**PPTP-Verify**

**班级：2014211312 姓名：郭瀚涛 学号：2014211469**

### PPTP原理

PPTP将PPP（Point-to-Point Protocol）帧封装进IP数据报中，通过IP网络如Internet或其他企业专用Intranet等发送。PPTP通过PPTP控制连接来创建、维护、终止一条隧道，并使用通用路由封装GRE（Generic Routing Encapsulation）对PPP帧进行封装。

首先，PPTP客户机使用动态分配的TCP端口号，与PPTP服务器使用的保留TCP端口号1723建立控制连接（PPTP控制连接携带PPTP呼叫控制盒管理信息，用于维护PPTP隧道）。

其次，客户端与服务器通过控制连接来创建、维护、终止一条隧道。

然后，PPP帧的有效载荷经过加密、压缩或是两者的混合处理。

接着，使用通用路由封装GRE对PPP帧进行封装。

再者，将PPP帧封装进IP数据报文中。通过IP网络如Internet或其他企业准用INTRANET灯发送给PPTP服务器。

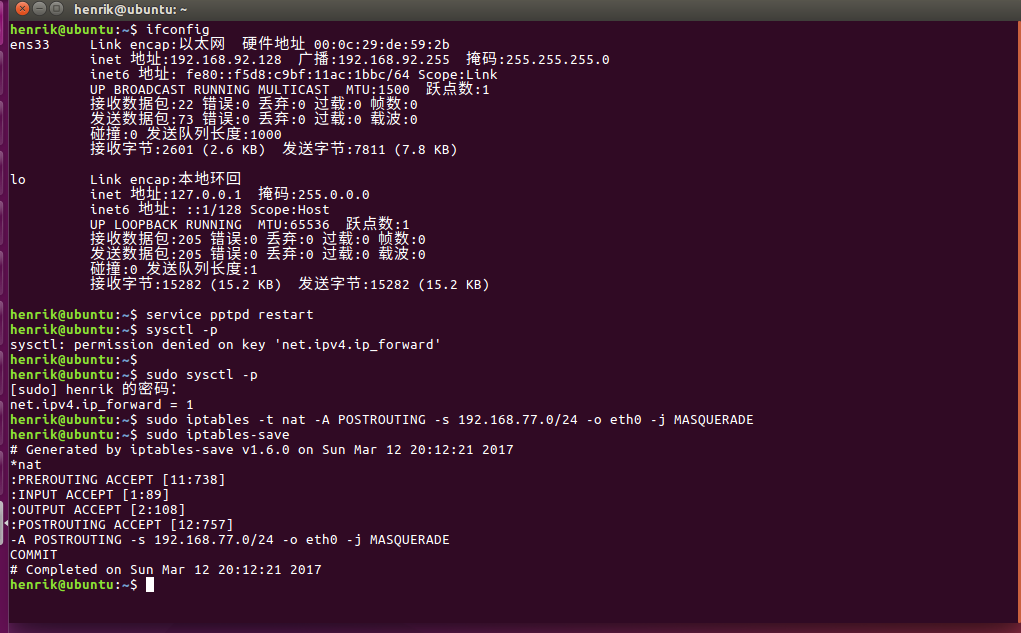
最后，服务器接收到PPTP数据包后进行常规处理。

**PPTP控制连接数的数据包格式：**

包括一个IP报头，一个TCP报头和PPTP控制信息，还包括数据链路层报头和报尾。

### Linux配置PPTP

系统环境： Ubuntu 16.04



更改文件时，会遇到权限不够的情况，需要用 sudo chmod 777 来提升权限

### Win 10 添加PPTP连接

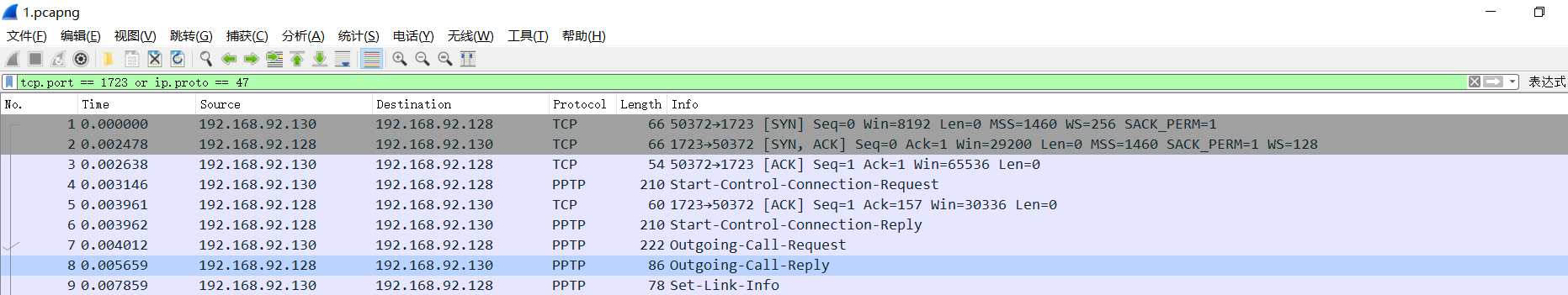


因为用VM虚拟机，网卡模式为NAT，所以IP地址会以192开头，不是以学校的10开头

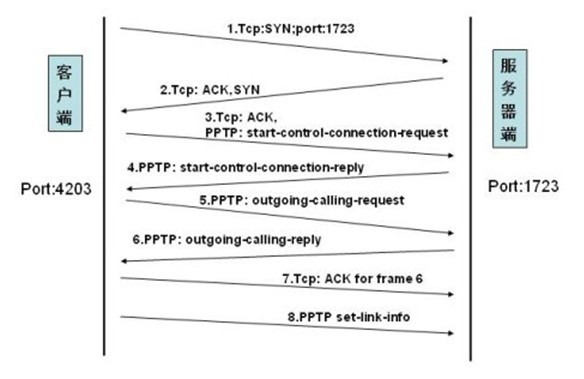
### 分析报文包

建立连接并用Wireshark抓包：

Win10 :192.168.92.130 Linux：192.168.92.128



由上图可知，PPTP的链接过程为：



通过网上查阅资料得知各包作用如下：

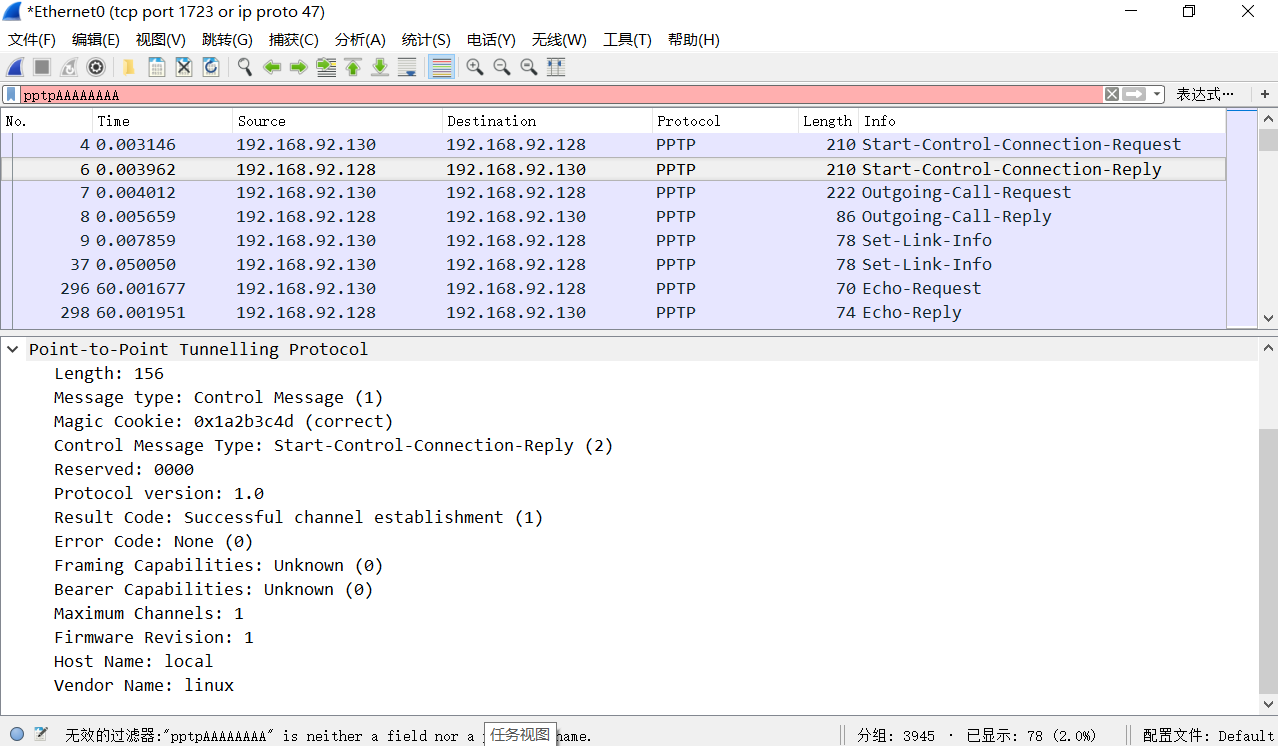
* start-control-connection-request ： 由PPTP客户端发出，请求简历控制连接。PPTP隧道要求在发送任何其他PPTP消息之前，先建立一条控制连接。
* start-control-connection-reply：由PPTP服务器发出，回应start-controlconnection-request消息。
* outgoing-call-request：由PPTP客户机发出，请求创建PPTP隧道，outgoing-call-request消息包含GRE报头钟的Call ID，该ID可唯一地标识一条隧道。
* outgoing-call-reply：PPTP服务器对outgoing-call-request消息的回应。
* echo-request：作为保持连线机制，可由PPTP客户机或服务器任何一方发出，若echo-request了没有应答，则PPTP隧道逐渐终止。
* echo-reply：对echo-request的应答。注：PPTP的echo-request和echo-reply的消息与ICMP回送请求和回送应答消息无关。
* wan-error-notify：由PPTP服务器向所有VPN客户机发出，指示服务器的PPP接口处于错误状态。
* set-link-info：可由PPTP客户机或服务器任何一方发出，设置PPP协商选项。
* call-clear-request：由PPTP客户机发出，请求终止隧道。
* call-disconnect-notify：PPTP服务器回应call-clear-request，或因其他原因指示必须终止隧道。如果PPTP服务器终止隧道，则发送出call-disconnect-notify消息。
* stop-control-connection-request：可由PPTP客户机或服务器任何一方发出，通知对方控制连接将被终止。
* stop-control-connection-reply：回应stop-control-connection-request消息。

----------------------------对各报文截图分析-----------------------------------

* PPTP控制消息

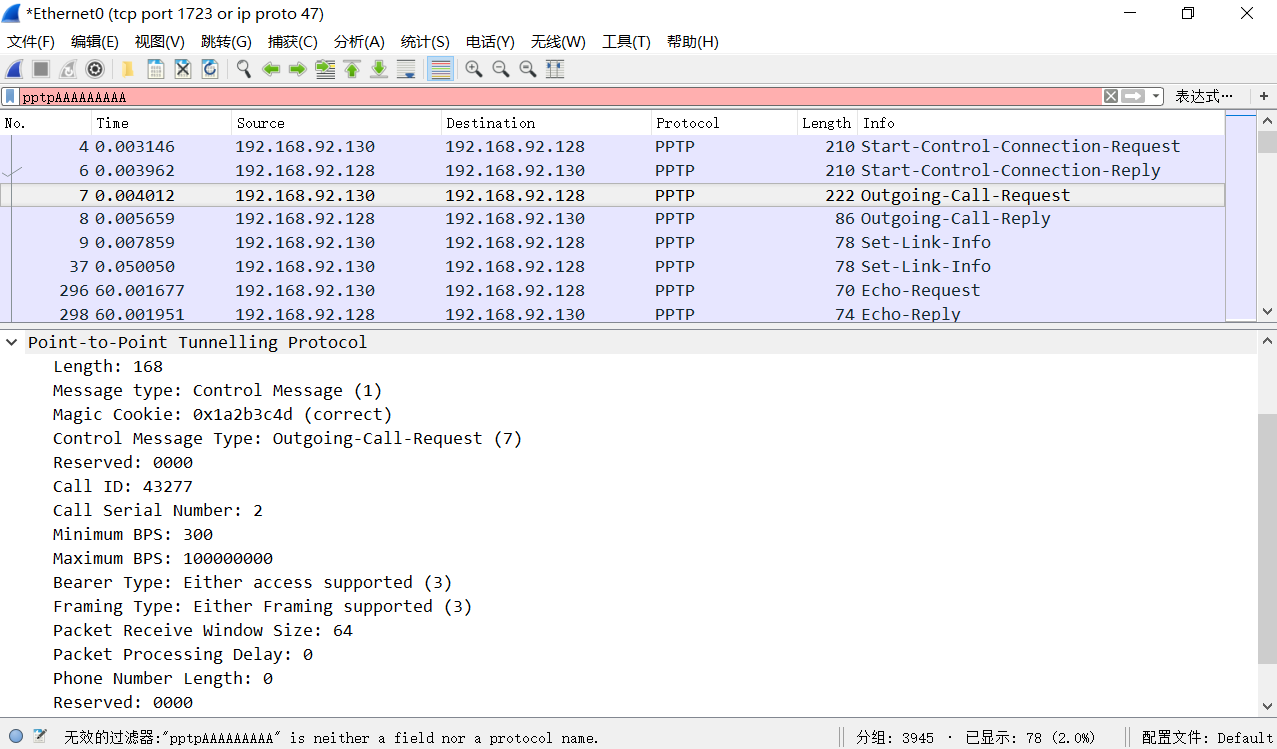
#### start-control-connection-request

#### start-control-connection-reply



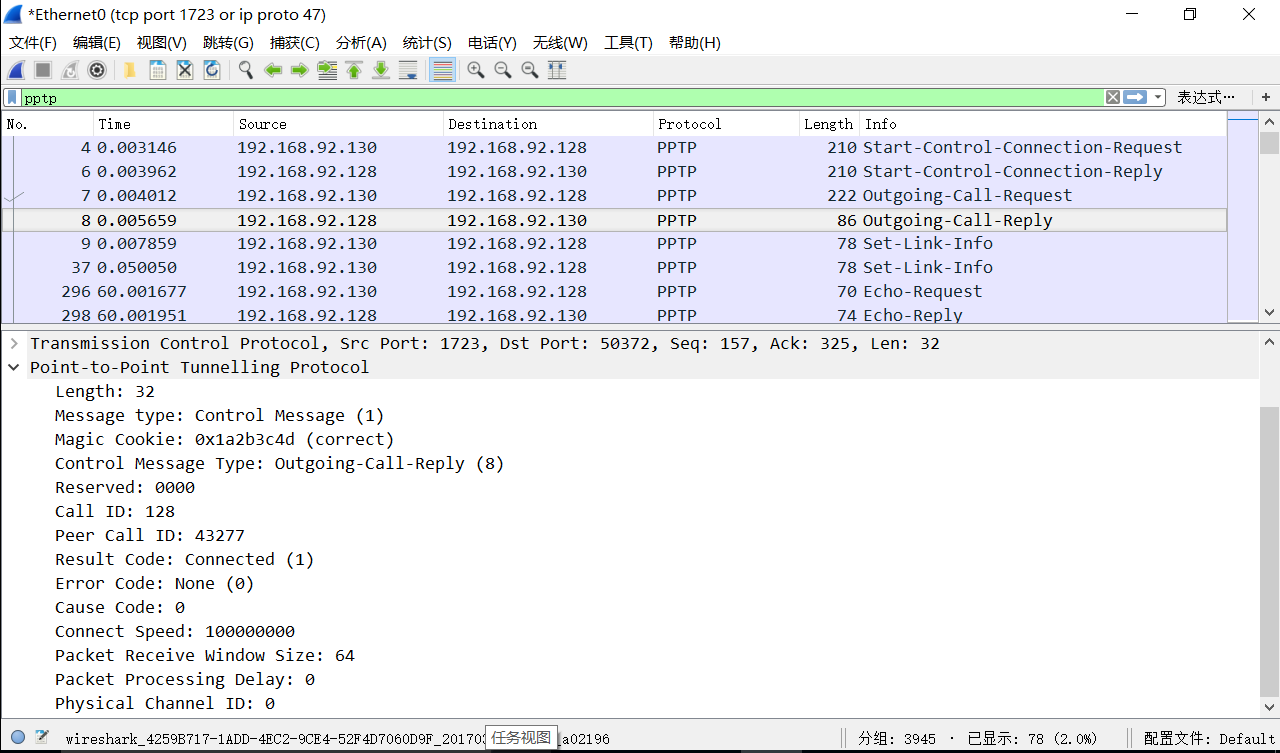
Win10 向Linux 发送连接建立请求，Linux 回应

#### outgoing-call-request



Call ID:由PPTP客户端指定的唯一的会话ID

#### outgoing-call-reply

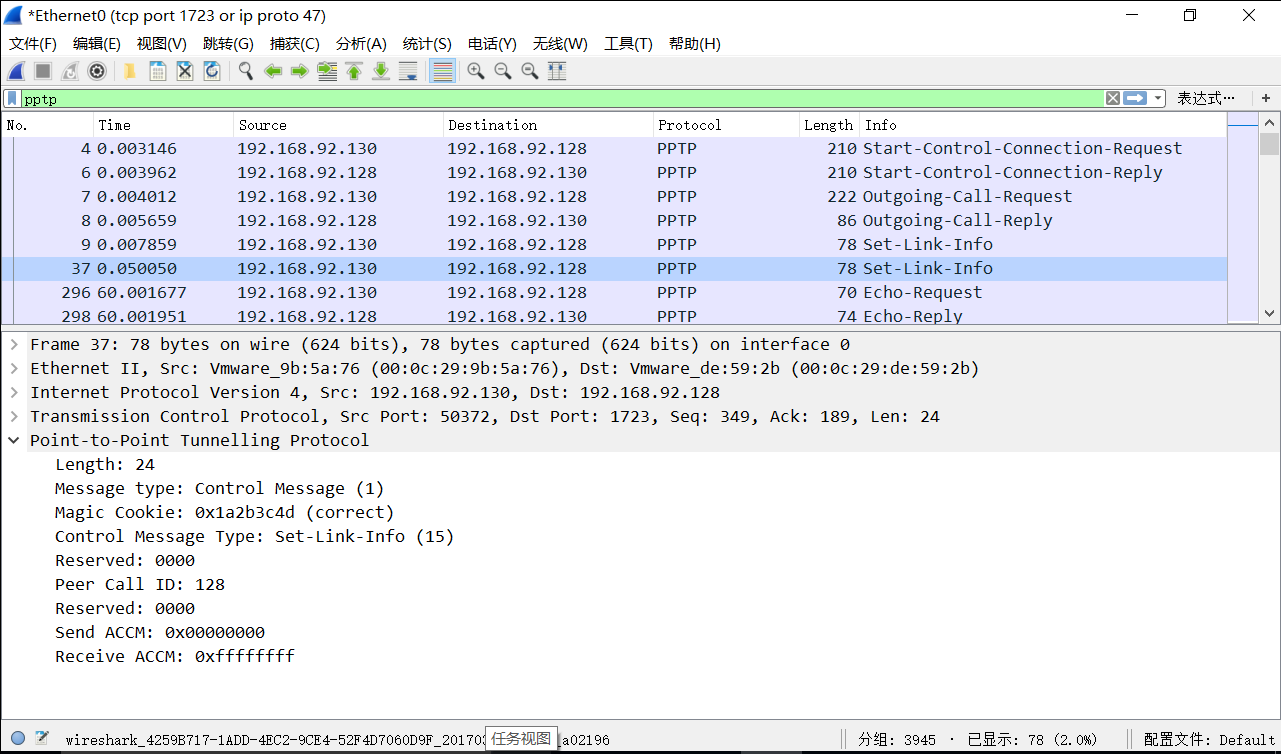
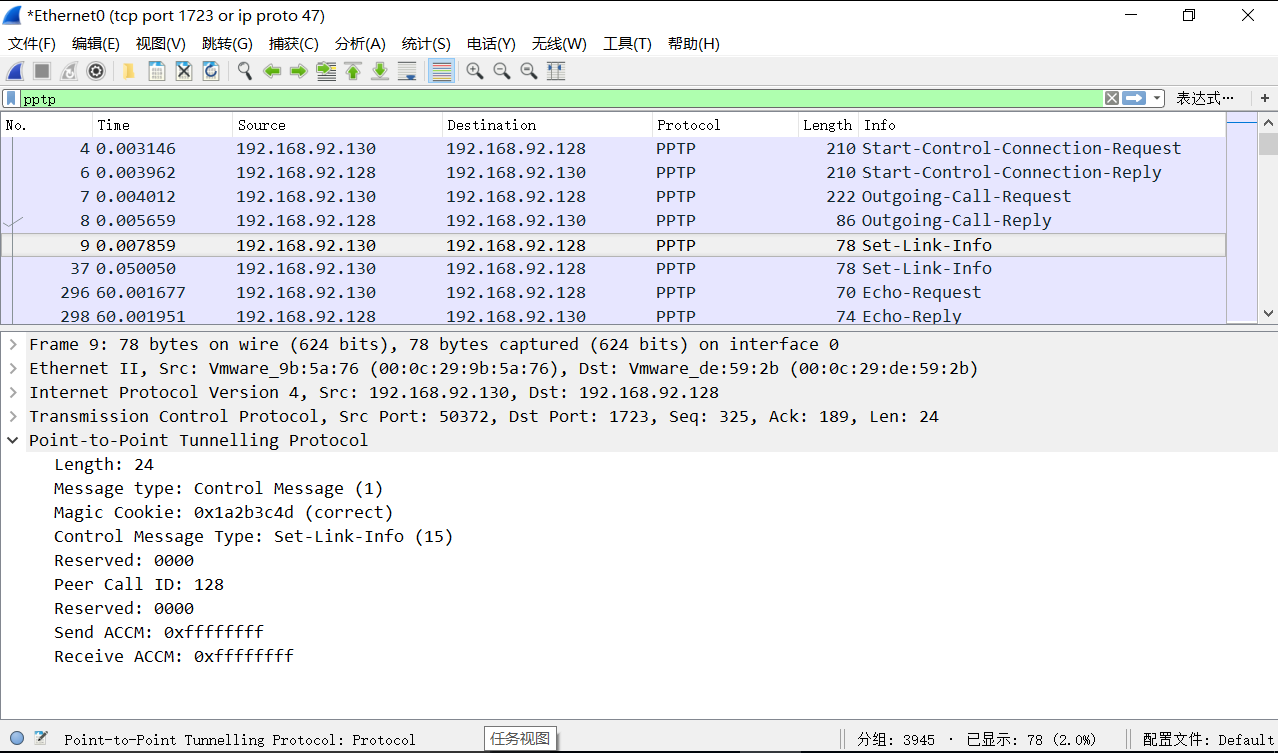


Call ID:由PPTP服务器指定的唯一的会话ID。主要用于在PPTP服务器与PPTP客户端建立的会话上，复用与解封装隧道包使用的。

Peer’s Call ID：设置的值是从接收到的Outgoing-call-request中Call ID值，是由PPTP客户端指定的，用于GRE中对于隧道数据解封与复用

由以上的 request 和 reply 可知 CALL-ID 和 PEER CALL ID 为两个方向上各自对CALL ID 的分配

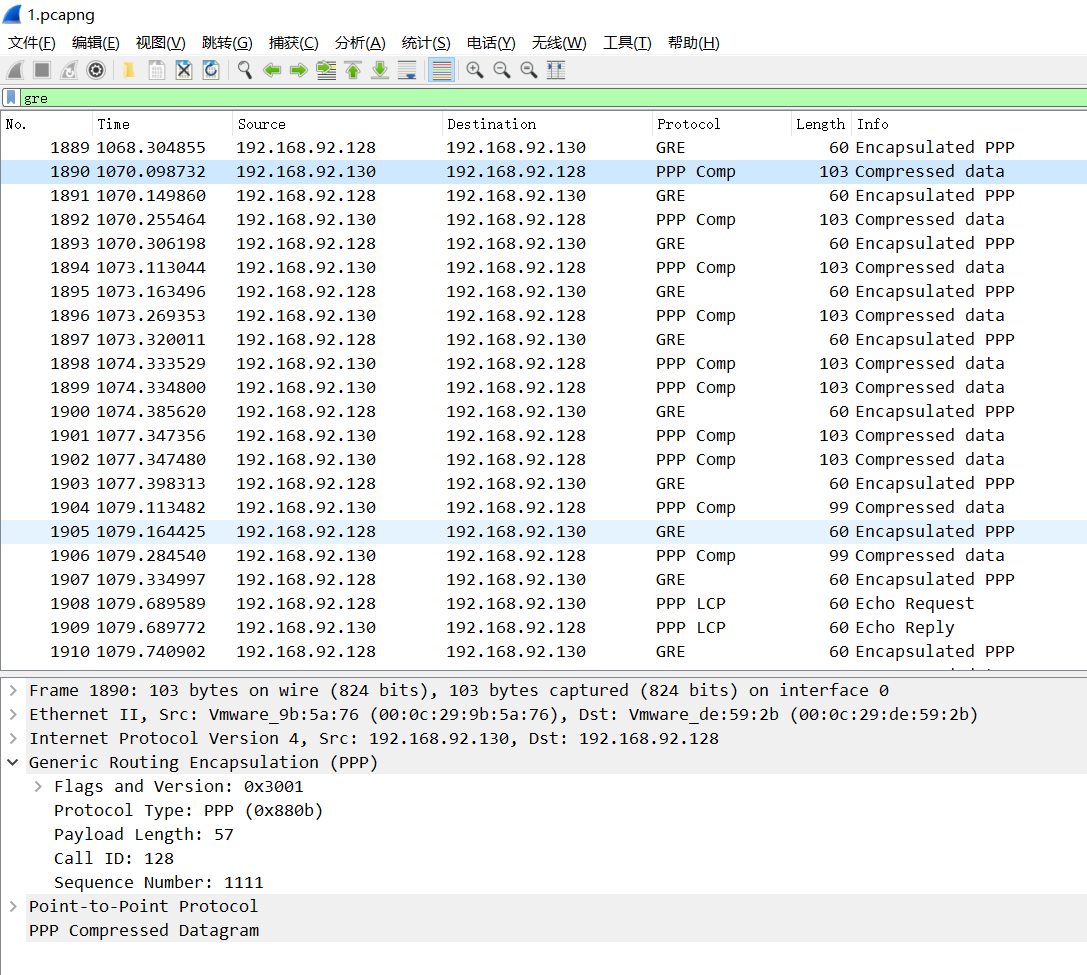
#### set-link-info



由以上两图可知， 192.168.92.130（win）对 Linux 的回应 peer call id 为 128（即Linux的 call id）

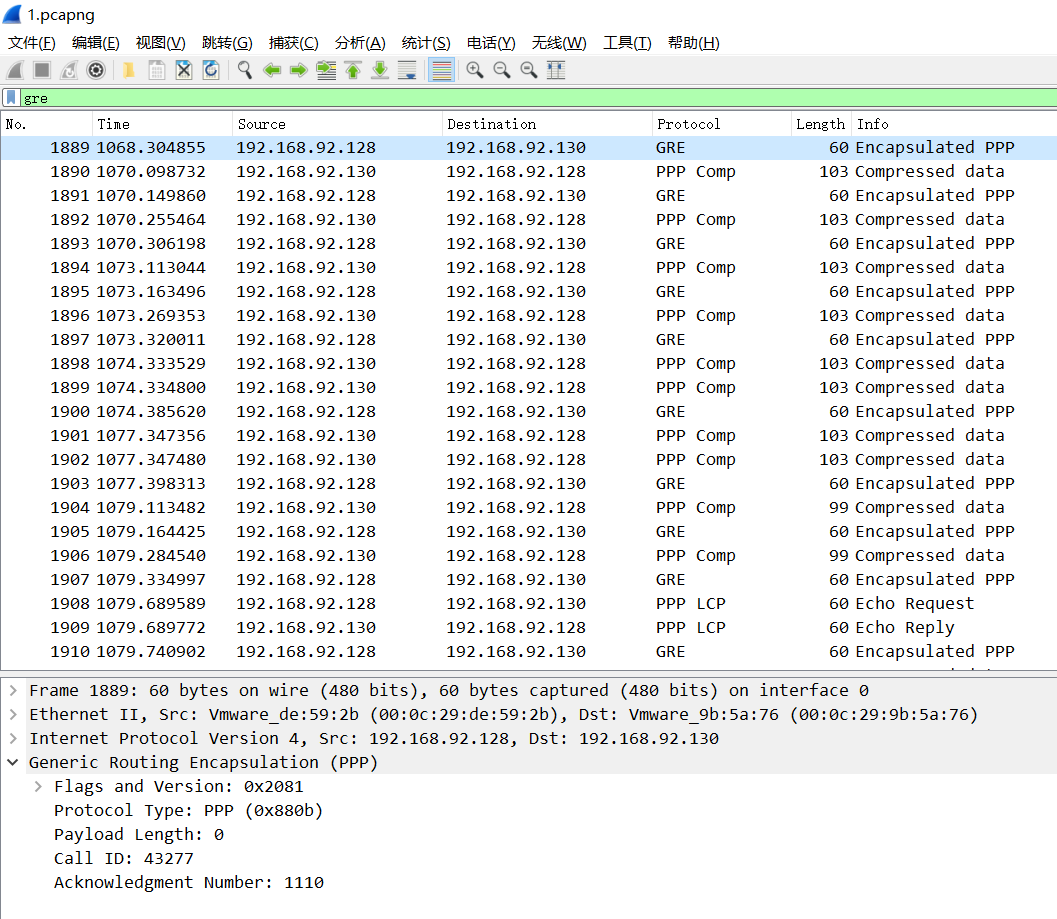
* PPTP GRE报文

#### Win10 -> Linux



Call id – 128 （ PPTP 控制报文 call id -43277 ）

#### Linux -> Win10



Call id – 43277 （ PPTP 控制报文 call id -128 ）

由GRE报文可知，GRE报文的CALL ID 与 PPTP 控制报文的CALL ID 相反。

自己的猜想： 建立PPTP控制报文 的call id为建立会话的唯一标识ID。 而GRE为报文字段，GRE 的 call id 代表使用的会话ID，即建立连接时候各自规定的ID。通过这个确定会话。

在PPTP中，GRE负责对PPP帧封装，PPTP控制报文负责对隧道的建立和维护，所以LRP只需处理以上三个字段的转换即可