RFC1483橋接基線架構

目錄

簡介

本檔案介紹使用RFC1483橋接時的端到端非對稱數位使用者線路(ADSL)架構。請注意，大多數xDSL資料機的早期版本是主機端10BaseT乙太網路和WAN端的RFC1483封裝橋接器框架之間的橋接器。即使在今天，現場部署的大部分ADSL客戶端裝置(CPE)仍採用純橋接模式。

假設

基線架構的設計假設為使用RFC1483橋接模型和ATM作為核心骨幹網為終端使用者提供高速網際網路接入。本文檔的內容基於現有部署架構和一些內部測試。

技術簡介

RFC1483描述了在ATM網路上傳送無連線網路互連流量的兩種不同方法：路由通訊協定資料單元(PDU)和橋接PDU。

路由允許在單個ATM虛擬電路(VC)上多路複用多個協定。 通過用IEEE 802.2邏輯鏈路控制(LLC)報頭對PDU進行字首來識別承載PDU的協定。

橋接通過ATM虛擬電路隱式執行高層協定多路複用。如需詳細資訊，請參閱RFC1483。

本檔案僅提及橋接PDU。

RFC1483橋接的優缺點

以下是RFC1483橋接架構優缺點總結。此架構有一些重要的缺點，其中大部分是橋接模型所固有的。在客戶站點部署ADSL時注意到一些缺點。

優勢

- 簡單易懂。橋接非常易於理解和實施，因為不存在路由或使用者身份驗證要求等複雜問題。
- CPE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。
- 易於安裝。橋接體系結構由於其簡單化而易於安裝。建立端到端永久虛擬電路(PVC)後，上層協定中的IP等活動變為透明的。
- 對使用者的多協定支援。當CPE處於橋接模式時，它不考慮封裝的是哪種上層協定。
- 非常適合在單一使用者環境中訪問Internet。由於CPE充當機頂盒，因此上層協定不需要複雜的故障排除。終端PC不需要安裝其他客戶端。

缺點

- 橋接在很大程度上依賴廣播建立連線。成千上萬使用者之間的廣播本質上是不可擴展的。這是因為廣播會消耗使用者的xDSL回圈中的頻寬，且廣播需要頭端路由器的資源透過點對點(ATM PVC)媒體複製廣播的封包。
- 橋接本身並不安全，需要可信的環境。地址解析協定(ARP)應答可能被欺騙，網路地址被劫持。此外，可以在本地子網發起廣播攻擊，從而拒絕向本地子網的所有成員提供服務。
- IP地址劫持是可能的。

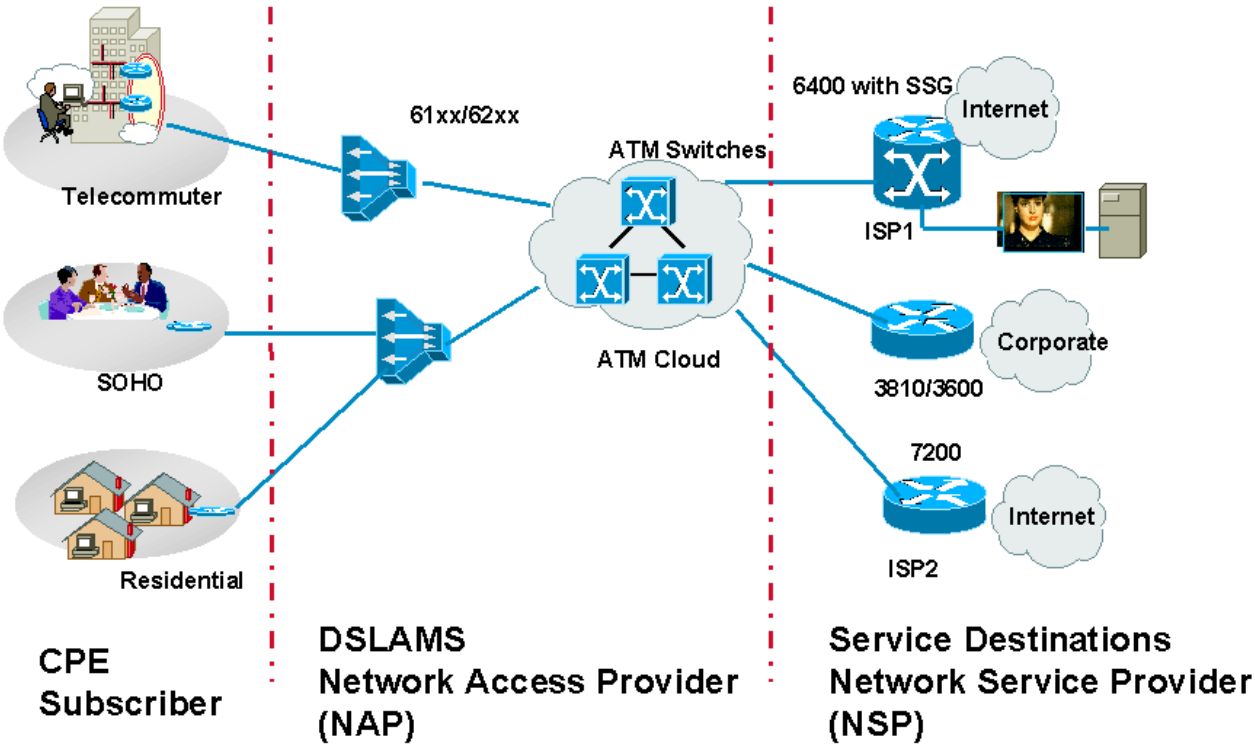
實施注意事項

在實施RFC1483橋接架構之前，請考慮以下問題。

- 要服務的當前訂戶和計畫訂戶數量是多少？
- 使用者是否需要相互通訊？
- 這些使用者是單使用者住宅客戶嗎？您是否服務於CPE後面可能有小型LAN的小型辦公室、家庭辦公室(SOHO)客戶？
- CPE、數字使用者線路接入複用器(DSLAM)和聚合郵局協定(POP)的部署和調配是什麼？
- 網路訪問提供商(NAP)和網路服務提供商(NSP)是否屬於同一實體？NAP的業務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）？
- NSP是否希望提供服務選擇功能？
- 如何實現會計和計費？它是按使用率、按頻寬還是按服務？
- 公司的業務模式是獨立本地交換運營商(ILEC)、競爭性本地交換運營商(CLEC)還是網際網路服務提供商(ISP)?
- NSP希望為終端使用者提供哪些型別的應用程式？
- 上游和下游的資料流量是什麼？

考慮到這些要點，以下將介紹RFC1483橋接架構如何適應和擴展到不同的業務模式。

網路架構



RFC1483橋接：網路架構

設計注意事項

如前所述，RFC1483橋接架構存在一些固有問題。

IOS使用者橋接功能可以解決其中的一些問題。將使用者策略選擇性應用到網橋組可以控制ARP、未知資料包和其他流量在每個ADSL環路中的泛洪。例如，通過阻止廣播ARP，惡意使用者無法發現其他使用者的IP地址。

另一種解決方案是將所有使用者置於一個子介面中。正常的橋接行為不會將幀轉發到接收幀的埠。實質上，這強制實施一種使用者橋接，其中過濾使用者之間的所有資料包。但是，此方法存在以下缺陷：

- 使用者策略僅在子介面之間應用。要在兩個不同的使用者之間應用使用者策略，每個使用者必須位於不同的ATM子介面中。
- 由於獲知了第2層到第3層地址對映（通過ARP），惡意使用者仍然可以劫持其他使用者的連線。這是通過使用其他使用者的IP地址和使用其他MAC地址來生成ARP流量來實現的。

對於運營商或ISP而言，第二種情況更為嚴重。在這種情況下，任何使用者都可能將錯誤的地址分配給PC或乙太網連線的裝置（如印表機），並導致其他使用者的連線問題。此類錯誤或攻擊很難查明和糾正，因為只有跟蹤犯罪人的MAC地址才能跟蹤犯罪人。

一些運營商試圖通過跨網橋組隔離使用者以及跨子介面實施使用者橋接來解決此問題。在這種情況

下，當需要整合路由和橋接(IRB)時，會為每個使用者分配一個唯一的網橋組和網橋組虛擬介面(BVI)。 此方法每個使用者使用兩個介面，管理起來非常困難。

在Cisco 6400上的Cisco IOS®軟體版本12.0(5)DC中引入的路由橋接封裝(RBE)功能能夠以某些方式解決和解決這些問題。

考慮到橋接的一些缺點，您可能想知道為什麼會實施橋接架構。答案很簡單。現場安裝的大多數ADSL CPE只能轉發橋接幀。在這些情況下，NSP必須實施橋接。

如今，CPE可以通過ATM進行點對點協定(PPPoA)、RFC1483橋接和RFC1483路由。NSP確定是執行橋接還是PPP。除每個架構的利弊之外，該決策還基於前面提到的實施注意事項。

即使有橋接架構的缺點，它也可能適用於小型ISP（可能不是NAP）或服務較少使用者的NAP/NSP。在這些情況下，NAP通常會將所有使用者流量轉發到ISP/NSP，ISP/NSP將終止這些使用者。NAP可以選擇使用ATM或幀中繼作為第2層協定來提供使用者流量。

使用當前代DSLAM的NAP只能使用ATM傳輸使用者流量。在這種情況下，ISP應將ATM永久虛擬電路(PVC)端接到路由器。

如果ISP/NSP沒有ATM介面，可以使用封裝了ATM資料交換介面(DXI)的常規串列介面（可能位於其它裝置上）來接受傳入橋接PDU。

在這兩種情況下，NSP/ISP都可能需要在路由器上配置IRB（使用封裝ATM DXI或透明橋接時除外）。 如今，在NSP/ISP路由器上終止橋接使用者的最常見做法是實施IRB。（預計服務提供商將逐步遷移到RBE。）

由於上述某些限制，NSP/ISP可以選擇為每組使用者配置單獨的網橋組，或者在一個網橋組中配置所有使用者。常見的做法是配置幾個網橋組，然後在單獨的多點介面下配置所有使用者。如前所述，同一多點介面下的使用者可能無法相互通訊。如果某些使用者需要通訊，請在不同的介面下配置這些使用者（它們仍然可以位於同一個網橋組中）。

對於小型ISP/NSP，用於終止橋接使用者的最常見路由器是Cisco 3810、Cisco 3600和Cisco 7200。對於擁有大型使用者群的ISP/NSP，首選思科6400。在計算這些路由器的記憶體要求之前，請考慮與任何其他環境相同的因素：使用者數量、頻寬和路由器資源。

此架構的要點

以下是體系結構的要點。

CPE

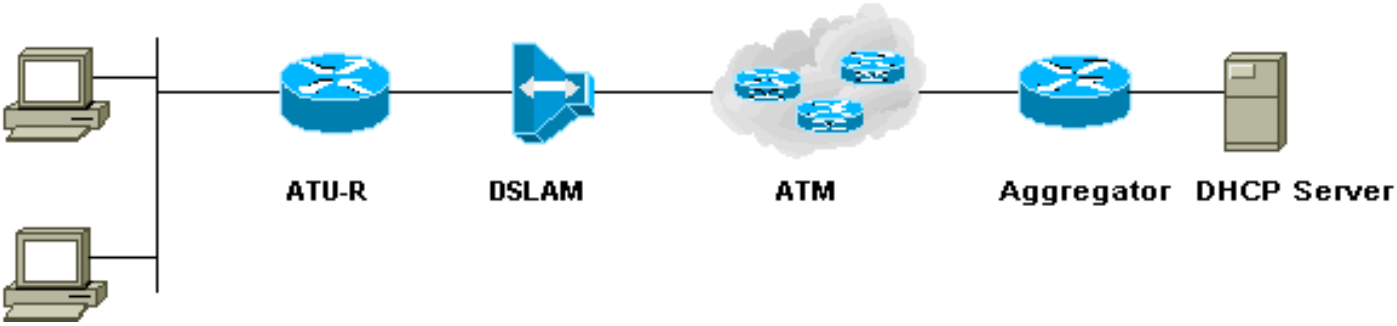
思科提供可與思科和非思科DSLAM一起運行的各種CPE。這些CPE中的每一個配置都是無問題的，不需要使用者輸入。主要要求是CPE定義ATM虛擬路徑識別符號/虛擬通道識別符號(VPI/VCI)。這允許CPE通過DSLAM進行培訓並開始傳遞流量。在大多數情況下，NAP會選擇為所有使用者配置相同的VPI/VCI。NAP通常會在將CPE部署到使用者位置之前預先調配CPE。

在橋接架構中，CPE及其部署的主要考慮因素是NAP在現場安裝CPE後將如何對其進行管理。這是一個問題，因為橋接不需要CPE的IP地址。但是，可以在橋接模式下為Cisco CPE設定IP地址。NAP可以使用此功能Telnet至CPE以收集統計資訊或幫助使用者進行故障排除。為了允許通過DSLAM管理CPE，正在新增新的代理元素功能。

在橋接模式下，如果沒有為CPE分配管理IP地址，則運營商只能通過CPE管理埠管理CPE。如果分配了管理IP地址，操作員可以使用超文本傳輸協定(HTTP)瀏覽器來管理裝置。但是，此選項通常不可用。

當CPE處於橋接模式時，服務目標（可能是NSP/ISP）應提供一個IP地址，該地址將用作CPE後面的PC的預設網關。這些PC必須設定為正確的預設網關。否則，即使數據機經過培訓（這意味著CPE和DSLAM之間的物理層良好），使用者也可能無法傳遞流量。如果使用動態主機配置協定(DHCP)分配使用者DHCP地址，則這不是問題，因為DHCP伺服器返回了預設路由器。

IP管理



RFC1483橋接：IP管理

在橋接環境中，IP地址由位於服務目標（通常位於NSP/ISP網路中）的DHCP伺服器分配給終端站。這是最常見的方法，大多數使用此模型的NSP/ISP都實施了該方法。

另一種方法是向使用者提供靜態IP地址。在這種情況下，根據使用者要求，為每個使用者分配IP地址子網或單個IP地址。例如，想要託管Web伺服器或電子郵件伺服器的使用者需要一組IP地址，而不是一個IP地址。問題在於NSP/ISP必須提供公有IP地址，這些地址可能很快就會耗盡。

有些NSP/ISP已經為其使用者提供私有IP地址。然後在服務目的地路由器上執行網路地址轉換(NAT)。

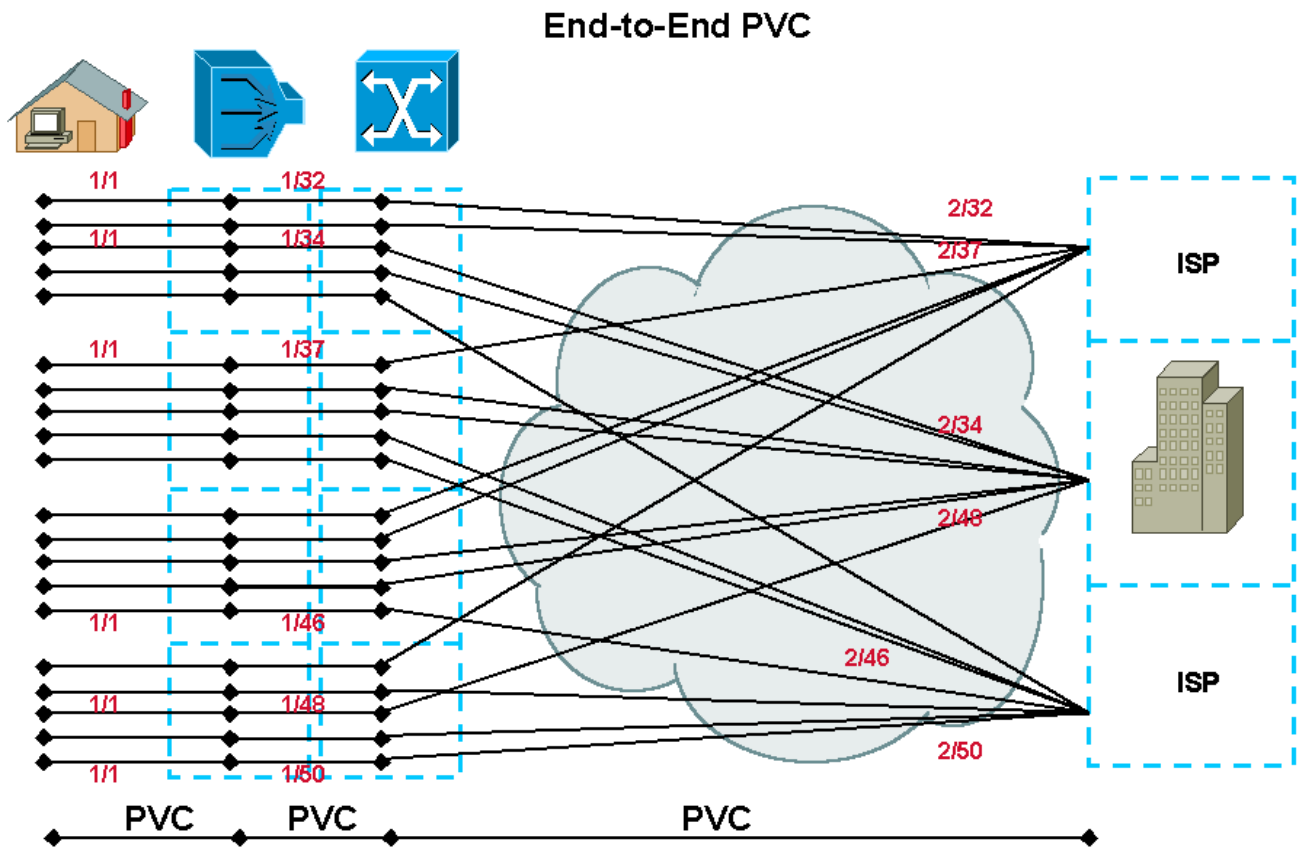
為一個網橋組（有多個使用者）提供完整子網的NSP/ISP應知道一個使用者可以將錯誤的地址分配給PC或乙太網連線的裝置（如印表機），並造成另一個使用者的連線問題。

NSP/ISP還可以限制可以同時訪問服務的PC數量。這是通過在乙太網介面上配置最大使用者數完成的。

但是，此方法具有以下缺陷。如果三台PC配置為使用該服務，並且其中一台訂戶在一台PC空閒時新增一台網路印表機（它有自己的MAC地址），則該PC的MAC地址將從CPE的ARP條目中消失。

如果PC空閒時印表機變為活動狀態，則印表機的MAC地址將輸入到ARP條目中。當使用者決定使用此PC訪問Internet時，它將不可用，因為CPE已允許三個MAC條目。可以使用CPE上的限制使用者策略，但應小心調整數量。

如何到達服務目的地



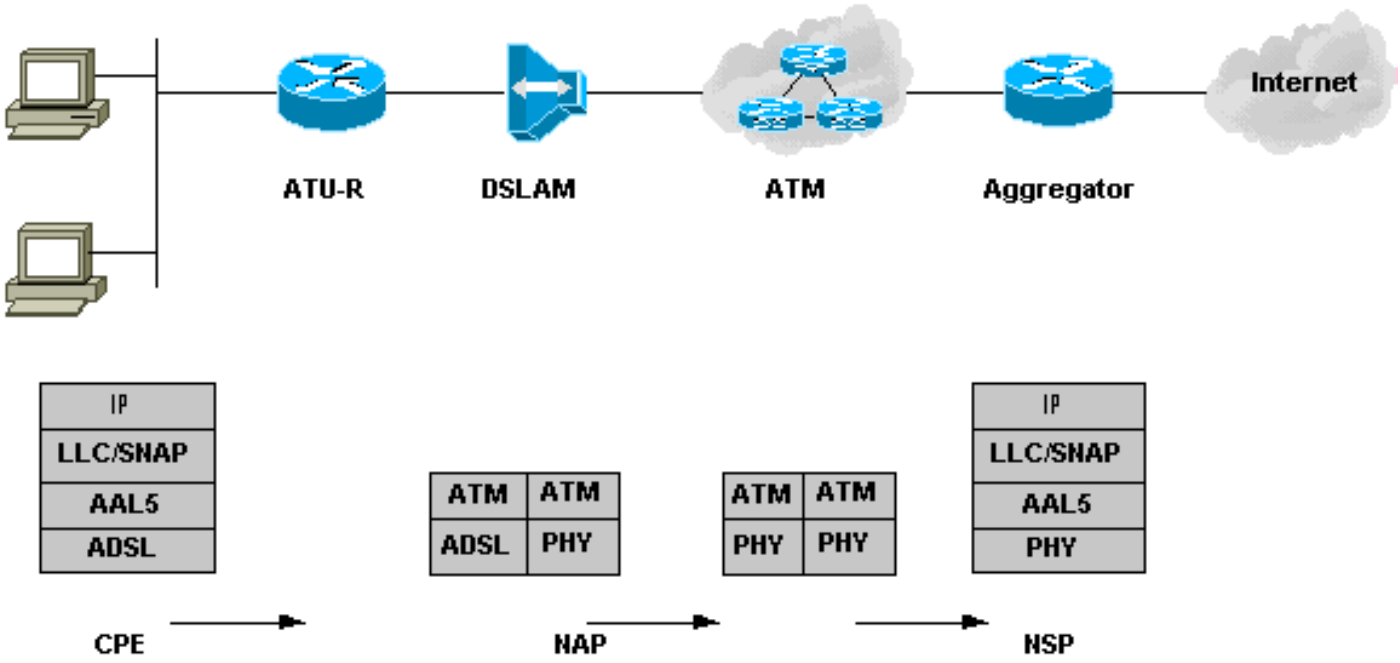
RFC1483橋接：端到端PVC

在具有橋接的端到端PVC架構中，服務目的地可以通過在每個躍點之間建立PVC來實現。但是，這些永久氯乙烯的管理對於國家行動方案/國家戰略計畫來說可能具有挑戰性。此外，可通過ATM雲定義的PVC的數量也有限。此限制會影響採用端到端PVC模型的許多NAP/NSP。對於每個使用者，在整個路徑上都將有一組固定、唯一的VPI/VCI。交換虛擬電路(SVC)有助於克服其中一些問題，許多接入提供商正在遷移到支援IP的核心網路，以解決VC耗盡的問題。

NSP/ISP還可以選擇使用思科服務選擇網關(SSG)功能向使用者提供不同的服務。

在此架構中，通過在第2層的公司路由器中直接終止使用者流量PVC來實現對企業網關的安全訪問。當與其他服務目標共用資料時，基於PVC的架構本身是安全的。

操作說明



RFC1483橋接：操作說明

Cisco 6xx CPE預設為路由模式。因此，當它被配置為橋接模式並安裝在使用者的位置上並安裝必要的分路器/微濾波器時，它會在通電時自動啟動。當CPE啟動時，表明CPE和DSLAM之間的物理層正常。根據終端站的IP地址配置方式（即它是通過DHCP伺服器分配的，還是具有預設網關資訊的靜態IP地址），終端站即可與服務目的地通訊。

以下是資料包流的說明。

使用者的資料從PC封裝在IEEE 802.3中，進入Cisco 6xx CPE。接著將其封裝到邏輯連結控制/子網路存取通訊協定(LLC/SNAP)標頭中，該標頭接著被封裝在ATM適配層5(AAL5)中並傳遞到ATM層。

ATM信元然後通過ADSL傳輸技術、無載波幅度和相位(CAP)調制或離散多音(DMT)進行調制，並通過線路傳送到DSLAM。在DSLAM時，首先由POTS分離器接收這些調制訊號，以檢查訊號的頻率是否低於或高於4 kHz。識別出訊號高於4 kHz後，會將其傳送到DSLAM中的ADSL傳輸單元 — 中央辦公室(ATU-C)。

ATU-C解調訊號並檢索ATM信元，然後將其傳送到複用裝置(MUX)中的網路介面卡(NIC)。 NIC檢視ATM報頭中的使用者端VPI/VCI資訊，並對將要轉發到服務目的地路由器的另一個VPI/VCI做出交換決策。服務目的地路由器在特定的ATM介面上收到這些信元後，會將其重組、檢視上層並將資訊傳遞到BVI介面。BVI介面檢視第3層資訊並決定資料包的傳送位置。

結論

RFC1483橋接模式更適合於可擴充性沒有問題的較小ISP或企業訪問。因為它的理解和實施非常簡單，所以它已成為許多小型ISP的選擇。但是，由於一些安全性和可擴充性問題，橋接架構正在失去其普及性。NSP/ISP選擇RBE或向PPPoA或PPPoE發展，這些產品具有高度可擴充性和非常安全，但更複雜，更難實施。

相關資訊

- DSL技術支援

- 技術支援 - Cisco Systems