L2TP no StarOS - Implementação no ASR5k e Troubleshooting L2TP Peering - L2TPTunnelDownPeerUnreachable

Contents

[Introduction](#)
[O que é L2TP?](#)
[Onde usamos isso na mobilidade?](#)
[O que é ASR5x00 nessa configuração?](#)
[Suporte a LAC L2TP](#)
[Suporte LNS L2TP](#)
[Configuração para ativar serviços nos dispositivos Cisco no ASR5k](#)
[Exemplo de configuração para LAC em ASR5k](#)
[Exemplo de configuração para LNS em ASR5k](#)
[Exemplo de configuração para LNS no dispositivo IOS Cisco](#)
[Identificar e Solucionar Problemas de Evento Inalcançável de Peer](#)
[Caso de uso: Falha na configuração inicial do túnel devido a tempos limite de repetição](#)
[Caso de uso: Falha na configuração inicial do túnel devido aos keepalives](#)
[Mostrar considerações de saída](#)

Introduction

Este documento descreve como o L2TP (Layer 2 Tunneling Protocol) no StarOS é implementado no ASR5k e Troubleshoot L2TP Peering - L2TPTunnelDownPeerUnreachable.

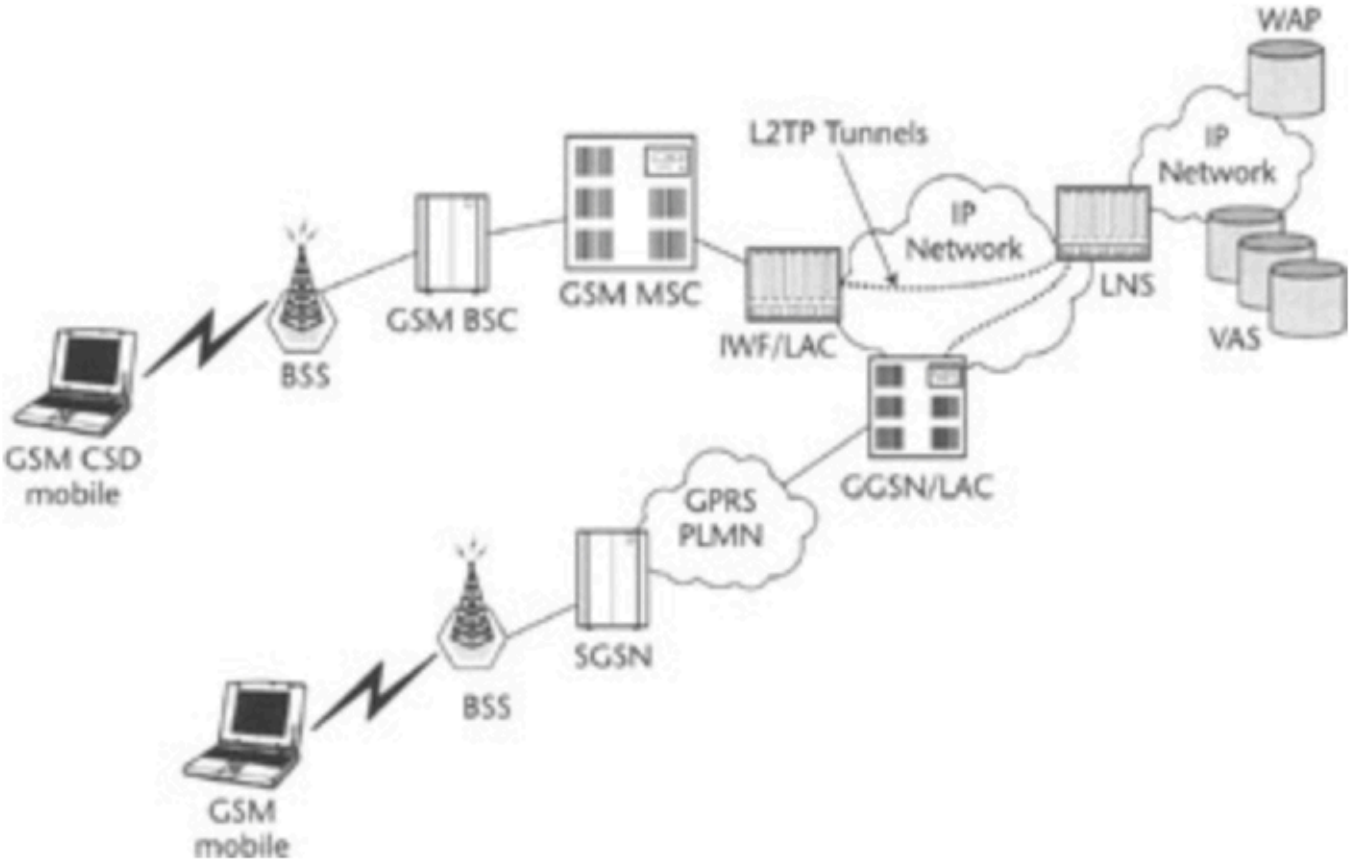
O que é L2TP?

L2TP estende a natureza ponto-a-ponto de PPP. L2TP fornece um método de encapsulamento para a transmissão de frames PPP encapsulados, o que permite aos pontos de extremidade PPP serem encapsulados em uma rede comutada por pacote. L2TP é o mais implantado em cenários do tipo de acesso remoto que utilizam a Internet para oferecer serviços de tipo intranet. O conceito é de uma Rede Virtual Privada (VPN, Virtual Private Network).

Os dois elementos físicos primários de L2TP são o Concentrador de Acesso L2TP (LAC, L2TP Access Concentrator) e o Servidor de Rede L2TP (LNS, L2TP Network Server):

- LAC: O LAC é um peer do LNS que atua como um lado do endpoint do túnel. O LAC termina a conexão PPP remota e passa entre o remoto e o LNS. Os pacotes são encaminhados da e para a conexão remota pela conexão PPP. Os pacotes para e de LNS são encaminhados pelo túnel L2TP.
- LNS: O LNS é um peer do LAC que atua como um lado do endpoint do túnel. O LNS é o ponto de terminação para as sessões encapsuladas LAC PPP. Ele é utilizado para agregar as várias sessões PPP encapsuladas por LAC e entrar na rede privada.

Configuração L2TP simplificada na rede móvel, como mostrado nesta imagem.



Há dois tipos de mensagem diferentes utilizados por L2TP:

- Mensagens de controle: O L2TP passa as mensagens de controle e de dados por canais separados de controle e de dados. O canal de controle dentro da banda passa pelo gerenciamento de conexão de controle em sequência, pelo gerenciamento de chamadas, pelos relatórios de erro e pelas mensagens de controle de sessão. O início da conexão de controle não é específico do LAC ou do LNS, mas o originador de túnel e o receptor com relevância no estabelecimento da conexão de controle. Um método de autenticação de desafio com segredo compartilhado é utilizado entre os pontos de extremidade do túnel.
- Mensagens de dados: As mensagens de dados são usadas para encapsular os quadros PPP enviados para o túnel L2TP.

O fluxo de chamadas detalhado e o estabelecimento do túnel são explicados aqui:

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

Onde usamos isso na mobilidade?

A implantação típica é para usuários corporativos onde o GGSN atua como LAC e estabelece túneis seguros para o LNS que é operado na rede corporativa. Fluxos de chamada detalhados estão disponíveis no apêndice do guia de configuração GGSN que pode ser encontrado, por versão de software específica, aqui:

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

O que é ASR5x00 nessa configuração?

O ASR5k pode suportar a funcionalidade LAC e LNS.

Suporte a LAC L2TP

O L2TP estabelece túneis de controle L2TP entre o LAC e o LNS antes de tunelar as conexões PPP do assinante como sessões L2TP. O serviço LAC é baseado na mesma arquitetura do GGSN e se beneficia da alocação dinâmica de recursos e do processamento distribuído de mensagens e dados. Esse design permite que o serviço LAC suporte mais de 4.000 configurações por segundo ou um máximo de mais de 3G de throughput. Pode haver um máximo de 65535 sessões em um único túnel e até 500.000 sessões L2TP usando 32.000 túneis por sistema.

Suporte LNS L2TP

O sistema configurado como um LNS (Layer 2 Tunneling Protocol Network Server) suporta os túneis de VPN (Virtual Private Network) de terminação entre os LACs (Concentradores de Acesso L2TP).

O L2TP estabelece túneis de controle L2TP entre o LAC e o LNS antes de tunelar as conexões PPP do assinante como sessões L2TP. Pode haver um máximo de 65535 sessões em um único túnel e até 500.000 sessões por LNS.

A arquitetura LNS é semelhante à GGSN e utiliza o conceito de um desmultiplexador para atribuir de forma inteligente novas sessões L2TP através dos recursos de software e hardware disponíveis na plataforma, sem intervenção do operador.

Para obter mais informações, consulte os guias de configuração PGW/GGSN.

Configuração para habilitar serviços nos dispositivos Cisco no ASR5k

Exemplo de configuração para LAC em 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
```

Exemplo de configuração para LNS em 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
}
```

> **Note**: Vários endereços na mesma interface IP podem ser vinculados a serviços LNS diferentes. No entanto, cada endereço pode ser vinculado a apenas um serviço LNS. Além disso, o serviço LNS não pode ser vinculado à mesma interface que outros serviços, como um serviço LAC.

Exemplo de configuração para LNS no dispositivo IOS Cisco

Isso pode ser usado como uma amostra de configuração de suporte para a configuração do Cisco IOS e não está sujeito a este artigo.

configuração de 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
```

Identificar e Solucionar Problemas de Evento Inalcançável de Peer

Esta seção dará algumas diretrizes sobre como solucionar problemas de evento L2TPTunnelDownPeerUnreachable na rede. Ele é explicado aqui com referência ao RP fechado de PDSN, mas as etapas de solução de problemas são as mesmas ao Troubleshoot com

GGSN/PGW.

Como lembrete, um túnel LAC para LNS é criado para conter sessões de assinantes enquanto estende a conexão do assinante de um PDSN/HA/GGSN/PGW para o LNS onde ele é terminado e onde um endereço IP é fornecido. Se estiver em um chassi StarOS, o LNS obterá um endereço IP de um pool IP configurado. Se estiver em algum outro LNS, por exemplo nas instalações do cliente, o endereço IP é fornecido pelo LNS. No último cenário, isso poderia permitir que os usuários se conectassem à sua rede residencial por meio de um LAC em execução em um parceiro de roaming.

Um túnel LAC LNS é criado pela primeira vez quando se tenta configurar a primeira sessão de assinante e permanecerá ativa enquanto houver sessões no túnel.

Quando a última sessão termina para um determinado túnel, esse túnel é fechado ou desligado. Mais de um túnel pode ser estabelecido entre os mesmos pares LAC-LNS.

Aqui está um trecho de saída do comando **show l2tp tunels all** que mostra isso neste caso, o chassi hospeda os serviços LAC e LNS (TestLAC e TestLNS). Observe que os túneis LAC e LNS TODOS têm sessões, enquanto alguns túneis fechados de RP não têm sessões.

```
 [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
```

A configuração dos serviços pode ser vista com

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

Aqui está um exemplo da armadilha L2TPTunnelDownPeerUnreachable com o serviço LAC 1.1.1.2 e o serviço 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
```

Obtenha uma contagem de quantas vezes essa armadilha foi disparada (desde a recarga ou a última redefinição de estatísticas) usando o comando **show snmp trap statistics**

A armadilha L2TPTunnelDownPeerUnreachable é disparada para L2TP quando ocorre um tempo limite de configuração de túnel OU os pacotes de manutenção de atividade (Hello) não são respondidos. A causa geralmente se deve ao peer LNS que não responde a solicitações do LAC ou a problemas de transporte em qualquer direção.

Não há armadilha para indicar que o peer se torna acessível, o que, se não for entendido como investigar mais a fundo, pode levar a confusão sobre se ainda há um problema ou não no

momento da investigação (solicitação de recurso enviada).

Para continuar, a parte mais importante de que precisamos é o endereço IP do peer. A primeira etapa é garantir que haja conectividade IP que possa ser verificada com o PING. Se houver conectividade, você poderá prosseguir com as depurações

```
****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 controla a configuração específica da sessão do assinante

l2tp-control rastreia o estabelecimento do túnel:

Aqui está um exemplo de depuração desta saída

Caso de uso: Falha na configuração inicial do túnel devido a tempos limite de repetição

```
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
```

Aqui está a armadilha SNMP resultante disparada para corresponder aos registros acima no momento em que o sistema determinou a falha

```
 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: Falha na configuração inicial do túnel devido a tempos limite de repetição - Análise

O que vemos é que o túnel aparece às 16h34 e tenta enviar o desafio por cinco vezes. Aparentemente, não há resposta e, eventualmente, o túnel se desconecta.

Examinar os padrões de configuração ou valores configurados e ver

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

Essa configuração deve ser interceptada como primeira retransmissão após 1 segundo, depois aumento exponencial - dobrando a cada vez: 1, 2, 4, 8, 8.

Observe que o termo max-retransmissions (cinco) inclui a primeira tentativa/transmissão.
retransmission-timeout-max é a quantidade máxima de tempo entre transmissões após (se) esse limite ser atingido
retransmission-timeout-first é o ponto de partida de quanto tempo esperar antes da primeira retransmissão.

Então, fazendo as contas, no caso dos parâmetros padrão, uma falha ocorreria após 1+ 2 + 4 + 8 + 8 segundos = 23 segundos, o que é exatamente como na saída abaixo.

Caso de uso: Falha na configuração inicial do túnel devido aos keepalives

A outra razão para a armadilha L2TPTunnelDownPeerUnreachable é a ausência de resposta às mensagens keepalive-interval. Eles são usados durante os períodos em que não há mensagens de controle ou dados sendo enviados pelo túnel, para garantir que a outra extremidade ainda esteja viva. Se houver sessões no túnel, mas elas não estiverem fazendo nada, esse comando garante que o túnel ainda esteja funcionando corretamente, pois ao ativá-lo, as mensagens de keepalive são enviadas após o período configurado de ausência de troca de pacotes (ou seja, 60 segundos) e as respostas são esperadas. A frequência de envio do keepalive após o envio do primeiro e não obtenção de uma resposta é a mesma descrita acima para a configuração do túnel. Assim, após 23 segundos de não receber uma resposta às mensagens de saudação (keepalive), o túnel será destruído. Consulte intervalo de keepalive configurável (padrão = 60s).

Aqui estão exemplos de troca bem-sucedida de manutenção de atividade, tanto do assinante de monitoramento quanto do registro. Observe o intervalo de um minuto entre os conjuntos de mensagens como resultado de nenhum dado do usuário ser transmitido por um minuto. Neste exemplo, os serviços LAC e LNS estão localizados no mesmo chassi, em contextos chamados **destino** e **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, aqui está um exemplo em que, para um túnel EXISTENTE, as mensagens de saudação não são respondidas e a chamada e o túnel são desligados. Monitorar saída do assinante:

```
 <<<<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)
```

Aqui estão os respectivos registros.

Observe o tempo limite do túnel de controle de saída - tentativa de tentativa de cinco, último intervalo de 8000 ms para as tentativas com falha.

```
 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
```

E armadilha SNMP correspondente

```
 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 considerações de saída

A execução do comando a seguir indicará se houve problemas de alcançabilidade de peer com um peer específico (ou para todos os túneis em um serviço lac/lns específico)

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

```
service name>))
```
O contador de Conexões Ativas corresponde ao número de túneis existentes para esse peer que pode haver mais de um, conforme visto na saída de show l2tp tunels, todos do anterior.

O contador Falha ao conectar indicará quantas falhas de configuração de túnel ocorreram.
O contador Max Retry Exceeded é provavelmente o mais importante, pois indica falha de conexão devido a um tempo limite (cada Retry excedeu o resultado em uma armadilha L2TPTunnelDownPeerUnreachable). Essas informações informam apenas a frequência do problema para um determinado peer. Elas não informam por que o tempo limite ocorreu. Mas conhecer a frequência pode ser útil para reunir as partes no processo geral de solução de problemas.

A seção Sessões fornece detalhes no nível de sessão do assinante (em relação ao nível do túnel)
O contador Sessões Ativas corresponde à soma (se mais de um túnel para um peer) da saída da coluna Sess Ativo de show l2tp túneis para o peer específico.
O contador Falha ao conectar indica quantas sessões falharam na conexão. Observe que as configurações de sessão com falha NÃO disparam a armadilha L2TPTunnelDownPeerUnreachable, mas somente as configurações de túnel com falha disparam.

Também há uma versão de contadores do comando show l2tp tunels que pode ser útil.

```
show l2tp tunnels counters peer-address <peer address>
```
Finalmente, no nível da sessão, todos os assinantes de um determinado peer podem ser vistos.

```
show l2tp sessions peer-address <peer ip address>
```
O número de assinantes encontrado deve corresponder ao número de sessões ativas conforme discutido.