Red remota a local con la función Cisco Multiservice IP-to-IP Gateway

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Convenciones
Antecedentes
Configurar
Diagrama de la red
Configuraciones
Verificación
Troubleshoot
Procedimiento de Troubleshooting
Comandos para resolución de problemas
Información Relacionada

Introducción

Este documento proporciona una configuración de ejemplo para una red remota a local mediante la función Cisco Multiservice IP-to-IP Gateway (IPGW). La función IPGW proporciona un mecanismo para habilitar las llamadas de voz sobre IP (VoIP) H.323 de una red IP a otra.

Prerequisites

Requirements

Antes de intentar esta configuración, asegúrese de cumplir estos requisitos:

- Realice la configuración básica del gateway H.323. Para obtener instrucciones detalladas, vea la Guía de Configuración de H.323 de Cisco IOS, Biblioteca de Configuración de Voz de Cisco IOS, Versión 12.3.
- Realice la configuración básica del gatekeeper H.323. Para obtener instrucciones detalladas, vea la Guía de Configuración de H.323 de Cisco IOS, Biblioteca de Configuración de Voz de Cisco IOS, Versión 12.3.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Tres routers Cisco H.323 Gatekeeper (Cisco 2610, Cisco 2611, Cisco 2612, Cisco 2613, Cisco 2620, Cisco 2621, Cisco 2650, Cisco 2651, Cisco 2691 y Cisco 266 Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 3620, Cisco 3649, Cisco 3660, Cisco 3725, Cisco 37441 Cisco 7200 Series o Cisco 7400 Series) con Cisco IOS Software Release 12.3(4)T o posterior.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Antecedentes

La función IPGW multiservicio de Cisco introduce el control de acceso por zonas. Via-zone es un término de Cisco para una zona que contiene gateways IP a IP y gatekeepers habilitados para vía-zone. Un gatekeeper habilitado para vía-zone es capaz de reconocer zonas a través y de enviar tráfico a gateways de zona a través. Los gatekeepers habilitados para zonas de conexión a través de Cisco incluyen un comando de interfaz de línea de comandos (CLI) de zona de conexión a través.

Las zonas de vía generalmente se encuentran en el borde de una red ITSP, y son como un punto de transferencia VoIP, o zona de tándem, donde el tráfico pasa en el camino al destino de la zona remota. Las puertas de enlace de esta zona finalizan las llamadas solicitadas y vuelven a originar el tráfico hasta su destino final. Los gatekeepers Via-zone funcionan como de costumbre para las aplicaciones que no son de IP a IP. Los controles de acceso en zonas de entrada admiten la administración de recursos (por ejemplo, selección de gateway y equilibrio de carga) usando el campo de capacidades en los mensajes RAS H.323 Versión 4.

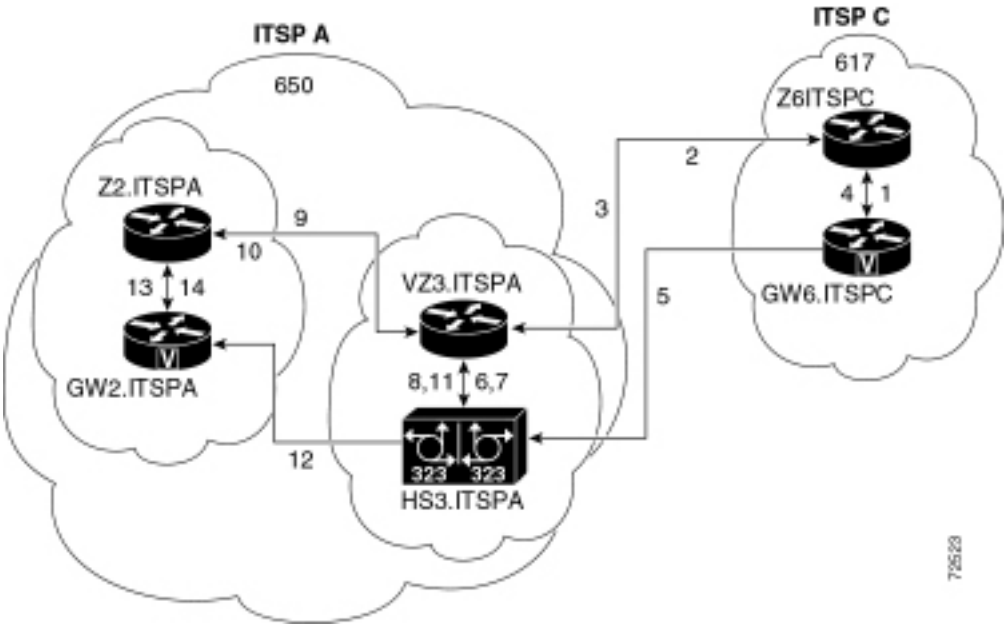
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice la Command Lookup Tool (sólo clientes registrados) .

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Control de acceso de origen (Z6.ITSPC)
- Gatekeeper Via-zone (VZ3.ITSPA)
- Gatekeeper de terminación (Z2.ITSPA)

En este ejemplo, una persona que llama desde el código de área 617 llama a una persona en el código de área 650 y se producen las siguientes acciones:

1. GW6.ITSPC envía un ARQ con el número basado en 650 a Z6.ITSPC.
2. Z6.ITSPC sabe que el prefijo 650 pertenece a VZ3.ITSPA, por lo que Z6.ITSPC envía un LRQ a VZ3.ITSPA.
3. VZ3.ITSPA recibe el LRQ para el número 650. VZ3.ITSPA observa el ID H.323 en el LRQ entrante para encontrar la zona remota. Luego busca una palabra clave via-zone asociada a esa zona remota. Dado que el ID del gatekeeper de zona via es una zona local, asigna la llamada al gateway de IP a IP en la zona de vía y envía de vuelta un LCF que especifica HS3.ITSPA.
4. Z6.ITSPC devuelve un ACF que especifica HS3.ITSPA.
5. GW6.ITSPC envía un mensaje SETUP a HS3.ITSPA para la llamada 650.
6. HS3.ITSPA consulta a VZ3.ITSPA con un ARQ (que contiene answerCall=true) para admitir la llamada entrante.
7. VZ3.ITSPA responde con un ACF para admitir la llamada.
8. HS3.ITSPA tiene un par de marcado que especifica RAS VZ3.ITSPA para el prefijo 650 (o para todos los prefijos), por lo que envía el ARQ (con answerCall configurado en FALSE) a VZ3.ITSPA para el prefijo 650.
9. VZ3.ITSPA ve el prefijo 650 como Z2.ITSPA, así que VZ3.ITSPA envía un LRQ a Z2.ITSPA.
10. Z2.ITSPA ve el prefijo 650 como en su propia zona y devuelve un LCF que apunta a GW2.ITSPA.
11. VZ3.ITSPA devuelve un ACF que especifica GW2.ITSPA.
12. HS3.ITSPA envía un mensaje SETUP a GW2.ITSPA para la llamada 650.
13. GW2.ITSPA envía una respuesta ARQ a Z2.ITSPA.

14. Z2.ITSPA envía un ACF a GW2.ITSPA para answerCall.

Control de acceso de origen (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
```

Gatekeeper Via-zone (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
```

Gatekeeper de terminación (Z2.ITSPA)

```
termgatekeeper# show running-config
 Building configuration...
 .
 .
 .
 gatekeeper
  zone local Z2ITSPA zone2 10.16.10.144
 .
 .
 .
 !
 end
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos

comandos “show” y ver un análisis del resultado de estos comandos.

Para verificar la configuración del gatekeeper, utilice el comando **show running config | comando de inicio del gatekeeper**:

```
 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
```

También puede utilizar el comando **show gatekeeper zone status** para verificar la configuración del gatekeeper:

```
           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
```

Ingrese el comando **show gatekeeper status** para ver los umbrales de capacidad de llamada:

```
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
```

Ingrese el comando **show gatekeeper performance stats** para ver la información de RAS, incluidas las estadísticas vía-zone:

```
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
```

En la tabla siguiente se describen los campos significativos de la zona a través de RAS que se muestran en la visualización.

Campo	Descripción
inLRQ	Asociado a la palabra clave invia. Si el invia es una zona local, este contador identifica el número de LRQs terminadas por el gatekeeper de invia local.
infwdLRQ	Asociado a la palabra clave invia. Si el invia es una zona remota, este contador identifica el número de LRQ que se reenviaron al gatekeeper de invia remoto.
inerrLRQ	Asociado a la palabra clave invia. Número de veces que no se pudo procesar la cola de espera porque no se pudo encontrar la ID de gatekeeper de invia. Por lo general, debido a un nombre de gatekeeper mal escrito.
outLRQ	Asociado a la palabra clave outvia. Si la salida es una zona local, este contador identifica el número de LRQs terminados por el gatekeeper de salida local. Este contador se aplica solamente en configuraciones donde no se especifica ningún gatekeeper de invia.
outfwdLRQ	Asociado a la palabra clave outvia. Si la salida es una zona remota, este contador identifica el número de LRQ que se reenviaron al gatekeeper de salida remoto. Este contador se aplica solamente en configuraciones donde no se especifica ningún gatekeeper de invia.
OUTERRLR	Asociado a la palabra clave outvia. Número de veces que no se pudo procesar el LRQ porque

Q	no se pudo encontrar el ID de gatekeeper saliente. Por lo general, debido a un nombre de gatekeeper mal escrito. Este contador se aplica solamente en configuraciones donde no se especifica ningún gatekeeper de invia.
outARQ	Asociado a la palabra clave outvia. Identifica el número de ARQs de origen manejadas por el gatekeeper local si la salida es esa zona local.
outfwdARQ	Asociado a la palabra clave outvia. Si el gatekeeper de salida es una zona remota, este número identifica el número de ARQ de origen recibidos por este gatekeeper que resultó en que los LRQs se enviaran al gatekeeper de salida.
outerrARQ	Asociado a la palabra clave outvia. Número de veces que no se pudo procesar el ARQ de origen porque no se pudo encontrar el ID de gatekeeper de salida. Por lo general, debido a un nombre de gatekeeper mal escrito.

Ingrese el comando **show gatekeeper circuit** para ver información sobre las llamadas en curso:

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

Nota: La palabra "llamadas" se refiere a los tramos de llamada en algunos comandos y resultados.

Ingrese el comando **show gatekeeper endpoint** para ver información sobre registros de terminales:

```
          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

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Procedimiento de Troubleshooting

A continuación, encontrará información relevante para resolver problemas en esta configuración. Para obtener información adicional sobre la resolución de problemas, vea Cisco Multiservice IP-to-IP Gateway. Siga estas instrucciones para resolver problemas de su configuración.

Los procedimientos para la resolución de problemas de un IPIPGW son similares a los de troubleshooting de un gateway TDM-to-IP H.323. En general, los esfuerzos de resolución de problemas deben continuar de la siguiente manera:

1. Aislar y reproducir el escenario que falla.
2. Recopile información relevante de los comandos **debug** y **show**, archivos de configuración y analizadores de protocolo.
3. Identifique la primera indicación de falla en los seguimientos de protocolo o en la salida de depuración interna.
4. Busque la causa en los archivos de configuración.

Si se sospecha que la zona vía es el origen de una falla de llamada, aísle el problema a un IPGW o gatekeeper identificando la subfunción afectada y concéntrese en los comandos show y debug relacionados con esa subfunción.

Antes de poder comenzar la resolución de problemas, primero debe aislar el problema a una puerta de enlace o a un control de acceso. Los gateways y los gatekeepers son responsables de las siguientes tareas:

Tareas de la puerta de enlace

- Gestión de flujo de medios e integridad de la ruta de voz
- relé DTMF
- Fax relay y passthrough.
- Traducción de dígitos y procesamiento de llamadas
- Dial-peers y filtrado de códecs
- Gestión de ID de operador
- Facturación basada en gateway

Tareas del gatekeeper

- Selección de gateway y equilibrio de carga
- Routing de llamada (selección de zona)
- Facturación basada en el control de acceso
- Control de admisión de llamadas, seguridad y ancho de banda
- Aplicación de las capacidades de llamada

Comandos para resolución de problemas

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Nota: Antes de ejecutar **comandos debug**, consulte Información Importante sobre Comandos Debug.

Comandos de depuración de la puerta de enlace

- **debug voip ipipgw**: Este comando muestra información relacionada con el manejo de llamadas de IP a IP
- **debug h225 asnl**: Este comando muestra el contenido real de la parte asn1 de los mensajes H.225 y los eventos asociados.
- **debug h225 events**: Este comando muestra el contenido real de la parte asn1 de los

mensajes H.225 y los eventos asociados.
- **debug h245 asn1**: Este comando muestra el contenido real de la parte asn1 de los mensajes H.245 y los eventos asociados.
- **debug h245 events**: Este comando muestra el contenido real de la parte asn1 de los mensajes H.245 y los eventos asociados.
- **debug cch323 all**: cuando **debug cch323** se utiliza con las palabras clave **h225**, **h245** o **ras, el resultado de la depuración rastrea las transiciones de estado de las máquinas de estado asociadas según los eventos procesados.**
- **debug voip ccapi inout**: Este comando rastrea la trayectoria de ejecución a través de la API de control de llamadas, que sirve como interfaz entre la aplicación de sesión de llamada y el software específico de la red subyacente.
- **debug voice ccapi error** —Este comando rastrea los registros de errores en la API de control de llamadas. Los registros de errores se generan durante el procesamiento normal de llamadas cuando no hay recursos suficientes o cuando hay problemas en el código específico de la red subyacente, la aplicación de sesión de llamada más alta o la API de control de llamadas en sí.

Comandos de depuración del gatekeeper

- **debug h225 asn1**: Este comando muestra el contenido real de la parte asn1 de los mensajes H.225 RAS y los eventos asociados.
- **debug h225 events**: Este comando muestra el contenido real de la parte asn1 de los mensajes H.225 RAS y los eventos asociados.
- **debug gatekeeper main 10** Este comando rastrea las principales funciones del gatekeeper, tales como el procesamiento de LRQ, la selección de gateway, el procesamiento de solicitudes de admisión, la coincidencia de prefijos y las capacidades de llamadas.
- **debug gatekeeper zone 10**: Este comando rastrea las funciones orientadas a la zona del gatekeeper.
- **debug gatekeeper call 10**: este comando rastrea las funciones orientadas a llamadas del gatekeeper, como el seguimiento de las referencias de llamadas.
- **debug gatekeeper gup asn1**: Este comando muestra el contenido real de la parte asn1 de los mensajes del protocolo de actualización del gatekeeper y los eventos asociados para la comunicación entre los gatekeepers en un agrupamiento.
- **debug gatekeeper gup events**: Este comando muestra el contenido real de la parte asn1 de los mensajes del protocolo de actualización del gatekeeper y los eventos asociados para la comunicación entre los gatekeepers en un cluster.
- **debug ras**: Este comando muestra los tipos y el direccionamiento de los mensajes RAS enviados y recibidos.

Comandos show de la puerta de enlace

- **show h323 gateway h225**: Este comando mantiene el recuento de los mensajes y eventos H.225.
- **show h323 gateway ras**: Este comando mantiene los recuentos de mensajes RAS enviados y recibidos.
- **show h323 gateway cause**: Este comando muestra los recuentos de códigos de causa recibidos de gateways conectados.
- **show call active voice [brief]**—Estos comandos agregan información sobre las llamadas activas y borradas.
- **show crm**: Este comando muestra los recuentos de capacidad de llamada asociados con los

circuitos IP en el IPGW.
- **show processes cpu**: este comando muestra estadísticas detalladas de utilización de CPU (uso de CPU por proceso).
- **show gateway**: este comando muestra el estado actual de la gateway.

Comandos show del gatekeeper

- **show/clear gatekeeper performance stats**: Este comando muestra las estadísticas del gatekeeper asociadas con el procesamiento de llamadas.
- **show gatekeeper zone status**: este comando enumera información sobre las zonas locales y remotas conocidas por el gatekeeper.
- **show gatekeeper endpoint**: Este comando enumera información clave sobre los extremos registrados al gatekeeper, incluidos los IPGW.
- **show gatekeeper circuit**: este comando combina información sobre el uso del circuito a través de múltiples gateways.
- **show gatekeeper calls**: este comando enumera información clave sobre las llamadas que se manejan en la zona local.

Información Relacionada

- Soporte de tecnología de voz
- Soporte de Productos de Voice and Unified Communications
- Troubleshooting de Cisco IP Telephony
- Soporte Técnico - Cisco Systems