**L2TP协议分析**

**杨卓宇 1652292**

**计算机科学与技术2班**

**2018/12/15**

1. 简介

第二层隧道协议（英语：Layer Two Tunneling Protocol，缩写为L2TP)是一种虚拟隧道协议，通常用于虚拟专用网。L2TP协议自身不提供加密与可靠性验证的功能，可以和安全协议搭配使用，从而实现数据的加密传输。经常与L2TP协议搭配的加密协议是IPsec，当这两个协议搭配使用时，通常合称L2TP/IPsec。

L2TP支持包括IP、ATM、帧中继、X.25在内的多种网络。在IP网络中，L2TP协议使用注册端口UDP 1701。因此，在某种意义上，尽管L2TP协议的确是一个数据链路层协议，但在IP网络中，它又的确是一个会话层协议。

1. 技术内容

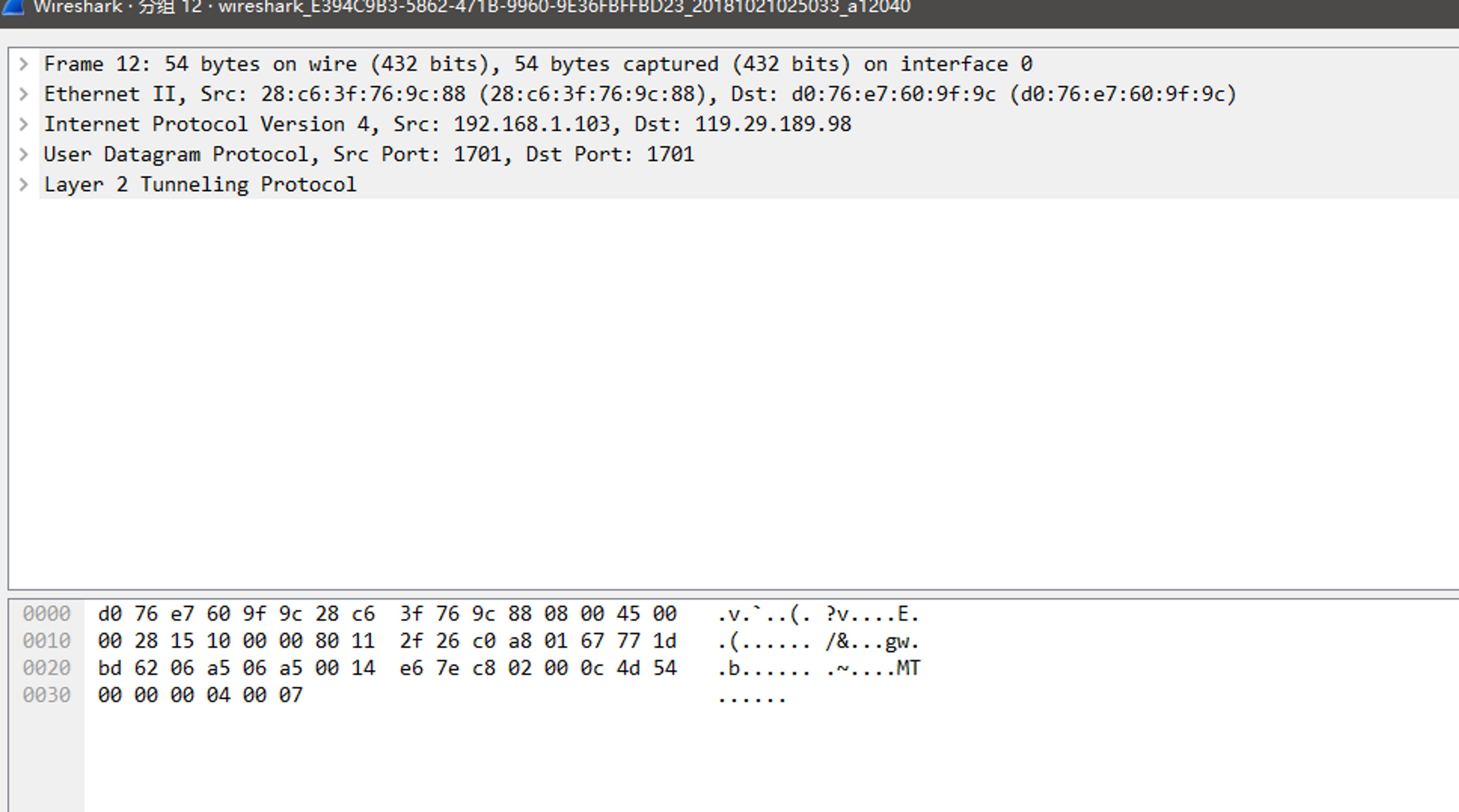
整个L2TP数据包，包括有效附载（payload）及标头（header），皆是使用用户数据报协议（UDP）来发送。L2TP本身并不提供加密和认证，但常用IPsec来确保L2TP的安全及完整性，两种协议的组合一般被称为L2TP/IPsec。L2TP tunnel的两端分别是LAC（L2TP Access Concentrator）与 LNS (L2TP Network Server)。LAC扮演起始者的角色；LNS则是服务器，等待新的隧道建立。而一旦隧道创建之后，两点之间的沟通就是双向性的。为了让更高层级的协议更容易使用L2TP隧道，每个更高层协议，例如：PPP，都会在隧道中创建一个L2TP会话（或称为"通话"）。无论是LAC或是LNS都可以打开会话，而每个会话的流量都会被L2TP隔开，因此在一个隧道之中可以创建多个虚拟网络。运行L2TP的时候应要考虑最大传输单元（MTU）。在L2TP隧道中交换的数据包可分类为控制数据包或是数据包。L2TP提供控制数据包的可靠性，数据包则没有。

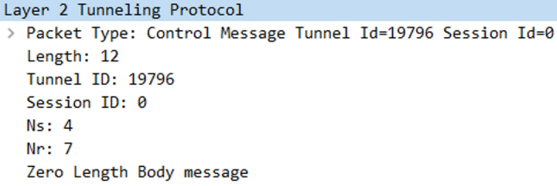
1. 实验
2. 配置好L2TP服务器并建立VPN连接



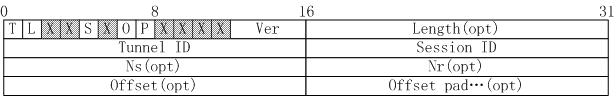
1. 使用wireshark进行抓包

IP address设置为我们想要抓包的特定IP，输入指令l2tp专门抓取l2tp包。下图中我们抓到了一个L2TP控制包，我们对其内容进行分析，找出L2TP报文头。





1. 分析报文需要的背景知识

Type(T)：标识消息的类型，0表示是数据消息，1表示控制消息。

Length(L)：置1时，说明Length域的值是存在的，对于控制消息L位必须置1。

X bit：保留位，所有保留位均置0。

Sequence(S)：置1时，说明Ns和Nr是存在的，对于控制消息S必须置1。

Offset(O)：置1时，说明Offset Size域是存在的，对于控制消息O必须置0。

Priority(P)：只用于数据消息，对于控制消息P位置0，当数据消息此位置1时，说明该消息在本列队和传输时应得到优先处理。

Ver：必须是2，表示L2TP数据报头的版本。

Length：标识整个报文的长度(以字节为单位)。

Tunnel ID：标识L2TP控制链接，L2TP Tunnel标识符只有本地意义，一个Tunnel两端被分配的Tunnel ID可能会不同，报头中的Tunnel是指接收方的Tunnel ID，而不是发送方的。本端的Tunnel ID在创建Tunnel时分配。通过Tunnel ID AVPs和对端交换Tunnel ID信息。

Session ID：标识Tunnel中的一个session，只有本地意义，一个session两端Session ID可能不同。

Ns：标识发送数据或控制消息的序号，从0开始，以1递增，到216再从0开始。

Nr：标识下一个期望接收到的控制消息。Nr的值设置成上一个接收到的控制消息的Ns+1。这样是对上一个接收到的控制消息的确认。数据消息忽略Nr。

Offset Size：如果值存在的话，标识有效载荷数据的偏移。

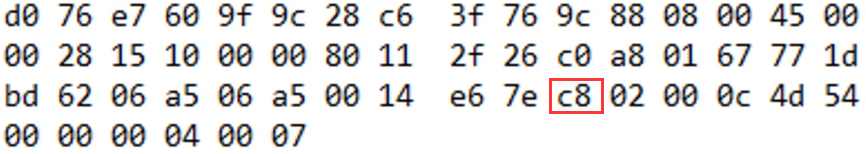
1. 对报文进行分析

已知该包为L2TP控制包，因此T=1，L=1，O=0，P=0；

已知Ns=4，Nr=7，所以S=1；

已知Ns=4，Nr=7，所以S=1；

所以报文头前八位二进制为11001000，转为十六进制为C8；



如此，找到了L2TP报文头的起始地址。可以对后面进行分析来进一步验证报文头的正确性。



C8之后紧跟02，其中X为保留位均为0，Ver必须是2，表示L2TP数据报头的版本，合并后与02符合。

02之后为十六进制000c，转为十进制后为12，表示报文长度为12字节，符合实际情况。

000c之后为十六进制4d54，转为十进制后为19796，Tunnel ID=19796，符合实际情况。

4d54之后为十六进制000，转为十进制后为0，Session ID=0，符合实际情况。

Ns=0004，Nr=0007，符合实际情况。

