Architettura di base PPPoE per Cisco 6400 UAC

Sommario

Introduzione

Questo documento descrive un'architettura ADSL (Asymmetric Digital Subscriber Line) end-to-end che utilizza il protocollo PPPoE (Point-to-Point over Ethernet).

Nell'ambiente attuale delle tecnologie di accesso è consigliabile collegare più host in un sito remoto tramite lo stesso dispositivo di accesso locale del cliente. È inoltre essenziale fornire funzionalità di controllo dell'accesso e di fatturazione simili ai servizi di accesso remoto che utilizzano il protocollo PPP (Point-to-Point Protocol). In molte tecnologie di accesso, il metodo più conveniente per collegare più host al dispositivo di accesso alla sede del cliente è tramite Ethernet. Inoltre, è consigliabile mantenere il costo di questo dispositivo il più basso possibile e i requisiti di configurazione meno o nessuno.

Quando i clienti implementano l'ADSL, devono supportare l'autenticazione e l'autorizzazione di tipo PPP su un'ampia base installata di apparecchiature CPE (Customer Premise) di bridging preesistenti. PPPoE consente di connettere una rete di host tramite un semplice dispositivo di accesso di bridging a un concentratore di accesso remoto o di aggregazione. Con questo modello, ciascun host utilizza il proprio stack PPP. In questo modo, l'utente dispone di un'interfaccia utente familiare. È possibile accedere al controllo, alla fatturazione e al tipo di servizio per singolo utente anziché per singolo sito.

Presupposto

L'architettura di base presuppone che siano stati forniti gli elementi seguenti:

- Accesso a Internet ad alta velocità e accesso aziendale all'utente finale che utilizza PPPoE.
- ATM è la tecnologia backbone principale, implementata da Cisco 6400 Universal Access

Concentrator (UAC).

Questa restrizione all'implementazione del progetto può limitare l'uso di questa architettura su altre piattaforme, ma PPPoE è in continua evoluzione. Per sfruttare le funzionalità nuove e aggiornate, leggere le note sulla versione più recenti dei prodotti correlati.

Questo documento si basa sulle implementazioni correnti e sui test interni che usano Cisco 6400 UAC. Questo documento è una continuazione del documento PPPoA Baseline Architecture e vi fa spesso riferimento. Si presume che l'utente abbia letto il white paper relativo all'architettura di base PPPoA e abbia compreso i concetti fondamentali di PPP e che abbia letto le note sulla versione per l'ultima versione del software.

Tecnologie in breve

Come specificato nella RFC 2516, il protocollo PPPoE prevede due fasi distinte: una fase di individuazione e una fase di sessione PPP. Quando un host avvia una sessione PPPoE, deve prima eseguire il rilevamento per identificare il server in grado di soddisfare la richiesta del client. In secondo luogo, deve identificare l'indirizzo MAC Ethernet del peer e stabilire un ID sessione PPPoE. Mentre PPP definisce una relazione peer-to-peer, l'individuazione è intrinsecamente una relazione client-server.

Nel processo di rilevamento, un host (il client) individua uno o più concentratori di accesso (i server) e ne seleziona uno. Al termine del rilevamento, sia l'host che il concentratore di accesso selezionato dispongono delle informazioni necessarie per creare la connessione point-to-point su Ethernet. Dopo aver stabilito una sessione PPP, sia l'host che il concentratore degli accessi devono allocare le risorse per un'interfaccia virtuale PPP (probabilmente non è così per tutte le implementazioni). Per ulteriori dettagli sulla specifica PPPoE, fare riferimento alla RFC 2516.

Vantaggi e svantaggi dell'architettura PPPoE

L'architettura PPPoE eredita la maggior parte dei vantaggi del protocollo PPP utilizzato nel modello di connessione remota e nell'architettura PPPoA. In queste sezioni vengono elencati alcuni vantaggi e svantaggi principali del PPPoE e le differenze rispetto al PPPoA.

Vantaggi

Di seguito sono riportati alcuni vantaggi principali del PPPoE e le differenze rispetto al PPPoA:

- Autenticazione per sessione basata su PAP (Password Authentication Protocol) o CHAP (Challenge Handshake Authentication Protocol). Questo è il vantaggio principale del PPPoE, in quanto l'autenticazione consente di superare il problema relativo alla 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. Il fornitore di servizi può anche richiedere un costo di accesso minimo.
- Èpossibile utilizzare PPPoE sulle installazioni CPE correnti che non possono essere aggiornate a PPP o che non hanno la capacità di eseguire PPPoA, che estende la sessione PPP sulla LAN Ethernet con bridging al PC.
- Il protocollo PPPoE mantiene la sessione point-to-point utilizzata dai provider di servizi Internet (ISP) nel modello di connessione remota corrente. Il PPPoE è l'unico protocollo in

grado di eseguire operazioni point-to-point su Ethernet senza la necessità di uno stack IP intermedio.
- Il provider di accesso alla rete (NAP) o il provider di servizi di rete (NSP) può fornire accesso sicuro a un gateway aziendale senza la gestione di PVC (Permanent Virtual Circuit) end-to-end e senza l'utilizzo del routing di layer 3 e/o di tunnel Layer 2 Tunneling Protocol (L2TP). Questo rende scalabile il modello di business della vendita di servizi all'ingrosso e di reti private virtuali (VPN).
- Il protocollo PPPoE può fornire a un host (PC) l'accesso a più destinazioni alla volta. È possibile avere più sessioni PPPoE per PVC.
- L'NSP può sovrascrivere la distribuzione dei timeout di inattività e di sessione con l'aiuto di un server RADIUS (Remote Authentication Dial-In User Service) standard del settore per ogni sottoscrittore.
- Èpossibile utilizzare il protocollo PPP con la funzionalità Service Selection Gateway (SSG).

Svantaggi

Di seguito sono riportati alcuni svantaggi principali del PPPoE e le differenze rispetto al PPPoA:

- Ènecessario installare il software client PPPoE su tutti gli host (PC) che si connettono al segmento Ethernet. Ciò significa che il provider di accesso deve mantenere il CPE e il software client sul PC.
- Poiché l'implementazione PPPoE utilizza il bridging RFC 1483, è soggetta a tempeste di trasmissione e a possibili attacchi di negazione del servizio.

Considerazioni sull'implementazione dell'architettura PPPoE

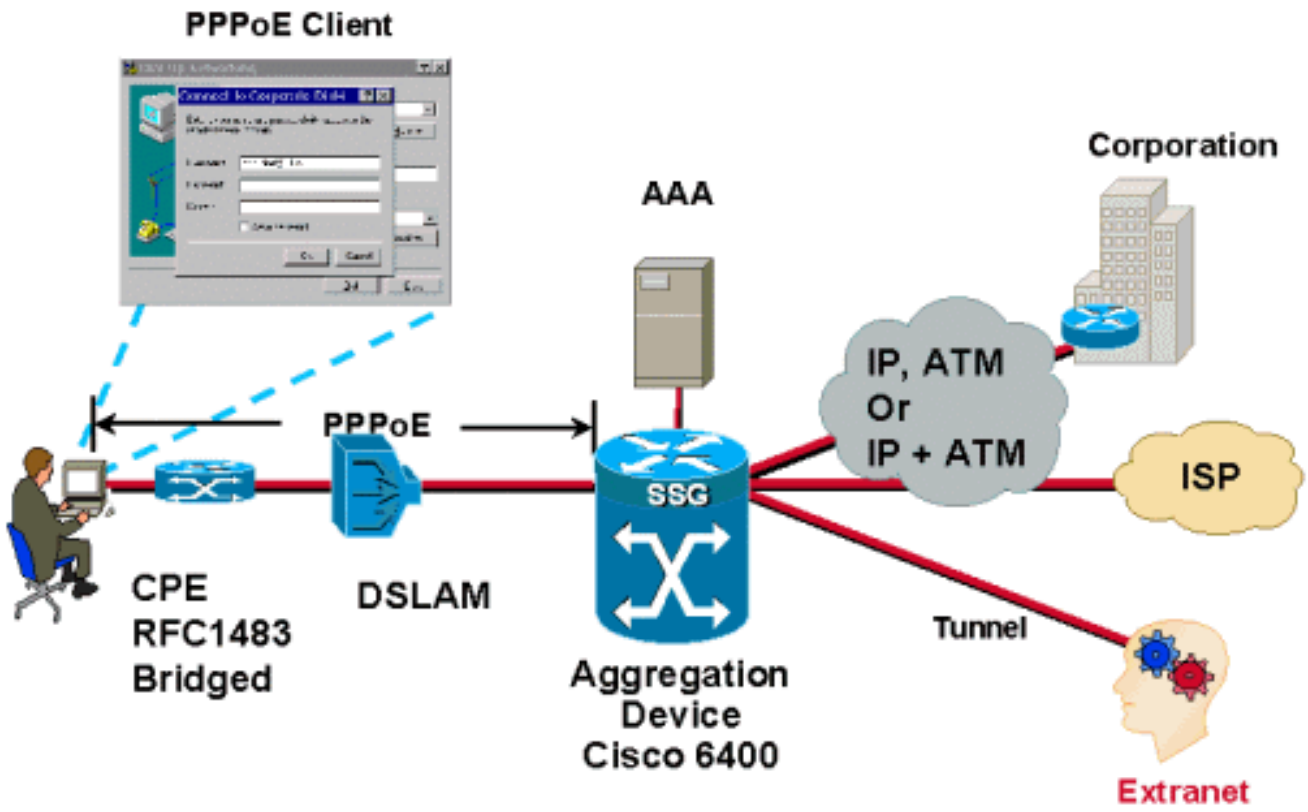
Di seguito sono riportati alcuni punti chiave da considerare prima di implementare questo tipo di architettura.

- Numero di sottoscrittori supportato. Il numero di server PPPoE richiesto dipende dal numero di sessioni.
- Se le sessioni PPP vengono terminate sul router di aggregazione del provider di servizi o inoltrate ad altri gateway aziendali o ISP.
- Se l'indirizzo IP è fornito dal provider di servizi o dalla destinazione finale del servizio.
- Nel caso di più utenti, indicare se tutti gli utenti devono raggiungere la stessa destinazione finale o lo stesso servizio oppure se hanno tutti destinazioni di servizio diverse. Gli abbonati finali richiedono l'accesso simultaneo a più destinazioni?
- Il software client PPPoE utilizzato dal provider di accesso e se il software è stato testato, il sistema operativo utilizzato dall'host e se tale sistema operativo può prendere una decisione di routing intelligente.
- Modalità di fatturazione degli abbonati da parte del provider di servizi in base a una tariffa fissa, all'utilizzo per sessione o ai servizi utilizzati.
- Installazione e fornitura di CPE, DSLAM e punti di presenza di aggregazione (POP).
- Modello di business per Protezione accesso alla rete. Il modello include anche la vendita di servizi all'ingrosso come l'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 offre all'utente finale.
- Volume previsto a monte e a valle del flusso di dati. Considerare il throughput NRP, l'ingegneria del traffico e qualsiasi problema QoS.

In questo documento viene descritto come l'architettura PPPoE si adatta e si adatta a diversi modelli aziendali per i provider di servizi e come i provider possono trarre vantaggio dall'utilizzo di questa architettura.

Architettura di rete



Considerazioni sulla progettazione dell'architettura PPPoE

In questa sezione vengono illustrati i problemi specifici dell'architettura PPPoE.

Prima di implementare un'architettura, è essenziale comprendere il modello di business del provider di servizi e i servizi offerti. È necessario conoscere il software client utilizzato sul PC. Il software più comune è quello di RouterWare. Poiché il software client è installato su un PC, il tecnico del provider di servizi deve avere una buona conoscenza di tale PC e del relativo sistema operativo.

Come specificato nella RFC 2516, l'opzione MRU (Maximum Receive Unit) non deve essere negoziata su una dimensione maggiore di 1492. Ethernet ha una dimensione massima del payload di 1500 ottetti. L'intestazione PPPoE è 6 ottetti e l'ID del protocollo PPP è 2 ottetti, quindi l'unità massima di trasmissione (MTU) del PPP non deve essere superiore a 1492. A tale scopo, è

necessario configurare l'MTU IP 1492 per le interfacce del modello virtuale PPPoE.

Per impostazione predefinita, quando si configura un gruppo VPDN PPPoE non viene preclonata alcuna interfaccia di accesso virtuale. Gli utenti possono modificare il numero massimo di interfacce di accesso virtuale preclonate usando il comando globale **pre-clonazione <numero> del modello virtuale**.

Per proteggere il router dagli attacchi di negazione del servizio, il protocollo PPPoE (per impostazione predefinita) consente di originare una sola sessione da un indirizzo MAC su un server VC. Per modificare le impostazioni predefinite, gli utenti possono usare i comandi **pppoe session-limit per-mac** e **pppoe session-limit per-vc**.

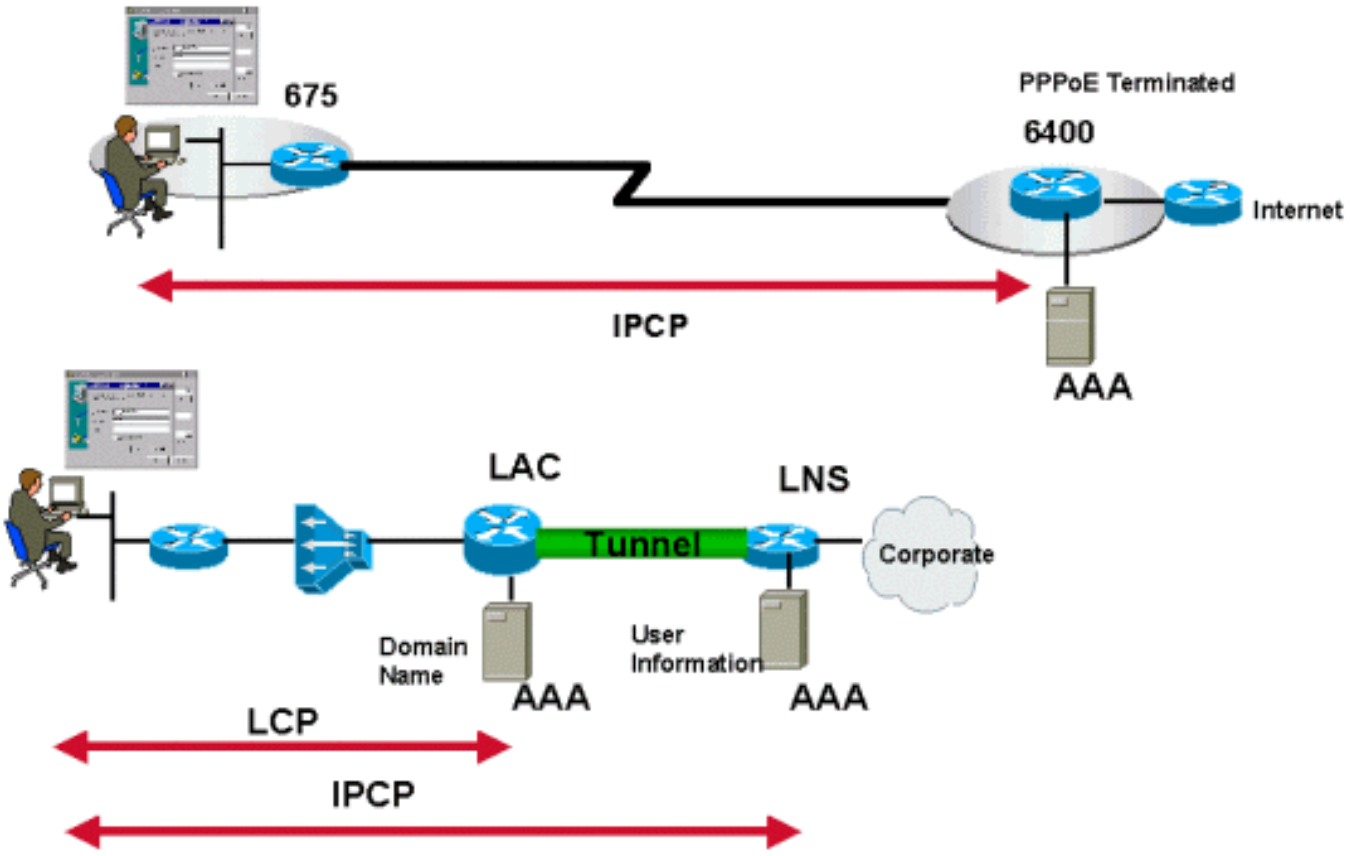
Il processo di contabilità, autorizzazione e autenticazione è lo stesso di PPPoA. L'unica differenza è che attualmente l'autenticazione basata su VPI/VCI, disponibile per il PPPoA e non per il PPPoE, può utilizzare le architetture L2TP e SSG per i servizi all'ingrosso.

Punti chiave dell'architettura PPPoE

CPE

Il CPE è configurato per il bridging RFC 1483 puro. Ogni CPE utilizza solo una coppia VPI/VCI e tutte le sessioni PPPoE avviate dagli host dietro questo CPE vengono trasferite in questo singolo VC.

Gestione IP



L'allocazione degli indirizzi IP per il singolo host che esegue il client PPPoE si basa sullo stesso

principio del protocollo PPP in modalità di composizione, ossia la negoziazione IPCP. L'origine dell'indirizzo IP dipende dal tipo di servizio acquistato dal sottoscrittore e dal punto in cui vengono terminate le sessioni PPP. Il protocollo PPPoE utilizza la funzionalità di connessione remota di Microsoft Windows e l'indirizzo IP assegnato viene visualizzato nella scheda PPP.

L'assegnazione dell'indirizzo IP può provenire dal concentratore di accesso che termina le sessioni PPPoE o, nel caso di L2TP, dai gateway di casa. L'indirizzo IP viene assegnato a ciascuna sessione PPPoE.

Il CPE non è in grado di eseguire il protocollo NAT/DHCP (Network Address Translation/Dynamic Host Configuration Protocol) perché è un bridge a cui non è allocato alcun indirizzo IP.

Come si raggiunge la destinazione del servizio

Per raggiungere la destinazione del servizio, procedere come segue:

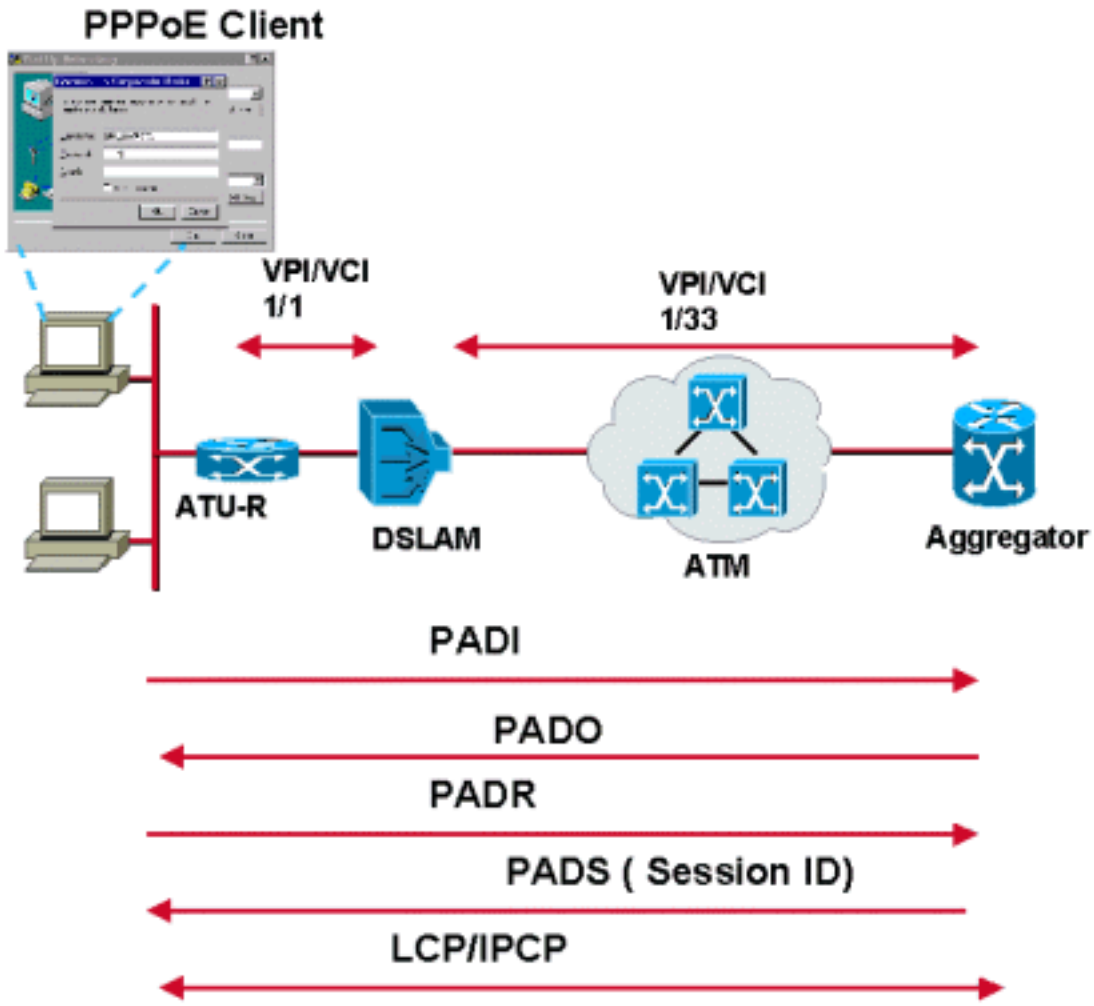
- Chiusura delle sessioni PPP presso il provider di servizi
- Tunneling L2TP
- Con l'uso di SSG

Le spiegazioni dettagliate di queste architetture sono illustrate in documenti separati.

Descrizione operativa di PPPoE

Questa versione del software client PPPoE supporta le fasi di individuazione e sessione descritte nella RFC 2516. Ci sono quattro passaggi per la fase di scoperta. Al termine, entrambi i peer conoscono l'ID sessione PPPoE e l'indirizzo Ethernet del peer, che insieme definiscono in modo univoco la sessione PPPoE. Di seguito sono riportati i passaggi:

1. L'host invia un pacchetto di avvio.L'host invia il pacchetto PADI (Active Discovery Initiation) PPPoE con destination_addr impostato sull'indirizzo di broadcast. Il PADI è costituito da un tag che indica il tipo di servizio richiesto.
2. Uno o più concentratori di accesso inviano pacchetti di offerta.Quando il concentratore di accesso o il router riceve un PADI che può servire, invia un pacchetto PADO (PPPoE active discovery offer). destination_addr è l'indirizzo unicast dell'host che ha inviato il PADI. Se il concentratore di accesso non può servire il PADI, non deve rispondere con un PADO. Poiché è stato trasmesso il PADI, l'host può ricevere più di un



PADO.

3. L'host invia un pacchetto di richiesta di sessione unicast.L'host cerca i pacchetti PADO ricevuti e ne sceglie uno. La scelta si basa sui servizi offerti da ciascun concentratore di accesso. L'host invia quindi un pacchetto PADR al concentratore di accesso scelto. Il campo destination_addr viene impostato sull'indirizzo Ethernet unicast del concentratore di accesso o del router che invia il PADO.
4. Il concentratore di accessi selezionato invia un pacchetto di conferma.Quando il concentratore di accesso riceve un pacchetto PADR, si prepara a iniziare una sessione PPP. Genera un ID sessione univoco per la sessione PPPoE e risponde all'host con un pacchetto PPPoE (Active Discovery Session-CONFIRMation) di conferma della sessione PPPoE. Il campo destination_addr corrisponde all'indirizzo Ethernet unicast dell'host che invia il PADR.

Una volta avviata la sessione PPPoE, i dati PPP vengono inviati come in qualsiasi altro incapsulamento PPP. Tutti i pacchetti Ethernet sono unicast.

Un pacchetto PPPoE active discovery terminate (PADT) può essere inviato dall'host o dal concentratore degli accessi in qualsiasi momento dopo la creazione di una sessione, a indicare che una sessione PPPoE è stata terminata.

Per una spiegazione più dettagliata, fare riferimento alla RFC 2516.

Conclusioni

Per l'ADSL, il protocollo PPPoE è seconda solo a PPPoA.

Riferimenti

- RFC 2516 - Un metodo per trasmettere il protocollo PPP over Ethernet (PPPoE)
- RFC 1483 - Incapsulamento multiprotocollo su layer 5 di adattamento ATM
- RFC 2364 - Point-to-point su AAL5

Informazioni correlate

- Architettura di base PPPoA
- Supporto tecnico DSL
- Supporto tecnico – Cisco Systems