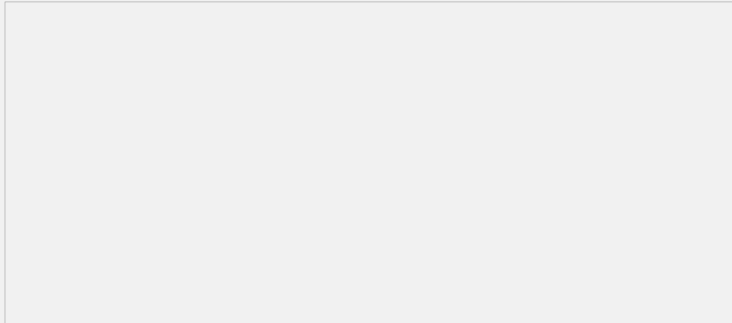


SR66路由器L2TP对接异常经验案例

一、组网：

客户希望使用L2TP技术构建安全的虚拟专网，使得企业驻外机构和出差人员可从远程经由公共网络，通过虚拟隧道实现和企业总部之间的网络连接，而公共网络上其它用户则无法穿过虚拟隧道访问企业网内部的资源。

客户使用一台SR66路由器作为LNS设备，同时使用一台友商设备作为LAC（一般为运营商设备），如图所示：



在L2TP对接过程中，因为各厂家对于协议的理解差异，可能造成参数协商的不正确，下面为大家介绍其中三种情况。

二、问题描述：

1. 用户通过L2TP拨号到LNS设备上，L2TP会话成功建立，PPP LCP协商成功，CH AP认证通过，IPCP成功获取到地址，但是一分钟左右后用户会自动下线，LCP/IPCP DOWN；
2. 用户通过L2TP拨号到LNS设备上，L2TP会话可成功建立，但是在短时间内，L2TP会话会被清除掉，从而导致用户掉线。
3. 用户通过L2TP拨号到LNS设备上，L2TP会话成功建立，因为配置了LCP重协商，所以接下来LNS与终端设备重新进行LCP协商，但是LCP协商完成后PPP LCP会立即DOWN，从而导致用户拨号不成功。

三、过程分析：

1. 第一个问题用户可以正常上线，但是一分钟左右便会出现掉线现象，查看debug ppp all信息，发现LCP建立成功后，每隔10s（可调整）会发送Echo-Request报文,但是对端并没有回复我们Echo-reply报文，总计重传5次（可调整）Echo-Request报文后，还没有收到对端的回应，我们设备就会认为链路发生故，所以导致LCP/IPCP Down。示例：

```
*May 4 16:40:07:247 2014 YNSW-YD3G-SR6616 PPP/7/debug2: -Slot=7;
PPP Event:
```

```
Virtual-Template1:2 : Echo Timer Expired Retransmit = 3
```

```
*May 4 16:40:07:247 2014 YNSW-YD3G-SR6616 PPP/7/debug2: -Slot=7;
PPP Packet:
```

```
Virtual-Template1:2 Output LCP(c021) Pkt, Len 12
State opened, code EchoRequest(09), id 2, len 8
Magic Number 603f9431
```

```
*May 4 16:40:17:247 2014 YNSW-YD3G-SR6616 PPP/7/debug2: -Slot=7;
PPP Event:
```

```
Virtual-Template1:2 : Echo Timer Expired Retransmit = 2
```

```
*May 4 16:40:17:247 2014 YNSW-YD3G-SR6616 PPP/7/debug2: -Slot=7;
PPP Packet:
```

```
Virtual-Template1:2 Output LCP(c021) Pkt, Len 12
State opened, code EchoRequest(09), id 3, len 8
Magic Number 603f9431
```

```
*May 4 16:40:27:247 2014 YNSW-YD3G-SR6616 PPP/7/debug2: -Slot=7;
PPP Event:
```

```
Virtual-Template1:2 : Echo Timer Expired Retransmit = 1
```

```
*May 4 16:40:27:247 2014 YNSW-YD3G-SR6616 PPP/7/debug2: -Slot=7;
PPP Packet:
```

```
Virtual-Template1:2 Output LCP(c021) Pkt, Len 12
```

State opened, code EchoRequest(09), id 4, len 8

Magic Number 603f9431

%May 4 16:40:37:247 2014 YNSW-YD3G-SR6616 IFNET/5/LINEPROTO_UPDOWN

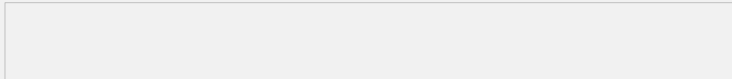
N: -Slot=7; **Line protocol on the interface Virtual-Template1:2 is DOWN.**

%May 4 16:40:37:248 2014 YNSW-YD3G-SR6616 IFNET/5/PROTOCOL_UPDOWN

N: -Slot=7; **Protocol PPP IPCP on the interface Virtual-Template1:2 is DOWN.**

与对端设备确认，**对端LAC设备不支持Keepalive报文**，接收到Keepalive报文后不处理，所以便会发生超时重传掉线现象。

2. 这个问题会发生在SR66系列路由器**R3103版本之前**，在之前的版本中，建立L2TP链接后，我司设备默认会自动发送**SLI报文**，SLI报文是LNS用于通知LAC，LNS与Client的**ACCM (异步)** 选项协商结果。当协商结果与默认不一致时，就会发送。实际应用中，各设备制造商的LAC对ACCM要求可能不同，LNS需要根据LAC的要求配置是否发送ACCM消息。通过这个L2TP的消息，LNS告知对端LAC发送和接收的ACCM掩码。当对端不支持ACCM报文时，SLI报文会重传三次，然后控制报文**ACK消息超时**，此时便会清掉隧道中的所有会话，从而导致用户下线。抓包信息如图所示：



而相应的debug信息：

```
*May 4 16:29:22:298 2014 YNSW-YD3G-SR6616 L2TP/7/L2TDBG: L2TP_PAYLOAD
D: Tunnel 1 proc ctrl ack timer expired, SendUp=9 SendLow=4 //Tunnel 1 检测到控制报文超时
```

```
*May 4 16:29:22:298 2014 YNSW-YD3G-SR6616 L2TP/7/L2TDBG: L2TP_CONTR
OL: Calls on tunnel 1 cleared because 1 //Tunnel 1 在控制报文超时后开始清会话
```

```
*May 4 16:29:22:299 2014 YNSW-YD3G-SR6616 L2TP/7/L2TDBG: L2TP_CONTR
OL: Cleared calls on tunnel pstNode=133d8cd0 total=2
```

```
*May 4 16:29:22:299 2014 YNSW-YD3G-SR6616 L2TP/7/L2TDBG: L2TP_CONTR
OL: Cleared the data structure of call 2186
```

```
*May 4 16:29:22:300 2014 YNSW-YD3G-SR6616 L2TP/7/L2TDBG: L2TP_CONTR
OL: Cleared calls on tunnel pstNode=1337d110 total=1
```

```
*May 4 16:29:22:300 2014 YNSW-YD3G-SR6616 L2TP/7/L2TDBG: L2TP_CONTR
OL: Cleared the data structure of call 2235
```

```
*May 4 16:29:22:301 2014 YNSW-YD3G-SR6616 L2TP/7/L2TDBG: L2TP_CONTR
OL: Tunnel 1 sent StopCCN to Tunnel 1 // 发送StopCCN消息
```

```
*May 4 16:29:22:301 2014 YNSW-YD3G-SR6616 L2TP/7/L2TDBG: L2TP_CONTR
OL: Put AVP Message Type: STOP_CONTROL_CONNECTION_NOTIFICATION // StopCCN消息
```

```
*May 4 16:29:22:301 2014 YNSW-YD3G-SR6616 L2TP/7/L2TDBG: L2TP_CONTR
OL: Put AVP Assigned Tunnel ID: 1
```

```
*May 4 16:29:22:302 2014 YNSW-YD3G-SR6616 L2TP/7/L2TDBG: L2TP_CONTR
OL: Put AVP Result code: LOSS_OF_CARRIER
```

```
*May 4 16:29:22:302 2014 YNSW-YD3G-SR6616 L2TP/7/L2TDBG: L2TP_PAYLOAD
D: Tunnel 1 sent control (SendUp & RcvLow): Ns (9) Nr (8)
```

```
*May 4 16:29:22:303 2014 YNSW-YD3G-SR6616 L2TP/7/L2TDBG: L2TP_EVENT:
Cleared Tunnel remote ID:1, local ID:1
```

```
*May 4 16:29:22:303 2014 YNSW-YD3G-SR6616 L2TP/7/L2TDBG: -Slot=7; L2TP_
EVENT: IPC recv Src IPC ID=11 Dst node=5 Dst IPC ID=11 Len=16
```

```
*May 4 16:29:22:304 2014 YNSW-YD3G-SR6616 L2TP/7/L2TDBG: -Slot=7; L2TP_
EVENT: IPC recv data type=100 len=16
```

```
%May 4 16:29:22:305 2014 YNSW-YD3G-SR6616 IFNET/5/LINEPROTO_UPDOWN
N: -Slot=7; Line protocol on the interface Virtual-Template1:0 is DOWN. // LCP DOWN
```

```
*May 4 16:29:22:306 2014 YNSW-YD3G-SR6616 L2TP/7/L2TDBG: -Slot=7; L2TP_
EVENT: IPC processed IPC data result 0
```

```
%May 4 16:29:22:307 2014 YNSW-YD3G-SR6616 IFNET/5/PROTOCOL_UPDOWN
N: -Slot=7; Protocol PPP IPCP on the interface Virtual-Template1:0 is DOWN. // IP CP DOWN
```

在SR66路由器**R3103 (不包括)** 之前版本中,是通过人为控制是否发送SLI消息的，但实际上这个消息的发送并不应该是人为的通过命令行设置，而是应该真正的通过PPP上报来决定它的发送。在**R3103 (含)** 之后的版本中只有当PPP设置为异步模式时，才会向L2TP上报ACCM的设置情况（通过命令字IOCTL_SERIAL_SET_ACCM）。

如果PPP的工作模式为同步方式，则不会上报。即**LNS可自动识别是否为同步异步方式来决定是否发送SLI报文**。

3. 当LAC对用户进行验证后，为了增强安全性，LNS可以再次对用户进行验证。此时将对用户进行两次验证，第一次发生在LAC侧，第二次发生在LNS侧，只有两次验证全部成功后，L2TP隧道才能建立。

在L2TP组网中，LNS侧对用户的验证方式有三种：

- 1) 代理验证：由LAC代替LNS对用户进行验证，并将用户的所有验证信息及LAC端本身配置的验证方式发送给LNS。LNS根据接收到的信息及本端配置的验证方式，判断用户是否合法。
- 2) 强制CHAP验证：强制在LAC代理验证成功后，LNS再次对用户进行CHAP验证。
- 3) LCP重协商：忽略LAC侧的代理验证信息，**强制LNS与用户间重新进行LCP (Link Control Protocol, 链路控制协议) 协商**。

为了增加安全性，有时我们会在LNS上配置LCP重协商，但是配置LCP重协商后，会出现用户不能拨号的现象。查看debug信息：

```
PPP Packet:
  Virtual-Template1:0 Input LCP(c021) Pkt, Len 14
  State acksent, code ConfAck(02), id 1, len 10
  MagicNumber(5), len 6, val 3909544c
*Mar 20 14:32:15:840 2014 DLWP_R2 PPP/7/debug2: -Slot=3;
PPP Event:
  Virtual-Template1:0 LCP RCA(Receive Config Ack) Event
  state acksent
*Mar 20 14:32:15:841 2014 DLWP_R2 PPP/7/debug2: -Slot=3;
PPP Event:
  Virtual-Template1:0 LCP Close Event //在acksent状态会突然出现一个close
事件
  state acksent
*Mar 20 14:32:15:841 2014 DLWP_R2 PPP/7/debug2: -Slot=3;
PPP State Change:
  Virtual-Template1:0 LCP : acksent --> closing
*Mar 20 14:32:15:842 2014 DLWP_R2 PPP/7/debug2: -Slot=3;
PPP Packet:
  Virtual-Template1:0 Output LCP(c021) Pkt, Len 8
  State closing, code TermReq(05), id 2, len 4
```

在LCP重协商阶段，LCP协商完成时，会突然有一个Close事件发生，然后关闭PPP链接，导致协商不成功。

经与LAC厂家确认，**对端LAC设备不支持LCP重协商**，所以导致PPP协商不成功。

四、 解决方法：

1. 如果对端设备不支持对PPP Keepalive报文的处理，我们可以在VT口下使用**timer hold 0**命令关闭Keepalive报文的发送，这样设备就不会发送echo-request报文，同样也就不会出现超时从而导致PPP down 的现象。
2. 如果对端设备使用PPP同步方式进行协商而且不支持对于SLI报文的回应，在SR66路由器R3103之后的版本中会自动判断是否发送ACCM报文，所以不会出现控制报文ACK消息超时的情况；
如果是R3103之前的版本，可以使用**undo l2tp sendaccm enable**命令取消ACCM报文的发送。
3. 如果对端不支持LCP重协商，取消LCP重协商即可。