Lokal zu Remote-Netzwerk mithilfe der Cisco Multiservice-Funktion IP-to-IP Gateway

Inhalt

Einleitung

Dieses Dokument enthält eine Beispielkonfiguration für ein lokales zu einem Remote-Netzwerk mithilfe der IPGW-Funktion (Cisco Multiservice IP-to-IP Gateway). Die IPIPGW-Funktion ermöglicht H.323-VoIP-Anrufe von einem IP-Netzwerk in ein anderes.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie diese Konfiguration ausprobieren:

- Durchführen einer grundlegenden H.323-Gateway-Konfiguration Weitere Informationen finden Sie im Cisco IOS H.323 Configuration Guide, Cisco IOS Voice Configuration Library, Release 12.3.
- Durchführen einer grundlegenden H.323-Gatekeeper-Konfiguration Weitere Informationen finden Sie im Cisco IOS H.323 Configuration Guide, Cisco IOS Voice Configuration Library, Release 12.3.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Drei Cisco H.323-Gatekeeper-Router (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 3640, Cisco 3660, Cisco 3725, 3745, Cisco 7200 oder Cisco 7400) mit Cisco IOS Software, Version 12.2(13)T oder höher.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

Die Cisco Multiservice IPIPGW-Funktion führt Gatekeeper-Via-Zonen ein. Via-Zone ist ein Begriff von Cisco für eine Zone, die IP-to-IP-Gateways und Via-Zone-fähige Gatekeeper enthält. Ein für die Via-Zone aktivierter Gatekeeper kann Via-Zonen erkennen und Datenverkehr an Via-Zone Gateways senden. Zu den von Cisco für die via-Zone aktivierten Gatekeepern gehört der Befehl via-zone Command-Line Interface (CLI).

Via-Zonen befinden sich in der Regel am Rand eines Internet Telefony Service Provider (ITSP)-Netzwerks und sind wie ein VoIP-Übertragungspunkt oder eine Tandemzone, an dem der Datenverkehr auf dem Weg zum Remote-Zonenziel weitergeleitet wird. Gateways in dieser Zone beenden angeforderte Anrufe und leiten den Datenverkehr wieder an sein endgültiges Ziel weiter. Via-Zone-Gatekeeper arbeiten wie gewohnt für Nicht-IP-to-IP-Anwendungen. Gatekeepers in Via-Zonen unterstützen das Ressourcenmanagement (z. B. Gateway-Auswahl und Lastenausgleich) mithilfe des Kapazitätsfelds in den H.323 Version 4 RAS-Meldungen.

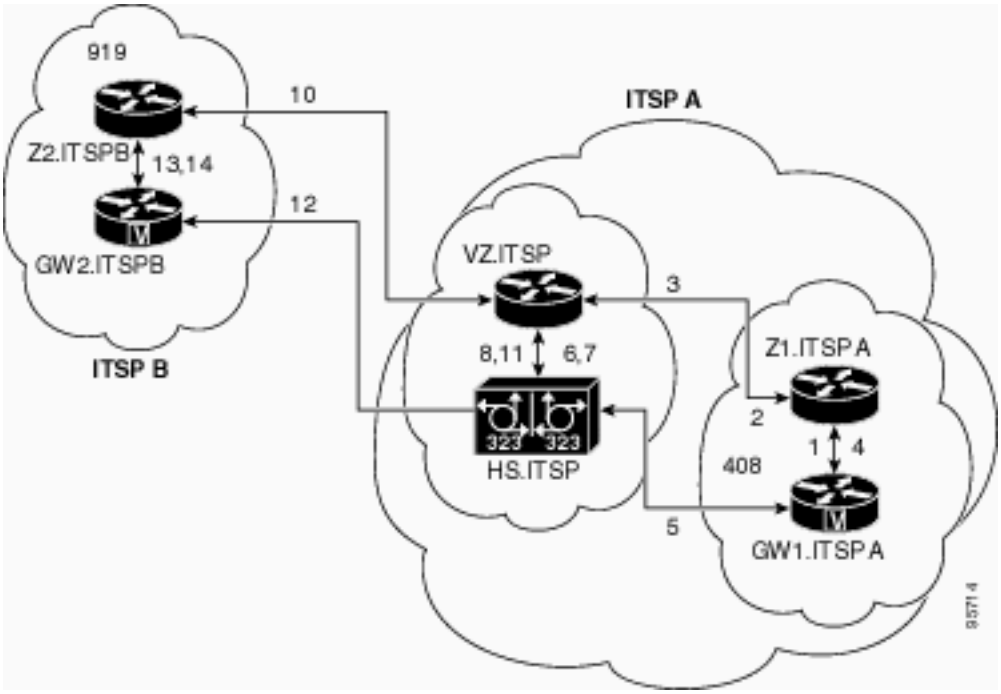
Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Hinweis: Verwenden Sie das Tool für die Suche nach Befehlen (nur für registrierte Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Ursprungs-Gatekeeper (Z1.ITSPA)
- Via-Zone-Gatekeeper (VZ.ITSP)
- Terminierender Gatekeeper (Z2.ITSPB)

In diesem Beispiel ruft ein Anrufer mit der Ortsvorwahl 408 einen Teilnehmer mit der Ortsvorwahl 919 an. Die folgenden Aktionen werden ausgeführt:

1. GW1.ITSPA sendet eine ARQ-Nachricht (Admission Request) mit der 919-basierten Nummer an Z1.ITSPA.
2. Z1.ITSPA löst 919 zu VZ.ITSP auf und sendet eine Location Request (LRQ)-Nachricht an VZ.ITSP.
3. Die LRQ für die 919-Nummer aus der Z1ITSPA-Zone wird von VZ.ITSP empfangen. VZ.ITSP überprüft die Remote-Zonenkonfiguration für Z1ITSPA und stellt fest, dass seine VZITSP-Zone als "Invia"-Zone konfiguriert ist. Anschließend wird eine Location Confirm (LCF)-Nachricht an Z1.ITSPA gesendet, und HS.ITSP wird als Ziel-Gateway für den 919-Anruf angegeben.
4. Z1.ITSPA sendet eine ACF-Nachricht (Admission Confirm) an GW1.ITSPA und gibt HS.ITSP als Ziel-Gateway an.
5. GW1.ITSPA sendet eine SETUP-Nachricht für den 919-Anruf an HS.ITSP.
6. HS.ITSP berät VZ.ITSP mit einem ARQ (mit answerCall=true), um den eingehenden Anruf zuzulassen.
7. VZ.ITSP antwortet mit einer ACF, um den Anruf zuzulassen.
8. HS.ITSP verfügt über einen DFÜ-Peer, der RAS VZ.ITSP für das 919-Präfix (oder für alle Präfixe) angibt, sodass ein ARQ (mit answerCall auf FALSE gesetzt) für das Präfix 919 an VZ.ITSP gesendet wird.
9. Der VZ.ITSP-Gatekeeper identifiziert, dass die Z2ITSPB-Zone das Präfix "919" verarbeitet, indem er in der Zonenpräfixtabelle nachschaut. Anschließend wird die Zone-Remote-Konfiguration verwendet, und es weiß, dass seine eigene lokale Zone VZITSP als "Outvia"-

Zone konfiguriert ist. Anschließend wird der LRQ an den Z2.ITSPB-Gatekeeper gesendet, anstatt einen LRQ an einen anderen IP-to-IP-Gatekeeper zu senden.

10. Z2.ITSPB erkennt das Präfix 919 wie in seiner eigenen Zone und gibt eine LCF zurück, die auf GW2.ITSPB verweist.
11. VZ.ITSP gibt eine ACF zurück, die GW2.ITSPB als Ziel-Gateway für HS.ITSP angibt.
12. HS.ITSP sendet eine SETUP-Nachricht für den 919-Anruf an GW2.ITSPB.
13. GW2.ITSPB sendet einen ARQ (der answerCall=true enthält) an Z2.ITSPB.
14. Z2.ITSPB sendet eine ACF für answerCall.
15. Der H.323-Anruf zwischen HS.ITSP und GW2.ITSPB wird verbunden. Der H.323-Anruf zwischen GW1.ITSPA und HS.ITSP wird verbunden.

Ursprungs-Gatekeeper (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
```

Terminierender Gatekeeper (Z2.ITSPB)

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

```
.
!
end
```

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter-Tool (OIT) (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **show**-Befehlsausgabe anzuzeigen.

Hinweis: Diese Ausgabe des Befehls show wurde vom VZ.ITSP-Gatekeeper bezogen.

Geben Sie die **ausgeführte Konfiguration anzeigen ein. | Begin gatekeeper**-Befehl, um die Gatekeeper-Konfiguration zu überprüfen:

```
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
```

Sie können auch den Befehl **show gatekeeper zone status** verwenden, um die Gatekeeper-Konfiguration zu überprüfen:

```
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
```

Führen Sie den Befehl **show gatekeeper status** aus, um die Anrufkapazitätsgrenzwerte anzuzeigen:

```
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
```

Führen Sie den Befehl **show gatekeeper performance stats** aus, um RAS-Informationen einschließlich Statistiken über die Zone anzuzeigen:

```
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
```

Folgende signifikante RAS-Überzonenfelder werden im Display angezeigt:

- inLRQ: - Dem invia-Schlüsselwort zugeordnet. Wenn die Invia eine lokale Zone ist, gibt dieser Zähler die Anzahl der LRQs an, die vom lokalen Invia-Gatekeeper terminiert werden.
- infwdLRQ: Dem invia-Schlüsselwort zugeordnet. Wenn es sich bei der Invia um eine Remote-Zone handelt, identifiziert dieser Zähler die Anzahl der LRQs, die an den Remote-Invia-Gatekeeper weitergeleitet wurden.
- inerrLRQ: Dem invia-Schlüsselwort zugeordnet. Anzahl der Male, die die LRQ nicht verarbeitet werden konnte, weil die ID des Invia-Gatekeepers nicht gefunden wurde. Wird normalerweise durch einen falsch geschriebenen Gatekeeper-Namen verursacht.
- outLRQ: Dem outvia-Schlüsselwort zugeordnet. Handelt es sich bei dem Outvia um eine lokale Zone, gibt dieser Zähler die Anzahl der vom lokalen Outvia-Gatekeeper terminierten LRQs an. Dieser Zähler gilt nur für Konfigurationen, bei denen kein invia Gatekeeper angegeben ist.
- outfwdLRQ: Dem outvia-Schlüsselwort zugeordnet. Wenn es sich bei dem Outvia um eine Remote-Zone handelt, gibt dieser Zähler die Anzahl der LRQs an, die an den Remote-Outvia-Gatekeeper weitergeleitet wurden. Dieser Zähler gilt nur für Konfigurationen, bei denen kein invia Gatekeeper angegeben ist.
- outerLRQ: Wird dem outvia-Schlüsselwort zugeordnet. Die Anzahl der Fälle, in denen die LRQ nicht verarbeitet werden konnte, weil die ID des externen Gatekeepers nicht gefunden wurde. Wird normalerweise durch einen falsch geschriebenen Gatekeeper-Namen verursacht. Dieser Zähler gilt nur für Konfigurationen, bei denen kein invia Gatekeeper angegeben ist.
- outARQ: Dem outvia-Schlüsselwort zugeordnet. Gibt die Anzahl der vom lokalen Gatekeeper

verarbeiteten ARQs an, wenn es sich bei der Ausgangsverbindung um diese lokale Zone handelt.
- outfwdARQ: Dem outvia-Schlüsselwort zugeordnet. Handelt es sich bei dem Outvia-Gatekeeper um eine Remote-Zone, gibt diese Nummer die Anzahl der von diesem Gatekeeper empfangenen ARQs an, die zum Senden von LRQs an den Outvia-Gatekeeper geführt haben.
- outerARQ: Wird dem outvia-Schlüsselwort zugeordnet. Die Anzahl der Fälle, in denen der ursprüngliche ARQ nicht verarbeitet werden konnte, weil die Ausgangs-Gatekeeper-ID nicht gefunden wurde. Dies wird normalerweise durch einen falsch geschriebenen Gatekeeper-Namen verursacht.

Geben Sie den Befehl **show gatekeeper circuit** (Gatekeeper-Schaltung anzeigen) ein, um Informationen zu laufenden Anrufen anzuzeigen:

```
                    CIRCUIT INFORMATION
                    ===================

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

Hinweis: In einigen Befehlen und Ausgaben bezieht sich das Wort "calls" auf Rufabschnitte.

Geben Sie den Befehl **show gatekeeper endpoint** ein, um Informationen zu Endpunktregistrierungen anzuzeigen:

```
             GATEKEEPER ENDPOINT REGISTRATION
                   ================================
CallSignalAddr  Port  RASSignalAddr   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
```

Fehlerbehebung

Verwenden Sie diesen Abschnitt, um Probleme mit Ihrer Konfiguration zu beheben.

Fehlerbehebungsverfahren

Dies sind Informationen zur Fehlerbehebung, die für diese Konfiguration relevant sind. Führen Sie diese Schritte aus, um Probleme mit Ihrer Konfiguration zu beheben.

Die Verfahren zur Fehlerbehebung bei einem IPGW ähneln der Fehlerbehebung bei einem TDM-to-IP H.323-Gateway. Im Allgemeinen sollten Sie die Fehlerbehebung wie folgt durchführen:

1. Isolieren und reproduzieren Sie das Fehlerszenario.
2. Sammeln relevanter Informationen von Debug- und Anzeigebefehlen, Konfigurationsdateien und Protokollanalysatoren
3. Identifizieren Sie den ersten Hinweis auf einen Fehler in Protokoll-Traces oder der internen Debug-Ausgabe.

4. Suchen Sie in den Konfigurationsdateien nach der Ursache.

Wenn die Via-Zone als Ursache eines Anruffehlers vermutet wird, isolieren Sie das Problem auf ein IPGW oder einen Gatekeeper, indem Sie die betroffene Unterfunktion identifizieren und sich auf Show- und Debug-Befehle für diese Unterfunktion konzentrieren.

Bevor Sie mit der Fehlerbehebung beginnen können, müssen Sie das Problem zunächst auf ein Gateway oder einen Gatekeeper zurückführen. Gateways und Gatekeeper sind für diese Aufgaben verantwortlich:

Gateway-Aufgaben:

- Mediendatenstrom-Verarbeitung und Integrität des Sprachpfads
- DTMF-Relay
- Fax-Relay und -Passthrough
- Ziffernübersetzung und Anrufbearbeitung
- DFÜ-Peers und Codec-Filterung
- Bearbeitung der Carrier ID
- Gateway-basierte Abrechnung

Gatekeeper-Aufgaben:

- Gateway-Auswahl und Lastenausgleich
- Anrufweiterleitung (Zonenauswahl)
- Gatekeeper-basierte Abrechnung
- Steuerung von Anrufzugabe, Sicherheit und Bandbreite
- Durchsetzung von Anrufkapazitäten

Befehle für die Fehlerbehebung

Das Output Interpreter-Tool (OIT) (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **show**-Befehlsausgabe anzuzeigen.

Hinweis: Lesen Sie Wichtige Informationen zu Debug-Befehlen, bevor Sie **Debug-**Befehle verwenden.

Gateway-Debug-Befehle:

- **debug voip ipipgw** - Dieser Befehl zeigt Informationen zur Behandlung von IP-to-IP-Anrufen an.
- **debug h225 asnl**: Dieser Befehl zeigt den tatsächlichen Inhalt des asn1-Teils von H.225-Meldungen und zugehörigen Ereignissen an.
- **debug h225 events** (h225 Ereignisse debuggen): Dieser Befehl zeigt den tatsächlichen Inhalt des asn1-Teils von H.225-Meldungen und den damit verbundenen Ereignissen an.
- **debug h245 asn1**: Dieser Befehl zeigt den tatsächlichen Inhalt des asn1-Teils von H.245-Meldungen und zugehörigen Ereignissen an.

Gatekeeper debug-Befehle:

- **debug h225 asn1**: Dieser Befehl zeigt den tatsächlichen Inhalt des asn1-Abschnitts von H.225 RAS-Nachrichten und zugehörigen Ereignissen an.
- **debug h225 events** (h225 Ereignisse debuggen): Dieser Befehl zeigt den tatsächlichen Inhalt

des asn1-Abschnitts von H.225 RAS-Meldungen und den zugehörigen Ereignissen an.
- **debug gatekeeper main 10**: Dieser Befehl verfolgt wichtige Gatekeeper-Funktionen wie LRQ-Verarbeitung, Gateway-Auswahl, Verarbeitung von Zulassungsanträgen, Präfix-Abgleich und Anrufkapazitäten nach.
- **debug gatekeeper Zone 10**: Dieser Befehl verfolgt gatekeeper-zonenorientierte Funktionen.
- **debug gatekeeper call 10 (**Gatekeeper-**Anruf 10 debuggen**): Dieser Befehl verfolgt gatekeeper-anruforientierte Funktionen, z. B. das Verfolgen von Anrufreferenzen.
- **debug gatekeeper gup asn1** - Dieser Befehl zeigt den tatsächlichen Inhalt des asn1-Abschnitts von Gatekeeper-Aktualisierungsprotokollnachrichten und zugehörigen Ereignissen für die Kommunikation zwischen Gatekeepern in einem Cluster an.
- **debug gatekeeper gup events (**Gatekeeper-Gruppenereignisse debuggen) - Dieser Befehl zeigt den tatsächlichen Inhalt des asn1-Abschnitts von Gatekeeper-Aktualisierungsprotokollnachrichten und der zugehörigen Ereignisse für die Kommunikation zwischen Gatekeepern in einem Cluster an.
- **debug ras**: Dieser Befehl zeigt die Typen und Adressierungen der gesendeten und empfangenen RAS-Nachrichten an.

Gateway-Befehle anzeigen:

- **show h323 gateway h225 (h225 anzeigen**): Dieser Befehl verwaltet die Anzahl von H.225-Meldungen und -Ereignissen.
- **show h323 gateway ras (h323 Gateway-Ras**): Dieser Befehl verwaltet die Anzahl der gesendeten und empfangenen RAS-Nachrichten.
- **show h323 gateway Cause (Ursache anzeigen**): Dieser Befehl zeigt die Anzahl der von verbundenen Gateways empfangenen Ursachencodes an.
- **show call active voice [brief]**: Mit diesen Befehlen werden Informationen zu aktiven und abgebrochenen Anrufen zusammengefasst.
- **show crm (**Anrufkapazitätszähler anzeigen): Dieser Befehl zeigt die Anzahl der Anrufe an, die IP-Schaltungen auf dem IPGW zugeordnet sind.
- **show processes cpu**: Dieser Befehl zeigt detaillierte Statistiken zur CPU-Auslastung (CPU-Auslastung pro Prozess) an.
- **show gateway**: Dieser Befehl zeigt den aktuellen Status des Gateways an.

Gatekeeper show-Befehle:

- **show/clear gatekeeper performance stats (Leistungsstatistiken des Gatekeepers anzeigen/löschen**): Dieser Befehl zeigt die Statistiken des Gatekeepers an, die mit der Verarbeitung von Anrufen verknüpft sind.
- **show gatekeeper zone status (Status der Gatekeeper-Zone anzeigen**) - Dieser Befehl listet Informationen zu den lokalen und Remote-Zonen auf, die dem Gatekeeper bekannt sind.
- **show gatekeeper endpoint (Endpunkt des Gatekeepers anzeigen**): Dieser Befehl listet wichtige Informationen zu den beim Gatekeeper registrierten Endpunkten auf, einschließlich IPIPGWs.
- **show gatekeeper circuit (Gatekeeper-Schaltung anzeigen**): Dieser Befehl kombiniert Informationen zur Leitungsnutzung über mehrere Gateways.
- **show gatekeeper calls (Gatekeeper-Anrufe anzeigen**): Dieser Befehl listet wichtige Informationen zu Anrufen auf, die in der lokalen Zone behandelt werden.

Zugehörige Informationen

- Cisco Multiservice IP-to-IP Gateway - Anwendungsleitfaden
- Unterstützung von Sprachtechnologie
- Produktsupport für Sprach- und Unified Communications
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.