L2TP en StarOS - Implementación en ASR5k y Troubleshooting de L2TP Peering - L2TPTunnelDownPeerUnreachable

Contenido

Introducción

Este documento describe cómo se implementa el protocolo de túnel de capa 2 (L2TP) en StarOS en el ASR5k y la solución de problemas del peering L2TP - L2TPTunnelDownPeerUnreachable.

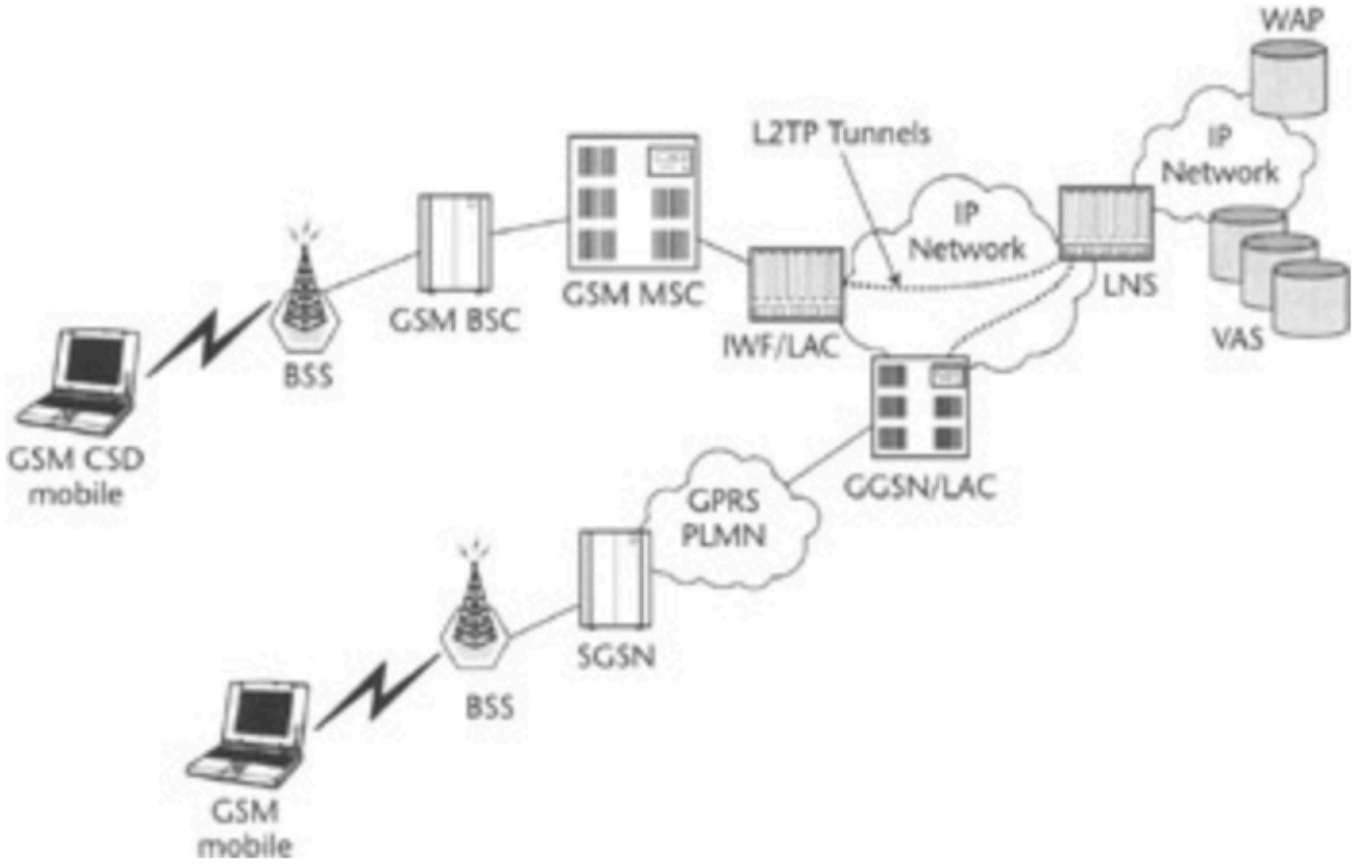
¿Qué es L2TP?

L2TP amplía la naturaleza punto a punto de PPP. L2TP proporciona un método de encapsulación para la transmisión de tramas PPP tunelizadas, que permite que los extremos PPP sean tunelizados a través de una red conmutada por paquetes. L2TP se suele implementar en escenarios de tipo acceso remoto que utilizan Internet para ofrecer servicios de tipo intranet. El concepto es el de una red privada virtual (VPN).

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

- LAC: El LAC es un peer al LNS que actúa como un lado del extremo del túnel. LAC finaliza la conexión remota PPP y se ubica entre el remoto y el LNS. Los paquetes se reenvían a y desde la conexión remota a través de la conexión PPP. Los paquetes hacia y desde el LNS se reenvían a través del túnel L2TP.
- LNS: El LNS es un peer para el LAC que actúa como un lado del extremo del túnel. El LNS es el punto de terminación para las sesiones tunelizadas PPP de LAC. Esto se utiliza para agregar las sesiones PPP tunelizadas LAC múltiples y el ingreso a la red privada.

Configuración L2TP simplificada en red móvil, como se muestra en esta imagen.



Hay dos tipos de mensajes diferentes que L2TP utiliza:

- Mensajes de control: L2TP pasa los mensajes de datos y control por canales de datos y control independientes. El canal de control en banda pasa los mensajes de control de conexión secuenciada, administración de llamadas, informes de errores y control de sesión. La iniciación de la conexión de control no es específica para el LAC o el LNS sino más bien para el originador y receptor del túnel que tiene relevancia en el establecimiento de conexión de control. Se utiliza un método de autenticación de desafío secreto compartido entre los puntos finales del túnel.
- Mensajes de datos: Los mensajes de datos se utilizan para encapsular las tramas PPP que se envían al túnel L2TP.

El flujo de llamadas detallado y el establecimiento del túnel se explican aquí:

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

¿Dónde la utilizamos en la movilidad?

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

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

¿Qué es ASR5x00 en esta configuración?

ASR5k puede soportar la funcionalidad LAC y LNS.

Soporte de LAC L2TP

L2TP establece túneles de control L2TP entre LAC y LNS antes de tunelizar las conexiones PPP del suscriptor como sesiones L2TP. El servicio LAC se basa en la misma arquitectura que el GGSN y se beneficia de la asignación dinámica de recursos y el procesamiento distribuido de mensajes y datos. Este diseño permite que el servicio LAC admita más de 4000 configuraciones por segundo o un máximo de más de 3G de rendimiento. Puede haber un máximo de 65535 sesiones en un único túnel y hasta 500 000 sesiones L2TP usando 32 000 túneles por sistema.

Soporte LNS L2TP

El sistema configurado como servidor de red de protocolo de túnel de capa 2 (LNS) admite los túneles de terminación de red privada virtual (VPN) segura entre los concentradores de acceso L2TP (LAC).

L2TP establece túneles de control L2TP entre LAC y LNS antes de tunelizar las conexiones PPP del suscriptor como sesiones L2TP. Puede haber un máximo de 65535 sesiones en un único túnel y hasta 500 000 sesiones por LNS.

La arquitectura LNS es similar a la GGSN y utiliza el concepto de un desmultiplexor para asignar de forma inteligente nuevas sesiones L2TP a través de los recursos de software y hardware disponibles en la plataforma sin intervención del operador.

Para obtener más información, consulte las guías de configuración de PGW/GGSN.

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

Ejemplo de configuración para 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
```

Ejemplo de configuración para 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:** Múltiples direcciones en la misma interfaz IP se pueden enlazar a diferentes servicios LNS. Sin embargo, cada dirección puede estar enlazada a un solo servicio LNS. Además, el servicio LNS no puede enlazarse a la misma interfaz que otros servicios como un servicio LAC.

Ejemplo de configuración para LNS en el dispositivo Cisco IOS

Esto se puede utilizar como ejemplo de configuración auxiliar para la configuración de Cisco IOS y no está sujeto 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
```

Solución de problemas de evento de par inalcanzable

En esta sección se proporcionan algunas pautas sobre cómo resolver problemas de L2TPTunnelDownPeerUnreachable en la red. Se explica aquí con referencia al RP cerrado de PDSN, pero los pasos de resolución de problemas son los mismos cuando se resuelve el problema con GGSN/PGW.

Como recordatorio, se crea un túnel LAC a LNS para contener sesiones de suscriptor mientras extiende la conexión del suscriptor de una PDSN/HA/GGSN/PGW al LNS donde se termina y donde se proporciona una dirección IP. Si se encuentra en un chasis StarOS, el LNS obtendrá una dirección IP de un conjunto IP configurado. Si en otros LNS, por ejemplo en las instalaciones del cliente, la dirección IP la proporciona el LNS allí. En esta última situación, esto podría permitir que los usuarios se conecten a su red doméstica a través de un LAC que se ejecuta en un partner de roaming.

Se crea por primera vez un túnel LNS de LAC cuando se intenta configurar la primera sesión del suscriptor y se mantiene activa mientras haya sesiones en el túnel.

Cuando la última sesión finaliza para un túnel determinado, ese túnel se cierra o se cierra. Se puede establecer más de un túnel entre los mismos pares LAC-LNS.

Aquí hay un fragmento de salida del comando **show l2tp tunnels all** que muestra esto en este caso el chasis aloja los servicios LAC y LNS (TestLAC y TestLNS). Tenga en cuenta que los túneles LAC y LNS TODOS tienen sesiones, mientras que algunos túneles Cerrados RP no tienen sesiones.

```
 [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>
```

Este es un ejemplo de la trampa L2TPTunnelDownPeerUnreachable con el servicio 1.1.1.2 de LAC y el servicio LNS (peer) 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 un recuento de cuántas veces se ha disparado esta trampa (desde la recarga o el último reinicio de las estadísticas) usando el comando **show snmp trap statistics**

La trampa L2TPTunnelDownPeerUnreachable se activa para L2TP cuando se produce un tiempo de espera de configuración del túnel O cuando no se responde a los paquetes keep-alive (Hello). La causa suele deberse a que el peer LNS no responde a las solicitudes del LAC o a problemas de transporte en cualquier dirección.

No hay ninguna trampa que indique que el par se puede alcanzar, lo que, si no se entiende cómo investigar más a fondo, puede dar lugar a confusión sobre si todavía hay un problema o no en el momento de la investigación (solicitud de característica presentada).

Para continuar, la parte más importante que necesitamos es la dirección IP del par. El primer paso es asegurarse de que hay conectividad IP que se puede verificar con PING. Si hay conectividad, puede continuar con las depuraciones

```
****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 realiza un seguimiento de la configuración de la sesión de suscriptor específica

l2tp-control rastrea el establecimiento del túnel:

Aquí hay un ejemplo de depuración de este resultado

Caso de uso: Error de configuración de túnel inicial debido a tiempos de espera de reintento

```
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
```

Esta es la trampa SNMP resultante disparada para coincidir con los registros anteriores por el momento en que el sistema determinó la falla

```
 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 de uso: Error de configuración inicial del túnel debido a tiempos de espera de reintento - Análisis

Lo que vemos es que el túnel sale a las 16:34 y trata de enviar el desafío cinco veces. Aparentemente, no hay respuesta y finalmente el túnel se desconecta.

Busque los valores predeterminados de configuración o los valores configurados y consulte

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

Esta configuración se interpretará como primera retransmisión después de 1 segundo, luego aumento exponencial - duplicando cada vez: 1, 2, 4, 8, 8.

Tenga en cuenta que el término max-retransmission (cinco) incluye el primer intento/transmisión.
retransmit-timeout-max es la cantidad máxima de tiempo entre las transmisiones después (si) de alcanzar este límite
retransmit-timeout-first es el punto de partida de cuánto tiempo esperar antes de la primera retransmisión.

Por lo tanto, haciendo la matemática, en el caso de los parámetros predeterminados, se produciría una falla después de 1+ 2 + 4 + 8 + 8 segundos = 23 segundos, lo que se ve exactamente como en la salida a continuación.

Caso de uso: Fallo de configuración inicial del túnel debido a keepalives

La otra razón para la trampa L2TPTunnelDownPeerUnreachable no es respuesta a los mensajes del intervalo de keepalive. Estos se utilizan durante periodos en los que no se envían mensajes de control o datos a través del túnel, para asegurarse de que el otro extremo aún esté vivo. Si hay sesiones en el túnel, pero no están haciendo nada, este comando asegura que el túnel siga funcionando correctamente, porque al habilitarlo, los mensajes keepalive se envían después del período configurado de no intercambio de paquetes (es decir, 60 segundos) y se esperan respuestas. La frecuencia de envío de la señal de mantenimiento después de enviar la primera y de no recibir respuesta es la misma que se describe anteriormente para la configuración del túnel. Por lo tanto, después de 23 segundos de no recibir una respuesta a los mensajes hello (keepalive), el túnel se desactivará. Consulte el intervalo de keepalive configurable (valor predeterminado = 60).

A continuación se muestran ejemplos de intercambio "keep-alive" exitoso, tanto del suscriptor de monitor como del registro. Observe el intervalo de un minuto entre conjuntos de mensajes como resultado de que no se transmitió ningún dato de usuario durante un minuto. En este ejemplo, los servicios LAC y LNS se encuentran en el mismo chasis, en contextos denominados **destination** y **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)
```

Por último, aquí hay un ejemplo en el que, para un túnel EXISTENTE, no se responde a los mensajes de saludo y se desactivan la llamada y el túnel. Salida del suscriptor del monitor:

```
 <<<<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)
```

Estos son los registros respectivos.

Observe el tiempo de espera del túnel de control de salida - intento de reintento cinco, último intervalo 8000 ms 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 trampa SNMP 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
```

Mostrar consideraciones de salida

Si se ejecuta el siguiente comando, se indicará si ha habido problemas de alcance de peer con un peer específico (o para todos los túneles en un servicio lac/lns determinado)

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

El contador Conexiones activas coincide con el número de túneles existentes para ese par que puede haber más de uno, como se ve en el resultado de show l2tp tunnels all desde antes.

El contador Error al conectar indicará cuántos errores de configuración del túnel se han producido.
El contador Max Retry Exceeded es probablemente el contador más importante, ya que indica una falla en la conexión debido a un tiempo de espera (cada Retry excedido resulta en una trampa L2TPTunnelDownPeerUnreachable). Esta información sólo le indica la frecuencia del problema para un par dado, no le indica por qué ocurrió el tiempo de espera. Sin embargo, conocer la frecuencia puede ser útil para reunir las piezas en el proceso general de resolución de problemas.

La sección Sesiones proporciona detalles en el nivel de sesión del suscriptor (frente al nivel de túnel)
El contador de sesiones activas coincide con la suma de (si hay más de un túnel para un par) el resultado de la columna de Sess activo de show l2tp tunnels para el par en particular.
El contador Error al conectar indica cuántas sesiones no se han podido conectar. Tenga en cuenta que las configuraciones de sesión fallidas NO activan la trampa L2TPTunnelDownPeerUnreachable, sólo las configuraciones de túnel fallidas lo hacen.

También hay una versión de contadores del comando show l2tp tunnels que puede ser útil.

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

Por último, en el nivel de sesión, se pueden ver todos los suscriptores de un par determinado.

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

El número de suscriptores encontrados debe coincidir con el número de sesiones activas tal y como se ha discutido.