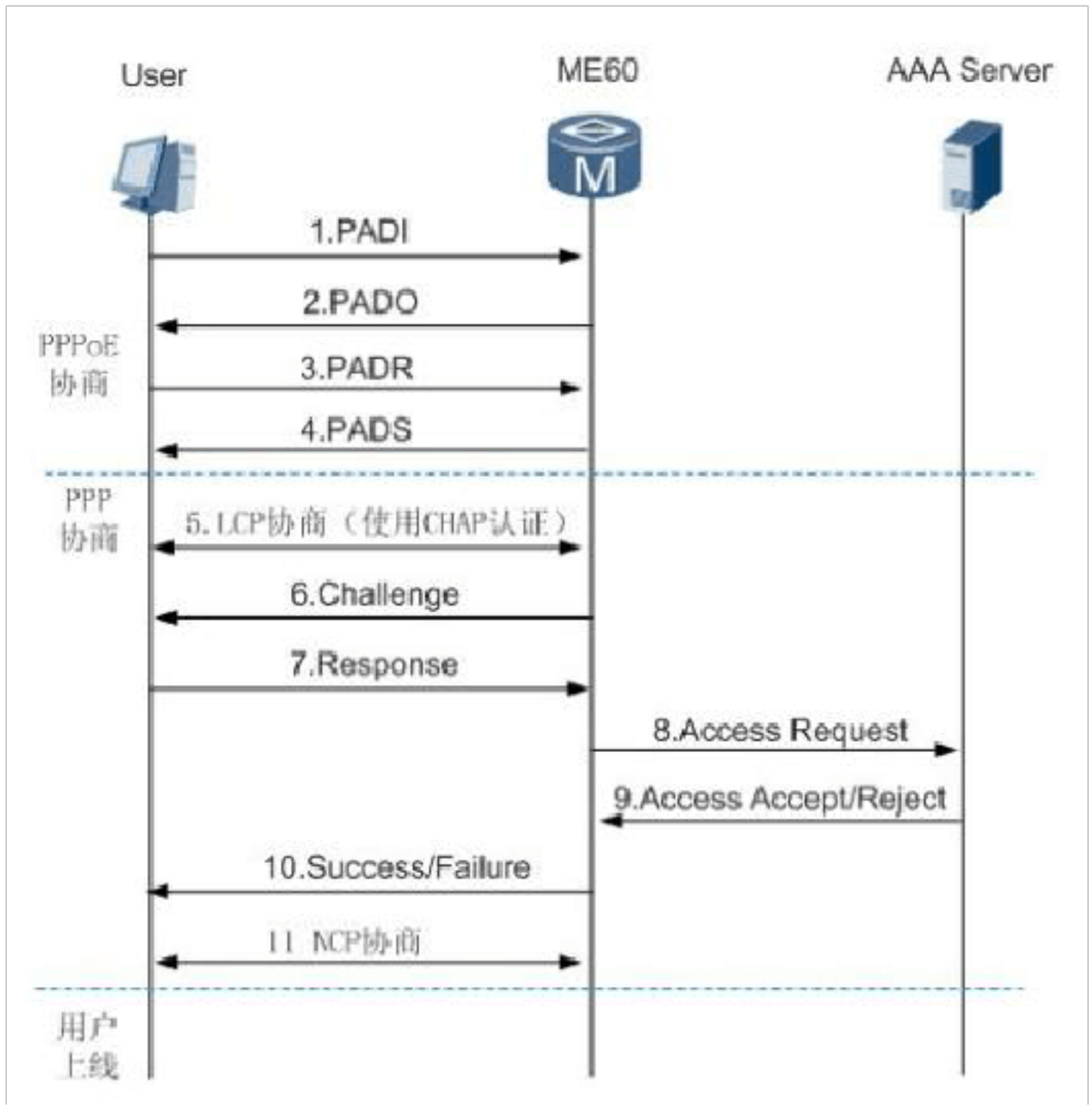
第一天：pppoe 的数据包深入了解，点对点协议（ppp）



Pppoe 分为发现阶段和会话阶段，发现阶段分为 PADI,PADO,PADR,PADS.

pppoe 的数据报文依次为目的 MAC （6 字节=48bit），源 MAC （6 字节），协议类型（2 字节 为 ox8863），版本（VER 4bit为 0001），字段和类型（TYPE 4bit 0001,代码（CODE 8bit），版本标识号码（SESSION-ID 16bi为 ox0000），长度（LENGTH 16bit）,静载荷（数据域）。

发现报文的数据域格式为 TAG（类型-长度），主机名称（15 个字节），TAG（类型-长度），主机标识符（4 个字节），TAG （类型-长度），AC-Cookie（18 个字节）。采用的是 TLV（类型-长度-值）

阶段	源 MAC	目的 MAC	CODE
	48bit	48bit	8bit
PADI	主机 A	广播(FF:FF:FF:FF:FF:FF)	0x09
PADO	服务器 B	主机 A	0x07
PADR	主机 A	服务器 B	0x19
PADS	服务器 B	主机 A	0x65

PPPOE 数据报文中 Tag（标记）的格式

对于发现阶段的 PPPOE 数据报文而言，它的净载荷可能包含零个或多个 Tag（标记），实际上这些标记的意义非常类似于 PPP 配置参数选项，它同样也是要经过协商的。对于 PPPOE 协议而言，没有像 PPP 的配置参数选项那样定义了很多细节，而只是一个初略的定义，因此在实际当中实现这个过程会依据不同厂商的设备有不同。首先还是让我们看一下承载在 PPPOE 报文数据域中的标记封装格式，如图 2。

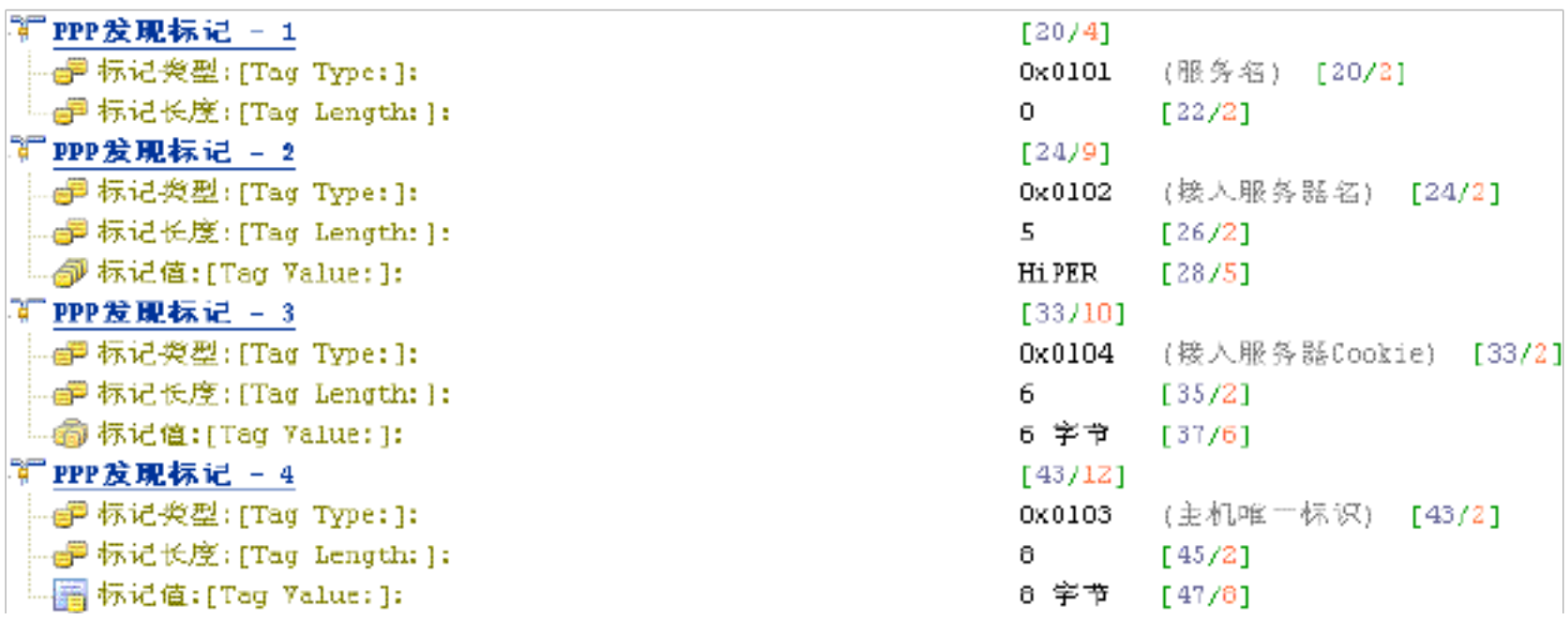
类型	长度

数据

（图 2 标记的封装格式）

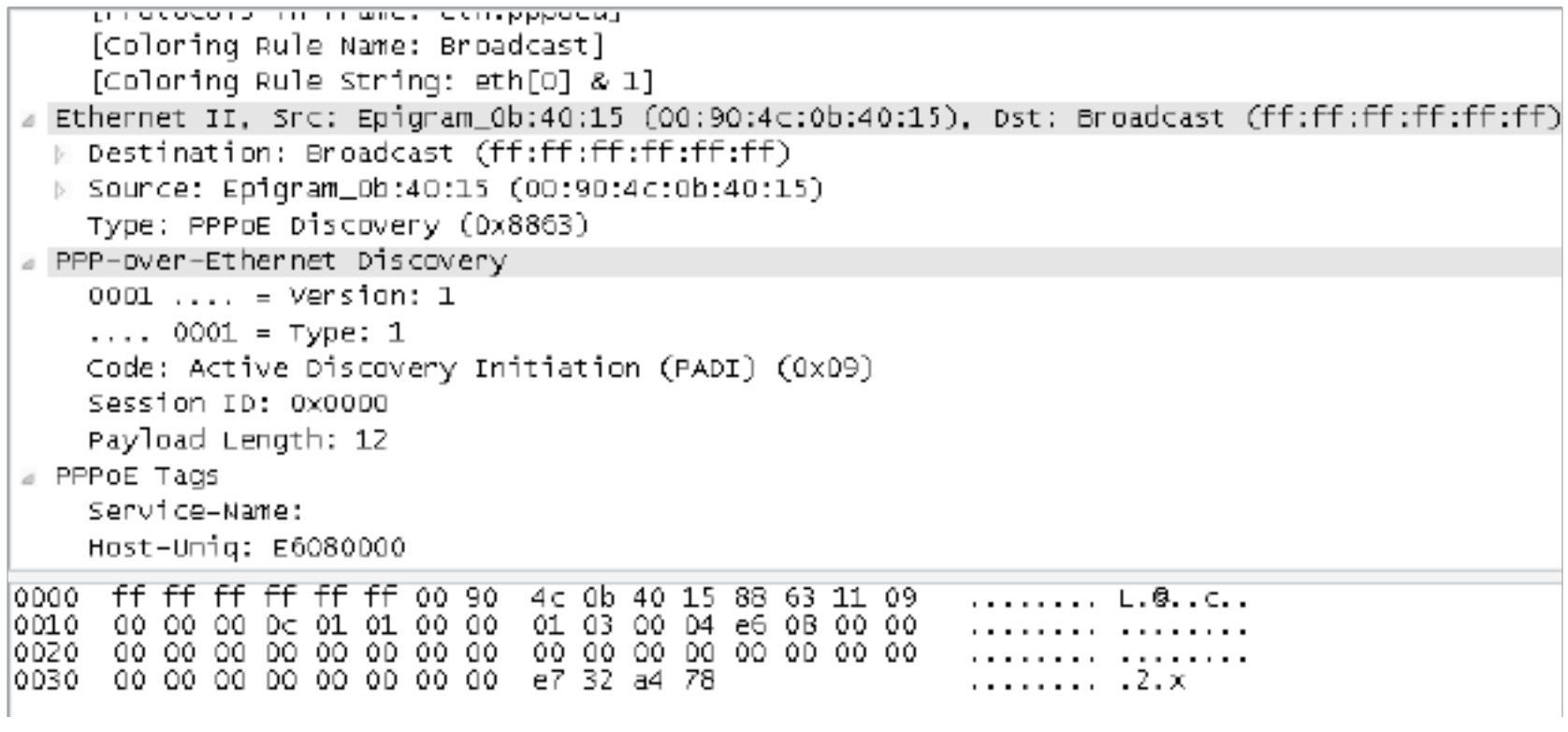
从图 2 中可以看出，标记的封装格式采用的是大家所熟知的 TLV 结构，也即是（类型+长度+数据）。标记的类型域为 2 个字节，下表列出了各种标记类型的含义：

标记类型	标记说明
0x0000	表示 PPPOE 报文数据域中一串标记的结束，为了保证版本的兼容性而保留，在有些报文中有应用。
0x0101	服务名，主要用来表明网络侧所能提供给用户的一些服务。
0x0102	访问集中器名，当用户侧接收到了 AC 的回应的 PADO 报文时，就可获从所携带的标记中获知访问集中器的名子,而且还可以据此来选择相应的访问集中器。
0x0103	主机唯一标识，类似于 PPP 数据报文中的标识域，主要是用来匹配发送和接收端的，因为对于广播式的网络中会同时存在很多个 PPPOE 的数据报文。
0x0104	AC-Cookies，主要被用来防止恶意性 DOS 功击。
0x0105	销售商的标识符。
0x0110	中继会话 ID，对于 PPPOE 的数据报文也同样可以像 DHCP 报文一样被中断到另外的 AC 上终结，这个字段则是用来维护另一个连接的。
0x0201	服务名错误，当请求的服务名不被对端所接受时，会在响应的报文中携带这个标记。
0x0202	访问集中器名出错。
0x0203	一般性错误。



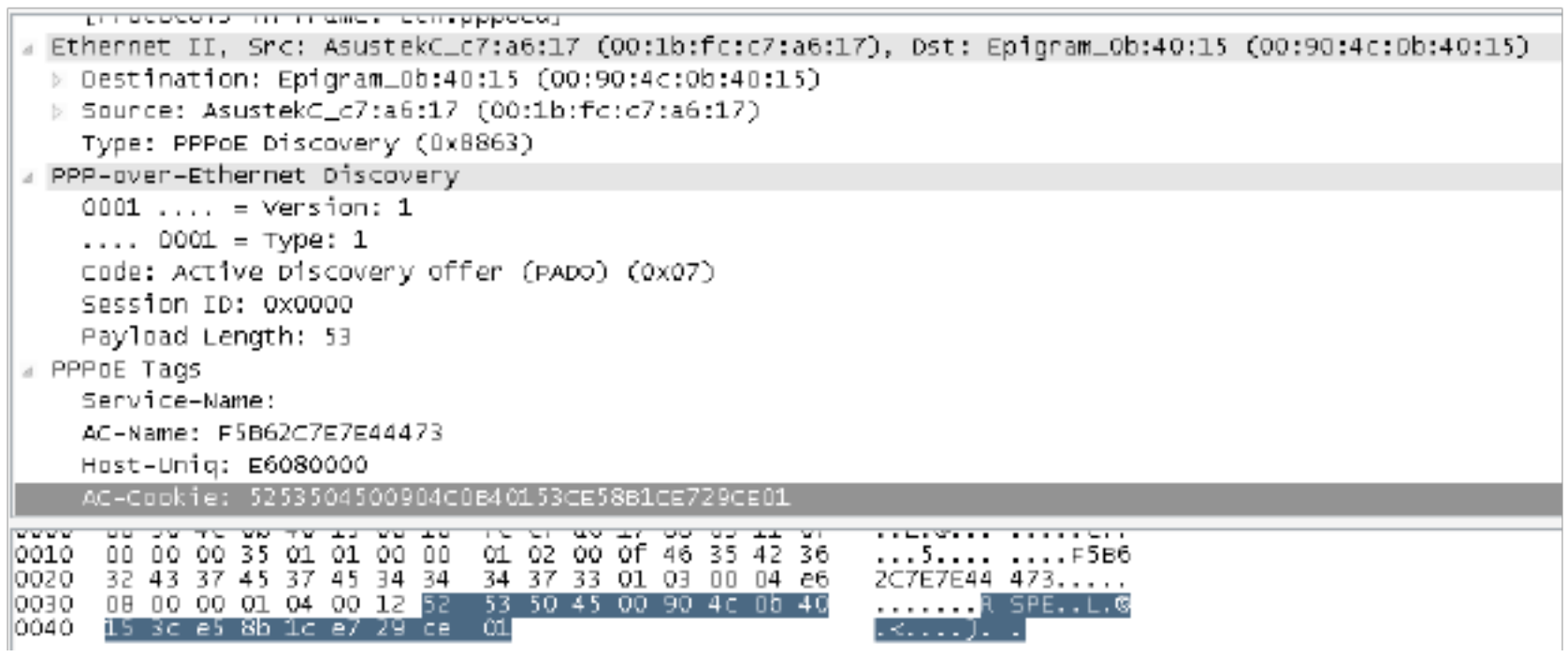
1. PADI

PPPOE 发现阶段的第一步，也即是由用户首先发送这样一个报文。用户主机是以广播的方式发送这个报文，所以该报文所对应的以太网帧的目的地址域应填充为全 1，而源地址域填充用户主机的 MAC 地址。广播包可能会被多个访问集中器接收到。



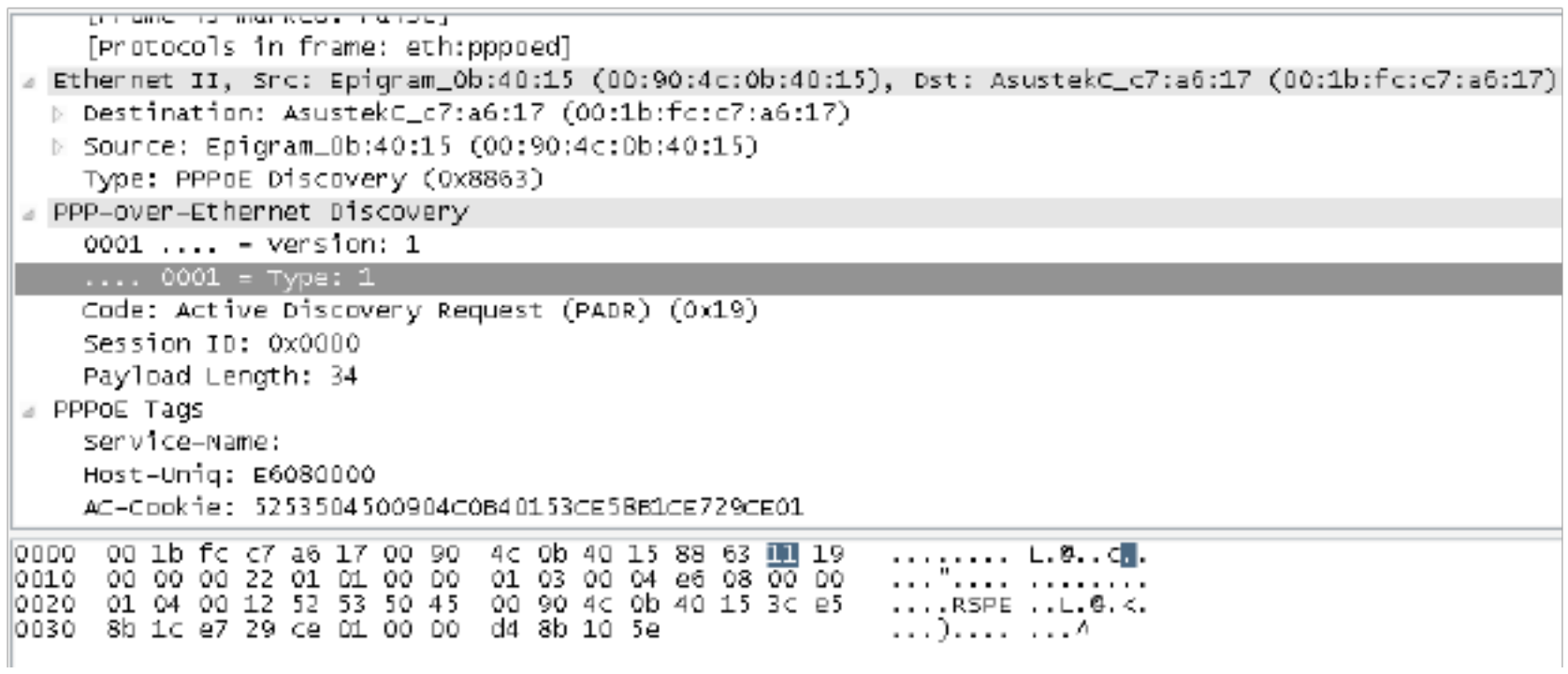
2. PADO

PPPOE 发现阶段的第二步，也即是由访问集中器回应各用户主机发送的 PADI 报文，此时该报文所对应的以太网帧的源地址填充访问集中器的 MAC 地址,而目的地址则填充从PADI中所获取的用户主机的MAC地址。



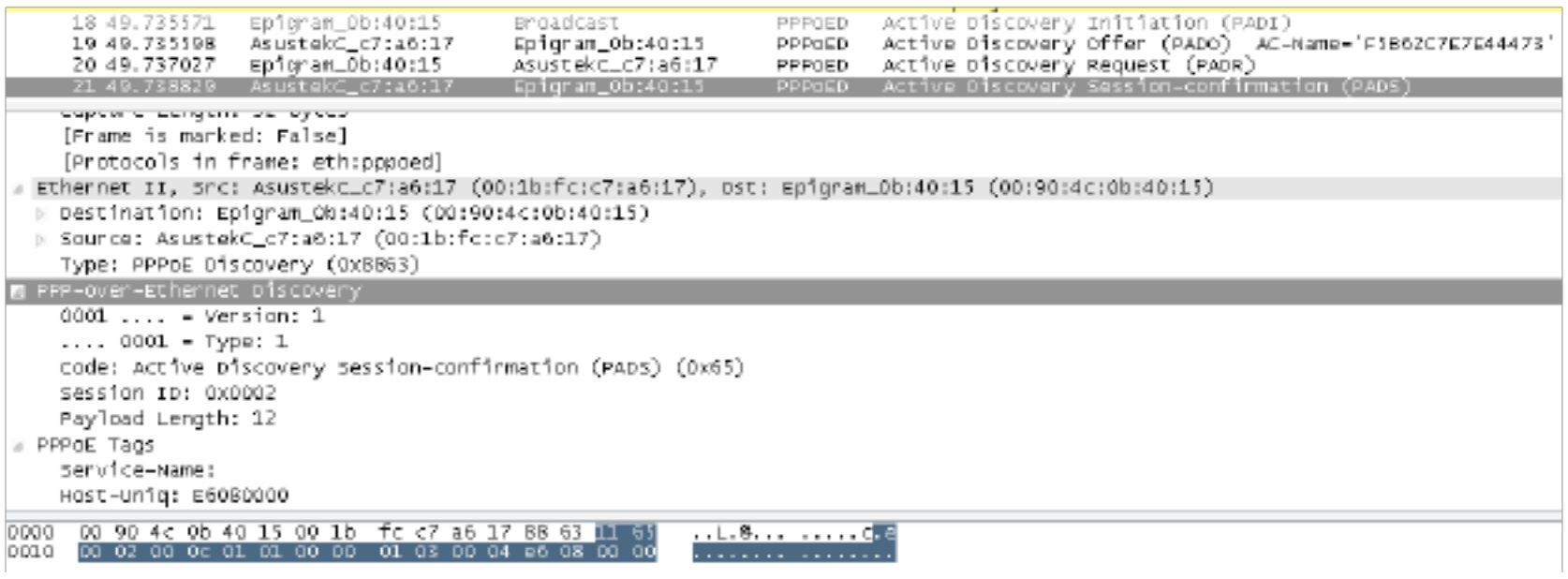
3. PADR

PPPOE 发现阶段的第三步，也即是由用户主机向访问服务器发送单播的请求报文。当用户主机收到PADO 报文后，会从这些报文中挑选一个访问集中器作为后续会话的对象。由于用户主机在收到 PADO 报文后，就获知了访问集中器的 MAC 地址，因此 PADR 报文所以应的以太网帧的源地址填充用户主机的 MAC 地址，而以太网的目的地址填充为访问集中器的 MAC 地址。



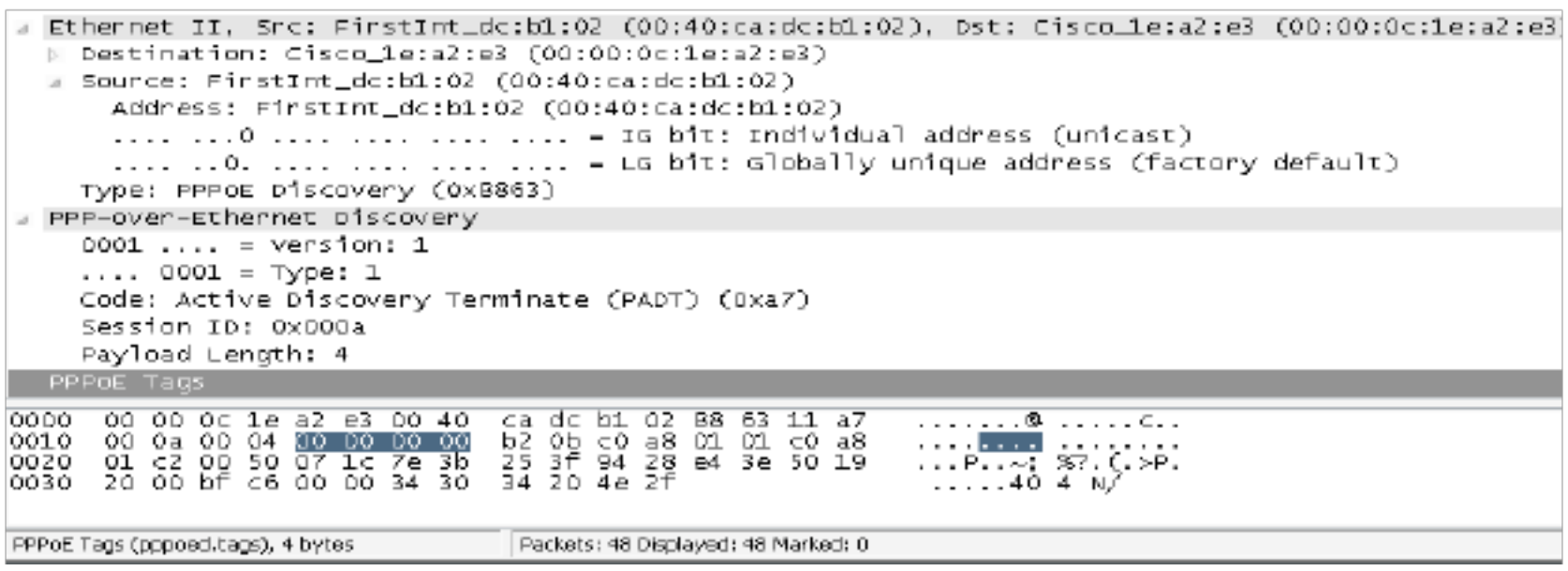
4. PADS

PPPOE 发现阶段的第四步，也即是最后一步，此时访问集中器当收到 PADR 报文时，就准备进入开始一个 PPP 的会话了,而此时访问集中器会为在这个会话分配一个唯一的会话进程 ID,并在发送给主机的 PADS 报文中携带上这个会话 ID。当然如果访问集中器不满足用户所申请的服务的话，则会向用户发送一个 PADS 报文，而其中携带一个服务名错误的标记，而且此时该 PADS 报文中的会话 ID 填充 0x0000。



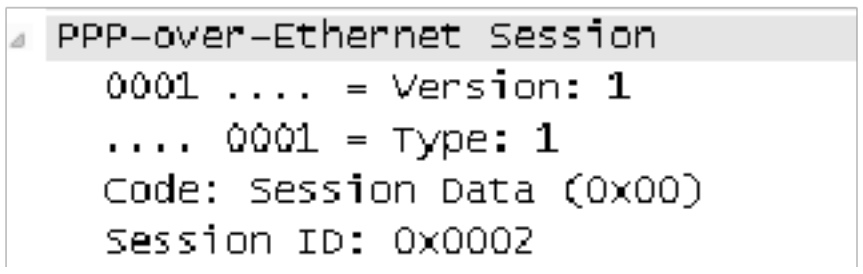
5. PADT

PADT 报文可能在会话进行开始之后的任意时间内被发送， 主要是用来终止一个 PPPOE 会话的止。它可以由主机或访问集中器发送，目的地址填充为对端的以太网的 MAC 地址。



会话阶段：（ppp 全过程）

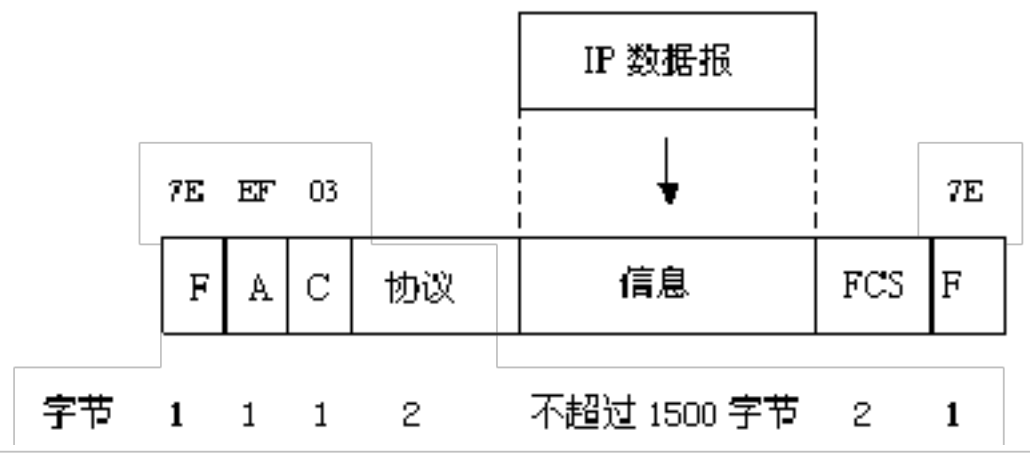
数据帧在数据域中，不变的有如下信息：



协议的组成：

- 链路控制协议(LCP)：建立、拆除和监控 PPP 数据链路
- 网络控制协议(NCP)：协商网络层协议
- PPP 扩展协议：如压缩、链路捆绑
- PPP 验证协议：如 PAP、CHAP

Ppp 帧格式：



标志字段 F 为 0x7E(0x 表示 7E),但地址字段 A 和控制字段 C 都是固定不变的,分别为 0xFF、0x03。PPP 协议不是面向比特的，因而所有的 PPP 帧长度都是整数个字节。

与 HDLC 不同的是多了 2 个字节的协议字段。协议字段不同，后面的信息字段类型就不同。如：

0x0021——信息字段是 IP数据报

0xC021——信息字段是链路控制数据 LCP

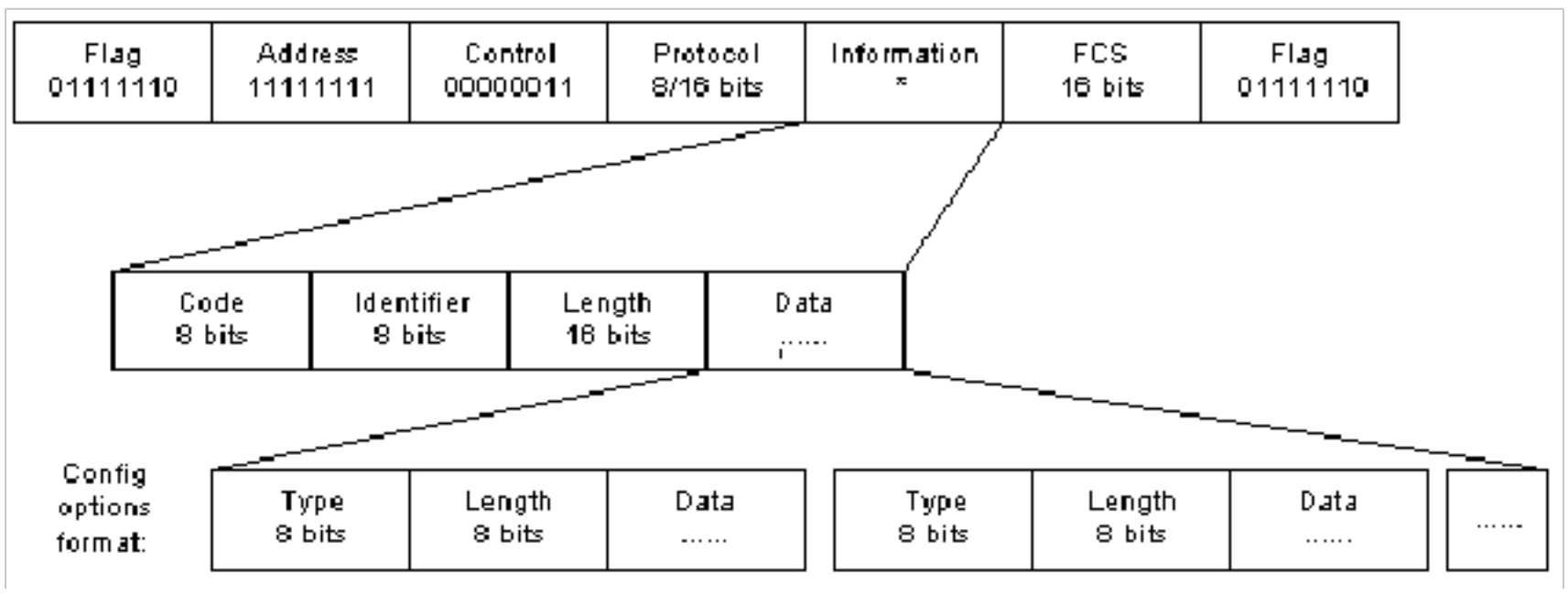
0x8021——信息字段是网络控制数据 NCP

0xC023——信息字段是安全性认证 PAP

0xC025——信息字段是 LQR

0xC223——信息字段是安全性认证 CHAP

当信息字段中出现和标志字段一样的比特 0x7E 时，就必须采取一些措施。因 PPP 协议是面向字符型的,所以它不能采用 HDLC 所使用的零比特插入法,而是使用一种特殊的字符填充。具体的做法是将信息字段中出现的每一个 0x7E 字节转变成 2 字节序列（0x7D，0x5E)。若信息字段中出现一个 0x7D 的字节，则将其转变成 2 字节序列（0x7D，0x5D)。若信息字段中出现 ASCII码的控制字符，则在该字符前面要加入一个 0x7D 字节。这样做的目的是防止这些表面上的 ASCII码控制字符被错误地解释为控制字符。



- Flag标志域：每一个 PPP 数据帧均是以一个标志字节起始和结束的，该字节为 0x7E。
- Address地址域：该字节为 0xFF。由于 PPP 协议是被运用在点对点的链路上，点对点的链路可以唯一标示对方，因此使用 PPP 协议互连的通信设备的两端无须知道对方的数据链路层地址，所以该字节已无任何意义，按照协议的规定将该字节填充为全 1 的广播地址。
- Control控制域：也没有实际意义，按照协议的规定通信双方将该字节的内容填充为 0x03。
- Protoco协议域：用来区分 PPP 数据帧中信息域所承载的数据报文的内容。
- Information 信息域：缺省时最大长度不能超过 1500 字节，其中包括填充域的内

容。

- FCS 校验域：主要是对 PPP 数据帧传输的正确性进行检测的。
- Code 域表明了此报文为哪种 PPP 协商报文；Identifier域用于进行协商报文的匹配；Length域为此协商报文长度（包含 Code 及 Identifier域）；Data域所包含的为协商报文内容；Type 为协商选项类型；其后的 Length为此协商选项长度（包含 Type 域）；紧接着的 Data域为协商选项具体内容。

PPP 主要由三类协议组成：链路控制协议族(LCP)、网络控制协议族(NCP)和 PPP 扩展协议族。其中，链路控制协议主要用于建立、拆除和监控 PPP 数据链路；网络控制协议族主要用于协商在该数据链路上所传输的网络层数据包的类型以及网络层协议自身需要的一些内容（如 IPCP要协商 IP地址等）；PPP 扩展协议族主要用于提供对 PPP 功能的进一步支持，实际上就是为提供一些特性服务，基于 PPP 协议框架设计的一些扩展协议。

同时，PPP 还提供了用于网络安全方面的验证协议族(PAP 和 CHAP)。

LCP 包有 3 类：

1. 链路配置包，用于建立和配置链路（Configure-Request、Configure-Ack、Configure-Nak和 Configure-Reject）。
2. 链路结束包被用于结束一个链路（Terminate-Request和 Terminate-Ack）
3. 链路维修包被用于管理和调试一个链路（Code-Reject、Protocol-Reject、Echo-Request、Echo-Reply 和 Discard-Request）。

确切的说一个 LCP 包被封装在 PPP 信息域中，该 PPP 协议域表示类型为十六进制 c021（链路控制协议）。

8	16	32 bit	Variable
Code	Identifier（匹配请求和响应报文）	Length	Data

Code — 十进制值，表示 LCP 数据包类型。

- 1 — Configure-Reques配置请求报文
- 2 — Configure-Ac配置确定报文
- 3 — Configure-Nak支持对端的协商选项，但不认可该项协商的内容，回复自己认可的配置方式并放入其中
- 4 — Configure-Reje配置拒接
- 5 — Terminate-Reques终止请求
- 6 — Terminate-Ack终止确认
- 7 — Code-Reject代码拒绝
- 8 — Protocol-Reject
- 9 — Echo-Request
- 10 — Echo-Reply
- 11 — Discard-Request
- 12 — Link-Quality Repor

Identifier — 十进制值，表示匹配 Request 和 Reply。

Length — LCP 数据包长度，包括 Code、Identifier、Length 和 Data 字段。

Data — 可变长字段，可能包括一或多个配置选项。

- Address-and-Control-Field-Compress地址控制字段压缩
- Authentication-Protocol身份验证协议
- Protocol-Field-Compress协议域压缩
- Maximum-Recieve-Unit最大接受单元（4 个字节）
- Multilink-Protocol多重协议（5 个字节）
- Magic-Number 避免在 PPP 帧的循环使用（6 个字节）
- Callback回调（3 个字节）
- Multilink MRRU多链路协议（4 个字节）
- Multilink endpoint discrimination多链路端点鉴别（23 个字节）
- Link discriminator链路鉴别。（4 个字节）

Request:

```
Point-to-Point Protocol
  Protocol: Link Control Protocol (0xc021)
PPP Link Control Protocol
  Code: Configuration Request (0x01)
  Identifier: 0x00
  Length: 53
  Options: (49 bytes)
    Maximum Receive Unit: 1492
    Authentication protocol: 5 bytes
      Authentication protocol: Challenge Handshake Authentication Protocol (0xc223)
      Algorithm: MS-CHAP-2 (0x81)
    Magic number: 0x66e50620
    Callback: 3 bytes
    Multilink MRRU: 1614
    Multilink endpoint discriminator: 23 bytes
      Class: Locally assigned address (1)
      Address (20 bytes)
    Link discriminator for BAP: 0x0005
```

Ack：

```
Point-to-Point Protocol
  Protocol: Link Control Protocol (0xc021)
PPP Link Control Protocol
  Code: Configuration Ack (0x02)
  Identifier: 0x01
  Length: 42
  Options: (38 bytes)
    Maximum Receive Unit: 1492
    Authentication protocol: 5 bytes
      Authentication protocol: Challenge Handshake Authentication Protocol (0xc223)
      Algorithm: MS-CHAP-2 (0x81)
    Magic number: 0x66e50620
    Multilink endpoint discriminator: 23 bytes
```

Termination reques报文：

```
PPP-over-Ethernet Session
  0001 .... = Version: 1
  .... 0001 = Type: 1
  Code: Session Data (0x00)
  Session ID: 0x0002
  Payload Length: 18
Point-to-Point Protocol
  Protocol: Compression Control Protocol (0x80fd)
PPP Compression Control Protocol
  Code: Termination Request (0x05)
  Identifier: 0x05
  Length: 16
  Data (12 bytes)
```

Termination ac报文：

```
PPP-over-Ethernet Session
  0001 .... = Version: 1
  .... 0001 = Type: 1
  Code: Session Data (0x00)
  Session ID: 0x0002
  Payload Length: 6
Point-to-Point Protocol
  Protocol: Compression Control Protocol (0x80fd)
PPP Compression Control Protocol
  Code: Termination Ack (0x06)
  Identifier: 0x05
  Length: 4
```

:

PPP 扩展认证协议（EAP）是一个用于 PPP 认证的通用协议，可以支持多种认证方法。EAP 并不在链路控制阶段指定认证方法，而是把这个过程推迟到认证阶段。这样认证方就可以在得到更多的信息以后再决定使用什么认证方法。这种机制还允许 PPP 认证方简单地把收到的认证报文透传给后方的认证服务器，由后方的认证服务器来真正实现各种认证方法。

1. 在链路阶段完成以后，认证方向对端发送一个或多个请求报文。在请求报文中有一个类型字用来指明认证方所请求的信息类型，例如是对端的 ID、MD5 的挑战字、一次密码（OTP）以及

通用令牌卡等。MD5 的挑战字对应于 CHAP 认证协议的挑战字。典型情况下，认证方首先发送一个 ID 请求报文随后再发送其他的请求报文。当然，并不是必须要首先发送这个 ID 请求报文，在对端身份是已知的情况下（如租用线、拨号专线等）可以跳过这个步骤。

2. 对端对每一个请求报文回应一个应答报文。和请求报文一样，应答报文中也包含一个类型字段，对应于所回应的请求报文中的类型字段。
3. 认证方通过发送一个成功或者失败的报文来结束认证过程。

EAP 可以支持多种认证机制，而无需在 LCP 阶段预协商过程中指定。某些设备（如：网络接入服务器）不需要关心每一个请求报文的真正含义，而是作为一个代理把认证报文直接透传给后端的认证服务器。设备只需关心认证结果是成功还是失败，然后结束认证阶段。

EAP 需要在 LCP 中增加一个新的认证协议，这样现有的 PPP 实现要想使用 EAP 就必须进行修改。同时，使用 EAP 也和现有的在 LCP 协商阶段指定认证方法的模型不一致。

8	16	32 bit	Variable
Type	Length	Authentication-Protocol	Data

Type — 3

Length — 4

Authentication-Protocol 对于 PPP 中的 EAP，该字段为 C227（十六进制）。

一个 PPP EAP 数据包封装在 PPP 数据链路层帧的 Information字段，其中的 Protocol字段表示类型为十六进制 C227（PPP EAP）。EAP 数据包格式如下所示：

8	16	32 bit	Variable
Code	Identifier	Length	Data

Code — Code 字段识别 EAP 数据包类型。

EAP 代码分配如下：1、请求（Request）；2、响应（Response）；3、成功（Success）；4、失败（Failure）

Identifier — Identifier 字段用于匹配响应和请求信息。

Length — Length 字段表示 EAP 数据包的长度，包括 Code、Identifier、Length 和 Data 字段

Data — Data 字段的格式取决于 Code 字段。

Ipcp request报文：

```
PPP-over-Ethernet Session
    0001 .... = Version: 1
    .... 0001 = Type: 1
    Code: Session Data (0x00)
    Session ID: 0x0002
    Payload Length: 24
Point-to-Point Protocol
PPP IP Control Protocol
    Code: Configuration Request (0x01)
    Identifier: 0x01
    Length: 22
  Options: (18 bytes)
```

Ipcp ack报文：

```
PPP-over-Ethernet Session
    0001 .... = Version: 1
    .... 0001 = Type: 1
    Code: Session Data (0x00)
    Session ID: 0x0002
    Payload Length: 12
Point-to-Point Protocol
    Protocol: IP Control Protocol (0x8021)
PPP IP Control Protocol
    Code: Configuration Ack (0x02)
    Identifier: 0x06
    Length: 10
  Options: (6 bytes)
```

Ccp request报文：

```
PPP-over-Ethernet Session
    0001 .... = Version: 1
    .... 0001 = Type: 1
    Code: Session Data (0x00)
    Session ID: 0x0002
    Payload Length: 12
Point-to-Point Protocol
    Protocol: Compression Control Protocol (0x80fd)
PPP Compression Control Protocol
    Code: Configuration Request (0x01)
    Identifier: 0x03
    Length: 10
  Options: (6 bytes)
```

Cc pack报文：