瞭解VPDN

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[IPS簽名提示](#)
[VPDN流程概述](#)
[通道通訊協定](#)
[配置VPDN](#)
[相關資訊](#)

簡介

虛擬專用撥號網路(VPDN)允許專用網路撥入服務跨接至遠端訪問伺服器（定義為L2TP訪問集中器[LAC]）。

當點對點通訊協定(PPP)使用者端撥入LAC時，LAC判斷它應該將該PPP作業階段轉送到該使用者端的L2TP網路伺服器(LNS)。然後，LNS對使用者進行身份驗證並啟動PPP協商。PPP設定完成後，所有幀都通過LAC傳送到客戶端和LNS。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

慣例

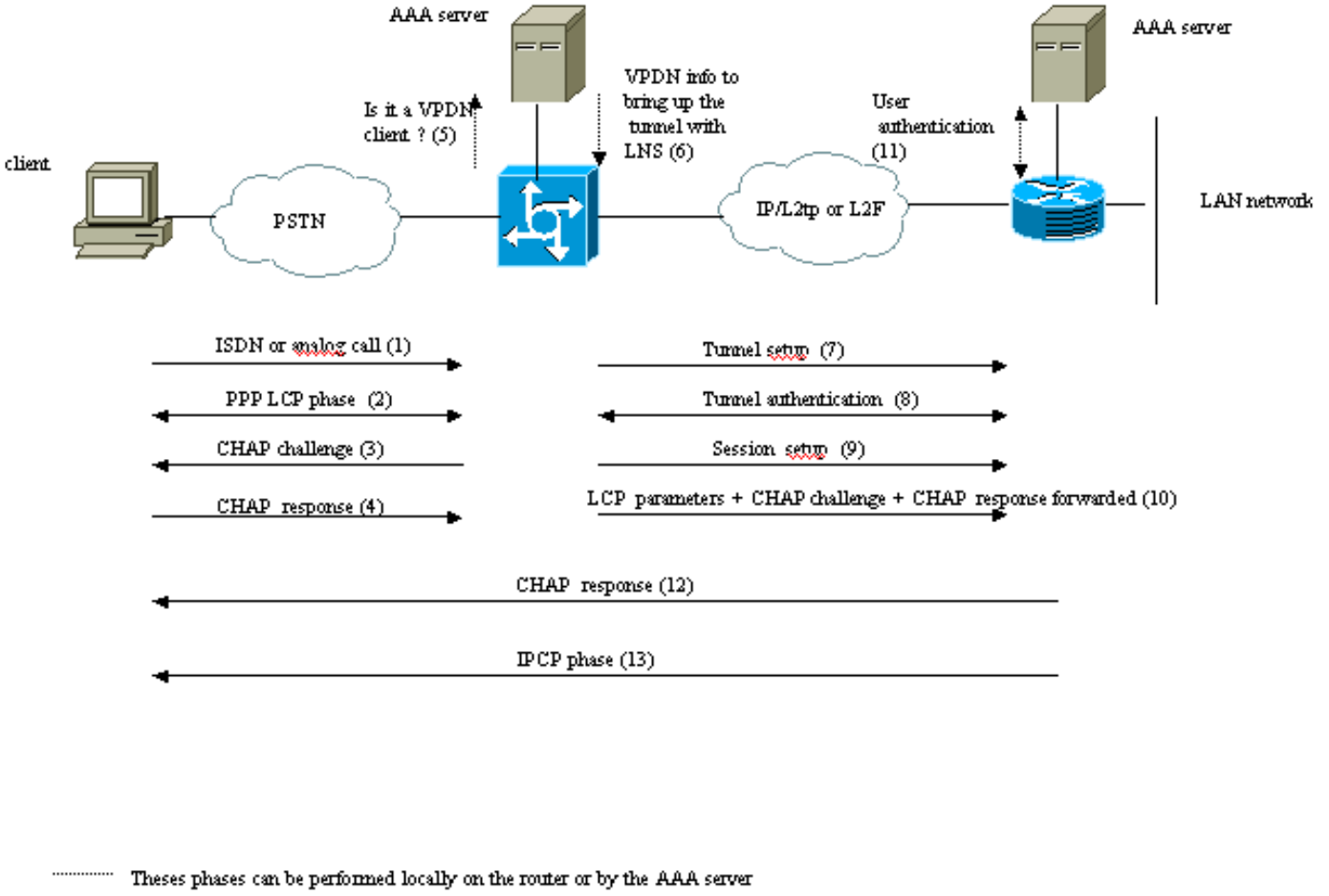
如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

IPS簽名提示

- **客戶端**：連線到遠端訪問網路（呼叫發起方）的PC或路由器。
- **L2TP**:第2層通道通訊協定。PPP定義了在第2層(L2)點對點連結中傳輸多通訊協定封包的封裝機制。通常，使用者使用諸如撥號普通舊式電話服務(POTS)、ISDN或非對稱數字使用者線路(ADSL)等技術來獲得到網路接入伺服器(NAS)的L2連線。 然後，使用者通過該連線運行PPP。在這樣的配置中，第2層終端點和PPP會話終端駐留在同一物理裝置(NAS)上。L2TP通過允許L2和PPP終端駐留在由網路互連的不同裝置上，來擴展PPP模型。使用L2TP時，使用者與訪問集中器建立L2連線，然後集中器將單個PPP幀隧道連線到NAS。這允許將PPP資料包的實際處理與L2電路的終止分離。
- **L2F**:第2層轉發協定。L2F是比L2TP更舊的隧道協定。
- **LAC**:L2TP訪問集中器。充當L2TP隧道端點的一方並且是LNS對等點的節點。LAC位於LNS和客戶端之間，將資料包轉發到每個客戶端或從每個客戶端轉發資料包。從LAC傳送到LNS的資料包需要使用L2TP協定進行隧道傳輸。從LAC到客戶端的連線通常通過ISDN或模擬連線。
- **LNS**:L2TP網路伺服器。充當L2TP隧道端點的一方並且是LAC對等體的節點。LNS是通過LAC從客戶端通過隧道傳輸的PPP會話的邏輯終止點。
- **家庭網關**:定義與L2F術語中的LNS相同。
- **NAS**:定義與L2F術語中的LAC相同。
- **通道**:在L2TP術語中，LAC-LNS對之間存在隧道。隧道包含控制連線和零個或多個L2TP會話。隧道在LAC和LNS之間傳輸封裝的PPP資料包和控制消息。L2F的流程相同。
- **會話**:L2TP是面向連線的。LNS和LAC為LAC發起或應答的每個呼叫保持狀態。當在客戶端和LNS之間建立端到端PPP連線時，在LAC和LNS之間建立L2TP會話。與PPP連線相關的資料包通過LAC和LNS之間的隧道傳送。已建立的L2TP會話與其關聯呼叫之間存在一對一關係。L2F的流程相同。

VPDN流程概述

在下面的VPDN過程描述中，我們使用L2TP術語（LAC和LNS）。



1. 客戶端呼叫LAC（通常使用數據機或ISDN卡）。
2. 客戶端和LAC通過協商LCP選項（身份驗證方法密碼身份驗證協定[PAP]或質詢握手身份驗證協定[CHAP]、PPP多鏈路、壓縮等）來啟動PPP階段。
3. 假設已在步驟2中協商CHAP。LAC向客戶端傳送CHAP質詢。
4. LAC收到響應(例如username@DomainName和密碼)。
5. LAC根據CHAP響應中接收的域名或ISDN設定消息中接收的撥號號碼資訊服務(DNIS)，檢查客戶端是否為VPDN使用者。它通過使用本地VPDN配置或聯絡身份驗證、授權和記帳(AAA)伺服器來完成此操作。
6. 由於使用者端是VPDN使用者，LAC會取得一些資訊（來自其本地VPDN組態或AAA伺服器），用來開啟與LNS的L2TP或L2F通道。
7. LAC與LNS建立L2TP或L2F隧道。
8. 根據從LAC的請求中收到的名稱，LNS檢查是否允許LAC開啟隧道（LNS檢查其本地VPDN配置）。 此外，LAC和LNS相互進行身份驗證（它們使用其本地資料庫或聯絡AAA伺服器）。接著兩台裝置之間的通道都已啟動。在此通道中，可傳輸多個VPDN作業階段。
9. 對於客戶端username@DomainName，從LAC到LNS觸發VPDN會話。每個客戶端有一個VPDN會話。
10. LAC轉發與客戶端協商的LCP選項以及從客戶端接收的username@DomainName和密碼。
11. LNS從VPDN配置中指定的虛擬模板克隆虛擬訪問。LNS獲取從LAC接收的LCP選項，並在本地或通過聯絡AAA伺服器對客戶端進行身份驗證。
12. LNS向客戶端傳送CHAP響應。
13. 會執行IP控制通訊協定(IPCP)階段，然後安裝路由：客戶端和LNS之間的PPP會話已啟動並正在運行。LAC僅轉發PPP幀。PPP幀在LAC和LNS之間通過隧道傳輸。

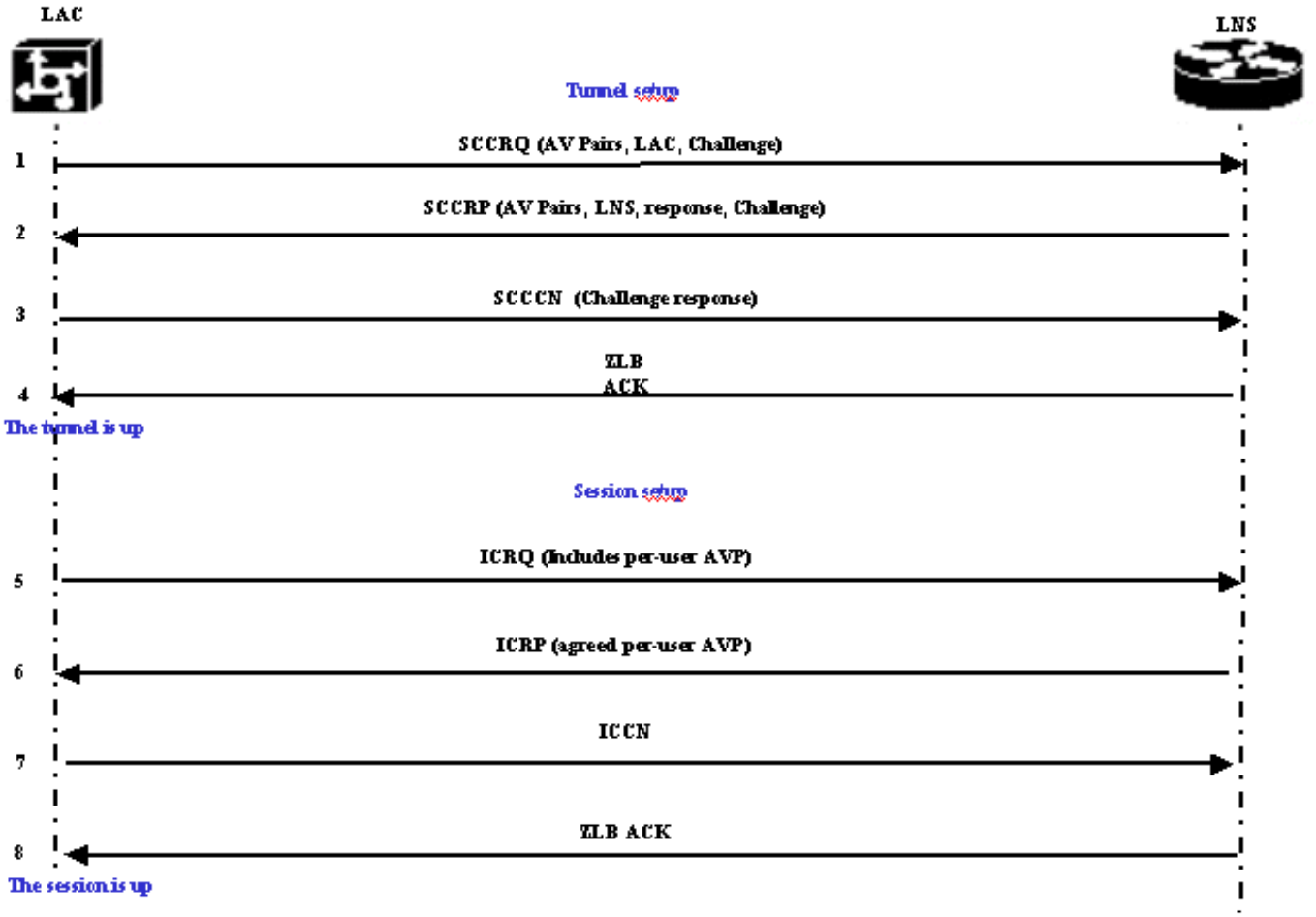
通道通訊協定

VPDN通道可以使用第2層轉送(L2F)或第2層通道通訊協定(L2TP)建立。

- L2F是由思科在要求建議(RFC)2341中匯入，也用於轉送多機箱多重連結PPP的PPP作業階段。
- RFC 2661中引入的L2TP結合了思科L2F協定和Microsoft點對點隧道協定(PPTP)的最佳組合。此外，L2F僅支援撥入VPDN，而L2TP同時支援撥入和撥出VPDN。

這兩種協定都使用UDP埠1701通過IP網路構建隧道來轉發鏈路層幀。對於L2TP，對PPP會話建立隧道的設定包括兩個步驟：

1. 在LAC和LNS之間建立隧道。只有在兩台裝置之間沒有活動隧道時，才會發生此階段。
2. 在LAC和LNS之間建立會話。



LAC決定必須啟動從LAC到LNS的隧道。

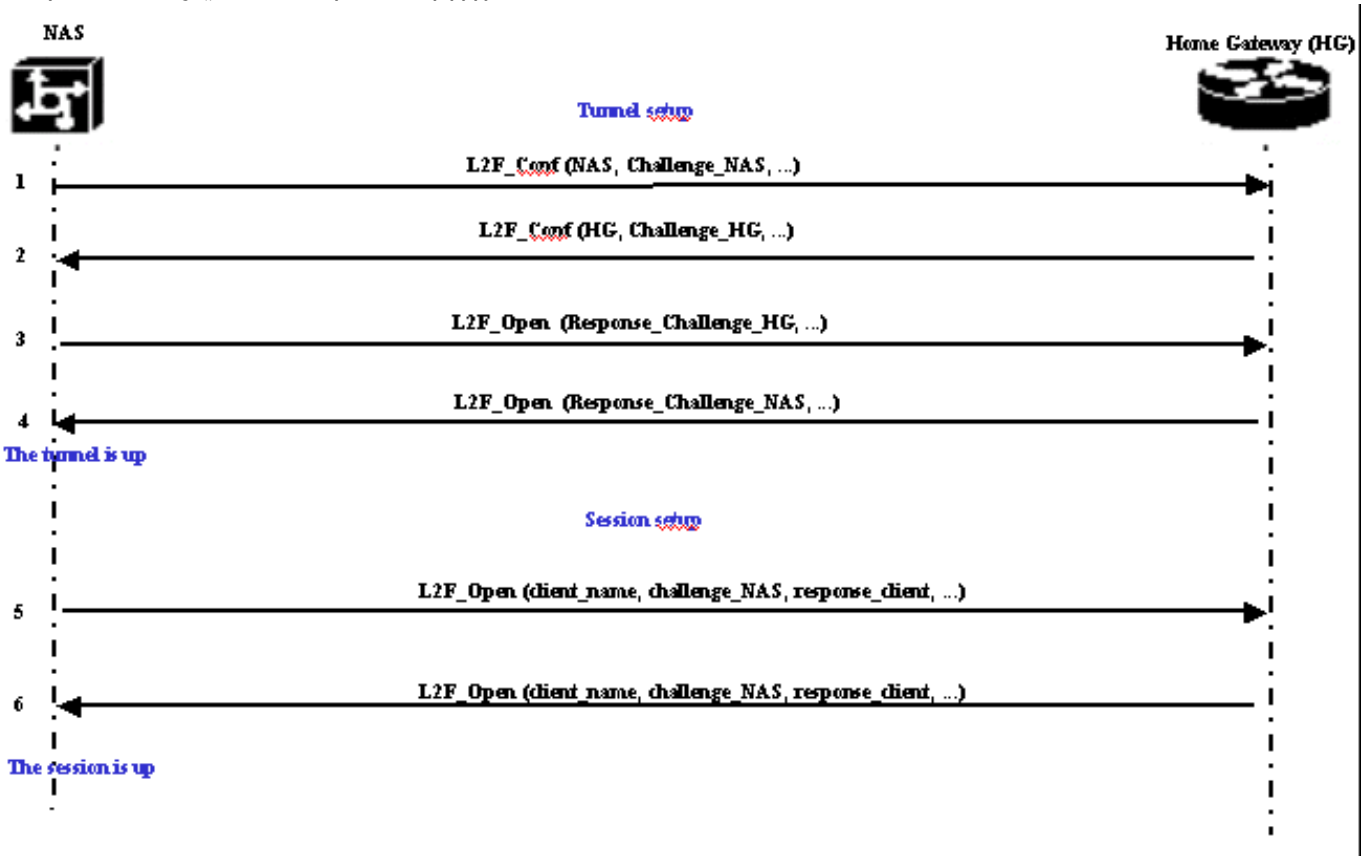
1. LAC傳送Start-Control-Connection-Request(SCCRQ)。此消息中包括CHAP質詢和AV配對。
2. LNS使用Start-Control-Connection-Reply(SCCRP)進行響應。CHAP質詢、對LAC質詢的響應以及AV對包含在此消息中。
3. LAC會傳送一個Start-Control-Connection-Connected(SCCN)。 CHAP響應包含在此消息中。
4. LNS使用零長度正文確認(ZLB ACK)進行響應。 該確認可以在另一消息中攜帶。隧道已開啟。
5. LAC向LNS傳送傳入呼叫請求(ICRQ)。
6. LNS使用傳入呼叫應答(ICRP)消息進行響應。
7. LAC會傳送傳入呼叫已連線(ICCN)。
8. LNS使用ZLB ACK進行響應。該確認也可以攜帶在另一消息中。
9. 會話已啟動。

注意：上述用於開啟隧道或會話的消息攜帶RFC 2661中定義的屬性值對(AVP)。它們描述屬性和資訊（例如Bearercap、主機名、供應商名稱和視窗大小）。 某些AV對是強制性的，其它則是可選的。

註：通道ID用於在LAC和LNS之間多路複用和解多路複用隧道。作業階段ID用於識別與通道的特定作業階段。

對於L2F，對PPP會話建立隧道的設定與L2TP相同。它包括：

1. 在NAS和家庭網關之間建立隧道。只有在兩台裝置之間沒有活動隧道時，才會發生此階段。
2. 在NAS和家庭網關之間建立會話。



NAS決定必須從NAS啟動到家庭網關的隧道。

1. NAS向家庭網關傳送L2F_Conf。CHAP質詢包含在此消息中。
2. 家庭網關以L2F_Conf響應。CHAP質詢包含在此消息中。
3. NAS傳送L2F_Open。此消息中包含家庭網關質詢的CHAP響應。
4. 家庭網關使用L2F_Open進行響應。NAS質詢的CHAP響應包含在此消息中。隧道已開啟。
5. NAS向家庭網關傳送L2F_Open。資料包包括客戶端的使用者名稱(client_name)、NAS傳送到客戶端的CHAP質詢(challenge_NAS)及其響應(response_client)。
6. 家庭網關通過回送L2F_OPEN來接受客戶端。現在流量可在客戶端和家庭網關之間自由地沿任一方向流動。

注意：隧道用CLID（客戶端ID）標識。 多工ID(MID)用於識別通道中的特定連線。

配置VPDN

有關配置VPDN的資訊，請參閱配置虛擬專用網路手冊，並轉至配置VPN一節。

相關資訊

- 撥號和存取技術支援頁面
- 技術支援與文件 - Cisco Systems