Réseau distant à local avec la fonction de passerelle Cisco multiservice IP à IP

Contenu

Introduction

Ce document fournit un exemple de configuration pour un réseau distant à local à l'aide de la fonctionnalité de passerelle IP-to-IP multiservice (IPGW) de Cisco. La fonction IPIPGW fournit un mécanisme permettant d'activer les appels VoIP (Voice over IP) H.323 d'un réseau IP à un autre.

Conditions préalables

Conditions requises

Avant d'essayer cette configuration, assurez-vous de respecter les conditions suivantes :

- Effectuez la configuration de base de la passerelle H.323. Pour obtenir des instructions détaillées, reportez-vous au Guide de configuration de Cisco IOS H.323, Bibliothèque de configuration vocale Cisco IOS, version 12.3.
- Effectuez la configuration de base du contrôleur d'accès H.323. Pour obtenir des instructions détaillées, reportez-vous au Guide de configuration de Cisco IOS H.323, Bibliothèque de configuration vocale Cisco IOS, version 12.3.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Trois routeurs de garde-barrière Cisco H.323 (Cisco 2610, Cisco 2611, Cisco 2612, Cisco 2613, Cisco 2620, Cisco 2621, Cisco 2650, Cisco 2651, Cisco 2691, Cisco 2 610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 3620, Cisco 3649, Cisco 3660, Cisco 3725, 3745, Cisco 7200 ou Cisco 7400) avec le logiciel Cisco IOS version 12.3(4)T ou ultérieure.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Informations générales

La fonctionnalité IPGW multiservice de Cisco introduit le gatekeeper via des zones. Via-zone est un terme Cisco désignant une zone qui contient des passerelles IP à IP et des contrôleurs d'accès via-zone. Un contrôleur d'accès via-zone est capable de reconnaître les zones via et d'envoyer le trafic aux passerelles via-zone. Les contrôleurs d'accès via-zone Cisco incluent une commande d'interface de ligne de commande via-zone.

Les zones de communication vocale sont généralement situées à la périphérie d'un réseau ITSP et sont comme un point de transfert VoIP, ou zone en tandem, où le trafic passe sur le chemin de la destination de la zone distante. Les passerelles de cette zone mettent fin aux appels demandés et redirigent le trafic vers sa destination finale. Les contrôleurs d'accès de zone intermédiaire fonctionnent normalement pour les applications non IP vers IP. Les contrôleurs d'accès dans les zones via prennent en charge la gestion des ressources (par exemple, la sélection des passerelles et l'équilibrage de charge) à l'aide du champ Capacités des messages RAS H.323 Version 4.

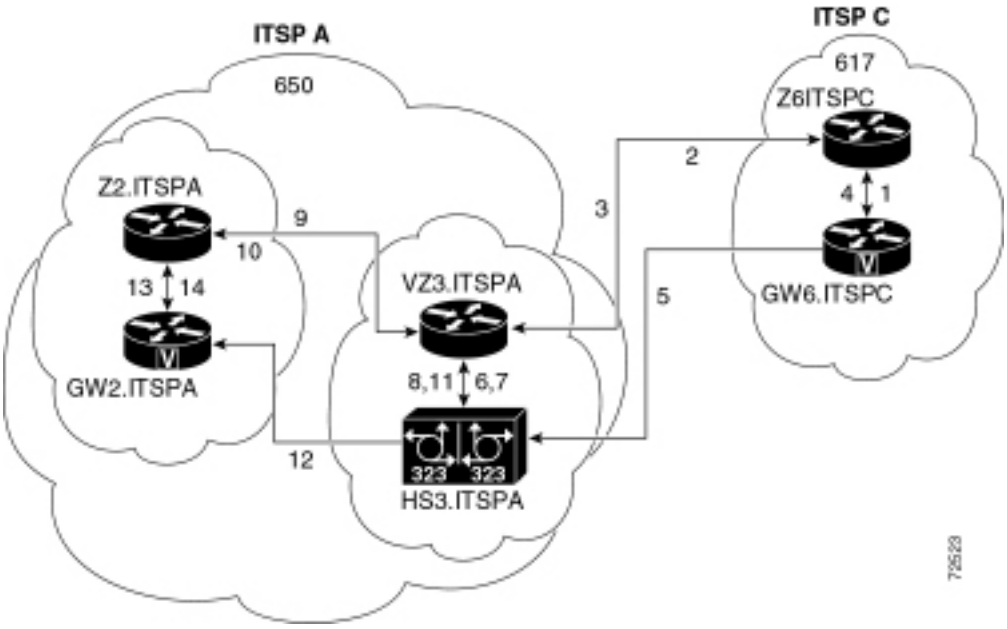
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez l'outil de recherche de commandes (clients inscrits seulement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

- Contrôleur d'accès d'origine (Z6.ITSPC)
- Contrôleur d'accès via zone (VZ3.ITSPA)
- Terminaison du contrôleur d'accès (Z2.ITSPA)

Dans cet exemple, un appelant de l'indicatif régional 617 appelle une personne de l'indicatif régional 650 et les actions suivantes se produisent :

1. GW6.ITSPC envoie un ARQ avec le numéro basé sur 650 à Z6.ITSPC.
2. Z6.ITSPC sait que le préfixe 650 appartient à VZ3.ITSPA, donc Z6.ITSPC envoie un LRQ à VZ3.ITSPA.
3. Le LRQ du numéro 650 est reçu par VZ3.ITSPA. VZ3.ITSPA examine l'ID H.323 dans le LRQ entrant pour trouver la zone distante. Il recherche ensuite un mot clé via-zone associé à cette zone distante. Comme l'ID du contrôleur d'accès via-zone est une zone locale, il alloue l'appel à la passerelle IP-to-IP dans la zone via et renvoie un LCF spécifiant HS3.ITSPA.
4. Z6.ITSPC renvoie une ACF spécifiant HS3.ITSPA.
5. GW6.ITSPC envoie un message SETUP à HS3.ITSPA pour l'appel 650.
6. HS3.ITSPA consulte VZ3.ITSPA avec un ARQ (contenant responseCall=true) pour autoriser l'appel entrant.
7. VZ3.ITSPA répond avec un ACF pour admettre l'appel.
8. HS3.ITSPA a un terminal de numérotation dial-peer spécifiant RAS VZ3.ITSPA pour le préfixe 650 (ou pour tous les préfixes), il envoie donc l'ARQ (avec la valeur FALSE pour AnswerCall) à VZ3.ITSPA pour le préfixe 650.
9. VZ3.ITSPA voit le préfixe 650 comme Z2.ITSPA, de sorte que VZ3.ITSPA envoie un LRQ à Z2.ITSPA.
10. Z2.ITSPA voit le préfixe 650 comme dans sa propre zone et retourne un LCF pointant vers GW2.ITSPA.
11. VZ3.ITSPA retourne un ACF spécifiant GW2.ITSPA.
12. HS3.ITSPA envoie un message SETUP à GW2.ITSPA pour l'appel 650.
13. GW2.ITSPA envoie un appel de réponse ARQ à Z2.ITSPA.

14. Z2.ITSPA envoie un ACF à GW2.ITSPA pour AnswCall.

Contrôleur d'accès d'origine (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
```

Contrôleur d'accès 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
```

Terminaison du contrôleur d'accès (Z2.ITSPA)

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

Vérification

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients

enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Pour vérifier la configuration du contrôleur d'accès, utilisez la commande **show running config | begin gatekeeper**, commande :

```
 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
```

Vous pouvez également utiliser la commande **show gatekeeper zone status** pour vérifier la configuration du 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
```

Entrez la commande **show gatekeeper status** pour afficher les seuils de capacité d'appel :

```
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
```

Entrez la commande **show gatekeeper performance stats** pour afficher les informations RAS, y compris les statistiques via-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
```

Le tableau suivant décrit les champs RAS via zone significatifs affichés dans l'affichage.

Champ	Description
inLRQ	Associé au mot clé invia. Si l'invia est une zone locale, ce compteur identifie le nombre de LRQ terminés par le contrôleur d'accès invia local.
infwdLRQ	Associé au mot clé invia. Si l'entrée est une zone distante, ce compteur identifie le nombre de LRQ qui ont été transférés au contrôleur d'accès d'entrée distant.
InterrLRQ	Associé au mot clé invia. Nombre de fois où le LRQ n'a pas pu être traité, car l'ID du contrôleur d'accès invia est introuvable. Généralement le résultat d'un nom de garde-porte mal épelé.
outLRQ	Associé au mot clé outvia. Si la sortie est une zone locale, ce compteur identifie le nombre de LRQ terminés par le contrôleur d'accès local de sortie. Ce compteur s'applique seulement dans des configurations où aucun contrôleur d'accès n'est spécifié.
outfwdLRQ	Associé au mot clé outvia. Si la sortie est une zone distante, ce compteur identifie le nombre de LRQ qui ont été transférés au contrôleur d'accès sortant distant. Ce compteur s'applique seulement dans des configurations où aucun contrôleur d'accès n'est spécifié.
RouterLRQ	Associé au mot clé outvia. Nombre de fois où le LRQ n'a pas pu être traité, car l'ID du contrôleur d'accès sortant est introuvable. Généralement le résultat d'un nom de garde-porte mal épelé. Ce compteur s'applique seulement dans des

	configurations où aucun contrôleur d'accès n'est spécifié.
outARQ	Associé au mot clé outvia. Identifie le nombre d'ARQ d'origine traitées par le contrôleur d'accès local si la sortie est cette zone locale.
outfwdARQ	Associé au mot clé outvia. Si le contrôleur d'accès sortant est une zone distante, ce numéro identifie le nombre d'ARQ d'origine reçues par ce contrôleur d'accès qui ont abouti à l'envoi de LRQ au contrôleur d'accès sortant.
ARQ outerr	Associé au mot clé outvia. Nombre de fois où l'ARQ d'origine n'a pas pu être traitée, car l'ID du contrôleur d'accès sortant est introuvable. Généralement le résultat d'un nom de garde-porte mal épelé.

Entrez la commande **show gatekeeper circuit** pour afficher les informations sur les appels en cours :

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

Remarque : Le mot “ appels ” fait référence aux branches d'appel dans certaines commandes et sorties.

Entrez la commande **show gatekeeper endpoint** pour afficher les informations sur les enregistrements de points d'extrémité :

```
           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
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Procédure de dépannage

Voici les informations de dépannage concernant cette configuration. Pour plus d'informations sur le dépannage, consultez Passerelle IP à IP multiservice Cisco. Suivez les instructions ci-dessous pour dépanner votre configuration.

Les procédures de dépannage d'un IPGW sont similaires à celles d'une passerelle TDM-IP H.323. En règle générale, vos efforts de dépannage doivent se dérouler comme suit :

1. Isolez et reproduisez le scénario défaillant.
2. Recueillez les informations pertinentes à partir des commandes **debug** et **show**, des fichiers de configuration et des analyseurs de protocole.
3. Identifiez la première indication de défaillance dans les traces de protocole ou la sortie de débogage interne.
4. Recherchez la cause dans les fichiers de configuration.

Si la zone via est suspectée d'être la source d'un échec d'appel, isolez le problème sur un IPGW ou un contrôleur d'accès en identifiant la sous-fonction affectée et en vous concentrant sur les commandes show et debug liées à cette sous-fonction.

Avant de commencer le dépannage, vous devez d'abord isoler le problème à une passerelle ou à un contrôleur d'accès. Les passerelles et les contrôleurs d'accès sont chargés des tâches suivantes :

Tâches de passerelle

- Gestion des flux multimédias et intégrité des chemins de voix
- Relais DTMF
- Relais et transfert de télécopie.
- Traduction de chiffres et traitement des appels
- Filtrage des terminaux de numérotation dial-peer et des codecs
- Gestion des ID de transporteur
- Facturation basée sur la passerelle

Tâches du contrôleur d'accès

- Sélection de la passerelle et équilibrage de charge
- Routage des appels (sélection de zone)
- Facturation basée sur un contrôleur d'accès
- Contrôle de l'admission des appels, de la sécurité et de la bande passante
- Application des capacités d'appel

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Note : Avant d'émettre des commandes **debug**, consultez Informations importantes sur les commandes de débogage.

Commandes de débogage de passerelle

- **debug voip ipipgw** - Cette commande affiche des informations relatives au traitement des appels IP à IP.
- **debug h225 asnl** - Cette commande affiche le contenu réel de la partie asn1 des messages H.225 et des événements associés.
- **debug h225 events** - Cette commande affiche le contenu réel de la partie asn1 des messages H.225 et des événements associés.
- **debug h245 asn1** : cette commande affiche le contenu réel de la partie asn1 des messages H.245 et des événements associés.

- **debug h245 events** - Cette commande affiche le contenu réel de la partie asn1 des messages H.245 et des événements associés.
- **debug cch323 all** - Lorsque **debug cch323** est utilisé avec **h225**, **h245** ou **ras** mots clés, la sortie de débogage trace les transitions d'état des machines d'état associées en fonction des événements traités.
- **debug voip ccapi inout** - Cette commande trace le chemin d'exécution via l'API de contrôle d'appel, qui sert d'interface entre l'application de session d'appel et le logiciel spécifique au réseau sous-jacent.
- **debug voice ccapi error** - Cette commande trace les journaux d'erreurs dans l'API de contrôle d'appel. Les journaux d'erreurs sont générés lors du traitement normal des appels lorsque les ressources sont insuffisantes ou lorsqu'il y a des problèmes dans le code spécifique au réseau sous-jacent, l'application de session d'appel supérieure ou l'API de contrôle d'appel elle-même.

Commandes de débogage du contrôleur d'accès

- **debug h225 asn1** - Cette commande affiche le contenu réel de la partie asn1 des messages H.225 RAS et des événements associés.
- **debug h225 events** - Cette commande affiche le contenu réel de la partie asn1 des messages H.225 RAS et des événements associés.
- **debug gatekeeper main 10** Cette commande trace les principales fonctions de gatekeeper, telles que le traitement LRQ, la sélection de passerelle, le traitement des demandes d'admission, la correspondance de préfixe et les capacités d'appel.
- **debug gatekeeper zone 10** : cette commande trace les fonctions orientées zone du gatekeeper.
- **debug gatekeeper call 10** - Cette commande trace les fonctions orientées appel gatekeeper, telles que le suivi des références d'appels.
- **debug gatekeeper gup asn1** - Cette commande affiche le contenu réel de la partie asn1 des messages de protocole de mise à jour de gatekeeper et les événements associés pour la communication entre les contrôleurs d'accès dans un cluster.
- **debug gatekeeper gup events** - Cette commande affiche le contenu réel de la partie asn1 des messages de protocole de mise à jour de gatekeeper et les événements associés pour la communication entre les contrôleurs d'accès dans un cluster.
- **debug ras** : cette commande affiche les types et l'adressage des messages RAS envoyés et reçus.

Commandes Gateway show

- **show h323 gateway h225** - Cette commande conserve le nombre de messages et d'événements H.225.
- **show h323 gateway ras** : cette commande gère le nombre de messages RAS envoyés et reçus.
- **show h323 gateway cause** - Cette commande affiche le nombre de codes de cause reçus des passerelles connectées.
- **show call active voice [brief]** : ces commandes regroupent les informations sur les appels actifs et supprimés.
- **show crm** : cette commande affiche le nombre de capacité d'appel associé aux circuits IP sur l'IPIPGW.
- **show processes cpu** - Cette commande affiche des statistiques détaillées sur l'utilisation du CPU (utilisation du CPU par processus).

- **show gateway** - Cette commande affiche l'état actuel de la passerelle.

Commandes show du contrôleur d'accès

- **show/clear gatekeeper performance stats** : cette commande affiche les statistiques de gatekeeper associées au traitement des appels.
- **show gatekeeper zone status** : cette commande répertorie les informations relatives aux zones locales et distantes connues du gatekeeper.
- **show gatekeeper endpoint** - Cette commande répertorie les informations clés relatives aux terminaux enregistrés auprès du gatekeeper, y compris les IPGW.
- **show gatekeeper circuit** - Cette commande combine des informations sur l'utilisation des circuits sur plusieurs passerelles.
- **show gatekeeper Calls** - Cette commande répertorie les informations clés sur les appels traités dans la zone locale.

Informations connexes

- Assistance technique concernant la technologie vocale
- Assistance concernant les produits vocaux et de communications unifiées
- Dépannage des problèmes de téléphonie IP Cisco
- Support technique - Cisco Systems