دراسة حالة نشر خدمة IP الهاتفية - ACU

المحتويات

المقدمة

الشبكة الأكاديمية والبحثية الأسترالية (AARNet) هي شبكة عبر بروتوكول الإنترنت عالية السرعة على الصعيد الوطني تربط بين 37 جامعة أسترالية فضلا عن منظمة الكومنولث للبحوث العلمية والصناعية.

تم إنشاء ARNet في البداية كشبكة بيانات، ولكنها نقلت الصوت عبر IP (VoIP) منذ أوائل عام 2000. شبكة الصوت عبر بروتوكول الإنترنت (VoIP) المنتشرة حاليا هي حل تمرير إجباري يحمل مكالمات الصوت عبر بروتوكول الإنترنت (VoIP) بين الجامعات وبطاقات التبادل الفرعية التلقائية الخاصة ببروتوكول PABX) CSIRO). وهو يوفر أيضا بوابات شبكة الهاتف المحولة العامة (PSTN) التي تسمح ل PSTN بالإنفصال عند النقطة الأكثر توفيرا للتكلفة. على سبيل المثال، تم نقل مكالمة من هاتف يعمل عبر بروتوكول PABX في ملبورن إلى هاتف يعمل عبر بروتوكول PSTN في سيدني مع نقل الصوت عبر بروتوكول الإنترنت (VoIP) من ملبورن إلى بوابة سيدني PSTN. وهو متصل هناك ب PSTN.

الجامعة الكاثوليكية الأسترالية هي إحدى الجامعات التي ترتبط بشبكة ARNet. وفي أواخر عام 2000، بدأت وحدة التحكم في الوصول نشر خدمة IP الهاتفية التي نشرت ما يقرب من 2 000 هاتف بروتوكول الإنترنت عبر ستة مجمعات جامعية.

تغطي دراسة الحالة هذه نشر خدمة IP الهاتفية لوحدة التحكم في الوصول. اكتمل المشروع. ومع ذلك، هناك مسائل معمارية هامة يتعين معالجتها في العمود الفقري للشبكة إذا أريد توسيع نطاق الشبكة عندما تحذو جامعات أخرى حذو وحدة تنسيق الشؤون الإدارية. وتصف هذه الوثيقة هذه المسائل وتقترح وتناقش مختلف الحلول. من المرجح تعديل

نشر خدمة IP الهاتفية الخاصة بوحدة التحكم في الوصول لاحقا ليتوافق مع البنية النهائية الموصى بها.

ملاحظة: كانت جامعة ديكين أول جامعة أسترالية تقوم بنشر خدمة IP الهاتفية. ومع ذلك، لا تستخدم جامعة ديكين شبكة آرنت لحمل خدمة الإتصالات الهاتفية عبر بروتوكول الإنترنت.

آرنيت

وقد أنشأت الجامعات الأسترالية ومركز أبحاث العلوم والتكنولوجيا في عام 1990 شبكة آرون عبر لجنة نواب المستشارين الأستراليين. تسعة وتسعون في المئة من حركة الإنترنت في أستراليا كانت للأعضاء المؤسسين خلال السنوات القليلة الأولى. وهناك قدر ضئيل من حركة المرور التجارية من المنظمات التي تربطها صلة وثيقة بقطاع الخدمات والبحوث. وازداد إستخدام قاعدة المستخدمين غير AARNet إلى 20 في المائة من إجمالي حركة المرور في أواخر عام 1994.

وقد باع المركز قاعدة العملاء التجاريين لشركة آرنيت إلى شركة تلسترا في تموز/يوليه 1995. وقد ولد هذا الحدث ما كان سيصير أخيرا "تلسترا بيغ بوند". وحفز ذلك على زيادة نمو الاستخدام التجاري والخاص للإنترنت في أستراليا. وأدى نقل الملكية الفكرية والخبرة الفنية إلى تطوير شبكة الإنترنت في أستراليا. وإلا فما كان هذا ليحدث بمثل هذا المعدل السريع.

وقد طور المجلس ARNet2 في أوائل عام 1997. وقد كان ذلك بمثابة تحسين آخر لشبكة الإنترنت في أستراليا، التي تستخدم وصلات الصراف الآلي ذات النطاق الترددي العريض وخدمات الإنترنت بموجب عقد مع شركة Cable & Wireless Optus (CWO) Limited. ويعزى جزئيا النشر السريع لخدمات الملكية الفكرية من قبل المنظمة العالمية للأرصاد الجوية لتلبية متطلبات AARNet2 إلى نقل المعرفة والخبرة الفنية من شبكة AARNet.

ACU

يذكر أن جامعة وحدة الرعاية الاجتماعية هي جامعة عامة تأسست عام 1991. وتضم الجامعة نحو 10 آلاف طالب و 1000 موظف. هنالك ستة مجمعات على الساحل الشرقي لاستراليا. يوضح هذا الجدول حرم وحدة التحكم بالوصول (ACU) ومواقعها:

حرم الجامعة	مدينة	الحالة
جبل سانت ماري	ستراثفيلد	نيو ساوث ويلز (نيو ساوث ويلز)
ماكيلوب	شمال سيدني	نيو ساوث ويلز (نيو ساوث ويلز)
باتريك	ملبورن	فيكتوريا (فيتش)
الأكويني	بالارات	فيكتوريا (فيتش)
سينادو	كانبرا	إقليم العاصمة الأسترالية
ماكاولي	بريزبان	كوينزلاند (QLD)

اعتمدت ACU على حل CENTX) Telstra Spectrum) قبل طرح حل IP Telephony الذي تصفه دراسة الحالة هذه. كان الانتقال إلى خدمة IP الهاتفية مدفوعا في الأساس بالرغبة في خفض التكاليف.

سيرو

يعمل في المركز نحو 6500 موظف في عدة مواقع في أستراليا. ويجري المركز أبحاثا في مجالات مثل الزراعة والمعادن والطاقة والتصنيع والاتصالات والبناء والصحة والبيئة.

كانت CSIRO أول مؤسسة تستخدم AARNet ل VoIP. وكانت الهيئة رائدة في العمل الباكر الذي أنجز في هذا المجال.

آرنيت

ويعتبر العمود الفقري ل ARNet مكونا هاما في أي عملية نشر لهاتف بروتوكول الإنترنت في الجامعة. وهي توفر الترابط بين الجامعات وبين خدمتين رئيسيتين في المجال الصوتي:

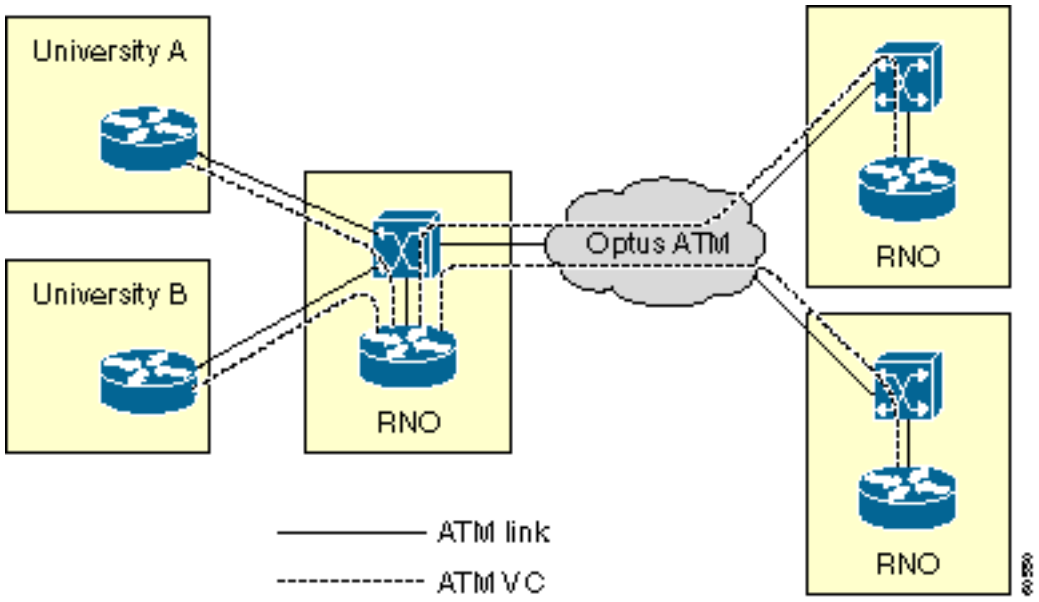
- نقل حزم بروتوكول نقل الوقت الفعلي (RTP) بتقنية VoIP مع ضمان جودة الخدمة (QoS) المناسبة للصوت
- نقطة وصول منخفضة التكلفة إلى شبكات PSTN في جميع أنحاء البلاد

يصف هذا القسم بنية ARNet الحالية وكيفية تقديمها لهذه الخدمات. كما يوضح أيضا بعض مشاكل قابلية التوسعة التي تنشأ مع نشر المزيد من الجامعات لحل خدمة IP الهاتفية. أخيرا، يناقش الحلول الممكنة لمشاكل قابلية التوسيع هذه.

طبولوجيا آرنيت

تتكون ARNet من POP واحد (نقطة التواجد) في كل ولاية. ويشار إلى الملوثات العضوية الثابتة باسم عمليات الشبكة الإقليمية (RNOs). وتتصل الجامعات بمركز البحوث الإقليمية في ولاية كل منها. ويتم توصيل وحدات RNO بدورها بواسطة شبكة كاملة من شبكات Optus ATM PVCs. ومعا تشكل AARNet.

يتكون RNO النموذجي من محول Cisco LS1010 ATM واحد وموجه واحد مرفق ATM. يتصل موجه RNO بكل موجه جامعي من خلال ATM PVC واحد عبر إرتباط ميكروويف من الفئة E3. يحتوي كل موجه RNO أيضا على شبكة كاملة من ATM PVCs التي توفرها شبكة Optus ATM لجميع RNO الأخرى. يمثل هذا المخطط مخطط ARNet العام للشبكة:



هناك إستثناءات عديدة للمخطط. بعضها ذو أهمية من منظور صوتي. هذه بعض الاستثناءات:

- يستخدم رقم الملكية في فيكتوريا IP التقليدي عبر ATM (RFC 1577) بدلا من PVCs لربط الجامعات برقم الملكية.
- تتصل الجامعات الريفية عادة ب RNO بواسطة ترحيل الإطارات أو ISDN.
- وهناك بعض الجامعات الكبرى التي ترتبط إرتباطا أكثر من واحد باتفاقية ترخيص المواد.

يوضح هذا الجدول الدول والأقاليم التي لديها حاليا إتفاقية ترخيص المواد المسترجعة. يشمل الجدول المدن الكبرى للقراء الذين لا يعرفون الجغرافيا الأسترالية.

الحالة	العاصمة	رنو؟	إتصالات المجمع
نيو ساوث ويلز	سيدني	نعم	تي بي دي
فيكتوريا	ملبورن	نعم	تي بي دي

كوينزلاند	بريزبان	نعم	تي بي دي
جنوب أستراليا	أديلايد	نعم	تي بي دي
أستراليا الغربية	بيرث	نعم	تي بي دي
إقليم العاصمة الأسترالية	كانبرا	نعم	تي بي دي
الإقليم الشمالي	داروين	لا	—
تسمانيا	هوبارت	لا	—

جودة الخدمة

تم تمكين QoS بالفعل لأجزاء من AARNet للصوت نتيجة لمشروع تجاوز رسوم المكالمات VoIP. جودة الخدمة ضروري لحركة المرور الصوتية من أجل توفير هذه الميزات، والتي تقلل التأخير والتشوه وتقضي على فقدان الحزمة:

- السياسة - قم بتمييز حركة مرور البيانات الصوتية من مصادر غير موثوق بها.
- قوائم الانتظار — يجب إعطاء أولوية للصوت على جميع حركات المرور الأخرى لتقليل التأخير أثناء إزدحام الارتباط.
- تجزئة ودمج الارتباط (LFI)- يجب تجزئة حزم البيانات وتفريغ الحزم الصوتية على إرتباطات بطيئة.

يجب تصنيف حركة المرور إلى الحزم الصوتية الخاصة بالشرطة وقائمة الانتظار بشكل صحيح. يصف هذا القسم كيفية إجراء التصنيف على AARNet. تصف الفصول التالية وضع السياسات وتنفيذ قوائم الانتظار.

تصنيف

لا تحصل كل حركة المرور على نفس جودة الخدمة. يتم تصنيف حركة المرور في هذه الفئات لتوفير جودة الخدمة بشكل انتقائي:

- البيانات
- صوت من مصادر معروفة وموثوق بها
- صوت من مصادر غير معروفة

يتم إعطاء فقط الأجهزة الموثوق بها جودة جودة جودة جودة جودة جودة الخدمة على AARNet. هذه الأجهزة هي في الأساس بوابات يتم تعريفها بواسطة عنوان IP. يتم إستخدام قائمة التحكم في الوصول (ACL) لتحديد هذه المصادر الصوتية الموثوقة.

```
access-list 20 permit 192.168.134.10
access-list 20 permit 192.168.255.255
```

يتم إستخدام أسبقية IP لتمييز حركة مرور البيانات الصوتية عن حركة مرور البيانات. يتمتع الصوت بأولوية IP تبلغ 5.

```
class-map match-all VOICE
    match ip precedence 5
```

دمج الأمثلة السابقة لتعريف الحزم من مصدر موثوق به.

```
class-map match-all VOICE-GATEWAY
            match class-map VOICE
            match access-group 20
```

أستخدم نفس المبادئ لتعريف الحزم الصوتية من مصدر غير معروف.

```
class-map match-all VOICE-NOT-GATEWAY
            match class-map VOICE
```

```
match not access-group 20
```

وضع السياسات

يتم تصنيف حركة مرور الصوت من مصدر غير موثوق به ووضع علامة عليها أسفل عند وصول حركة المرور إلى واجهة. يوضح هذان المثالان كيفية تنفيذ السياسة حسب نوع حركة المرور المتوقع وصولها على واجهة معينة:

يبحث الموجه عن الحزم الصوتية غير الموثوق بها ويغير أسبقية IP الخاصة بها إلى 0 إذا كان هناك مصادر صوت موثوق بها بعد التدفق.

```
policy-map INPUT-VOICE
class VOICE-NOT-GATEWAY
    set ip precedence 0

interface FastEthernet2/0/0
description Downstream voice gateways
service-policy input INPUT-VOICE
```

يبحث الموجه عن جميع الحزم الصوتية ويغير أسبقية IP الخاصة بها إلى 0 إذا لم تكن هناك مصادر صوت معروفة من الخادم.

```
policy-map INPUT-DATA
          class VOICE
    set ip precedence 0

interface FastEthernet2/0/1
description No downstream voice gateways
service-policy input INPUT-DATA
```

قوائم الانتظار غير الصوتية

جميع عمليات نقل الصوت عبر بروتوكول الإنترنت في آرنيت كانت مجرد عمليات تجاوز حتى وقت قريب. ينتج عن هذا الشرط عدد قليل نسبيا من نقاط نهاية VoIP. يميز تصميم قوائم الانتظار الحالي بين الواجهات التي تحتوي على أجهزة VoIP من الخادم والواجهات التي لا تحتوي على هذه الواجهات. يناقش هذا القسم قوائم الانتظار على الواجهات غير الخاصة ب VoIP.

يتم تكوين واجهة غير صوتية إما لقوائم الانتظار العادلة المرجحة (WFQ) أو الكشف المبكر العشوائي المرجح (WRED). ويمكن تكوين هذه العناصر مباشرة على الواجهة. ومع ذلك، يتم تطبيق آلية قوائم الانتظار من خلال مخطط سياسة لتسهيل تغيير آلية قوائم الانتظار على نوع واجهة محدد. هناك تعيين نهج واحد لكل نوع واجهة. وهذا يعكس حقيقة عدم دعم جميع آليات قوائم الانتظار على جميع الواجهات.

```
policy-map OUTPUT-DATA-ATM
        class class-default
            fair-queue

policy-map OUTPUT-DATA-VIP-ATM
        class class-default
            random-detect

policy-map OUTPUT-DATA-ETHERNET
        class class-default
            fair-queue

policy-map OUTPUT-DATA-VIP-ETHERNET
        class class-default
            random-detect
```

```
policy-map OUTPUT-DATA-SERIAL
 class class-default
  fair-queue

policy-map OUTPUT-DATA-VIP-SERIAL
 class class-default
  random-detect
```

يتم إرفاق خرائط النهج بالواجهات الخاصة وهي خاصة بأنواع الواجهات. على سبيل المثال، يعمل هذا على تبسيط عملية تغيير آلية قوائم الانتظار على منافذ إيثرنت متعددة الاستخدامات القائمة على معالج الواجهة (VIP) من WRED إلى WFQ. وهو يتطلب تغييرا واحدا في خريطة السياسة. يتم إجراء التغييرات على جميع واجهات إيثرنت المستندة إلى الشخصيات المهمة.

```
interface ATM0/0
 service-policy output OUTPUT-DATA-ATM

interface ATM1/0/0
 service-policy output OUTPUT-DATA-VIP-ATM

interface Ethernet2/0
 service-policy output OUTPUT-DATA-ETHERNET

interface Ethernet3/0/0
 service-policy output OUTPUT-DATA-VIP-ETHERNET

interface Serial4/0
 service-policy output OUTPUT-DATA-SERIAL

interface Serial5/0/0
 service-policy output OUTPUT-DATA-VIP-SERIAL
```

قوائم انتظار تقليل التأخير

يتم تكوين أي واجهة تحتوي على أجهزة VoIP موثوقة لتدفق البيانات لقوائم انتظار تقليل التأخير (LLQ). تخضع أي حزمة تجعلها من خلال تصنيف الواجهة الواردة وتحتفظ بأولوية مقدارها 5 إلى LLQ. تخضع أي حزمة أخرى إلى WFQ أو WRED. يعتمد هذا على نوع الواجهة.

يتم إنشاء مخططات سياسة منفصلة لكل نوع واجهة من أجل تسهيل إدارة جودة الخدمة. وهذا مماثل للتصميم غير الصوتي في قائمة الانتظار. ومع ذلك، توجد خرائط نهج متعددة لكل نوع واجهة. وذلك نظرا لتباين سعة أنواع الواجهة لحركة مرور الصوت حسب سرعة الارتباط وإعدادات PVC وما إلى ذلك. يعكس الرقم الموجود في اسم خريطة السياسة عدد المكالمات التي تمت صيانتها ل 30 مكالمة، و 60 مكالمة، وما إلى ذلك.

```
policy-map OUTPUT-VOICE-VIP-ATM-30
 class VOICE
  priority 816
 class class-default
  random-detect

policy-map OUTPUT-VOICE-VIP-ATM-60
 class VOICE
  priority 1632
 class class-default
  random-detect

policy-map OUTPUT-VOICE-ATM-30
 class VOICE
  priority 816
 class class-default
  random-detect
```

```
policy-map OUTPUT-VOICE-ATM-60
                                                 class VOICE
                                              priority 1632
                                           class class-default
                                                 random-detect

policy-map OUTPUT-VOICE-ETHERNET-30
                                                 class VOICE
                                               priority 912
                                           class class-default
                                                  fair-queue

policy-map OUTPUT-VOICE-VIP-ETHERNET-30
                                                 class VOICE
                                                    priority
                                           class class-default
                                                 random-detect

policy-map OUTPUT-VOICE-HDLC-30
                                                 class VOICE
                                               priority 768
                                           class class-default
                                                  fair-queue
```

يتم إرفاق خرائط النهج بالواجهات المعنية. في هذا المثال، يتم تحديد خريطة السياسة لنوع واجهة. لا يتم حاليا منح معالجة خاصة لإرسال الإشارات الصوتية. يمكن تعديل خرائط السياسة بسهولة في مكان واحد إذا أصبح هذا متطلبا في مرحلة لاحقة على نوع واجهة معين. يؤثر التغيير على جميع الواجهات من هذا النوع.

```
                                                 Interface ATM0/0
                                    service-policy output OUTPUT-VOICE-ATM-30

                                                interface ATM1/0/0
                                service-policy output OUTPUT-VOICE-VIP-ATM-30

                                                interface Ethernet2/0
                                service-policy output OUTPUT-VOICE-ETHERNET-60

                                              interface Ethernet3/0/0
                            service-policy output OUTPUT-VOICE-VIP-ETHERNET-60

                                                interface Serial4/0
                                service-policy output OUTPUT-VOICE-SERIAL-30

                                              interface Serial5/0/0
                            service-policy output OUTPUT-VOICE-VIP-SERIAL-60
```

قابلية توسع LLQ

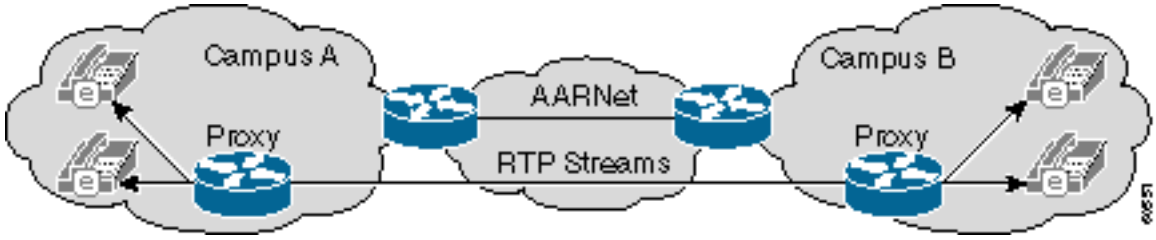
تتضمن آلية قوائم الانتظار بعض مشاكل قابلية التوسعة. تتمثل المشكلة الرئيسية في أنها تعتمد على معرفة عنوان IP لكل جهاز VoIP موثوق به في الشبكة. كان ذلك قيدا معقولا في الماضي عندما كان هناك عدد محدود من بوابات بروتوكول VoIP التي تتعامل مع رسوم المكالمات البعيدة. ويتزايد عدد نقاط نهاية بروتوكول VoIP بشكل كبير، ويصبح غير عملي بشكل متزايد مع نشر خدمة IP الهاتفية. تصبح قوائم التحكم في الوصول (ACL) طويلة للغاية وصعبة الإدارة.

تم إلحاق قوائم التحكم في الوصول (ACL) لضمان حركة المرور من شبكة IP فرعية صوت معينة في كل مجمع ACU في حالة وحدة التحكم في الوصول (ACU). هذا حل مؤقت. والآن يجري التحقيق في هذه الحلول الأطول أمدا:

- وكيل H.323

• وضع سياسات دخول جودة الخدمة

تتمثل الفكرة الرئيسية وراء حل وكيل H.323 في إدخال حركة مرور RTP بالكامل إلى ARNet من مجمع معين بواسطة وكيل. ترى ArnEt جميع حركة مرور RTP من مجمع معين بعنوان IP واحد، كما يوضح هذا المخطط:

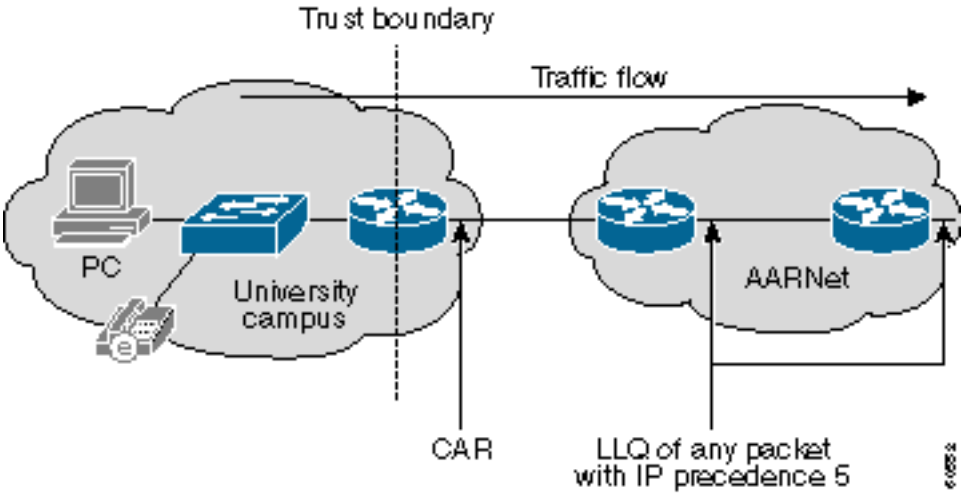


يقتصر عدد الإدخالات في قوائم التحكم بالوصول لجودة الخدمة على سطر واحد لكل مجمع إذا تم نشر هذا النظام بشكل متسق. ولا يزال هذا النظام قادرا على إضافة ما يصل إلى 100 مدخل أو أكثر نظرا لوجود 37 جامعة ذات مجمعات متعددة. وهذا أيضا ليس قابلا للتغيير. قد يكون من الضروري الانتقال إلى تصميم باستخدام عدد واحد أو محدود من البروكسيات الفائقة المشتركة في كل RNO. وهذا يقلل عدد عناوين IP الموثوقة إلى ستة. ومع ذلك، يؤدي ذلك إلى حدوث مشكلة في تنظيم جودة الخدمة على المسار من الجامعة إلى الوكيل في RNO.

ملاحظة: لا تعمل خطوط اتصال نظام المجموعة البينية ل Cisco CallManager حاليا من خلال وكيل H.323 لأن إرسال إشارات نظام المجموعة البينية ليس H.225 أصلي.

تنظيم دخول جودة الخدمة هو حل بديل. يتم إنشاء حدود الثقة عند النقطة التي يتصل فيها الحرم الجامعي ب RNO بهذا التصميم. يتم تنظيم حركة المرور التي تدخل ARNet بواسطة ميزة معدل الوصول الملتزم (CAR) من Cisco IOS® عند هذا الحد. تشترك جامعة تستخدم ARNet ل VoIP بكمية معينة من عرض نطاق جودة الخدمة (QoS) في AARNet. وتقوم السيارة بعد ذلك بمراقبة حركة المرور التي تدخل "آرنيت". تحتوي حركة المرور الزائدة على أسبقية IP تم تمييزها إلى 0 إذا كان مقدار حركة مرور RTP مع أسبقية IP 5 يتجاوز النطاق الترددي المشترك.

يوضح هذا الرسم التخطيطي تكوين سيارة:



يوضح هذا المثال كيفية معالجة تكوين CAR لعملية ضبط النظام هذه:

```
                                                Interface a1/0.100
rate-limit input access-group 100 2400000 0 0 conform-action set-prec-transmit 5
                                                exceed-action set-prec-transmit 0

                                    access-list 100 permit udp any range 16384 32767 any range
                                                  precedence critical 32767 16384
```

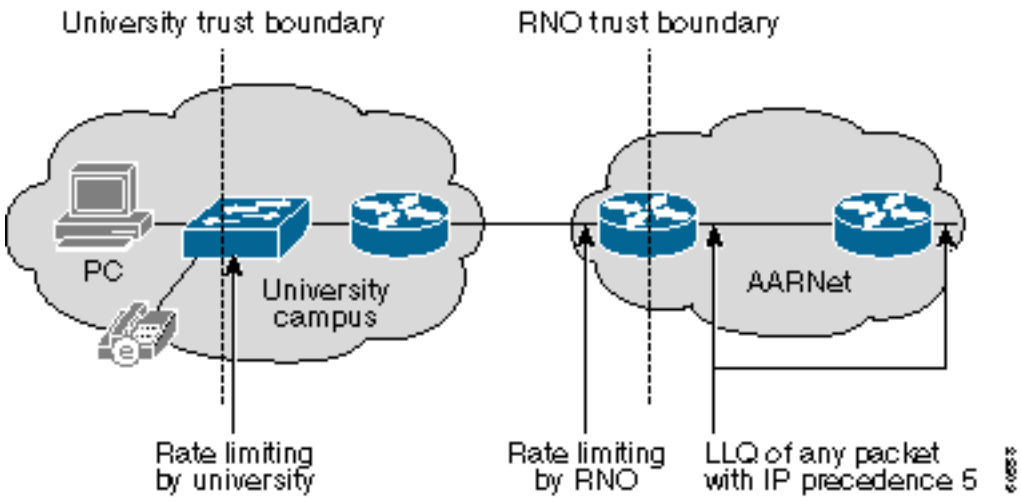
هذه بعض المزايا من نهج تكوين CAR:

• لم يعد المركز بحاجة إلى معالجة النهج. ويتم التعامل معها الآن عند حدود الثقة. لذلك، لا يلزم أن يعرف LLQ

الموجود في المركز حول عناوين IP الموثوق بها. يمكن أن تخضع أي حزمة ذات أسبقية IP رقم 5 في الأساسي بأمان إلى LLQ لأنها قد إجتازت النهج عند المدخل.

- لم يتم وضع أية افتراضات على بنية بروتوكول VoIP ومعداته وبروتوكولاته التي تختارها الجامعات الفردية. يمكن أن تختار الجامعة نشر بروتوكول بدء جلسة عمل (SIP) أو بروتوكول التحكم في عبارة الوسائط (MGCP) الذي لا يعمل مع وكلاء H.323. تتلقى حزم VoIP جودة الخدمة المناسبة في المركز طالما أنها تمتلك أسبقية IP قدرها 5.
- تتمتع جمهورية أفريقيا الوسطى بالمرونة في مواجهة هجمات رفض الخدمة (DoS). إن هجوم جودة الخدمة (QoS DoS) الذي يأتي من الجامعة لا يمكن أن يضر القلب. تحدد CAR الهجوم، والذي لا يمكن أن يولد حركة مرور أكثر مما هو موجود عندما يكون الحد الأقصى لعدد مكالمات VoIP المسموح بها نشطا.يمكن أن تتأثر إتصالات VoIP من أو إلى ذلك المجمع أثناء الهجوم. بيد ان الامر يرجع إلى كل جامعة على حدة في حماية نفسها داخليا. يمكن أن تشدد الجامعة قوائم التحكم في الوصول (ACL) الخاصة بالسيارات على الموجه حتى يكون لكل الشبكات الفرعية الخاصة ب VoIP باستثناء الشبكات الفرعية المحددة أسبقية IP المميزة.تحتوي كل مجموعة على حد ثقة داخلي عند النقطة التي يتصل فيها المستخدمون بشبكة LAN الجامعة في التصميم النهائي. تقتصر حركة المرور ذات أسبقية IP 5 التي تتلقاها حدود الثقة هذه على 160 كيلوبت/ثانية لكل منفذ محول، أو استدعاءان G.711 VoIP. تم وضع علامة على حركة المرور التي تتجاوز هذا المعدل. يتطلب تنفيذ هذا النظام محولات Catalyst 6500 switches أو أي شيء مماثل مع وظيفة تحديد المعدل.
- ويعمل توفير عرض النطاق الترددي في اللب على تبسيطه مع اشتراك كل جامعة في مقدار ثابت من عرض النطاق الترددي لجودة الخدمة. وهذا يجعل أيضا عملية فوترة جودة الخدمة بسيطة لأن كل جامعة تستطيع دفع رسوم شهرية ثابتة استنادا إلى الاشتراك في النطاق الترددي لجودة الخدمة.

نقطة الضعف الرئيسية في هذا التصميم هي أن حدود الثقة موجودة في موجه الجامعة، لذلك يجب أن تكون الجامعات قادرة على إدارة CAR بشكل صحيح. يتم سحب حدود الثقة مرة أخرى إلى RNO. تتولى المعدات التي تدار بواسطة RNO تنفيذ مهام الشرطة في التصميم النهائي. يتطلب هذا التصميم تحديد المعدل المستند إلى الأجهزة مثل المحول Catalyst 6000 switch أو معالج محرك خدمات الشبكات Cisco 7200 Network Services Engine (Cisco 7200 NSE-1)). ومع ذلك، فإنه يمنح ARNet و RNO سيطرة كاملة على تنظيم جودة الخدمة. يوضح هذا المخطط هذا التصميم:



تجزئة ودمج الارتباط

يتم نقل الصوت عبر بروتوكول VoIP فقط عبر دوائر ATM الظاهرية (VC) عالية السرعة نسبيا. لذلك، لا يتطلب وجود LFI. كما يمكن نقل بروتوكول VoIP عبر منتدى ترحيل الإطارات (FRF) أو خطوط الإيجار إلى الجامعات الريفية في المستقبل. يتطلب هذا آليات LFI مثل Multilink PPP (MLP) مع Interleave أو FRF.12.

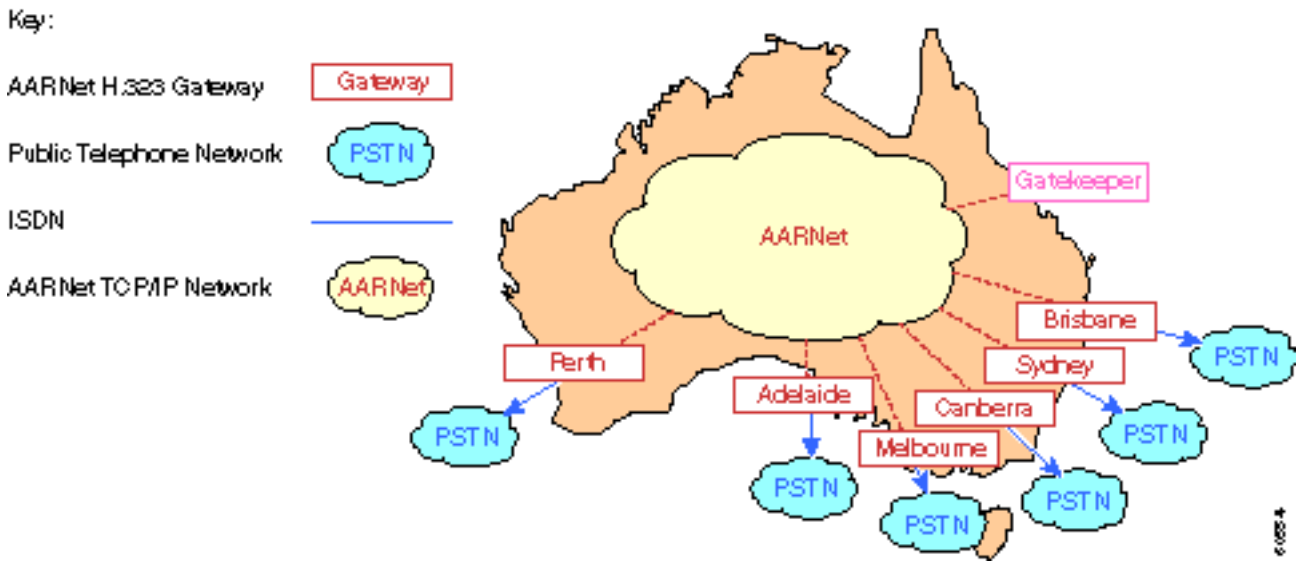
بوابات

يوجد نوعان من بوابات H.323 في AARNet:

- بوابة PSTN—PSTN إلى VoIP
- بوابة PABX—PABX إلى VoIP

ويمارس التمييز بين الشبكة الخاصة ببروتوكول الشجرة المتفرعة (PSTN) وبوابة بروتوكول الغلاف الآمن (PABX) وظائفه بشكل رئيسي. توفر بوابات PSTN الاتصال ب PSTN. تقوم بوابات PABX بتوصيل PABX بجامعة بالنظام الأساسي لبروتوكول VoIP. يعمل نفس المربع المادي ككل من PSTN وبوابة PABX في العديد من الحالات. هناك حاليا 31 بوابة في حل خدمة IP الهاتفية لوحدة التحكم في الوصول. معظم هذه البوابات هي خوادم الوصول العام Cisco AS5300. والعبارات الأخرى هي موجهات سلسلة 3600 من Cisco أو موجهات سلسلة 2600 من Cisco. ومن المتوقع إضافة عشر بوابات إضافية كحد أدنى خلال الربع الثاني من العام الجاري. وحملت شركة AARNet حوالي 145 000 مكالمة هاتفية عبر بروتوكول الإنترنت في نيسان/أبريل 2001.

قامت ARNet بنشر بوابات H.323 المتصلة ببروتوكول PSTN في معظم المدن الرئيسية، كما يوضح هذا المخطط:



يمكن للجامعات إستخدام هذه البوابات لإجراء مكالمات صادرة إلى PSTN. يجب على الجامعات الاحتفاظ بشبكاتها الخاصة للمكالمات الواردة لأنها غير مدعومة حاليا. يمكن لشركة AarnEt التفاوض على سعر تنافسي للغاية مع شركة النقل بسبب حجم المكالمات التي تمر عبر هذه البوابات. كما يمكن إيقاف المكالمات عند أكثر النقاط توفيرا للتكلفة. على سبيل المثال، يمكن لشخص في سيدني يتصل برقم بيرث إستخدام بوابة بيرث، ولا يتم تحميله سوى تكلفة مكالمة محلية. وهذا يعرف أيضا باسم "Tail End Hop off" (TEHO).

يتم نشر برنامج حماية بوابة واحد لإجراء حل E.164 لعنوان IP. يتم إرسال جميع المكالمات إلى PSTN إلى "حارس البوابة"، والذي يرجع بعد ذلك عنوان IP الخاص بأكثر البوابة ملاءمة. ارجع إلى أقسام خطط الطلب وبرنامج حماية البوابة للحصول على مزيد من المعلومات التفصيلية حول حراس البوابات.

إعداد الفواتير والمحاسبة

تستخدم بوابات PSTN RADIUS والمصادقة والتخويل والمحاسبة (AAA) لأغراض الفوترة. تقوم كل مكالمة من خلال بوابة بإنشاء سجل تفاصيل المكالمة (CDR) لكل مرحلة اتصال. يتم نشر وحدات CDR هذه إلى خادم RADIUS. يحدد عنوان IP الخاص ب Cisco CallManager في CDR الجامعة بشكل فريد ويضمن فوترة الطرف الصحيح.

أمان البوابة

وتشكل حماية بوابات "الشبكات الخاصة" من الهجمات والاحتيال بسبب رفض الخدمة مصدر قلق كبير. يتوفر عملاء H.323 على نطاق واسع. يتم تجميع Microsoft NetMeeting مع نظام التشغيل Microsoft Windows 2000، لذلك يكون من السهل نسبيا للمستخدم غير الفني إجراء مكالمات مجانية عبر هذه البوابات. تكوين قائمة تحكم في الوصول (ACL) واردة تسمح بإرسال إشارات H.225 من عناوين IP الموثوق بها لحماية هذه البوابات. يعاني هذا الأسلوب من مشكلات قابلية التطوير نفسها التي يصفها قسم جودة الخدمة. يتزايد عدد الإدخالات في قائمة التحكم بالوصول

(ACL) كلما زاد عدد نقاط النهاية H.323 الموثوق بها.

يقدم وكلاء H.323 بعض الراحة في هذه المنطقة. تحتاج قوائم التحكم في الوصول (ACLs) للعبارة إلى السماح بعنوان IP واحد لكل مجمع جامعي إذا مرت جميع المكالمات عبر بوابة PSTN عبر وكيل مجمع. من المفضل وجود عنوانين ل IP كوكيل متكرر في معظم الحالات. حتى مع الوكلاء، يمكن أن تحتوي قائمة التحكم في الوصول (ACL) على أكثر من 100 إدخال.

يجب حماية الوكيل عبر قوائم التحكم في الوصول (ACL) نظرا لأنه يمكن لأي H.323 إعداد مكالمة من خلال الوكيل. يجب أن تسمح قائمة التحكم في الوصول (ACL) للوكيل بأجهزة H.323 المحلية كما تتطلب السياسة المحلية نظرا لأن هذا يتم على أساس كل مجمع.

يجب تضمين عناوين IP الخاصة بمنفذي Cisco CallManager في قوائم التحكم في الوصول للبوابة إذا كان أحد الجامعات يريد السماح فقط للمكالمات من هواتف IP باستخدام بوابات PSTN ل ArnEt. لا تقوم الوكلاء بإضافة أي قيمة في هذه الحالة. يعد عدد إدخالات قائمة التحكم في الوصول (ACL) المطلوبة في الاتجاهين.

لاحظ أنه لا يلزم تمرير مكالمات هاتف إلى IP داخل مجمع IP عبر الوكيل.

خطط الطلب

إن خطة طلب الصوت عبر بروتوكول الإنترنت (VoIP) الحالية واضحة ومباشرة. يمكن للمستخدمين وضع هذين النوعين من المكالمات من منظور بوابة نقل الصوت عبر بروتوكول الإنترنت (VoIP):

- اتصل هاتفيا في حرم جامعي مختلف ولكن في نفس الجامعة.
- اتصل بهاتف أو هاتف في جامعة أخرى.

تعكس نظائر طلب البوابة حقيقة وجود نوعين فقط من المكالمات. هناك بشكل أساسي نوعان من نظراء اتصال VoIP، كما يوضح المثال التالي:

```
dial-peer voice 1 voip
…destination-pattern 7
session-target ipv4:x.x.x.x

dial-peer voice 1 voip
……destination-pattern 0
session-target ras
```

يتم إستخدام نظير الطلب الأول إذا قام شخص ما باستدعاء الملحق 7... في مجمع آخر في هذا المثال. يتم توجيه هذه المكالمة مباشرة إلى عنوان IP الخاص بالبوابة البعيدة. بما أنه قد تم تجاوز برنامج حماية البوابة، لم يتم إجراء "التحكم بإذن دخول المكالمة" (CAC).

يتم إستخدام نظير الطلب الثاني عندما تكون المكالمة لرقم PSTN. يمكن أن يكون هذا أحد العنصرين التاليين:

- عدد الهاتف في PSTN
- رقم هاتف بروتوكول الشجرة المتفرعة (PSTN) المؤهل بالكامل في جامعة مختلفة

يتم إرسال الاستدعاء إلى برنامج حماية البوابة بواسطة رسالة طلب قبول (ARQ) في الحالة الأولى. ترجع حماية البوابة عنوان IP الخاص بأفضل بوابة PSTN في رسالة تأكيد الإدخال (ACF).

يتم إرسال المكالمة أيضا إلى "حارس البوابة" من خلال رسالة ARQ في الحالة الثانية. ومع ذلك، ترجع حماية البوابة رسالة ACF بعنوان IP الخاص بوابة VoIP في الجامعة التي تتلقى المكالمة.

بواب

تشغل AARNet حاليا حارس بوابة واحد. والغرض الوحيد من برنامج حماية البوابة هذا هو تنفيذ توجيه المكالمات في

شكل E.164 إلى تحليل عنوان IP. لا يقوم برنامج حماية البوابة بتنفيذ CAC. يحد عدد خطوط اتصال PABX المتصلة بالبوابات من عدد المكالمات المتزامنة. يوفر عرض النطاق الترددي الأساسي لجميع خطوط الاتصال المستخدمة في وقت واحد. يتغير هذا مع بدء تشغيل خدمة IP الهاتفية في ACU وجامعات أخرى. لا يوجد حد طبيعي لعدد مكالمات VoIP المتزامنة التي يمكن الحصول عليها من أو إلى مجمع معين في هذه البيئة الجديدة. يمكن زيادة الاشتراك في النطاق الترددي المتاح لجودة الخدمة إذا تم بدء العديد من المكالمات. قد تعاني جميع المكالمات من ضعف الجودة في ظل هذه الحالة. أستخدم برنامج حماية البوابة لتوفير CAC.

تضفي الطبيعة الموزعة والحجم المحتمل للشبكة الصوتية للجامعة نفسها على بنية برنامج حماية البوابة الموزعة. أحد الحلول الممكنة هو تصميم بوابات هرمية من مستويين تحتفظ كل جامعة فيها ببوابتها الخاصة. تتم الإشارة إلى "حارس بوابة الجامعة" هذا كحارس بوابة من الطبقة 2. تقوم ArnEt بتشغيل حارس *بوابة دليل* يشار إليه باسم "حارس بوابة من الطبقة 1".

يجب على الجامعات إستخدام هذا النهج ثنائي المستويات لاستخدام برنامج حماية البوابة لتوجيه المكالمات بين مجموعات Cisco CallManager. يقوم برنامج حماية البوابة بتوجيه المكالمات استنادا إلى ملحق مكون من 4 أو 5 أرقام في هذا السيناريو. وكل جامعة تحتاج إلى حارس لها. وذلك لأن نطاقات الامتداد تتداخل بين الجامعات نظرا لأنها مساحة عنوان تتم إدارتها محليا.

يقوم حراس بوابات المستوى الثاني في الجامعة بتنفيذ CAC للمكالمات من وإلى تلك الجامعة فقط. كما أنها تنفذ دقة E.164 للمكالمات بين حرم الجامعة فقط. يتم توجيه المكالمة من قبل برنامج حماية البوابة للطبقة 2 إلى برنامج حماية البوابة للطبقة 1 من خلال رسالة طلب موقع (LRQ) إذا اتصل شخص ما بهاتف بروتوكول الإنترنت في جامعة أخرى أو اتصل ب PSTN من خلال بوابة ARNet. تتم إعادة توجيه LRQ إلى مسؤول بوابة الطبقة 2 في تلك الجامعة إذا كان الاتصال لجامعة أخرى. بعد ذلك، يقوم هذا المسؤول عن البوابة بإرجاع رسالة ACF إلى مسؤول بوابة الطبقة 2 في الجامعة التي تنشأ فيها المكالمة. يقوم كل من بوابات الطبقة 2 بتنفيذ CAC. لا تقوم بمتابعة المكالمة إلا إذا كان هناك نطاق ترددي كاف متوفر في كل من منطقتي الاتصال والمطالبة.

يمكن ل AarnEt أن تختار معاملة بوابات ARNet PSTN مثل تلك الخاصة بأي جامعة. يتولى حراس الصف الثاني الخاص بهم العناية بهم. كما يمكن أن يعمل برنامج حماية البوابة من الطبقة 1 كبرنامج حماية للبوابات من الطبقة 2 لهذه البوابات إذا سمح الحمل والأداء.

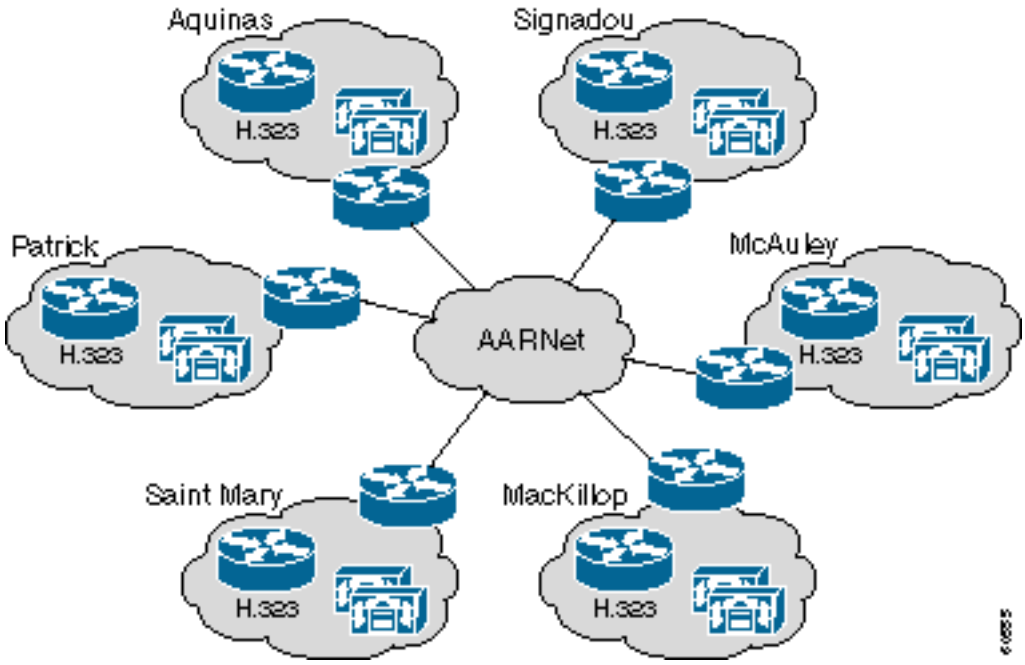
يجب تكرار كل من بوابات البوابات (بما في ذلك "حارس دليل AARNet") لأن البوابات تشكل مكونا هاما. تحتاج كل جامعة إلى حارسي بوابين. من الممكن أن يكون لبوابات Cisco IOS بوابات بديلة، كما في حالة برنامج Cisco IOS الإصدار 12.0(7)T. مهما، هذا لا يساند حاليا cisco CallManager أو أي آخر طرف ثالث H.323 أداة. لا تستخدم هذه الميزة في الوقت الحالي. أستخدم بدلا من ذلك حلا بسيطا قائما على بروتوكول الموجه الاحتياطي الفعال (قائما على HSRP). وهذا يتطلب أن يجلس كل من مسئولي البوابة على شبكة IP الفرعية نفسها. يحدد HSRP أي برنامج حماية البوابة نشط.

شبكة IP ACU الهاتفية

يوضح هذا الجدول العدد التقريبي لهواتف IP المثبتة في حرم وحدة التحكم بالوصول (ACU):

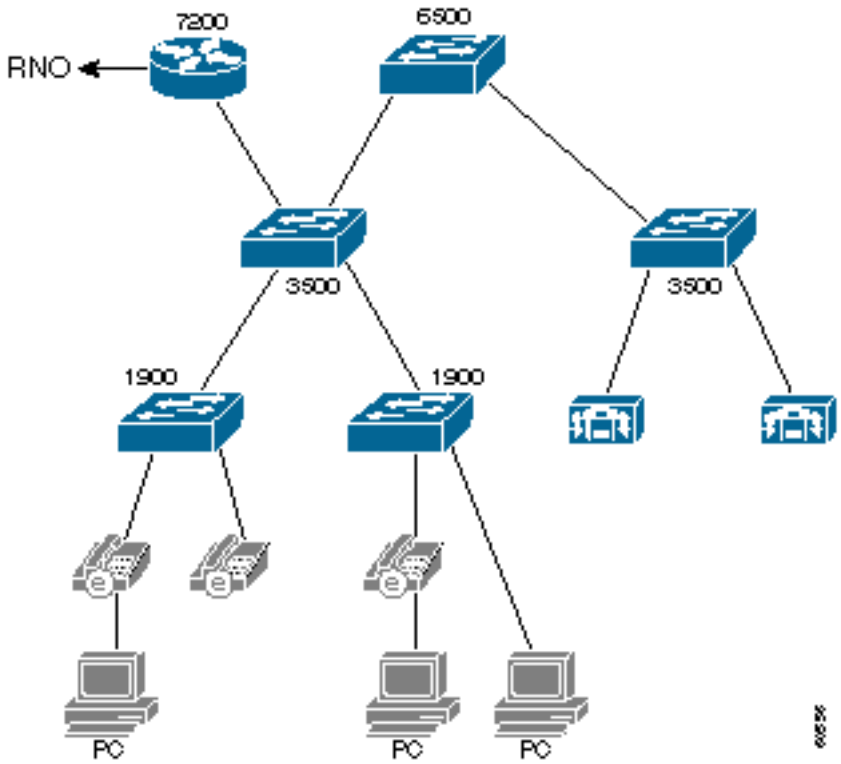
حرم الجامعة	مدينة	هواتف بروتوكول الإنترنت التقريبية
جبل سانت ماري	ستراثفيلد	400
ماكيلوب	شمال سيدني	300
باتريك	ملبورن	400
الأكويني	بالارات	100
سينادو	كانبرا	100
ماكاولي	بريزبان	400
	الإجمالي:	***1700***

قامت وحدة التحكم في الوصول (ACU) مؤخرا بنشر حل خدمة IP الهاتفية. يتكون الحل من مجموعة من إثنين من Cisco CallManager، وبوابة Cisco 3640 في كل مجمع، وهواتف بروتوكول الإنترنت (IP). تتصل ARNet بالحرم. يوضح هذا المخطط المخطط المخطط المخطط الهيكلي عالي المستوى والمكونات المختلفة لشبكة ACU IP الهاتفية:



طوبولوجيا شبكة ACU

يوضح هذا المخطط مجمع ACU نموذجي. يحتوي كل مجمع على ثلاث طبقات من محولات Catalyst Switches. تحتوي خزانة أسلاك الأسلاك على محولات Catalyst 1900 القديمة. المادة حفازة 1900 ربطت مفتاح مرة أخرى إلى المادة حفازة 3500xl مفتاح بوسائل من موسع إطار. والتي تتصل مرة أخرى بمحول Catalyst 6509 واحد بواسطة شبكة جيجابت إيثرنت (GE). يقوم موجه VXR واحد من Cisco 7200 بتوصيل المجمع ب ARNet بواسطة ATM VC ب RNO المحلي.



يختلف أسلوب الاتصال ب RNO إختلافا طفيفا من دولة إلى أخرى، كما يوضح هذا الجدول. تعتمد فيكتوريا على IP

التقليدي عبر ATM (RFC 1577). تحتوي وحدات RNO الأخرى على إعداد PVC مستقيم باستخدام تضمين RFC 1483. يمثل "فتح أقصر مسار أولا (OSPF)" بروتوكول التوجيه المستخدم بين وحدة التحكم في الوصول (ACU) و RNOs.

حرم الجامعة	الحالة	الاتصال ب RNO	بروتوكول التوجيه
جبل سانت ماري	إن إس دبليو	RFC 1483 PVC	بروتوكول أقصر مسار أولاً (OSPF)
ماكيلوب	إن إس دبليو	RFC 1483 PVC	بروتوكول أقصر مسار أولاً (OSPF)
باتريك	فيك	RFC 1577 IP التقليدي عبر ATM	بروتوكول أقصر مسار أولاً (OSPF)
الأكويني	فيك	RFC 1577 IP التقليدي عبر ATM	بروتوكول أقصر مسار أولاً (OSPF)
سينادو	فعل	RFC 1483 PVC	بروتوكول أقصر مسار أولاً (OSPF)
ماكاولي	QLD	RFC 1483 PVC	بروتوكول أقصر مسار أولاً (OSPF)

المادة حفازة sery 1900 يساند مفتاح trunking على الوصلات فقط. لذلك، ال ip هاتف و pcS كل في واحد كبير VLAN. في الواقع، الحرم الجامعي بأكمله هو شبكة VLAN كبيرة ومجال بث. يتم إستخدام شبكات IP الفرعية بسبب العدد الكبير من الأجهزة. توجد هواتف IP على شبكة IP فرعية واحدة، كما توجد أجهزة الكمبيوتر على شبكة أخرى. يثق مركز ARNet بشبكة هاتف IP الفرعية، وتخضع حركة مرور البيانات من شبكة IP الفرعية هذه وإليها إلى LLQ.

يقوم الموجه Cisco 7200 بالتوجيه بين شبكات IP الفرعية الأساسية والثانوية. متعدد طبقات مفتاح سمة بطاقة (MSFC) في المادة حفازة 6500 مفتاح لا يستعمل حاليا.

يتضمن المحولات Catalyst 3500XL و Catalyst 6500 switches ميزات جودة الخدمة، ولكن لا يتم تمكينها حاليا.

جودة الخدمة في الحرم الجامعي

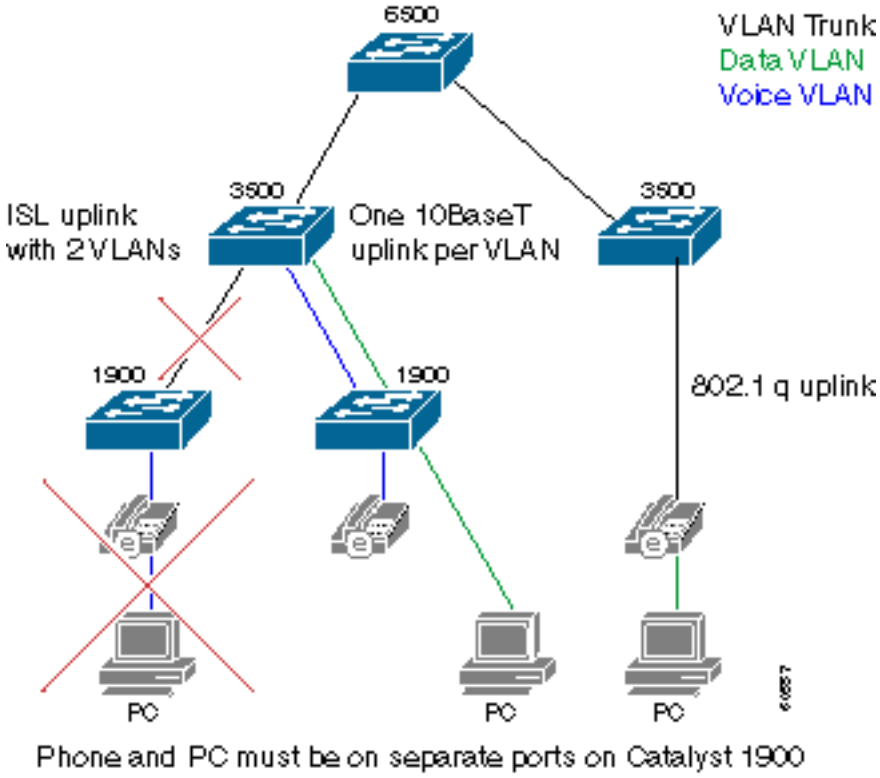
لا يتوافق تصميم المجمع الحالي مع إرشادات التصميم الموصى بها من Cisco لهاتف IP. هذه بعض المخاوف حول جودة الخدمة:

- مجال البث كبير جدا. حيث يمكن أن يؤثر الإرسال المفرط على أداء هواتف بروتوكول الإنترنت (IP)، والتي يجب

عليها معالجتها.

- لا تدعم محولات Catalyst 1900 جودة الخدمة. إذا تم توصيل هاتف IP وجهاز كمبيوتر شخصي بنفس منفذ المحول، يمكن إسقاط الحزم الصوتية إذا كان الكمبيوتر الشخصي يستلم البيانات بمعدل مرتفع.

قم بإعادة تصميم أجزاء من البنية التحتية للمجمع لتحقق تحسينات ملحوظة. ترقية الأجهزة غير مطلوبة. يوضح هذا الرسم التخطيطي المبادئ الكامنة وراء إعادة التصميم الموصى بها:



يجب تقسيم المجمع إلى شبكة VLAN صوتية وشبكة VLAN للبيانات. يجب أن تتصل الهواتف وأجهزة الكمبيوتر الشخصية التي تتصل بمحول Catalyst 1900 switch الآن بمنافذ مختلفة لتحقيق الفصل بين شبكات VLAN. تتم إضافة وصلة إضافية من كل محول من محولات Catalyst 1900 إلى محول Cisco 3500XL switch. واحد من الوصلين عضو من الصوت VLAN. الوصلة الأخرى عضو من المعطيات VLAN. لا تستخدم توصيل InterSwitch Link (ISL) كبديل لوحدتين. وهذا لا يوفر حركة مرور البيانات والصوت بقوائم انتظار منفصلة. كما يجب تحويل روابط GE من المحول Catalyst 3500XL switch إلى المحول Catalyst 6000 switch إلى خطوط اتصال 802.1q حتى يمكن حمل كل من الصوت والبيانات لشبكة VLAN عبر هذا المحول الأساسي.

يتلقى ميناء على المادة حفازة 3500xl مفتاح أن يكون في المعطيات VLAN تقصير صنف الخدمة (CoS) من صفر. ميناء أن يكون عضو من الصوت VLAN يتلقى تقصير CoS من 5. ونتيجة لذلك، يتم ترتيب حركة مرور الصوت بشكل صحيح بمجرد وصولها إلى مركز Catalyst 3500 أو Catalyst 6500. تختلف تكوينات منافذ محول Catalyst 3500 QoS بشكل طفيف حسب منفذ محول VLAN الذي يكون عضوا، كما يوضح هذا المثال:

```
Interface fastethernet 0/1
description Port member of voice VLAN
switchport priority 5
switchport access vlan 1

Interface fastethernet 0/2
description Port member of data VLAN
switchport priority 0
switchport access vlan 2
```

يمكنك توصيل جهاز كمبيوتر بمنفذ المحول الخلفي على هاتف IP في الحالة النادرة التي تتصل فيها هواتف IP مباشرة بمحول Catalyst 3500XL. تتصل هواتف IP بالمحول عن طريق خط اتصال 802.1Q في هذه الحالة. هذا يسمح صوت وبيانات ربط أن يسافر على VLANs منفصل، وأنت يستطيع منحت ربط ال يصح مساعد عند مدخل. استبدلت مادة حفازة 1900 مفتاح مع مادة حفازة 3500xl مفتاح أو آخر QoS قادر مفتاح بما أن هم يصلون إلى نهاية الحياة.

ويصبح هذا المخطط بعد ذلك الطريقة القياسية لتوصيل هواتف IP وأجهزة الكمبيوتر الشخصية بالشبكة. يوضح هذا السيناريو تكوين جودة خدمة المحول Catalyst 3500XL:

```
Interface fastethernet 0/3
description Port connects to a 79xx IPhone
switchport trunk encapsulation dot1q
switchport priority extend 0
```

أخيرا، يجب أن يكون لكلا المنفذين المتصلين بمنفذي Cisco CallManager ترميز CoS ترميزا ثابتا إلى 3. يعمل Cisco CallManager على تعيين أسبقية IP على 3 في جميع حزم إرسال الإشارات الصوتية. مهما، ال link من ال cisco CallManager إلى المادة حفازة 3500xl مفتاح لا يستعمل 801.1p. لذلك، فرضت قيمة COs في المفتاح كما يوضح هذا مثال:

```
Interface fastethernet 0/1
description Port member of voice VLAN
switchport priority 3
switchport access vlan 1
```

تتمثل العقبة الرئيسية التي تواجه هذا التصميم في أنه يلزم توفر منفذين للمحول في "سطح المكتب". قد يتطلب مجمع Patrick 400 منفذ محول إضافي ل 400 هاتف بروتوكول الإنترنت. يجب نشر محولات Catalyst 3500XL الإضافية إذا لم تكن المنافذ الكافية متوفرة. يتطلب فقط واحد مادة حفازة 3500xl مفتاح ميناء ل كل إثنان مفقود مادة حفازة 1900 مفتاح ميناء.

تتضمن محولات Catalyst 6500 الحالية لوحدة التحكم في الوصول إمكانيات جودة الخدمة، ولكنها لا يتم تمكينها حاليا. هذه الوحدات النمطية موجودة في محول ACU Catalyst 6000 switch مع قدرات قوائم الانتظار هذه:

فتحة	وحدة	المنافذ	قوائم انتظار Rx	قوائم انتظار Tx
1	WS-X6K-SUP1A-2GE	2	1p1q4t	1p2q2t
3	WS-X6408-GBIC	8	1q4t	2q2t
4	WS-X6408-GBIC	8	1q4t	2q2t
5	WS-X6248-RJ-45	48	1q4t	2q2t
15	WS-F6K-MSFC	0	—	—

أكمل الخطوات التالية لتنشيط ميزات جودة الخدمة المناسبة على المحول Catalyst 6000 switch:

1. اطلب من المحول توفير جودة الخدمة لكل شبكة محلية ظاهرية (VLAN) باستخدام هذا الأمر:
```
Cat6K>(enable)set port qos 1/1-2,3/1-8,4/1-8 vlan-based
```

2. أخبرت المفتاح أن يثق ال coS قيمة يستلم من المادة حفازة 3500xl مفتاح مع هذا أمر:
```
Cat6K>(enable)set port qos 1/1-2,3/1-8,4/1-8 trust trust-cos
```

يجب تعيين CoS الآن على تعيين نقطة كود الخدمات (DSCP) المميزة. وهذا مطلوب لأن المحول Catalyst 6000 switch يعيد كتابة قيمة DSCP في رأس IP استنادا إلى قيمة CoS المستلمة. يجب أن يكون لحزم إرسال إشارات VoIP CoS من 3، معاد كتابتها باستخدام DSCP من 26) AF31). يجب أن تحتوي حزم RTP على CoS من 5، معاد كتابتها باستخدام DSCP من 46) EF). قم بإصدار هذا الأمر:

```
Cat6K>(enable)set qos cos-dscp-map 0 8 16 26 32 46 48 56
```

أستخدم هذا المثال للتحقق من تعيين CoS إلى DSCP.

```
Cat6K> (enable) show qos map run COs-DSCP-map
:CoS - DSCP map
CoS DSCP
---- ---
  0   0
  8   1
 16   2
 26   3
 32   4
 46   5
 48   6
 56   7
```

قم بتكوين MSFC للتوجيه بين شبكات IP الفرعية المختلفة.

جودة الخدمة في RNO

لا يتوافق تصميم RNO الحالي مع إرشادات التصميم الموصى بها من Cisco لهاتف IP. هذه المخاوف موجودة فيما يتعلق بجودة الخدمة:

- لا يتم تطبيق LLQ على موجه WAN سلسلة Cisco ACU 7200.
- تتصل مجمعات باتريك وأكويناس بشبكة RNO من خلال أجهزة ATM المحولة (LLQ .(SVCs غير مدعوم على SVCs.

يعمل موجه Cisco 7200 السريع المتصل بشبكة الإيثرنت على توصيل مجمع المباني ب RNO بواسطة إرتباط E4 ATM بسرعة 34 ميجابت في الثانية. من المحتمل أن تصطف حركة المرور في قائمة الانتظار الصادرة على إرتباطات 34 م بسبب عدم تطابق السرعة التي تبلغ 4 م مقابل 100 م. لذلك من الضروري اعطاء الأولوية لحركة المرور الصوتية. إستخدام LLQ. تكوين الموجه Cisco 7200 مماثل لهذا المثال:

```
class-map VoiceRTP
match access-group name IP-RTP

policy-map RTPvoice
     class VoiceRTP
     priority 10000

interface ATM1/0.1 point-to-point
       description ATM PVC to RNO
                pvc 0/100
          tx-ring-limit 3
service-policy output RTPvoice

ip access-list extended IP-RTP
     deny ip any any fragments
permit udp any range any range 16384 32768 precedence critical
```

يجب أن يكون النطاق الترددي المخصص ل LLQ *N x 24 كيلوبت لكل ثانية*، حيث يمثل N عدد مكالمات G.729 المتزامنة.

قم بإعداد بطاقة PVC واحدة من كل موجه من موجهات Patrick و Aquinas Cisco 7200 إلى موجه ArnEt. لا تدعم أجهزة ATM SVC في Victoria RNO تقنية LLQ، لأنها تستند إلى بروتوكول IP التقليدي عبر ATM (RFC 1577). وبوسع الجامعات الأخرى في منطقة بيرنو في فيكتوريا أن تستمر في إستخدام معيار RFC 1577 في الوقت الحالي. ومع ذلك، استبدل في نهاية المطاف البنية الأساسية التقليدية لبروتوكول IP عبر ATM.

بوابات

تحتوي كل حرم من حرم وحدة التحكم في الوصول على موجه Cisco 3640 الذي يعمل كبوابة H.323. تتصل هذه البوابات ب PSTN بواسطة ISDN. يعتمد عدد واجهات المعدل الأولي (PRIs) والقنوات b على حجم المجمع. يسرد هذا الجدول عدد قنوات PRI و B لكل مجمع:

حرم الجامعة	كمية PRI	كمية قناة B
جبل سانت ماري	2	30
ماكيلوب	2	50
باتريك	2	50
الأكويني	1	20
سينادو	1	20
ماكاولي	1	30

يتم إستخدام هذه البوابات كبوابات ثانوية فقط ل DOD (الطلب الخارجي المباشر). تعد بوابات AARNet هي البوابات الأساسية. يتم إستخدام بوابات وحدة التحكم بالوصول (ACU) ل DID (الطلب الداخلي المباشر).

خطة الطلب

تستند خطة الطلب إلى أرقام ملحق من 4 أرقام. الملحق هو أيضا آخر أربعة أرقام من الرقم DID. يسرد هذا الجدول نطاقات الامتداد وأرقام DID لكل مجمع:

حرم الجامعة	إمتدادا	فعلت
جبل سانت ماري	9xxx	9xxx 9764 02
ماكيلوب	8xxx	8xxx 9463 02
باتريك	3xxx	3xxx 8413 03
الأكويني	5xxx	5xxx 5330 03
سينادو	×××	2xxx 6123 02
ماكاولي	7xxx	7xxx 354 07

يؤدي إدخال `num-exp` بسيط على البوابات إلى اقتطاع رقم DID إلى الملحق المكون من 4 أرقام قبل تمريره إلى Cisco CallManager. على سبيل المثال، تحتوي بوابة حرم جامعي باتريك على هذا الإدخال:

```
...num-exp 84133... 3
```

يطلب المستخدمون صفر لتحديد سطر خارجي. يتم تمرير هذا صفر بادئ إلى البوابة. يقوم نظير طلب POTS الأحادي بتوجيه الاستدعاء إلى منفذ ISDN استنادا إلى صفر البادئة.

```
Dial-peer voice 100 pots
destination-pattern 0
```

```
direct-inward-dial
port 2/0:15
```

تستخدم المكالمات الواردة إدخال num-exp هذا لتحويل رقم الطرف الذي تم إستدعائه إلى ملحق من 4 أرقام. بعد ذلك تتطابق المكالمة مع كلا نظامي طلب VoIP. بناء على التفضيل الأقل، فإنه يفضل هذا المسار إلى المشترك في Cisco CallManager:

```
dial-peer voice 200 voip
preference 1
...destination-pattern 3
session target ipv4:172.168.0.4

dial-peer voice 201 voip
preference 2
...destination-pattern 3
session target ipv4:172.168.0.5
```

Cisco CallManager

تحتوي كل مجموعة على نظام مجموعة يتكون من خادمين من Cisco CallManager. تعد خوادم Cisco CallManager بمثابة مزيج من خادم تقارب الوسائط طراز 7835 (MCS-7835) وخادم تقارب الوسائط طراز 7820 (MCS-7820). قام كلا الخادمين بتشغيل الإصدار 3.0(10) في وقت نشر هذا المنشور. أحدهما Cisco CallManager هو *الناشر* والآخر Cisco CallManager هو *المشترك*. يعمل المشترك كمدير المكالمات الأساسي من Cisco لجميع هواتف IP. يسرد هذا الجدول الأجهزة التي تم نشرها في كل مجمع:

حرم الجامعة	النظام الأساسي	مديرو المكالمات
جبل سانت ماري	MCS-7835	2
ماكيلوب	MCS-7835	2
باتريك	MCS-7835	2
الأكويني	MCS-7820	2
سينادو	MCS-7820	2
ماكاولي	MCS-7835	2

يتم تكوين كل مجموعة باستخدام منطقتين:

- واحد للمكالمات داخل الكارامبوس (G.711)
- واحد للمكالمات بين المجمعات (G.729)

لا تعد CAC المستندة إلى الموقع مناسبة لوحدة التحكم بالوصول (ACU) لأن جميع هواتف IP التي تخدمها كل مجموعة موجودة في مجمع واحد. هناك مزايا خاصة ب CAC المستندة إلى برنامج حماية البوابة للمكالمات بين الحرم الجامعي، ولكن هذا لم يتم تنفيذه حاليا. غير أن هناك خططا للقيام بذلك في المستقبل القريب.

يتم تكوين كل Cisco CallManager باستخدام 22 بوابة H.323. يتكون هذا المحول من قنوات اتصال بين المجموعات إلى مجموعات Cisco CallManager الخمس الأخرى، وستة بوابات PSTN من ARNet، وبوابة وحدة تحكم في الوصول (ACU) واحدة في كل مجمع.

نوع جهاز H.323	الكمية
Intercampus CallManager	2 × 5 = 10
بوابة ARNet PSTN	6
بوابة ACU PSTN	6
الإجمالي:	***22***

يتم إستخدام قوائم المسارات ومجموعات المسارات لتصنيف بوابات PSTN. على سبيل المثال، يوضح هذا الجدول كيفية إستخدام المكالمات من Patrick Cisco CallManager في ملبورن إلى PSTN في سيدني للبوابات الأربع لربط المكالمات معا مع مجموعة مسار.

البوابة	أولوية
آرنت سيدني	1
ACU سيدني	2
آرنيت ملبورن	3
إتحاد ملبورن لكرة السلة	4

يتم تكوين Cisco CallManager باستخدام 30 نمط مسار تقريبا، كما يوضح هذا الجدول. ويتم تصميم أنماط المسار بحيث تكون هناك تطابقات محددة لجميع الأرقام الأسترالية المحلية. بهذه الطريقة، لا يحتاج المستخدمون إلى الانتظار حتى تنتهي صلاحية المهلة بين الخانات قبل أن يبدأ Cisco CallManager المكالمة. يتم إستخدام حرف البدل "!" فقط في نمط المسار للأرقام الدولية. يجب على المستخدمين الانتظار حتى تنتهي صلاحية المهلة بين الأرقام (الافتراضية 10 ثوان) قبل تقدم الاستدعاء عندما يطلبون وجهة دولية. كما يمكن للمستخدمين إضافة نمط المسار "0.0011!#". يمكن للمستخدمين بعد ذلك إدخال "#" بعد آخر رقم للإشارة إلى اكتمال الرقم المطلوب إلى Cisco CallManager. ويسرع هذا الإجراء من الاتصال الدولي.

نمط المسار	الوصف
xxxxx[2-9].0	مكالمة محلية
0.00	مكالمة طوارئ - إذا نسي المستخدم الطلب 0 للخط الخارجي
0.000	مكالمة طوارئ
0.013	مساعدة الدليل
0.1223	—
0.0011!	المكالمات الدولية
0.02xxxxxx	المكالمات إلى نيو ساوث ويلز
0.03xxxxxx	نداءات إلى فيكتوريا
0.04xxxxxx	المكالمات للهواتف المحمولة
0.07xxxxxx	دعوات إلى كوينزلاند
0.086xxxxx	النداءات إلى أستراليا الغربية
0.08xxxxx	النداءات الموجهة إلى جنوب أستراليا والمنطقة الشمالية
xxxxx[8-9]0.1	يدعو إلى 1800 xxx و 1900 xxxx
0.1144X	طوارئ
0.119[4-6]	الوقت والجو
0.1245X	دليل
xxx[1-9]0.13	يدعو إلى أرقام 13xxxx
0.130xxxxx	يدعو إلى أرقام

1300 xxxx	
مكالمات Intercluster إلى Signado	XX[0-1]2
اتصال Intercluster ب Patrick	XX[0-4]3
إجتماع عنقودي يدعو إلى الأكوينات	XX[3-4]5
Intercluster يتصل ب McAuley	XX[2-5]7
Intercluster يتصل ب MacKillop	xx[0-3]8
Intercluster يدعو إلى جبل سانت ماري	XX[3-4]9
Intercluster يدعو إلى جبل سانت ماري	XX[6-7]9

يمكن أن ينمو عدد البوابات ومجموعات المسارات وقوائم المسارات وأنماط المسارات التي تم تكوينها على ACU Cisco CallManager إلى عدد كبير. إذا تم نشر بوابة RNO جديدة، فيجب إعادة تكوين جميع مجموعات Cisco CallManager الخمس باستخدام بوابة إضافية. والأسوأ من ذلك، يلزم إضافة مئات البوابات إذا قامت وحدة التحكم في الوصول Cisco CallManager بتوجيه المكالمات عبر بروتوكول VoIP مباشرة إلى جميع الجامعات الأخرى وتجاوز PSTN بالكامل. من الواضح أن هذا لا يتدرج بشكل جيد.

الحل هو جعل Cisco CallManager Gatekeeper مضبوطا. يجب عليك فقط تحديث برنامج حماية البوابة عند إضافة بوابة جديدة أو Cisco CallManager في مكان ما في AARNet. يجب أن يكون لكل Cisco CallManager بوابة الحرم الجامعي المحلية فقط والجهاز المجهول الذي تم تكوينه عند حدوث ذلك. يمكنك التفكير في هذا الجهاز على أنه خط اتصال من نقطة إلى عدة نقاط. وهو يزيل ضرورة شبكات اتصال PPP المجمعة في نموذج خطة طلب Cisco CallManager. تشير مجموعة مسار واحدة إلى الجهاز المجهول كبوابة مفضلة وإلى البوابة المحلية كبوابة نسخ إحتياطي. يتم إستخدام بوابة PSTN المحلية لبعض المكالمات المحلية وأيضا لمكالمات الشبكة الخارجية العامة إذا أصبح برنامج حماية البوابة غير متاح. حاليا، الجهاز المجهول يمكن أن يكون إما InterCluster أو H.225، ولكن ليس كلاهما في نفس الوقت.

يحتاج Cisco CallManager إلى أنماط مسار أقل مع برنامج حماية البوابة مقارنة بما هو عليه الآن. من حيث المبدأ، لا يحتاج Cisco CallManager إلا إلى نمط مسار واحد من "!" يشير إلى برنامج حماية البوابة. في الواقع، يجب أن تكون الطريقة التي يتم بها توجيه المكالمات أكثر تحديدا لهذه الأسباب:

- يجب توجيه بعض المكالمات (مثل المكالمات إلى رقم 1-800 أو أرقام الطوارئ) من خلال بوابة محلية جغرافيا. شخص ما في ملبورن يقوم بإبلاغ الشرطة أو سلسلة مطاعم مثل بيتزا هت لا يريد أن يكون متصلا بالشرطة أو كوخ بيتزا في بيرث. يلزم وجود أنماط مسار محددة تشير مباشرة إلى بوابة PSTN للمجمع المحلي لهذه الأرقام.يمكن للجامعات التي تخطط لتنفيذ عمليات نشر خدمة IP الهاتفية في المستقبل أن تختار الاعتماد فقط على بوابات آرنت وعدم إدارة بواباتها المحلية الخاصة. يجب أن تحتوي هذه الأرقام على كود منطقة ظاهري تم تكليفه بواسطة Cisco CallManager قبل إرساله إلى "حماية البوابة" لجعل هذا التصميم يعمل للمكالمات التي يجب إسقاطها محليا. على سبيل المثال، يمكن أن يرتب Cisco CallManager رقم 003 للمكالمات من هاتف قائم على Melbourne إلى رقم بيتزا 800-1 Hut. وهذا يسمح لعامل البوابة بتوجيه المكالمة إلى بوابة ARNet المستندة إلى ملبورن. تتخطى البوابة 003 الرائدة قبل أن تقوم بوضع المكالمة في PSTN.
- أستخدم أنماط المسار ذات التطابقات المحددة لجميع الأرقام المحلية لتجنب انتظار المستخدم للمهلة بين الخانات قبل بدء الاستدعاء.

يوضح هذا الجدول أنماط المسار ل Cisco CallManager الذي يتم التحكم فيه بواسطة برنامج حماية البوابة:

نمط المسار	الوصف	طريق	بواب
0.[-2 9]xx xxx	مكالمة محلية	قائمة المسارات	آرنيت
0.00	مكالمة طوارئ	البوابة المحلية	None
0.000	مكالمة طوارئ	البوابة المحلية	None
0.013	مساعدة الدليل	البوابة المحلية	None
0.1223	—	البوابة المحلية	None
0.0011!	المكالمات الدولية	قائمة المسارات	آرنيت
0.0011!#	المكالمات الدولية	قائمة المسارات	آرنيت
0.0[2-4]xx xxxx	المكالمات إلى نيو ساوث ويلز، فيكتوريا، والهواتف الخلوية	قائمة المسارات	آرنيت
0.0[7-8]xx xxx	النداءات إلى اوستراليا الجنوبية، اوستراليا الغربية، والاقليم الشمالي	قائمة المسارات	آرنيت
0.1[8-9]xx xxx	يدعو إلى 1800 xxx و 1900 xxxx	البوابة المحلية	None
0.1144X	طوارئ	البوابة المحلية	None
0.114-[9 6]	الوقت والجو	البوابة المحلية	None
0.131-[9]xx x	يدعو إلى أرقام 13xxxx	البوابة المحلية	None
0.13	يدعو إلى	البوابة المحلية	None

0xxxxx	أرقام xxxx 1300		
[2-3]xxx	المكالمات إلى Signado	قائمة المسارات	ACU
5xxx	دعوات إلى الأكوينات	قائمة المسارات	ACU
[7-9]xxx	الاتصال بماكوولي، ماكيلوب، وجبل سانت ماري	قائمة المسارات	ACU

يقوم برنامج حماية البوابة بتوجيه المكالمات الدولية، التي لا يتم إرسالها من خلال البوابة المحلية. وهذا أمر هام لأن "ARNet" يمكنها نشر بوابات دولية في المستقبل. إذا تم نشر بوابة في الولايات المتحدة، يسمح تغيير بسيط في تكوين البوابات للجامعات بإجراء مكالمات إلى الولايات المتحدة وفقا للأسعار المحلية في الولايات المتحدة.

يقوم برنامج حماية البوابة بتوجيه المكالمات عبر نظام المجموعة البينية استنادا إلى ملحق وحدة التحكم بالوصول (ACU) المكون من 4 أرقام. تتداخل مساحة العنوان هذه على الأرجح مع جامعات أخرى. وهذا يفرض على وحدة التحكم في الوصول إدارة برنامج حماية البوابة الخاص بها واستخدام برنامج حماية البوابة AARNet كحارس *بوابة دليل*. يشير عمود Gatekeeper في هذا الجدول إلى ما إذا كان توجيه المكالمات يتم إجراؤه بواسطة "حارس بوابة ACU" أو "حارس بوابة AARNet".

ملاحظة: التحذير الوحيد باستخدام حل برنامج حماية البوابة المقترح هو أن الجهاز المجهول يمكن أن يكون حاليا إما بين نظام المجموعة أو H.225، ولكن ليس كلاهما في نفس الوقت. يعتمد Cisco CallManager على برنامج حماية البوابة لتوجيه المكالمات إلى كل من البوابات (H.225) وغيرها من Cisco CallManager (نظام المجموعة البينية) باستخدام التصميم المقترح. الحل البديل لهذه المشكلة إما أن لا تستخدم البوابة للتوجيه بين المجموعات أو أن تعامل جميع المكالمات عبر البوابة على أنها H.225. يعني الحل الأخير أنه قد لا تتوفر بعض الميزات الإضافية على مكالمات نظام المجموعة البينية.

البريد الصوتي

كانت وحدة التحكم في الوصول (ACU) مزودة بثلاثة خوادم للبريد الصوتي قائمة على نظام التشغيل Voice Repartee OS/2 مع لوحات هاتف Dialogic قبل الترحيل إلى خدمة IP الهاتفية. تتمثل الخطة في إعادة إستخدام هذه الخوادم في بيئة خدمة IP الهاتفية. عند تنفيذ هذا الإجراء، يتصل كل خادم تعويض ب Cisco CallManager عن طريق واجهة مكتب رسائل مبسطة (SMDI) وبطاقة Catalyst 6000 مزودة ب24 منفذا ومحطة صرف أجنبي (FXS). وهذا يوفر البريد الصوتي لثلاثة من المجمعات الست، مما يترك ثلاثة مجمعات بدون بريد صوتي. لا يمكن مشاركة خادم Repartee واحد بشكل صحيح بين المستخدمين على مجموعتي Cisco CallManager لأنه لا توجد طريقة لنشر مؤشر انتظار الرسائل (MWI) عبر خط اتصال H.323 لنظام المجموعة البينية.

قد تقوم وحدة التحكم في الوصول (ACU) بشراء ثلاثة خوادم Cisco Unity للمجمعات المتبقية. تستند هذه الخوادم إلى خوادم قليلة السمك، لذلك لا يلزم إستخدام أية بوابات. يسرد هذا الجدول حلول البريد الصوتي في حالة شراء ACU لخوادم البريد الصوتي الإضافية:

حرم الجامعة	نظام البريد الصوتي	البوابة
جبل سانت ماري	تعويض الصوت النشط	Catalyst 6000

		24-Port FXS
ماكيلوب	تعويض الصوت النشط	Catalyst 6000 24-Port FXS
باتريك	تعويض الصوت النشط	Catalyst 6000 24-Port FXS
الأكويني	Cisco Unity	—
سينادو	Cisco Unity	—
ماكاولي	Cisco Unity	—

تعمل خوادم البريد الصوتي الستة كجزر بريد صوتي معزولة في هذه الخطة. لا توجد شبكة للبريد الصوتي.

مصادر إعلامية

لا يتم حاليا نشر معالجات الإشارة الرقمية للأجهزة (DSP) في وحدة التحكم في الوصول (ACU). يستخدم المؤتمرات جسر المؤتمرات المستند إلى البرامج على Cisco CallManager. المؤتمرات بين المجموعات غير مدعومة حاليا.

التحويل البرمجي غير مطلوب حاليا. يتم إستخدام أجهزة فك التشفير G.711 و G.729 فقط، وهي مدعومة من قبل جميع الأجهزة الطرفية المنشورة.

دعم الفاكس والمودم

حركة مرور الفاكس والمودم غير مدعومة حاليا بواسطة شبكة IP الهاتفية لوحدة التحكم في الوصول. تخطط الجامعة لاستخدام بطاقة Catalyst 6000 ذات 24 منفذا FXS لهذا الغرض.

إصدارات البرامج

يسرد هذا الجدول إصدارات البرامج ACU المستخدمة في وقت هذا المنشور:

النظام الأساسي	دالة	إصدار البرامج
CallManager	IP-PBX	3.0(10)
Catalyst 3500XL	مفتاح التوزيع	12.0(5.1)XP
Catalyst 6500	مفتاح اللب	5.5(5)
Catalyst 1900	محول خزانة الأسلاك	—
المعالج Cisco 7200	موجه WAN	12.1(4)
موجّه Cisco 3640	بوابة H.323	12.1(XI6)3a

معلومات ذات صلة

- دعم تقنية الصوت
- دعم منتجات الاتصالات الصوتية واتصالات IP
- استكشاف أخطاء خدمة IP الهاتفية من Cisco وإصلاحها
- 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).