



## **Cisco Gatekeeper External Interface Reference, Version 4.2**

Cisco IOS Release 12.2(15)T  
March 2003

### **Corporate Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Net Readiness Scorecard, Networking Academy, and ScriptShare are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0303R)

*Cisco Gatekeeper External Interface Reference, Version 4.2*  
Copyright © 2003, Cisco Systems, Inc.  
All rights reserved.



<b>About This Guide</b>	<b>xi</b>
Document History	xi
Document Objectives	xi
Audience	xii
Document Organization	xii
Related Documentation	xii
Syntax Conventions	xiii
Obtaining Documentation	xiii
Cisco.com	xiii
Documentation CD-ROM	xiii
Ordering Documentation	xiv
Documentation Feedback	xiv
Obtaining Technical Assistance	xiv
Cisco.com	xv
Technical Assistance Center	xv
Cisco TAC Website	xv
Cisco TAC Escalation Center	xvi
Obtaining Additional Publications and Information	xvi

---

**CHAPTER 1**

<b>Overview of H.323</b>	<b>1-1</b>
H.323 Terminals	1-2
Gatekeepers	1-3
Gatekeeper Zones	1-3
MCUs	1-3
Gateways	1-3
How Terminals, Gatekeepers, and Gateways Work Together	1-4

---

**CHAPTER 2**

<b>Overview of the Cisco IOS Gatekeeper</b>	<b>2-1</b>
Zone and Subnet Configuration	2-1
Terminal Name Registration	2-1
Inter-Zone Communication	2-2
Accounting Using RADIUS/TACACS+	2-2
Inter-Zone Routing	2-2

**CHAPTER 3**

**Implementing an External Interface to the Cisco IOS Gatekeeper 3-1**

- How the External Interface Works 3-1
- How Gatekeeper Triggers Work 3-2
  - Statically Configured Triggers 3-3
  - Dynamically Configured Triggers 3-4
    - API Functions 3-4
    - GKTMP Messages 3-5
    - Example of a Dynamic Trigger Registration Message 3-6
  - Specifying Wildcards in Triggers 3-6
  - Notification-Only Triggers 3-7
- How RAS Messages are Processed 3-7
  - Processing of xRQ Requests 3-8
  - Processing of LCF Requests 3-9
  - Processing of LRJ Requests 3-9
- How Security Works 3-10
  - CryptoTokens and Cisco Gateways 3-10
  - Requirements for using CryptoTokens 3-10
  - Validating a CryptoToken 3-10
  - CryptoTokens in RAS Messages 3-11
- GKTMP Message Examples 3-11
  - Populating an External Application’s Registration Database 3-11
  - 800 Number Lookup 3-12
  - Internet Call-Waiting 3-12
- How the API Works 3-14
  - Linking with the Gatekeeper API 3-15
  - Guidelines for Using the Gatekeeper API 3-15
- Gatekeeper API Examples 3-16

**CHAPTER 4**

**GKTMP Messages 4-1**

- GKTMP RAS Messages 4-1
  - Message Line 4-1
  - Message Header 4-2
  - Message Body 4-3
  - Registration Messages 4-4
    - Request RRQ 4-5
    - Response RRQ 4-5
    - Response RCF 4-5
    - Response RRJ 4-6

Unregistration Message	4-7
Request URQ	4-7
Command URQ	4-7
Result URQ	4-8
Admission Messages	4-8
Request ARQ	4-8
Response ARQ	4-10
Response ACF	4-11
Response ARJ	4-12
Location Messages	4-14
Request LRQ	4-14
Response LRQ	4-15
Request LCF	4-16
Response LCF	4-18
Request LRJ	4-19
Response LRJ	4-19
Disengage Messages	4-21
Request DRQ	4-21
Resource Messages	4-21
Request RAI	4-21
Bandwidth Messages	4-22
Request BRQ	4-22
Response BRQ	4-23
Response BCF	4-23
Response BRJ	4-23
Progress Messages	4-24
Response RIP	4-24
Request IRR	4-24
Request ALV	4-25
Response ALV	4-25
Trigger Registration Messages	4-25
Message Line	4-25
Message Header	4-26
Message Body	4-27
Register RRQ and RAI	4-28
Register URQ	4-28
Register ARQ, DRQ, IRR, and BRQ	4-28
Register LRQ	4-28
Register LCF	4-29
Register LRJ	4-29

- Additional Messages 4-29
  - GTD 4-29
  - AlternateGK 4-30
  - FromReplyAddress 4-31
  - ServiceControlSession 4-31
  - CallCapacity 4-31
  - CarrierInfo 4-32
  - TrunkGroupInfo 4-32
  - Alias-Address 4-33
  - PerCallInfo 4-33
  - RemoteZone 4-33
  - Transport-Address 4-34
  - ClearToken 4-34
  - CryptoToken 4-34

**CHAPTER 5**

**Gatekeeper API Functions and Structures 5-1**

- Gatekeeper API Functions 5-1
  - GkapiSetupClient 5-2
    - Input 5-2
    - Return 5-2
  - GkapiSetupServer 5-2
    - Input 5-2
    - Return 5-3
  - GkapiClientConnected 5-3
    - Input 5-3
    - Return 5-3
  - GkapiAcceptConnection 5-4
    - Input 5-4
    - Return 5-4
  - GkapiGetVersion 5-4
    - Input 5-4
    - Return 5-4
  - CloseGateKeeperConnection 5-5
    - Input 5-5
    - Return 5-5
  - GetReadMsgBuffer 5-5
    - Input 5-5
    - Return 5-5
  - ReadMsgBuffer 5-5
    - Input 5-6

Return	5-6
FreeReadMsgBuffer	5-7
Input	5-7
Return	5-7
WriteCommandMsg	5-7
Input	5-7
Return	5-7
WriteResponseMsg	5-8
Input	5-8
Return	5-8
WriteRegisterMessage	5-9
Input	5-9
Return	5-9
WriteUnregisterMessage	5-10
Input	5-10
Return	5-10
GkapiSetupReport	5-11
Input	5-11
Return	5-11
GkapiQueryReport	5-11
Input	5-11
Return	5-11
API Structures	5-12
GKAPI_SOCK_INFO	5-14
GKAPI_TCP_ADDR_INFO	5-14
GKAPI_VERSION_INFO	5-15
GK_CMD_MSG_TYPE	5-15
CMD_HEADER_INFO	5-15
GK_REGISTER_MSG	5-16
GK_UNREGISTER_MSG	5-16
REG_UNREG_RESP_MSG	5-17
REGISTER_REQUEST_HEADER	5-17
REGISTER_RESPONSE_HEADER	5-18
ARQ_REGISTER_MSG	5-18
RRQ_REGISTER_MSG	5-19
URQ_REGISTER_MSG	5-19
LRQ_REGISTER_MSG	5-19
LCF_REGISTER_MSG	5-20
LRJ_REGISTER_MSG	5-20
RAI_REGISTER_MSG	5-20

DRQ_REGISTER_MSG	5-21
BRQ_REGISTER_MSG	5-21
GK_READ_MSG	5-21
HEADER_INFO	5-22
ARQ_REQUEST_MSG	5-23
RRQ_REQUEST_MSG	5-24
URO_REQUEST_MSG	5-25
LRQ_REQUEST_MSG	5-25
LCF_REQUEST_MSG	5-26
LRJ_REQUEST_MSG	5-27
RAI_REQUEST_MSG	5-28
DRQ_REQUEST_MSG	5-28
BRQ_REQUEST_MSG	5-29
IRR_REQUEST_MSG	5-29
ALV_REQUEST_MSG	5-29
GK_WRITE_MSG	5-30
ARQ_RESPONSE_MSG	5-30
ACF_RESPONSE_MSG	5-31
ARJ_RESPONSE_MSG	5-32
RRQ_RESPONSE_MSG	5-32
RCF_RESPONSE_MSG	5-33
RRJ_RESPONSE_MSG	5-33
LRQ_RESPONSE_MSG	5-33
LCF_RESPONSE_MSG	5-34
LRJ_RESPONSE_MSG	5-34
BRQ_RESPONSE_MSG	5-35
BCF_RESPONSE_MSG	5-35
BRJ_RESPONSE_MSG	5-35
ALV_RESPONSE_MSG	5-36
CRYPTO_H323_TOKEN	5-36
CRYPTO_EP_PWD_HASH	5-36
CRYPTO_EP_PWD_ENCR	5-37
CRYPTO_EP_CERT	5-37
CLEAR_TOKEN	5-37
ALTERNATE_GK	5-38
ALTERNATE_ENDPOINT	5-38
ALTERNATE_TRANSPORT_ADDR_TYPE	5-38
RIP_RESPONSE_MSG	5-39
UNSUPPORTED_MSG	5-39
SERV_CNTRL_TYPE	5-39

URQ_CMD_MSG_TYPE	5-40
URQ_RESULT_MSG	5-40
CALL_CAPACITY	5-40
CALLS_AVAILABLE	5-40
CARRIER_INFO	5-41
PER_CALLINFO	5-41
REMOTE_ZONE	5-41
TERMINATION_CAUSE_TYPE	5-42
Enumerations	5-43
STATUS_TYPE	5-43
REG_STATUS_TYPE	5-44
ENDPOINT_TYPE	5-44
REDIRECT_REASON_TYPE	5-44
DRQ_REASON_TYPE	5-45
LRJ_REJECT_REASON_TYPE	5-45
REQUEST_MSG_TYPE	5-45
RRJ_REJECT_REASON_TYPE	5-46
ARJ_REJECT_REASON_TYPE	5-46
BRJ_REJECT_REASON_TYPE	5-47
URQ_REASON_TYPE	5-47
RESPONSE_MSG_TYPE	5-47
REGISTER_MSG_TYPE	5-48
REPORT_DEST_T	5-48
CRYPTO_H323_TOKEN_TYPE_S	5-48
USE_SPECIFIED_TRANSPORT_TYPE_T	5-48
CMD_MSG_TYPE	5-49
Limits	5-49

**CHAPTER 6****GKMP Command Reference 6-1**

server trigger	6-1
Trigger Submodes	6-2
info-only	6-2
shutdown	6-3
destination-info	6-3
redirect-reason	6-3
remote-ext-address	6-4
endpoint-type	6-5
supported-prefix	6-5
timer server timeout	6-5

- server registration-port 6-6
- server flow-control 6-6
- show gatekeeper servers 6-8
- show gatekeeper status 6-9
- debug gatekeeper servers 6-11



## About This Guide

This section describes the objectives, audience, organization, and conventions of the *Cisco Gatekeeper External Interface Reference, Version 4.2*.

## Document History

The versions of this guide are listed in [Table 1](#).

**Table 1** Document History

Title	Cisco IOS Release	Location
<i>Cisco Gatekeeper External Interface Reference, Version 1</i>	12.2(1)T	<a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121rel/gktmp/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121rel/gktmp/index.htm</a>
<i>Cisco Gatekeeper External Interface Reference, Version 2</i>	12.1(5)XM	<a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121rel/gktmpv2/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121rel/gktmpv2/index.htm</a>
<i>Cisco Gatekeeper External Interface Reference, Version 3</i>	12.2(2)XA	<a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/rel_docs/gktmpv3/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/rel_docs/gktmpv3/index.htm</a>
<i>Cisco Gatekeeper External Interface Reference, Version 3.1</i>	12.2(2)XB 12.2(4)T 12.2(8)T	<a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/rel_docs/gktmpv31/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/rel_docs/gktmpv31/index.htm</a>
<i>Cisco Gatekeeper External Interface Reference, Version 4.1</i>	12.2(11)T	<a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/rel_docs/gktmp4_1/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/rel_docs/gktmp4_1/index.htm</a>
<i>Cisco Gatekeeper External Interface Reference, Version 4.2</i>	12.2(15)T	<a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/rel_docs/gktmp4_2/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/rel_docs/gktmp4_2/index.htm</a>

## Document Objectives

This guide is designed to help you understand and implement an external interface to the Cisco IOS Gatekeeper using the Cisco Gatekeeper Transaction Message Protocol (GKTMP) and application programming interface (API).

# Audience

This guide is intended for application programmers who want to develop an application that interfaces with the Cisco IOS Gatekeeper.

## Document Organization

This document is divided into the following chapters shown in [Table 2](#):

**Table 2**     **Organization**

Chapter	Title	Description
Chapter 1	<a href="#">Overview of H.323</a>	Provides a high-level overview of H.323.
Chapter 2	<a href="#">Overview of the Cisco IOS Gatekeeper</a>	Provides an overview of the features and functions of the Cisco IOS Gatekeeper.
Chapter 3	<a href="#">Implementing an External Interface to the Cisco IOS Gatekeeper</a>	Provides information about and examples of implementing an external interface to the Cisco IOS Gatekeeper using the GKTMP and the Cisco IOS Gatekeeper API.
Chapter 4	<a href="#">GKTMP Messages</a>	Describes the messages used with the GKTMP.
Chapter 5	<a href="#">Gatekeeper API Functions and Structures</a>	Describes the functions provided with the Cisco IOS Gatekeeper API.
Chapter 6	<a href="#">GKTMP Command Reference</a>	Describes the Cisco IOS software commands used to configure triggers for a Cisco IOS Gatekeeper.

## Related Documentation

For additional information about the commands used in conjunction with the GKTMP, see the following documents:

*Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2

*Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2

*Cisco High Performance Gatekeeper*

*Cisco H.323 Scalability and Interoperability Enhancements*

# Syntax Conventions

Table 3 describes the syntax used with the commands in this document.

**Table 3** *Command Syntax Conventions*

Convention	Description
<b>boldface</b>	Commands and keywords.
<i>italic</i>	Command input that is supplied by you.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x   x   x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. You must select one.
^ or Ctrl	Represent the key labeled <i>Control</i> . For example, when you read ^D or <i>Ctrl-D</i> , you should hold down the Control key while you press the D key.
screen font	Examples of information displayed on the screen.
<b>boldface screen font</b>	Examples of information that you must enter.
< >	Nonprinting characters, such as passwords, appear in angle brackets in contexts where italics are not available.
[ ]	Default responses to system prompts appear in square brackets.

## Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco web sites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

<http://www.cisco.com/go/subscription>

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:  
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

## Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

## Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

<http://tools.cisco.com/RPF/register/register.do>

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

<http://www.cisco.com/en/US/support/index.html>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:  
[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:  
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:  
[http://www.cisco.com/en/US/about/ac123/ac114/about\\_cisco\\_packet\\_magazine.html](http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html)
- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:  
[http://business.cisco.com/prod/tree.taf%3fasset\\_id=44699&public\\_view=true&kbns=1.html](http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html)
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:  
[http://www.cisco.com/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)
- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:  
[http://www.cisco.com/en/US/learning/le31/learning\\_recommended\\_training\\_list.html](http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html)



## Overview of H.323

---

This chapter provides an overview of H.323 and includes the following sections:

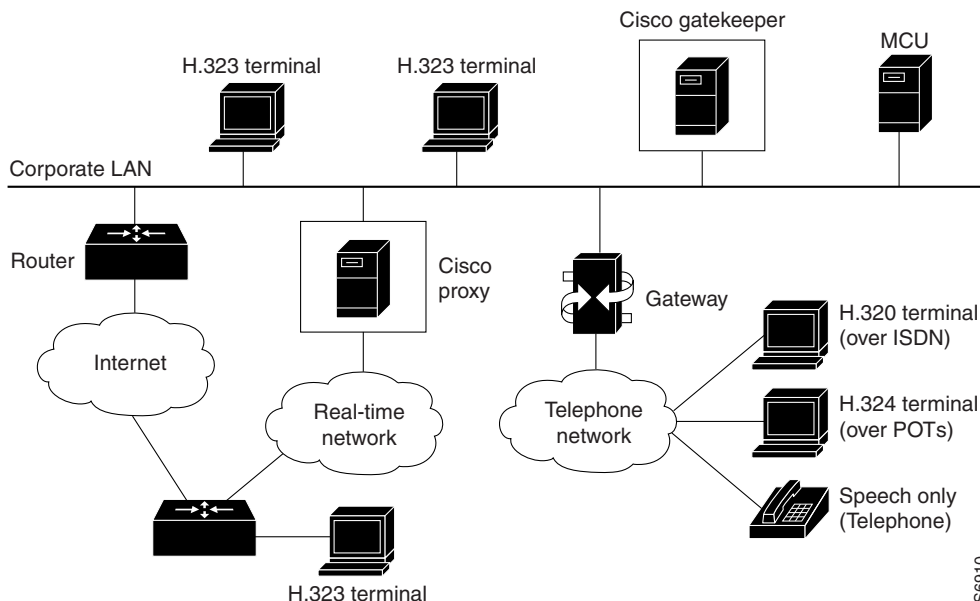
- [H.323 Terminals, page 1-2](#)
- [Gatekeepers, page 1-3](#)
- [MCUs, page 1-3](#)
- [Gateways, page 1-3](#)
- [How Terminals, Gatekeepers, and Gateways Work Together, page 1-4](#)

H.323 is an ITU standard for transmitting audio, video, and data conferencing data on an IP-based internetwork. The H.323 standard provides for the following types of *endpoints* in the network:

- [H.323 Terminals](#)
- [Gatekeepers](#)
- [MCUs](#)
- [Gateways](#)

[Figure 1-1](#) shows a typical H.323 network:

Figure 1-1 H.323 Network



## H.323 Terminals

An H.323 terminal is an endpoint in the LAN that participates in real-time, two-way communications with another H.323 terminal, gateway, or multipoint control unit (MCU). A terminal must support audio communication and can also support audio with video, audio with data, or a combination of all three.

H.323 terminals must support the following standards and protocols:

- H.245—An ITU standard used by the terminal to negotiate its use of the channel. The H.245 control channel provides in-band reliable transport for capabilities exchange, mode preference from the receiving end, logical channel signaling, and control and indication. Part of the capabilities exchange includes specifying which coder-decoders (CODECs) are available. Recommended audio CODECs include G.711, G.722, G.723, G.723.1, G.728, and G.729. Recommended video CODECs include H.261 and H.263.
- H.225.0—An ITU standard that uses a variant of Q.931 to set up the connection between two H.323 endpoints.
- RAS—(Registration Admission Status) A protocol used to communicate with the H.323 gatekeeper.
- RTP and RTCP—(Real-Time Transport Protocol and Real-Time Control Protocol) Protocols used to sequence the audio and video packets. The RTP header contains a time stamp and sequence number, allowing the receiving device to buffer as much as necessary to remove jitter and latency by synchronizing the packets to play back a continuous stream of sound. RTCP controls RTP and gathers reliability information and periodically passes this information onto session participants.

# Gatekeepers

Gatekeepers are optional nodes that manage other nodes in an H.323 network. Other nodes communicate with the gatekeeper using the RAS protocol. A gatekeeper is not required in an H.323 network, but it must be used if one is present.

The H.323 nodes attempt to *register* with a gatekeeper on startup. When an H.323 node wants to communicate with another endpoint, it requests *admission* to the call, using a symbolic alias for the endpoint name such as an E.164 (ITU-T recommendation for international telecommunication numbering) address or an e-mail ID. If the gatekeeper decides the call can proceed, it returns a destination IP address to the originating H.323 node. This IP address can be the actual address of the target endpoint or it can be an intermediate address. Finally, a gatekeeper and its registered endpoints exchange *status* information.

## Gatekeeper Zones

H.323 endpoints are grouped together in zones. Each zone has one gatekeeper that manages all the endpoints in the zone. A zone is an administrative convenience similar to a DNS domain. Gatekeeper zones are normally set up to correspond to geographic zones.

## MCUs

An MCU is an endpoint on the LAN that provides the capability for three or more terminals and gateways to participate in a multipoint conference. It controls and mixes video, audio, and data from terminals to create a robust video conference. An MCU can also connect two terminals in a point-to-point conference that can later develop into a multipoint conference.

**Note**

---

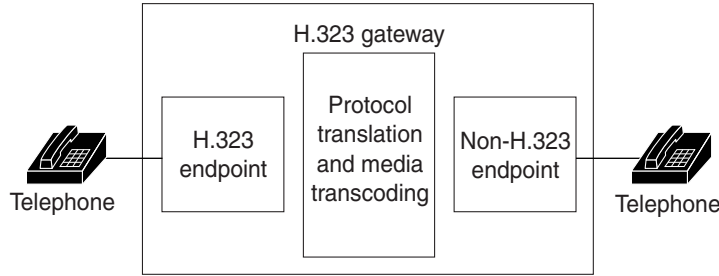
Some terminals have limited multipoint-control built into them. These terminals might not require an MCU with all the functionality mentioned previously.

---

## Gateways

An H.323 gateway can provide an interface between H.323 and the Public Switched Telephone Network (PSTN), H.320 terminals, V.70 terminals, H.324 terminals, and other speech terminals. It provides standard interfaces to the PSTN, processes the voice and fax signals using CODECs to convert between circuit-switched and packet formats, and works with the gatekeeper through the RAS protocol to route calls through the network. Gateways provide translation between transmission formats, such as H.245 and H.242. [Figure 1-2](#) shows a gateway between an H.323 terminal and a speech-only telephone.

**Figure 1-2 Gateway Between an H.323 Terminal and a Speech-only Telephone**



27847

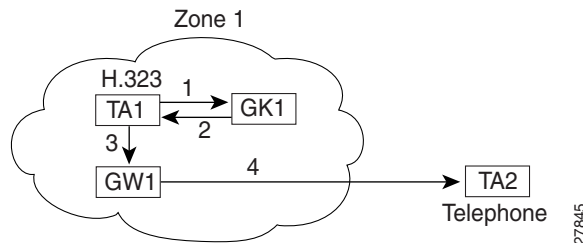
## How Terminals, Gatekeepers, and Gateways Work Together

Gateways provide protocol conversion between terminals running different types of protocols. Gateways communicate with gatekeepers using the RAS protocol. The gatekeeper maintains resource computing information, which it uses to select the appropriate gateway during the admission of a call. In [Figure 1-3](#) and [Figure 1-4](#):

- TA1 is an H.323 terminal registered to GK1.
- GW1 is an H.323-to-H.320 gateway registered to GK1.
- TA2 is a telephone.

[Figure 1-3](#) illustrates the processing of a call that originates with a device in the zone (TA1) and is intended for a device outside the zone (TA2).

**Figure 1-3 Processing of Calls Going Out of the Zone**

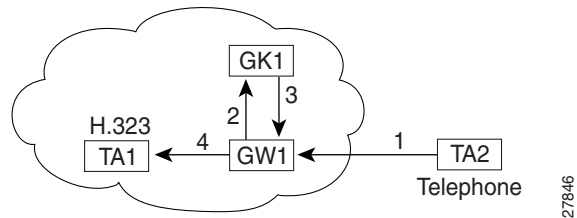


27845

A call from TA1 to TA2 is set up as follows:

1. TA1 asks GK1 for permission to connect to TA2's E.164 address.
2. The gatekeeper looks through its local registrations and does not find any H.323 terminals registered with that E.164 address, so the gatekeeper assumes that it is a telephone outside the scope of H.323. The gatekeeper instructs TA1 to connect to the GW1 IP address.
3. TA1 connects to GW1.
4. GW1 completes the call to TA2.

[Figure 1-4](#) illustrates the processing of a call that originates with a device outside the zone (TA2) and is intended for a device in the zone (TA1).

**Figure 1-4 Processing of Calls Coming Into the Zone**

A call from TA2 to TA1 is set up as follows:

1. TA2 calls GW1 and provides the TA1 E.164 address as the final destination.
2. GW1 sends a message to GK1 asking to connect to that address.
3. GK1 gives GW1 the address of TA1.
4. GW1 completes the call with TA1.





## Overview of the Cisco IOS Gatekeeper

---

This chapter describes the main functions of a gatekeeper and includes the following sections:

- [Zone and Subnet Configuration, page 2-1](#)
- [Terminal Name Registration, page 2-1](#)
- [Inter-Zone Communication, page 2-2](#)
- [Accounting Using RADIUS/TACACS+, page 2-2](#)
- [Inter-Zone Routing, page 2-2](#)

Cisco offers a Voice over IP gatekeeper called the Multimedia Conference Manager, which is an H.323-compliant program implemented as part of the Cisco IOS software. The Multimedia Conference Manager software can run on Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 Multiservice Access Concentrators.

### Zone and Subnet Configuration

A zone is defined as the set of H.323 nodes controlled by a single gatekeeper. Gatekeepers co-existing on a network can be configured so that they register endpoints from different subnets.

Endpoints attempt to discover a gatekeeper, and consequently what zone they are members of, using the RAS message protocol. The protocol supports a discovery message that can be sent multicast or unicast.

If the message is sent multicast, the endpoint registers nondeterministically with the first gatekeeper to respond. Any endpoint on a subnet that is not enabled for the gatekeeper is not accepted as a member of that gatekeeper's zone. If the gatekeeper receives a discovery message from such an endpoint, it sends an explicit reject message.

### Terminal Name Registration

Gatekeepers recognize one of the following types of terminal aliases, or terminal names:

- H.323 identifiers (IDs), which are arbitrary, case-sensitive text strings.
- E.164 addresses, which are telephone numbers.
- E-mail IDs.

If an H.323 network deploys inter-zone communication, each terminal should at least have a fully-qualified e-mail name as its H.323 ID. For example, *bob@cisco.com*. The domain name of the e-mail ID should be the same as the configured domain name for the gatekeeper of which it is a member. As in the previous example, the domain name is *cisco.com*.

## Inter-Zone Communication

To allow endpoints to communicate between zones, gatekeepers must be able to determine which zone an endpoint is in and locate the gatekeeper responsible for that zone. If DNS is available, you can associate a DNS domain name to each gatekeeper.

## Accounting Using RADIUS/TACACS+

If you enable AAA on the gatekeeper, the gatekeeper emits an accounting record each time an endpoint registers or unregisters, or each time a call is admitted or disconnected.

## Inter-Zone Routing

There are three types of address destinations used in H.323 calls. The destination can be specified using either an H.323-ID address (a character string), an E.164 address (a string containing telephone keypad characters), or an e-mail ID (a character string). The way inter-zone calls are routed by the Cisco IOS Gatekeeper depends on the type of address being used.

- When using H.323-ID addresses, inter-zone routing is handled through the use of domain names. For example, to resolve the domain name *bob@cisco.com*, the source endpoint's gatekeeper finds the gatekeeper for *cisco.com* and sends the location request for target address *bob@cisco.com* to that gatekeeper. The destination gatekeeper looks in its registration database, sees *bob* registered, and returns the appropriate IP address to get to *bob*.




---

**Note** Although H.225 does not require the use of a domain name with H.323 IDs, the Cisco IOS Gatekeeper does require a domain name.

---

- When using E.164 addresses, call routing is handled through means of zone prefixes and gateway type prefixes, also referred to as technology prefixes. The zone prefixes, which are typically area codes, serve the same purpose as domain names in H.323-ID address routing. Unlike domain names, however, more than one zone prefix can be assigned to one gatekeeper, but the same prefix cannot be shared by more than one gatekeeper. With Cisco IOS Release 12.0(3)T and later, you can configure inter-zone routing using E.164 addresses.
- When using e-mail IDs, inter-zone routing is handled through the use of domain names—just as it is with H.323 IDs. Again, the source endpoint's gatekeeper finds the gatekeeper for the specified domain and sends the location request for the target address to that gatekeeper.



# Implementing an External Interface to the Cisco IOS Gatekeeper

This chapter describes how to implement an external interface to the Cisco IOS Gatekeeper and contains the following sections:

- [How the External Interface Works, page 3-1](#)
- [How Gatekeeper Triggers Work, page 3-2](#)
- [How RAS Messages are Processed, page 3-7](#)
- [How Security Works, page 3-10](#)
- [GKTMP Message Examples, page 3-11](#)
- [How the API Works, page 3-14](#)
- [Gatekeeper API Examples, page 3-16](#)

Although the Cisco IOS Gatekeeper provides many functions, there might be the occasion when additional function is desired or needed. For example, an organization could require additional authentication functions, need to implement specific policy controls, or want to use Internet call waiting.

The Gatekeeper Transaction Message Protocol (GKTMP) and the gatekeeper application programming interface (API) were developed to allow communication between the Cisco IOS Gatekeeper and an external application.

GKTMP is based on RAS and provides a set of ASCII request/response messages that can be used to exchange information between the Cisco IOS Gatekeeper and the external application over a TCP connection, and through the use of the gatekeeper API.

The gatekeeper API is object code that contains the API functions, which are designed to work with GKTMP. An external application links with the object code and calls the functions as necessary.

Using the GKTMP and the gatekeeper API, organizations can supplement the functions of the Cisco IOS Gatekeeper with their own external application.

## How the External Interface Works

As part of its normal function, a gatekeeper receives certain RAS registration, admission, location, resource, and disengage messages from H.323 endpoints. Typically, the gatekeeper processes these messages and responds to the request. However, with the Cisco IOS Gatekeeper, the GKTMP, and the gatekeeper API, you can supplement or offload the processing of the request to an external application.

In general, the process works as follows:

1. You establish triggers for each external application on the Cisco IOS Gatekeeper. These triggers are based on RAS tags and values.
2. When the Cisco IOS Gatekeeper receives a RAS message from an H.323 endpoint, it compares the message to the triggers.
3. If there is a match, the Cisco IOS Gatekeeper repackages the contents of the RAS message and sends it to the appropriate external application.
4. The gatekeeper API decodes the byte stream and creates a usable C structure.
5. The external application processes the data and sends the results back to the gatekeeper API.
6. The gatekeeper API encodes the response message and sends the data to the Cisco IOS Gatekeeper.
7. The Cisco IOS Gatekeeper performs any additional processing, if necessary, and forwards the results to the requesting H.323 endpoint.

The interaction between the Cisco IOS Gatekeeper and the external application is completely transparent to the H.323 endpoint.

Communication between the Cisco IOS Gatekeeper and the external application is over a TCP connection through the gatekeeper API. Multiple Cisco IOS Gatekeepers can be configured on a single Cisco IOS router as logical gatekeepers. The same TCP connection can be used by all the logical Cisco IOS Gatekeepers. The individual Cisco IOS Gatekeepers are identified by their gatekeeper IDs. This ID is included in all messages that the Cisco IOS Gatekeeper sends to the external application and in all responses that the external application sends back to the Cisco IOS Gatekeeper. If there are different external applications running on the same host, messages to the different external applications can also be multiplexed on the same TCP connection. The external applications are identified by their server IDs.

## How Gatekeeper Triggers Work

By default, the Cisco IOS Gatekeeper does not forward any RAS messages to any external applications. If an application is interested in receiving certain RAS messages, it must register this interest with the Cisco IOS Gatekeeper. To determine which RAS messages the Cisco IOS Gatekeeper forwards to the external application, you can specify trigger parameters. If the Cisco IOS Gatekeeper receives a message that satisfies the specified trigger conditions, the message is forwarded to the external application.

If multiple trigger conditions are specified in a single registration message, the Cisco IOS Gatekeeper treats the trigger conditions as “OR” conditions. In other words, if a RAS message received by the gatekeeper meets any of the trigger conditions the message is sent to the external application.

Trigger conditions are optional. If the Cisco IOS Gatekeeper receives a registration that contains no trigger conditions, it forwards all messages of the specified RAS message type to the external application.

If the Cisco IOS Gatekeeper has a registration for a RAS message type and receives another registration for the same RAS message from the same external application with the same priority, the Cisco IOS Gatekeeper uses the new registration and discards the previous one. The Cisco IOS Gatekeeper allows registrations for the same RAS message type with the same priority from multiple servers.

To indicate that the external application is no longer interested in a message, it must unregister its interest. The contents of the unregistration message must match that of the corresponding registration message before the trigger can be removed.

A Cisco IOS Gatekeeper can be statically (through a command-line interface) or dynamically (through the gatekeeper API) configured with trigger parameters.

**Note**

Triggers that are statically configured can be removed only through the command-line interface. Likewise, those triggers that are dynamically configured can be removed or modified only through the gatekeeper API.

## Statically Configured Triggers

Statically configured triggers are established on the router using Cisco IOS commands. To configure triggers using the Cisco IOS command line, do the following:

- 
- Step 1** Access the Cisco IOS Gatekeeper configuration mode. Enter the following command:
- ```
gatekeeper
```
- Step 2** Enter the trigger configuration mode and specify the RAS message type for the trigger. Enter the following command:
- ```
server trigger {arq | lcf | lrj | lrq | rrq | urq | rai | drq | brq} gkid priority  
server-id server-ip_address server-port
```
- Step 3** If the trigger is to send qualifying messages on a notification-only basis, enter the following command:
- ```
info-only
```
- Step 4** If you want to limit the qualifying messages based on the destination information, enter the following command:
- ```
destination-info {e164 | email-id | h323-id} value
```
- You can repeat this command to enter multiple destinations. This command cannot be used with an RAI message trigger.
- Step 5** If you want to limit the qualifying messages based on the redirect reason, enter the following command:
- ```
redirect-reason value
```
- You can repeat this command to enter multiple redirect reasons. This command cannot be used with an RAI message trigger.
- Step 6** If you want to limit the qualifying messages based on the remote extension address, enter the following command:
- ```
remote-ext-address value
```
- You can repeat this command to enter multiple remote extension addresses.
- Step 7** If you want to limit the qualifying messages based on the endpoint type, enter the following command:
- ```
endpoint-type value
```
- You can repeat this command to enter multiple endpoint types. This command cannot be used with a DRQ message trigger.
- Step 8** If you want to limit the qualifying messages based on the supported prefix, enter the following command:
- ```
supported-prefix value
```

You can repeat this command to enter multiple supported prefixes. This command cannot be used with a DRQ message trigger.

**Step 9** When you have specified all the parameters for this trigger, exit trigger submode by entering the following command:

```
exit
```

**Step 10** Repeat steps [Step 2](#) through [Step 9](#) for each trigger that you want to define.

**Step 11** If you want to change the server timeout value for triggers, enter the following command:

```
timer server timeout value
```

To remove a trigger, use the **no server trigger** command. To temporarily suspend a trigger, enter the trigger configuration mode, as described in [step 2](#) and enter the **shutdown** subcommand.

---

For more information about the Cisco IOS commands for configuring triggers, see [Chapter 6, “GKTMP Command Reference.”](#)



**Note**

With statically configured triggers, the gatekeeper initiates the connection to the external application and keeps the connection open for as long as it is running. If the connection is terminated by the external application, the Cisco IOS Gatekeeper periodically attempts to re-establish the connection.

---

## Dynamically Configured Triggers

Dynamically configured triggers are established using the gatekeeper API and the GKTMP trigger registration messages.

1. The external application creates a trigger and sends it to the Cisco IOS Gatekeeper using the WriteRegisterMessage API function. The triggers are sent in the format for trigger registration messages as prescribed by the GKTMP.
2. In response, the Cisco IOS Gatekeeper sends a message back that indicates whether the registration request has been accepted.

You must send a separate registration message for each message type that you want sent to the external application. If you send a registration message that does not contain any trigger definitions, all messages of the specified type are sent to the external application.

Dynamically configured triggers are removed using the WriteUnregisterMessage API function and GKTMP trigger unregistration messages. Again, the response from the Cisco IOS Gatekeeper indicates whether the unregistration request has been accepted.

## API Functions

You can use the following API functions to dynamically configure triggers:

- WriteRegisterMessage—Sends a registration message to the Cisco IOS Gatekeeper. This function reads the information in the GK\_REGISTER\_MSG\_TYPE structure and sends the contents to the Cisco IOS Gatekeeper using the gkHandle read from the GKAPI SOCK\_INFO\_T structure. The header structure, REGISTER\_REQUEST\_HEADER\_TYPE, within each message structure must

contain information for the From, To, and Priority fields. Optionally, if the external application is interested in receiving only notification of a message (not in processing any data for the message), the `notificationOnly` field should be set to `True`. Otherwise, it is set to `False`.

If no filter conditions are to be sent, the parameters within the registration structure should be set to their initialization values or to `NULL` for pointers. `WriteRegisterMessage` processes the filters for sending until it reaches the first initialization value for the parameter, or the first null pointer for pointer types.

- `WriteUnregisterMessage`—Sends an unregistration message to the Cisco IOS Gatekeeper. This function reads the information in the `GK_REGISTER_MSG_TYPE` structure and sends the contents to the Cisco IOS Gatekeeper using the `gkHandle` read from the `GKAPI_SOCKET_INFO_T` structure. The header structure, `REGISTER_REQUEST_HEADER_TYPE`, within each message structure must contain information for the From, To, and Priority fields.

## GKTMP Messages

The format of the GKTMP registration/unregistration request and response messages is as follows:

```
Message line
Message header line 1
Message header line 2
Message header line x

Message body line 1
Message body line 2
Message body line x
```

The request and response messages contain the following fields:

- `Message line`—A single line indicating whether this message is a `REGISTRATION` or `UNREGISTRATION` request from the external application. This line is echoed in the response from the Cisco IOS Gatekeeper. The format is `REGISTER xxx` or `UNREGISTER xxx`.
- `Message header`—A series of lines indicating the server ID of the external application, the gatekeeper ID of the Cisco IOS Gatekeeper, and the priority of the trigger. The priority indicates the order in which this trigger should be processed with respect to other triggers. The message header also includes a version ID, which indicates the version of the GKTMP. The version ID must be the first header in every GKTMP message.

For trigger registration requests, if the message contains a body, the header can also contain a line indicating the content length of the body. The message header might also contain a line that indicates whether the external application only wants to be notified of the specified RAS messages that the Cisco IOS Gatekeeper receives. For more information on notification only, see the [“Notification-Only Triggers” section on page 3-7](#).

For trigger registration and unregistration responses, the header also contains a line that indicates the status of the registration or unregistration request.

The format of each line is *field:value*.

- An empty line.
- `Message body (optional)`—The body of trigger registration messages contains the RAS tags and values that define the desired triggering parameters. Each triggering parameter occupies a single line. The format of each line is *tag=value*.

The message body can be included only in trigger registration requests. Trigger registration responses and trigger unregistration requests and responses cannot contain a message body.

For more information about the format of trigger registration and unregistration messages, see [Chapter 4, “GKTMP Messages.”](#)

With dynamically configured triggers, the external application establishes a TCP connection to the gatekeeper and registers its interest in any of the RAS message types. The external application should then leave the connection open for receiving such messages and for sending its responses. If the external application closes the connection, its registrations are considered cancelled. The Cisco IOS Gatekeeper does not attempt to re-establish the connection.

## Example of a Dynamic Trigger Registration Message

In the following example the trigger registration request indicates that the Cisco IOS Gatekeeper should forward to the external application any RRQ messages from a voice gateway or a gateway with a supported prefix of 1# or 2#:

```
REGISTER RRQ
Version-id: 100
From: server-12
To: gk-dallas1
Priority: 20
Notification-Only:
Content-Length: 29
```

```
t=voice-gateway
p=1#
p=2#
```

## Specifying Wildcards in Triggers

Within a trigger, certain wildcard characters are allowed for an alias-address field that contains an E.164 address. Trigger criteria for E.164 alias-addresses can include trailing wildcard characters as follows:

- One or more periods can be used, each denoting a single character
- An asterisk can be used to denote zero or more characters.

Examples of legal E164 address patterns are:

1800.....	The digits 1800 followed by seven characters.
011*	The digits 011 followed by any number of characters.

Examples of illegal E164 address patterns are:

...4567	Wildcard characters must be used as trailing characters. They cannot be used at the beginning of a field.
4802*2	Wildcard characters cannot be used within a field. In this case, the asterisk is interpreted as a literal character.

## Notification-Only Triggers

If the application needs to be aware of messages but will not be performing any processing of the message, you can indicate that the messages should be forwarded on a notification-only basis. If notification-only is present in a GKTMP registration message (which means that notification-only is set to true at the API), the Cisco IOS Gatekeeper forwards messages that meet the trigger criteria but does not expect a response. If notification-only is not present (which means that notification-only is set to false at the API), the Cisco IOS Gatekeeper forwards messages that meet the trigger criteria and awaits a corresponding RESPONSE message from the external application.

This header line is typically used for REQUEST RRQ and REQUEST URQ messages, so that the Cisco IOS Gatekeeper can populate an external application's registration database.

## How RAS Messages are Processed

When the Cisco IOS Gatekeeper receives an RAS message that meets the specified trigger conditions, it packages the contents of the fields of the RAS message into the message body of a GKTMP REQUEST message. When the external application receives a request, it must package the response into the message body of a GKTMP RESPONSE message.

The GKTMP specifies formats for exchanging the following types of RAS messages:

- RRQ—Registration request
- RCF—Registration confirm
- RRJ—Registration reject
- URQ—Unregistration request
- ARQ—Admission request
- ACF—Admission confirm
- ARJ—Admission reject
- LRQ—Location request
- LCF—Location confirm
- LRJ—Location reject
- RIP—Request in progress
- RAI—Resource availability indication
- DRQ—Disengage request
- BRQ—Bandwidth request
- BCF—Bandwidth confirm
- BRJ—Bandwidth reject
- IRR—Information request

The URQ, RAI, and DRQ messages are issued as a request from the Cisco IOS Gatekeeper, but do not have a corresponding response. Other messages (RCF, RRJ, ACF, ARJ, BCF, and BRJ) are sent only as responses from the external application. Using Command URQ, an application server can send an unsolicited, untriggered URQ message to the Gatekeeper to unregister an endpoint.

**Note**

The Cisco IOS Gatekeeper does not generate GKTMP Request RRQ messages for lightweight RRQ messages, which are used by H.323 endpoints as a keep-alive mechanism to refresh existing registrations.

The general format of the GKTMP RAS messages is:

```
Message line
Message header line 1
Message header line 2
Message header line x
```

```
Message body line 1
Message body line 2
Message body line x
```

These messages include the following fields:

- **Message line**—A single line indicating whether this message is a REQUEST or RESPONSE. The format is REQUEST *xxx* or RESPONSE *xxx*.
- **Message header**—A series of lines indicating the server ID of the external application and the gatekeeper ID of the Cisco IOS Gatekeeper. The message header also includes a version ID, which indicates the version of the GKTMP. The version ID must be the first header in every GKTMP message.

If the message contains a body, the header can also contain a line indicating the content length of the body. The header can also contain a transaction ID, which uniquely identifies the request/response message. The message header might also contain a line that indicates whether the message is being sent on a notification-only basis. For more information on notification only, see the “[Notification-Only Triggers](#)” section on page 3-7.

The format of each line is *field:value*.

- An empty line.
- **Message body (optional)**—The body of trigger registration messages contains the RAS tags and values for the corresponding RAS message. The tags included in the body vary depending on the type of RAS message. Responses from the external application should contain only changed or new body information. The format of each line is *tag=value*.

For more information about the format of GKTMP RAS messages, see [Chapter 4, “GKTMP Messages.”](#)

How the external application processes requests from the Cisco IOS Gatekeeper depends on the type of RAS message and how the external application has been configured to respond.

**Note**

The Cisco IOS Gatekeeper maintains a timeout value for the processing of requests. If a response is not received within the timeout value, the Cisco IOS Gatekeeper assumes the external application is unavailable. Therefore, when the external application receives a message that will take additional time to process, it should send a message back to the Cisco IOS Gatekeeper to request an extension to the timeout. This message is a RESPONSE RIP.

## Processing of xRQ Requests

When the external application receives a REQUEST xRQ message from the Cisco IOS Gatekeeper it must take one of the following actions:

- Instruct the Cisco IOS Gatekeeper to reject the request. In this case, the external application sends a RESPONSE xRJ message to the Cisco IOS Gatekeeper.
- Modify one or more of the fields and return the request to the Cisco IOS Gatekeeper for further processing. In this case, the external application sends a RESPONSE xRQ message with the altered information in the body. Only fields that the external application changes can be included in the body. Unchanged fields must not be present in the response message body.
- Indicate no interest in the message and instruct the gatekeeper to continue normal processing. In this case, the external application sends a RESPONSE xRQ message with a null message body.
- Complete the processing of the request and send the results to the Cisco IOS Gatekeeper. In this case, the external application sends a RESPONSE xCF message. The body of this message must contain all the fields that the Cisco IOS Gatekeeper needs to respond with an xCF to the client. This message indicates to the gatekeeper that no further processing is required. If multiple triggers have been configured such that the REQUEST is sent to more than one external application, the RESPONSE xCF preempts any other external applications from receiving this message.
- Send no response. This action must be taken only if the request message contains the line Notification-Only: in the header.

## Processing of LCF Requests

An LCF message is sent by a peer gatekeeper to confirm the location of a destination endpoint in its zone. You can configure the Cisco IOS Gatekeeper to forward any LCF messages that it receives to the external application. This gives the application an opportunity to alter any of the fields in the confirmation.

When the external application receives a REQUEST LCF message from the Cisco IOS Gatekeeper, the application must take one of the following actions:

- Confirm the information contained in the request. In this case, the external application sends a RESPONSE LCF with a null message body.
- Alter the information contained in the request. In this case, the external application sends a RESPONSE LCF message with the altered information in the message body. Only fields that the external application changes can be included in the body. Unchanged fields must not be present in the response message body.
- Reject the information contained in the LCF. In this case, the external application sends a RESPONSE LRJ.

## Processing of LRJ Requests

An LRJ message is sent by a peer gatekeeper to reject the location of a destination endpoint, meaning the endpoint does not exist in the peer gatekeeper's zone. You can configure the Cisco IOS Gatekeeper to forward to the external application any LRJ messages that it receives. This gives the external application an opportunity to recommend an alternate destination.

When the external application receives a REQUEST LRJ message from the Cisco IOS Gatekeeper it must take one of the following actions:

- Accept the LRJ. In this case, the external application sends a RESPONSE LRJ with a null message body.

- Suggest an alternate destination. In this case, the external application sends a RESPONSE LCF message with the altered information in the message body. Only fields that the external application changes can be included in the body. Unchanged fields must not be present in the response message body.

## How Security Works

The GKTMP supports the use of CryptoH323Tokens for authentication. The CryptoH323Token is defined in H.225 Version 2 and is used in a “password with hashing” security scheme as described in section 10.3.3 of the H.235 specification.

A cryptoToken can be included in any RAS message and is used to authenticate the sender of the message. The use of cryptoTokens allows you to use a separate database for user ID and password verification.

## CryptoTokens and Cisco Gateways

Cisco gateways support the following levels of authentication:

- Registration—Tokens are generated for RRQ and URQ messages.
- Per-Call—Tokens are generated for ARQ messages.
- All—Tokens are generated for RRQ, URQ, and ARQ messages.

You can configure the level of authentication for the gateway using the Cisco IOS software command-line interface.

CryptoTokens for RRQ, URQ, and the terminating side of ARQ messages contain information about the gateway that generated the token, including the gateway ID (which is the H.323 ID configured on the gateway) and the gateway password. CryptoTokens for the originating side ARQ messages contain information about the user that is placing the call, including the user ID and personal identification number (PIN).

Therefore, if you want to use cryptoTokens for authentication, all clients in your network must include a cryptoToken in every message that they send to the Cisco IOS Gatekeeper.

## Requirements for using CryptoTokens

To participate in this authentication scheme, a GKTMP-based application must have the following:

- Access to a database of user IDs, gateway IDs, and their associated passwords.
- Access to an ASN.1 encoder.

The application should be set up to authenticate the messages that you deem necessary. If you want to authenticate gateways when they register, your application should validate RRQ messages. If you want per-call authentication, your application should validate ARQ messages. Or, you can have your application validate all messages.

## Validating a CryptoToken

To validate a cryptoToken received in a RAS message, the application should:

1. Use the alias in the cryptoToken to look up the associated password.

2. Use the password, the timestamp, and the alias, to ASN.1 encode a ClearToken. The ClearToken is a PwdCertToken. The application should maintain the password and alias as NULL-terminated strings and include the NULL when performing the ASN.1 encoding.
3. Perform an MD5 Hash on the ASN.1 encoded buffer. This results in a 16-byte Hash.
4. Compare the calculated Hash with the one found in the token field of the cryptoEPPwdHash.

If the hash values match, the application should issue a confirmation message (xCF) to the gatekeeper, which is transmitted to the gateway. Otherwise, the application should send a rejection message (xRJ) with a reject reason of securityDenial.

## CryptoTokens in RAS Messages

The cryptoToken message body line contains a type identifier followed by a colon and a sequence of space separated tag=value parameters that are associated with the particular type of cryptoToken.

For example, a message body line containing a cryptoToken could look like the following:

```
$=E:a=H:gw1-rtp T=940647784 h=FFABCD0067AE12436780167364847343
```

For more information about the parameters included in cryptoTokens, see [Chapter 4, “GKTMP Messages.”](#)

## GKTMP Message Examples

The following examples show the GKTMP messages that are generated in some uses of the external interface.

### Populating an External Application’s Registration Database

An external application might need to maintain a database of active gateways so that it can select gateways for ARQ or LRQ resolution. In this case, triggers can be configured on the Cisco IOS Gatekeepers so that any RRQ or URQ messages will be forwarded to the external application on a notification-only basis. [Example 3-1](#) shows an RRQ notification for a gateway. [Example 3-2](#) shows a URQ notification for a gateway.

#### **Example 3-1 RRQ Notification**

```
REQUEST RRQ
Version-id: 100
From: gk1-sj
Notification-only:
Content-Length:90

c=I:171.69.136.205:1720
r=I:171.69.136.205:16523
a=H:gw3-sj
t=voice-gateway
p=2# 99#
```

#### **Example 3-2 URQ Notification**

```
REQUEST URQ
Version-id: 100
```

```

From: gk1-sj
Notification-only:
Content-Length:23

c=I:171.69.136.205:1720

```

## 800 Number Lookup

You might want the Cisco IOS Gatekeeper to forward ARQs to an external application to determine the mapping for an 800 number. [Example 3-3](#) shows an ARQ request from the Cisco IOS Gatekeeper. [Example 3-4](#) shows the corresponding response from the external application.

### **Example 3-3 Gatekeeper Request**

```

REQUEST ARQ
Version-id: 100
From: gk1-sj
Transaction-Id: 5de04245
Content-Length: 127

s=E:4085552132
d=E:8005721234
b=560
A=f
m=t
c=f81d4fae-7dec-11d0-a765-00a0c91e6bf6
C=f81d4fae-7dec-11d0-a765-00a0c91e6bf6

```

### **Example 3-4 External Application Response**

```

RESPONSE ARQ
Version-id: 100
To: gk1-sj
Transaction-Id: 5de04245
Content-Length:14

d=E:4155551212

```

## Internet Call-Waiting

If you have an internet call-waiting (ICW) server in your network, you might want configure the Cisco IOS Gatekeeper to forward all LRQ requests to the ICW server. [Example 3-5](#) shows the LRQ request from the Cisco IOS Gatekeeper.

### **Example 3-5 Gatekeeper LRQ Request**

```

REQUEST LRQ
Version-id: 100
From: gk1-sj
Transaction-Id: 5de04246
Content-Length:64

s=H:gk3-la
d=E:4085551111
p=0
c=4085552222

```

If the ICW server determines that the destination (4085551111) is not a subscriber, it sends back a RESPONSE LRQ with a null message body. The Cisco IOS Gatekeeper then proceeds with normal processing. [Example 3-6](#) shows the response.

**Example 3-6 Null Response**

```
RESPONSE LRQ
Version-id: 100
To: gk1-sj
Transaction-Id: 5de04246
```

If the ICW server determines that the destination (4085551111) is a subscriber and is currently logged on, it pings the subscriber to determine how the call should be handled. Because this can take several seconds, the ICW server first sends a RESPONSE RIP to the Cisco IOS Gatekeeper asking for a 60-second extension to the timeout. [Example 3-7](#) shows the response.

**Example 3-7 RIP Response**

```
RESPONSE RIP
Version-id: 100
To: gk1-sj
Transaction-Id: 5de04246
Content-Length:7

d=60000
```

If the subscriber refuses the call, the ICW server sends a rejection to the Cisco IOS Gatekeeper. [Example 3-8](#) shows the response.

**Example 3-8 Rejection**

```
RESPONSE LRJ
Version-id: 100
To: gk1-sj
Transaction-Id: 5de04246
Content-Length:15

R=requestDenied
```

If the subscriber hangs up to accept the call, the ICW server sends a RESPONSE LRQ with a null message body, which instructs the Cisco IOS Gatekeeper to proceed with the call. [Example 3-9](#) shows the response.

**Example 3-9 Null Response**

```
RESPONSE LRQ
Version-id: 100
To: gk1-sj
Transaction-Id: 5de04246
```

If the subscriber chooses to route the call to voicemail (4085553333) and the ICW server knows the IP address of the voicemail gateway (172.45.63.49), the server instructs the Cisco IOS Gatekeeper to route the call to the voicemail system. [Example 3-10](#) shows the response.

**Example 3-10 Response to Reroute**

```

RESPONSE LCF
Version-id: 100
To: gk1-sj
Transaction-Id: 5de04246
Content-Length:94

d=E:4085553333
D=I:172.45.63.49:1720
r=I:172.45.63.49:13982
t=voice-gateway
X=4085551111

```

## How the API Works

The gatekeeper API is offered as a library that contains the API functions, which are designed to work with GKTMP. An external application must link with the GKAPI object code and call the API functions to communicate with the Cisco IOS Gatekeeper.

The GKAPI includes the following files:

- gk\_api—The gatekeeper API object code.
- gk\_api.h—The gatekeeper API interface header file, which must be included by the application.

The gatekeeper API provides functions and structures that allow an external application to obtain data from and return information to the Cisco IOS Gatekeeper. Using the API functions and structures, as well as some standard functions, the external client application:

1. Establishes a connection with the Cisco IOS Gatekeeper using the GkapiSetupClient function.
2. Monitors the appropriate socket using a standard function.
3. When a connect complete is detected, the application notifies the gatekeeper API using the GkapiClientConnected function.
4. When a read message is detected, it allocates memory for the storage of the message using the GetReadMsgBuffer function.
5. Stores the contents of the message in the appropriate structure using the ReadMsgBuffer function.

**Note**

If the message received from the Cisco IOS Gatekeeper is a RAS message that is not supported by the API function, the msgType will be set to MSG\_NOT\_SUPPORTED. If a response is required, an appropriate response will be constructed by the API function and sent to the Cisco IOS Gatekeeper. The header information in the UNSUPPORTED\_MSG\_TYPE structure will be filled in by the API function. This situation could occur if the Cisco IOS Gatekeeper has been upgraded to support new messages but the API function has not been correspondingly upgraded.

If the message received from the Cisco IOS Gatekeeper, is not recognized by the API function, the msgType will be set to UNKNOWN\_MSG and the STATUS\_TYPE will be set to MSG\_READ\_ERROR. In this case, the external application should close the connection to the Cisco IOS Gatekeeper by calling the CloseGateKeeperConnection function.

If the application has specified the use of non-blocking I/O, the GkapiSetupClient and ReadMsgBuffer functions can return with a CONNECT\_IN\_PROGRESS or INCOMPLETE\_MSG\_READ error. These errors indicate that either the connection setup is still in progress or a complete GKTMP message has not been received. If either of these errors is returned, additional socket events will indicate the further

processing and completion of these requests. The application should *not* call `CloseGateKeeperConnection` in these conditions. Instead, the application must monitor the socket using the appropriate handles to detect the additional socket events.

6. Obtains the data from the structure and performs the processing as designed.
7. Frees the memory allocated for the read message using the `FreeReadMsgBuffer` function.
8. Writes the resulting data to the appropriate structure using the `WriteResponseMsg` function.

The external application can repeat these steps as often as necessary. If a read error is encountered or if the external application wants to terminate the connection to the Cisco IOS Gatekeeper, the application should use the `CloseGateKeeperConnection` function.

The API functions and structures are described in [Chapter 5, “Gatekeeper API Functions and Structures.”](#)

## Linking with the Gatekeeper API

As stated earlier, an external application must be linked with the GKAPI object code and call the API functions in order to communicate with the Cisco IOS Gatekeeper. If you have an external application to use with the gatekeeper API and GKTMP, be sure that you link you it with the gatekeeper API library.

The following is an example makefile for building an application using the GNU “C” compiler and linking with the gatekeeper API library.

This sample makefile is bundled with the GKAPI binary and the header file and can be extracted from the GK software .tar file on the Cisco.com website. The sample file can be modified and used to meet the individual requirements of the end user.

```
rm -f gkapiver.c
echo \#ifndef GKAPI_MAX_VER_STR_LEN >>gkapiver.c
echo \#define GKAPI_MAX_VER_STR_LEN 128 >>gkapiver.c
echo \#endif >>gkapiver.c
echo char version_string\[GKAPI_MAX_VER_STR_LEN\]= \"Compiled `date +%a
%d-%h-%y %H:%M` OS target: `uname -sr` \"; >>gkapiver.c
gcc -g -Wall -c gkapiver.c -o gkapiver
gcc -g gk_api gkapiver gk_application.c
/usr/lib/libintl.a -lsocket -lnsl -ldl -lthread
-lpthread -lposix4 -ogk_application
```

## Guidelines for Using the Gatekeeper API

When you are writing an application that uses the gatekeeper API, keep the following in mind:

- For response messages, the application must send *only* changed or new parameters. Any unchanged fields must not be included in the response message body. If unchanged fields are sent to the Cisco IOS Gatekeeper in a response message, the performance of the Cisco IOS Gatekeeper could be severely impacted.
- For messages received from the Cisco IOS Gatekeeper, the API function removes the tag fields. The type prefix (H:, E:, M: for alias-addresses and I: for transport-addresses) is preserved and is stored in the appropriate structure. The application must interpret the type of address based on the type prefix.
- For responses from the application, the application must insert the type prefix (H:, E:, M: for alias-addresses and I: for transport-addresses). The API function inserts the appropriate tag before constructing the response message.

- For sequence of parameters in messages received from the Cisco IOS Gatekeeper, the API function removes the tag field and stores the parameter in the appropriate structure in the same format as it was read—with the spaces included in the string.
- For sequence of parameters in responses from the application, the application must separate the parameters with spaces. The API function inserts the appropriate tag before constructing the response message.
- For register functions, “sequence of” parameters are not supported. However, the application can have multiple trigger conditions. This is limited by the maximum size of the array in the registration structures.
- The application is responsible for receiving all signals from the operating system. In order for the API function to detect a closed connection with the gatekeeper during a write operation (so that the STATUS\_TYPE can be set to TCP\_CONNECTION\_CLOSED), the application must install a signal handler for SIGPIPE.

## Gatekeeper API Examples

The following examples show how the gatekeeper API functions can be used in an external application. These examples are meant to illustrate how the API functions can be called. They are not examples of actual implementations of the API. Two examples are included in this section; one in which the application is the client and one in which the application is the server.



### Note

The examples that follow are cursory examples only and will not actually compile.

### Example 3-11 Client Example

```
#include "gk_api.h" /* API header file */
#include </usr/include/sys/fcntl.h>
#include </usr/include/sys/socket.h>
#include </usr/include/sys/select.h>
#include <signal.h>

#define APP_VER 1

void sig_int(int sigNo);
STATUS_TYPE BuildRRQRegisterMsg(GKAPI_SOCK_INFO_T *clientConnect);
STATUS_TYPE BuildRRQResponse(GK_READ_MSG_TYPE *ptr,
                             GKAPI_SOCK_INFO_T *connectPtr);

main()
{
    GKAPI_SOCK_INFO_T clientConnect;
    STATUS_TYPE status;
    GK_READ_MSG_TYPE *readMsgPtr;
    struct timeval tval;
    int conn_handle;
    int n;
    fd_set wset, rset;
    BOOLEAN read_pending = FALSE;

    readMsgPtr=NULL;

    /* Install signal handler for SIGPIPE */
    if (signal(SIGPIPE, sig_int) == SIG_ERR) {
```

```

    printf("error registering signal \n");
}

/* Open Connection to GateKeeper */
/* Fill in TCP port and IP address of GateKeeper */
clientConnect.IPAddress = inet_addr("111.222.111.222");
clientConnect.TCPPort=2000;

/* Setup the connection for nonblocking I/O */
conn_handle=GkapiSetupClient(&clientConnect, &status, TRUE);

/* Check status for errors */
/* If status == PROCESSING_SUCCESSFUL, no errors were encountered */
/* status == TCP_CONNECT_ERROR, error in connecting to GateKeeper */
/* status == TCP_HANDLE_ERROR, error in handle creation */
/* For error conditions, retry connecting to the GateKeeper */

/* Check for following errors:
 * status = MEM_ALLOC_FAIL
 *          INVALID_MSG_SPECIFIED
 *          INVALID_ENDPOINT_SPECIFIED
 *          INVALID_REDIRECT_REASON_SPECIFIED
 *          HEADER_INFO_INCOMPLETE
 *          NULL_POINTER_PASSED
 */

/* If status is PROCESSING_SUCCESSFUL or CONNECT_IN_PROGRESS,
wait for connect and read event */
if (status == CONNECT_IN_PROGRESS) {
    FD_ZERO(&rset);
    FD_SET(conn_handle, &rset);
    wset = rset;
    tval.tv_sec = 1;
    tval.tv_usec = 0;
    if ( (n = select(conn_handle + 1, &rset, &wset, NULL,
                    &tval)) == 0) {
        printf("\nApplication connect timed out");
        CloseGateKeeperConnection(&clientConnect);
        exit(1);
    }

    if (FD_ISSET(conn_handle, &rset) ||
        FD_ISSET(conn_handle, &wset)) {
        status = PROCESSING_SUCCESSFUL;
    } else {
        printf("\nSelect error");
        CloseGateKeeperConnection(&clientConnect);
        exit(1);
    }
}

/* If a connect event has occurred tell GKAPI so */
conn_handle = GkapiClientConnected(&clientConnect, &status, conn_handle);

/* If conn_handle is valid and */
/* If status is PROCESSING_SUCCESSFUL, register triggers if required */
/* Build an RRQ Register message */
status = BuildRRQRegisterMsg(&clientConnect);
/* Check status for errors */
/* If status == PROCESSING_SUCCESSFUL, no errors were encountered */
if ((status == TCP_WRITE_ERROR) || /* TCP error encountered */
    (status == TCP_CONNECTION_CLOSED)) { /* TCP connection closed */
    /* Close connection to GateKeeper and free system resources */
    CloseGateKeeperConnection(&clientConnect);
}

```

```

}

for(;;) {
    FD_ZERO(&rset);
    FD_SET(conn_handle, &rset);
    select(conn_handle + 1, &rset, NULL, NULL, NULL);
    printf("Select event occurred \n");
    if (FD_ISSET(conn_handle, &rset)) {

/* If a read event has occurred:
 * Allocate a read buffer
 * Call ReadMsgBuffer
 * Process Message
 * Build Response if required
 */
        if (!read_pending)
            readMsgPtr=GetReadMsgBuffer();

/* Check if readMsgPtr is NULL, if NULL, memory allocation failed. */
/* if readMsgPtr != NULL, continue */
        read_pending = FALSE;
        status=ReadMsgBuffer(&clientConnect, readMsgPtr);

/* Check status for errors */
/* If status == PROCESSING_SUCCESSFUL, no errors were encountered */
        if ((status == TCP_READ_ERROR) || /* TCP error encountered */
            (status == TCP_CONNECTION_CLOSED) || /* TCP connection closed */
            (status == MSG_READ_ERROR)) { /* Message not understood */
            /* Free the read buffer
             * Close connection to GateKeeper and free system resources
             */
            FreeReadMsgBuffer(readMsgPtr);
            CloseGateKeeperConnection(&clientConnect);
            /* Reopen connection to GateKeeper */
        }

/* Check for other error conditions:
 * status==MEM_ALLOC_FAIL
 * status==NULL_POINTER_PASSED
 */
        FreeReadMsgBuffer(readMsgPtr);

/* status==INCOMPLETE_MSG_READ */
/* Call ReadMsgBuffer on the next read event */
        if (status == INCOMPLETE_MSG_READ)
            read_pending = TRUE;

/* status == PROCESSING_SUCCESSFUL */
/* Extract message received */
        switch(readMsgPtr->msgType) {
            case RRQ_REQUEST_MSG:
                status=BuildRRQResponse(readMsgPtr, &clientConnect);
                /* Check status for errors.
                 * If TCP_WRITE_ERROR or TCP_CONNECTION_CLOSED
                 * call CloseGateKeeperConnection(&clientConnect)
                 * Reopen connection to GateKeeper.
                 * Check for other errors.
                 */
                FreeReadMsgBuffer(readMsgPtr);
                break;

```

```

        case ARQ_REQUEST_MSG:
            /* Do processing */
            FreeReadMsgBuffer(readMsgPtr);
            break;

        case MSG_NOT_SUPPORTED:
            FreeReadMsgBuffer(readMsgPtr);
            break;

        default:
            FreeReadMsgBuffer(readMsgPtr);
            break;
    }
}

STATUS_TYPE BuildRRQResponse(GK_READ_MSG_TYPE *ptr,
                             GKAPI SOCK_INFO_T *connectPtr)
{
    GK_WRITE_MSG_TYPE *writePtr;
    HEADER_INFO_TYPE *headerPtr;
    char buffer1[100];
    char buffer2[100];
    STATUS_TYPE status;

    headerPtr=&ptr->MESSAGE_TYPE.rrqReqMsg.headerInfo;
    /* allocate memory for writePtr, writePtr=malloc(...) */
    /* Fill in msgType and header information */
    writePtr->msgType=RRQ_RESPONSE_MSG;

    writePtr->WRITE_MESSAGE_TYPE.rrqRespMsg.headerInfo.versionId = APP_VER;
    strcpy(writePtr->WRITE_MESSAGE_TYPE.rrqRespMsg.headerInfo.from,
           headerPtr->to);
    strcpy(writePtr->WRITE_MESSAGE_TYPE.rrqRespMsg.headerInfo.to,
           headerPtr->from);
    strcpy(writePtr->WRITE_MESSAGE_TYPE.rrqRespMsg.headerInfo.
           transactionID, headerPtr->transactionID);

    /* Fill in paramters */
    strcpy(buffer1, "M:joe_smith");
    strcpy(buffer2, "1800");
    writePtr->WRITE_MESSAGE_TYPE.rrqRespMsg.terminalAlias=buffer1;
    writePtr->WRITE_MESSAGE_TYPE.rrqRespMsg.supportedPrefix=buffer2;

    /* Send message to GateKeeper */
    status=WriteResponseMsg(connectPtr, writePtr);
    /* If memory was allocated for writePtr, free(writePtr) */
    return(status);
}

STATUS_TYPE BuildRRQRegisterMsg(GKAPI SOCK_INFO_T *clientConnect)
{
    GK_REGISTER_MSG_TYPE *regPtr;
    STATUS_TYPE status;
    int i=0;
    char buffer1[20];

    /* Allocate memory for regPtr, regPtr=malloc(...) */
    /* After allocating memory:
     * Fill in header info and
     * message parameters if needed

```

```

    */

    /* Fill in message type */
    regPtr->msgType = RRQ_REGISTER_MSG;

    /* Fill in header info */
    regPtr->
        REGISTRATION_MESSAGE_TYPE.rrqRegMsg.headerInfo.versionId =
            APP_VER;
    strcpy(regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.headerInfo.from,
            "APPL 1");
    strcpy(regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.headerInfo.to,
            "GK 1");
    regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.headerInfo.notificationOnly
        =FALSE;

    /* Set priority */
    regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.headerInfo.priority=1;

    /* Specify filters for RRQ message */
    regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.terminalType[0] =
        VOICEGATEWAY;
    regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.terminalType[1] = MCU;

    for (i=2; i<MAX_NUM_ENDPOINT_TYPES; i++) {
        regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.terminalType[i] =
            ENDPOINT_INFO_NOT_RCVD;
    }

    strcpy(buffer1, "1#");
    regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.supportedPrefix[0]=buffer1;
    for (i=1; i< MAX_NUM_SUPPORTED_PREFIX; i++) {
        regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.supportedPrefix[i] = NULL;
    }
    /* Now gatekeeper will only send an RRQ message to the application
    * if filter conditions are satisfied.
    */
    status=WriteRegisterMessage(clientConnect, regPtr);
    /* If memory was allocated for regPtr, free(regPtr) */
    return(status);
}

STATUS_TYPE BuildRRQUnRegisterMsg(GKAPI_SOCK_INFO_T *clientConnect)
{
    GK_UNREGISTER_MSG_TYPE unRegMsg;
    STATUS_TYPE status;

    unRegMsg.versionId = APP_VER;
    strcpy(unRegMsg.from, "APPL 1");
    strcpy(unRegMsg.to, "GK 1");
    unRegMsg.unregisterMsg = RRQ_REGISTER_MSG;
    /* Set priority */
    unRegMsg.priority=1;

    status=WriteUnregisterMessage(clientConnect, &unRegMsg);
    return(status);
}

void sig_int(int sigNo)
{
    switch (sigNo) {
        case SIGPIPE:
            printf("SIGPIPE received\n");
            break;
    }
}

```

```

        /* case ... */
        default:
    }
}

```

### Example 3-12 Server Example

```

#include "gk_api.h" /* API header file */
#include </usr/include/sys/socket.h>
#include </usr/include/sys/select.h>
#include </usr/include/netinet/in.h>
#include </usr/include/sys/errno.h>
#include <signal.h>

typedef struct client_db_t_ {
    int handle;
    GK_READ_MSG_TYPE *buf;
    GKAPI SOCK_INFO_T *conn_info;
} client_db_t;

#define MAX_CLIENTS 1024
#define APP_VER 1

void sig_int(int sigNo);
STATUS_TYPE BuildRRQRegisterMsg(GKAPI SOCK_INFO_T *clientConnect);
STATUS_TYPE BuildRRQResponse(GK_READ_MSG_TYPE *ptr,
                             GKAPI SOCK_INFO_T *connectPtr);

main()
{
    GKAPI SOCK_INFO_T ServerInfo;
    GKAPI_TCP_ADDR_INFO_T client_addr;
    STATUS_TYPE status;
    GK_READ_MSG_TYPE *readMsgPtr;
    GKAPI SOCK_INFO_T *connInfo;
    client_db_t client[MAX_CLIENTS+1];
    int conn_handle, serverHandle, max_fd;
    int i, n;
    fd_set rset;
    BOOLEAN read_pending = FALSE;

    readMsgPtr=NULL;

    for (i=0; i<=MAX_CLIENTS; i++) {
        client[i].handle=0;
        client[i].buf=0;
        client[i].conn_info=0;
    }

    /* Install signal handler for SIGPIPE */
    if (signal(SIGPIPE, sig_int) == SIG_ERR) {
        printf("error registering signal \n");
    }

    /* Open Connection to GateKeeper */
    /* Fill in TCP port and IP address of Application */
    ServerInfo.IPAddress = inet_addr("111.222.111.222");
    ServerInfo.TCPPort=2000;

    /* Setup the connection for nonblocking I/O */
    serverHandle=GkapiSetupServer(&ServerInfo, &status, TRUE);

    /* Check status for errors */

```

```

/* If the serverHandle < 0, there was an error. Check status for
/* for the error code.
/* If status == TCP_CONNECT_ERROR, error in connecting to GateKeeper */
/* status == TCP_BIND_ERROR, error in connecting to Gatekeeper */
/* status == TCP_LISTEN_ERROR, error in connecting to Gatekeeper */
/* status == TCP_NONBLOCK_ERROR, error setting up for */
/* nonblocking connection */
/* status == TCP_HANDLE_ERROR, error in handle creation */
/* For error conditions, quit */
if (serverHandle < 0)
    exit(1);

/* Set up select mask with the server's handle to listen for
* incoming connections.
*/

max_fd = serverHandle;

FD_ZERO(&rset);
FD_SET(serverHandle, &rset);

for ( ; ; ) {
    /* If status is PROCESSING_SUCCESSFUL wait for incoming connections
    * and read events */
    n = select(max_fd + 1, &rset, NULL, NULL, NULL);

    /* If the select event has occurred on the server handle,
    * it is a new incoming connection.
    */
    if (FD_ISSET(serverHandle, &rset)) {
        connInfo = (GKAPI SOCK_INFO_T *)malloc(sizeof(GKAPI SOCK_INFO_T));
        connInfo->TCPPort = ServerInfo.TCPPort;
        connInfo->IPAddress = ServerInfo.IPAddress;
        conn_handle = GkapiAcceptConnection(connInfo, &status,
            serverHandle, &client_addr);
        /* If conn_handle < 0, there is an error. Ignore and continue to
        * to process other select events.
        * If conn_handle is valid, add new connection
        * to select read list
        */
        FD_SET(conn_handle, &rset);

        /* Setup the max file descriptor we need to select on */
        if (conn_handle > max_fd)
            max_fd = conn_handle;

        /* Add this new connection to list of active connections */
        for (i=0; i<MAX_CLIENTS; i++) {
            if (client[i].handle == 0) {
                client[i].handle = conn_handle;
                client[i].buf = 0;
                client[i].conn_info = connInfo;
            }
        }

        /* The application set GK triggers for this connection at
        * this point.
        */
    }

    /*
    * Check to see if the select event is a read occurring
    * on one of the existing connections. If so, have GKAPI process the
    * received buffer.

```

```

*/
for (i=0; n>0,i<=MAX_CLIENTS; i++,n--) {
    if (client[i].handle <= 0)
        continue;

    if (FD_ISSET(client[i].handle, &rset)) {
        if (client[i].buf == 0) {
            readMsgPtr=GetReadMsgBuffer();
        } else {
            readMsgPtr=client[i].buf;
        }
    }

    /* If a read event has occurred:
    * Allocate a read buffer if it isn't a pending read.
    * Call ReadMsgBuffer
    * Process Message
    * Build Response if required
    */
    if(readMsgPtr != NULL) {
        status=ReadMsgBuffer(client[i].conn_info, readMsgPtr);

        /* Check if readMsgPtr is NULL, if NULL,
        * memory allocation failed.
        */
        /* if readMsgPtr != NULL, continue */
        if(status == PROCESSING_SUCCESSFUL) {
            client[i].buf = 0;
            /* Process the Message */
            /* Extract message received */
            switch(readMsgPtr->msgType) {
                case RRQ_REQUEST_MSG:
                    status=BuildRRQResponse(readMsgPtr, &ServerInfo);
                    /* Check status for errors.
                    * If TCP_WRITE_ERROR or TCP_CONNECTION_CLOSED
                    * call CloseGateKeeperConnection(&ServerInfo)
                    * Reopen connection to GateKeeper.
                    * Check for other errors.
                    */
                    FreeReadMsgBuffer(readMsgPtr);
                    break;

                case ARQ_REQUEST_MSG:
                    /* Do processing */
                    FreeReadMsgBuffer(readMsgPtr);
                    break;

                case MSG_NOT_SUPPORTED:
                    FreeReadMsgBuffer(readMsgPtr);
                    break;

                default:
                    FreeReadMsgBuffer(readMsgPtr);
                    break;
            }
        }

        /* End of status == PROCESSING_SUCCESSFUL */

        /* Check status for errors */

        if ((status == TCP_READ_ERROR) || /* TCP error encountered */
            (status == TCP_CONNECTION_CLOSED) || /*connection closed*/
            (status == MSG_READ_ERROR)) { /* Message not understood */
            /* Free the read buffer
            * Close connection to GateKeeper and

```

```

        * free system resources
        */
        FreeReadMsgBuffer(readMsgPtr);
        CloseGateKeeperConnection(client[i].conn_info);
        /* Reopen connection to GateKeeper */
    }

    /* Check for other error conditions:
    * status==MEM_ALLOC_FAIL
    * status==NULL_POINTER_PASSED
    */
    FreeReadMsgBuffer(readMsgPtr);

    /* status==INCOMPLETE_MSG_READ */
    /* Call ReadMsgBuffer on the next read event */
    if (status == INCOMPLETE_MSG_READ)
        client[i].buf = readMsgPtr;
    }
}
}
}

STATUS_TYPE BuildRRQResponse(GK_READ_MSG_TYPE *ptr,
                             GKAPI SOCK_INFO_T *connectPtr)
{
    GK_WRITE_MSG_TYPE *writePtr;
    HEADER_INFO_TYPE *headerPtr;
    char buffer1[100];
    char buffer2[100];
    STATUS_TYPE status;

    headerPtr=&ptr->MESSAGE_TYPE.rrqReqMsg.headerInfo;
    /* allocate memory for writePtr, writePtr=malloc(...) */
    /* Fill in msgType and header information */
    writePtr->msgType=RRQ_RESPONSE_MSG;

    writePtr->WRITE_MESSAGE_TYPE.rrqRespMsg.headerInfo.versionId = APP_VER;
    strcpy(writePtr->WRITE_MESSAGE_TYPE.rrqRespMsg.headerInfo.from,
           headerPtr->to);
    strcpy(writePtr->WRITE_MESSAGE_TYPE.rrqRespMsg.headerInfo.to,
           headerPtr->from);
    strcpy(writePtr->WRITE_MESSAGE_TYPE.rrqRespMsg.headerInfo.
           transactionID, headerPtr->transactionID);

    /* Fill in parameters */
    strcpy(buffer1, "M:joe_smith");
    strcpy(buffer2, "1800");
    writePtr->WRITE_MESSAGE_TYPE.rrqRespMsg.terminalAlias=buffer1;
    writePtr->WRITE_MESSAGE_TYPE.rrqRespMsg.supportedPrefix=buffer2;

    /* Send message to GateKeeper */
    status=WriteResponseMsg(connectPtr, writePtr);
    /* If memory was allocated for writePtr, free(writePtr) */
    return(status);
}

STATUS_TYPE BuildRRQRegisterMsg(GKAPI SOCK_INFO_T *ServerInfo)
{
    GK_REGISTER_MSG_TYPE *regPtr;
    STATUS_TYPE status;

```

```

int i=0;
char buffer1[20];

/* Allocate memory for regPtr, regPtr=malloc(...) */
/* After allocating memory:
 * Fill in header info and
 * message parameters if needed
 */

/* Fill in message type */
regPtr->msgType = RRQ_REGISTER_MSG;

/* Fill in header info */
regPtr->
REGISTRATION_MESSAGE_TYPE.rrqRegMsg.headerInfo.versionId =
APP_VER;
strcpy(regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.headerInfo.from,
"APPL 1");
strcpy(regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.headerInfo.to,
"GK 1");
regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.headerInfo.notificationOnly
=FALSE;

/* Set priority */
regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.headerInfo.priority=1;

/* Specify filters for RRQ message */
regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.terminalType[0] =
VOICEGATEWAY;
regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.terminalType[1] = MCU;

for (i=2; i<MAX_NUM_ENDPOINT_TYPES; i++) {
regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.terminalType[i] =
ENDPOINT_INFO_NOT_RCVD;
}

strcpy(buffer1, "1#");
regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.supportedPrefix[0]=buffer1;
for (i=1; i< MAX_NUM_SUPPORTED_PREFIX; i++) {
regPtr->REGISTRATION_MESSAGE_TYPE.rrqRegMsg.supportedPrefix[i] = NULL;
}
/* Now gatekeeper will only send an RRQ message to the application
 * if filter conditions are satisfied.
 */
status=WriteRegisterMessage(ServerInfo, regPtr);
/* If memory was allocated for regPtr, free(regPtr) */
return(status);
}

STATUS_TYPE BuildRRQUnRegisterMsg(GKAPI_SOCKET_INFO_T *ServerInfo)
{
GK_UNREGISTER_MSG_TYPE unRegMsg;
STATUS_TYPE status;

unRegMsg.versionId = APP_VER;
strcpy(unRegMsg.from, "APPL 1");
strcpy(unRegMsg.to, "GK 1");
unRegMsg.unregisterMsg = RRQ_REGISTER_MSG;
/* Set priority */
unRegMsg.priority=1;

status=WriteUnregisterMessage(ServerInfo, &unRegMsg);
return(status);
}

```

```
void sig_int(int sigNo)
{
    switch (sigNo) {
        case SIGPIPE:
            printf("SIGPIPE received\n");
            break;

            /* case ... */
        default:
    }
}
```



## GKTMP Messages

---

This chapter describes GKTMP messages and contains the following sections:

- [GKTMP RAS Messages, page 4-1](#)
- [Trigger Registration Messages, page 4-25](#)

The GKTMP messages are used for communication between the Cisco IOS Gatekeeper and the external application. There are two types of GKTMP messages:

- [GKTMP RAS Messages](#)—Used to exchange the contents RAS messages between the Cisco IOS Gatekeeper and the external application.
- [Trigger Registration Messages](#)—Used by the external application to indicate to the Cisco IOS Gatekeeper which RAS message should be forwarded.

## GKTMP RAS Messages

The general format of all GKTMP RAS messages is as follows:

- Single message line
- One or more message header lines
- Blank line, which separates the message header from the message body
- Zero or more message body lines

### Message Line

Each GKTMP RAS message is either a request or a response. Requests are generated by the Cisco IOS Gatekeeper and responses are generated by the external application.

The first line of each GKTMP RAS message sent by the Cisco IOS Gatekeeper uses the format:

```
REQUEST RAS_message_type
```

The first line of each GKTMP RAS message sent by the external application uses the format:

```
RESPONSE RAS_message_type
```

Possible RAS message types are as follows:

- RRQ—Registration request
- RCF—Registration confirm

- RRJ—Registration reject
- URQ—Unregistration request
- ARQ—Admission request
- ACF—Admission confirm
- ARJ—Admission reject
- LRQ—Location request
- LCF—Location confirm
- LRJ—Location reject
- RIP—Request in progress
- DRQ—Disengage request
- RAI—Resource availability information
- BRQ—Bandwidth request
- BCF—Bandwidth confirm
- BRJ—Bandwidth reject
- IRR—Information request

**Note**

The Cisco IOS Gatekeeper does not generate GKTMP Request RRQ messages for lightweight RRQ messages, which are used by H.323 endpoints as a keep-alive mechanism to refresh existing registrations.

## Message Header

The message line is immediately followed by the message header. Each message header contains a field name and a value, separated by a colon (*field:value*). [Table 4-1](#) shows the possible fields:

**Table 4-1 Message Header Fields**

Field Names	Field Values
Version-Id	Version of the protocol that the sender is running. The version ID consists of a major number (gk_major) and a minor number (gk_minor). For example, version 1 is represented as 100.
From	String that identifies the originator of the message. For requests from the Cisco IOS Gatekeeper, this field contains the gatekeeper ID. For responses from the external application, this field contains the server ID.
To	String that identifies the receiver of the message. For requests from the Cisco IOS Gatekeeper, this field contains the server ID. For responses from the external application, this field contains the ID of the gatekeeper that initiated the request.
Content-Length	Number of octets contained in the message body. If the message body is null, this field can be omitted.

**Table 4-1 Message Header Fields**

Field Names	Field Values
Transaction-Id	String that identifies the transaction. If this field is present in the request from the Cisco IOS Gatekeeper, it must be echoed in the response from the external application.
Notification-Only	None. No value is included after the colon. If this field name is present, it indicates to the external application no response should be sent. Request URQ must contain this field. Also, Request RRQ contains this field when that message is used to populate the external application's registration database.

The message header is followed immediately by a blank line.

## Message Body

The message body follows the blank line. Each line in the message body contains a tag and a value, separated by an equal sign (*tag=value*). The tags are case-sensitive and denote an RAS message field. The possible tags depend on the GKTMP RAS message.



### Note

If the message body is null, the message must terminate with a CRFL after the message header.

In some cases, depending on the field type, the value is preceded a value-type identifier followed by a colon (*tag=type:value*).

Possible field types are as follows:

- **Alias-Address**—This type of field can contain a series of addresses separated by spaces. Each is preceded by a value-type identifier that indicates the type of address. H indicates that the address is an H.323 ID; E indicates that the address is an E.164 address; M indicates that the address is an e-mail ID.
- **Transport-Address**—This type of field contains an address. Currently, only one value-type identifier is possible for this field type. That is I, which indicates that the address is an IP version 4 address. The address is specified in dotted-decimal notation and can be followed by a colon and a port number.
- **Endpoint-Type**—This type of field indicates the type of endpoint. Possible values are: gatekeeper, terminal, mcu, proxy, voice-gateway, h320-gateway, and other-gateway.
- **Supported-Prefix**—This type of field indicates a supported technology prefix. Possible values are the digits 0 through 9 and the pound sign (#).
- **Globally-Unique-Identifier (GUID)**—This type of field contains the 16-octet conference ID or call ID that uniquely identifies the call or conference. The IDs are specified in hexadecimal format.
- **Bandwidth**—This type of field contains an unsigned integer from 0 through 4294967295 that indicates the bandwidth in 100 bits per second.
- **Boolean**—This type of field contains a single character. T or t for true; F or f for false.
- **IA5 String**—This type of field contains characters from the International Alphabet 5 (IA5), which is a character set defined by the ITU X.400 Message Handling System specification.

- **cryptoToken**—This type of field contains one of the cryptoToken types defined for the CryptoH323Token field specified in H.225. Currently, the only type of cryptoToken supported is the cryptoEPPwdHash.
- **HASHED-EncodedPwdCertToken**—This type of field contains a 16 octet IA5String. It represents the RAS Message Digest 5 (MD5) hashed encoded PwdCertToken.
- **TimeStamp**—This type of field contains a 32-bit integer that represents Universal Time Coordinated (UTC) time.
- **OBJECT-IDENTIFIER**—This type of field contains a sequence of non-negative integer values separated by dots, which is used to uniquely identify an object.
- **UseSpecifiedTransport**—This type of field contains a string that indicates the transport layer that is used for the signaling: Annex E/UDP or TCP.
- **AlternateGK**—This type of field contains a set of fields enclosed in braces ( { } ). Each field is identified by a tag and separated from the other fields by SP (ASCII space, 0x20) characters. This field can contain more than one set of fields, each enclosed by braces.
- **AlternateEndpoint**—This type of field contains a set of fields enclosed in braces. Each field is identified by a tag and separated from the other fields by SP (ASCII space, 0x20) characters. A message body line containing an AlternateEndpoint field must pertain to a single endpoint. Multiple call signal addresses and tokens that pertain to the same endpoint can be provided in a single message body line. If there are multiple AlternateEndpoints, each pertaining to a different H.323 endpoint, the information about the alternate endpoints must be provided in separate message body lines.
- **AlternateTransportAddress**—This type of field contains a single sub-field enclosed in braces. The fields within the braces pertain to a single instance of a RAS AlternateTransportAddress structure. They are defined as a Transport-Address and are encoded as defined for the Transport-Address field.
- **clearToken**—This type of field contains a set of fields enclosed in braces. Each field is identified by a tag and separated from the other fields by SP (ASCII space, 0x20) characters. The fields within the braces pertain to a single instance of a RAS ClearToken structure. However, the message line of a clearToken field can contain multiple instances, each enclosed in braces and separated by a space character. The clearToken field can be embedded within an AlternateEndpoint field.
- **remoteZone**—This type of field contains a set of fields enclosed in braces. Each field is identified by a tag and separated from the other fields by SP (ASCII space, 0x20) characters. The fields within the braces pertain to a single instance of a remoteZone structure. However, the message line of a remoteZone field can contain multiple instances, each enclosed in braces and separated by a space character.

This section describes the possible fields for each message. When the external application sends a response, it includes only the fields that it has altered. Unaltered fields must not be included.

## Registration Messages

Registration messages are used to control which H.323 endpoints are in the gatekeeper's zone.

This section describes the following:

- [Request RRQ](#)
- [Response RRQ](#)
- [Response RCF](#)
- [Response RRJ](#)

## Request RRQ

This message is sent from the Cisco IOS Gatekeeper to the external application when an H.323 endpoint wants to join the zone. This message can be used to populate the external application's registration database. In this case, the request is sent as a notification only and no response is expected from the external application.

Table 4-2 shows the possible Request RRQ tags:

**Table 4-2 Request RRQ Tags**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
c	Transport-Address	Mandatory	RRQ:callSignalAddress. See <a href="#">Transport-Address</a> .
r	Transport-Address	Mandatory	RRQ:rasAddress. See <a href="#">Transport-Address</a> .
a	Alias-Address	Optional	RRQ:terminalAlias
t	Endpoint-Type	Mandatory	RRQ:terminalType
p	Supported-Prefix	Optional	RRQ:terminalType:gateway:protocol:*:supportedPrefixes
\$	cryptoToken	Optional	RRQ:cryptoTokens. See <a href="#">CryptoToken</a> .
T	clearToken	Optional	RRQ:tokens. See <a href="#">ClearToken</a> .
C	Boolean	Optional	RRQ:callCapacityReportingCapability
K	CallCapacity	Optional	RRQ:capacity. See <a href="#">CallCapacity</a> .

## Response RRQ

This message is sent from the external application to the Cisco IOS Gatekeeper in response to a Request RRQ message. If the external application has no interest in the Request RRQ message, it returns a Response RRQ with a null body. Otherwise, the external application modifies the fields as appropriate and sends the response with the updated information to the Cisco IOS Gatekeeper for further processing.

For Response RRQ, the possible tags are shown in Table 4-3:

**Table 4-3 Response RRQ Tags**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
a	Alias-Address	Optional	RRQ:terminalAlias
p	Supported-Prefix	Optional	RRQ:terminalType:gateway:protocol:*:supportedPrefixes
F	Boolean	Optional	Do not propagate this message onward.

## Response RCF

This message is sent from the external application to the Cisco IOS Gatekeeper in response to a Request RRQ. This message indicates that the external application has completed the processing of the request.

For Response RCF, the possible tags are shown in Table 4-4:

**Table 4-4 Response RCF Tags**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
a	Alias-Address	Optional	RRQ:terminalAlias
p	Supported-Prefix	Optional	RRQ:terminalType:gateway:protocol: *:supportedPrefixes
G	AlternateGK	Optional	RCF:alternateGatekeeper. See <a href="#">AlternateGK</a> .

## Response RRJ

This message is sent from the external application to the Cisco IOS Gatekeeper in response to a Request RRQ. It indicates that the Cisco IOS Gatekeeper should reject the request for the specified reason.

For Response RRJ, the possible tag is shown in [Table 4-5](#):

**Table 4-5 Response RRJ Tag**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
R	RRJ-Reason	Mandatory	RRJ:rejectReason

Possible values for the rejectReason are:

- undefinedReason
- securityDenial
- resourceUnavailable
- discoveryRequired
- invalidRevision
- invalidCallSignalAddress
- invalidRASAddress
- duplicateAlias
- invalidTerminalType
- transportNotSupported
- transportQOSNotSupported
- invalidAlias
- fullRegistrationRequired
- additiveRegistrationNotSupported
- invalidTerminalAlias
- genericDataReason

## Unregistration Message

Unregistration messages are used to remove an H.323 endpoint from a gatekeeper zone.

This section describes the following:

- [Request URQ](#)
- [Command URQ](#)
- [Result URQ](#)

### Request URQ

This message is sent from the Cisco IOS Gatekeeper to the external application when the H.323 endpoint wants to leave the zone or when its registration expires. This request is sent as a notification only. No response is generated by the external application.

For Request URQ, the possible tag is shown in [Table 4-6](#):

**Table 4-6 Request URQ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
c	Transport-Address	Mandatory	URQ:callSignalAddress. See <a href="#">Transport-Address</a> .

### Command URQ

The Command URQ message is sent from the application server to the gatekeeper at any time to unregister an endpoint. The gatekeeper sends a URQ message to the endpoint and removes it from its registration database. The endpoint is identified by its call signaling address (IP address and port). The server can also specify an optional reason and alternate gatekeeper information.

[Table 4-7](#) shows the new Command URQ tags:

**Table 4-7 New Command URQ Tags**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
c	Transport-Address	Mandatory	URQ:callSignalAddress. See <a href="#">Transport-Address</a> .
R	URQ-Reason	Optional	URQ:reason
G	AlternateGK	Optional	URQ:alternateGatekeeper. See <a href="#">AlternateGK</a> .

Possible values for the reason are:

- reregistrationRequired
- ttlExpired
- securityDenial
- undefinedReason

## Result URQ

The Result URQ message is sent from the gatekeeper to the application server to report the result of a Command URQ transaction as long as the command did not specify *Notification-Only*: in the message header. The endpoint is identified by its call signaling address (IP address and port).

If the endpoint was found and unregistered, the message header indicates *Status: success*. Otherwise it indicates *Status: invalidGKID* or *Status: invalidEndpoint*.



### Note

Success just means that a URQ message was sent to the endpoint and that it was removed from the gatekeeper registration database without error. It does not mean that a UCF message was received from the endpoint. The gatekeeper does not wait to receive a UCF message before sending the Result URQ message to the server.

Table 4-8 shows the new Result URQ tags:

**Table 4-8 New Result URQ Tags**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
c	Transport-Address	Mandatory	URQ:callSignalAddress. See <a href="#">Transport-Address</a> .

## Admission Messages

Admission messages are used to control which H.323 endpoints can participate in calls.

This section describes the following:

- [Request ARQ](#)
- [Response ARQ](#)
- [Response ACF](#)
- [Response ARJ](#)

## Request ARQ

This message is sent from the Cisco IOS Gatekeeper to the external application when an H.323 endpoint wants to initiate a call.

For Request ARQ, the possible tags are shown in [Table 4-9](#):

**Table 4-9 Request ARQ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
s	Alias-Address	Mandatory	ARQ:srcInfo
S	Transport-Address	Optional	ARQ:srcCallSignalAddress. See <a href="#">Transport-Address</a> .
d	Alias-Address	Optional	ARQ:destinationInfo
D	Transport-Address	Optional	ARQ:destCallSignalAddress. See <a href="#">Transport-Address</a> .
x	Alias-Address	Optional	ARQ:destExtraCallInfo

Table 4-9 Request ARQ (continued)

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
b	Bandwidth	Mandatory	ARQ:bandWidth
A	Boolean	Mandatory	ARQ:answerCall
c	GUID	Optional	ARQ:callIdentifier
C	GUID	Mandatory	ARQ:conferenceID
m	Boolean	Optional	ARQ:canMapAlias
e	IA5String	Optional	ARQ:nonStandardData:redirectNumber
E	integer	Optional	ARQ:nonStandardData:redirectReason <sup>1</sup>
p	integer	Optional	ARQ:nonStandardData:callingPartyNumOctet3a <sup>2</sup>
w	IA5string	Optional	ARQ:nonStandardData:displayIE
i	TransportAddress	Mandatory	arqing-endpoint identifier <sup>3</sup>
\$	cryptoToken	Optional	ARQ:cryptoTokens. See <a href="#">CryptoToken</a> .
T	clearToken	Optional	ARQ:tokens. See <a href="#">ClearToken</a> .
B	IA5string	Optional	ARQ:nonStandardData:interfaceSpecific:BillingInfo
g	GTD	Optional	ARQ:nonStandardData:gtd. See <a href="#">GTD</a> .
I	IA5String	Optional	ARQ:nonStandardData:interfaceDescriptor
J	IA5String	Optional	ARQ:circuitInfo:destinationCircuitID:group
K	callCapacity	Optional	ARQ:capacity. See <a href="#">CallCapacity</a> .
L	IA5String	Optional	ARQ:circuitInfo:sourceCircuitID:group
P	IA5String	Optional	ARQ:circuitInfo:sourceCircuitID:group
Q	IA5String	Optional	ARQ:circuitInfo:destinationCircuitID:group
U	IA5String	Optional	ARQ:tokens:cisco_IZCT_OID:IZCToken:izctSrcZone
W	IA5String	Optional	ARQ:tokens:cisco_IZCT_OID:IZCToken:izctDstZone
V	Integer	Optional	ARQ:nonStandardInfo:reRouteCount
v	IA5 String	Optional	ARQ:nonStandardInfo:terminationCause:releaseCompleteCauseIE

Possible values for the redirectReason are:

- 0—Unknown
- 1—Call forwarding busy or called DTE busy
- 2—Call forwarded, no reply
- 4—Call deflection
- 9—Called DTE out of order
- 10—Call forwarding by the called DTE
- 15—Call forwarding unconditional or systematic call redirection

CallingPartyNumOctet3a is from the Q.931 Setup octet 3a of calling party number.

When an H.323 endpoint sends an ARQ to the Cisco IOS Gatekeeper, it includes its endpointIdentifier. Because this value is local and has meaning to the Cisco IOS Gatekeeper only and not to the external application, the Cisco IOS Gatekeeper substitutes a more meaningful value of CallSignalAddress in its Request ARQ messages.

## Response ARQ

This message is sent from the external application to the Cisco IOS Gatekeeper in response to a Request ARQ message. If the external application has no interest in the Request ARQ message, it returns a Response ARQ with a null body. Otherwise, it modifies the fields as appropriate and sends the response with the updated information to the Cisco IOS Gatekeeper for further processing.

For Response ARQ, the possible tags are shown in [Table 4-10](#):

**Table 4-10 Response ARQ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
d	Alias-Address	Optional	ARQ:destinationInfo
D	Transport-Address	Optional	ARQ:destCallSignalAddress. See <a href="#">Transport-Address</a> .
x	Alias-Address	Optional	ARQ:destExtraCallInfo
b	Bandwidth	Optional	ARQ:bandWidth
e	IA5String	Optional	ARQ:nonStandardData:redirectNumber
E	integer	Optional	ARQ:nonStandardData:redirectReason
w	IA5string	Optional	ARQ:nonStandardData:displayIE
z	remoteZone	Optional	None. See <a href="#">RemoteZone</a> .
T	clearToken	Optional	ARQ:tokens. See <a href="#">ClearToken</a> .
c	integer	Optional	None <sup>1</sup>
p	integer	Optional	None <sup>2</sup>
A	alternateEndpoint	Optional	ARQ:alternateEndpoints
g	GTD	Optional	ARQ:nonStandardData:gtd. See <a href="#">GTD</a> .
I	IA5String	Optional	ARQ:circuitInfo:sourceCircuitID:group
J	carrierInfo	Optional	See <a href="#">CarrierInfo</a> .
F	Boolean	Optional	Do not propagate this message onward.
s	Alias-Address	Optional	ARQ:srcInfo. See <a href="#">Alias-Address</a> .
P	IA5String	Optional	ARQ:circuitInfo:sourceCircuitID:group
Q	trunkGroupInfo	Optional	See <a href="#">TrunkGroupInfo</a> .
y	ServiceControlSession	Optional	ACF:ServiceControlSession. See <a href="#">ServiceControlSession</a> .

1. Reflects the cost value of the primary endpoint, if any, whose address is returned in the 'D' field of this message. It should only be sent if the endpoint is filled in.
2. Reflects the priority value of the primary endpoint, if any whose address is returned in the 'D' field of this message. It should only be sent if the endpoint is filled in.

The external application has the option of reducing the bandwidth.

If this field is included, the Cisco IOS Gatekeeper sends LRQs to all the listed zones. The zone with the least cost and highest priority that returns and LCF is chosen for inclusion in the ACF that is sent to the endpoint.

If the message contains an alternateEndpoint field, the additional fields shown in [Table 4-11](#) are included:

**Table 4-11 Additional Fields**

Tag	Field Type	Mandatory or Optional	Description
C	Integer	Optional	Cost value associated with the zone
p	Integer	Optional	Priority value associated with the zone
c	Transport-Address	Mandatory	alternateEndpoints:callSignalAddress. See <a href="#">Transport-Address</a> .
J	IA5string	Optional	CarrierId
Q	IA5string	Optional	TrunkGroupLabel
T	clear-Token	Optional	alternateEndpoints:tokens

## Response ACF

This message is sent from the external application to the Cisco IOS Gatekeeper in response to a Request ARQ. The message indicates that the external application has completed the processing of the request.

For Response ACF, the possible tags are shown in [Table 4-12](#):

**Table 4-12 Response ACF**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
d	Alias-Address	Optional	ACF:destinationInfo
D	Transport-Address	Mandatory	ACF:destCallSignalAddress. See <a href="#">Transport-Address</a> .
x	Alias-Address	Optional	ACF:destExtraCallInfo
X	Alias-Address	Optional	ACF:remoteExtensionAddress
b	Bandwidth	Optional	ARQ:bandWidth
t	Endpoint-type	Optional	ACF:destinationType
T	ClearToken	Optional	ACF:tokens. See <a href="#">ClearToken</a> .
A	AlternateEndpoint	Optional	ACF:alternateEndpoints
N	AlternateTransportAddr	Optional	ACF:alternateTransportAddress
u	useSpecifiedTransport	Optional	ACF:useSpecifiedAddress. See <a href="#">Message Body</a> .
g	GTD	Optional	ACF:nonStandardData:gtd:gtdData. See <a href="#">GTD</a> .
s	Service-Descriptor	Optional	ACF:nonStandardData:serviceDescriptor
y	ServiceControlSession	Optional	ACF:ServiceControlSession. See <a href="#">ServiceControlSession</a> .

**Table 4-12 Response ACF (continued)**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
J	carrierInfo	Optional	See <a href="#">CarrierInfo</a> .
Q	trunkGroupInfo	Optional	See <a href="#">TrunkGroupInfo</a> .

If the message contains an AlternateEndpoint field, the additional fields shown in [Table 4-13](#) are included:

**Table 4-13 Additional Fields**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
c	Transport-Address	Mandatory	alternateEndpoints:callSignalAddress. See <a href="#">Transport-Address</a> .
T	clearToken	Optional	alternateEndpoints:tokens. See <a href="#">ClearToken</a> .
C	Integer	Optional	None <sup>1</sup>
p	Integer	Optional	None <sup>1</sup>
J	IA5string	Optional	CarrierId
Q	IA5string	Optional	TrunkGroupLabel

1. The 'C' and 'p' parameters define the associated cost and priority of using this endpoint. The Gatekeeper merges the endpoints in order of their cost/priority and present an ordered list. Remote endpoints, if any (obtained by sending LRQs), are assigned the cost value of the zone and merged accordingly.

If the message contains an AlternateTransportAddr field, the additional field shown in [Table 4-14](#) is included:

**Table 4-14 Additional Field**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
I	Transport-Address	Mandatory	IP address and port for Annex E. See <a href="#">Transport-Address</a> .

## Response ARJ

This message is sent from the external application to the Cisco IOS Gatekeeper in response to a Request ARQ. The message indicates that the Cisco IOS Gatekeeper should reject the request for the specified reason.

For Response ARJ, the possible tag is shown in [Table 4-15](#):

**Table 4-15 Response ARJ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
R	ARJ-Reason	Mandatory	ARJ:rejectReason
y	ServiceControlSession	Optional	ACF:ServiceControlSession. See <a href="#">ServiceControlSession</a> .
v	IA5String	Optional	ARJ:terminationCause:releaseCompleteCauseIE <sup>1</sup>

1. This field is included if the GKTMP server wishes to provide a Q.850 cause code that it wants to be used to release the call.

Possible values for rejectReason are:

- calledPartyNotRegistered
- invalidPermission
- requestDenied
- undefinedReason
- resourceUnavailable
- securityDenial
- carrierIdUnspecified (maps to undefinedReason)
- carrierIdUnknown (maps to undefinedReason)
- ingressCarrierInactive (maps to undefinedReason)
- carrierOrigPcntExceeded (maps to undefinedReason)
- carrierMaxUnitsExceeded (maps to undefinedReason)
- destinationUnknown (maps to undefinedReason)
- noRouteAvailable (maps to undefinedReason)
- callerNotRegistered
- routeCallToGatekeeper
- invalidEndpointID
- qosControlNotSupported
- incompleteAddress
- aliasesInconsistent
- routeCallToSCN
- exceedsCallCapacity
- collectDestination
- collectPin
- genericDataReason
- neededFeatureNotSupported

## Location Messages

Location messages are used by gatekeepers to communicate with each other to process interzone calls.

This section describes the following:

- [Request LRQ](#)
- [Response LRQ](#)
- [Request LCF](#)
- [Response LCF](#)
- [Request LRJ](#)
- [Response LRJ](#)

### Request LRQ

This message is sent from the Cisco IOS Gatekeeper to the external application when the Cisco IOS Gatekeeper has received an interzone location request.

For Request LRQ, the possible tags are shown in [Table 4-16](#):

**Table 4-16 Request LRQ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
s	Alias-Address	Optional	LRQ:srcInfo
d	Alias-Address	Mandatory	LRQ:destinationInfo
e	IA5String	Optional	LRQ:nonStandardData:redirectNumber
E	integer	Optional	LRQ:nonStandardData:redirectReason <sup>1</sup>
p	integer	Optional	LRQ:nonStandardData:callingPartyNumOctet3a <sup>2</sup>
w	IA5String	Optional	LRQ:nonStandardData:displayIE
c	IA5String	Optional	LRQ:nonStandardData:callingPartyNum
T	clearToken	Optional	LRQ:tokens. See <a href="#">ClearToken</a> .
g	GTD	Optional	LRQ:nonStandardData:gtd. See <a href="#">GTD</a> .
I	IA5String	Optional	LRQ:nonStandardData:interfaceDescriptor
J	IA5String	Optional	LRQ:circuitInfo:destinationCircuitID:group
L	IA5String	Optional	LRQ:circuitInfo:sourceCarrierID:group
b	Integer	Optional	LRQ:nonStandardData:bandwidth
C	IA5String	Optional	LRQ:nonStandardData:callIdentifier
P	IA5String	Optional	LRQ:circuitInfo:sourceCircuitID:group
Q	IA5String	Optional	LRQ:circuitInfo:destinationCircuitID:group
S	IA5String	Optional	LRQ:tokens:cisco_IZCT_OID:IZCTToken:izctSrcZone
D	IA5String	Optional	LRQ:tokens:cisco_IZCT_OID:IZCTToken:izctDstZone
i	FromReplyAddress	Optional	See <a href="#">FromReplyAddress</a> .

**Table 4-16 Request LRQ (continued)**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
V	Integer	Optional	ARQ:nonStandardInfo:reRouteCount
v	IA5 String	Optional	ARQ:nonStandardInfo:terminationCause: releaseCompleteCauseIE

Possible values for the redirectReason are:

- 0—Unknown
- 1—Call forwarding busy or called DTE busy
- 2—Call forwarded, no reply
- 4—Call deflection
- 9—Called DTE out of order
- 10—Call forwarding by the called DTE
- 15—Call forwarding unconditional or systematic call redirection

CallingPartyNumOctet3a is from the Q.931 Setup octet 3a of calling party number.

## Response LRQ

This message is sent from the external application to the Cisco IOS Gatekeeper in response to a Request LRQ message. If the external application has no interest in the Request LRQ message, it returns a Response LRQ with a null body. Otherwise, it modifies the fields as appropriate and sends the response with the updated information to the Cisco IOS Gatekeeper for further processing.

For Response LRQ, the possible tags are shown in [Table 4-17](#):

**Table 4-17 Response LRQ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
d	Alias-Address	Optional	LRQ:destinationInfo
z	remoteZone	Optional	None. See <a href="#">RemoteZone</a> .
T	clearToken	Optional	ARQ:tokens. See <a href="#">ClearToken</a> .
c	integer	Optional	None <sup>1</sup>
p	integer	Optional	None <sup>2</sup>
A	alternateEndpoint	Optional	ARQ:alternateEndpoints
g	GTD	Optional	LRQ:nonStandardData:gtd. See <a href="#">GTD</a> .
I	IA5String	Optional	LRQ:circuitInfo:sourceCircuitID:group
J	carrierInfo	Optional	See <a href="#">CarrierInfo</a> .
F	Boolean	Optional	Do not propagate this message onward.
s	Alias-Address	Optional	LRQ:srcInfo. See <a href="#">Alias-Address</a> .

**Table 4-17 Response LRQ (continued)**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
Q	trunkGroupInfo	Optional	See <a href="#">TrunkGroupInfo</a> .
P	IA5String	Optional	LRQ:circuitInfo:sourceCircuitID:group

1. Reflects the cost value of the primary endpoint, if any, whose address is returned in the 'D' field of this message. It should only be sent if the endpoint is filled in.
2. Reflects the priority value of the primary endpoint, if any whose address is returned in the 'D' field of this message. It should only be sent if the endpoint is filled in.

If the message contains an alternateEndpoint field, the additional fields shown in [Table 4-18](#) are included:

**Table 4-18 Additional Fields**

Tag	Field Type	Mandatory or Optional	Description
C	Integer	Optional	Cost value associated with the zone
p	Integer	Optional	Priority value associated with the zone
c	Transport-Address	Mandatory	alternateEndpoints:callSignalAddress. See <a href="#">Transport-Address</a> .
J	IA5string	Optional	CarrierId
Q	IA5string	Optional	TrunkGroupLabel
T	clear-Token	Optional	alternateEndpoints:tokens

## Request LCF

This message is sent from the Cisco IOS Gatekeeper to the external application when the Cisco IOS Gatekeeper has received an LCF from the remote Cisco IOS Gatekeeper. This gives the external application an opportunity to accept (Response LCF), modify (Response LCF), or reject (Response LRJ) the information contained in the LCF.

For Request LCF, the possible tags are shown in [Table 4-19](#):

**Table 4-19 Request LCF**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
s	Alias-Address	Optional	LRQ:srcInfo
e	IA5String	Optional	LRQ:nonStandardData:redirectNumber
E	integer	Optional	LRQ:nonStandardData:redirectReason
p	integer	Optional	LRQ:nonStandardData:callingPartyNumOctet3a
w	IA5String	Optional	LRQ:nonStandardData:displayIE
c	IA5String	Optional	LRQ:nonStandardData:callingPartyNum
d	Alias-Address	Mandatory	LRQ/LCF:destinationInfo
D	Transport-Address	Mandatory	LCF:callSignalAddress. See <a href="#">Transport-Address</a> .
r	Transport-Address	Mandatory	LCF:rasAddress. See <a href="#">Transport-Address</a> .
x	Alias-Address	Optional	LCF:destExtraCallInfo
X	Alias-Address	Optional	LCF:remoteExtensionAddress
t	Endpoint-Type	Optional	LCF:destinationType
N	AlternateTransportAddr	Optional	LCF:AlternateTransportAddress
u	useSpecifiedTransport	Optional	ACF:useSpecifiedAddress
T	clearToken	Optional	LCF:tokens. See <a href="#">ClearToken</a> .
g	GTD	Optional	LCF:nonStandardData:gtg:gtgData. See <a href="#">GTD</a> .
y	ServiceControlSession	Optional	LCF:ServiceControlSession. See <a href="#">ServiceControlSession</a> .
C	IA5String	Optional	ARQ:callIdentifier

The destinationInfo from the LCF is used if one is available. Otherwise, the destinationInfo from the LRQ is used.

If the message contains an AlternateTransportAddr field, the following additional field shown in [Table 4-20](#) is included:

**Table 4-20 Additional Field**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
I	Transport-Address	Mandatory	IP address and port for Annex E. See <a href="#">Transport-Address</a> .

## Response LCF

This message is sent from the external application to the Cisco IOS Gatekeeper in response to a Request LRQ. The message indicates that the external application has completed the processing of the request.

This message can also be sent to the Cisco IOS Gatekeeper from the external application in response to a Request LCF or a Request LRJ. In the case of a Request LCF, the response can contain:

- A null message body, which indicates that the external application accepts the information in the Request LCF.
- Modified fields, which indicates that the external application wants to use different values than those included in the Request LCF.

In the case of a Request LRJ, the response contains an alternate destination.

For Response LCF, the possible tags are shown in [Table 4-21](#):

**Table 4-21 Response LCF**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
d	Alias-Address	Optional	LCF:destinationInfo
D	Transport-Address	Mandatory	LCF:destCallSignalAddress. See <a href="#">Transport-Address</a> .
r	Transport-Address	Mandatory	LCF:rasAddress. See <a href="#">Transport-Address</a> .
x	Alias-Address	Optional	LCF:destExtraCallInfo
X	Alias-Address	Optional	LCF:remoteExtensionAddress
t	Endpoint-Type	Optional	LCF:destinationType
A	AlternateEndpoint	Optional	ACF:alternateEndpoints
N	AlternateTransportAddr	Optional	LCF:AlternateTransportAddress
u	useSpecifiedTransport	Optional	ACF:useSpecifiedAddress
T	clearToken	Optional	LCF:tokens. See <a href="#">ClearToken</a> .
g	GTD	Optional	LCF:nonStandardData:gtg:gtgData. See <a href="#">GTD</a> .
s	Service-Descriptor	Optional	LCF:nonStandardData:serviceDescriptor
y	ServiceControlSession	Optional	ACF:ServiceControlSession. See <a href="#">ServiceControlSession</a> .
J	carrierInfo	Optional	See <a href="#">CarrierInfo</a> .
Q	trunkGroupInfo	Optional	See <a href="#">TrunkGroupInfo</a> .



### Note

The D and r are not required if the Response LCF is being sent in reply to a Request LCF.

If the message contains an AlternateTransportAddr field, the additional field shown in [Table 4-22](#) included:

**Table 4-22 Additional Field**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
I	Transport-Address	Mandatory	IP address and port for Annex E. See <a href="#">Transport-Address</a> .

## Request LRJ

This message is sent from the Cisco IOS Gatekeeper to the external application when the Cisco IOS Gatekeeper has received an LRJ from a remote Cisco IOS Gatekeeper. This gives the Cisco IOS Gatekeeper the opportunity to accept the rejection (Response LRJ) or propose an alternative destination (Response LCF).

For Request LRJ, the possible tags are shown in [Table 4-23](#):

**Table 4-23 Request LRJ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
s	Alias-Address	Optional	LRQ:srcInfo
d	Alias-Address	Mandatory	LRQ:destinationInfo
e	IA5String	Optional	LRQ:nonStandardData:redirectNumber
E	integer	Optional	LRQ:nonStandardData:redirectReason
p	integer	Optional	LRQ:nonStandardData:callingPartyNumOctet3a
w	IA5String	Optional	LRQ:nonStandardData:displayIE
c	IA5String	Optional	LRQ:nonStandardData:callingPartyNum
R	LRJ-reason	Mandatory	LRJ:rejectReason
y	ServiceControl Session	Optional	ARJ:ServiceControlSession. See <a href="#">ServiceControlSession</a> .
C	IA5String	Optional	ARQ:callIdentifier
v	IA5String	Optional	LRJ:terminationCause:releaseCompleteCauseIE <sup>1</sup>

1. This field is included if the GKTMP server wishes to provide a Q.850 cause code that it wants to be used to release the call.

## Response LRJ

This message is sent from the external application to the Cisco IOS Gatekeeper in response to a Request LRQ. The message indicates that the Cisco IOS Gatekeeper should reject the request for the specified reason.

This message can also be sent to the Cisco IOS Gatekeeper from the external application in response to a Request LCF or a Request LRJ. In the case of a Request LCF, this response rejects the information provided in the LCF for the specified reason. In the case of a Request LRJ, this response acknowledges the rejection. The reason is optional when the Response LRJ is sent due to a Request LRJ.

For Response LRJ, the possible tag is shown in [Table 4-24](#):

**Table 4-24 Response LRJ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
R	LRJ-Reason	Mandatory (LRQ, LCF) Optional (LRJ)	LRJ:rejectReason
y	ServiceControlSession	Optional	ACF:ServiceControlSession
v	IA5String	Optional	LRJ:terminationCause:releaseCompleteCauseIE <sup>1</sup>

1. This field is included if the GKTMP server wishes to provide a Q.850 cause code that it wants to be used to release the call.

Possible values for rejectReason are:

- notRegistered
- invalidPermission
- requestDenied
- undefinedReason
- securityDenial
- carrierIdUnspecified (maps to undefinedReason)
- carrierIdUnknown (maps to undefinedReason)
- ingressCarrierInactive (maps to undefinedReason)
- carrierOrigPcntExceeded (maps to undefinedReason)
- carrierMaxUnitsExceeded (maps to undefinedReason)
- destinationUnknown (maps to undefinedReason)
- noRouteAvailable (maps to undefinedReason)
- aliasesInconsistent
- routeCallToSCN
- resourcesUnavailable
- genericDataReason
- neededFeatureNotSupported
- hopcountExceeded
- incompleteAddress

## Disengage Messages

Disengage messages are used to indicate that a party wants to end the call.

### Request DRQ

This message is sent from the Cisco IOS Gatekeeper to the external application to indicate that an endpoint wants to end the call.

For Request DRQ, the possible tags are shown in [Table 4-25](#):

**Table 4-25 Request DRQ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
c	GUID	Optional	DRQ:callIdentifier
C	GUID	Mandatory	DRQ:conferenceID
R	DRQ-reason	Mandatory	DRQ:disengageReason
A	Boolean	Mandatory	DRQ:answeredCall
S	Transport-Address	Mandatory	ARQ:srcCallSignalAddress. See <a href="#">Transport-Address</a> .
T	clearToken	Optional	DRQ:tokens. See <a href="#">ClearToken</a> .
g	GTD	Optional	DRQ:gtd. See <a href="#">GTD</a> .
K	callCapacity	Optional	DRQ:capacity. See <a href="#">CallCapacity</a> .
v	IA5String	Optional	DRQ:terminationCause:releaseCompleteCauseIE
r	IA5String	Optional	DRQ:terminationCause:releaseCompleteReason
v	IA5 String	Optional	DRQ:terminationCause:releaseCompleteCauseIE

Possible values for the DRQ-reason are:

- forcedDrop
- normalDrop
- undefinedReason



**Note**

All Request DRQ messages must contain Notification-only in the header. No response to this message is sent.

## Resource Messages

Resource messages are used to indicate the current call capacity of the gateway.

### Request RAI

This message is sent from the Cisco IOS Gatekeeper to the external application to indicate the call capacity and data rate of the gateway for H.323 calls.

For Request RAI, the possible tags are shown in [Table 4-26](#):

**Table 4-26 Request RAI**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
c	Transport-Address	Mandatory	RRQ:callSignalAddress. See <a href="#">Transport-Address</a> .
r	Boolean	Mandatory	RAI:almostOutOfResources
K	callCapacity	Optional	RAI:capacity. See <a href="#">CallCapacity</a> .



**Note**

All Request RAI messages must contain Notification-only in the header. No response to this message is sent.

## Bandwidth Messages

Bandwidth messages are used to request a change in bandwidth.

This section describes the following:

- [Request BRQ](#)
- [Response BCF](#)
- [Response BRJ](#)

### Request BRQ

This message is sent from the Cisco IOS Gatekeeper to the external application to request that an endpoint be allowed to change (increase or decrease) its bandwidth.

For Request BRQ, the possible tags are shown in [Table 4-27](#):

**Table 4-27 Request BRQ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
i	Transport-Address	Mandatory	See Note. See <a href="#">Transport-Address</a> .
b	Bandwidth	Mandatory	BRQ:bandWidth
C	GUID	Mandatory	BRQ:conferenceID
c	GUID	Mandatory	BRQ:callIdentifier
A	Boolean	Mandatory	BRQ:answeredCall



**Note**

When sending a BRQ message, an endpoint identifies itself to the gatekeeper using the endpointIdentifier that it received from the gatekeeper in the RCF. Because this endpointIdentifier has only local significance to the gatekeeper and no significance to the server, the endpoint's CallSignalAddress is used here as an identifier.

## Response BRQ

The server may modify the fields shown in [Table 4-28](#) in the BRQ.

**Table 4-28 Response BRQ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
b	Bandwidth	Optional	BRQ:bandWidth
F	Boolean	Optional	None

## Response BCF

This message is sent from the external application to the Cisco IOS Gatekeeper to confirm the request to allow an endpoint to change (increase or decrease) its bandwidth. This response gives the external application the opportunity to modify the Bandwidth field of a received LCF, but because the Cisco IOS Gatekeeper is not prepared to make changes in its bandwidth, any change in the BCF will automatically generate a BRJ back to the endpoint.

For Response BCF, the possible tag is shown in [Table 4-29](#):

**Table 4-29 Response BCF**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
b	Bandwidth	Mandatory	BCF:bandWidth

## Response BRJ

This message is sent from the external application the Cisco IOS Gatekeeper to deny the request to allow an endpoint to change (increase or decrease) its bandwidth.

For Response BRJ, the possible tag is shown in [Table 4-30](#):

**Table 4-30 Response BRJ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
R	BRJ-Reason	Mandatory	BRJ:rejectReason

Possible values for rejectReason are:

- notBound
- invalidConferenceID
- invalidPermission
- insufficientResource
- invalidRevision
- undefinedReason
- securityDenial

## Progress Messages

Progress messages provide information about the progress of a request. Progress messages include:

- [Response RIP](#)
- [Request IRR](#)
- [Request ALV](#)
- [Response ALV](#)

### Response RIP

This message is sent from the external application to the Cisco IOS Gatekeeper when the external application cannot immediately process the request. This message indicates that the request is in progress (RIP) and that additional time is needed. When the Cisco IOS Gatekeeper receives this message, it forwards a request to the H.323 endpoint indicating that an extension of the timeout is required. The external application can send more than one Response RIP as is needed to process the request.

For Response RIP, the possible tag is shown in [Table 4-31](#):

**Table 4-31 Response RIP**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
d	Integer	Mandatory	RIP:delay

Possible values of the delay are 1 through 65535 milliseconds.

### Request IRR

This message is sent to the GK and contains details for the call after a successful connect. A Request IRR message is sent at both the originating and terminating side of the call. If both legs reference the same GK, only one Request IRR is sent. The GK sends information for only one call in each Request IRR message.

[Table 4-32](#) shows the new Request IRR tags:

**Table 4-32 New Request IRR Tags**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
S	Transport-Address	Mandatory	IRR:srcCallSignalAddress. See <a href="#">Transport-Address</a> .
P	PerCallInfo	Optional	IRR:perCallInfo. See <a href="#">PerCallInfo</a> .
K	callCapacity	Optional	IRR:capacity. See <a href="#">CallCapacity</a> .

## Request ALV

The REQUEST ALV is sent from the Gatekeeper to a GKTMP server on the detection of slower response or server failure.

This message does not contain any parameters in its body.

## Response ALV

This message is returned in response to a REQUEST ALV message and does not contain any parameters in its body.

# Trigger Registration Messages

Trigger registration messages are used by external applications to inform the Cisco IOS Gatekeeper which RAS messages are interesting to the external application. Interesting RAS messages trip a trigger in the Cisco IOS Gatekeeper and cause the Cisco IOS Gatekeeper to send a GKTMP RAS message to the external application.

As with the GKTMP RAS messages, trigger registration messages have the following format:

- Single message line
- One or more message header lines
- Blank line, which separates the message header from the message body
- Zero or more message body lines

## Message Line

There are two types of trigger registration messages: register and unregister.

The first line of each trigger registration request/response message uses the format:

```
REGISTER RAS_message_type
```

The first line of each trigger unregistration request/response message uses the format:

```
UNREGISTER RAS_message_type
```

Possible RAS message types are as follows:

- RRQ—Registration request
- URQ—Unregistration request
- ARQ—Admission request
- LRQ—Location request
- LCF—Location confirm
- LRJ—Location reject
- DRQ—Disengage request
- RAI—Resource availability information
- BRQ—Bandwidth request

## Message Header

The message line is immediately followed by the message header. Each message header contains a field name and a value, separated by a colon (*field:value*). Possible fields are shown in [Table 4-33](#):

**Table 4-33 Message Header Fields**

Field Names	Field Values
Version-ID	Version of the GKTMP. The version ID consists of a major number (gk_major) and a minor number (gk_minor). For example, Version 1 is represented as 100.
From	String that identifies the originator of the message. For trigger registration requests from the external application, this field contains the server ID. For trigger registration responses from the Cisco IOS Gatekeeper, this field contains the gatekeeper ID. This field is required for trigger registration and unregistration requests and responses.
To	String that identifies the receiver of the message. For trigger registration requests from the external application, this field contains the gatekeeper ID. For trigger registration responses from the Cisco IOS Gatekeeper, this field contains the ID of the external application that initiated the request. This field is required for trigger registration and unregistration requests and responses.
Priority	A number indicating the priority of this trigger in relation to other triggers for the same RAS message type. Possible values are 1 through 20. 1 is the highest priority.  If the Cisco IOS Gatekeeper has a registration for a RAS message type and receives another registration for the same RAS message from the same external application with the same priority, the Cisco IOS Gatekeeper uses the new registration and discards the previous one. If the Cisco IOS Gatekeeper has a registration for a RAS message type and receives another registration with the same priority from a different external application, the Cisco IOS Gatekeeper discards the new registration. This field is required for trigger registration and unregistration requests and is echoed in trigger registration and unregistration responses.
Content-length	The number of octets contained in the message body. If the message body is null, this field is omitted. This field is used only in trigger registration requests.

**Table 4-33 Message Header Fields (continued)**

Field Names	Field Values
Notification-only	None. No value is included after the colon. If this field name is present, it indicates to the Cisco IOS Gatekeeper that it should forward requests for the specified RAS messages as a notification only. This field is used only in trigger registration requests.
Status	<p>String that indicates the response code from the Cisco IOS Gatekeeper. This field is used only in trigger registration and unregistration responses.</p> <p>Possible response codes for unregistration requests are:</p> <ul style="list-style-type: none"> <li>• success—The registration has been accepted.</li> <li>• invalidPriority—The registration has been rejected because the Gatekeeper already has a registration for this RAS message type with the same priority from another application.</li> <li>• invalidFilters—Parsing of the message body failed.</li> <li>• invalidGKID—The gatekeeper ID specified in the “To” field of the request does not match the ID of any gatekeepers on this Cisco router.</li> </ul> <p>Possible response codes for unregistration responses are:</p> <ul style="list-style-type: none"> <li>• success—The unregistration has been accepted.</li> <li>• invalidPriority—The unregistration has been rejected because the Gatekeeper does not have a registration for this RAS message type with the same priority from this application.</li> <li>• invalidGKID—The gatekeeper ID specified in the “To” field of the request does not match the ID of any gatekeepers on this Cisco router.</li> </ul>

The message header is followed immediately by a blank line.

## Message Body

The message body follows the blank line. Only trigger registration requests contain a message body. Trigger registration responses, unregistration requests, and unregistration responses end after the blank line.

The message body in a trigger registration request can be used to narrow the circumstances under which the Cisco IOS Gatekeeper sends a REQUEST *xxx* to the external application. In this case, the external application includes tags and values in the message body that if matched will trigger the Cisco IOS Gatekeeper to generate a REQUEST *xxx*.

The tags that can be included vary depending on the RAS message type, and are a subset of the types that can be included in GKTMP RAS messages.

For the field type of Alias-Address, trailing wildcards can be used with E.164 addresses. An asterisk can be used to indicate a string of characters (for example, 1800\*). A period can be used to indicate a single character (for example, 1800.....).



### Note

Wildcards cannot be used at the beginning or in the midst of a value, only at the end. If you include a wildcard at the beginning or in the midst of a value, it will be interpreted as a literal character.

## Register RRQ and RAI

For Register RRQ and RAI, the tags shown in [Table 4-34](#) can be used to filter messages:

**Table 4-34 Register RRQ and RAI**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
t	Endpoint-Type	Optional	RRQ:terminalType
p	Supported-Prefix	Optional	RRQ:terminalType:gateway:protocol*:supportedPrefixes
S	Boolean	Optional	Synchronize current registrations (send notification-only Request RRQs)

## Register URQ

For Register URQ, the tags shown in [Table 4-35](#) can be used to filter messages:

**Table 4-35 Register URQ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
t	Endpoint-Type	Optional	RRQ:terminalType
p	Supported-Prefix	Optional	RRQ:terminalType:gateway:protocol*:supportedPrefixes

## Register ARQ, DRQ, IRR, and BRQ

For Register ARQ, DRQ, IRR, and BRQ the tags shown in [Table 4-36](#) can be used to filter messages:

**Table 4-36 Register ARQ, DRQ, IRR, and BRQ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
d	Alias-Address	Optional	ARQ:destinationInfo
E	integer	Optional	ARQ:nonStandardData:redirectReason

## Register LRQ

For Register LRQ, the tags shown in [Table 4-37](#) can be used to filter messages:

**Table 4-37 Register LRQ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
d	Alias-Address	Optional	LRQ:destinationInfo
E	integer	Optional	LRQ:nonStandardData:redirectReason

**Note**

A gatekeeper might not be the final destination of the LRQ messages that it receives. If the queried address in an LRQ is in another Gatekeeper's zone, the LRQ is forwarded to that gatekeeper and is not resolved locally. This means that there might not be a local zone that can be associated with the LRQ. To address this situation, the gatekeeper arbitrarily uses the server registrations for the first configured local zone. Because the order in which configured zones appear can change with deletions and additions, servers should send identical LRQ registrations to all zones (all logical gatekeepers) on the same router.

## Register LCF

For Register LCF, the tags shown in [Table 4-38](#) can be used to filter messages:

**Table 4-38 Register LCF**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
d	Alias-Address	Optional	LRQ/LCF:destinationInfo
X	Alias-Address	Optional	LCF:remoteExtensionAddress

## Register LRJ

For Register LRJ, the tag shown in [Table 4-39](#) can be used to filter messages:

**Table 4-39 Register LRJ**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
d	Alias-Address	Optional	LRQ:destinationInfo

# Additional Messages

## GTD

The Generic Transparency Descriptor (GTD) field type is a structure comprising of two sub-fields: length and data. This field type is required for values that contain `<cr><lf>` pairs in its body. The *length* (B) sub-field indicates the size of the *data* sub-field and indicates to the parser that any occurrence of `<cr><lf>` within the *data* sub-field is not a `<tag>=<value>` delimiter.

[Table 4-40](#) shows the new GTD tags:

**Table 4-40 New GTD Tags**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
B	IA5String	Mandatory	Length of the data sub-field. Contains 5-digit ASCII characters.
Data	subfield	Mandatory	Opaque data transported by GKTMP.

### Usage Notes

The GTD field type is different from other GKTMP fields in that <cr><lf> does not indicate the end of the GTD line. The following rules must be followed in processing the GTD field type:

- Use 'g' as a GTD tag across all *REQUEST* and *RESPONSE* messages.
- The length of the GTD data sub-field is specified by 'B' and is represented by five ASCII digits.
- A 'B' sub-field is delimited by ':'.
  - <cr><lf> or <lf> within the GTD body should not be interpreted as a tag or value delimiter. The <cr><lf> after the GTD sub-field—specified by length sub-field—is the delimiter.
- The GTD field should not be included in any tag other than 'g'.
- Gatekeeper to Server:
  - 'g=B:<Five ASCII digits>:<data>' should be used to send the GTD.
  - 'g=' is illegal.
  - The absence of a 'g' tag indicates there is no GTD data.
  - All other 'g' tag formats are illegal
- Server to Gatekeeper:
  - The 'g' tag can only be sent in a *RESPONSE* message corresponding to a *REQUEST* message from the gatekeeper in which a GTD is present. The server cannot generate and send a GTD if it has not received a GTD from the gatekeeper.
  - 'g=B:<Five ASCII digits>:<data>' indicates the server is returning the GTD it received in a request from the gatekeeper. (This GTD could be a modified version of gatekeeper GTD.) The gatekeeper should replace its cached copy of the GTD with the received copy of the GTD.
  - 'g=' indicates that server wants the gatekeeper to retain its copy of the GTD.
  - The absence of a 'g' tag indicates that the gatekeeper should delete its copy of GTD.
- The gatekeeper should not send a 'g' tag or value if the server GKTMP version is less than version 4.1. Versions below version 4.1 cannot interpret the GTD and <cr><lf> may not delimit the GTD tag or value, so these lower versions cannot to skip the 'g' tag line.

### Format

g=B:<Length in 5 ASCII digits>:<Data>

### Example

g=B:00003:1AB

## AlternateGK

A message body line containing a field of type AlternateGK contains a set of fields enclosed within curly braces "{ }". Each of the fields within the curly braces are identified by a tag, with each field separated by SP (ascii space, 0x20) characters.

Table 4-41 shows the AlternateGK tags:

**Table 4-41 AlternateGK Tags**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
r	Transport-Address	Mandatory	AlternateGK:rasAddress. See <a href="#">Transport-Address</a> .
g	Alias-Address	Optional	AlternateGK:gatekeeperIdentifier. See <a href="#">Alias-Address</a> .
n	Boolean	Mandatory	AlternateGK:needToRegister
p	integer	Mandatory	AlternateGK:priority

## FromReplyAddress

The **from** IP address is the address from which an LRQ message was received. The **reply-to** address is the mandatory IP address specified in the RAS LRQ message replyAddress field. A GKTMP application can use these fields to authenticate the source of LRQ message.

Table 4-42 shows the FromReplyAddress tags:

**Table 4-42 FromReplyAddress Tags**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
f	IP address	Mandatory	Address of the gatekeeper from which this LRQ message was received.
r	IP address	Mandatory	LRQ::replyAddress:ipAddress:ip

## ServiceControlSession

Table 4-43 shows the new Service Control Session tags:

**Table 4-43 New ServiceControl Sessions Tags**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
d	IA5String	Optional	serviceControl:contents
r	IA5String	Mandatory	serviceControl:reason
s	Integer	Mandatory	serviceControl:sessionId

## CallCapacity

The CallCapacity message indicates the ability of the gateway to accept each type of call the gateway supports, such as voice calls.

Table 4-44 shows the CallCapacity tags:

**Table 4-44 CallCapacity Tags**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
T	CallCapacityType	Mandatory	xRQ::callCapacity:maximum/currentCallCapacity:xxxxGwCallsAvailable
G	IA5String	Mandatory	xRQ::callCapacity:maximum/currentCallCapacity:xxxxGwCallsAvailable:group
C	Integer	Mandatory	xRQ::callCapacity:maximumCallCapacity:xxxxGwCallsAvailable:calls
c	Integer	Mandatory	xRQ::callCapacity:currentCallCapacity:xxxxGwCallsAvailable:calls

## CarrierInfo

The gatekeeper sends incoming carrier information received in a RAS ARQ message from the gateway to an external GKTMP application. This information allows the application to select an outbound carrier and remote zones that the carrier may exist in. The gatekeeper uses this outbound carrier and zone information to query for the egress gateway.

Table 4-45 shows the new Carrier Information tags:

**Table 4-45 CarrierInfo Tags**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
i	IA5String	Mandatory	destination carrierID
p	Integer	Optional	Priority of this carrier
z	remoteZone	Optional	Remote zone information. See <a href="#">RemoteZone</a> .

## TrunkGroupInfo

Table 4-46 shows the new Trunk Group Information tags:

**Table 4-46 TrunkGroupInfo Tags**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
i	IA5String	Mandatory	Destination trunk group
p	Integer	Optional	Priority of this trunk group
z	remoteZone	Optional	Remote zone information. See <a href="#">RemoteZone</a> .

## Alias-Address

A field of type Alias-Address contains a sequence of aliases separated by SP (ascii space, 0x20) characters. Each alias is prefixed by one of the following type characters, followed by a colon:

- H: an H.323-ID
- E: an E.164 address
- M: an email ID

For example, in an RRQ message, a terminal alias containing the sequence of an H.323-ID of "John Smith", an E164 address of 4085551212, and an email-id of "jsmith@somewhere.com" is indicated by the line:  
a=H:"John Smith" E:4085551212 M:jsmith@somewhere.com

## PerCallInfo

If the message contains a PerCallInfo field, the following fields shown in [Table 4-47](#) are included:

**Table 4-47 PerCallInfo Fields**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
c	GUID	Optional	IRR:perCallInfo:callIdentifier
C	GUID	Mandatory	IRR:perCallInfo:conferenceID
A	Boolean	Optional	IRR:perCallInfo:originator
b	Bandwidth	Mandatory	IRR:perCallInfo:bandwidth
t	System Time	Optional	IRR:perCallInfo:NonStandard:start_time
s	IA5String	Optional	IRR:perCallInfo:tokens:IZCT:srcZone
d	IA5String	Optional	IRR:perCallInfo:tokens:IZCT:dstZone
S	IA5String	Optional	IRR:perCallInfo:srcCarrierId
D	IA5String	Optional	IRR:perCallInfo:dstCarrierId

## RemoteZone

[Table 4-48](#) shows the remoteZone field tags:

**Table 4-48 RemoteZone Tags**

Tag	Field Type	Mandatory or Optional	Description
r	Transport-Address	Mandatory	RAS address of the zone. See <a href="#">Transport-Address</a> .
c	Integer	Optional	Cost value associated with the zone
p	Integer	Optional	Priority value associated with the zone
T	clearToken	Optional	ARQ:tokens. See <a href="#">ClearToken</a> .

## Transport-Address

The only type of transport address currently supported by the gatekeeper is IP version 4. However, a type prefix is defined for future extensibility. For example, I: IP version 4 address.

The address is specified in the usual dotted string form, followed by a colon and port number. For example, the callSignalAddress in an RRQ message may be specified as: c=I:172.21.137.4:1720.

## ClearToken

If the message contains a clearToken field, the fields shown in [Table 4-49](#) are included:

**Table 4-49 ClearToken Fields**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
O	OBJECT-IDENTIFIER	Mandatory	tokens:objectIdentifier
p	IA5string	Optional	tokens:password
t	integer	Optional	tokens:timestamp
s	IA5string	Optional	tokens:challengeString
r	integer	Optional	tokens:random
G	IA5string	Optional	tokens:generalID
o	OBJECT-IDENTIFIER	Optional	tokens:nonStandard:objectIdentifier
d	IA5string	Optional	tokens:nonStandard:data

## CryptoToken

If the message contains a cryptoToken field, the additional fields shown in [Table 4-50](#) are included:

**Table 4-50 CryptoToken Fields**

Tag	Field Type	Mandatory or Optional	Corresponding RAS Message Field
H	IA5string	Optional	CryptoToken:alias
t	IA5string	Optional	CryptoToken:timestamp
h	IA5string	Optional	CryptoToken:token



## Gatekeeper API Functions and Structures

---

This chapter describes the API functions and structures that an external application must use to exchange messages with the Cisco IOS Gatekeeper, and contains the following sections:

- [Gatekeeper API Functions, page 5-1](#)
- [API Structures, page 5-12](#)

The external application links with the object code, which contains the API functions. The header file contains API prototypes and type definitions.

### Gatekeeper API Functions

This section describes the functions provided with the API. These functions should be used by the external application to gather information from and provide information to the Cisco IOS Gatekeeper. The functions described in this section are:

- [GkapiSetupClient, page 5-2](#)
- [GkapiSetupServer, page 5-2](#)
- [GkapiClientConnected, page 5-3](#)
- [GkapiAcceptConnection, page 5-4](#)
- [GkapiGetVersion, page 5-4](#)
- [CloseGateKeeperConnection, page 5-5](#)
- [GetReadMsgBuffer, page 5-5](#)
- [ReadMsgBuffer, page 5-5](#)
- [FreeReadMsgBuffer, page 5-7](#)
- [WriteCommandMsg, page 5-7](#)
- [WriteResponseMsg, page 5-8](#)
- [WriteRegisterMessage, page 5-9](#)
- [WriteUnregisterMessage, page 5-10](#)
- [GkapiSetupReport, page 5-11](#)
- [GkapiQueryReport, page 5-11](#)

## GkapiSetupClient

This function sets up the socket for the application to communicate as a client with the Cisco IOS Gatekeeper. In this situation, the application is the client and the Gatekeeper is the server, which means the application must initiate the communication with the Cisco IOS Gatekeeper.

### Input

The input to this function is:

- A pointer to the [GKAPI SOCK INFO](#) structure. The application must set up the TCP Port and IP Address fields and must preserve this structure for the duration of the connection.
- A pointer to the [STATUS\\_TYPE](#) enumeration. Possible values for STATUS\_TYPE are:
  - PROCESSING\_SUCCESSFUL—Successful connection to the Cisco IOS Gatekeeper.
  - CONNECT\_IN\_PROGRESS—Connection is pending.
  - TCP\_HANDLE\_ERROR—Error was encountered in handle creation.
  - TCP\_CONNECT\_ERROR—Error was encountered in connecting to the Cisco IOS Gatekeeper.
  - TCP\_NONBLOCK\_ERROR—Error was encountered when setting up the socket for nonblocking I/O
- A boolean value that allows the application to specify if the socket I/O should be nonblocking or blocking. If the application specifies blocking, the Gatekeeper API calls to setup the connection and read a message that does not return until the action is complete.

### Return

The return for this function is an integer. If the client socket connection has been set up successfully or is in progress, a connection handle is returned. This connection handle is the socket descriptor that the application uses to wait on a connection completion or read socket event. If an error occurs while setting up the client connection, the value -1 is returned. In this case, the error information is provided in the STATUS\_TYPE.

## GkapiSetupServer

This function sets up the socket for the application to communicate as a server with the Cisco IOS Gatekeeper. In this situation, the application is the server and the Gatekeeper is the client, which means that the application will accept incoming connections from Cisco IOS Gatekeeper clients.

### Input

- A pointer to the [GKAPI SOCK INFO](#) structure. The application must set up the TCP Port and IP Address fields and must preserve this structure for the duration of the connection.
- A pointer to the [STATUS\\_TYPE](#) enumeration. Possible values for STATUS\_TYPE are:
  - PROCESSING\_SUCCESSFUL—Successful connection to the Cisco IOS Gatekeeper.
  - TCP\_HANDLE\_ERROR—Error was encountered in handle creation.
  - TCP\_ADDRESS\_ALREADY\_IN\_USE—Specified local IP address is already in use.

- TCP\_ADDRESS\_NOT\_AVAIL—Specified local IP address is not available on the local machine.
- TCP\_BIND\_ERROR—Error was encountered in setting up the server socket.
- TCP\_LISTEN\_ERROR—Error was encountered in setting up the server socket.
- TCP\_NONBLOCK\_ERROR—Error was encountered when setting up the socket for nonblocking I/O.
- A boolean value that allows the application to specify if the socket I/O should be nonblocking or blocking. If the application specifies blocking, the Gatekeeper API calls to setup the connection and read a message that does not return until the action is complete.

## Return

The return for this function is an integer. If the client socket connection has been set up successfully or is in progress, a connection handle is returned. This connection handle is the socket descriptor that the application uses to wait on a connection completion or read socket event. If an error occurs while setting up the client connection, the value -1 is returned. In this case, the error information is provided in the STATUS\_TYPE.

## GkapiClientConnected

This function must be called by the application to indicate that a select event for a connect complete has occurred.

## Input

The input to this function is:

- A pointer to the [GKAPI SOCK\\_INFO](#) structure.
- A pointer to the STATUS\_TYPE enumeration. Possible values for STATUS\_TYPE are:
  - PROCESSING\_SUCCESSFUL—Successful connection to the Gatekeeper.
  - TCP\_CONNECT\_ERROR—Error was encountered in connecting to the Gatekeeper.
- An integer that indicates that a connect complete has occurred.

## Return

The return for this function is an integer. If the socket connection has been set up successfully or is in progress, a connection handle is returned. This connection handle is the socket descriptor that the application uses to wait on a connection completion or read socket event. If an error occurs while setting up the client connection, the value -1 is returned. In this case, the error information is provided in the STATUS\_TYPE.

## GkapiAcceptConnection

This function must be called by the application (when it is running in the server mode) to indicate that a select event for an incoming connection has occurred.

### Input

The input to this function is

- A pointer to the [GKAPI SOCK\\_INFO](#) structure.
- A pointer to the STATUS\_TYPE enumeration. Possible values for STATUS\_TYPE are:
  - PROCESSING\_SUCCESSFUL—Successful connection to the Cisco IOS Gatekeeper.
  - TCP\_CONNECT\_ERROR—Error was encountered in connecting to the Cisco IOS Gatekeeper.
- An integer that indicates that an incoming connection has occurred.
- A pointer to the [GKAPI\\_TCP\\_ADDR\\_INFO](#) structure. The Gatekeeper API provides the IP address and TCP port of the client with which this connection is associated.

### Return

The return for this function is an integer. If the socket connection has been set up successfully or is in progress, a connection handle is returned. This connection handle is the socket descriptor that the application uses to wait on a connection completion or read socket event. If an error occurs while setting up the client connection, the value -1 is returned. In this case, the error information is provided in the STATUS\_TYPE.

## GkapiGetVersion

Applications can use this function to obtain the GKTMP version used by the API and the gatekeeper. The version number consists of a major number (gk\_major) and a minor number (gk\_minor). For example, Version 1 is represented as 100.

### Input

The input to this function is

- A pointer to the [GKAPI\\_VERSION\\_INFO](#) structure.

### Return

The return for this function is an integer. The integer indicates one of the following status codes:

- GKAPI\_RET\_OK—Gatekeeper TMP version is prior to or the same as the gatekeeper API version.
- GKAPI\_RET\_NOK—Gatekeeper TMP version is later than the gatekeeper API version.
- GKAPI\_RET\_OK\_NOGKDATA—Version used by the gatekeeper is not known. In this case, the gk\_major and gk\_minor members of GKAPI\_VERSION\_INFO\_T are invalid and set to -1.

## CloseGateKeeperConnection

This function closes the TCP connection between the external application and the Cisco IOS Gatekeeper. This function is called under error circumstances and when the external application no longer wants to maintain a relationship with the Cisco IOS Gatekeeper.

### Input

The input for this function is a pointer to the [GKAPI SOCK\\_INFO](#) structure.

### Return

There is no return for this function.

## GetReadMsgBuffer

This function allocates memory for the size of GK\_READ\_MSG structure. This structure is used to store messages received from the Cisco IOS Gatekeeper. This function contains an enumeration of the messages that can be received (REQUEST messages from the Cisco IOS Gatekeeper for RRQ, ARQ, LRQ, LCF, LRJ, as well as registration and unregistration responses from the Cisco IOS Gatekeeper for ARQ, RRQ, URQ, LRQ, LCF, LRJ messages) and a union of structures for the different messages.

**Note**

---

When the external application no longer needs the message buffer, the application must call FreeReadMsgBuffer to release the memory back to the system.

---

### Input

There is no input to this function.

### Return

The return for this function is a pointer to the [GK\\_READ\\_MSG](#) structure. If the memory allocation fails, this pointer will be NULL.

## ReadMsgBuffer

This function reads a message from the TCP socket and should be called when the external application has detected a read event on the socket. This function stores the message type into the structure. The parameters received in the message are stored in the structure that corresponds with the message type.

**Note**

---

GetReadMsgBuffer must be called to allocate an empty buffer before this function can be used. FreeReadMsgBuffer must be called after this function has completed, except when the STATUS\_TYPE returns INCOMPLETE\_MSG\_READ.

---

After reading a message, this function sets the message type and populates the appropriate structure. For example, if an ARQ message has been received from the Cisco IOS Gatekeeper, the `msgType` parameter is set to `ARQ_REQUEST_MSG` and the `ARQ_REQUEST_MSG` structure is populated.

Because some parameters are optional, these parameters might not be received for a particular message. Structure members that are character pointers are initialized to `NULL`. Integers and enumerations are set to their initialization values. Therefore, the API can assume that if a structure member has a pointer set to `NULL` or to its initialization value, that particular parameter has not been received.

The following initialization values indicate that the parameter was not received from the Cisco IOS Gatekeeper:

- `canMapAlias`—`INITIALIZE_CAN_MAP_ALIAS_VALUE`
- `bandWidthPresent`—`TRUE` (indicating that `bandWidth` has been received and filled in) or `FALSE` (indicating that `bandWidth` has not been received)
- `answerCall`—`INITIALIZE_ANSWER_CALL_VALUE`
- `REDIRECT_REASON_TYPE`—`REDIRECT_REASON_INFO_NOT_RCVD`
- `ENDPOINT_TYPE`—`ENDPOINT_INFO_NOT_RCVD`

## Input

The input for this function is:

- A pointer to the [GKAPI SOCK INFO](#) structure.
- A pointer to the [GK\\_READ\\_MSG](#) structure that was allocated by the `GetReadMsgBuffer` function. The `GK_READ_MSG` structure contains an enumeration of the message types expected from the Cisco IOS Gatekeeper and a union of structures for various messages expected from the Cisco IOS Gatekeeper.

## Return

The return for this function is the [STATUS\\_TYPE](#). Possible values for `STATUS_TYPE` are:

- `PROCESSING_SUCCESSFUL`—No errors were encountered.
- `TCP_READ_ERROR`—A TCP read error was encountered. The application should call `CloseGateKeeperConnection` to close the connection to the Cisco IOS Gatekeeper.
- `MEM_ALLOC_FAIL`—Memory allocation failed. This function, dynamically allocates memory for fields within the `GK_READ_MSG` structure.
- `MSG_READ_ERROR`—The message read was not understood by the API function. The application should call `CloseGateKeeperConnection` to close the connection to the Cisco IOS Gatekeeper.
- `INCOMPLETE_MSG_READ`—The message was not completely read from the TCP connection because of network conditions. The application should call the function again in order to continue reading the data. In this situation, `FreeMsgBuffer` should not be called. After all the data has been read, the `STATUS_TYPE` is set to one of the other possible values, and after processing the message type the `FreeMsgBuffer` can be called.
- `TCP_CONNECTION_CLOSED`—The connection to the Cisco IOS Gatekeeper has been closed. The application must call `CloseGateKeeperConnection` to free resources such as `gkHandle` in the `GKAPI SOCK INFO` structure.
- `NULL_POINTER_PASSED`—The pointer to the `GK_READ_MSG` is null.

## FreeReadMsgBuffer

This function frees memory that was allocated by the call to `GetReadMsgBuffer` and `ReadMsgBuffer`. This function **must** be called after processing the information returned by `ReadMsgBuffer`.

### Input

The input for this function is a pointer to the [GK\\_READ\\_MSG](#) structure.

### Return

There is no return for this function.

## WriteCommandMsg

This function sends a command message to the Cisco IOS Gatekeeper, which can respond with a result message. This structure, `CMD_MSG_TYPE`, contains an enumeration of messages that can be sent as spontaneous commands to the Cisco IOS Gatekeeper. The `CMD_HEADER_INFO_TYPE` structure must include the *from*, *to*, *transaction-id*, and *notification-only* fields.

### Input

The input for this function is:

- A pointer to the [GKAPI SOCK\\_INFO](#) structure.
- A pointer to the `GK_CMD_MSG_TYPE` structure, which contains a union of the structures for the various command messages that can be sent to the Cisco IOS Gatekeeper. Each structure contains a header, `CMD_HEADERINFO_TYPE`, that must be filled in by the application. The `msgType` field must be filled in to indicate which command message should be sent to the Cisco IOS Gatekeeper.

### Return

The return for this function is the [STATUS\\_TYPE](#). Possible values for `STATUS_TYPE` are:

- `PROCESSING_SUCCESSFUL`—No errors were encountered.
- `CONNECT_IN_PROGRESS`—Connection is pending. The application should retry this API call after some time has passed.
- `TCP_WRITE_ERROR`—A TCP write error was encountered. The application should call `CloseGateKeeperConnection` to close the connection to the Cisco IOS Gatekeeper.
- `MEM_ALLOC_FAIL`—Memory allocation failed.
- `TCP_CONNECTION_CLOSED`—The connection to the Cisco IOS Gatekeeper has been closed. The application must call `CloseGateKeeperConnection` to free resources such as `gkHandle` in the `GKAPI SOCK_INFO` structure.
- `HEADER_INFO_INCOMPLETE`—One of the fields in the header (*To*, *From*, *TransactionID*) is incomplete.
- `NULL_POINTER_PASSED`—The pointer to the `GK_CMD_MSG` is null.

## WriteResponseMsg

This function writes a response message to the Cisco IOS Gatekeeper. This structure contains [RESPONSE\\_MSG\\_TYPE](#), which is an enumeration of the response messages that can be sent to the Cisco IOS Gatekeeper.

The calling function must set the message type and populate the appropriate structure within the union. For example, if a response RCF needs to be sent to the Cisco IOS Gatekeeper, the application should set the `msgType` to `RCF_RESPONSE_MSG` and populate the `RCF_RESPONSE_MSG` structure.

The following rules apply to responses sent by the external application to the Cisco IOS Gatekeeper:

- Transport-addresses must be preceded with “I:”, followed by the address.
- Alias-addresses must be preceded with either “H:”, “E:”, or “M:” followed by the alias address.
- Values in a “sequence of values” must be separated by a space.
- [HEADER\\_INFO](#) must include the “from”, “to” and “transactionID” fields. The notification field is not used with the `WriteResponseMsg` function.

Only changed or new fields should be populated and sent to the Cisco IOS Gatekeeper. Parameters that are not to be sent to the Cisco IOS Gatekeeper must either be set to their initialization value or to NULL (for pointers). The API assumes that if a structure member is set to its initialization value or has a pointer set to NULL, that parameter should not be sent to the Cisco IOS Gatekeeper.

The following initialization values indicate that the parameter should not be sent to the Cisco IOS Gatekeeper:

- `bandWidthPresent`—TRUE (indicating that the `bandWidth` should be sent) or FALSE (indicating that the `bandWidth` should not be sent)
- `REDIRECT_REASON_TYPE`—`REDIRECT_REASON_INFO_NOT_RCVD`
- `ENDPOINT_TYPE`—`ENDPOINT_INFO_NOT_RCVD`



### Note

If the application requires additional time before responding to a message from the Cisco IOS Gatekeeper, the application can send a “delay” message by setting `msgType` to `RIP_RESPONSE_MSG`. The delay value (1 through 65536) must be specified and the `transactionID` must be the same as the one received from the Cisco IOS Gatekeeper.

## Input

The input for this function is:

- A pointer to the [GKAPI\\_SOCK\\_INFO](#) structure.
- A pointer to the [IRR\\_REQUEST\\_MSG](#) structure, which contains an enumeration of message types for which a response might be sent to the Cisco IOS Gatekeeper. The input also contains a union of structures for each message response.

## Return

The return for this function is the [STATUS\\_TYPE](#). Possible values for `STATUS_TYPE` are:

- `PROCESSING_SUCCESSFUL`—No errors were encountered.
- `CONNECT_IN_PROGRESS`—Connection is pending. The application should retry this API call after some time has passed.

- **TCP\_WRITE\_ERROR**—A TCP write error was encountered. The application should call `CloseGateKeeperConnection` to close the connection to the Cisco IOS Gatekeeper.
- **MEM\_ALLOC\_FAIL**—Memory allocation failed.
- **TCP\_CONNECTION\_CLOSED**—The connection to the Cisco IOS Gatekeeper has been closed. The application must call `CloseGateKeeperConnection` to free resources such as `gkHandle` in the `GKAPI SOCK_INFO` structure.
- **INVALID\_MSG\_SPECIFIED**—The message type is not within the `RESPONSE_MSG_TYPE` range.
- **INVALID\_ENDPOINT\_SPECIFIED**—The endpoint does not match one of the possible values for `ENDPOINT_TYPE`.
- **INVALID\_REDIRECT\_REASON\_SPECIFIED**—The redirect reason does not match one of the possible values for `REDIRECT_REASON_TYPE`.
- **INVALID\_REJECT\_REASON\_SPECIFIED**—The rejection reason does not match one of the possible values for `REJECT_REASON_TYPE`.
- **INVALID\_DELAY\_SPECIFIED**—The delay is not within the valid range.
- **HEADER\_INFO\_INCOMPLETE**—One of the fields in the header (To, From, TransactionID) is incomplete.
- **NULL\_POINTER\_PASSED**—The pointer to `GK_WRITE_MSG` is null.

## WriteRegisterMessage

This function sends a registration message to the Cisco IOS Gatekeeper and allows triggers to be dynamically registered with the Cisco IOS Gatekeeper. This structure, [REGISTER\\_MSG\\_TYPE](#), contains an enumeration of messages that can be registered with the Cisco IOS Gatekeeper.

The `REGISTER_REQUEST_HEADER` structure must include the “from,” “to,” “priority,” and “notification-only” fields.

### Input

The input for this function is:

- A pointer to the [GKAPI SOCK\\_INFO](#) structure.
- A pointer to the [GK\\_REGISTER\\_MSG](#) structure, which contains a union of the structures for the various registration messages that can be sent to the Cisco IOS Gatekeeper. Each structure contains a header, `REGISTER_REQUEST_HEADER`, that must be filled in by the application. The `msgType` field must be filled in to indicate which registration message should be sent to the Cisco IOS Gatekeeper.

### Return

The return for this function is the [STATUS\\_TYPE](#). Possible values for `STATUS_TYPE` are:

- **PROCESSING\_SUCCESSFUL**—No errors were encountered.
- **CONNECT\_IN\_PROGRESS**—Connection is pending. The application should retry this API call after some time has passed.

- **TCP\_WRITE\_ERROR**—A TCP write error was encountered. The application should call `CloseGateKeeperConnection` to close the connection to the Cisco IOS Gatekeeper.
- **MEM\_ALLOC\_FAIL**—Memory allocation failed.
- **TCP\_CONNECTION\_CLOSED**—The connection to the Cisco IOS Gatekeeper has been closed. The application must call `CloseGateKeeperConnection` to free resources such as `gkHandle` in the `GKAPI SOCK_INFO` structure.
- **INVALID\_MSG\_SPECIFIED**—The message type is not within the `RESPONSE_MSG_TYPE` range.
- **INVALID\_ENDPOINT\_SPECIFIED**—The endpoint does not match one of the possible values for `ENDPOINT_TYPE`.
- **INVALID\_REDIRECT\_REASON\_SPECIFIED**—The redirect reason does not match one of the possible values for `REDIRECT_REASON_TYPE`.
- **HEADER\_INFO\_INCOMPLETE**—One of the fields in the header (To, From, TransactionID) is incomplete.
- **NULL\_POINTER\_PASSED**—The pointer to the `GK_REGISTER_MSG` is null.

The following initialization values indicate that the parameter should not be sent to the Cisco IOS Gatekeeper for Registration, and the external application is not interested in these parameters:

- `REDIRECT_REASON_TYPE - REDIRECT_REASON_INFO_NOT_RCVD`
- `ENDPOINT_TYPE - ENDPOINT_INFO_NOT_RCVD`

## WriteUnregisterMessage

This function sends an unregister message to the Cisco IOS Gatekeeper when the application no longer wants to receive a particular message. This structure contains `REGISTER_MSG_TYPE`, which is an enumeration of messages that can be unregistered with the Cisco IOS Gatekeeper.

### Input

The input for this function is:

- A pointer to the `GKAPI SOCK_INFO` structure.
- A pointer to the `GK_UNREGISTER_MSG` structure, which contains the To, From, and Priority fields that must be filled in by the application. The `msgType` must be filled in to indicate which message needs to be unregistered.

### Return

The return for this function is the `STATUS_TYPE`. Possible values for `STATUS_TYPE` are:

- **PROCESSING\_SUCCESSFUL**—No errors were encountered.
- **CONNECT\_IN\_PROGRESS**—Connection is pending. The application should retry this API call after some time has passed.
- **TCP\_WRITE\_ERROR**—A TCP write error was encountered. The application should call `CloseGateKeeperConnection` to close the connection to the Cisco IOS Gatekeeper.
- **MEM\_ALLOC\_FAIL**—Memory allocation failed.

- **TCP\_CONNECTION\_CLOSED**—The connection to the Cisco IOS Gatekeeper has been closed. The application must call `CloseGateKeeperConnection` to free resources such as `gkHandle` in the `GKAPI SOCK_INFO` structure.
- **INVALID\_MSG\_SPECIFIED**—The message type is not within the `RESPONSE_MSG_TYPE` range.
- **HEADER\_INFO\_INCOMPLETE**—One of the fields in the header (To, From, TransactionID) is incomplete.
- **NULL\_POINTER\_PASSED**—The pointer to the `GK_UNREGISTER_MSG` is null.

## GkapiSetupReport

This function allows the application to control the type of debug messages that the Gatekeeper API provides and the location of the debug output.

### Input

The input for this function is:

- An integer that indicates the type of debugging. If the debugging is set to 0, the Gatekeeper API will not output any debug messages.
- A pointer to the [REPORT\\_DEST\\_T](#) enumeration, which indicates the destination for the debug messages.

### Return

There is no return for this function.

## GkapiQueryReport

This function returns the current debug setting for the Gatekeeper API.

### Input

There is no input for this function.

### Return

The return for this function is an integer that indicates the type of debugging being performed by the Gatekeeper API.

# API Structures

The Gatekeeper API stores all data received from the Cisco IOS Gatekeeper in structures. The structures point to character strings, integers, and often enumerations (which are lists of possible values for a specific field). The structures used by the Gatekeeper API are:

- GKAPI SOCK\_INFO
- GKAPI\_TCP\_ADDR\_INFO
- GKAPI\_VERSION\_INFO
- GK\_CMD\_MSG\_TYPE
- CMD\_HEADER\_INFO
- GK\_REGISTER\_MSG
- GK\_UNREGISTER\_MSG
- REG\_UNREG\_RESP\_MSG
- REGISTER\_REQUEST\_HEADER
- REGISTER\_RESPONSE\_HEADER
- ARQ\_REGISTER\_MSG
- RRQ\_REGISTER\_MSG
- URQ\_REGISTER\_MSG
- LRQ\_REGISTER\_MSG
- LCF\_REGISTER\_MSG
- LRJ\_REGISTER\_MSG
- RAI\_REGISTER\_MSG
- DRQ\_REGISTER\_MSG
- BRQ\_REGISTER\_MSG
- GK\_READ\_MSG
- HEADER\_INFO
- ARQ\_REQUEST\_MSG
- RRQ\_REQUEST\_MSG
- URQ\_REQUEST\_MSG
- LRQ\_REQUEST\_MSG
- LCF\_REQUEST\_MSG
- LRJ\_REQUEST\_MSG
- RAI\_REQUEST\_MSG
- DRQ\_REQUEST\_MSG
- BRQ\_REQUEST\_MSG
- IRR\_REQUEST\_MSG
- ALV\_REQUEST\_MSG
- GK\_WRITE\_MSG

- ARQ\_RESPONSE\_MSG
- ACF\_RESPONSE\_MSG
- ARJ\_RESPONSE\_MSG
- RRQ\_RESPONSE\_MSG
- RCF\_RESPONSE\_MSG
- RRJ\_RESPONSE\_MSG
- LRQ\_RESPONSE\_MSG
- LCF\_RESPONSE\_MSG
- LRJ\_RESPONSE\_MSG
- BRQ\_RESPONSE\_MSG
- BCF\_RESPONSE\_MSG
- BRJ\_RESPONSE\_MSG
- ALV\_RESPONSE\_MSG
- CRYPTO\_H323\_TOKEN
- CRYPTO\_EP\_PWD\_HASH
- CRYPTO\_EP\_PWD\_ENCR
- CRYPTO\_EP\_CERT
- CLEAR\_TOKEN
- ALTERNATE\_GK
- ALTERNATE\_ENDPOINT
- ALTERNATE\_TRANSPORT\_ADDR\_TYPE
- RIP\_RESPONSE\_MSG
- UNSUPPORTED\_MSG
- SERV\_CNTRL\_TYPE
- URQ\_CMD\_MSG\_TYPE
- URQ\_RESULT\_MSG
- CALL\_CAPACITY
- CALLS\_AVAILABLE
- CARRIER\_INFO
- PER\_CALLINFO
- REMOTE\_ZONE
- TERMINATION\_CAUSE\_TYPE

## GKAPI SOCK\_INFO

The GKAPI SOCK\_INFO structure is used by several API functions to identify the connection to the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-1](#):

**Table 5-1 GKAPI SOCK\_INFO**

Field	Field Type	Description
TCPPort	Integer	The TCP port of the Cisco IOS Gatekeeper that is establishing the incoming connection to the application.
IPAddress	Character string	The IP address of the Cisco IOS Gatekeeper that is establishing the incoming connection to the application.
gkHandle	Integer	Handle to the Cisco IOS Gatekeeper function.
serverHandle	Integer	Handle to the server function.

TCPPort and IPAddress are provided by the calling function. The API writes the handle into gkHandle and serverHandle when the connection is established. If an error is encountered in the handle creation or in the connection, the gkHandle will be set to -1. The external application is responsible for storing the handle and using it to read, write, and close the connection.

## GKAPI TCP\_ADDR\_INFO

The GKAPI TCP\_ADDR\_INFO structure is used to store the TCP Port and IP address. This structure contains the fields shown in [Table 5-2](#):

**Table 5-2 GKAPI TCP\_ADDR\_INFO**

Field	Field Type	Description
TCPPort	Integer	The TCP port that the Cisco IOS Gatekeeper uses for handling GKTMP messages. For GkapiSetupServer, this is the TCP port that the application uses for interacting with the Gatekeeper.
IPAddress	Unsigned long	For GkapiSetupClient, this is the IP address that the Cisco IOS Gatekeeper uses for handling GKTMP messages. For GkapiSetupServer, this is the IP address that the application uses for interacting with the Gatekeeper.

## GKAPI\_VERSION\_INFO

The GKAPI\_VERSION\_INFO structure is used to store the major and minor version numbers of the gatekeeper TMP and API. This structure contains the fields shown in [Table 5-3](#):

**Table 5-3 GKAPI\_VERSION\_INFO**

Field	Field Type	Description
gkapi_major	Integer	The major number identifying the version of the API.
gkapi_minor	Integer	The minor number identifying the version of the API.
gktmp_major	Integer	The major number identifying the version of the TMP.
gktmp_minor	Integer	The minor number identifying the version of the TMP.
GKAPI_MAX_VER_STR_LEN	Character string	The build date and target operating system of the protocol.
gkapi_release_num	Integer	The release number of the gatekeeper API.

## GK\_CMD\_MSG\_TYPE

The GK\_CMD\_MSG\_TYPE structure is used to process commands from the external application to the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-4](#):

**Table 5-4 GK\_CMD\_MSG\_TYPE**

Field	Field Type	Description
msgType	Enumeration	See <a href="#">CMD_MSG_TYPE</a> .
urqCmdMsg	Structure	See <a href="#">URQ_CMD_MSG_TYPE</a> .

## CMD\_HEADER\_INFO

The CMD\_HEADER\_INFO structure is used to process header information sent by the application to the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-5](#):

**Table 5-5 CMD\_HEADER\_INFO**

Field	Field Type	Description
versionId	Integer	Identifier of the version of GKTMP being used. For the initial release, the only possible value is 1.
from	Character string	Originator of the message. For commands from the external application, this field contains the server ID. The limit of this field is MAX_ENDPOINT_LENGTH + 1.
to	Character string	Receiver of the message. For commands from the external application, this field contains the ID of the gatekeeper that initiated the request. The limit of this field is MAX_ENDPOINT_LENGTH+1.

**Table 5-5** *CMD\_HEADER\_INFO (continued)*

Field	Field Type	Description
transactionID	Character string	Identifier of the transaction. If this field is present in the command to the Cisco IOS Gatekeeper, it must be echoed in the result to the external application. The limit of this field is MAX_TRANSACTION_ID_LENGTH + 1.
notification	Boolean	Whether the message is for notification purposes only.

## GK\_REGISTER\_MSG

The GK\_REGISTER\_MSG structure is used to send registration messages to the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-6](#):

**Table 5-6** *GK\_REGISTER\_MSG*

Field	Field Type	Description
msgType	Enumeration	See <a href="#">REGISTER_MSG_TYPE</a> .
rrqRegMsg	Structure	See <a href="#">RRQ_REGISTER_MSG</a> .
urqRegMsg	Structure	See <a href="#">URQ_REGISTER_MSG</a> .
arqRegMsg	Structure	See <a href="#">ARQ_REGISTER_MSG</a> .
lrqRegMsg	Structure	See <a href="#">LRQ_REGISTER_MSG</a> .
lcfRegMsg	Structure	See <a href="#">LCF_REGISTER_MSG</a> .
lrjRegMsg	Structure	See <a href="#">LRJ_REGISTER_MSG</a> .

## GK\_UNREGISTER\_MSG

The GK\_UNREGISTER\_MSG structure is used to send unregistration messages to the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-7](#):

**Table 5-7** *GK\_UNREGISTER\_MSG*

Field	Field Type	Description
unregisterMsg	Enumeration	See <a href="#">REGISTER_MSG_TYPE</a> .
versionId	Integer	Identifier of the version of GKTMP being used. For the initial release, the only possible value is 1.
from	Character string	Originator of the message. For requests from the Cisco IOS Gatekeeper, this field contains the gatekeeper ID. For responses from the external application, this field contains the server ID. The limit of this field is MAX_ENDPOINT_LENGTH + 1.

**Table 5-7 GK\_UNREGISTER\_MSG (continued)**

Field	Field Type	Description
to	Character string	Receiver of the message. For requests from the Cisco IOS Gatekeeper, this field contains the server ID. For responses from the external application, this field contains the ID of the gatekeeper that initiated the request. The limit of this field is MAX_ENDPOINT_LENGTH + 1.
priority	Integer	Priority of the filter. Possible values are 1 through 20. 1 is the highest priority.

## REG\_UNREG\_RESP\_MSG

The REG\_UNREG\_RESP\_MSG structure is used to process registration and unregistration responses from the Cisco IOS Gatekeeper. This structure contains the field shown in [Table 5-8](#):

**Table 5-8 REG\_UNREG\_RESP\_MSG**

Field	Field Type	Description
regHeader	Structure	See <a href="#">REGISTER_RESPONSE_HEADER</a> .

## REGISTER\_REQUEST\_HEADER

The REGISTER\_REQUEST\_HEADER structure is used when a registration request is to be sent to Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-9](#):

**Table 5-9 REGISTER\_REQUEST\_HEADER**

Field	Field Type	Description
versionId	Integer	Identifier of the version of GKTMP being used. For the initial release, the only possible value is 1.
from	Character string	Originator of the message, which for registration requests is the server ID. The limit of this field is MAX_ENDPOINT_LENGTH+1.
to	Character string	Receiver of the message, which for registration requests is the gatekeeper ID. The limit of this field is MAX_ENDPOINT_LENGTH+1.
priority	Integer	Priority of the filter. Possible values are 1 through 20. 1 is the highest priority.
notificationOnly	Boolean	Whether the registration request is for notifications only. If this field is set to True, messages that match the specified trigger parameters are sent on a notification-only basis.

## REGISTER\_RESPONSE\_HEADER

The REGISTER\_RESPONSE\_HEADER structure is used when a registration or unregistration response is received from the Cisco IOS Gatekeeper. The registration or unregistration response is received after the application sends a registration or unregistration request to the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-10](#):

**Table 5-10 REGISTER\_RESPONSE\_HEADER**

Field	Field Type	Description
version-id	Integer	Identifier of the version of GKTMP being used. For the initial release, the only possible value is 1.
from	Character string	Originator of the message, which for registration responses is the gatekeeper ID. The limit of this field is MAX_ENDPOINT_LENGTH+1.
to	Character string	Receiver of the message, which for registration responses is the server ID. The limit of this field is MAX_ENDPOINT_LENGTH+1.
priority	Integer	Priority of the filter. Possible values are 1 through 20. 1 is the highest priority.
regStatus	Enumeration	See <a href="#">REG_STATUS_TYPE</a> .

## ARQ\_REGISTER\_MSG

The ARQ\_REGISTER\_MSG structure is used to send registrations for ARQ requests to the Cisco IOS Gatekeeper.

This structure contains the fields shown in [Table 5-11](#):

**Table 5-11 ARQ\_REGISTER\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">REGISTER_REQUEST_HEADER</a> .
destinationInfo	Character string	Sequence of alias addresses for the destination endpoint. The limit of this field is MAX_NUM_ARQ_DEST_INFO.
redirectReason	Enumeration	Taken from the Q.931 Setup Redirecting Number IE. See <a href="#">REDIRECT_REASON_TYPE</a> . The limit of this field is MAX_NUM_ARQ_REDIRECT_REASON.

## RRQ\_REGISTER\_MSG

The RRQ\_REGISTER\_MSG structure is used to send registrations for RRQ requests to the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-12](#):

**Table 5-12 RRQ\_REGISTER\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">REGISTER_REQUEST_HEADER</a> .
terminalType	Enumeration	Type of endpoint being registered. See <a href="#">ENDPOINT_TYPE</a> . The limit of this field is MAX_NUM_ENDPOINT_TYPES.
supportedPrefix	Character string	Prefix associated with the supported protocol. The limit of this field is MAX_NUM_SUPPORTED_PREFIX.

## URQ\_REGISTER\_MSG

The URQ\_REGISTER\_MSG structure is used to send registrations for URQ requests to the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-13](#):

**Table 5-13 URQ\_REGISTER\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">REGISTER_REQUEST_HEADER</a> .
terminalType	Enumeration	Type of endpoint being unregistered. See <a href="#">ENDPOINT_TYPE</a> . The limit of this field is MAX_NUM_ENDPOINT_TYPES.
supportedPrefix	Character string	Prefix associated with the supported protocol. The limit of this field is MAX_NUM_SUPPORTED_PREFIX.

## LRQ\_REGISTER\_MSG

The LRQ\_REGISTER\_MSG structure is used to send registrations for LRQ requests to the Cisco IOS Gatekeeper.

This structure contains the fields shown in [Table 5-14](#):

**Table 5-14 LRQ\_REGISTER\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">REGISTER_REQUEST_HEADER</a> .
destinationInfo	Character string	Sequence of alias addresses for the destination endpoint. The limit of this field is MAX_NUM_LRQ_DEST_INFO.
redirectReason	Enumeration	Taken from the Q.931 Setup Redirecting Number IE. See <a href="#">REDIRECT_REASON_TYPE</a> . The limit of this field is MAX_NUM_LRQ_REDIRECT_REASON.

## LCF\_REGISTER\_MSG

The LCF\_REGISTER\_MSG structure is used to send registrations for LCF requests to the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-15](#):

**Table 5-15 LCF\_REGISTER\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">REGISTER_REQUEST_HEADER</a> .
destinationInfo	Character string	Sequence of alias addresses for the destination endpoint. The limit of this field is MAX_NUM_LCF_DEST_INFO.
rmotExtensionAddr	Character String	Alias address of a called endpoint, present in cases where this information is required to traverse multiple gateways. The limit of this field is MAX_NUM_LCF_RMOT_EXTENSION_ADDR.

## LRJ\_REGISTER\_MSG

The LRJ\_REGISTER\_MSG structure is used to send registrations for LRJ requests to the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-16](#):

**Table 5-16 LRJ\_REGISTER\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">REGISTER_REQUEST_HEADER</a> .
destinationInfo	Character string	Sequence of alias addresses for the destination endpoint. The limit of this field is MAX_NUM_LRJ_DEST_INFO.

## RAI\_REGISTER\_MSG

The RAI\_REGISTER\_MSG structure is used to send registrations for RAI requests to the Cisco IOS Gatekeeper.

This structure contains the fields shown in [Table 5-17](#):

**Table 5-17 RAI\_REGISTER\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">REGISTER_REQUEST_HEADER</a> .
terminalType	Enumeration	Type of endpoint. See <a href="#">ENDPOINT_TYPE</a> . The limit of this field is MAX_NUM_ENDPOINT_TYPES.
supportedPrefix	Character string	Prefix associated with the supported protocol. The limit of this field is MAX_NUM_SUPPORTED_PREFIX.

## DRQ\_REGISTER\_MSG

The DRQ\_REGISTER\_MSG structure is used to send registrations for DRQ requests to the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-18](#):

**Table 5-18 RAI\_REGISTER\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">REGISTER_REQUEST_HEADER</a> .
destinationInfo	Character string	Sequence of alias addresses for the destination endpoint. The limit of this field is MAX_NUM_ARQ_DEST_INFO.
redirectReason	Enumeration	Taken from the Q.931 Setup Redirecting Number IE. See <a href="#">REDIRECT_REASON_TYPE</a> . The limit of this field is MAX_NUM_LRQ_REDIRECT_REASON.

## BRQ\_REGISTER\_MSG

The BRQ\_REGISTER\_MSG structure is used to send registrations for BRQ requests to the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-19](#):

**Table 5-19 BRQ\_REGISTER\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">REGISTER_REQUEST_HEADER</a> .
destinationInfo	Character string	Sequence of alias addresses for the destination endpoint. The limit of this field is MAX_NUM_ARQ_DEST_INFO.
redirectReason	Enumeration	Taken from the Q.931 Setup Redirecting Number IE. See <a href="#">REDIRECT_REASON_TYPE</a> . The limit of this field is MAX_NUM_ARQ_REDIRECT_REASON.

## GK\_READ\_MSG

The GK\_READ\_MSG structure is used process REQUEST messages from the Cisco IOS Gatekeeper for the supported RAS messages, as well as registration and unregistration responses from the Cisco IOS Gatekeeper for the supported RAS messages. This structure contains the fields shown in [Table 5-20](#):

**Table 5-20 GK\_READ\_MSG**

Field	Field Type	Description
msgType	Enumeration	See <a href="#">REQUEST_MSG_TYPE</a> .
rrqReqMsg	Structure	See <a href="#">RRQ_REQUEST_MSG</a> .
urqReqMsg	Structure	See <a href="#">URQ_REQUEST_MSG</a> .
arqReqMsg	Structure	See <a href="#">ARQ_REQUEST_MSG</a> .

**Table 5-20 GK\_READ\_MSG (continued)**

Field	Field Type	Description
lrqReqMsg	Structure	See <a href="#">LRQ_REQUEST_MSG</a> .
lcfReqMsg	Structure	See <a href="#">LCF_REQUEST_MSG</a> .
lrjReqMsg	Structure	See <a href="#">LRJ_REQUEST_MSG</a> .
raireqMsg	Structure	See <a href="#">RAI_REQUEST_MSG</a> .
drqreqMsg	Structure	See <a href="#">DRQ_REQUEST_MSG</a> .
brqreqMsg	Structure	See <a href="#">BRQ_REQUEST_MSG</a> .
unsupportedMsg	Structure	See <a href="#">UNSUPPORTED_MSG</a> .
regUnregRespMsg	Structure	See <a href="#">REG_UNREG_RESP_MSG</a> .

If the message received from the Cisco IOS Gatekeeper is a RAS message that is not supported by the API function, the msgType is set to MSG\_NOT\_SUPPORTED. If a response is required, an appropriate response is constructed by the API function and sent to the Cisco IOS Gatekeeper. The header information in the [UNSUPPORTED\\_MSG](#) structure is filled in by the API function. This situation could occur if the Cisco IOS Gatekeeper has been upgraded to support new messages but the API function has not been correspondingly upgraded.

If the message received from the Cisco IOS Gatekeeper, is not recognized by the API function, the msgType is set to UNKNOWN\_MSG and the STATUS\_TYPE is set to MSG\_READ\_ERROR. In this case, the external application should close the connection to the Cisco IOS Gatekeeper by calling the CloseGateKeeperConnection function.

## HEADER\_INFO

The HEADER\_INFO structure is used to process header information sent from the Cisco IOS Gatekeeper or information that is sent by the application to the Cisco IOS Gatekeeper.

This structure contains the fields shown in [Table 5-21](#):

**Table 5-21 HEADER\_INFO**

Field	Field Type	Description
versionId	Integer	Identifier of the version of GKTMP being used. For the initial release, the only possible value is 1.
from	Character string	Originator of the message. For requests from the Cisco IOS Gatekeeper, this field contains the gatekeeper ID. For responses from the external application, this field contains the server ID. The limit of this field is MAX_ENDPOINT_LENGTH + 1.
to	Character string	Receiver of the message. For requests from the Cisco IOS Gatekeeper, this field contains the server ID. For responses from the external application, this field contains the ID of the gatekeeper that initiated the request. The limit of this field is MAX_ENDPOINT_LENGTH+1.

**Table 5-21** *HEADER\_INFO (continued)*

Field	Field Type	Description
transactionID	Character string	Identifier of the transaction. If this field is present in the request from the Cisco IOS Gatekeeper, it must be echoed in the response from the external application. The limit of this field is MAX_TRANSACTION_ID_LENGTH + 1.
notification	Boolean	Whether the message is for notification purposes only. This field is used only in REQUEST messages that are received from the Cisco IOS Gatekeeper.

## ARQ\_REQUEST\_MSG

The ARQ\_REQUEST\_MSG structure is used to process ARQ requests from the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-22](#):

**Table 5-22** *ARQ\_REQUEST\_MSG*

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
srcInfo	Character string	Sequence of alias addresses for the source endpoint.
srcCallSignalAddress	Character string	Transport address used at the source for call signaling.
destinationInfo	Character string	Sequence of alias addresses for the destination endpoint.
destCallSignalAddress	Character string	Transport address used at the destination for call signaling.
destExtraCallInfo	Character string	External addresses for multiple calls.
bandWidthPresent	Boolean	Whether a specified bandwidth is present in the request.
bandWidth	Unsigned integer	Bandwidth (in 100 kbps) requested for the bi-directional call.
answerCall	Integer	Indicates to the Cisco IOS Gatekeeper that the call is incoming.
callIdentifier	Character string	A unique call identifier (set by the originating endpoint), which can be used to associate RAS signaling with the modified Q.931 signaling used in H.225.0.
conferenceID	Character string	A unique conference identifier.
canMapAlias	Integer	Whether the endpoint can copy information from the resulting ACF into the destinationAddress, destExtraCallInfo, and remoteExtensionAddress fields of the SETUP message.
redirectNumber	Character string	Taken from the Number Digits field of Q.931 Setup Redirecting Number IE.
redirectReason	Enumeration	Taken from the Q.931 Setup Redirecting Number IE. See <a href="#">REDIRECT_REASON_TYPE</a> .
callingOctet3a	Character String	Whether the calling number information can be displayed.

**Table 5-22 ARQ\_REQUEST\_MSG (continued)**

Field	Field Type	Description
displayIE	Character String	Taken from the Q.931 Setup, display IE.
endPointCallSignalAddress	Character String	Call signaling transport address of the endpoint sending the ARQ.
cryptoToken	Pointer	See <a href="#">ALV_RESPONSE_MSG</a> .
clearToken	Pointer	See <a href="#">CLEAR_TOKEN</a> .
srcCarrierID	Character String	Carrier identifier of an inbound call
dstCarrierID	Character String	Target carrier identifier of an outbound call
srcTrunkGroup	Character String	Trunk group of an inbound call
dstTrunkGroup	Character String	Target trunk group of an outbound call
call_capacity	Pointer	The call capacity information of the gateway
gtd	Character String	Generic Transparency Descriptor. Defines parameters and messages of existing SS7 ISUP protocols
terminationCause	Character String	Informs the GKTMP server of the release complete Cause IE that was sent to the gatekeeper. See <a href="#">TERMINATION_CAUSE_TYPE</a> .
r_count	Unsigned Integer	Used to send additional ARQ messages to the gatekeeper and then to a route server after all alternative endpoints returned in the first ARQ message have failed. Subsequent ARQ messages use the same global call ID and also have a reroute count of one for the first reroute request, which is incremented for each subsequent reroute request.
serviceCntrl	Character String	Service control. See <a href="#">SERV_CNTRL_TYPE</a> .

## RRQ\_REQUEST\_MSG

The RRQ\_REQUEST\_MSG structure is used to process RRQ requests from the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-23](#):

**Table 5-23 RRQ\_REQUEST\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
callSignalAddress	Character string	Call signaling transport address for this endpoint.
rasAddress	Character string	Registration and status transport address for this endpoint.
terminalAlias	Character string	List of alias addresses by which other terminals can identify this terminal.
terminalType	Enumeration	Type of endpoint being registered. See <a href="#">ENDPOINT_TYPE</a> .
supportedPrefix	Character string	Prefix associated with the supported protocol.

**Table 5-23 RRO\_REQUEST\_MSG (continued)**

Field	Field Type	Description
cryptoToken	Pointer	See <a href="#">ALV_RESPONSE_MSG</a> .
clearToken	Pointer	See <a href="#">CLEAR_TOKEN</a> .
altTranspAddr	Pointer	See <a href="#">ALTERNATE_TRANSPORT_ADDR_TYPE</a> .
capacityReportingCapability	Boolean	If True, indicates the gateway can report call capacity
call_capacity	Pointer	The call capacity information of the gateway

## URQ\_REQUEST\_MSG

The URQ\_REQUEST\_MSG structure is used to process URQ requests from the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-24](#):

**Table 5-24 URQ\_REQUEST\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
callSignalAddress	Character string	Call signaling transport address for this endpoint.

## LRQ\_REQUEST\_MSG

The LRQ\_REQUEST\_MSG structure is used to process LRQ requests from the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-25](#):

**Table 5-25 LRQ\_REQUEST\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
srcInfo	Character string	Sequence of alias addresses for the source endpoint.
destinationInfo	Character string	Sequence of alias addresses for the destination endpoint.
redirectNumber	Character string	Taken from the Number Digits field of Q.931 Setup Redirecting Number IE.
redirectReason	Enumeration	Taken from the Q.931 Setup Redirecting Number IE. See <a href="#">REDIRECT_REASON_TYPE</a> .
callingOctet3a	Character String	Whether the calling number information can be displayed.
displayIE	Character String	Taken from the Q.931 Setup, display IE.
callingPartyNum	Character String	Taken from the Q.931.
srcCarrierID	Character String	Carrier identifier of an inbound call
dstCarrierID	Character String	Target carrier identifier of an outbound call
bandWidthPresent	Boolean	Indicates if bandwidth has been received

**Table 5-25 LRO\_REQUEST\_MSG (continued)**

Field	Field Type	Description
bandWidth	Unsigned Integer	Bandwidth (in 100 kpbs) requested for a bidirectional call
callIdentifier	Character String	Indicates the type of call, such as a voice call
srcTrunkGroup	Character String	Source trunk group identifier of an inbound call
dstTrunkGroup	Character String	Destination trunk group identifier of an outbound call
gtd	Character String	Generic Transparency Descriptor. Defines parameters and messages of existing SS7 ISUP protocols
terminationCause	Character String	Informs the GKTMP server of the release complete Cause IE that was sent to the gatekeeper. See <a href="#">TERMINATION_CAUSE_TYPE</a> .
r_count	Unsigned Integer	Used to send additional ARQ messages to the gatekeeper and then to a route server after all alternative endpoints returned in the first ARQ message have failed. Subsequent ARQ messages use the same global call ID and also have a reroute count of one for the first reroute request, which is incremented for each subsequent reroute request.

## LCF\_REQUEST\_MSG

The LCF\_REQUEST\_MSG structure is used to process LCF requests from the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-26](#):

**Table 5-26 LCF\_REQUEST\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
srcInfo	Character string	Sequence of alias addresses for the source endpoint.
destinationInfo	Character string	Sequence of alias addresses for the destination endpoint.
callSignalAddress	Character string	Call signaling transport address for this endpoint.
destExtraCallInfo	Character string	External addresses for multiple calls.
redirectNumber	Character string	Taken from the Number Digits field of Q.931 Setup Redirecting Number IE.
redirectReason	Enumeration	Taken from the Q.931 Setup Redirecting Number IE. See <a href="#">REDIRECT_REASON_TYPE</a> .
callingOctet3a	Character String	Whether the calling number information can be displayed.
callingPartyNum	Character String	Taken from the Q.931.
displayIE	Character String	Taken from the Q.931 Setup, display IE.
rasAddress	Character String	Registration and status transport address for this endpoint.

**Table 5-26 LCF\_REQUEST\_MSG (continued)**

Field	Field Type	Description
rmotExtensionAddr	Character String	Alias address of a called endpoint, present in cases where this information is required to traverse multiple gateways.
destinationType	Enumeration	Type of destination endpoint. See <a href="#">ENDPOINT_TYPE</a> .
altTranspAddr	Pointer	See <a href="#">ALTERNATE_TRANSPORT_ADDR_TYPE</a> .
gtd	Character String	Generic Transparency Descriptor. Defines parameters and messages of existing SS7 ISUP protocols
serviceCntrl	Parameter	LRQ:serviceControl. See <a href="#">SERV_CNTRL_TYPE</a> .
callIdentifier	Character String	ARQ:callIdentifier

## LRJ\_REQUEST\_MSG

The LRJ\_REQUEST\_MSG structure is used to process LRJ requests from the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-27](#):

**Table 5-27 LRJ\_REQUEST\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
srcInfo	Character string	Sequence of alias addresses for the source endpoint.
destinationInfo	Character string	Sequence of alias addresses for the destination endpoint.
redirectNumber	Character string	Taken from the Number Digits field of Q.931 Setup Redirecting Number IE.
redirectReason	Enumeration	Taken from the Q.931 Setup Redirecting Number IE. See <a href="#">REDIRECT_REASON_TYPE</a> .
callingOctet3a	Character String	Whether the calling number information can be displayed.
displayIE	Character String	Taken from the Q.931 Setup, display IE.
callingPartyNum	Character String	Taken from the Q.931.
rejectReason	Enumeration	Reason for the rejection of the request. See <a href="#">LRJ_REJECT_REASON_TYPE</a> .
serviceCntrl	Parameter	LRQ:serviceControl. See <a href="#">SERV_CNTRL_TYPE</a> .
callIdentifier	Character String	LRQ:callIdentifier

## RAI\_REQUEST\_MSG

The RAI\_REQUEST\_MSG structure is used to process RAI requests from the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-28](#):

**Table 5-28 RAI\_REQUEST\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">REGISTER_REQUEST_HEADER</a> .
callSignalAddress	Character string	Call signaling transport address for this endpoint.
almostOut	Integer	Resource usage indication. The value is TRUE or FALSE.
call_capacity	Pointer	The call capacity information of the gateway

## DRQ\_REQUEST\_MSG

The DRQ\_REQUEST\_MSG structure is used to process DRQ requests from the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-29](#):

**Table 5-29 DRQ\_REQUEST\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">REGISTER_REQUEST_HEADER</a> .
drqReason	Enumeration	Reason received for a DRQ sent by an endpoint. See <a href="#">DRQ_REASON_TYPE</a> .
srcCallSignalAddress	Character string	Transport address used at the source for call signaling.
answeredCall	Integer	Indicates that this party was the original destination. The value is TRUE or FALSE.
callIdentifier	Character string	A unique call identifier (set by the originating endpoint) which can be used to associate RAS signaling with the modified Q.931 signaling used in H225.0.
conferenceID	Character string	A unique identifier.
clearToken	Pointer	See <a href="#">CLEAR_TOKEN</a> .
call_capacity	Pointer	The call capacity information of the gateway
gtd	Character String	Generic Transparency Descriptor. Defines parameters and messages of existing SS7 ISUP protocols
terminationCause	Character String	Informs the GKTMP server of the release complete Cause IE that was sent to the gatekeeper. See <a href="#">TERMINATION_CAUSE_TYPE</a> .

## BRQ\_REQUEST\_MSG

The BRQ\_REQUEST\_MSG structure is used to process BRQ requests from the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-30](#):

**Table 5-30 BRQ\_REQUEST\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
answerCall	Integer	Indicates to the Cisco IOS Gatekeeper that the call is incoming.
bandWidth	Unsigned integer	Bandwidth (in 100 kbps) requested for the bi-directional call.
callIdentifier	Character string	A unique call identifier (set by the originating endpoint), which can be used to associate RAS signaling with the modified Q.931 signaling used in H.225.0.
conferenceID	Character string	A unique conference identifier.
endPointCallSignal Address	Character string	Call signalling transport address for this endpoint.
cryptoToken	Pointer	See <a href="#">ALV_RESPONSE_MSG</a> .
clearToken	Pointer	See <a href="#">CLEAR_TOKEN</a> .

## IRR\_REQUEST\_MSG

The IRR\_REQUEST\_MSG structure is used to process IRR requests from the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-31](#).

**Table 5-31 IRR\_REQUEST\_MSG**

Field	Field Type	Description
srcCallSignalAddress	Character String	Transport address used at the source for call signaling.
perCallInfo	Character String	Contains information about the call, including the call identifier, conference ID, originator, bandwidth, and call start time.

## ALV\_REQUEST\_MSG

The ALV\_REQUEST\_MSG structure is used to process ALV requests from the Cisco IOS Gatekeeper. This structure contains the fields shown in [Table 5-32](#):

**Table 5-32 ALV\_REQUEST\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .

## GK\_WRITE\_MSG

The GK\_WRITE\_MSG structure is used to process responses from the external application to the Cisco IOS Gatekeeper.

This structure contains the fields shown in [Table 5-33](#):

**Table 5-33 GK\_WRITE\_MSG**

Field	Field Type	Description
msgType	Enumeration	See <a href="#">RESPONSE_MSG_TYPE</a> .
arqRespMsg	Structure	See <a href="#">ARQ_RESPONSE_MSG</a> .
acfRespMsg	Structure	See <a href="#">ACF_RESPONSE_MSG</a> .
arjRespMsg	Structure	See <a href="#">ARJ_RESPONSE_MSG</a> .
rrqRespMsg	Structure	See <a href="#">RRQ_RESPONSE_MSG</a> .
rrjRespMsg	Structure	See <a href="#">RRJ_RESPONSE_MSG</a> .
rcfRespMsg	Structure	See <a href="#">RCF_RESPONSE_MSG</a> .
lrqRespMsg	Structure	See <a href="#">LRQ_RESPONSE_MSG</a> .
lcfRespMsg	Structure	See <a href="#">LCF_RESPONSE_MSG</a> .
lrjRespMsg	Structure	See <a href="#">LRJ_RESPONSE_MSG</a> .
ripRespMsg	Structure	See <a href="#">RIP_RESPONSE_MSG</a> .

## ARQ\_RESPONSE\_MSG

The ARQ\_RESPONSE\_MSG structure is used to process ARQ responses from the external application. This structure contains the fields shown in [Table 5-34](#):

**Table 5-34 ARQ\_RESPONSE\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
destinationInfo	Character string	Sequence of alias addresses for the destination endpoint.
destCallSignalAddress	Character string	Transport address used at the destination for call signaling.
destExtraCallInfo	Character string	External addresses for multiple calls.
bandWidthPresent	Boolean	Whether a specified bandwidth is present in the request.
bandWidth	Unsigned integer	Bandwidth (in 100 kbps) requested for the bidirectional call.
redirectNumber	Character string	Taken from the Number Digits field of Q.931 Setup Redirecting Number IE.
redirectReason	Enumeration	Taken from the Q.931 Setup Redirecting Number IE. See <a href="#">REDIRECT_REASON_TYPE</a> .

**Table 5-34 ARQ\_RESPONSE\_MSG (continued)**

Field	Field Type	Description
displayIE	Character String	Taken from the Q.931 Setup, display IE.
srcCarrierID	Character String	Change source carrier ID to this value
dstCarrierInfo	Pointer	Information about destination carrier
srcInfo	Character String	Identifies the service provider offering the VoIP call to the gateway
rzone	Pointer	Remote zone information to which the gateway can LRQ to
final	Boolean	Do not propagate this message onward
gtd	Character String	Generic Transparency Descriptor. Defines parameters and messages of existing SS7 ISUP protocols
serviceCntrl	Parameter	See <a href="#">SERV_CNTRL_TYPE</a> .

## ACF\_RESPONSE\_MSG

The ACF\_RESPONSE\_MSG structure is used to process ACF responses from the external application. This structure contains the fields shown in [Table 5-35](#):

**Table 5-35 ACF\_RESPONSE\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
destinationInfo	Character string	Sequence of alias addresses for the destination endpoint.
destCallSignalAddress	Character string	Transport address used at the destination for call signaling.
destExtraCallInfo	Character string	External addresses for multiple calls.
rmotExtensionAddr	Character string	Alias address of a called endpoint, present in cases where this information is required to traverse multiple gateways.
bandWidthPresent	Boolean	Whether a specified bandwidth is present in the request.
bandWidth	Unsigned integer	Bandwidth (in 100 kbps) requested for the bidirectional call.
destinationType	Enumeration	Type of destination endpoint. See <a href="#">ENDPOINT_TYPE</a> .
altEndpt	Structure	See <a href="#">ALTERNATE_ENDPOINT</a> .
clearToken	Pointer	See <a href="#">CLEAR_TOKEN</a> .
altTranspAddr	Pointer	See <a href="#">ALTERNATE_TRANSPORT_ADDR_TYPE</a> .
use_transport	Enumeration	See <a href="#">USE_SPECIFIED_TRANSPORT_TYPE_T</a> .
dstCarrierInfo	Pointer	Information about the destination carrier
srcTrunkGroup	Character String	Change source trunk group ID to this value

**Table 5-35** *ACF\_RESPONSE\_MSG (continued)*

Field	Field Type	Description
dstTrunkInfo	Pointer	Information about the destination trunk group
serviceDescriptor	Parameter	See <a href="#">SERV_CNTRL_TYPE</a> .
gtd	Character String	Generic Transparency Descriptor. Defines parameters and messages of existing SS7 ISUP protocols

## ARJ\_RESPONSE\_MSG

The ARJ\_RESPONSE\_MSG structure is used to process ARJ responses from the external application. This structure contains the fields shown in [Table 5-36](#):

**Table 5-36** *ARJ\_RESPONSE\_MSG*

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
rejectReason	Enumeration	Reason the request was rejected. See <a href="#">ARJ_REJECT_REASON_TYPE</a> .
terminationCause	Character String	Informs the GKTMP server of the release complete Cause IE that was sent to the gatekeeper. See <a href="#">TERMINATION_CAUSE_TYPE</a> .

## RRQ\_RESPONSE\_MSG

The RRQ\_RESPONSE\_MSG structure is used to process RRQ responses from the external application. This structure contains the fields shown in [Table 5-37](#):

**Table 5-37** *RRQ\_RESPONSE\_MSG*

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
terminalAlias	Character string	List of alias addresses by which other terminals can identify this terminal.
supportedPrefix	Character string	Prefix associated with the supported protocol.
final	Boolean	Do not propagate this message onward

## RCF\_RESPONSE\_MSG

The RCF\_RESPONSE\_MSG structure is used to process RCF responses from the external application. This structure contains the fields shown in [Table 5-38](#):

**Table 5-38 RCF\_RESPONSE\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
terminalAlias	Character string	List of alias addresses by which other terminals can identify this terminal.
supportedPrefix	Character string	Prefix associated with the supported protocol.
alternateGK	Structure	See <a href="#">ALTERNATE_GK</a> .

## RRJ\_RESPONSE\_MSG

The RRJ\_RESPONSE\_MSG structure is used to process RRJ responses from the external application. This structure contains the fields shown in [Table 5-39](#):

**Table 5-39 RRJ\_RESPONSE\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
rejectReason	Enumeration	Reason the request was rejected. See <a href="#">RRJ_REJECT_REASON_TYPE</a> .

## LRQ\_RESPONSE\_MSG

The LRQ\_RESPONSE\_MSG structure is used to process LRQ responses from the external application. This structure contains the fields shown in [Table 5-40](#):

**Table 5-40 LRQ\_RESPONSE\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
destinationInfo	Character string	Sequence of alias addresses for the destination endpoint.
srcCarrierID	Character String	Change source carrier ID to this value
dstCarrierInfo	Pointer	Information about destination carrier
srcInfo	Character String	Identifies the service provider offering the VoIP call to the gateway
rzone	Pointer	Remote zone information to which the gateway can LRQ to
final	Boolean	Do not propagate this message onward

**Table 5-40 LRO\_RESPONSE\_MSG (continued)**

Field	Field Type	Description
srcTrunkGroup	Character String	Source trunk group identifier of an outbound call
gtd	Character String	Generic Transparency Descriptor. Defines parameters and messages of existing SS7 ISUP protocols

## LCF\_RESPONSE\_MSG

The LCF\_RESPONSE\_MSG structure is used to process LCF responses from the external application. This structure contains the fields shown in [Table 5-41](#):

**Table 5-41 LCF\_RESPONSE\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
destinationInfo	Character string	Sequence of alias addresses for the destination endpoint.
destExtraCallInfo	Character string	External addresses for multiple calls.
callSignalAddress	Character string	Call signaling transport address for this endpoint.
rasAddress	Character String	Registration and status transport address for this endpoint.
rmtExtensionAddr	Character String	Alias address of a called endpoint, present in cases where this information is required to traverse multiple gateways.
destinationType	Enumeration	Type of destination endpoint. See <a href="#">ENDPOINT_TYPE</a> .
altTranspAddr	Pointer	See <a href="#">ALTERNATE_TRANSPORT_ADDR_TYPE</a> .
dstCarrierInfo	Pointer	Information about destination carrier
gtd	Character String	Generic Transparency Descriptor. Defines parameters and messages of existing SS7 ISUP protocols
serviceDescriptor	Parameter	See <a href="#">SERV_CNTRL_TYPE</a> .

## LRJ\_RESPONSE\_MSG

The LRJ\_RESPONSE\_MSG structure is used to process LRJ responses from the external application. This structure contains the fields shown in [Table 5-42](#):

**Table 5-42 LRJ\_RESPONSE\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .

**Table 5-42** *LRJ\_RESPONSE\_MSG (continued)*

Field	Field Type	Description
rejectReason	Enumeration	Reason the request was rejected. See <a href="#">LRJ_REJECT_REASON_TYPE</a> .
terminationCause	Character String	Informs the GKTMP server of the release complete Cause IE that was sent to the gatekeeper. See <a href="#">TERMINATION_CAUSE_TYPE</a> .

## BRQ\_RESPONSE\_MSG

The BRQ\_RESPONSE\_MSG structure is used to process BRQ responses from the external application. This structure contains the fields shown in [Table 5-43](#):

**Table 5-43** *BRQ\_RESPONSE\_MSG*

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
bandWidth	Unsigned integer	Bandwidth (in 100 kbps) requested for the bidirectional call.

## BCF\_RESPONSE\_MSG

The BCF\_RESPONSE\_MSG structure is used to process BCF responses from the external application. This structure contains the fields shown in [Table 5-44](#):

**Table 5-44** *BCF\_RESPONSE\_MSG*

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
bandWidth	Unsigned integer	Bandwidth (in 100 kbps) requested for the bidirectional call.

## BRJ\_RESPONSE\_MSG

The BRJ\_RESPONSE\_MSG structure is used to process BRJ responses from the external application. This structure contains the fields shown in [Table 5-45](#):

**Table 5-45** *BRJ\_RESPONSE\_MSG*

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
rejectReason	Enumeration	See BRJ_REJECT_REASON_TYPE.

## ALV\_RESPONSE\_MSG

The ALV\_RESPONSE\_MSG structure is used to process ALV responses from the external application. This structure contains the fields shown in [Table 5-46](#):

**Table 5-46 ALV\_RESPONSE\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .

## CRYPTO\_H323\_TOKEN

The CRYPTO\_H323\_TOKEN structure is used to process cryptoTokens. This structure contains the fields shown in [Table 5-47](#):

**Table 5-47 CRYPTO\_H323\_TOKEN**

Field	Field Type	Description
token_type	Enumeration	See <a href="#">CRYPTO_H323_TOKEN_TYPE_S</a> .
cryptoEPPwdHash	Structure	See <a href="#">CRYPTO_EP_PWD_HASH</a> .
cryptoEPPwdEncr	Structure	See <a href="#">CRYPTO_EP_PWD_ENCR</a> .
cryptoEPCert	Structure	See <a href="#">CRYPTO_EP_CERT</a> .

## CRYPTO\_EP\_PWD\_HASH

The CRYPTO\_EP\_PWD\_HASH structure is used to process cryptoTokens. This structure contains the sections shown in [Table 5-48](#):

**Table 5-48 CRYPTO\_EP\_PWD\_HASH**

Field	Field Type	Description
alias	Character string	Registration and status transport address for this endpoint.
timestamp	Character string	32-bit integer that represents UTC time.
token	Character string	16 octet IA5String that represents the MD5 hashed encoded PwdCertToken.

## CRYPTO\_EP\_PWD\_ENCR

The CRYPTO\_EP\_PWD\_ENCR structure is used to process the encrypted data of a cryptoToken. This structure contains the fields shown in [Table 5-49](#):

**Table 5-49 CRYPTO\_EP\_PWD\_ENCR**

Field	Field Type	Description
paramS	Character string	Any runtime parameters.
encryptedData	Character string	Encrypted data from the cryptoToken.

## CRYPTO\_EP\_CERT

The CRYPTO\_EP\_CERT structure is used to process the authentication certificate of a cryptoToken. This structure contains the fields shown in [Table 5-50](#):

**Table 5-50 CRYPTO\_EP\_CERT**

Field	Field Type	Description
toBeSigned	Character string	Whether the certificate requires a signature.
signature	Character string	Digital signature assigned to the authentication certificate.

## CLEAR\_TOKEN

The CLEAR\_TOKEN structure is used to process the clear tokens field. This structure contains the fields shown in [Table 5-51](#):

**Table 5-51 CLEAR\_TOKEN**

Field	Field Type	Description
objectIdentifier	Character string	Object identifier.
password	Character string	Secret character string that is used to authenticate a user or H.323 endpoint.
timestamp	Character string	32-bit integer that represents UTC time.
challengeString	Character string	Challenge string used for authentication.
random	Character string	Integer value, for example a monotonically increasing sequence number.
generalID	Character string	Character string that uniquely identifies either the sender or receiver.
nonstd_objectID	Character string	Object identifier that is used to indicate the type and format of the nonstandard data being sent in the clear token.
nonstd_data	Character string	Nonstandard data in the clear tokens field.

## ALTERNATE\_GK

The ALTERNATE\_GK structure is used to process information about an alternate gatekeeper. This structure contains the fields shown in [Table 5-52](#):

**Table 5-52 ALTERNATE GK**

Field	Field Type	Description
rasAddress	Character string	Registration and status transport address for this endpoint.
gkIdentifier	Character string	Identifier of the gatekeeper.
needToRegister	Boolean	Whether there is a need to register with this gatekeeper.
priority	Integer	Priority of this gatekeeper. Possible values are 1 through 127.

## ALTERNATE\_ENDPOINT

The ALTERNATE\_ENDPOINT structure is used to process information about an alternate H.323 endpoint.

This structure contains the fields shown in [Table 5-53](#):

**Table 5-53 ALTERNATE\_ENDPOINT**

Field	Field Type	Description
callSignalAddress	Character string	Registration and status transport address for this endpoint.
tokenP	Structure	See <a href="#">CLEAR_TOKEN</a> .
carrierID	Character string	Carrier identifier
destinationTrunkGroupLabel	Character string	Outgoing trunk group identifier

## ALTERNATE\_TRANSPORT\_ADDR\_TYPE

The ALTERNATE\_TRANSPORT\_ADDR\_TYPE structure is used to convey information about an Annex E transport address of the destination H.323 endpoint. This structure contains the fields shown in [Table 5-54](#):

**Table 5-54 ALTERNATE\_TRANSPORT\_ADDR\_TYPE**

Field	Field Type	Description
annexE	Character string	Annex E transport address of the destination endpoint.
nextP	Pointer	Pointer to the next node in the linked list.

## RIP\_RESPONSE\_MSG

The RIP\_RESPONSE\_MSG structure is used to process requests from the external application for additional time. This structure contains the fields shown in [Table 5-55](#):

**Table 5-55 RIP\_RESPONSE\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .
delay	Integer	Amount of time, in milliseconds (1 through 65,536), that the endpoint should wait before retrying the request.

## UNSUPPORTED\_MSG

The UNSUPPORTED\_MSG structure is used to process requests from the Cisco IOS Gatekeeper that contain a RAS message type that is not supported by the API. This structure contains the field shown in [Table 5-56](#):

**Table 5-56 UNSUPPORTED\_MSG**

Field	Field Type	Description
headerInfo	Structure	See <a href="#">HEADER_INFO</a> .

## SERV\_CNTRL\_TYPE

[Table 5-57](#) shows the fields for the SERV\_CNTRL\_TYPE structure:

**Table 5-57 SERV\_CNTRL\_TYPE**

Field	Field Type	Description
serviceDescriptor	Character String	Code for use in authentication with RADIUS server by endpoint
reason	Character String	Indicates whether this is a new session (open), a modification to an existing session (refresh), or that the session is being terminated by the provider (close) and existing resources, such as a GUI, should be closed.
sessionId	Unsigned Integer	Integer that identifies the current session. This integer is unique for each client.  <b>Note</b> Identifiers received through different signaling paths may overlap.

## URQ\_CMD\_MSG\_TYPE

Table 5-58 shows the fields for the URQ\_CMD\_MSG\_TYPE structure:

**Table 5-58 URQ\_CMD\_MSG\_TYPE**

Field	Field Type	Description
callSignalAddress	Character String	Call signaling address of the endpoint to unregister.
urqReason	Enumeration	See <a href="#">URQ_REASON_TYPE</a> .
altGK	Pointer	Alternate gatekeeper information.

## URQ\_RESULT\_MSG

Table 5-59 shows the fields for the URQ\_RESULT\_MSG structure:

**Table 5-59 URQ\_RESULT\_MSG**

Field	Field Type	Description
callSignalAddress	Character String	Call signaling address of the unregistered endpoint.

## CALL\_CAPACITY

Table 5-60 shows the fields for the CALL\_CAPACITY structure:

**Table 5-60 CALL\_CAPACITY**

Field	Field Type	Description
call_protocol	Pointer	Defines the protocol supported by the endpoint for the call
calls_available	Pointer	Provides call statistics

## CALLS\_AVAILABLE

Table 5-61 shows the fields for the CALLS\_AVAILABLE structure:

**Table 5-61 CALLS\_AVAILABLE**

Field	Field Type	Description
groupID	Character String	Name of the carrier or service provider
bit_mask	Unsigned Character	Used to present either maximum or current calls available
max_call_available	Integer	Maximum calls available
current_calls_available	Integer	Current calls available

## CARRIER\_INFO

Table 5-62 shows the fields for the CARRIER\_INFO structure:

**Table 5-62 CARRIER\_INFO**

Field	Field Type	Description
dstCarrierID	Character String	Target carrier identifier of an outbound call
destinationInfo	Character String	Identifies the service provider offering the VoIP call to the gateway
sourceInfo	Character String	Identifies the service provider offering the VoIP call to the gateway
priority	Integer	Priority associated with the carrier
rzone	Pointer	Remote zone information to which the gateway can LRQ to

## PER\_CALLINFO

Table 5-63 shows the fields for the PER\_CALLINFO structure:

**Table 5-63 PER\_CALLINFO**

Field	Field Type	Description
callIdentifier	Character String	Call Identifier of the call
conferenceID	Character String	Conference identifier for the call
originator	Boolean	Whether the sender was the originator of the call
bandWidth	Unsigned Integer	Bandwidth (in 100 kpbs) requested for a bidirectional call
startTime	Unsigned Long	Start time of the call
srcZone	Character String	Source zone for the call
dstZone	Character String	Destination zone for the call
srcCarrierID	Character String	Source carrier identifier of the call
dstCarrierID	Character String	Destination carrier identifier for the call
sourceTrunk	Character String	Source trunk group identifier of the call
destTrunk	Character String	Destination trunk group identifier for the call

## REMOTE\_ZONE

Table 5-64 shows the fields for the REMOTE\_ZONE structure:

**Table 5-64 REMOTE\_ZONE**

Field	Field Type	Description
rasAddress	Character String	Registration and status address for the remote gatekeeper
cost	Unsigned Integer	Cost factor associated with the remote zone
priority	Unsigned Integer	Priority associated with the remote zone

## TERMINATION\_CAUSE\_TYPE

Table 5-65 shows the fields for the TERMINATION\_CAUSE\_TYPE structure:

**Table 5-65** *TERMINATION\_CAUSE\_TYPE*

Field	Field Type	Description
codingStd	Unsigned Integer	Coding standard
location	Unsigned Integer	Location
recommend	Unsigned Integer	Recommendation
relCause	Unsigned Integer	Cause value
diag0	Unsigned Integer	Diagnostic
diag1	Unsigned Integer	Diagnostic
diag2	Unsigned Integer	Diagnostic
relReason	Unsigned Integer	Reason value

# Enumerations

Some of the API structures contain enumerations. An enumeration is simply a list of possible values. This section lists the enumerations used by the structures and includes the following sections:

- [STATUS\\_TYPE](#), page 5-43
- [REG\\_STATUS\\_TYPE](#), page 5-44
- [ENDPOINT\\_TYPE](#), page 5-44
- [REDIRECT\\_REASON\\_TYPE](#), page 5-44
- [DRQ\\_REASON\\_TYPE](#), page 5-45
- [LRJ\\_REJECT\\_REASON\\_TYPE](#), page 5-45
- [REQUEST\\_MSG\\_TYPE](#), page 5-45
- [RRJ\\_REJECT\\_REASON\\_TYPE](#), page 5-46
- [ARJ\\_REJECT\\_REASON\\_TYPE](#), page 5-46
- [BRJ\\_REJECT\\_REASON\\_TYPE](#), page 5-47
- [URQ\\_REASON\\_TYPE](#), page 5-47
- [RESPONSE\\_MSG\\_TYPE](#), page 5-47
- [REGISTER\\_MSG\\_TYPE](#), page 5-48
- [REPORT\\_DEST\\_T](#), page 5-48
- [CRYPTO\\_H323\\_TOKEN\\_TYPE\\_S](#), page 5-48
- [USE\\_SPECIFIED\\_TRANSPORT\\_TYPE\\_T](#), page 5-48

## STATUS\_TYPE

The STATUS\_TYPE enumeration lists the possible return values from calls to read, write, register and unregister functions. The possible values are:

- PROCESSING\_SUCCESSFUL
- CONNECT\_IN\_PROGRESS
- NULL\_POINTER\_PASSED
- TCP\_HANDLE\_ERROR
- TCP\_CONNECT\_ERROR
- TCP\_READ\_ERROR
- TCP\_BIND\_ERROR
- TCP\_LISTEN\_ERROR
- TCP\_ADDRESS\_ALREADY\_IN\_USE
- TCP\_ADDRESS\_NOT\_AVAIL
- TCP\_NONBLOCK\_ERROR
- MEM\_ALLOC\_FAIL
- MSG\_READ\_ERROR
- TCP\_WRITE\_ERROR

- TCP\_CONNECTION\_CLOSED
- INCOMPLETE\_MSG\_READ
- INVALID\_MSG\_SPECIFIED
- INVALID\_ENDPOINT\_SPECIFIED
- INVALID\_REDIRECT\_REASON\_SPECIFIED
- INVALID\_REJECT\_REASON\_SPECIFIED
- INVALID\_DELAY\_SPECIFIED
- HEADER\_INFO\_INCOMPLETE

## REG\_STATUS\_TYPE

The REG\_STATUS\_TYPE enumeration lists the possible status values for registration and unregistration responses received from the Cisco IOS Gatekeeper. The possible values are:

- SUCCESSFUL
- INVALID\_PRIORITY
- INVALID\_FILTERS
- INVALID\_GKID

## ENDPOINT\_TYPE

The ENDPOINT\_TYPE enumeration lists the possible types of endpoints. The possible values are:

- GATEKEEPER
- TERMINAL
- MCU
- PROXY
- VOICEGATEWAY
- H320GATEWAY
- OTHERGATEWAY
- ENDPOINT\_INFO\_NOT\_RCVD

## REDIRECT\_REASON\_TYPE

The REDIRECT\_REASON\_TYPE enumeration lists the possible reasons that a call might be redirected. The possible values are:

- REDIRECT\_REASON\_UNKNOWN = 0
- REDIRECT\_REASON\_CALL\_FWD\_BUSY = 1
- REDIRECT\_REASON\_CALL\_FWD\_NO\_REPLY = 2
- REDIRECT\_REASON\_CALL\_DEFLECTION = 4
- REDIRECT\_REASON\_CLED\_DTE\_OUT\_OF\_ORDER = 9

- REDIRECT\_REASON\_CALL\_FWDING\_BY\_CLED\_DTE = 10
- REDIRECT\_REASON\_CALL\_FWDING\_UNCONDNL = 15
- REDIRECT\_REASON\_INFO\_NOT\_RCVD= 99

## DRQ\_REASON\_TYPE

The DRQ\_REASON\_TYPE enumeration lists the reasons received for a DRQ sent by an endpoint. The possible values are:

- DRQ\_REASON\_FORCED\_DROP = 1
- DRQ\_REASON\_NORMAL\_DROP = 2
- DRQ\_REASON\_UNDEF\_REASON = 3

## LRJ\_REJECT\_REASON\_TYPE

The LRJ\_REJECT\_REASON\_TYPE enumeration lists the possible reasons that an LRQ request might be rejected. The possible values are:

- LRJ\_NOT\_REGISTERED
- LRJ\_INVALID\_PERMISSION
- LRJ\_REQUEST\_DENIED
- LRJ\_UNDEFINED\_REASON
- LRJ\_SECURITY\_DENIAL

## REQUEST\_MSG\_TYPE

The REQUEST\_MSG\_TYPE enumeration lists the possible messages that can be received from the Cisco IOS Gatekeeper. The possible values are:

- UNKNOWN\_MSG
- MSG\_NOT\_SUPPORTED
- RRQ\_REQUEST\_MSG
- URQ\_REQUEST\_MSG
- ARQ\_REQUEST\_MSG
- LRQ\_REQUEST\_MSG
- LRJ\_REQUEST\_MSG
- LCF\_REQUEST\_MSG
- BRQ\_REQUEST\_MSG
- RAI\_REQUEST\_MSG
- DRQ\_REQUEST\_MSG
- RRQ\_REGISTER\_RESPONSE\_MSG
- URQ\_REGISTER\_RESPONSE\_MSG

- ARQ\_REGISTER\_RESPONSE\_MSG
- LRQ\_REGISTER\_RESPONSE\_MSG
- LCF\_REGISTER\_RESPONSE\_MSG
- LRJ\_REGISTER\_RESPONSE\_MSG
- BRQ\_REGISTER\_RESPONSE\_MSG
- RAI\_REGISTER\_RESPONSE\_MSG
- DRQ\_REGISTER\_RESPONSE\_MSG
- RRQ\_UNREGISTER\_RESPONSE\_MSG
- URQ\_UNREGISTER\_RESPONSE\_MSG
- ARQ\_UNREGISTER\_RESPONSE\_MSG
- LRQ\_UNREGISTER\_RESPONSE\_MSG
- LCF\_UNREGISTER\_RESPONSE\_MSG
- LRJ\_UNREGISTER\_RESPONSE\_MSG
- BRQ\_UNREGISTER\_RESPONSE\_MSG
- RAI\_UNREGISTER\_RESPONSE\_MSG
- DRQ\_UNREGISTER\_RESPONSE\_MSG

## RRJ\_REJECT\_REASON\_TYPE

The RRJ\_REJECT\_REASON\_TYPE enumeration lists the possible reasons that an RRQ request might be rejected. The possible values are:

- RRJ\_UNDEFINED\_REASON
- RRJ\_SECURITY\_DENIAL
- RRJ\_RESOURCE\_UNAVAIL

## ARJ\_REJECT\_REASON\_TYPE

The ARJ\_REJECT\_REASON\_TYPE enumeration lists the possible reasons that an ARQ request might be rejected. The possible values are:

- CALLED\_PARTY\_NOT\_REGISTERED
- INVALID\_PERMISSION
- REQUEST\_DENIED
- UNDEFINED\_REASON
- ARJ\_RESOURCE\_UNAVAIL
- ARJ\_SECURITY\_DENIAL

## BRJ\_REJECT\_REASON\_TYPE

The BRJ\_REJECT\_REASON\_TYPE enumeration lists the possible reasons that a BRQ request might be rejected. The possible values are:

- BRJ\_NOT\_BOUND
- BRJ\_INVALID\_CONF\_ID
- BRJ\_INVALID\_PERMISSION
- BRJ\_INSUFFICIENT\_RSC
- BRJ\_INVALID\_REVISION
- BRJ\_UNDEFINED\_REASON
- BRJ\_SECURITY\_DENIAL

## URQ\_REASON\_TYPE

The URQ\_REASON\_TYPE enumeration lists the reasons sent in the URQ message to unregister an endpoint. The possible values are:

- URQ\_REASON\_REREG\_REQ = 1
- URQ\_REASON\_TTL\_EXP = 2
- URQ\_REASON\_SEC\_DNL = 3
- URQ\_REASON\_UNDEF = 4
- URQ\_REASON\_MAINTENANCE = 5
- URQ\_REASON\_NOT\_SPECIFIED = 99

## RESPONSE\_MSG\_TYPE

The RESPONSE\_MSG\_TYPE enumeration lists the possible messages that the external application can send to the Cisco IOS Gatekeeper. The possible values are:

- RRQ\_RESPONSE\_MSG
- RCF\_RESPONSE\_MSG
- RRJ\_RESPONSE\_MSG
- ARQ\_RESPONSE\_MSG
- ACF\_RESPONSE\_MSG
- ARJ\_RESPONSE\_MSG
- LRQ\_RESPONSE\_MSG
- LCF\_RESPONSE\_MSG
- LRJ\_RESPONSE\_MSG
- RIP\_RESPONSE\_MSG
- BRQ\_RESPONSE\_MSG
- BCF\_RESPONSE\_MSG
- BRJ\_RESPONSE\_MSG

## REGISTER\_MSG\_TYPE

The REGISTER\_MSG\_TYPE enumeration lists the possible registration messages that the external application can send to the Cisco IOS Gatekeeper. The possible values are:

- RRQ\_REGISTER\_MSG
- URQ\_REGISTER\_MSG
- ARQ\_REGISTER\_MSG
- LRQ\_REGISTER\_MSG
- LCF\_REGISTER\_MSG
- LRJ\_REGISTER\_MSG
- BRQ\_REGISTER\_MSG
- RAI\_REGISTER\_MSG
- DRQ\_REGISTER\_MSG

## REPORT\_DEST\_T

The REPORT\_DEST\_T enumeration lists the possible destinations for the Gatekeeper API debug output. The possible values are:

- REPORT\_CONSOLE
- REPORT\_SYSLOG

## CRYPTO\_H323\_TOKEN\_TYPE\_S

The CRYPTO\_H323\_TOKEN\_TYPE\_S enumeration lists the possible types of cryptoTokens. The possible values are:

- NO\_CRYPTOTOKEN
- CRYPTO\_EP\_PWD\_HASH
- CRYPTO\_EP\_PWD\_ENCR
- CRYPTO\_EP\_CERT

**Note**

---

In the first release of the GKTMP and API, the CRYPTO\_EP\_PWD\_HASH is the only type of cryptoToken supported.

---

## USE\_SPECIFIED\_TRANSPORT\_TYPE\_T

The USE\_SPECIFIED\_TRANSPORT\_TYPE\_T enumeration lists the possible transport types that an endpoint can select for H.225 signalling. The possible values are:

- TRANSPORT\_NONE
- ANNEX\_E
- TCP

## CMD\_MSG\_TYPE

The CMD\_MSG\_TYPE enumeration lists the possible messages that the external application can send as spontaneous commands to the Cisco IOS Gatekeeper. The possible value is:

- URQ\_CMD\_MSG

## Limits

Some of the fields are limited in size. The limits are set using variables in the header file. The limits as set in the default header file are shown in [Table 5-66](#):

**Table 5-66 Field Size Limits**

Variable	Initial Value
MAX_IP_ADDR_LENGTH	15
MAX_VERSION_ID_LENGTH	4
MAX_ENDPOINT_LENGTH	128
MAX_TRANSACTION_ID_LENGTH	24
MAX_NUM_ENDPOINT_TYPES	7
MAX_NUM_SUPPORTED_PREFIX	10
MAX_NUM_ARQ_DEST_INFO	20
MAX_NUM_ARQ_REDIRECT_REASON	7
MAX_NUM_LRQ_DEST_INFO	20
MAX_NUM_LRQ_REDIRECT_REASON	7
MAX_NUM_LCF_DEST_INFO	20
MAX_NUM_LCF_RMOT_EXTENSION_ADDR	20
MAX_NUM_LRJ_DEST_INFO	20
MAX_CRYPT_TOKEN_FIELDS	5





## GKTMP Command Reference

---

This chapter describes commands that support the new Cisco IOS Gatekeeper functions and includes the following commands:

- [server trigger](#)
- [timer server timeout](#)
- [server registration-port](#)
- [server flow-control](#)
- [show gatekeeper servers](#)
- [show gatekeeper status](#)
- [debug gatekeeper servers](#)



### Note

As with all Cisco IOS commands, you can abbreviate the Cisco IOS Gatekeeper trigger registration commands. To abbreviate a command, simply enter the first few characters of the command and press tab. To obtain online help for a command, enter the first few characters of the command followed by a question mark.

For additional Cisco IOS commands, see the following documents:

*Cisco High Performance Gatekeeper*

*Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2

*Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2

## server trigger

To configure a static server trigger for external applications, enter the **server trigger** command from Gatekeeper mode. Enter the **no** form of this command to remove a single statically configured trigger entry. Enter the “all” form of the command to remove every static trigger you configured if you want to delete them all.

```
server trigger {arq | lcf | lrj | lrq | rrq | urq | drq | rai | brq} gkid priority server-id  
server-ip_address server-port
```

```
no server trigger { arq | lcf | lrj | lrq | rrq | urq | drq | rai | brq} gkid priority
```

```
no server trigger all
```

Syntax Description	
<b>arq</b>   <b>lcf</b>   <b>lrj</b>   <b>lrq</b>   <b>rrq</b>   <b>urq</b>   <b>drq</b>   <b>rai</b>   <b>brq</b>	The RAS messages for which you can create triggers on the Cisco IOS Gatekeeper. You can specify only one message type per server trigger command. There is a different trigger submode for each message type. Each trigger submode has its own set of applicable commands.
<i>gkid</i>	The identifier of the Cisco IOS Gatekeeper.
<i>priority</i>	The priority for this particular trigger. Possible values are 1 through 20. 1 is the highest.
<i>server-id</i>	The identifier of the external application.
<i>server-ip_address</i>	The IP address of the server on which the external application is running.
<i>server-port</i>	The port on which the server listens for messages from the Cisco IOS Gatekeeper.

**Command Modes** Gatekeeper configuration

**Related Commands** The following subcommands can be used in any of the trigger submodes:

- [Trigger Submodes](#)
- [shutdown](#)

The following subcommands can be used in specific trigger submodes to configure certain types of trigger conditions:

- [destination-info](#)
- [redirect-reason](#)
- [remote-ext-address](#)
- [endpoint-type](#)
- [supported-prefix](#)

## Trigger Submodes

### info-only

To indicate to the Cisco IOS Gatekeeper that messages that meet the specified trigger parameters should be sent as notifications only and that the Cisco IOS Gatekeeper should not wait for a response from the external application, use the **info-only** subcommand.

**info-only**

Syntax Description	
<b>info-only</b>	Informational only. No need to wait for acknowledgment.

**Command Modes** Any of the Cisco IOS Gatekeeper trigger submodes

## shutdown

To temporarily disable a trigger, use the **shutdown** subcommand. Cisco IOS Gatekeepers do not consult triggers in shutdown state when determining whether a message should be forwarded to an external application.

**shutdown**

<b>Syntax Description</b>	<b>shutdown</b>	Changes the administrative state of a trigger to shutdown.
---------------------------	-----------------	--

**Command Modes** Any of the Cisco IOS Gatekeeper trigger submodes

## destination-info

To configure a trigger that is based on a particular destination, use the **destination-info** subcommand.

**destination-info** {**e164** | **email-id** | **h323-id**} *value*

<b>Syntax Description</b>	<b>e164</b>	Indicates that the destination address is an E.164 address.
	<b>email-id</b>	Indicates that the destination address is an e-mail ID.
	<b>h323-id</b>	Indicates that the destination address is an H.323 ID.
	<i>value</i>	Specifies the value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used: <ul style="list-style-type: none"> <li>• A trailing series of periods, each of which represents a single character.</li> <li>• A trailing asterisk, which represents one or more characters.</li> </ul>

**Command Modes** Cisco IOS Gatekeeper ARQ, LRQ, LCF, LRJ, and DRQ trigger submodes

## redirect-reason

To configure a trigger that is based on a specific redirect reason, use the **redirect-reason** subcommand.

**redirect-reason** *value*

<b>Syntax Description</b>	<i>value</i>	<p>Specifies the value against which to compare the redirect reason in the RAS messages. Possible values are 0-65535. Currently-used redirect reasons are:</p> <ul style="list-style-type: none"> <li>• 0—Unknown reason</li> <li>• 1—Call forwarding busy or called DTE busy</li> <li>• 2—Call forwarded no reply</li> <li>• 4—Call deflection</li> <li>• 9—Called DTE out of order</li> <li>• 10—Call forwarding by the call DTE</li> <li>• 15—Call forwarding unconditionally</li> </ul>
---------------------------	--------------	---

**Command Modes** Cisco IOS Gatekeeper ARQ, LRQ, DRQ, and BRQ trigger submodes

### remote-ext-address

To configure a trigger that is based on a specific remote extension address, use the **remote-ext-address** subcommand.

**remote-ext-address** *e164 value*

<b>Syntax Description</b>	<i>e164</i>	Indicates that the remote extension address is an E.164 address.
	<i>value</i>	<p>Specifies the value against which to compare the destination address in the RAS messages. The following wildcards can be used:</p> <ul style="list-style-type: none"> <li>• A trailing series of periods, each of which represents a single character.</li> <li>• A trailing asterisk, which represents one or more characters.</li> </ul>

**Command Modes** Cisco IOS Gatekeeper LCF trigger submode

## endpoint-type

To configure a trigger that is based on a specific endpoint, use the **endpoint-type** subcommand.

**endpoint-type** *value*

<b>Syntax Description</b>	<i>value</i>	<p>Specifies the value against which to compare the endpoint-type in the RAS messages. The possible values are:</p> <ul style="list-style-type: none"> <li>• gatekeeper—The endpoint is an H.323 gatekeeper.</li> <li>• h320-gateway—The endpoint is an H.320 gateway.</li> <li>• mcu—The endpoint is an MCU.</li> <li>• other-gateway—The endpoint is a type of gateway not specified on this list.</li> <li>• proxy—The endpoint is an H.323 proxy.</li> <li>• terminal—The endpoint is an H.323 terminal.</li> <li>• voice-gateway—The endpoint is a voice type gateway.</li> </ul>
---------------------------	--------------	--

**Command Modes** Cisco IOS Gatekeeper RRQ, URQ, and RAI trigger submodes

## supported-prefix

To configure a trigger that is based on a specific supported prefix, use the **supported-prefix** subcommand.

**supported-prefix** *value*

<b>Syntax Description</b>	<i>value</i>	<p>Specifies the value against which to compare the supported prefix in the RAS messages. The possible values are any E.164 pattern used as a gateway technology prefix. The value string can contain any of the following: 0123456789#*,</p>
---------------------------	--------------	---

**Command Modes** Cisco IOS Gatekeeper RRQ, URQ, and RAI trigger submodes

## timer server timeout

To define the server timeout for GKTMP messages, use the **timer server timeout** command.

**timer server timeout** *value*

<b>Syntax Description</b>	<i>value</i>	The timeout in seconds. Possible values are 1 through 5. The default value is 3.
---------------------------	--------------	--

---

**Command Modes** Gatekeeper configuration

## server registration-port

To define a listener port to be used by the external applications to establish connections to the gatekeeper on this router, use the **server registration-port** gatekeeper configuration command.

**server registration-port** *port\_number*

**no server registration-port**

The **no** form of this command forces the gatekeeper on this router to close the listener port so that it cannot receive any additional registrations. However, existing connections between the gatekeeper and external application are left open.

---

<b>Syntax Description</b>	<i>port_number</i>	The port on which the Cisco IOS Gatekeeper should listen for registration messages from external applications.
---------------------------	--------------------	--

---



---

**Command Modes** Gatekeeper configuration

## server flow-control

To enable flow control on the Cisco IOS Gatekeeper (GK) and reset all thresholds to default, use the **server flow-control** command in gatekeeper configuration mode. To disable GK flow control, use the **no** form of this command.

**server flow-control** [*onset value*] [*abatement value*] [*qcount value*]

**no server flow-control**

---

<b>Syntax Description</b>	<i>onset value</i>	<p>A percentage of the server timeout value that is used to mark the server as usable or unusable. The range of valid values is 1 through 100; the default value is 80.</p> <p>For example, if the server time out value is 3 seconds, the onset value is 50, and the abatement value is 40, when the average response time from the server to the GKTMP reaches 1.5 seconds (the onset percentage of the server timeout value), the server is marked as unusable. During the period that the server is marked as unusable, REQUEST ALV messages are still sent to the unusable server. When the response time is lowered to 1.2 seconds (the abatement percentage of the timeout value), the server is marked usable again and the GKTMP resumes sending messages to the server.</p>
---------------------------	--------------------	---

---

---

<b>abatement value</b>	<p>A percentage of the server timeout value that is used to mark the server as unusable or usable. The range of valid values is 1 through 100; the default value is 50.</p> <p>For example, if the server time out value is 3 seconds, the onset value is 50, and the abatement value is 40, when the average response time from the server to the GKTMP reaches 1.5 seconds (the onset percentage of the server timeout value), the server is marked as unusable. During the period that the server is marked as unusable, REQUEST ALV messages are still sent to the unusable server. When the response time is lowered to 1.2 seconds (the abatement percentage of the timeout value), the server is marked usable again and the GKTMP resumes sending messages to the server.</p> <p><b>Note</b> The abatement value cannot be greater than or equal to the onset value.</p>
<b>qcount value</b>	<p>Identifies the threshold for the length of the outbound queue on the GK. The queue contains messages waiting to be transmitted to the server. The TCP socket between the GK and GKTMP server queues messages if it has too many to transmit. If the count of outbound queue length on the server reaches the qcount value, the server is marked unusable. Range is from 1 to 1000. The default is 400.</p>

---

## Command Modes

Gatekeeper configuration

## Examples

The following example shows using the command with the default values:

```
Router# server flow-control
```

In the following example, the GKTMP Interface Resiliency Enhancement feature is enabled with an onset level of 50:

```
Router# server flow-control onset 50
*Mar 8 20:05:34.081: gk_srv_handle_flowcontrol: Flow control enabled
Router# show running configuration
```

```
Building configuration...
```

```
Current configuration : 1065 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname snet-3660-3
!
.
.
.
gatekeeper
 zone local snet-3660-3 cisco.com
 zone remote snet-3660-2 cisco.com 209.165.200.225 1719
 zone prefix snet-3660-2 408*
 lrq forward-queries
no use-proxy snet-3660-3 default inbound-to terminal
```

```

no use-proxy snet-3660-3 default outbound-from terminal
no shutdown
server registration-port 8000
server flow-control onset 50
!
!
.
.
.
end

```

## show gatekeeper servers

To display a list of the triggers (whether dynamically registered from the external applications or statically configured from the command-line interface), use the **show gatekeeper servers EXEC** command.

**show gatekeeper servers** [*gkid*]

### Syntax Description

<i>gkid</i>	Specifies the ID of the gatekeeper. If you specify a gatekeeper ID, only the information about the external applications that are registered with the specified gatekeeper is displayed. If you do not specify a gatekeeper ID, information about all the external applications that are registered with any of the Cisco IOS Gatekeepers on this router is displayed.
-------------	--

### Command Modes

EXEC mode

### Examples

The following example shows the **show gatekeeper servers** command output:

#### Example 6-1 show gatekeeper servers Output (version 2.0)

```

router# show gatekeeper servers gk102

GATEKEEPER SERVERS STATUS
=====

Gatekeeper Server listening port: 20000
Gatekeeper GKTMP version:2.0

Gatekeeper-ID: gk102
-----
RRQ Priority: 1
Server-ID: sj-server
Server IP address: 1.14.93.28:42387
Server type: dynamically registered
Connection Status: active
Server GKAPI version:2.0
Trigger Information:
Supported Prefix: 10#
Supported Prefix: 3#
RRQ Priority: 2
Server-ID: sf-server

```

```

Server IP address: 1.14.93.43:3820
Server type: CLI-configured
Connection Status: inactive
  Server GKAPI version:2.0
Trigger Information:
  Endpoint-type: MCU
  Endpoint-type: VOIP-GW
  Supported Prefix: 99#
ARQ Priority: 1
  Server-ID: sj-server
  Server IP address: 1.14.93.28:42387
  Server type: dynamically registered
  Connection Status: active
  Server GKAPI version:2.0
Trigger Information:
  Destination Info: M:nilkant@zone14.com
  Destination Info: E:1800.....
  Redirect Reason: Call forwarded no reply
  Redirect Reason: Call deflection

```

### Example 6-2 show gatekeeper servers Output (version 3.1)

```

Router# show gatekeeper server

GATEKEEPER SERVERS STATUS
=====

Gatekeeper Server listening port: 8250
Gatekeeper Server timeout value: 30 (100ms)
GateKeeper GKTMP version: 3.1

Gatekeeper-ID: Gatekeeper1
-----
RRQ Priority: 5
  Server-ID: Server43
  Server IP address: 209.165.200.254:40118
  Server type: dynamically registered
  Connection Status: active
  Trigger Information:
    Trigger unconditionally

Server Statistics:
REQUEST RRQ Sent=0
RESPONSE RRQ Received = 0
RESPONSE RCF Received = 0
RESPONSE RRJ Received = 0
Timeout encountered=0
Average response time(ms)=0
Server Usable=TRUE

```

## show gatekeeper status

To display statistics about the gatekeeper, including authorization and authentication status and if load balancing and flow control are enabled, use the show gatekeeper status command in EXEC mode.

**show gatekeeper status**

### Syntax Description

This command has no arguments or keywords.

### Command Modes

EXEC mode

### Examples

The following example shows output from the show gatekeeper status command:

```
Router# show gatekeeper status

Gatekeeper State: UP
  Load Balancing:  DISABLED
  Flow Control:   ENABLED
  Zone Name:      snet-3660-3
  Accounting:     DISABLED
  Endpoint Throttling:  DISABLED
  Security:       DISABLED
  Maximum Remote Bandwidth:          unlimited
  Current Remote Bandwidth:          0 kbps
  Current Remote Bandwidth (w/ Alt GKs): 0 kbps
```

Table 6-1 describes the significant fields shown in the display.

**Table 6-1** show gatekeeper status Field Descriptions

Field	Description
Gatekeeper State	Gatekeeper state has the following values: <ul style="list-style-type: none"> <li>UP is operational.</li> <li>DOWN is administratively shut down.</li> <li>INACTIVE is administratively enabled, that is, the no shutdown command has been issued, but no local zones have been configured.</li> <li>HSRP STANDBY indicates that the gatekeeper is on hot standby and will take over when the currently active gatekeeper fails.</li> </ul>
Load Balancing	Shows if load balancing is enabled.
Flow Control	Shows if server flow control is enabled.
Zone Name	Displays the zone name to which the gatekeeper belongs.
Accounting	Shows if authorization and accounting features are enabled.
Endpoint Throttling	Shows if endpoint throttling is enabled.
Security	Shows if security features are enabled.
Bandwidth	Shows the maximum remote bandwidth, current remote bandwidth, and current remote bandwidth with alternate gatekeepers.

# debug gatekeeper servers

To turn debugging on, use the **debug gatekeeper servers EXEC** command. This command traces all the message exchanges between the Cisco IOS Gatekeeper and the external application. This command also displays any errors that occur when sending messages to the external application or when parsing messages from the external application. The **no** form of this command turns debugging off.

**debug gatekeeper servers**

**no debug gatekeeper servers**

---

**Syntax Description** This command has no keywords or arguments.

---

**Command Modes** EXEC mode

---

**Examples** The following example shows the debug gatekeeper servers output:

**Example 6-3 debug gatekeeper servers Output**

```
router#debug gatekeeper servers
##### begin screen trace
00:08:47:GK:processing server msg:
REGISTER RRQ
From:server1
To:gk617
Priority:1

00:08:47:GK TMSG encoded to write buffer:
"REGISTER RRQ
From:gk617
To:server1
Priority:1
Status:success

"

00:11:16:GK TMSG encoded to write buffer:
"REQUEST RRQ
From:gk617
To:server1
Transaction-Id:6121529400000001
Content-Length:62

c=I:1.14.93.92:1720
r=I:1.14.93.92:24999
t=proxy
a=H:px14
"

00:11:16:GK:processing server msg:
RESPONSE RRQ
From:server1
To:gk617
```

```
Transaction-Id:6121529400000001
Content-Length:35

a=M:jsmith
p=1# 2 # 3# 1800...

00:11:45:GK TMSG encoded to write buffer:
"REQUEST RRQ
From:gk617
To:server1
Transaction-Id:6121529400000002
Content-Length:72

c=I:1.14.93.130:1720
r=I:1.14.93.130:4307
t=voice-gateway
a=H:gw130
"

00:11:45:GK:processing server msg:
RESPONSE RRJ
From:server1
To:gk617
Transaction-Id:6121529400000002
Content-Length:18

R=securityDenial
##### end screen trace
```