L2TP en StarOS - Implementación en el peering ASR5k y del Troubleshooting L2TP - L2TPTunnelDownPeerUnreachable

Contenido

Introducción

Este documento describe cómo el protocolo Layer 2 Tunneling Protocol (L2TP) en StarOS se implementa en el peering ASR5k y del Troubleshooting L2TP - L2TPTunnelDownPeerUnreachable.

¿Cuál es L2TP?

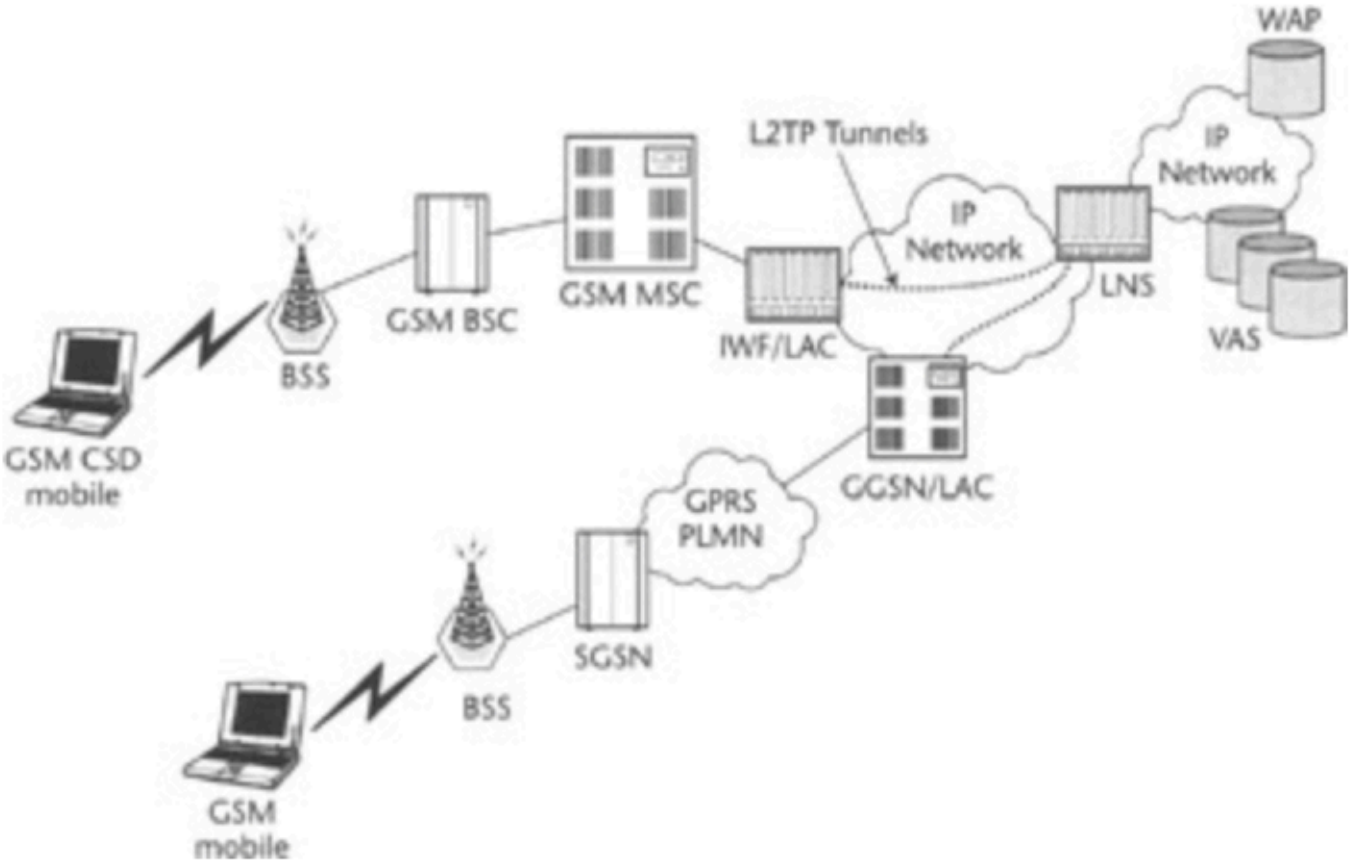
El L2TP extiende la naturaleza de punto a punto del PPP. El L2TP proporciona un método de encapsulación para el transmitir de los bastidores tunneled PPP, que permite que los puntos finales PPP sean tunneled sobre un Packet Switched Network. El L2TP se despliega lo más comúnmente posible en los escenarios del telecontrol-acceso-tipo que utilizan Internet para ofrecer los servicios del intranet-tipo. El concepto es el de un Red privada virtual (VPN).

Los dos elementos físicos primarios del L2TP son el L2TP Access Concentrator (LAC) y el L2TP Network Server (LNS):

- LAC: El LAC es un par al LNS que actúa como un lado del punto final del túnel. LAC finaliza la conexión remota PPP y se ubica entre el remoto y el LNS. Los paquetes se remiten a y desde la conexión remota sobre la conexión PPP. Los paquetes a y desde el LNS se remiten sobre el túnel L2TP.
- LNS: El LNS es un par al LAC que actúa como un lado del punto final del túnel. El LNS es la punta de terminación para las sesiones en túnel PPP LAC. Esto se utiliza para agregar las

sesiones PPP múltiple en túnel por LAC y el ingreso en la red privada.

El L2TP simplificado puso en la red móvil, tal y como se muestra en de esta imagen.



Hay dos diversos Tipos de mensaje que el L2TP utiliza:

- Mensajes del control: El L2TP pasa el control y los mensajes de datos sobre el control y los canales de datos separados. El canal de control de la en-banda pasa la Administración, la administración de llamadas, el informe de errores, y los mensajes de control de sesión ordenados del control de conexión. El lanzamiento del control de conexión no es específico al LAC o al LNS sino, bastante, al terminal original del túnel y al receptor que tiene importancia en el establecimiento del control de conexión. Un método de autentificación del desafío del secreto compartido se utiliza entre los puntos finales del túnel.
- Mensajes de datos: Los mensajes de datos se utilizan para encapsular las tramas PPP que se envían en el túnel L2TP.

Explican el flujo de llamada y al establecimiento del túnel detallados aquí:

http://www.cisco.com/c/en/us/support/docs/dial-access/virtual-private-dialup-network-vpdn/23980-l2tp-23980.html

¿Dónde lo utilizamos en la movilidad?

La instalación típica es para los usuarios corporativos donde el GGSN actúa como LAC y establece los túneles seguros hacia el LNS que se actúa en la red corporativa. Los flujos de llamada detallados están disponibles en el apéndice de la guía de configuración GGSN que se puede encontrar, por la versión de software específica, aquí:

http://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html

¿Cuál es ASR5x00 en esta configuración?

ASR5k puede soportar las funciones LAC y LNS.

Soporte L2TP LAC

El L2TP establece los túneles del control L2TP entre el LAC y el LNS antes de hacer un túnel las conexiones PPP del suscriptor como sesiones L2TP. El servicio LAC se basa en la misma arquitectura que el GGSN y las ventajas de la asignación del recurso dinámico y mensaje y la informática distribuidos. Este diseño permite que el servicio LAC soporte sobre 4000 configuraciones por segundo o un máximo de 3G excesivo de la producción. Puede haber un máximo arriba a 65535 sesiones en un solo túnel y tanto como 500,000 sesiones L2TP usando 32,000 túneles por el sistema.

Soporte L2TP LNS

El sistema configurado como servidor de red del protocolo Layer 2 Tunneling Protocol (LNS) soporta los túneles seguros del Red privada virtual (VPN) de la terminación en medio de los concentradores de acceso L2TP (LAC).

El L2TP establece los túneles del control L2TP entre el LAC y el LNS antes de hacer un túnel las conexiones PPP del suscriptor como sesiones L2TP. Puede haber un máximo de hasta 65535 sesiones en un solo túnel y de hasta 500,000 sesiones por el LNS.

La arquitectura LNS es similar al GGSN y utiliza el concepto de un demultiplexor para asignar inteligente las nuevas sesiones L2TP a través del software disponible y a los Recursos de hardware en la plataforma sin la intervención del operador.

Para más información refiera las guías de configuración PGW/GGSN.

Configuración para habilitar los servicios en los dispositivos de Cisco en el ASR5k

Ejemplos de configuración para el LAC en ASR5k

```
 apn test-apn
accounting-mode none
     aaa group AAA
     authentication msisdn-auth
     ip context-name destination
     tunnel l2tp peer-address 1.1.1.1 local-hostname lac_l2tp     configure
context destination-gi
lac-service l2tp_service
     allow called-number value apn
     peer-lns 1.1.1.1 encrypted secret pass
```

```
    bind address 1.1.1.2
```

Ejemplos de configuración para el LNS en ASR5k

```
  configure
context destination-gi
lns-service lns-svc
bind address 1.1.1.1
authentication { { [ allow-noauth | chap < pref > | mschap < pref > | | pap < pref > | msid-auth
}
```

> Nota: Las múltiples direcciones en la misma interfaz IP pueden estar limitadas a diversos servicios LNS. Sin embargo, cada direccionamiento se puede limitar a solamente un servicio LNS. Además, el servicio LNS no se puede limitar a la misma interfaz que los otros servicios tales como un servicio LAC.

Ejemplos de configuración para el LNS en el dispositivo Cisco IOS

Esto se puede utilizar como ejemplos de configuración que soportan para la configuración del Cisco IOS y no está conforme a este artículo.

Configuración LNS

```
 aaa group server radius AAA
server 2.2.2.2 auth-port 1812 acct-port 1813
ip radius source-interface GigabitEthernet0/1
!  aaa authentication login default local
aaa authentication ppp AAA group AAA
aaa authorization network AAA group AAA
aaa accounting network default
action-type start-stop
group radius   vpdn-group vpdn
accept-dialin
protocol l2tp
virtual-template 10
l2tp tunnel password pass   interface Virtual-Template10
ip unnumbered GigabitEthernet0/1
peer default ip address pool AAA
ppp authentication pap chap AAA
ppp authorization AAA
```

Evento inalcanzable del par del Troubleshooting

Esta sección dará algunas guías de consulta en cómo resolver problemas el evento L2TPTunnelDownPeerUnreachable en la red. Se explica aquí referente al RP cerrado PDSN pero los pasos del Troubleshooting son lo mismo al resolver problemas con GGSN/PGW.

Como recordatorio, un LAC al túnel LNS se crea para contener las sesiones del suscriptor mientras que extiende la conexión del suscriptor de un PDSN/HA/GGSN/PGW al LNS donde se termina y donde se proporciona una dirección IP. Si en un chasis de StarOS, el LNS conseguirá una dirección IP de una agrupación IP configurada. Si en algún otro LNS, por ejemplo en las instalaciones del cliente, la dirección IP es proporcionada por el LNS allí. En el último escenario, esto podía permitir con eficacia para que los usuarios conecten con su red doméstica con un LAC que se ejecutaba en un partner de itinerancia.

Un túnel LAC LNS primero se crea como la primera sesión del suscriptor se intenta para ser puesta, y permanecerá para arriba mientras haya sesiones en el túnel.

Cuando la sesión del último termina para un túnel dado, ese túnel es cerrado o apagado. Más de un túnel se puede establecer entre los mismos pares LAC-LNS.

Aquí está un snippet de la salida del comando show que **l2tp hace un túnel todo** que muestre que esto en este caso el chasis recibe los servicios LAC y LNS (TestLAC y TestLNS). Observe que el LAC y el LNS hace un túnel TODO tienen sesiones, mientras que algunos túneles cerrados RP no tienen ninguna sesión.

```
 [local]1X-PDSN# show l2tp tunnels all | more
|+----State: (C) - Connected       (c) - Connecting
|            (d) - Disconnecting   (u) - Unknown
|
|
v  LocTun ID  PeerTun ID Active Sess Peer IPAddress  Service Name   Uptime
--- ---------- ---------- ----------- --------------- ------------   ---------
.............
C  30         1          511         214.97.107.28   TestLNS         00603h50m
C  31         56         468         214.97.107.28   TestLNS         00589h31m
C  10         105        81          79.116.237.27   TestLAC         00283h53m
C  29         16         453         79.116.231.27   TestLAC         00521h32m
C  106        218        63          79.116.231.27   TestLAC         00330h10m
C  107        6          464         79.116.237.27   TestLAC         00329h47m
C  30         35         194         214.97.107.28   TestLNS         00596h06m
```

La configuración de los servicios se puede ver con

```
  show (lac-service | lns-service) name <lac or lns service name>
```

Aquí está un ejemplo del desvío L2TPTunnelDownPeerUnreachable con el servicio 1.1.1.2 LAC y el servicio LNS (par) 1.1.1.1

```
 Internal trap notification 92 (L2TPTunnelDownPeerUnreachable)  context destination service lac
peer address 1.1.1.1 local address 1.1.1.2
```

Consiga una cuenta de cuántas veces se ha accionado este desvío (puesto que la recarga o dura la restauración de las estadísticas) usando las **estadísticas del desvío del** comando show snmp

El desvío L2TPTunnelDownPeerUnreachable se acciona para el L2TP cuando ocurre un descanso de la configuración de túnel O (hola) los paquetes señales de mantenimiento no se responden a. La causa es generalmente debido al par LNS que no responde a las peticiones del LAC o a los problemas del transporte en cualquier dirección.

No hay desvío para indicar que el par hace accesible, que, si no se entiende cómo investigar más lejos, puede llevar a la confusión si todavía hay un problema o no a la hora de la investigación (petición de la característica sometida).

Para proceder, la mayoría de la parte importante que necesitamos es el IP Address de Peer. El primer paso es asegurarse de que hay la conectividad del IP que se puede marcar con el PING. Si hay Conectividad usted puede proceder con los debugs

```
****THIS IS TO BE RUN CAREFULLY and UPON verification of TAC/BU****


Active logging (exec mode) – logs written to terminal window

logging filter active facility l2tpmgr level debug
logging filter active facility l2tp-control level debug
```

```
logging active

To stop logging:

no logging active

Runtime logging (global config mode) – logs saved internally

logging filter runtime facility l2tpmgr level debug
logging filter runtime facility l2tp-control level debug

To view logs:

show logs (and/or check the syslog server if configured)
```

Notas:

l2tpmgr sigue la configuración específica de la sesión del suscriptor

l2tp-control sigue al establecimiento del túnel:

Aquí está el debug de la muestra de esta salida

Caso del uso: Falla debido inicial de la configuración de túnel para revisar los descansos

```
16:34:00.017 [l2tpmgr 48140 debug] [7/0/555 <l2tpmgr:1> l2tpmgr_call.c:591] [callid 4144ade2]
[context: destination, contextID: 3]  [software internal system] L2TPMgr-1  msid 0000012345
username laclnsuser  service <lac> - IPSEC tunnel does not exist
16:34:00.018 [l2tp-control 50069 debug] [7/0/555 <l2tpmgr:1> l2tpsnx_fsm.c:105] [callid
4144ade2] [context: destination, contextID: 3]  [software internal user] l2tp fsm: state
L2TPSNX_STATE_OPEN event L2TPSNX_EVNT_APP_NEW_SESSION ---------------------
16:34:00.018 [l2tp-control 50001 debug] [7/0/555 <l2tpmgr:1> l2tpsnx_proto.c:1474] [callid
4144ade2] [context: destination, contextID: 3]  [software internal user outbound protocol-log]
L2TP Tx PDU, from 1.1.1.2:13660 to 1.1.1.1:1701 (138)
l2tp:[TLS](0/0)Ns=0,Nr=0 *MSGTYPE(SCCRQ) *PROTO_VER(1.0) *FRAMING_CAP(AS) *BEARER_CAP(AD)
TIE_BREAKER(0706050403020100) FIRM_VER(256) *HOST_NAME(lac) VENDOR_NAME(StarentNetworks)
*ASSND_TUN_ID(10) *RECV_WIN_SIZE(16) *CHALLENGE(dbed79cdc497f266bd374d427607cd52)
16:34:00.928 [l2tp-control 50001 debug] [7/0/555 <l2tpmgr:1> l2tpsnx_proto.c:1474] [callid
4144ade2] [context: destination, contextID: 3]  [software internal user outbound protocol-log]
L2TP Tx PDU, from 1.1.1.2:13660 to 1.1.1.1:1701 (138)
l2tp:[TLS](0/0)Ns=0,Nr=0 *MSGTYPE(SCCRQ) *PROTO_VER(1.0) *FRAMING_CAP(AS) *BEARER_CAP(AD)
TIE_BREAKER(0706050403020100) FIRM_VER(256) *HOST_NAME(lac) VENDOR_NAME(StarentNetworks)
*ASSND_TUN_ID(10) *RECV_WIN_SIZE(16) *CHALLENGE(dbed79cdc497f266bd374d427607cd52)
16:34:02.943 [l2tp-control 50001 debug] [7/0/555 <l2tpmgr:1> l2tpsnx_proto.c:1474] [callid
4144ade2] [context: destination, contextID: 3]  [software internal user outbound protocol-log]
L2TP Tx PDU, from 1.1.1.2:13660 to 1.1.1.1:1701 (138)
l2tp:[TLS](0/0)Ns=0,Nr=0 *MSGTYPE(SCCRQ) *PROTO_VER(1.0) *FRAMING_CAP(AS) *BEARER_CAP(AD)
TIE_BREAKER(0706050403020100) FIRM_VER(256) *HOST_NAME(lac) VENDOR_NAME(StarentNetworks)
*ASSND_TUN_ID(10) *RECV_WIN_SIZE(16) *CHALLENGE(dbed79cdc497f266bd374d427607cd52)
16:34:06.870 [l2tp-control 50001 debug] [7/0/555 <l2tpmgr:1> l2tpsnx_proto.c:1474] [callid
4144ade2] [context: destination, contextID: 3]  [software internal user outbound protocol-log]
L2TP Tx PDU, from 1.1.1.2:13660 to 1.1.1.1:1701 (138)
l2tp:[TLS](0/0)Ns=0,Nr=0 *MSGTYPE(SCCRQ) *PROTO_VER(1.0) *FRAMING_CAP(AS) *BEARER_CAP(AD)
TIE_BREAKER(0706050403020100) FIRM_VER(256) *HOST_NAME(lac) VENDOR_NAME(StarentNetworks)
*ASSND_TUN_ID(10) *RECV_WIN_SIZE(16) *CHALLENGE(dbed79cdc497f266bd374d427607cd52)
16:34:14.922 [l2tp-control 50001 debug] [7/0/555 <l2tpmgr:1> l2tpsnx_proto.c:1474] [callid
4144ade2] [context: destination, contextID: 3]  [software internal user outbound protocol-log]
L2TP Tx PDU, from 1.1.1.2:13660 to 1.1.1.1:1701 (138)
l2tp:[TLS](0/0)Ns=0,Nr=0 *MSGTYPE(SCCRQ) *PROTO_VER(1.0) *FRAMING_CAP(AS) *BEARER_CAP(AD)
TIE_BREAKER(0706050403020100) FIRM_VER(256) *HOST_NAME(lac) VENDOR_NAME(StarentNetworks)
*ASSND_TUN_ID(10) *RECV_WIN_SIZE(16) *CHALLENGE(dbed79cdc497f266bd374d427607cd52)
```

```
------------------  16:34:22.879 [l2tp-control 50001 debug] [7/0/555 <l2tpmgr:1>
l2tpsnx_proto.c:1474] [callid 4144ade2] [context: destination, contextID: 3]  [software internal
user outbound protocol-log] L2TP Tx PDU, from 1.1.1.2:13660 to 1.1.1.1:1701 (38)
l2tp:[TLS](0/0)Ns=1,Nr=0 *MSGTYPE(StopCCN) *RESULT_CODE(2/0) *ASSND_TUN_ID(10)
16:34:22.879 [l2tp-control 50069 debug] [7/0/555 <l2tpmgr:1> l2tpsnx_fsm.c:105] [callid
4144ade2] [context: destination, contextID: 3]  [software internal user] l2tp fsm: state
L2TPSNX_STATE_WAIT_TUNNEL_ESTB event L2TPSNX_EVNT_PROTO_TUNNEL_DISCONNECTED
```

Aquí está el SNMP trap resultante accionado para corresponder con los registros antedichos que el sistema determinó por el momento el incidente

```
 16:34:22 2009 Internal trap notification 92 (L2TPTunnelDownPeerUnreachable)  context
destination service lac peer address 1.1.1.1 local address 1.1.1.2
```

Caso del uso: Falla debido inicial de la configuración de túnel para revisar los descansos - Análisis

Qué vemos somos ese túnel subimos en 16:34 e intenta enviar el desafío por cinco veces. Al parecer, no hay contestación y eventual las desconexiones del túnel.

Mire en los valores por defecto o los valores configurados de la configuración y vea

```
 max-retransmission 5
retransmission-timeout-first 1
retransmission-timeout-max 8
```

Esta configuración debe interpeted como primero retransmite después de 1 segundo, entonces aumento exponencial - doblando cada vez: 1, 2, 4, 8, 8.

Observe las MAX-retransmisiones del término (cinco) incluye la primera tentativa/transmisión.
se alcanza el retransmisión-descanso-MAX es cantidad máxima de tiempo entre las transmisiones después (si) de este límite
el retransmisión-descanso-primer es el punto de partida de cuánto tiempo esperar antes de la primera retransmisión.

Así pues, haciendo la matemáticas, en el caso de los parámetros predeterminados, un error ocurriría después de 1+ 2 + 4 + 8 + 8 segundos = 23 segundos, que se ve exactamente como en la salida abajo.

Caso del uso: Falla debido inicial de la configuración de túnel al Keepalives

La otra razón del desvío L2TPTunnelDownPeerUnreachable no es ninguna respuesta a los mensajes del intervalo de keepalive. Éstos se utilizan durante los períodos donde no hay mensajes o datos del control que son enviados sobre el túnel, para asegurarse de que el otro extremo está todavía vivo. Si hay sesiones en el túnel, pero no están haciendo cualquier cosa, este comando se asegura de que el túnel todavía esté funcionando correctamente, porque habilitandolo, los mensajes de keepalive se envían después del periodo configurado de ningún intercambio de paquetes (es decir 60 segundos), y se esperan las respuestas. La frecuencia de enviar el keepalive después de enviar primer y de no conseguir una respuesta es lo mismo como se describe anteriormente para la configuración de túnel. Así pues, después de 23 segundos de no recibir una respuesta hola a los mensajes (del keepalive), el túnel será derribado. Vea el intervalo de keepalive configurable (valor por defecto = 60s).

Aquí están los ejemplos del intercambio señal de mantenimiento acertado, del suscriptor del monitor y del registro. Observe el intervalo de un minuto entre los conjuntos de los mensajes como resultado de ningunos datos del usuario que son transmitidos para un minuto. En este ejemplo, los servicios LAC y LNS están situados en el mismo chasis, en los contextos nombrados

destino y los lns respectivamente.

```
 INBOUND>>>>>  12:54:35:660 Eventid:50000(3)
L2TP Rx PDU, from 1.1.1.1:13660 to 1.1.1.2:13661 (20)
l2tp:[TLS](5/0)Ns=19,Nr=23 *MSGTYPE(HELLO)

<<<<OUTBOUND  12:54:35:661 Eventid:50001(3)
L2TP Tx PDU, from 1.1.1.2:13661 to 1.1.1.1:13660 (12)
l2tp:[TLS](1/0)Ns=23,Nr=20 ZLB

<<<<OUTBOUND  12:55:35:617 Eventid:50001(3)
L2TP Tx PDU, from 1.1.1.2:13661 to 1.1.1.1:13660 (20)
l2tp:[TLS](1/0)Ns=23,Nr=20 *MSGTYPE(HELLO)

INBOUND>>>>>  12:55:35:618 Eventid:50000(3)
L2TP Rx PDU, from 1.1.1.1:13660 to 1.1.1.2:13661 (12)
l2tp:[TLS](5/0)Ns=20,Nr=24 ZLB  12:54:35.660 [l2tp-control 50001 debug] [7/0/555 <l2tpmgr:1>
l2tpsnx_proto.c:1474] [callid 106478e8] [context: lns, contextID: 11]  [software internal user
outbound protocol-log] L2TP Tx PDU, from 1.1.1.1:13660 to 1.1.1.2:13661 (20)
l2tp:[TLS](5/0)Ns=19,Nr=23 *MSGTYPE(HELLO)

12:55:35.618 [l2tp-control 50000 debug] [7/0/555 <l2tpmgr:1> l2tp.c:13050] [callid 106478e8]
[context: lns, contextID: 11]  [software internal user inbound protocol-log] L2TP Rx PDU, from
1.1.1.2:13661 to 1.1.1.1:13660 (20) l2tp:[TLS](1/0)Ns=23,Nr=20 *MSGTYPE(HELLO)
```

Finalmente, aquí está un ejemplo al donde, para un túnel existente, los mensajes Hello Messages no se responden, y se derriban la llamada y el túnel. Suscriptor del monitor hecho salir:

```
 <<<<OUTBOUND  14:06:21:406 Eventid:50001(3)
L2TP Tx PDU, from 1.1.1.2:13661 to 1.1.1.1:13661 (20)
l2tp:[TLS](2/0)Ns=4,Nr=2 *MSGTYPE(HELLO)

<<<<OUTBOUND  14:06:22:413 Eventid:50001(3)
L2TP Tx PDU, from 1.1.1.2:13661 to 1.1.1.1:13661 (20)
l2tp:[TLS](2/0)Ns=4,Nr=2 *MSGTYPE(HELLO)

<<<<OUTBOUND  14:06:24:427 Eventid:50001(3)
L2TP Tx PDU, from 1.1.1.2:13661 to 1.1.1.1:13661 (20)
l2tp:[TLS](2/0)Ns=4,Nr=2 *MSGTYPE(HELLO)

<<<<OUTBOUND  14:06:28:451 Eventid:50001(3)
L2TP Tx PDU, from 1.1.1.2:13661 to 1.1.1.1:13661 (20)
l2tp:[TLS](2/0)Ns=4,Nr=2 *MSGTYPE(HELLO)

<<<<OUTBOUND  14:06:36:498 Eventid:50001(3)
L2TP Tx PDU, from 1.1.1.2:13661 to 1.1.1.1:13661 (20)
l2tp:[TLS](2/0)Ns=4,Nr=2 *MSGTYPE(HELLO)

<<<<OUTBOUND  14:06:44:446 Eventid:50001(3)
L2TP Tx PDU, from 1.1.1.2:13661 to 1.1.1.1:13661 (38)
l2tp:[TLS](2/0)Ns=5,Nr=2 *MSGTYPE(StopCCN) *RESULT_CODE(2/0) *ASSND_TUN_ID(6)
```

Aquí están los registros respectivos.

Observe el descanso del túnel del control de salida - cinco recomprobación-frustrados, ms del último-intervalo 8000 para los intentos fallidos.

```
 14:06:21.406 [l2tp-control 50001 debug] [7/0/9133 <l2tpmgr:2> l2tpsnx_proto.c:1474] [callid
42c22625] [context: destination, contextID: 3]  [software internal user outbound protocol-log]
L2TP Tx PDU, from 1.1.1.2:13661 to 1.1.1.1:13661 (20)
l2tp:[TLS](2/0)Ns=4,Nr=2 *MSGTYPE(HELLO)
14:06:22.413 [l2tp-control 50001 debug] [7/0/9133 <l2tpmgr:2> l2tpsnx_proto.c:1474] [callid
42c22625] [context: destination, contextID: 3]  [software internal user outbound protocol-log]
```

```
L2TP Tx PDU, from 1.1.1.2:13661 to 1.1.1.1:13661 (20)
l2tp:[TLS](2/0)Ns=4,Nr=2 *MSGTYPE(HELLO)
14:06:24.427 [l2tp-control 50001 debug] [7/0/9133 <l2tpmgr:2> l2tpsnx_proto.c:1474] [callid
42c22625] [context: destination, contextID: 3]  [software internal user outbound protocol-log]
L2TP Tx PDU, from 1.1.1.2:13661 to 1.1.1.1:13661 (20)
l2tp:[TLS](2/0)Ns=4,Nr=2 *MSGTYPE(HE LLO)
14:06:28.451 [l2tp-control 50001 debug] [7/0/9133 <l2tpmgr:2> l2tpsnx_proto.c:1474] [callid
42c22625] [context: destination, contextID: 3]  [software internal user outbound protocol-log]
L2TP Tx PDU, from 1.1.1.2:13661 to 1.1.1.1:13661 (20)
l2tp:[TLS](2/0)Ns=4,Nr=2 *MSGTYPE(HELLO)
14:06:36.498 [l2tp-control 50001 debug] [7/0/9133 <l2tpmgr:2> l2tpsnx_proto.c:1474] [callid
42c22625] [context: destination, contextID: 3]  [software internal user outbound protocol-log]
L2TP Tx PDU, from 1.1.1.2:13661 to 1.1.1.1:13661 (20)
l2tp:[TLS](2/0)Ns=4,Nr=2 *MSGTYPE(HELLO)
14:06:44.446 [l2tp-control 50068 warning] [7/0/9133 <l2tpmgr:2> l2tp.c:14841] [callid 42c22625]
[context: destination, contextID: 3]  [software internal user] L2TP (Local[svc: lac]: 6
Remote[1.1.1.1]: 2): Control tunnel timeout -  retry-attempted 5 , last-interval 8000 ms, Sr 2,
Ss 5, num-pkt-not-acked 1, Sent-Q-len 1, tun-recovery-flag 0, instance-recovery-flag 0, msg-type
Hello
14:06:44.446 [l2tp-control 50001 debug] [7/0/9133 <l2tpmgr:2> l2tpsnx_proto.c:1474] [callid
42c22625] [context: destination, contextID: 3]  [software internal user outbound protocol-log]
L2TP Tx PDU, from 1.1.1.2:13661 to 1.1.1.1:13661 (38)
l2tp:[TLS](2/0)Ns=5,Nr=2 *MSGTYPE(StopCCN) *RESULT_CODE(2/0) *ASSND_TUN_ID(6)
14:06:44.447 [l2tp-control 50069 debug] [7/0/9133 <l2tpmgr:2> l2tpsnx_fsm.c:105] [callid
42c22625] [context: destination, contextID: 3]  [software internal user] l2tp fsm: state
L2TPSNX_STATE_CONNECTED event L2TPSNX_EVNT_PROTO_SESSION_DISCONNECTED
```

Y SNMP trap correspondiente

```
 14:06:44 2009 Internal trap notification 92 (L2TPTunnelDownPeerUnreachable)  context
destination service lac peer address 1.1.1.1 local address 1.1.1.2
```

Muestre las consideraciones de la salida

Funcionar con el siguiente comando indicará si ha habido los problemas del alcance del peer con un par específico (o para todos los túneles en un servicio determinado de la laca/de los lns)

```
 show l2tp statistics (peer-address <peer ip address> | ((lac-service | lns-service) <lac or lns
service name>))
```

Las conexiones activas contradicen las coincidencias que el número de túneles existentes para ese par allí puede ser más de uno, como se ve en la salida de la demostración l2tp hace un túnel todos de anterior.

No podido para conectar al revés indicará han ocurrido cuántos errores de la configuración de túnel.
El Reintento máximo excedido al revés es probablemente el contador más importante, pues indica el error conectar debido a un descanso (cada recomprobación excedida da lugar a un desvío L2TPTunnelDownPeerUnreachable). Esta información le dice solamente que la frecuencia del problema para un par dado, él no le dice porqué ocurrió el descanso. Pero conocer la frecuencia puede ser útil en poner juntos los pedazos en el proceso de Troubleshooting total.

La sección de las sesiones da el detalle en el nivel de la sesión del suscriptor (contra el nivel del túnel)
Las sesiones activas contradicen las coincidencias que la suma (si más de un túnel para un par) de la salida activa de la columna de Sess de la demostración l2tp hace un túnel para el peer particular.
No podido para conectar al revés indica cuántas sesiones no han podido conectar. Observe que las configuraciones falladas de la sesión no accionan el desvío L2TPTunnelDownPeerUnreachable, sólo lo hacen las configuraciones de túnel falladas.

Hay también los contadores que la versión de los túneles de la demostración l2tp ordena que pueden ser útiles.

```
show l2tp tunnels counters peer-address <peer address>
```

Finalmente, en el nivel de la sesión, todos los suscriptores para un par dado pueden ser vistos.

```
show l2tp sessions peer-address <peer ip address>
```

El número de suscriptores encontrados debe hacer juego el número de sesiones activas según lo discutido.