Architettura Bridging Baseline RFC1483

Sommario

Introduzione

In questo documento viene descritta l'architettura ADSL (Asymmetric Digital Subscriber Line) end-to-end quando si utilizza il bridging RFC1483. Notare che la maggior parte delle prime versioni dei modem xDSL erano bridge tra Ethernet 10BaseT sul lato host e bridge frame incapsulati RFC1483 sul lato WAN. Ancora oggi, la maggior parte delle apparecchiature ADSL presso la sede del cliente (CPE) installate sul campo sono in pura modalità bridging.

Presupposto

L'architettura di base è stata progettata partendo dal presupposto che l'accesso a Internet ad alta velocità venga fornito al sottoscrittore finale utilizzando il modello di bridging RFC1483 e ATM come backbone principale. Il contenuto di questo documento si basa sull'architettura delle distribuzioni esistenti e su alcuni test interni.

Tecnologie in breve

RFC1483 descrive due metodi diversi per trasportare il traffico di interconnessione di rete senza connessione su una rete ATM: PDU (Routed Protocol Data Unit) e PDU con bridging.

Il routing consente il multiplexing di più protocolli su un singolo circuito virtuale ATM (VC). Il protocollo di una PDU trasportata viene identificato inserendo un'intestazione LLC (Logical Link Control) IEEE 802.2 come prefisso della PDU.

Il bridging esegue il multiplexing del protocollo di livello superiore in modo implicito da circuiti virtuali ATM. Per ulteriori informazioni, consultare la RFC 1483.

Questo documento si riferisce solo a PDU con bridging.

Vantaggi e svantaggi del bridging RFC1483

Di seguito è riportato un riepilogo dei vantaggi e degli svantaggi dell'architettura di bridging RFC1483. Questa architettura presenta alcuni importanti svantaggi, la maggior parte dei quali sono inerenti al modello di bridging. Alcuni svantaggi sono stati rilevati durante le installazioni ADSL presso le sedi dei clienti.

Vantaggi

- Semplice da capire.Il bridging è molto semplice da comprendere e implementare perché non vi sono problemi complessi quali i requisiti di routing o autenticazione per gli utenti.
- Configurazione minima del CPE.Il fornitore di servizi lo considera importante in quanto non richiede più un gran numero di rulli compressi e non deve più investire ingenti risorse di personale per il supporto di protocolli di livello superiore. Il CPE in modalità bridge funziona come un dispositivo molto semplice. Il CPE richiede una risoluzione minima dei problemi in quanto tutto ciò che proviene da Ethernet passa direttamente al lato WAN.
- Facile da installare.L'architettura di bridging è facile da installare a causa della sua natura semplicistica. Dopo la creazione di PVC (Permanent Virtual Circuit) end-to-end, attività quali l'IP al livello superiore diventano trasparenti.
- Supporto multiprotocollo per il sottoscrittore.Quando il CPE è in modalità bridging, non si preoccupa del protocollo del livello superiore da incapsulare.
- Ideale per l'accesso a Internet in un ambiente a singolo utente.Poiché CPE funge da set-top box, non è necessaria una risoluzione dei problemi complessa per i protocolli di livello superiore. I PC finali non richiedono un'installazione client aggiuntiva.

Svantaggi

- Il bridging dipende in larga misura dalle trasmissioni per stabilire la connettività.Le trasmissioni tra migliaia di utenti sono per loro natura non scalabili. Le ragioni di questo problema sono che il broadcast utilizza la larghezza di banda attraverso il loop xDSL degli utenti e richiede l'uso di risorse sul router headend per replicare i pacchetti per il broadcast su supporti point-to-point (ATM PVC).
- Il bridging è intrinsecamente non sicuro e richiede un ambiente attendibile.Le risposte ARP (Address Resolution Protocol) possono essere oggetto di spoofing e un indirizzo di rete può essere dirottato. Inoltre, gli attacchi broadcast possono essere iniziati sulla subnet locale, negando così il servizio a tutti i membri della subnet locale.
- Il dirottamento dell'indirizzo IP è possibile.

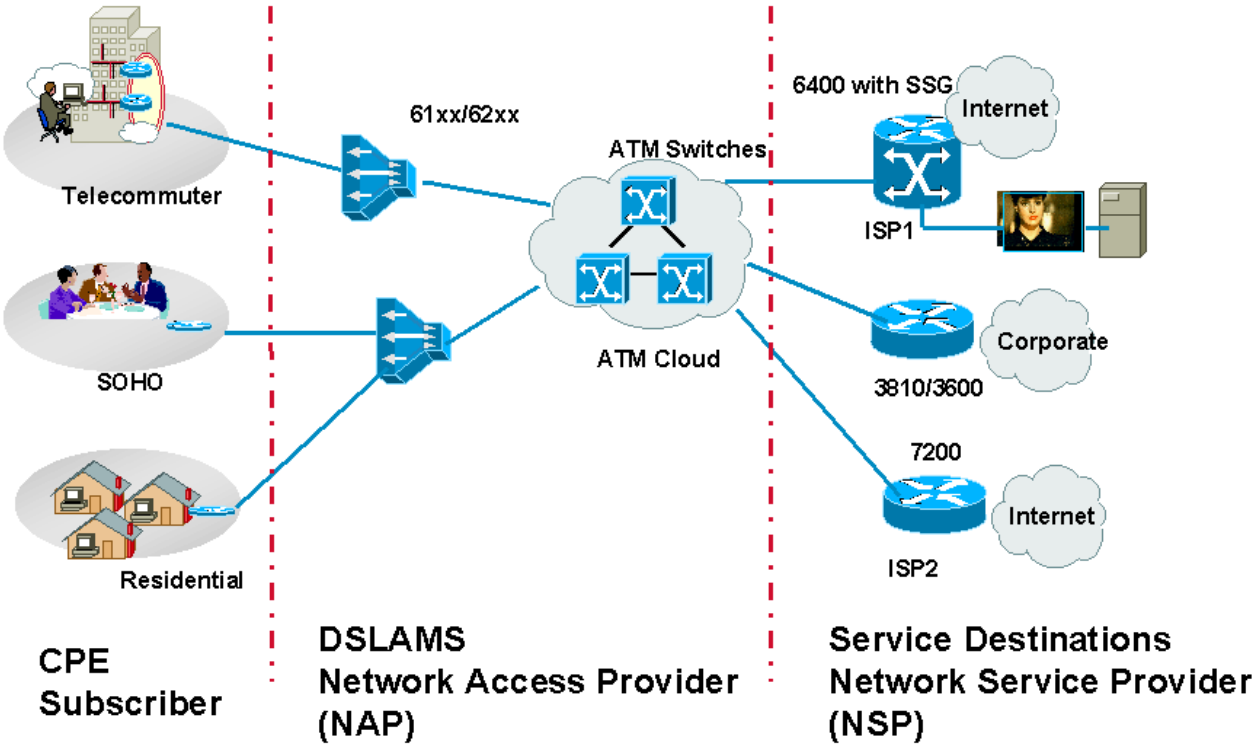
Considerazioni sull'implementazione

Prima di implementare l'architettura di bridging RFC1483, considerare le domande seguenti.

- Qual è il numero attuale e previsto di abbonati da soddisfare?
- Gli abbonati devono comunicare tra loro?
- Questi abbonati sono clienti residenziali con un solo utente? Servite clienti di piccoli uffici o uffici domestici (SOHO) che potrebbero avere una piccola LAN dietro CPE?
- Che cos'è la distribuzione e il provisioning di CPE, DSLAM (Digital Subscriber Line Access Multiplexer) e POP (Aggregation Post Office Protocol)?
- Il provider di accesso alla rete e il provider di servizi di rete sono la stessa entità? Il modello di business per il NAP prevede anche la vendita di servizi all'ingrosso quali l'accesso sicuro alle aziende e servizi a valore aggiunto quali voce e video?
- L'NSP desidera offrire funzionalità di selezione dei servizi?
- Come si possono ottenere la contabilità e la fatturazione? È per uso, larghezza di banda o per servizio?
- Il modello di business della società è quello di un operatore locale indipendente di cambio (ILEC), di un operatore di cambio locale competitivo (CLEC) o di un provider di servizi Internet (ISP)?
- Quali tipi di applicazioni intende offrire l'NSP all'utente finale?
- Che cos'è il volume del flusso di dati sia a monte che a valle?

Di seguito vengono descritte le caratteristiche dell'architettura di bridging RFC1483 per adattarla e adattarla a diversi modelli aziendali.

Architettura di rete



Considerazioni sulla progettazione

Come accennato in precedenza, l'architettura di bridging RFC1483 presenta alcuni problemi.

La funzione IOS Subscriber Bridging risolve alcuni di questi problemi. L'applicazione selettiva dei criteri degli utenti a un gruppo bridge controlla il flusso di ARP, pacchetti sconosciuti e altri elementi lungo ciascun loop ADSL. Ad esempio, impedendo la trasmissione degli ARP, un utente ostile non può individuare l'indirizzo IP di un altro utente.

Un'altra soluzione è quella di mettere tutti i sottoscrittori in una singola sottointerfaccia. Il normale comportamento di bridging non inoltra i frame alla porta su cui sono stati ricevuti. In sostanza, questo applica un tipo di subscriber bridging in cui tutti i pacchetti tra sottoscrittori sono filtrati. Tuttavia, questo approccio presenta i seguenti difetti:

- I criteri del sottoscrittore vengono applicati solo tra sottointerfacce. Per applicare i criteri sottoscrittore tra due utenti diversi, ogni utente deve trovarsi in un'interfaccia secondaria ATM diversa.
- Poiché viene appresa la mappatura degli indirizzi dal layer 2 al layer 3 (tramite ARP), gli utenti ostili possono ancora dirottare la connessione di altri utenti. A tale scopo, viene generato il traffico ARP con l'indirizzo IP di un altro utente e viene utilizzato un indirizzo MAC diverso.

Il secondo scenario è più grave per il vettore o l'ISP. In questo caso, qualsiasi utente può assegnare l'indirizzo errato a un PC o a un dispositivo Ethernet, ad esempio una stampante, e causare problemi di connessione per un altro utente. Tali errori o attacchi sono difficili da individuare e correggere perché il colpevole può essere rintracciato solo tracciando l'indirizzo MAC del colpevole.

Alcuni vettori cercano di risolvere questo problema separando gli utenti tra i gruppi di bridge e implementando il bridging del sottoscrittore tra le sottointerfacce. In questo caso, quando è richiesto il routing e il bridging integrati (IRB), a ciascun utente viene assegnato un gruppo di bridge e un'interfaccia virtuale (BVI) del gruppo di bridge univoci. Questo approccio utilizza due interfacce per ogni utente e può essere difficile da gestire.

Questi problemi vengono affrontati e risolti in qualche modo dalla funzionalità RBE (Routed Bridged Encapsulation) introdotta nel software Cisco IOS® versione 12.0(5)DC sul server Cisco 6400.

Considerando alcuni degli svantaggi del bridging, ci si potrebbe chiedere come mai l'architettura del bridging sarebbe mai stata implementata. La risposta è semplice. La maggior parte dei CPE ADSL installati sul campo sono in grado solo di inoltrare frame con bridging. In questi casi, l'NSP deve implementare il bridging.

Oggi i CPE possono eseguire il protocollo Point-to-Point su ATM (PPPoA), il bridging RFC1483 e il routing RFC1483. L'NSP determina se eseguire il bridging o il PPP. La decisione si basa sulle considerazioni relative all'implementazione menzionate in precedenza, oltre che sui pro e i contro di ogni architettura.

Anche con gli svantaggi dell'architettura di bridging, può essere adatta per un piccolo ISP (che potrebbe non essere il NAP) o un NAP/NSP che serve un numero inferiore di abbonati. In questi scenari, Protezione accesso alla rete in genere inoltra tutto il traffico degli utenti all'ISP/NSP, che

termina tali utenti. Protezione accesso alla rete può scegliere di fornire il traffico del sottoscrittore utilizzando ATM o Frame Relay come protocollo di livello 2.

I Protezione accesso alla rete che utilizzano DSLAM di generazione corrente possono solo trasportare il traffico dei sottoscrittori tramite ATM. In questo caso, l'ISP deve terminare i circuiti virtuali permanenti (PVC) ATM su un router.

Se l'ISP/NSP non dispone di un'interfaccia ATM, è possibile usare un'interfaccia seriale regolare con incapsulamento ATM Data Exchange Interface (DXI) (possibilmente su un dispositivo aggiuntivo) per accettare le PDU con bridging in ingresso.

In entrambi gli scenari, l'NSP/ISP potrebbe dover configurare l'IRB sul router (tranne quando si utilizza l'incapsulamento ATM DXI o nel caso del bridging trasparente). Oggi, la prassi più comune per terminare gli abbonati con bridging sul router NSP/ISP è implementare l'IRB (si prevede che i provider di servizi migreranno gradualmente alla RBE).

A causa di alcune delle limitazioni di cui sopra, l'NSP/ISP può scegliere di configurare gruppi di bridge distinti per ogni gruppo di sottoscrittori o di configurare tutti gli abbonati in un gruppo di bridge. In genere, è consigliabile configurare alcuni gruppi di bridge e quindi configurare tutti i sottoscrittori in interfacce multipoint separate. Come accennato in precedenza, gli abbonati con la stessa interfaccia multipunto potrebbero non essere in grado di comunicare tra loro. Se alcuni utenti devono comunicare, configurare tali sottoscrittori con interfacce diverse (possono ancora trovarsi nello stesso gruppo di bridge).

Per un ISP/NSP di piccole dimensioni, i router più comuni utilizzati per terminare gli abbonati con bridging sono Cisco 3810, Cisco 3600 e Cisco 7200. Per un ISP/NSP con una base di utenti ampia, è preferibile Cisco 6400. Prima di calcolare i requisiti di memoria per questi router, considerare gli stessi fattori di qualsiasi altro ambiente: numero di utenti, larghezza di banda e risorse router.

Punti chiave di questa architettura

Di seguito sono riportati i punti chiave dell'architettura.

CPE

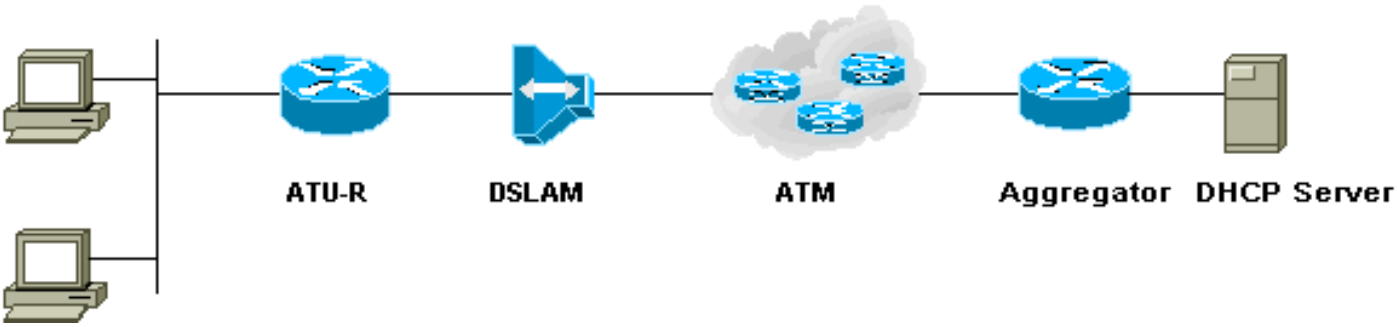
Cisco offre diversi CPE che operano con DSLAM Cisco e non Cisco. La configurazione di ciascuno di questi CPE è priva di problemi e non richiede alcun input da parte del sottoscrittore. Il requisito principale è che il CPE definisca un identificatore di percorso virtuale/VCI (Virtual Channel Identifier) ATM. Questo consente al CPE di allenarsi con il DSLAM e iniziare a trasmettere il traffico. Nella maggior parte dei casi, Protezione accesso alla rete sceglie di configurare lo stesso VPI/VCI per tutti i sottoscrittori. Protezione accesso alla rete esegue in genere il pre-provisioning del CPE prima di distribuirlo nella posizione del sottoscrittore.

Nell'architettura di bridging, la considerazione principale per il CPE e la relativa distribuzione è il modo in cui Protezione accesso alla rete gestirà il CPE dopo l'installazione sul campo. Questo problema è dovuto al fatto che il bridging non richiede un indirizzo IP per il CPE. Tuttavia, i CPE Cisco possono essere forniti con un indirizzo IP in modalità bridging. Protezione accesso alla rete può utilizzare questa funzionalità per eseguire una connessione Telnet a CPE per raccogliere statistiche o per agevolare la risoluzione dei problemi del sottoscrittore. Per consentire la gestione dei CPE tramite i DSLAM, è in corso l'aggiunta di una nuova funzionalità per gli elementi proxy.

In modalità bridging, se al CPE non è assegnato alcun indirizzo IP di gestione, l'operatore può gestire il CPE solo attraverso la porta di gestione del CPE. Se viene assegnato un indirizzo IP di gestione, l'operatore può utilizzare un browser HTTP (Hypertext Transfer Protocol) per gestire il dispositivo. Tuttavia, questa opzione non è generalmente disponibile.

Quando il CPE è in modalità bridging, la destinazione del servizio (che potrebbe essere l'NSP/ISP) deve fornire un indirizzo IP che verrà utilizzato come gateway predefinito per i PC dietro il CPE. Questi PC devono essere impostati sul gateway predefinito corretto. In caso contrario, anche se il modem è addestrato (ossia se il livello fisico è buono tra CPE e DSLAM), l'utente potrebbe non essere in grado di passare il traffico. Questo non è un problema se si utilizza il protocollo DHCP (Dynamic Host Configuration Protocol) per assegnare gli indirizzi DHCP del sottoscrittore, in quanto il server DHCP restituisce il router predefinito.

Gestione IP



Bridging RFC1483: Gestione IP

In un ambiente con bridging, gli indirizzi IP vengono allocati alle unità terminali da un server DHCP situato nella destinazione del servizio, generalmente nella rete NSP/ISP. Si tratta dell'approccio più comune e viene implementato dalla maggior parte degli NSP/ISP che utilizzano questo modello.

Un altro approccio consiste nel fornire indirizzi IP statici agli abbonati. In questo caso, viene allocata una subnet di indirizzi IP o un singolo indirizzo IP per sottoscrittore, a seconda dei requisiti del sottoscrittore. Ad esempio, gli abbonati che desiderano ospitare un server Web o un server di posta elettronica dovranno disporre di un set di indirizzi IP anziché di un singolo indirizzo IP. Il problema è che l'NSP/ISP deve fornire indirizzi IP pubblici che potrebbero esaurirsi rapidamente.

Alcuni NSP/ISP hanno fornito indirizzi IP privati ai propri abbonati. Quindi, eseguono Network Address Translation (NAT) sul router di destinazione del servizio.

Gli NSP/ISP che forniscono una subnet completa per un gruppo di bridge (con più di un sottoscrittore) devono sapere che un utente può assegnare l'indirizzo errato a un PC o a un dispositivo Ethernet, ad esempio una stampante, e causare problemi di connessione per un altro utente.

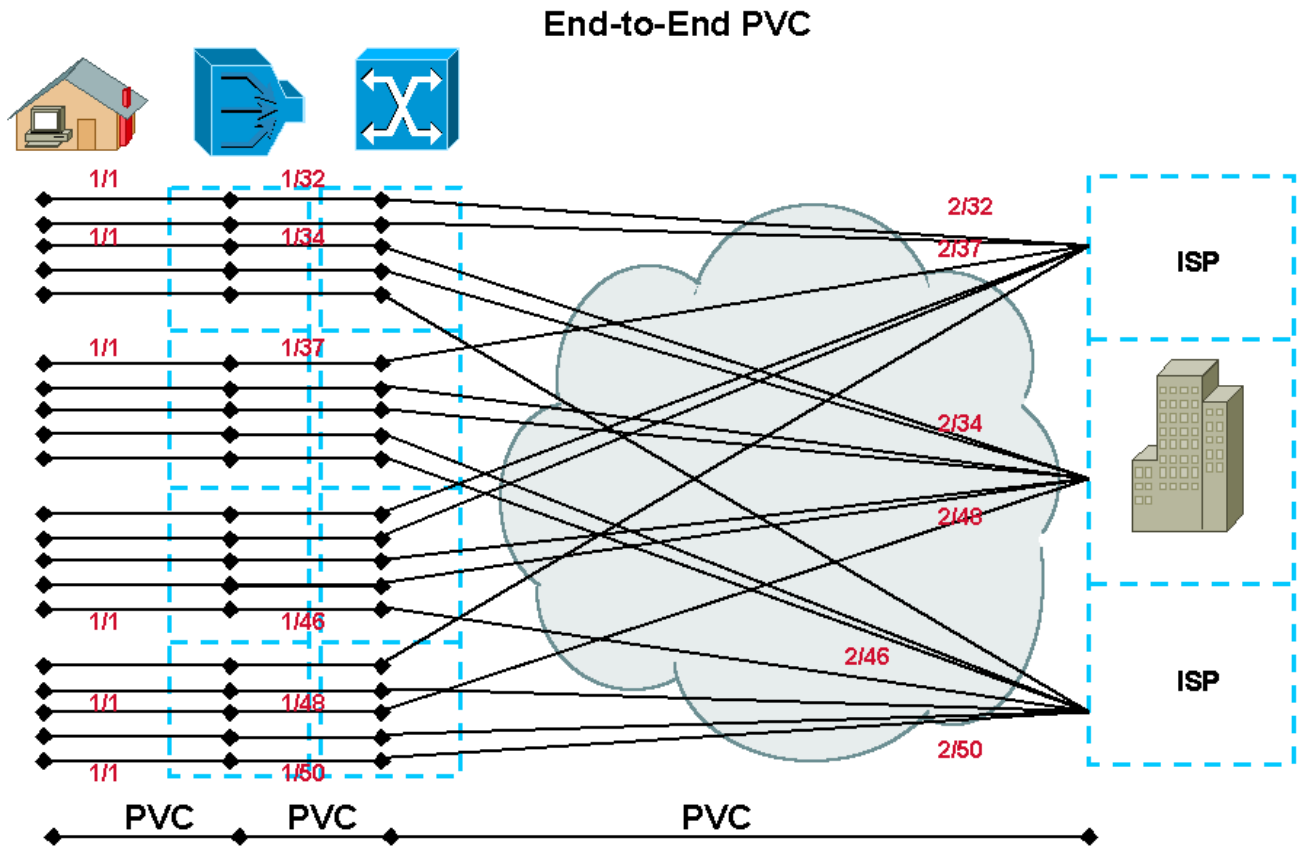
Èinoltre possibile per un NSP/ISP limitare il numero di PC che possono accedere contemporaneamente al servizio. A tale scopo, è necessario configurare il numero massimo di utenti sull'interfaccia Ethernet.

Tuttavia, questo metodo presenta il seguente difetto. Se tre PC sono configurati per utilizzare il servizio e uno degli abbonati aggiunge una stampante di rete (con il proprio indirizzo MAC)

durante un periodo di inattività di uno dei PC, l'indirizzo MAC del PC scompare dalla voce ARP del CPE.

Se la stampante diventa attiva mentre il PC è inattivo, nella voce ARP verrà immesso l'indirizzo MAC della stampante. Quando un utente decide di utilizzare questo PC per accedere a Internet, non sarà disponibile perché CPE ha già consentito tre voci MAC. Si può utilizzare la strategia di limitare gli utenti sul CPE, ma si deve fare attenzione nel fissare i numeri.

Come raggiungere una destinazione di servizio



Bridging RFC1483: PVC completo

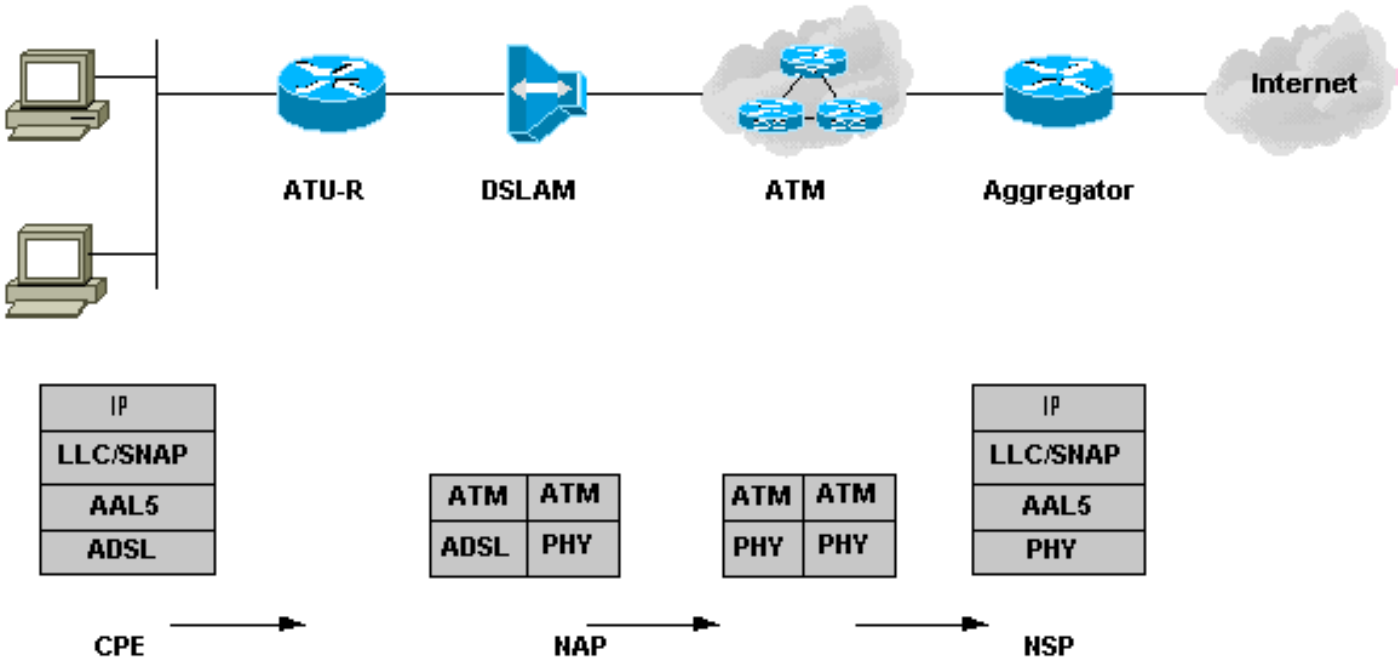
In un'architettura PVC end-to-end con bridging, la destinazione del servizio viene raggiunta creando i PVC tra ciascun hop. Tuttavia, la gestione di questi PVC può essere problematica per NAP/NSP. Inoltre, il numero di PVC che possono essere definiti tramite il cloud ATM è limitato. Questa limitazione interessa molti dei NAP/NSP che adottano un modello di PVC end-to-end. Per ciascun sottoscrittore vi sarà un set fisso e univoco di VPI/VCI lungo l'intero percorso. I circuiti virtuali commutati (SVC) aiutano a risolvere alcuni di questi problemi e molti provider di accesso stanno migrando alle reti principali IP per risolvere il problema dell'esaurimento delle reti VC.

L'NSP/ISP ha anche la possibilità di utilizzare la funzionalità Cisco Service Selection Gateway (SSG) per fornire servizi diversi agli utenti.

In questa architettura l'accesso protetto a un gateway aziendale viene ottenuto terminando il PVC

del traffico degli utenti direttamente nel router aziendale al layer 2. Le architetture basate su PVC sono intrinsecamente sicure quando si condividono i dati con altre destinazioni di servizio.

Descrizione operativa



Bridging RFC1483: Descrizione operativa

Cisco 6xx CPE utilizza per impostazione predefinita la modalità di routing. Pertanto, quando è configurato per la modalità bridging e installato presso la postazione dell'utente con gli splitter/microfiltri necessari, si allena automaticamente all'accensione. Quando il CPE si prepara, indica che il livello fisico tra il CPE e il DSLAM è corretto. A seconda della configurazione dell'indirizzo IP della stazione terminale (ossia se viene assegnato tramite un server DHCP o se si tratta di un indirizzo IP statico con informazioni sul gateway predefinito), può comunicare con la destinazione del servizio.

Di seguito è riportata una descrizione del flusso dei pacchetti.

I dati dell'utente vengono incapsulati in IEEE 802.3 dal PC e immessi nel CPE Cisco 6xx. Viene quindi incapsulato in un'intestazione LLC/SNAP (Logical Link Control/Subnetwork Access Protocol), che a sua volta viene incapsulata nel layer di adattamento ATM 5 (AAL5) e consegnata al layer ATM.

Le celle ATM vengono quindi modulate dalla tecnologia di trasmissione ADSL, dalla modulazione Carrierless Amplitude and Phase (CAP) o dalla tecnologia DMT (Discrete Multi-Tone) e inviate tramite cavo al DSLAM. Nel DSLAM, questi segnali modulati vengono ricevuti per la prima volta dallo splitter POTS, che controlla se la frequenza del segnale è inferiore o superiore a 4 kHz. Dopo aver identificato i segnali come superiori a 4 kHz, li passa all'unità di trasmissione ADSL - ufficio centrale (ATU-C) nella DSLAM.

L'ATU-C demodula il segnale e recupera le celle ATM, che vengono quindi passate alla scheda di interfaccia di rete (NIC) nel dispositivo multiplexing (MUX). La scheda NIC analizza le informazioni VPI/VCI del lato utente nell'intestazione ATM e decide di passare a un altro VPI/VCI che verrà inoltrato al router di destinazione del servizio. Dopo aver ricevuto le celle su un'interfaccia ATM specifica, il router di destinazione del servizio le ricompone, controlla il livello superiore e passa le

informazioni all'interfaccia BVI. L'interfaccia BVI analizza le informazioni del layer 3 e decide dove consegnare il pacchetto.

Conclusioni

Il modello di bridging RFC1483 è più adatto per gli ISP di piccole dimensioni o per l'accesso aziendale, per i quali la scalabilità non diventa un problema. Poiché è molto semplice da comprendere e implementare, è diventata la scelta di molti ISP più piccoli. Tuttavia, a causa di alcuni problemi di sicurezza e scalabilità, l'architettura ponte sta perdendo la sua popolarità. Gli NSP/ISP optano per la tecnologia RBE o si muovono verso PPPoA o PPPoE, che sono altamente scalabili e molto sicuri, ma più complessi e difficili da implementare.

Informazioni correlate

- Supporto tecnico DSL
- Supporto tecnico – Cisco Systems