

適用於Cisco 6400 UAC的PPPoE基線架構

目錄

[簡介](#)

[假設](#)

[技術簡介](#)

[PPPoE體系結構的優缺點](#)

[優勢](#)

[缺點](#)

[PPPoE架構的實施注意事項](#)

[PPPoE架構要點](#)

[結論](#)

[參考資料](#)

[相關資訊](#)

簡介

本檔案介紹使用乙太網路上的點對點通訊協定(PPPoE)的端到端非對稱數位使用者線路(ADSL)架構。

在當前的接入技術環境中，希望通過同一客戶端接入裝置連線遠端站點上的多個主機。此外，還必須以類似於使用點對點通訊協定(PPP)的撥號服務的方式提供存取控制和計費功能。在許多接入技術中，將多台主機連線到客戶駐地接入裝置的最經濟有效的方法是通過乙太網。此外，最好將此裝置成本保持在儘可能低的水準上，並使配置要求降低或不降低。

在部署ADSL時，客戶必須在大量現有橋接客戶端裝置(CPE)上支援PPP風格的身份驗證和授權。PPPoE通過簡單的橋接接入裝置將主機網路連線到遠端訪問集中器或聚合集中器。使用此模式時，每個主機使用自己的PPP堆疊。因此，它向使用者呈現熟悉的使用者介面。您可以按使用者（而不是按站點）訪問控制、計費和服務型別。

假設

基線架構假設提供以下專案：

- 對使用PPPoE的終端使用者進行高速網際網路訪問和企業訪問。
- ATM作為核心主幹技術，由Cisco 6400通用接入集中器(UAC)實施。

這種設計實施限制會限制此架構在其他平台上的使用，但PPPoE會不斷演變。閱讀相關產品的最新版本說明，以利用新的和更新的功能。

本文基於當前部署以及使用Cisco 6400 UAC的內部測試。本文是PPPoA基線架構[論文的延續](#)，經常引用它。假設您已閱讀PPPoA基線架構白皮書並瞭解PPP的基本原理，而且您已閱讀最新軟體版

本的發行說明。

技術簡介

如RFC 2516中所述，PPPoE有兩個不同的階段：發現階段和PPP會話階段。當主機發起PPPoE會話時，它必須首先執行發現以確定哪台伺服器能夠滿足客戶端的請求。其次，它需要確定對等裝置的乙太網MAC地址並建立PPPoE會話ID。雖然PPP定義了點對點關係，但發現本質上是客戶端—伺服器關係。

在發現過程中，主機（客戶端）發現一個或多個訪問集中器（伺服器）並選擇一個。發現成功完成後，主機和選定的訪問集中器都會獲取資訊，以便通過乙太網建立其點對點連線。建立PPP會話後，主機和訪問集中器都必須為PPP虛擬介面分配資源（對於所有實施可能並非如此）。有關PPPoE規範的更多詳細資訊，請參閱RFC 2516。

PPPoE體系結構的優缺點

PPPoE體系結構繼承了撥號模型和PPPoA體系結構中使用的PPP的大部分優勢。以下各節列出PPPoE的一些主要優點和缺點，以及它們與PPPoA的不同之處。

優勢

以下是PPPoE的一些關鍵優勢及其與PPPoA的不同之處：

- 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PPPoE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。服務提供商也可以要求最低訪問費用。
- 您可以在當前的CPE安裝上使用PPPoE，這些安裝無法升級到PPP或無法運行PPPoA，從而將PPP會話通過橋接乙太網LAN擴展到PC。
- PPPoE保留網際網路服務提供商(ISP)在當前撥號模式下使用的點對點作業階段。PPPoE是唯一一種無需中間IP堆疊即可通過乙太網運行點對點協定的協定。
- 網路訪問提供商(NAP)或網路服務提供商(NSP)可以提供對企業網關的安全訪問，而無需管理端到端永久虛擬電路(PVC)，也不需要第3層路由和/或第2層隧道協定(L2TP)隧道。這使得批發服務和虛擬專用網路(VPN)銷售的業務模式更具可擴充性。
- PPPoE可以在給定時間為主機(PC)提供到多個目標的訪問。每個PVC可以有許多個PPPoE會話。
- 在行業標準遠端身份驗證撥入使用者服務(RADIUS)伺服器的幫助下，NSP可以通過部署閒置和會話超時進行超訂用。
- 您可以將PPP與服務選取閘道(SSG)功能搭配使用。

缺點

以下是PPPoE的一些主要缺點以及它們與PPPoA的不同之處：

- 必須在連線到乙太網段的所有主機(PC)上安裝PPPoE客戶端軟體。這意味著訪問提供商必須在PC上維護CPE和客戶端軟體。
- 由於PPPoE實施使用RFC 1483橋接，因此很容易受到廣播風暴和可能的拒絕服務攻擊。

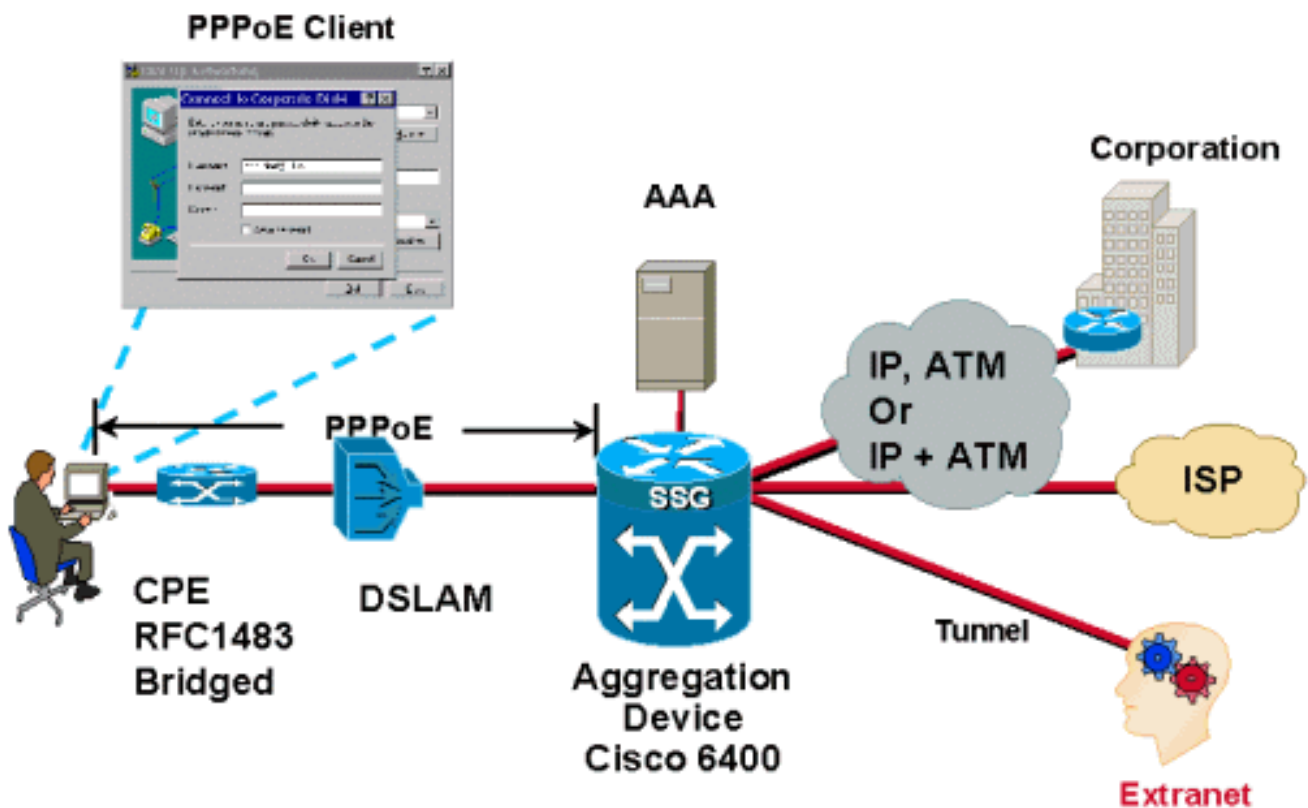
PPPoE架構的實施注意事項

以下是實施此類架構之前需要考慮的一些要點。

- 支援的訂閱伺服器數量。所需的PPPoE伺服器數量取決於會話數量。
- 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ISP。
- 服務提供商還是最終服務目標提供IP地址。
- 在多使用者的情況下，無論所有使用者是否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。終端使用者是否需要同時訪問多個目標？
- 接入提供商使用的PPPoE客戶端軟體，軟體是否已經過測試，主機使用的作業系統，以及作業系統能否做出智慧路由決策。
- 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。
- 部署和提供CPE、DSLAM和匯聚線上點(POP)。
- NAP的業務模式。這一模式是否還包括批發服務（如安全的企業訪問）和增值服務（如語音和影片）的銷售？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為終端使用者提供的應用型別。
- 預期的上游和下游資料流量。考慮NRP吞吐量、流量工程和任何QoS問題。

本文檔討論PPPoE架構如何適合和擴展為服務提供商的不同業務模式，以及提供商如何藉助此架構獲益。

網路架構



PPPoE架構的設計注意事項

本節介紹特別適用於PPPoE架構的問題。

在部署任何架構之前，必須瞭解服務提供商的業務模式以及提供商提供的服務。您需要瞭解PC上使用的客戶端軟體。最常見的軟體來自Routerware。由於客戶端軟體安裝在一台PC上，因此服務提供商技術人員需要很好地瞭解該PC及其作業系統。

如RFC 2516所述，最大接收單元(MRU)選項不得協商大於1492的大小。乙太網的最大負載大小為1500個八位位元組。PPPoE報頭是6個八位位元組，PPP協定ID是2個八位位元組，因此PPP最大傳輸單元(MTU)不得大於1492。這是通過為PPPoE虛擬模板介面配置IP MTU 1492實現的。

預設情況下，在配置PPPoE VPDN組時，不會預先克隆虛擬訪問介面。使用者可以通過發出**virtual-template <number> pre-clone <number> global**命令更改預克隆虛擬訪問介面的最大數量。

為了保護路由器免受拒絕服務攻擊，PPPoE (預設) 只允許一個會話源自VC上的MAC地址。使用者可以發出**pppoe session-limit per-mac**和**pppoe session-limit per-vc**命令以變更預設值。

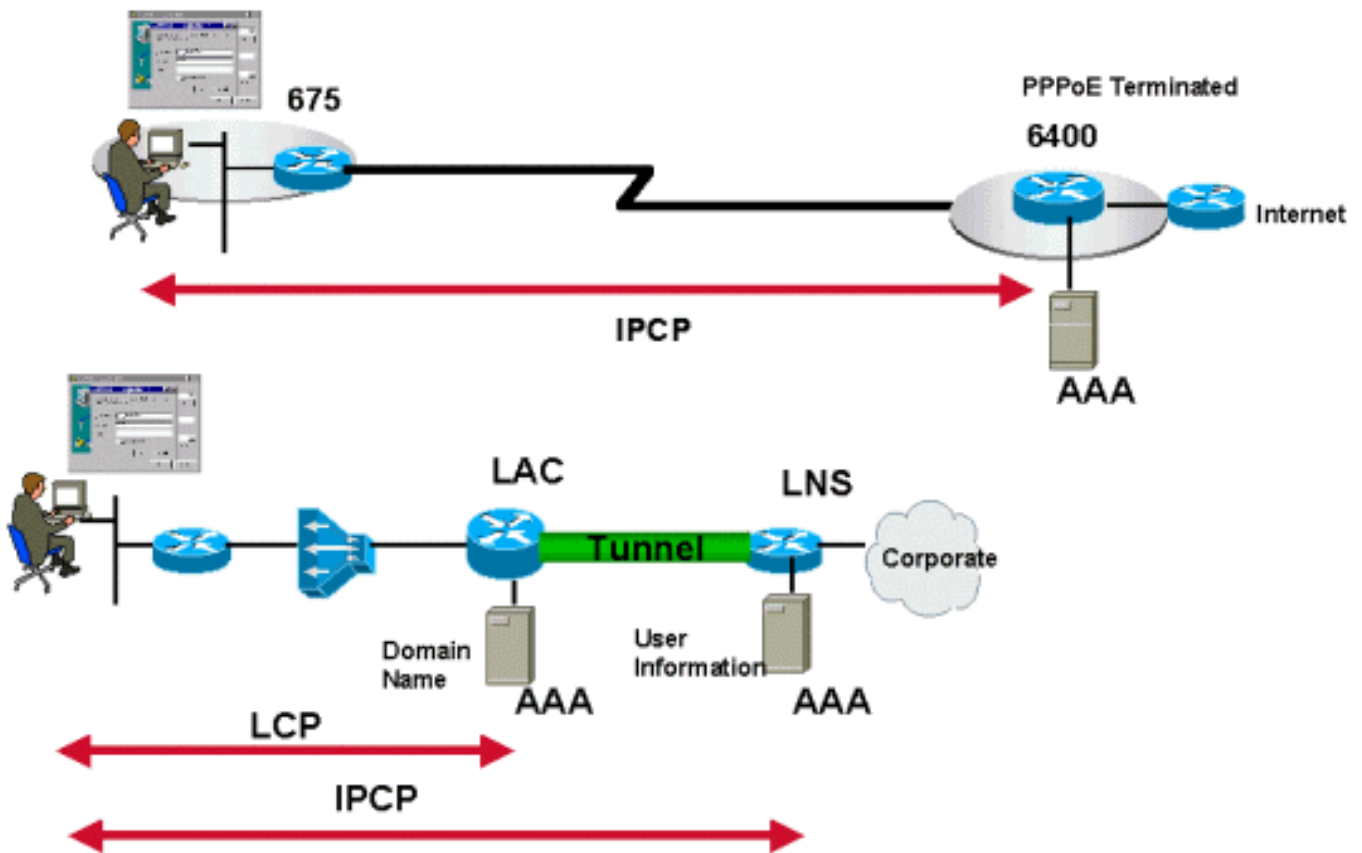
記帳、授權和身份驗證過程與PPPoA相同。唯一的區別是，目前，基於VPI/VCI的身份驗證 (可用於PPPoA，不可用於PPPoE) 可以使用L2TP和SSG架構進行批發服務。

PPPoE架構要點

CPE

CPE配置為純RFC 1483橋接。每個CPE僅使用一個VPI/VCI對，此CPE後面的主機啟動的所有PPPoE會話都在此單一VC中傳輸。

IP管理



運行PPPoE客戶端的單個主機的IP地址分配基於撥號模式IPCP協商中的PPP相同原則。IP地址來源取決於使用者購買的服務型別以及PPP會話終止的位置。PPPoE利用Microsoft Windows的撥號聯網功能，分配的IP地址反映在PPP介面卡中。

IP地址分配可以來自終止PPPoE會話的接入集中器，或者（對於L2TP）來自主網關。為每個PPPoE會話分配IP地址。

CPE無法執行網路地址轉換/動態主機配置協定(NAT/DHCP)，因為它已橋接，並且沒有分配給它的IP地址。

如何到達服務目的地

以下是到達服務目的地的方式：

- 在服務提供商處終止PPP會話
- L2TP通道
- 使用SSG

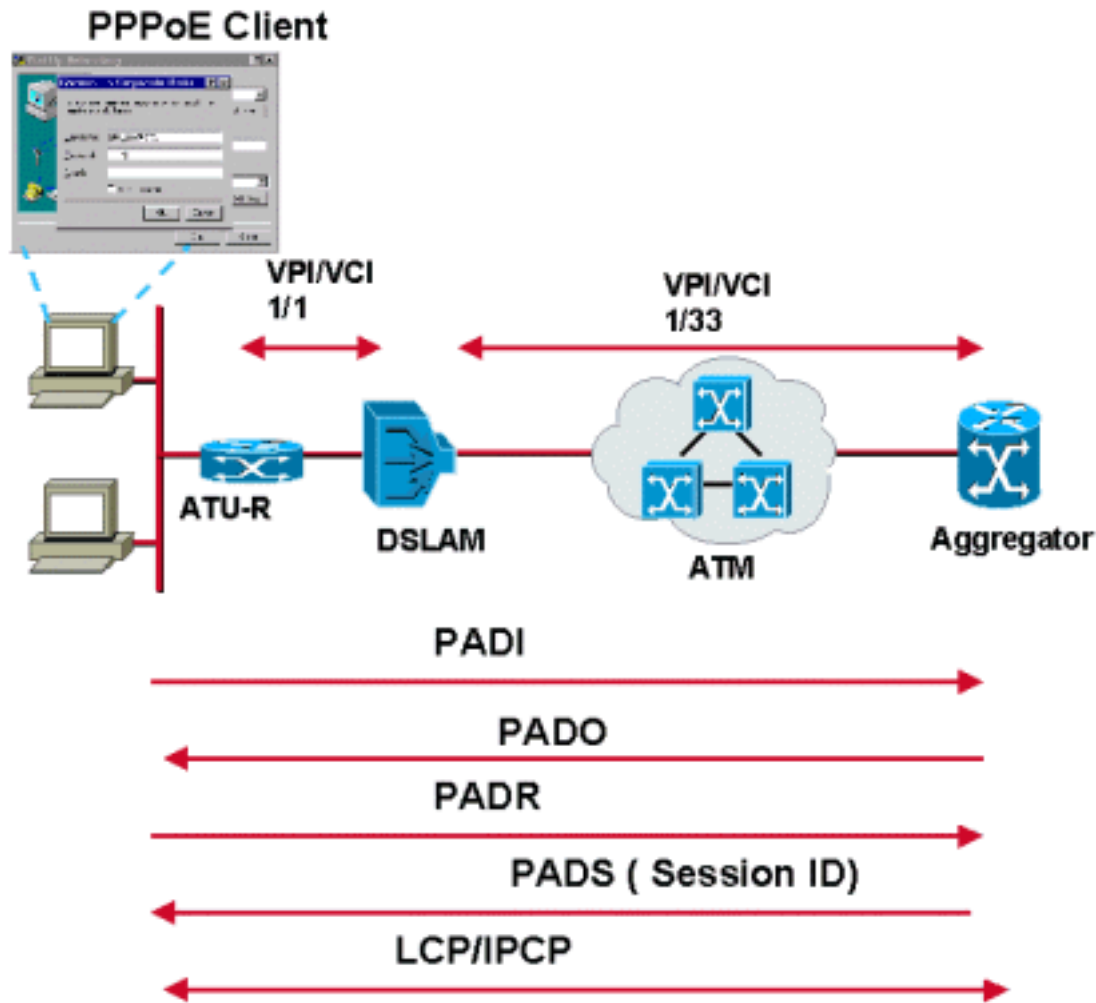
有關這些體系結構的詳細解釋將在不同的論文中介紹。

PPPoE的操作說明

此版本的PPPoE客戶端軟體支援RFC 2516中所述的發現和會話階段。到發現階段有四個步驟。完

成後，兩個對等體都知道PPPoE會話ID和對等體的乙太網地址，它們一起唯一地定義PPPoE會話。以下是步驟：

1. 主機廣播一個啟動資料包。主機將目的地址設定為廣播地址的PPPoE主動發現啟動(PADI)資料包傳送。PADI包含一個標籤，指示它請求的服務型別。
2. 一個或多個訪問集中器傳送提供資料包。當存取集中器或路由器收到其可提供服務的PADI時，它會傳送PPPoE主動探索提供(PADO)封包。destination_addr是傳送PADI的主機的單播地址。如果訪問集中器無法為PADI提供服務，則它不得使用PADO進行響應。由於PADI已廣播，因此主機可以接收多個PADO。



3. 主機傳送單點傳播作業階段要求封包。主機檢視其接收的PADO資料包並選擇一個。選擇取決於每個接入集中商提供的服務。然後，主機將一個PADR資料包傳送到其選擇的訪問集中器。destination_addr欄位設定為接入集中器或傳送PADO的路由器的單播乙太網地址。
4. 所選訪問集中器傳送確認資料包。當接入集中器收到PADR資料包時，它將準備開始PPP會話。它會為PPPoE會話生成一個唯一的會話ID，並使用PPPoE主動發現會話確認(PADS)資料包回覆主機。destination_addr欄位是傳送PADR的主機的單播乙太網地址。

PPPoE會話開始後，PPP資料會像任何其他PPP封裝一樣被傳送。所有乙太網資料包都是單播。

在建立會話之後的任何時間，主機或接入集中器都可以傳送PPPoE主動發現終止(PADT)資料包，以指示PPPoE會話已終止。

如需更多詳細說明，請參閱RFC 2516。

結論

對於ADSL，PPPoE更受歡迎，僅次於PPPoA。

參考資料

- RFC 2516 — 透過乙太網路(PPPoE)傳輸PPP的方法
- RFC 1483 - ATM適配第5層上的多協定封裝
- RFC 2364 — 使用AAL5的點對點

相關資訊

- [PPPoA基線體系結構](#)
- [DSL技術支援](#)
- [技術支援 - Cisco Systems](#)