Grundarchitektur der gerouteten Bridge-Kapselung

Inhalt

Einführung

Dieses Dokument beschreibt eine End-to-End-Architektur für asymmetrische digitale Teilnehmeranschlussleitungen (ADSL), die die Funktion Routed Bridged Encapsulation (RBE) für den Cisco 6400 Universal Access Concentrator (UAC) verwendet. RBE wurde entwickelt, um bekannte RFC1483-Bridging-Probleme wie Broadcast-Stürme und Sicherheit zu beheben. Außer, dass sie ausschließlich über ATM betrieben wird, funktioniert die RBE-Funktion identisch mit Halbüberbrückung. Zusätzliche Skalierbarkeit, Leistung und Sicherheit können durch die einzigartigen Merkmale von xDSL-Abonnenten erreicht werden.

Annahme

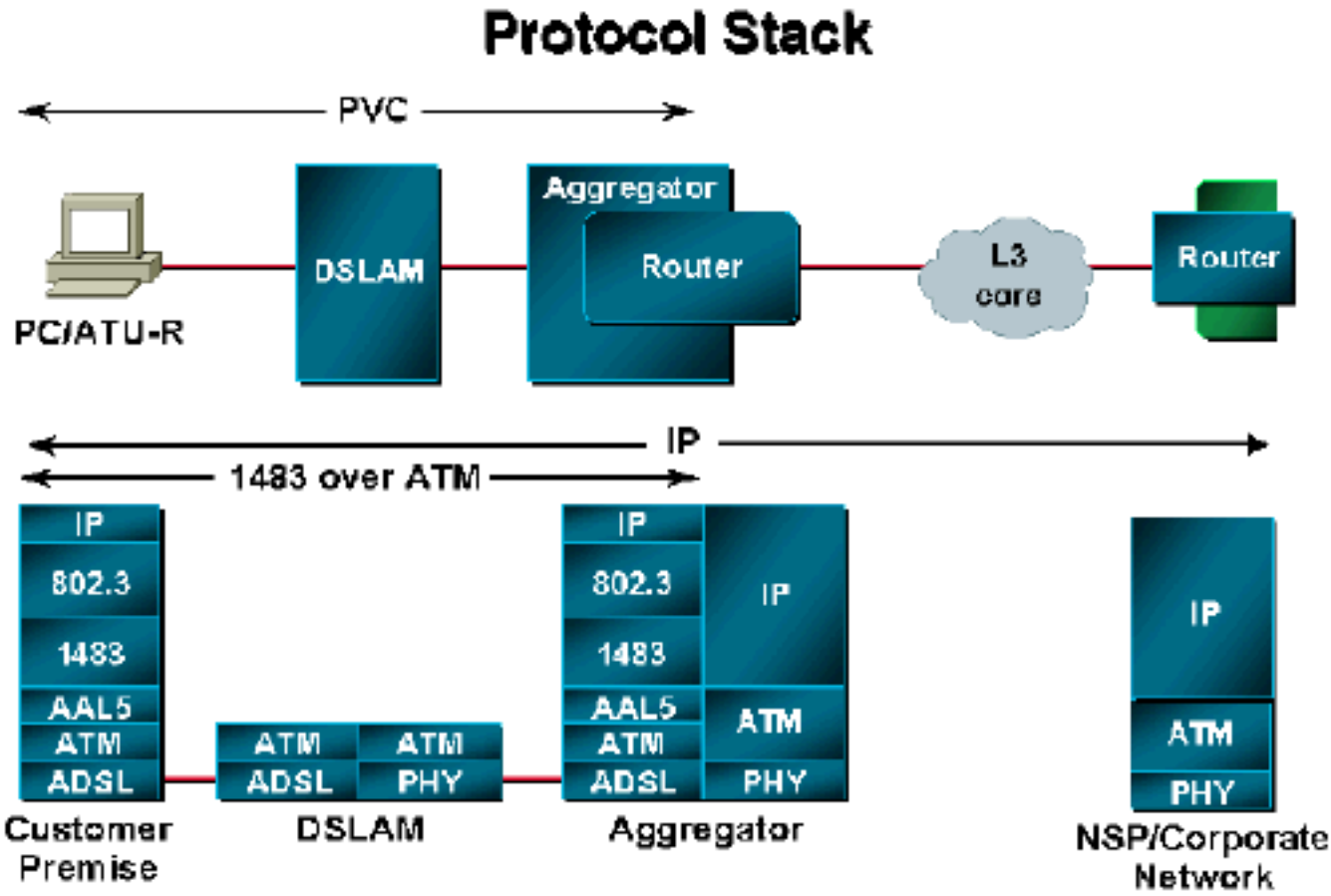
Die Basisarchitektur wird mithilfe des ADSL-Forum-Referenzarchitekturmodells entwickelt. Die Architektur umfasst verschiedene Serviceangebote des Network Access Providers (NAP) sowie verschiedene Szenarien für die Weiterleitung des Teilnehmerdatenverkehrs an den Network Service Provider (NSP). In dieser Architektur ist RBE die vom Cisco 6400 vermutlich verwendete Kapselungsmethode. Der Inhalt dieses Dokuments basiert auf vorhandenen Bereitstellungen sowie auf einigen internen Tests, die mit der Architektur durchgeführt wurden. Weitere

Informationen zu erweiterten Funktionen und Änderungen finden Sie in den Versionshinweisen zur aktuellen Version der Cisco IOS® Software. Derzeit wird RBE auf den Plattformen Cisco 6400, Cisco 7200 und Cisco 7500 unterstützt. Dieses Dokument beschränkt sich auf Gespräche mit dem Cisco 6400.

Technologiebeschreibung

Aus Netzwerksicht sieht die ATM-Verbindung wie eine geroutete Verbindung aus. Datenverkehr wird als RFC1483-Pakete empfangen, aber es handelt sich um RFC1483-Ethernet- oder IEEE 802.3-Frames. Anstatt den Ethernet- oder IEEE 802.3-Frame zu überbrücken, wie bei der regulären RFC 1483-Bridging, routet der Router auf den Layer-3-Header. Mit Ausnahme einiger Cursorprüfungen wird der Bridge-Header ignoriert. Dies wird im nächsten Abschnitt ausführlich erläutert.

Betriebsbeschreibung



Aus betrieblicher Sicht funktioniert der Router so, als ob die geroutete Bridge-Schnittstelle mit einem Ethernet-LAN verbunden wäre. Der Vorgang wird nachfolgend auf zwei Arten beschrieben: Pakete, die vom Kundenstandort ausgehen, und Pakete, die für den Kundenstandort bestimmt sind.

Bei Paketen, die vom Kundenstandort ausgehen, wird der Ethernet-Header übersprungen, und die Ziel-IP-Adresse wird überprüft. Wenn sich die Ziel-IP-Adresse im Route-Cache befindet, wird das Paket auf die ausgehende Schnittstelle umgeschaltet. Wenn sich die Ziel-IP-Adresse nicht im Route-Cache befindet, wird das Paket für das Prozess-Switching in die Warteschlange gestellt. Im Prozess-Switch-Modus wird die Ausgangsschnittstelle, über die das Paket geroutet werden soll, in der Routing-Tabelle angezeigt. Nachdem die ausgehende Schnittstelle identifiziert wurde, wird

das Paket über diese Schnittstelle geroutet. Dies geschieht ohne Bridge-Gruppe oder Bridge Group Virtual Interface (BVI).

Bei Paketen, die für den Kundenstandort bestimmt sind, wird zuerst die Ziel-IP-Adresse des Pakets überprüft. Die Zielschnittstelle wird aus der IP-Routing-Tabelle bestimmt. Anschließend überprüft der Router die ARP-Tabelle (Address Resolution Protocol), die dieser Schnittstelle zugeordnet ist, damit eine MAC-Zieladresse im Ethernet-Header platziert wird. Wenn keine gefunden wird, generiert der Router eine ARP-Anfrage für die Ziel-IP-Adresse. Die ARP-Anfrage wird nur an die Zielschnittstelle weitergeleitet. Im Gegensatz zu Bridging wird die ARP-Anforderung an alle Schnittstellen in der Bridge-Gruppe gesendet.

In einem Szenario, in dem unnummerierte Schnittstellen verwendet werden (in dem Sie möglicherweise zwei Teilnehmer im gleichen Subnetz finden), verwendet die geroutete Bridge-Schnittstelle Proxy-ARP. Beispielsweise möchte 192.168.1.2 (Host A) mit 192.168.1.3 (Host B) kommunizieren. Host A ist jedoch im gleichen Subnetz wie Host B.

Host A muss die MAC-Adresse von Host B erlernen, indem er eine ARP-Broadcast an Host B sendet. Wenn die geroutete Bridge-Schnittstelle am Aggregationsgerät diese Übertragung empfängt, sendet sie eine Proxy-ARP-Antwort mit der MAC-Adresse 192.168.1.1, Host A. Diese MAC-Adresse wird übernommen, in den Ethernet-Header eingefügt und das Paket gesendet. Wenn der Router das Paket empfängt, verwirft er den Header und überprüft die Ziel-IP-Adresse und leitet es dann über die richtige Schnittstelle weiter.

Vorteile von RBE

RBE wurde mit der Absicht entwickelt, einige der Probleme der RFC1483-Bridging-Architektur zu lösen. RBE behält die Hauptvorteile der RFC1483-Bridging-Architektur bei und beseitigt die meisten Nachteile.

- Minimale Konfiguration am Standort des Kunden (CPE)Der Service Provider hält dies für wichtig, da er nicht mehr eine große Anzahl von Technikereinsätzen benötigt und nicht mehr viel in Personal für die Unterstützung von Protokollen höherer Ebene investieren muss. Der CPE im Bridge-Modus fungiert als sehr einfaches Gerät. Beim CPE ist nur eine minimale Fehlerbehebung erforderlich, da alles, was aus dem Ethernet kommt, direkt auf die WAN-Seite übertragen wird.
- Einfache Migration von reinen Bridging-Architekturen zu RBE Am Teilnehmerende ist keine Änderung erforderlich.
- Vermeidet IP-Hijacking und ARP-Spoofing, denen typische reine Bridging-Architekturen gegenüberstehen. RBE verhindert auch Broadcast-Stürme über Punkt-zu-Punkt-Verbindungen. Sicherheit ist der größte Nachteil reiner Bridging-Architekturen.
- Im Vergleich zu reinen Bridging-Architekturen bietet RBE aufgrund der Routing-Implementierung auf dem Aggregationsgerät eine überragende Leistung. RBE ist außerdem skalierbarer, da es keine Bridge-Gruppen-Beschränkungen aufweist.
- Unterstützt die Layer-3-Webauswahl mithilfe des Cisco Service Selection Gateway (SSG).

Überlegungen zur Implementierung

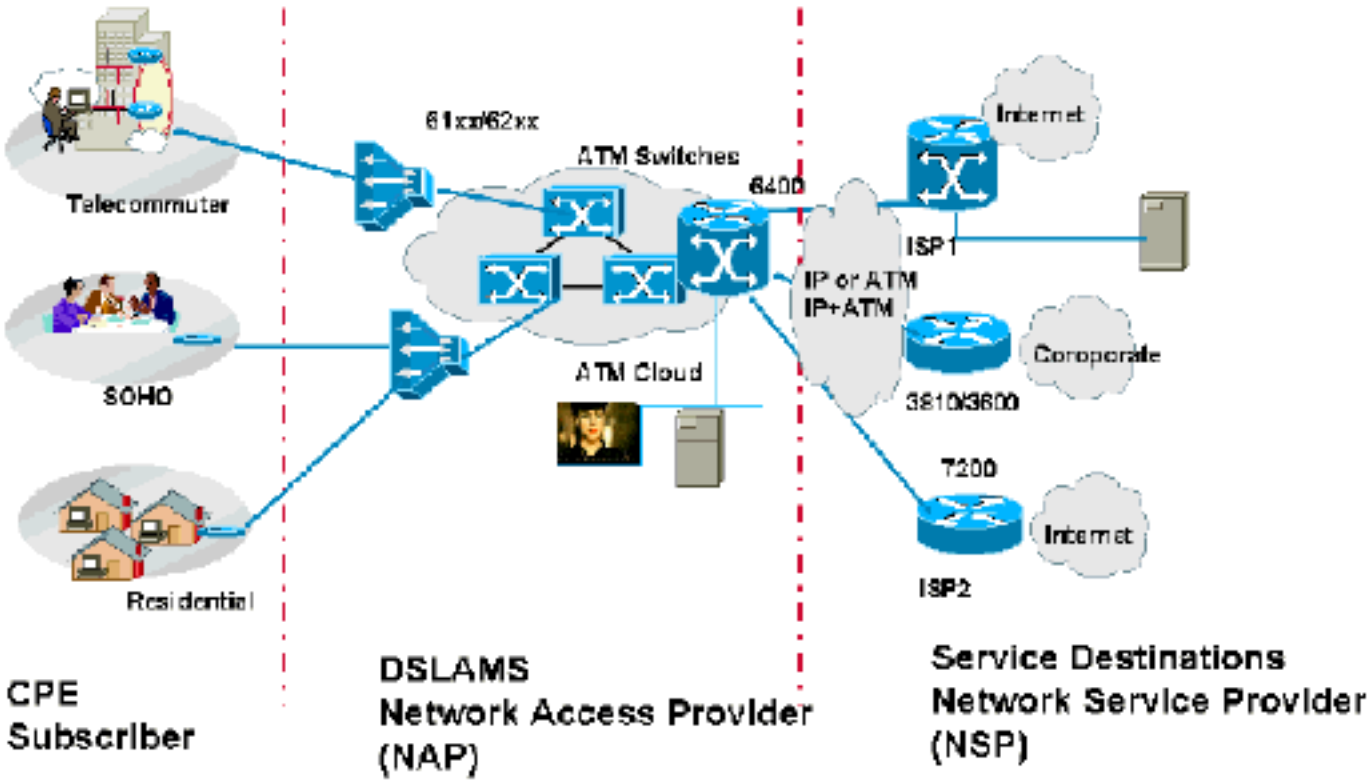
Einige der wichtigsten Punkte, die vor der Implementierung dieser Architektur zu berücksichtigen sind, sind dieselben, die im Whitepaper RFC1483 Bridging Baseline Architecture erwähnt werden.

RBE wird in folgenden Fällen empfohlen:

- Die Szenarien entsprechen denen in vorhandenen Bridging-Architekturen.
- Der NAP möchte nur eine minimale CPE-Verwaltung durchführen. Das Konzept einer einfachen CPE erfordert nur minimale oder gar keine Konfiguration, nachdem die CPE am Standort des Abonnenten bereitgestellt wurde.
- Das NAP möchte keine Host-Clients auf den Hosts hinter dem überbrückten CPE installieren und warten. Diese Installations- und Wartungsaufgaben erhöhen die Bereitstellungs- und Wartungskosten, einschließlich der Bereitstellung von Helpdesk-Mitarbeitern mit Kenntnis der Client-Software und des Betriebssystems, auf dem der Client ausgeführt wird.
- Das NAP möchte ein skalierbares und sicheres überbrücktes Netzwerk mithilfe *vorhandener* CPEs bereitstellen (die nur im RFC1483-Bridging-Modus betrieben werden können) und Service-Auswahlfunktionen anbieten.

In der nächsten Diskussion wird erläutert, wie die RBE-Architektur auf unterschiedliche Geschäftsmodelle zugeschnitten ist und skaliert werden kann.

Netzwerkarchitektur



Die RBE-Netzwerkarchitektur ähnelt der RFC1483-Bridging-Architektur. Wie in dieser Architektur festgelegt, kann sich das Aggregationsgerät entweder im NAP oder beim NSP befinden. Wenn eine End-to-End-Architektur für permanente virtuelle Schaltungen (PVC) verwendet wird, terminiert der NSP die Teilnehmer und konfiguriert das RBE auf dem Aggregationsgerät. Wenn der NAP vorzieht, Großkundenservices plus Serviceauswahl bereitzustellen, kann er diese Teilnehmer beenden und IP-Adressen von einem lokalen DHCP-Server (Dynamic Host Configuration Protocol) beziehen. Bei Großkundenservices kann der NAP die IP-Adressen vom NSP beziehen. Diese Szenarien werden im Abschnitt IP-Management dieses Dokuments ausführlich behandelt.

Überlegungen zum Design der RBE-Architektur

RBE beseitigt die größten Sicherheitsrisiken im Zusammenhang mit der RFC1483-Bridging-Architektur. Darüber hinaus bietet RBE eine höhere Leistung und ist skalierbarer, da die Subschnittstellen als geroutete Schnittstellen behandelt werden.

In diesem Abschnitt werden einige der wichtigsten Punkte erläutert, die vor der Entwicklung der RBE-Architektur berücksichtigt werden müssen. Für Teilnehmer gelten dieselben Designprinzipien wie für die RFC1483-Bridging-Architektur.

In der RBE wird einem einzelnen virtuellen Circuit (VC) eine Route, eine Reihe von Routen oder ein CIDR-Subnetz (Classless Interdomain Routing) zugewiesen. Somit wird die vertrauenswürdige Umgebung auf den Standort eines einzelnen Kunden reduziert, der entweder durch die IP-Adressen in der Routengruppe oder den CIDR-Block repräsentiert wird. Der ISP steuert außerdem die dem Benutzer zugewiesenen Adressen. Hierzu wird ein Subnetz auf der Subschnittstelle für diesen Benutzer konfiguriert. Wenn ein Benutzer Geräte mit einer IP-Adresse außerhalb des zugewiesenen Adressbereichs falsch konfiguriert (was dazu führen kann, dass ARP-Pakete bis zum Router laufen), generiert der Router einen "falschen Kabelfehler" und weigert sich, die falsche IP-MAC-Adressenzuordnung in die ARP-Tabelle einzugeben.

RBE kann nur über Point-to-Point ATM-Subschnittstellen bereitgestellt werden. Sie kann nicht auf Multipoint-Subschnittstellen bereitgestellt werden. Obwohl die Teilnehmernseite überbrückt ist, müssen Sie keine Bridge-Gruppen oder BVI-Schnittstellen definieren, da die Subschnittstellen als geroutete Schnittstellen behandelt werden.

Die Point-to-Point-ATM-Subschnittstellen können nummerierte Schnittstellen sein oder zu anderen Schnittstellen nicht nummeriert sein.

Eine nummerierte Schnittstelle ist per Definition eine Schnittstelle, der eine bestimmte IP-Adresse mit einer festen Subnetzmaske zugewiesen ist. Beispiel:

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

Wie in diesem Beispiel gezeigt, sollte bei der Bereitstellung von RBE mit einer nummerierten Schnittstelle ein separates Subnetz für jeden Teilnehmer vorhanden sein. Der Host am Teilnehmerende sollte für 192.168.1.2 konfiguriert werden. Am Teilnehmerende gibt es nur einen Host. Wenn mehr als ein Host unterstützt werden soll, sollte die gewählte Subnetzmaske mehr Hosts aufnehmen.

Nummerierte Schnittstellen ermöglichen dem NAP die Kontrolle über die Anzahl der Hosts, die der Teilnehmer hinter dem CPE verbunden hat. Wie oben erläutert, war dieser Mangel an Kontrolle ein großes Problem in der RFC1483-Bridging-Architektur.

Diese Methode belegt jedoch zu viele IP-Adressen. Sie müssen jedem Teilnehmer ein Subnetz zuweisen, eine IP-Adresse für die ATM-Subschnittstelle verwenden und die Broadcast-Adresse und alle Nulladressen nicht verwenden. Um also einen Host hinter der CPE zu haben, müssen Sie mindestens die Subnetzmaske 255.255.255.252 definieren. Angesichts der Knappheit an IP-Adressen ist dies möglicherweise nicht umsetzbar, es sei denn, der NAP/NSP verwendet privaten Adressbereich und führt Network Address Translation (NAT) aus, um nach außen zu gelangen.

Um IP-Adressen zu sparen, wäre die Verwendung nicht nummerierter Schnittstellen eine

Alternative. Eine nicht nummerierte Schnittstelle ist definitionsgemäß eine Schnittstelle, die mithilfe des Befehls **ip unnumbered** (**ip unnumbered)** die IP-Adresse einer anderen Schnittstelle verwendet. Beispiel:

```
!
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
```

Wie im obigen Beispiel gezeigt, werden eine IP-Adresse und ein Subnetz nur auf die Loopback-Schnittstelle angewendet. Alle ATM-Subschnittstellen werden für diese Loopback-Schnittstelle nicht nummeriert. In diesem Szenario befinden sich alle Teilnehmer, die an ATM-Subschnittstellen (ohne Loopback 0) terminiert werden, im gleichen Subnetz wie Loopback 0. Dies impliziert, dass Teilnehmer demselben Subnetz angehören, jedoch über verschiedene geroutete Schnittstellen eintreffen. In dieser Situation wird es für den Router problematisch festzustellen, welcher Teilnehmer hinter welcher ATM-Subschnittstelle liegt. Für Cisco IOS wird 192.168.1.0 (im IP-Management-Diagramm) direkt über das Schnittstellen-Loopback 0 verbunden und niemals Datenverkehr an eine der Host-Adressen in diesem Subnetz über eine andere Schnittstelle senden. Um dieses Problem zu beheben, müssen Sie statische Hostrouten explizit konfigurieren. Beispiel:

```
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
```

Wenn der Router eine Routing-Entscheidung treffen und den für 192.168.1.2 bestimmten Datenverkehr weiterleiten muss, wählt er, wie in diesem Beispiel beschrieben, ATM 0/0/0.132 als ausgehende Schnittstelle usw. Ohne Angabe dieser statischen Host-Routen würde der Router die ausgehende Schnittstelle als Loopback 0 auswählen und das Paket verwerfen.

Obwohl die nicht nummerierte Schnittstelle IP-Adressen sparen würde, ist eine zusätzliche Aufgabe erforderlich, statische Hostrouten auf dem Knoten-Route-Prozessor (NRP) für jeden Teilnehmer zu konfigurieren. Wenn ein Teilnehmer beispielsweise 14 Hosts hinter dem CPE hat, müssen für jeden Host keine statischen Host-Routen vorhanden sein. Für die ATM-Subschnittstelle kann eine zusammengefasste Route definiert werden.

Bisher wurde in dieser Erklärung davon ausgegangen, dass die Hosts hinter dem CPE für statische IP-Adressen konfiguriert werden. Diese Annahme gilt nicht für Designs im realen Leben. In der Praxis möchte das NAP eine minimale Konfiguration und Wartung für die CPE und die angeschlossenen Hosts durchführen. Um dies zu erreichen, sollten die Hosts ihre Adressen dynamisch über einen DHCP-Server abrufen.

Um ihre IP-Adressen dynamisch abrufen zu können, müssen Hosts so konfiguriert werden, dass sie IP-Adressen von einem DHCP-Server beziehen. Beim Hochfahren sendet der Host DHCP-Anfragen. Diese Anfragen werden dann an den entsprechenden DHCP-Server weitergeleitet, der dem Host eine IP-Adresse aus dem zuvor definierten Bereich zuweist.

Um die ersten DHCP-Anfragen vom Host an den entsprechenden DHCP-Server weiterzuleiten, sollten Sie den Befehl **ip helper address** auf die Schnittstelle anwenden, die die Broadcasts empfängt. Nachdem die Broadcasts empfangen wurden, prüft das Cisco IOS die Konfiguration der IP-Helper-Adresse für diese Schnittstelle und leitet diese Anfragen in einem Unicast-Paket an den

entsprechenden DHCP-Server weiter, dessen IP-Adresse in der IP-Helper-Adresse angegeben ist. Nachdem der DHCP-Server mit der IP-Adresse antwortet, sendet er die Antwort an die Schnittstelle auf dem Router, der die Anfrage ursprünglich weitergeleitet hat. Diese wird als Ausgangsschnittstelle verwendet, um die DHCP-Serverantwort an den Host zu senden, der den Dienst ursprünglich angefordert hat. Der Router installiert auch automatisch eine Hostroute für diese Adresse.

Wenn RBE auf einer Subschnittstelle aktiviert ist und eine IEEE 802.3 Bridged Protocol Data Unit (PDU) ist, wird die Ethernet-Kapselung nach der Kapselung der ATM-Bridge überprüft. Wenn es sich um ein IP/ARP-Paket handelt, wird es wie jedes andere IP/ARP-Paket behandelt. Das IP-Paket ist schnell geswitcht. Bei einem Fehler wird die Warteschlange für das Switching von Prozessen festgelegt.

Leistung für RBE ist ein großer Vorteil. Der moderne Standard-Bridging-Code hat das Problem, dass zwei separate Klassifizierungen für ein Paket erforderlich sind, bevor eine Weiterleitungsentscheidung getroffen werden kann. Eine Klassifizierung ist definiert als der Prozess der Überprüfung (auf der Upstream-Ebene) und Modifizierung (auf der Downstream-Ebene) des Paket-Headers für die Weiterleitung von Informationen, was relativ teuer ist. Um festzustellen, ob das Paket geroutet oder überbrückt werden muss, ist eine Layer-2-Suche erforderlich. Auf Layer 3 ist dann eine Suche erforderlich, um den Speicherort zu identifizieren, an den das Paket weitergeleitet werden soll. Diese Klassifizierung erfolgt sowohl in der Vor- als auch in der Downstream-Richtung, was sich auf die Leistung auswirkt.

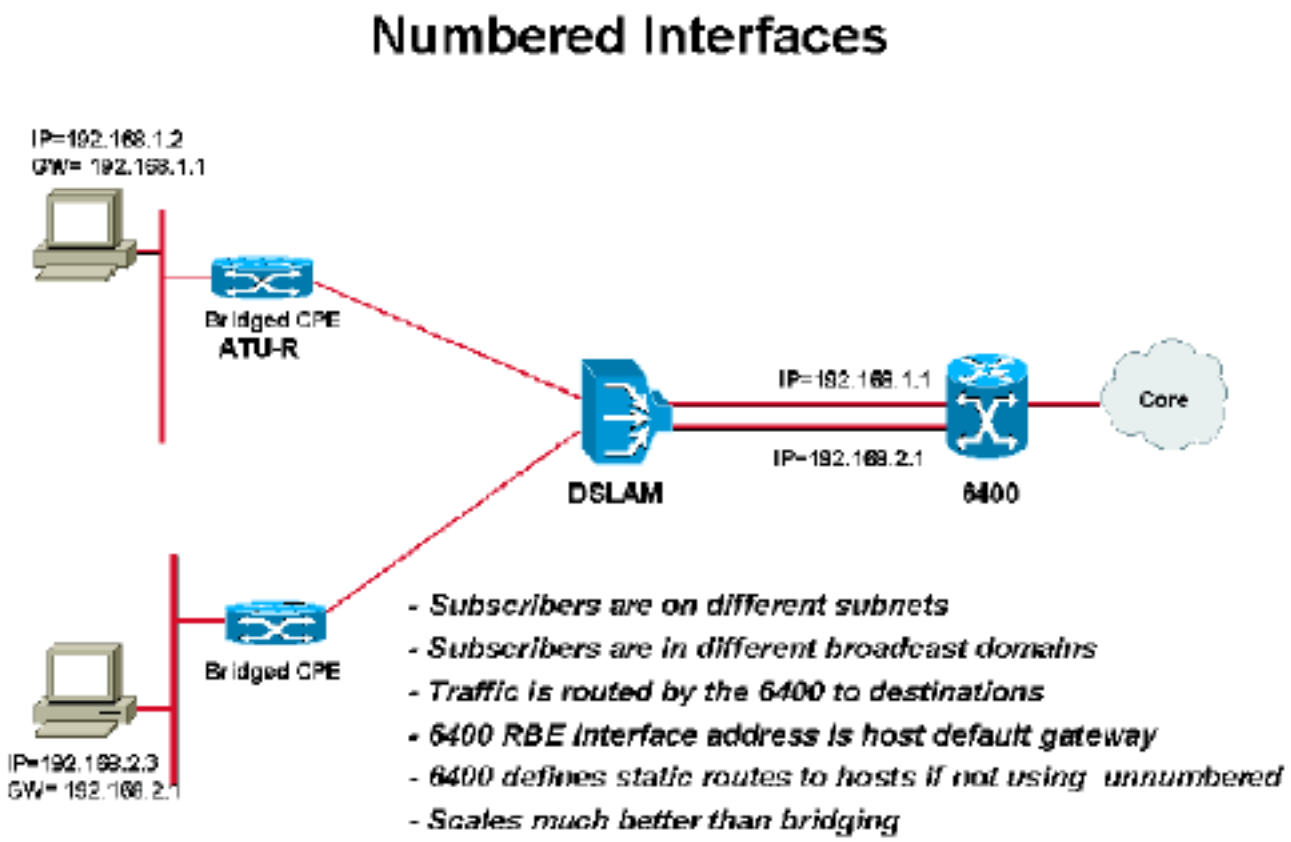
Für RBE wird durch die Konfiguration festgelegt, dass das Paket in die Upstream-Richtung geroutet wird. Daher ist es nicht erforderlich, den Bridging Forwarding-Pfad zu durchlaufen, was bei Standard-Bridging erforderlich war.

Wichtigste Punkte von RBE

CPE

Die CPE-Konfiguration bleibt die gleiche wie beim Standard-Bridging. Für die Bereitstellung von RBE sind keine Änderungen am CPE erforderlich.

IP-Management



Bei der Bereitstellung der nummerierten Schnittstellen für RBE wird die IP-Adressenzuweisung an den Host hinter dem überbrückten CPE in der Regel über einen DHCP-Server abgewickelt. Wie bereits erwähnt, kann sich der DHCP-Server im NAP oder im NSP befinden. In beiden Fällen sollte die nummerierte ATM-Subschnittstelle mit dem Befehl **ip helper address** konfiguriert werden. Wenn sich der DHCP-Server im NSP befindet, muss das NAP-Aggregationsgerät über eine Route verfügen, um diesen Server zu erreichen. Das einzige Szenario, in dem ein NAP einen eigenen DHCP-Server und einen eigenen IP-Adressbereich verwenden würde, besteht darin, den Abonnenten Serviceoptionen anzubieten, und diese Abonnenten sind LAN-verbunden mit dem NAP.

Wenn der NAP den IP-Adressbereich des NSP verwenden möchte, sollte eine der IP-Adressen für jedes Subnetz der ATM-Subschnittstelle zugewiesen werden. Darüber hinaus sollten sich NAP und NSP einigen, sodass die richtige Adresse vom NAP konfiguriert wird. Wenn der DHCP-Server des NSP IP-Adressen zuweist, sollte diese Vereinbarung getroffen werden, um sicherzustellen, dass der Server dem Host die richtigen Standard-Gateway-Informationen bereitstellt. Der NAP kann dann entweder eine statische Route für alle den Teilnehmern zugewiesenen Adressen zusammenfassen oder ein Routing-Protokoll mit dem NSP ausführen, um diese Routen anzukündigen. In den meisten Szenarien ziehen sowohl NAP als auch NSP es vor, kein Routing-Protokoll zu verwenden. Die Bereitstellung einer statischen Route ist eine gute Option.

Dies ist die grundlegende Konfiguration, die im NRP für die Bereitstellung des RBE mit nummerierten Schnittstellen erforderlich ist:

```
!
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
```

Die Verwendung nicht nummerierter Schnittstellen ist die beste Möglichkeit, IP-Adressen zu sparen. Wie bereits erläutert, werden Host-Routen dynamisch installiert, wenn nicht nummerierte Schnittstellen mit DHCP verwendet werden. Dies ist möglicherweise der beste Ansatz für die Bereitstellung von RBE. Der DHCP-Server kann sich dann wie bei nummerierten Schnittstellen entweder am NAP oder am NSP befinden.

Dies ist die grundlegende Konfiguration, die im NRP für die Bereitstellung von RBE mit nicht nummerierten Schnittstellen erforderlich ist:

```
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
```

Erreichen eines Serviceziels

Bisher wurde in diesem Dokument die grundlegende Zugriffstechnologie mit RBE als Kapselungsmethode beschrieben. Mithilfe dieser Architektur kann der NAP/NSP jedoch auch verschiedene Services und Optionen anbieten, über die der NAP den Teilnehmerverkehr an den NSP weiterleiten kann. Diese Konzepte werden in den nächsten Abschnitten erläutert.

Bereitstellen von Internetzugang

In diesem Szenario besteht die primäre Funktion des NSP darin, Endabonnenten Hochgeschwindigkeits-Internetzugang bereitzustellen. Da der NSP den endgültigen Service bereitstellen wird, ist der NSP für das IP-Adressmanagement zuständig. Er kann seinen Endabonnenten mithilfe eines DHCP-Servers öffentliche IP-Adressen zuweisen oder den Abonnenten private IP-Adressen zur Verfügung stellen und dann NAT ausführen, um die Außenwelt zu erreichen.

Großhandel

Wenn der NAP anderen ISPs Großkundenservices anbieten möchte, kann er dies tun. In diesem

Szenario behandelt der NAP normalerweise keine IP-Adressen für alle Teilnehmer verschiedener NSPs. Das NAP trifft einige Vereinbarungen mit dem ISP, um diesen Abonnenten IP-Adressen zur Verfügung zu stellen. Dies kann durch die NAP erreicht werden, die die DHCP-Anfragen der Teilnehmer an die DHCP-Server der NSP weiterleitet. Der NAP muss seine ATM-Subschnittstellen mit einer der IP-Adressen aus diesem Bereich konfigurieren und diese Routen dem NSP melden. Die Routenwerbung kann entweder in Form einer statischen Route oder eines Routing-Protokolls zwischen dem NAP und dem NSP erfolgen. Statische Routen sind die bevorzugte Methode für das NAP und den NSP.

Unternehmenszugriff

Für den Zugriff auf Unternehmen sind in der Regel VPN-Services (Virtual Private Network) erforderlich. Das bedeutet, dass das Unternehmen dem NAP keine IP-Adressen zur Verfügung stellt und es dem NAP nicht gestattet, den firmeneigenen IP-Adressraum im IP-Core des NAP anzukündigen, da dies zu einer Sicherheitsverletzung führen könnte. Unternehmen verwenden ihre eigenen IP-Adressen in der Regel lieber für ihre Clients, oder sie ermöglichen den Zugriff über gesicherte Mittel wie Multiprotocol Label Switching/Virtual Private Network (MPLS/VPN) oder Layer 2 Tunneling Protocol (L2TP).

Der andere Ansatz für die Bereitstellung eines sicheren Unternehmenszugriffs besteht darin, dass das NAP diesen Teilnehmern die ersten IP-Adressen bereitstellt. Daher werden die Teilnehmer an das NAP mit einem LAN verbunden. Wenn die Abonnenten über anfängliche IP-Adressen verfügen, können sie über die auf dem Host ausgeführte L2TP-Client-Software einen Tunnel zum Unternehmen initiieren. Das Unternehmen authentifiziert diesen Teilnehmer und stellt eine IP-Adresse aus seinem IP-Adressbereich bereit. Diese IP-Adresse wird vom L2TP VPN-Adapter verwendet. Auf diese Weise können die Teilnehmer entweder eine Internetverbindung mit ihrem ISP herstellen oder über einen gesicherten L2TP-Tunnelzugriff auf ihren Betrieb zugreifen. Dies erfordert jedoch, dass das Unternehmen dem Teilnehmer die IP-Adresse des Tunnelziels zur Verfügung stellt, die über den IP-Core des NAP geroutet werden kann.

Service-Auswahlfunktionen

Das NAP kann mithilfe der Funktionen der Cisco SSG verschiedene Serviceauswahlfunktionen bereitstellen. Die SSG bietet zwei Methoden zur Bereitstellung der Serviceauswahl: über die Web-Auswahl von Layer 2 (PTA-MD) und Layer 3. Bei RBE kann nur die Web-Auswahlmethode für Layer 3 verwendet werden. Dazu müssen die Teilnehmer an das NAP LAN angeschlossen sein. Das heißt, das NAP stellt dem Teilnehmer die erste IP-Adresse zur Verfügung und ermöglicht den Zugriff auf das Cisco Service Selection Dashboard (SSD).

Im Fall der RBE-Architektur ist die Web-Auswahlmethode der Cisco SSG eine gute Möglichkeit, um den Teilnehmerverkehr zu berücksichtigen.

Schlussfolgerung

RBE bietet eine bessere Leistung und ist skalierbarer als Standard-Bridging. Darüber hinaus werden alle Sicherheitsprobleme, die beim Standard-Bridging auftreten, behoben. RBE beseitigt die Broadcast-Sturm-Probleme durch Standard-Bridging. Das RBE bietet eine robuste Architektur für das NAP, die die Wartung von Client-Host-Software, Bridging-bezogene Probleme und geringere Bereitstellungskosten vermeiden möchte. Mit RBE ist all dies möglich, während die vorhandene Bridging-Architektur verwendet wird.

Zugehörige Informationen

- Support-Informationen für Cisco ADSL-Produkte
- Technischer Support und Dokumentation - Cisco Systems