Architettura di base PPPoA

Sommario

Introduzione

Questo documento descrive un'architettura ADSL (Asymmetric Digital Subscriber Line) end-to-end che utilizza il protocollo Point-to-Point sulla modalità di trasferimento asincrono (PPPoA). Sebbene la maggior parte delle implementazioni sia basata sull'architettura di bridging, il protocollo PPPoA sta acquisendo un'enorme popolarità e formerà una porzione più ampia delle future implementazioni ADSL.

Presupposto

L'architettura di base presuppone la necessità di fornire accesso ad alta velocità a Internet e accesso aziendale all'utente finale utilizzando il protocollo PPPoA come backbone principale. Questa architettura si baserà sui canali virtuali privati (PVC), il metodo utilizzato più di frequente nelle installazioni correnti. L'architettura basata su circuiti virtuali commutati (SVC) verrà illustrata in un documento separato.

Questo documento si basa su implementazioni esistenti e su test interni dell'architettura.

Questo documento presuppone che il lettore sia a conoscenza delle considerazioni di progettazione di un provider di accesso alla rete (NAP), come descritto nel white paper RFC1483 Bridging Baseline Architecture.

Tecnologie in breve

Il protocollo PPP (Point-to-Point) (RFC 1331) costituisce un metodo standard per l'incapsulamento dei protocolli di livello superiore nelle connessioni punto-punto. Estende la struttura dei pacchetti HDLC (High-Level Data Link Control) con un identificatore di protocollo a 16 bit che contiene informazioni sul contenuto del pacchetto.

Il pacchetto contiene tre tipi di informazioni:

- LCP (Link Control Protocol) - negozia i parametri del collegamento, le dimensioni del pacchetto o il tipo di autenticazione
- Protocollo NCP (Network Control Protocol): contiene informazioni sui protocolli di livello superiore, inclusi IP e IPX, e sui relativi protocolli di controllo (IPCP per IP)
- Frame di dati contenenti dati

Il protocollo PPP over ATM adaptation layer 5 (AAL5) (RFC 2364) utilizza AAL5 come protocollo con frame, che supporta sia PVC che SVC. Il protocollo PPPoA è stato implementato principalmente nell'ambito dell'ADSL. Si basa sulla RFC 1483, che funziona in modalità LLC-SNAP (Logical Link Control-Subnetwork Access Protocol) o VC-Mux. Un dispositivo CPE (Customer Premise Equipment) incapsula la sessione PPP basata su questa RFC per il trasporto attraverso il loop ADSL e il DSLAM (Digital Subscriber Line Access Multiplexer).

Vantaggi e svantaggi dell'architettura PPPoA

L'architettura PPPoA eredita la maggior parte dei vantaggi del protocollo PPP utilizzato nel modello di composizione. Alcuni dei punti chiave sono elencati di seguito.

Vantaggi

- Autenticazione per sessione basata su PAP (Password Authentication Protocol) o CHAP (Challenge Handshake Authentication Protocol). Questo è il massimo vantaggio del PPPoA, in quanto l'autenticazione consente di superare il problema della sicurezza in un'architettura di bridging.
- L'accounting per sessione è possibile e consente al provider di servizi di addebitare al sottoscrittore il costo in base al tempo di sessione per i vari servizi offerti. L'accounting per sessione consente a un provider di servizi di offrire un livello di accesso minimo a un costo minimo e quindi di addebitare agli abbonati i servizi aggiuntivi utilizzati.
- Conservazione degli indirizzi IP nel CPE. In questo modo il provider di servizi può assegnare un solo indirizzo IP per CPE, con CPE configurato per NAT (Network Address Translation). Tutti gli utenti dietro un CPE possono utilizzare un singolo indirizzo IP per raggiungere diverse destinazioni. Il sovraccarico di gestione IP per il provider di accesso alla rete/provider di servizi di rete (NAP/NSP) per ogni singolo utente viene ridotto conservando gli indirizzi IP. Inoltre, il provider di servizi può fornire una piccola subnet di indirizzi IP per superare le limitazioni di Port Address Translation (PAT) e NAT.
- I NAP/NSP forniscono accesso sicuro ai gateway aziendali senza la gestione di PVC end-to-end e l'utilizzo del routing di livello 3 o dei tunnel L2F/L2TP (Layer 2 Forwarding/Layer 2 Tunneling Protocol). Pertanto, possono scalare i loro modelli commerciali per la vendita di servizi all'ingrosso.
- Risoluzione dei problemi dei singoli sottoscrittori. L'NSP è in grado di identificare facilmente i sottoscrittori attivi o inattivi in base alle sessioni PPP attive, evitando di risolvere i problemi di interi gruppi come nel caso dell'architettura di bridging.

- L'NSP può sovrascrivere distribuendo timeout di inattività e di sessione utilizzando un server RADIUS (Remote Authentication Dial-In User Service) standard del settore per ogni sottoscrittore.
- Altamente scalabile in quanto è possibile terminare un numero molto elevato di sessioni PPP su un router di aggregazione. L'autenticazione, l'autorizzazione e l'accounting possono essere gestiti per ogni utente tramite server RADIUS esterni.
- Utilizzo ottimale delle funzionalità di SSG (Service Selection Gateway).

Svantaggi

- Una sola sessione per CPE su un canale virtuale (VC). Poiché il nome utente e la password sono configurati sul CPE, tutti gli utenti del CPE per quel particolare VC possono accedere a un solo set di servizi. Gli utenti non possono selezionare diversi gruppi di servizi, sebbene sia possibile utilizzare più VC e stabilire diverse sessioni PPP su diverse VC.
- Maggiore complessità dell'impostazione di CPE. Il personale dell'help desk presso il provider di servizi deve essere più informato. Poiché il nome utente e la password sono configurati sul CPE, il sottoscrittore o il fornitore del CPE dovrà apportare le modifiche necessarie alla configurazione. L'utilizzo di più VC aumenta la complessità della configurazione. Tuttavia, per evitare questo problema, occorre usare una funzionalità di configurazione automatica non ancora rilasciata.
- Il provider di servizi deve gestire un database di nomi utente e password per tutti i sottoscrittori. Se si utilizzano tunnel o servizi proxy, l'autenticazione può essere eseguita sulla base del nome di dominio e l'autenticazione dell'utente viene eseguita sul gateway aziendale. In questo modo si riducono le dimensioni del database che il provider di servizi deve gestire.
- Se viene fornito un singolo indirizzo IP al CPE e viene implementato NAT/PAT, alcune applicazioni come IPTV, che incorporano le informazioni IP nel payload, non funzioneranno. Inoltre, se si utilizza una subnet IP, è necessario riservare un indirizzo IP anche per il CPE.

Considerazioni sull'implementazione dell'architettura PPPoA

Prima di implementare l'architettura PPPoA, è necessario considerare i seguenti aspetti principali:

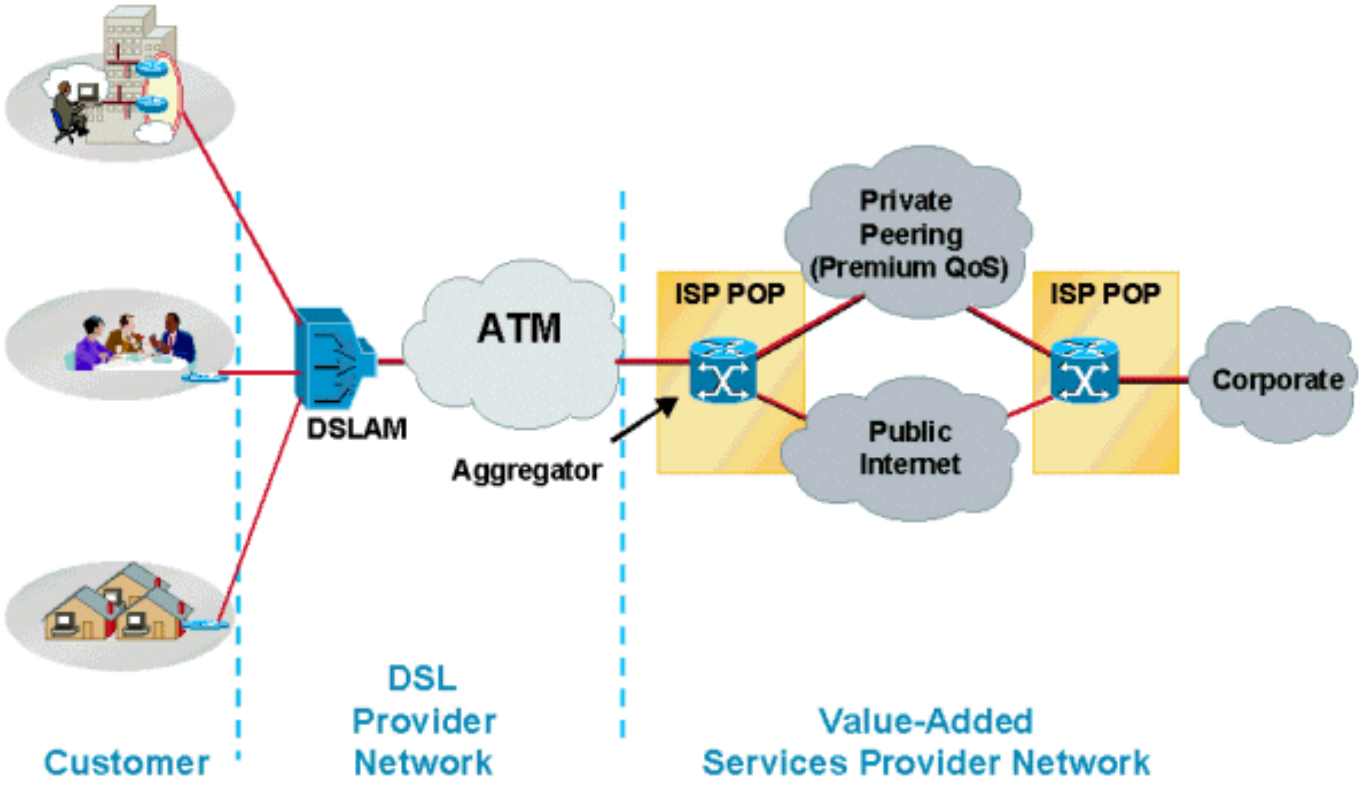
- Il numero di sottoscrittori che verranno serviti attualmente e in futuro, in quanto influisce sul numero di sessioni PPP richieste.
- Se le sessioni PPP vengono terminate sul router di aggregazione del provider di servizi o inoltrate ad altri gateway aziendali o provider di servizi Internet (ISP).
- Se l'indirizzo IP viene fornito dal provider di servizi o dalla destinazione finale del servizio al CPE dell'abbonato.
- Indica se gli indirizzi IP forniti sono pubblici o privati. Il CPE eseguirà NAT/PAT o NAT nella destinazione di terminazione?
- Profili di utenti finali, utenti privati, utenti di piccole imprese e telelavoratori.
- Nel caso di più utenti, se tutti gli utenti devono raggiungere la stessa destinazione finale o lo stesso servizio o se hanno tutti destinazioni di servizio diverse.
- Il fornitore di servizi fornisce servizi a valore aggiunto come voce o video? Il provider di servizi richiede a tutti gli abbonati di accedere a una determinata rete prima di raggiungere una destinazione finale? Quando gli abbonati utilizzano SSG, utilizzano servizi pass-through, PPP Terminated Aggregation (PTA), un dispositivo di mediazione o un proxy?

- Modalità di fatturazione dei sottoscrittori da parte del provider di servizi in base a una tariffa fissa, all'utilizzo per sessione o ai servizi utilizzati.
- Installazione e provisioning di CPE, DSLAM e punti di presenza di aggregazione (POP).
- Modello di business per Protezione accesso alla rete. Il modello include anche la vendita all'ingrosso di servizi quali accesso sicuro alle aziende e servizi a valore aggiunto come voce e video? Protezione accesso alla rete e NSP sono la stessa entità?
- Il modello di business della società. È paragonabile a un operatore locale indipendente di borsa (ILEC), a un operatore locale di borsa (CLEC) competitivo o a un ISP?
- I tipi di applicazioni che l'NSP offrirà all'utente finale.
- Volume previsto a monte e a valle del flusso di dati.

Tenendo presenti questi punti, discuteremo di come l'architettura PPPoA si adatta e si adatta a diversi modelli di business per i fornitori di servizi e di come i fornitori possono trarre vantaggio dall'utilizzo di questa architettura.

Architettura di rete PPPoA tipica

Il diagramma seguente mostra una tipica architettura di rete PPPoA. I clienti che utilizzano i CPE si connettono alla rete del provider di servizi tramite un Cisco DSLAM, che si connette a un aggregatore Cisco 6400 tramite ATM.



Considerazioni sulla progettazione dell'architettura PPPoA

Nella sezione "Considerazioni sull'implementazione" di questo documento, le architetture PPPoA possono essere distribuite utilizzando scenari diversi a seconda del modello aziendale del provider di servizi. In questa sezione verranno descritte le diverse possibilità e considerazioni che i provider di servizi devono tenere presenti prima di implementare una soluzione.

Prima di implementare un'architettura PPPoA e una particolare soluzione per questa architettura, è essenziale comprendere il modello di business del provider di servizi. Considerare i servizi che verranno offerti dal provider di servizi. Il fornitore di servizi offrirà ai suoi abbonati finali un servizio come l'accesso a Internet ad alta velocità o venderà servizi all'ingrosso a diversi fornitori di servizi Internet e fornirà servizi a valore aggiunto a tali abbonati? Il fornitore di servizi li offrirà tutti?

In caso di accesso a Internet ad alta velocità in un ambiente in cui NSP e Protezione accesso alla rete sono gli stessi, le sessioni PPP del sottoscrittore devono essere terminate nel router di aggregazione distribuito. In questo scenario, i provider di servizi devono considerare il numero di sessioni PPP che possono essere terminate su un singolo dispositivo di aggregazione di router, il modo in cui gli utenti verranno autenticati, il modo in cui eseguiranno l'accounting e il percorso a Internet una volta terminate le sessioni utente. A seconda del numero di sessioni PPP e di sottoscrittori, il router di aggregazione può essere un Cisco 6400 o un Cisco 7200. Attualmente Cisco 6400 con NRP (Route Processor) a 7 nodi può terminare fino a 14.000 sessioni PPP. Cisco 7200 è limitato a 2.000 sessioni PPP. Questi numeri cambieranno con le nuove versioni. Per il numero esatto di sessioni supportate da ciascun router di aggregazione, consultare le note sulla versione e i documenti del prodotto.

In questi scenari l'autenticazione e l'accounting degli utenti vengono gestiti in modo ottimale tramite un server RADIUS standard del settore, che può autenticare un utente in base al nome utente o all'identificatore del percorso virtuale o all'identificatore del canale virtuale (VPI/VCI) utilizzato.

Per l'accesso a Internet ad alta velocità, gli NSP di solito fatturano ai clienti una tariffa fissa. La maggior parte delle distribuzioni correnti viene implementata in questo modo. Quando NSP e Protezione accesso alla rete sono la stessa entità, ai clienti viene fatturata una tariffa di accesso fissa e un'altra tariffa fissa per l'accesso a Internet. Questo modello cambia quando il provider di servizi inizia a offrire servizi a valore aggiunto. I fornitori di servizi possono addebitare al cliente un costo in base al tipo di servizio e alla durata del servizio. I clienti si connettono a Internet tramite il router di aggregazione utilizzando protocolli di routing come Open Shortest Path First (OSPF) o Enhanced Interior Gateway Routing Protocol (EIGRP) su un router perimetrale che potrebbe eseguire Border Gateway Protocol (BGP).

Un'altra opzione di cui dispone il provider di servizi per fornire l'accesso a Internet ad alta velocità consiste nell'inoltrare le sessioni PPP in arrivo dagli abbonati a un ISP separato utilizzando il tunneling L2TP/L2F. Quando si usa il tunneling L2x, occorre prestare particolare attenzione a come raggiungere la destinazione del tunnel. Le opzioni disponibili consistono nell'eseguire alcuni protocolli di routing o nel fornire route statiche nel router di aggregazione. Limitazioni per l'utilizzo dei tunnel L2TP o L2F: 1) il numero di tunnel e il numero di sessioni che possono essere supportate in tali tunnel; e 2) l'uso di protocolli di routing incompatibili con ISP di terze parti, che potrebbero richiedere l'uso di route statiche.

Se il provider di servizi offre servizi per diversi ISP o gateway aziendali al destinatario finale, potrebbe essere necessario implementare le funzionalità SSG sul router di aggregazione. In questo modo il sottoscrittore può selezionare diverse destinazioni del servizio utilizzando la selezione del servizio basata sul Web. Il provider di servizi può inoltrare le sessioni PPP degli abbonati alle destinazioni selezionate combinando tutte le sessioni destinate all'ISP in un unico PVC per il trasporto oppure, se il provider di servizi offre più livelli di servizio, è possibile stabilire più PVC nel core.

In un modello di servizio all’ingrosso, il fornitore di servizi non può utilizzare le funzioni SSG. In questo modello, il provider di servizi estende tutte le sessioni PPP ai gateway principali. I gateway principali forniscono gli indirizzi IP al sottoscrittore finale e autenticano l'utente finale.

Un aspetto importante da considerare in ciascuno di questi scenari è il modo in cui il provider di servizi può offrire una diversa qualità del servizio (QoS) per i diversi servizi e il modo in cui calcola l'assegnazione della larghezza di banda. Attualmente, il modo in cui la maggior parte dei provider di servizi distribuisce questa architettura offre QoS diversi su PVC diversi. Possono avere PVC separati sul core per i clienti privati e aziendali. L'utilizzo di PVC diversi consente ai provider di servizi di specificare QoS diversi per servizi diversi. In questo modo, QoS potrebbe trovarsi su PVC separati o sul layer 3.

L'applicazione di QoS al layer 3 richiede che il provider di servizi conosca la destinazione finale, il che potrebbe rappresentare un fattore limitante. Tuttavia, se usato in combinazione con la funzionalità QoS di layer 2 (applicandolo a sistemi di videoconferenza diversi), può essere utile al provider di servizi. Il limite di questo modello è che è fisso e il provider di servizi deve provvedere in anticipo al servizio QoS. QoS non viene applicato dinamicamente alla selezione del servizio. Al momento, non è possibile per un utente selezionare diverse larghezze di banda per diversi servizi con un clic del mouse; tuttavia, sono stati effettuati notevoli sforzi tecnici per sviluppare questa funzione.

L'installazione, la gestione e il provisioning dei CPE potrebbero essere molto impegnativi in questa architettura, in quanto i CPE devono essere configurati per nomi utente e password. Come soluzione semplice, alcuni provider di servizi utilizzano lo stesso nome utente e la stessa password per tutti i CPE. Ciò comporta un rischio significativo per la sicurezza. Inoltre, se il CPE deve aprire contemporaneamente diverse sessioni, è necessario eseguire il provisioning di altri VC in CPE, NAP e NSP. Le DSLAM e i dispositivi di aggregazione Cisco sono in grado di semplificare la configurazione e il provisioning CPE. Per il provisioning PVC end-to-end sono inoltre disponibili strumenti di gestione del flusso. Il provisioning nell'NSP per un numero così elevato di utenti che utilizzano PVC è un fattore limitante, poiché è necessario gestire tutti i diversi PVC. Inoltre, non esiste un modo semplice per effettuare il provisioning di 2000 PVC su un singolo NRP facendo clic con il mouse o immettendo alcuni tasti.

Attualmente sono disponibili diverse applicazioni di gestione per i diversi componenti di questa architettura, ad esempio Viewrunner per DSLAM e SCM per Cisco 6400. Non esiste un'unica piattaforma di gestione in grado di effettuare il provisioning di tutti i componenti. Si tratta di una limitazione ben nota e si sta investendo molto per avere un'unica applicazione di gestione completa per il provisioning di CPE, DSLAM e Cisco 6400. Inoltre, attualmente disponiamo di una soluzione per implementare il PPPoA con SVC, che agevolerà notevolmente l'implementazione. Il PPPoA con SVC consente inoltre agli utenti finali di selezionare dinamicamente la destinazione e la QoS.

Un altro punto importante da tenere presente per le distribuzioni ADSL di grandi dimensioni che utilizzano questa architettura è la comunicazione tra il router di aggregazione e il server RADIUS. Se si verifica un errore nel blade del protocollo NRP quando diverse migliaia di sessioni PPP vengono terminate su un dispositivo di aggregazione, è necessario ristabilire tutte le sessioni PPP. Ciò significa che tutti i sottoscrittori devono essere autenticati e che i relativi record di accounting devono essere arrestati e riavviati una volta stabilita la connessione. Quando un numero così elevato di sottoscrittori tenta di ottenere l'autenticazione contemporaneamente, la pipe al server RADIUS può rappresentare un collo di bottiglia. Alcuni sottoscrittori potrebbero non essere in grado di essere autenticati e ciò potrebbe causare problemi al provider di servizi.

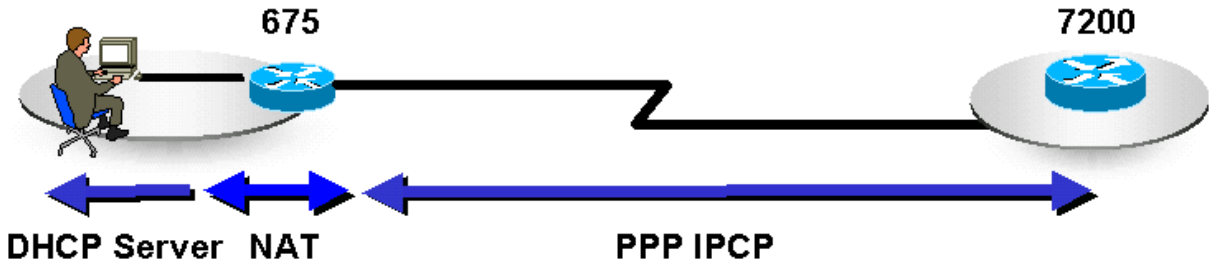
Èmolto importante disporre di un collegamento al server RADIUS con una larghezza di banda sufficiente per consentire l'accesso simultaneo di tutti gli utenti. Inoltre, il server RADIUS deve essere sufficientemente potente da concedere le autorizzazioni a tutti i sottoscrittori. Nel caso di migliaia di sottoscrittori, è opportuno considerare un'opzione per il bilanciamento del carico tra i server RADIUS disponibili. Questa funzionalità è disponibile nel software Cisco IOS®.

Come ultima considerazione, il router di aggregazione deve funzionare in modo adeguato per supportare molte sessioni PPP. Applicare gli stessi principi di progettazione del traffico utilizzati da altre implementazioni. In precedenza, l'utente doveva configurare i PVC su sottointerfacce point-to-point. Oggi il PPPoA consente agli utenti di configurare più PVC su sottointerfacce multipoint e point-to-point. Ogni connessione PPPoA non richiede più due IDB (Interface Descriptor Block), uno per l'interfaccia di accesso virtuale e uno per l'interfaccia secondaria ATM. Questo miglioramento aumenta il numero massimo di sessioni PPPoA in esecuzione su un router.

Il numero massimo di sessioni PPPoA supportate in una piattaforma dipende dalle risorse di sistema disponibili, ad esempio memoria e velocità della CPU. Ogni sessione PPPoA accetta un'interfaccia di accesso virtuale. Ogni interfaccia di accesso virtuale è costituita da un blocco descrittore di interfaccia hardware e da una coppia descrittore di interfaccia software (hwidb/swidb). Ogni widb impiega circa 4.5K. Ogni swidb impiega circa 2.5K. Insieme, le interfacce di accesso virtuale richiedono 7.5K. Le interfacce di accesso virtuale 2000 richiedono 2000 * 7.5K o 15M. Per eseguire 2000 sessioni, un router ha bisogno di altri 15 MB. A causa dell'aumento del limite di sessioni, il router deve supportare più IDB. Questo supporto influisce sulle prestazioni poiché un numero maggiore di cicli della CPU comporta l'esecuzione di più istanze della macchina a stati PPP.

Punti chiave dell'architettura PPPoA

In questa sezione vengono descritti tre punti chiave dell'architettura PPPoA: CPE, gestione IP e raggiungimento della destinazione del servizio.



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.

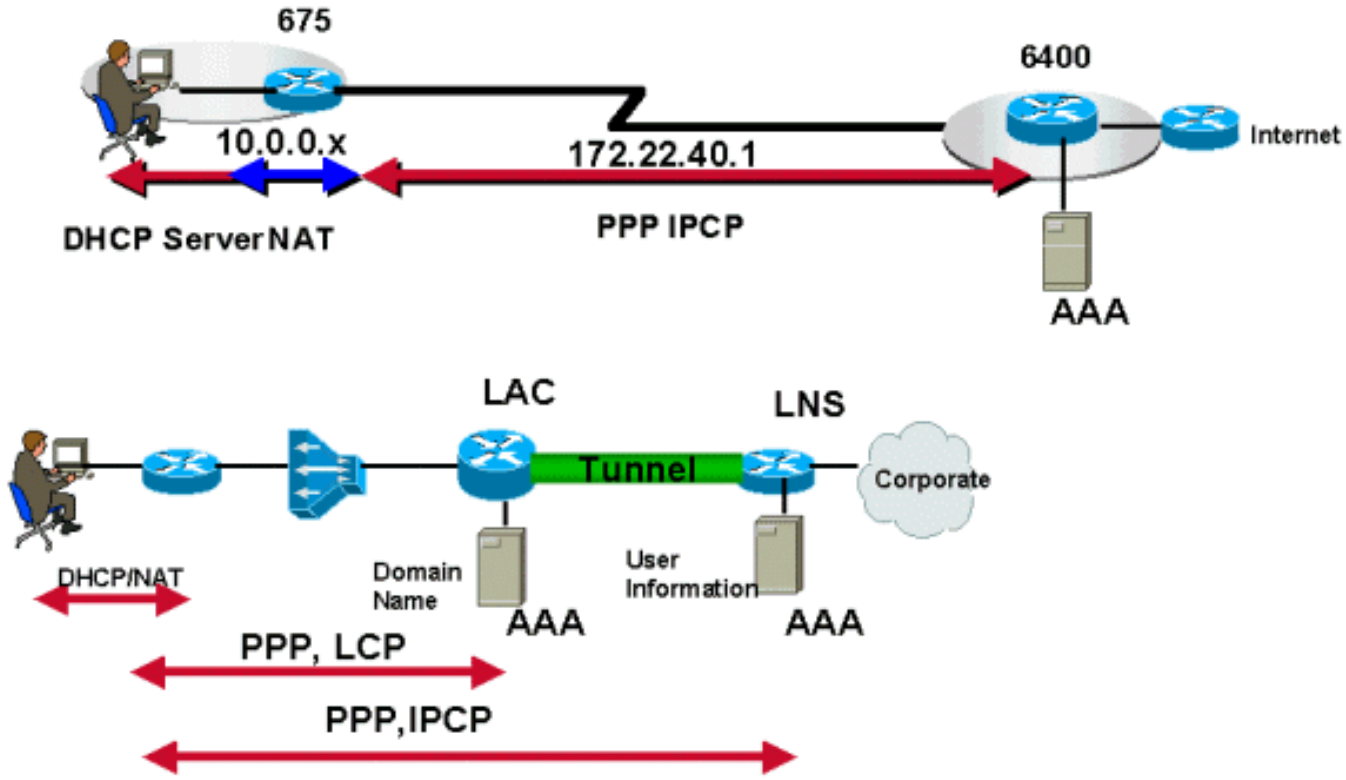
Optionally, the CPE may be configured as a DHCP server to provide private IP addresses to end stations on the LAN. The CPE can also be configured to do Port Address Translation (PAT). A CPE configured for PAT and DHCP usually gets a single public IP address from the final destination and all the stations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

A causa della natura di PAT, alcune applicazioni che incorporano informazioni IP nel payload non possono funzionare in questo scenario. Per risolvere il problema, applicare una subnet di indirizzi IP anziché un singolo indirizzo IP.

In questa architettura è più semplice per Protezione accesso alla rete/Server dei criteri di rete eseguire la connessione Telnet nel CPE per la configurazione e la risoluzione dei problemi, poiché un indirizzo IP viene assegnato al CPE.

I CPE possono utilizzare opzioni diverse a seconda del profilo del sottoscrittore. Ad esempio, per un utente residenziale, il CPE può essere configurato senza PAT/DHCP. Per gli abbonati con più PC, i CPE possono essere configurati per PAT/DHCP o allo stesso modo di un utente residenziale. Se al CPE è collegato un telefono IP, il CPE può essere configurato per più PVC.

Gestione IP



Nell'architettura PPPoA, l'allocazione degli indirizzi IP per la CPE del sottoscrittore utilizza la negoziazione IPCP, lo stesso principio del PPP in modalità dial. Gli indirizzi IP vengono allocati a seconda del tipo di servizio utilizzato da un sottoscrittore. Se il destinatario dispone solo dell'accesso a Internet dall'NSP, l'NSP interromperà le sessioni PPP dal destinatario e assegnerà un indirizzo IP. L'indirizzo IP viene allocato da un pool definito localmente, da un server DHCP o può essere applicato dal server RADIUS. È inoltre possibile che il provider di servizi Internet abbia fornito al sottoscrittore un insieme di indirizzi IP statici e non assegni dinamicamente gli indirizzi IP quando il sottoscrittore avvia la sessione PPP. In questo scenario, il provider di servizi utilizzerà solo il server RADIUS per autenticare l'utente.

Se l'abbonato preferisce avere più servizi disponibili, l'NSP potrebbe dover implementare SSG. Di seguito sono elencate le possibilità per assegnare indirizzi IP.

- L'SP può fornire un indirizzo IP al sottoscrittore tramite il pool locale o il server RADIUS. Dopo aver selezionato un servizio, il servizio SSG inoltra il traffico dell'utente a tale destinazione. Se il SSG utilizza la modalità proxy, la destinazione finale può fornire un indirizzo IP che il SSG utilizzerà come indirizzo visibile per NAT.
- Le sessioni PPP non vengono terminate sul router di aggregazione del provider di servizi. Vengono sottoposti a tunneling o inoltrati alla destinazione finale o al gateway principale, che termina le sessioni PPP. La destinazione finale o il gateway principale negozia l'IPCP con il sottoscrittore, fornendo così un indirizzo IP in modo dinamico. Gli indirizzi statici sono possibili

anche se la destinazione finale ha allocato tali indirizzi IP e dispone di una route per essi. Prima del software Cisco IOS versione 12.0.5DC per Cisco 6400 NRP, il provider di servizi non era in grado di fornire una subnet di indirizzi IP al destinatario. La piattaforma Cisco 6400 e i CPE Cisco serie 600 consentono di configurare dinamicamente le subnet IP sul CPE durante la negoziazione PPP. Un indirizzo IP di questa subnet viene assegnato al CPE e gli altri indirizzi IP vengono allocati dinamicamente alle stazioni tramite DHCP. Quando si utilizza questa funzionalità, non è necessario configurare i CPE per PAT, che non funziona con alcune applicazioni.

Come si raggiunge la destinazione del servizio

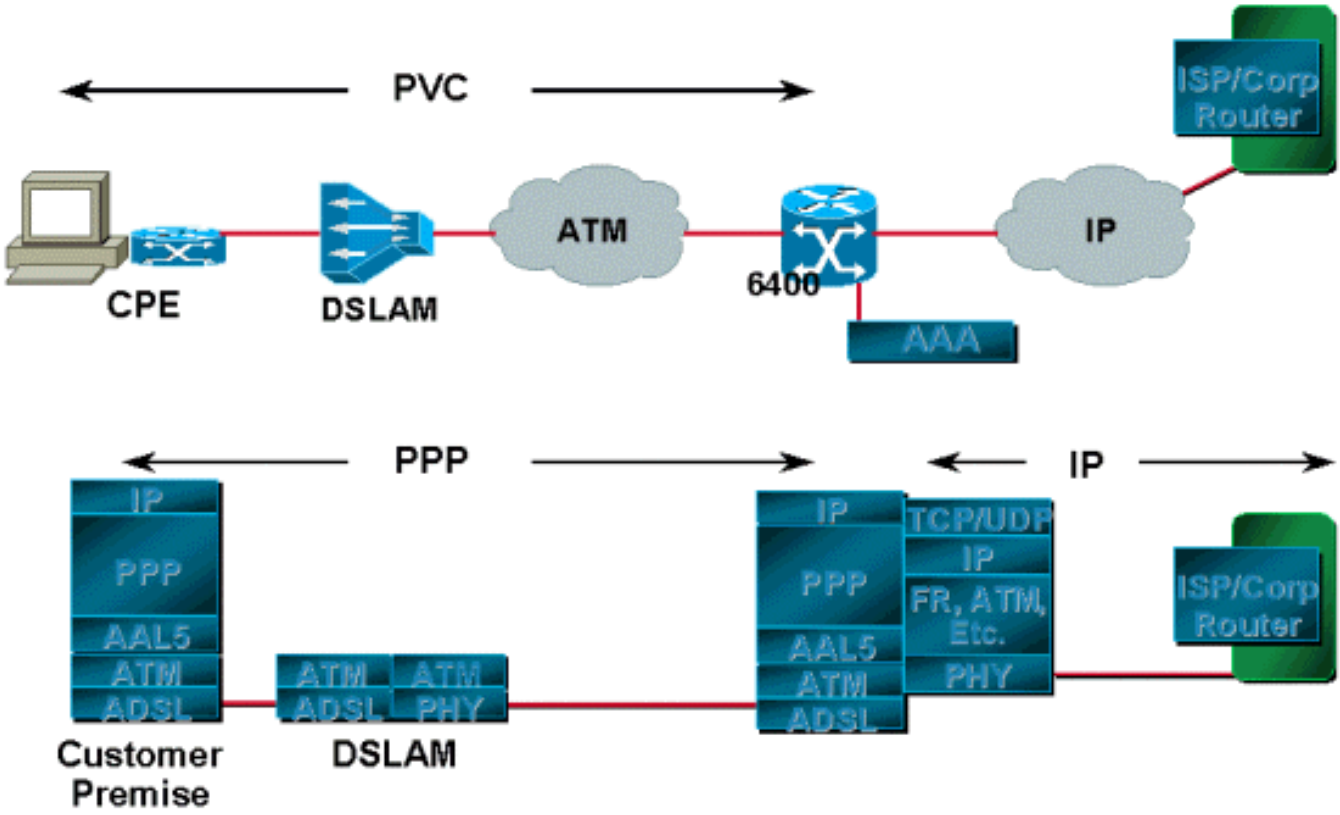
Nelle architetture PPPoA, la destinazione del servizio può essere raggiunta in modi diversi. Alcuni dei metodi più comuni sono:

- Interruzione delle sessioni PPP nel provider di servizi
- Tunneling L2TP
- Uso di SSG

In tutti e tre i metodi è presente un insieme fisso di PVC definito dal CPE al DSLAM che viene commutato in un insieme fisso di PVC sul router di aggregazione. I PVC vengono mappati dal DSLAM al router di aggregazione tramite un cloud ATM.

La destinazione del servizio può essere raggiunta anche utilizzando altri metodi, ad esempio PPPoA con SVC o Multiprotocol Label Switching/Virtual Private Network. Tali metodi esulano dall'ambito del presente documento e saranno discussi in documenti separati.

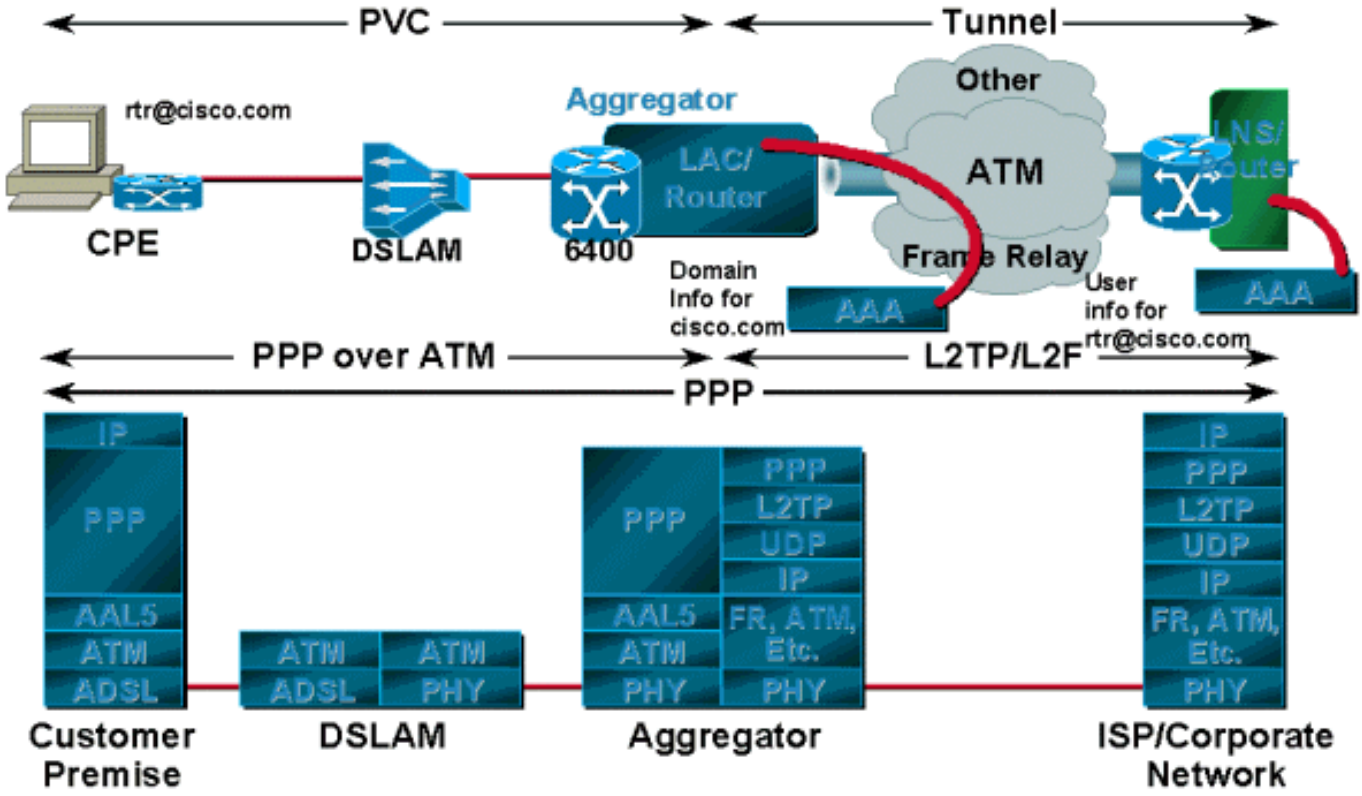
Terminazione di PPP all'aggregazione



Le sessioni PPP avviate dal sottoscrittore vengono terminate dal provider di servizi che autentica gli utenti utilizzando un database locale sul router o tramite server RADIUS. Dopo l'autenticazione

dell'utente, viene eseguita la negoziazione IPCP e l'indirizzo IP viene assegnato al CPE. Dopo aver assegnato l'indirizzo IP, esiste un percorso host definito sia sul CPE sia sul router di aggregazione. Gli indirizzi IP allocati al sottoscrittore, se validi, vengono annunciati al router perimetrale. Il router perimetrale è il gateway attraverso il quale il sottoscrittore può accedere a Internet. Se gli indirizzi IP sono privati, il provider di servizi li converte prima di pubblicizzarli sul router perimetrale.

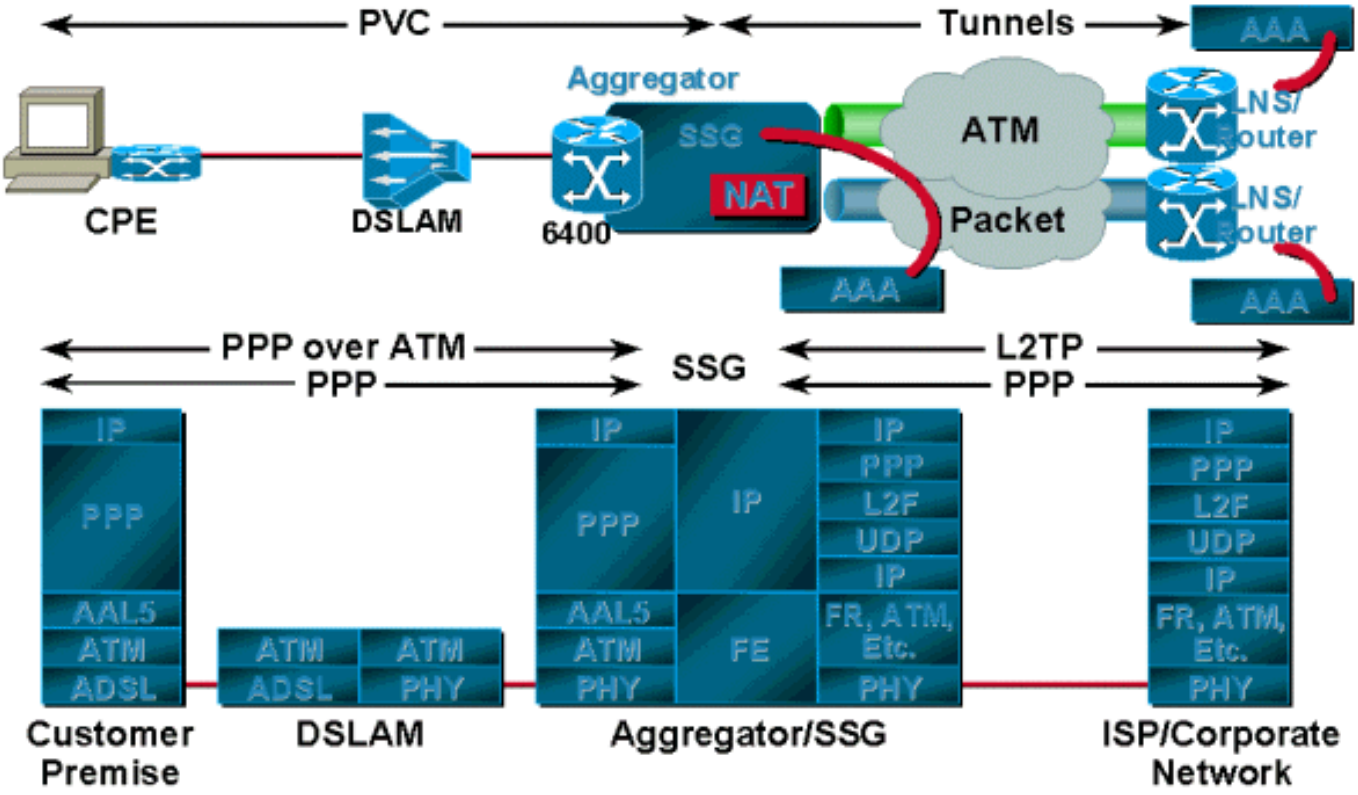
Tunneling L2TP/L2F



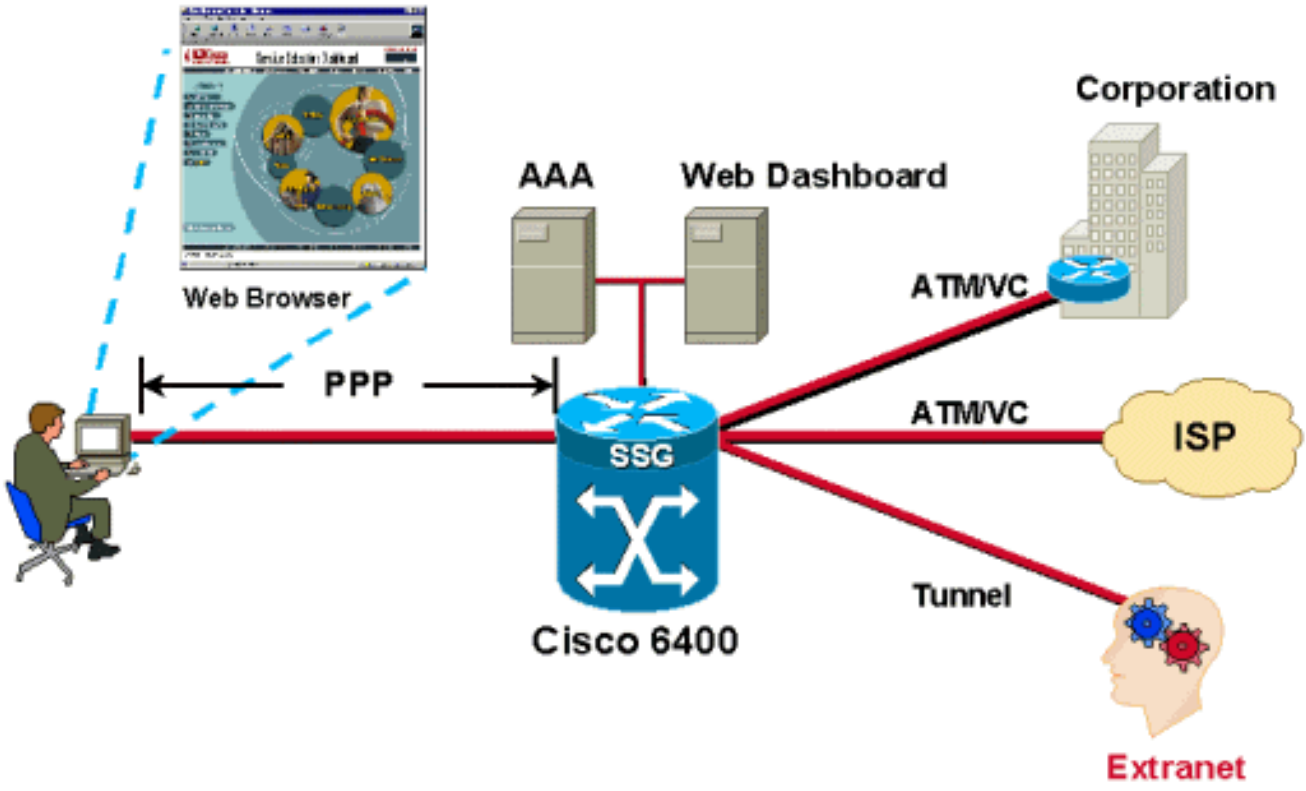
Le sessioni PPP, a seconda del provider di servizi o della società, eseguono il tunnel fino al punto di terminazione a monte utilizzando L2TP o L2F anziché essere terminate sul router di aggregazione del provider di servizi. Questo punto di terminazione autentica il nome utente e al sottoscrittore viene assegnato un indirizzo IP tramite DHCP o un pool locale. In questo scenario, in genere è presente un tunnel stabilito tra il server L2TP Access Concentrator/Network Access Server (LAC/NAS) e il gateway locale o il server di rete L2TP (LNS). L'ACL autentica la sessione in arrivo in base al nome di dominio; il nome utente viene autenticato nella destinazione finale o nel gateway principale.

In questo modello, tuttavia, l'utente può accedere solo alla destinazione finale e a una sola destinazione alla volta. Ad esempio, se il CPE è configurato con il nome utente rtr@cisco.com, i PC su cui si basa il CPE possono accedere solo al dominio Cisco. Se si desidera connettersi a un'altra rete aziendale, è necessario modificare il nome utente e la password del CPE in modo da riflettere il nome di dominio aziendale. In questo caso, la destinazione del tunnel viene raggiunta utilizzando un protocollo di routing, route statiche o eseguendo l'IP classico su ATM (se si preferisce il protocollo ATM come layer 2).

Uso di SSG (Service Selection Gateway)



Il vantaggio principale di SSG rispetto al tunneling è che SSG fornisce la mappatura dei servizi uno-a-molti, mentre il tunneling fornisce solo la mappatura uno-a-uno. Ciò risulta molto utile quando un singolo utente ha bisogno di accedere a più servizi o quando più utenti in un'unica posizione hanno necessità di accedere a un servizio univoco. SSG utilizza il dashboard di selezione dei servizi (SSD, Service Selection Dashboard) basato sul Web, che è costituito da servizi diversi ed è disponibile per l'utente. L'utente può accedere a uno o più servizi contemporaneamente. Un altro vantaggio dell'utilizzo di SSG consiste nel fatto che il provider di servizi può fatturare all'utente i servizi utilizzati e la durata della sessione, nonché attivare e disattivare i servizi tramite SSD.



Gli utenti vengono autenticati quando la sessione PPP arriva dai sottoscrittori. Agli utenti vengono assegnati indirizzi IP dal pool locale o dal server RADIUS. Dopo che un utente è stato autenticato correttamente, un oggetto di origine viene creato dal codice SSG e all'utente viene concesso l'accesso a una rete predefinita. La rete predefinita contiene il server SSD. Utilizzando un browser, l'utente accede al dashboard, viene autenticato dal server AAA e, a seconda del profilo dell'utente archiviato nel server RADIUS, viene offerto un insieme di servizi a cui accedere.

Ogni volta che un utente autenticato seleziona un servizio, SSG crea un oggetto di destinazione per tale utente. L'oggetto di destinazione contiene informazioni quali l'indirizzo di destinazione, l'indirizzo del server DNS per la destinazione e l'indirizzo IP di origine assegnato dal gateway principale. I pacchetti provenienti dall'utente vengono inoltrati alla destinazione in base alle informazioni contenute nell'oggetto di destinazione.

SSG può essere configurato per il servizio proxy, il pass-through trasparente o il PTA. Quando un sottoscrittore richiede l'accesso a un servizio proxy, NRP-SSG passa la richiesta di accesso al server RADIUS remoto. Dopo aver ricevuto la clausola di accettazione dell'accesso, il SSG risponde al destinatario con la clausola di accettazione dell'accesso. SSG viene visualizzato come client sul server RADIUS remoto.

La modalità passthrough trasparente consente di instradare il traffico degli utenti non autenticati attraverso il gateway di servizi condivisi in entrambe le direzioni. Utilizzare i filtri per controllare il traffico passthrough trasparente.

PTA può essere utilizzato solo da utenti di tipo PPP. L'autenticazione, l'autorizzazione e l'accounting vengono eseguiti esattamente come nel tipo di servizio proxy. Un sottoscrittore accede a un servizio utilizzando un nome utente nel formato user@service. Il SSG inoltra il messaggio al server RADIUS, che carica il profilo del servizio nel SSG. SSG inoltra la richiesta al server RADIUS remoto come specificato dall'attributo server RADIUS del profilo del servizio. Dopo l'autenticazione della richiesta, al sottoscrittore viene assegnato un indirizzo IP. Non viene eseguito alcun NAT. Tutto il traffico degli utenti viene aggregato alla rete remota. Con PTA, gli

utenti possono accedere a un solo servizio e non hanno accesso alla rete predefinita o all'unità SSD.

Descrizione operativa dell'architettura PPPoA

Quando CPE viene acceso per la prima volta, inizia a inviare le richieste di configurazione LCP al server di aggregazione. Il server di aggregazione, con i PVC configurati, invia anche la richiesta di configurazione LCP su un'interfaccia di accesso virtuale (associata al PVC). Quando ognuno vede la richiesta di configurazione dell'altro, riconosce le richieste e lo stato LCP viene aperto.

Per la fase di autenticazione, il CPE invia la richiesta di autenticazione al server di aggregazione. A seconda della configurazione, il server esegue l'autenticazione dell'utente in base al nome di dominio (se specificato) oppure in base al nome utente tramite il database locale o i server RADIUS. Se la richiesta del sottoscrittore è nel formato username@domainname, il server di aggregazione tenterà di creare un tunnel verso la destinazione, se non è già presente. Dopo la creazione del tunnel, il server di aggregazione inoltra le richieste PPP dal sottoscrittore alla destinazione. La destinazione, a sua volta, autentica l'utente e assegna un indirizzo IP. Se la richiesta del sottoscrittore non include il nome di dominio, l'utente viene autenticato dal database locale. Se SSG è configurato sul router di aggregazione, l'utente può accedere alla rete predefinita come specificato e può ottenere un'opzione per selezionare servizi diversi.

Conclusioni

Il protocollo PPPoA sta diventando l'architettura più adatta per molti provider di servizi in quanto è altamente scalabile, utilizza la funzionalità SSG e garantisce la sicurezza. Poiché l'argomento principale di questo documento era l'architettura PPPoA, non è stato possibile trattare in modo approfondito aspetti quali SSG. Tali caratteristiche saranno illustrate in documenti successivi. Anche le configurazioni di esempio per i diversi scenari discussi in questo documento saranno presentate e spiegate in documenti separati.

Informazioni correlate

- Informazioni di supporto sui prodotti Cisco DSL
- Supporto tecnico – Cisco Systems