2.2 PPP 协议

PPP（Point-to-Point Protocol）协议为在点到点链路上传输多协议数据报提供了一种标准方法。为了便于使用 Wireshark 进行观察，本实验中重点配置和观察在以太网上运行的 PPP 协议——PPPoE（PPP over Ethernet）。PPPoE 主要被 ISP 用于 xDSL 和 cable modems 与用户端的连接，实现提供用户身份认证、鉴权、计费（即通常提到的 AAA，全称是 authentication, authorization & accounting）和分发 IP 地址等功能。

2.2.1 实验目的

掌握 PPP 协议的原理，理解 PPP 协议的帧结构，了解 PPPoE 连接的 3 个阶段。

2.2.2 协议简介

PPP 协议是一个在点到点链路上的传输控制协议，有用户验证功能。以太网没有用户验证功能，同时以太网是多点网络，所以，不能在以太网上直接使用 PPP 协议。PPPoE 是在标准 PPP 报文的前面加上以太网的帧头，这样就可以在以太网上建立点到点的虚拟连接，该连接上使用 PPP 协议，实现对用户的验证和数据传输。

PPP 协议有 3 个主要的组成部分：

1）封装 PPP 报文的方法。

2）建立、配置和测试数据链路链接的 LCP（Link Control Protocol）协议。

3）建立和配置不同网络层协议的 NCP（Network Control Protocol）协议。

PPP 协议是为能够在对等单元之间传输数据报的简单链路而设计的。这种链路提供全双工操作，并按照顺序传递数据报。PPP 协议主要是为通过广域网或者拨号线连接到 PPP 网络服务器的路由器和主机服务的，也可以被用到专用链路中。PPP 服务器在为网络层磋商选择选项时，可以对连接的主机或路由器进行身份验证。

PPP 协议是一种面向连接的协议，在建连过程中，首先需要基于 LCP 子协议完成对数据链路连接的配置、建连和测试，然后根据 LCP 协商结果，可以基于 PAP 子协议或 CHAP 子协议进行身份认证，最后基于 IPCP 子协议（NCP 协议的一种）完成对 IP 网络层的配置和建连。至此 PPP 连接建立成功，可以开始进行 IP 分组的封装和收发。

PPP 封装提供了不同网络层协议使用统一链路的技术。精心设计的 PPP 封装，硬件兼容性非常好。当使用默认的类 HDLC 帧（HDLC-like framing）时，仅需要 8 个额外的字节，就可以形成封装。为减少占用带宽，帧头部可以减少到 2 或 4 个字节。为了支持高速的执行，默认的封装只使用简单的字段，多路分解只需要对其中的一个字段进行检验。默认的头部和信息字段落在 32-bit 边界上，尾字节可以被填补到任意的边界。

PPP 帧格式如 图 2-1 所示。

字节	1	1	1	2	<=1500	2	1
	标志	地址	控制	协议	净荷	校验和	标志

图 2-1　PPP 帧格式

下面介绍 PPP 帧中的各个字段的含义：

- 标志：标准的 HDLC 标志字节，值为 0x7E。
- 地址：地址域，值为 0xFF，表示所有的站都可以接受该帧。
- 控制：控制域，默认值为 0x03，表明该帧为一个无序号帧。
- 协议：协议域指明净荷域中是哪一种分组，默认为 2 字节，可以协商为 1 字节，以 0 作为开始的协议是网络层协议，以 1 作为开始的协议被用于协商其他的协议。
- 净荷：最大 1500 字节。
- 校验和：净荷域的检验和，默认为 2 字节，可以通过协商变为 4 字节。

PPPoE 的报文格式如图 2-2 所示。需要说明一下，封装 PPPoE 报文的以太网帧中的“类型”字段（参见本章第一小节）在 PPPoE 发现阶段取值为 0x8863，在会话阶段取值为 0x8864。

图 2-2　PPPoE 报文格式

下面介绍 PPPoE 报文各个字段的含义：

- 版本：协议规定取值为 0x01。
- 类型：协议规定取值为 0x01。
- 代码：在 PPPoE 的发现阶段和会话阶段有不同的定义。
- 会话 ID：访问集中器还未分配惟一的会话 ID 给用户主机时，则该域取值为 0x0000，主机获取了会话 ID 后，在后续的所有报文中，该域取值为相应的会话 ID 值。
- 长度：指示 PPPoE 报文中净荷的长度。
- 净荷：在 PPPoE 的发现阶段，该域内会填充一些 Tag（标记），在 PPPoE 的会话阶段，该域携带的是 PPP 的报文。

2.2.3　实验内容

下面将通过实验了解 PPPoE，进而理解 PPP 协议的工作过程。

本次实验不限制实验环境操作系统，只要能配置 PPPoE 协议的 Server/Client 进行连接并抓到报文进行分析即可。

要求：1. 必须使用 CHAP 认证。2. 必须动态协商 IP。

1．搭建 PPPoE 实验环境

我们推荐使用 Linux 搭建 PPPoE 服务器，具体可见下发的 tutorial.pdf。

2．捕捉数据帧分析

在上面搭建好的实验环境下，通过 Wireshark 将实验主机 PC1 的网卡设置为通常模式（非混杂模式），捕捉 PPPoE 在不同阶段的报文。由于 PPPoE 报文中没有 IP 头，所以无需设置捕捉条件，实际中捕捉的报文可能有许多与 PPPoE 无关，所以可以在显示过滤条件中增加 PPP

条件，将无关报文过滤掉。

当用户和接入服务器之间的 PPPoE 连接建立之后，就可以在上面建立 PPP 会话。PPP 会话的建立分为 3 个阶段：LCP 协商、认证和 IPCP 协商。

对于 PPP 终结和 PPP 续传，LCP 协商阶段是相同的，认证和 IPCP 协商阶段则不同。在不同的阶段分别获取不同的 PPPoE 报文。

PPPoE 在发现阶段发送报文的过程如下。

1）当主机 PC1 希望接入 PC2（实际中可能是 ISP 网络）时，发送 PPPoE 发现报文（PADI），报文被封装在以太网帧中并以广播方式在网络上发送，希望发现网络中所有的 PPPoE 服务，PADI 报文如图 2-3 所示。

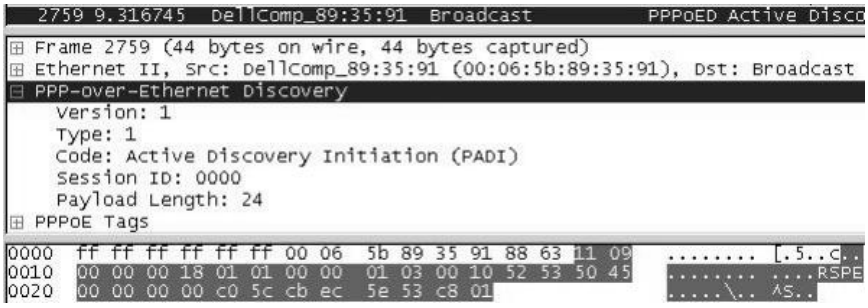

图 2-3　PPPoE-PADI 报文

2）PC2 上的 PPPoE 服务器（实际中可能有多个）向发起发现的主机 PC1 发送给予报文（PADO），PADO 报文如图 2-4 所示。

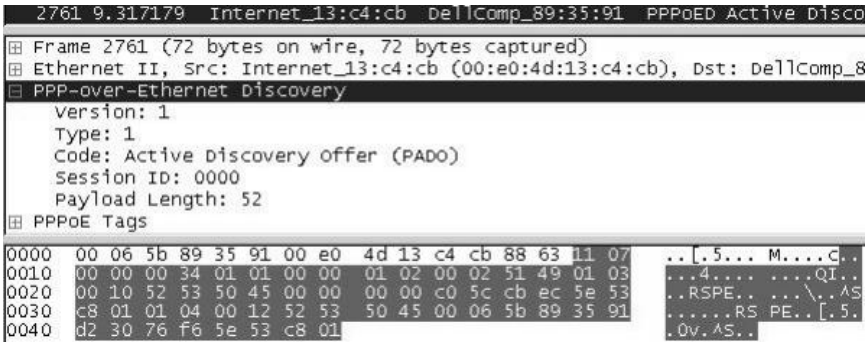

图 2-4　PPPoE-PADO 报文

3）PC1 选择一个 PPPoE 服务器（这里就是 PC2），向 PPPoE 服务器发送单播会话请求报文（PADR），PADR 报文如图 2-5 所示。

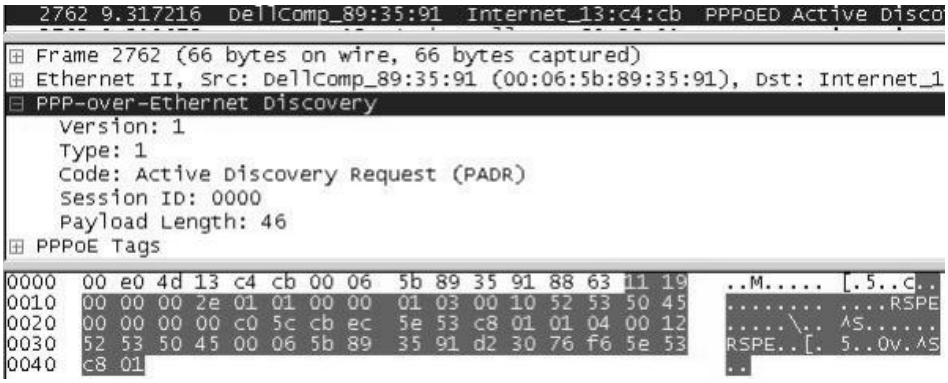

图 2-5　PPPoE-PADR 报文

4）PC2 上的 PPPoE 服务器发送一个确认报文（PADS），为接入主机 PC1 分配一个会话 ID（Session ID），如图 2-6 所示，这里的 Session ID 是 0x001d，主机用这个 ID 作标识传送数据，未获得 ID 时主机将不能传送数据。

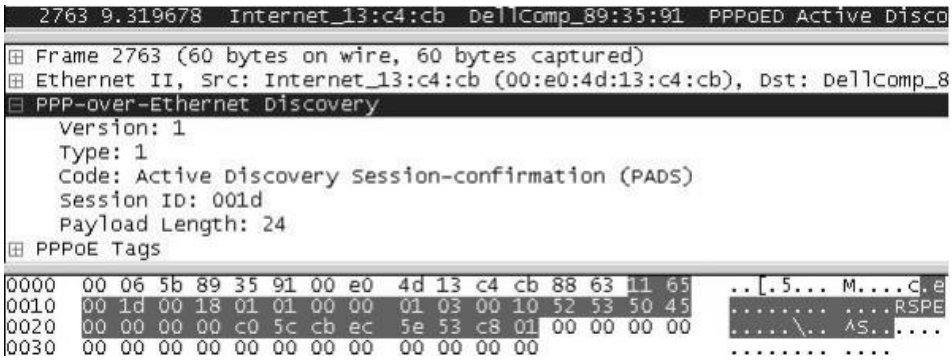

图 2-6　PPPoE-PADS 报文

经过了 PPPoE 发现阶段之后，进入了 PPPoE 会话阶段，也称为 PPP 数据传输阶段。在这个阶段，双方在 PPPoE 逻辑链路上传输 PPP 数据帧。PPP 数据帧封装在 PPPoE 数据报文中，PPPoE 数据报文封装在以太网帧的数据域中传输。在会话阶段，PPP 协议包括链路创建、用户认证和网络协商等阶段。

在 PPP 链路创建阶段，利用 LCP 创建链路。主机 PC1 向 PPPoE 服务器发送配置信息报文，PPPoE 服务器返回配置确认报文，就完成了配置信息交换，PPP 链路建立完成。LCP 报文如图 2-7 所示，这里只给出了配置信息报文，没有给出确认报文。

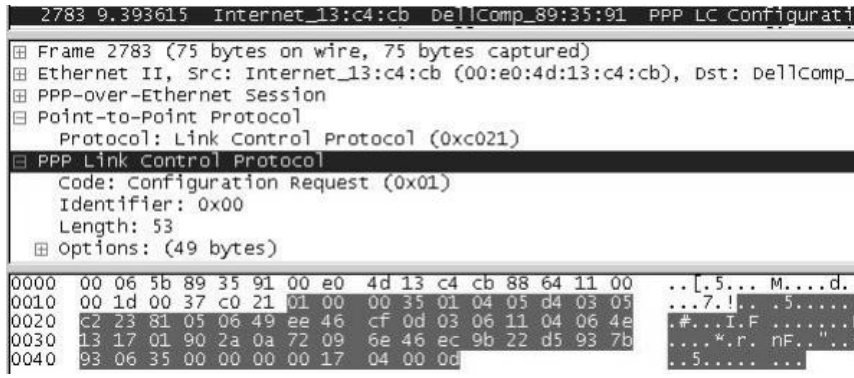

图 2-7 PPP-LCP 报文

用户认证时采用的是挑战握手验证协议（CHAP），报文如图 2-8 所示。

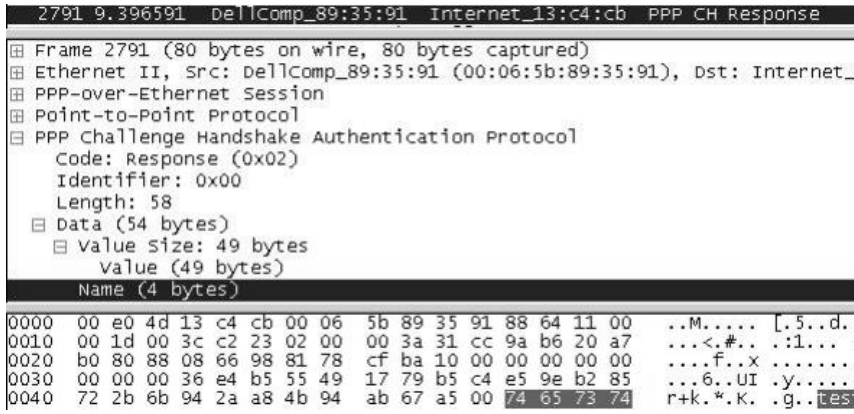

图 2-8 PPP-CHAP 报文

在网络协商阶段 IP 控制协议 (IPCP) 向拨号用户分配动态地址。IPCP 报文如图 2-9 所示。

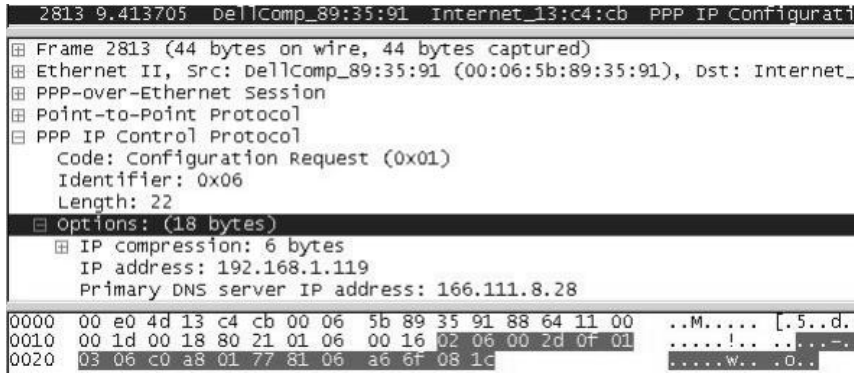

图 2-9 PPP-IPCP 报文

最后数据传输完毕进入 PPPoE 终止阶段。PPPoE 终止报文（PPPoE Active Discovery

Terminate，PADT）可以在会话之后的任意时间内被发送，用来终止一个 PPPoE 会话，由主机或 PPPoE 服务器发送。当收到 PADT 报文时，PPPoE 连接被终止，PPP 数据传输结束。图 2-10 和图 2-11 给出了在终止阶段捕捉的报文。

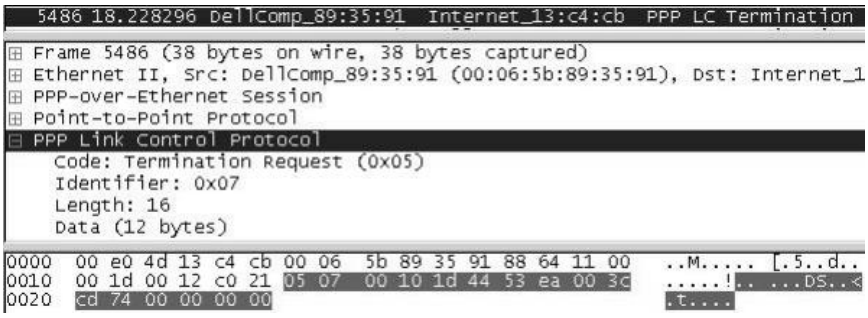

图 2-10　PPP 连接终止报文

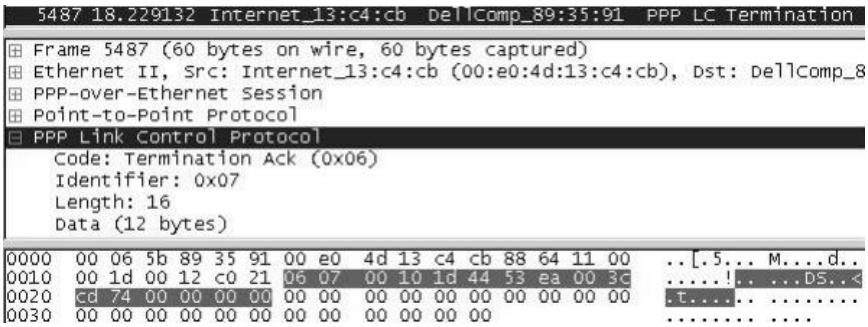

图 2-11　PPP 连接终止确认报文

2.2.4　思考问题

1）给出 Wireshark 捕获的 PADS 报文、PPP-CHAP response 报文、PPP-IPCP request（携带分配后地址的）报文的截图，并指出 PPP-CHAP response 中的加密摘要字段。

2）在通常的以太网（MTU=1500）上，使用 PPPoE 协议传递 UDP 数据报（IP 头不包含可选字段）。每个报文可以携带的上层应用的数据容量至多为多少？解释计算过程。

3）观察捕捉的报文可以发现，用 PPPoE 封装的 PPP 帧头部不包含标志、地址和控制字段，为什么？

4）PPP LCP 协商中的 MRU 值受到哪些因素的影响？

5）查阅相关资料，说明应该如何在 PPPoE 链路上进行 IPv6 协议的配置，并给出涉及到的协议名称、相关 RFC 编号。（本题不止一种方案，言之有理即可）

6）你认为 PPPoE 有哪些优点和缺点？（开放式问题，言之有理即可）