Remote to Local Network with the Cisco Multiservice IP–to–IP Gateway Feature

Document ID: 48303

Contents

Introduction

This document provides a sample configuration for a remote to local network using the Cisco Multiservice IP–to–IP Gateway (IPIPGW) feature. The IPIPGW feature provides a mechanism to enable H.323 Voice over IP (VoIP) calls from one IP network to another.

Prerequisites

Requirements

Before attempting this configuration, please ensure that you meet these requirements:

- Perform basic H.323 gateway configuration. For detailed instructions, see the Cisco IOS H.323 Configuration Guide, Cisco IOS Voice Configuration Library, Release 12.3.
- Perform basic H.323 gatekeeper configuration. For detailed instructions, see the Cisco IOS H.323 Configuration Guide, Cisco IOS Voice Configuration Library, Release 12.3.

Components Used

The information in this document is based on these software and hardware versions:

- Three Cisco H.323 Gatekeeper Routers (Cisco 2610, Cisco 2611, Cisco 2612, Cisco 2613, Cisco 2620, Cisco 2621, Cisco 2650, Cisco 2651, Cisco 2691, Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 3620, Cisco 3649, Cisco 3660, Cisco 3725, Cisco 3745, Cisco 7200 Series, or Cisco 7400 Series) with Cisco IOS Software Release 12.3(4)T or later.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live

network, ensure that you understand the potential impact of any command before using it.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Background Information

The Cisco Multiservice IPIPGW feature introduces gatekeeper via−zones. Via−zone is a Cisco term for a zone that contains IP-to−IP gateways and via−zone−enabled gatekeepers. A via−zone−enabled gatekeeper is capable of recognizing via−zones and sending traffic to via−zone gateways. Cisco via−zone enabled gatekeepers include a via−zone command−line interface (CLI) command.

Via−zones are usually located on the edge of an ITSP network, and are like a VoIP transfer point, or tandem zone, where traffic passes through on the way to the remote zone destination. Gateways in this zone terminate requested calls and re−originate traffic to its final destination. Via−zone gatekeepers operate as usual for non−IP to IP applications. Gatekeepers in via−zones support resource management (for example, gateway selection and load balancing) using the capacities field in the H.323 Version 4 RAS messages.
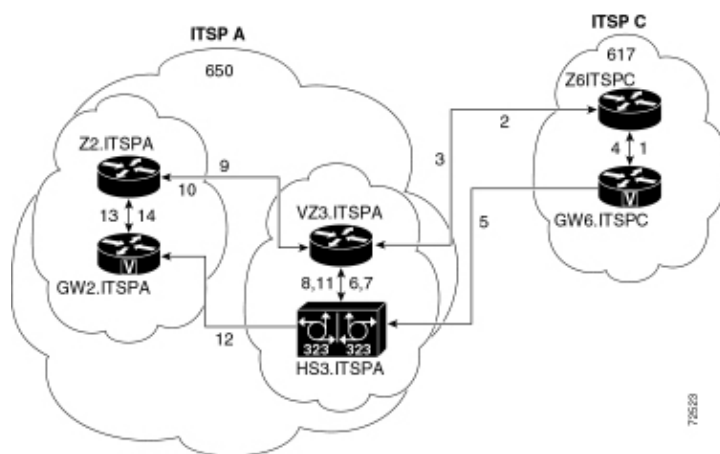
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses this network setup:

Configurations

This document uses these configurations:

- Originating Gatekeeper (Z6.ITSPC)
- Via−zone Gatekeeper (VZ3.ITSPA)
- Terminating Gatekeeper (Z2.ITSPA)

In this example, a caller from area code 617 calls a party in area code 650, and the following actions occur:

1. GW6.ITSPC sends an ARQ with the 650–based number to Z6.ITSPC.
2. Z6.ITSPC knows that prefix 650 belongs to VZ3.ITSPA, so Z6.ITSPC sends an LRQ to VZ3.ITSPA.
3. The LRQ for the 650 number is received by VZ3.ITSPA. VZ3.ITSPA looks at the H.323 ID in the inbound LRQ to find the remote zone. Then it looks for a via–zone keyword associated with that remote zone. Since the via–zone gatekeeper ID is a local zone, it allocates the call to the IP–to–IP gateway in the via–zone and sends back an LCF specifying HS3.ITSPA.
4. Z6.ITSPC returns an ACF specifying HS3.ITSPA.
5. GW6.ITSPC sends a SETUP message to HS3.ITSPA for the 650 call.
6. HS3.ITSPA consults VZ3.ITSPA with an ARQ (containing answerCall=true) to admit the incoming call.
7. VZ3.ITSPA responds with an ACF to admit the call.
8. HS3.ITSPA has a dial peer specifying RAS VZ3.ITSPA for the 650 prefix (or for all prefixes), so it sends the ARQ (with answerCall set to FALSE) to VZ3.ITSPA for prefix 650.
9. VZ3.ITSPA sees prefix 650 as Z2.ITSPA, so VZ3.ITSPA sends an LRQ to Z2.ITSPA.
10. Z2.ITSPA sees prefix 650 as in its own zone and returns an LCF pointing to GW2.ITSPA.
11. VZ3.ITSPA returns an ACF specifying GW2.ITSPA.
12. HS3.ITSPA sends a SETUP message to GW2.ITSPA for the 650 call.
13. GW2.ITSPA sends an ARQ answerCall to Z2.ITSPA.
14. Z2.ITSPA sends an ACF to GW2.ITSPA for answerCall.

Originating Gatekeeper (Z6.ITSPC)

```
origgatekeeper# show running-config
 Building configuration...
 .
 .
 .
 gatekeeper
  zone local Z6ITSPC zone2 10.16.6.158
  zone remote VZ3ITSPA zone2 10.16.10.139 1719
  zone prefix VZ3ITSPA 650*
 .
 .
 .
 !
 end
```

Via–zone Gatekeeper (VZ3.ITSPA)

```
vzgatekeeper# show running-config
 Building configuration...
 .
 .
 .
 gatekeeper
  zone local VZ3ITSPA zone2 10.16.10.139
  zone remote Z2ITSPA zone2 10.16.10.144 1719 outvia VZ3ITSPA
  zone remote Z6ITSPC zone1 10.16.6.158 1719 invia VZ3ITSPA
  zone prefix Z2ITSPA 650*
 .
 .
 .
 !
 end
```

Terminating Gatekeeper (Z2.ITSPA)

```
termgatekeeper# show running-config
```

```
Building configuration...
.
.
.
gatekeeper
 zone local Z2ITSPA zone2 10.16.10.144
.
.
.
!
end
```

Verify

This section provides information you can use to confirm your configuration is working properly.

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

To verify gatekeeper configuration, use the **show running config | begin gatekeeper** command:

```
gatekeeper
 zone local VZ3ITSPA zone2 10.16.10.139
 zone remote Z2ITSPA zone2 10.16.10.144 1719 outvia VZ3ITSPA
 zone remote Z6ITSPC zone1 10.16.6.158 1719 invia VZ3ITSPA
 zone prefix Z2ITSPA 650*
            no shutdown
```

You can also use the **show gatekeeper zone status** command to verify gatekeeper configuration:

```
          GATEKEEPER ZONES
          ================
GK name       Domain Name  RAS Address    PORT  FLAGS
-------       -----------  -----------    ----- -----

VZ3ITSPA      zone2        10.16.128.40   1719  LSV
  BANDWIDTH INFORMATION (kbps) :
    Maximum total bandwidth :unlimited
    Current total bandwidth :0
    Maximum interzone bandwidth :unlimited
    Current interzone bandwidth :0
    Maximum session bandwidth :unlimited
    Total number of concurrent calls :3
  SUBNET ATTRIBUTES :
    All Other Subnets :(Enabled)
  PROXY USAGE CONFIGURATION :
    Inbound Calls from all other zones :
      to terminals in local zone hurricane :use proxy
      to gateways in local zone hurricane  :do not use proxy
      to MCUs in local zone hurricane  :do not use proxy
    Outbound Calls to all other zones :
      from terminals in local zone hurricane :use proxy
      from gateways in local zone hurricane  :do not use proxy
      from MCUs in local zone hurricane  :do not use proxy

  Z1.ITSPA     cisco        10.16.10.139   1719  RS
    VIAZONE INFORMATION :
      invia:VZ4.ITSPA,  outvia:VZ4.ITSPA

  Z5.ITSPB     cisco        10.16.8.144    1719  RS
    VIAZONE INFORMATION :
      invia:VZ4.ITSPA,  outvia:VZ4.ITSPA
```

Enter the **show gatekeeper status** command to view call capacity thresholds:

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

Enter the **show gatekeeper performance stats** command to view RAS information, including via−zone statistics:

```
Performance statistics captured since: 08:16:51 GMT Tue Jun 11 2002

RAS inbound message counters:
        Originating ARQ: 462262 Terminating ARQ: 462273 LRQ: 462273
RAS outbound message counters:
        ACF: 924535      ARJ: 0  LCF: 462273      LRJ: 0
        ARJ due to overload: 0
        LRJ due to overload: 0

RAS viazone message counters:
        inLRQ: 462273    infwdLRQ 0       inerrLRQ 0
        outLRQ: 0        outfwdLRQ 0      outerrLRQ 0
        outARQ: 462262  outfwdARQ 0      outerrARQ 0
Load balancing events: 0
Real endpoints: 3
```

The following table describes the significant RAS via−zone fields shown in the display.

Field	Description
inLRQ	Associated with the invia keyword. If the invia is a local zone, this counter identifies the number of LRQs terminated by the local invia gatekeeper.
infwdLRQ	Associated with the invia keyword. If the invia is a remote zone this counter identifies the number of LRQs that were forwarded to the remote invia gatekeeper.
inerrLRQ	Associated with the invia keyword. Number of times the LRQ could not be processed because the invia gatekeeper ID could not be found. Usually caused by a misspelled gatekeeper name.
outLRQ	Associated with the outvia keyword. If the outvia is a local zone, this counter identifies the number of LRQs terminated by the local outvia gatekeeper. This counter applies only in configurations where no invia gatekeeper is specified.
outfwdLRQ	Associated with the outvia keyword. If the outvia is a remote zone, this counter identifies the number of LRQs that were forwarded to the remote outvia gatekeeper. This counter applies

	only in configurations where no invia gatekeeper is specified.
outerrLRQ	Associated with the outvia keyword. Number of times the LRQ could not be processed because the outvia gatekeeper ID could not be found. Usually caused by a misspelled gatekeeper name. This counter applies only in configurations where no invia gatekeeper is specified.
outARQ	Associated with the outvia keyword. Identifies the number of originating ARQs handled by the local gatekeeper if the outvia is that local zone.
outfwdARQ	Associated with the outvia keyword. If the outvia gatekeeper is a remote zone, this number identifies the number of originating ARQs received by this gatekeeper that resulted in LRQs being sent to the outvia gatekeeper.
outerrARQ	Associated with the outvia keyword. Number of times the originating ARQ could not be processed because the outvia gatekeeper ID could not be found. Usually caused by a misspelled gatekeeper name.

Enter the **show gatekeeper circuit** command to view information on calls in progress:

```
                    CIRCUIT INFORMATION
                    ===================
   Circuit        Endpoint   Max Calls Avail Calls Resources     Zone
   -------        --------   --------- ----------- ---------     ----
   ITSP B         Total Endpoints: 1
                  hs4.itspa  200       198         Available
```

Note: The word calls refers to call legs in some commands and output.

Enter the **show gatekeeper endpoint** command to view information on endpoint registrations:

```
        GATEKEEPER ENDPOINT REGISTRATION
              ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type     Flags
--------------- ----- --------------- ----- ---------         ----     -----
10.16.10.140    1720  10.16.10.140    50594 vz4.itspa         H323-GW
    H323-ID: hs4.itspa
    H323 Capacity Max.= 200  Avail.= 198
Total number of active registrations = 1
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Procedure

Below is troubleshooting information relevant to this configuration. For additional information on troubleshooting, see Cisco Multiservice IP–to–IP Gateway. Follow the instructions below to troubleshoot your configuration.

The procedures for troubleshooting an IPIPGW are similar to troubleshooting a TDM−to−IP H.323 gateway. Generally, your troubleshooting efforts should proceed as follows:

1. Isolate and reproduce the failing scenario.
2. Collect relevant information from **debug** and **show** commands, configuration files, and protocol analyzers.
3. Identify the first indication of failure in protocol traces or internal debug output.
4. Look for the cause in configuration files.

If the via−zone is suspected as the source of a call failure, isolate the problem to an IPIPGW or gatekeeper by identifying affected the subfunction and focus on show and debug commands related to that subfunction.

Before you can begin troubleshooting, you first must isolate the problem to either a gateway or gatekeeper. Gateways and gatekeepers are responsible for the following tasks:

Gateway Tasks

- Media stream handling and speech path integrity
- DTMF relay
- Fax relay and passthrough.
- Digit translation and call processing
- Dial−peers and codec filtering
- Carrier ID handling
- Gateway−based billing

Gatekeeper Tasks

- Gateway selection and load balancing
- Call routing (zone selection)
- Gatekeeper−based billing
- Control of call admission, security, and bandwidth
- Enforcement of call capacities

Troubleshooting Commands

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

Note: Before issuing **debug** commands, please see Important Information on Debug Commands.

Gateway debug Commands

- **debug voip ipipgw** This command displays information related to the handling of IP−to−IP calls
- **debug h225 asnl** This command displays the actual contents of the asn1 part of H.225 messages and associated events.
- **debug h225 events** This command displays the actual contents of the asn1 part of H.225 messages and associated events.
- **debug h245 asn1** This command displays the actual contents of the asn1 part of H.245 messages and associated events.
- **debug h245 events** This command displays the actual contents of the asn1 part of H.245 messages and associated events.
- **debug cch323 all** When **debug cch323** is used with **h225**, **h245**, or **ras** keywords, the debug output traces the state transitions of the associated state machines based on the processed events.

- **debug voip ccapi inout** This command traces the execution path through the call control API, which serves as the interface between the call session application and the underlying network–specific software.
- **debug voice ccapi error** This command traces the error logs in the call control API. Error logs are generated during normal call processing when there are insufficient resources or when there are problems in the underlying network–specific code, the higher call session application, or the call control API itself.

Gatekeeper debug Commands

- **debug h225 asn1** This command displays the actual contents of the asn1 portion of H.225 RAS messages and associated events.
- **debug h225 events** This command displays the actual contents of the asn1 portion of H.225 RAS messages and associated events.
- **debug gatekeeper main 10**This command traces major gatekeeper functions, such as LRQ processing, gateway selection, admission request processing, prefix matching, and call capacities.
- **debug gatekeeper zone 10** This command traces gatekeeper zone–oriented functions.
- **debug gatekeeper call 10** This command traces gatekeeper call–oriented functions, such as tracking call references.
- **debug gatekeeper gup asn1** This command displays the actual contents of the asn1 portion of gatekeeper update protocol messages and associated events for communication between gatekeepers in a cluster.
- **debug gatekeeper gup events** This command displays the actual contents of the asn1 portion of gatekeeper update protocol messages and associated events for communication between gatekeepers in a cluster.
- **debug ras** This command displays the types and addressing of RAS messages sent and received.

Gateway show Commands

- **show h323 gateway h225** This command maintains counts of H.225 messages and events.
- **show h323 gateway ras** This command maintains counts of RAS messages sent and received.
- **show h323 gateway cause** This command shows counts of cause codes received from connected gateways.
- **show call active voice [brief]** These commands aggregate information about active and cleared calls.
- **show crm** This command shows the call capacity counts associated with IP circuits on the IPIPGW.
- **show processes cpu** This command shows detailed CPU utilization statistics (CPU use per process).
- **show gateway** This command shows the current status of the gateway.

Gatekeeper show Commands

- **show/clear gatekeeper performance stats** This command shows the gatekeeper statistics associated with processing calls.
- **show gatekeeper zone status** This command lists information about the local and remote zones known to the gatekeeper.
- **show gatekeeper endpoint** This command lists key information about the endpoints registered to the gatekeeper, including IPIPGWs.
- **show gatekeeper circuit** This command combines information about circuit utilization across multiple gateways.
- **show gatekeeper calls** This command lists key information about calls being handled in the local zone.

Related Information

- **Voice Technology Support**
- **Voice and Unified Communications Product Support**
- **Troubleshooting Cisco IP Telephony**
- **Technical Support – Cisco Systems**

Updated: Feb 02, 2006   Document ID: 48303