



# Configuring Cisco Unified Border Element with Gatekeeper

---

**Revised: Month Day, Year**  
**First Published: June 19, 2006**  
**Last Updated: July 11, 2008**

This chapter describes fundamental configuration tasks required for Configuring Cisco Unified Border Element with gatekeeper functionality. A Cisco Unified Border Element, in this guide also called an IP-to-IP gateway (IPIPGW), border element (BE), or session border controller, facilitates connectivity between independent VoIP networks by enabling H.323 VoIP and videoconferencing calls from one IP network to another. This gateway performs most of the same functions of a PSTN-to-IP gateway, but typically joins two IP call legs, rather than a PSTN and an IP call leg.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [Feature Information for Cisco Unified Border Element with Gatekeeper Configuration Guide, page 52](#)

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



### Activation

---

Before you can configure the software features described in this guide, you will need a Product Authorization Key (PAK). Before you start the configuration process, please register your products and activate your PAK at the following URL <http://www.cisco.com/go/license>.

---



---

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

# Contents

- Prerequisites for Configuring Cisco Unified Border Element with Gatekeeper, page 24
- How to Configure Cisco Unified Border Element with Gatekeeper, page 24
- Configuration Examples for Gatekeepers, page 46
- Additional References, page 49
- Feature Information for Cisco Unified Border Element with Gatekeeper Configuration Guide, page 52

## Prerequisites for Configuring Cisco Unified Border Element with Gatekeeper

- Perform the prerequisites listed in the *Cisco Unified Border Element* at:  
<http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-overview.html#wp1158812>
- Perform basic H.323 gatekeeper configuration.

**Note**

For configuration instructions, see the “*Configuring H.323 Gatekeepers and Proxies*” chapter of the [Cisco IOS H.323 Configuration Guide, Release 15.0](#)

## How to Configure Cisco Unified Border Element with Gatekeeper

This section describes how to configure and verify the Cisco UBE features on gatekeepers.

- [Configuring Via-Zones, page 25](#) (required)
- [In-Service Updates to Gatekeeper Zone Prefix Configuration, page 28](#)
- [Configuring Call-Capacity Thresholds, page 28](#)
- [Configuring LRQ Resource Rejection, page 29](#)
- [Configuring the Sequential LRQ Timer, page 30](#)
- [H.323 Standard-Based Hopcount Field in LRQ, page 31](#)
- [Dynamic Control of Gatekeeper Sequential LRQ Processing Through GKTMP, page 31](#)
- [Enhanced ARQ and RRQ Security for Gatekeeper Registrations, page 31](#)
- [Configuring Extended InterZone Clear Token Support, page 34](#)
- [Configuring RAS Retry and Timer, page 37](#)
- [Configuring Real-Time Call Type Reporting Through GKTMP, page 38](#)
- [Configuring Alternate Endpoint Call Attempts in RADIUS Call Accounting Records, page 39](#)
- [Unique Calling Party Information with Alternate Endpoints, page 40](#)

- [Verifying Gatekeeper Configuration and Operation, page 41](#)
- [Troubleshooting Gatekeeper Configuration and Operation, page 45](#)

**Note**

For sample gatekeeper configurations, see the [“Configuration Examples for Gatekeepers” section on page 46](#).

## Configuring Via-Zones

Via-zone gatekeepers differ from legacy gatekeepers in how LRQ and ARQ messages are used for call routing. Using via-zone gatekeepers will maintain normal clusters and functionality. Legacy gatekeepers examine incoming LRQs based on the called number, and more specifically the dialedDigits field in the destinationInfo portion of the LRQ. Via-zone gatekeepers look at the origination point of the LRQ before looking at the called number. If an LRQ comes from a gatekeeper listed in the via-zone gatekeeper’s remote zone configurations, the gatekeeper checks to see that the **zone remote** configuration contains an **invia** or **outvia** keyword. If the configuration contains these keywords, the gatekeeper uses the new via-zone behavior; if not, it uses legacy behavior.

For ARQ messages, the gatekeeper determines if an **outvia** keyword is configured on the destination zone. If the **outvia** keyword is configured, and the zone named with the **outvia** keyword is local to the gatekeeper, the call is directed to a Cisco Multiservice IP-to-IP Gateway in that zone by returning an ACF pointing to the Cisco Multiservice IP-to-IP Gateway. If the zone named with the **outvia** keyword is remote, the gatekeeper sends a location request to the outvia gatekeeper rather than the remote zone gatekeeper. The **invia** keyword is not used in processing the ARQ.

**Note**

- Video calls can take advantage of the benefits offered by via-zone gatekeeper processing. For a more detailed description of how via-zone gatekeepers process calls, see the [“Configuring Via-Zones” section on page 25](#).
- Using the **zone local** command, you can specify **invia** and **outvia** gatekeepers to be used for intrazone video calls. You can also use the **enable-intrazone** keyword to force all intrazone calls to use the via-zone gatekeeper.

This section contains the following information:

- [Configure Remote Zones, page 25](#)
- [Configure Local Zones, page 27](#)

## Configure Remote Zones

To configure remote zones on the gatekeeper, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **gatekeeper**
4. **zone remote** *gatekeeper-name domain-name* [*ras-IP-address*] [**invia** *inbound-gatekeeper* | **outvia** *outbound-gatekeeper* [**enable-intrazone**]]
5. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>gatekeeper</b>  <b>Example:</b> Router(config)# gatekeeper	Enters gatekeeper configuration mode.
Step 4	<b>zone remote</b> <i>gatekeeper-name domain-name</i> [ <i>ras-IP-address</i> ] [ <b>invia</b> <i>inbound-gatekeeper</i>   <b>outvia</b> <i>outbound-gatekeeper</i> [ <b>enable-intrazone</b> ]]  <b>Example:</b> Router(config-gk)# zone remote termGK cisco 10.16.193.158 1719 invia hurricane outvia hurricane	Defines the remote gatekeeper zone. Keywords and arguments are as follows: <ul style="list-style-type: none"> <li>• <i>zone-name</i>—Name (ID) of the remote zone gatekeeper.</li> <li>• <i>domain-name</i>—Name (ID) of the domain that the remote zone is serving.</li> <li>• <i>ip-address</i>—IP address for the remote gatekeeper.</li> <li>• <i>port-number</i>—RAS signaling port number for the remote zone. Range: 1 to 65535. Default: the well-known RAS port number 1719.</li> <li>• <b>invia</b> <i>inbound-gatekeeper</i>—Name of the via-zone gatekeeper to use for calls coming from the remote zone name.</li> <li>• <b>outvia</b> <i>outbound-gatekeeper</i>—Name of the via-zone gatekeeper to use for calls coming to the remote zone name.</li> </ul>
Step 5	<b>exit</b>  <b>Example:</b> Router(config-gk)# exit	Exits the current mode.

## Configure Local Zones

To configure local zones on the gatekeeper, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **gatekeeper**
4. **zone local** *gatekeeper-name domain-name [ras-IP-address] [invia inbound-gatekeeper | outvia outbound-gatekeeper [enable-intrazone]]*
5. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>gatekeeper</b>  <b>Example:</b> Router(config)# gatekeeper	Enters gatekeeper configuration mode.
Step 4	<b>zone local</b> <i>gatekeeper-name domain-name [ras-IP-address] [invia inbound-gatekeeper   outvia outbound-gatekeeper [enable-intrazone]]</i>  <b>Example:</b> Router(config-gk)# zone local termGK example.com 10.16.193.158 invia hurricane outvia hurricane enable-intrazone	Defines the local gatekeeper zone. Keywords and arguments are as follows: <ul style="list-style-type: none"> <li>• <i>gatekeeper-name</i>—Gatekeeper name or zone name</li> <li>• <i>domain-name</i>—Domain name served by this gatekeeper</li> <li>• <i>ras-IP-address</i>—IP address of one of the interfaces on the gatekeeper</li> <li>• <b>invia</b> <i>inbound-gatekeeper</i>—Gatekeeper for calls entering this zone</li> <li>• <b>outvia</b> <i>outbound-gatekeeper</i>—Gatekeeper for calls leaving this zone</li> <li>• <b>enable-intrazone</b>—All intrazone calls must use the via-zone gatekeeper</li> </ul>
Step 5	<b>exit</b>  <b>Example:</b> Router(config-gk)# exit	Exits the current mode.

## In-Service Updates to Gatekeeper Zone Prefix Configuration

This feature increases the availability of H.323 VoIP networks by allowing changes to a gatekeeper zone prefix while the gatekeeper is running and managing active E.164 registrations.

Prior to Cisco IOS Release 12.4(6)T the gatekeeper had to be shut down before changes can be applied. The shutdown removed all existing calls and registrations, making modification of zone prefix configurations inconvenient and costly for customers.

No configuration is required.

## Configuring Call-Capacity Thresholds

To configure call-capacity thresholds on the gatekeeper, perform the following steps.



### Note

Setting the threshold on the gatekeeper causes the gatekeeper to send an ARJ message to the gateway if call capacity is exceeded. If LRJ resource rejection is configured, the gatekeeper also sends an LRJ message in response to an LRQ message when call capacity is exceeded.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **gatekeeper**
4. **endpoint resource threshold onset** *high-water-mark* **abatement** *low-water-mark*
5. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>gatekeeper</b>  <b>Example:</b> Router(config)# gatekeeper	Enters gatekeeper configuration mode.

	Command or Action	Purpose
Step 4	<p><b>endpoint resource threshold onset</b> <i>high-water-mark</i> <b>abatement</b> <i>low-water-mark</i></p> <p><b>Example:</b> Router(config-gk)# endpoint resource threshold onset 85 abatement 65</p>	<p>Sets the call volume thresholds in the gatekeeper for monitoring its gateway. Keywords and arguments are as follows:</p> <ul style="list-style-type: none"> <li>• <b>onset</b> <i>high-water-mark</i>—Maximum call-volume usage for the gateway, as a percentage. Range: 1 to 99. Default: 90.</li> <li>• <b>abatement</b> <i>low-water-mark</i>—Minimum call-volume usage for the gateway, as a percentage. Range: 1 to 99. Default: 80.</li> </ul>
Step 5	<p><b>exit</b></p> <p><b>Example:</b> Router(config-gk)# exit</p>	Exits the current mode.

## Configuring LRQ Resource Rejection

By default, the gatekeeper does not reject LRQs based on resource limits of the endpoints. To configure the gatekeeper to reject LRQs, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **gatekeeper**
4. **lrq reject-resource-low**
5. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	Enters global configuration mode.
Step 3	<p><b>gatekeeper</b></p> <p><b>Example:</b> Router(config)# gatekeeper</p>	Enters gatekeeper configuration mode.

	Command or Action	Purpose
Step 4	<code>lrq reject-resource-low</code>  <b>Example:</b> Router(config-gk)# lrq reject-resource-low	Configures the gatekeeper to reject an LRQ if the endpoints that can service a call are out of resources.
Step 5	<code>exit</code>  <b>Example:</b> Router(config-gk)# exit	Exits the current mode.

## Configuring the Sequential LRQ Timer

This feature allows service providers the ability to define the time window during which the gatekeeper collects responses from the gateway before resending a RAS message to a gatekeeper and to set the number of times to resend the RAS message after the timeout period expires. To configure the sequential LRQ timer, perform the following tasks.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `gatekeeper`
4. `timer lrq seq delay`
5. `timer lrq window decisecc`
6. `no shutdown`
7. `exit`

### DETAILED STEPS

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

	Command or Action	Purpose
Step 4	<code>timer lrq seq delay</code>  <b>Example:</b> Router(config-gk)# timer lrq seq delay 1	Defines the time interval between successive sequential LRQs.
Step 5	<code>timer lrq window decisec</code>  <b>Example:</b> Router(config-gk)# timer lrq window decisec 3	Defines the time window during which the gatekeeper collects responses to one or more outstanding LRQs.
Step 6	<code>no shutdown</code>  <b>Example:</b> Router(config-gk)# no shutdown	Enables the gatekeeper.
Step 7	<code>exit</code>  <b>Example:</b> Router(config-gk)# exit	Exits the current mode.

## H.323 Standard-Based Hopcount Field in LRQ

This feature adds support for H.225 version 4 standard hopCount field in the LocationRequest RAS message.

The hopCount field defines the number of gatekeepers through which a message may propagate. If hopCount is greater than 0, the gatekeeper inserts the new hop count value into the message to be forwarded. If hopCount has reached 0, the gatekeeper will not forward the message.

The hopCount field was added in H225 version 4. The Cisco gatekeeper supported the same mechanism before it was added to the standard using Non-Standard fields. Support for the Non-Standard mechanism for backward compatibility exists.

No configuration is required.

## Dynamic Control of Gatekeeper Sequential LRQ Processing Through GKTMP

If a gatekeeper receives a location reject message (LRJ) When an alternate gatekeeper is connected, the default process is to repeat the location request (LRQ). This feature allows service providers to reject traffic at the Gatekeeper Transaction Message Protocol (GKTMP) server.

No configuration is required.

## Enhanced ARQ and RRQ Security for Gatekeeper Registrations

This feature provides additional security checks upon receiving the registration request (RRQ) from an endpoint. Enhanced ARQ and RRQ Security for gatekeepers describes comparisons made in the endpoint ID, aliases, source address, RAS address, and call signaling address for the end point to its registration and reject the request if the appropriate fields don't match.

The enhanced security checks at the gatekeeper compares source address, RAS address and call signaling addresses for the endpoint and sends the reject RRQ if the appropriate fields don't match. To configure enhanced security checks at the gatekeeper for RRQ, perform the steps in this section. This section contains the following subsections:

- [Restrictions for ARQ and RRQ Security for Gatekeeper Registrations, page 32](#)
- [Information About ARQ and RRQ Security for Gatekeeper Registrations, page 32](#)
- [Configuring ARQ and RRQ Security for Gatekeeper Registrations, page 33](#)
- [Verifying Enhanced ARQ and RRQ Security for Gatekeeper Registrations, page 34](#)

## Restrictions for ARQ and RRQ Security for Gatekeeper Registrations

Security enhancements on the ARQ to not enforce control between ARQ and Setup; it is still possible for an unauthorized user with a VoIP account to:

- Establish a call on behalf of another user by sending the correct source info in the ARQ along with spoofed source info in the Setup.
- Send a valid ARQ to enable any unregistered third party endpoint to pass the call.

## Information About ARQ and RRQ Security for Gatekeeper Registrations

The Gatekeeper in the Cisco UBE performs the initial security checks upon receiving the registration request (RRQ) from an endpoint. The GK should reject the RRQ if the security checks fail. The enhanced security features are beneficial for networks that have the Cisco Unified Border Element co-located in the same box as their gatekeeper.

This feature describes how the gatekeeper should be less verbose when the security checks fails and return a generic error condition (securityDenial) and how to handle legitimate endpoints that return specific error causes.

The following enhanced checks should be done by the gatekeeper on a RRQ:

### High RRQ—new registrations or repeated refresh RRQ

- Match transport address. Reject RAS messages from endpoints if they do not use the same ip address for both RAS as well as call signaling.

Check the RAS address presented, if the address is not “source address == ras address (RRQ) == call signaling address (RRQ)”; send a security denial (RRJ).

- Match alias address(es) list sent in the RAS message with the alias address(es) already registered with the GK. If any alias address is found to be duplicate (i.e. registered with another endpoint), reject the RAS message.

For all alias addresses in the RRQ if a registered endpoint is found

- If the register endpoint call signaling address is not the same as call signaling address in the RRQ: send security denial (RRJ).
- If the endpoint ID is present in the RRQ and is not the same as the registers endpoint; send security denial (RRJ).

### Low RRQ—keepalives

- Check the RAS address presented in the RRQ, if the address is not “ras address == source address == registered endpoint's address”; send a security denial (RRJ).

- If the call signaling address present in the RRQ is not “call sig address= = source address= = registered endpoint’s call signaling address; send security denial (RRJ)

#### Enhanced Security checks at GK for ARQ/DRQ/ BRQ/URQ/IIR

Security loopholes addressed by:

- Checks done for RRQ/ARQ/URQ/BRQ/DRQ requests.
- Checks done for IRR responses to maintain uniformity

## Configuring ARQ and RRQ Security for Gatekeeper Registrations

To enable ARQ and RRQ Security for Gatekeeper Registrations, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **gatekeeper**
4. **security match source-ip**
5. **security match alias-address-list**
6. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>gatekeeper</b>  <b>Example:</b> Router(config)# gatekeeper	Enters gatekeeper configuration mode.
Step 4	<b>security match source-ip</b>  <b>Example:</b> Router(config-gk)# security	Configures the gatekeeper to check the source, ras, and call signaling address for all relevant RAS messages.

	Command or Action	Purpose
Step 5	<b>security match alias-address-list</b>  <b>Example:</b> Router(config-gk)# security match alias-address-list	Configures the gatekeeper to perform checks on the alias-address list for all relevant RAS messages.
Step 6	<b>exit</b>  <b>Example:</b> Router(config-gk)# exit	Exits the current mode.

## Examples

```
Router# config terminal
Router(config)# gatekeeper
Router(config-gk)# security match source-ip
Router(config-gk)# security match alias-address-list
Router(config-gk)# exit
```

## Verifying Enhanced ARQ and RRQ Security for Gatekeeper Registrations

The following example shows the configuration of a gatekeeper with the Enhanced ARQ and RRQ Security for Gatekeeper Registrations feature enabled. Note that the **aaa alias-address** command must be enabled for the gatekeeper to send the source address and alias-address information in the AAA requests. This command is enabled by default and not visible to users for manual configuration.

```
Router# show run all | security gatekeeper

gatekeeper
zone local OGK cisco.com 10.10.10.4 invia OGK outvia OGK
zone remote TGK cisco.com 10.10.10.5 1719
zone prefix TGK 54*
zone prefix OGK 63*
security match source-ip
security match alias-address-list
security aaa alias-address
no shutdown
```

## Configuring Extended InterZone Clear Token Support

The Extended InterZone Clear Token support provides the ability for terminating gatekeeper (TGK) or originating gatekeeper (OGK) to compute the Inter-Zone Clear Token (IZCT) hash token based on the Destination Alias, Destination CSA, Destination epid, Source Alias, Source CSA & Source epid. Currently gatekeepers compute the IZCT hash token only based on the Destination Alias. Extending the IZCT abilities increases Billing and Service integrity.

This feature provides additional security checks upon receiving the registration request (RRQ) from an endpoint. Enhanced Admission Request (ARQ) and RRQ Security for gatekeepers describes comparisons made in the endpoint ID, aliases, source address, RAS address, and call signaling address for the end point to its registration and reject the request if the appropriate fields don't match.

The enhanced security checks at the gatekeeper compares source address, RAS address and call signaling addresses for the endpoint and sends the reject RRQ if the appropriate fields don't match. To configure enhanced security checks at the gatekeeper for RRQ, perform the steps in this section. This section contains the following subsections:

- [Restrictions for ARQ and RRQ Security for Gatekeeper Registrations, page 32](#)
- [Information About ARQ and RRQ Security for Gatekeeper Registrations, page 32](#)
- [Configuring ARQ and RRQ Security for Gatekeeper Registrations, page 33](#)
- [Verifying Enhanced ARQ and RRQ Security for Gatekeeper Registrations, page 34](#)

## Restrictions for Extended InterZone Clear Token Support

- The **security izct** command must be configured at OGK/TGK in order to enable the feature.
- The call will fail if the hash keyword at TGK is changed from the point of computation of IZCT hash token to the point of re-computation of IZCT hash token after receiving the ARQ from TGW.
- The IZCT token generated is valid only for 30 seconds
- IZCT Hash token generated by TGK can be used for multiple calls only within 30 seconds.
- When configuring an outgoing gateway (OGW) <-> outgoing gatekeeper (OGK) <-> a trunking gatekeeper (TGK) <-> a trunking gateway (TGW). The **security izct** command is optional at the OGK, and required at the TGK. If hash parameter is not specified at the TGK, then dest-alias (default) will be used for hash token computation.

## Information About Extended InterZone Clear Token Support

- The **Hash** keyword at OGK and TGK do not need to match.
- More than one **hash** keyword can be configured for the **security izct** command

## Configuring Extended InterZone Clear Token Support

To enable Extended InterZone Clear Token Support, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **gatekeeper**
4. **security izct password *password* [hash {dest-alias | src-alias | src-csa | dest-csa | src-epid | dst-epid}]**
5. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>gatekeeper</b>  <b>Example:</b> Router(config)# gatekeeper	Enters gatekeeper configuration mode.
Step 4	<b>security izct password password[hash {dest-alias  src-alias  src-csa  dest-csa  src-epid  dst-epid}]</b>  <b>Example:</b> Router(config-gk)# security izct password example hash dest-alias	Configures the gatekeeper to perform checks on the alias-address list for all relevant RAS messages.
Step 5	<b>exit</b>  <b>Example:</b> Router(config-gk)# exit	Exits the current mode.

## Verifying Enhanced ARQ and RRQ Security for Gatekeeper Registrations

The following example shows the configuration of a gatekeeper with the Enhanced ARQ and RRQ Security for Gatekeeper Registrations feature enabled. Note that the **aaa alias-address** command must be enabled for the gatekeeper to send the source address and alias-address information in the AAA requests. This command is enabled by default and not visible to users for manual configuration.

```
Router# show run all | security gatekeeper

gatekeeper
zone local OGK cisco.com 10.10.10.4 invia OGK outvia OGK
zone remote TGK cisco.com 10.10.10.5 1719
zone prefix TGK 54*
zone prefix OGK 63*
security match source-ip
security match alias-address-list
security aaa alias-address
no shutdown
```

## Configuring RAS Retry and Timer

This feature allows service providers the ability to control transmit time margins on Cisco gatekeepers by changing the RAS message timeout LRQ value and message retry counter values.

The **ras timeout lrq** command configures the number of seconds for the gateway to wait before resending an RAS message to a gatekeeper. The **ras retry** command configures the number of times to resend the RAS message after the timeout period expires. The default values for timeouts and retries are acceptable in most networks. You can use these commands if you are experiencing problems in RAS message transmission between gateways and gatekeepers. For example, if you have gatekeepers that are slow to respond to a type of RAS request, increasing the timeout value and the number of retries increases the call success rate, preventing lost billing information and unnecessary switchover to an alternate gatekeeper.

To configure RAS message timeout values and retry counters, perform the following tasks.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **gatekeeper**
4. **ras timeout lrq 2**
5. **ras retry lrq 1**
6. **no shutdown**
7. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>gatekeeper</b>  <b>Example:</b> Router(config)# gatekeeper	Enters gatekeeper configuration mode.
Step 4	<b>ras timeout lrq 2</b>  <b>Example:</b> Router(config-gk)# ras timeout lrq 2	Configures the gatekeeper RAS message timeout values.

	Command or Action	Purpose
Step 5	<code>ras retry lrq 1</code>  <b>Example:</b> Router(config-gk)# <code>ras retry lrq 1</code>	Configures the gatekeeper RAS message retry value.
Step 6	<code>no shutdown</code>  <b>Example:</b> Router(config-gk)# <code>no shutdown</code>	Enables the gatekeeper.
Step 7	<code>exit</code>  <b>Example:</b> Router(config-gk)# <code>exit</code>	Exits the current mode.

## Configuring Real-Time Call Type Reporting Through GKTMP

This feature allows Cisco H.323 VoIP gateways to report the call type to a Cisco IOS Gatekeeper at the end of each call through an RAS DRQ message using an external call routing application through GKTMP. This allows an external call routing application to consider the call type when it makes decisions about how to route subsequent calls to the same destination.

To configure the call-type trigger from the gatekeeper to the RouteServer on receipt of the DRQ perform the following tasks.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `gatekeeper`
4. `server trigger drq`
5. `destination-info call-info-type`
6. `exit`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# <code>configure terminal</code>	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<b>gatekeeper</b>  <b>Example:</b> Router(config)# gatekeeper	Enters gatekeeper configuration mode.
Step 4	<b>server trigger drq</b>  <b>Example:</b> Router(config-gk)# server trigger drq ZGK2 1 RouteServer 1.1.1.1 10000	Configures the disengage request (DRQ) trigger statically on the gatekeeper.
Step 5	<b>destination-info call-info-type voice</b>  <b>Example:</b> Router(config-gk_drqtrigger)# destination-info call-info-type voice	Specifies the call type filter in the gatekeeper DRQ trigger submode.
Step 6	<b>exit</b>  <b>Example:</b> Router(config-gk_drqtrigger)# <b>exit</b>	Exits the gatekeeper DRQ trigger submode.

## Examples

The following example shows the configuration to trigger the call type from the gatekeeper to RouteServer on receipt of a disengage request (DRQ). In this example the DRQ will be sent to a route server for voice, fax, and modem:

```
!
gatekeeper
 zone local ZGK2 example.com
 zone remote DGK example.com 10.5.5.5 1719
 zone prefix ZGK2 1...
 zone prefix DGK 2...
 gw-type-prefix 1#* default-technology
 no shutdown
 server registration-port 8888
 !
 server trigger drq ZGK2 1 RouteServer 10.1.1.1 10000
 info-only
 call-info-type voice
 call-info-type fax
 call-info-type modem
 !
```

## Configuring Alternate Endpoint Call Attempts in RADIUS Call Accounting Records


This feature controls alternate endpoint hunting based on call disconnect cause codes. Alternate end point hunt is enabled by default. If you configure this feature you can control (disable) hunting based on call disconnect cause codes.

To configure alternate endpoint call attempts in RADIUS call accounting records tried in an Cisco UBE, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service {voip | voatm}**
4. **no h225 alt-ep hunt [all | cause-code]**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>voice service {voip   voatm}</b>  <b>Example:</b> Router(config)# voice service voip	Enters voice service configuration mode and specifies a voice encapsulation type.
Step 4	<b>h323</b>  <b>Example:</b> Router(config-voice-service)# h323	Enters H.323 voice-service configuration mode.
Step 5	<b>no h225 alt-ep hunt [all   cause-code]</b>  <b>Example:</b> Router(conf-serv-h323)# no h225 alt-ep hunt user-busy	Disables alternate endpoint hunts based on call disconnect cause codes. <ul style="list-style-type: none"> <li>• all—Continue hunt for all disconnect cause codes.</li> <li>• cause-code—May be entered as standard Q.850 number or as text.</li> </ul>  <b>Note</b> Alternate endpoint hunt is enabled for all cause codes by default. Command will be visible only for the negated hunt cause codes (with <b>no</b> prefixed).

## Unique Calling Party Information with Alternate Endpoints

This feature enables alternate endpoint capabilities of the Cisco IOS H.323 gatekeeper and voice gateway to associate a unique calling party number automatic number identification (ANI) with each alternate endpoint using the GKTMP.

## Verifying Gatekeeper Configuration and Operation

To verify gatekeeper configuration and operation, perform the following steps (listed alphabetically) as appropriate.

- 
- Step 1** **show gatekeeper circuit**  
Use this command to view information on calls in progress.
- Step 2** **show gatekeeper endpoint**  
Use this command to view information on endpoint registrations.
- Step 3** **how gatekeeper performance stats**  
Use this command to view RAS information, including via-zone statistics.
- Step 4** **show gatekeeper status**  
Use this command to view call-capacity thresholds.
- Step 5** **show gatekeeper zone status**  
Use this command to verify gatekeeper configuration.
- Step 6** **show running-config | begin gatekeeper**  
Use this command to verify gatekeeper configuration.
- 

## Examples

This section contains the following output examples:

- [Sample Output for the show gatekeeper circuit Command, page 41](#)
- [Sample Output for the show gatekeeper endpoint Command, page 42](#)
- [Sample Output for the show gatekeeper performance stats Command, page 42](#)
- [Sample Output for the show gatekeeper status Command, page 43](#)
- [Sample Output for the show gatekeeper zone status Command, page 44](#)
- [Sample Output for the show running-config Command, page 45](#)

### Sample Output for the show gatekeeper circuit Command

Router# **show gatekeeper circuit**

```

                                CIRCUIT INFORMATION
                                =====
Circuit      Endpoint    Max Calls Avail Calls Resources      Zone
-----
cisco-default-h323-circuit
              Total Endpoints: 1
              ipipgw
                                1000      1000      Available

```



#### Note

The word “calls” refers to call legs in some commands and output.

**Sample Output for the show gatekeeper endpoint Command**

```
Router# show gatekeeper endpoint
```

```

                                GATEKEEPER ENDPOINT REGISTRATION
                                =====
CallSignalAddr  Port  RASignalAddr  Port  Zone Name        Type  Flags
-----
172.19.148.202  1720  172.19.148.202  2052  vepzone          TERM
    E164-ID: 1025
    H323-ID: cjb.office
172.19.148.205  1720  172.19.148.205  55995  vepzone          H323-GW
    H323-ID: ipipgw
    Voice Capacity Max.= 1000  Avail.= 1000  Current.= 0
172.19.148.208  1720  172.19.148.208  17201  vepzone          TERM
    E164-ID: 130512344
    E164-ID: 1024
    H323-ID: vep4
172.19.232.138  1720  172.19.232.138  17201  vepzone          TERM
    E164-ID: 4203
    H323-ID: ipvc-pt900-2
Total number of active registrations = 4

```

**Sample Output for the show gatekeeper performance stats Command**

[Table 1](#) describes the significant RAS via-zone fields shown in the display.

```
Router# show gatekeeper performance stats
```

```

-----Gatekeeper Performance Statistics-----

Performance statistics captured since: 01:50:17 UTC Sun Mar 3 2002

Gatekeeper level Admission Statistics:
    ARQs received: 28
    ARQs received from originating endpoints: 14
    ACFs sent: 28
    ACFs sent to the originating endpoint: 14
    ARJs sent: 0
    ARJs sent to the originating endpoint: 0
    ARJs sent due to overload: 0
    Number of concurrent calls: 0
    Number of concurrent originating calls: 0

Gatekeeper level Location Statistics:
    LRQs received: 0
    LRQs sent: 0
    LCFs received: 0
    LCFs sent: 0
    LRJs received: 0
    LRJs sent: 0
    LRJs sent due to overload: 0

Gatekeeper level Registration Statistics:
    RRJ due to overload: 0
    Total Registered Endpoints: 4

Gatekeeper level Disengage Statistics:
    DRQs received: 24
    DRQs sent: 0
    DCFs received: 0
    DCFs sent: 24
    DRJs received: 0
    DRJs sent: 0

```

Gatekeeper viazone message counters:

```

inARQ: 7
infwdARQ: 0
inerrARQ: 0
inLRQ: 0
infwdLRQ: 0
inerrLRQ: 0
outLRQ: 0
outfwdLRQ: 0
outerrLRQ: 0
outARQ: 0
outfwdARQ: 0
outerrARQ: 0

```

Load balancing events: 0

**Table 1** *show gatekeeper performance stats Field Descriptions*

Field	Description
inLRQ	Message counter associated with the <b>invia</b> keyword. If the invia is a local zone, this counter identifies the number of LRQs terminated by the local invia gatekeeper.
infwdLRQ	Message counter associated with the <b>invia</b> keyword. If the invia is a remote zone, this counter identifies the number of LRQs that were forwarded to the remote invia gatekeeper.
inerrLRQ	Message counter associated with the <b>invia</b> keyword. Number of times the LRQ could not be processed because the invia gatekeeper ID could not be found. Usually caused by a misspelled gatekeeper name.
outLRQ	Message counter associated with the <b>outvia</b> keyword. If the outvia is a local zone, this counter identifies the number of LRQs terminated by the local outvia gatekeeper. This counter applies only in configurations where no invia gatekeeper is specified.
outfwdLRQ	Message counter associated with the <b>outvia</b> keyword. If the outvia is a remote zone, this counter identifies the number of LRQs that were forwarded to the remote outvia gatekeeper. This counter applies only in configurations where no invia gatekeeper is specified.
outerrLRQ	Message counter associated with the <b>outvia</b> keyword. Number of times the LRQ could not be processed because the outvia gatekeeper ID could not be found. Usually caused by a misspelled gatekeeper name. This counter applies only in configurations where no invia gatekeeper is specified.
outARQ	Message counter associated with the <b>outvia</b> keyword. Identifies the number of originating ARQs handled by the local gatekeeper if the outvia is in the local zone.
outfwdARQ	Message counter associated with the <b>outvia</b> keyword. If the outvia gatekeeper is a remote zone, this number identifies the number of originating ARQs received by this gatekeeper that resulted in LRQs being sent to the outvia gatekeeper.
outerrARQ	Message counter associated with the <b>outvia</b> keyword. Number of times the originating ARQ could not be processed because the outvia gatekeeper ID could not be found. Usually caused by a misspelled gatekeeper name.

### Sample Output for the show gatekeeper status Command

```
Router# show gatekeeper status
```

```
Gatekeeper State: UP
```

```

Load Balancing:   DISABLED
Flow Control:    DISABLED
Zone Name:       vepzone
Accounting:      DISABLED
Endpoint Throttling:  DISABLED
Security:        DISABLED
Maximum Remote Bandwidth: unlimited
Current Remote Bandwidth: 0 kbps
Current Remote Bandwidth (w/ Alt GKs): 0 kbps

```

### Sample Output for the show gatekeeper zone status Command

```

Router# show gatekeeper zone status

                        GATEKEEPER ZONES
                        =====
GK name      Domain Name  RAS Address  PORT  FLAGS
-----
vepzone      172.19.148.10 172.19.148.209 1719  LSV
VIAZONE INFORMATION :
  invia:vepzone,  outvia:vepzone
  intrazone:enabled
BANDWIDTH INFORMATION (kbps) :
  Maximum total bandwidth : unlimited
  Current total bandwidth : 0
  Maximum interzone bandwidth : unlimited
  Current interzone bandwidth : 0
  Maximum session bandwidth : unlimited
SUBNET ATTRIBUTES :
  All Other Subnets : (Enabled)
PROXY USAGE CONFIGURATION :
  Inbound Calls from all other zones :
    to terminals in local zone vepzone : do not use proxy
    to gateways in local zone vepzone : do not use proxy
    to MCUs in local zone vepzone : do not use proxy
  Outbound Calls to all other zones :
    from terminals in local zone vepzone : do not use proxy
    from gateways in local zone vepzone : do not use proxy
    from MCUs in local zone vepzone : do not use proxy

```

**Sample Output for the show running-config Command**

```
Router# show running-config
```

```
.
.
.
gatekeeper
 zone local viagk2local1 mcebutest2.example.com 200.1.1.96 invia viagk2 outvia viagk2
enable-intrazone
 zone local viagk2 mcebutest.example.com invia viagk2 outvia viagk2 enable-intrazone
 zone local viagk2local2 mcebutest2.example.com
 zone remote viagk1 mcebutest.example.com 200.1.1.76 1719 invia viagk2 outvia viagk2
 zone remote dgk-us mcebutest.example.com 200.1.1.90 1719
 zone remote viagk3 mcebutest.example.com 200.1.1.85 1719 invia viagk2 outvia viagk2
 zone prefix viagk1 131013720..
 zone prefix viagk3 14122351...
send-cisco-circuit-info
gw-type-prefix 7#* default-technology
no use-proxy viagk2local1 default inbound-to terminal
no use-proxy viagk2local1 default outbound-from terminal
no use-proxy viagk2 default inbound-to terminal
no use-proxy viagk2 default outbound-from terminal
no shutdown
```

## Troubleshooting Gatekeeper Configuration and Operation

**Caution**

Under moderate traffic loads, these **debug** commands produce a high volume of output.

- Use the **debug voip ipipgw** command to debug the Cisco Unified Border Element with Gatekeeper feature.
- Use any of the following additional **debug** commands (listed alphabetically) on the gatekeeper as appropriate:
  - **debug gatekeeper call 10**
  - **debug gatekeeper endpoint 10**
  - **debug gatekeeper main 10**
  - **debug gatekeeper zone 10**
  - **debug h225 asn1**
  - **debug ras**

**Note**

For examples of **show** and **debug** command output and details on interpreting the output, see the following resources:

- [Cisco IOS Debug Command Reference](#)
- [Cisco IOS Voice Troubleshooting and Monitoring Guide](#)
- [Troubleshooting and Debugging VoIP Call Basics](#)
- [VoIP Debug Commands](#)

# Configuration Examples for Gatekeepers

This chapter includes the following configuration examples:

- [Universal Gatekeeper Configurations: Example, page 46](#)
- [Via-Zone Gatekeeper: Example, page 47](#)

## Universal Gatekeeper Configurations: Example

The size and complexity of gatekeeper configuration become greater as the number of interoperating gatekeepers increases in the VoIP network. One solution to minimize the configuration complexity of the gatekeepers is to maintain a “master list” of remote zones. With this strategy, the master list is applied to the gatekeeper configuration, and the proper remote zone is changed to be the local zone. For example:

```
zone remote Scotland example.com 10.18.194.165
zone remote transAtlantic example.com 10.18.194.183
zone remote transPacific example.com 10.18.194.180
zone remote USA example.com 10.18.200.135 outvia transPacific
zone remote Brazil example.com 10.18.194.179
zone prefix Scotland 44*
zone prefix USA 1*
zone prefix Brazil 55*
```

The call flow between USA and Scotland now has calls originating from Scotland to the USA going through a trans-Pacific Cisco UBE and calls from the USA to Scotland going through a trans-Atlantic Cisco UBE.

To add another example, if you want all calls originated from Scotland to be routed through Cisco UBEs in the trans-Atlantic zone, the master file is changed as shown in the following example:

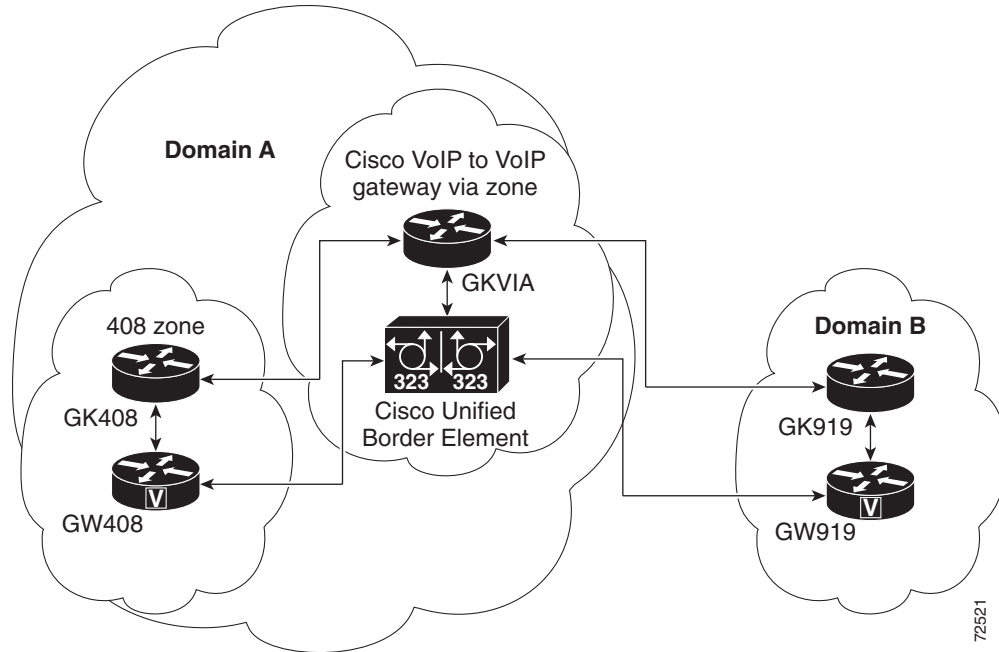
```
zone remote transAtlantic example.com 10.18.194.183
zone remote transPacific example.com 10.18.194.180
zone remote Scotland example.com 10.18.194.165 outvia transAtlantic
zone remote USA example.com 10.18.200.135 outvia transAtlantic
zone remote Brazil example.com 10.18.194.179
zone prefix Scotland 44*
zone prefix USA 1*
zone prefix Brazil 55*
```

All of the examples shown illustrate the concept of a master gatekeeper configuration. Also, even though the USA and Scotland gatekeepers have a via-zone keyword in their configuration, this does not imply that they have any Cisco UBEs registered to them. Call resolution for Brazil, for example, happens according to the traditional logic for calls originating from the USA and Scotland.

# Via-Zone Gatekeeper: Example

Figure 1 shows an example configuration of the Via-zone Gatekeeper feature.

Figure 1 Via-zone Gatekeeper Feature Topology



### Originating Gateway Configuration: Example

```
interface Ethernet0/0
 ip address 10.16.8.132 255.255.255.0
 half-duplex
 h323-gateway voip interface
 h323-gateway voip id GK408 ipaddr 10.16.8.123 1718
 h323-gateway voip h323-id GW408
 !
 dial-peer voice 919 voip
 destination-pattern 919.....
 session target ras
 !
 gateway
```

### Originating Gatekeeper Configuration: Example

```
gatekeeper
 zone local GK408 usa 10.16.8.123
 zone remote GKVIA usa 10.16.8.24 1719
 zone prefix GKVIA 919*
 gw-type-prefix 1#*
 no shutdown
```

### Cisco Unified Border Element with Gatekeeper Configuration: Example

```
!
 voice service voip
 no allow-connections any to pots
 no allow-connections pots to any
```

```

allow-connections h323 to h323
h323
  ip circuit max-calls 1000
  ip circuit default only
!
!
interface FastEthernet0/0
ip address 10.16.8.145 255.255.255.0
ip route-cache same-interface
duplex auto
speed auto
h323-gateway voip interface
h323-gateway voip id GKVIA ipaddr 10.16.8.24 1718
h323-gateway voip h323-id IPIPGW
h323-gateway voip tech-prefix 1#
!
!
dial-peer voice 919 voip
incoming called-number 919.....
destination-pattern 919.....
session target ras
codec transparent
!
gateway

```

### Via-Zone Gatekeeper Configuration: Example

```

gatekeeper
zone local GKVIA usa 10.16.8.24
zone remote GK919 usa 10.16.8.146 1719 invia GKVIA outvia GKVIA
zone prefix GK919 919*
no shutdown

```

### Terminating Gateway: Example

```

interface Ethernet0/0
ip address 10.16.8.134 255.255.255.0
half-duplex
h323-gateway voip interface
h323-gateway voip id GK919 ipaddr 10.16.8.146 1718
h323-gateway voip h323-id GW919
h323-gateway voip tech-prefix 919
!
dial-peer voice 919 pots
destination-pattern 919.....
port 1/0:1
!
gateway

```

### Terminating Gatekeeper Configuration: Example

```

gatekeeper
zone local GK919 usa 10.16.8.146
gw-type-prefix 1#* default-technology
no shutdown

```

## Additional References

The following sections provide additional references related to the Cisco Unified Border Element with Gatekeeper.



### Note

- In addition to the references listed below, each chapter provides additional references related to Cisco Unified Border Element.
- Some of the products and services mentioned in this guide may have reached end of life, end of sale, or both. Details are available at [http://www.cisco.com/en/US/products/prod\\_end\\_of\\_life.html](http://www.cisco.com/en/US/products/prod_end_of_life.html).
- The preface and glossary for the entire voice-configuration library suite of documents is listed below.

## Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
Cisco IOS Voice commands	<a href="#">Cisco IOS Voice Command Reference</a>
Cisco IOS Voice Configuration Library	For more information about Cisco IOS voice features, including feature documents, and troubleshooting information—at <a href="http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm">http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm</a>
Cisco IOS Release 15.0	<a href="#">Cisco IOS Release 15.0 Configuration Guides</a>
Cisco IOS Release 12.4	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.4 Configuration Guides</a></li> <li>• <a href="#">Cisco IOS Release 12.4T Configuration Guides</a></li> </ul>
Cisco IOS Release 12.3	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.3 documentation</a></li> <li>• <a href="#">Cisco IOS Voice commands</a></li> <li>• <a href="#">Cisco IOS Voice Troubleshooting and Monitoring Guide</a></li> <li>• <a href="#">Tcl IVR Version 2.0 Programming Guide</a></li> </ul>
Cisco IOS Release 12.2	<a href="#">Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2</a>
DSP documentation	High-Density Packet Voice Feature Card for Cisco AS5350XM and AS5400XM Universal Gateways <a href="http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/vfc_dsp.html">http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/vfc_dsp.html</a>
GKTMP (GK API) Documents	<ul style="list-style-type: none"> <li>• <i>GKTMP Command Reference:</i> <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm</a></li> <li>• <i>GKTMP Messages:</i> <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html</a></li> </ul>

Related Topic	Document Title
internet Low Bitrate Codec (iLBC) Documents	<ul style="list-style-type: none"> <li>• Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/dp_ovrvw.html">http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/dp_ovrvw.html</a></li> <li>• Dial Peer Features and Configuration section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/dp_config.html">http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/dp_config.html</a></li> </ul>
Cisco Unified Border Element Configuration Examples	<ul style="list-style-type: none"> <li>• Local-to-remote network using the IPIPGW <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml</a></li> <li>• Remote-to-local network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml</a></li> <li>• Remote-to-remote network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml</a></li> <li>• Remote-to-remote network using two IPIPGWs: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml</a></li> </ul>
Related Application Guides	<ul style="list-style-type: none"> <li>• <a href="#">Cisco Unified Communications Manager and Cisco IOS Interoperability Guide</a></li> <li>• <a href="#">Cisco IOS Fax, Modem, and Text Support over IP Configuration Guide</a></li> <li>• “Configuring T.38 Fax Relay” chapter</li> <li>• <a href="#">Cisco IOS SIP Configuration Guide</a></li> <li>• <a href="#">Cisco Unified Communications Manager (CallManager) Programming Guides</a></li> <li>• <a href="#">Quality of Service for Voice over IP</a></li> </ul>
Related Platform Documents	<ul style="list-style-type: none"> <li>• <a href="#">Cisco 2600 Series Multiservice Platforms</a></li> <li>• <a href="#">Cisco 2800 Series Integrated Services Routers</a></li> <li>• <a href="#">Cisco 3600 Series Multiservice Platforms</a></li> <li>• <a href="#">Cisco 3700 Series Multiservice Access Routers</a></li> <li>• <a href="#">Cisco 3800 Series Integrated Services Routers</a></li> <li>• <a href="#">Cisco 7200 Series Routers</a></li> <li>• <a href="#">Cisco 7301</a></li> </ul>
Related gateway configuration documentation	<p>Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways.</p> <p><a href="http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm">http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm</a></p>

Related Topic	Document Title
Cisco IOS NAT Configuration Guide, Release 12.4T	<p><i>Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller</i></p> <p><a href="http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html">http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html</a></p>
Troubleshooting and Debugging guides	<ul style="list-style-type: none"> <li>• Cisco IOS Debug Command Reference, Release 12.4 at <a href="http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html">http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html</a></li> <li>• <i>Troubleshooting and Debugging VoIP Call Basics</i> at <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml</a></li> <li>• <i>VoIP Debug Commands</i> at <a href="http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html">http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html</a></li> </ul>

## Standards

Standard	Title
H.323 Version 4 and earlier	<i>H.323 (ITU-T VOIP protocols)</i>

## MIBs

MIB	MIBs Link
None.	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFC	Title
RFC 2833	<i>RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals</i>
RFC 3261	<i>SIP: Session Initiation Protocol</i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for Cisco Unified Border Element with Gatekeeper Configuration Guide

Table 2 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(13)T3 or a later release appear in the table. Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2** Feature Information for Cisco Unified Border Element Overview

Feature Name	Release	Feature Information
Cisco UBE Image Consolidation	12.3(7)T	This feature was introduced.
Dynamic Control of Gatekeeper Sequential LRQ Processing Through GKTMP	12.4(4)T	This feature was introduced.
Enhanced ARQ and RRQ Security for Gatekeeper Registrations	12.4(15)XY 12.4(20)T	This feature was introduced.
Extended InterZone Clear Token	12.4(15)XZ 12.4(20)T	This feature was introduced.
H.323 Standard Based Hopcount Field in LRQ.	12.4(4)T	This feature was introduced.
In-Service Updates to Gatekeeper Zone Prefix Configuration	12.4(6)T	This feature was introduced.
RAS Retry and Timer; Sequential LRQ Timer	12.4(4)T	This feature was introduced.
Real-Time Call Type Reporting Through GKTMP	12.4(4)T	This feature was introduced.
Restriction for Video Calls made from a Cisco Unified Communications Manager to an Cisco Unified Border Element	12.3(8)T	This restriction was added.
Support for Cisco 7200 and Cisco 7301	12.3(8)T	This feature was introduced.

**Table 2**      **Feature Information for Cisco Unified Border Element Overview**

Feature Name	Release	Feature Information
Support for the Cisco 2801	12.4(4)T	This feature was introduced.
Support for the Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3825, and Cisco 3845	12.3(11)T	This feature was introduced.
Unique Calling Party Information with Alternate Endpoints	12.4(6)T	This feature was introduced.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo 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. (0910R)

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.

© 2008 Cisco Systems, Inc. All rights reserved.

