الشبكة المحلية إلى البعيدة باستخدام IP إلى IP ميزة عبارة Cisco متعددة الخدمات من IP إلى

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
معلومات أساسية
التكوين
الرسم التخطيطي للشبكة
التكوينات
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
إجراء استكشاف الأخطاء وإصلاحها
أوامر استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يقدم هذا المستند نموذجا لتكوين شبكة محلية إلى بعيدة باستخدام ميزة عبارة IP إلى IP متعددة الخدمات (IPIPGW) من Cisco. توفر ميزة IPIPGW آلية لتمكين مكالمات H.323 عبر IP (VoIP) من شبكة IP إلى أخرى.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل محاولة هذا التكوين:

- أنجزت أساسي H.323 مدخل تشكيل. للحصول على تعليمات تفصيلية، ارجع إلى دليل التكوين Cisco IOS H.323، مكتبة تكوين الصوت Cisco IOS، الإصدار 12.3.
- قم بإجراء تكوين أساسي ل H.323 برنامج حماية البوابة. للحصول على تعليمات تفصيلية، ارجع إلى دليل التكوين Cisco IOS H.323، مكتبة تكوين الصوت Cisco IOS، الإصدار 12.3.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ثلاثة موجهات Cisco Cisco H.323 Gatekeeper (Cisco 2610، Cisco 2611، Cisco 2612، Cisco 2613

2620، Cisco 2621، Cisco 2650، Cisco 2651، Cisco 2691، Cisco 2610XM، Cisco 2611XM، Cisco 21XM، Cisco 666220XM، Cisco 26200XM أو cisco 2650XM أو cisco 2651XM أو cisco 3620 أو cisco 3640 أو cisco 3660 أو cisco 3725 أو cisco 3745 أو cisco 7200 Series أو cisco 7400 Series) مع برنامج Cisco IOS الإصدار 12.2(13)T أو إصدار أحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

تقدم ميزة IPIPGW متعددة الخدمات من Cisco برنامج حماية البوابة عبر المناطق. Via-Zone هو مصطلح Cisco للمنطقة التي تحتوي على بوابات من IP إلى IP وبوابات ممكنة من خلال المنطقة. بإمكان برنامج حماية البوابة الذي يدعم تقنية Via-zone التعرف على عبر المناطق وإرسال حركة مرور البيانات إلى بوابات عبر المنطقة. تتضمن بوابات Cisco Via-Zone التي تم تمكينها أمر واجهة سطر الأوامر (via-zone CLI).

عادة ما توجد مناطق Via-Areas على حافة شبكة مزود خدمة الإنترنت الهاتفية (ITSP)، وتكون مثل نقطة نقل VoIP، أو منطقة الترادف، حيث تمر حركة المرور عبر الطريق إلى وجهة المنطقة البعيدة. تقوم البوابات في هذه المنطقة بإنهاء الاستدعاءات المطلوبة وإعادة إنشاء حركة المرور إلى الوجهة النهائية. تعمل بوابات عبر المنطقة كالمعتاد للتطبيقات التي لا تدعم بروتوكول الإنترنت (IP) إلى بروتوكول الإنترنت (IP). يدعم حراس البوابات في المناطق البعيدة إدارة الموارد (على سبيل المثال، تحديد البوابة وموازنة التحميل) باستخدام حقل السعات في رسائل RAS الإصدار 4 من H.323.

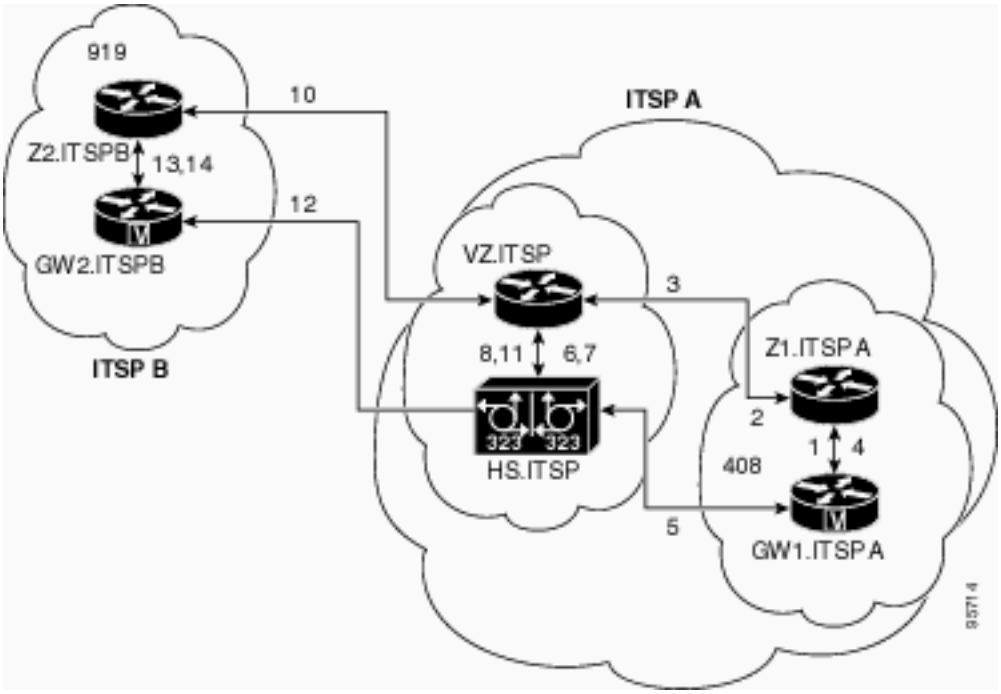
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للعثور على مزيد من المعلومات حول الأوامر المستخدمة في هذا المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- (Originating Gatekeeper (Z1.ITSPA
- برنامج (Via-Zone Gatekeeper (VZ.ITSP
- (Terminating Gatekeeper (Z2.ITSPB

في هذا المثال، يتصل متصل من رمز المنطقة 408 بطرف في رمز المنطقة 919، وتظهر هذه الإجراءات:

1. يرسل GW1.ITSPA رسالة طلب قبول (ARQ) مع الرقم المستند إلى 919 إلى Z1.ITSPA.
2. Z1.ITSPA يقوم بحل الأمر 919 إلى VZ.ITSP وإرسال رسالة طلب موقع (LRQ) إلى VZ.ITSP.
3. ال LRQ ل 919 رقم من z1ITSPA منطقة يستلم ب VZ.ITSP. يتحقق VZ.ITSP من تكوين المنطقة عن بعد ل Z1ITSPA ويخلص إلى تكوين المنطقة VZITSP الخاصة بها كمنطقة "invia". ثم يرسل رسالة تأكيد الموقع (LCF) إلى Z1.ITSPA ويحدد HS.ITSP كبوابة الوجهة لاستدعاء 919.
4. يرسل Z1.ITSPA رسالة تأكيد الإدخال (ACF) إلى GW1.ITSPA ويحدد HS.ITSP كبوابة الوجهة.
5. يرسل GW1.ITSPA رسالة إعداد إلى HS.ITSP لمكالمة 919.
6. يقوم HS.ITSP باستشارة VZ.ITSP باستخدام ARQ (يحتوي على ANSWERcall=true) لقبول المكالمة الواردة.
7. VZ.ITSP يستجيب مع ACF لقبول المكالمة.
8. يحتوي HS.ITSP على نظير طلب يحدد VZ.ITSP RAS للبادئة 919 (أو لكل البادئات)، لذلك فإنه يرسل ARQ (مع تعيين responseCall على FALSE) إلى VZ.ITSP للبادئة 919.
9. يحدد VZ.ITSP gatekeeper أن منطقة Z2ITSPB تتعامل مع البادئة "919" من خلال البحث عن جدول بادئة المنطقة. ثم يستخدم تكوين المنطقة عن بعد ويعرف أنه تم تكوين منطقة VZITSP المحلية الخاصة به كمنطقة "خارج". ثم يقوم بإرسال LRQ إلى Z2.ITSPB Gatekeeper بدلا من إرسال LRQ إلى برنامج حماية بوابة آخر من IP إلى IP.
10. يرى Z2.ITSPB البادئة 919 على أنها في منطقته الخاصة ويرجع LCF الذي يشير إلى GW2.ITSPB.
11. ترجع VZ.ITSP ACF يحدد GW2.ITSPB كبوابة الوجهة إلى HS.ITSP.
12. يرسل HS.ITSP رسالة إعداد إلى GW2.ITSPB لاستدعاء 919.
13. يرسل GW2.ITSPB ARQ (يحتوي على responseCall=true) إلى Z2.ITSPB.
14. Z2.ITSPB يرسل قائمة تحكم في الوصول (ACF) ل ResponseCall.
15. يتم توصيل الاتصال ب H.323 بين HS.ITSP و GW2.ITSPB. يتم توصيل مكالمة H.323 بين GW1.ITSPA

و HS.ITSP.

(Originating 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
```

برنامج VZ.ITSP) Via-Zone Gatekeeper)

```
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
```

(Terminating Gatekeeper (Z2.ITSPB

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

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض

تحليل مُخرَج الأمر **show** .

ملاحظة: تم الحصول على مخرجات أوامر العرض هذه من برنامج حماية البوابة VZ.ITSP.

قم بإصدار **show running config | بدء** أمر **برنامج حماية البوابة** للتحقق من تكوين برنامج حماية البوابة:

```
                                                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
```

يمكنك أيضا إستخدام الأمر **show gatekeeper zone status** للتحقق من تكوين برنامج حماية البوابة:

```
                                                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
```

قم بإصدار الأمر **show gatekeeper status** لعرض حدود سعة المكالمة:

```
                                                   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
```

قم بإصدار الأمر **show gatekeeper performance stats** لعرض معلومات RAS، بما في ذلك إحصائيات عبر

المنطقة:

```
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
```

يتم عرض حقول RAS عبر المنطقة الهامة التالية في العرض:

- InLRQ: —مرتبط بالكلمة الأساسية invia. إذا كانت Invia منطقة محلية، فإن هذا العداد يحدد عدد LRQs التي تم إنهاؤها بواسطة Invia Gatekeeper المحلي.
- infwdLRQ—مرتبط بالكلمة الأساسية invia. إذا كانت Invia منطقة بعيدة، فإن هذا العداد يحدد عدد أرقام LRQ التي تم إعادة توجيهها إلى برنامج حماية البوابة البعيد.
- inrLRQ—مرتبط بالكلمة الأساسية invia. عدد المرات التي تعذر فيها معالجة LRQ لتعذر العثور على معرف Invia Gatekeeper. ينتج عادة عن اسم حارس بوابة غير صحيح إملائيا.
- outLRQ—مرتبط بالكلمة الأساسية Outvia. إذا كانت منطقة الصادر منطقة محلية، فسيقوم هذا العداد بتعريف عدد LRQs التي تم إنهاؤها بواسطة برنامج حماية البوابة الخارجية المحلي. لا ينطبق هذا العداد إلا في التكوينات التي لم يتم فيها تحديد أية بوابات.
- outfwdLRQ—مرتبط بالكلمة الأساسية Outvia. إذا كانت منطقة الصادر منطقة بعيدة، يحدد هذا العداد عدد أرقام LRQ التي تم إعادة توجيهها إلى برنامج حماية البوابة البعيدة. لا ينطبق هذا العداد إلا في التكوينات التي لم يتم فيها تحديد أية بوابات.
- خارج LRQ—مرتبط بالكلمة الأساسية Outvia. عدد المرات التي تعذر فيها معالجة LRQ لتعذر العثور على معرف البوابة الخارجية. ينتج عادة عن اسم حارس بوابة غير صحيح إملائيا. لا ينطبق هذا العداد إلا في التكوينات التي لم يتم فيها تحديد أية بوابات.
- outARQ—مرتبط بالكلمة الأساسية Outvia. يحدد عدد ARQs المنشئة التي تتم معالجتها بواسطة "برنامج حماية البوابة المحلية" إذا كانت المنطقة الخارجية هي المنطقة المحلية.
- OutfwdARQ — مرتبط بالكلمة الأساسية Outvia. إذا كان برنامج حماية البوابة الصادرة منطقة بعيدة، فإن هذا الرقم يحدد عدد ARQs المنشئة التي تم تلقيها بواسطة برنامج حماية البوابة هذا والتي نتج عنها إرسال قوائم التحكم في الوصول (LRQ) إلى برنامج حماية البوابة الخارجية.
- outerrARQ—مرتبط بالكلمة الأساسية Outvia. عدد المرات التي تعذر فيها معالجة ARQ الأصلي بسبب تعذر العثور على معرف البوابة الخارجية. يحدث ذلك عادة بسبب اسم حارس بوابة غير صحيح إملائيا.

أدخل الأمر **show gatekeeper circuit** لعرض المعلومات حول المكالمات قيد التقدم:

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

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

ملاحظة: تشير كلمة "يدعو" إلى إستدعاء الأرجل في بعض الأوامر والمخرجات.

أدخل الأمر **show gatekeeper endpoint** لعرض المعلومات حول تسجيلات نقاط النهاية:

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

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

إجراء استكشاف الأخطاء وإصلاحها

هذه معلومات أستكشاف الأخطاء وإصلاحها المتعلقة بهذا التكوين. أكمل هذه الخطوات لاستكشاف أخطاء التكوين وإصلاحها.

تشبه إجراءات أستكشاف أخطاء IPIPGW وإصلاحها بوابة TDM-to-IP H.323. بشكل عام، يجب أن تمضي جهود أستكشاف المشكلات وحلها كما هو موضح هنا:

1. عزل السيناريو الفاشل وإعادة إنتاجه.
2. قم بتجميع المعلومات ذات الصلة من أوامر show و debug وملفات التكوين ومحللي البروتوكول.
3. حدد المؤشر الأول للفشل في تعقب البروتوكول أو إخراج تصحيح الأخطاء الداخلي.
4. ابحث عن السبب في ملفات التكوين.

إذا كان يشتبه في أن via-zone هي مصدر فشل المكالمة، فقم بعزل المشكلة إلى IPIPGW أو حارس البوابة عن طريق تحديد الوظيفة الفرعية المتأثرة والتركيز على أوامر show و debug المتعلقة بتلك الوظيفة الفرعية.

قبل أن تتمكن من بدء أستكشاف الأخطاء وإصلاحها، يجب أولا عزل المشكلة إلى عبارة أو حارس بوابة. تكون البوابات وحراس البوابات مسؤولين عن هذه المهام:

مهام البوابة:

- معالجة تدفق الوسائط وسلامة مسار الكلام
- ترحيل DTMF
- ترحيل الفاكس والعبور
- ترجمة الأرقام ومعالجة المكالمات
- أنداد الطلب وتصفية الترميز
- معالجة معرف الناقل
- الفوترة المستندة إلى البوابة

مهام برنامج حماية البوابة:

- تحديد البوابة وموازنة الحمل
- توجيه المكالمات (تحديد المنطقة)
- الفوترة المستندة إلى برنامج حماية البوابة
- التحكم بإذن دخول المكالمة والأمان وعرض النطاق الترددي
- إنفاذ قدرات الاتصال

أوامر استكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

أوامر تصحيح أخطاء البوابة:

- **debug voip ip ip ip** — يعرض هذا الأمر المعلومات المتعلقة بمعالجة مكالمات IP إلى IP.
- **debug h225 asnl**—يعرض هذا الأمر المحتويات الفعلية للجزء ASN1 من رسائل H.225 والأحداث المقترنة بها.
- **debug h225 events**— يعرض هذا الأمر المحتويات الفعلية للجزء ASN1 من رسائل H.225 والأحداث المقترنة بها.
- **debug h245 asn1**— يعرض هذا الأمر المحتويات الفعلية للجزء ASN1 من رسائل H.245 والأحداث المقترنة بها.

أوامر تصحيح أخطاء برنامج حماية البوابة:

- **debug h225 asn1**— يعرض هذا الأمر المحتويات الفعلية لجزء ASN1 من رسائل H.225 RAS والأحداث المقترنة بها.
- **debug h225 events**— يعرض هذا الأمر المحتويات الفعلية للجزء ASN1 من رسائل H.225 RAS والأحداث المقترنة بها.
- **debug gatekeeper main 10**—يقوم هذا الأمر بتتبع وظائف حماية البوابة الرئيسية، مثل معالجة LRQ وتحديد البوابة ومعالجة طلب الدخول ومطابقة البادئة وسعات المكالمات.
- **debug gatekeeper zone 10**—يقوم هذا الأمر بتعقب الوظائف الموجهة إلى المنطقة ل Gatekeeper.
- **debug gatekeeper call 10**—يتعقب هذا الأمر الدوال الموجهة من قبل برنامج حماية البوابة، مثل تعقب مراجع المكالمات.
- **debug gatekeeper gup asn1**— يعرض هذا الأمر المحتويات الفعلية لجزء ASN1 من رسائل بروتوكول تحديث برنامج حماية البوابة والأحداث المرتبطة للاتصال بين حراس البوابات في نظام مجموعة.
- **debug gatekeeper gup events**—يعرض هذا الأمر المحتويات الفعلية لجزء ASN1 من رسائل بروتوكول تحديث برنامج حماية البوابة والأحداث المقترنة للاتصال بين حراس البوابات في نظام مجموعة.
- **debug ras**— يعرض هذا الأمر أنواع رسائل RAS التي تم إرسالها واستقبالها وعنونة هذه الرسائل.

أوامر عرض البوابة:

- **show h323 gateway h225**—يحتفظ هذا الأمر بتعدادات رسائل H.225 والأحداث.
- **show h323 gateway ras**— يحتفظ هذا الأمر بحصر رسائل RAS المرسلة والمستلمة.
- **show h323 gateway cause**— يعرض هذا الأمر عدد رموز السبب التي تم تلقيها من البوابات المتصلة.
- **show call active voice [brief]**—تقوم هذه الأوامر بتجميع المعلومات حول المكالمات النشطة والمسموحة.
- **show crm**— يعرض هذا الأمر عمليات عد سعة المكالمة المرتبطة بدوائر IP على IPIPGW.
- **show process cpu**—يعرض هذا الأمر إحصائيات إستخدام وحدة المعالجة المركزية (إستخدام وحدة المعالجة المركزية لكل عملية).
- **show gateway**— يعرض هذا الأمر الحالة الحالية للعبارة.

أوامر عرض برنامج حماية البوابة:

- **show/clear** gatekeeper **performance stats**— يعرض هذا الأمر إحصائيات برنامج حماية البوابة المرتبطة بمعالجة المكالمات.
- **show gatekeeper zone status** — يسرد هذا الأمر معلومات حول المناطق المحلية والمناطق البعيدة المعروفة ل gatekeeper.
- **show gatekeeper endpoint**— يسرد هذا الأمر المعلومات الأساسية حول نقاط النهاية المسجلة إلى البوابة، بما في ذلك IPIPGW.

- **show gatekeeper circuit** — يجمع هذا الأمر بين المعلومات حول إستخدام الدائرة عبر بوابات متعددة.
- **show gatekeeper call**—يسرد هذا الأمر المعلومات الأساسية حول المكالمات التي تتم معالجتها في المنطقة المحلية.

معلومات ذات صلة

- دليل تطبيق عبارة Cisco متعددة الخدمات من IP إلى IP
- دعم تقنية الصوت
- دعم منتجات الاتصالات الصوتية والاتصالات الموحّدة
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).