

# PPPoA基線體系結構

## 目錄

[簡介](#)

[假設](#)

[技術簡介](#)

[PPPoA體系結構的優缺點](#)

[優勢](#)

[缺點](#)

[PPPoA架構的實施注意事項](#)

[典型的PPPoA網路架構](#)

[PPPoA架構的設計注意事項](#)

[PPPoA架構要點](#)

[IP管理](#)

[如何到達服務目的地](#)

[PPPoA架構的操作說明](#)

[結論](#)

[相關資訊](#)

## 簡介

本檔案介紹使用非同步傳輸模式(PPPoA)上的點對點通訊協定的端到端非對稱數位使用者線路(ADSL)架構。雖然大多數部署都基於橋接架構，但PPPoA正在獲得極高的普及度，並將在未來的ADSL部署中佔更大的比例。

## 假設

基線架構假設需要使用PPPoA作為核心骨幹網為終端使用者提供高速網際網路接入和企業訪問。我們將討論基於私有虛擬通道(PVC)的此體系結構，當前部署中經常使用這種方法。使用交換虛擬電路(SVC)的架構將在另一篇論文中討論。

本文檔基於現有部署以及內部架構測試。

本文的編寫假設前提是讀者瞭解並熟悉網路訪問提供商(NAP)的設計注意事項，如[RFC1483橋接基線架構白皮書](#)中所述。

## 技術簡介

點對點通訊協定(PPP)(RFC 1331)提供了一種透過點對點連線封裝較高層通訊協定的標準方法。它使用16位協定識別符號擴展了高級資料鏈路控制(HDLC)資料包結構，該協定識別符號包含有關資料包內容的資訊。

資料包包含三種型別的資訊：

- 鏈路控制協定(LCP) — 協商鏈路引數、資料包大小或身份驗證型別
- 網路控制通訊協定(NCP) — 包含有關更高層通訊協定 ( 包括IP和IPX ) 及其控制通訊協定 ( 適用於IP的IPCP ) 的資訊
- 包含資料的資料幀

使用ATM的PPP適配第5層(AAL5)(RFC 2364)使用AAL5作為框架協定，該協定支援PVC和SVC。PPPoA主要作為ADSL的一部分實現。它依賴於RFC1483，在邏輯鏈路控制 — 子網訪問協定(LLC-SNAP)或VC-Mux模式下運行。使用者駐地裝置(CPE)裝置基於此RFC封裝PPP會話，以便通過ADSL環路和數字使用者線接入複用器(DSLAM)進行傳輸。

## PPPoA體系結構的優缺點

PPPoA架構繼承了撥號模式中使用的PPP的大部分優勢。下面列出了一些要點。

### 優勢

- 基於口令驗證協定(PAP)或質詢握手驗證協定(CHAP)的每會話身份驗證。這是PPPoA的最大優勢，因為身份驗證克服了橋接架構中的安全漏洞。
- 每個會話計費(Per session accounting)是可能的，它允許服務提供商根據會話時間為提供的各種服務對使用者計費。每會話記賬使服務提供商能夠以最低的收費提供最低的接入級別，然後對使用者使用的附加服務收費。
- CPE的IP地址保留。這允許服務提供商僅為CPE分配一個IP地址，並將CPE配置為網路地址轉換(NAT)。一個CPE後面的所有使用者都可以使用一個IP地址到達不同的目的地。在節省IP地址的同時，減少了每個單獨使用者的網路接入提供商/網路服務提供商(NAP/NSP)的IP管理開銷。此外，服務提供商可以提供IP地址的小型子網，以克服埠地址轉換(PAT)和NAT的限制。
- NAP/NSP提供對公司網關的安全訪問，而無需管理端到端PVC並使用第3層路由或第2層轉發/第2層隧道協定(L2F/L2TP)隧道。因此，它們可以擴展其銷售批發服務的業務模式。
- 排除單個使用者的故障。NSP可以基於活動的PPP會話輕鬆確定哪些使用者是開啟還是關閉的，而不是像橋接架構那樣排除整個組的故障。
- NSP可以使用行業標準遠端身份驗證撥入使用者服務(RADIUS)伺服器為每個使用者部署空間和會話超時，從而超額訂閱。
- 高度可擴展，因為我們可以終止聚合路由器上非常多的PPP會話。可使用外部RADIUS伺服器為每個使用者處理驗證、授權和計量。
- 最佳使用服務選取閘道(SSG)上的功能。

### 缺點

- 在一個虛擬通道(VC)上每個CPE只有一個會話。由於使用者名稱和密碼是在CPE上配置的，因此該特定VC的CPE後面的所有使用者只能訪問一組服務。使用者不能選擇不同的服務集，儘管可以使用多個VC並在不同的VC上建立不同的PPP會話。
- CPE設定的複雜性增加。服務提供商的幫助台人員需要更博學。由於使用者名稱和密碼是在CPE上配置的，因此使用者或CPE供應商需要更改設定。使用多個VC會增加配置複雜性。但是，這可以通過尚未發佈的自動配置功能來解決。
- 服務提供商需要維護所有訂戶的使用者名稱和密碼資料庫。如果使用隧道或代理服務，則身份驗證可以基於域名完成，使用者身份驗證在公司網關完成。這將減小服務提供商必須維護的資料庫大小。

- 如果為CPE提供單個IP地址並實施NAT/PAT，則某些將IP資訊嵌入負載中的應用程式（如IPTV）將無法工作。此外，如果使用IP子網功能，也必須為CPE保留IP地址。

## PPPoA架構的實施注意事項

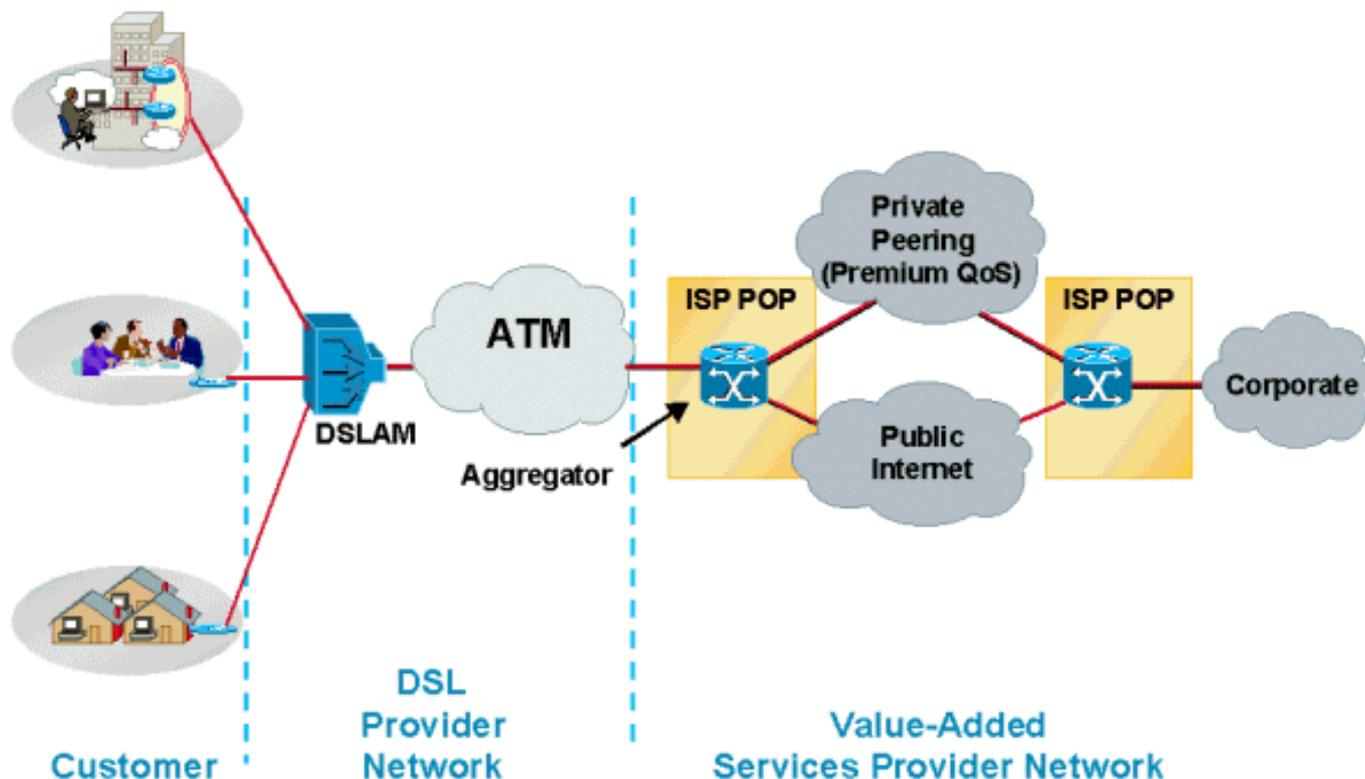
實施PPPoA架構之前需要考慮的要點包括：

- 當前和將來要服務的訂閱者數量，因為這影響所需的PPP會話數量。
- PPP會話是在服務提供商的匯聚路由器上終止，還是轉發到其他企業網關或Internet服務提供商(ISP)。
- 服務提供商還是最終服務目的地向使用者的CPE提供IP地址。
- 提供的IP地址是合法的公有地址還是私有地址。CPE將要執行NAT/PAT還是將在終端目標執行NAT？
- 終端使用者、住宅使用者、小型辦公室家庭辦公室(SOHO)客戶和遠端工作者的簡檔。
- 在多使用者的情況下，無論所有使用者都需要到達同一個最終目標或服務，還是他們都擁有不同的服務目標。
- 服務提供商是否提供語音或影片等增值服務？服務提供商是否要求所有訂戶在到達最終目的地之前先訪問特定網路？當使用者使用SSG時，他們會使用直通服務、PPP終止聚合(PTA)、中介裝置還是代理？
- 服務提供商如何根據固定費率、每個會話的使用情況或使用的服務對使用者計費。
- 部署和調配CPE、DSLAM和匯聚線上點(POP)。
- NAP的業務模式。這一模式是否還包括銷售批發服務（如安全的企業訪問）和增值服務（如語音和影片）？NAP和NSP是否屬於同一個實體？
- 公司的業務模式。它是否可與獨立本地交換運營商(ILEC)、競爭性本地交換運營商(CLEC)或ISP相比？
- NSP將提供給終端使用者的應用型別。
- 預期的上游和下游資料流量。

牢記這些要點，我們將討論PPPoA架構如何適合和擴展為服務提供商的不同業務模式，以及提供商如何使用此架構獲益。

## 典型的PPPoA網路架構

下圖顯示了典型的PPPoA網路體系結構。使用CPE的客戶通過Cisco DSLAM連線到服務提供商的網路，DSLAM使用ATM連線到Cisco 6400聚合器。



## PPPoA架構的設計注意事項

在本文檔的「實施注意事項」部分中，PPPoA架構可以根據服務提供商的業務模式使用不同的方案進行部署。在本節中，我們將討論服務提供商在部署解決方案之前必須牢記的不同可能性和注意事項。

在部署PPPoA架構和此架構的特定解決方案之前，必須瞭解服務提供商的業務模式。考慮服務提供商將提供的服務。服務提供商會向其終端使用者提供諸如高速網際網路接入之類的服務嗎？還是會向不同的ISP銷售批發服務，並向這些使用者提供增值服務？服務提供商會提供所有這些服務嗎？

在NSP和NAP相同的環境中高速訪問Internet時，使用者的PPP會話必須在部署的聚合路由器中終止。在這種情況下，服務提供商需要考慮在單個路由器聚合裝置上可終止多少個PPP會話、如何對使用者進行身份驗證、如何執行記帳，以及終止使用者會話後到網際網路的路徑。根據PPP會話和使用者的數量，匯聚路由器可能是Cisco 6400或Cisco 7200。目前，配備7個節點路由處理器(NRP)的Cisco 6400最多可以終止14,000個PPP會話。Cisco 7200僅限於2,000個PPP會話。這些數字會隨著新版本而改變。請檢視版本說明和產品文檔，瞭解每台聚合路由器可以支援的會話的確切數量。

在這些場景中，最好使用行業標準RADIUS伺服器來處理使用者身份驗證和記帳，該伺服器可以根據正在使用的使用者名稱或虛擬路徑識別符號/虛擬通道識別符號(VPI/VCI)對使用者進行身份驗證。

對於高速網際網路接入，NSP通常向客戶收取固定費用。大多數當前部署都以這種方式實施。當NSP和NAP是同一實體時，客戶按固定費率收費，而網際網路訪問則按另一固定費率收費。當服務提供商開始提供增值服務時，此模式將發生變化。服務提供商可以根據服務型別和服務的使用期限向客戶收費。客戶使用開放最短路徑優先(OSPF)或增強型內部網關路由協定(EIGRP)等路由協定，通過匯聚路由器連線到網際網路，連線到可能運行邊界網關協定(BGP)的邊緣路由器。

服務提供商用於提供高速Internet訪問的另一個選項是使用L2TP/L2F隧道將傳入的PPP會話從使用者轉發到單獨的ISP。使用L2x通道時，應特別考慮如何到達通道目的地。可用選項包括運行某些路

由協定或在匯聚路由器中提供靜態路由。使用L2TP或L2F隧道時的限制如下：(一)隧道數量以及隧道中能夠支援的會話數量；(2)使用的路由協定與第三方ISP不相容，這可能需要使用靜態路由。

如果服務提供商為不同ISP或公司網關向終端使用者提供服務，則他們可能需要在匯聚路由器上實施SSG功能。這允許使用者使用基於Web的服務選擇來選擇不同的服務目標。服務提供商可以將所有目的地為ISP的會話合併到單個PVC中以進行傳輸，從而將使用者PPP會話轉發到其選定的目標；或者，如果服務提供商提供多個服務級別，則可以在核心層建立多個PVC。

在批發服務模型中，服務提供商可能不使用SSG功能。在此模型中，服務提供商將所有PPP會話擴展到家庭網關。家庭網關向終端使用者提供IP地址並對終端使用者進行身份驗證。

在這些場景中，主要考慮事項是服務提供商如何為不同的服務提供不同的服務品質(QoS)，以及他們如何計算頻寬分配。目前，大多數服務提供商部署此架構的方式在不同的PVC上提供不同的QoS。核心層可能有單獨的PVC，用於住宅和企業客戶。使用不同的PVC允許服務提供商為不同的服務指定不同的QoS。這樣，QoS可以位於單獨的PVC上或位於第3層。

在第3層應用QoS需要服務提供商知道最終目的地，這可能是一個限制因素。但是，如果與第2層QoS結合使用(通過在不同的VC上應用它)，則它對服務提供商非常有用。這種模式的侷限性在於它是固定的，並且服務提供商需要提前提供QoS。QoS不會在選擇服務時動態應用。目前，使用者沒有通過按一下滑鼠為不同服務選擇不同頻寬的選項；但是，為了開發這一功能，已經投入了大量的工程工作。

在此架構中，CPE的部署、管理和調配可能極具挑戰性，因為需要為CPE配置使用者名稱和密碼。作為一個簡單的解決方案，一些服務提供商對所有CPE使用相同的使用者名稱和密碼。這會帶來巨大的安全風險。此外，如果CPE需要同時開啟不同的會話，則需要在CPE、NAP和NSP上調配其他VC。Cisco DSLAM和匯聚裝置能夠簡化CPE配置和調配。直通管理工具也可用於端到端PVC調配。使用PVC在NSP為這麼多使用者調配資源是一個限制因素，因為必須管理所有不同的PVC。此外，通過按一下滑鼠或輸入少許按鍵來調配單個NRP上的2000 PVC沒有簡單的方法。

現在，我們針對此架構的不同元件擁有不同的管理應用，例如適用於DSLAM的Viewrunner和適用於Cisco 6400的SCM。沒有單一的管理平台可以調配所有元件。這是公認的侷限性，為了提供單一的綜合管理應用程式來調配CPE、DSLAM和Cisco 6400，我們投入了大量精力。此外，我們目前有一個實施PPPoA with SVC的解決方案，這將大大簡化部署。含SVC的PPPoA也允許終端使用者動態選擇目的地和QoS。

對於使用此架構的大型ADSL部署，需要記住的另一個重要一點是從匯聚路由器到RADIUS伺服器的通訊。如果在聚合裝置上終止數千個PPP會話時，NRP刀片發生故障，則必須重新建立所有這些PPP會話。這意味著一旦建立連線，所有訂閱者都必須通過身份驗證，並且其記帳記錄必須停止並重新啟動。當這麼多使用者同時嘗試獲得驗證時，通向RADIUS伺服器的管道可能是個瓶頸。某些訂閱者可能無法進行身份驗證，這可能會給服務提供商帶來問題。

具有足夠頻寬以同時容納所有訂戶的指向RADIUS伺服器的鏈路非常重要。此外，RADIUS伺服器必須足夠強大，才能向所有訂閱者授予許可權。如果有成千上萬的使用者，應考慮在可用RADIUS伺服器之間進行負載均衡的選項。Cisco IOS®軟體提供此功能。

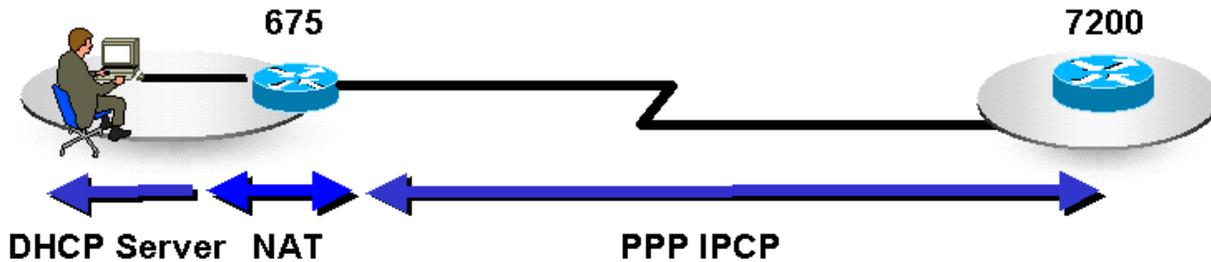
作為最後考慮因素，聚合路由器的效能必須足以容納許多PPP會話。應用其他實施使用的相同流量工程原則。以前，使用者必須在點對點子介面上配置PVC。如今，PPPoA允許使用者在多點子介面和點對點上配置多個PVC。每個PPPoA連線不再需要兩個介面描述符塊(IDB)，一個用於虛擬訪問介面，另一個用於ATM子介面。此增強功能增加了路由器上運行的PPPoA會話的最大數量。

平台支援的最大PPPoA會話數取決於可用的系統資源，如記憶體和CPU速度。每個PPPoA會話採用一個虛擬接入介面。每個虛擬訪問介面都包括一個硬體介面描述符塊和一個軟體介面描述符塊(hwidb/swidb)對。每個硬碟大約需要4千5百。每台swidb大約需要2千5百。虛擬訪問介面總共需要

7.5K。2000個虛擬訪問介面需要2000 \* 7.5K或15M。要運行2000個會話，路由器需要額外的15M。由於會話限制增加，路由器需要支援更多IDB。由於運行更多PPP狀態機例項需要更多CPU週期，因此這種支援會影響效能。

## PPPoA架構要點

本節介紹PPPoA體系結構的三個要點：cpe、IP Management和到達服務目標。



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.

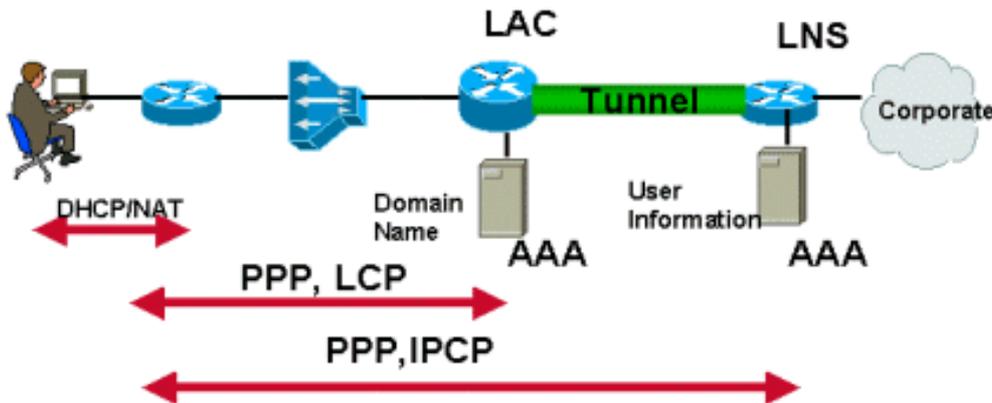
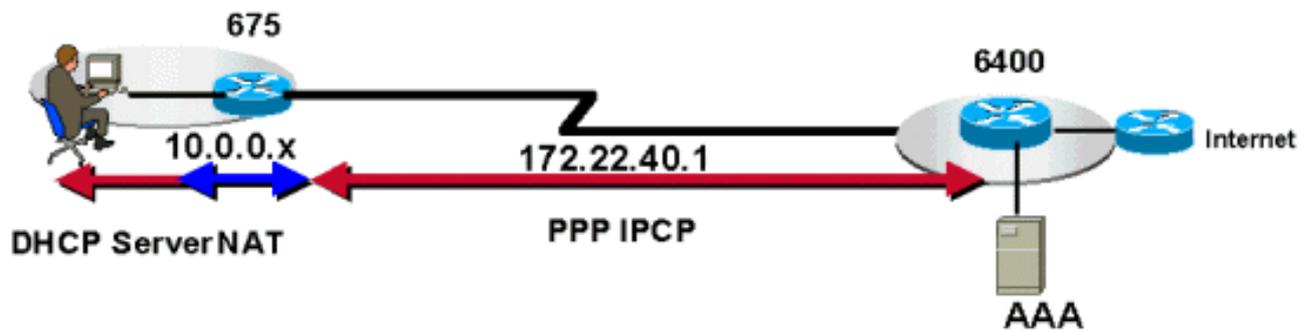
Optionally, the CPE may be configured as a DHCP server to provide private IP addresses to end stations on the LAN. The CPE can also be configured to do Port Address Translation (PAT). A CPE configured for PAT and DHCP usually gets a single public IP address from the final destination and all the stations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

由於PAT的性質，某些將IP資訊嵌入負載的應用程式無法在此情況下工作。要解決此問題，請應用IP地址子網而非單個IP地址。

在此架構中，由於IP地址已分配給CPE，NAP/NSP更易於通過Telnet連線到CPE進行配置和故障排除。

CPE可以根據使用者配置檔案使用不同的選項。例如，對於住宅使用者，可以不使用PAT/DHCP配置CPE。對於有多台PC的使用者，可以為PAT/DHCP配置CPE，也可以採用與住宅使用者相同的方式配置CPE。如果有一台IP電話連線到CPE，則該CPE可能配置為使用多個PVC。

## IP管理



在PPPoA架構中，使用者CPE的IP地址分配使用IPCP協商，與撥號模式中的PPP原理相同。根據使用者使用的服務型別分配IP地址。如果使用者只能從NSP訪問Internet，則NSP將終止來自使用者的這些PPP會話，並分配IP地址。IP地址是從本地定義的池、DHCP伺服器分配的，或者可以從RADIUS伺服器應用。此外，ISP可能為使用者提供了一組靜態IP地址，並且當使用者發起PPP會話時不會動態分配IP地址。在此案例中，服務供應商將僅使用RADIUS伺服器驗證使用者。

如果使用者希望有多個可用服務，NSP可能需要實施SSG。以下是分配IP地址的可能性。

- SP可能通過其本地池或RADIUS伺服器向使用者提供IP地址。使用者選擇服務後，SSG會將使用者的流量轉發到該目標。如果SSG使用代理模式，則最終目標可能提供一個IP地址，SSG將使用該地址作為NAT的可見地址。
- PPP會話不會在服務提供商的聚合路由器上終止。它們通過隧道傳輸或轉發到最終目的地或主網關，最終會終止PPP會話。最終目的地或歸屬網關與使用者協商IPCP，從而動態提供IP地址。只要最終目標已分配這些IP地址並且有通往這些地址的路由，靜態地址也是可能的。

在Cisco 6400 NRP的Cisco IOS軟體版本12.0.5DC之前，服務提供商無法向使用者提供IP地址子網。Cisco 6400平台和Cisco 600系列CPE允許在PPP協商期間在CPE上動態配置IP子網。此子網中的一個IP地址分配給CPE，而其餘的IP地址通過DHCP動態分配給站點。使用此功能時，不需要為PAT配置CPE，PAT不適用於某些應用程式。

## 如何到達服務目的地

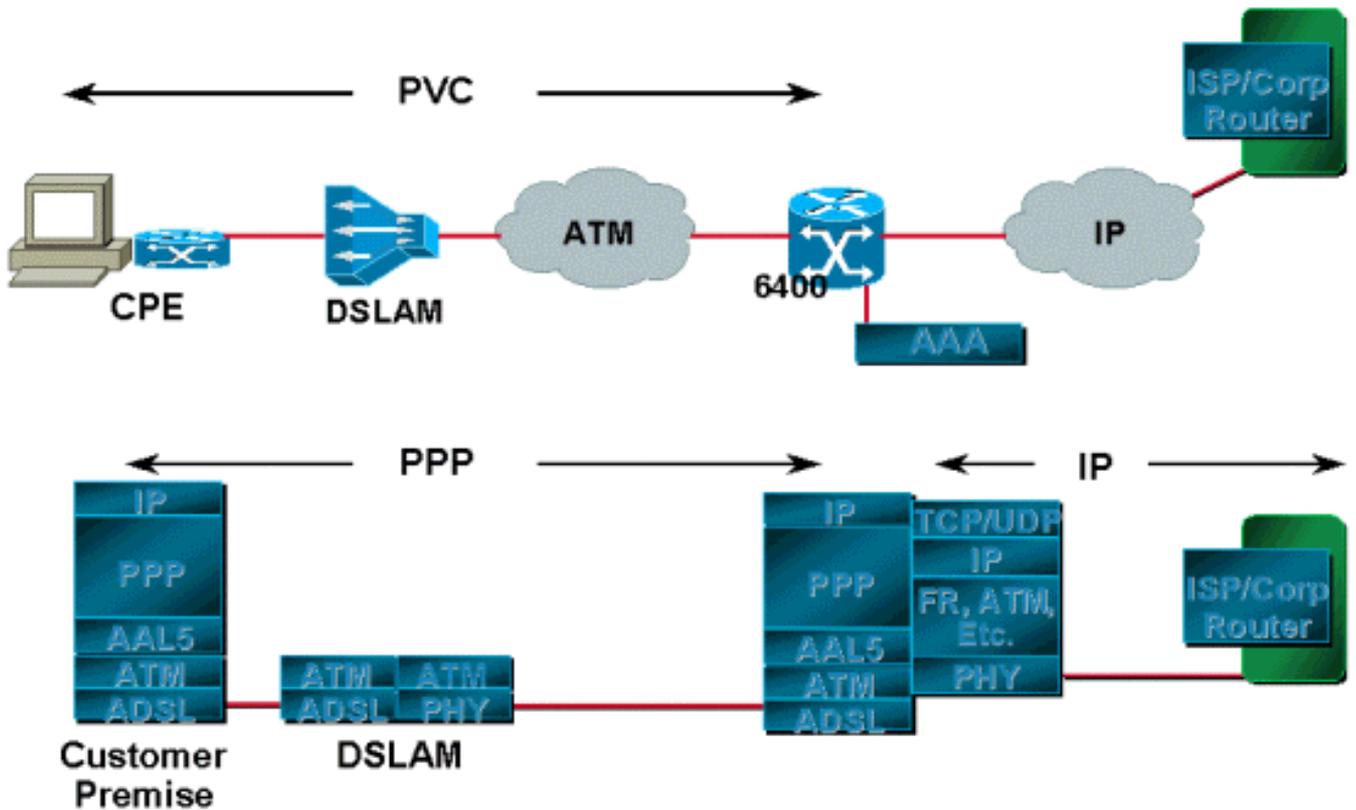
在PPPoA架構中，可以通過不同方式到達服務目的地。一些最常用的部署方法是：

- 在服務提供商處終止PPP會話
- L2TP通道
- 使用SSG

在這三種方法中，都有一組固定的PVC從CPE定義到DSLAM，並在聚合路由器上切換到一組固定的PVC。PVC通過ATM雲從DSLAM對映到匯聚路由器。

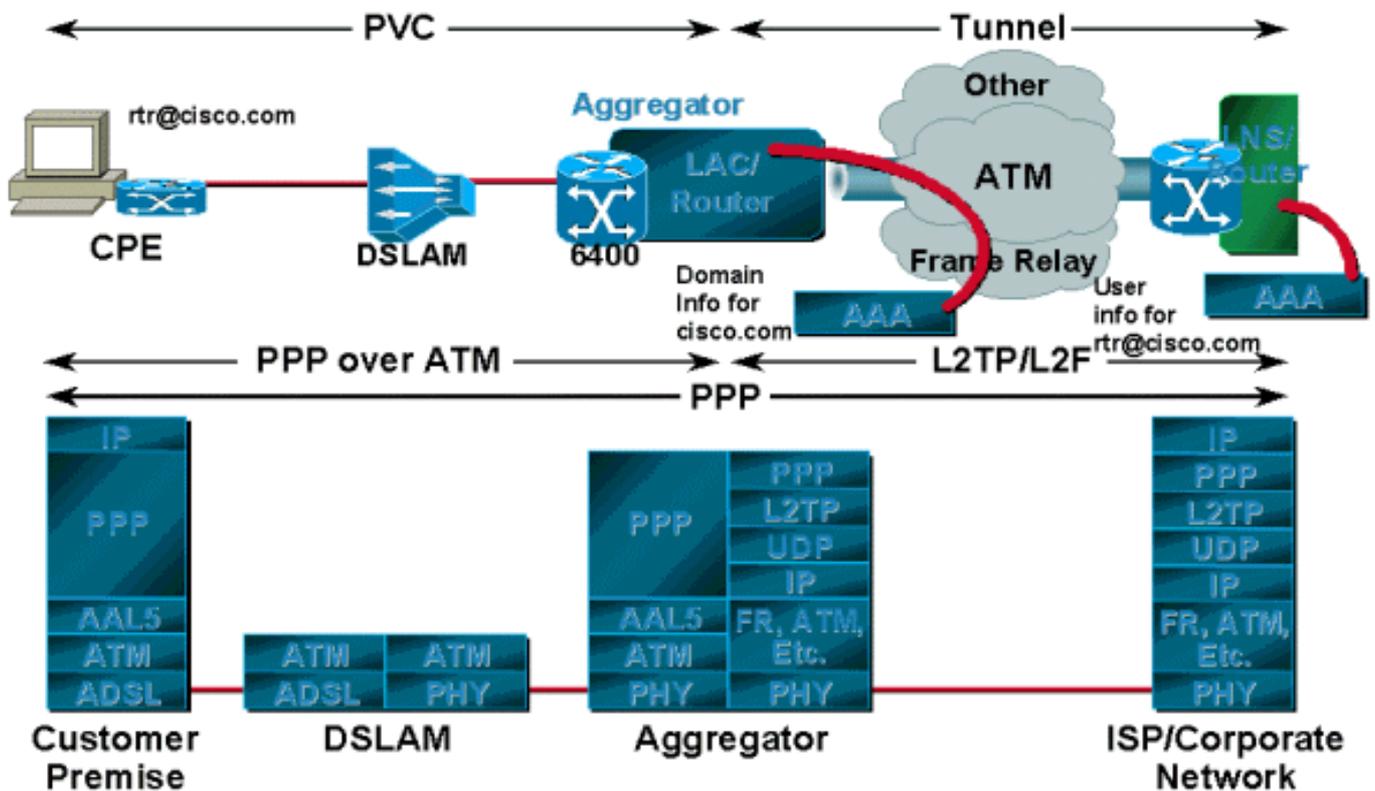
也可以使用其他方法（例如含SVC的PPPoA或多通訊協定標籤交換/虛擬私人網路）到達服務目的地。這些方法不在本檔案的範圍之內，將在單獨的檔案中進行討論。

### 在聚合時終止PPP



由使用者發起的PPP會話將在使用路由器上的本地資料庫或通過RADIUS伺服器對使用者進行身份驗證的服務提供商處終止。在使用者通過身份驗證後，會進行IPCP協商，並將IP地址分配給CPE。分配IP地址後，在CPE和聚合路由器上都建立了主機路由。分配給使用者的IP地址（如果合法）會通告給邊緣路由器。邊緣路由器是使用者訪問網際網路的網關。如果IP地址是私有地址，服務提供商會在向邊緣路由器通告這些地址之前對其進行轉換。

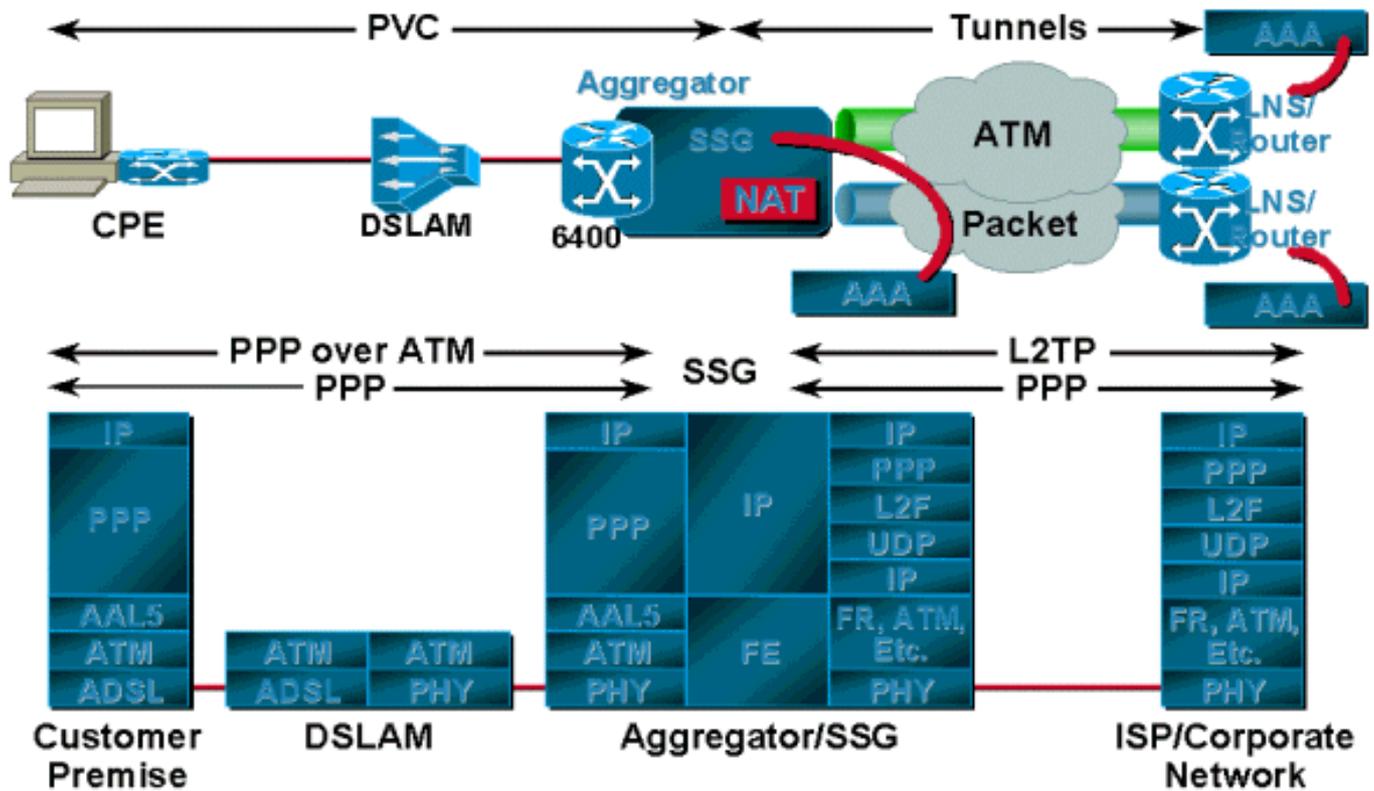
### L2TP/L2F通道



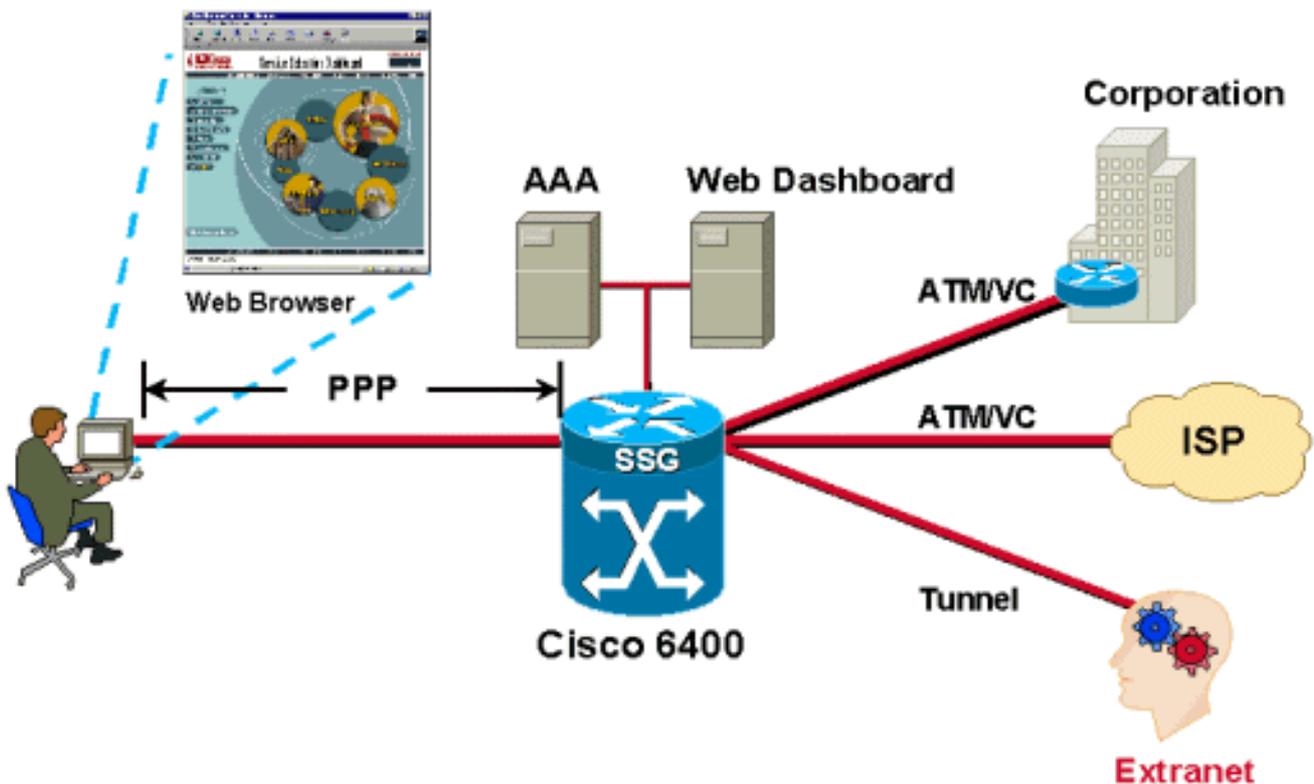
PPP會話（取決於服務提供商或公司）使用L2TP或L2F隧道連線到上游終端點，而不是在服務提供商的聚合路由器上終止。此終止點驗證使用者名稱，並且通過DHCP或本地池為訂戶分配IP地址。在此案例中，通常在L2TP訪問集中器/網路訪問伺服器(LAC/NAS)與家庭網關或L2TP網路伺服器(LNS)之間建立一個隧道。LAC基於域名對傳入會話進行身份驗證；使用者名稱在最終目的地或主網道進行驗證。

但是，在此模型中，使用者只能訪問最終目標，且一次只能訪問一個目標。例如，如果使用rtr@cisco.com使用者名稱配置CPE，則該CPE後面的PC只能訪問思科域。如果想要連線到另一個公司網路，他們需要更改CPE上的使用者名稱和密碼以反映該公司域名。在此案例中，通道目的地是透過使用路由通訊協定、靜態路由或透過ATM執行傳統IP（如果首選ATM作為第2層）而到達。

### [使用服務選取閘道\(SSG\)](#)



SSG相對於通道的主要優勢是SSG提供一對多服務的對應，而通道僅提供一對一對應。當單個使用者需要訪問多個服務，或者位於單個位置的多名使用者需要訪問唯一的服務時，該選項會非常有用。SSG使用基於Web的服務選擇控制面板(SSD)，該控制面板包含不同的服務，可供使用者使用。使用者可以一次訪問一項或多項服務。使用SSG的另一個優勢是，服務提供者可以根據使用的服務和會話時間對使用者計費，使用者可以通過SSD開啟和關閉服務。



當PPP會話從使用者傳入時，對使用者進行身份驗證。從本地池或RADIUS伺服器為使用者分配IP地址。在使用者成功通過身份驗證後，將使用SSG代碼建立源對象，並授予使用者訪問預設網路

的許可權。預設網路包含SSD伺服器。使用者使用瀏覽器登入到控制面板，由AAA伺服器進行身份驗證，然後根據儲存在RADIUS伺服器中的使用者配置檔案提供一組訪問服務。

每次經過身份驗證的使用者選擇服務時，SSG都會為該使用者建立一個目標對象。目標對象包含目標地址、該目標的DNS伺服器地址以及來自家庭網關的已分配源IP地址等資訊。來自使用者端的資料包將根據目標對象中包含的資訊轉發到目標。

可以將SSG配置為代理服務、透明直通或PTA。當使用者請求訪問代理服務時，NRP-SSG會將訪問請求傳遞給遠端RADIUS伺服器。當接收到接入接受時，SSG用接入接受來響應訂戶。SSG顯示為遠端RADIUS伺服器的客戶端。

透明傳輸允許未經驗證的使用者流量在任一方向通過SSG路由。使用過濾器控制透明直通流量。

PTA只能由PPP型別的使用者使用。身份驗證、授權和記帳的執行方式與代理服務型別完全相同。使用者使用user@service形式的使用者名稱登入服務。SSG會將該服務轉送到RADIUS伺服器，然後RADIUS伺服器會將服務設定檔載入到SSG。SSG將請求轉發到由服務配置檔案的RADIUS伺服器屬性指定的遠端RADIUS伺服器。在請求通過身份驗證後，會將IP地址分配給使用者。不執行NAT。所有使用者流量都會匯聚到遠端網路。使用PTA，使用者只能訪問一項服務，不能訪問預設網路或SSD。

## [PPPoA架構的操作說明](#)

當CPE首次通電時，它將開始向聚合伺服器傳送LCP配置請求。配置了PVC的聚合伺服器還會在虛擬訪問介面（與PVC關聯）上傳送LCP配置請求。當每個使用者看到另一個使用者的配置請求時，它們會確認該請求，並開啟LCP狀態。

對於身份驗證階段，CPE將身份驗證請求傳送到聚合伺服器。根據伺服器配置，伺服器會根據域名（如果提供）或使用者名稱（使用本地資料庫或RADIUS伺服器）對使用者進行身份驗證。如果來自訂戶的請求採用username@domainname形式，則聚合伺服器將嘗試建立通向目標的隧道（如果尚未建立隧道）。建立隧道後，聚合伺服器會將PPP請求從使用者轉發到目的地。然後，目標對使用者進行身份驗證並分配IP地址。如果來自訂閱伺服器的請求不包含域名，則使用者通過本地資料庫進行身份驗證。如果在聚合路由器上配置了SSG，則使用者可以訪問指定的預設網路，並可獲得選擇不同服務的選項。

## [結論](#)

PPPoA因其高度可擴充性、使用SSG功能並提供安全性，正成為許多服務提供商最合適的架構。由於本文的重點是PPPoA架構，無法深入瞭解SSG等功能。這些功能將在後續文章中介紹。本文檔中討論的不同方案的示例配置也將在不同的文檔中介紹和說明。

## [相關資訊](#)

- [Cisco DSL產品支援資訊](#)
- [技術支援 - Cisco Systems](#)