了解 VPDN

目录

简介

使用虚拟专用拨号网络 (VPDN) 可以将服务中的专用网络拨号分布到远程接入服务器（定义为 L2TP 接入集中器 [LAC]）。

当一个点对点协议 (PPP) 客户端拨入 LAC 时，LAC 将确定是否应将该 PPP 会话继续转发到该客户端的 L2TP 网络服务器 (LNS)。然后，LNS 将对该用户进行身份验证并启动 PPP 协商。完成 PPP 设置后，所有帧都将通过 LAC 发送到客户端和 LNS。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

规则

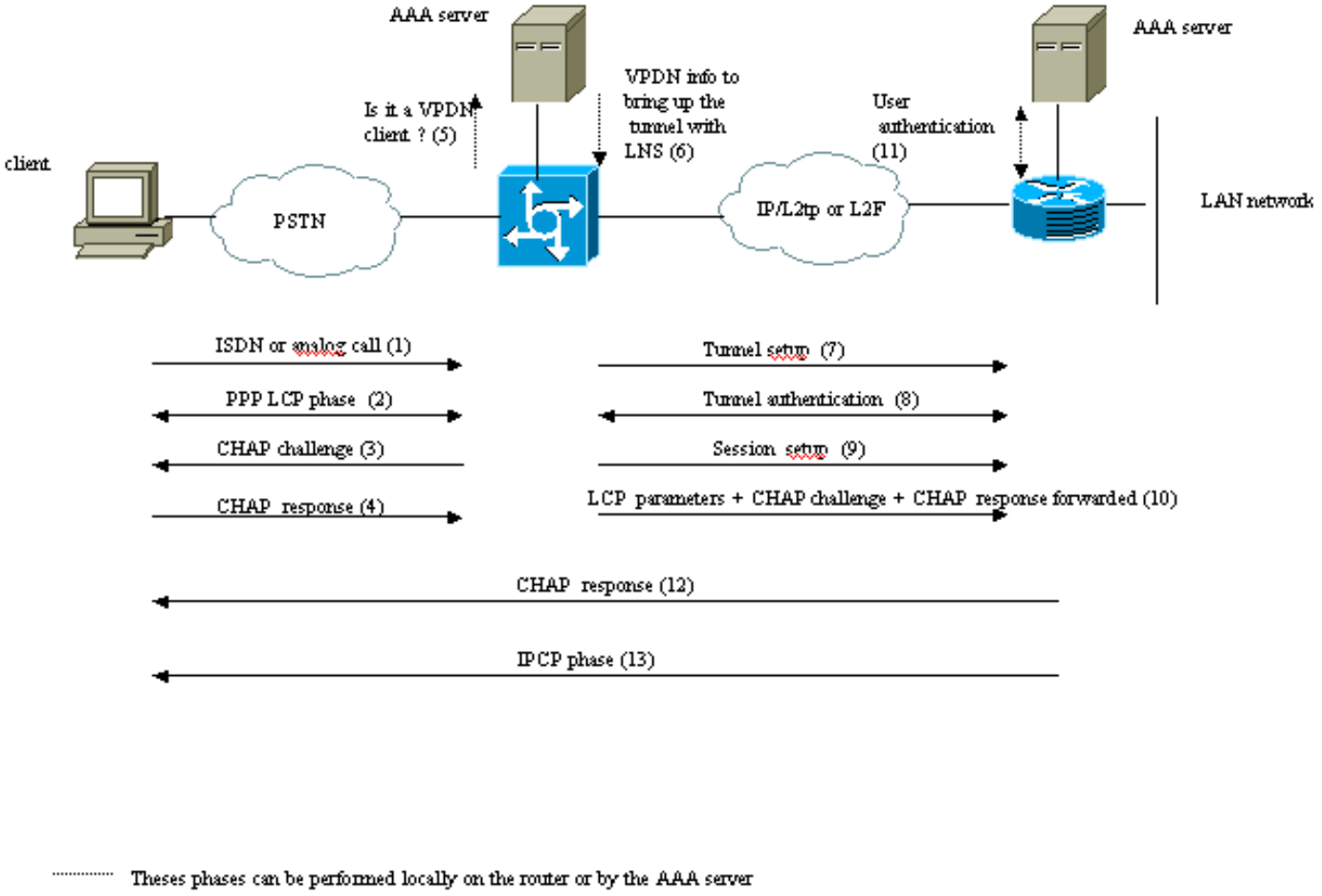
有关文件规则的更多信息请参见“ Cisco技术提示规则”。

词汇表

- **客户端**：与远程访问网络相连并且作为呼叫的发起者的 PC 或路由器。
- **L2TP**:第二层隧道协议。PPP 定义用于跨越第二层 (L2) 点对点链路传输多协议数据包的封装机制。通常，用户使用拨号普通老式电话服务 (POTS)、ISDN 或非对称数字用户线 (ADSL) 等技术获取与网络接入服务器 (NAS) 的 L2 连接。 然后，用户通过该连接运行 PPP。在此类配置中，L2 终结点和 PPP 会话终点位于相同物理设备 (NAS) 中。L2TP 通过允许 L2 和 PPP 终点位于通过网络互连的不同设备上来扩展 PPP 模型。使用 L2TP，用户可以通过 L2 连接到接入集中器，然后该集中器在各个 PPP 帧与 NAS 之间建立隧道。这使得 PPP 数据包的实际处理可以与 L2 电路的终止分开。
- **L2F**:第 2 层转发协议。L2F 是早于 L2TP 的隧道协议。
- **LAC**:L2TP访问集中器。充当 L2TP 隧道终点的一端并且与 LNS 对等的一个节点。LAC 位于 LNS 与客户端之间，用于在二者之间转发数据包。从 LAC 发送到 LNS 的数据包要求使用 L2TP 协议建立隧道。从 LAC 到客户端的连接通常通过 ISDN 或模拟线路进行。
- **LNS**:L2TP网络服务器。充当 L2TP 隧道终点的一端并且与 LAC 对等的一个节点。LNS 是要通过 LAC 从客户端建立隧道的 PPP 会话的终结点。
- **Home Gateway**（家庭网关）：与 L2F 术语中 LNS 的定义相同。
- **NAS**:与 L2F 术语中 LAC 的定义相同。
- **隧道**:在 L2TP 术语中，隧道存在于 LAC-LNS 对之间。隧道包含一个控制连接和零个或多个 L2TP 会话。隧道在 LAC 和 LNS 之间传输封装的 PPP 数据报和控制消息。L2F 也执行此相同过程。
- **会话**:L2TP 是面向连接的。LNS 和 LAC 维护通过 LAC 发起或应答的每次呼叫的状态。当在客户端与 LNS 之间建立端对端 PPP 连接时，将在 LAC 与 LNS 之间创建 L2TP 会话。与 PPP 连接相关的数据报将通过 LAC 与 LNS 之间的隧道发送。已建立的 L2TP 会话与其关联呼叫之间存在一对一关系。L2F 也执行此相同过程。

VPDN 进程概述

在下面的 VPDN 过程的说明中，将使用 L2TP 术语（LAC 和 LNS）。



1. 客户端呼叫 LAC（通常使用调制解调器或 ISDN 卡）。
2. 客户端和 LAC 通过协商 LCP 选项（身份验证方法口令身份验证协议 [PAP] 或质询握手身份验证协议 [CHAP]、PPP 多链路、压缩等）启动 PPP 阶段。
3. 假设已在步骤2中协商CHAP。LAC向客户端发送CHAP质询。
4. LAC 获取响应（例如，username@DomainName 和口令）。
5. 基于 CHAP 响应中收到的域名或 ISDN 设置消息中收到的拨号信息服务 (DNIS)，LAC 将确认客户端是否为 VPDN 用户。执行该操作的方法是使用其本地 VPDN 配置或联系身份验证、授权和记帐 (AAA) 服务器。
6. 由于客户端为 VPDN 用户，因此 LAC 将获取用于通过 LNS 启动 L2TP 或 L2F 隧道的信息（从其本地 VPDN 配置或 AAA 服务器中）。
7. LAC 通过 LNS 启动 L2TP 或 L2F 隧道。
8. 基于请求中从 LAC 收到的名称，LNS 将确认是否允许 LAC 建立隧道（LNS 检查其本地 VPDN 配置）。 此外，LAC 和 LNS 将彼此进行身份验证（它们使用其本地数据库或联系 AAA 服务器）。 然后，将在两个设备之间建立隧道。在该隧道中，可以传输多个 VPDN 会话。
9. 对于客户端 username@DomainName，将触发从 LAC 到 LNS 的 VPDN 会话。每个客户端存在一个 VPDN 会话。
10. LAC 将已协商的 LCP 选项通过客户端转发到 LNS，同时还转发从客户端收到的 username@DomainName 和口令。
11. LNS 克隆 VPDN 配置中指定的虚拟模板中的虚拟访问。LNS 接受从 LAC 收到的 LCP 选项并在本地或通过联系 AAA 服务器对客户端进行身份验证。
12. LNS 将 CHAP 响应发送到客户端。
13. 将执行 IP 控制协议 (IPCP) 阶段，然后安装路由：PPP 会话将在客户端与 LNS 之间启动并运行。LAC 仅转发 PPP 帧。将在 LAC 与 LNS 之间建立隧道以传输 PPP 帧。

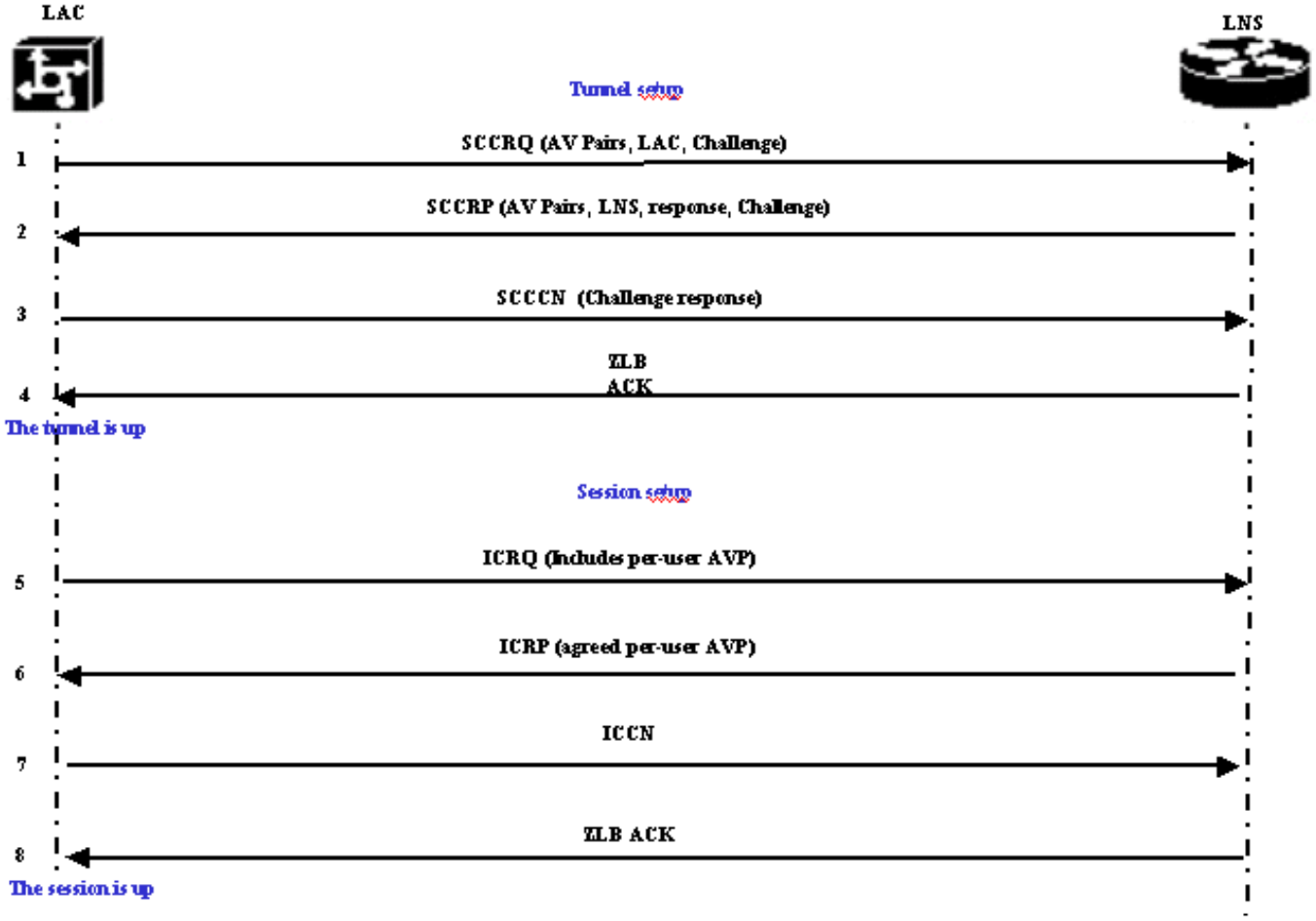
隧道协议

可以使用第 2 层转发 (L2F) 或第 2 层隧道协议 (L2TP) 建立 VPDN 隧道。

- L2F 由 Cisco 在请求注解 (RFC) 2341 中引入，也用于转发多机箱多链路 PPP 的 PPP 会话。
- RFC 2661 中引入的 L2TP 结合了 Cisco L2F 协议和 Microsoft 点对点隧道协议 (PPTP) 的优点。 此外，L2F 仅支持拨入 VPDN，而 L2TP 同时支持拨入和拨出 VPDN。

这两种协议都使用 UDP 端口 1701 通过 IP 网络建立隧道以转发链路层帧。对于 L2TP，建立 PPP 会话隧道的过程包括两步：

1. 在 LAC 与 LNS 之间建立隧道。仅当两个设备之间不存在活动隧道时，才会发生此阶段。
2. 在 LAC 与 LNS 之间建立会话。



LAC 确定必须启动从 LAC 到 LNS 的隧道。

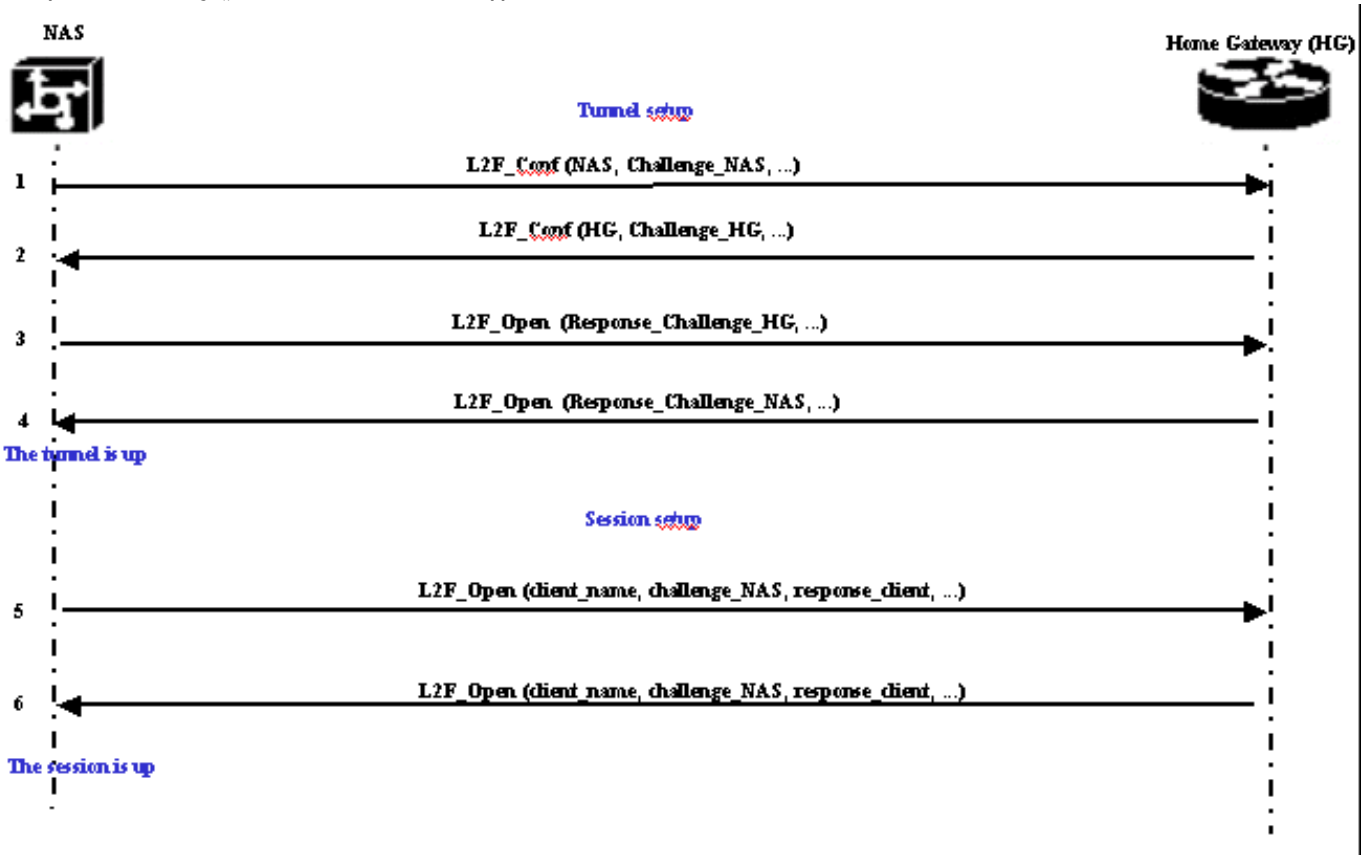
1. LAC 发送 Start-Control-Connection-Request (SCCRQ)。此消息中包括 CHAP 质询和 AV 对。
2. LNS 使用 Start-Control-Connection-Reply (SCCRP) 响应。此消息中包括 CHAP 质询、LAC 的质询的响应和 AV 对。
3. LAC 发送 Start-Control-Connection-Connected (SCCCN)。 此消息中包括 CHAP 响应。
4. LNS 使用零长度正文确认 (ZLB ACK) 响应。 该确认可能通过另一条消息传输。通道已启动。
5. LAC 将传入呼叫请求 (ICRQ) 发送到 LNS。
6. LNS 使用传入呼叫应答 (ICRP) 消息响应。
7. LAC 发送传入呼叫已连接 (ICCN)。
8. LNS 重新使用 ZLB ACK 响应。该确认也可能通过另一条消息传输。
9. 会话已启动。

注意：上述用于打开隧道或会话的消息携带RFC 2661中定义的属性值对(AVP)。这些属性值对描述相应属性和信息（例如，Bearercap、主机名、供应商名称和窗口大小）。 一些 AV 对是必需的，另一些是可选的。

注意：隧道ID用于在LAC和LNS之间多路复用和多路分离隧道。会话 ID 用于确定隧道的特定会话。

对于 L2F，建立 PPP 会话隧道的过程与 L2TP 相同。该过程涉及：

1. 在 NAS 和家庭网关之间建立隧道。仅当两个设备之间不存在活动隧道时，才会发生此阶段。
2. 在 NAS 和家庭网关之间建立会话。



NAS 确定必须启动从 NAS 到家庭网关的隧道。

1. NAS 将 L2F_Conf 发送到家庭网关。此消息中包括 CHAP 质询。
2. 家庭网关使用 L2F_Conf 响应。此消息中包括 CHAP 质询。
3. NAS 发送 L2F_Open。此消息中包括家庭网关质询的 CHAP 响应。
4. 家庭网关使用 L2F_Open 响应。此消息中包括 NAS 质询的 CHAP 响应。通道已启动。
5. NAS 将 L2F_Open 发送到家庭网关。数据包中包括客户端的用户名 (client_name)、由 NAS 发送到客户端的 CHAP 质询 (challenge_NAS) 及其响应 (response_client)。
6. 发送回 L2F_OPEN 的家庭网关接受该客户端。流量现在可以在客户端和家庭网关之间按任意方向流动。

注意：隧道用CLID（客户端ID）标识。 多路复用 ID (MID) 标识隧道中的特定连接。

配置 VPDN

有关配置 VPDN 的信息，请参阅配置虚拟专用网络手册，然后转至有关配置 VPN 的部分。

相关信息

- 拨号和接入技术支持页
- 技术支持和文档 - Cisco Systems