 网络协议分析

PPP协议：了解拨号上网

16272203 黄萍萍

**什么是PPP？**

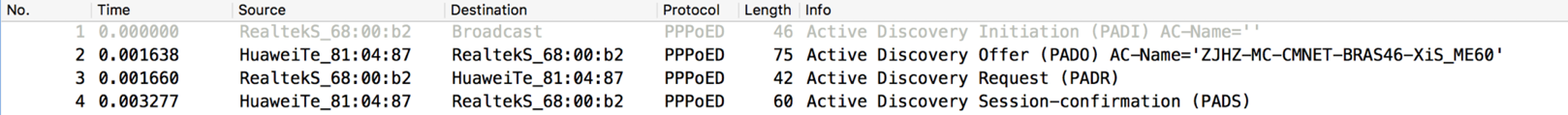
PPP是用于点对点信道的用户PC和服务提供商ISP进行通信时所使用的数据链路层协议。他使用链路控制协议LCP和网络控制协议NCP来创建链路、认证、网络配置。

**工作原理**

PPPoE拨号流程包括两个阶段：发现阶段和会话阶段。

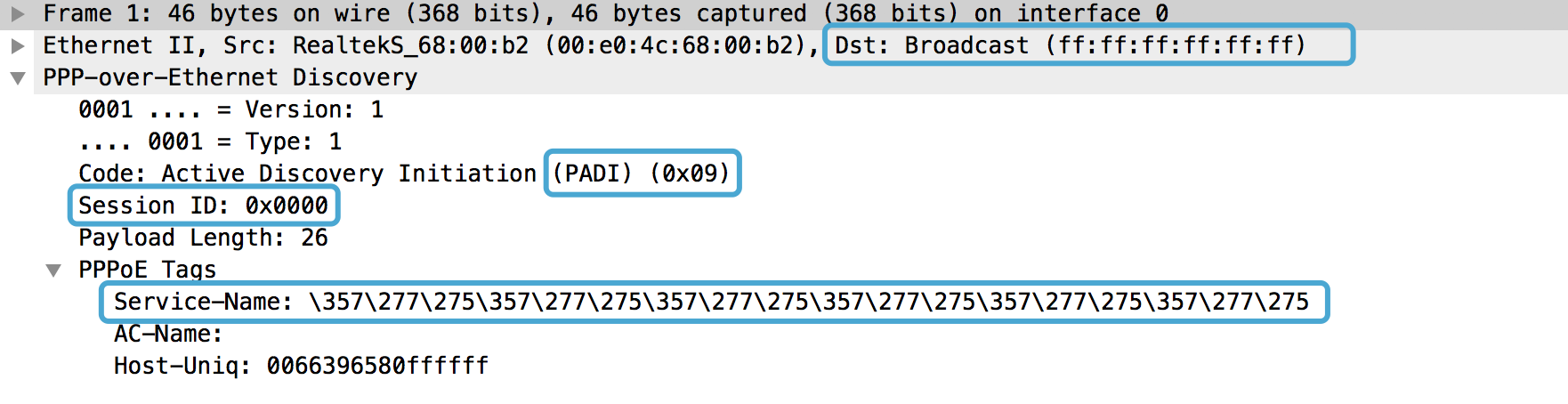
**发现阶段（PPPoED：PPPoE Discovery）：**

该初始阶段链路不可用，无状态，目的是获得 PPPoE 终端（在局端的ADSL设备上）的以太网 MAC 地址，并建立一个唯一的 PPPoE SESSION-ID。



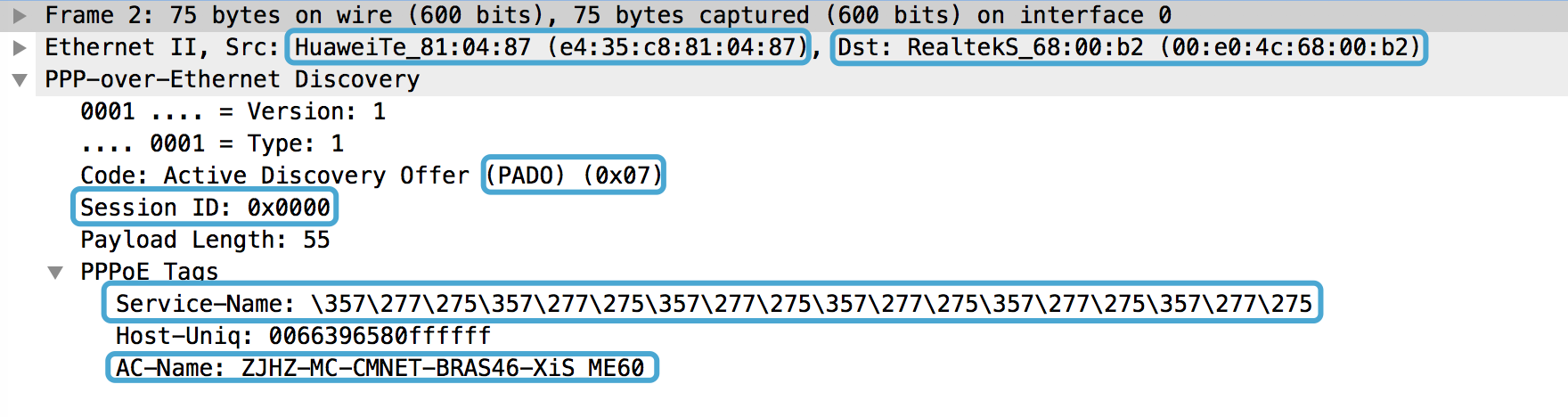
**1.1 PADI（PPPoE Active Discovery Initiation）**

主机RealtekS\_68:00:b2 (00:e0:4c:68:00:b2)发送以以太网广播地址0xffffffffffff为目的地址的分组，寻找PPPoE终端，CODE字段值为0×09（表示PADI Code），SESSION-ID（会话ID）字段值为0x0000，并用Service-Name标识请求的服务名称类型，用以向接入集中器提出所要求的服务。

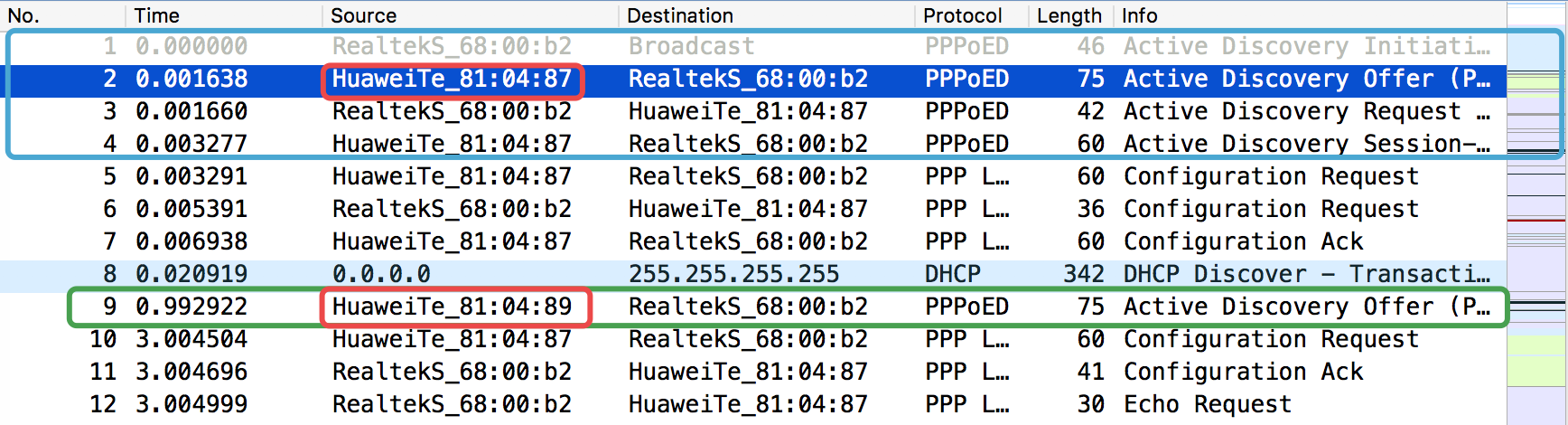


**1.2 PADO（PPPoE Active Discovery Offer）**

接入集中器HuaweiTe\_81:04:87 (e4:35:c8:81:04:87)收到在其服务范围内的PADI分组，发送PPPoE offer报文，响应主机请求。CODE字段值为0×07（表示PADO Code），SESSION-ID字段值仍为0x0000。使用AC-Name（Access Concentrator Name）表示接入集中器名称，用Service-Name标识接入集中器可向主机提供的服务种类的名称。Host-Uniq 值与PADI相同。

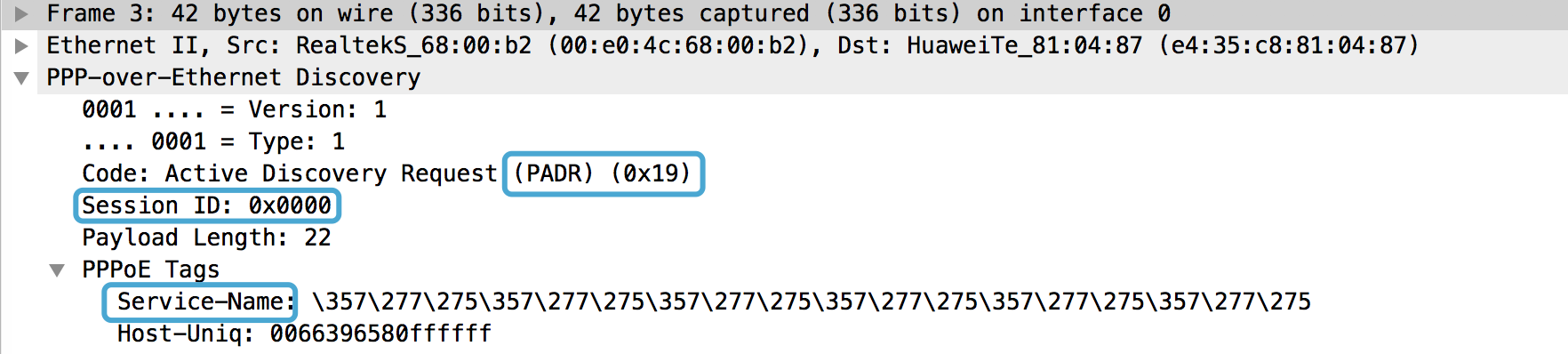


这个过程（discovery）中主机由于发送的是广播请求，可能会收到多个接入集中器响应的PADO offer报文。此时会选择一个合适的PADO进行下一步请求，其他的PADO忽略。如上图向HuaweiTe\_81:04:87进行下一步请求，忽略HuaweiTe\_81:04:89的offer响应。当主机在指定的时间内没有接收到PADO，它会重新发送PADI分组，并且加倍等待时间。此过程会重复指定的数次。



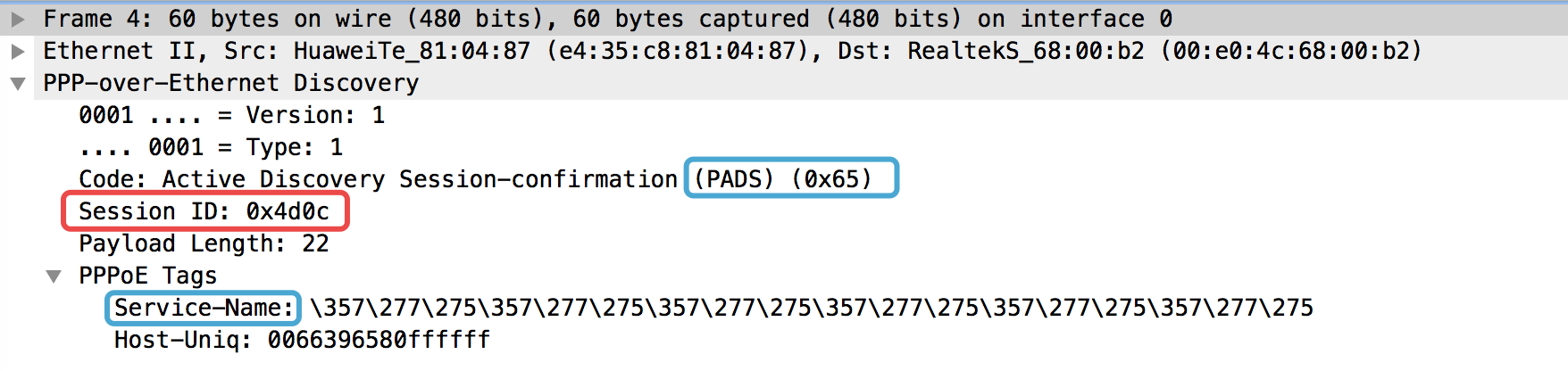
**1.3 PADR（PPPoE Active Discovery Request）**

主机向所选择的接入集中器发送PPPoE Request分组。CODE字段为0x19（PADR Code），SESSION\_ID字段值仍为0x0000。PADR分组Tags中Service-Name标识主机向接入集线器（或交换机）请求的服务种类。



**1.4 PADS（PPPoE Active Discovery Session-confirmation）**

接入集中器收到PADR分组后发送一个PPPoE有效发现会话确认PADS分组。CODE字段值为0×65（PADS Code），SESSION-ID字段值为一个唯一的PPPoE会话标识号码，由接入集中器所产生。Service-Name标签确认向主机提供的服务。PADS和PADR的Host-Uniq Tag值相同。当主机收到PADS分组确认后，双方就进入PPP会话阶段。



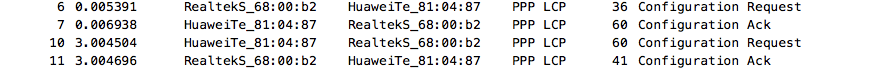
**会话阶段（PPPoES：PPPoE Session）**

**1. 链路建立阶段： LCP协商**

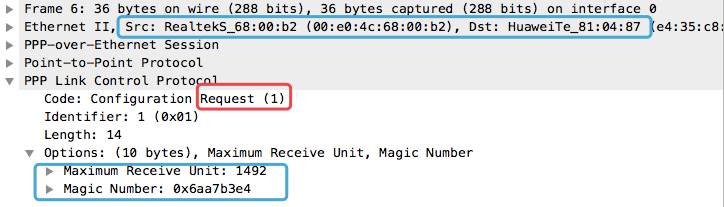
LCP：Link Control Protocol 链路控制协议。

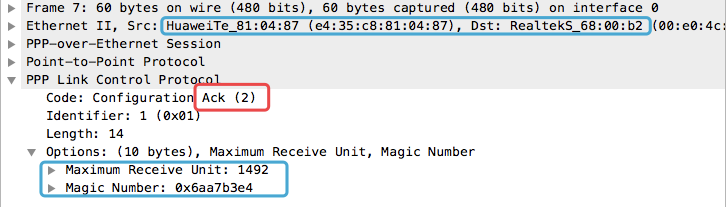
LCP协商过程：

协商双方互相发送一个LCP Configuration-Request报文，并确认收到的Configuration-Request报文中的协商选项，根据这些选项的支持与接受情况，做出适当的回应。此时由报文可见两端都回应了Config-ACK，标志LCP链路建立成功。



对比Request和ACK报文可见，若完全支持对端的LCP选项，则回应Config-ACK报文，报文中完全协带对端Request报文中的选项，且值相同。





**2. 认证阶段： PAP/CHAP认证**

查看数据报可发现，该PPPoE连接采用CHAP进行认证。

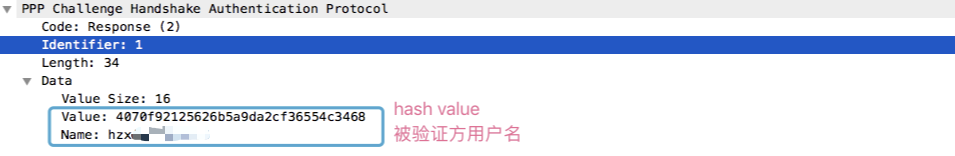
CHAP为三次握手协议，只在网络上传输用户名，不传输用户口令

https://uploader.shimo.im/f/MSIEwbDzNMg5Tivf.png!thumbnail

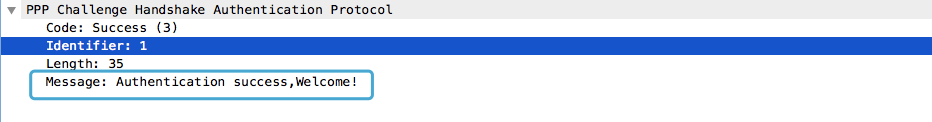
首先由认证方server向被认证方client发送Challenge报文，包含认证序列号identifier，Data部分包含一串随机产生的Value，及认证端的主机名Name。



被认证方收到Challenge后，根据报文中认证方的主机名到本地数据库中查找对应密码，并结合id和value进行hash运算。使用response报文进行应答，id与challenge中的序列号相同，value部分为id，random value，huawei password三者hash的结果，name为被认证方（本地）的认证用户名



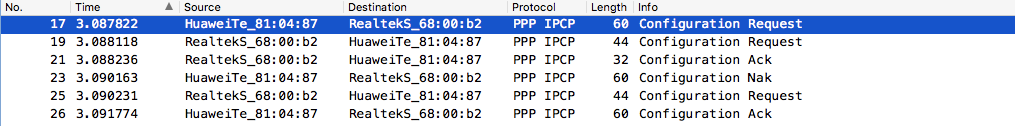
认证方接收response报文，查找被认证方用户名对应的口令，使用相同的hash算法计算id，原value，被认证方password三者的hash值，与收到的response hash进行比较，相同则应答Success报文，告知认证通过。



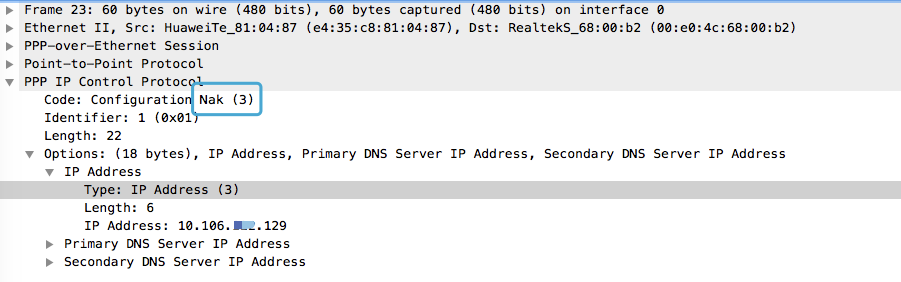
**3. 网络层配置协商阶段：NCP协商**

NCP的主要功能是协商PPP报文的网络层参数，如IP地址，DNS Server IP地址，WINS Server IP地址等。

用户与ME设备之间互相发送NCP Config-Request报文并且互相回应NCP Config-Ack报文后，标志NCP己协商完，用户上线成功，可正常访问网络。



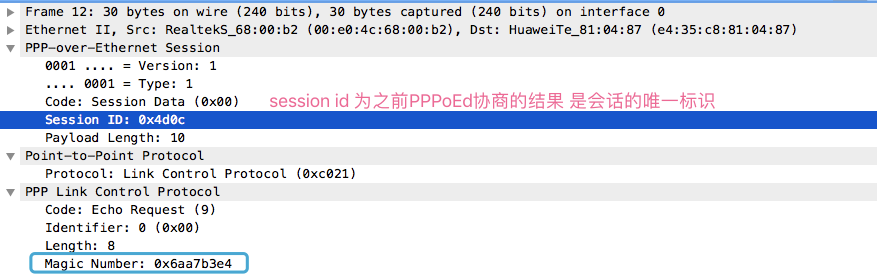
本次PPPoE中使用IPCP进行协商网络层参数。HuaweiTe\_81:04:87 (e4:35:c8:81:04:87)发送的conf-Request中说明了HuaweiTe\_81:04:87 的ip地址，主机回应ack确认。同时，HuaweiTe\_81:04:87 在用于回应主机发出的conf-Request的conf-Nak中给出了主机可用的ip地址、首选dns服务器、备用dns服务器。



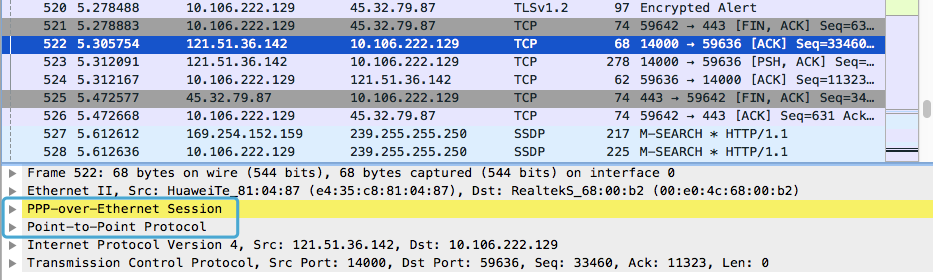
**4. PPP会话维持阶段：定时发送Echo Request、响应Echo Reply**

连接建立中还包含有Echo-Request/Echo-Reply数据帧，用于训练双方通信的数据链路层上的循环通信机制。信息域中包含Magic Number，通过发送和接收到的megic number是否相同来探测短路连接和其它数据链路层异常。如下

https://uploader.shimo.im/f/5V3jW5o3R8gFa3Mf.png!thumbnail



用户正常访问网络过程中数据传输都基于PPP。



**5. 网络终止阶段： 终止PPP会话，回到链路不可用阶段。**

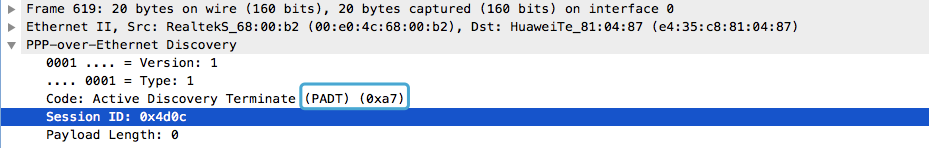
主机在建立会话后，LCP协议发送Terminate-Request和Terminate-Reply报文来终止一条链路

https://uploader.shimo.im/f/x4rmpX5kfp0R1kpm.png!thumbnail

最后，主机发送PADT（PPPOE Active Discovery Terminate）分组，用于终止连接，对端步骤回应。

https://uploader.shimo.im/f/VAxG2XLgE8MMFU4I.png!thumbnail

PADT报文的session id为该会话的session id。



至此，PPP会话释放完成。