**课程设计2 网络协议及流程分析 报告范本**

**PPPoE协议实现（交互）过程分析**

## 1.PPPoE协议简介

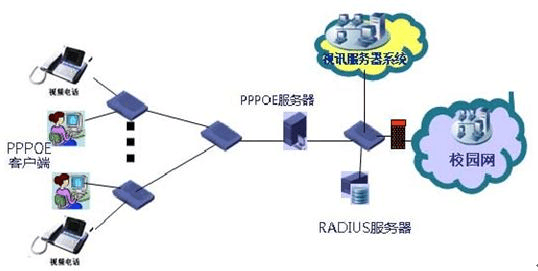
PPP协议是在点到点链路上承载网络层数据包的一种链路层协议，可以提供良好的访问控制和计费的功能。PPPoE（PPP Over Ethernet）是基于以太网实现的PPP协议。

PPPoE的实质是以太网和拨号网络之间的一个中继协议，它继承了以太网的快速和PPP拨号的简捷、用户验证和动态IP地址分配等优势。

PPPoE协议通过以太网来传输PPP报文，即以太帧的数据部分是按照PPP的格式定义封装的PPP报文，如数据链路控制报文（LCP)、网络层控制报文(NCP)、认证报文等。

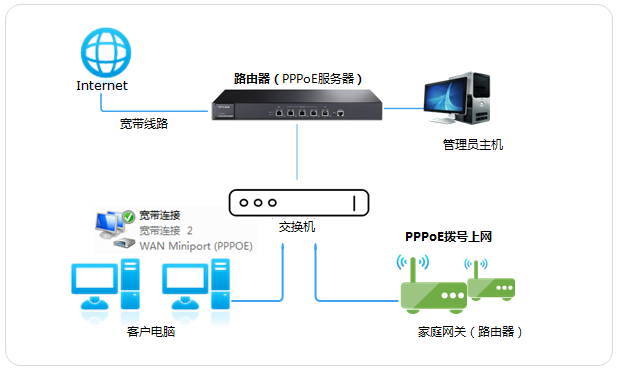
PPPoE主要协议标准：RFC2516

PPPoE网络连接：



AC

AAA服务器



## 2.PPPoE报文封装

### 2.1 PPPoE报文封装

PPPoE将PPP协议报文封装在以太帧中传输，其报文格式如图1所示。其中的以太帧TYPE取值为：0x8863（发现阶段）或0x8864（会话阶段）。PPPoE报头



图1 PPPoE报文封装

相对于标准的以太网帧，PPPOE增加了8个字节大小，所以PPPOE会话的MTU一般是比以太网的小8个字节。一般的以太网的MTU是1500个字节，所以PPPOE的话是1492个字节了。

### 2.2 PPPoE报文格式

**2.2.1 PPPoE报文格式**

PPPoE协议工作的两个阶段，PPPoE帧格式也包括两种类型：发现阶段的以太网帧中的类型字段值为0×8863；PPP会话阶段的以太网帧中的类型字段值为0×8864。

PPPoE分组帧结构如图4-6所示。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VER  （4bit） | TYPE  （4bit） | CODE （16bit） | SESSION-ID  （8bit） | LENGTH  （16bit） | 净载荷（或数据域） |
| PPPOE帧格式 一共为48位 8字节  图 4-6 | | | | | |

1. PPPoE数据报文最开始的4位为版本域（Version），协议中给出了明确的规定，这个域填充的内容为0x01。
2. 版本域后是4位的类型域（Type），根据协议规定，这个域填充的内容也是0x01。
3. 字段长度为8比特，根据两阶段中各种数据包的不同功能其值不同。

CODE的定义:

0x00 PPP session stage

0x09 PPPOE active discovery initialization(PADI) packet

0x07 PPPOE active discovery offer (PADO) packet

0x19 PPPOE active discovery request (PADR) packet

0x65 PPPOE active discovery session-confirmation (PADS) packet

0xa7 PPPOE active discovery terminated (PADT) packet

1. 会话ID（Session ID）占用两个字节，当访问集中器（Access Concentrator）还没有分配唯一的会话ID给用户主机的话，改域的内容必须填充为0x0000；一旦主机获取了会话ID后，那么在后续的所有报文里面必须填充那个唯一的会话ID。
2. 长度（Length）字段为16比特，指示PPPoE净荷长度。发现阶段PPPoE载荷可以为空或由多个标记（TAG）组成，每个标记都是TLV（类型–长度–值）的结构；PPP会话阶段PPPoE载荷为标准的点对点协议包PPP。
3. 数据域，有时也称之为净载荷域，在PPPOE的不同阶段该域内的内容会有很大的不同。在PPPOE的发现阶段时，该域内会填充一些Tag（标记）；而在PPPOE的会话阶段，该域则携带的是PPP的报文。

**2.2.2 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所示。

|  |  |  |
| --- | --- | --- |
| 类型 Tpye | 长度 Length | 值 Value |

图2 PPPoE 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（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。 |

PPPoE实例：

1. **Host-Uniq**

在PPPoE发现阶段的四个步骤中，PPPoE头的Payload中始终含有这样一个TLV：

Tag\_Type = 0103 (表示为Host-Uniq)

Tag\_Length = 8 （8个字节的长度）

Tag\_Value = 0500000008000000

Host-Uniq为主机唯一标识，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。

2. AC-Cookie

PADO和PADR数据包里面都含有Tag\_Type为AC-Cookie的Tag，16Bytes。Ac-Cookie是为了防止拒绝服务攻击（Denial of Service，简称DOS）。访问集中器（AC）能够根据PADR的源地址来重新产生唯一的Tag\_Value。使用这种方法，AC可以确保PADI的源地址是可达的，并对该地址的并行会话数进行限制。

### 2.3 PPP报文格式

PPP报文格式如图3所示。



图3 PPP报文格式

其中协议字段决定了信息字段里信息的意义，协议字段包括：

0x0021——信息字段是IP数据报

0x002D——Van Jacobson Compressed TCP/IP（压缩的TCP/IP）

0x002F——Van Jacobson Uncompressed TCP/IP（未压缩的TCP/IP）

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IPCP

0xC023——PAP(Password Authentication Protocol，口令认证协议)

0xC025——LQR（Link Quality Report，链路质量报告）

0xC223——CHAP(Change Handshake Authentication Protocol,竞争握手认证协议)

LCP和IPCP中CODE 字段的定义：



LCP常用配置选项类型：



IPCP类型定义：

1      IP-Addresses（IP地址群）

2      IP-Compression protocol（IP压缩协议）

3      IP-Address（IP地址）

4       Mobil-Ipv4

129   Primary DNS Server Address（基本域名服务器地址）

130   Primary NBNS Server Address(基本NetBIOS域名服务器地址)

131    Secondary DNS Server Address

132 Secondary NBNS Server Address

## 3. PPPoE工作流程

## 3.1 PPPoE接入流程

PPPoE协议的工作流程包含发现和会话两个阶段，如图4所示。发现阶段是无状态的，目的是获得PPPoE接入集中器（在局端的ADSL设备上）的以太网MAC地址，并建立一个惟一的PPPoESESSION-ID。发现阶段结束后，就进入标准的PPP会话阶段。

PPPoE客户端

PPPoE接入服务器

AAA服务器

1.PADI

2.PADO

3.PADR

4.PADS

4. LCP Configuration-Request

6. LCP Configuration-Ack/Nak/Reject

5. LCP Configuration-Request

7. LCP Configuration-Ack/Nak/Reject

8. Challenge

9.Response

9.Access-Resqest

10. Access-Accept/Access-Reject

11.IPCP Configuration-Request

13.IPCP Configuration-Ack/Nak/Reject

12.IPCP Configuration-Request

14.IP LCP Configuration-Ack/Nak/Reject

18.Terminate-Requst

19.Terminate-Ack

20.Accounting-Request/Stop

21.Accounting-Response/Stop

17.数据传输

PPPoE发现阶段

链路参数协商阶段

网络参数协商阶段

认证阶段

数传阶段

下线阶段

15.Accounting-Resqest/Start

16.Accounting-Response/Start

PPP

PPPoE

发现阶段

PPPoE

会话阶段

图4 （A）PPPOE交互示意图

### 3.1.1 PPPoE发现阶段

当一个主机想开始一个PPPoE会话，它必须首先进行发现阶段，以识别局端的以太网MAC地址，并建立一个PPPoE SESSION-ID。在发现阶段，基于网络的拓扑，主机可以发现多个接入集中器，然后允许用户选择一个。当发现阶段成功完成，主机和选择的接入集中器都有了他们在以太网上建立PPP连接的信息。直到PPP会话建立，发现阶段一直保持无状态的Client/Server（客户/服务器）模式。

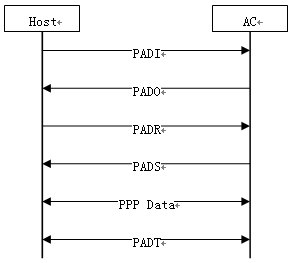


图4（B）PPPoE 发现阶段流程

PPPoE协议会话的发现和会话两个阶段具体进程如下。

**（1）发现（Discovery）阶段**

在发现（Discovery）阶段中用户主机以广播方式寻找所连接的所有接入集中器（或交换机），并获得其以太网MAC地址。然后选择需要连接的接入集中器，并确定所要建立的PPP会话标识号码。

发现阶段有4个步骤，当此阶段完成，通信的两端都知道PPPoE SESSION-ID和对端的以太网地址，他们一起唯一定义PPPoE会话。

1. 主机广播发起分组（**PADI**）（**PPPOE Active Discovery Initiation**）

分组的目的地址为以太网的广播地址0×ffffffffffff，CODE（代码）字段值为0×09，SESSION-ID（会话ID）字段值为0×0000。PADI分组必须至少包含一个服务名称类型的标签（标签类型字段值为0×0101），向接入集中器提出所要求提供的服务。

（2）接入集中器收到在服务范围内的PADI分组，发送PPPoE有效发现提供包（**PADO**）（**PPPOE Active Discovery Offer**）分组，以响应请求。其中CODE字段值为0×07，SESSION-ID字段值仍为0×0000。PADO分组必须包含一个接入集中器名称类型的标签（标签类型字段值为0×0102，以及一个或多个服务名称类型标签，表明可向主机提供的服务种类。

通过PADO得到：接入集中器的MAC地址和名称。

（3）主机在可能收到的多个PADO分组中选择一个合适的PADO分组，然后向所选择的接入集中器发送PPPoE有效发现请求分组（**PADR**）（**PPPOE Active Discovery Request**）。其中CODE字段为0×19，SESSION\_ID字段值仍为0×0000。PADR分组必须包含一个服务名称类型标签，确定向接入集线器（或交换机）请求的服务种类。当主机在指定的时间内没有接收到PADO，它应该重新发送它的PADI分组，并且加倍等待时间，这个过程会被重复期望的次数。

（4） 接入集中器收到PADR分组后准备开始PPP会话，它发送一个PPPoE有效发现会话确认（**PADS**）（**PPPOE Active Discovery Session-confirmation**）分组。其中CODE字段值为0×65，SESSION-ID字段值为接入集中器所产生的一个惟一的PPPoE会话标识号码。PADS分组也必须包含一个接入集中器名称类型的标签以确认向主机提供的服务。当主机收到PADS分组确认后，双方就进入PPP会话阶段。

### 3.1.2 PPP 会话阶段

PPP会话阶段辅助PPP连接的建立。

PPP链接的建立过程分为三个阶段：创建，认证和网络协商阶段。创建阶段主要是工作是对基本的通信方式进行选择，链路两端的设备通过LCP向对方发送配置信息分组，一旦配置信息分组被发送且被接收。就完成交换，进入LCP开启状态。认证阶段主要工作是客户机将自己的身份发送给远程的接入服务器，该阶段使用一种安全的验证方式避免第三方窃取数据或冒充远程客户机服务器的链接。最常用的验证协议是（PAP）和（CHAP）。网络协商阶段的主要工作是调用创建阶段协商的网络控制协议模块解决PPP链路上高层协议问题。

PPP会话的建立，需要两端的设备都发送LCP（Link Control Protocol）数据包来配置和测试数据通信链路。

LCP报文可以分为三类：链路配置报文（LCP Configure Request，LCP Configure Reject，LCP Configure Ack和LCP Configure Nak）、链路终止报文和链路维护报文。

**Ⅰ 协商阶段**

LCP的Request主机和AC都要给对方发送，LCP协商阶段完成最大传输单元、是否进行认证和采用何种认证方式等的协商。

LCP协商阶段的数据帧由三部分组成：以太网帧头、PPPoE头和PPP头。PPPoE Session的以太网类型域为0x8864。

PPP信息包括：

Code＝01（Configure Request，请求同意Option中的内容）

02（Configure Ack，完全同意）

                   03（Configure Nak，不同意部分Option中的内容，还需要再协商）

                    04（Configure Reject，完全不同意）

                    06（Terminate Ack，终止确认，正常下网）

1. 某一端发送Config-Request报文，在本文的选项域中按TLV格式列出需要协商的TAG（选项）。
2. 当接收到Config-Request报文的另一端能识别并同意发送过来的所有配置参数选项，且认可所有配置参数选项数据域的内容时，接收端将会给请求发送端回一个Config-Ack报文，将配置请求报文中的配置参数选项原封不动的放置在Config-Ack报文的数据域内。
3. 当接收Config-Request报文的一端能识别发送端所发送过来的所有配置参数选项，但对部分配置参数选项数据域中的内容不认可时，接收端将会给对端回应一个Config-Nak报文，该报文只携带不认可的配置参数选项，并且这些配置参数选项的数据内容改为本端希望的值。
4. 当发送端接收到Config-Nak报文后，会重新发送Config-Request报文。这次的报文和上一次报文的区别在于那些被对端不认可的配置参数选项的内容被替换成Config-Nak报文里面相应的内容。
5. 当接收Config-Request报文的一端不能识别所发送端发送过来的配置参数选项时，此时接收端将会向对端回一个Config-Reject报文，该报文中的数据域只携带那些不能识别的配置参数选项。当对端接收到Config-Reject报文后，会再次发送Config-Request报文，只是将不被识别的那些配置参数选项给删除了。

**Ⅱ 认证阶段**

会话双方通过LCP协商好的认证方法进行认证，如果认证通过了，才可以进行后续的网络层的协商。认证过程在链路协商结束后就进行。但此时可能链路质量的协商还在进行。所以会延缓认证过程。

认证阶段包括：Challenge Packet Identifier，Response Packet Identifier，Success Packet Identifier和Failure Packet Identifier

认证报文包括：以太帧头，PPPOE头、PPP头和CHAP头（采用的是Chap认证）。

以太帧头和PPPOE头与LCP中的相似。PPP头中，Protocol＝0xc223（Challenge Handshake Authentication）

认证通过要经过三个步骤：首先AC发送Challenge Packet Identifier，然后客户端发送Response Packet Identifier，最后AC发送Success Packet Identifier。

认证失败要经过三个步骤：首先AC发送Challenge Packet Identifier，然后客户端发送两次Response Packet Identifier，最后AC发送 Failure Packet Identifier。

**Ⅲ IPCP协商阶段**

用户和接入设备对IP服务阶段的一些要求进行多次协商，以决定双方都能够接收的约定。如：IP业务阶段使用的IP压缩协议等。双方的协议是通过报文中包含的Option项进行协商的，每一个Option都是一个需要协商的问题。最后双方都需要对方答复Configure\_Ack的同意报文。

IPCP阶段的报文：以太网帧头、PPPoE头、PPP。以太网帧头和PPPOE头与LCP阶段相同。

PPP中存放的是多个Option。Option格式与LCP的TLV相同。

Configure\_Request：要求协商的Option

Configure\_Nak：表示对收到的Option都可识别，但是一些不能够接收。

Configure\_Ack：表示对收到的都能够接收。

Configure\_Reject：收到的Option不能够接收。

达成一致后，进入数据包的真正传输阶段，即IP阶段。用户和AC之间通信都开始使用对方的IP地址而不是MAC地址。

## 3.2 PPPoE下线流程

## PPPoE用户下线流程包括用户主动下线和异常下线两种情况

## 3.2.1 主动下线

## 用户主动下线流程如下图所示。

PPPoE客户端

用户在线

1.Terminate-Requet

2.Terminate-Ack

PPPoE服务器

3.Accounting-Requet/Stop

AAA服务器

4.Accounting-Response/Stop

## 图 用户主动下线流程

## 用户通过PPPoE客户端，主动向PPPoE服务器发送Terminate-Request；

## PPPoE服务器向PPPoE客户端返回Terminate-Ack报文；

## PPPoE服务器向AAA服务器发送计费停止请求的报文

## AAA服务器向认证点回计费停止请求报文的回应

## 3.2.2 异常下线

## 异常下线流程如下图所示。

PPPoE客户端

用户在线

1.检测用户已经不在线t

PPPoE服务器

2.Accounting-Requet/Stop

AAA服务器

3.Accounting-Response/Stop

## 图 异常下线流程

1)PPPoE服务器检测到用户已经不在线；

2)PPPoE服务器向AAA服务器发送计费停止请求的报文；

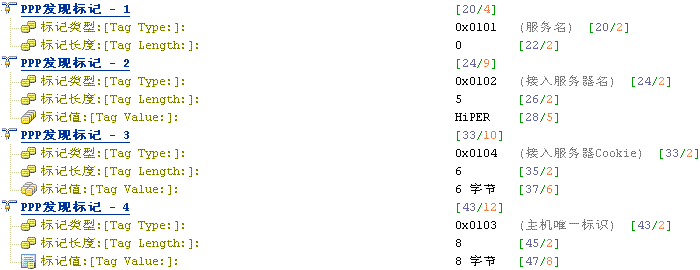
3)AAA服务器向认证点回计费停止请求报文的回应。

在PPP架构中，用户通常会通过传送IPCP（IP控制协议）终止消息而中断已建立的会话。否则，LCP（链路控制协议）周期性轮检机制能够检测出PPP会话是否已终止。如果检测到会话已中止，则分配给用户终端的IP地址将被释放回IP地址池中。因此，由于PPP会话的安全性、健壮性等特征，而被广泛应用于ADSL接入认证。

## 4.PPPoE协议的实现过程报文分析

### 4.0发现阶段(PPPoE Discovery)

PPPoE标记实例：



### 4.1 发现阶段(PPPoE Discovery)

PPPOE发现阶段的交互过程包括4步，有四个包，即PADI，PADO，PADR，PADS。PPPoE Discovery的帧类型值(TYPE)为0x8863。

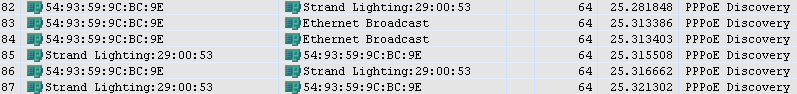


图5 PPPoE Discovery交互示意图

### 4.1.1 PADI(Active Discovery Initiation)

用户主机发出主动发现初始包（PADI）。以太网目的地址为广播地址(FF:FF:FF:FF:FF:FF)，CODE字段为0x09， SESSION\_ID为0x0000。

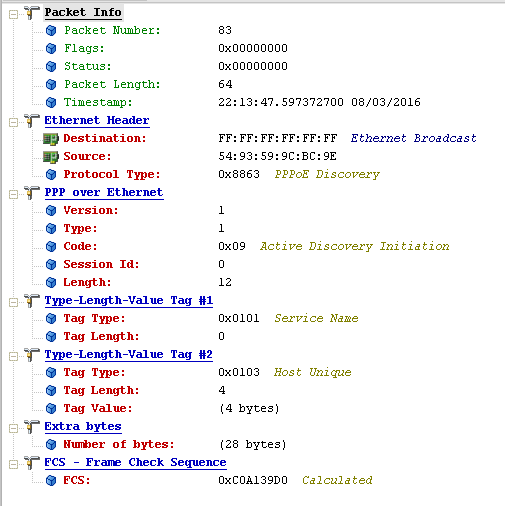


图6 PADI详细报文

### 4.1.2 PADO(Active Discovery Offer)

接入设备收到在服务范围内的PADI包后，发送主动发现提供包（PADO)以响应请求。其CODE字段为0x07,SESSION\_ID为0x0000。PADO包必须包含一个接入设备名称（AC-Name）类型的标签（标签类型字段为0x0102）以及一个或多个服务名称类型标签，表明可向用户主机提供的服务种类。

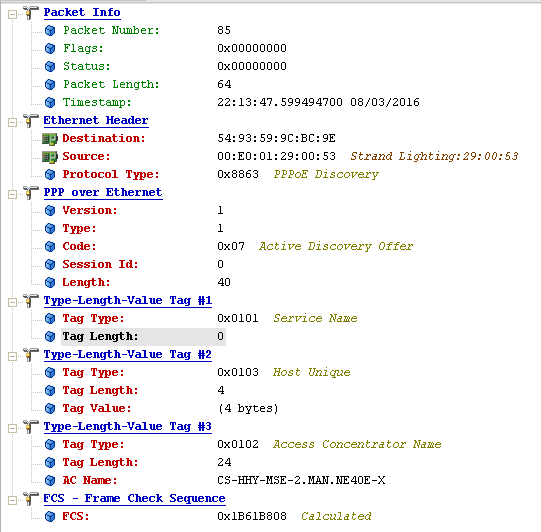


图7 PADO详细报文

### 4.1.3 PADR(Active Discovery Request)

用户主机在可能收到的多个PADO包中选择一个合适的接入设备，选择的原则是根据PADO中接入设备名称类型标签和服务名称类型标签的内容。然后向所选择的接入设备发送PPPOE主动发现请求（PADR）包。其CODE字段为0x19，SESSION\_ID为0x0000。PADR包必须包一个服务名称类型标签，确定向接入设备请求的服务种类。当一个用户主机在确定时间没有收到PADO，他会重发一个PADI，同时等待两倍的时间。这种过程可以根据需要重复多次。

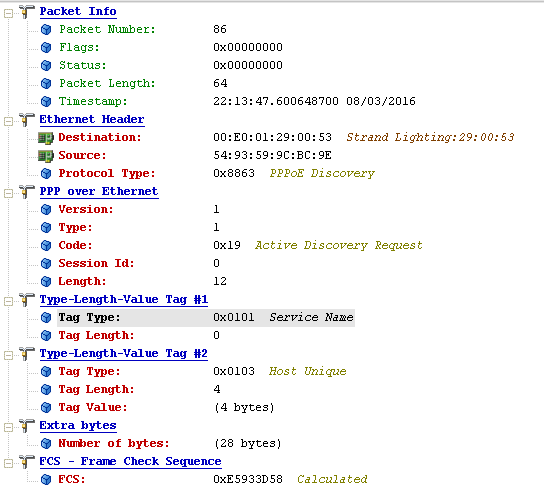


 图8 PADR详细报文

### 4.1.4 PADS(Active Discovery Session-confirmation)

接入设备收到PADR包后准备开始PPP会话，它发送一个主动发现会话确认（PADS）包，返回一个会话号。其CODE字段为0x65，SESSION\_ID为接入设备所产生的一个唯一的PPPOE会话标识号码。



 图9 PADS详细报文

### 4.2 会话阶段

PPPoE会话阶段（PPP连接建立）主要分LCP协商阶段、认证阶段、IPCP阶段等，在这些阶段顺利完成后，就可以进行数据传输了。

### 4.2.1 链路控制协议LCP(Link Control Protocol)

此阶段主要是协商链路的一些参数，如最大接收单元MRU、Magic Number，以及后续认证时使用的协议等。LCP协商分为Configure Request，Configure Ack，Terminate Request,Echo Request。

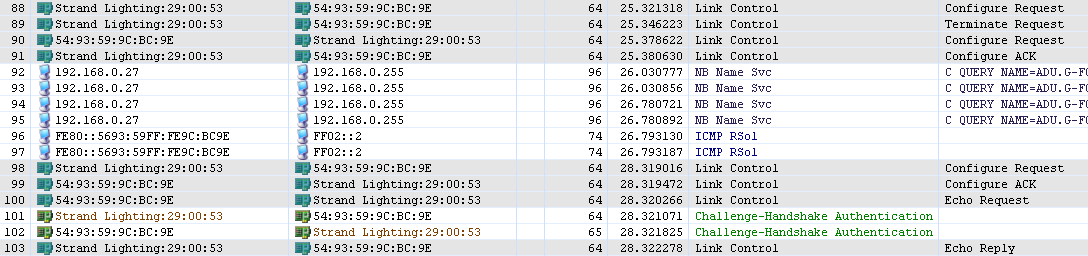


 图10 LCP交互示意图

SessionID就是PADS获得的SessionID，主要协商了MRU（Maximun Receive Ubit），并且提出认证使用的Magic Number。一般而言，MRU和MTU取值相同，PPPOE的最大MTU不能超过1492。计算方法如下:

首先，以太网帧大小限制：

Ethernet MinSize = 64 Byte

Ethernet MaxSize = 1518 Byte

去掉以太帧头(6字节SRCMAC+6字节DSTMAC+2字节TYPE+4字节CRC)后的净荷为：

EthernetIP MTU =1518–18= 1500 Byte

所以，再去掉(6字节PPPoE\_SESSION+2字节PPP\_HEADER)的开销，所以PPPOE的MRU最大值为：

PPPoE MTU/MRU=1500–8=1492Byte。

Magic-number选项用来协商双方的魔数，两端魔数不能重复，魔数可用来检测链路的环回情况。

该选项提供了一种探测短路连接和其它数据链路层异常的方法。当一方接收到带有魔数选项的配置请求数据帧后，将接收到的魔数与上次发送的魔数进行比较，如果不相同就认为没有发生短路。如果两个魔数相同，则需要发送一个携带不同魔数的配置否认帧，然后将接收到的魔数与发送的魔数进行比较。

在广域链路上，最常用的一种检测链路的方法就是在远端将发送和接收短接成环路，在本端发送的信号如果能被自己成功的接收到，那么线路就有可能是Ok的，这就是LoopBack测试。如果环路在测试之后并未撤掉，PPP又没有引入Magic-Number的话，就可能自己和自己建立PPP关系。

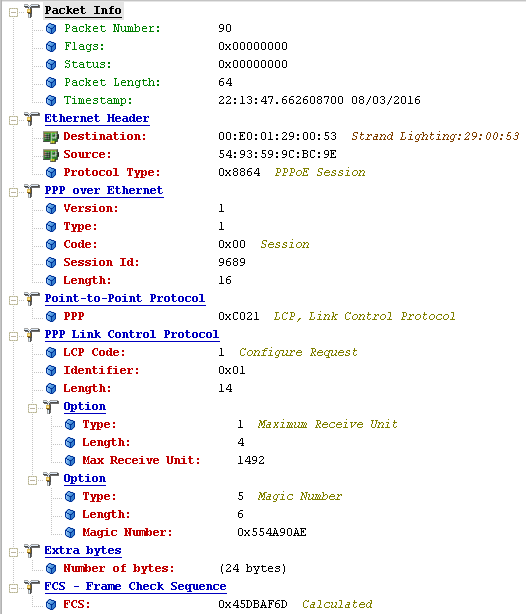


 图11 C→S Configure Request



 图12 S→C Configure Ack

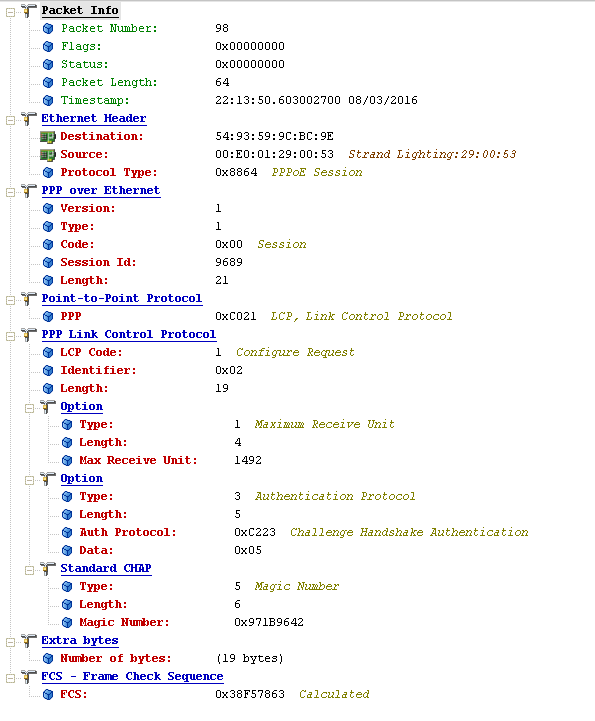


 图13 S→C Configure Request

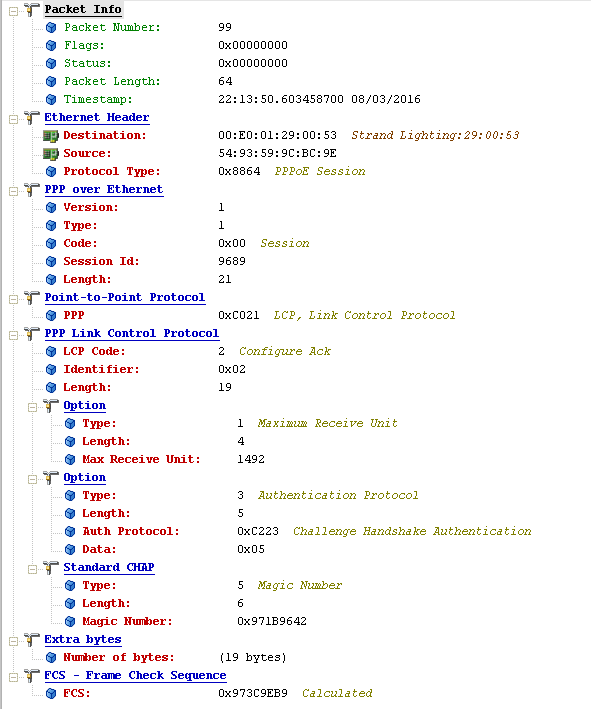


 图14 C→S Configure Ack

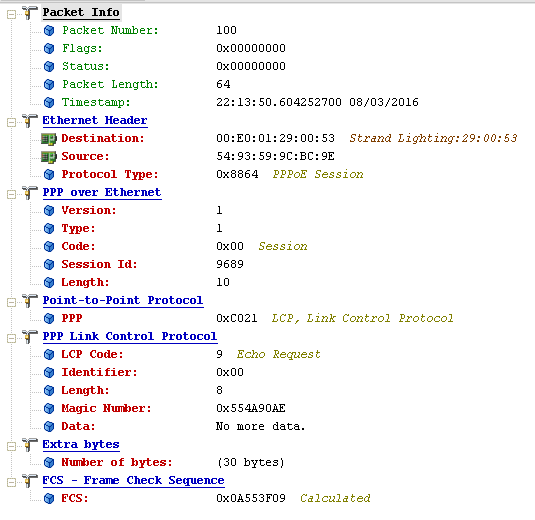


 图15 C→S echo

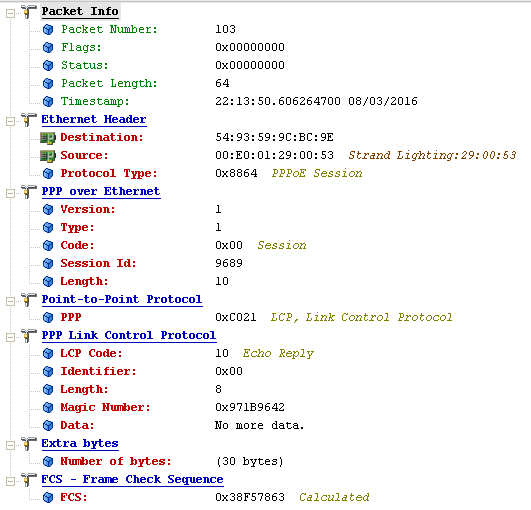


 图16 S→C echo

### 4.2.2 认证阶段

认证阶段服务器端将验证客户端的合法性。最常见的两种就是PAP和CHAP；

PAP（Password Authentication Protocol）验证为两次握手验证，密码为明文。

PAP验证的过程如下：

(1)被验证方发送用户名和密码到验证方；

(2)验证方根据本端用户表查看是否有此用户以及密码是否正确，然后返回不同的响应。

注意：PAP不是一种安全的验证协议。当验证时，口令以明文方式在链路上发送，并且由于完成PPP链路建立后，被验证方会不停地在链路上反复发送用户名和口令，直到身份验证过程结束，所以不能防止攻击。

CHAP（Challenge-Handshake Authentication Protocol）验证为三次握手验证，密码为密文（密钥）。

CHAP验证过程如下：

(1)Challenge：验证方主动发起验证请求，验证方向被验证方发送一些随机产生的报文，并同时将本端的用户名附带上一起发送给被验证方；

(2)Response：若被验证方接到验证方的验证请求后，检查本端接口上是否配置了缺省的CHAP密码，如果配置了则被验证方利用报文ID、该缺省密码和MD5算法对该随机报文进行加密，将生成的密文和自己的用户名发回验证方；若被验证方检查发现本端接口上没有配置缺省的CHAP密码，则被验证方根据此报文中验证方的用户名在本端的用户表查找该用户对应的密码，如果在用户表找到了与验证方用户名相同的用户，便利用报文ID、此用户的密钥（密码）和MD5算法对该随机报文进行加密，将生成的密文和被验证方自己的用户名发回验证方；

(3)result:验证方用自己保存的被验证方密码和MD5算法对原随机报文加密，比较二者的密文，根据比较结果返回不同的响应。

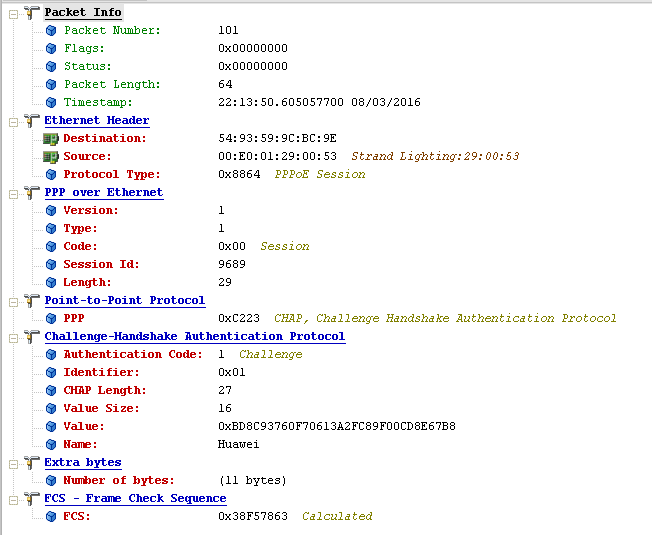


 图17 S→C Challenge



 图18 C→S Response

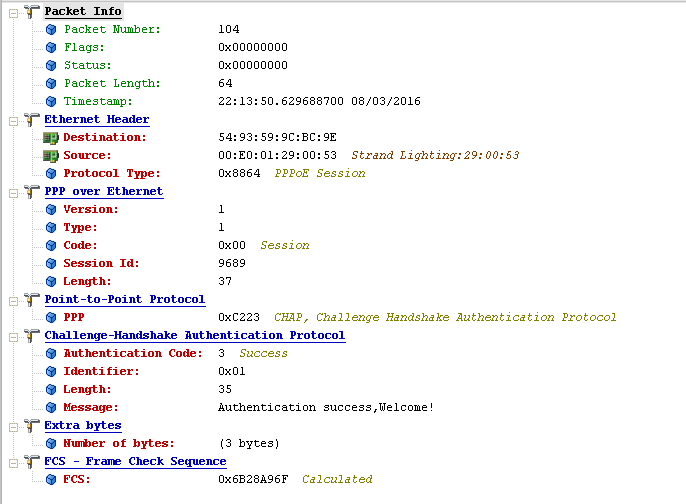


 图19 S→C Sucess

### 4.2.3 IPCP(IP Control Protocol)阶段

此阶段进行IP地址、DNS地址、WINS等的协商。

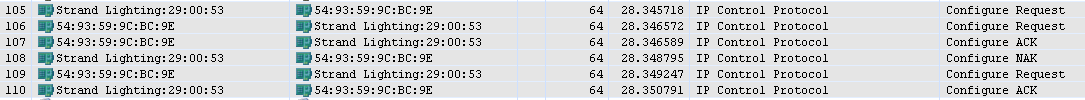


图20 IPCP交互示意图

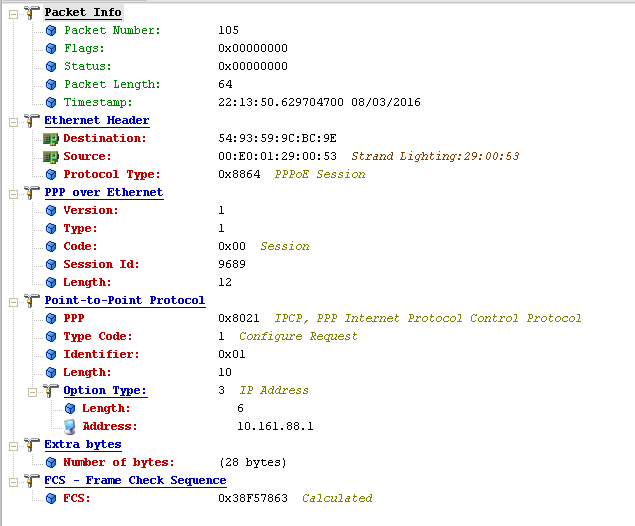


 图21 S→C Configure Request

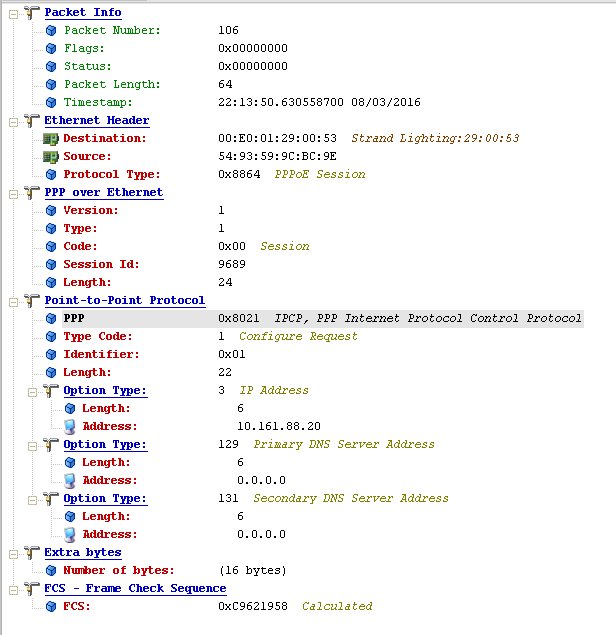


 图22 C→S Configure Request

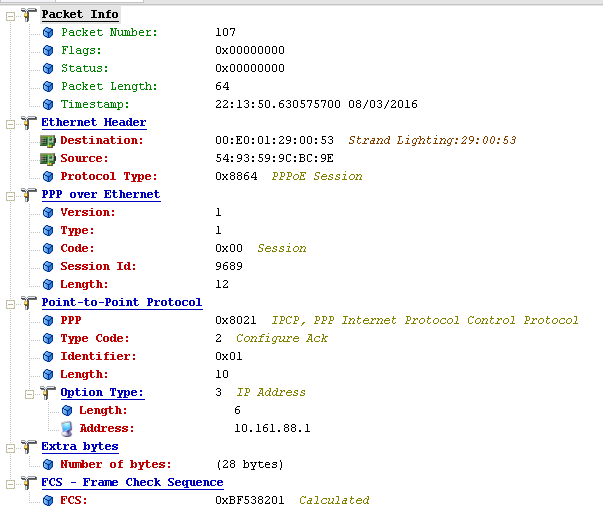


 图23 C→S Configure Ack

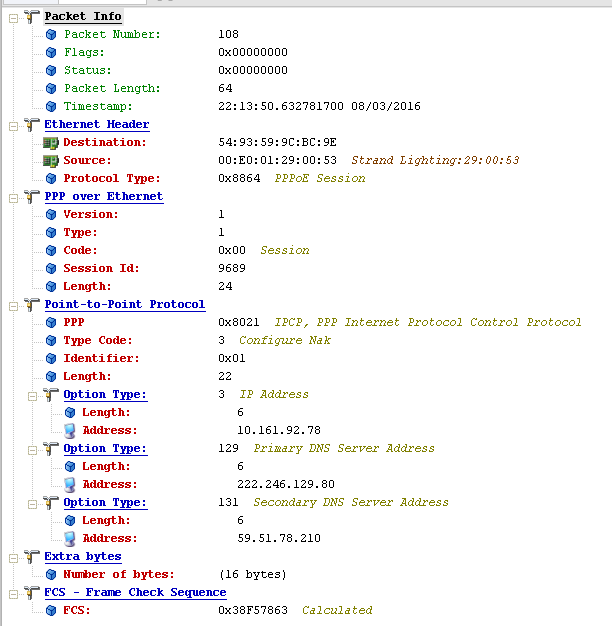


 图24 S→C Configure Nak

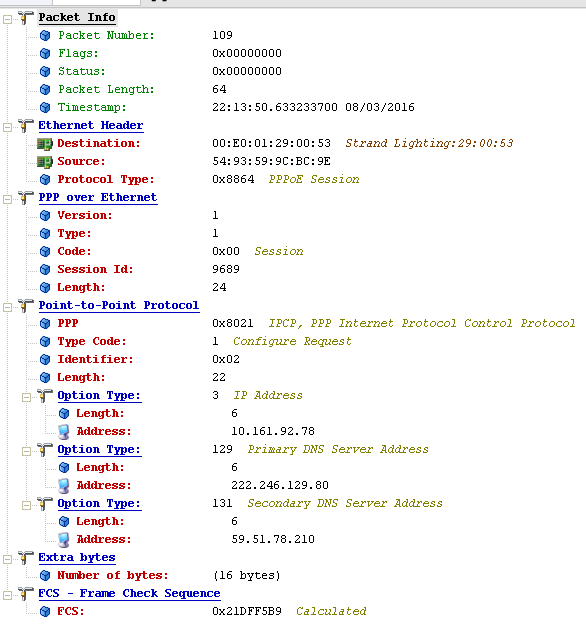


 图25 C→S Configure Request



 图26 S→C Configure Ack

### 4.3数据传输

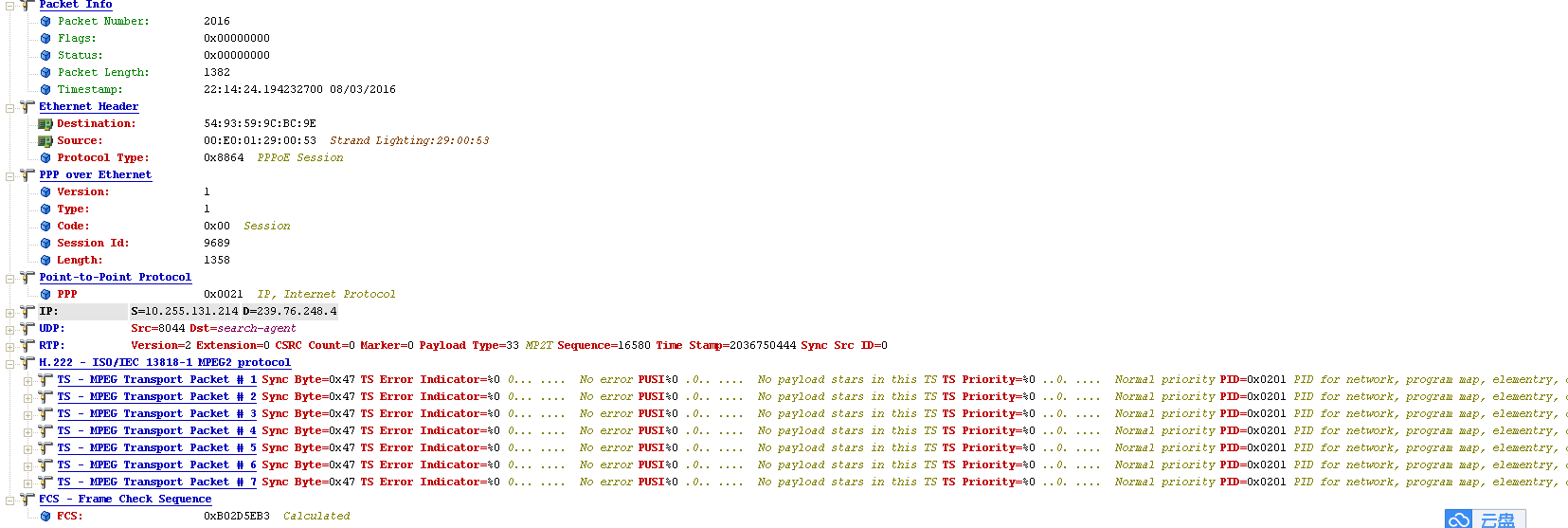


 图27 PPPoE数据传输