

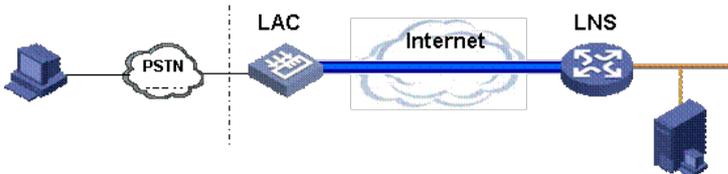
### 解析L2TP协议报文

#### 一. L2TP协议概述

L2TP: Layer 2 Tunnel Protocol 第二层隧道协议, 是为在用户和企业的服务器之间透明传输PPP报文而设置的隧道协议。特点是: (1) 非加密; (2) 网络层。

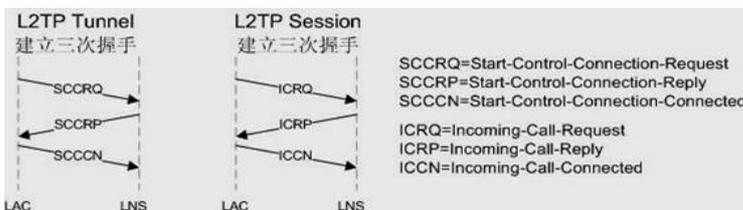
#### 二. L2TP隧道和会话建立流程

L2TP的组网图如图1-1所示。在一个LNS和LAC对之间存在着两种类型的连接, 一种是隧道 (Tunnel) 连接, 它定义了一个LNS和LAC对; 另一种是会话 (Session) 连接, 它复用在一个隧道连接之上, 用于表示承载在隧道连接中的每个PPP会话过程。



1-1 L2TP组网示意图

L2TP的会话建立由PPP触发, 隧道建立由会话触发。由于多个会话可以复用在一条隧道上, 如果会话建立前隧道已经建立, 则隧道不用重新建立。L2TP的建立流程如图1-2所示。



1-2 L2TP隧道和会话建立流程

#### 三. L2TP报文解析

在L2TP隧道建立过程中, 用Ethereal软件抓包, 所抓报文如图1-3所示。从图中可以看出最初的三个报文实现了tunnel建立的三次握手, 接下来的三个报文实现了session建立的三次握手。

No.	Time	Source	Destination	Protocol	Info
1	0.000000	202.0.0.2	202.0.0.1	L2TP	Control Message - SCCRQ (tunnel id=0, session id=0)
2	0.001154	202.0.0.1	202.0.0.2	L2TP	Control Message - SCCRP (tunnel id=0, session id=0)
3	0.001312	202.0.0.2	202.0.0.1	L2TP	Control Message - SCCCN (tunnel id=0, session id=0)
4	0.001366	202.0.0.2	202.0.0.1	L2TP	Control Message - ICRO (tunnel id=1, session id=0)
5	0.002990	202.0.0.1	202.0.0.2	L2TP	Control Message - ICRP (tunnel id=1, session id=0)
6	0.003102	202.0.0.2	202.0.0.1	L2TP	Control Message - ICCN (tunnel id=1, session id=0)
7	0.003144	202.0.0.2	202.0.0.1	PPP LCP	Configuration Request
8	0.004927	202.0.0.1	202.0.0.2	L2TP	Control Message - SLI (tunnel id=1, session id=38)
9	0.019915	202.0.0.2	202.0.0.1	L2TP	Control Message - ZLB (tunnel id=1, session id=0)
10	0.248363	202.0.0.2	202.0.0.255	NBNS	Name query NB H3CAV02-SS<00>
11	0.988751	202.0.0.2	202.0.0.255	NBNS	Name query NB H3CAV02-SS<00>
12	1.738664	202.0.0.2	202.0.0.255	NBNS	Name query NB H3CAV02-SS<00>
13	1.998874	202.0.0.1	202.0.0.2	PPP CHAP	Challenge
14	3.066918	202.0.0.2	202.0.0.1	PPP LCP	Configuration Request
15	3.070307	202.0.0.1	202.0.0.2	PPP LCP	Configuration Request
16	3.070393	202.0.0.2	202.0.0.1	PPP LCP	Configuration Reject
17	3.070681	202.0.0.1	202.0.0.2	PPP LCP	Configuration Ack
18	3.072333	202.0.0.1	202.0.0.2	PPP LCP	Configuration Request
19	3.072668	202.0.0.2	202.0.0.1	PPP LCP	Configuration Ack
20	3.073911	202.0.0.1	202.0.0.2	PPP CHAP	Challenge
21	3.074022	202.0.0.2	202.0.0.1	PPP CHAP	Response
22	3.074339	202.0.0.1	202.0.0.2	L2TP	Control Message - SLI (tunnel id=1, session id=38)

图1-3 L2TP协议报文

除了在隧道建立时的报文, 我们还发现有14至19号报文, 这是用于PPP LCP重协商的。LNS侧在收到ICCN消息后, 通知PPP LNS要求进行强制CHAP验证。PPP此时会先进行一次LCP重新协商, 然后向用户侧首先发送Challenge (如上图所示), 开始CHAP验证。LCP重协商的一个目的是考虑到LAC与LNS可能是不同厂商的设备, LAC之前已经协商出来的LCP参数可能并不是LNS所期望的, 因此在这种情况下就需要重协商了。

在这里还提到了ICCN这个报文, 下图1-4所示即为该报文的具体内容。

```

# Frame 6 (176 bytes on wire, 176 bytes captured)
# Ethernet II, Src: 00:1e:ec:64:2c:5c (00:1e:ec:64:2c:5c), Dst: Hangzhou_13:
# Internet Protocol, Src: 202.0.0.2 (202.0.0.2), Dst: 202.0.0.1 (202.0.0.1)
# User Datagram Protocol, Src Port: 1272 (1272), Dst Port: 12tp (1701)
# Layer 2 Tunneling Protocol
# Packet Type: Control Message Tunnel Id=1 Session Id=14558
# Length: 134
# Tunnel ID: 1
# Session ID: 14558
# NS: 3
# NP: 2
# Control Message AVP
# Connect Speed AVP
# Framing Type AVP
# Last Sent LCP CONFREQ AVP
# Last Received LCP CONFREQ AVP
# Proxy Authen Type AVP
# Proxy Authen Name AVP
# Proxy Authen ID AVP
# Proxy Authen Response AVP
# Private group ID AVP
# RxConnect Speed AVP
    
```

图1-4 ICCN报文

可见在ICCN报文中承载了PPP协商和代理认证相关的AVP。这些信息有最后发送LCP Confreq, 如PP

P验证类型 (CHAP/PAP); 最后接收的LCP Confreq; 代理认证的类型、用户名、标识、challenge等等。LNS侧将LCP协商和认证的一些相关参数交给PPP处理。当LNS侧认证通过, 将以L2TP数据报文的形式通知用户认证成功。然后用户和LNS在L2TP数据通道上进行IPCP协商。