

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 Modem 与用户端的连接, 实现用户身份认证、鉴权、计费 (即通常提到的 AAA, 全称为 Authentication, Authorization, and 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 (Password Authentication Protocol) 子协议或 CHAP (Challenge-Handshake Authentication Protocol) 子协议进行身份认证, 最后基于 IPCP (IP Control Protocol) 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唯一的会话 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

下面将通过数据帧观察与分析实验了解 PPPoE，进而理解 PPP 协议的工作过程。

使用 Wireshark 打开 pppoe.pcap 文件，观察 PPPoE 在不同阶段的报文。实验者若希望自行捕捉报文，由于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。由于不同版本的 Wireshark 过滤器语义不同，建议将过滤器设置为“ppp or pppoe or pppoes or ppposed or ppp_hdlc”，以显示所有相关的报文。

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。

在不同的阶段可以观察到不同的 PPPoE 报文，PPPoE 在发现阶段发送报文的过程如下。

1)当主机 PC2 希望接入 PC1(实际中可能是 ISP 网络)时,发送 PPPoE 发现报文(PPPoE

Active Discovery Initiation, 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 报文示例如图2-3所示。

2759 9.316745 DellComp_89:35:91 Broadcast PPPoED Active Disco	
Frame 2759 (44 bytes on wire, 44 bytes captured)	
Ethernet II, Src: DellComp_89:35:91 (00:06:5b:89:35:91), Dst: Broadcast	
PPP-over-Ethernet Discovery	
Version: 1	
Type: 1	
Code: Active Discovery Initiation (PADI)	
Session ID: 0000	
Payload Length: 24	
PPPoE Tags	
0000	ff ff ff ff ff ff 00 06 5b 89 35 91 88 63 11 09 [5..G..
0010	00 00 00 18 01 01 00 00 01 03 00 10 52 53 50 45 RSPE
0020	00 00 00 00 c0 5c cb ec 5e 53 c8 01 \.. AS..

图 2-3 PPPoE-PADI 报文

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

2761 9.317179 Internet_13:c4:cb DellComp_89:35:91 PPPoED Active Disco	
Frame 2761 (72 bytes on wire, 72 bytes captured)	
Ethernet II, Src: Internet_13:c4:cb (00:e0:4d:13:c4:cb), Dst: DellComp_8	
PPP-over-Ethernet Discovery	
Version: 1	
Type: 1	
Code: Active Discovery offer (PADO)	
Session ID: 0000	
Payload Length: 52	
PPPoE Tags	
0000	00 06 5b 89 35 91 00 e0 4d 13 c4 cb 88 63 11 07 ..[5... M...C..
0010	00 00 00 34 01 01 00 00 01 02 00 02 51 49 01 03 ..4.... ..QI..
0020	00 10 52 53 50 45 00 00 00 00 c0 5c cb ec 5e 53 RSPE.. \.. AS
0030	c8 01 01 04 00 12 52 53 50 45 00 06 5b 89 35 91 RS PE.. [5..
0040	d2 30 76 f6 5e 53 c8 01 0v.. AS..

图 2-4 PPPoE-PADO 报文

3) PC2 选择一个 PPPoE 服务器 (此处为 PC1), 向 PPPoE 服务器发送单播会话请求报文 (PPPoE Active Discovery Request, PADR), PADR 报文示例如图2-5所示。

2762 9.317216 DellComp_89:35:91 Internet_13:c4:cb PPPoED Active Disco	
Frame 2762 (66 bytes on wire, 66 bytes captured)	
Ethernet II, Src: DellComp_89:35:91 (00:06:5b:89:35:91), Dst: Internet_1	
PPP-over-Ethernet Discovery	
Version: 1	
Type: 1	
Code: Active Discovery Request (PADR)	
Session ID: 0000	
Payload Length: 46	
PPPoE Tags	
0000	00 e0 4d 13 c4 cb 00 06 5b 89 35 91 88 63 11 19 ..M.... [5..G..
0010	00 00 00 2e 01 01 00 00 01 03 00 10 52 53 50 45 RSPE
0020	00 00 00 00 c0 5c cb ec 5e 53 c8 01 01 04 00 12 \.. AS.....
0030	52 53 50 45 00 06 5b 89 35 91 d2 30 76 f6 5e 53 RSPE.. [5..0v.. AS
0040	c8 01 ..

图 2-5 PPPoE-PADR 报文

4) PC1 上的 PPPoE 服务器发送一个确认报文 (PPPoE Active Discovery Session-confirmation, PADS), 为接入主机 PC2 分配一个会话 ID (Session ID), 示例如图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。

2763 9.319678 Internet_13:c4:cb DellComp_89:35:91 PPPoE Active Disco															
Frame 2763 (60 bytes on wire, 60 bytes captured)															
Ethernet II, Src: Internet_13:c4:cb (00:e0:4d:13:c4:cb), Dst: DellComp_8															
PPP-over-Ethernet Discovery															
Version: 1															
Type: 1															
Code: Active Discovery Session-confirmation (PADS)															
Session ID: 001d															
Payload Length: 24															
PPPoE Tags															
0000	00	06	5b	89	35	91	00	e0	4d	13	c4	cb	88	63	11 65
0010	00	1d	00	18	01	01	00	00	01	03	00	10	52	53	50 45
0020	00	00	00	00	c0	5c	cb	ec	5e	53	c8	01	00	00	00 00
0030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00 00

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 PC2 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 报文示例如图2-7所示, 这里只给出了配置信息报文, 没有给出确认报文。

2783 9.393615 Internet_13:c4:cb DellComp_89:35:91 PPP LC Configuration															
Frame 2783 (75 bytes on wire, 75 bytes captured)															
Ethernet II, Src: Internet_13:c4:cb (00:e0:4d:13:c4:cb), Dst: DellComp_8															
PPP-over-Ethernet Session															
Point-to-Point Protocol															
Protocol: Link Control Protocol (0xc021)															
PPP Link Control Protocol															
Code: Configuration Request (0x01)															
Identifier: 0x00															
Length: 53															
Options: (49 bytes)															
0000	00	06	5b	89	35	91	00	e0	4d	13	c4	cb	88	64	11 00
0010	00	1d	00	37	c0	21	01	00	00	35	01	04	05	d4	03 05
0020	c2	23	81	05	06	49	ee	46	cf	0d	03	06	11	04	06 4e
0030	13	17	01	90	2a	0a	72	09	6e	46	ec	9b	22	d5	93 7b
0040	93	06	35	00	00	00	00	17	04	00	0d				

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), 报文示例如图2-8所示。

```

2791 9.396591 DellComp_89:35:91 Internet_13:c4:cb PPP CH Response
┌─ Frame 2791 (80 bytes on wire, 80 bytes captured)
┌─ Ethernet II, Src: DellComp_89:35:91 (00:06:5b:89:35:91), Dst: Internet_1
┌─ PPP-over-Ethernet Session
┌─ Point-to-Point Protocol
└─ PPP Challenge Handshake Authentication Protocol
    Code: Response (0x02)
    Identifier: 0x00
    Length: 58
    ┌─ Data (54 bytes)
    │   value size: 49 bytes
    │   value (49 bytes)
    │   Name (4 bytes)
    └─
0000  00 e0 4d 13 c4 cb 00 06 5b 89 35 91 88 64 11 00  ..M.... [.5..d..
0010  00 1d 00 3c c2 23 02 00 00 3a 31 cc 9a b6 20 a7  ...<.#. .:1...
0020  b0 8d 88 08 66 98 81 78 cf ba 10 00 00 00 00 00  ...f..x .....
0030  00 00 00 36 e4 b5 55 49 17 79 b5 c4 e5 9e b2 85  ...6..UI .y.....
0040  72 2b 6b 94 2a a8 4b 94 ab 67 a5 00 74 65 73 74  r+k.*.K. .g..test

```

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 报文示例如图 2-9 所示。

```

2813 9.413705 DellComp_89:35:91 Internet_13:c4:cb PPP IP Configuratio
┌─ Frame 2813 (44 bytes on wire, 44 bytes captured)
┌─ Ethernet II, Src: DellComp_89:35:91 (00:06:5b:89:35:91), Dst: Internet_1
┌─ PPP-over-Ethernet Session
┌─ Point-to-Point Protocol
└─ PPP IP Control Protocol
    Code: Configuration Request (0x01)
    Identifier: 0x06
    Length: 22
    ┌─ Options: (18 bytes)
    │   IP compression: 6 bytes
    │   IP address: 192.168.1.119
    │   Primary DNS server IP address: 166.111.8.28
    └─
0000  00 e0 4d 13 c4 cb 00 06 5b 89 35 91 88 64 11 00  ..M.... [.5..d..
0010  00 1d 00 18 80 21 01 06 00 16 02 06 00 2d 0f 01  ....!.. ..-..
0020  03 06 c0 a8 01 77 81 06 a6 6f 08 1c          ....w.. .0..

```

图 2-9 PPP-IPCP 报文

在数据传输完毕后，进入 PPP 连接终止阶段，利用 LCP 终止链路。图 2-10 和图 2-11 给出了在终止阶段的 LCP 报文示例。

```

5486 18.228296 DellComp_89:35:91 Internet_13:c4:cb PPP LC Termination
┌─ Frame 5486 (38 bytes on wire, 38 bytes captured)
┌─ Ethernet II, Src: DellComp_89:35:91 (00:06:5b:89:35:91), Dst: Internet_1
┌─ PPP-over-Ethernet Session
┌─ Point-to-Point Protocol
└─ PPP Link Control Protocol
    Code: Termination Request (0x05)
    Identifier: 0x07
    Length: 16
    Data (12 bytes)
0000  00 e0 4d 13 c4 cb 00 06 5b 89 35 91 88 64 11 00  ..M.... [.5..d..
0010  00 1d 00 12 c0 21 05 07 00 10 1d 44 53 ea 00 3c  ....!.. ...DS.<
0020  cd 74 00 00 00 00          .t....

```

图 2-10 PPP 连接终止报文

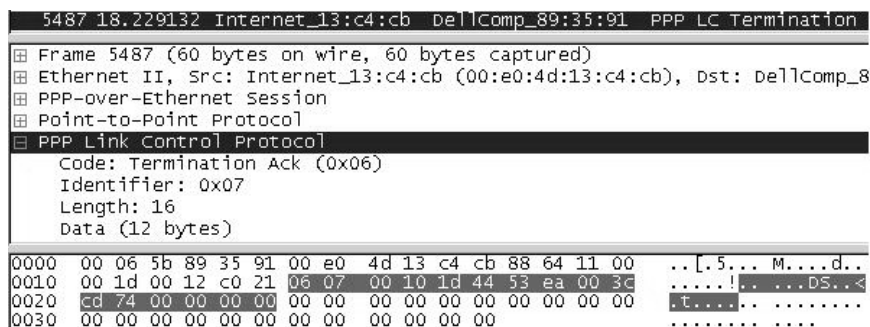


图 2-11 PPP 连接终止确认报文

最后, 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。

2.2.4 思考问题

1) 给出 pppoe.pcap 文件中 Wireshark 捕获的 PADS 报文的截图, 并指出 PPPoE 服务器和客户端的 MAC 地址分别是多少。

2) 给出 pppoe.pcap 文件中 Wireshark 捕获的 PPP-CHAP Response 报文、客户端发出的 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。

3) 在通常的以太网 (MTU=1500) 上, 使用 PPPoE 协议传递 IPv4 的 UDP 数据报 (IPv4 分组头不包含可选字段)。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。

4) 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?

5) PPP LCP 协商中的 MRU 值受到哪些因素的影响?

6) 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)

7) 你认为 PPPoE 有哪些优点和缺点? (开放式问题, 言之有理即可)