...

Current configuration :2791 bytes
!
version 12.2
no parser cache
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname GW-1
!
no boot startup-test
!
!
resource-pool disable
spe default-firmware spe-firmware-1
!
!
aaa new-model
!
!
aaa group server radius h323
!
aaa authentication login h323 group radius group h323
aaa authorization config-commands
aaa authorization exec h323 group h323
aaa accounting connection h323 start-stop group radius group h323
aaa session-id common
!
isdn switch-type primary-5ess
!
```

The following lines show optional IEC configuration information:

```
voice iec syslog
voice cause-code
  error-category 128 q850-cause 27
  error-category 129 q850-cause 38
!
```

```
!  
!  
controller T1 3/0  
  framing esf  
  linecode b8zs  
  pri-group timeslots 1-24  
!  
controller T1 3/1  
  shutdown  
  framing sf  
  linecode ami  
gw-accounting aaa  
!  
!  
!  
interface FastEthernet0/0  
  ip address 172.18.195.28 255.255.255.0  
  no ip route-cache  
  no ip mroute-cache  
  duplex full  
  speed 100  
  no cdp enable  
  h323-gateway voip interface  
  h323-gateway voip id GK-1 ipaddr 172.18.195.41 1718  
  h323-gateway voip h323-id GW-1  
!  
interface FastEthernet0/1  
  no ip address  
  no ip route-cache  
  no ip mroute-cache  
  shutdown  
  duplex auto  
  speed auto  
  no cdp enable  
!  
interface Serial0/0  
  no ip address  
  no ip route-cache  
  no ip mroute-cache  
  shutdown  
  clockrate 2000000  
  no cdp enable  
!  
interface Serial0/1  
  no ip address  
  no ip route-cache  
  no ip mroute-cache  
  shutdown  
  clockrate 2000000  
  no cdp enable  
!  
interface Serial3/0:23  
  no ip address  
  dialer-group 1  
  isdn switch-type primary-5ess  
  isdn incoming-voice modem  
  no cdp enable  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 172.18.195.1  
no ip http server  
!  
!  
!
```

```

radius-server host 172.18.200.222 auth-port 1645 acct-port 1646
radius-server key lab
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
voice-port 3/0:D
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
dial-peer voice 100 pots
 destination-pattern 1#919....
 direct-inward-dial
 port 3/0:D
 prefix 919
!
dial-peer voice 301 voip
 destination-pattern 7190003
 session target ras
!
!
gateway
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
 logging synchronous
line vty 0 4
 password lab
line 1/00 1/59
 no flush-at-activation
 modem InOut
!
scheduler allocate 10000 400
end

```

Sample Output from the show voice iec description Command: Example

```

Router# show voice iec description 1.1.128.1.5.0

IEC Version:1
Entity:1 (Gateway)
Category:128 (Destination address resolution failure)
Subsystem:1 (CCAPI)
Error:5 (No dial peer match)
Diagnostic Code:0

```

Sample Output from the show voice statistics iec Command: Example

```

Router# show voice statistics iec since-reset

Internal Error Code counters

```

```

-----
Counters since last reset (2002-11-28T01:55:31Z):
  SUBSYSTEM CCAPI [subsystem code 1]
    [errcode  6] No DSP resource                5

  SUBSYSTEM SSAPP [subsystem code 4]
    [errcode  5] No dial peer match            2
    [errcode  3] CPU high                       96

  SUBSYSTEM H323 [subsystem code 5]
    [errcode 22] No Usr Responding, H225 timeout  1
    [errcode 27] H225 invalid msg                1
    [errcode 79] H225 chn, sock fail            27

  SUBSYSTEM VTSP [subsystem code 9]
    [errcode  6] No DSP resource                83

```

```

Router# show voice statistics iec since-reboot
Internal Error Code counters
-----
Counters since reboot:
  SUBSYSTEM CCAPI [subsystem code 1]
    [errcode  6] No DSP resource                93

  SUBSYSTEM SSAPP [subsystem code 4]
    [errcode  5] No dial peer match            830
    [errcode  3] CPU high                       1423

  SUBSYSTEM H323 [subsystem code 5]
    [errcode 21] No Usr Responding, H225 timeout  21
    [errcode 23] H225 invalid msg                17
    [errcode 39] H225 chn, sock fail            2073

  SUBSYSTEM VTSP [subsystem code 9]
    [errcode  6] No DSP resource                429

```

Before using the **show voice statistics iec interval** command, first determine the intervals available for display by using the **show voice statistics interval-tag** command:

```

Router# show voice statistics interval-tag
Current Time:2002-11-28T06:04:21Z
INTERVAL-TAG  START TIME                END TIME
=====
1              2002-11-28T02:00:00Z  2002-11-28T02:30:01Z
2              2002-11-28T02:30:01Z  2002-11-28T03:00:01Z
3              2002-11-28T03:00:01Z  2002-11-28T03:30:01Z
4              2002-11-28T03:30:01Z  2002-11-28T04:00:01Z
5              2002-11-28T04:00:01Z  2002-11-28T04:30:01Z
6              2002-11-28T04:30:01Z  2002-11-28T05:00:01Z
7              2002-11-28T05:00:01Z  2002-11-28T05:30:01Z
8              2002-11-28T05:30:01Z  2002-11-28T06:00:01Z
9              2002-11-28T06:00:01Z  2002-11-28T06:04:21Z

```

The following example shows **interval-tag 8** statistics:

```

Router# show voice statistics iec interval 8

Internal Error Code counters
-----
Counters for interval 8, beginning 2002-11-28T05:30:01Z,ending 2002-11-28T06:00:01Z:
  SUBSYSTEM CCAPI [subsystem code 1]

```

```

[errcode 6] No DSP resource 1
SUBSYSTEM SSAPP [subsystem code 4]
[errcode 3] CPU high 15
SUBSYSTEM H323 [subsystem code 5]
[errcode 23] H225 invalid msg 1
[errcode 39] H225 chn, sock fail 1
SUBSYSTEM VTSP [subsystem code 9]
[errcode 6] No DSP resource 6

```

Sample Output from the clear voice statistics Command: Example

The following examples show **voice statistics iec since-reset** output before and after you issue the **clear voice statistics** command:

```

Router# show voice statistics iec since-reset

Internal Error Code counters
-----
Counters since last reset (2002-11-28T01:55:31Z):
SUBSYSTEM CCAPI [subsystem code 1]
[errcode 6] No DSP resource 5

SUBSYSTEM SSAPP [subsystem code 4]
[errcode 5] No dial peer match 2
[errcode 3] CPU high 96

SUBSYSTEM H323 [subsystem code 5]
[errcode 21] No Usr Responding, H225 timeout 1
[errcode 23] H225 invalid msg 1
[errcode 39] H225 chn, sock fail 27

SUBSYSTEM VTSP [subsystem code 9]
[errcode 6] No DSP resource 83

Router# clear voice statistics iec
Router# show voice statistics iec since-reset
Internal Error Code counters
-----
Counters since last reset (2002-12-12T22:33:25Z):
No errors.

```

Sample Output from the show voice cause-code category-q850 Command: Example

```

Router# show voice cause-code category-q850

The Internal Error Category to Q850 cause code mapping table:-

Error Configured Default Description
Category Q850 Q850
128 27 3 Destination address resolution failure
129 38 102 Call setup timeout
178 41 41 Internal Communication Error
179 41 41 External communication Error
180 47 47 Software Error
181 47 47 Software Resources Unavailable
182 47 47 Hardware Resources Unavailable
183 41 41 Capability Exchange Failure
184 49 49 QoS Error
185 41 41 RTP/RTCP receive timer expired or bearer layer failure
186 38 38 Signaling socket failure
187 38 38 Gateway or signaling interface taken out of service

```

228	50	50	User is denied access to this service
278	65	65	Media Negotiation Failure due to non-existing Codec

Troubleshooting VoIP Networks Using Cisco VoIP Internal Error Codes

IECs are generated for errors that cause the gateway to release or refuse a call. This section provides procedural and reference information used to troubleshoot gateway-detected errors and resolve problems on the gateway and with other VoIP network entities.

Because fields within the IEC identify which network entity and subsystem originated an error, they can be used to diagnose and isolate failures that can cause call disconnects.

This section discusses troubleshooting scenarios using IECs to diagnose and resolve the problems described in the following sections:

- [Troubleshooting Two-Stage Dialing Failures, page 49](#)
- [Troubleshooting Socket Failures, page 53](#)

Troubleshooting Two-Stage Dialing Failures

The following example shows how to troubleshoot a two-stage dialing failure.

Symptom

The Cisco router or gateway rejects a call placed by a PSTN ISDN user after all the digits have been dialed.

Problem Description

The PSTN user enters a destination number that is routed through the PSTN ISDN switch, which sends an ISDN SETUP message to the router. The router tags the incoming call leg and sends back an ISDN CONNECT message. The caller receives second dial tone. The router then enters the digit collection stage to use the collected digits to route the call to the next hop, at which point the router rejects the call.

Troubleshooting Tasks

Perform the following steps to determine the reason for call failure.

-
- Step 1** Use the **voice iec syslog** command to enable displaying of IECs as they are encountered in real-time.
 - Step 2** Use the **voice iec statistics type iec** command to configure the collection of IEC statistics.
 - Step 3** Use the **show running-config** command to verify IEC, ISDN, and dial-peer configuration, as shown in the following partial sample output:

```
Router> show running-config  
  
Building configuration...  
!
```

```
voice rtp send-recv
!
voice service voip
```

The following lines show the IEC configuration:

```
voice iec syslog
no voice hpi capture buffer
no voice hpi capture destination
voice statistics type iec
!
!
!
```

The following lines show the T1 configuration:

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 cablelength short 133
 pri-group timeslots 1-24
!
```

The following lines show the ISDN configuration:

```
interface Serial0:23
 no ip address
 no logging event link-status
 isdn switch-type primary-ni
 isdn incoming-voice modem
 no cdp enable
!
```

The following lines show the dial-peer configuration. Because the dial-peer voice 1 is not configured for direct inward dialing (DID), the inbound call leg is considered to be configured for two-stage dialing, and the router returns a second dial tone.

```
dial-peer voice 1 pots
 incoming called-number .
 port 0:D
!
dial-peer voice 2 voip
 destination-pattern 83101
 session target ipv4:172.69.85.107
 dtmf-relay h245-alphanumeric
 codec g711ulaw
 ip qos dscp cs5 media
!
!end
```

Step 4 Use the **show controller t1** command to display T1 status. Verify that the T1 is UP and that there are no errors.

```
Router> show controller t1 0
```

```
T1 0 is up.
 Applique type is Channelized T1
 Cablelength is short 133
 No alarms detected.
 alarm-trigger is not set
 Version info of slot 0: HW: 1, PLD Rev: 11
 Framer Version: 0x8
!
!
```

```
!
Framing is ESF, Line Code is B8ZS, Clock Source is Line Primary.
Data in current interval (0 seconds elapsed):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

- Step 5** Use the **show isdn status** command to display ISDN status. Verify the ISDN Layer 2 status is **MULTIPLE_FRAME_ESTABLISHED**.

```
Router> show isdn status

Global ISDN Switchtype = primary-ni
ISDN Serial0:23 interface
  dsl 0, interface ISDN Switchtype = primary-ni
  Layer 1 Status:
    ACTIVE
  Layer 2 Status:
    TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
  Layer 3 Status:
    0 Active Layer 3 Call(s)
  Active dsl 0 CCBs = 0
  The Free Channel Mask: 0x807FFFFFFF
  Number of L2 Discards = 0, L2 Session ID = 3
  Total Allocated ISDN CCBs = 0
```

- Step 6** Use the **show isdn service** command to display the status of each ISDN channel. Verify that the channels are **IDLE** and **IN-SERVICE**.

```
Router> show isdn service
PRI Channel Statistics:
ISDN Se0:23, Channel [1-24]
Configured Isdn Interface (dsl) 0
Channel State (0=Idle 1=Proposed 2=Busy 3=Reserved 4=Restart 5=Maint_Pend)
Channel : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
State : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Service State (0=Inservice 1=Maint 2=Outofservice)
Channel : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
State : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2
```

- Step 7** Use the **show dial-peer voice summary** command to display voice dial peer information. Verify that Admin and Operation status are up and up.

```
Router> show dial-peer voice summary

          AD                PRE PASS
TAG   TYPE  MIN  OPER  PREFIX    DEST-PATTERN    FER THRU SESS-TARGET  PORT
1     pots  up   up                    0                                0:D
2     voip  up   up      83101     0  syst ipv4:172.69.85.107
```

- Step 8** Use the **debug isdn q931** command to display information about call setup and teardown of ISDN network connections. Use the **debug vtsp dsp**, **debug vtsp session**, and **debug voip ccapi inout** commands to get digit collection information, as shown in the following partial output.

```
Router# debug isdn q931
Router# debug vtsp dsp
Router# debug vtsp session
Router# debug voip ccapi inout

Aug 18 23:56:20.125: ISDN Se0:23 Q931: RX <- SETUP pd = 8 callref = 0x0226
  Bearer Capability i = 0x8090A2
    Standard = CCITT
    Transer Capability = Speech
    Transfer Mode = Circuit
    Transfer Rate = 64 kbit/s
```

```

Channel ID i = 0xA98381
    Exclusive, Channel 1
Calling Party Number i = 0x2181, '40855501124'
    Plan:ISDN, Type:National
Called Party Number i = 0x80, '83101'
    Plan:Unknown, Type:Unknown
Aug 18 23:56:20.133: VDEV_ALLOCATE: 1/1 is allocated
!
!
!

```

The following lines show the digit collection process, starting with the digit 8:

```

Aug 18 23:56:28.265: //6/65F920768011/VTSP:(0:D):0:112:4386/vtsp_dsm_digit_begin_cb: Digit
begin: 8
Aug 18 23:56:28.265: //6/xxxxxxxxxxx/CCAPI/cc_api_call_digit_begin: (dstVdbPtr=0x0,
dstCallId=0xFFFFFFFF, srcCallId=0x6,
!
!
!

```

The router collects the next digit, 3, followed by 1, 0 and 2:

```

Aug 18 23:56:30.253: //6/65F920768011/VTSP:(0:D):0:112:4386/vtsp_dsm_digit_begin_cb: Digit
begin: 3
Aug 18 23:56:30.253: //6/xxxxxxxxxxx/CCAPI/cc_api_call_digit_begin: (dstVdbPtr=0x0,
dstCallId=0xFFFFFFFF, srcCallId=0x6,
    digit=3, digit_begin_flags=0x1, rtp_timestamp=0xFFFFFE70
    rtp_expiration=0x0, dest_mask=0x1)
!
!
!
Aug 18 23:56:30.885: //6/65F920768011/VTSP:(0:D):0:112:4386/vtsp_dsm_digit_begin_cb: Digit
begin: 1
Aug 18 23:56:30.885: //6/xxxxxxxxxxx/CCAPI/cc_api_call_digit_begin: (dstVdbPtr=0x0,
dstCallId=0xFFFFFFFF, srcCallId=0x6,
    digit=1, digit_begin_flags=0x1, rtp_timestamp=0xFFFFFE70
    rtp_expiration=0x0, dest_mask=0x1)
!
!
!
Aug 18 23:56:31.913: //6/65F920768011/VTSP:(0:D):0:112:4386/vtsp_dsm_digit_begin_cb: Digit
begin: 0
Aug 18 23:56:31.913: //6/xxxxxxxxxxx/CCAPI/cc_api_call_digit_begin: (dstVdbPtr=0x0,
dstCallId=0xFFFFFFFF, srcCallId=0x6,
    digit=0, digit_begin_flags=0x1, rtp_timestamp=0xFFFFFE70
    rtp_expiration=0x0, dest_mask=0x1)
!
!
!
Aug 18 23:56:33.185: //6/65F920768011/VTSP:(0:D):0:112:4386/vtsp_dsm_digit_begin_cb: Digit
begin: 2
Aug 18 23:56:33.185: //6/xxxxxxxxxxx/CCAPI/cc_api_call_digit_begin: (dstVdbPtr=0x0,
dstCallId=0xFFFFFFFF, srcCallId=0x6,
    digit=2, digit_begin_flags=0x1, rtp_timestamp=0xFFFFFE70
    rtp_expiration=0x0, dest_mask=0x1)
!
!
!
Aug 18 23:56:33.265: //6/65F920768011/VTSP:(0:D):0:112:4386/vtsp_report_digit_control:
digit reporting disabled
Aug 18 23:56:33.265:
//6/65F920768011/DSM:(0:D):0:112:4386/dsp_stream_mgr_register_disposition: Ev:
E_DSM_DSP_DTMF_DIGIT_BEGIN Disp: DS

```

```

M_DISP_IGNORE
Aug 18 23:56:33.265:
//6/65F920768011/DSM:(0:D):0:112:4386/dsp_stream_mgr_register_disposition: Ev:
E_DSM_DSP_DTMF_DIGIT Disp: DSM_DISP_IGNORE
Aug 18 23:56:33.269: //6/xxxxxxxxxxxxx/CCAPI/cc_api_call_report_digits_done:
(vdbPtr=0x639DB450, callID=0x6, disp=0)
Aug 18 23:56:33.269: //6/65F920768011/VTSP:(0:D):0:112:4386/vtsp_get_digit_timeouts: Inter
digit = 10, Initial digit = 10

```

Because the router does not have an outgoing dial peer with destination pattern 83102, the call fails and an IEC is generated.

```

Aug 18 23:56:33.269: %VOICE_IEC-3-GW: AFSAPP: Internal Error (Digit collect failed):
IEC=1.1.179.10.24.6 on callID 6 GUID=65F92076D10E11D7801100B0640E6622

```

Step 9 Use the **show voice iec description** command to display the IEC definition:

```

Router> show voice iec description 1.1.179.10.24.6

IEC Version: 1
Entity:
Category: 179 (External communication Error)
Subsystem: 10 (AFSAPP)
Error: 24 (Digit collect failed)
Diagnostic Code: 6

```

IEC field definitions pinpoint the problem. Category code 179 indicates an external communication error, and an error code 24 indicates digit collection failure. For more information on IEC field definitions, see the [“Internal Error Code Notation” section on page 7](#).

Troubleshooting Socket Failures

The following example, which describes a TCP session failure, shows how errors detected by the gateway can be used to troubleshoot other devices on the VoIP network.

Symptom

An inbound call from an IP phone to the H.323 gateway fails.

Problem Description

A call is initially routed to the gateway and fails when a TCP session to Cisco CallManager session target cannot be established. The router pings Cisco CallManager, sending a TCP synchronization packet and receiving an ICMP destination unreachable error. Cisco CallManager cannot be pinged because the Cisco CallManager IP address is incorrect. After the IP address for Cisco CallManager is corrected, a second call fails, due to a different socket error. The router tries to establish another TCP session and sends an H225 setup message but Cisco CallManager drops the connection.

Troubleshooting Tasks

Perform the following steps to determine the reasons for both call failures.

Step 1 Use the **voice iec syslog** command to enable display of IECs as they are encountered in real-time.

- Step 2** Use the **voice iec statistics type iec** command to configure the collection of IEC statistics.
- Step 3** Use the **show running-config** command to verify IEC, ISDN, and dial-peer configuration, as shown in the following partial sample output:

```
Router> show running-config
Building configuration...

Current configuration : 3466 bytes
!
```

The following lines show the IEC configuration:

```
voice service voip
!
voice iec syslog
no voice hpi capture buffer
no voice hpi capture destination
voice statistics type iec
!
!
```

The following lines show the T1 configuration:

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 cablelength short 133
 pri-group timeslots 1-24
!
```

The following lines show the ISDN configuration:

```
interface Serial0:23
 no ip address
 no logging event link-status
 isdn switch-type primary-ni
 isdn incoming-voice modem
 no cdp enable
!
!
voice-port 0:D
!
```

The following lines show the dial-peer configuration, including the destination gateway IP address of Cisco CallManager:

```
dial-peer voice 1 pots
 incoming called-number
 direct-inward-dialed
 port 0:D
!
dial-peer voice 2 voip
 destination-pattern 83101
 session target ipv4:10.1.1.1
 dtmf-relay h245-alphanumeric
 codec g711ulaw
 ip qos dscp cs5 media
!
!
end
```

- Step 4** Use the **debug isdn q931** command to display information about call setup and teardown of ISDN network connections.

```

Router# debug isdn q931
Aug 19 01:46:02.886: ISDN Se0:23 Q931: RX <- SETUP pd = 8  callref = 0x022D
  Bearer Capability i = 0x8090A2
    Standard = CCITT
    Transer Capability = Speech
    Transfer Mode = Circuit
    Transfer Rate = 64 kbit/s
  Channel ID i = 0xA98381
    Exclusive, Channel 1
  Calling Party Number i = 0x2181, '4085550111'
    Plan:ISDN, Type:National
  Called Party Number i = 0x80, '83101'
    Plan:Unknown, Type:Unknown

```

The following lines show the IEC and specify a network problem.

```

Aug 19 01:46:03.342: %VOICE_IEC-3-GW: H323: Internal Error (SETUP send sock fail):
IEC=1.1.186.5.83.0 on callID 14 GUID=B99ACE6ED11D11D7801500B0640E6622
Aug 19 01:46:03.350: ISDN Se0:23 Q931: TX -> CALL_PROC pd = 8  callref = 0x822D
  Channel ID i = 0xA98381
    Exclusive, Channel 1
Aug 19 01:46:03.362: ISDN Se0:23 Q931: TX -> DISCONNECT pd = 8  callref = 0x822D
  Cause i = 0x80A6 - Network out of order
Aug 19 01:46:03.374: ISDN Se0:23 Q931: RX <- RELEASE pd = 8  callref = 0x022D
  Cause i = 0x82E4 - Invalid information element contents
Aug 19 01:46:03.374: ISDN Se0:23 Q931: TX -> RELEASE_COMP pd = 8  callref = 0x822D

```

Step 5 Use the following commands to further isolate the problem:

- The **show voice iec description** command displays the IEC definition.
- The **debug ip tcp transaction** command displays output for packets the router sends and receives.
- The **debug cch323 h225** command provides the trace of the state transition of the H.225 state machine based on the processed events.

The following partial sample outputs from each command help you to isolate the cause of the network out of order message:

In the following example, the IEC definition indicates a category code of 186, a signaling socket failure, and shows that an error occurred during the SETUP PDU operation. The explanation for the error code 83 states that this error can happen if the remote IP address is a reachable address for pinging but is not a valid H.323 endpoint.

```

Router# show voice iec description 1.1.186.5.83.0
  IEC Version: 1
  Entity: 1
  Category: 186
  Subsystem: 5
  Error: 83
  Diagnostic Code: 0

```

Because the IEC specifies a signaling socket failure as the reason for call failure, you should enable the following **debug** commands to get more information.

```

Router# debug ip tcp transaction

TCP special event debugging is on

Router# debug cch323 h225

H225 State Machine tracing is enabled

Router# terminal monitor

```

```

% Console already monitors

Router#
Aug 19 01:46:28.746: ISDN Se0:23 Q931: RX <- SETUP pd = 8  callref = 0x022E
  Bearer Capability i = 0x8090A2
    Standard = CCITT
    Transer Capability = Speech
    Transfer Mode = Circuit
    Transfer Rate = 64 kbit/s
  Channel ID i = 0xA98381
    Exclusive, Channel 1
  Calling Party Number i = 0x2181, '4085551090'
    Plan:ISDN, Type:National
  Called Party Number i = 0x80, '83101'
    Plan:Unknown, Type:Unknown
Aug 19 01:46:29.198: TCB63D2DAC8 created
Aug 19 01:46:29.198: TCB63D2DAC8 setting property TCP_PID (8) 63A2C044
Aug 19 01:46:29.198: TCB63D2DAC8 setting property TCP_NO_DELAY (1) 63A2C048
Aug 19 01:46:29.198: TCB63D2DAC8 setting property TCP_TOS (11) 63A2C070
Aug 19 01:46:29.198: TCB63D2DAC8 setting property TCP_NONBLOCKING_WRITE (10) 63A2C0D0
Aug 19 01:46:29.198: TCB63D2DAC8 setting property TCP_NONBLOCKING_READ (14) 63A2C0D0
Aug 19 01:46:29.198: TCB63D2DAC8 setting property unknown (15) 63A2C0D0
Aug 19 01:46:29.198: TCB63D2DAC8 setting property TCP_NO_DELAY (1) 63A2C08C
Aug 19 01:46:29.198: TCB63D2DAC8 setting property TCP_ALWAYS_PUSH (17) 63A2C08C
Aug 19 01:46:29.198: TCB63D2DAC8 bound to 172.16.13.16.11005
Aug 19 01:46:29.198: TCP: sending SYN, seq 3651477840, ack 0
Aug 19 01:46:29.198: TCP0: Connection to 10.1.1.1:1720, advertising MSS 536
Aug 19 01:46:29.198: TCP0: state was CLOSED -> SYNSENT [11005 -> 10.1.1.1(1720)]

```

The following lines show the 10.1.1.1 CallManager address is unreachable as it is configured, and the network out of order IEC is generated:

```

Aug 19 01:46:29.202: TCP0: ICMP destination unreachable received
!
!
!Aug 19 01:46:29.206: %VOICE_IEC-3-GW: H323: Internal Error (SETUP send sock fail):
IEC=1.1.186.5.83.0 on callID 16 GUID=C904C18BD11D11D7801600B0640E6622
Aug 19 01:46:29.206: TCB 0x63D2DAC8 destroyed
Aug 19 01:46:29.206: //16/C904C18B8016/H323/run_h225_sm: Received event H225_EV_CONN_LOST
while at state H225_IDLE
Aug 19 01:46:29.214: ISDN Se0:23 Q931: TX -> CALL_PROC pd = 8  callref = 0x822E
  Channel ID i = 0xA98381
    Exclusive, Channel 1
Aug 19 01:46:29.218: //16/C904C18B8016/H323/run_h225_sm: Received event H225_EV_RELEASE
while at state H225_IDLE
Aug 19 01:46:29.218: //16/C904C18B8016/H323/cch323_h225_set_new_state: Changing from
H225_IDLE state to H225_IDLE state
Aug 19 01:46:29.226: ISDN Se0:23 Q931: TX -> DISCONNECT pd = 8  callref = 0x822E
  Cause i = 0x80A6 - Network out of order
!
!

```

Step 6 Use the **show ip route** command to display static routes, then use the **ping** command to check network connectivity to the destination address 10.1.1.1 using the **ping** command.

```
Router> show ip route
```

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

```

```
Gateway of last resort is 172.16.13.3 to network 0.0.0.0
```

```
    172.16.0.0/27 is subnetted, 1 subnets
C       172.16.13.0 is directly connected, Ethernet0
S*    0.0.0.0/0 [1/0] via 172.16.13.3
```

The following lines show that the reason for Cisco CallManager TCP session failure is the incorrect 10.1.1.1 IP address:

```
Router# ping 10.1.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
..U.U
Success rate is 0 percent (0/5)
Router# ping 10.1.1.1
```

Step 7 Configure the correct IP address for Cisco CallManager and verify the configuration using the **show running-config** command.

```
Router# config term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# dial-peer voice 2
Router(config-dial-peer)# session target ipv4:172.31.85.107
Router(config-dial-peer)# end
```

```
Router# show running-config
!
!
!
dial-peer voice 2 voip
 destination-pattern 83101
 session target ipv4:172.31.85.107
 dtmf-relay h245-alphanumeric
 codec g711ulaw
 ip qos dscp cs5 media
```

Step 8 Use the **show debug** command to display call traces enabled during a second call attempt.

```
Router# show debug
```

```
CSM Voice:
  Voice Call Switching Module debugging is on
```

The following ISDN debugs are enabled on all DSLs:

```
debug isdn error is          ON.
debug isdn q931 is          ON. (filter is OFF)
```

```
Router#
Aug 19 02:05:36.349: ISDN Se0:23 Q931: RX <- SETUP pd = 8 callref = 0x0237
  Bearer Capability i = 0x8090A2
    Standard = CCITT
    Transer Capability = Speech
    Transfer Mode = Circuit
    Transfer Rate = 64 kbit/s
  Channel ID i = 0xA98381
    Exclusive, Channel 1
  Calling Party Number i = 0x2181, '4085550111'
    Plan:ISDN, Type:National
  Called Party Number i = 0x80, '83101'
    Plan:Unknown, Type:Unknown
```

```

Aug 19 02:05:36.353: VDEV_ALLOCATE: 1/2 is allocated
Aug 19 02:05:36.353: csm_vtsp_init_tdm: vdev@ 0x6355AAF4, voice_vdev@ 0x6355AA80
Aug 19 02:05:36.353: csm_vtsp_init_tdm: dsprm_tdm_allocate: tdm slot 1, dspm 1, dsp 2,
dsp_channel 1
Aug 19 02:05:36.353: csm_vtsp_init_tdm: dsprm_tdm_allocate: tdm stream 4, channel 3, bank
2, bp_channel 1, bp_stream 255
Aug 19 02:05:36.357: VDEV_DEALLOCATE: slot 1, port 4 is deallocated
Aug 19 02:05:36.805: ISDN Se0:23 Q931: TX -> CALL_PROC pd = 8 callref = 0x8237
      Channel ID i = 0xA98381
      Exclusive, Channel 1

```

The second call attempt also fails, generating a different IEC:

```

Aug 19 02:05:36.845: %VOICE_IEC-3-GW: H323: Internal Error (Socket error):
IEC=1.1.186.5.7.6 on callID 8 GUID=750AFC91D12011D7800600B0640E6622
Aug 19 02:05:36.865: ISDN Se0:23 Q931: TX -> DISCONNECT pd = 8 callref = 0x8237
      Cause i = 0x80A6 - Network out of order
Aug 19 02:05:36.873: ISDN Se0:23 Q931: RX <- RELEASE pd = 8 callref = 0x0237
      Cause i = 0x82E4 - Invalid information element contents
Aug 19 02:05:36.877: ISDN Se0:23 Q931: TX -> RELEASE_COMP pd = 8 callref = 0x8237

```

The following lines show that the subsequent call failed due to a different socket error. However, in this instance sending a ping to the remote IP address is successful:

```
Router> show voice iec description 1.1.186.5.7.6
```

```

IEC Version: 1
Entity: 1 (Gateway)
Category: 186 (Signaling socket failure)
Subsystem: 5 (H323)
Error: 7 (Socket error)
Diagnostic Code: 6

```

```
Router> ping 172.69.85.107
```

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.69.85.107, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

```

Use the **debug ip tcp transaction**, **show debug**, and **debug cch323 h225** commands again.

```
Router# debug ip tcp transaction
```

```
TCP special event debugging is on
```

```
Router# show debug
```

```

CSM Voice:
  Voice Call Switching Module debugging is on
TCP:
  TCP special event debugging is on

```

The following ISDN debugs are enabled on all DSLs:

```

debug isdn error is          ON.
debug isdn q931 is          ON. (filter is OFF)

```

```
Router# debug cch323 h225
```

```
H225 State Machine tracing is enabled
```

```

Router#
Aug 19 02:06:36.637: ISDN Se0:23 Q931: RX <- SETUP pd = 8  callref = 0x0238
    Bearer Capability i = 0x8090A2
        Standard = CCITT
        Transer Capability = Speech
        Transfer Mode = Circuit
        Transfer Rate = 64 kbit/s
    Channel ID i = 0xA98381
        Exclusive, Channel 1
    Calling Party Number i = 0x2181, '4085550111'
        Plan:ISDN, Type:National
    Called Party Number i = 0x80, '83101'
        Plan:Unknown, Type:Unknown
Aug 19 02:06:36.641: VDEV_ALLOCATE: 1/3 is allocated
Aug 19 02:06:36.641: csm_vtsp_init_tdm: vdev@ 0x6355B240, voice_vdev@ 0x6355B1CC
Aug 19 02:06:36.641: csm_vtsp_init_tdm: dsprm_tdm_allocate: tdm slot 1, dspm 1, dsp 3,
dsp_channel 1
Aug 19 02:06:36.641: csm_vtsp_init_tdm: dsprm_tdm_allocate: tdm stream 4, channel 5, bank
2, bp_channel 2, bp_stream 255
Aug 19 02:06:36.645: VDEV_DEALLOCATE: slot 1, port 8 is deallocated
Aug 19 02:06:37.089: TCB63604218 created
Aug 19 02:06:37.089: TCB63604218 setting property TCP_PID (8) 632036B4
Aug 19 02:06:37.089: TCB63604218 setting property TCP_NO_DELAY (1) 632036B8
Aug 19 02:06:37.089: TCB63604218 setting property TCP_TOS (11) 632036E0
Aug 19 02:06:37.089: TCB63604218 setting property TCP_NONBLOCKING_WRITE (10) 63203740
Aug 19 02:06:37.089: TCB63604218 setting property TCP_NONBLOCKING_READ (14) 63203740
Aug 19 02:06:37.089: TCB63604218 setting property unknown (15) 63203740
Aug 19 02:06:37.089: TCB63604218 setting property TCP_NO_DELAY (1) 632036FC
Aug 19 02:06:37.089: TCB63604218 setting property TCP_ALWAYS PUSH (17) 632036FC
Aug 19 02:06:37.089: TCB63604218 bound to 172.16.13.16.11001
Aug 19 02:06:37.089: TCP: sending SYN, seq 1593750728, ack 0
Aug 19 02:06:37.093: TCP0: Connection to 172.31.85.107:1720, advertising MSS 536
Aug 19 02:06:37.093: TCP0: state was CLOSED -> SYNSENT [11001 -> 172.31.85.107(1720)]
Aug 19 02:06:37.093: TCP0: state was SYNSENT -> ESTAB [11001 -> 172.31.85.107(1720)]
Aug 19 02:06:37.093: TCP0: Connection to 172.31.85.107:1720, received MSS 1460, MSS is 536
Aug 19 02:06:37.093: //10/98FA43DC8007/H323/run_h225_sm: Received event H225_EV_SETUP
while at state H225_IDLE
Aug 19 02:06:37.093: //10/98FA43DC8007/H323/check_qos_and_send_setup: Setup ccb 0x635F80E8
Aug 19 02:06:37.093: //10/98FA43DC8007/H323/run_h225_sm: Received event H225_EV_FS_SETUP
while at state H225_IDLE
Aug 19 02:06:37.093: //10/98FA43DC8007/H323/idle_fsSetup_hdlr: Setup ccb 0x635F80E8
Aug 19 02:06:37.097: //10/98FA43DC8007/H323/generic_send_setup: sending calling IE
Aug 19 02:06:37.097: //10/98FA43DC8007/H323/generic_send_setup: ===== PI = 0
Aug 19 02:06:37.097: //10/98FA43DC8007/H323/generic_send_setup: Send infoXCap=128,
infoXRate=157, rateMult=89
Aug 19 02:06:37.097: //10/98FA43DC8007/H323/generic_send_setup: src address =
172.16.13.16; dest address = 172.31.85.107
Aug 19 02:06:37.097: //10/98FA43DC8007/H323/cch323_h225_set_new_state: Changing from
H225_IDLE state to H225_REQ_FS_SETUP state
Aug 19 02:06:37.101: TCP0: FIN processed

```

The following lines show that the router was able to initialize the TCP session to Cisco CallManager, and the session went into the established state. After the router sent an H225 SETUP message it received a TCP RESET message to tear down the TCP session, indicating Cisco CallManager dropped the connection.

```

Aug 19 02:06:37.101: TCP0: state was ESTAB -> CLOSEWAIT [11001 -> 172.31.85.107(1720)]
Aug 19 02:06:37.101: TCP0: RST received, Closing connection
Aug 19 02:06:37.101: TCP0: state was CLOSEWAIT -> CLOSED [11001 -> 172.31.85.107(1720)]
Aug 19 02:06:37.105: ISDN Se0:23 Q931: TX -> CALL_PROC pd = 8  callref = 0x8238
    Channel ID i = 0xA98381
        Exclusive, Channel 1

```

```

Aug 19 02:06:37.105: %VOICE_IEC-3-GW: H323: Internal Error (Socket error):
IEC=1.1.186.5.7.6 on callID 10 GUID=98FA43DCD12011D7800700B0640E6622
Aug 19 02:06:37.105: TCB 0x63604218 destroyed
Aug 19 02:06:37.105: //10/98FA43DC8007/H323/run_h225_sm: Received event H225_EV_CONN_LOST
while at state H225_REQ_FS_SETUP
Aug 19 02:06:37.113: //10/98FA43DC8007/H323/run_h225_sm: Received event H225_EV_RELEASE
while at state H225_REQ_FS_SETUP
Aug 19 02:06:37.113: //10/98FA43DC8007/H323/cch323_h225_set_new_state: Changing from
H225_REQ_FS_SETUP state to H225_IDLE state
Aug 19 02:06:37.121: ISDN Se0:23 Q931: TX -> DISCONNECT pd = 8 callref = 0x8238
Cause i = 0x80A6 - Network out of order
Aug 19 02:06:37.133: ISDN Se0:23 Q931: RX <- RELEASE pd = 8 callref = 0x0238
Cause i = 0x82E4 - Invalid information element contents
Aug 19 02:06:37.137: ISDN Se0:23 Q931: TX -> RELEASE_COMP pd = 8 callref = 0x8238

```

Step 9 Verify Cisco CallManager setting for the H.323 gateway to determine if the H.225 session was rejected by Cisco CallManager because the wrong IP address was configured for the H.323 gateway. Configure the correct IP address for the H.323 gateway, 172.16.13.16. For more information on CallManager configuration and IP address configuration, see the *Cisco CallManager Administration Guide, Release 3.3(2)* “Device Configuration” chapter, “Adding Gateways to Cisco CallManager” and “Adding a Cisco IOS H.323 Gateway” sections.

Step 10 Use **debug** commands to verify that the next call completes, as shown in the following partial **debug** output:

```

Aug 19 02:10:36.707: ISDN Se0:23 Q931: RX <- SETUP pd = 8 callref = 0x0239
Bearer Capability i = 0x8090A2
Standard = CCITT
Transer Capability = Speech
Transfer Mode = Circuit
Transfer Rate = 64 kbit/s
Channel ID i = 0xA98381
Exclusive, Channel 1
Calling Party Number i = 0x2181, '4085550111'
Plan:ISDN, Type:National
Called Party Number i = 0x80, '83101'
Plan:Unknown, Type:Unknown
Aug 19 02:10:36.711: VDEV_ALLOCATE: 1/2 is allocated
Aug 19 02:10:36.711: csm_vtsp_init_tdm: vdev@ 0x6355B98C, voice_vdev@ 0x6355B918
Aug 19 02:10:36.711: csm_vtsp_init_tdm: dsprm_tdm_allocate: tdm slot 1, dsprm 1, dsp 4,
dsp_channel 1
Aug 19 02:10:36.711: csm_vtsp_init_tdm: dsprm_tdm_allocate: tdm stream 5, channel 1, bank
2, bp_channel 3, bp_stream 255
Aug 19 02:10:36.711: VDEV_DEALLOCATE: slot 1, port 12 is deallocated
Aug 19 02:10:37.155: TCB63604A4C created
Aug 19 02:10:37.159: TCP: sending SYN, seq 3088300316, ack 0
Aug 19 02:10:37.159: TCP0: Connection to 172.69.85.107:1720, advertising MSS 536
Aug 19 02:10:37.159: TCP0: state was CLOSED -> SYNSENT [11003 -> 172.69.85.107(1720)]
Aug 19 02:10:37.163: TCP0: state was SYNSENT -> ESTAB [11003 -> 172.69.85.107(1720)]
Aug 19 02:10:37.163: TCP0: Connection to 172.69.85.107:1720, received MSS 1460, MSS is 536
Aug 19 02:10:37.163: //12/281160848008/H323/run_h225_sm: Received event H225_EV_SETUP
while at state H225_IDLE
Aug 19 02:10:37.163: //12/281160848008/H323/check_qos_and_send_setup: Setup ccb 0x635F80E8
!
!
!
Aug 19 02:10:37.171: ISDN Se0:23 Q931: TX -> CALL_PROC pd = 8 callref = 0x8239
Channel ID i = 0xA98381
Exclusive, Channel 1
Aug 19 02:10:38.151: //-1/xxxxxxxxxxxx/H323/cch323_h225_receiver: Received msg of type
CALLPROCIND_CHOSEN
Aug 19 02:10:38.155: //12/281160848008/H323/callproc_ind: ===== PI = 0
Aug 19 02:10:38.155: //12/281160848008/H323/callproc_ind: Call Manager detected

```

```

Aug 19 02:10:38.155: //12/281160848008/H323/cch323_h225_receiver: CALLPROCIND_CHOSEN: src
address = 172.16.13.16; dest address = 172.69.85.107
Aug 19 02:10:38.155: //12/281160848008/H323/run_h225_sm: Received event
H225_EV_CALLPROC_IND while at state H225_REQ_FS_SETUP
Aug 19 02:10:41.347: TCP0: state was SYNSENT -> ESTAB [11004 -> 172.69.85.107(1778)]
Aug 19 02:10:41.347: TCP0: Connection to 172.69.85.107:1778, received MSS 1460, MSS is 536
Aug 19 02:10:41.699: //12/281160848008/H323/run_h225_sm: Received event
H225_EV_H245_SUCCESS while at state H225_WAIT_FOR_H245
Aug 19 02:10:41.703: //12/281160848008/H323/cch323_h225_set_new_state: Changing from
H225_WAIT_FOR_H245 state to H225_ACTIVE state
Aug 19 02:10:41.703: //12/281160848008/H323/setup_cfm_notify: status = 4800261B
Aug 19 02:10:41.703: //12/281160848008/H323/generic_setup_cfm_notify: ===== PI = 0;
status = C800261B

```

In the next lines, the call connects and two-way communication is established.

```

Aug 19 02:10:41.711: ISDN Se0:23 Q931: TX -> CONNECT pd = 8 callref = 0x8239
Aug 19 02:10:41.719: ISDN Se0:23 Q931: RX <- CONNECT_ACK pd = 8 callref = 0x0239

```

The following lines show that after a two-minute call, the IP phone user hangs up and the call is disconnected with normal call clearing:

```

Aug 19 02:10:43.635: TCP0: RST received, Closing connection
Aug 19 02:10:43.635: TCP0: state was ESTAB -> CLOSED [11004 -> 172.69.85.107(1778)]
Aug 19 02:10:43.635: TCB 0x6361C070 destroyed
!
!
!
Aug 19 02:10:43.663: TCP0: sending FIN
Aug 19 02:10:43.663: TCP0: state was FINWAIT1 -> FINWAIT2 [11003 -> 172.69.85.107(1720)]
Aug 19 02:10:43.663: TCP0: FIN processed
Aug 19 02:10:43.663: TCP0: state was FINWAIT2 -> TIMEWAIT [11003 -> 172.69.85.107(1720)]
Aug 19 02:10:43.671: ISDN Se0:23 Q931: TX -> DISCONNECT pd = 8 callref = 0x8239
Cause i = 0x8090 - Normal call clearing
Aug 19 02:10:43.679: ISDN Se0:23 Q931: RX <- RELEASE pd = 8 callref = 0x0239
Aug 19 02:10:43.683: ISDN Se0:23 Q931: TX -> RELEASE_COMP pd = 8 callref = 0x8239
Router#
Router# undebug all
All possible debugging has been turned off.

```

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0710R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.

