PPPoA-Basisarchitektur

Inhalt

Einführung

Dieses Dokument beschreibt eine End-to-End-ADSL-Architektur (Asynchronous Digital Subscriber Line), die Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA) verwendet. Obwohl die meisten Bereitstellungen auf der Bridging-Architektur basieren, gewinnt PPPoA immer mehr an Popularität und wird einen größeren Teil der zukünftigen ADSL-Bereitstellungen ausmachen.

Annahme

Bei der Basisarchitektur wird davon ausgegangen, dass der Endbenutzer über PPPoA als Core-Backbone Hochgeschwindigkeits-Internetzugriff und Unternehmenszugriff erhalten muss. Wir werden diese Architektur auf der Grundlage von Private Virtual Channels (PVCs) besprechen, der Methode, die am häufigsten in aktuellen Bereitstellungen verwendet wird. Die Architektur mit geswitchten virtuellen Schaltungen (SVCs) wird in einem separaten Dokument behandelt.

Dieses Dokument basiert auf vorhandenen Bereitstellungen sowie internen Tests der Architektur.

Dieses Dokument wurde unter der Annahme verfasst, dass der Leser mit den Designüberlegungen eines Network Access Provider (NAP) vertraut ist, wie im Whitepaper RFC1483 Bridging Baseline Architecture beschrieben.

Technologiebeschreibung

Point-to-Point Protocol (PPP) (RFC 1331) bietet eine Standardmethode zur Kapselung von Protokollen höherer Layer über Punkt-zu-Punkt-Verbindungen. Sie erweitert die HDLC-Paketstruktur (High-Level Data Link Control) um eine 16-Bit-Protokollkennung, die Informationen über den Inhalt des Pakets enthält.

Das Paket enthält drei Arten von Informationen:

- Link Control Protocol (LCP) - handelt Link-Parameter, Paketgröße oder Authentifizierungstyp aus
- Network Control Protocol (NCP) - Enthält Informationen zu übergeordneten Protokollen wie IP und IPX sowie deren Steuerungsprotokollen (IPCP für IP)
- Datenpakete mit Daten

PPP over ATM Adaptive Layer 5 (AAL5) (RFC 2364) verwendet AAL5 als gerahmtes Protokoll, das sowohl PVC als auch SVC unterstützt. PPPoA wurde vorwiegend als Teil von ADSL implementiert. Sie ist auf RFC1483 angewiesen und wird entweder im Logical Link Control-Subnetwork Access Protocol (LLC-SNAP)- oder im VC-Mux-Modus betrieben. Ein Gerät am Kundenstandort (CPE) kapselt die PPP-Sitzung auf Basis dieser RFC für die Übertragung über die ADSL-Schleife und den Digital Subscriber Line Access Multiplexer (DSLAM).

Vorteile und Nachteile der PPPoA-Architektur

Die PPPoA-Architektur erbt die meisten Vorteile von PPP, die im Wählmodell verwendet werden. Nachfolgend sind einige der wichtigsten Punkte aufgeführt.

Vorteile

- Pro Sitzung Authentifizierung basierend auf Password Authentication Protocol (PAP) oder Challenge Handshake Authentication Protocol (CHAP). Dies ist der größte Vorteil von PPPoA, wenn die Authentifizierung die Sicherheitslücke in einer Bridging-Architektur überwindet.
- Pro Session Accounting ist möglich, sodass der Service Provider den Abonnenten basierend auf der Sitzungszeit für verschiedene angebotene Services berechnen kann. Die Sitzungsabrechnung ermöglicht es einem Service Provider, eine Mindestzugriffsstufe für minimale Kosten anzubieten und den Abonnenten dann zusätzliche Dienste in Rechnung zu stellen.
- IP-Adresserhaltung am CPE Dadurch kann der Service Provider nur eine IP-Adresse für eine CPE zuweisen, wobei die CPE für die NAT (Network Address Translation) konfiguriert ist. Alle Benutzer hinter einem CPE können eine einzige IP-Adresse verwenden, um verschiedene Ziele zu erreichen. Der IP-Management-Overhead für den Network Access Provider/Network Services Provider (NAP/NSP) für jeden einzelnen Benutzer wird bei gleichzeitiger Einsparung von IP-Adressen reduziert. Darüber hinaus kann der Service Provider ein kleines Subnetz von IP-Adressen bereitstellen, um die Einschränkungen bei der Port-Adressenumwandlung (PAT) und NAT zu überwinden.
- NAPs/NSPs bieten sicheren Zugriff auf Unternehmens-Gateways, ohne End-to-End-PVCs zu verwalten, und verwenden Layer-3-Routing oder Layer-2-Forwarding/Layer-2-Tunneling Protocol (L2F/L2TP)-Tunnel. Daher können sie ihre Geschäftsmodelle für den Verkauf von Großkundenservices skalieren.
- Fehlerbehebung bei einzelnen Abonnenten. Der NSP kann anhand aktiver PPP-Sitzungen leicht erkennen, welche Teilnehmer ein- oder ausgeschaltet sind, anstatt wie bei Bridging-

Architekturen die Fehlerbehebung für ganze Gruppen durchzuführen.
- Der NSP kann eine Überbelegung vornehmen, indem er Leerlauf- und Sitzungs-Timeouts mithilfe eines RADIUS-Servers (Remote Authentication Dial-In User Service) nach Branchenstandard für jeden Teilnehmer bereitstellt.
- Hohe Skalierbarkeit, da eine sehr hohe Anzahl an PPP-Sitzungen auf einem Aggregation Router beendet werden kann. Authentifizierung, Autorisierung und Abrechnung können für jeden Benutzer über externe RADIUS-Server erfolgen.
- Optimale Nutzung der Funktionen des Service Selection Gateway (SSG).

Nachteile

- Nur eine Sitzung pro CPE auf einem Virtual Channel (VC). Da der Benutzername und das Kennwort auf dem CPE konfiguriert sind, können alle Benutzer hinter dem CPE für diese VC nur auf einen Service-Satz zugreifen. Die Benutzer können keine verschiedenen Servicesätze auswählen, obwohl die Verwendung mehrerer VCs und die Einrichtung unterschiedlicher PPP-Sitzungen auf verschiedenen VCs möglich sind.
- Höhere Komplexität der CPE-Einrichtung Die Helpdesk-Mitarbeiter des Service Providers müssen über mehr Fachwissen verfügen. Da der Benutzername und das Kennwort auf dem CPE konfiguriert sind, muss der Teilnehmer oder der CPE-Anbieter die Konfiguration ändern. Die Verwendung mehrerer VCs erhöht die Komplexität der Konfiguration. Dies kann jedoch durch eine noch nicht veröffentlichte automatische Konfigurationsfunktion überwunden werden.
- Der Service Provider muss eine Datenbank mit Benutzernamen und Kennwörtern für alle Abonnenten pflegen. Wenn Tunnel oder Proxy-Services verwendet werden, kann die Authentifizierung anhand des Domänennamens und die Benutzerauthentifizierung am Corporate Gateway erfolgen. Dadurch wird die Datenbankgröße reduziert, die der Service Provider pflegen muss.
- Wenn dem CPE eine einzige IP-Adresse bereitgestellt und NAT/PAT implementiert wird, funktionieren bestimmte Anwendungen wie IPTV, die IP-Informationen in die Nutzlast einbetten, nicht. Wenn eine IP-Subnetzfunktion verwendet wird, muss außerdem eine IP-Adresse für die CPE reserviert werden.

Überlegungen zur Implementierung der PPPoA-Architektur

Die wichtigsten Punkte, die vor der Implementierung der PPPoA-Architektur zu berücksichtigen sind, sind:

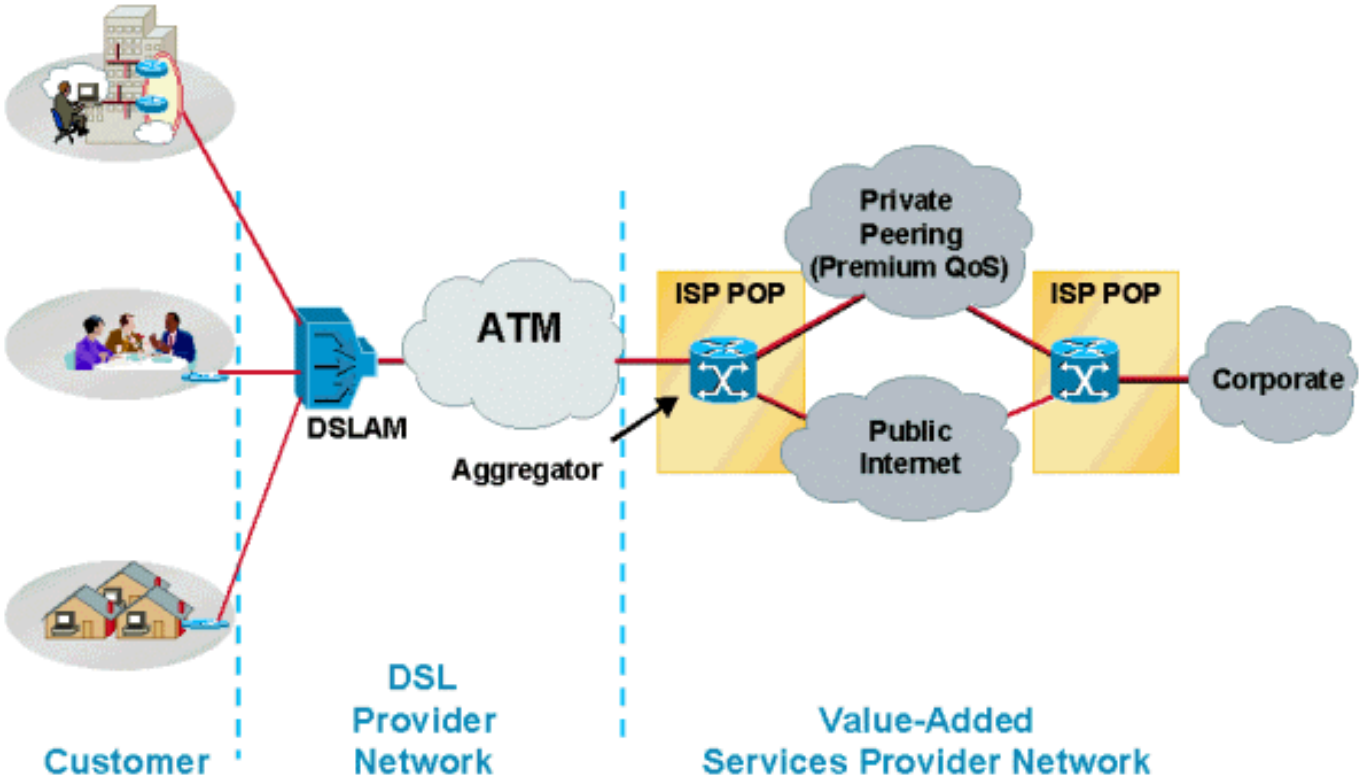
- Die Anzahl der Teilnehmer, die derzeit und in Zukunft betreut werden, da sich dies auf die Anzahl der erforderlichen PPP-Sitzungen auswirkt.
- Legt fest, ob die PPP-Sitzungen am Aggregation Router des Service Providers beendet oder an andere Unternehmens-Gateways oder Internetdienstanbieter (ISPs) weitergeleitet werden.
- Legt fest, ob der Service Provider oder das endgültige Service-Ziel die IP-Adresse für die CPE des Abonnenten bereitstellt.
- Legt fest, ob die angegebenen IP-Adressen öffentlich oder privat legal sind. Wird NAT/PAT vom CPE ausgeführt, oder wird NAT am Ziel für die Terminierung durchgeführt?
- Profile von Endabonnenten, Privatanwendern, Heimbüro-Kunden (Small Office Home Office, SOHO) und Telearbeitern.

- Bei mehr als einem Benutzer, ob alle Benutzer dasselbe Endziel oder denselben Enddienst erreichen müssen, oder ob alle Benutzer unterschiedliche Serviceziele haben.
- Stellt der Service Provider Mehrwert-Services wie Sprache oder Video bereit? Verlangt der Service Provider, dass alle Teilnehmer zuerst in ein bestimmtes Netzwerk gehen, bevor sie ein endgültiges Ziel erreichen? Werden bei der Nutzung von SSG Passthrough-Services, PPP Terminated Aggregation (PTA), ein Vermittlungsgerät oder ein Proxy verwendet?
- Legt fest, wie der Service Provider die Abonnenten auf Grundlage einer Pauschalzahlung, Sitzungsnutzung oder genutzter Services abrechnet.
- Bereitstellung und Bereitstellung von CPEs, DSLAMs und Aggregation Points of Presence (POPs).
- Das Geschäftsmodell für das NAP. Umfasst das Modell auch den Verkauf von Großkundenservices wie sicheren Unternehmenszugang und Mehrwert-Services wie Sprach- und Videodienste? Sind NAPs und NSPs dieselbe Einheit?
- Das Geschäftsmodell des Unternehmens. Ist sie mit einem unabhängigen lokalen Börsenbetreiber (ILEC), einem konkurrierenden lokalen Börsenbetreiber (CLEC) oder einem ISP vergleichbar?
- Die Anwendungstypen, die der NSP dem Endkunden anbietet.
- Das erwartete Upstream- und Downstream-Datenverkehrsvolumen.

Unter Berücksichtigung dieser Aspekte werden wir erörtern, wie die PPPoA-Architektur für Service Provider auf unterschiedliche Geschäftsmodelle zugeschnitten und skaliert werden kann und wie die Provider von der Nutzung dieser Architektur profitieren können.

Typische PPPoA-Netzwerkarchitektur

Das folgende Diagramm zeigt eine typische PPPoA-Netzwerkarchitektur. Kunden, die CPEs verwenden, stellen über einen Cisco DSLAM, der über ATM mit einem Cisco 6400-Aggregator verbunden ist, eine Verbindung zum Netzwerk des Service Providers her.



Überlegungen zum Design der PPPoA-Architektur

Im Abschnitt "Überlegungen zur Implementierung" dieses Dokuments können PPPoA-Architekturen je nach Geschäftsmodell des Service Providers in verschiedenen Szenarien bereitgestellt werden. In diesem Abschnitt werden die verschiedenen Möglichkeiten und Überlegungen erläutert, die Service Provider vor der Bereitstellung einer Lösung berücksichtigen müssen.

Vor der Bereitstellung einer PPPoA-Architektur und einer bestimmten Lösung für diese Architektur ist es wichtig, das Geschäftsmodell des Service Providers zu verstehen. Berücksichtigen Sie die Services, die der Service Provider anbietet. Bietet der Dienstanbieter seinen Endabonnenten einen Hochgeschwindigkeits-Internetzugang, oder wird er Großkundendienste an verschiedene ISPs verkaufen und diesen Abonnenten Mehrwert-Services anbieten? Bietet der Service Provider all diese Angebote?

Bei Hochgeschwindigkeitsinternetzugang in Umgebungen, in denen der NSP und der NAP identisch sind, müssen die PPP-Sitzungen des Teilnehmers im bereitgestellten Aggregation Router terminiert werden. In diesem Szenario müssen Service Provider berücksichtigen, wie viele PPP-Sitzungen auf einem einzelnen Router-Aggregationsgerät terminiert werden können, wie die Benutzer authentifiziert werden sollen, wie sie die Abrechnung durchführen und wie der Internetzugang nach Beendigung der Benutzersitzungen eingerichtet werden soll. Je nach Anzahl der PPP-Sitzungen und Teilnehmer kann es sich beim Aggregation Router um einen Cisco 6400 oder einen Cisco 7200 handeln. Heute können mit dem Cisco 6400 mit 7 Node-Route-Prozessoren (NRPs) bis zu 14.000 PPP-Sitzungen terminiert werden. Der Cisco 7200 ist auf 2.000 PPP-Sitzungen beschränkt. Diese Zahlen werden sich mit neuen Versionen ändern. In den Versionshinweisen und Produktdokumenten finden Sie die genaue Anzahl der Sitzungen, die von den einzelnen Aggregation Routern unterstützt werden können.

Die Benutzerauthentifizierung und -abrechnung wird in diesem Szenario am besten mithilfe eines RADIUS-Servers nach Branchenstandard verwaltet, der einen Benutzer anhand des Benutzernamens oder der verwendeten VPI/VCI (Virtual Path Identifier/Virtual Channel Identifier) authentifizieren kann.

Für Hochgeschwindigkeitsinternetzugang berechnen NSP Kunden in der Regel einen Pauschalpreis. Die meisten aktuellen Bereitstellungen werden auf diese Weise implementiert. Wenn NSP und NAP dieselbe Einheit sind, werden Kunden für den Zugriff zu einem festen Preis und für den Internetzugriff zu einem anderen festen Preis berechnet. Dieses Modell ändert sich, wenn der Service Provider Mehrwert-Services anbietet. Service Provider können den Kunden je nach Art des Service und Dauer des Service in Rechnung stellen. Kunden stellen über den Aggregation Router mithilfe von Routing-Protokollen wie Open Shortest Path First (OSPF) oder Enhanced Interior Gateway Routing Protocol (EIGRP) eine Verbindung zum Internet mit einem Edge-Router her, auf dem Border Gateway Protocol (BGP) ausgeführt werden könnte.

Eine weitere Option des Service Providers für Hochgeschwindigkeitsinternetzugang besteht darin, eingehende PPP-Sitzungen von Abonnenten mithilfe von L2TP/L2F Tunneling an einen separaten ISP weiterzuleiten. Bei Verwendung von L2x Tunneling sollte besonders darauf geachtet werden, wie das Tunnelziel erreicht werden kann. Die verfügbaren Optionen sind entweder die Ausführung einiger Routing-Protokolle oder die Bereitstellung statischer Routen im Aggregation Router. Einschränkungen bei der Verwendung von L2TP- oder L2F-Tunneln sind: (1) die Anzahl der Tunnel und die Anzahl der Sitzungen, die in diesen Tunneln unterstützt werden können; und (2) die Verwendung von Routing-Protokollen, die nicht mit ISPs von Drittanbietern kompatibel sind und die die Verwendung statischer Routen erfordern können.

Wenn der Service Provider Services für verschiedene ISPs oder Unternehmens-Gateways an den Endkunden anbietet, müssen diese möglicherweise SSG-Funktionen auf dem Aggregation Router implementieren. Dadurch kann der Teilnehmer mithilfe einer webbasierten Serviceauswahl verschiedene Serviceziele auswählen. Der Service Provider kann Teilnehmer-PPP-Sitzungen entweder an ihre ausgewählten Ziele weiterleiten, indem er alle Sitzungen, die für den ISP bestimmt sind, in einer einzigen PVC für den Transport kombiniert. Wenn der Service Provider mehrere Servicelevel anbietet, kann im gesamten Kern mehr als eine PVC eingerichtet werden.

In einem Großhandelsservicemodell darf der Service Provider keine SSG-Funktionen verwenden. Bei diesem Modell erweitert der Service Provider alle PPP-Sitzungen auf die Haupt-Gateways. Die Heimgateways stellen dem Endkunden IP-Adressen zur Verfügung und authentifizieren den Endbenutzer.

Eine wichtige Überlegung in allen diesen Szenarien ist, wie der Service Provider eine andere Quality of Service (QoS) für verschiedene Services anbieten kann und wie die Bandbreitenzuweisung berechnet wird. Derzeit bieten die meisten Service Provider bei der Bereitstellung dieser Architektur unterschiedliche QoS auf verschiedenen PVCs. Sie können für Privat- und Geschäftskunden separate PVCs im Core verwenden. Mithilfe verschiedener PVCs können Service Provider unterschiedliche QoS für verschiedene Services angeben. Auf diese Weise kann QoS auf separaten PVCs oder auf Layer 3 ausgeführt werden.

Bei der Anwendung von QoS auf Layer 3 muss der Service Provider das endgültige Ziel kennen, was ein begrenzender Faktor sein kann. Wird sie jedoch in Kombination mit Layer-2-QoS (durch Anwendung auf verschiedene VCs) verwendet, kann sie für den Service Provider nützlich sein. Dieses Modell ist begrenzt, da es fest konfiguriert ist und der Service Provider QoS im Voraus bereitstellen muss. QoS wird bei der Serviceauswahl nicht dynamisch angewendet. Zurzeit besteht für einen Benutzer keine Option, verschiedene Bandbreiten für verschiedene Dienste mit einem Mausklick auszuwählen. Für die Entwicklung dieser Funktion wurden jedoch erhebliche

technische Anstrengungen unternommen.

CPE-Bereitstellung, -Verwaltung und -Bereitstellung könnten in dieser Architektur eine große Herausforderung darstellen, da CPE für Benutzernamen und Kennwörter konfiguriert werden muss. Als einfache Lösung verwenden einige Service Provider für alle CPEs denselben Benutzernamen und dasselbe Kennwort. Dies stellt ein erhebliches Sicherheitsrisiko dar. Wenn die CPE gleichzeitig verschiedene Sitzungen öffnen muss, müssen zusätzliche VCs über CPE, NAP und NSP bereitgestellt werden. Cisco DSLAMs und Aggregationsgeräte können die Konfiguration und Bereitstellung von CPE vereinfachen. Flow-Through-Management-Tools sind auch für die End-to-End-PVC-Bereitstellung verfügbar. Die Bereitstellung am NSP für so viele Teilnehmer, die PVCs verwenden, ist ein begrenzender Faktor, da alle verschiedenen PVCs verwaltet werden müssen. Darüber hinaus gibt es keine einfache Möglichkeit, 2000 PVCs auf einem einzigen NRP bereitzustellen, indem Sie auf eine Maus klicken oder einige Tastenanschläge eingeben.

Heute gibt es für die verschiedenen Komponenten dieser Architektur verschiedene Verwaltungsanwendungen, wie Viewrunner für DSLAM und SCM für Cisco 6400 Es gibt keine einzige Verwaltungsplattform, die alle Komponenten bereitstellt. Dies ist eine allgemein anerkannte Einschränkung, und es wird viel Aufwand in die Bereitstellung einer einzigen, umfassenden Verwaltungsanwendung für CPE, DSLAM und Cisco 6400 investiert. Darüber hinaus gibt es derzeit eine Lösung zur Implementierung von PPPoA mit SVC, die die Bereitstellung erheblich erleichtert. PPPoA mit SVC ermöglicht Endbenutzern auch die dynamische Auswahl von Ziel und QoS.

Ein weiterer wichtiger Punkt, der bei großen ADSL-Bereitstellungen mit dieser Architektur beachtet werden sollte, ist die Kommunikation vom Aggregation Router zum RADIUS-Server. Wenn der NRP-Blade ausfällt, wenn mehrere Tausend PPP-Sitzungen auf einem Aggregationsgerät beendet werden, müssen alle diese PPP-Sitzungen wiederhergestellt werden. Das bedeutet, dass alle Teilnehmer authentifiziert werden müssen und ihre Buchhaltungsdaten angehalten und neu gestartet werden müssen, sobald die Verbindung hergestellt ist. Wenn so viele Abonnenten versuchen, gleichzeitig authentifiziert zu werden, kann die Leitung zum RADIUS-Server ein Engpass sein. Einige Abonnenten können möglicherweise nicht authentifiziert werden, was zu Problemen für den Service Provider führen kann.

Es ist sehr wichtig, eine Verbindung zum RADIUS-Server mit ausreichender Bandbreite zu haben, um alle Teilnehmer gleichzeitig unterzubringen. Darüber hinaus sollte der RADIUS-Server leistungsfähig genug sein, um allen Teilnehmern Berechtigungen zu gewähren. Bei Tausenden von Teilnehmern sollte eine Option für den Lastenausgleich zwischen verfügbaren RADIUS-Servern in Betracht gezogen werden. Diese Funktion ist in der Cisco IOS® Software verfügbar.

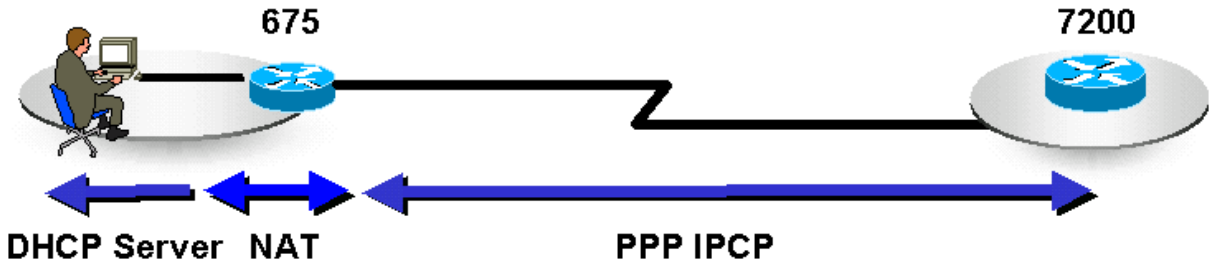
Schließlich muss der Aggregation Router ausreichend arbeiten, um eine Vielzahl von PPP-Sitzungen zu ermöglichen. Verwenden Sie die gleichen Traffic Engineering-Prinzipien wie bei anderen Implementierungen. Bisher musste der Benutzer PVCs auf Point-to-Point-Subschnittstellen konfigurieren. Heute können Benutzer mit PPPoA mehrere PVCs auf Multipoint-Subschnittstellen sowie Point-to-Point konfigurieren. Für jede PPPoA-Verbindung sind nicht mehr zwei Schnittstellendeskriptorblöcke (IDBs) erforderlich, einer für die virtuelle Zugriffsschnittstelle und einer für die ATM-Subschnittstelle. Diese Erweiterung erhöht die maximale Anzahl von PPPoA-Sitzungen, die auf einem Router ausgeführt werden.

Die maximale Anzahl von PPPoA-Sitzungen, die von einer Plattform unterstützt werden, hängt von verfügbaren Systemressourcen wie Arbeitsspeicher und CPU-Geschwindigkeit ab. Jede PPPoA-Sitzung benötigt eine virtuelle Zugriffsschnittstelle. Jede virtuelle Zugriffsschnittstelle besteht aus einem Hardware Interface Descriptor Block und einem Software Interface Descriptor Block

(hwidb/swidb) Paar. Jedes Widb benötigt etwa 4,5 K. Jede Swidb benötigt etwa 2,5 K. Zusammen erfordern die virtuellen Zugriffsschnittstellen 7,5 K. Für 2.000 virtuelle Zugriffsschnittstellen sind 2.000 x 7.500 oder 15 Mio. erforderlich. Für die Ausführung von 2000 Sitzungen benötigt ein Router zusätzlich 15 Mio. Aufgrund der Erhöhung der Sitzungsgrenze muss der Router mehr IDBs unterstützen. Diese Unterstützung wirkt sich auf die Leistung aus, da mehr CPU-Zyklen erforderlich sind, um mehr Instanzen des PPP-Statuscomputers auszuführen.

Die wichtigsten Punkte der PPPoA-Architektur

In diesem Abschnitt werden drei Hauptpunkte der PPPoA-Architektur beschrieben: CPE, IP-Management und Erreichen des Serviceziels.



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.

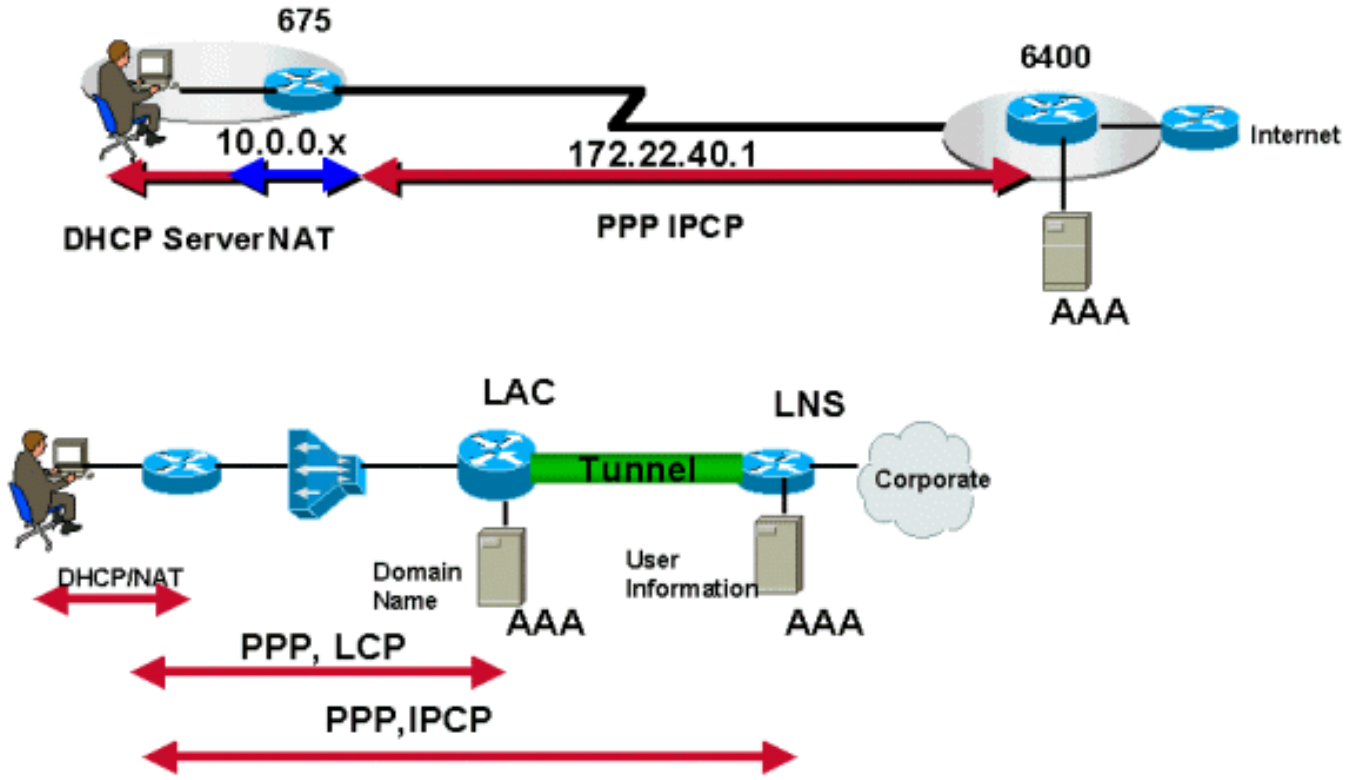
Optionally, the CPE may be configured as a DHCP server to provide private IP addresses to end stations on the LAN. The CPE can also be configured to do Port Address Translation (PAT). A CPE configured for PAT and DHCP usually gets a single public IP address from the final destination and all the stations 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.

Aufgrund der Art von PAT können bestimmte Anwendungen, die IP-Informationen in die Nutzlast einbetten, in diesem Szenario nicht funktionieren. Um dieses Problem zu beheben, wenden Sie ein Subnetz von IP-Adressen anstelle einer einzigen IP-Adresse an.

In dieser Architektur ist es für NAP/NSP einfacher, Telnet in das CPE zu konfigurieren und Fehler zu beheben, da dem CPE eine IP-Adresse zugewiesen wurde.

CPEs können je nach Profil des Teilnehmers verschiedene Optionen verwenden. Beispielsweise kann für Privatanwender das CPE ohne PAT/DHCP konfiguriert werden. Bei Abonnenten mit mehr als einem PC können CPEs entweder für PAT/DHCP oder auf die gleiche Weise konfiguriert werden wie Benutzer in Privatwohnungen. Wenn ein an die CPE angeschlossenes IP-Telefon vorhanden ist, kann die CPE für mehrere PVCs konfiguriert werden.

IP-Management



In der PPPoA-Architektur verwendet die IP-Adressenzuweisung für die CPE-Teilnehmer IPCP-Aushandlung, das gleiche Prinzip wie PPP im Wählmodus. IP-Adressen werden abhängig vom Typ des Dienstes zugewiesen, den ein Abonnent verwendet. Wenn der Teilnehmer nur über Internetzugang des NSP verfügt, beendet der NSP diese PPP-Sitzungen vom Teilnehmer und weist ihm eine IP-Adresse zu. Die IP-Adresse wird aus einem lokal definierten Pool, einem DHCP-Server, zugewiesen oder kann vom RADIUS-Server übernommen werden. Außerdem kann der ISP dem Teilnehmer eine Reihe statischer IP-Adressen bereitgestellt haben und die IP-Adressen nicht dynamisch zuweisen, wenn der Teilnehmer die PPP-Sitzung initiiert. In diesem Szenario verwendet der Dienstanbieter nur den RADIUS-Server, um den Benutzer zu authentifizieren.

Wenn der Teilnehmer mehrere Dienste zur Verfügung stellen möchte, muss der NSP möglicherweise SSG implementieren. Im Folgenden finden Sie Möglichkeiten zum Zuweisen von IP-Adressen.

- Der SP kann dem Abonnenten über seinen lokalen Pool oder RADIUS-Server eine IP-Adresse bereitstellen. Nachdem der Benutzer einen Service ausgewählt hat, leitet die SSG den Datenverkehr des Benutzers an dieses Ziel weiter. Wenn die SSG den Proxymodus verwendet, kann das endgültige Ziel eine IP-Adresse bereitstellen, die die SSG als sichtbare Adresse für die NAT verwendet.
- Die PPP-Sitzungen werden nicht auf dem Aggregation Router des Service Providers beendet. Sie werden entweder getunnelt oder an das endgültige Ziel- oder Heim-Gateway weitergeleitet, das die PPP-Sitzungen schließlich beendet. Das Ziel- oder Home-Gateway handelt IPCP mit dem Teilnehmer aus und stellt so dynamisch eine IP-Adresse bereit. Statische Adressen sind auch möglich, solange das endgültige Ziel diese IP-Adressen zugewiesen hat und eine Route zu ihnen hat.

Vor der Cisco IOS Software-Version 12.0.5DC für das Cisco 6400 NRP gab es für den Service Provider keine Möglichkeit, dem Abonnenten ein Subnetz von IP-Adressen bereitzustellen. Die Cisco 6400-Plattform und die CPEs der Cisco 600-Serie ermöglichen die dynamische

Konfiguration von IP-Subnetzen auf dem CPE während der PPP-Aushandlung. Dem CPE wird eine IP-Adresse aus diesem Subnetz zugewiesen, und die verbleibenden IP-Adressen werden den Stationen dynamisch über DHCP zugewiesen. Wenn diese Funktion verwendet wird, müssen CPEs nicht für PAT konfiguriert werden, das mit einigen Anwendungen nicht funktioniert.

Erreichen des Dienstziels

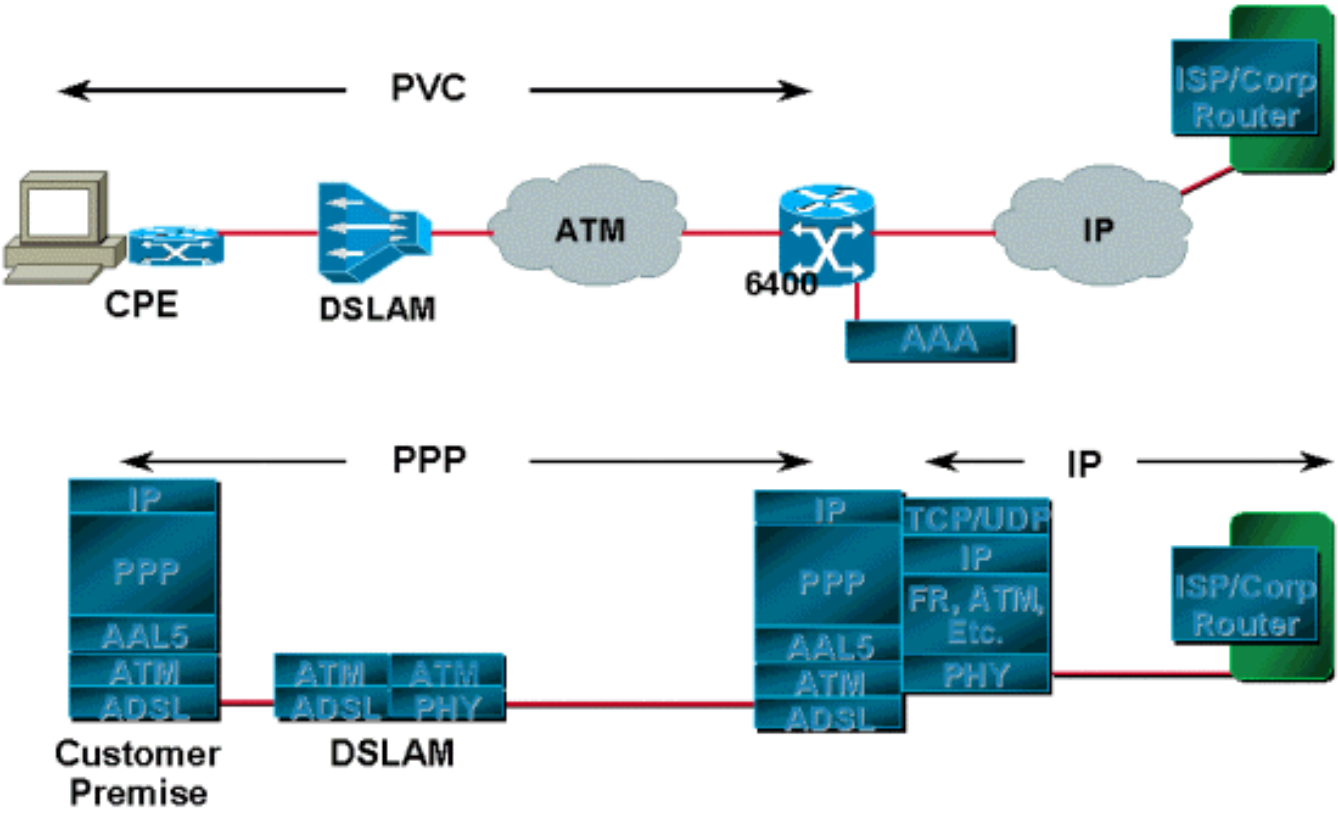
In PPPoA-Architekturen kann das Serviceziel auf verschiedene Weise erreicht werden. Zu den am häufigsten eingesetzten Methoden gehören:

- Beenden von PPP-Sitzungen beim Service Provider
- L2TP-Tunneling
- Verwenden von SSG

In allen drei Methoden ist ein fester Satz von PVCs vom CPE zum DSLAM definiert, der auf einen festen Satz von PVCs auf dem Aggregation Router umgestellt wird. Die PVCs werden über eine ATM-Cloud vom DSLAM zum Aggregation Router zugeordnet.

Das Service-Ziel kann auch mit anderen Methoden wie PPPoA mit SVCs oder Multiprotocol Label Switching/Virtual Private Network erreicht werden. Diese Methoden gehen über den Rahmen dieses Dokuments hinaus und werden in separaten Dokumenten behandelt.

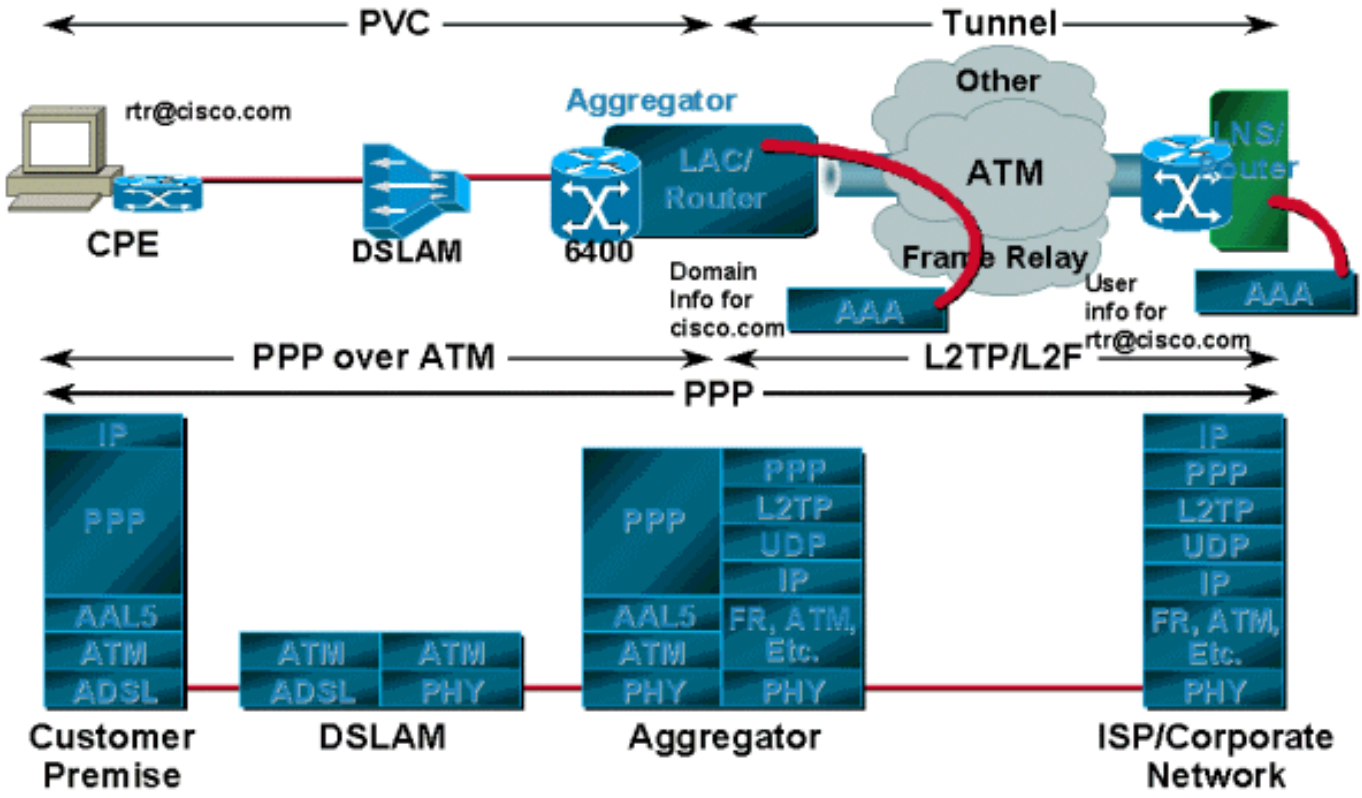
Terminierendes PPP bei Aggregation



Die vom Abonnenten initiierten PPP-Sitzungen werden vom Dienstanbieter beendet, der Benutzer entweder über eine lokale Datenbank auf dem Router oder über RADIUS-Server authentifiziert. Nach der Authentifizierung des Benutzers wird IPCP-Aushandlung durchgeführt, und die IP-Adresse wird dem CPE zugewiesen. Nachdem die IP-Adresse zugewiesen wurde, wird sowohl auf dem CPE als auch auf dem Aggregation Router eine Host-Route eingerichtet. Die dem

Abonnenten zugewiesenen IP-Adressen werden, falls legal, dem Edge-Router angekündigt. Der Edge-Router ist das Gateway, über das der Teilnehmer auf das Internet zugreifen kann. Wenn die IP-Adressen privat sind, übersetzt der Service Provider sie, bevor er sie an den Edge-Router weitergibt.

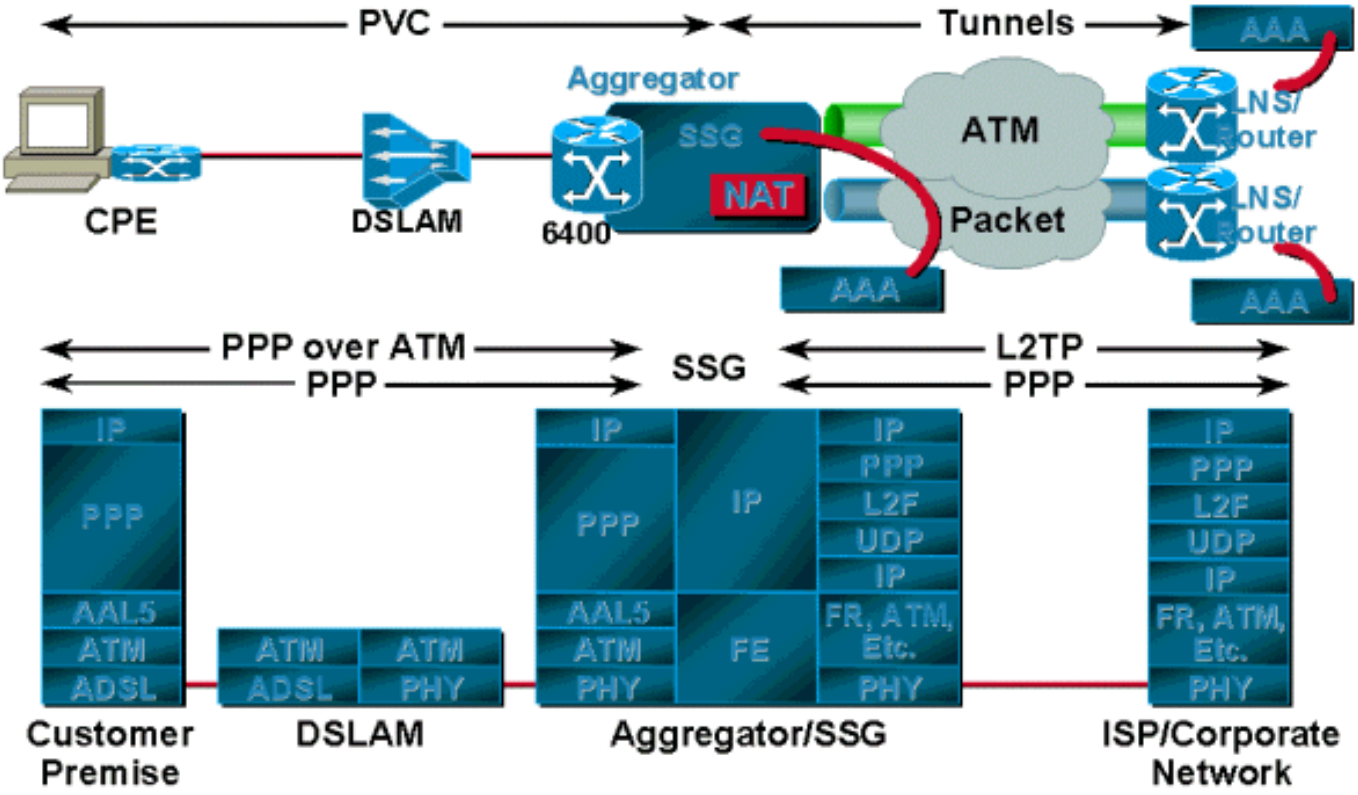
L2TP/L2F-Tunneling



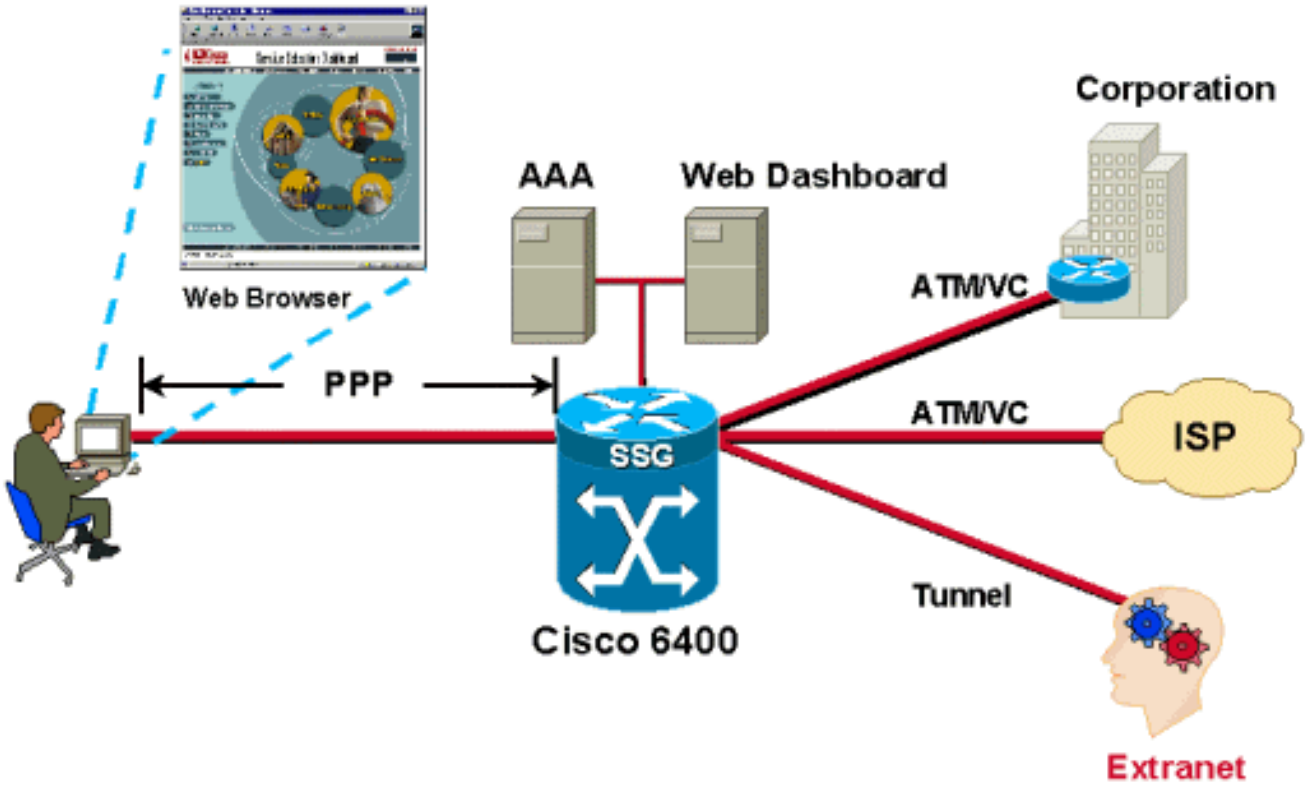
PPP-Sitzungen werden je nach Service Provider oder Unternehmen mithilfe von L2TP oder L2F auf den Upstream-Terminierungspunkt übertragen, anstatt auf dem Aggregation Router des Service Providers terminiert zu werden. Dieser Endpunkt authentifiziert den Benutzernamen, und dem Teilnehmer wird über DHCP oder einen lokalen Pool eine IP-Adresse zugewiesen. In diesem Szenario wird in der Regel ein Tunnel zwischen dem L2TP Access Concentrator/Network Access Server (LAC/NAS) und dem Home Gateway oder dem L2TP Network Server (LNS) eingerichtet. Die LAC authentifiziert die eingehende Sitzung anhand des Domänennamens. Der Benutzername wird am Zielort oder Gateway authentifiziert.

Bei diesem Modell kann der Benutzer jedoch nur auf das endgültige Ziel zugreifen und gleichzeitig nur auf ein Ziel zugreifen. Wenn die CPE beispielsweise mit dem Benutzernamen rtr@cisco.com konfiguriert ist, können die PCs hinter diesem CPE nur auf die Cisco-Domäne zugreifen. Wenn sie eine Verbindung zu einem anderen Unternehmensnetzwerk herstellen möchten, müssen sie den Benutzernamen und das Passwort auf dem CPE ändern, um diesen Firmendomänennamen wiederzugeben. Das Tunnelziel wird in diesem Fall mithilfe eines Routing-Protokolls, statischer Routen oder mittels klassischer IP-over-ATM erreicht (wenn der ATM als Layer 2 bevorzugt wird).

Verwenden des Service Selection Gateway (SSG)



Der Hauptvorteil von SSG gegenüber Tunneling besteht darin, dass SSG die Zuordnung von Eins-zu-Mehren-Diensten ermöglicht, während Tunneling nur Eins-zu-Eins-Zuordnungen bietet. Dies ist besonders nützlich, wenn ein einzelner Benutzer Zugriff auf mehrere Services benötigt oder mehrere Benutzer an einem Standort jeweils Zugriff auf einen eindeutigen Service benötigen. Die SSG verwendet das webbasierte Service Selection Dashboard (SSD), das aus verschiedenen Diensten besteht und dem Benutzer zur Verfügung steht. Der Benutzer kann auf einen oder mehrere Dienste gleichzeitig zugreifen. Ein weiterer Vorteil von SSG besteht darin, dass der Service Provider dem Benutzer die Kosten für die verwendeten Services und die Sitzungszeit berechnen kann und dass der Benutzer die Services über die SSD ein- und ausschalten kann.



Benutzer werden authentifiziert, sobald die PPP-Sitzung von den Teilnehmern eingeht. Benutzern werden entweder vom lokalen Pool oder vom RADIUS-Server IP-Adressen zugewiesen. Nachdem ein Benutzer erfolgreich authentifiziert wurde, wird vom SSG-Code ein Quellobjekt erstellt, und der Benutzer erhält Zugriff auf ein Standardnetzwerk. Das Standardnetzwerk enthält den SSD-Server. Über einen Browser meldet sich der Benutzer beim Dashboard an, wird vom AAA-Server authentifiziert, und je nach dem Benutzerprofil, das auf dem RADIUS-Server gespeichert ist, erhält er eine Reihe von Diensten für den Zugriff.

Jedes Mal, wenn ein authentifizierter Benutzer einen Dienst auswählt, erstellt die SSG ein Zielobjekt für diesen Benutzer. Das Zielobjekt enthält Informationen wie die Zieladresse, die DNS-Serveradresse für dieses Ziel und die zugewiesene Quell-IP-Adresse des Home-Gateways. Pakete, die von der Benutzerseite eingehen, werden basierend auf den im Zielobjekt enthaltenen Informationen an das Ziel weitergeleitet.

SSG kann für Proxydienste, transparente Passthrough oder PTA konfiguriert werden. Wenn ein Teilnehmer den Zugriff auf einen Proxydienst anfordert, leitet das NRP-SSG die Zugriffsanforderung an den Remote-RADIUS-Server weiter. Beim Empfang der Zugriffsannahme antwortet die SSG dem Teilnehmer mit der Zugriffsannahme. Das SSG wird dem Remote-RADIUS-Server als Client angezeigt.

Durch transparentes Passthrough kann nicht authentifizierter Teilnehmerdatenverkehr in beide Richtungen über das SSG weitergeleitet werden. Verwenden Sie Filter, um den transparenten Passthrough-Datenverkehr zu kontrollieren.

PTA kann nur von Benutzern verwendet werden, die PPP-Typen verwenden. Authentifizierung, Autorisierung und Abrechnung werden genau wie im Proxydiensttyp ausgeführt. Ein Teilnehmer meldet sich mit einem Benutzernamen im Formular user@service bei einem Dienst an. Das SSG leitet dies an den RADIUS-Server weiter, der dann das Serviceprofil in das SSG lädt. Das SSG leitet die Anforderung an den Remote-RADIUS-Server weiter, wie im RADIUS-Serverattribut des Serviceprofils festgelegt. Nach der Authentifizierung der Anfrage wird dem Teilnehmer eine IP-

Adresse zugewiesen. Es wird keine NAT durchgeführt. Der gesamte Benutzerdatenverkehr wird in das Remote-Netzwerk aggregiert. Mit PTA können Benutzer nur auf einen Service zugreifen und haben keinen Zugriff auf das Standardnetzwerk oder die SSD.

Betriebsbeschreibung der PPPoA-Architektur

Wenn die CPE zum ersten Mal eingeschaltet wird, sendet sie LCP-Konfigurationserfordernisse an den Aggregationsserver. Der Aggregationsserver sendet bei konfigurierten PVCs auch die LCP-Konfigurationsanforderung an eine Virtual Access Interface (eine Schnittstelle für den virtuellen Zugriff). Wenn jeder die Konfigurationsanforderung der anderen empfängt, werden die Anfragen bestätigt, und der LCP-Status wird geöffnet.

Für die Authentifizierungsphase sendet das CPE die Authentifizierungsanfrage an den Aggregationsserver. Der Server authentifiziert den Benutzer je nach Konfiguration entweder anhand des Domänennamens (falls vorhanden) oder anhand des Benutzernamens mithilfe seiner lokalen Datenbank oder der RADIUS-Server. Wenn die Anfrage des Teilnehmers in Form von username@domainname erfolgt, versucht der Aggregationsserver, einen Tunnel zum Ziel zu erstellen, falls dieser noch nicht vorhanden ist. Nachdem der Tunnel erstellt wurde, leitet der Aggregationsserver die PPP-Anfragen vom Teilnehmer an das Ziel weiter. Das Ziel wiederum authentifiziert den Benutzer und weist ihm eine IP-Adresse zu. Wenn die Anfrage des Teilnehmers den Domänennamen nicht enthält, wird der Benutzer von der lokalen Datenbank authentifiziert. Wenn SSG auf dem Aggregation Router konfiguriert ist, kann der Benutzer wie angegeben auf das Standardnetzwerk zugreifen und verschiedene Services auswählen.

Schlussfolgerung

PPPoA ist für viele Service Provider die am besten geeignete Architektur, da es hochgradig skalierbar ist, SSG-Funktionen verwendet und für Sicherheit sorgt. Da der Schwerpunkt dieses Whitepapers auf der PPPoA-Architektur lag, war es nicht möglich, Funktionen wie SSG eingehend zu behandeln. Diese Funktionen werden in späteren Artikeln behandelt. Beispielkonfigurationen für die verschiedenen in diesem Dokument behandelten Szenarien werden ebenfalls in separaten Dokumenten vorgestellt und erläutert.

Zugehörige Informationen

- Informationen zum Cisco DSL-Produktsupport
- Technischer Support - Cisco Systems