بنية أساسية للتضمين الوسيط الموجه

المحتويات

المقدمة
إفتراض
ملخص عن التقنية
الوصف التشغيلي
مزايا RBE
اعتبارات التنفيذ
بنية الشبكة
اعتبارات التصميم لبنية RBE
النقاط الرئيسية في RBE
CPE
إدارة IP
كيفية الوصول إلى وجهة الخدمة
توفير الوصول إلى الإنترنت
خدمات الجملة
الوصول إلى الشركات
إمكانات تحديد الخدمة
القرار
معلومات ذات صلة

المقدمة

يصف هذا المستند بنية خط المشترك الرقمي غير المتماثل من نهاية إلى نهاية (ADSL) التي تستخدم ميزة التضمين الوسيط الموجه (RBE) لمركز الوصول العالمي (Cisco 6400 (UAC. تم تطوير تقنية RBE لمعالجة المشكلات المعروفة المتمثلة في عملية التوصيل بين مراكز البيانات (RFC1483)، بما في ذلك العواصف التي تعمل بالبث والأمان. وباستثناء حقيقة أنه يعمل بشكل حصري عبر ATM، تعمل ميزة RBE بشكل مماثل لنصف جسر. يمكن تحقيق قابلية توسع وأداء وأمان إضافي باستخدام الخصائص الفريدة لمشتركي xDSL.

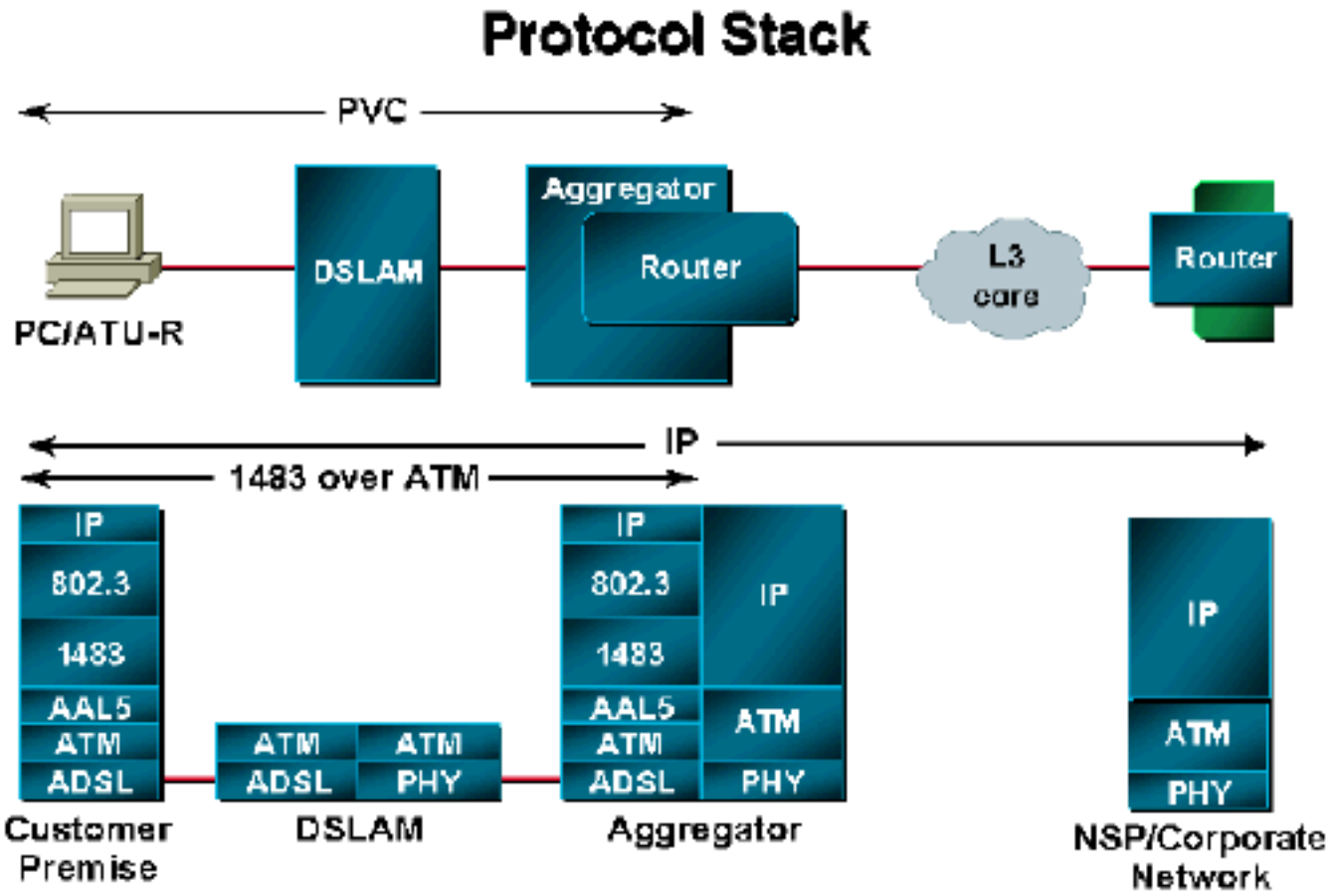
إفتراض

تم تصميم البنية الأساسية باستخدام نموذج بنية مرجع منتدى ADSL. تغطي البنية عروض الخدمة المختلفة بواسطة موفر الوصول إلى الشبكة (NAP) وسيناريوهات مختلفة لكيفية إعادة توجيه حركة مرور المشترك إلى موفر خدمة الشبكة (NSP). في هذه البنية، RBE هو طريقة التضمين المفترضة المستخدمة من قبل Cisco 6400. يستند محتوى هذا المستند إلى عمليات النشر الحالية، بالإضافة إلى بعض الاختبارات الداخلية التي تم إجراؤها على البنية الأساسية. للحصول على الميزات والتعديلات المحسنة، ارجع إلى ملاحظات الإصدار لأحدث إصدار من برنامج Cisco IOS®. حاليا، يتم دعم RBE على الأنظمة الأساسية Cisco 6400 و Cisco 7200 و Cisco 7500. يقتصر هذا المستند على مناقشات Cisco 6400.

ملخص عن التقنية

من وجهة نظر الشبكة، يبدو اتصال ATM كاتصال موجه. يتم إستلام حركة مرور البيانات كحزم RFC1483، ولكنها إطارات إيثرنت RFC1483 أو إطارات IEEE 802.3. بدلا من جسر إطار إيثرنت أو IEEE 802.3، كما في حالة التوصيل العادي RFC1483، يقوم الموجه بالتوجيه على رأس الطبقة 3. باستثناء بعض التحققات الالتفافية، يتم تجاهل رأس الجسر. وهذا موضح بالتفصيل في القسم التالي.

الوصف التشغيلي



من وجهة نظر تشغيلية، يعمل الموجه كما لو كانت الواجهة الموجهة-الجسر متصلة بشبكة Ethernet LAN. يتم وصف العملية أدناه بطريقتين: الحزم الناشئة من مباني العميل والحزم الموجهة إلى أماكن عمل العميل.

بالنسبة للحزم التي يتم إنشاؤها من أماكن عمل العميل، يتم تخطي رأس الإيثرنت وفحص عنوان IP للوجهة. إذا كان عنوان IP للوجهة في ذاكرة التخزين المؤقت للمسار، فسيتم تحويل الحزمة بسرعة إلى الواجهة الصادرة. إذا لم يكن عنوان IP للوجهة في ذاكرة التخزين المؤقت للمسار، فسيتم وضع الحزمة في قائمة الانتظار لتحويل العملية. في وضع محول العملية، يتم العثور على الواجهة الصادرة التي يجب توجيه الحزمة من خلالها من خلال البحث في جدول التوجيه. بعد تحديد الواجهة الصادرة، يتم توجيه الحزمة عبر تلك الواجهة. يحدث هذا بدون متطلبات لمجموعة جسر أو واجهة ظاهرية لمجموعة جسور (BVI).

بالنسبة للحزم الموجهة إلى أماكن عمل العميل، يتم فحص عنوان IP للوجهة الخاص بالحزمة أولا. يتم تحديد الواجهة الوجهة من جدول توجيه IP. بعد ذلك، يتحقق الموجه من جدول بروتوكول تحليل العنوان (ARP) المرتبط بتلك الواجهة لوضع عنوان MAC للوجهة في رأس الإيثرنت. إذا لم يتم العثور على أي شيء، يقوم الموجه بإنشاء طلب ARP لعنوان IP للوجهة. يتم إعادة توجيه طلب ARP إلى واجهة الوجهة فقط. هذا على النقيض من التوصيل، حيث يتم إرسال طلب ARP إلى جميع الواجهات في مجموعة الجسر.

لسيناريو يستخدم واجهات غير مرقمة (حيث قد تجد مشتركين إثنين على الشبكة الفرعية نفسها)، تستخدم واجهة الجسر الموجه ARP للوكيل. على سبيل المثال، 192.168.1.2 (المضيف A) يريد الاتصال ب 192.168.1.3 (المضيف B). ومع ذلك، فإن المضيف A موجود على الشبكة الفرعية نفسها الخاصة بالمضيف B.

المضيف a ينبغي أن يعلم المضيف mac address{upper} b ب يرسل من ARP بث إلى المضيف b. عندما تتلقى

واجهة الجسر الموجه في جهاز التجميع هذا البث، فإنها سترسل إستجابة ARP للوكيل باستخدام عنوان MAC الخاص ب 192.168.1.1، المضيف A. سيأخذ عنوان MAC ذلك، يضعه في رأس الإيثرنت، ويرسل الحزمة. عندما يستلم المسحاج تخديد الربط، هو يتجاهل الرأس وينظر إلى الغاية عنوان، بعد ذلك يوجهها على القارن صحيح.

مزايا RBE

وقد تم تطوير شبكة منطقة التخزين (RBE) بهدف معالجة بعض القضايا التي تواجهها بنية الربط التي تعمل وفقا لمعيار RFC1483. يحتفظ بروتوكول معلومات التوجيه (RBE) بالمزايا الرئيسية لبنية التوصيل عبر بروتوكول RFC1483، مع التخلص من معظم مساوئ هذه البنية.

- الحد الأدنى من التكوين في معدات موقع العميل (CPE).ويعتبر مزود الخدمة هذا الأمر مهما لأنه لم يعد يتطلب عددا كبيرا من قوائم الشاحنات ولم يعد بحاجة إلى الاستثمار بكثافة في الموظفين لدعم البروتوكولات ذات المستوى الأعلى. يعمل CPE في وضع الجسر كجهاز بسيط للغاية. يتضمن CPE الحد الأدنى من أستكشاف الأخطاء وإصلاحها حيث يتم تمرير كل ما يأتي من إيثرنت مباشرة إلى جانب شبكة WAN.
- سهولة الترحيل من بنى التوصيل النقية إلى تقنية RBE. لا يوجد تغيير مطلوب في نهاية المشترك.
- تجنب تحديات خطف IP وانتحال بروتوكول حل العناوين (ARP) التي تواجهها في بنى التوصيل النقي النموذجية. كما تعمل تقنية التزويد بالطاقة عبر شبكة إيثرنت (RBE) على منع البث عبر العواصف من خلال إستخدام إتصالات من نقطة إلى نقطة. يعد الأمان هو العائق الرئيسي في بنى التوصيل الصافي.
- بالمقارنة مع بنى التوصيل الصافي، توفر تقنية RBE أداء فائقا بسبب تنفيذ التوجيه على جهاز التجميع. كما أن RBE أكثر قابلية للتطوير لأنه لا يحتوي على قيود مجموعة الجسور.
- يدعم تحديد ويب للطبقة 3 باستخدام بوابة تحديد خدمة (SSG) من Cisco.

اعتبارات التنفيذ

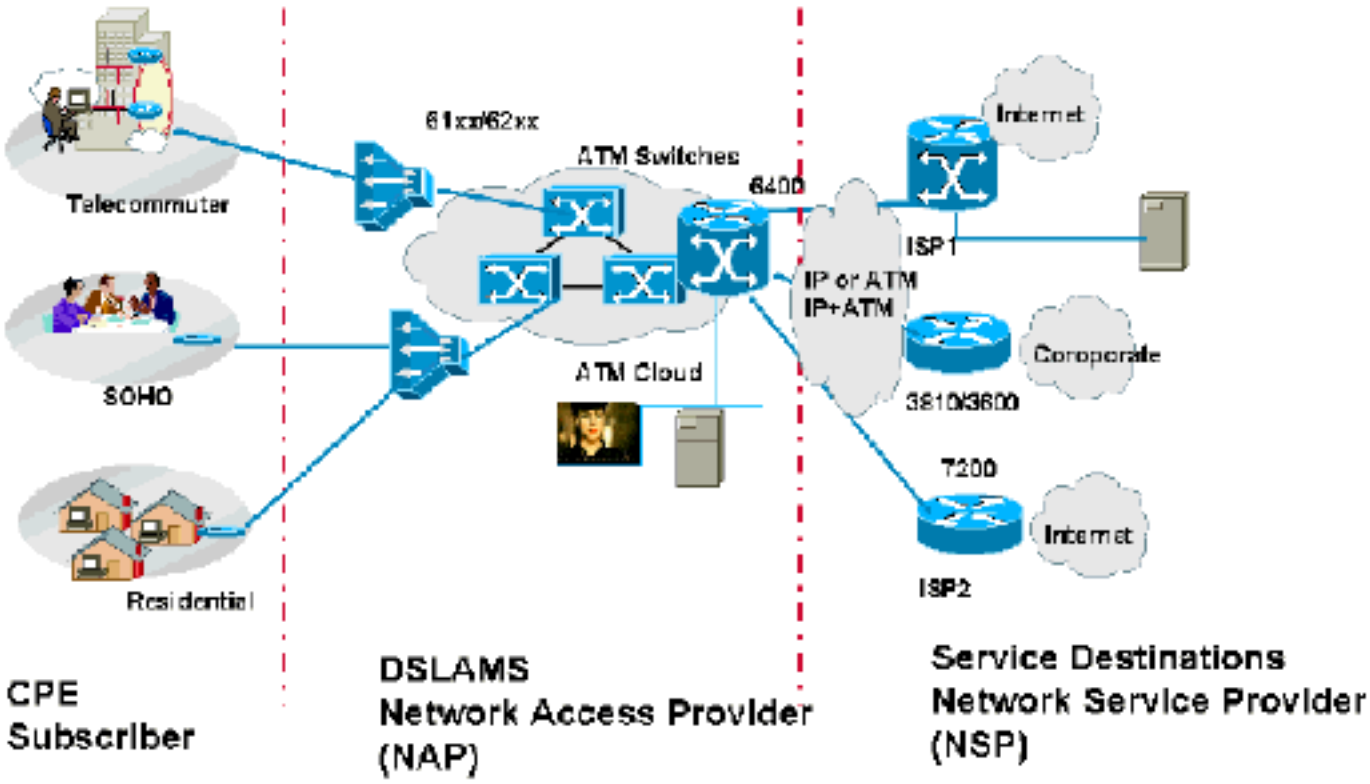
بعض النقاط الأساسية التي يجب أخذها في الاعتبار قبل تنفيذ هذه البنية هي نفسها المشار إليها في ورقة بنية خط الأساس للربط مع المعيار RFC1483.

يوصى ب RBE عندما:

- والسيناريوهات هي نفسها الموجودة في بنى التوصيل الموجودة.
- ولا تريد خطة العمل الوطنية سوى تنفيذ الحد الأدنى من إدارة برامج التكيف الهيكلي. يتطلب مفهوم CPE البسيط أدنى تكوين أو لا يتطلب أي تكوين بعد نشر CPE في موقع المشترك.
- لا تريد حماية مستوى التحكم (NAP) تثبيت العملاء المضيفين والاحتفاظ بهم على الأجهزة المضيفة الموجودة خلف بروتوكول CPE الجسر. وتؤدي مهام التركيب والصيانة هذه إلى زيادة تكاليف النشر والصيانة، بما في ذلك توفير موظفي مكتب المساعدة الذين لديهم معرفة ببرنامج العميل ونظام التشغيل الذي يعمل عليه العميل.
- تريد حماية الوصول إلى الشبكة (NAP) نشر شبكة جسر يمكن تطويرها وتأمينها باستخدام منافذ CPE *الموجودة* (التي يمكن تشغيلها فقط في وضع التوصيل عبر RFC1483) وتريد توفير إمكانات تحديد الخدمة.

وتشرح المناقشة التالية كيفية ملاءمة بنية RBE مع نماذج الأعمال المختلفة وقياسها.

بنية الشبكة



بنية شبكة RBE مماثلة لبنية التوصيل RFC1483. وكما هو محدد في هذه البنية، يمكن أن يكون جهاز التجميع إما في NAP أو في NSP. في حال إستخدام بنية دائرة افتراضية دائمة من نهاية إلى نهاية (PVC)، يقوم NSP بإنهاء المشتركين ويقوم بتكوين RBE في جهاز التجميع. إذا كانت NAP تفضل توفير خدمات بالجملة بالإضافة إلى تحديد الخدمة، فقد تختار إنهاء هؤلاء المشتركين والحصول على عناوين IP من خادم بروتوكول التكوين الديناميكي للمضيف (DHCP) المحلي. في حالة الخدمات بالجملة، قد تختار برامج العمل الوطنية الحصول على عناوين IP من NSP. تتم تغطية هذه السيناريوهات بالتفصيل في قسم إدارة IP في هذا المستند.

اعتبارات التصميم لبنية RBE

يعمل بروتوكول RBE على التخلص من المخاطر الأمنية الرئيسية التي تتضمنها بنية التوصيل عبر بروتوكول RFC1483. وبالإضافة إلى ذلك، يوفر نظام تمهيد تشغيل الشبكات (RBE) أداء أفضل وقابلية تطوير أكبر نظرا لأنه يتم التعامل مع الواجهات الفرعية كواجهات موجهة.

يوضح هذا القسم بعض النقاط الأساسية التي يجب مراعاتها قبل تصميم بنية RBE. بالنسبة لجانب المشترك، تظل مبادئ التصميم هي نفسها الموجودة في بنية جسر RFC1483.

في RBE، يتم تخصيص دائرة ظاهرية واحدة (VC) لموجه ما أو مجموعة من المسارات أو شبكة فرعية لتوجيه المجال التبادلي دون فئات (CIDR). وبالتالي، يتم تقليل البيئة الموثوق بها إلى أماكن عمل العميل الفردية الممثلة إما بعناوين IP في مجموعة المسارات أو كتلة توجيه المجال التبادلي دون فئات (CIDR). كما يتحكم ISP في العناوين التي تم تعيينها للمستخدم. ويتم ذلك من خلال تكوين شبكة فرعية على الواجهة الفرعية لذلك المستخدم. لذلك، إذا قام المستخدم بتكوين المعدات باستخدام عنوان IP خارج نطاق العنوان المخصص (قد يتسبب في تدفق حزم ARP إلى الموجه)، يقوم الموجه بإنشاء خطأ "كبل خطأ" ويرفض إدخال تعيين عنوان IP إلى MAC الخاطئ في جدول ARP الخاص به.

يمكن نشر RBE باستخدام واجهات ATM الفرعية من نقطة إلى نقطة فقط. لا يمكن نشره على الواجهات الفرعية متعددة النقاط. على الرغم من أنه يتم ربط جانب المشترك، إلا أنك لا تحتاج إلى تعريف مجموعات الجسر أو واجهات BVI لأن الواجهات الفرعية يتم معالجتها كواجهات موجهة.

يمكن أن يتم ترقيم الواجهات الفرعية من نقطة إلى نقطة ATM أو أن تكون غير مرقمة إلى بعض الواجهات الأخرى.

بحكم التعريف، فإن الواجهة المرقمة هي واجهة لها عنوان IP معين معين لها بقناع شبكة فرعية ثابت. على سبيل المثال:

```
Interface atm0/0/0.132 point-to-point
ip address 192.168.1.1 255.255.255.252
```

كما هو موضح في هذا المثال، عند نشر RBE باستخدام واجهة مرقمة، يجب أن تكون هناك شبكة فرعية منفصلة لكل مشترك. يجب تكوين المضيف في نهاية المشترك ل 192.168.1.2. يوجد مضيف واحد فقط في نهاية المشترك. إذا كان المتطلب هو دعم أكثر من مضيف واحد، فيجب أن يستوعب قناع الشبكة الفرعية الذي تم إختياره المزيد من البيئات المضيفة.

تعطي الواجهات المرقمة التحكم في NAP في عدد البيئات المضيفة التي ربطها المشترك خلف CPE. وكما هو موضح أعلاه، كان هذا الافتقار إلى التحكم مشكلة رئيسية في بنية التوصيل عبر بروتوكول RFC1483.

ومع ذلك، تستهلك هذه المنهجية العديد من عناوين IP. ستحتاج إلى تخصيص شبكة فرعية واحدة لكل مشترك، واستخدام عنوان IP واحد للواجهة الفرعية ل ATM، وترك عنوان البث وجميع العناوين الصفرية غير المستخدمة. لذلك، لكي يكون لديك مضيف واحد خلف CPE، يلزمك على الأقل تعريف قناع شبكة فرعية 255.255.255.252. ونظرا لندرة عناوين IP، قد لا يكون هذا خيارا مجديا ما لم تكن خطة العمل الوطنية/خطة العمل الوطنية تستخدم مساحة عنوان خاصة وتقوم بإجراء ترجمة عنوان الشبكة (NAT) للوصول إلى العالم الخارجي.

للحفاظ على عناوين IP، سيكون البديل هو إستخدام الواجهات غير المرقمة. حسب التعريف، فإن الواجهة غير المرقمة هي واجهة تستخدم عنوان IP الخاص بواجهة أخرى باستخدام الأمر **ip unnumber**. على سبيل المثال:

```
!
interface loopback 0
ip address 192.168.1.1 255.255.255.0
!
interface atm0/0/0.132 point-to-point
ip unnumbered loopback 0
!
interface atm0/0/0.133 point-to-point
ip unnumbered loopback 0
```

كما هو موضح في المثال أعلاه، يتم تطبيق عنوان IP وشبكة فرعية فقط على واجهة الاسترجاع. ستكون جميع واجهات ATM الفرعية غير مرقمة على واجهة الاسترجاع تلك. في هذا السيناريو، سيكون جميع المشتركين الذين يتم إنهاؤهم على واجهات ATM الفرعية (غير المرقمة إلى الاسترجاع 0) على الشبكة الفرعية نفسها الخاصة بالاسترجاع 0. وهذا يعني ضمنا أن المشتركين سوف يكونون على نفس الشبكة الفرعية، ولكنهم سوف يدخلون من خلال واجهات مختلفة موجهة. في هذه الحالة، تصبح مشكلة للموجه لتحديد المشترك الذي يكمن وراءه أي واجهة فرعية ل ATM. بالنسبة ل Cisco IOS، يتم توصيل 192.168.1.0 (في الرسم التخطيطي إدارة IP) مباشرة عبر إسترجاع الواجهة 0، ولن يقوم بإرسال حركة مرور البيانات الموجهة إلى أي من عناوين المضيف على هذه الشبكة الفرعية عبر أي واجهة أخرى. لحل هذه المشكلة، يلزمك تكوين مسارات المضيف الثابتة بشكل صريح. على سبيل المثال:

```
ip route 192.168.1.2 255.255.255.255 atm0/0/0.132
ip route 192.168.1.3 255.255.255.255 atm0/0/0.133
```

كما هو محدد في هذا المثال، عندما يحتاج الموجه إلى إتخاذ قرار توجيه ويحتاج إلى إعادة توجيه حركة المرور الموجهة ل 192.168.1.2، فإنه سيختار ATM 0/0/0.132 كواجهة صادرة، وما إلى ذلك. بدون تحديد مسارات المضيف الثابتة هذه، سيختار الموجه الواجهة الصادرة كإعادة توجيه 0 ويسقط الحزمة.

على الرغم من أن الواجهة غير المرقمة ستحافظ على عناوين IP، إلا أنها تتطلب مهمة إضافية لتكوين المسارات المضيفة الثابتة على معالج توجيه العقدة (NRP) لكل مشترك. لاحظ أنه إذا كان لدى المشترك، على سبيل المثال، 14 جهازا مضيفا خلف CPE، لا يلزم أن يكون لديه مسارات مضيف ثابتة لكل مضيف. يمكن تحديد مسار ملخص لواجهة ATM الفرعية.

حتى الآن، افترض هذا التفسير أن المضيفين وراء CPE سيتم تكوينهم لعناوين IP الثابتة. هذا الافتراض ليس صحيحا

في تصاميم الحياة الحقيقية. في العالم العملي، تريد خطة العمل الوطنية إجراء الحد الأدنى من التهيئة والصيانة ل CPE والأجهزة المضيفة الملحقة بها. لتحقيق ذلك، يجب على الأجهزة المضيفة الحصول على العناوين الخاصة بها بشكل ديناميكي باستخدام خادم DHCP.

للحصول على عناوين IP الخاصة بهم بشكل ديناميكي، يجب تكوين الأجهزة المضيفة للحصول على عناوين IP من خادم DHCP. عندما يقوم المضيف بالتمهيد، فإنه يرسل طلبات DHCP. ثم يتم نقل هذه الطلبات إلى خادم DHCP المناسب، الذي يعين عنوان IP للمضيف من واحد في نطاقه المحدد مسبقا.

in order to أرسلت ال DHCP أولي طلب من المضيف إلى ال DHCP نادل مناسب، أنت ينبغي طبقت **ال ip مساعد-address** أمر إلى القارن أن يكون يستلم البث. بعد تلقي عمليات البث، يبحث Cisco IOS في تكوين عنوان مساعد IP لتلك الواجهة ويعيد توجيه هذه الطلبات في حزمة البث الأحادي إلى خادم DHCP المناسب الذي يتم تحديد عنوان IP له في عنوان مساعد IP. بعد ردود خادم DHCP باستخدام عنوان IP، يرسل الاستجابة إلى الواجهة على الموجه التي قامت بإعادة توجيه الطلب في الأصل. يتم إستخدام هذا كواجهة صادرة لإرسال إستجابة خادم DHCP إلى المضيف الذي طلب الخدمة في الأصل. كما يقوم الموجه تلقائيا بتثبيت مسار مضيف لهذا العنوان.

إذا تم تمكين RBE على واجهة فرعية وكان وحدة بيانات بروتوكول الجسر (PDU) وفقا لمعيار IEEE 802.3، يتم فحص تضمين الإيثرنت بعد تضمين جسر ATM. إذا كانت حزمة IP/ARP، فإنها تتم معالجتها مثل أي حزمة IP/ARP أخرى. تم تحويل حزمة IP بسرعة. وفي حالة فشله، يتم وضعه في قائمة الانتظار للتحويل الخاص بالعملية.

يعتبر أداء RBE مكسبا كبيرا. تتضمن كود التوصيل القياسي اليوم مشكلة متأصلة في طلب تصنيفين منفصلين للحزمة قبل أن يمكن إتخاذ قرار إعادة التوجيه. يتم تعريف التصنيف بأنه عملية فحص (في الخادم) وتعديل (في الخادم) رأس الحزمة لإعادة توجيه المعلومات، وهو أمر مكلف نسبيا. يلزم بحث عن الطبقة 2 لتحديد ما إذا كانت الحزمة بحاجة إلى توجيه أو جسر. بعد ذلك، في الطبقة 3، يلزم بحث لتحديد الموقع الذي يجب توجيه الحزمة إليه. ويتم إجراء هذا التصنيف في أتجاهات المراحل التمهيدية والتدريجية، مما يؤثر على الأداء.

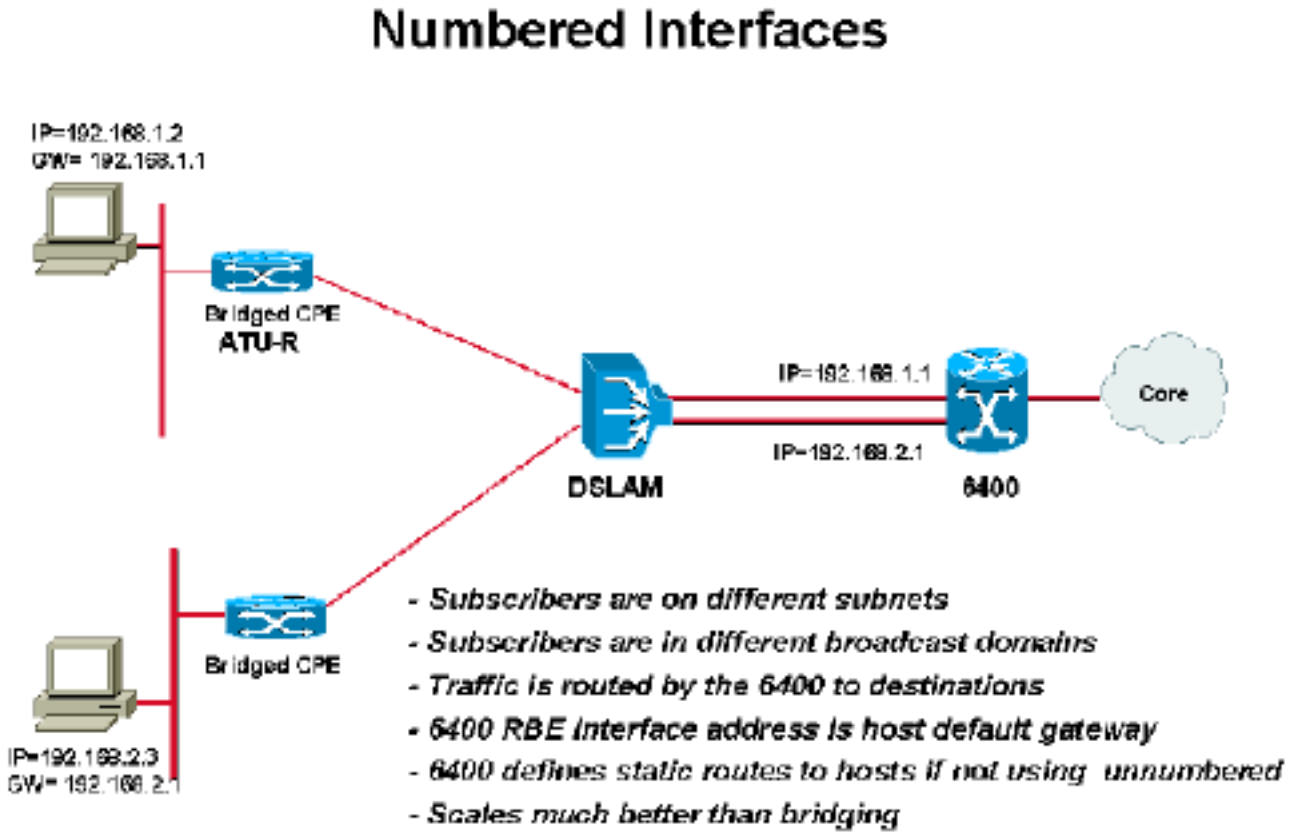
ل RBE، يتم تحديد ذلك مسبقا بواسطة التكوين الذي يجب توجيه الحزمة في إتجاه البث. وبالتالي، ليس من الضروري المرور عبر مسار إعادة توجيه الجسر، الذي كان ضروريا في حالة الربط القياسي.

النقاط الرئيسية في RBE

CPE

يبقى تكوين CPE هو نفسه الموجود في التوصيل القياسي. لا يلزم إجراء أي تغييرات على CPE لنشر RBE.

إدارة IP



أثناء نشر الواجهات المرقمة ل RBE، تتم عادة معالجة تخصيص عنوان IP للمضيف خلف CPE الجسر عبر خادم DHCP. كما تمت الإشارة مسبقا، يمكن أن يتواجد خادم DHCP في NAP أو في NSP. بالنسبة لأي من الحالتين، يجب تكوين الواجهة الفرعية ATM المرقمة باستخدام الأمر **ip helper-address**. إذا كان خادم DHCP سيتم وضعه في NSP، فيجب أن يكون لجهاز تجميع NAP مسار للوصول إلى هذا الخادم. السيناريو الوحيد الذي تستخدم فيه حماية الوصول (NAP) خادم DHCP الخاص بها ونطاق عنوان IP الخاص بها هو عندما تريد تقديم إمكانيات تحديد الخدمة للمشتركين، وعندما تكون تلك المشتركين ملحقة بشبكة LAN الخاصة بميزة حماية الوصول إلى الشبكة (NAP).

إذا كانت حماية مستوى التحكم (NAP) تريد إستخدام مساحة عنوان IP الخاصة ب NSP، فيجب تخصيص أحد عناوين IP لكل شبكة فرعية لواجهة ATM الفرعية. وينبغي أيضا أن يكون هناك إتفاق متبادل بين برنامج العمل الوطني وبرنامج العمل الوطني بحيث يكون العنوان الصحيح. عندما يقوم خادم DHCP الخاص ب NSP بتعيين عناوين IP، يجب أن تكون هذه الاتفاقية في موضعها لضمان أن الخادم يوفر معلومات العبارة الافتراضية الصحيحة للمضيف. ويمكن أن يلخص NAP بعد ذلك مسارا ثابتا لجميع العناوين التي تم تعيينها للمشتركين، أو يمكن أن يختار تشغيل بروتوكول توجيه مع NSP للإعلان عن هذه المسارات. وفي معظم السيناريوهات، يفضل كل من برنامج العمل الوطني وبرنامج العمل الوطني عدم إستخدام بروتوكول توجيه. يعد توفير مسار ثابت خيارا جيدا.

هذا هو التكوين الأساسي المطلوب على NRP لنشر RBE باستخدام الواجهات المرقمة:

```
!
interface ATM0/0/0.132 point-to-point
 ip address 192.168.1.1 255.255.255.0
        ip helper-address 192.168.3.1
             no ip directed-broadcast
                 atm route-bridged ip
                             pvc 1/32
                encapsulation aal5snap
                                    !
interface ATM0/0/0.133 point-to-point
 ip address 192.168.2.1 255.255.255.0
        ip helper-address 192.168.3.1
             no ip directed-broadcast
```

```
atm route-bridged ip
                pvc 1/33
encapsulation aal5snap
```

إستخدام الواجهات غير المرقمة هو أفضل طريقة للحفاظ على عناوين IP. كما هو موضح سابقا، عند إستخدام الواجهات غير المرقمة مع DHCP، يتم تثبيت المسارات المضيفة بشكل ديناميكي. قد يكون هذا هو النهج الأفضل لنشر وحدة التخزين المتصلة بالشبكة (RBE). بعد ذلك يمكن تحديد موقع خادم DHCP إما في NAP أو NSP، بالنسبة للواجهات المرقمة.

هذا هو التكوين الأساسي المطلوب على NRP لنشر RBE باستخدام الواجهات غير المرقمة:

```
interface Loopback0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface ATM0/0/0.132 point-to-point
ip unnumbered Loopback0
no ip directed-broadcast
ATM route-bridged ip
pvc 1/32
encapsulation aal5snap
!
interface ATM0/0/0.133 point-to-point
ip unnumbered Loopback0
no ip directed-broadcast
ATM route-bridged ip
pvc 1/33
encapsulation aal5snap
```

كيفية الوصول إلى وجهة الخدمة

حتى الآن، ناقش هذا المستند تقنية الوصول الأساسية باستخدام RBE كطريقة تضمين. ومع ذلك، وباستخدام هذه البنية، يمكن أن توفر أيضا برامج العمل الوطنية/خطة العمل الوطنية خدمات متنوعة وخيارات مختلفة حيث يمكن لخطط العمل الوطنية إعادة توجيه حركة مرور المشترك إلى NSP. وترد هذه المفاهيم في الأقسام التالية.

توفير الوصول إلى الإنترنت

في هذا السيناريو، تتمثل الوظيفة الأساسية ل NSP في توفير وصول الإنترنت عالي السرعة للمشتركين النهائيين. بما أن NSP سيقدم الخدمة النهائية، تصبح إدارة عنوان IP هي مسؤولية NSP. يمكن أن يعين هو عنوان عام إلى مشتركه نهائي يستعمل DHCP نادل، أو يستطيع أخترت أن يزود خاص ip عنوان إلى المشترك وبعد ذلك أنجزت NAT أن يصل إلى العالم الخارجي.

خدمات الجملة

إذا كانت خطة العمل الوطنية ترغب في تقديم خدمات بالجملة إلى مزودي خدمة الإنترنت الآخرين، فإنها تستطيع القيام بذلك. في هذا السيناريو، لا تفضل حماية الوصول (NAP) عادة معالجة عناوين IP لجميع المشتركين في عناوين NSP مختلفة. تقوم حماية الوصول (NAP) ببعض الترتيبات مع مزود خدمة الإنترنت (ISP) لتوفير عناوين IP لهؤلاء المشتركين. يمكن تحقيق ذلك من خلال إعادة توجيه NAP لطلبات DHCP الواردة من المشتركين إلى خوادم DHCP في NSPs. يجب أن تقوم حماية الوصول (NAP) بتكوين واجهات ATM الفرعية الخاصة بها باستخدام أحد عناوين IP من ذلك النطاق، كما تحتاج إلى الإعلان عن هذه الموجهات إلى NSP. يمكن أن يكون إعلان المسار في شكل مسار ثابت أو بعض بروتوكول التوجيه بين NAP و NSP. المسار الثابت هو الطريقة المفضلة لخطط العمل الوطنية، بالإضافة إلى برنامج العمل الوطني.

الوصول إلى الشركات

يتطلب وصول الشركة عادة خدمات الشبكة الخاصة الظاهرية (VPN). وهذا يعني أن الشركة لن تقدم أي عناوين IP إلى برنامج العمل الوطني ولا تسمح لبرنامج العمل الوطني بالإعلان عن مساحة عنوان IP الخاص بالشركة في مركز IP الخاص ببرنامج العمل الوطني، حيث قد يؤدي ذلك إلى حدوث خرق أمني. تفضل الشركات عادة تطبيق عناوين IP الخاصة بها على عملائها، أو أنها ستسمح بالوصول عبر بعض الوسائل الآمنة مثل تحويل التسمية متعدد البروتوكولات/الشبكة الخاصة الظاهرية (MPLS/VPN) أو بروتوكول الاتصال النفقي للطبقة 2 (L2TP).

والنهج الآخر لتوفير وصول آمن إلى الشركات هو حيث توفر برامج العمل الوطنية عناوين بروتوكول الإنترنت الأولية لهؤلاء المشتركين. وبالتالي، يصبح المشتركون ملحقين بشبكة LAN بشفرة الوصول إلى الشبكة (NAP). بعد أن يكون للمشتركين عناوين IP أولية، يمكنهم بدء نفق إلى الشركة من خلال برنامج عميل L2TP الذي يعمل على المضيف. وبدورها، ستقوم الشركة بمصادقة هذا المشترك وتوفير عنوان IP من مساحة عنوان IP الخاصة بها. يتم إستخدام عنوان IP هذا من قبل مهايئ L2TP VPN. وبهذه الطريقة، يكون للمشتركين الخيار إما الاتصال بموفر خدمة الإنترنت (ISP) لديهم لاتصال الإنترنت أو الوصول إلى شركتهم من خلال الوصول الآمن إلى نفق L2TP. ومع ذلك، يتطلب هذا من الشركة توفير عنوان IP لوجهة النفق للمشترك، والذي يجب أن يكون قابلا للتوجيه من خلال مركز IP لميزة NAP.

إمكانات تحديد الخدمة

يمكن أن توفر حماية الوصول (NAP) إمكانات متنوعة لاختيار الخدمة باستخدام وظائف Cisco SSG. توفر SSG طريقتين لتوفير تحديد الخدمة: من خلال الطبقة 2 (المعروفة باسم PTA-MD) وتحديد الويب من الطبقة 3. باستخدام RBE، يمكن إستخدام طريقة تحديد الويب للطبقة 3 فقط. وهذا يتطلب أن يكون المشتركون مرتبطين بشبكة LAN إلى NAP؛ أي أن توفر NAP عنوان IP الأولي للمشترك وتوفر الوصول إلى لوحة معلومات تحديد خدمة Cisco (SSD).

في حالة بنية RBE، تعد طريقة تحديد موقع SSG من Cisco طريقة جيدة لحساب حركة مرور المشترك.

القرار

يوفر الطراز RBE أداء أفضل، كما أنه أكثر قابلية للتطوير مقارنة بالجسر القياسي. كما أنه يتغلب على جميع مشاكل الأمان التي تتم مواجهتها في عملية التوصيل القياسية. تعمل تقنية RBE على التخلص من مشكلات البث العاصفة الناتجة عن التوصيل القياسي. يوفر برنامج الإرسال والاستقبال (RBE) بنية قوية لبروتوكول NAP تهدف إلى تجنب صيانة برامج الأجهزة المضيفة للعملاء ومعالجة المشكلات المتعلقة بالجسر، فضلا عن أنها تريد خفض تكاليف النشر. باستخدام RBE، يمكن تحقيق كل ذلك أثناء إستخدام بنية التوصيل الحالية.

معلومات ذات صلة

- معلومات دعم منتجات ADSL من Cisco
- 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).