An H.323 gatekeeper is an H.323 entity on the LAN that provides address translation and controls access to the LAN for H.323 terminals, gateways, and MCUs.

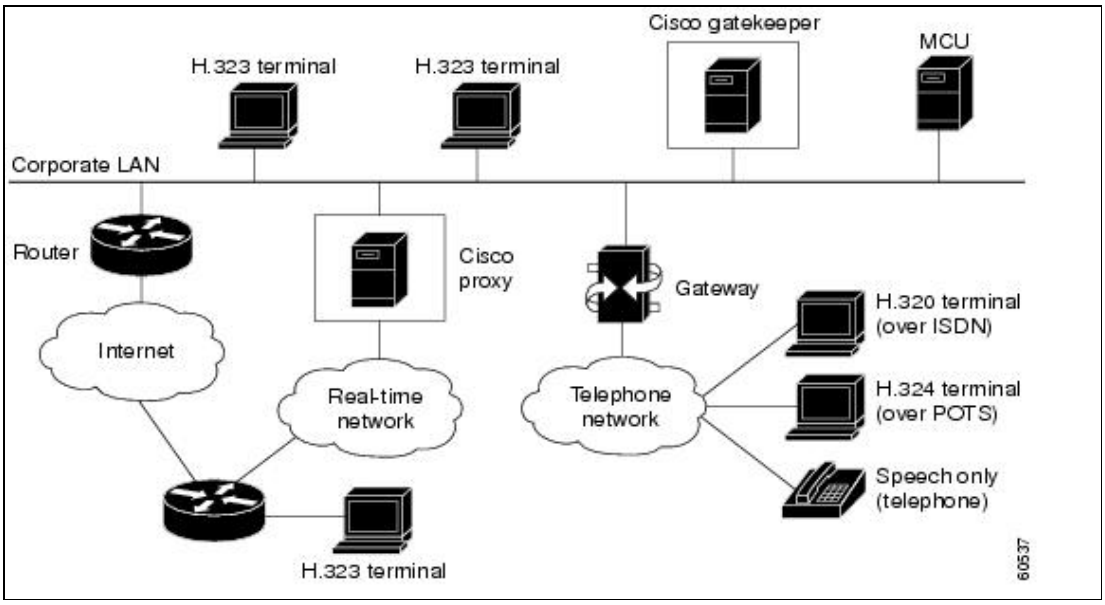
Guide Contents
Troubleshooting Cisco IOS Voice Overview
Debug Command Output on Cisco IOS Voice Gateways
Filtering Troubleshooting Output
Cisco VoIP Internal Error Codes
Troubleshooting Cisco IOS Voice Telephony
Troubleshooting Cisco IOS Voice Protocols
Troubleshooting Cisco IOS Telephony Applications
Monitoring the Cisco IOS Voice Network
Cause Codes and Debug Values

Contents

H.323 Gatekeeper Overview

Gatekeepers are optional nodes that manage endpoints in an H.323 network. The endpoints communicate with the gatekeeper using the RAS protocol. The following figure shows a typical H.323 network. For detailed information on H.323, refer to theCisco IOS H.323 Configuration Guide.

Figure: Gatekeeper in an H.323 Network



Endpoints attempt to register with a gatekeeper on startup. When an endpoint wishes to communicate with another endpoint, it requests admission to initiate a call using a symbolic alias for the endpoint, such as an E.164 address or an e-mail address. If the gatekeeper decides that the call can proceed, it returns a destination IP address to the originating endpoint. This IP address might not be the actual address of the destination endpoint; it might be an intermediate address, such as the address of a proxy or a gatekeeper that routes call signaling.

Note: Although the gatekeeper is an optional H.323 component, it must be included in the network if proxies are used.

For more information about H.323 gatekeepers, refer to Understanding H.323 Gatekeepers, document 5244.

Troubleshooting H.323 Gatekeeper Registration

Some of the common issues that are known to result in endpoints not registering with Cisco gatekeepers are described in the following section. This section also explains how to check if the endpoints or gateways are registered with the gatekeeper and suggests some debug commands for troubleshooting the issue. It is assumed here that the reader understands the basic concept of Registration, Admission, and Status (RAS) signaling and the functionality of the Cisco gatekeeper.

When you use a Cisco gatekeeper to route a call between Cisco gateways, the gateways do not register with the gatekeeper.

Related Commands

This section describes some show and debug commands to assist you while troubleshooting the issue.

show gatekeeper endpoint

Use the **show gatekeeper endpoints** command to verify the endpoints registration status to the gatekeeper.

The following example shows normal output of this command if an endpoint is registered.

```
 gatekeeper# show gatekeeper endpoint
 GATEKEEPER ENDPOINT REGISTRATION
 ================================
 CallSignalAddr Port RASSignalAddr Port Zone Name Type Flags
-------------- ----- -------------- ---- --------- ---- -----
172.16.13.35   1720  172.16.13.35 50890    gk     VOIP-GW
   E164-ID: 2073418
   E164-ID: 5251212
   H323-ID: Router
Total number of active registrations = 1
```

The following example shows normal output of this command if an endpoint is not registered.

```
 gatekeeper# show gatekeeper endpoint
 GATEKEEPER ENDPOINT REGISTRATION
 ================================
 CallSignalAddr Port RASSignalAddr Port Zone Name Type Flags
-------------- ----- -------------- ---- --------- ---- -----
Total number of active registrations = 0
```

show gateway

Use this gateway command to verify the registration status of the gateway to a gatekeeper.

The following example shows the common output of this command if the gateway is registered to a gatekeeper.

```
 Router# show gateway Gateway Router/ww is registered to Gatekeeper gk
 Alias list (CLI configured)
   E164-ID 2073418
   E164-ID 5251212
   H323-ID Router Alias list (last RCF)
   E164-ID 2073418
   E164-ID 5251212
   H323-ID Router
 H323 resource thresholding is Disabled
```

The following example shows the common output of this command if the gateway is not registered to a gatekeeper.

```
 Router#show gateway
 Gateway Router is not registered to any gatekeeper
 Alias list (CLI configured)
   E164-ID 2073418
   E164-ID 5251212
   H323-ID Router/ww Alias list (last RCF)
 H323 resource thresholding is Disabled
```

debug h225 asn1, debug ras

These are gatekeeper and gateway debug commands. In this document, we are looking only for the registration reject (RRJ) field and searching for the rejection reason. The following examples show the RRJ field output.

Output from Gateway

```
*Mar 8 06:03:53.629: RAS INCOMING PDU ::=
value RasMessage ::= registrationReject :
{ requestSeqNum 2829 protocolIdentifier { 0 0 8 2250 0 3 }
rejectReason securityDenial : NULL gatekeeperIdentifier {"gk"} }
```

Output from Gatekeeper

```
*Mar 1 06:49:32.699: RAS OUTGOING PDU ::=
value RasMessage ::= registrationReject :
{ requestSeqNum 3055 protocolIdentifier { 0 0 8 2250 0 3 }
rejectReason securityDenial : NULL gatekeeperIdentifier {"gk"} }
```

Reject Reasons

When a gatekeeper is not performing registration correctly, reject reasons (RRJs) can appear in debug commands. This section describes some common reject reasons.

Before running the debugs, verify that the gatekeeper is enabled:

```
gatekeeper zone local gk cisco.com no shutdown
```

The gateway is not registered if there are no **debug ras** and **debug h225 ans1** outputs from the gateway.

The **show gatekeeper endpoint** and **show gateway** commands indicate that no gateway is registered. Check the gateway for the following:

- The **gateway** command is enabled:

```
Router(config)# gateway
```

- At least one **dial-peer voice voip** is configured.

RRJ: rejectReason duplicateAlias

The following output from the **debug h225 asn1** command shows a registration reject reason of duplicateAlias.

```
RAS INCOMING PDU ::=

value RasMessage ::= registrationReject :
{
requestSeqNum 24
protocolIdentifier { 0 0 8 2250 0 3 }
rejectReason duplicateAlias:
{
} gatekeeperIdentifier {"gk"}
}
```

This is usually the result of the gateway registering a duplicate of an E164-ID or H323-ID-another gateway has already been registered to the gatekeeper. If it is a duplicated E164-ID, change the destination pattern configured under a POTS dial-peer associated with an FXS port. If it is a duplicated H323-ID, change the gateway's H.323 ID under the H.323 VoIP interface.

RRJ: rejectReason terminalExcluded

```
*Mar 1 09:48:09.553: RAS OUTGOING PDU ::=

value RasMessage ::= gatekeeperReject : { requestSeqNum 3421
protocolIdentifier { 0 0 8 2250 0 3 }
rejectReason terminalExcluded : NULL
}
```

This is the result of the gateway subnet being disabled in the gatekeeper. Check the gatekeeper configuration. The following configuration likely appears. If so, removing the **no zone subnet gk** command resolves the issue. To remove the command completely, remove the **zone local gk** command.

```
gatekeeper
 zone local gk cisco.com
 no zone subnet gk 172.16.13.0/27
 enable zone prefix gk 5*
 gw-type-prefix 510#* default-technology
 no shutdown
```

RRJ: rejectReason securityDenial

```
*Mar 1 09:54:32.372: RAS OUTGOING PDU ::=
value RasMessage ::= registrationReject :
{ requestSeqNum 3010
 protocolIdentifier { 0 0 8 2250 0 3 }
rejectReason securityDenial : NULL
gatekeeperIdentifier {"gk"}
}
```

This RRJ is the result of the security commands being enabled in the gatekeeper, and the inability of the gateway to match the H.323-ID, E.164-ID, passwords, or security token that the gatekeeper requires. To resolve the issue, check the securiy configuration in the gatekeeper. For further information on security, refer to *Understanding H.323 Gatekeepers*, document 5244.

If the **security h323-id** command is enabled, make sure the gatekeeper has been configured as follows:

```
username Router password 0 ww
gatekeeper
 zone local gk cisco.com
 no zone subnet gk 172.16.13.0/27 enable
 zone prefix gk 5*
 security h323-id
 security password separator /
 gw-type-prefix 510#* default-technology
 no shutdown
```

Also, make sure the gateway has been configured as follows:

```
interface Ethernet0/0
 ip address 172.16.13.35 255.255.255.224
 half-duplex
 h323-gateway voip interface
 h323-gateway voip id gk ipaddr 172.16.13.14 1718
```

```
h323-gateway voip h323-id Router/ww
```

Note: Make sure the gateway does not have the **gateway security password 010411 level endpoint** command configured.

If **security E164** is enabled, make sure the gatekeeper has been configured as follows:

```
username 5551212 ß- E164 address the gateway tries to registered to gatekeeper
gatekeeper
zone local gk cisco.com
no zone subnet gk 172.16.13.0/27 enable
zone prefix gk 5*
security E164
gw-type-prefix 510#* default-technology
no shutdown
```

If **security token** is enabled, make sure the gatekeeper has been configured as follows:

```
gatekeeper
 zone local gk cisco.com
 no zone subnet gk 172.16.13.0/27 enable
 zone prefix gk 5* security token required-for registration
 gw-type-prefix 510#* default-technology
 no shutdown
```

Also, make sure the gateway has the following configuration:

```
gateway
security password 010411 level endpoint
```

Note: Make sure the gatekeeper has been configured properly with the AAA and RADIUS, and that both the gatekeeper and gateway are pointing to the same NTP server.

RRJ: rejectReason invalidAlias

```
*Mar 1 22:03:28.929: RAS OUTGOING PDU ::=
value RasMessage ::= registrationReject :
{
requestSeqNum 2994
protocolIdentifier { 0 0 8 2250 0 3 }
rejectReason invalidAlias : NULL
gatekeeperIdentifier {"gk-A"} }
```

The RRJ is the result of a no-zone prefix defined in the gatekeeper. Check the configuration on the gatekeeper and add the zone prefix with the proper E.164 address. You should check the following Cisco IOS defects in CSCdu78917.

Configure the gatekeeper as follows:

```
!
gatekeeper
zone local gk-A cisco.com
zone prefix gk-A 2000*
zone prefix gk-A 3000*
zone prefix gk-A 4000*
no shutdown
!
```

For more information, refer to Troubleshooting Gatekeeper Registration Issues, document 22378.

Troubleshooting H.323 Gatekeeper Call Routing and Dial Peers

Cisco gatekeepers are used to group gateways into logical zones and perform call routing between them. Gateways are responsible for edge routing decisions between the PSTN and the H.323 network. Cisco gatekeepers handle the core call routing among devices in the H.323 network and provide centralized dial plan admistration. Without a Cisco gatekeeper, explicit IP addresses for each terminating gateway would have to be configured at the originating gateway and matched to a VoIP dial peer. With a Cisco gatekeeper, gateways query the gatekeeper when trying to establish VoIP calls with remote VoIP gateways.

For example, when presented with a call, the gateway determines whether to send it to the telephony leg or to the IP leg according to its dial plan. In the case of the IP leg, the gateway queries the Cisco gatekeeper to select the best endpoint. The Cisco gatekeeper determines if the called endpoint is within its local zone or is located at a remote zone controlled by a remote Cisco gatekeeper.

The following is a list of useful **show** and **debug** commands used to verify and troubleshoot gatekeeper and gateway call routing issues.

Certain show commands are supported by the Output Interpreter (registered customers only) tool, which allows you to view an analysis of show command output.

- **show gateway**-Used to verify E.164 and H.323 alias registration for the gateway
- **show gatekeeper endpoints**-Used to verify the E.164 and H.323 alias registered with the gatekeeper
- **show gatekeeper gw-type-prefix**-Used to verify E.164 prefix registrations on the gatekeeper
- **show gatekeeper zone prefix |** status-Used to verify zone status and configuration parameters
- **debug ras**-Applicable for gateways and gatekeepers
- **debug debug h225 asn1**-Applicable for gateways and gatekeepers
- **show dial-peer voice**-Used to verify configured technology prefixes under the dial-peers

For detailed information about troubleshooting gateway dial peer issues, refer to Understanding Cisco IOS Gatekeeper Call Routing, document 24462.

Troubleshooting H.323 Gatekeeper Bandwidth

According to the H.323 recommendation, Cisco IOS gatekeepers should support the following H.225 RAS bandwidth management messages:

- Bandwidth Request (BRQ)
- Bandwidth Rejection (BRJ)
- Bandwidth Confirmation (BCF)

Note: Cisco has implemented only the function of reporting any bandwidth changes when codecs change. See the How BRQ Is Triggered from the Gateway to Notify the Gatekeeper to Reduce Call Bandwidth for more information.

The need to support these messages is based on bandwidth management. The gatekeepers can also use a null function that accepts all requests for bandwidth changes. In other words, the gatekeeper can either use these messages to manage bandwidth (by allowing or rejecting requests) or just ignore them.

Bandwidth Management Operation Overview

The Cisco gatekeeper might reject calls from a terminal due to bandwidth limitations. This can occur if the gatekeeper determines that there is not sufficient bandwidth available on the network to support the call. Bandwidth determination also operates during an active call when a terminal requests additional bandwidth

or reports a change in bandwidth used for the call.

The Cisco gatekeeper maintains a record of all active calls so that it can manage the bandwidth resources in its zone. In a cluster configuration, the Gatekeeper Update Protocol (GUP) announcement indication message is exchanged at set intervals and carries information about the bandwidth utilization for the zone. This GUP message exchange allows the alternate gatekeepers to properly manage the bandwidth for a single zone, even though the gatekeepers are in separate physical devices.

When deciding whether there is enough bandwidth to accept a call Admission Request (ARQ), the Cisco gatekeeper calculates the available bandwidth with the following formula:

> Available bandwidth = (total allocated bandwidth) - (bandwidth used locally) - (bandwidth used by all alternates).

If the available bandwidth is sufficient for the call, an Admission Confirmation (ACF) is returned, otherwise an Admission Rejection (ARJ) is returned.

Voice gateways should consider codec, Layer 2 encapsulation, and compression features (such as cRTP) when requesting bandwidth from the Cisco gatekeeper. Sometimes these features are not defined at the time of call setup, in which case a bandwidth change request can be issued to the gatekeeper after call setup to adjust the amount of bandwidth used by the call.

Configuring the Bandwidth Management Feature on the Cisco Gatekeeper

The following types of zone bandwidth limitations can be configured on the Cisco gatekeeper:

- The maximum bandwidth for all H.323 traffic between the local zone and a specified remote zone. (If desired, this configuration can be repeated individually for each remote zone.)
- The maximum bandwidth allowed for a single session in the local zone (typically used for video applications, not for voice).
- The maximum bandwidth for all H.323 traffic allowed collectively to all remote zones.

To configure Cisco gatekeeper zone bandwidth, use the following commands:

- **bandwidth** {**interzone** | **total** | **session**} {**default** | **zone** *zone-name*} *max-bandwidth*
- **bandwidth remote** *max-bandwidth*

These configured values are used for processing ARQs and BRQs.

For an ARQ, the Cisco gatekeeper deducts the bandwidth specified in the message from the appropriate zone counters and/or remote counters. If this causes any counter to go negative, then the call is denied and an ARJ response is sent with the reason ARJ_REQ_DENIED. If the request is for a zone that has a maximum session bandwidth specified, then the request is validated against this value. If the call request exceeds this bandwidth, then the Cisco gatekeeper returns an ACF with the bandwidth set to the maximum session bandwidth. It is up the endpoint to continue or reject the call.

For a BRQ requesting a bandwidth increase, the Cisco gatekeeper validates the request against the zone and/or remote. If the validation fails, then a BRJ response is sent with a reason of BRJ_INSUFFICIENT_RSC and a specification of the maximum amount of bandwidth allowed.

Using Gatekeeper show Commands to Display Bandwidth Information

Enter the **show gatekeeper zone status** command to display the bandwidth information for all zones.

```
Router# show gatekeeper zone status
                        GATEKEEPER ZONES
                        ================
GK name      Domain Name   RAS Address     PORT  FLAGS
-------      -----------   -----------     ----- -----
Router        domainB.com   172.16.13.41    1719  LS
  BANDWIDTH INFORMATION (kbps) :
    Maximum total bandwidth : 512
    Current total bandwidth : 128
    Current total bandwidth (w/ Alt GKs) : 128
    Maximum interzone bandwidth : 512
    Current interzone bandwidth : 128
    Current interzone bandwidth (w/ Alt GKs) : 128
    Maximum session bandwidth : 512
  SUBNET ATTRIBUTES :
    All Other Subnets : (Enabled)
  PROXY USAGE CONFIGURATION :
    Inbound Calls from all other zones :
      to terminals in local zone Router : use proxy
      to gateways in local zone Router  : do not use proxy
      to MCUs in local zone Router  : do not use proxy
    Outbound Calls to all other zones :
      from terminals in local zone Router : use proxy
      from gateways in local zone Router  : do not use proxy
      from MCUs in local zone Router  : do not use proxy
gka-1        domainA.com   172.16.13.35    1719  RS
```

Enter the **show gatekeeper zone cluster** command to display the bandwidth information, in case the gatekeeper is part of a cluster.

```
Router# show gatekeeper zone cluster
                   LOCAL CLUSTER INFORMATION
                   =========================
                                TOT BW   INT BW   REM BW   LAST      ALT GK

LOCAL GK NAME ALT GK NAME   PRI (kbps)   (kbps)   (kbps)   ANNOUNCE  STATUS
------------- -----------   --- ------   ------   ------   --------  ------
Router         gkb-2         0   0        0        0        22s       CONNECTED
```

Enter the **show gatekeeper calls** command to display the active calls permitted by that gatekeeper and how much bandwidth each call is using.

```
Router# show gatekeeper calls
Total number of active calls = 1.
                        GATEKEEPER CALL INFO
                        ====================
LocalCallID                          Age(secs)   BW
3-63466                              9           128(Kbps)
 Endpt(s): Alias                   E.164Addr
   src EP: gwa-1                   4085272923
 Endpt(s): Alias                   E.164Addr
   dst EP: gwb-1                   3653
           CallSignalAddr  Port  RASSignalAddr   Port
           172.16.13.23    1720  172.16.13.23    54670
```

Bandwidth-Related RAS Messages (BRQ, BCF, and BRJ)

The BRQ message is used to request a change in bandwidth from the Cisco gatekeeper. The procedure is as follows:

1. The Cisco gatekeeper verifies the request by the endpointIdentifier to locate the endpoint in the registration database.
2. The Cisco gatekeeper locates the call record by using the callReferenceValue to find a call associated with the endpoint with the same callReferenceValue.
3. If the gatekeeper locates the call record, it then computes the change in bandwidth, then adds or subtracts from the global zone bandwidth, as necessary. It does the same for any proxy or gateway resources in use.
4. The Cisco gatekeeper sends a BCF or BRJ back to the endpoint, depending on success or failure.

RAS Messages Used to Report Bandwidth Status

The Information Request Response (IRR) Non-Standard Data field also carries information about the currently used bandwidth on a gateway or proxy.

How BRQ Is Triggered from the Gateway to Notify the Gatekeeper to Reduce Call Bandwidth

With unidirectional bandwidth, calls were always reported to require a bandwidth of 64 kbps, which is the unidirectional bandwidth for a Cisco G.711 codec. If the endpoints in the call chose to use a more efficient codec, this was not reported to the Cisco gatekeeper. In the version of the Cisco H.323 gateway in Cisco IOS Release 12.2(2)XA or later (which conforms with H.323 version 3), the reported bandwidth is bidirectional. Initially, 128 kbps is reserved. If the endpoints in the call select a more efficient codec, the Cisco gatekeeper is notified of the bandwidth change.

To use the reported bandwidth behavior used prior to Cisco IOS Release 12.2(2)XA for zone bandwidth management, configure the Cisco H.323 gateway with the following command in global configuration mode:

```
Router(config-gateway)# emulate cisco h323 bandwidth
}
```

For more information about gatekeeper bandwidth management, refer to Troubleshooting and Understanding Cisco Gatekeeper Bandwidth Management, document 18731.

Checking Cisco Gateway Failover to Alternate Gatekeeper

Prior to Cisco H.323 version 2, each zone was only controlled by only a single gatekeeper. Cisco H.323 version 2 introduces the alternate gatekeeper to provide gatekeeper redundancy. Implementing the alternate gatekeeper feature allows multiple gatekeepers to control one zone. When an endpoint registers with a gatekeeper, it is provided with a list of alternate gatekeepers for the zone in which the endpoint registers, and for which alternates were specified using the CLI. If the gatekeeper fails, the endpoint may use the alternate gatekeepers in order to continue operation.

The alternate gatekeeper list is provided to the Cisco gatekeeper through the CLI for each zone and is transmitted to endpoints through the RCF (including lightweight) and GRQ messages. This list might also be transmitted in other messages, such as ARJ or URQ, to facilitate a controlled gatekeeper shutdown.

Alternate gatekeepers learn about existing calls through an Interrupt Request (IRQ) and Information Request Response (IRR) exchange between the gateways and the gatekeepers, and they keep track of these calls.

An endpoint that detects the failure of its gatekeeper can safely recover from that failure by utilizing an alternate gatekeeper for future requests, including requests for existing calls. Alternate gatekeepers have to be configured in a cluster. They share the information about the endpoints and active calls using the GUP that runs on TCP.

By default, Cisco gateways send a lightweight RRQ every 45 seconds. In case the gatekeeper did not send any URQ to the gateway (due to a broken routing issue, for example), the gateway (upon not hearing an RCF or RRJ for its lightweight RRQ) tries twice with 5 seconds between attempts. If the third attempt fails, the gateway immediately considers the gatekeeper dead and registers with the alternate gatekeeper using RRQ. In a scenario where the gateway starts the initial registration process with the gatekeeper, it sends out the GRQ to locate the gatekeeper IP address. If there is a GCF reply, the gateway sends the RRQ to the primary gatekeeper specified. If for any reason the gatekeeper rejects the registration request, the gateway does not try to contact its alternate gatekeeper. It starts this process (GRQ, GCF, and RRQ) over again with the primary gatekeeper.

The gateway contacts the alternate gatekeeper only when the connectivity to the primary gatekeeper is lost and there is no reply. If the primary gatekeeper does not reply to the GRQ message when the gateway first sends it out to discover the gatekeeper, then after three failed attempts (approximately 5 minutes per attempt), the gateway contacts the alternate gatekeeper. In a situation where the primary gatekeeper goes down after the gateway has registered with it, the gateway loses keepalive messages from the primary gatekeeper. After missing three consecutive keepalive messages, the gateway declares the primary gatekeeper down, and it starts the registration process again.

Gatekeeper Update Protocol

Here are some major GUP considerations that should also help with troubleshooting.

- Once a gatekeeper that is configured to be part of a cluster comes on line, it opens a TCP port for listening for incoming connections for the GUP.
- Then it announces its presence by sending a GRQ message on a periodic basis. The default period is 30 seconds and is configurable through the gatekeeper CLI **timer cluster-element announce** command. This GRQ message contains nonstandard data for each alternate gatekeeper. This nonstandard data is an indicator to the alternates that the GRQ is really not a GRQ at all, but rather is just an "announcement" message. Inside the GRQ message, the gatekeeper indicates the port number that it has open for listening for the GUP protocol.
- Upon receiving a GRQ from the new gatekeeper, other gatekeepers in the cluster open TCP channels to that port.
- GUP GRQ messages can be one of the following: announcementIndication, announcementReject, registrationIndication, unregistrationIndication, and resourceIndication.
- The announcement indication also carries information about the bandwidth utilization for the zone. This allows the alternate gatekeepers to properly manage the bandwidth for a single zone, even though the gatekeepers are in separate physical devices.
- To verify whether the alternate gatekeepers are properly communicating or not, use the flowing **show gatekeeper zone cluster** command. This command also reports the bandwidth information for the alternate gatekeepers.
- The gatekeeper acts as if the alternate gatekeeper has failed (and assumes any previously allocated bandwidth is now available), if the gatekeeper does not receive an announcement message within six announcement periods, or if the TCP connection with the gatekeeper is detected as broken. With six announcement periods every 30 seconds, the time is 3 minutes, which equates to what we are assuming to be the average length of a call. It should then be fairly safe to assume that bandwidth has been freed. After the 3 minutes, this gatekeeper declares its alternate as down and sends out an update to notify all of its registered endpoints that there is no alternate gatekeeper.

- When an endpoint registers/unregisters with a gatekeeper in a cluster, that gatekeeper uses the registrationIndication/unregistrationIndication message to update all other gatekeepers in that cluster about this change.
- If an endpoint reported a resource change using resource availability indicator (RAI) to a gatekeeper in a cluster, that gatekeeper reports the change to all alternate gatekeepers in that cluster by using the GUP message resourceIndication.
- The GUP messages are needed for the gatekeeper in a cluster to have sufficient knowledge about every endpoint in the zone (registration, bandwidth, active calls, resources) to be able to resolve all queries locally.
- When an endpoint is switched from one gatekeeper to an alternate, the alternate needs to learn about the calls that are active on the endpoint. When a gatekeeper sends an RCF for a new registration, it also sends an IRQ to get a list of all calls on the endpoint. It is important to ensure that the IRQ does not reach the endpoint before the RCF.
- Gatekeepers in a cluster permit a shutdown, even though there are active calls, as long as there is an alternate gatekeeper defined for all zones for which there are active calls. If any zone has an active call and no alternate gatekeeper defined, the gatekeeper refuses the shutdown.
- Alternate gatekeepers accept any Disconnect Requests (DRQs) for calls they were not aware of and pass appropriate information to the Authentication, Authorization, and Accounting (AAA) and Cisco Gatekeeper Transaction Message Protocol (GKTMP) servers. This happens when that endpoint moved to the alternate gatekeeper while there were active calls. In addition, IRR messages may be sent that contain call information for calls that were not previously known. For those IRRs, call records are constructed and bandwidth is allocated accordingly.
- The gatekeeper creates a unique announcementIndication message for each alternate gatekeeper. If an alternate gatekeeper receives a message that contains a gatekeeper identifier it does not recognize (which might happen if the alternate gatekeeper is an alternate for one zone), but not another, that information is simply ignored. However, the alternate gatekeeper detects errors in the configuration of the alternates by examining those messages and it reports those errors to the user.
- The true power of the GUP is realized in the resolving of addresses for a remote zone. Instead of the remote zone needing to send LRQs (either in sequence or blast) to all the gatekeepers, thus increasing the messaging overhead on wide-area links, it now needs to send this query to just one of the gatekeepers in the cluster. Coupled with the **zone cluster remote** command, it can round-robin between the gatekeepers in the cluster and not attempt to send LRQs to other gatekeeper in the cluster if it receives a reject from any one.
- In case a gateway was moved to an alternate gatekeeper, it always tries to register to that gatekeeper unless you issue a **no gateway** and then a **gateway** command. When the endpoint's primary gatekeeper is back online, the endpoint does not reregister to it unless the endpoint lost communication with the alternate gatekeeper. It continues to use the alternate gatekeeper for its call routing information.

For more information, refer to Troubleshooting GUP, Alternate Endpoint and Load Balancing, document 18730.

Troubleshooting Issues with Alternate Endpoints

A calling endpoint can recover from a call setup failure by sending a setup message to one of the alternate endpoints. The call can fail for many reasons:

- The gateway is down and gatekeeper is not aware of it at the time of sending the ACF or LCF.
- There are no resources on the gateway and that was not reported to the gatekeeper.
- There was an incorrect configuration on the main endpoint.

Note: The originating endpoint tries to contact the alternate gatekeepers only if the call fails before the alert stage (alert or progress). If the calls fails due to user busy or no answer, the originating

endpoint does not try any other alternates.

The gatekeeper learns about the alternate for a certain endpoint either by manual configuration using the gatekeeper **endpoint alt-ep** command or from any received RAS messages. Cisco supports a maximum of 20 alternates for each endpoint, no matter how the gatekeeper learns about them.

Here are some issues you need to consider:

- If the gatekeeper has the correct alternate endpoint as desired.
- If the gatekeeper includes the alternate endpoints in its LCF or ACF RAS messages.
- If the OGW tries to contact the alternates in case the main destination endpoint fails.

Use the following commands to verify alternate endpoints:

- Verify that the gatekeeper has the correct alternate endpoints. To see if the gatekeeper has the right alternate endpoints, use the **show gatekeeper endpoints alternates** command.
- Verify that the gatekeeper includes alternate endpoints in its LCF or ACF RAS messages. To see if the gatekeeper sends the IP address for alternate endpoints, you can turn on **debug h225 asn1** and look at the ACF message or LCF.
- Verify that the OGW tries to contact alternates in case the main destination endpoint fails. Debugs to turn on here are **debug voip ccapi inout** and **debug h225 asn1**. Check how the OGW reacts upon receiving alternate endpoints in its ACF message.

For more information, refer to Troubleshooting GUP, Alternate Endpoint and Load Balancing, document 18730.

Troubleshooting Gatekeeper Endpoint Call Admission Issues

This section addresses some of the common issues that are known to result in endpoints not being able to make calls involving Cisco gateways or third-party gateways and terminals, and Cisco gatekeepers.

When there is a problem with gatekeeper endpoint call admission, after configuring an H.323 endpoint to register to a Cisco gatekeeper, the endpoints are not able to make calls. When this occurs, check the **show gatekeeper endpoint** command to make sure the endpoints are all registered to the gatekeeper.

Admission Confirmed (Busy Tone Back)

If the Admission Confirmed (ACF) message has been sent by the gatekeeper and arrived at the endpoint side, but the call still received a busy signal, check to see if the terminating IP address in the ACF is an expected valid endpoint IP.

```
value RasMessage ::= admissionConfirm :
     {
       requestSeqNum 18
       bandWidth 5120
       callModel direct : NULL
       destCallSignalAddress ipAddress :
       {
         ip '0AAAC80A'H
!--- The hex for IP, 0A AA C8 0A== 10.170.200.10.
         port 1720
         port 1720
       }
       irrFrequency 240
       willRespondToIRR FALSE
       uuiesRequested
```

```
      {
        setup FALSE
        callProceeding FALSE
        connect FALSE
        alerting FALSE
        information FALSE
        releaseComplete FALSE
        facility FALSE
        progress FALSE
        empty FALSE
      }
    }
```

If the ACF has an IP address of the terminating endpoint, remove the gatekeeper and make a direct endpoint-to-endpoint call to see if a call can be established.

Admission Reject (ARJ) rejectReason calledPartyNotRegistered

The following **debug h225 asn1** command shows calledPartyNotRegistered.

```
*Mar 15 06:49:19.685: RAS OUTGOING PDU ::=
value RasMessage ::= admissionReject :
    {
      requestSeqNum 34
      rejectReason calledPartyNotRegistered : NULL
    }
```

This is a common reason for rejection. It is captured from the local or originating gatekeeper when the gatekeeper has no information on where the called number should be terminated. There are two ways this problem can occur. One reason is that the call terminates at a gateway, and the gateway is not registered with the E.164 address or with a tech-prefix. To resolve this, make sure the gateway is registered with a tech-prefix to the gatekeeper.

The following is a corrected gateway configuration example.

```
interface Ethernet0/0
 ip address 172.16.13.16 255.255.255.224
 half-duplex
 h323-gateway voip interface
 h323-gateway voip id hwei-gk ipaddr 172.16.13.14 1718
 h323-gateway voip h323-id gw2
 h323-gateway voip tech-prefix 2
....
!
voice-port 2/0/0
!
voice-port 2/0/1
!
voice-port 2/1/0
 station-id name BLARG
 caller-id enable
!
voice-port 2/1/1
!
dial-peer cor custom
!
dial-peer voice 456 pots
 destination-pattern 456
 port 2/1/0
!
```

```
dial-peer voice 123 pots
 destination-pattern 2415...
 port 2/1/1
!
gateway
"show gatekeeper gw" from gatekeeper
GATEWAY TYPE PREFIX TABLE
=========================
Prefix: 1*
  Zone hwei-gk master gateway list:
    172.16.13.35:1720 gw1
Prefix: 2*
  Zone hwei-gk master gateway list:
    172.16.13.16:1720 456
```

A second possible explanation for this error message arises if the called party is a terminal in a remote zone. It might be that the terminal does not have a proxy enabled in the same gatekeeper zone where it is registered. By default, a Cisco IOS gatekeeper uses a proxy for inter-zone terminal calls. Issue the **show gatekeeper zone status** command to view the proxy. Either configure a proxy register to the same local zone as the terminal or issue the **no use-proxy hwei-gk default inbound-to terminal** command or the **no use-proxy hwei-gk default outbound-from terminal** command to disable the use of a proxy for terminal calls.

Note: Intrazone calls do not require the match of a zone prefix.

ARJ "rejectReason requestDenied"

```
*Mar  1 10:34:46.093: RAS OUTGOING PDU ::=
 value RasMessage ::= admissionReject :
      {
        requestSeqNum 11084
        rejectReason requestDenied : NULL
      }
```

The rejection shown here comes about because the endpoint-requested bandwidth exceeds the limit configured in the gatekeeper. To resolve this, increase the bandwidth in the gatekeeper using the **bandwidth** command under the gatekeeper mode, or lower the bandwidth request from the endpoint.

The following example shows a call that failed because the bandwidth request exceeded the configured limit:

```
Value RasMessage ::= admissionRequest :
      {
        requestSeqNum 11084
        callType pointToPoint : NULL
        callModel gatekeeperRouted : NULL
        endpointIdentifier {"6284945400000058"}
        destinationInfo
        {
          e164 : "415525",
          e164 : "415525"
        }
        srcInfo
        {
          e164 : "415526",
          h323-ID : {"hwei-term"}
        }
        srcCallSignalAddress ipAddress :
        {
          ip '0AAAC837'H
          port 1720
```

```
        }
        bandwidth 102400
!--- Requested bandwidth was 10240 K.
        callReferenceValue 1022
        conferenceID '37CE425F850A41468B40D72F145C5C14'H
        activeMC FALSE
        answerCall TRUE
        canMapAlias FALSE
        callIdentifier
        {
          guid '4138E0D40EF0D14C9DB84E54F5190BF4'H
        }
        gatekeeperIdentifier {"hwei-gk"}
        willSupplyUUIEs FALSE
      }

 *Mar  1 10:34:46.093: ARQ (seq# 11084) rcvd
 *Mar  1 10:34:46.093: gk_rassrv_arq: arqp=0x62905E20, crv=0x3FE,
 answerCall=1
 *Mar  1 10:34:46.093: RAS OUTGOING PDU ::=

 value RasMessage ::= admissionReject :
      {
        requestSeqNum 11084
        rejectReason requestDenied : NULL
      }
!--- The show gatekeeper zone status command is issued and it shows the
!--- bandwidth limit is much smaller then the requested bandwidth.
 GATEKEEPER ZONES
                          ================
HWEI-GK name      Domain Name   RAS Address     PORT  FLAGS
-------      -----------   -----------     ----- -----
hwei-gk           cisco.com     172.16.13.14    1719  LS
  BANDWIDTH INFORMATION (kbps) :
    Maximum total bandwidth     :
    Current total bandwidth     :    0
    Maximum interzone bandwidth :                                          4000  _-----limit was 400
    Current interzone bandwidth :    0
    Maximum session   bandwidth :
........
hwei-gk1          cisco.com     172.16.13.37    1719  RS
```

For more information about VoIP bandwidth consumption, refer to Voice Over IP - Per Call Bandwidth Consumption, document ID 7934.

If this rejection reason is offer but there is no bandwidth issue, see if the called party is a terminal and if there is a proxy registered to the local zone. Issue the **show gatekeeper zone status** command to do that. Either configure a proxy register to the same local zone as the terminal or issue the **no use-proxy hwei-gk default inbound-to terminal** or **no use-proxy hwei-gk default outbound-from terminal** command to disable the use of a proxy for terminal calls.

Verification Commands

This section describes a few show commands and debugs that can help you verify the configuration required on the gatekeeper and the gateway. Sample show command outputs are included.

Certain show commands are supported by the Output Interpreter tool, which allows you to view an analysis of show command output; a link to this tool can be found in the Cisco IOS Voice Troubleshooting Tools article.

show gatekeeper endpoint Command

The **show gatekeeper endpoint** command is used to verify the endpoint's registration status with the gatekeeper. The normal outputs of this command are shown in the following example.

```
gatekeeper# show gatekeeper endpoint
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type    Flags
--------------- ----- --------------- ----- ---------         ----    -----
172.16.13.35    1720  172.16.13.35    50890 hwei-gk                VOIP-GW
    E164-ID: 2073418
    E164-ID: 5251212
    H323-ID: Router
Total number of active registrations = 1
!--- The endpoint is registered.
Gatekeeper# show gatekeeper endpoint
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type    Flags
--------------- ----- --------------- ----- ---------         ----    -----
Total number of active registrations = 0
!--- The endpoint is not registered.
```

show gatekeeper gw Command

The **show gatekeeper gw** command is used to verify the endpoints registration status for the tech prefix. The common outputs of this command are shown in the following example.

```
Gatekeeper# show gatekeeper gw
GATEWAY TYPE PREFIX TABLE
=========================
Prefix: 1*
  Zone hwei-gk master gateway list:
    172.16.13.35:1720 gw1
```

show gatekeeper zone status Command

The **show gatekeeper zone status** command is used to display the local zone status and the remote zone information, as shown in the following example.

```
2611-3# show gatekeeper zone status
                         GATEKEEPER ZONES
                         ================
HWEI-GK name      Domain Name   RAS Address     PORT  FLAGS
-------      -----------   -----------     ----- -----
hwei-gk           cisco.com     172.16.13.14    1719  LS
  BANDWIDTH INFORMATION (kbps) :
    Maximum total bandwidth     :
    Current total bandwidth     :    0
    Maximum interzone bandwidth :                                          4000
    Current interzone bandwidth :    0
    Maximum session   bandwidth :
  SUBNET ATTRIBUTES :
    All Other Subnets : (Enabled)
  PROXY USAGE CONFIGURATION :
    Inbound Calls from all other zones :
      to terminals in local zone hwei-gk : use proxy
      to gateways in local zone hwei-gk  : do not use proxy
      to MCUs in local zone hwei-gk  : do not use proxy
    Outbound Calls to all other zones :
```

```
      from terminals in local zone hwei-gk : use proxy
      from gateways in local zone hwei-gk  : do not use proxy
      from MCUs in local zone hwei-gk  : do not use proxy
hwei-gk1          cisco.com     172.16.13.37    1719  RS
```

show gateway Command

The **show gateway** command is used to verify the registration status with a gatekeeper. The common outputs of this command are shown in the following example:

```
Router# show gateway
 Gateway  Router/ww  is registered to Gatekeeper hwei-gk
Alias list (CLI configured)
 E164-ID 2073418
 E164-ID 5251212
 H323-ID Router
Alias list (last RCF)
 E164-ID 2073418
 E164-ID 5251212
 H323-ID Router
 H323 resource thresholding is Disabled
!--- The gateway is registered to gatekeeper (hwei-gk).

Router# show gateway
 Gateway  Router  is not registered to any gatekeeper
Alias list (CLI configured)
 E164-ID 2073418
 E164-ID 5251212
 H323-ID Router/WW
Alias list (last RCF)
 H323 resource thresholding is Disabled
!--- The gateway is not registered to the gatekeeper.
```

debug h225 asn1 Command

The **debug h225 asn1** command is the gatekeeper and Cisco gateway **debug** command. In this document, you are looking only for the ARJ field and searching for the rejection reason. The following example is a sample output showing the ARJ field.

Output from gateway:

```
*Mar 26 04:12:38.508: RAS INCOMING PDU ::=
value RasMessage ::= admissionReject :
    {
      requestSeqNum 34
      rejectReason calledPartyNotRegistered : NULL
    }
```

Output from gatekeeper:

```
*Mar 15 06:49:19.685: RAS OUTGOING PDU ::=
value RasMessage ::= admissionReject :
    {
      requestSeqNum 34
      rejectReason calledPartyNotRegistered : NULL
    }
```

Troubleshoot Load Balancing

With the Load Balance feature, you can set the gatekeeper with a certain threshold for the number of calls, memory, CPU, and number of registered endpoints. Once that threshold is reached, the gatekeeper moves registered Cisco H.323 endpoints to an alternate gatekeeper or rejects new calls and registrations. Load balancing is enabled by use of the following gatekeeper CLI command:

```
Router(config-gk)#load-balance {endpoints max-endpoints} {calls max-calls} {cpu max-%cpu}{memory
```

When the threshold is met, the gatekeeper uses the RRJ RAS message to inform the endpoint about the alternate gatekeepers and the reject reason. Upon receiving that message, the endpoint sends a new RRQ to the alternate gatekeeper. Once the endpoint is registered with the alternate gatekeeper, it uses the GUP message to inform all gatekeepers in the cluster about the new registered endpoint.

When troubleshooting, check the configuration on the gatekeeper and make sure that alternate gatekeepers and load balancing are functional. To debug the load balancing feature, use **debug gatekeeper load** and **debug h225 asn1** to see how the gatekeeper reacts when the threshold is met.

For more information, refer to Troubleshooting GUP, Alternate Endpoint and Load Balancing, document 18730.