

Conceptos y Troubleshooting de Pseudowire

Contenido

[Introducción](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Concepto de Pseudowire](#)

[Resolución de problemas de Pseudowire](#)

Introducción

Los pseudowires (PW) se utilizan para proporcionar servicios de extremo a extremo a través de una red MPLS. Son los bloques de creación básicos que pueden proporcionar un servicio punto a punto, así como un servicio multipunto como VPLS, que es prácticamente una malla de PW utilizada para crear el dominio de puente a través del cual fluyen los paquetes.

Editado por: Kumar Sridhar

Prerequisites

Quienes lean este documento deben tener conocimiento de lo siguiente:

- Conceptos de MPLS Tunneling

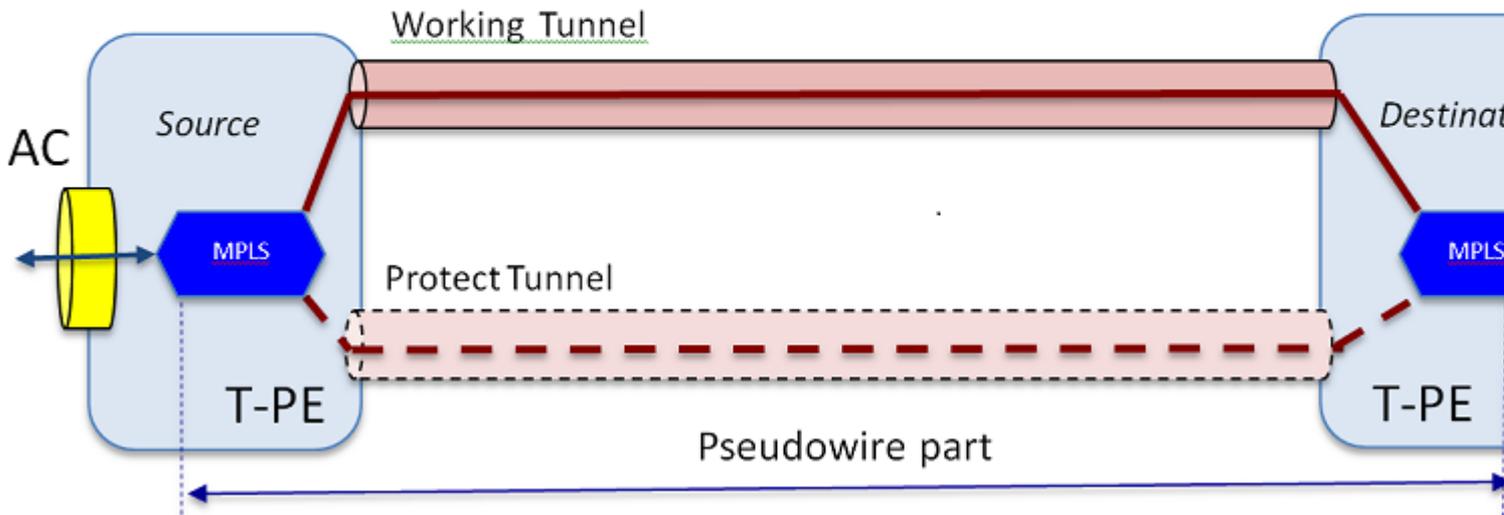
Componentes Utilizados

La información de este documento se basa en la familia de productos Cisco® Carrier Packet Transport (CPT) y, en particular, CPT50.

Concepto de Pseudowire

Los pseudowires conceptualmente se ven de la siguiente manera:

Pseudowire on Port/VLAN



El servicio integral se compone de 2 partes. Las piezas Circuito de acoplamiento (AC) y Pseudowire. En Cisco Transport Controller (CTC), se sigue haciendo referencia a todo el circuito de extremo a extremo como Pseudowire, pero hay que tener en cuenta la distinción de dos partes que se muestra aquí para la resolución de problemas que sigue.

También recuerde que se debe haber creado un túnel para alojar el servicio Pseudowire configurado anteriormente. El túnel puede estar protegido (como se muestra aquí) o desprotegido.

La parte de Pseudowire prácticamente comienza y se detiene en los puntos finales del túnel (si excluye el bloque de encapsulación MPLS que se muestra aquí).

La parte de CA comienza desde el punto final del túnel hasta la interfaz orientada al cliente, donde se define el punto de flujo Ethernet (EFP), para identificar el tráfico de cliente específico que se transporta a través de este Pseudowire. Hay 2 AC; uno en cada extremo.

El AC transporta el tráfico del cliente en su forma nativa, es decir, las tramas Ethernet con o sin etiquetado VLAN dependiendo de si estamos creando un Pseudowire basado en VLAN o un Pseudowire basado en Ethernet (casilla AC Type en el asistente de creación de PW). A continuación, se añaden las etiquetas MPLS para el servicio PW específico, así como para el túnel por el que circula. A continuación, los paquetes se envían a través de la parte Pseudowire del circuito a la nube MPLS. Este proceso se denomina imposición de etiquetas en la terminología MPLS. En el extremo lejano, ocurre el proceso inverso, es decir, las etiquetas se eliminan o se produce la Disposición de la Etiqueta, y los paquetes, que ahora están de regreso a las tramas Ethernet nativas, se entregan al otro extremo a través de la parte de CA del extremo lejano del circuito Pseudowire.

Resolución de problemas de Pseudowire

Para que el servicio Pseudowire funcione de extremo a extremo, la pieza Pseudowire y las dos piezas AC deben funcionar juntas. La resolución de problemas del circuito implica cada parte, donde cada una de las partes de AC-PW-AC se depuran por separado para identificar dónde está el problema.

En el siguiente análisis de solución de problemas, se supone que el PW se ha configurado correctamente y que todos los problemas de capa 1 o capa física ya se han depurado y descartado.

En primer lugar, depurar la parte PW es fácil. Comience por identificar el circuito a través del comando

"**show mpls l2 vc**" ejecutado en la ventana IOS en un nodo final. Observe el identificador de circuito virtual (VCID), así como la dirección del nodo de destino de la conexión.

```
10.88.130.201#show mpls l2 vc
```

```
Local intf Local circuit Dest address VC ID Status
```

```
-----  
-----
```

```
Gi36/2 Eth VLAN 200 202.202.202.202 12 UP
```

```
VFI vfi::1 VFI 202.202.202.202 124 UP
```

```
VFI vfi::1 VFI 204.204.204.204 124 UP
```

Aquí, el PW de interés es el primer PW que se configuró como VLAN 200 basada en la interfaz Gi36/2. Asegúrese de que el estado de la interfaz es **ACTIVO**.

el comando **show mpls l2 vc 12 detail** le brinda mucha información sobre el PW. A continuación se destacan los campos importantes como **ID de túnel, ID de nodo remoto, pila de etiquetas, número PWID y estadísticas**.

```
10.88.130.201#show mpls l2 vc 12 detail
```

```
Interfaz local: Gi36/2 up, protocolo de línea up, Eth VLAN 200 up
```

```
Dirección de destino: 202.202.202.202, ID de VC: 12, estado de VC: activo
```

```
Interfaz de salida: Tp102, pila de etiquetas impuestas {16/19}
```

```
Ruta preferida: Tunnel-tp102, activo
```

```
Ruta predeterminada: listo
```

```
Salto siguiente: point2point
```

```
Hora de creación: 00:32:52, hora del último cambio de estado: 00:05:42
```

```
Protocolo de señalización: manual
```

```
Compatibilidad con TLV de estado (local/remoto): habilitada/N/A
```

```
Vigilancia de ruta LDP: habilitada
```

```
Máquina de estado de etiqueta/estado: establecida, LruRru
```

```
Último estado del plano de datos local recibido: sin fallo
```

```
Último estado del plano de datos BFD recibido: No enviado
```

```
Último estado del circuito SSS local recibido: sin fallo
```

```
Último estado del circuito SSS local enviado: sin fallo
```

```
Último estado TLV LDP local enviado: sin error
```

Último estado de LDP TLV remoto recibido: sin error

Último estado de ADJ de LDP remoto recibido: sin fallo

Etiquetas de VC MPLS: local 18, remoto 19

PWID: 7

ID de grupo: local 0, remoto 0

MTU: local 1500, remoto 1500 <---- Los valores local y remoto deben coincidir

Secuenciación: recepción deshabilitada, envío deshabilitado

Palabra de control: Activado

Descriptor de SSO: 202.202.202.202/12, etiqueta local: 18

ID de switch/segmento SSM: 20513/12320 (usado), PWID: 7

Estadísticas de VC:

totales de paquetes de tránsito: recibir 10, enviar 0

totales de bytes de tránsito: recibir 1320, enviar 0

caídas de paquetes de tránsito: recepción 0, error de secuencia 0, envío 0

Si el PW no funciona, asegúrese de que el túnel (en este caso, el túnel 102) esté en buen estado y, si no es así, solucione el problema del túnel. La resolución de problemas del túnel está fuera del alcance de este artículo.

Asegúrese de que las etiquetas de la pila estén definidas como se muestra anteriormente, es decir, que no estén en blanco. Asegúrese de que el PW esté programado en el hardware mediante la ejecución del comando **show platform mpls pseudowire pwid** con el número PWID apropiado.

10.88.130.201#**show platform mpls pseudowire pwid 7**

ID de PW: 7

Clave de VC de PW: 7

Clave PW AC: 786434

¿Es PW bind receive en HW?: sí

¿Está configurado PW en hardware?: sí

Está actualmente en espera: no

â€"Datos de CA â€"

¿Está la configuración de CA en hardware?:sí

Interfaz de CA: GigabitEthernet36/2

ID del circuito de CA: 2

AC- VLAN interna: 0

AC- VLAN externa: 200

AC- ID de puerto MPLS: 0x1800000A

AC- ID de puerto: 31

Id. de AC-Mod: 36

AC- Es efp: sí

AC- Encap: Una etiqueta

CA- Ing RW Oper: ninguna

CA- Oper RW de salida: ninguna

AC- Ing RW TPID: 0

AC- Ing RW VLAN: 0

Indicador AC- Ing RW: 0x0

â€"Datos ATOMâ€"

Tipo de interconexión: Vlan

ID de Vlan solicitada por el par para el tipo 4 PW 4091

ID de puerto MPLS: 0x1800000B

Etiqueta SD habilitada: sí

Palabra de control habilitada: sí

â€"Imposición de datosâ€"

Etiqueta de VC remota: 19

Número de int. saliente: 9

Puerto BCM: 28

Id. de módulo BCM: 4

Objeto de salida de túnel: 100008

Id De Conmutación Por Error: 1

Objeto de egreso de túnel de failover: 100009

Puerto BCM de failover: 0

BCMModId de conmutación por error: 0

"Datos de disposición"

Etiqueta local: 18

IF núm.: 12

¿Es MSPW : No

" LADO DE LA IMPOSICIÓN "

No se encontró la entrada para VlanId 200 en la tabla VLAN_XLATE

SOURCE_VP[10]

dvp: 11

ING_DVP_TABLE[11]

nh_index: 411

ING_L3_NEXT_HOP[411]

vlan_id: 4095

port_num: 28

module_id: 4

caída: 0

EGR_L3_NEXT_HOP[411]

mac_da_profile_index: 1

vc_and_swap_index: 4099

intf_num: 22

dvp: 11

EGR_MAC_DA_PROFILE[1]

DA Mac: 1 80,C20,0 0

EGR_MPLS_VC_AND_SWAP_LABEL_TABLE[4099]
mpls_label(VC Label): 19

EGR_L3_INTF[22]
SA Mac: 405.3958.E0E1
MPLS_TUNNEL_INDEX: 4

EGR_IP_TUNNEL_MPLS[4]
(lsp) MPLS_LABEL0
(lsp) MPLS_LABEL1
(lsp) MPLS_LABEL2
(lsp) MPLS_LABEL3

â€” LADO DE DISPOSICIÓN â€”

MPLS_ENTRY[1592]
Etiqueta: 18
source_vp: 11
nh_index: 11

SOURCE_VP[11]
DVP: 10

ING_DVP_TABLE[10]
nh_index: 410

ING_L3_NEXT_HOP[410]
Número de puerto: 31
module_id: 36
caída: 0

EGR_L3_NEXT_HOP[410]
SD_TAG:VINTF_CTR_IDX: 134
SD_TAG:RESERVED_3: 0
SD_TAG:SD_TAG_DOT1P_MAPPING_PTR: 0
SD_TAG:NEW_PRI: 0
SD_TAG:NEW_CFI: 0

```
SD_TAG:SD_TAG_DOT1P_PRI_SELECT: 0
SD_TAG:RESERVED_2: 0
SD_TAG:SD_TAG_TPID_INDEX: 0
SD_TAG:SD_TAG_ACTION_IF_NOT_PRESENT: 0
SD_TAG:SD_TAG_ACTION_IF_PRESENT: 3
SD_TAG:HG_L3_OVERRIDE: 0
SD_TAG:HG_LEARN_OVERRIDE: 1
SD_TAG:HG_MC_DST_PORT_NUM: 0
SD_TAG:HG_MODIFY_ENABLE: 0
SD_TAG:DVP_IS_NETWORK_PORT: 0
SD_TAG:DVP: 10
SD_TAG:SD_TAG_VID: 0
TIPO_ENTRADA: 2
```

Error: no se ha encontrado la entrada en la tabla EGR_VLAN_XLATE.

```
EGR_VLAN_XLATE[-1]
```

soc_mem_read: índice no válido -1 para la memoria EGR_VLAN_XLATE

Los registros indican que el PW está enlazado y configurado en el hardware, con la VLAN y las etiquetas correctas, de acuerdo con lo que se vio antes.

Si algún punto de datos no coincide o falta, el problema está en el controlador, que no configuró y enlazó el PW en el hardware. Esto apunta a un defecto de software o hardware.

Si hasta ahora todo está bien, puede intentar hacer ping a la parte PW internamente usando el comando del IOS "**ping mpls pseudowire 202.202.202.202 12 reply mode control-channel**". Tenga en cuenta de nuevo que esto hace ping en la parte PW solo de un extremo del túnel al otro y no toca la parte AC del circuito.

```
10.88.130.201#ping mpls pseudowire 202.202.202.202 12 reply mode
control-channel
```

Envío de eco MPLS de 5 y 100 bytes a 202.202.202.202.

el tiempo de espera es de 2 segundos, el intervalo de envío es de 0 ms:

Códigos: '!' - correcto, 'Q' - solicitud no enviada, '.' - tiempo de espera,

'L' - interfaz de salida etiquetada, 'B' - interfaz de salida sin etiquetar,

'D' - Discordancia de mapa DS, 'F' - sin asignación FEC, 'f' -

Discordancia FEC,

'M' - solicitud incorrecta, 'm' - tlvs no compatibles, 'N' - entrada sin etiqueta,

'P' - no rx intf label port, 'p' - terminación prematura de LSP,

'R' - router de tránsito, 'I' - índice ascendente desconocido,

'l' - Etiqueta conmutada con cambio FEC, 'd' - consulte DMAP para el código de retorno,

'X' - código de retorno desconocido, 'x' - código de retorno 0

Ingrese escape sequence para abortar.

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Ahora compruebe las estadísticas sobre el PW como lo hemos hecho antes:

```
10.88.130.201#show mpls 12 vc 12 det | estadísticas de mendigar
```

Estadísticas de VC:

totales de paquetes de tránsito: **recibir 5, enviar 0**

totales de bytes de tránsito: recibir 650, enviar 0

caídas de paquetes de tránsito: recepción 0, error de secuencia 0, envío 0

Observe que el ping fue exitoso y que los 5 paquetes de eco de ping se registran como recibidos. Además, tenga en cuenta que los paquetes de solicitud de ping no se registran como enviados. Parece que los paquetes de solicitud/respuesta de eco son enviados por la CPU al flujo después del contador y, por lo tanto, no se registran.

Si los pings no funcionan, entonces deberíamos retroceder y depurar el túnel para asegurarnos de que esté operativo.

Si la parte PW todavía se ve bien, entonces céntrese en la parte AC en cada extremo. Esta es la parte difícil, ya que no hay mucho soporte de depuración para él, y la trayectoria de AC puede incluir varias tarjetas e interfaces como en el caso de Cisco CPT50.

Pero hay pocas cosas que se puedan comprobar.

Puede enviar un patrón desde un probador o hacer un ping desde el equipo del lado del cliente y observar los paquetes recibidos por la interfaz de cara al cliente en la caja CPT. Esto sería fácil de hacer para un PW basado en puerto, pero no para un PW basado en VLAN ya que la interfaz no muestra paquetes por VLAN. En cualquier caso, el comando "**show int ...**" para la interfaz de cara al cliente debe mostrar el aumento del recuento de paquetes al menos como una señal de que los paquetes ingresan correctamente y si no hay otros circuitos basados en VLAN activos.

Tenga en cuenta que estos paquetes que ingresan a través de la CA, se supone que deben ser etiquetados con MPLS y luego enviados a través de la PW al otro lado. Por lo tanto, deben mostrar en las estadísticas de la

parte PW como paquetes enviados. Así que búsquelos en el comando " **show mpls l2 vc 12 detail | beg statistics**"

```
10.88.130.201#show mpls l2 vc 12 detail | estadísticas de mendigar
```

Estadísticas de VC:

totales de paquetes de tránsito: recibir 0, enviar **232495**

totales de bytes de tránsito: recibir 0, enviar **356647330**

caídas de paquetes de tránsito: recepción 0, error de secuencia 0, envío 0

Y deben mostrar como paquetes "reciben" en el mismo comando en el otro extremo. Por lo tanto, los paquetes PW enviados en este extremo y los paquetes PW recibidos en el extremo lejano deben coincidir con el número de paquetes enviados desde el equipo cliente. Uso del mismo comando " **show mpls l2 vc 12 detail | beg statistics**" en el otro extremo muestra:

```
10.88.130.202#show mpls l2 vc 12 detail | beg statis
```

Estadísticas de VC:

totales de paquetes de tránsito: recibir **23.2495**, enviar 0

totales de bytes de tránsito: reciba **356.647.330**, envíe 0

caídas de paquetes de tránsito: recepción 0, error de secuencia 0, envío 0

Puede ver la coincidencia en los paquetes entre el envío en un extremo y la recepción en el otro.

En caso de que necesite borrar los contadores MPLS, utilice el comando "**clear mpls counters**".

Otra manera de verificar las estadísticas es utilizar la función SPAN para replicar el tráfico EFP entrante en un puerto de repuesto en el nodo CPT y luego buscar las estadísticas en este puerto para monitorear los paquetes recibidos de la interfaz del cliente.

Y, por último, puede ejecutar comandos de shell BCM en las diferentes tarjetas de línea y fabric para realizar un seguimiento interno de los paquetes, pero eso está fuera del alcance de este artículo.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).