

路由橋接封裝基線架構

目錄

[簡介](#)

[假設](#)

[技術簡介](#)

[操作說明](#)

[RBE優勢](#)

[實施注意事項](#)

[網路架構](#)

[RBE架構的設計注意事項](#)

[RBE的要點](#)

[CPE](#)

[IP管理](#)

[如何到達服務目的地](#)

[提供網際網路接入](#)

[批發服務](#)

[企業訪問](#)

[服務選擇功能](#)

[結論](#)

[相關資訊](#)

簡介

本檔案介紹使用Cisco 6400通用存取集中器(UAC)的路由橋接封裝(RBE)功能的端對端非對稱數位使用者線路(ADSL)架構。開發RBE是為了解決已知的RFC1483橋接問題，包括廣播風暴和安全。除了它只在ATM上運作外，RBE功能的作用與半橋接完全相同。通過使用xDSL使用者的獨特特性，可以實現更高的可擴充性、效能和安全性。

假設

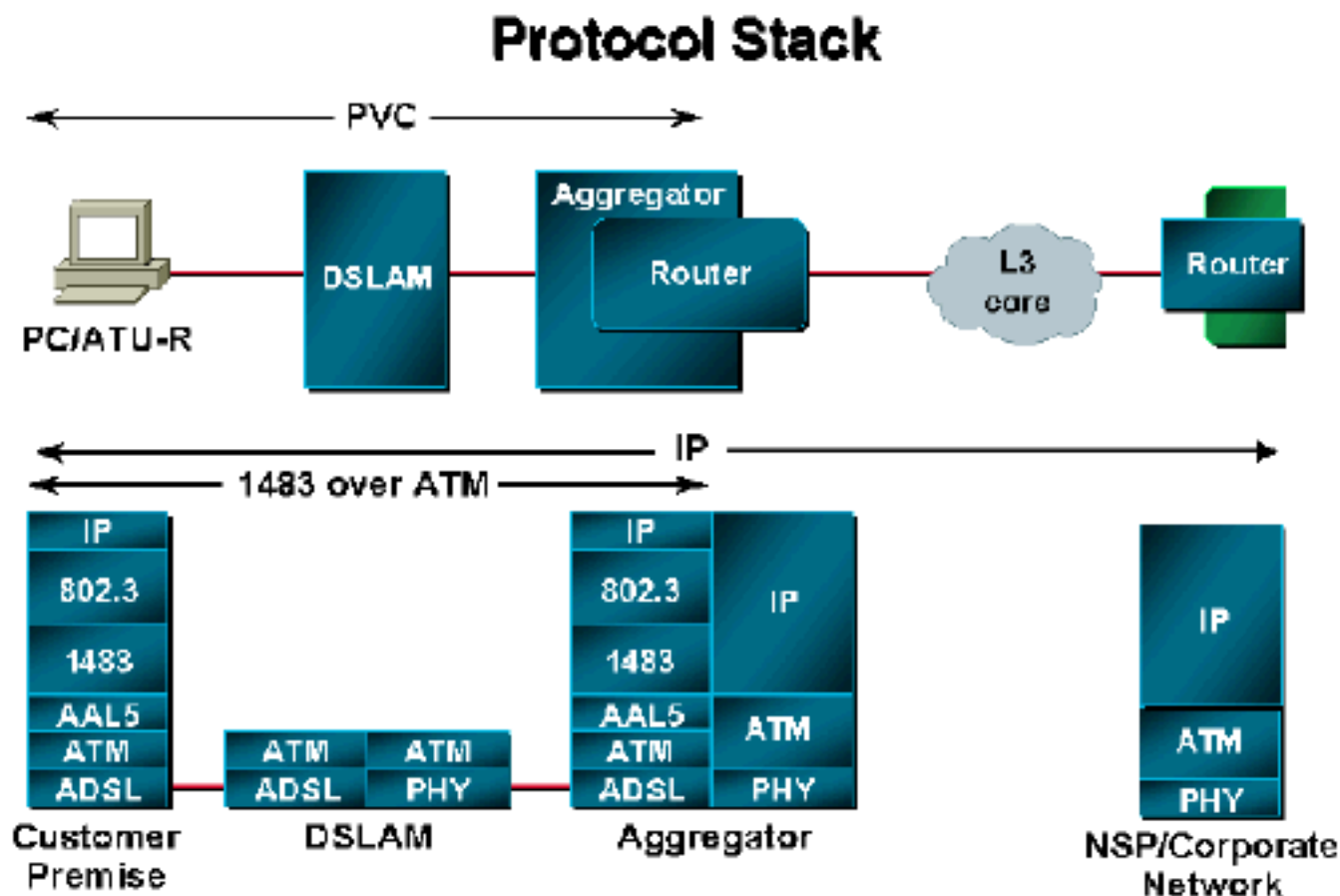
基線架構使用ADSL論壇參考架構模型設計。此架構涵蓋網路存取提供商(NAP)提供的不同服務產品，以及使用者流量如何轉送到網路服務提供商(NSP)的不同案例。在此架構中，RBE是Cisco 6400使用的假定封裝方法。本文檔的內容基於現有部署以及一些對架構執行的內部測試。有關增強功能和修改的資訊，請參閱最新版本的Cisco IOS®軟體的發行說明。目前，Cisco 6400、Cisco 7200和Cisco 7500平台支援RBE。本文僅討論思科6400。

技術簡介

從網路的角度來看，ATM連線看起來像路由連線。資料流量以RFC1483資料包的形式接收，但它們是RFC1483乙太網或IEEE 802.3幀。路由器不會像常規RFC1483橋接那樣橋接乙太網或IEEE

802.3 幀，而是在第3層報頭上路由。除一些粗略檢查外，橋頭會被忽略。下一節將對此進行詳細解釋。

操作說明



從運行角度看，路由器的運行就如同路由網橋介面連線到乙太網LAN一樣。下面以兩種方式介紹該操作：來自客戶駐地的資料包和目的地為客戶駐地的資料包。

對於來自客戶駐地的資料包，將跳過乙太網報頭並檢查目標IP地址。如果目的地IP地址在路由快取中，則封包會快速交換到傳出介面。如果目的IP地址不在路由快取中，則資料包將排隊等待進程交換。在進程交換模式下，通過檢視路由表可以找到資料包必須經過的出站介面。識別出站介面後，封包將透過該介面路由。這不需要網橋組或網橋組虛擬介面(BVI)。

對於目的地為客戶端的資料包，首先檢查資料包的目的IP地址。目的地介面是根據IP路由表確定的。接下來，路由器會檢查與該介面相關的位址解析通訊協定(ARP)表，以找出將放在乙太網路標頭中的目的地MAC位址。如果未找到任何地址，路由器將生成目的IP地址的ARP請求。ARP請求僅轉發到目的介面。這與橋接不同，在橋接中，ARP請求被傳送到橋接組中的所有介面。

對於使用未編號介面（其中可以在同一子網中找到兩個使用者）的情況，路由網橋介面使用代理ARP。例如，192.168.1.2（主機A）希望與192.168.1.3（主機B）通訊。但是，主機A與主機B位於同一子網中。

主機A必須通過向主機B傳送ARP廣播來獲知主機B的MAC地址。當匯聚裝置上的路由網橋介面收到此廣播時，它將發出一個MAC地址為192.168.1.1的代理ARP響應，主機A。它將取得該MAC地址，將其置於乙太網報頭中，然後傳送資料包。路由器收到資料包時，會丟棄報頭並檢視目的IP地址，然後在正確的介面上路由它。

RBE優勢

開發RBE的目的是解決RFC1483橋接架構所面臨的一些問題。RBE保留了RFC1483橋接架構的主要優勢，同時消除了大部分缺點。

- 客戶端裝置(CPE)上的最低配置。服務提供商認為這一點很重要，因為它不再需要大量卡車載客量，也不再需要大量人員投資來支援更高級別的協定。橋接模式下的CPE充當非常簡單的裝置。CPE僅涉及最少的故障排除，因為從乙太網傳入的所有資料都直接傳入WAN端。
- 易於從純橋接架構遷移到RBE。使用者端不需要更改。
- 避免典型純橋接架構中面臨的IP劫持和ARP欺騙挑戰。RBE還通過使用點對點連線來防止廣播風暴。安全性是純橋接架構的主要缺點。
- 與純粹的橋接架構相比，RBE由於在匯聚裝置上實施路由而提供了卓越的效能。此外，RBE的可擴充性更高，因為它沒有網橋組限制。
- 使用思科服務選擇閘道(SSG)支援第3層Web選擇。

實施注意事項

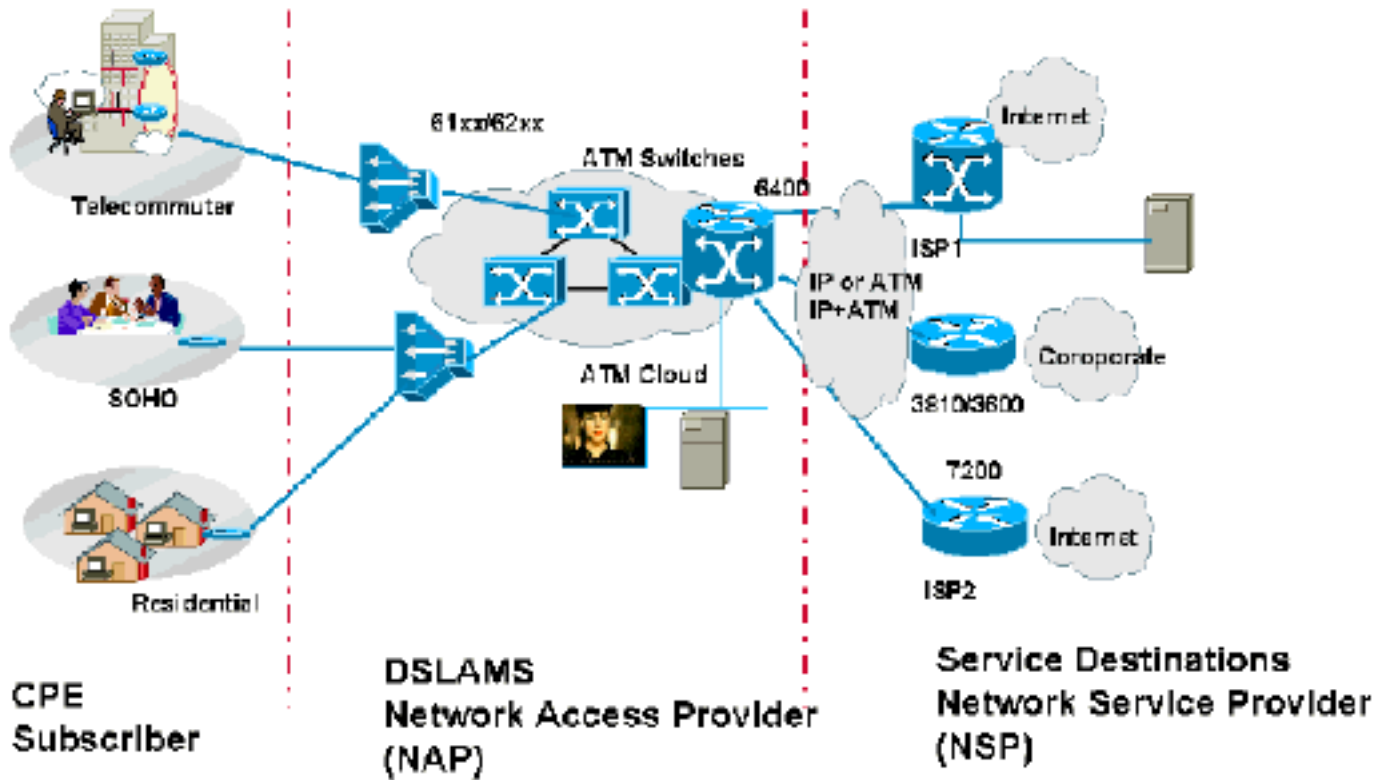
實施此架構之前需要考慮的一些要點與[RFC1483橋接基線架構](#)一文中提到的要點相同。

建議在以下情況下使用RBE:

- 場景與現有橋接架構中的場景相同。
- NAP僅希望對CPE執行最小管理。簡單的CPE的概念需要在使用者位置部署CPE後進行最低配置或無配置。
- NAP不希望在橋接CPE後的主機上安裝和維護主機客戶端。這些安裝和維護任務會增加部署成本和維護，包括提供瞭解客戶端軟體和運行客戶端的作業系統的幫助台人員。
- NAP希望使用現有CPE (只能在RFC1483橋接模式下運行) 部署可擴展的安全橋接網路，並希望提供服務選擇功能。

接下來的討論將說明RBE架構如何適應和擴展不同的業務模式。

網路架構



RBE網路架構類似於RFC1483橋接架構。按照該體系結構中的規定，聚合裝置可以位於NAP中或NSP中。如果使用端到端永久虛擬電路(PVC)架構，NSP將終止使用者並在匯聚裝置上配置RBE。如果NAP更願意提供批發服務和服務選擇，它可以選擇終止這些使用者，並從本地動態主機配置協定(DHCP)伺服器獲取IP地址。對於批發服務，NAP可以選擇從NSP獲取IP地址。本文檔的IP管理部分詳細介紹了這些方案。

RBE架構的設計注意事項

RBE可消除RFC1483橋接架構涉及的主要安全風險。此外，RBE提供了更好的效能和可擴充性，因為子介面被視為路由介面。

本節說明了設計RBE架構之前必須考慮的一些要點。對於使用者端，設計原則與RFC1483橋接架構相同。

在RBE中，為單個虛擬電路(VC)分配一個路由、一組路由或無類域間路由(CIDR)子網。因此，可信環境被減少到僅由路由集中的IP地址或CIDR塊表示的單個客戶駐地。ISP還控制分配給使用者的地址。這可以通過在該使用者的子介面上配置子網來實現。因此，如果使用者使用分配地址範圍之外的IP地址錯誤地配置裝置（可能導致ARP資料包流向路由器），路由器將生成「錯誤電纜」錯誤並拒絕將錯誤的IP到MAC地址對映輸入其ARP表中。

RBE只能使用點對點ATM子介面進行部署。不能在多點子介面上部署。即使使用者端已橋接，您也不需要定義橋接組或BVI介面，因為子介面被視為路由介面。

ATM點對點子介面可以是已編號的介面，也可以是未編號的介面。

根據定義，編號介面是指具有為其分配特定IP地址並具有固定子網掩碼的介面。例如：

```
Interface atm0/0/0.132 point-to-point
ip address 192.168.1.1 255.255.255.252
```

如本例所示，當使用編號介面部署RBE時，每個使用者都應有一個單獨的子網。使用者端的主機應配置為192.168.1.2。使用者端只有一個主機。如果要求支援多台主機，則選擇的子網掩碼應能容納更多主機。

通過編號介面，NAP可以控制使用者在CPE後面連線的主機數量。如上所述，缺乏控制是RFC1483橋接架構中的主要問題。

但是，此方法消耗的IP地址太多。您需要為每個使用者分配一個子網，為ATM子介面使用一個IP地址，並且保持廣播地址和所有零地址未使用。因此，要在CPE後面有一個主機，您至少需要定義子網掩碼255.255.255.252。考慮到IP地址稀缺，這可能不是可行的選項，除非NAP/NSP使用私有地址空間並執行網路地址轉換(NAT)來到達外部世界。

為了節省IP地址，另一種方法是使用未編號介面。根據定義，未編號介面是指使用ip unnumbered命令使用其他介面的IP地址的介面。例如：

```
!  
interface loopback 0  
ip address 192.168.1.1 255.255.255.0  
!  
interface atm0/0/0.132 point-to-point  
ip unnumbered loopback 0  
!  
interface atm0/0/0.133 point-to-point  
ip unnumbered loopback 0
```

如上例所示，IP地址和子網只應用於環回介面。所有ATM子介面將未編號到環回介面。在此方案中，在ATM子介面上終止的所有訂戶（未編號到環回0）將與環回0的訂戶位於同一子網中。這意味著訂戶將位於同一子網中，但將通過不同的路由介面進入。在這種情況下，路由器將難以確定哪一個使用者位於哪個ATM子介面之後。對於Cisco IOS，192.168.1.0(在IP管理圖中)通過介面loopback 0直接連線，並且它絕不會通過任何其他介面傳送目的地為該子網上的任何主機地址的流量。為了解決此問題，您需要明確配置靜態主機路由。例如：

```
ip route 192.168.1.2 255.255.255.255 atm0/0/0.132  
ip route 192.168.1.3 255.255.255.255 atm0/0/0.133
```

如以下範例所示，當路由器需要做出路由決定並需要轉送目的地為192.168.1.2的流量時，它會選擇ATM 0/0/0.132作為傳出介面，以此類推。如果不指定這些靜態主機路由，路由器會選擇傳出介面作為loopback 0並丟棄資料包。

即使未編號的介面會保留IP地址，它仍需要在節點路由處理器(NRP)上為每個使用者配置靜態主機路由的額外任務。請注意，例如，如果一個使用者在CPE後面有14台主機，則不需要為每台主機配置靜態主機路由。可以為ATM子介面定義總結路由。

到目前為止，此解釋假定在CPE後面的主機將配置為靜態IP地址。這種假設在現實生活中並不成立。在現實世界中，NAP希望對CPE及其所連線的主機執行最小的配置與維護。為此，主機應使用DHCP伺服器動態獲取地址。

為了動態獲取主機的IP地址，必須將主機配置為從DHCP伺服器獲取IP地址。當主機啟動時，它發出DHCP請求。然後這些請求被中繼到相應的DHCP伺服器，DHCP伺服器從主機先前定義的範圍內向主機分配IP地址。

為了將初始DHCP請求從主機轉發到相應的DHCP伺服器，您應該對接收廣播的介面應用ip helper-address命令。收到廣播後，Cisco IOS會檢視該介面的ip helper-address配置，並將單播資料包中的這些請求轉發到IP helper-address中指定的相應DHCP伺服器。在DHCP伺服器使用IP地址進行回覆後，它將響應傳送到最初轉發該請求的路由器上的介面。它用作出站介面，將DHCP伺服器響應

傳送到最初請求該服務的主機。路由器還會自動安裝此地址的主機路由。

如果在子介面上啟用了RBE，且它是IEEE 802.3橋接通訊協定資料單元(PDU)，則在ATM橋接器封裝後會檢查乙太網路封裝。如果是IP/ARP資料包，則處理方式與處理任何其他IP/ARP資料包的方式相同。IP封包是快速交換的。如果失敗，它會排隊等待進程交換。

RBE的效能是大贏家。當今的標準橋接代碼有一個固有的問題：在做出轉發決策之前，需要兩個不同的資料包分類。分類是指檢查（在上游）和修改（下游）資料包報頭以轉發資訊的過程，其成本相對較高。需要第2層查詢來確定資料包是否需要路由或橋接。然後，在第3層，需要查詢來確定資料包應路由到的位置。這種分類是在上游和下游方向進行的，這對效能有影響。

對於RBE，通過配置預先確定該分組將在上游方向上路由。因此，沒有必要通過橋接轉發路徑，這在標準橋接的情況下是必需的。

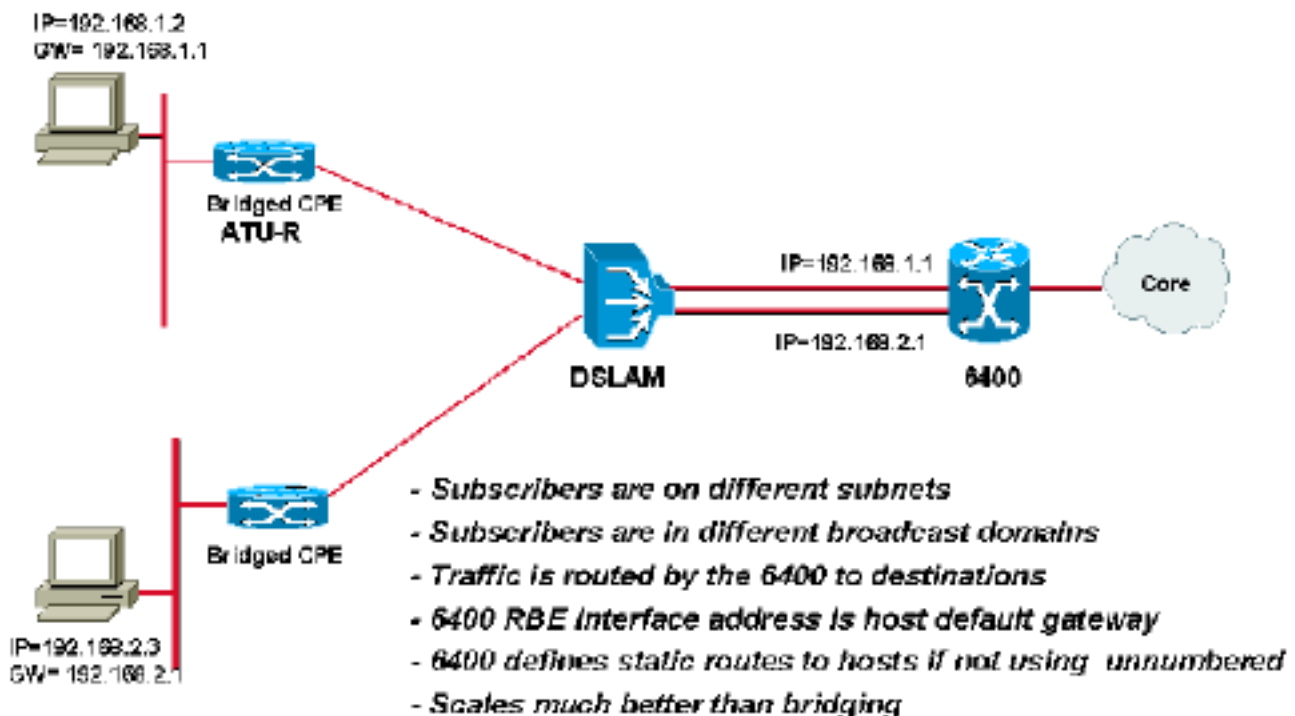
RBE的要點

CPE

CPE配置與標準橋接中的配置相同。部署RBE無需對CPE進行任何更改。

IP管理

Numbered Interfaces



在為RBE部署編號介面時，通常通過DHCP伺服器處理橋接CPE後面主機的IP地址分配。如前所述，DHCP伺服器可以駐留在NAP或NSP中。無論哪種情況，都應使用ip helper-address命令配置編號的ATM子介面。如果DHCP伺服器將位於NSP，則NAP聚合裝置必須具有到達該伺服器的路由。NAP使用自己的DHCP伺服器和IP地址範圍的唯一情況是，它希望向使用者提供服務選擇功能，並且這些使用者是連線到NAP的LAN。

如果NAP要使用NSP的IP地址空間，則應為每個子網分配一個IP地址給ATM子介面。此外，NAP和NSP之間應該有一些相互協定，以便NAP配置正確的地址。當NSP的DHCP伺服器分配IP地址時，應簽訂此協定以確保伺服器向主機提供正確的預設網關資訊。然後，NAP可以為分配給使用者的所有地址總結靜態路由，也可以選擇與NSP一起運行路由協定來通告這些路由。在大多數情況下，NAP和NSP都不希望使用路由協定。提供靜態路由是很好的選擇。

以下是在NRP上部署帶編號介面的RBE所需的基本配置：

```
!  
interface ATM0/0/0.132 point-to-point  
ip address 192.168.1.1 255.255.255.0  
ip helper-address 192.168.3.1  
no ip directed-broadcast  
atm route-bridged ip  
pvc 1/32  
encapsulation aal5snap  
!  
interface ATM0/0/0.133 point-to-point  
ip address 192.168.2.1 255.255.255.0  
ip helper-address 192.168.3.1  
no ip directed-broadcast  
atm route-bridged ip  
pvc 1/33  
encapsulation aal5snap
```

使用未編號介面是節省IP地址的最佳方式。如前所述，當未編號介面與DHCP一起使用時，主機路由會動態安裝。這可能是部署RBE的最佳方法。然後，DHCP伺服器可以位於NAP或NSP中，與編號介面一樣。

以下是NRP上部署具有未編號介面的RBE所需的基本配置：

```
interface Loopback0  
ip address 192.168.1.1 255.255.255.0  
no ip directed-broadcast  
!  
interface ATM0/0/0.132 point-to-point  
ip unnumbered Loopback0  
no ip directed-broadcast  
ATM route-bridged ip  
pvc 1/32  
encapsulation aal5snap  
!  
interface ATM0/0/0.133 point-to-point  
ip unnumbered Loopback0  
no ip directed-broadcast  
ATM route-bridged ip  
pvc 1/33  
encapsulation aal5snap
```

[如何到達服務目的地](#)

到目前為止，本文已經討論了使用RBE作為封裝方法的基本訪問技術。但是，使用此架構，NAP/NSP還可以提供各種服務和不同選項，NAP可以將使用者流量轉發到NSP。這些概念將在下一節中說明。

[提供網際網路接入](#)

在此方案中，NSP的主要功能是向終端使用者提供高速網際網路訪問。因為NSP將提供最終服務，所以IP地址管理成為NSP的責任。它可以使用DHCP伺服器為其終端使用者分配公有IP地址，也可以選擇為使用者提供私有IP地址，然後執行NAT以訪問外界。

[批發服務](#)

如果NAP希望向其他ISP提供批發服務，它可以這樣做。在這種情況下，NAP通常不偏好處理不同NSP的所有使用者的IP地址。NAP與ISP達成某種協定，為這些使用者提供相應的IP地址。這可以通過NAP將來自使用者的DHCP請求轉發到NSP上的DHCP伺服器來實現。NAP必須用該範圍內的一個IP地址配置其ATM子介面，並且它需要將這些路由通告給NSP。路由通告的形式可以是靜態路由，也可以是NAP和NSP之間的某種路由協定。靜態路由是NAP和NSP的首選方法。

[企業訪問](#)

企業訪問通常需要虛擬專用網路(VPN)服務。這意味著公司不會向NAP提供任何IP地址，並且不允許NAP在NAP的IP核心中通告公司IP地址空間，因為它可能導致安全漏洞。企業通常喜歡將自己的IP地址應用到客戶端，或者允許通過某種安全方式進行訪問，例如多協定標籤交換/虛擬專用網路(MPLS/VPN)或第2層隧道協定(L2TP)。

另一種提供安全企業訪問的方法是NAP向這些使用者提供初始IP地址。因此，使用者連線到NAP的LAN。在訂閱者擁有初始IP地址後，他們可以通過主機上運行的L2TP客戶端軟體啟動通往公司的隧道。反過來，公司將驗證該使用者並從其IP地址空間提供IP地址。此IP地址由L2TP VPN介面卡使用。這樣，使用者可選擇連線到其ISP進行Internet連線，或通過安全的L2TP隧道訪問其公司。但是，這要求公司向訂戶提供隧道目標IP地址，該地址應可通過NAP的IP核心路由。

[服務選擇功能](#)

NAP可以使用思科SSG的功能提供各種服務選擇功能。SSG提供兩種提供服務選擇的方法：通過第2層（稱為PTA-MD）和第3層Web選擇。在RBE中，只能使用第3層Web選擇方法。這就要求使用者通過LAN連線到NAP；即，NAP為使用者提供初始IP地址，並提供對思科服務選擇控制面板(SSD)的訪問。

在RBE架構的情況下，Cisco SSG的Web選擇方法是一種很好的方法，可以考慮使用者流量。

[結論](#)

與標準橋接相比，RBE提供了更好的效能和可擴充性。它還克服了標準橋接所面臨的所有安全問題。RBE消除了標準橋接的廣播風暴問題。RBE為NAP提供了強大的體系結構，它希望避免維護客戶端主機軟體、橋接相關問題，並希望降低部署成本。在RBE中，使用現有橋接架構時這一切都是可能的。

[相關資訊](#)

- [Cisco ADSL產品支援資訊](#)
- [技術支援與文件 - Cisco Systems](#)