## 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。

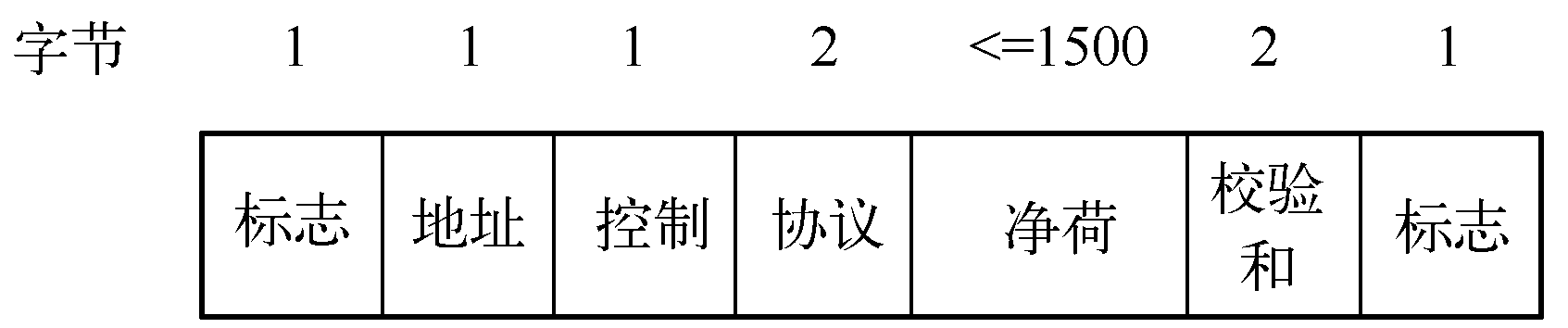


图2-1 PPP帧格式

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。

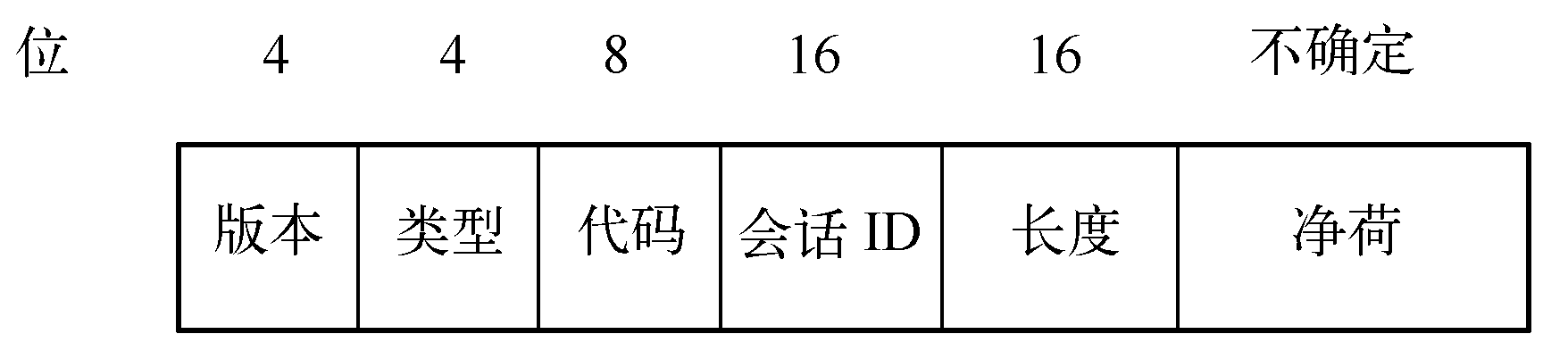


图2-2 PPPoE报文格式

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。

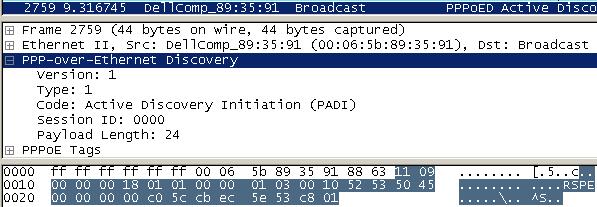


图2-3 PPPoE-PADI报文

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。

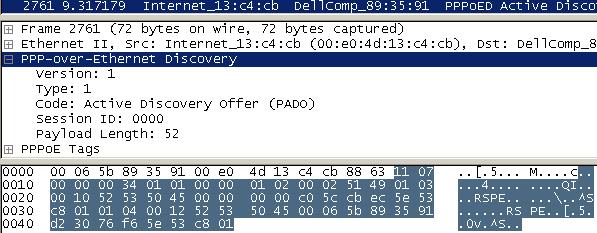


图2-4 PPPoE-PADO报文

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。

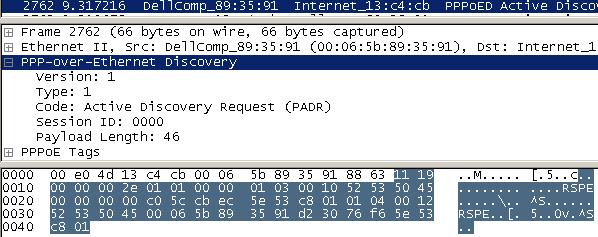


图2-5 PPPoE-PADR报文

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。

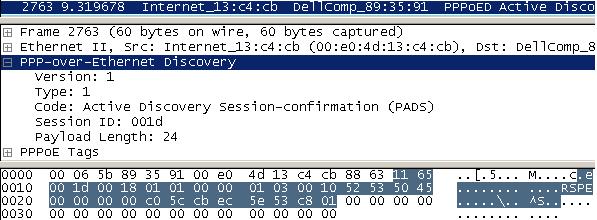


图2-6 PPPoE-PADS报文

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。

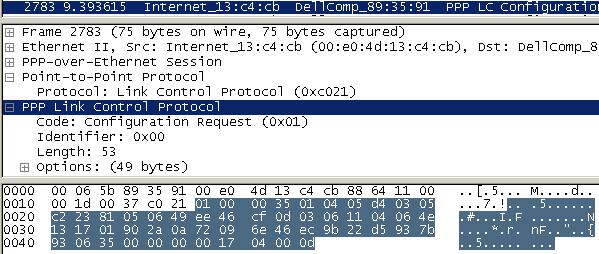


图2-7 PPP-LCP报文

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。

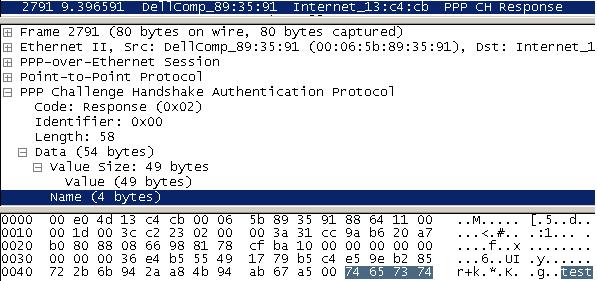


图2-8 PPP-CHAP报文

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。

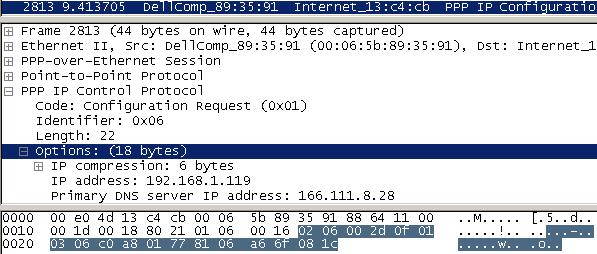


图2-9 PPP-IPCP报文

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。

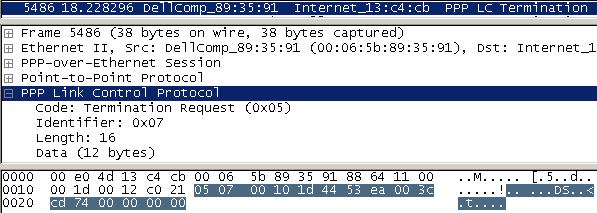


图2-10 PPP连接终止报文

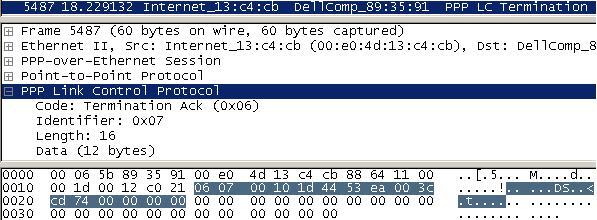


图2-11 PPP连接终止确认报文

### 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）