

# Rete da locale a remota usando la funzionalità Cisco Multiservice IP-to-IP Gateway

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Procedura di risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene fornita una configurazione di esempio per una rete locale-remota usando la funzionalità Cisco Multiservice IP-to-IP Gateway (IPIPGW). La funzione IPIPGW fornisce un meccanismo per abilitare le chiamate H.323 Voice over IP (VoIP) da una rete IP all'altra.

## Prerequisiti

### Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Eseguire una configurazione di base del gateway H.323. Per istruzioni dettagliate, consultare la [guida alla configurazione di Cisco IOS H.323](#), Cisco IOS Voice Configuration Library, versione 12.3.
- Eseguire una configurazione di base H.323 gatekeeper. Per istruzioni dettagliate, consultare la [guida alla configurazione di Cisco IOS H.323](#), Cisco IOS Voice Configuration Library, versione 12.3.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Tre router Gatekeeper Cisco H.323 (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 266 1XM, Cisco 2650XM, Cisco 2651XM, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 3725, Cisco 3745, Cisco serie 7200 o Cisco serie 7400) con software Cisco IOS versione 12.2(13)T o successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

## Premesse

La funzione Cisco Multiservice IPIGW introduce il gatekeeper nelle zone di accesso. Via-zone è un termine Cisco che indica una zona contenente gateway IP-to-IP e gatekeeper abilitati per via-zona. Un gatekeeper abilitato per la zona di accesso può riconoscere le zone di accesso e inviare il traffico ai gateway della zona di accesso. I gatekeeper Cisco abilitati per zona includono un comando via-zone command-line interface (CLI).

Le zone di trasmissione si trovano in genere ai margini di una rete ITSP (Internet Telephony Service Provider) e sono simili a punti di trasferimento VoIP, o a zone tandem, nelle quali il traffico attraversa il percorso verso la destinazione della zona remota. I gateway di questa zona terminano le chiamate richieste e rigenerano il traffico verso la destinazione finale. I gatekeeper via-zona funzionano come al solito per applicazioni non IP-to-IP. I gatekeeper nelle zone di trasmissione supportano la gestione delle risorse (ad esempio, la selezione del gateway e il bilanciamento del carico) utilizzando il campo capabilities nei messaggi RAS H.323 versione 4.

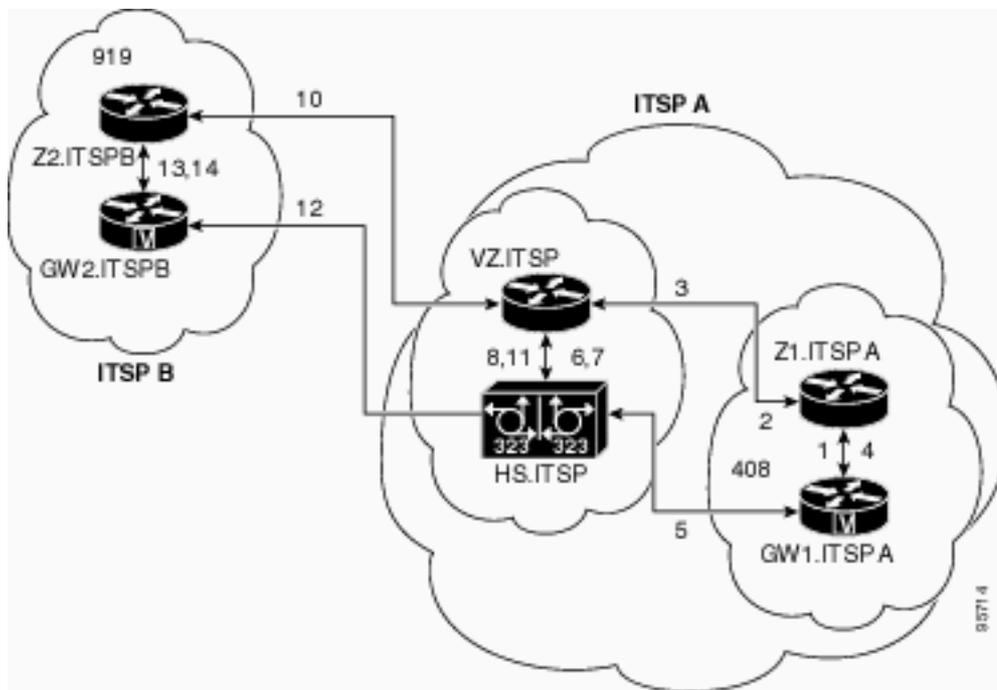
## Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

**Nota:** per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

## Esempio di rete

Nel documento viene usata questa impostazione di rete:



## Configurazioni

Nel documento vengono usate queste configurazioni:

- [Gatekeeper di origine \(Z1.ITSPA\)](#)
- [Via-zone Gatekeeper \(VZ.ITSP\)](#)
- [Gatekeeper terminante \(Z2.ITSPB\)](#)

In questo esempio, un chiamante con prefisso 408 chiama una parte con prefisso 919 e si verificano le seguenti azioni:

1. GW1.ITSPA invia a Z1.ITSPA un messaggio di richiesta di ammissione (ARQ) con il numero basato su 919.
2. Z1.ITSPA risolve 919 in VZ.ITSP e invia un messaggio di richiesta di posizione (LRQ) a VZ.ITSP.
3. L'LRQ per il numero 919 dalla zona Z1ITSPA è stato ricevuto da VZ.ITSP. VZ.ITSP controlla la configurazione remota della zona per Z1ITSPA e scopre che la sua zona VZITSP è configurata come zona "invia". Quindi invia un messaggio LCF (Location Confirm) a Z1.ITSPA e specifica HS.ITSP come gateway di destinazione per la chiamata 919.
4. Z1.ITSPA invia un messaggio di conferma dell'ammissione (ACF) a GW1.ITSPA e specifica HS.ITSP come gateway di destinazione.
5. GW1.ITSPA invia un messaggio SETUP a HS.ITSP per la chiamata 919.
6. HS.ITSP consulta VZ.ITSP con un ARQ (contenente answerCall=true) per ammettere la chiamata in arrivo.
7. VZ.ITSP risponde con un ACF per ammettere la chiamata.
8. HS.ITSP dispone di un peer di composizione che specifica RAS VZ.ITSP per il prefisso 919 (o per tutti i prefissi), quindi invia un ARQ (con answerCall impostato su FALSE) a VZ.ITSP per il prefisso 919.
9. VZ.ITSP gatekeeper identifica che la zona Z2ITSPB gestisce il prefisso "919" cercando la tabella dei prefissi della zona. Utilizza quindi la configurazione remota della zona e sa che la propria zona locale VZITSP è configurata come zona "in uscita". Quindi, invia il modulo LRQ al gatekeeper Z2.ITSPB anziché inviare un modulo LRQ a un altro gatekeeper IP-to-IP.

10. Z2.ITSPB vede il prefisso 919 come nella propria zona e restituisce un LCF che punta a GW2.ITSPB.
11. VZ.ITSP restituisce un ACF che specifica GW2.ITSPB come gateway di destinazione per HS.ITSP.
12. HS.ITSP invia un messaggio SETUP a GW2.ITSPB per la chiamata 919.
13. GW2.ITSPB invia un messaggio ARQ (contenente answerCall=true) a Z2.ITSPB.
14. Z2.ITSPB invia un ACF per answerCall.
15. La chiamata H.323 tra HS.ITSP e GW2.ITSPB viene connessa. La chiamata H.323 tra GW1.ITSPA e HS.ITSP viene connessa.

#### Gatekeeper di origine (Z1.ITSPA)

```
origgatekeeper#show running-config
Building configuration...
.
.
.
gatekeeper
 zone local Z1ITSPA cisco 10.16.8.158
 zone remote VZITSP cisco 10.16.10.139
 zone remote Z2ITSPB china 10.16.8.139 1719
 zone prefix VZITSP 919*
.
.
.
!
end
```

#### Via-zone Gatekeeper (VZ.ITSP)

```
vzgatekeeper#show running-config
Building configuration...
.
.
.
gatekeeper
 zone local VZITSP cisco 10.16.10.139
 zone remote Z1ITSPA cisco 10.16.8.158 invia VZITSP
 zone remote Z2ITSPB china 10.16.8.144 1719 outvia
VZITSP
 zone prefix Z2ITSPB 919*
.
.
.
!
end
```

#### Gatekeeper terminante (Z2.ITSPB)

```
termgatekeeper#show running-config
Building configuration...
.
.
.
gatekeeper
 zone local Z2ITSPB china 10.16.8.144
.
.
.
```

```
!  
end
```

## Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

**Nota:** questi output del comando show sono stati ottenuti dal gatekeeper VZ.ITSP.

Eseguire il comando **show running config | avviare il comando gatekeeper** per verificare la configurazione gatekeeper:

```
gatekeeper  
zone local VZITSP cisco 10.16.10.139  
zone remote Z1ITSPA cisco 10.16.8.158 invia VZITSP  
zone remote Z2ITSPB china 10.16.8.144 1719 outvia VZITSP  
zone prefix Z2ITSPB 919*  
no shutdown
```

È possibile anche usare il comando **show gatekeeper zone status** per verificare la configurazione del gatekeeper:

```
GATEKEEPER ZONES  
=====
```

GK name	Domain Name	RAS Address	PORT	FLAGS
VZITSP	cisco	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:VZ.ITSP, outvia:VZ.ITSP  
Z2.ITSPB cisco 10.16.8.144 1719 RS  
VIAZONE INFORMATION :  
invia:VZ.ITSP, outvia:VZ.ITSP
```

Immettere il comando **show gatekeeper status** per visualizzare le soglie della capacità di chiamata:

```
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
```

Immettere il comando **show gatekeeper performance stats** per visualizzare le informazioni RAS, incluse le statistiche della zona di accesso:

```
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
```

Sul display sono visualizzati i seguenti campi significativi via-zone RAS:

- **inLRQ:** — Associato alla parola chiave `invia`. Se l'invio è una zona locale, questo contatore identifica il numero di LRQ terminati dal gatekeeper dell'invio locale.
- **infwdLRQ:** associato alla parola chiave `invia`. Se l'invio è una zona remota, questo contatore identifica il numero di LRQ inoltrati al gatekeeper dell'invio remoto.
- **interLRQ** - Associato alla parola chiave `invia`. Numero di volte in cui non è stato possibile elaborare l'LRQ perché non è stato possibile trovare l'ID Gatekeeper dell'invio. Generalmente causato da un nome di gatekeeper errato.
- **outLRQ** - Associato alla parola chiave `outvia`. Se l'uscita è una zona locale, questo contatore identifica il numero di LRQ terminati dal gatekeeper esterno locale. Questo contatore si applica solo nelle configurazioni in cui non è specificato alcun Gatekeeper di invio.
- **outfwdLRQ** - Associato alla parola chiave `outvia`. Se l'outvia è una zona remota, questo contatore identifica il numero di LRQ inoltrati al gatekeeper di uscita remoto. Questo contatore si applica solo nelle configurazioni in cui non è specificato alcun Gatekeeper di invio.
- **outerrLRQ** - Associato alla parola chiave `outvia`. Numero di volte in cui l'LRQ non è stato elaborato perché non è stato possibile trovare l'ID gatekeeper in uscita. Generalmente causato da un nome di gatekeeper errato. Questo contatore si applica solo nelle configurazioni in cui non è specificato alcun Gatekeeper di invio.
- **outARQ** - Associato alla parola chiave `outvia`. Identifica il numero di ARQ di origine gestiti dal gatekeeper locale se l'uscita è la zona locale.
- **outfwdARQ** - Associato alla parola chiave `outvia`. Se il gatekeeper esterno è una zona remota, questo numero identifica il numero di ARQ originari ricevuti da questo gatekeeper, che hanno causato l'invio di LRQ al gatekeeper esterno.
- **outerrARQ** - Associato alla parola chiave `outvia`. Numero di volte in cui non è stato possibile elaborare l'ARQ di origine perché non è stato possibile trovare l'ID gatekeeper in uscita.

Questo problema è in genere causato da un nome di gatekeeper errato.

Immettere il comando **show gatekeeper circuit** per visualizzare le informazioni sulle chiamate in corso:

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

**Nota:** in alcuni comandi e output, il termine "chiamate" si riferisce alle gambe di chiamata.

Immettere il comando **show gatekeeper endpoint** per visualizzare le informazioni sulle registrazioni degli endpoint:

```
GATEKEEPER ENDPOINT REGISTRATION
=====
CallSignalAddr  Port  RASignalAddr  Port  Zone Name      Type      Flags
-----
10.16.10.140    1720  10.16.10.140  50594  vz.itsp        H323-GW
    H323-ID: hs.itsp
    H323 Capacity Max.= 200 Avail.= 198
Total number of active registrations = 1
```

## Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

### Procedura di risoluzione dei problemi

Queste sono informazioni utili per risolvere eventuali problemi con questa configurazione. Completare la procedura seguente per risolvere i problemi relativi alla configurazione.

Le procedure per la risoluzione dei problemi relativi a IPIPGW sono simili a quelle per la risoluzione dei problemi relativi a un gateway H.323 da TDM a IP. In generale, le operazioni di risoluzione dei problemi devono procedere come indicato di seguito:

1. Isolare e riprodurre lo scenario di errore.
2. Raccogliere informazioni importanti dai comandi debug e show, dai file di configurazione e dagli analizzatori di protocollo.
3. Identificare la prima indicazione di errore nelle tracce del protocollo o nell'output del debug interno.
4. Cercare la causa nei file di configurazione.

Se si sospetta che la via-zone sia all'origine di un errore di chiamata, isolare il problema con un IPIPGW o un gatekeeper, identificando la sottofunzione interessata e focalizzando l'attenzione sui comandi show e debug relativi a tale sottofunzione.

Prima di iniziare la risoluzione dei problemi, è necessario isolare il problema in un gateway o in un gatekeeper. I gateway e i gatekeeper sono responsabili delle seguenti attività:

Attività gateway:

- Gestione dei flussi multimediali e integrità del percorso vocale
- Relay DTMF
- Fax Relay and Passthrough
- Traduzione della cifra ed elaborazione delle chiamate
- Peer di composizione e filtro codec
- Gestione ID vettore
- Fatturazione basata su gateway

Attività Gatekeeper:

- Selezione del gateway e bilanciamento del carico
- Routing delle chiamate (selezione zona)
- Fatturazione basata su Gatekeeper
- Controllo dell'ammissione di chiamata, sicurezza e larghezza di banda
- Applicazione delle capacità di chiamata

## [Comandi per la risoluzione dei problemi](#)

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

**Nota:** consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di **debug**.

**Comandi di debug del gateway:**

- **debug voip ipipgw:** questo comando visualizza le informazioni correlate alla gestione delle chiamate IP-to-IP.
- **debug h225 asn1:** questo comando visualizza il contenuto effettivo della parte asn1 dei messaggi H.225 e degli eventi associati.
- **debug h225 events:** questo comando visualizza il contenuto effettivo della parte asn1 dei messaggi H.225 e degli eventi associati.
- **debug h245 asn1:** questo comando visualizza il contenuto effettivo della parte asn1 dei messaggi H.245 e degli eventi associati.

**Comandi di debug Gatekeeper:**

- **debug h225 asn1:** questo comando visualizza il contenuto effettivo della parte asn1 dei messaggi RAS H.225 e degli eventi associati.
- **debug h225 events:** questo comando visualizza il contenuto effettivo della parte asn1 dei messaggi RAS H.225 e degli eventi associati.
- **debug gatekeeper main 10:** questo comando traccia le principali funzioni gatekeeper, ad esempio l'elaborazione LRQ, la selezione del gateway, l'elaborazione delle richieste di ammissione, la corrispondenza dei prefissi e le capacità di chiamata.
- **debug gatekeeper zone 10:** questo comando traccia le funzioni orientate alla zona del gatekeeper.
- **debug gatekeeper call 10:** questo comando traccia le funzioni orientate alle chiamate gatekeeper, ad esempio la traccia dei riferimenti delle chiamate.
- **debug gatekeeper gup asn1:** questo comando visualizza il contenuto effettivo della parte asn1 dei messaggi del protocollo di aggiornamento gatekeeper e gli eventi associati per la

comunicazione tra gatekeeper in un cluster.

- **debug gatekeeper gup events**: questo comando visualizza il contenuto effettivo della parte asn1 dei messaggi del protocollo di aggiornamento gatekeeper e gli eventi associati per la comunicazione tra gatekeeper in un cluster.
- **debug ras**: questo comando visualizza i tipi e gli indirizzi dei messaggi RAS inviati e ricevuti.

#### Comandi show gateway:

- **show h323 gateway h225**: questo comando conserva il conteggio dei messaggi e degli eventi H.225.
- **show h323 gateway ras**: questo comando mantiene il numero di messaggi RAS inviati e ricevuti.
- **show h323 gateway cause**: questo comando visualizza il numero di codici causa ricevuti dai gateway connessi.
- **show call active voice [brief]**: questi comandi aggregano le informazioni sulle chiamate attive e cancellate.
- **show crm**: questo comando mostra i conteggi della capacità di chiamata associati ai circuiti IP sull'interfaccia IPIPGW.
- **show PROCESSES cpu**: questo comando mostra le statistiche dettagliate sull'utilizzo della CPU (utilizzo CPU per processo).
- **show gateway**: questo comando visualizza lo stato corrente del gateway.

#### Comandi show Gatekeeper:

- **show/clear gatekeeper performance stats**: questo comando visualizza le statistiche gatekeeper associate all'elaborazione delle chiamate.
- **show gatekeeper zone status**: questo comando elenca le informazioni sulle zone locali e remote note al gatekeeper.
- **show gatekeeper endpoint**: questo comando elenca le informazioni principali sugli endpoint registrati sul gatekeeper, inclusi gli IPIPGW.
- **show gatekeeper circuit**: questo comando combina le informazioni sull'utilizzo del circuito su più gateway.
- **show gatekeeper call**: questo comando elenca le informazioni principali sulle chiamate gestite nella zona locale.

## [Informazioni correlate](#)

- [Guida alle applicazioni Cisco Multiservice IP-to-IP Gateway](#)
- [Supporto alla tecnologia vocale](#)
- [Supporto ai prodotti voce e Unified Communications](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).