PPPoA-basislijnarchitectuur

Inhoud

Inleiding

In dit document wordt een end-to-end asymmetrische ADSL-architectuur (Digital Subscriber Line) beschreven met Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA). Hoewel de meeste implementaties zijn gebaseerd op de overbruggingsarchitectuur, wint PPPoA een enorme populariteit en zal het een groter deel van toekomstige ADSL-implementaties vormen.

veronderstelling

De basisarchitectuur veronderstelt de noodzaak om snelle internettoegang en zakelijke toegang tot de eindabonnee te bieden door PPPoA als kernbackbone te gebruiken. We zullen deze architectuur bespreken, gebaseerd op private virtuele kanalen (PVC's), de methode die het meest wordt gebruikt in de huidige implementaties. De architectuur met switched virtuele circuits (SVC's) wordt in een afzonderlijk document besproken.

Dit document is gebaseerd op bestaande implementaties en interne tests van de architectuur.

Dit document is geschreven onder de aanname dat de lezer kennis heeft en bekend is met de ontwerpoverwegingen van een Network Access Provider (NAP), zoals beschreven in het witboek RFC1483 Bridging Baseline Architecture.

Technologische overzichten

Point-to-Point Protocol (PPP) (RFC 1331) biedt een standaardmethode om hogere laagprotocollen tussen point-to-point verbindingen in te kapselen. Het verlengt de HDLC-pakketstructuur (High-Level Data Link Control) met een 16-bits protocol-identificator die informatie over de inhoud van het pakket bevat.

Het pakket bevat drie soorten informatie:

- Link Control Protocol (LCP) - onderhandelt over linkparameters, pakketgrootte of type verificatie
- Network Control Protocol (NCP) - bevat informatie over meerlaagse protocollen inclusief IP en IPX, en hun controleprotocollen (IPCP voor IP)
- Gegevensframes

PPP over ATM adapterlaag 5 (AAL5) (RFC 2364) gebruikt AAL5 als het framed protocol, dat zowel PVC als SVC ondersteunt. PPPoA werd primair ten uitvoer gelegd als deel van ADSL. Het maakt gebruik van RFC1483, die werkt in een Logical Link Control-Subnetwork Access Protocol (LLC-SNAP) of in een VC-Mux-modus. Een CPE-apparaat (Customer Space Equipment) kapselt de PPP-sessie in die op deze RFC is gebaseerd voor transport over de ADSL-lijn en de digitale DSLAM-toegangsmultiplexer (Digital Subscriber Line).

Voordelen en nadelen van PPPoA-architectuur

De architectuur PPPoA erft de meeste voordelen van PPP die in het Stealmodel wordt gebruikt. Hieronder worden een aantal belangrijke punten genoemd.

Voordelen

- Elke sessie gebaseerd op Wachtwoord Verificatie Protocol (PAP) of Challenge Handshake Authentication Protocol (CHAP). Dit is het grootste voordeel van PPPoA aangezien de authenticatie het veiligheidsgat in een overbruggingsarchitectuur overtreft.
- Per sessie is een boekhouding mogelijk, waardoor de dienstverlener de abonnee kan aanrekenen op basis van de sessietijd voor verschillende aangeboden diensten. Per sessie-accounting stelt een dienstverlener in staat om een minimum toegangsniveau voor minimale kosten aan te bieden en dan abonnees voor extra gebruikte diensten in rekening te brengen.
- IP-adresbehoud op de CPE. Hiermee kan de serviceprovider slechts één IP-adres voor een CPE toewijzen, waarbij CPE is ingesteld voor netwerkadresomzetting (NAT). Alle gebruikers achter één CPE kunnen één enkel IP-adres gebruiken om verschillende bestemmingen te bereiken. IP-beheeroverhead voor de Network Access Provider/Network Services Provider (NAP/NSP) voor elke individuele gebruiker wordt verminderd terwijl IP-adressen worden bewaard. Daarnaast kan de serviceprovider een klein subnetwerk van IP-adressen bieden om de beperkingen van PAT-adresomzetting (Port Adapters) en NAT te overwinnen.
- NAP's/NSP's bieden veilige toegang tot bedrijfsgateways zonder end-to-end PVC's te beheren en Layer 3-routing of Layer 2 Forwarding/Layer 2 Tunneling Protocol-tunnels (L2F/L2TP) te gebruiken. Daarom kunnen zij hun bedrijfsmodellen voor de verkoop van wholesale-diensten opschalen.
- Problemen oplossen bij individuele abonnees. NSP kan gemakkelijk identificeren welke abonnees op of uit op actieve PPP sessies zijn gebaseerd, in plaats van volledige groepen op te lossen zoals bij het overbruggen van architectuur het geval is.
- NSP kan een overabonnement nemen door inactiviteitstimpjes en sessieopties te

implementeren met behulp van een industriestandaard afstandsverificatie, inbel-gebruikersservice (RADIUS) server voor elke abonnee.
- Zeer schaalbaar aangezien we een zeer hoog aantal PPP-sessies op een aggregatie-router kunnen beëindigen. Verificatie, autorisatie en accounting kunnen voor elke gebruiker worden verwerkt met externe RADIUS-servers.
- Optimaal gebruik van functies in de Service Selection Gateway (SSG).

nadelen

- Slechts één sessie per CPE op één virtueel kanaal (VC). Aangezien de gebruikersnaam en het wachtwoord op de CPE zijn ingesteld, kunnen alle gebruikers achter de CPE voor die specifieke VC slechts tot één reeks diensten toegang hebben. De gebruikers kunnen geen verschillende sets services selecteren, alhoewel het gebruik van meerdere VC's en het instellen van verschillende PPP-sessies op verschillende VC's mogelijk is.
- Verhoogde complexiteit van de CPE-instellingen. Het personeel van de helpdesk bij de dienstverlener moet meer kennis hebben. Aangezien de gebruikersnaam en het wachtwoord op de CPE zijn ingesteld, moet de abonnee of de CPE-verkoper een setup-wijziging doorvoeren. Het gebruik van meerdere VC's verhoogt de complexiteit van de configuratie. Dit kan echter worden overwonnen door een automatische configuratie optie die nog niet is vrijgegeven.
- De dienstverlener moet een database van gebruikersnamen en wachtwoorden voor alle abonnees bijhouden. Indien tunnels of proxydiensten worden gebruikt, kan de authenticatie plaatsvinden op basis van de domeinnaam en de gebruikersverificatie gebeurt via de poort van het bedrijf. Dit beperkt de omvang van de gegevensbank die de dienstverlener moet onderhouden.
- Als één enkel IP-adres aan CPE wordt verstrekt en NAT/PAT wordt geïmplementeerd, zullen bepaalde toepassingen zoals IPTV, die IP-informatie in de lading insluiten, niet werken. Als bovendien een IP-subnetoptie wordt gebruikt, moet een IP-adres ook voor CPE worden gereserveerd.

Overwegingen bij implementatie voor PPPoA-architectuur

Belangrijkste punten die in overweging moeten worden genomen voordat u de PPPoA-architectuur implementeert zijn:

- Het aantal abonnees dat momenteel en in de toekomst zal worden onderhouden, aangezien dit het aantal vereiste PPP-sessies beïnvloedt.
- Of de PPP sessies bij de serviceprovider worden beëindigd?s aggregation router of doorgestuurd naar andere zakelijke gateways of Internet Service Providers (ISP's).
- Of de dienstverlener of de eindbestemming het IP-adres aan de abonnee verstrekt?
- Of de opgegeven IP-adressen wettelijk openbaar of privé zijn. Gaat de CPE NAT/PAT doen of wordt NAT uitgevoerd bij de eindbestemming?
- profielen van eindabonnees, residentiële gebruikers, klanten van klein kantoor huiskantoor (SOHO), en telecombedrijven.
- Bij meer dan één gebruiker, of alle gebruikers dezelfde eindbestemming of -dienst moeten bereiken, of ze allemaal verschillende dienstbestemmingen hebben.
- Levert de dienstverlener diensten met toegevoegde waarde zoals spraak of video? Vereist de

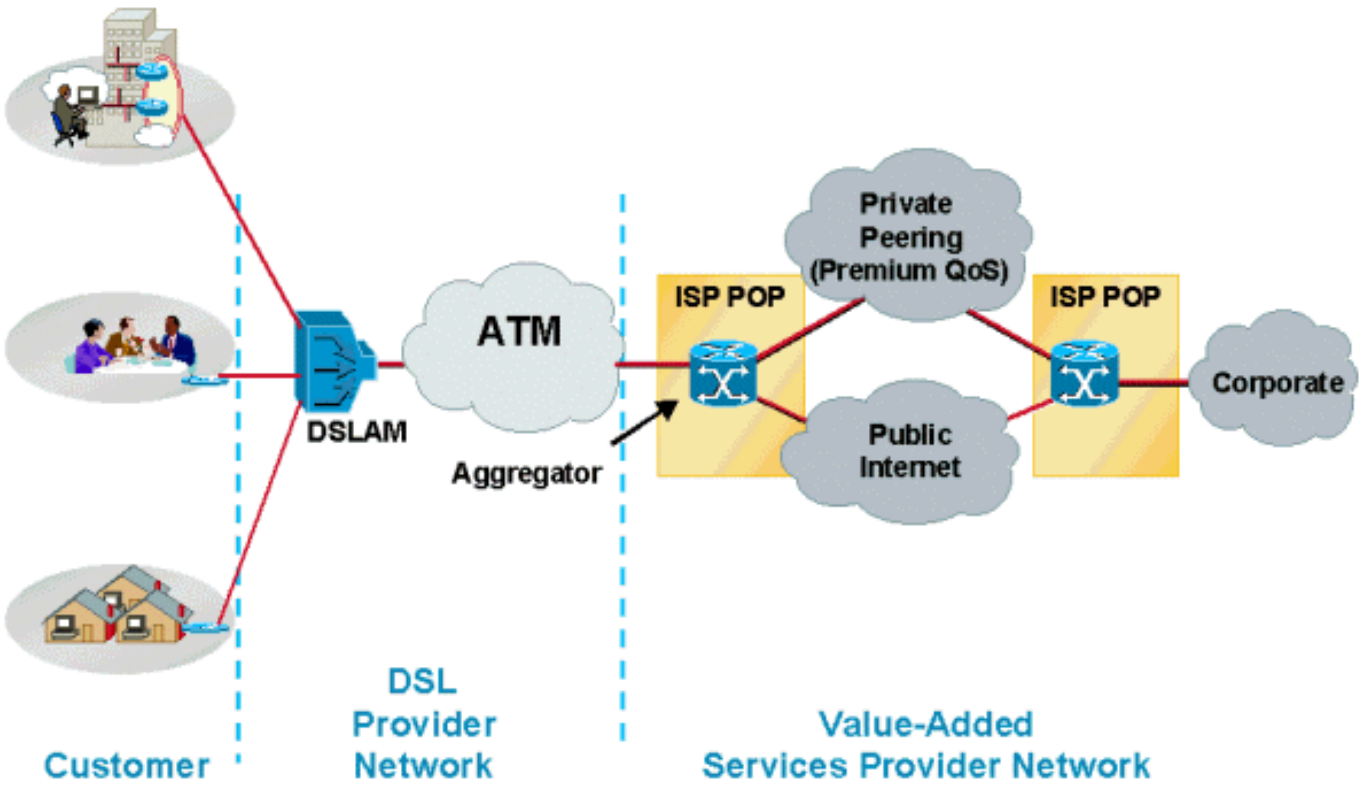
dienstverlener dat alle abonnees eerst naar een bepaald netwerk gaan voordat zij een eindbestemming bereiken? Wanneer abonnees SSG gebruiken, gaan zij passthrough services, PPP Terminated Aggregation (PTA), een bemiddelings apparaat of proxy gebruiken?

- Hoe de serviceprovider abonnees factureert—op basis van een plat tarief, gebruik per sessie of gebruikte services.
- Invoering en bevoorrading van CPE's, DSLAM's en aggregatiepunten van aanwezigheid (POP's).
- Het bedrijfsmodel voor de NAP. Omvat het model ook de verkoop van wholesale-diensten zoals veilige zakelijke toegang en diensten met toegevoegde waarde zoals spraak en video? Zijn NAP's en NSP's dezelfde entiteit?
- Het bedrijfsmodel van de onderneming. Is deze vergelijkbaar met een onafhankelijke lokale beursluchtvaartmaatschappij (ILEC), een concurrerende lokale beursvervoerder (CLEC) of een ISP?
- De typen toepassingen die NSP aanbiedt aan de eindabonnee.
- Het verwachte stroomvolume en stroomafwaartse gegevensstroom.

Met deze punten in gedachten houden zullen we bespreken hoe de PPPoA-architectuur zal passen en opschalen naar verschillende bedrijfsmodellen voor serviceproviders en hoe de providers ervan kunnen profiteren door gebruik te maken van deze architectuur.

Standaard PPPoA-netwerkarchitectuur

In het volgende diagram wordt een typische PPPoA-netwerkarchitectuur weergegeven. Klanten die CPEs gebruiken verbinden met het netwerk van de dienstverrichter door een DSLAM van Cisco, die aan een Cisco 6400 aggregator met ATM verbindt.



Ontwerpoverwegingen voor PPPoA-architectuur

In het gedeelte "Overwegingen bij implementatie" van dit document kunnen PPPoA-architecturen worden ingezet met verschillende scenario's, afhankelijk van het bedrijfsmodel van de serviceprovider. In dit deel zullen we de verschillende mogelijkheden en overwegingen bespreken die de dienstverleners in gedachten moeten houden alvorens een oplossing te vinden.

Voordat u een PPPoA-architectuur en een bepaalde oplossing voor deze architectuur implementeert, is het van essentieel belang om het bedrijfsmodel van de serviceprovider te begrijpen. Neem de diensten die de dienstverlener zal aanbieden. Zal de dienstverlener één dienst zoals snelle internettoegang aanbieden aan zijn eindabonnees of zal hij groothandelsdiensten aan verschillende ISP's verkopen en aan die abonnees diensten met toegevoegde waarde leveren? Zal de dienstverlener deze allemaal aanbieden?

In het geval van snelle internettoegang in een omgeving waar NSP en NAP hetzelfde zijn, moeten de PPP-sessies van de abonnee in de ingestelde aggregatie-router worden beëindigd. In dit scenario moeten serviceproviders overwegen hoeveel PPP sessies op één apparaat voor routeraggregatie kunnen worden afgesloten, hoe de gebruikers geauthentiseerd zullen worden, hoe ze accounting gaan uitvoeren en het pad naar het internet wanneer gebruikerssessies beëindigd worden. Afhankelijk van het aantal PPP sessies en abonnees, kan de aggregation router een Cisco 6400 of een Cisco 7200 zijn. Vandaag de dag? kan Cisco 6400 met 7 knoop routeprocessors (NRPs) tot 14.000 PPP sessies beëindigen. Cisco 7200 is beperkt tot 2.000 PPP-sessies. Deze aantallen zullen veranderen door nieuwe releases. Controleer de release opmerkingen en productdocumenten op het exacte aantal sessies dat elke aggregatie-router kan ondersteunen.

Verificatie en accounting door gebruikers in dit scenario kan het best worden afgehandeld door gebruik te maken van een industriestandaard RADIUS-server, die een gebruiker kan authenticeren op basis van de gebruikersnaam of de virtuele pad-ID/virtuele kanaalidentificator (VPI/VCI) die wordt gebruikt.

Voor snelle internettoegang betalen NSP's doorgaans een vast tarief aan hun klanten. De meeste van de huidige implementaties worden op deze manier geïmplementeerd. Wanneer NSP en NAP dezelfde entiteit zijn, worden klanten gefactureerd tegen een vast tarief voor toegang en een ander vast tarief voor internettoegang. Dit model verandert wanneer de dienstverlener diensten met toegevoegde waarde begint aan te bieden. Serviceproviders kunnen de klant aanrekenen op basis van het soort dienst en de duur van de dienst. Klanten verbinden met internet door de aggregatie router die protocollen zoals Open Snelste Pad (OSPF) of Enhanced Interior Gateway Routing Protocol (DHCP) gebruikt naar een randrouter die Border Gateway Protocol (BGP) kon uitvoeren.

Een andere optie die de serviceprovider heeft voor het aanbieden van snelle internettoegang is om de inkomende PPP-sessies van abonnees naar een afzonderlijke ISP te verzenden met behulp van L2TP/L2F-tunneling. Wanneer L2x-tunneling wordt gebruikt, moet bijzondere aandacht worden besteed aan de wijze waarop de tunnelbestemming kan worden bereikt. Beschikbare opties zijn om een aantal routingprotocollen uit te voeren of statische routes in de aggregatie router te bieden. Beperkingen bij gebruik van L2TP- of L2F-tunnels zijn: 1) het aantal tunnels en het aantal sessies dat in deze tunnels kan worden ondersteund; en (2) het gebruik van routingprotocollen die niet compatibel zijn met ISP's van derden, wat het gebruik van statische routes kan vereisen.

Als de serviceprovider services voor verschillende ISP's of bedrijfsgateways aan de eindabonnee

aanbiedt, moeten ze mogelijk SSG-functies op de aggregation router implementeren. Dit staat de abonnee toe om verschillende servicesbestemmingen te selecteren door op Web-gebaseerde servicesselectie te gebruiken. De dienstverlener kan of PPP-sessies van abonnees naar hun geselecteerde bestemmingen doorsturen door alle sessies die voor de ISP bestemd zijn te combineren met één PVC voor transport, of als de serviceprovider meerdere serviceniveaus aanbiedt, kan meer dan één PVC voor de gehele kern worden gecreëerd.

In een wholesale-servicemodel mag de dienstverlener geen SSG-functies gebruiken. In dit model, breidt de serviceprovider alle PPP sessies uit naar de home gateways. De huisgateways bieden IP-adressen aan de eindabonnee aan en authentiek de eindgebruiker.

Een belangrijke overweging in elk van deze scenario's is hoe de dienstverlener een andere Quality of Service (QoS) voor verschillende services kan aanbieden en hoe zij de bandbreedtetoewijzing berekenen. Op dit moment biedt de manier waarop de meeste serviceproviders deze architectuur implementeren verschillende QoS op verschillende PVC’s. Zij kunnen afzonderlijke PVC’s in de kern hebben voor huishoudelijke en zakelijke klanten. Het gebruik van verschillende PVC's staat serviceproviders toe om verschillende QoS voor verschillende services te specificeren. Op deze manier kan QoS op afzonderlijke PVC’s of op Layer 3 worden gebruikt.

Voor het toepassen van QoS op Layer 3 is het nodig dat de dienstverlener de eindbestemming kent, wat een beperkende factor zou kunnen zijn. Maar indien gebruikt in combinatie met Layer 2 QoS (door dit op verschillende VC's toe te passen) kan dit handig zijn voor de serviceprovider. De beperking met dit model is dat het vaststaat en dat de dienstverlener vooraf QoS moet aanbieden. QoS wordt niet dynamisch toegepast op de selectie van de service. Op dit moment is er geen optie voor een gebruiker om verschillende bandbreedte voor verschillende services te selecteren met een klik op de muis; er zijn echter aanzienlijke technische inspanningen gedaan om deze functie te ontwikkelen .

CPE-implementatie, -beheer en -voorzieningen zouden in deze architectuur een hele uitdaging kunnen zijn, omdat de CPE voor gebruikersnamen en wachtwoorden moet worden geconfigureerd. Als eenvoudige oplossing gebruiken sommige dienstverleners dezelfde gebruikersnaam en wachtwoord voor alle CPE's. Dit houdt een aanzienlijk veiligheidsrisico in. Daarnaast moeten, indien de CPE verschillende sessies gelijktijdig moet openen, extra VC’s worden voorzien bij de CPE, NAP en NSP. Cisco DSLAM’s en aggregation-apparaten kunnen de configuratie en provisioning van CPE vereenvoudigen. Er zijn ook doorstroombeheertools beschikbaar voor end-to-end PVC-provisioning. Provisioning bij de NSP voor zoveel abonnees die PVC’s gebruiken is een beperkende factor, aangezien alle verschillende PVC’s moeten worden beheerd. Bovendien is er geen eenvoudige manier om 2000 PVC’s op één NRP te bevoorraden door op een muis te klikken of een paar belangrijke slagen in te voeren.

Vandaag hebben we verschillende beheertoepassingen voor verschillende componenten van deze architectuur, zoals ViewMail voor DSLAM en SCM voor Cisco 6400 Er is geen enkel beheerplatform dat alle componenten zal leveren. Dit is een goed herkende beperking en er worden grote inspanningen geïnvesteerd om één enkele, uitgebreide beheertoepassing te hebben om de CPE, DSLAM en Cisco 6400 te leveren. Daarnaast hebben we op dit moment een oplossing om PPPoA met SVC te implementeren, wat de implementatie zeer zal vergemakkelijken. PPPoA met SVC stelt de eindgebruikers ook in staat om de bestemming en QoS dynamisch te selecteren.

Een ander belangrijk punt om in gedachten te houden voor grote implementaties van ADSL die deze architectuur gebruiken is de communicatie van de aggregatie router naar de RADIUS-server. Als het NRP-blad faalt wanneer enkele duizenden PPP-sessies op een aggregatiemiddel worden beëindigd, moeten al die PPP-sessies opnieuw worden ingesteld. Dit betekent dat alle abonnees

gewaarmerkt moeten worden en dat hun boekhouding gestopt en opnieuw opgestart moet worden zodra de verbinding tot stand is gebracht. Wanneer zoveel abonnees proberen tegelijkertijd geauthentiseerd te worden, kan de leiding naar de RADIUS-server een knelpunt zijn. Sommige abonnees kunnen mogelijk niet worden geauthentiseerd en dit kan problemen voor de serviceprovider veroorzaken.

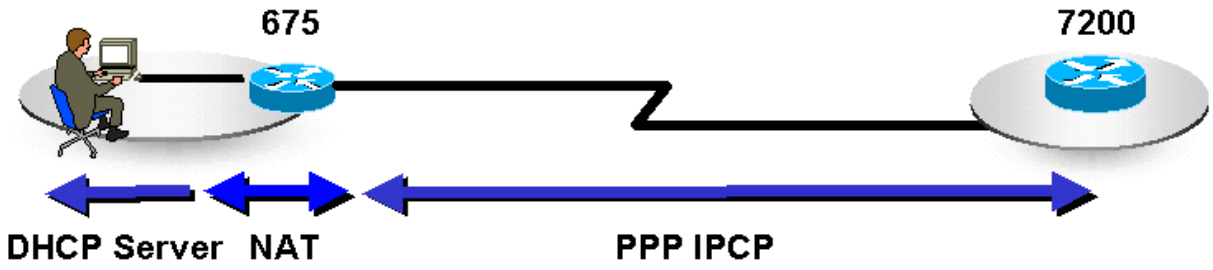
Het is zeer belangrijk om een verbinding met de RADIUS-server te hebben met voldoende bandbreedte om alle abonnees tegelijkertijd te kunnen ontvangen. Bovendien moet de RADIUS-server krachtig genoeg zijn om alle abonnees toestemming te geven. In het geval van duizenden abonnees moet een optie worden overwogen om de balans tussen de beschikbare RADIUS-servers te laden. Deze optie is beschikbaar in Cisco IOS® Software.

Als laatste overweging moet de aggregatie router voldoende prestaties leveren om vele PPP sessies te ontvangen. Pas dezelfde verkeerstechnische beginselen toe die door andere implementaties worden gebruikt. Eerder moest de gebruiker PVC’s op point-to-point subinterfaces configureren. Vandaag de dag staat PPPoA gebruikers toe om meerdere PVCs op multipoint subinterfaces evenals point-to-point te configureren. Voor elke PPPoA-verbinding zijn niet langer twee interfacebeschrijvingsblokken (IDB’s) nodig, een voor de virtuele toegangsinterface en een voor de ATM-subinterface. Deze verbetering verhoogt het maximum aantal PPPoA sessies die op een router lopen.

Het maximum aantal PPPoA-sessies dat op een platform wordt ondersteund, is afhankelijk van beschikbare systeembronnen zoals geheugen en CPU-snelheid. Elke PPPoA-sessie neemt één virtuele access interface. Elke virtuele toegangsinterface bestaat uit een descriptorblok voor de hardware en een projectorblok (hwidb/swidb) voor de software-interface. Elke hwidb kost ongeveer 4,5 K. Elke swidb kost ongeveer 2,5 K. Samen vereisen de virtuele toegangsinterfaces 7.5K. 2000 virtuele toegangsinterfaces 2000 * 7.5K of 15M. Om 2000 sessies te kunnen uitvoeren, heeft een router een extra 15 miljoen nodig. Vanwege de verhoging van de sessielimiet moet de router meer IDB's ondersteunen. Deze ondersteuning heeft invloed op de prestaties door meer CPU-cycli om meer exemplaren van de PPP-staatsmachine te kunnen uitvoeren.

Belangrijkste punten van PPPoA-architectuur

In deze sectie worden drie belangrijke punten in de PPPoA-architectuur beschreven: CPE, IP Management en het bereiken van de dienstbestemming.



The CPE configuration in this architecture depends on NSP or the Corporate Gateway, which may terminate the PPP sessions from the subscriber. When the CPE is configured, it must have at least one set of VPI/VCI, and a username and password should be defined.

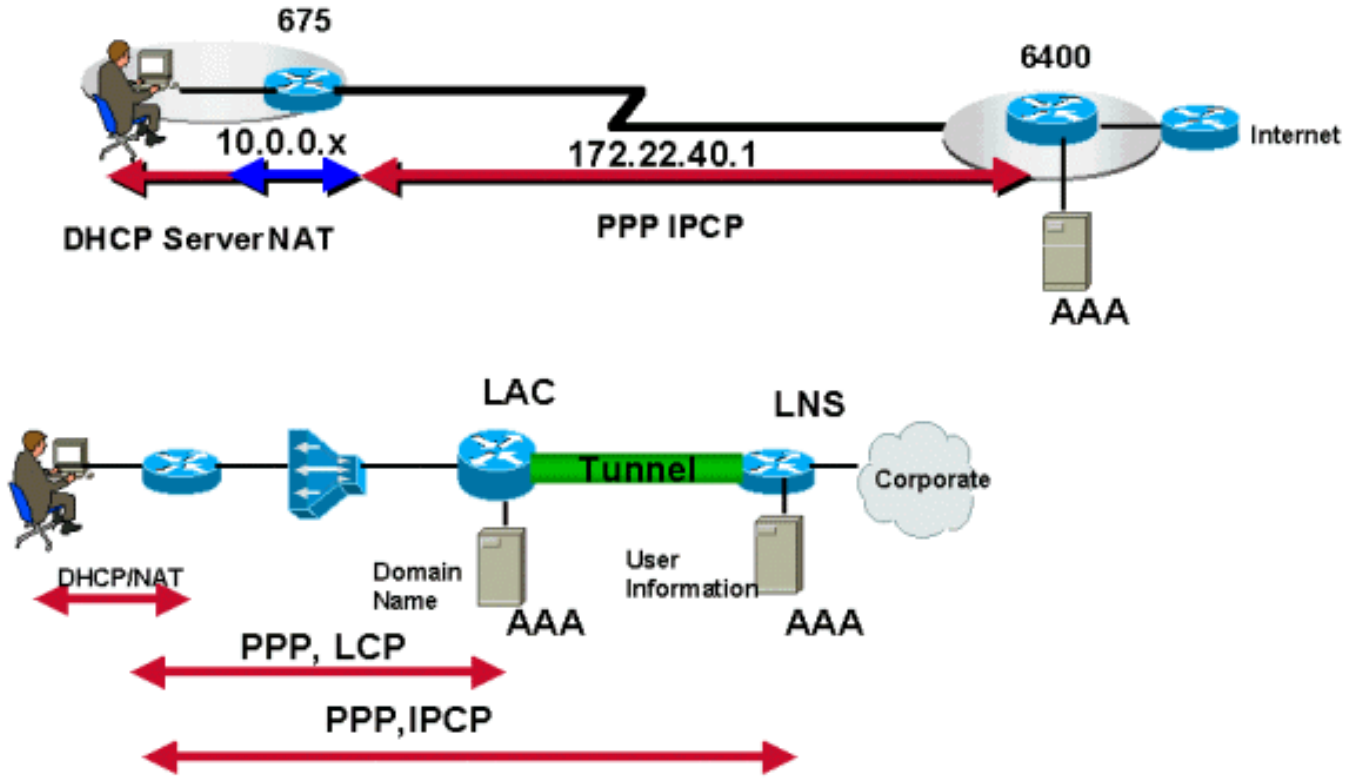
Optionally, the CPE may be configured as a DHCP server to provide private IP addresses to end stations on the LAN. The CPE can also be configured to do Port Address Translation (PAT). A CPE configured for PAT and DHCP usually gets a single public IP address from the final destination and all the stations on the LAN are translated to that address when they wish to go out of that network. Using this method the subscriber can easily host a Web or an email server using private IP addresses. Then, opening port 80 (HTTP) and port 25 (SMTP) on the static NAT entries in the CPE, these servers can be accessed from the outside. This is the most common scenario today.

Vanwege de aard van PAT kunnen bepaalde toepassingen die IP-informatie in de lading insluiten, in dit scenario niet werken. Om deze kwestie op te lossen, pas een netto van IP adressen in plaats van één enkel IP adres toe.

In deze architectuur is het voor NAP/NSP aan Telnet in CPE gemakkelijker om te vormen en probleemoplossing aangezien een IP adres aan CPE wordt toegewezen.

CPEs kunnen verschillende opties gebruiken afhankelijk van het profiel van de abonnee. Bijvoorbeeld, voor een residentiële gebruiker kan CPE zonder PAT/DHCP worden gevormd. Voor abonnees met meer dan één pc kunnen CPE's worden geconfigureerd voor PAT/DHCP of op dezelfde manier als die van een residentiële gebruiker. Als er een IP-telefoon is aangesloten op de CPE, kan CPE voor meer dan één PVC worden geconfigureerd.

IP-beheer



In PPPoA architectuur, IP adrestoewijzing voor de abonnee CPE gebruikt IPCP-onderhandeling, hetzelfde principe van PPP in kiesmodus. IP-adressen worden toegewezen afhankelijk van het type service dat een abonnee gebruikt. Als de abonnee alleen toegang tot internet heeft van NSP, zal NSP die PPP sessies van de abonnee beëindigen en een IP-adres toewijzen. Het IP-adres wordt toegewezen via een lokaal gedefinieerde pool, een DHCP-server, of kan worden toegepast vanaf de RADIUS-server. Bovendien kan de ISP een verzameling statische IP-adressen aan de abonnee hebben opgegeven en kan deze IP-adressen niet dynamisch toewijzen wanneer de abonnee de PPP-sessie initieert. In dit scenario zal de serviceprovider alleen de RADIUS-server gebruiken om de gebruiker voor authentiek te verklaren.

Als de abonnee er de voorkeur aan geeft meerdere diensten beschikbaar te hebben, moet NSP misschien SSG implementeren. Hieronder volgen de mogelijkheden om IP-adressen toe te wijzen.

- SP kan een IP-adres aan de abonnee aanbieden via de lokale pool of RADIUS-server. Nadat de gebruiker een service heeft geselecteerd, stuurt SSG het verkeer van de gebruiker naar die bestemming door. Als de SSG gebruik maakt van een proxy-modus, kan de eindbestemming een IP-adres opgeven, dat de SSG zal gebruiken als zichtbaar adres voor NAT.
- De PPP sessies worden niet afgesloten op de service provider? s aggregation router. Ze worden getunneld of naar de eindbestemming of de startgateway doorgestuurd, waardoor de PPP-sessies uiteindelijk worden afgesloten. De eindbestemming of de gateway van het huis onderhandelt IPCP met de abonnee, waarbij een IP-adres dynamisch wordt geleverd. Statische adressen zijn ook mogelijk zolang de eindbestemming die IP adressen heeft toegewezen en een route naar hen heeft.

Vóór Cisco IOS-softwarerelease 12.0.5DC voor Cisco 6400 NRP was er geen manier voor de serviceprovider om een subnetwerk van IP-adressen naar de abonnee te bieden. Met het Cisco 6400 platform en Cisco 600 Series CPEs kunnen IP-subnetten dynamisch op CPE tijdens PPP-onderhandeling worden geconfigureerd. Eén IP-adres van dit subtype wordt aan de CPE

toegewezen en de resterende IP-adressen worden dynamisch via DHCP aan de stations toegewezen. Wanneer deze optie wordt gebruikt, hoeven CPEs niet voor PAT te worden geconfigureerd, wat niet met sommige toepassingen werkt.

Hoe de dienstbestemming wordt bereikt

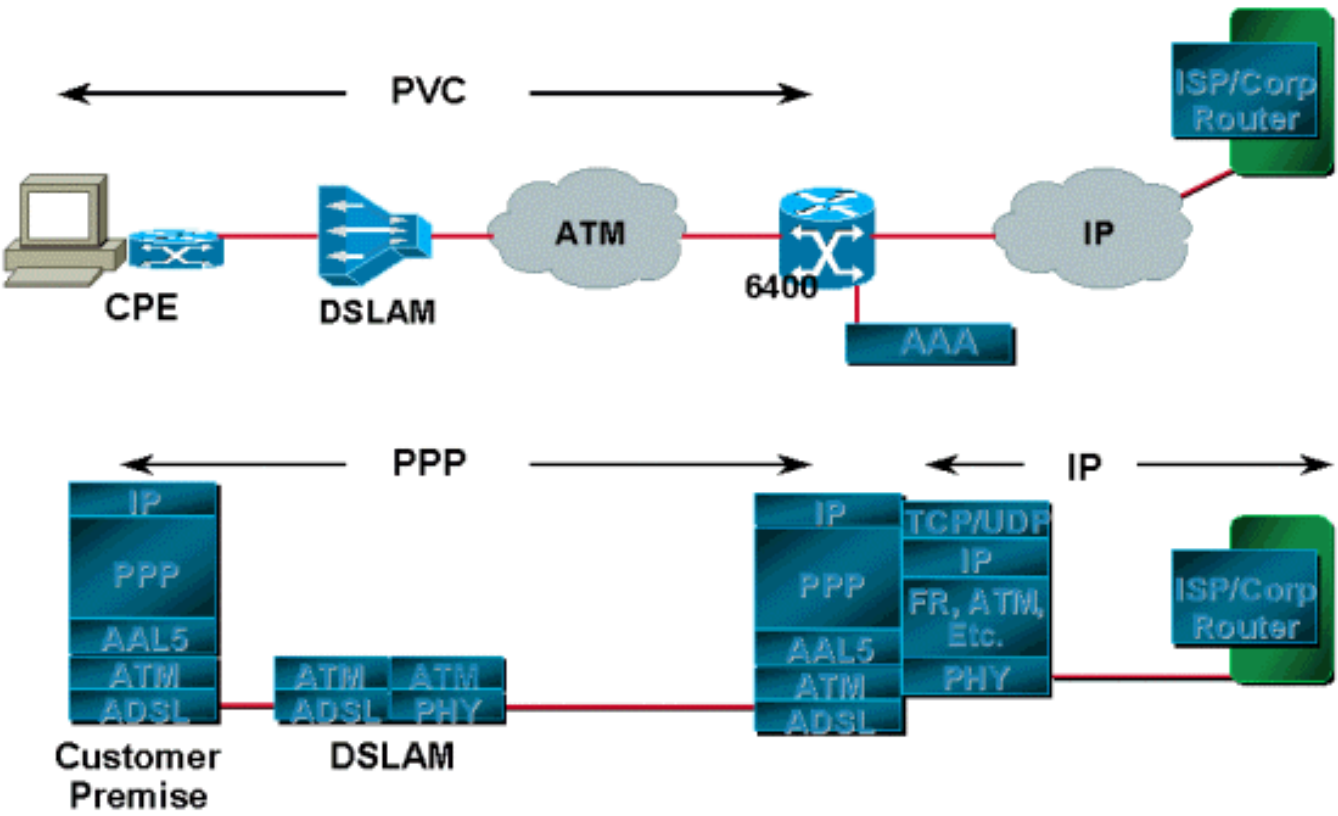
In PPPoA-architecturen kan de servicetoepassing op verschillende manieren worden bereikt. Enkele van de meest gebruikte methoden zijn:

- Beëindiging van PPP-sessies bij de serviceprovider
- L2TP-tunneling
- SSG gebruiken

In alle drie methoden is er een vaste reeks PVC's gedefinieerd vanuit de CPE naar de DSLAM die op de aggregatierouter is overgeschakeld op een vaste reeks PVC's. De PVC's worden in kaart gebracht van de DSLAM naar de aggregatierouter door een ATM-cloud.

De servicebestemming kan ook worden bereikt met andere methoden, zoals PPPoA met SVC's of Multiprotocol Label Switching/Virtual Private Network. Deze methoden vallen buiten het toepassingsgebied van dit document en zullen in afzonderlijke documenten worden besproken.

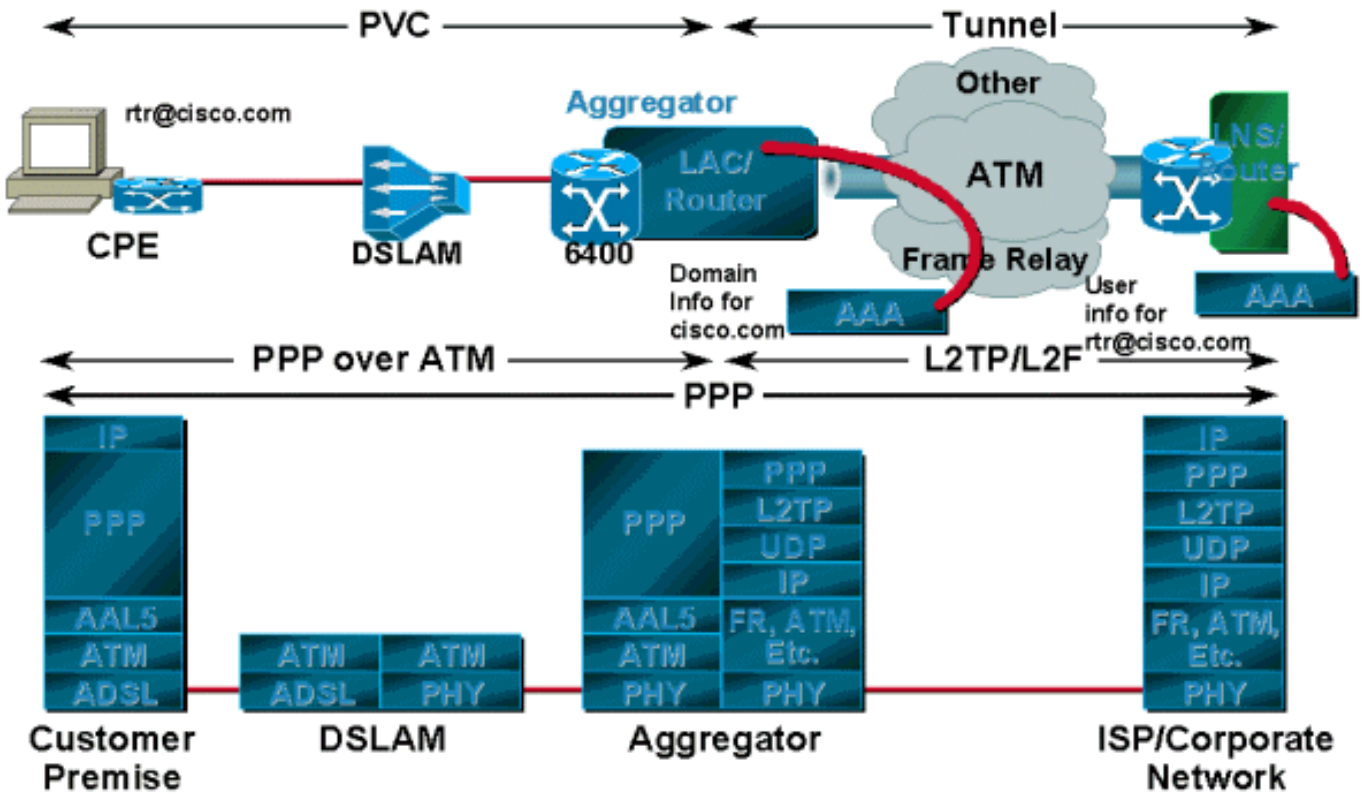
Beëindiging van PPP bij aggregatie



De PPP sessies die door de abonnee worden geïnitieerd, worden beëindigd bij de serviceprovider die gebruikers authenticeert door gebruik te maken van een lokale database op de router of door RADIUS-servers. Nadat de gebruiker voor authentiek is verklaard, wordt de IPCP- onderhandeling plaats en het IP adres wordt toegewezen aan CPE. Nadat het IP-adres is toegewezen, is er een host-route die zowel op CPE als op de aggregatie-router is gevestigd. De IP-adressen die, indien legaal, aan de abonnee zijn toegewezen, worden geadverteerd op de randrouter. De randrouter is

de gateway waardoor de abonnee tot internet kan toegang hebben. Als de IP-adressen privaat zijn, vertaalt de serviceprovider deze voordat u ze aan de randrouter aanbiedt.

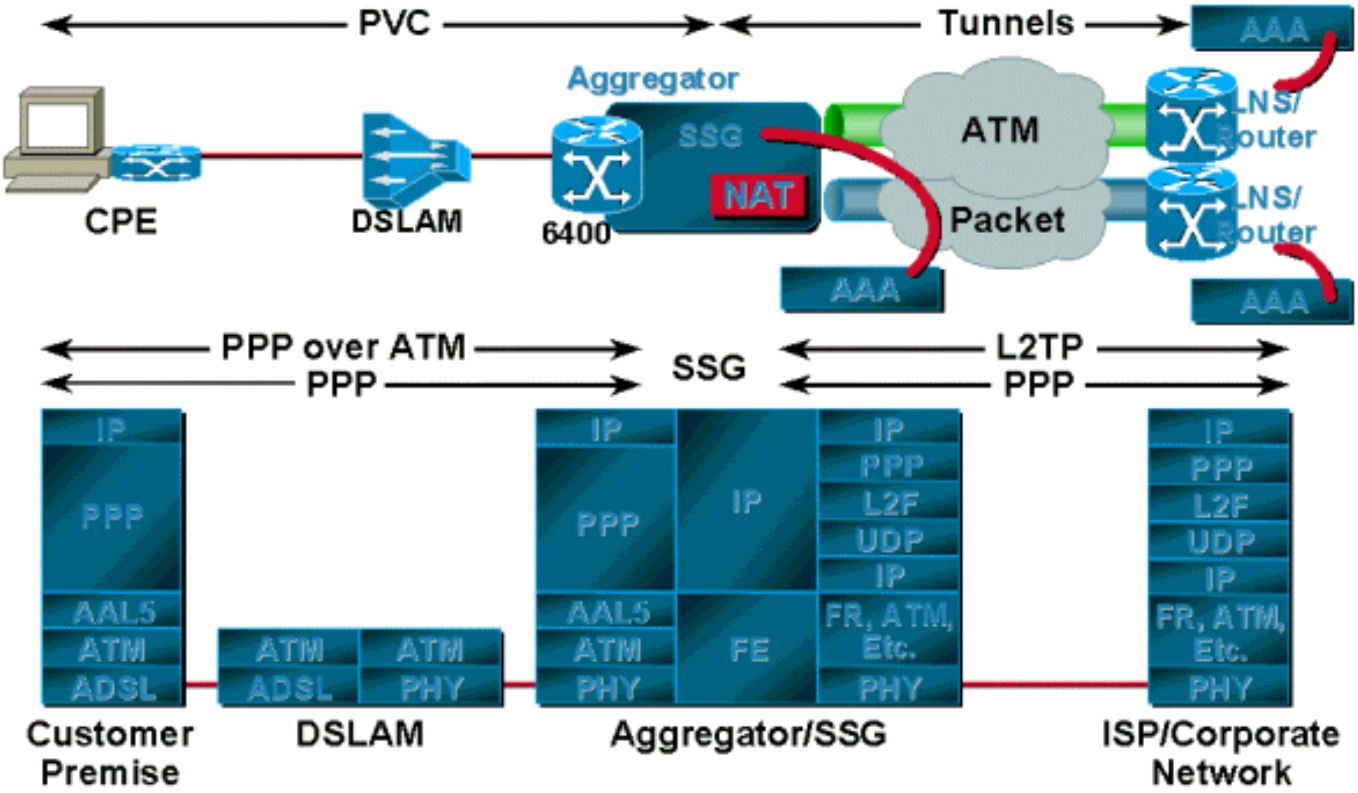
L2TP/L2F-tunneling



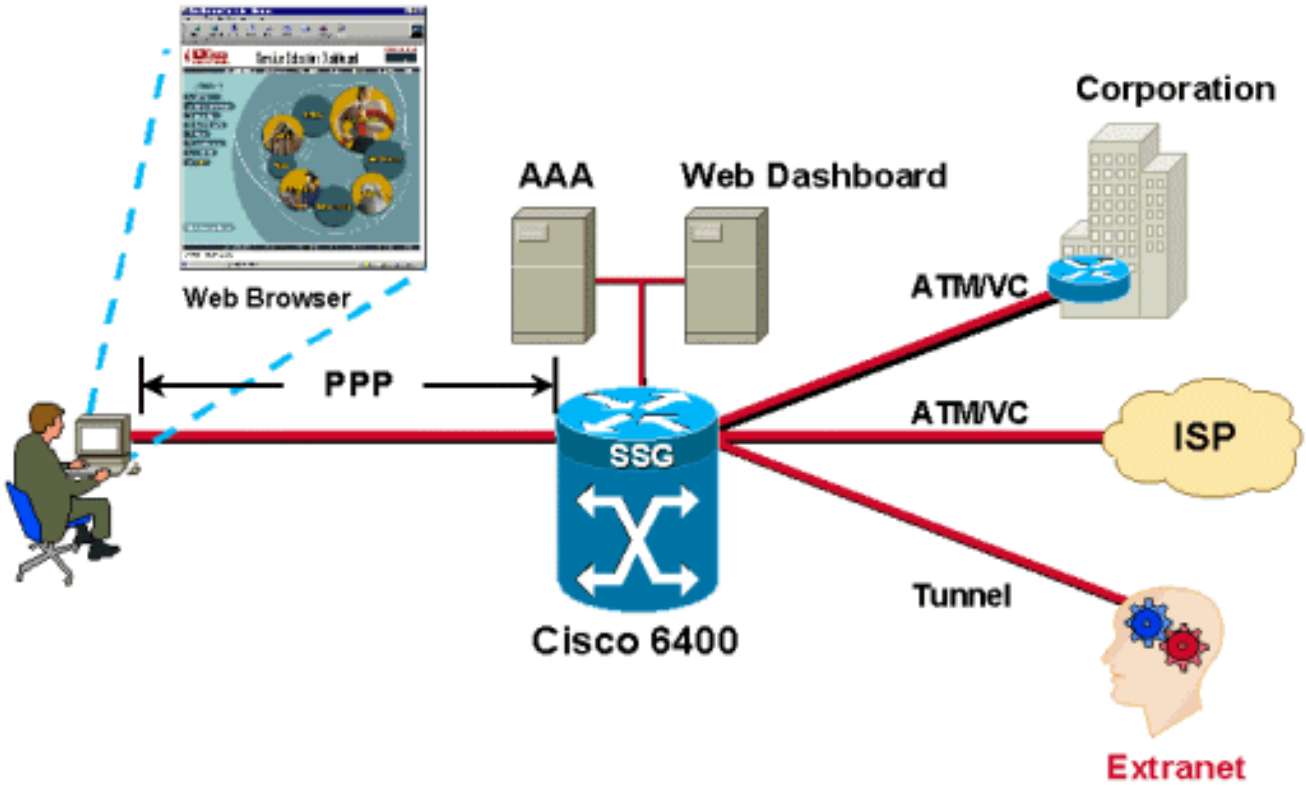
PPP-sessies, afhankelijk van de serviceprovider of het bedrijf, tunneleffect naar het upstream-aansluitpunt met behulp van L2TP of L2F in plaats van beëindigd te worden op de aggregatie-router van de serviceprovider. Dit eindpunt authenticeert de gebruikersnaam en de abonnee wordt een IP-adres toegewezen via DHCP of een lokale pool. Voor dit scenario is er gewoonlijk één tunnel gevestigd tussen de L2TP Access Concentrator/Network Access Server (LAC/NAS) en home gateway of L2TP Network Server (LNS). De LAC authenticeert de inkomende sessie op basis van de domeinnaam. de gebruikersnaam is geauthentificeerd op de eindbestemming of de startgateway.

In dit model heeft de gebruiker echter alleen toegang tot de eindbestemming en kan hij slechts één bestemming tegelijk benaderen. Als de CPE bijvoorbeeld met een gebruikersnaam voor rtr@cisco.com is ingesteld, kunnen de PC's achter die CPE alleen toegang tot het Cisco-domein hebben. Als zij met een ander bedrijfsnetwerk willen verbinden, moeten zij de gebruikersnaam en het wachtwoord op de CPE veranderen om die bedrijfs domeinnaam weer te geven. De tunnelbestemming in dit geval wordt bereikt door het gebruiken van een routingprotocol, statische routes, of het doen van klassieke IP over ATM (als het ATM als Layer 2) de voorkeur heeft.

Service Selection Gateway (SSG) gebruiken



Het belangrijkste voordeel van SSG in vergelijking met tunneling is dat SSG services in kaart brengt, terwijl tunneling slechts één-op-één-omzetting biedt. Dit wordt zeer nuttig wanneer één enkele gebruiker toegang tot meerdere diensten nodig heeft, of meerdere gebruikers op één plaats elk toegang tot een unieke dienst nodig hebben. SSG gebruikt het Web-Based Service Selection Dashboard (SSD), dat uit verschillende services bestaat en beschikbaar is voor de gebruiker. De gebruiker kan toegang krijgen tot één service of meerdere services tegelijk. Een ander voordeel van het gebruik van SSG is dat de dienstverlener de gebruiker kan betalen op basis van de gebruikte services en de sessietijd, en de gebruiker kan de services aan en uit zetten via de SSD.



De gebruikers zijn authentiek verklaard aangezien de PPP-sessie van de abonnees komt. De gebruikers worden toegewezen IP adressen van of de lokale pool of de server van de RADIUS. Nadat een gebruiker is geauthentiseerd, wordt een bronobject gemaakt met de SSG-code en krijgt de gebruiker toegang tot een standaardnetwerk. Het standaardnetwerk bevat de SSD-server. Wanneer een browser wordt gebruikt, logt de gebruiker in op het Dashboard, wordt geauthentiseerd door de AAA server en afhankelijk van het gebruikersprofiel dat opgeslagen is in de RADIUS server, wordt een set services aangeboden om toegang te krijgen.

Telkens wanneer een geauthentiseerde gebruiker een service selecteert, maakt SSG een doelobject voor die gebruiker. Het doelobject bevat informatie zoals het doeladres, het DNS-serveradres voor de bestemming en het IP-adres van de bron vanaf de startgateway. Pakketten die van de gebruiker komen?s zij worden doorgestuurd naar de bestemming op basis van de informatie in het doelobject.

SSG kan worden geconfigureerd voor proxy-service, transparante doorloop of PTA. Wanneer een abonnee om toegang tot een proxy-service vraagt, zal NRP-SSG het toegangsverzoek doorgeven aan de externe RADIUS-server. Na ontvangst van het toegangsaanvaarden, reageert SSG op de abonnee met de toegangsaanvaarden. De SSG verschijnt als client voor de externe RADIUS-server.

Transparent passthrough staat niet-echt gewaarmerkte abonneeverkeer toe om door SSG in beide richtingen te worden geleid. Gebruik filters om transparant doorvoerverkeer te besturen.

PTA kan alleen door PPP-type gebruikers worden gebruikt. Verificatie, autorisatie en accounting wordt precies uitgevoerd zoals in het proxy-servicetype. Een abonnee logt in bij een service met behulp van een gebruikersnaam voor het formulier user@service. SSG stuurt dat naar de RADIUS-server, die het serviceprofiel vervolgens naar de SSG laadt. De SSG stuurt het verzoek door naar de RADIUS-server op afstand zoals gespecificeerd door het serviceprofiel?s RADIUS-serverkenmerk. Nadat het verzoek voor authentiek is verklaard, wordt een IP adres toegewezen aan de abonnee. Er wordt geen NAT uitgevoerd. Alle gebruikersverkeer wordt naar het externe

netwerk geaggregeerd. Met PTA hebben gebruikers toegang tot slechts één service en hebben ze geen toegang tot het standaardnetwerk of de SSD.

Operationele beschrijving van PPPoA-architectuur

Wanneer CPE eerst wordt aangedreven, begint het verzenden van LCP configuratieverzoeken naar de aggregation server. De aggregatieserver, met de PVC's geconfigureerd, stuurt ook het LCP-configuratieverzoek in een Virtual Access Interface (gekoppeld aan het PVC). Wanneer ieder het configuratieverzoek van de ander ziet, erkennen ze de verzoeken en wordt de LCP-staat geopend.

Voor de authenticatiefase stuurt de CPE de authenticatieaanvraag naar de aggregatieserver. De server, afhankelijk van de configuratie, authenticeert de gebruiker op basis van de domeinnaam (indien meegeleverd) of de gebruikersnaam op basis van de lokale database of RADIUS-servers. Als het verzoek van de abonnee wordt gedaan in de vorm van username@domainname, zal de aggregation server proberen een tunnel naar de bestemming te creëren, als die nog niet is. Nadat de tunnel is gemaakt, stuurt de aggregatieserver de PPP verzoeken van de abonnee naar de bestemming door. De bestemming, op zijn beurt, authentiek de gebruiker en wijst een IP adres toe. Als het verzoek van de abonnee de domeinnaam niet bevat, wordt de gebruiker door de lokale database geauthentiseerd. Als SSG op de aggregation router is ingesteld, kan de gebruiker het standaard netwerk benaderen zoals opgegeven en kan hij een optie krijgen om verschillende services te selecteren.

Conclusie

PPPoA wordt de meest geschikte architectuur voor veel serviceproviders omdat het zeer schaalbaar is, SSG-functionaliteit gebruikt en beveiliging biedt. Aangezien de focus van dit document op PPPoA-architectuur lag, was het niet mogelijk om functies als SSG diepgaand te bestrijken. Deze functies worden in de daaropvolgende documenten besproken. Monsterconfiguraties voor de verschillende scenario's die in dit document worden besproken, worden ook in afzonderlijke documenten gepresenteerd en uitgelegd.

Gerelateerde informatie

- Cisco DSL-productondersteuningsinformatie
- Technische ondersteuning - Cisco-systemen