

H.323 Version 2 Support in Multimedia Conference Manager

The H.323 Version 2 Support in Multimedia Conference Manager feature adds H.323 Version 2 improvements to the existing Multimedia Conference Manager (MCM) feature module. This document contains the following sections:

- Feature Overview on page 1
- Supported Platforms on page 4
- Supported Standards, MIBs, and RFCs on page 4
- Prerequisites on page 4
- Configuration Tasks on page 5
- Configuration Examples on page 7
- Command Reference on page 10

Feature Overview

Multimedia Conference Manager provides gatekeeper and proxy capabilities required for service provisioning and management of H.323-compliant networks. It conforms to the H.323 standard (version 1) for sending audio, video, and data conferencing data on an IP-based internetwork.

The Cisco H.323 Version 2 Support in Multimedia Conference Manager feature upgrades Cisco IOS software to comply with the mandatory requirements and several of the optional features of the H.323 Version 2 specification. Future releases will add more H.323 Version 2 features to the Cisco IOS software.

H.323 Version 2 Compliance

The Cisco H.323 Version 2 Support in Multimedia Conference Manager feature enables gatekeepers and proxies to send and receive all the required fields in H.323 Version 2 messages.

Lightweight Registration

Prior to H.323 Version 2, Cisco gateways reregistered with the gatekeeper every 30 seconds. Each registration renewal used the same process as the initial registration, even though the gateway was already registered with the gatekeeper. This behavior generated considerable overhead at the gatekeeper.

H.323 Version 2 defines a lightweight registration procedure that still requires the full registration process for initial registration, but uses an abbreviated renewal procedure to update the gatekeeper and minimize overhead.

Lightweight registration requires each endpoint to specify a TimeToLive (TTL) value in its Registration Request (RRQ) message. When a gatekeeper receives an RRQ message with a TTL value, it returns an updated TTL timer value in a Registration Confirmation (RCF) message to the endpoint. Shortly before the TTL timer expires, the endpoint sends an RRQ message with KeepAlive field set to TRUE, which refreshes the existing registration.

An H.323 Version 2 endpoint is not required to indicate a time-to-live in its registration request. If the endpoint does not indicate a time-to-live, the gatekeeper assigns one and sends it to the gateway in the RCF message. No configuration changes are permitted during a lightweight registration, so all fields are ignored other than the endpoint identifier, gatekeeper identifier, tokens, and time-to-live. In the case of H.323 Version 1, endpoints cannot process the TTL field in the RCF; the gatekeeper probes the endpoint with IRQs for a predetermined grace period to learn if the endpoint is still alive.

Improved Gateway Selection Process

Prior to H.323 Version 2, the gatekeeper selected a destination gateway by choosing gateways defined with **zone prefix** commands. These commands assign a dialing prefix to a zone and allow the use of wildcards in the dialing prefix. In H.323 Version 1, the gatekeeper simply matched the destination number with the longest match in the defined dialing prefixes, and randomly selected a gateway registered in that zone.

The H.323 Version 2 software improves the gateway selection process as follows:

- When more than one gateway is registered in a zone, the updated **zone prefix** command allows you to assign selection priorities to these gateways based on the dialed prefix.
- Gateway resource reporting allows the gateway to notify the gatekeeper when H.323 resources are getting low. The gatekeeper uses this information to determine which gateway it will use to complete a call.

The gatekeeper maintains a separate gateway list, ordered by priority, for each of its zone prefixes. If a gateway does not have an assigned priority for a zone prefix, it defaults to priority 5, which is the median. To explicitly bar the use of a gateway for a zone prefix, define it as having a priority 0 for that zone prefix.

When selecting gateways, the gatekeeper identifies a target pool of gateways by performing a longest zone prefix match; then it selects from the target pool according to priorities and resource availability. If all high-priority gateways are busy, a low-priority gateway might be selected.

Support for Single-Proxy Configurations

In previous releases, the gatekeeper supported two-proxy and no-proxy call scenarios. The destination gatekeeper decided whether a call would be proxied or direct based on its zone configuration. The source gatekeeper would pick a proxy for its outbound calls only when the destination gatekeeper returned its inbound proxy in the location confirm message. This version of the gatekeeper software adds support for single-proxy calls and the option to independently configure proxies for inbound and outbound call scenarios.

Managing Gatekeeper Functionality

The H.323 Version 2 Support in Multimedia Conference Manager feature introduces the **clear h323 gatekeeper call** command. This command enables you to manage the functionality of gatekeeper endpoints by providing a way to force a disconnect on a specific call or all calls active on a particular gatekeeper.

Benefits

The Cisco H.323 Version 2 Support in Multimedia Conference Manager feature adds the following benefits to Cisco H.323 gatekeepers and proxies:

- H.323 Version 2 compliance.
- Lightweight registration. Gatekeepers, gateways, and proxies use a registration renewal process that requires fewer network and device resources than the reregistration process used for H.323 Version 1.
- Generation and processing of Request In Progress messages to dynamically extend Registration, Admission, and Status (RAS) timers when additional time is needed for address resolution.
- Gateway resource availability reporting.
- Gatekeeper selects gateways by using gateway resource availability data and priority levels defined at the gatekeeper.
- Support for single-proxy, dual-proxy, and no-proxy configurations previously supported.

Restrictions

- The H.323 Version 2 Support in Multimedia Conference Manager feature is meant to run with MCM gatekeeper or proxy functions enabled; a Cisco router configured to use the H.323 Version 2 Multimedia Conference Manager feature is not meant to be used as a regular router.
- H.323 Version 2 features will not interoperate with H.323 Version 1 features in Cisco IOS versions prior to 11.3(9)NA or 12.0(3)T. Earlier Cisco IOS versions contain H.323 Version 1 software that does not support protocol messages with an H.323 Version 2 protocol identifier. All systems must be running either Cisco IOS Release 11.3(9)NA and later or Cisco IOS Release 12.0(3)T and later to interoperate with H.323 Version 2.
- If you are planning to use a Cisco AS5300 Universal Access Server, your software requires VCWare Version 4.04.

Related Features and Technologies

- Hot Standby Routing Protocol (HSRP)
- Real-Time Transport Protocol (RTP)
- Registration, Admission, and Status (RAS) Protocol

Related Documents

- *Configuring H.323 VoIP Gatekeeper for Cisco Access Platforms*, Cisco IOS Release 11.2(7)NA
- *Multimedia Conference Manager*, Cisco IOS Release 12.0(3)T

- *H.323 Version 2*, Cisco IOS Release 12.0(5)T

Supported Platforms

The gatekeeper and proxy features apply to the following platforms:

- Cisco 2600 series
- Cisco 3600 series
- Cisco MC3810 multiservice concentrator

Supported Standards, MIBs, and RFCs

MIBs

None

RFCs

None

Standards

- H.225, *Call Signalling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication Systems*
- H.245, *Control Protocol for Multimedia Communication*
- H.323-2, *Packet-Based Multimedia Communications Systems*
- Q.931, *Digital Subscriber Signalling System No. 1 (DSS 1) - ISDN User-Network Interface Layer 3 Specification for Basic Call Control*
- T.120, *Data Protocols for Multimedia Conferencing*

Prerequisites

Your Cisco device must be configured as a gatekeeper endpoint using the configuration information contained in the Cisco IOS Release 12.0(3)T *Multimedia Conference Manager* feature module before you can use the H.323 Version 2 MCM enhancements. In general, to configure an MCM gatekeeper, you must perform the following tasks:

- Start MCM gatekeeper functionality on your Cisco device by defining the gatekeeper name and defining a set of subnets that constitute the zone of the gatekeeper.
- Set up intergateway communication, either manually or by using DNS.
- Control zone accessibility either by configuring your gatekeeper to offer an IP address of a local proxy when queried by a remote gatekeeper (*proxied* access) or by configuring your gatekeeper to offer the address of the local endpoint instead of the address of the local proxy (*direct* access).
- Define static nodes if the registration information of a particular terminal or endpoint is not accessible from any gatekeeper.
- Identify H.323 users using RADIUS/TACACS+ authentication.
- Send accounting records using RADIUS/TACACS+ accounting features.

- Configure interzone routing using E.164 addresses.

For more information about these configuration tasks, refer to the Cisco IOS Release 12.0(3)T *Multimedia Conference Manager* feature module.

Configuration Tasks

The H.323 Version 2 Support in Multimedia Conference Manager feature contains the following configuration tasks:

- Adding a Prefix to a Gatekeeper Zone List
- Configuring Inbound or Outbound Gatekeeper Proxied Access
- Forcing a Disconnect on an MCM Gatekeeper (optional)

Adding a Prefix to a Gatekeeper Zone List

Step	Command	Purpose
1	Router(config)# gatekeeper	Enters gatekeeper configuration mode.
2	Router(config-gk)# zone prefix <i>gatekeeper-name</i> <i>e164-prefix</i> [gw-priority <i>pri-0-to-10</i> <i>gw-alias</i> [<i>gw-alias</i> , ...]]	Adds a prefix to the gatekeeper zone list.

Note Note that the **zone prefix** command matches a prefix to a gateway. It does not register the gateway. The gateway must register with the gatekeeper before calls can be completed through that gateway.

Verifying an Added Prefix

Use the **show gatekeeper zone prefix** command to view the prefixes added to the gatekeeper zone list. Use the **show gatekeeper zone status** command to see gatekeeper zone information.

Configuring Inbound or Outbound Gatekeeper Proxied Access

By default, a gatekeeper will offer the IP address of the local proxy when queried by a remote gatekeeper (synonymous with remote zone). This is considered *proxied* access. In the previous version of MCM, you configure the local gatekeeper to offer the address of the local endpoint instead of the address of the local proxy (considered *direct* access) by using the **zone access** command. In the H.323 Version 2 Support in Multimedia Conference Manager feature, the **use-proxy** command replaces the **zone access** command.

The **use-proxy** command enables you to configure a proxy for inbound calls from remote zones to gateways in its local zone and to configure a proxy for outbound calls from gateways in its local zone to remote zones.

Step	Command	Purpose
1	Router(config)# gatekeeper	Enters gatekeeper configuration mode.

Verifying Gatekeeper Proxied Access Configuration

Step	Command	Purpose
2	Router(config-gk)# use-proxy <i>local-zone-name</i> { default remote-zone <i>remote-zone-name</i> }{ inbound-to outbound-from }{ gateway terminal }	Enables proxy communications for calls between local and remote zones.

Note When a previous version of gatekeeper is upgraded, any **zone access** commands are translated to the corresponding **use-proxy** commands.

Verifying Gatekeeper Proxied Access Configuration

Use the **show gatekeeper zone status** command to see information about the configured gatekeeper proxies and gatekeeper zone information.

```
router# show gatekeeper zone status

                        GATEKEEPER ZONES
                        =====
GK name          Domain Name    RAS Address    PORT  FLAGS  MAX-BW    CUR-BW
-----          -
sj.xyz.com      xyz.com        1.14.93.85    1719  LS          0
SUBNET ATTRIBUTES :
  All Other Subnets : (Enabled)
PROXY USAGE CONFIGURATION :
  inbound Calls from germany.xyz.com :
    to terminals in local zone sj.xyz.com :use proxy
    to gateways in local zone sj.xyz.com  :do not use proxy
  Outbound Calls to germany.xyz.com
    from terminals in local zone germany.xyz.com :use proxy
    from gateways in local zone germany.xyz.com  :do not use proxy
  Inbound Calls from all other zones :
    to terminals in local zone sj.xyz.com :use proxy
    to gateways in local zone sj.xyz.com  :do not use proxy
  Outbound Calls to all other zones :
    from terminals in local zone sj.xyz.com :do not use proxy
    from gateways in local zone sj.xyz.com  :do not use proxy
tokyo.xyz.co   xyz.com        172.21.139.89  1719  RS          0
milan.xyz.co   xyz.com        171.69.57.90   1719  RS          0
```

Forcing a Disconnect on an MCM Gatekeeper

Command	Purpose
Router# clear h323 gatekeeper call { all local-callID <i>local-callID</i> }	Forces a disconnect on a specific call or all calls currently active on this MCM gatekeeper.

If you want to force a particular call to be disconnected (as opposed to all active calls on the MCM gateway), use the local call identification number (CallID) to identify that specific call. You can find the local CallID number for a specific call by using the **show gatekeeper calls** command; the ID number is displayed in the LocalCallID column.

Verifying a Forced Disconnect

Use the **show gatekeeper calls** command to show the status of each ongoing call that a gatekeeper is aware of. If you have forced a disconnect for either a particular call or all calls associated with a particular MCM gatekeeper, the system will not display information about those calls.

```
router# show gatekeeper calls

Total number of active calls =1
                        Gatekeeper Call Info
                        =====
LocalCallID           Age (secs)      BW
12-3339                94              768 (Kbps)
Endpt(s): Alias      E.164Addr      CallSignalAddr  Port  RASignalAddr  Port
src EP: epA          10.0.0.11      1720            1700  10.0.0.11     1700
dst EP: epB2zoneB.com
src PX: pxA          10.0.0.1       1720            24999 10.0.0.11     24999
dst PX: pxB          172.21.139.90  1720            24999 172.21.139.90 24999
```

Configuration Examples

This section provides the following configuration examples:

- Defining Multiple Zones
- Defining One Zone for Multiple Gateways
- Configuring a Proxy for Inbound Calls
- Configuring a Proxy for Outbound Calls
- Removing a Proxy
- Prohibiting Proxy Use for Inbound Calls
- Disconnecting a Single Call Associated with an MCM Gateway
- Disconnecting All Calls Associated with an MCM Gateway

Defining Multiple Zones

The following example shows how you can define multiple local zones for separating your gateways:

```
router(config-gk) # zone local gk408or650 xyz.com
router(config-gk) # zone local gk415 xyz.com
router(config-gk) # zone prefix gk408or650 408.....
router(config-gk) # zone prefix gk408or650 650.....
router(config-gk) # zone prefix gk415 415.....
```

Now you can configure all the gateways to be used for area codes 408 or 650 to register with gk408or650 and all gateways to be used for area code 415 to register with gk415.

Defining One Zone for Multiple Gateways

The following example shows how you can put all your gateways in the same zone but use the **gw-priority** keyword to determine which gateways will be used for calling different area codes:

```
router(config-gk) # zone local localgk xyz.com
router(config-gk) # zone prefix localgk 408.....
router(config-gk) # zone prefix localgk 415..... gw-priority 10 gw1 gw2
router(config-gk) # zone prefix localgk 650..... gw-priority 0 gw1
```

The above commands accomplish the following tasks:

- Domain xyz.com is assigned to gatekeeper localgk.
- Prefix 408..... is assigned to gatekeeper localgk, and no gateway priorities are defined for it; therefore, all gateways registering to localgk can be used equally for calls to the 408 area code. No special gateway lists are built for the 408..... prefix; selection is made from the master list for the zone.
- The prefix 415..... is added to gatekeeper localgk, and priority 10 is assigned to gateways gw1 and gw2.
- Prefix 650..... is added to gatekeeper localgk, and priority 0 is assigned to gateway gw1.

A priority 0 is assigned to gateway gw1 to exclude it from the gateway pool for prefix 650..... When gateway gw2 registers with gatekeeper localgk, it is added to the gateway pool for each prefix as follows:

- For gateway pool for 415....., gateway gw2 is set to priority 10.
- For gateway pool for 650....., gateway gw2 is set to priority 5.

To change gateway gw2 from priority 10 for zone 415..... to the default priority 5, enter the following command:

```
router(config-gk) # no zone prefix localgk 415..... gw-pri 10 gw2
```

To change both gateways gw1 and gw2 from priority 10 for zone 415..... to the default priority 5, enter the following command:

```
router(config-gk) # no zone prefix localgk 415..... gw-pri 10 gw1 gw2
```

In the preceding example, the prefix 415..... remains assigned to gatekeeper localgk. All gateways that do not specify a priority level for this prefix are assigned a default priority of 5. To remove the prefix and all associated gateways and priorities from this gatekeeper, enter the following command:

```
router(config-gk) # no zone prefix localgk 415.....
```

Configuring a Proxy for Inbound Calls

In the following example, the local zone sj.xyz.com is configured to use a proxy for inbound calls from remote zones tokyo.xyz.com and milan.xyz.com to gateways in its local zone. The sj.xyz.com zone is also configured to use a proxy for outbound calls from gateways in its local zone to remote zones tokyo.xyz.com and milan.xyz.com:

```
router(config) # gatekeeper
router(config-gk) # use-proxy sj.xyz.com remote-zone tokyo.xyz.com inbound-to gateway
router(config-gk) # use-proxy sj.xyz.com remote-zone tokyo.xyz.com outbound-from gateway
router(config-gk) # use-proxy sj.xyz.com remote-zone milan.xyz.com inbound-to gateway
router(config-gk) # use-proxy sj.xyz.com remote-zone milan.xyz.com outbound-from gateway
```

Because the default mode disables proxy communications for all gateway calls, only the gateway call scenarios listed above can use the proxy.

Configuring a Proxy for Outbound Calls

In the next example, the local zone sj.xyz.com uses a proxy for only those calls that are outbound from H.323 terminals in its local zone to the specified remote zone germany.xyz.com:

```
router(config)# gatekeeper
router(config-gk)# no use-proxy sj.xyz.com default outbound-from terminal
router(config-gk)# use-proxy sj.xyz.com remote-zone germany.xyz.com outbound-from
terminal
```

Note that any calls inbound to H.323 terminals in the local zone sj.xyz.com from the remote zone germany.xyz.com use the proxy because the default applies.

Removing a Proxy

The following example shows how to remove one or more proxy statements for the remote zone germany.xyz.com from the proxy configuration list:

```
router(config-gk)# no use-proxy sj.xyz.com remote-zone germany.xyz.com
```

The command above removes all special proxy configurations for the remote zone germany.xyz.com. After you enter a command like this, all calls between the local zone (sj.xyz.com) and germany.xyz.com are processed according to the defaults defined by any **use-proxy** commands that use the **default** option.

Prohibiting Proxy Use for Inbound Calls

To prohibit proxy use for inbound calls to H.323 terminals in a local zone from a specified remote zone, enter a command similar to the following command:

```
router(config-gk)# no use-proxy sj.xyz.com remote-zone germany.xyz.com inbound-to
terminal
```

This command overrides the default and disables proxy use for inbound calls from remote zone germany.xyz.com to all H.323 terminals in the local zone sj.xyz.com.

Disconnecting a Single Call Associated with an MCM Gateway

The following example forces an active call on the MCM gateway to be disconnected. The local ID number of the active call is "12-3339."

```
router> enable
router# clear h323 gatekeeper call local-callID 12-3339
```

Disconnecting All Calls Associated with an MCM Gateway

The following example forces all active calls on the MCM gateway to be disconnected:

```
router> enable
router# clear h323 gatekeeper call all
```

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0(3) T *Multimedia Conference Manager* feature module.

- **clear h323 gatekeeper call**
- **show gatekeeper calls**
- **show gatekeeper endpoints**
- **show gatekeeper gw-type-prefix**
- **show gatekeeper zone status**
- **use-proxy**
- **zone prefix**

In Cisco IOS Release 12.0(1)T or later, you can search and filter the output for **show** and **more** commands. This functionality is useful when you need to sort through large amounts of output, or if you want to exclude output that you do not need to see.

To use this functionality, enter a **show** or **more** command followed by the “pipe” character (`|`), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search or filter on:

```
command | {begin | include | exclude} regular-expression
```

Following is an example of the **show atm vc** command in which you want the command output to begin with the first line where the expression “PeakRate” appears:

```
show atm vc | begin PeakRate
```

For more information on the search and filter functionality, refer to the Cisco IOS Release 12.0(1)T feature module titled *CLI String Search*.

clear h323 gatekeeper call

To force a disconnect on a specific call or all calls active on a particular Multimedia Conference Manager gateway, use the **clear h323 gatekeeper call** privileged EXEC command.

```
clear h323 gatekeeper call { all | local-callID local-callID }
```

Syntax Description

all	Forces all active calls currently associated with this MCM gatekeeper to be disconnected.
local-callID	Forces a single active call associated with this MCM gatekeeper to be disconnected.
<i>local-callID</i>	The local call identification number (CallID) that identifies the call to be disconnected.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 12.0(5)T	This command was introduced.

Usage Guidelines

If you want to force a particular call to be disconnected (as opposed to all active calls on the MCM gateway), use the CallID number to identify that specific call. You can find the local CallID number for a specific call by using the **show gatekeeper calls** command; the ID number is displayed in the LocalCallID column. Figure 1 shows output from the **show gatekeeper calls** command.

Figure 1 show gatekeeper calls Command Output

```
router# show gatekeeper calls

Total number of active calls =1
                        Gatekeeper Call Info
                        =====
LocalCallID           Age (secs)      BW
12-3339                94              768 (Kbps)
  Endpt(s): Alias      E.164Addr      CallSignalAddr  Port  RASignalAddr  Port
  src EP: epA          10.0.0.11      1720            10.0.0.11  1700
  dst EP: epB2zoneB.com
  src PX: pxA          10.0.0.1       1720            10.0.0.11  24999
  dst PX: pxB          172.21.139.90  1720            172.21.139.90  24999
```

Examples

The following example forces an active call on the MCM gateway to be disconnected. The local ID number of the active call is “12-3339.”

```
router> enable
router# clear h323 gatekeeper call local-callID 12-3339
```

The following example forces all active calls on the MCM gateway to be disconnected:

```
router> enable
router# clear h323 gatekeeper call all
```

Related Commands

Command	Description
show gatekeeper calls	Shows the status of each ongoing call that an MCM gatekeeper is aware of.

show gatekeeper calls

To show the status of each ongoing call that a gatekeeper is aware of, use the **show gatekeeper calls** Privileged EXEC command.

show gatekeeper calls

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Releases 11.3(2)NA and 12.(3)T	This command was introduced.
Cisco IOS Release 12.0(5)T	The output for this command was changed.

Usage Guidelines

Use the **show gatekeeper calls** command to show all active calls currently being handled by a particular MCM gatekeeper. If you have forced a disconnect for either a particular call or all calls associated with a particular MCM gatekeeper by using the **clear h323 gatekeeper call** command, the system will not display information about those calls.

Examples

The following is sample output from the **show gatekeeper calls** command:

```
router# show gatekeeper calls

Total number of active calls =1
      Gatekeeper Call Info
      =====
LocalCallID          Age (secs)      BW
12-3339              94              768 (Kbps)
Endpt(s): Alias      E.164Addr      CallSignalAddr  Port  RASSignalAddr  Port
src EP: epA          10.0.0.11      1720            1700  10.0.0.11      1700
dst EP: epB2zoneB.com
src PX: pxA          10.0.0.1       1720            24999 10.0.0.11      24999
dst PX: pxB          172.21.139.90  1720            24999 172.21.139.90  24999
```

Table 1 describes the fields contained in the **show gatekeeper calls** sample output.

Table 1 show gatekeeper calls Command Field Description

Field	Description
LocalCallID	Identification number of the call.
Age(secs)	The age of the call in seconds.
BW(Kbps)	The bandwidth in use in kilobits per second.
Endpoint(s)	Lists the role of each endpoints (terminal, gateway, or proxy) in the call (originator, target, or proxy), and the call signalling and RAS address.
Alias	H.323-ID or Email-ID of the endpoint.
E.164Addr	E.164 address of the endpoint.
CallSignalAddr	Call signalling IP address of the endpoint.
Port	Call signalling port number of the endpoint.
RASSignalAddr	RAS IP address of the endpoint.
Port	RAS port number of the endpoint.

Related Commands

Command	Description
clear h323 gateway call	Forces a disconnect on a specific call or all calls active on a particular MCM gateway.

show gatekeeper endpoints

To display the status of all registered endpoints for a gatekeeper, use the **show gatekeeper endpoints EXEC** command.

show gatekeeper endpoints

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2) NA	This command was introduced.
12.0(5) T	The display format was modified for H.323 Version 2.

Usage Guidelines

Use this command to display the status of all registered endpoints for a gatekeeper.

Examples

```
Router# show gatekeeper endpoints
CallSignalAddr  Port  RASignalAddr  Port  Zone Name  Type  F
-----
172.21.127.8    1720 172.21.127.8  24999 sj-gk      MCU   H323-ID:joe@cisco.com
172.21.13.88   1720 172.21.13.88  1719  sj-gk      VOIP-GW  O  H323-ID:la-gw
```

Table 2 describes the fields contained in the **show gatekeeper endpoints** sample output.

Table 2 show gatekeeper endpoints Command Field Descriptions

Field	Description
CallsignalAddr	Call signalling IP address of the endpoint. If the endpoint also registered with alias(s), a list of all aliases registered for that endpoint should also be listed on the line below.
Port	Call signalling port number of the endpoint.
RASSignalAddr	RAS IP address of the endpoint.
Port	RAS port number of the endpoint.
Zone Name	Zone name (gatekeeper ID) that this endpoint registered in..
Type	The endpoint type (for example, terminal, gateway, or MCU).
F	'S' — Indicates that the endpoint is statically entered from the alias command—rather than dynamically registered through RAS messages. 'O' — Indicates that the endpoint, which is a gateway, has sent notification that it is almost out of resources.

Related Commands

Command	Description
show gatekeeper gw-type-prefix	Displays the gateway technology prefix table.
show gatekeeper zone status	Displays current status of zones related to a gatekeeper.
show gateway	Displays current gateway status.

show gatekeeper gw-type-prefix

To display the gateway technology prefix table, use the **show gatekeeper gw-type-prefix** Privileged EXEC command.

show gatekeeper gw-type-prefix

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2) NA	This command was introduced.
12.0(5) T	The display format was modified for H.323 Version 2.

Usage Guidelines

Use the **show gatekeeper gw-type-prefix** command to display the gateway technology prefix table.

Examples

Following is a sample output for a gatekeeper that is controlling two local zones, “sj-gk” and “la-gk”:

```
router# show gatekeeper gw-type-prefix

GATEWAY TYPE PREFIX TABLE
=====
Prefix:12#*      (Default gateway-technology)
  Zone sj-gk master gateway list:
    172.21.13.11:1720 sj-gw1
    172.21.13.22:1720 sj-gw2 (out-of-resources)
    172.21.13.33:1720 sj-gw3
  Zone sj-gk prefix 408..... priority gateway list(s):
  Priority 10:
    172.21.13.11:1720 sj-gw1
  Priority 5:
    172.21.13.22:1720 sj-gw2 (out-of-resources)
    172.21.13.33:1720 sj-gw3
Prefix:7#*      (Hopoff zone la-gk)
  Statically-configured gateways (not necessarily currently registered):
    1.1.1.1:1720
    2.2.2.2:1720
  Zone la-gk master gateway list:
    171.69.127.11:1720 la-gw1
    171.69.127.22:1720 la-gw2
```

Table 3 describes the fields contained in the **show gatekeeper gw-type-prefix** sample output.

Table 3 show gatekeeper gw-type-prefix Command Field Descriptions

Field	Description
Prefix	The technology prefix defined with the gw-type-prefix command.
Zone sj-gk master gateway list	A list of all the gateways registered to zone sj-gk with the technology prefix, under which they are listed. (This display shows that gateways sj-gw1, sj-gw2, and sj-gw3 have registered in zone sj-gk with the technology prefix 12#.)
Zone sj-gk prefix 408..... priority gateway list(s)	A list of prioritized gateways to handle calls to area code 408.
Priority 10	Highest priority level. Gateways listed under priority 10 are given the highest priority when selecting a gateway to service calls to the specified area code. (In this display, <i>gateway sj-gw1</i> is given the highest priority to handle calls to the 408 area code.)
Priority 5	Any gateway that does not have a priority level assigned to it defaults to priority 5.
(out-of-resources)	This is an indication that the displayed gateway has sent a "low-in-resources" notification.
(Hopoff zone la-gk)	Any call specifying this technology prefix should be directed to hop off in the la-gk zone, no matter what the area code of the called number is. (In this display, calls specifying technology prefix 7# are always routed to zone la-gk, regardless of the actual zone prefix in the destination address.)
Zone la-gk master gateway list	A list of all the gateways registered to la-gk with the technology prefix under which they are listed. (This display shows that gateways la-gw1 and la-gw2 have registered in zone la-gk with the technology prefix 7#. No priority lists are displayed here because none were defined for zone la-gk.)
(Default gateway-technology)	If no gateway-type prefix is specified in a called number, then gateways registering with 12# are the default type to be used for the call.
(Statically-configured gateways)	Lists all IP addresses and port numbers of gateways that are incapable of supplying technology-prefix information when they register. This display shows that when gateways 1.1.1.1:1720 and 2.2.2.2:1720 register, they will be considered to be of type 7#.

Related Commands

Command	Description
show gatekeeper calls	Displays current gatekeeper status for each ongoing call.
show gatekeeper endpoints	Displays status of registered endpoints for a gatekeeper.
show gateway	Displays current gateway status.

show gatekeeper zone status

To display the status of zones related to a gatekeeper, use the **show gatekeeper zone status** Privileged EXEC command.

show gatekeeper zone status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2) NA	This command was introduced.
12.0(5)T	This display format was modified for H.323 Version 2.

Usage Guidelines

Use this command to display the status of all zones related to a gatekeeper.

Examples

```
router# show gatekeeper zone status

                                GATEKEEPER ZONES
                                =====
GK name      Domain Name    RAS Address    PORT  FLAGS  MAX-BW    CUR-BW
-----      -
sj.xyz.com   xyz.com          1.14.93.85     1719  LS           0
SUBNET ATTRIBUTES :
  All Other Subnets :(Enabled)
PROXY USAGE CONFIGURATION :
  inbound Calls from germany.xyz.com :
    to terminals in local zone sj.xyz.com :use proxy
    to gateways in local zone sj.xyz.com :do not use proxy
  Outbound Calls to germany.xyz.com
    from terminals in local zone germany.xyz.com :use proxy
    from gateways in local zone germany.xyz.com :do not use proxy
  Inbound Calls from all other zones :
    to terminals in local zone sj.xyz.com :use proxy
    to gateways in local zone sj.xyz.com :do not use proxy
  Outbound Calls to all other zones :
    from terminals in local zone sj.xyz.com :do not use proxy
    from gateways in local zone sj.xyz.com :do not use proxy
tokyo.xyz.co xyz.com          172.21.139.89  1719  RS           0
milan.xyz.co xyz.com          171.69.57.90  1719  RS           0
```

Table 4 describes the fields contained in the **show gatekeeper zone status** sample output.

Table 4 show gatekeeper zone status Command Field Descriptions

Field	Description
GK name	The gatekeeper name (also known as zone name), which is truncated after 12 characters in the display.
Domain Name	The domain with which the gatekeeper is associated.
RAS Address	The RAS address of the gatekeeper.
FLAGS	Displays the following information: S = Static (CLI-configured, not DNS-discovered) L = Local R = Remote
MAX-BW	The maximum bandwidth for the zone in kilobits per second.
CUR-BW	The current bandwidth in use, in kbps.
SUBNET ATTRIBUTES	A list of subnets controlled by the local gatekeeper.
PROXY USAGE CONFIGURATION	Inbound and outbound proxy policies as configured for the local gatekeeper (or zone).

Related Commands

Command	Description
show gatekeeper calls	Displays current gatekeeper status for each ongoing call.
show gatekeeper endpoints	Displays status of registered endpoints for a gatekeeper.
show gateway	Displays current gateway status.

use-proxy

Use the **use-proxy** command in gatekeeper configuration mode to enable proxy communications for calls between local and remote zones. The **no use-proxy** command has two forms and either removes a proxy configuration entry for a remote zone or disables proxy communications between local and remote zones.

```
use-proxy local-zone-name {default | remote-zone remote-zone-name } {inbound-to |
outbound-from } {gateway | terminal }
no use-proxy local-zone-name remote-zone remote-zone-name [ {inbound-to |
outbound-from } {gateway | terminal } ]
```

Syntax Description

<i>local-zone-name</i>	The name or zone name of the gatekeeper, which is usually the fully domain-qualified host name of the gatekeeper. For example, if the domain name is cisco.com, the gatekeeper name might be gk1.cisco.com. However, if the gatekeeper is controlling multiple zones, the name of the gatekeeper for each zone should be a unique string that has a mnemonic value.
default	Defines the default proxy policy for all calls that are not defined by a use-proxy command with the remote-zone keyword.
remote-zone <i>remote-zone-name</i>	Defines a proxy policy for calls to or from a specific remote gatekeeper or zone.
inbound-to	Applies the proxy policy to calls that are inbound to the local zone from a remote zone. Each use-proxy command defines the policy for only one direction.
outbound-from	Applies the proxy policy to calls that are outbound from the local zone to a remote zone. Each use-proxy command defines the policy for only one direction.
gateway	Defines the type of local device to which the policy applies. The gateway option applies the policy only to local gateways.
terminal	Defines the type of local device to which the policy applies. The terminal option applies the policy only to local terminals.

Defaults

The local zone uses proxy for both inbound and outbound calls to and from the local H.323 terminals only. Proxy is not used for both inbound and outbound calls to and from local gateways.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

This command replaces the **zone access** command used in the previous versions of the gatekeeper. When a previous version of gatekeeper is upgraded, any **zone access** commands are translated to **use-proxy** commands. You can use the **show gatekeeper zone status** command to see the gatekeeper proxy configuration.

Examples

In the following example, the local zone sj.xyz.com is configured to use a proxy for inbound calls from remote zones tokyo.xyz.com and milan.xyz.com to gateways in its local zone. The sj.xyz.com zone is also configured to use a proxy for outbound calls from gateways in its local zone to remote zones tokyo.xyz.com and milan.xyz.com:

```
router(config-gk) # use-proxy sj.xyz.com remote-zone tokyo.xyz.com inbound-to gateway
router(config-gk) # use-proxy sj.xyz.com remote-zone tokyo.xyz.com outbound-from gateway
router(config-gk) # use-proxy sj.xyz.com remote-zone milan.xyz.com inbound-to gateway
router(config-gk) # use-proxy sj.xyz.com remote-zone milan.xyz.com outbound-from gateway
```

Because the default mode disables proxy communications for all gateway calls, only the gateway call scenarios listed above can use the proxy.

In the next example, the local zone sj.xyz.com uses a proxy for only those calls that are outbound from H.323 terminals in its local zone to the specified remote zone germany.xyz.com:

```
router(config-gk) # no use-proxy sj.xyz.com default outbound-from terminal
router(config-gk) # use-proxy sj.xyz.com remote-zone germany.xyz.com outbound-from
terminal
```

Note that any calls inbound to H.323 terminals in the local zone sj.xyz.com from the remote zone germany.xyz.com use the proxy because the default applies.

The following example shows how to remove one or more proxy statements for the remote zone germany.xyz.com from the proxy configuration list:

```
router(config-gk) # no use-proxy sj.xyz.com remote-zone germany.xyz.com
```

The command above removes all special proxy configurations for the remote zone germany.xyz.com. After you enter a command like this, all calls between the local zone (sj.xyz.com) and germany.xyz.com are processed according to the defaults defined by any **use-proxy** commands that use the **default** option.

To prohibit proxy use for inbound calls to H.323 terminals in a local zone from a specified remote zone, enter a command similar to the following command:

```
router(config-gk) # no use-proxy sj.xyz.com remote-zone germany.xyz.com inbound-to
terminal
```

This command overrides the default and disables proxy use for inbound calls from remote zone germany.xyz.com to all H.323 terminals in the local zone sj.xyz.com.

Related Commands

Command	Description
show gatekeeper zone status	Displays the status of all zones related to a gatekeeper.

zone prefix

To add a prefix to the gatekeeper zone list, use the **zone prefix** gatekeeper configuration command. To remove knowledge of a zone prefix, use the **no** form of this command with the gatekeeper name and prefix. To remove the priority assignment for a specific gateway, use the **no** form of this command with the **gw-priority** option.

```
zone prefix gatekeeper-name e164-prefix [gw-priority pri-0-to-10 gw-alias [gw-alias, ...]]
```

```
no zone prefix gatekeeper-name e164-prefix [gw-priority pri-0-to-10 gw-alias [gw-alias, ...]]
```

Syntax Description

<i>gatekeeper-name</i>	The name of a local or remote gatekeeper, which must have been defined by using the zone local or zone remote command.
<i>e164-prefix</i>	An E.164 prefix in standard form followed by dots (.). Each dot represent a number in the E.164 address. For example, 212..... is matched by 212 and any seven numbers. Note Although a dot representing each digit in an E.164 address is the preferred configuration method, you can also enter an asterisk (*) to match any number of digits.
gw-priority <i>pri-0-to-10 gw-alias</i>	(Optional) Use the gw-priority option to define how the gatekeeper selects gateways in its local zone for calls to numbers beginning with prefix <i>e164-prefix</i> . Do not use this option to set priority levels for a prefix assigned to a remote gatekeeper. Use values from 0 to 10. A 0 value prevents the gatekeeper from using the gateway <i>gw-alias</i> for that prefix. Value 10 places the highest priority on gateway <i>gw-alias</i> . If you do not specify a priority value for a gateway, the value 5 is assigned. To assign the same priority value for one prefix to multiple gateways, list all the gateway names after the <i>pri-0-to-10</i> value. The <i>gw-alias</i> name is the H.323 ID of a gateway that is registered or will register with the gatekeeper. This name is set on the gateway with the h323-gateway voip h.323-id command.

Defaults

No knowledge of its own prefix or the prefix of any other zone is defined.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(6)Q	This command was introduced.
11.3(7)NA	This command was modified for H.323 Version 1.
12.0(5)T	This display format was modified for H.323 Version 2.

Usage Guidelines

A gatekeeper can handle more than one zone prefix, but a zone prefix cannot be shared by more than one gatekeeper. If you have defined a zone prefix as being handled by a gatekeeper and now define it as being handled by a second gatekeeper, the second assignment cancels the first.

If you need a gatekeeper to handle more than one prefix, but for cost reasons you want to be able to group its gateways by prefix usage, there are two ways to do it.

The first method is simpler, has less overhead, and is recommended if your gateways can be divided into distinct groups, where each group is to be used for a different set of prefixes. For instance, if a group of gateways is used for calling area codes 408 and 650, and another group is used for calling area code 415, you can use this method. In this case, you define a local zone for each set of prefixes, and have the group of gateways to be used for that set of prefixes register with that specific local zone. Do not define any gateway priorities. All gateways in each local zone are treated equally in the selection process.

However, if your gateways cannot be cleanly divided into nonintersecting groups (for instance if one gateway is used for calls to 408 and 415 and another gateway is used for calls to 415 and 650, and so on), you can put all these gateways in the same local zone and use the **gw-priority** option to define which gateways will be used for which prefixes.

When choosing a gateway, the gatekeeper first looks for the longest zone prefix match; then it uses the priority and the gateway status to select from the gateways. If all gateways are available, the gatekeeper chooses the highest priority gateway. If all the highest priority gateways are busy (see the gateway **resource threshold** command), a lower priority gateway is selected.

Note The **zone prefix** command matches a prefix to a gateway. It does not register the gateway. The gateway must register with the gatekeeper before calls can be completed through that gateway.

Examples

The following example shows how you can define multiple local zones for separating your gateways:

```
router(config-gk)# zone local gk408or650 xyz.com
router(config-gk)# zone local gk415 xyz.com
router(config-gk)# zone prefix gk408or650 408.....
router(config-gk)# zone prefix gk408or650 650.....
router(config-gk)# zone prefix gk415 415.....
```

Now you need to configure all the gateways to be used for area codes 408 or 650 to register with gk408or650 and all gateways to be used for area code 415 to register with gk415. On Cisco voice gateways, you configure the gateways to register with the appropriate gatekeepers by using the **h323 voip id** command.

The following example shows how you can put all your gateways in the same zone but use the **gw-priority** keyword to determine which gateways will be used for calling different area codes:

```
router(config-gk) # zone local localgk xyz.com
router(config-gk) # zone prefix localgk 408.....
router(config-gk) # zone prefix localgk 415..... gw-pri 10 gw1 gw2
router(config-gk) # zone prefix localgk 650..... gw-pri 0 gw1
```

The above commands accomplish the following tasks:

- Domain xyz.com is assigned to gatekeeper localgk.
- Prefix 408..... is assigned to gatekeeper localgk, and no gateway priorities are defined for it; therefore, all gateways registering to localgk can be used equally for calls to the 408 area code. No special gateway lists are built for the 408..... prefix; selection is made from the master list for the zone.
- The prefix 415..... is added to gatekeeper localgk, and priority 10 is assigned to gateways gw1 and gw2.
- Prefix 650..... is added to gatekeeper localgk, and priority 0 is assigned to gateway gw1.

A priority 0 is assigned to gateway gw1 to exclude it from the gateway pool for prefix 650..... When gateway gw2 registers with gatekeeper localgk, it is added to the gateway pool for each prefix as follows:

- For gateway pool for 415....., gateway gw2 is set to priority 10.
- For gateway pool for 650....., gateway gw2 is set to priority 5.

To change gateway gw2 from priority 10 for zone 415..... to the default priority 5, enter the following command:

```
router(config-gk) # no zone prefix localgk 415..... gw-pri 10 gw2
```

To change both gateways gw1 and gw2 from priority 10 for zone 415..... to the default priority 5, enter the following command:

```
router(config-gk) # no zone prefix localgk 415..... gw-pri 10 gw1 gw2
```

In the preceding example, the prefix 415..... remains assigned to gatekeeper localgk. All gateways that do not specify a priority level for this prefix are assigned a default priority of 5. To remove the prefix and all associated gateways and priorities from this gatekeeper, enter the following command:

```
router(config-gk) # no zone prefix localgk 415.....
```

Related Commands

Command	Description
resource threshold	Reports H.323 resource availability
register	Registers or de-register a fully-qualified dial-peer E.164 address with gatekeeper.
show call resource voice threshold	Displays current threshold configuration settings for H.323 gateway.
show gateway	Displays current gateway status.