H323: Gatekeepers

Calling Privileges

- Calling privileges define the destination a user is allowed to dial
- Primarily implemented on Cisco IOS gateways using class of restriction (COR)
- Dependant on proper call routing
- Higher granularity required for dial peers when deploying COR

Understanding COR on Cisco IOS Gateways

- Calling privileges are implemented using COR
- COR lists contain CORs and they are used to control call routing
- COR lists are assigned to dial peers:

  - Incoming COR list

  - Outgoing COR list

- For each call, the incoming COR list is matched against the outgoing COR list:

  - If the outgoing COR list is a subset of the incoming COR list, the call is routed

  - If no incoming COR list is configured, the call is always routed

Understanding COR for SRST and Cisco Unified Communications Manager Express

- Cisco Unified Communications Manager Express and Cisco Unified SRST use the standard Cisco IOS COR concept.
- Can be configured for inbound and outbound direction:

  - Inbound: Restrict destinations to which a user can dial

  - Outbound: Restrict who can call a user

- For Cisco Unified Communications Manager Express, COR lists are assigned to ephones.
- For Cisco Unified SRST, COR lists are assigned to number ranges.

Configuring COR for Cisco Unified Communications Manager Express

When using a standalone gateway:

- Define COR labels

- Configure COR lists

- Configure dial peers and assign COR lists

When using Cisco Unified Communications Manager Express:

- Assign COR lists to ephone-dn

H.323 Gatekeepers

- A gatekeeper is an optional network device that provides address translation and network access control for H.323 terminals, gateways, and multipoint control units.

Zones:

- H.323 endpoints are grouped into zones.

- Each zone has one logical gatekeeper that manages all the endpoints in the zone.

Zone prefixes:

- A zone prefix is the part of the called number that identifies the zone to which a call goes.

- Zone prefixes are usually used to associate an area or country code to a configured zone.

- The Cisco gatekeeper determines if a call is routed to a remote zone or handled locally.

Technology prefixes:

- This is an optional H.323 standard-based feature, supported by Cisco gateways and gatekeepers, that enables more flexibility in call routing within an H.323 network.

- The Cisco gatekeeper uses technology prefixes to group endpoints together by type such as voice or video, by class, or to define a pool of gateways.

Technology prefix with hopoff:

- Calls will be routed to a specified zone, regardless of what the zone prefix in the address is.

Cisco IOS gatekeeper functionality is available with the following hardware and software:

- IP Voice Image

- Advanced Enterprise Image

- IP H.323 Image

- Advanced IP Services Image

- Service Provider Services Image

Cisco gatekeepers use H.323 RAS, the Gatekeeper Update Protocol (GUP), and GKTMP as signaling methods when providing call services.

H.323 version 2 requires the full registration process for initial registration, but uses an abbreviated renewal procedure to update the gatekeeper and minimize overhead.

The gatekeeper periodically sends an IRQ to each registered endpoint to verify that it still exists. The gatekeeper can use the RAS channel to obtain status information from endpoints.

Two methods used to determine the address of the gatekeeper:

- An endpoint can be preconfigured to recognize the domain name or IP address of its gatekeeper. If configured to recognize the name, an endpoint must have a means to resolve the name to an IP address. A common address resolution technique is the Domain Name System (DNS).

- An endpoint can issue a multicast GRQ to the gatekeeper discovery address (224.0.1.41) to discover the IP address of its gatekeeper.

Directory gatekeepers are used to do the following:

- Scale large VoIP networks

- Forward LRQ messages between gatekeepers

- Eliminate the requirement for a full mesh by having gatekeepers point to the directory gatekeeper

- Provide a hierarchical centralized dial plan

- **Gatekeeper Transaction Message Protocol (GKTMP)** can extend the call control intelligence of a gatekeeper by providing an interface to a route application server where advanced routing decisions can be made. The server can override default gatekeeper behavior.

- **Gatekeeper Route Control Server (GKRCS)** is an independent platform using GKTMP, and it can run on Solaris, Linux, or Microsoft Windows NT.

- Use the **show gatekeeper status** command to display overall gatekeeper status, including authorization and authentication status and zone status.

- The **show gatekeeper endpoint** command displays the gateways that have registered to a gatekeeper.

- Use the **show gatekeeper zone prefix** command to display the zone prefix table for the gatekeeper.

- Use the **show gatekeeper zone status** command to display the status of zones related to a gatekeeper.

ITSP Connectivity

Gatekeeper Configuration Steps:

1. Configure local and remote zones on the gatekeeper.

   - Enter gatekeeper configuration mode:

   Router(config)# **gatekeeper**

   - Specify a local zone to be controlled by the gatekeeper:

   Router(config-gk)# **zone local** *gatekeeper-name domain-name* [*ras-IP-address*] [**invia** *inbound gatekeeper* | **outvia** *outbound gatekeeper* [**enable-intrazone**]]

   - Specify a remote gatekeeper to which the local gatekeeper can send LRQs:

   Router(config-gk)# **zone remote** *othergatekeeper-name otherdomain-name othergatekeeper-ip-address* [*portnumber*] [**cost** *cost-value*] [**priority** *priority-value*] [**foreign-domain**] [**invia** *inbound gatekeeper*] | [**outvia** *outbound gatekeeper*]

   - Activate the gatekeeper:

   Router(config-gk)# **no shutdown**

2. Configure zone prefixes.

   - Enter gatekeeper configuration mode:

   Router(config)# **gatekeeper**

Add a prefix to the gatekeeper zone list:

router(config-gk)# **zone prefix** *gatekeeper-name e164-prefix* **[blast | seq] [gw-priority** *priority gwalias [gw-alias, ...]* **]**

3. Configure technology prefixes:

Router(config)# **gw-type-prefix** *type-prefix* [[**hopoff** *gkid1*] [**hopoff** *gkid2*] [**hopoff** *gkidn*] [**seq** | **blast**]] [**default-technology**] [[**gw ipaddr** *ipaddr* [*port*]]]

4. Activate the gatekeeper:

Router(config-gk)# **no shutdown**

Steps for configuring gateways to use H.323 gatekeepers

1. Enable the H.323 VoIP gateway to register with the gatekeeper:

router(config)# **gateway**

2. Enter interface configuration mode for the interface you intend to use with the H.323 gatekeeper:

router(config)# **interface Loopback 0**

3. Give the interface an IP address:

router(config-if)# **ip-address** [*ip-address subnet-mask*]

4. Configure the interface as an H.323 gateway interface:

   router(config-if)# **h323-gateway voip interface**

5. Bind the interface:

   router(config-if)# **h323-gateway voip bind srcaddr** [*ip-address*]

6. Define the name and location of the gatekeeper (optional):

   router(config-if)# **h323-gateway voip id Houston ipaddr** *ip-address* [*port*] **priority** [*priority*]

7. Specify the H.323 gateway name to identify it to its associated gatekeeper (optional):

   router(config-if)# **h323-gateway voip h323-id Houston**

8. Specify the tech-prefix that the gateway registers with the gatekeeper (optional):

   router(config-if)# **h323-gateway voip tech-prefix** [*prefix*]

Steps to create a dial peer to be used with a gatekeeper:

1. Enter dial-peer configuration mode:

   Router(config)# **dial-peer voice 1 voip**

2. Specify the E.164 address associated with this dial peer:

   Router(config-dial-peer)# **destination pattern** [*string*]

3. Define the numbers used as the technology prefix that the gateway registers with the gatekeeper (optional):

   Router(config-dial-peer)# **tech-prefix** [*number*]

4. Specify that the RAS protocol is being used to determine the IP address of the session target:

   Router(config-dial-peer)# **session target ras**

Use the **show gatekeeper gw-type-prefix** command to display configured prefixes.

Use the **show gatekeeper status** command to display the status of the gatekeeper.

Use the **show gatekeeper zone prefix** command to display configured zone prefixes.

Use the **show gatekeeper endpoints** command to display registered endpoints of the gatekeeper.

Call Admission Control (CAC)

The CAC function is an essential component of any Cisco Unified Communications system that involves multiple sites connected through an IP WAN. It allows you to maintain a desired level of voice quality over a WAN link.

CAC regulates voice quality by limiting the number of calls that can be active on a particular link at the same time.

The Cisco IOS gatekeeper is the device in the IP communications network that is responsible for CAC between the following devices:

- Cisco Unified Communications Manager

- Cisco Unified Communications Manager Express

- H.323 gateways

Zone bandwidth in a gatekeeper network can be calculated with the following simple formula:

Bandwidth = (Number of calls) * (Codec Bandwidth) * 2

The **bandwidth** command allows the gatekeeper to manage the bandwidth limitations within a zone, across zones, and at a per-session level. By default, the maximum aggregate bandwidth is unlimited.

Resource Availability Indicator (RAI)

- RAI performs resource-availability in gatekeeper networks.

- RAS signaling allows a gateway to inform the gatekeeper when it is running short on resources. The information is sent via RAI messages. RAI messages are sent by endpoints to indicate when they have neared resource limits or are no longer near a resource limit. The gatekeeper replies with Resource Available Confirm (RAC) messages.

To configure a gateway to report H.323 resource availability to its gatekeeper, use the **resource threshold** command in gateway configuration mode.

router(config-gateway)# **resource threshold** [**all**] [**high** *percentage-value*] [**low** *percentage-value*] **report-policy [addressable** | **idle-only]**

RAI has to be configured on each endpoint that should send RAI information in your network.

The Cisco UBE is an intelligent unified communications network border element.

Cisco UBE Functionality

- Cisco UBE interconnects VoIP networks
- Also called session border controller
- Implemented on Cisco IOS gateways using special Cisco IOS release
- Ability to connect one VoIP dial peer with another VoIP dial peer
- Powerful protocol interworking tool set:

  - H.323-to-SIP

  - H.323-to-H.323

  - SIP-to-SIP

The Cisco UBE provides a network-to-network interface point for the following:

- Signaling interworking: H.323, SIP
- Media interworking: dual-tone multifrequency (DTMF), fax, modem, and coder-decoder (codec) transcoding
- Address and port translations: privacy and topology hiding
- Billing and call detail record (CDR) normalization
- Quality of service (QoS) and bandwidth management: QoS marking using differentiated services code point (DSCP) or type of service (ToS), bandwidth enforcement using Resource Reservation Protocol (RSVP) and codec filtering

Cisco IOS Image Support for Cisco UBE

- Cisco UBE functionality is supported on most current platforms including Cisco 2800 and 3800 Series ISR
- Introduced with Cisco IOS Release 12.2(13)T
- Requires one of the following Cisco IOS feature sets:

  - INT VOICE/VIDEO, IPIPGW, TDMIP GW AES

  - INT VOICE/VIDEO, IPIPGW, TDMIP GW

Cisco UBE in enterprise deployments serves two main purposes:

- **External connections:** A Cisco UBE can be used as a demarcation point within a unified communications network and it provides interconnectivity with external networks. This includes H.323 voice and video connections and SIP VoIP connections.
- **Internal connections:** When used within a VoIP network, a Cisco UBE can be used to increase the flexibility and interoperability between different devices.

The following are some key features offered by Cisco UBE:

- **Protocol interworking:** The Cisco UBE supports interworking of signaling protocols, including H.323-to-H.323, H.323-to-SIP, and SIP-to-SIP.
- **Address hiding:** A Cisco UBE can hide or replace the endpoint IP addresses used for the media connection.
- **Security:** A Cisco UBE can be placed in a demilitarized zone (DMZ) and it provides outside connectivity to external networks.
- **Video integration:** In addition to VoIP services, a Cisco UBE also supports H.323 video connections.
- **Call Admission Control (CAC):** A Cisco UBE can use Cisco IOS-based CAC mechanisms, including the Resource Reservation Protocol (RSVP).

Protocol Interworking on Cisco UBE

- Solves interoperability issues when using different signaling protocol or when devices have different capabilities
- Translates between signaling protocols:

  - Each call leg terminates on the Cisco UBE.

  - The Cisco UBE examines received information, performs translation, and reoriginates a new call leg.

Media Flows with Cisco UBE

- Cisco UBE can act as a proxy for H.323 and SIP (proxy signaling).
- Media flow-through (default): All media streams are routed through the Cisco UBE.

  - Solves IP interworking issues

  - Hides IP original addresses

  - Enables tighter security policies

- Media flow-around: Media streams flow directly between endpoints.

Codec Filtering on Cisco UBE

- VoIP networks support multiple codecs:

  - Preferences define which codecs are selected over others

- Cisco UBE can limit codec negotiation down to a single codec:

  - Ensures that a specific codec is negotiated

  - Simplifies design considerations

- Cisco UBE also support transparent codec negotiations:

  - Transparently passes codec capabilities between endpoints

- Implemented via dial peer configuration

Whether performing codec filtering or operating in transparent mode, a Cisco UBE is required to support the codec used between endpoints. The following codecs are supported:

- **Audio codecs:** G.711u, G.711a, G.723, G.726, G.729r8, G.728, and Adaptive Multirate Narrow Band (AMR-NB)
- **Video codecs (H.323 only):** H.261, H.263, and H.264

RSVP-Based CAC on Cisco UBE

- Cisco UBE can use standard Cisco IOS gateway RSVP call support.
- Enables RSVP-based CAC:

  - Cisco Unified Communications Manager intercluster RSVP-based CAC

  - Support for voice and video calls

- Requirements:

  - Two Cisco UBEs used as RSVP peers

  - Media-flow through to ensure that the reserved path is used

Cisco UBE and Gatekeeper Interworking

- Cisco UBE can register with a gatekeeper like any other Cisco IOS gateway.

  - The gatekeeper and Cisco UBE may be deployed on the same router.

- Cisco UBE can also be used by gatekeepers using via-zones.

  - A via-zone is a Cisco term for a zone that contains Cisco UBE and via-zone-enabled gatekeepers.

  - The via-zone-enabled gatekeeper is capable of recognizing via-zones and sending traffic to via-zone gateways.

  - Via-zones are usually located on the edge of an enterprise or Internet telephony service provider network, and are like a VoIP transfer point, or tandem zone, where traffic passes through on the way to the remote zone destination.

To enable protocol interworking, use the **allow-connections** *from-type* **to** *to-type* command in global voice service configuration mode. The *from-type* and *to-type* options specify the signaling protocols. The configuration for H.323 and SIP interworking is unidirectional, thus if bidirectional interworking is required, you need to configure the mirror-matching statement as well. For example, if bidirectional H.323-to-SIP interworking is required, you need to configure **allow connections h323 to sip** as well as **allow connections sip to h323**.

By default, a Cisco IOS gateway will not allow connections between two VoIP dial peers. To change this behavior and allow H.323-to-H.323 connections, use the **allow-connections h323 to h323** command in voice service configuration mode.

As with an H.323-to-H.323 connection, by default a Cisco IOS gateway will not allow connections between an H.323 and a SIP VoIP dial peer. To change this behavior and allow H.323-to-SIP connections, use the **allow-connections h323 to sip** command in voice service configuration mode. The last command enables SIP to H.323 calls.

Media Flow and Transparent Codec Commands

media

To configure media flow-through or media flow-around, use the **media** command. This can be done in dial-peer configuration mode or globally under the voice service configuration mode. The default is **media flow-through**.

codec transparent

To configure transparent codec pass-through, use the **codec transparent** command. This can be done in dial-peer configuration mode or via a codec class.

To enable endpoint-to-endpoint codec negotiation without the Cisco UBE, use the **codec transparent** command.

Media flow-around for SIP-to-SIP calls is not supported. Use the **media flowaround** command to enable media flow-around.

When a call is active, the **show gatekeeper calls** command will display two call legs. The first call leg is between the originating gateway (Router 1, in this case) and the Cisco UBE.

hunt-scheme sequential

To specify the sequential search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme sequential** command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of this command.

hunt-scheme sequential [**both** | **even** | **odd** [**up** | **down**]]

no **hunt-scheme**

Syntax Description

both	Searches both even- and odd-numbered channels.
even	Searches for an idle even-numbered channel. If no idle even-numbered channel is available, an odd-numbered channel is sought.
odd	Searches for an idle odd-numbered channel. If no idle odd-numbered channel is available, an even-numbered channel is sought.
up	Searches channels in ascending order based within a trunk group member. Used with **even**, **odd**, **both**.
down	Searches channels in descending order within a trunk group member. Used with **even**, **odd**, **both**.

Defaults

Hunt scheme: least-used
Channel number: both
Direction: up

Command Modes

Trunk group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The sequential hunt scheme selects an idle channel, starting with the trunk group member that has the highest preference within the trunk group. Regardless of where the last idle channel was found, an idle channel request starts searching with this highest-preference trunk group member.

For example, suppose a trunk group has three trunk group members: A, B, and C. Trunk group member A has the highest preference, B has the next highest, and C has the lowest. The software starts the search with trunk group A:

- If A has an idle channel, that channel is used, and the next request for an idle channel starts with A.
- If A does not have an idle channel, the search moves to B:
- If B has an idle channel, that channel is used, and the next request for an idle channel starts with A.
- If B does not have an idle channel, the search moves to C:
- If C has an idle channel, that channel is used, and the next request for an idle channel starts with A.
- If C does not have an idle channel, the software returns the standard "no service" message.

Compare this hunt scheme with **hunt-scheme round-robin**, where the next request for an idle channel starts with the next unused trunk group member of the trunk group.

If the **even** qualifier is set, the search looks for an even-numbered idle channel starting with the trunk group member having the highest preference. If no even-numbered idle channel is found, the search looks for an even-numbered idle channel in the next trunk group member. If no even-numbered idle channel is found, the search repeats the process for an odd-numbered idle channel.

If the **odd** qualifier is set, the search begins looking for an odd-numbered channel, starting with the trunk group member having the highest preference. If none is found in any of the trunk group members, the search repeats the process for an even-numbered channel.

If the **both** qualifier is set, the search looks for any idle channel in the trunk group member.

Use the sequential hunt scheme in situations that benefit from a predictable channel allocation. In addition, if one end of the routing path is defined with **sequential even up** and the other end with **sequential odd up**, glare conditions are avoided.

Examples

The following example searches in ascending order for an even-numbered idle channel starting with the trunk group member of highest precedence:

```
Router(config)# trunk group northwestsales
Router(config-trunk-group)# hunt-scheme sequential even up
```