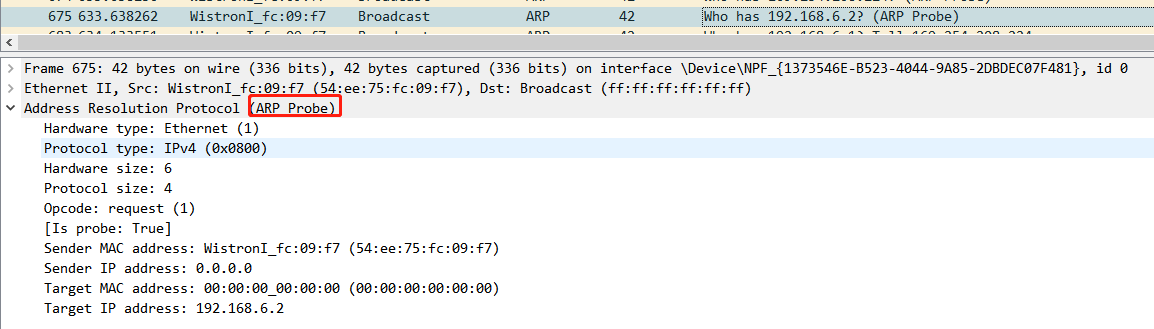
1. **ARP协议**

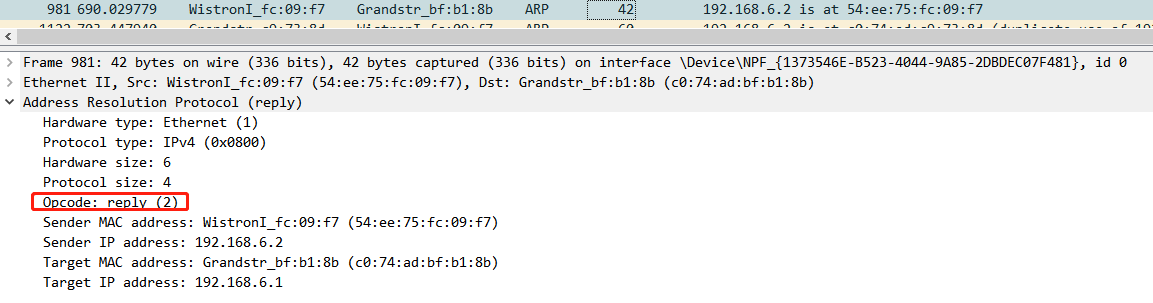
ARP请求触发机制：源主机已知目标主机的IP地址，数据在二层中需要通过MAC地址进行传输，但源主机未知目标主机的MAC地址，就需要发起ARP请求将目的IP地址解析出MAC地址。源主机发起ARP请求，给目的主机发送request报文，报文中包含想要获取主机的MAC的信息和已知目的主机的IP地址等。目的主机收到request报文，返回一个reply报文，其中携带了源、目的主机相应的MAC地址和IP地址等

1.1 ARP报文类型

1.1.1 arp probe(request)，用于检测当前的广播域中是否有其他设备使用这个IP

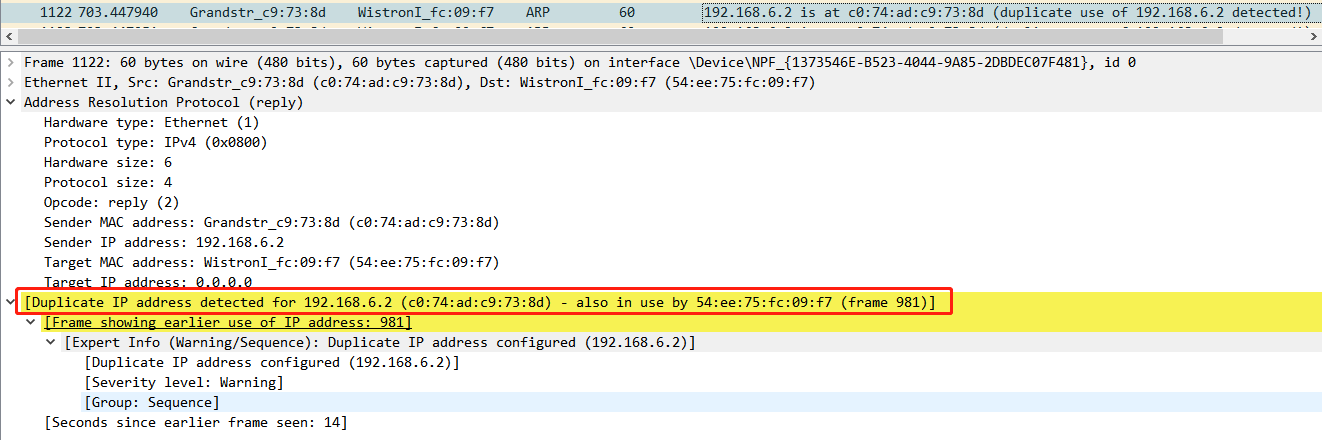
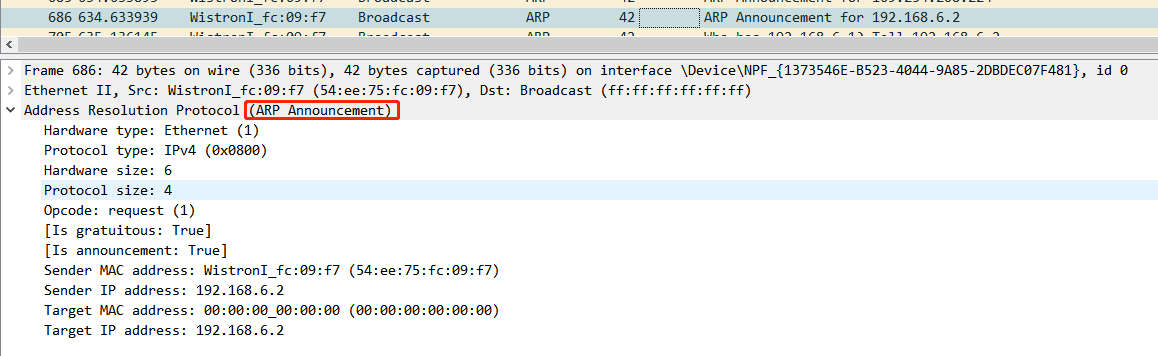


1.1.2 arp reply，若是该广播域中有设备使用arp probe(request)报文中的IP地址，在返回给主机一个reply报文，有说明使用这个IP的设备信息，如MAC,网关地址等



1.1.3 arp gratuitous request/reply（暂时未抓取到）

1.1.4 arp announcement(reply)：用于通知其他本机，本机要使用某个IP地址了，是一个SenderIP和Traget IP填充的都是本机IP地址的ARP request。这会让所有主机都会更新自己的ARP cache，将IP地址映射到发送者的MAC地址



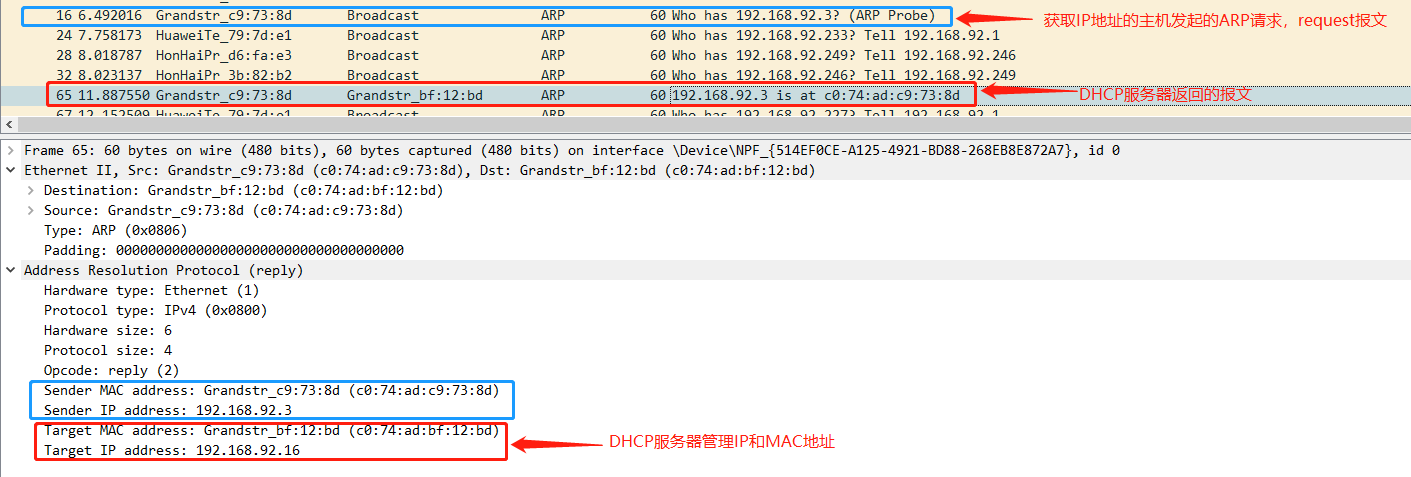
主机或者设备端口获取IP地址的形式：

1.2通过静态方式获取IP地址

1.3通过DHCP方式获取IP地址

目的主机通过DHCP方式获取的IP地址，首先进行的是IP地址检测，目的主机获取到IP地址后会发送一个免费ARP报文（ARP Probe）给DHCP服务器，以检测目的主机获取的IP是否存在地址冲突，若不冲突即返回一个reply报文。若IP地址冲突,返回一个Decline报文给DHCP 服务器，之后再则重新请求一个IP地址，再返回有个reply报文。

1.3.1 交换机作为路由设备wan口的DHCP服务器,在交换机上开启DHCP服务器功能，并配置相应的DHCP地址池（备注：截图中是交换机作为DHCP服务器的情况）



1.3.2路由设备作为wan口DHCP服务器，通过另外一台路由设备建立vlan的形式创建DHCP地址池，实现路由设备动态获取端口IP地址，如GWN 7002作为DHCP服务器，GWN 7003的设备wan口通过接入GWN 7002获取IP地址

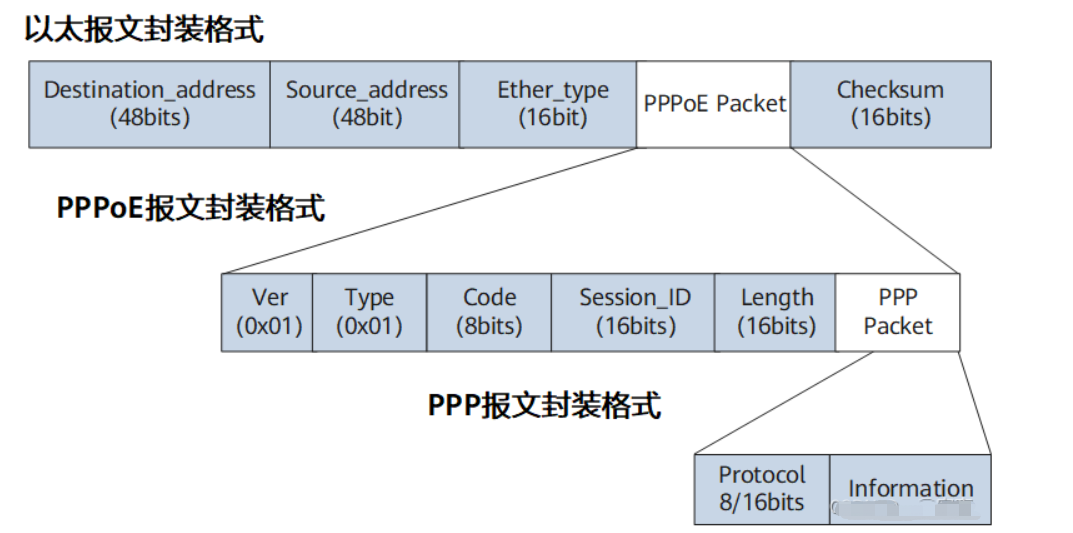
1.3.3路由设备作为LAN口DHCP服务器，通过建立vlan的形式创建DHCP地址池，实现接入lan口的设备动态获取端口IP地址

1. **PPPoE**

PPPoE（Point-to-Point Protocol over Ethernet）协议，又称作以太网上的点对点协议，PPPoE采用客户端-服务器（C/S）方，应用在链路层。它通过在以太网上提供点到点的连接，建立PPP会话，封装PPP报文为PPPoE报文。PPPoE技术可以将用户连接到远程接入设备上，并提供良好访问控制功能，提供了一种经济的用户接入技术，并实现了对用户的控制，PPPoE特点如下

1. PPPoE由于集成了PPP协议，实现了传统以太网不能提供的身份验证、加密以及压缩等功能。
2. PPPoE通过唯一的Session ID可以很好的保障用户的安全性。
3. PPPoE拨号上网作为一种最常见的方式让终端设备能够连接ISP从而实现宽带接入。
4. PPPoE可用于缆线调制解调器（Cable Modem）和数字用户线路（DSL）等以太网线，通过以太网协议向用户提供接入服务的协议体系。

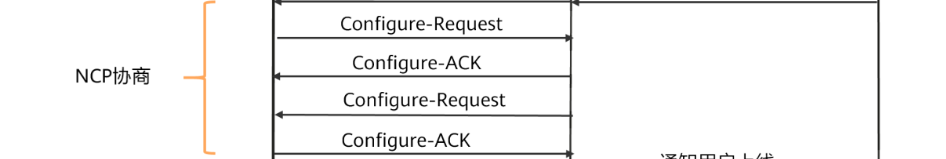
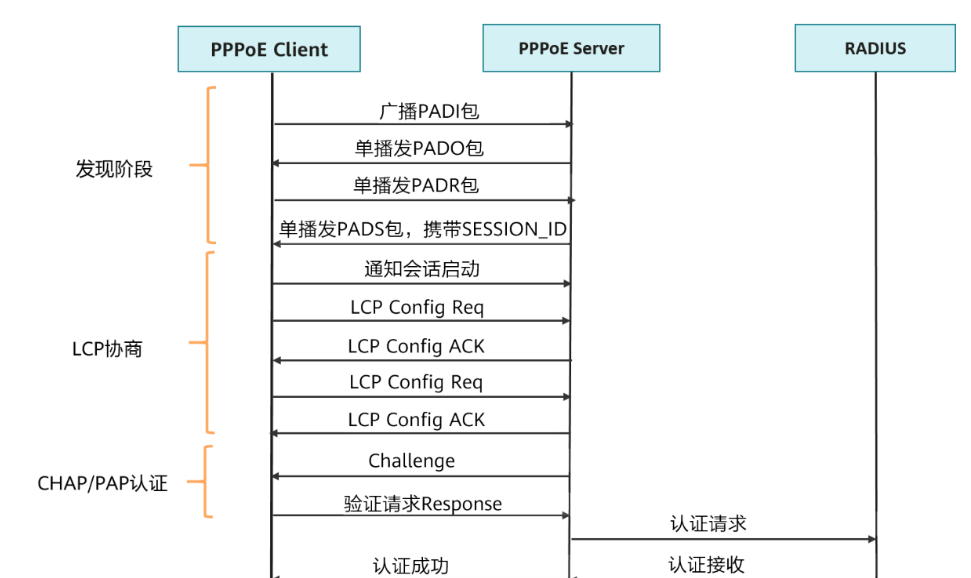
那PPPoE的报文结构是什么样的呢？



1. Destination\_address：一个以太网单播目的地址或者以太网广播地址（0xffffffff）。对于Discovery数据包来说，该域的值是单播或者广播地址，PPPoE Client寻找PPPoE Server的过程使用广播地址，确认PPPoE Server后使用单播地址。
2. Source\_address：源设备的以太网MAC地址。
3. Ether\_type：设置为0x8863（Discovery阶段）或者0x8864（Session阶段）。
4. Ver：PPPoE版本号，值为0x1。 Type域：4bits，PPPoE类型，值为0x1。
5. Code：PPPoE报文类型。PPPOE对应各自报文类型详细见抓包分析
6. Session\_ID：建立会话的唯一标识值
7. Length：定义PPPoE的Payload域长度。不包括以太网头部和PPPoE头部的长度。
8. 数据：有时也称之为净载荷域，在PPPOE的不同阶段该域内的数据内容会有很大的不同。

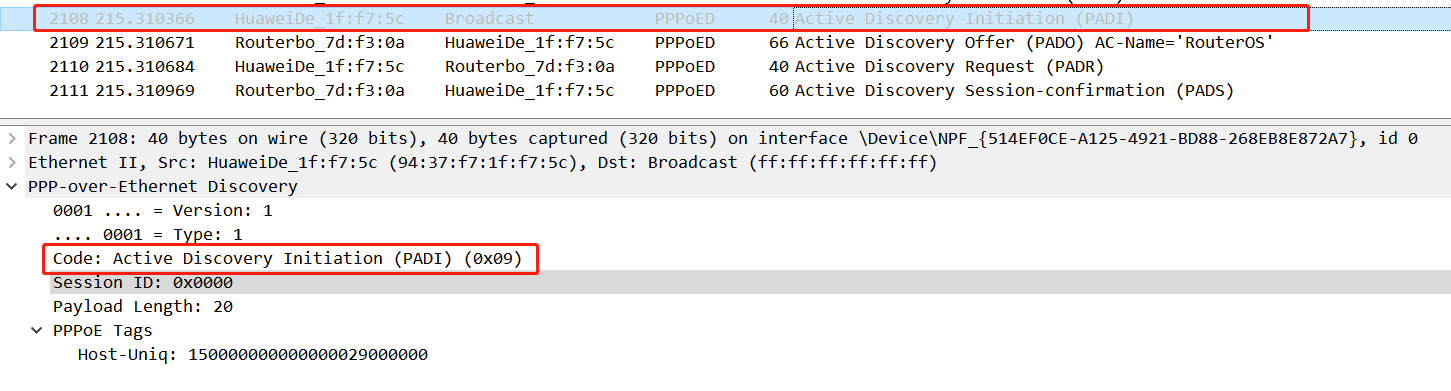
PPPoE交互过程及发送的报文

PPPoE交互过程分为三大阶段,包括发现阶段、会话阶段、结束会话，其中会话阶段包含LCP协商，CHAP/PAP认证、NCP协商三个阶段，会话建立成功之后即可传输数据



发现（Discovery）有4个部分，完成Discover阶段后，双方都知道PPPoE的会话ID和对方的以太网地址，他们共同确定了唯一的PPPoE会话，其中前三个发送的包Ssession ID值为0，0代表会话未建立，只有最后一个包才含有会话的唯一标识值

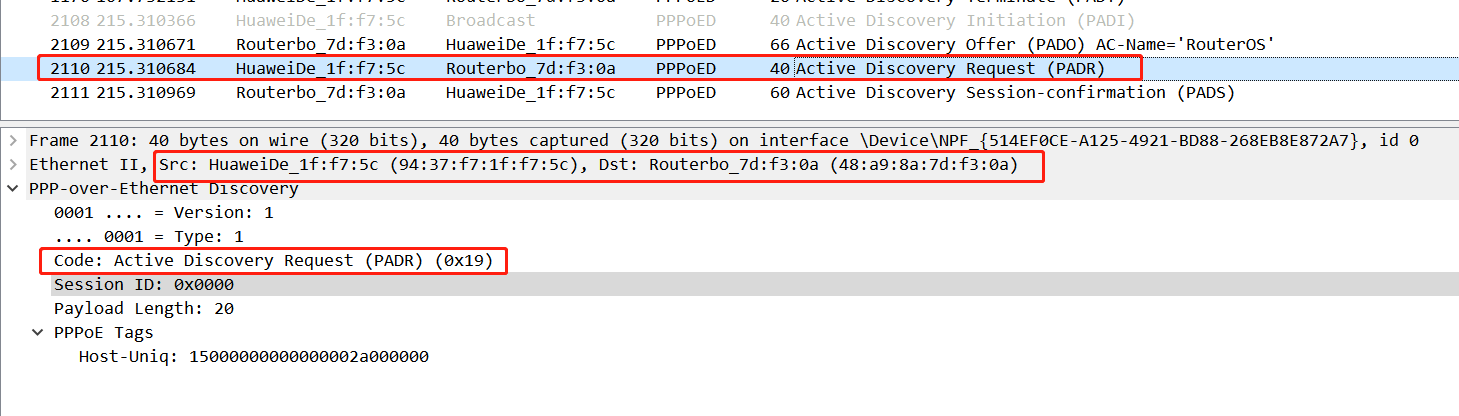
1. 广播PADI（PPPoE Active Discovery Initial）：包含客户端想要得到的服务信息类型，是由客户端发送给服务端，目的MAC地址为广播地址



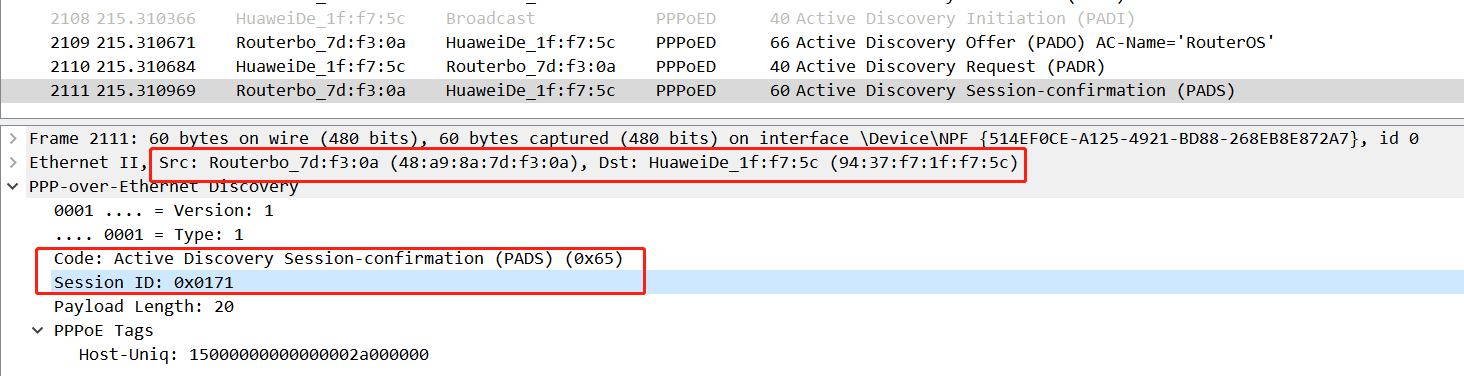
1. 单播PADO（PPPoE Active Discovery Offer）：PPPoE服务器收到PADI报文之后的回应报文PADO，目的MAC地址为客户端主机的MAC地址。



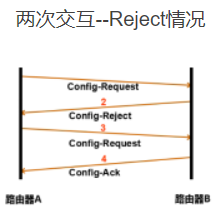
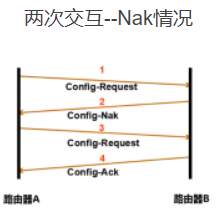
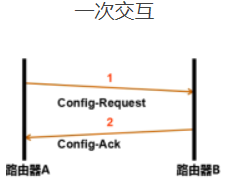
1. 单播PADR（PPPoE Active Discovery Request）：用户主机收到PPPoE服务器回应的PADO报文后，单播发起的请求报文，目的地址为此用户选定的那个PPPoE服务器的MAC地址。



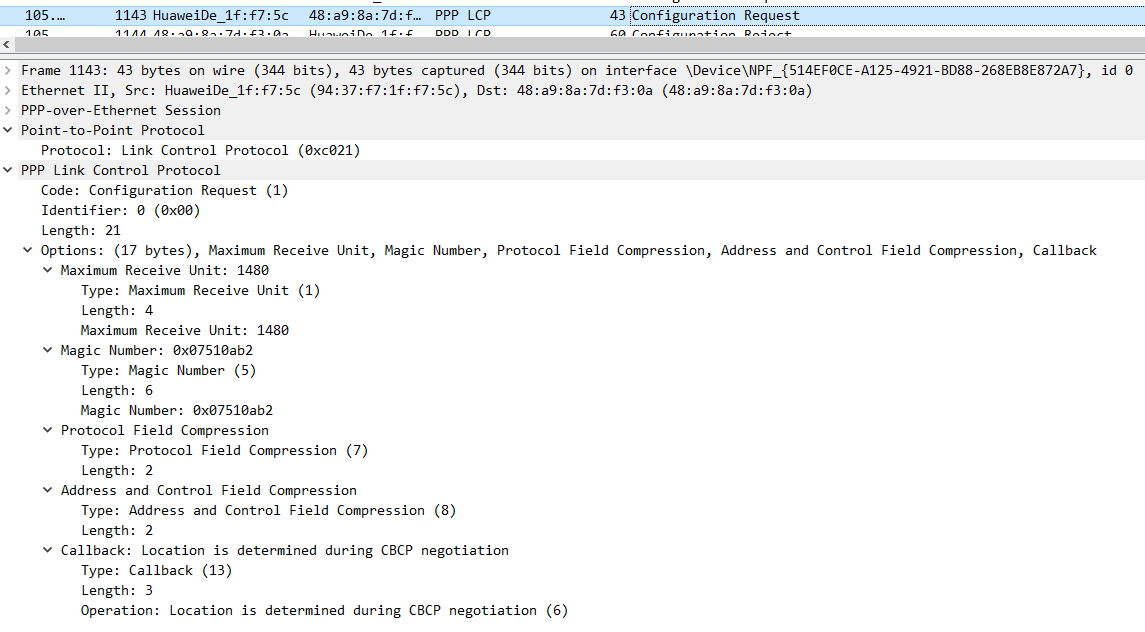
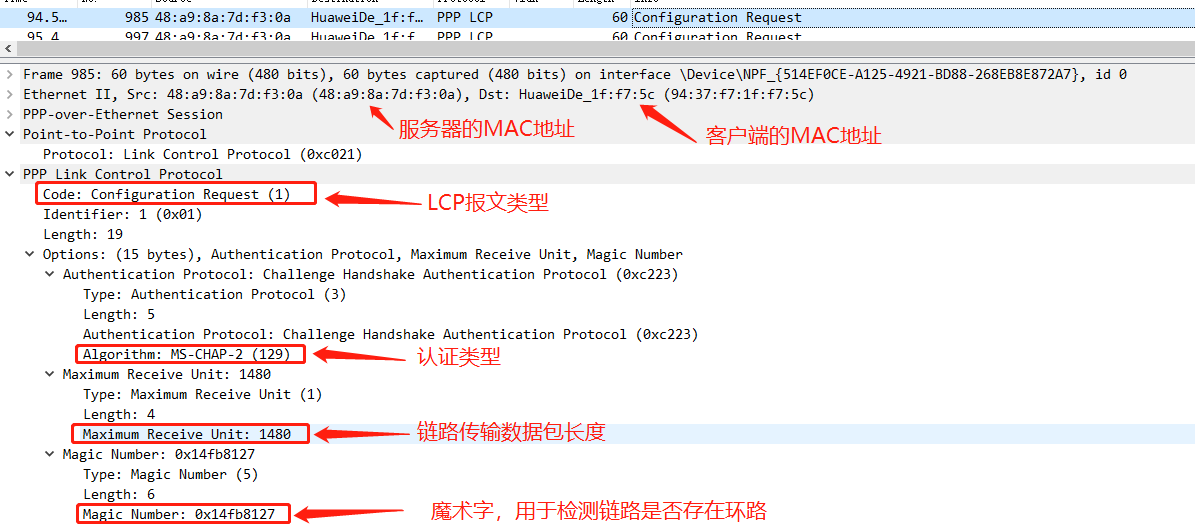
1. 单播PADS（Session-confirmation）：PPPoE Server会产生一个唯一的会话ID，标识和PPPoE Client的这个会话，将会话ID通过PADS发送给客户端



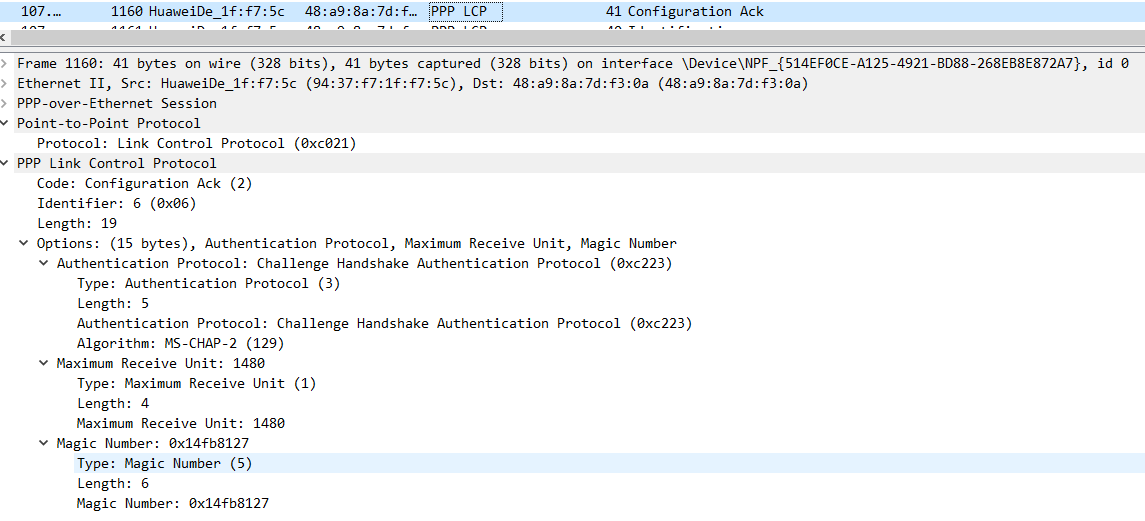
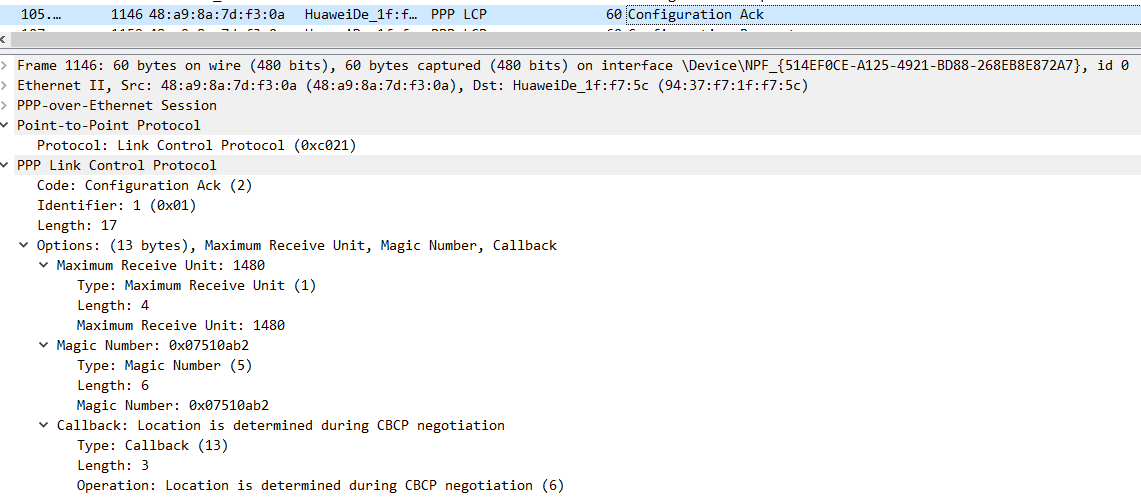
LCP协商，LCP阶段主要完成建立、配置和检测数据链路连接。客户端和服务器双方都回应了Configure-ACK，则标志LCP链路建立成功，否则会继续发送Request报文，其中LCP协商交互中出现四种报文，一次交互只有Config-Request和Config-ACK报文，两次交互会出现Config-NAK或者Config-Reject



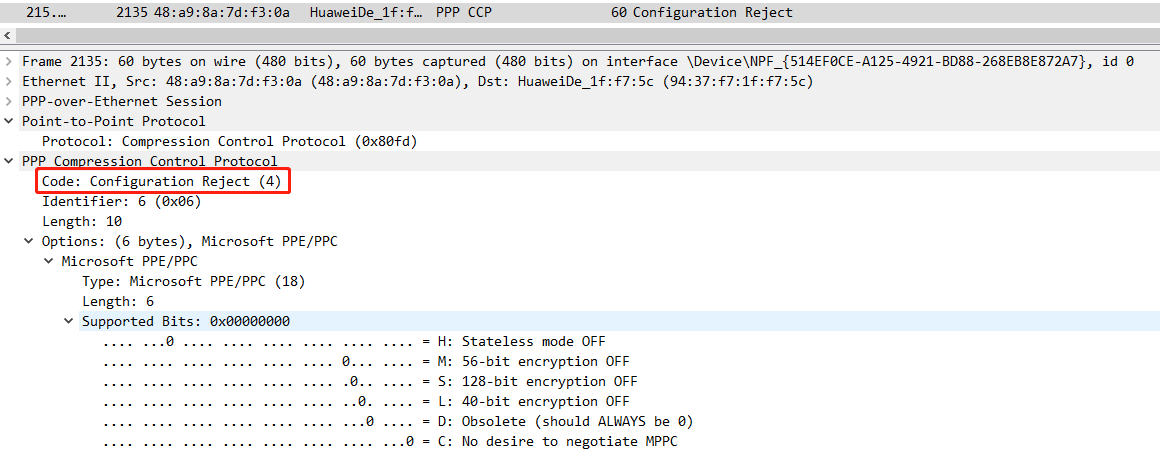
1. Config-Request:双方发送Config-Request报文，包含需要建立链路连接的参数,如认证模式，传输的数据包长度等，第一张图片是服务器发送的，第二张图片是客户端发送的



1. Config-ACK：若完全支持对端的LCP选项，则回应Config-ACK报文，报文中必须完全协带对端Request报文中的选项。第一张图片是服务器发送的，第二张图片是客户端发送的

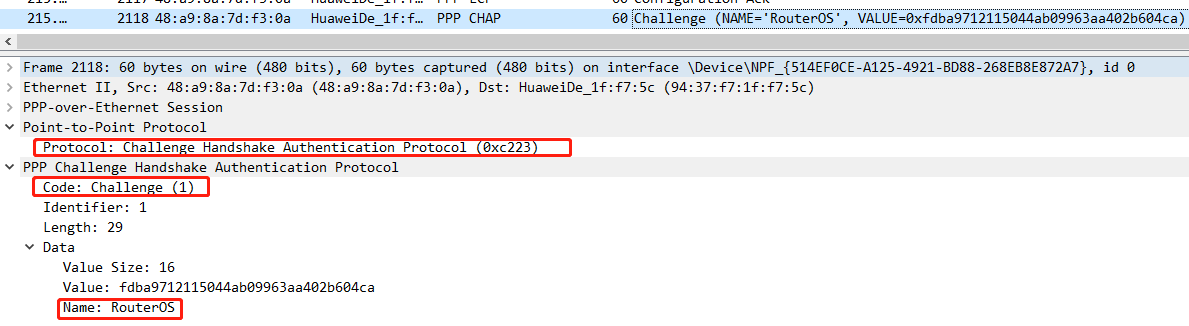


1. Config-NAK：若支持对端的协商选项，但不认可该项协商的内容，则回应Config-NAK报文，在Config-NAK的选项中填上自己期望的内容，如:对端MRU值为1500，而自己期望MRU值为1492，则在Config-NAK报文中埴上自己的期望值1492。两次协商交互出现该报文
2. Config-Reject：若不能支持对端的协商选项，则回应Config-Reject报文，报文中带上不能支持的选项

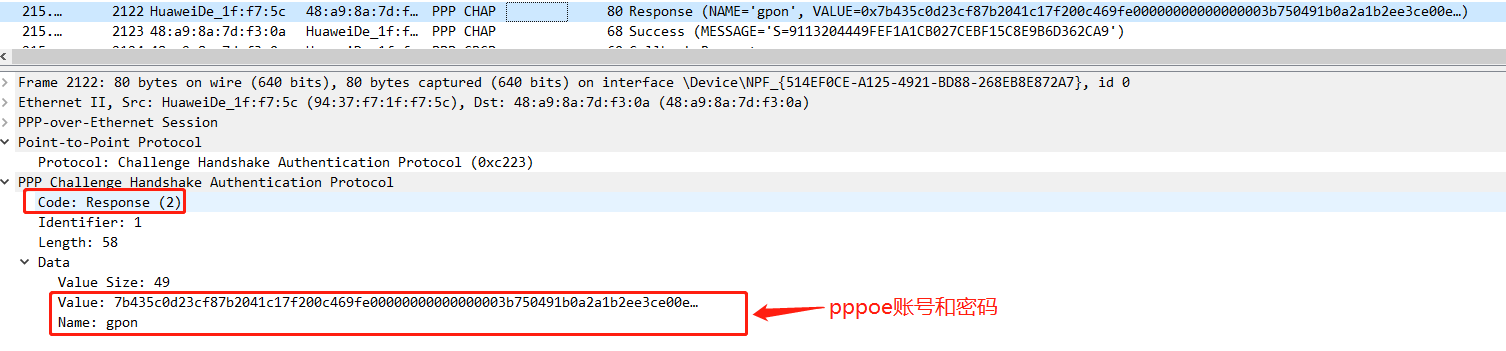


LCP协商成功后，已知认证的方式，开始进行认证，认证协议类型由LCP协商决定。目前搭建的环境默认是CHAP（质询握手认证协议），使用此认证需要进行三次握手，进行密文传输，CHAP三次握手交互过程如下：

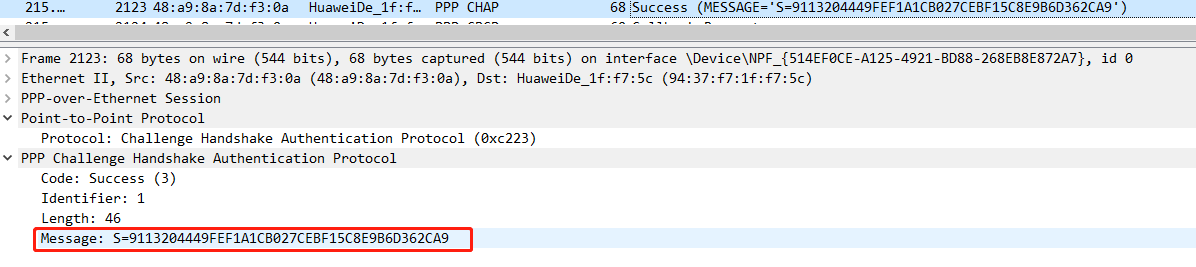
第一次握手：由服务端给客户端发送一个Challenge报文，报文中携带服务端的主机名等参数

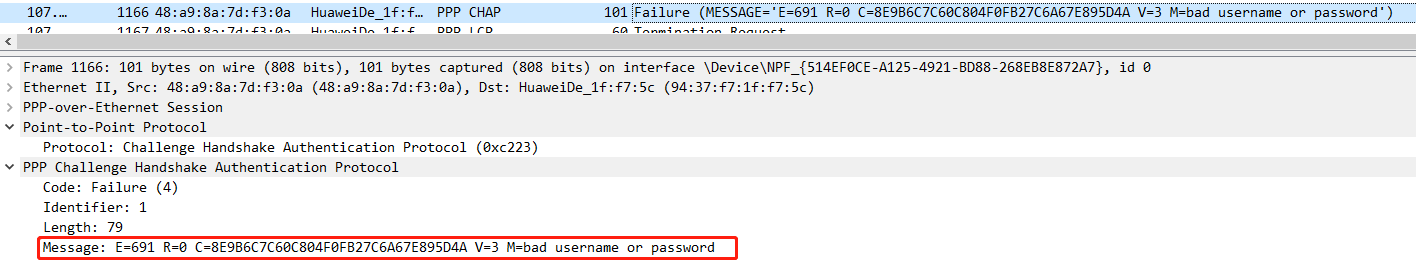


第二次握手：当客户端收到Challenge报文之后，客户端根据报文中的主机名和本机的用户名查找用户口令，查找成功之后将自己的用户名及经过算法生成密文的密码通过response报文发送给服务端



第三次握手：服务端收到客户端的response报文之后，经过认证之后，认证成功，给客户端返回一个success报文，认证失败则返回一个，且报文中由携带失败原因信息，如第二张图中失败的原因是691，代表密码错误或者账户信息到期不能使用等问题

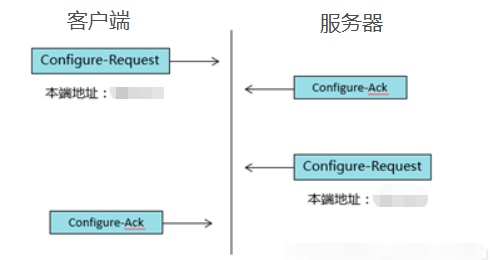




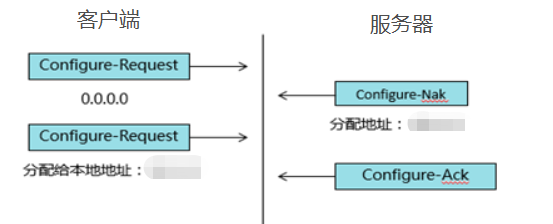
认证成功后，进入NPC阶段，NPC（网络控制协议）是一个协议族，用于配置不同的网络层协议，常用的是IP控制协议（IPCP），IPCP由静态协商和动态协商，它主要负责协商用户的IP地址和DNS服务器地址。两种协商过成如下：

静态协商交互过程

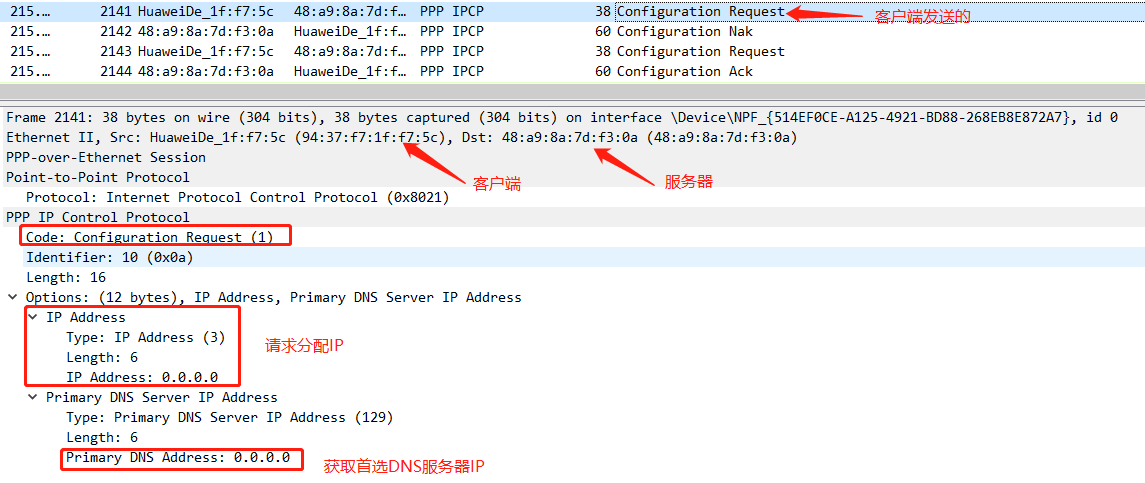
客户端和服务器双方都给对方发送一个Config-Request报文，告诉对端自己的本机IP地址，确认地址是合法的IP地址且没有IP地址冲突*之后进行通信*



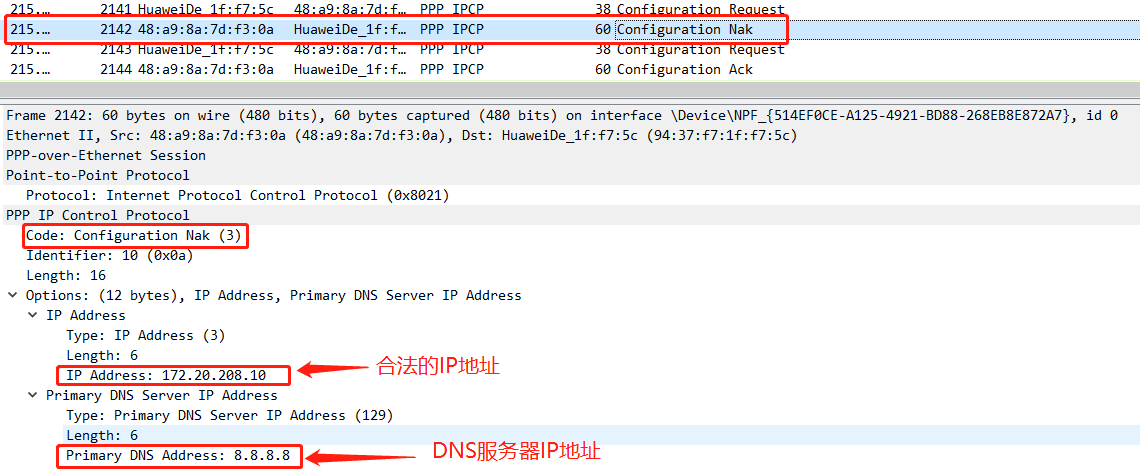
动态协商交互过程



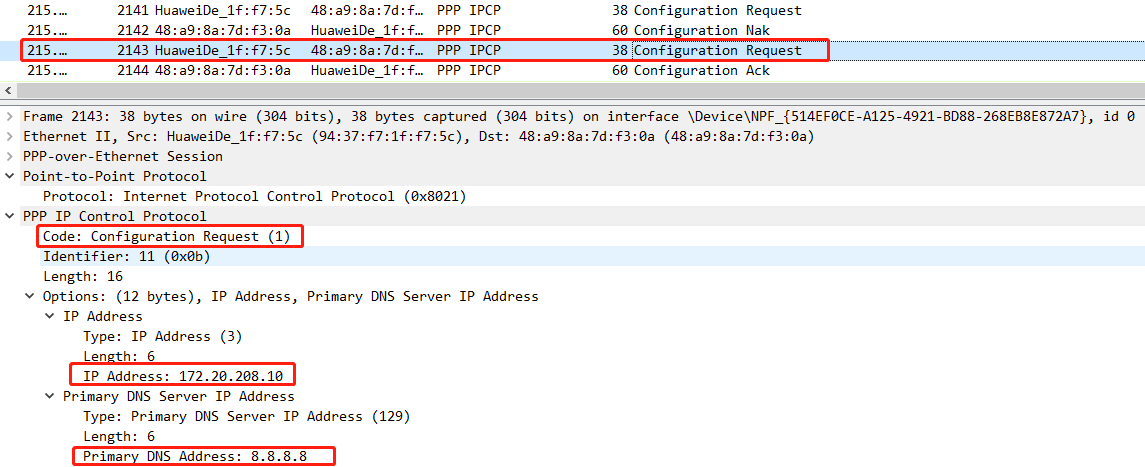
1. 客户端向服务器发送Config-Request报文，用于请求获取IP地址和DNS，且报文中携带不合法的IP地址0.0.0.0



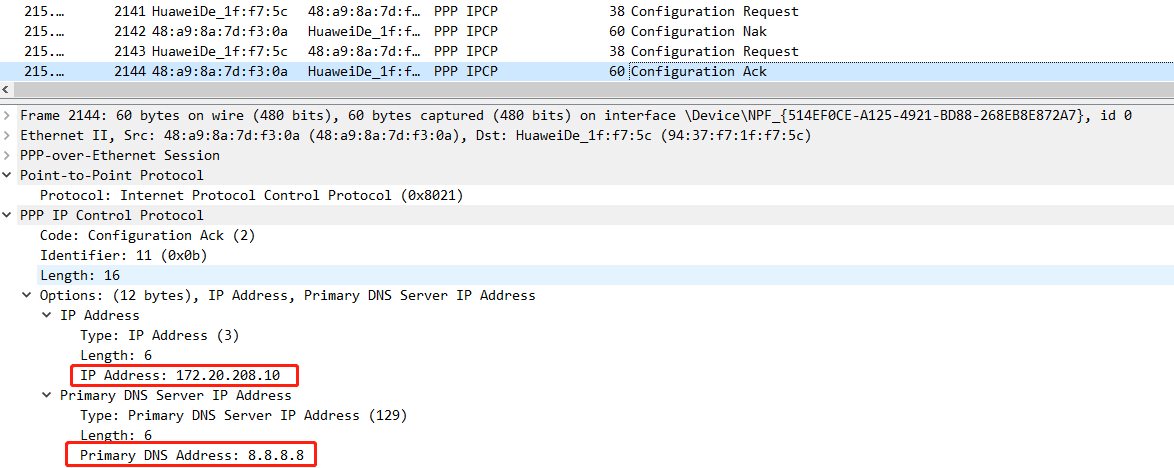
1. 服务器收到Config-Request报文，检测报文中IP地址不合法，想客户端发送Config-Nak报文，其中携带下一个新的且合法的IP地址和DNS



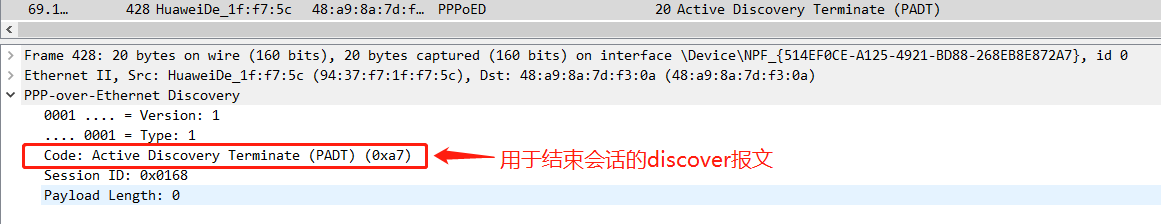
1. 客户端收到来自服务器的Config-Nak报文，更新自己的IP信息，重新发送一个Config-Request报文



1. 服务器再次进行客户端的IP进行检查，确认合法且没有地址冲突之后发送一个Config-Ack报文



NCP协商过程结束之后，用户就可以上线进行网络访问了，想要结束PPPOE会话的时候，服务器或者客户端发送一个PPPOE Active Discovery Terminate报文来结束PPPOE会话，

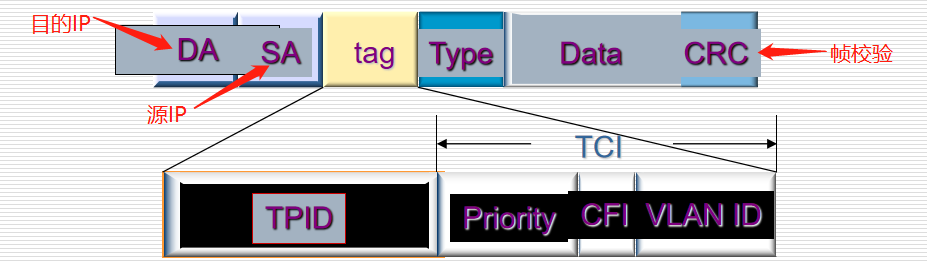


3、Vlan 及PVID

3.1、什么是vlan及vlan的实现

在vlan技术未出现之前，处在同一物理局域网中的所有用户处于同一个广播域，当发生广播风暴的时候影响非常大，vlan的产生，减少了广播风暴的范围及提高网络性能，减少实际物理资源的使用，节约费用等益处。Vlan（Virtual Local Area Network），简称虚拟局域网，将一个物理的局域网在逻辑上划分成多个局域网的通信技术，不同的虚拟局域网具有不同的广播域。实现不同vlan之间的广播域隔离

Vlan在IEEE 802.1Q中定义，通过在数据帧上加入一个tag标签(4字节)来实现的，vlan帧格式如下：



其中tag值中，含有四个参数值：

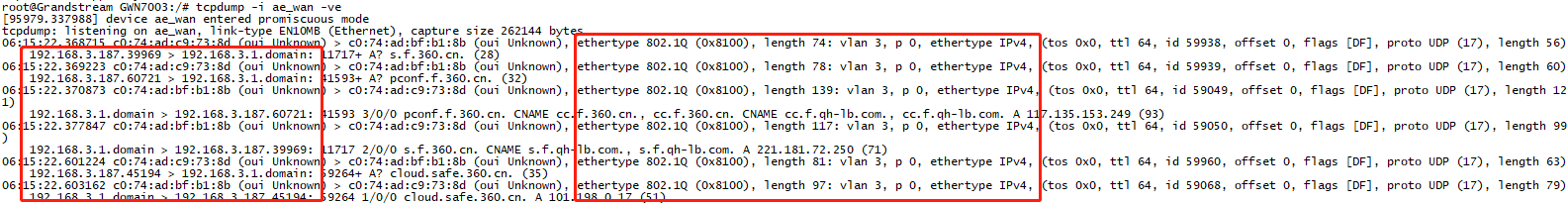
TPID：标签协议标识符，标识数据帧的类型，802.1q帧一般的参数值是0x8100

Priority:标识数据帧的优先级，主要用于qos

CFI:标准格式标识符，在以太网中，该值一般为0，其中0代表规范格式，1为非规范格式

Vlan ID:标识数据帧所属的vlan，俗称vid，vid值的范围为1-4096

在crt上7003抓wan1口，查看vlan



3.2、Pvid

pvid(Port-base VLAN ID)，是基于端口的VLAN ID，一个端口可以属于多个vlan，但一个端口只能有一个PVID，以太网数据帧格式有两种:一是无标记帧（Untagged帧），原始的、未加入4字节VLAN标签的帧；二是有标记帧（Tagged帧），加入了4字节VLAN标签的帧。

当端口收到一个不带tag(vlan id)头的数据包时，会打上PVID所表示的vlan号，视同该vlan的数据包处理，若是PVid与自身数据包vlan相同，查看端口是否允许此vlan通过，通过则进行转发，不通过则进行丢弃。

3.3、Vlan接口类型，接口类型不同，VLAN数据帧的处理过程也不同。

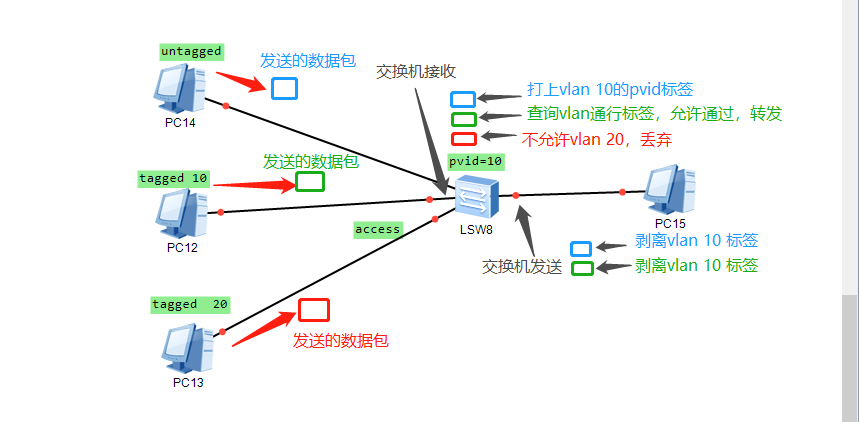
3.3.1 Access，只属于一个vlan，只能允许通过一个vlan

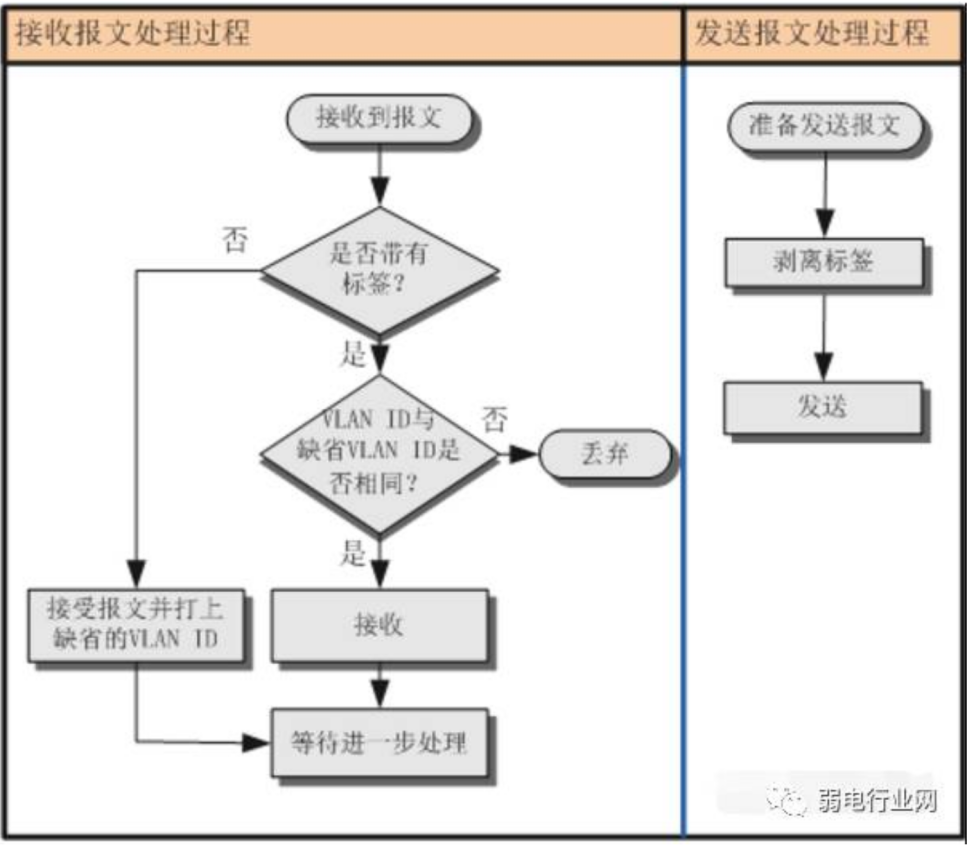
数据帧在Access端口入方向（发送报文）转发操作：

1. 当access端口收到一个Untagged帧时，给该帧打上PVID，并直接转发数据包
2. 当access端口收到一个tagged帧时，查看该PVID是否和tag中的vlan id相同，在发送带有Tag的帧前，Access接口会剥离Tag进行转发，如果不同，则直接丢弃

数据帧在Access端口出方向（接收报文）转发操作：

当数据从access端口1转发到另外一个access端口2的时候，在端口2接收到一个tagged帧时，查看帧tag中的vlan id是否与PVID相同。如果相同，则将这个Tagged帧的Tag进行剥离之后才进行转发。若不同，则直接丢弃这个Tagged帧。





3.3.2 Trunk

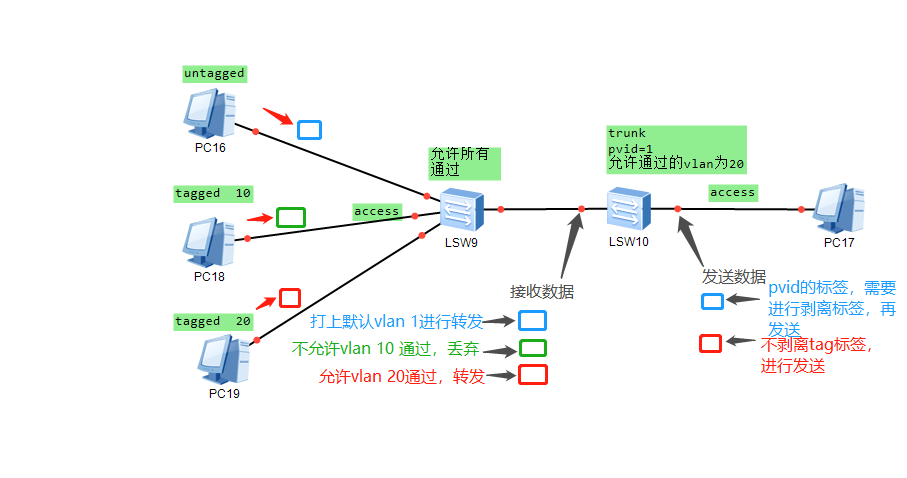
Trunk允许多个VLAN的帧带Tag通过，会为Untagged帧打上Native VLAN对应的Tag。

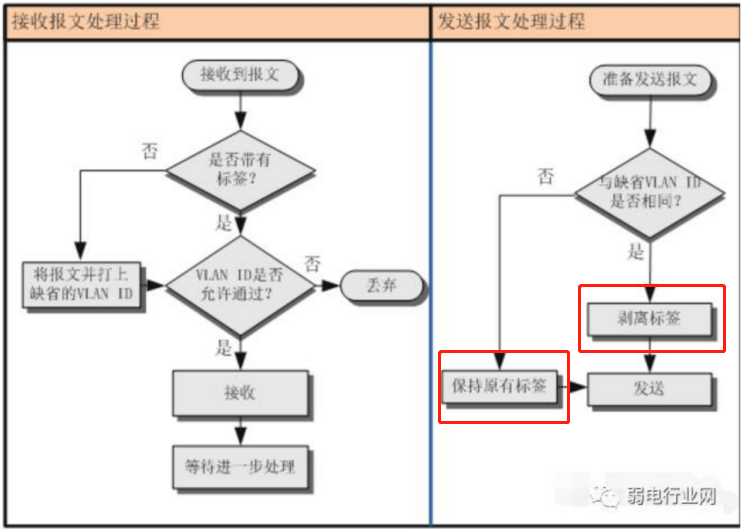
数据帧在Trunk端口入方向（发送报文）转发操作：

1. 当Trunk端口收到一个Untagged帧时，给该帧打上PVID，查看该端口是否允许此vlan通过，通过则转发，不允许则进行丢弃
2. 当Trunk端口收到一个tagged帧时，查看端口是否允许此vlan通过，允许则保留原始标签进行转发，不允许则进行丢弃

数据帧在trunk端口出方向（接收报文）转发操作：

1. 当Trunk端口收到一个Untagged帧时，给该帧打上PVID，查看该端口是否允许此vlan通过，通过则转发，不允许则进行丢弃
2. 当Trunk端口收到一个tagged帧时，查看此帧tag中vlan id值与PVID值是否相同，相同则剥离tag中vlan id，查看是否允许打上PVID标签的vlan通过,允许则进行转发，若不相同查看端口是否允许此vlan通过，允许则保留原始标签进行转发，不允许则进行丢弃





3.3.3 Hybrid

Hybrid这是一个混合接口，既能连接不能识别Tag的用户终端（如用户主机、服务器）和网络设备（如Hub），也可以用于连接交换机、路由器以及可同时收发Tagged帧和Untagged帧的语音终端、AP。在发送报文和trunk处理有一定的区别，接收报文处理和trunk一样

