Routed Brited Encapsulation Architecture

Inhoud

Inleiding

Dit document beschrijft een end-to-end asymmetric Digital Subscriber Line (ADSL)-architectuur die de Routed Bridging Encapsulation (RBE) gebruikt voor Cisco 6400 Universal Access Concentrator (UAC). RBE is ontwikkeld om de bekende RFC1483-overbruggingskwesties aan te pakken, inclusief uitzendstormen en beveiliging. Afgezien van het feit dat de RBE uitsluitend via ATM functioneert, functioneert zij op dezelfde wijze als een halve overbrugging. Aanvullende schaalbaarheid, prestaties en beveiliging kunnen worden bereikt door de unieke kenmerken van xDSL-abonnees te gebruiken.

veronderstelling

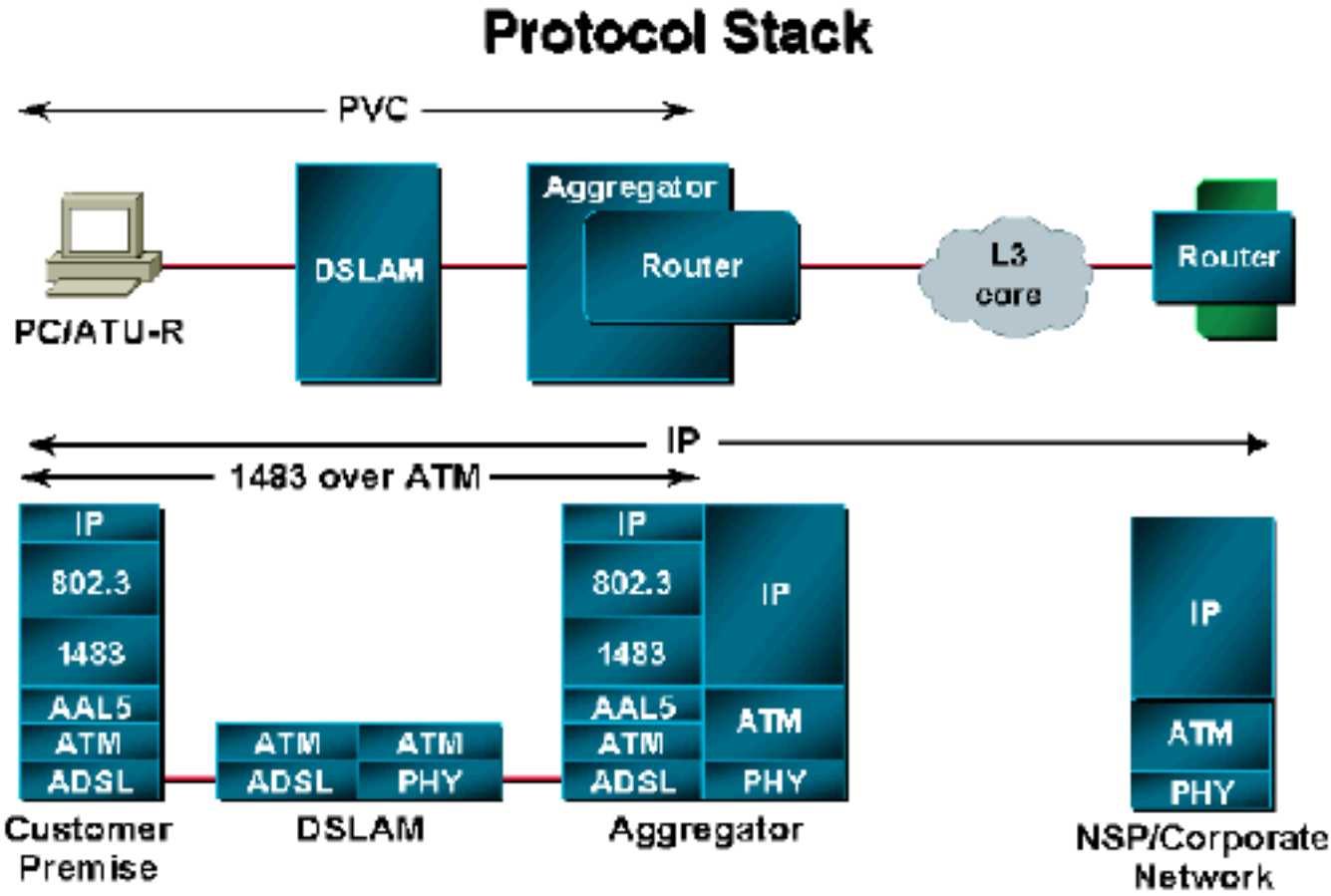
De basisarchitectuur is ontworpen met behulp van het ADSL Forum Reference Architecture Model. De architectuur bestrijkt verschillende serviceaanbiedingen van de Network Access Provider (NAP) en verschillende scenario's van de manier waarop het abonneeverkeer wordt doorgestuurd naar de Network Service Provider (NSP). In deze architectuur, is RBE de veronderstelde insluitingsmethode die door Cisco 6400 wordt gebruikt. De inhoud van dit document is gebaseerd op bestaande implementaties en op enkele interne tests die op de architectuur zijn uitgevoerd. Raadpleeg voor verbeterde functies en wijzigingen de releaseopmerkingen voor de laatste release van Cisco IOS® Software. Momenteel wordt RBE

ondersteund op de Cisco 6400-, Cisco 7200- en Cisco 7500-platforms. Dit document is beperkt tot discussies over Cisco 6400.

Technologische overzichten

Vanuit het netwerkstandpunt ziet de ATM-verbinding eruit als een routeverbinding. Het gegevensverkeer wordt ontvangen als RFC1483-pakketten, maar het zijn RFC1483 Ethernet- of IEEE 802.3-frames. In plaats van het Ethernet- of IEEE 802.3-frame te overbruggen, zoals bij regelmatig RFC1483-overbrugging, routeren de router op Layer 3-header. Met uitzondering van een aantal oppervlakkige controles, wordt de brugkop genegeerd. Dit wordt in de volgende paragraaf uitvoerig toegelicht.

Operationele beschrijving



Vanuit een operationeel standpunt bedient de router zich alsof de routed-bridge interface met een Ethernet LAN was verbonden. De bewerking wordt hieronder op twee manieren beschreven: pakketten die afkomstig zijn van de bedrijfsruimten van de klant en pakketten die bestemd zijn voor de bedrijfsruimten van de klant.

Voor pakketten afkomstig uit het klantengebouw, wordt de Ethernet header overgeslagen en wordt het IP-adres van de bestemming onderzocht. Als het IP-adres van de bestemming in het geheugen van de route is, wordt het pakket snel naar de uitgaande interface geschakeld. Als het bestemming IP adres niet in het routecache staat, wordt het pakket in de wachtrij geplaatst voor processwitching. In de modus van de switch van het proces wordt de uitgaande interface waardoor het pakket moet worden routeerd, gevonden door in de tabel te kijken. Nadat de uitgaande interface is geïdentificeerd, wordt het pakket via die interface routeerd. Dit gebeurt zonder de eis voor een bridge group of Bridge Group Virtual Interface (BVI).

Voor pakketten die voor het klantengebouw bestemd zijn, wordt het IP-adres van de bestemming van het pakket eerst onderzocht. De doelinterface wordt bepaald van de IP-routingtabel. Daarna controleert de router de tabel van het Protocol van de Resolutie van het Adres (ARP) verbonden met die interface voor een bestemming MAC-adres om in de Ethernet-header te plaatsen. Als geen wordt gevonden, genereert de router een ARP-verzoek voor het bestemming IP-adres. Het ARP-verzoek wordt alleen naar de doelinterface doorgestuurd. Dit is in tegenstelling tot het overbruggen, waarin het ARP verzoek wordt verzonden naar alle interfaces in de bridge groep.

Voor een scenario dat ongenummerde interfaces gebruikt (waar u twee abonnees op zelfde netwerk kunt vinden), gebruikt de routed-bridge interface volmacht ARP. Bijvoorbeeld, 192.168.1.2 (Host A) wil met 192.168.1.3 (Host B) communiceren. Host A is echter op dezelfde mate als Host B.

Host A moet het Host B MAC-adres leren door een ARP-uitzending naar Host B. te verzenden. Wanneer de routed-bridge interface bij het aggregation apparaat deze uitzending ontvangt, zal zij een proxy ARP-respons sturen met het MAC-adres van 192.168.1.1, Host A. Het zal dat MAC-adres nemen, het in de Ethernet-header plaatsen en het pakket verzenden. Wanneer de router het pakket ontvangt, verwerpt het de header en kijkt naar het IP-adres van de bestemming, dan routeert u het op de juiste interface.

RBE-voordelen

RBE is ontwikkeld met de bedoeling een aantal van de problemen aan te pakken waarmee de RFC1483-overbruggingsarchitectuur wordt geconfronteerd. RBE behoudt de belangrijkste voordelen van de RFC1483-overbruggingsarchitectuur, terwijl de meeste nadelen ervan worden uitgeschakeld.

- Minimale configuratie in de lokalen van de klant (CPE).De dienstverlener acht dit belangrijk omdat er niet langer een groot aantal vrachtwagenrollen nodig zijn en niet langer sterk in personeel hoeft te investeren om hogere protocollen te ondersteunen. De CPE in bridge mode werkt als een zeer eenvoudig apparaat. Minimale probleemoplossing is bij de CPE betrokken aangezien alles dat in van Ethernet komt recht op de kant van WAN passeert.
- Gemakkelijk te migreren van pure overbruggingsarchitecturen naar RBE. Er is geen wijziging vereist aan de kant van de abonnee.
- Vermijd het kapen van IP en ARP-tapijtproblemen waarmee typische pure overbruggingsarchitecturen worden geconfronteerd. RBE voorkomt ook uitzendstormen door point-to-point verbindingen te gebruiken. Veiligheid is het grootste nadeel in puur overbruggende architecturen.
- Vergeleken met pure overbruggingsarchitecturen, verstrekt RBE superieure prestaties wegens de routerende implementatie bij het aggregatie apparaat. RBE is ook schaalbaarder omdat zij geen bruggroepbeperkingen heeft.
- Ondersteunt Layer 3 webselectie met behulp van de Cisco Service Selection Gateway (SSG).

Uitvoeringsoverwegingen

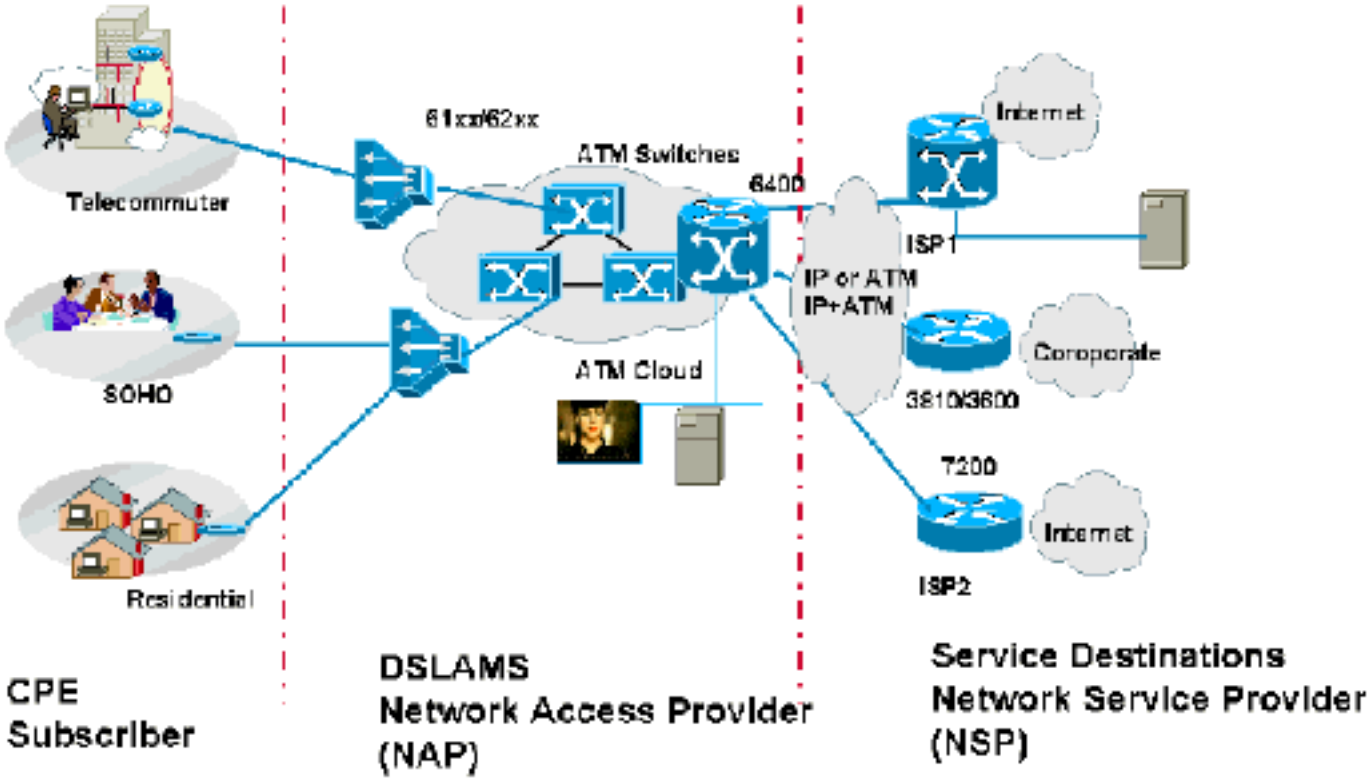
Enkele van de belangrijkste punten die voor de implementatie van deze architectuur in overweging moeten worden genomen zijn dezelfde als die in het RFC1483 Bridging Baseline Architecture-document worden genoemd.

RBE wordt aanbevolen wanneer:

- De scenario's zijn hetzelfde als in bestaande overbruggingsarchitecturen.
- De NAP wil slechts minimaal beheer van CPE's uitvoeren. Het concept van een eenvoudige CPE vereist minimale of geen configuratie nadat de CPE op de plaats van de abonnee wordt opgesteld.
- NAP wil geen gastcliënten op de gastheren achter de overbrugde CPE installeren en onderhouden. Deze installatie- en onderhoudswerkzaamheden verhogen de kosten voor de inzet en het onderhoud, met inbegrip van het ter beschikking stellen van helpdesk-personeel met kennis van de clientsoftware en het besturingssysteem waarop de klant actief is.
- De NAP wil een schaalbaar en beveiligd, overbrugd netwerk inzetten met *bestaande* CPEs (die alleen in RFC1483 overbruggingsmodus kunnen werken) en wil de mogelijkheden voor servicesselectie bieden.

De volgende discussie legt uit hoe de RBE - architectuur op verschillende bedrijfsmodellen past en schaalt.

Netwerkarchitectuur



De RBE netwerkarchitectuur is vergelijkbaar met RFC1483-overbruggingsarchitectuur. Zoals gespecificeerd in die architectuur, zou het aggregatiemiddel ofwel in het NAP ofwel bij het NSP kunnen zijn. Als een end-to-end permanent virtueel circuit (PVC) architectuur wordt gebruikt, beëindigt NSP de abonnees en vormt NSP RBE op het aggregatiemechanisme. Als de NAP er de voorkeur aan geeft om wholesale services plus service selectie te leveren, kan deze abonnees worden afgesloten en IP-adressen krijgen van een lokale DHCP-server (Dynamic Host Configuration Protocol). In het geval van wholesale-diensten kan de NAP ervoor kiezen de IP-adressen van het NSP te verkrijgen. Deze scenario's worden in detail besproken in het gedeelte IP-beheer van dit document.

Ontwerpoverwegingen voor RBE-architectuur

RBE heft de belangrijkste beveiligingsrisico's op die verbonden zijn met de RFC1483-overbruggingsarchitectuur. Daarnaast biedt RBE betere prestaties en is schaalbaar omdat de subinterfaces als routed interfaces worden behandeld.

In dit deel worden enkele van de kernpunten uiteengezet die in overweging moeten worden genomen alvorens de RBE - architectuur te ontwerpen. Voor de abonnee blijven de ontwerpprincipes hetzelfde als in de RFC1483-overbruggingsarchitectuur.

In RBE wordt één Virtual Circuit (VC) toegewezen aan een route, een reeks routes, of een klassen interdomein routing (CIDR). De vertrouwde omgeving wordt dus beperkt tot slechts één lokatie van de klant die wordt vertegenwoordigd door de IP-adressen in de reeks routes of het CIDR-blok. De ISP controleert ook de adressen die aan de gebruiker zijn toegewezen. Dit wordt gedaan door een subinterface op die gebruiker te configureren. Om deze reden, als een gebruiker apparatuur met een IP-adres buiten het toegewezen adresbereik onjuist instelt (mogelijk veroorzaakt dat ARP-pakketten naar de router stromen), genereert de router een "verkeerde kabel"-fout en weigert de onjuiste IP naar MAC-adrestoewijzing in zijn ARP-tabel in te voeren.

RBE kan worden ingezet met alleen point-to-point ATM subinterfaces. Het kan niet op multipoint subinterfaces worden ingezet. Zelfs al wordt de abonnee-kant overbrugd, hoeft u geen bruggroepen of BVI-interfaces te definiëren omdat de subinterfaces als routed interfaces worden behandeld.

De ATM point-to-point subinterfaces kunnen genummerd worden voor interfaces of niet genummerd worden naar andere interfaces.

Per definitie is een genummerde interface een interface die een specifiek IP adres aan het met een vast SUBNET masker heeft toegewezen. Bijvoorbeeld:

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

Zoals in dit voorbeeld wordt getoond, wanneer RBE met een genummerde interface wordt opgesteld, zou er een afzonderlijk netto voor elke abonnee moeten zijn. De host aan de abonnee-kant moet worden geconfigureerd voor 192.168.1.2. Er is slechts één host aan de abonnee-kant. Als het vereiste meer dan één host moet ondersteunen, zou het gekozen subnetmasker meer hosts moeten bevatten.

De genummerde interfaces geven de NAP controle over het aantal hosts dat de abonnee achter de CPE heeft aangesloten. Zoals hierboven is uitgelegd, was dit gebrek aan controle een groot probleem in de RFC1483-overbruggingsarchitectuur.

Deze methode gebruikt echter te veel IP-adressen. U moet één SUBSIDIE per abonnee toewijzen, één IP-adres voor de ATM-subinterface gebruiken en het adres van de uitzending en alle nul-adressen ongebruikt laten. Dus, om één host achter de CPE te hebben moet u op zijn minst een subnetmasker van 255.255.255.252 definiëren. Gezien de schaarste aan IP-adressen is dit mogelijk geen haalbare optie, tenzij NAP/NSP privéadresruimte gebruikt en netwerkadresomzetting (NAT) uitvoert om de buitenwereld te bereiken.

Om IP-adressen te behouden zou een alternatief zijn ongenummerde interfaces te gebruiken. Per definitie is een ongenummerde interface een interface die het IP-adres van een andere interface

gebruikt door de **ip ongenummerde** opdracht te gebruiken. Bijvoorbeeld:

```
!
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
```

Zoals in het bovenstaande voorbeeld wordt getoond, worden een IP adres en IP slechts toegepast op de loopback interface. Alle ATM-subinterfaces zouden niet genummerd zijn naar die loopback-interface. In dit scenario, zouden alle abonnees die op ATM subinterfaces (niet genummerd tot loopback 0) worden beëindigd op dezelfde ubnet zijn als die van loopback 0. Dit impliceert dat de abonnees op dezelfde vorm van net zouden zijn, maar zouden door verschillende routed interfaces worden binnengebracht. In deze situatie wordt het een probleem voor de router om te identificeren welke abonnee erachter zit welke ATM-subinterface. Voor Cisco IOS wordt 192.168.1.0 (in het diagram van het IP-beheer) direct verbonden via interface loopback 0 en het zal nooit verkeer verzenden dat voorbestemd is voor een van de host-adressen op dat subnetwerk via een andere interface. Om deze kwestie op te lossen, moet u expliciet statische hostroutes configureren. Bijvoorbeeld:

```
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
```

Zoals in dit voorbeeld wordt gespecificeerd, wanneer de router een Routing- besluit moet nemen en het verkeer dat voor 192.168.1.2 is bestemd moet doorsturen, zal de router ATM 0/0/132 als uitgaande interface kiezen, enzovoort. Zonder die statische hostroutes te specificeren, zou de router de uitgaande interface als loopback 0 kiezen en het pakket laten vallen.

Zelfs al zou de ongenummerde interface IP-adressen besparen, vereist het een extra taak om statische host-routes op de Node routeprocessor (NRP) te configureren voor elke abonnee. Merk op dat als een abonnee, bijvoorbeeld, 14 hosts achter de CPE heeft, het niet nodig is om statische host-routes voor elke host te hebben. Een samengevatte route kan worden gedefinieerd voor de ATM-subinterface.

Tot nu toe is deze uitleg ervan uitgegaan dat de hosts achter de CPE zullen worden geconfigureerd voor statische IP-adressen. Deze veronderstelling geldt niet voor echte ontwerpen. In de praktische wereld, wil NAP minimale configuratie en onderhoud voor de CPE en de gastheren uitvoeren die aan het verbonden zijn. Om dat te bereiken, zouden de hosts hun adressen dynamisch moeten krijgen met behulp van een DHCP-server.

Om hun IP adressen dynamisch te krijgen moeten de hosts worden geconfigureerd om IP-adressen te krijgen van een DHCP-server. Wanneer de host opstart, stuurt het DHCP-verzoeken uit. Deze verzoeken worden dan doorgegeven aan de juiste DHCP-server, die een IP-adres aan de host toewijzen in het eerder gedefinieerde bereik.

Om de eerste DHCP-verzoeken van de host naar de juiste DHCP-server door te sturen, moet u de opdracht **ip** hulpadres toepassen op de interface die de uitzendingen ontvangt. Nadat de uitzendingen worden ontvangen, bekijkt Cisco IOS de configuratie van het ip helper-adres voor die interface en zendt die verzoeken in een unicast pakket naar de aangewezen server van DHCP waarvan IP adres in ip helper-adres wordt gespecificeerd. Nadat de DHCP-server antwoordt met het IP-adres, stuurt het de reactie op de interface op de router die oorspronkelijk het verzoek had

doorgestuurd. Dit wordt gebruikt als de uitgaande interface om de DHCP-serverrespons naar de host te verzenden die oorspronkelijk om de service vroeg. De router installeert ook automatisch een ontvangstroute voor dit adres.

Als RBE op een subinterface is ingeschakeld en een IEEE 802.3-bridging protocol gegevenseenheid (PDU) is, wordt de Ethernet-insluiting onderzocht na ATM-bridge-insluiting. Als het een IP/ARP-pakket is, wordt het behandeld zoals een ander IP/ARP-pakket. Het IP-pakket is snel geschakeld. Als dit mislukt, wordt er een wachtrij voor processwitching geplaatst.

Prestaties voor RBE zijn een grote overwinning. De huidige standaard bridging code heeft het inherente probleem van het vereisen van twee afzonderlijke classificaties voor een pakket voordat een verzendende beslissing kan worden genomen. Een classificatie is gedefinieerd als het proces van het onderzoeken (in de upstream) en het wijzigen (in de downstream) van de pakketheader voor het doorsturen van informatie, wat relatief duur is. Een Layer 2 raadpleging is nodig om te bepalen of het pakket moet worden routeerd of overbrugd. Vervolgens is bij Layer 3 een raadpleging nodig om de locatie te bepalen waar het pakket moet worden routeerd. Deze indeling vindt plaats zowel in de stroomopwaarts als in de stroomafwaartse richting, hetgeen van invloed is op de prestaties.

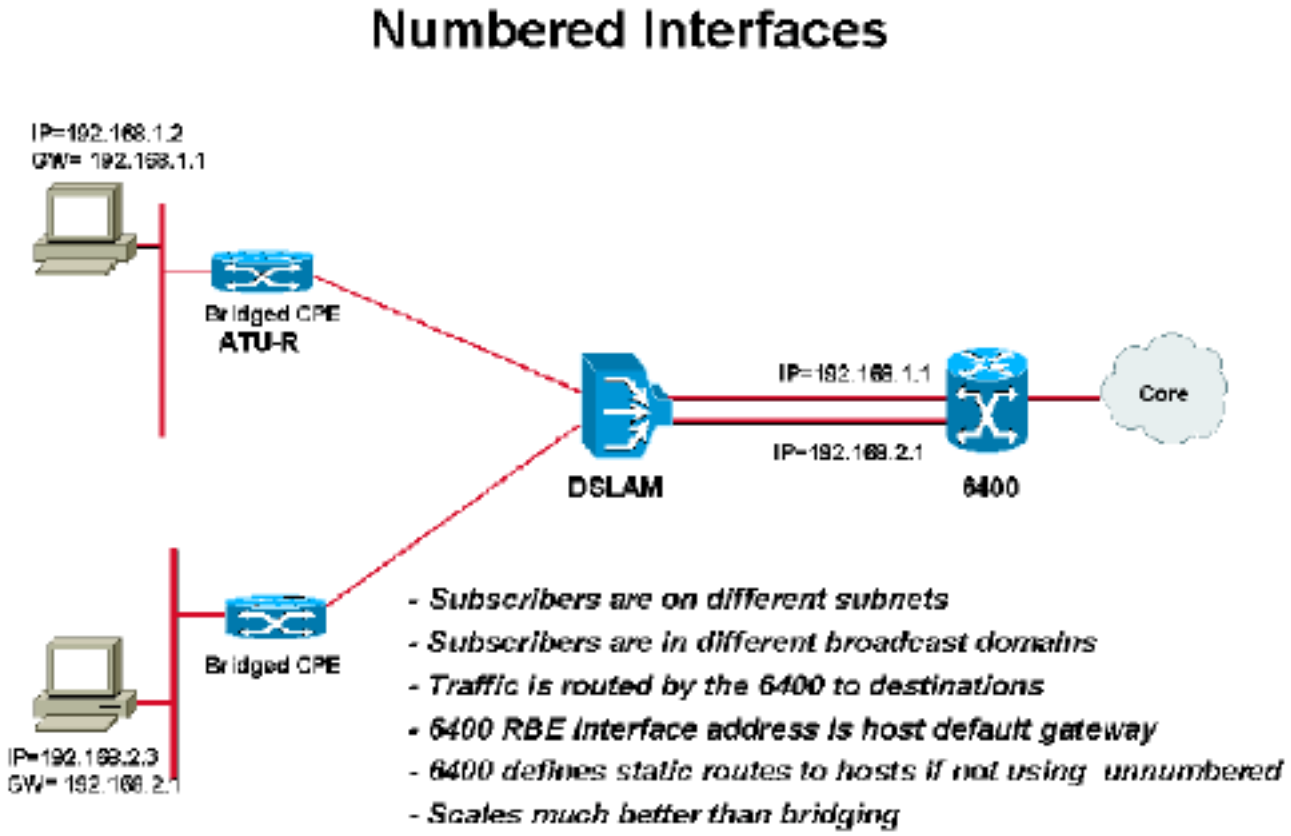
Voor RBE wordt door de configuratie vooraf bepaald dat het pakket in de stroomopwaartse richting moet worden verstuurd. Daarom is het niet nodig om door het overbruggingspad te gaan, dat noodzakelijk was bij standaardoverbrugging.

Belangrijkste punten van RBE

CPE

De CPE-configuratie blijft hetzelfde als in het standaardbruggen. Er zijn geen wijzigingen in de CPE nodig om RBE in te zetten.

IP-beheer



Terwijl het opstellen van de genummerde interfaces voor RBE, wordt de IP adrestoewijzing aan de gastheer achter de overbrugde CPE gewoonlijk behandeld via een server van DHCP. Zoals eerder vermeld, kan de DHCP-server in het NAP of in het NSP verblijven. In beide gevallen moet de genummerde ATM-subinterface worden geconfigureerd met de opdracht **ip-**adres. Als de DHCP-server zich op de NSP zal bevinden, moet het NAP-aggregatieapparaat een route hebben om die server te bereiken. Het enige scenario waarin een NAP zijn eigen DHCP-server en IP-adresbereik zou gebruiken is wanneer deze de servicesselectie functies aan de abonnees wil aanbieden, en deze abonnees zijn LAN aan de NAP verbonden.

Als NAP de IP adresruimte van NSP wil gebruiken, zou één van de IP adressen voor elke vorm van netwerk aan de ATM subinterface moeten worden toegewezen. Ook dient er enige onderlinge overeenstemming te zijn tussen de NAP en de NSP, zodat de NAP het juiste adres vormt. Wanneer de DHCP-server van de NSP IP-adressen toewijst, moet deze overeenkomst van kracht zijn om ervoor te zorgen dat de server de juiste standaard gateway-informatie aan de host levert. NAP kan dan een statische route voor al die adressen samenvatten die aan abonnees zijn toegewezen, of zij kan kiezen om een routingprotocol met NSP te lopen om die routes te adverteren. In de meeste scenario's, zouden zowel NAP als NSP liever geen routingprotocol gebruiken. Het verstrekken van een statische route is een goede optie.

Dit is de basisconfiguratie die op de NRP vereist is voor het inzetten van RBE met genummerde interfaces:

```
!
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
```

Ongenummerde interfaces gebruiken is de beste manier om IP-adressen te besparen. Zoals eerder uitgelegd, wanneer ongenummerde interfaces met DHCP worden gebruikt, zijn de hostroutes dynamisch geïnstalleerd. Dit kan de beste aanpak zijn om RBE in te zetten. De DHCP-server kan zich dan in de NAP of de NSP bevinden, zoals voor genummerde interfaces.

Dit is de basisconfiguratie die op de NRP vereist is voor het inzetten van RBE met ongenummerde interfaces:

```
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
```

Hoe een serviceresbestemming wordt bereikt

Tot nu toe heeft dit document de basis toegangstechnologie besproken met behulp van RBE als insluitingsmethode. Wanneer u deze architectuur gebruikt, kan NAP/NSP echter ook verschillende services en opties aanbieden waarvoor NAP het abonneeverkeer naar NSP kan doorsturen. Deze concepten worden in de volgende paragrafen toegelicht.

Internettoegang bieden

In dit scenario is de primaire functie van de NSP het verstrekken van snelle internettoegang aan de eindabonnees. Omdat het NSP de laatste service gaat leveren, wordt IP-adresbeheer de verantwoordelijkheid van het NSP. Het kan openbare IP-adressen aan zijn eindabonnees toewijzen met behulp van een DHCP-server, of het kan ervoor kiezen om privé IP-adressen aan de abonnees te geven en dan NAT uitvoeren om de buitenwereld te bereiken.

groothandel

Als het NAP wholesale services wil aanbieden aan andere ISP's, kan het dat doen. In dit scenario hanteert de NAP doorgaans geen IP-adressen voor alle abonnees voor verschillende NSP's. NAP treft enige regeling met de ISP om IP-adressen aan deze abonnees te verstrekken. Dit kan worden bereikt door de NAP die de DHCP-verzoeken van de abonnees naar de DHCP-servers bij de NSP's doorstuurt. NAP moet zijn ATM subinterfaces met één van de IP adressen van dat

bereik configureren en deze routes naar het NSP adverteren. De routereclame zou in de vorm van of een statische route of een of ander routingprotocol tussen NAP en NSP kunnen zijn. Statische route is de voorkeursmethode voor de NAP en de NSP.

Toegang tot bedrijven

Voor toegang tot bedrijven zijn doorgaans VPN-services (Virtual Private Network) nodig. Dit betekent dat de onderneming geen IP-adressen aan de NAP zal verstrekken en de NAP niet in staat zal stellen de zakelijke IP-adresruimte in de IP-kern van de NAP te adverteren, aangezien dit zou kunnen leiden tot een inbreuk op de beveiliging. Bedrijven geven er doorgaans de voorkeur aan hun eigen IP-adressen toe te passen aan hun klanten, of ze zullen toegang verlenen via bepaalde beveiligde middelen zoals Multiprotocol Label Switching/Virtual Private Network (MPLS/VPN) of Layer 2 Tunneling Protocol (L2TP).

De andere benadering van het bieden van beveiligde toegang voor ondernemingen is waar de NAP de eerste IP-adressen aan deze abonnees verstrekt. Daarom worden de abonnees LAN-aangesloten op de NAP. Nadat de abonnees de eerste IP-adressen hebben, kunnen zij een tunnel naar het bedrijf openen via L2TP-clientsoftware die op de host actief is. Het bedrijf zal deze abonnee op zijn beurt controleren en een IP-adres vanuit de IP-adresruimte verstrekken. Dit IP-adres wordt gebruikt door de L2TP VPN-adapter. Op deze manier kunnen de abonnees ofwel verbinding maken met hun ISP voor internetverbinding of toegang tot hun bedrijf verkrijgen via een beveiligde L2TP-tunneltoegang. Dit vereist echter dat de onderneming het IP-adres van de tunnelbestemming aan de abonnee verstrekt, dat routeerbaar moet zijn via de IP-kern van de NAP.

Servicesselectiecapaciteiten

NAP kan verschillende mogelijkheden voor servicesselectie bieden met behulp van de functionaliteit van Cisco SSG. De SSG biedt twee methoden voor de keuze van de diensten: via Layer 2 (dat bekend staat als PTA-MD) en Layer 3 webselectie. Met RBE kan alleen Layer 3 Web Selectiemethode worden gebruikt. Dit vereist dat de abonnees LAN-aangesloten zijn op de NAP; dwz, het NAP verstrekt het eerste IP-adres aan de abonnee en geeft toegang tot het Cisco Service Selection Dashboard (SSD).

In het geval van RBE-architectuur is de selectiemethode van Cisco SSG een goede manier om rekening te houden met abonneeverkeer.

Conclusie

RBE biedt betere prestaties en is schaalbaarder dan standaard overbrugging. Het voorziet ook in de oplossing van alle veiligheidsproblemen in verband met standaardoverbrugging. RBE heft de problemen van de uitzendstorm van standaard overbrugging op. RBE biedt een robuuste architectuur voor de NAP die het onderhoud van de software van de gastheer van de cliënt, overbruggingsgerelateerde kwesties, wil vermijden en lagere implementatiekosten wil. Met RBE is dit alles mogelijk bij gebruik van de bestaande overbruggingsarchitectuur.

Gerelateerde informatie

- Cisco ADSL-productondersteuningsinformatie
- Technische ondersteuning en documentatie – Cisco Systems