Concetti e risoluzione dei problemi relativi a pseudofili

Sommario

Introduzione

Gli pseudofili (PW) vengono utilizzati per fornire servizi end-to-end su una rete MPLS. Sono gli elementi di base che possono fornire un servizio point-to-point e un servizio multipunto come VPLS, che è praticamente una mesh di PW utilizzata per creare il dominio bridge attraverso cui passano i pacchetti.

Modificato da: Kumar Sridhar

Prerequisiti

I lettori di questo documento devono essere a conoscenza di quanto segue:

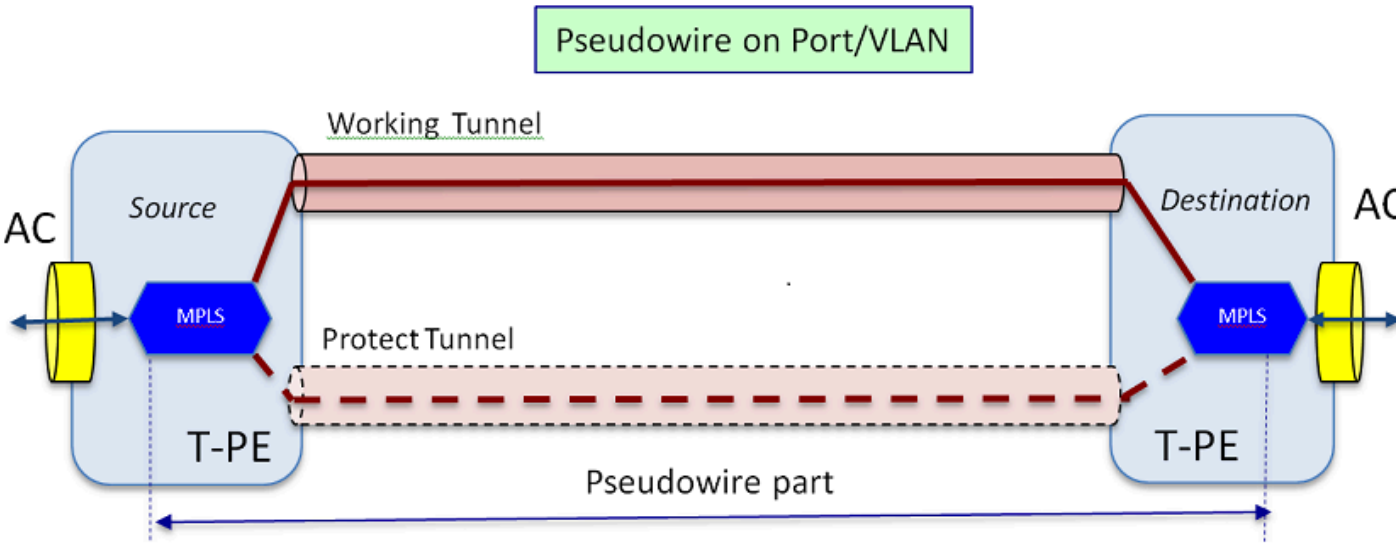
- Nozioni base sul tunneling MPLS

Componenti usati

Le informazioni fornite in questo documento si basano sulla famiglia di prodotti Cisco® Carrier Packet Transport (CPT) e in particolare sulla CPT50.

Concetto Di Pseudowire

L'aspetto concettuale degli pseudofili è il seguente:



Il servizio end-to-end è composto da 2 parti. La parte Attachment Circuit (AC) e la parte Pseudowire. L'intero circuito end-to-end è ancora indicato come Pseudowire in Cisco Transport Controller (CTC), ma bisogna tenere presente la distinzione tra due parti mostrata qui per la risoluzione dei problemi che segue.

È inoltre necessario che sia stato creato un tunnel per ospitare il servizio Pseudowire configurato in precedenza. Il tunnel potrebbe essere protetto (come mostrato di seguito) o non protetto.

La parte Pseudowire inizia e si ferma praticamente ai punti finali del tunnel (se si esclude il blocco di incapsulamento MPLS mostrato di seguito).

La parte AC inizia dal punto finale del tunnel fino all'interfaccia verso il client, dove è definito il punto di flusso Ethernet (EFP), per identificare il traffico client specifico che viene trasportato attraverso questo pseudofilo. Ci sono 2 ACL, uno per ogni estremità.

L'ACL trasmette il traffico del cliente nella sua forma nativa, ossia frame Ethernet con o senza tag VLAN a seconda che si stia creando uno Pseudowire basato su VLAN o uno Pseudowire basato su Ethernet (casella AC Type nella procedura guidata per la creazione di PW). Vengono quindi aggiunte le etichette MPLS per il servizio PW specifico e per il tunnel su cui sta viaggiando. I pacchetti vengono quindi inviati attraverso la parte Pseudowire del circuito nel cloud MPLS. Questo processo è denominato Label Imposition nella terminologia MPLS. All'estremità remota si verifica il processo inverso, ossia le etichette vengono rimosse o si verifica la disposizione dell'etichetta, e i pacchetti, che ora sono di nuovo ai frame Ethernet nativi, vengono quindi consegnati all'altra estremità attraverso la parte CA all'estremità remota del circuito Pseudowire.

Risoluzione dei problemi di uno pseudofilo

Affinché il servizio Pseudowire funzioni in modo completo, è necessario che la parte Pseudowire e le due parti CA lavorino insieme. La risoluzione dei problemi del circuito coinvolge ciascuna parte, dove ciascuna parte AC-PW-AC viene sottoposta a debug separatamente per identificare la posizione del problema.

Nella seguente discussione sulla risoluzione dei problemi, si presume che il PW sia stato

configurato correttamente e che tutti i problemi relativi al layer 1 o al layer fisico siano già stati sottoposti a debug ed esclusi.

In primo luogo, il debug della parte PW è semplice. Iniziare identificando il circuito con il comando "show mpls l2 vc" eseguito nella finestra di IOS su un nodo finale. Prendere nota del VCID (Virtual Circuit Identifier) e dell'indirizzo del nodo di destinazione della connessione.

```
10.88.130.201#show mpls l2 vc

Interfaccia locale Circuito locale Indirizzo di destinazione Stato ID
VC

— — — —

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
```

In questo caso, il PW di interesse è il primo PW configurato come VLAN 200 basato sull'interfaccia Gi36/2. Verificare che lo stato dell'interfaccia sia ATTIVO.

show mpls l2 vc 12 detail fornisce molte informazioni sul PW. Di seguito vengono evidenziati i campi importanti, quali l'ID del tunnel, l'ID del nodo remoto, lo stack di etichette, il numero PWID e le statistiche.

```
10.88.130.201#show mpls l2 vc 12 detail

Interfaccia locale: Gi36/2 up, protocollo di linea up, Eth VLAN 200 up

  Indirizzo di destinazione: 202.202.202.202, ID VC: 12, stato VC:
attivo

    Interfaccia di output: Tp102, stack di etichette imposto {16/19}

    Percorso preferito: Tunnel-tp102, attivo

    Percorso predefinito: pronto

    Hop successivo: point2point

  Ora creazione: 00:32:52, ora ultima modifica stato: 00:05:42

  Protocollo di segnalazione: manuale

    Supporto TLV stato (locale/remoto) : abilitato/N/D

      Controllo route LDP : abilitato

      Computer di stato/etichetta : stabilito, LruRu
```

```
      Ricevuto stato ultimo dataplane locale: nessun errore
      Ricevuto ultimo stato piano dati BFD: Non inviato
      Ricevuto ultimo stato del circuito SSS locale: nessun errore
      Stato ultimo circuito SSS locale inviato: nessun errore
      Ultimo stato TLV LDP locale inviato: nessun errore
      Ultimo stato TLV LDP remoto ricevuto: nessun errore
      Ultimo stato ADJ LDP remoto ricevuto: nessun errore
    Etichette MPLS VC: 18 locali, 19 remote
    PWID: 7
    ID gruppo: locale 0, remoto 0
    MTU: local 1500, remote 1500 <— I valori local e remote devono
corrispondere
  Sequenziamento: ricezione disabilitata, invio disabilitato
  Parola controllo: On
  Descrittore SSO: 202.202.202.202/12, etichetta locale: 18
    ID segmento/switch SSM: 20513/12320 (utilizzato), PWID: 7
  Statistiche VC:
    totale pacchetti in transito: ricezione 10, invio 0
    totali byte transito: ricezione 1320, invio 0
    pacchetti in transito scartati: ricezione 0, errore seq 0, invio 0
```

Se il PW è inattivo, verificare che il tunnel (qui tunnel 102) sia in buone condizioni e, in caso contrario, risolvere il problema del tunnel. La risoluzione dei problemi del tunnel esula dall'ambito di questo articolo.

Accertarsi che le etichette nello stack siano definite come indicato sopra, cioè che non siano vuote. Verificare che il PW sia programmato nell'hardware eseguendo il comando show platform mpls pseudowire pwid con il numero PWID appropriato.

```
10.88.130.201#show platform mpls pseudowire pwid 7
ID PW: 7
Chiave VC PW: 7
```

Tasto AC PW: 786434

Ricezione binding PW in hardware: sì

Impostazione PW in hardware: sì

Attualmente in standby: no

—

—dati AC —

Impostazione CA in HW:yes

Interfaccia AC: Gigabit Ethernet 36/2

ID circuito CA: 2

VLAN interna CA: 0

VLAN esterna CA: 200

AC- ID porta MPLS: 0x1800000A

AC- Port ID: 31

AC- Mod Id: 36

AC- È efp: sì

AC- Encap: etichetta singola

AC- Ing RW Oper: nessuna

AC- Operazione RW in uscita: nessuna

AC- Ing RW TIPID: 0

VLAN AC- Ing RW: 0

Indicatore AC- Ing RW: 0x0

—

—Dati ATOM—

Tipo di interworking: VLAN

ID Vlan richiesto dal peer per tipo 4 PW 4091

ID porta MPLS: 0x1800000B

Tag SD abilitato : yes

Parola controllo abilitata : yes

—

—Dati sull'imposizione—

—

Etichetta VC remota: 19

Numero int in uscita: 9

Porta BCM: 28

ID mod BCM: 4

Oggetto tunnel in uscita : 100008

ID failover: 1

Oggetto uscita tunnel di failover: 100009

Porta BCM di failover: 0

BCMModId di failover: 0

—

—Dati di smaltimento—

—

Etichetta locale: 18

IF Num: 12

È MSPW : No

—

— IMPOSIZIONE —

Impossibile trovare la voce per VlanId 200 nella tabella VLAN_XLATE

SOURCE_VP[10]

dvp: 1

ING_DVP_TABLE[11]

```
                    nh_index: 411
            ING_L3_NEXT_HOP[411]
                    id_vlan: 4095
                    num_porta: 28
                    module_id: 4
                    rilascio: 0
            EGR_L3_NEXT_HOP[411]
                    mac_da_profile_index: 1
                    vc_and_swap_index: 4099
                    num_intf: 22
                    dvp: 1
            EGR_MAC_DA_PROFILE[1]
                    DA Mac: 1 80,C20,0 0
            EGR_MPLS_VC_AND_SWAP_LABEL_TABLE[4099]
                    mpls_label(Etichetta VC): 19
            EGR_L3_INTF[22]
                    SA Mac: 4055.3958.E0E1
                    MPLS_TUNNEL_INDEX: 4
            EGR_IP_TUNNEL_MPLS[4]
                    (lsp) MPLS_LABEL0
                    (lsp) MPLS_LABEL1
                    (lsp) MPLS_LABEL2
                    (lsp) MPLS_LABEL3
— LATO DELLA DISPOSIZIONE —
            MPLS_ENTRY[1592]
                    Etichetta: 18
```

```
                source_vp: 11
                nh_index: 11
SOURCE_VP[11]
                DVP: 10
ING_DVP_TABLE[10]
                nh_index: 410
ING_L3_NEXT_HOP[410]
                Num_porta: 31
                module_id: 36
                rilascio: 0
EGR_L3_NEXT_HOP[410]
                SD_TAG:VINTF_CTR_IDX: 134
                SD_TAG:RISERVATO_3: 0
                SD_TAG:SD_TAG_DOT1P_MAPPING_PTR: 0
                SD_TAG:NUOVO_PRI: 0
                SD_TAG:NUOVO_CFI: 0
                SD_TAG:SD_TAG_DOT1P_PRI_SELECT: 0
                SD_TAG:RISERVATO_2: 0
                SD_TAG:SD_TAG_TIPID_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_VOCE: 2

Errore: voce non trovata nella tabella EGR_VLAN_XLATE.

                EGR_VLAN_XLATE[-1]

soc_mem_read: indice -1 non valido per la memoria EGR_VLAN_XLATE
```

I registri indicano che il firmware PW è associato e configurato nell'hardware, con le etichette e la VLAN corrette, in accordo con quanto osservato in precedenza.

Se uno dei punti dati non corrisponde o è mancante, il problema si verifica nel driver, che non è stato configurato e associato il PW nell'hardware. Ciò fa riferimento a un problema software o hardware.

Se tutto va bene, è possibile provare a eseguire il ping della parte PW internamente usando il comando IOS "ping mpls pseudowire 202.202.202.202 12 reply mode control-channel". Notare ancora che questo effettua il ping della parte PW solo da un punto terminale del tunnel all'altro e non tocca la parte CA del circuito.

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

Invio di 5 Echo MPLS da 100 byte a 202.202.202.202,

     il timeout è di 2 secondi, l'intervallo di invio è di 0 msec:

Codici: '!' - operazione riuscita, 'Q' - richiesta non inviata, '.' -
timeout,

  'L' - etichetta dell'interfaccia di uscita, 'B' - etichetta
dell'interfaccia di uscita,

  'D' - Mancata corrispondenza mappa DS, 'F' - Nessuna corrispondenza
FEC, 'f' - Mancata corrispondenza FEC,

  'M' - richiesta non valida, 'm' - tlvs non supportato, 'N' - nessuna
voce etichetta,

  'P' - no rx intf label port, 'p' - interruzione prematura di LSP,

  'R' - router di transito, 'I' - indice a monte sconosciuto,

  'l' - Etichetta commutata con modifica FEC, 'd' - vedere DMAP per il
codice restituito,

  'X' - codice restituito sconosciuto, 'x' - codice restituito 0
```

```
Digitare la sequenza di escape da interrompere.

!!!!!

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

Ora controlla le statistiche sul PW come abbiamo fatto prima:

10.88.130.201#show mpls l2 vc 12 det | statistiche di elemosina

  Statistiche VC:

    totale pacchetti in transito: ricezione 5, invio 0

    totali byte transito: ricezione 650, invio 0

    pacchetti in transito scartati: ricezione 0, errore seq 0, invio 0
```

Il ping è riuscito e i 5 pacchetti ping echo vengono registrati come ricevuti. Inoltre, i pacchetti di richiesta ping non vengono registrati come inviati. Sembra che i pacchetti di richiesta/risposta echo vengano inviati dalla CPU al flusso dopo il contatore, e quindi non vengono registrati.

Se i ping non funzionano, è necessario tornare indietro ed eseguire il debug del tunnel per verificare che sia operativo.

Se la parte PW è ancora ben visualizzata, attivare la parte AC su ciascuna estremità. Questa è la parte difficile, in quanto non supporta molto il debug e il percorso AC può includere diverse schede e interfacce, come nel caso di Cisco CPT50.

Ma ci sono poche cose che possono essere controllate.

È possibile inviare uno schema da un tester o eseguire un ping dall'apparecchiatura sul lato client e controllare i pacchetti ricevuti dall'interfaccia del client sul box CPT. Questa operazione è semplice per un PW basato su porta, ma non per un PW basato su VLAN, poiché l'interfaccia non visualizza i pacchetti per VLAN. In ogni caso, il comando "show int ..." per l'interfaccia rivolta verso il client deve indicare che il numero di pacchetti deve aumentare almeno per indicare che i pacchetti stanno entrando correttamente e che nessun altro circuito VLAN è attivo.

Tenete presente che questi pacchetti che entrano attraverso l'alimentazione CA devono avere l'etichetta MPLS e quindi devono essere inviati attraverso il PW all'altro lato. Pertanto, essi dovrebbero apparire nelle statistiche della parte PW come pacchetti inviati. Quindi cercarle nel comando" show mpls l2 vc 12 detail | statistiche"

```
10.88.130.201#show mpls l2 vc 12 detail | statistiche di base

  Statistiche VC:

    totali pacchetti in transito: ricezione 0, invio 232495

    totali byte transito: ricezione 0, invio 356647330
```

```
    pacchetti in transito scartati: ricezione 0, errore seq 0, invio 0
```

E devono mostrare come pacchetti "ricevuti" nello stesso comando sull'estremità remota. Pertanto, i pacchetti PW di invio su questa estremità e i pacchetti PW di ricezione sull'estremità remota devono corrispondere al numero di pacchetti inviati dall'apparecchiatura client. Utilizzando lo stesso comando" show mpls l2 vc 12 detail | beg statistics" mostra:

```
10.88.130.202#show mpls l2 vc 12 detail | imitare

  Statistiche VC:

    totale pacchetti in transito: ricezione 232495, invio 0

    totali byte transito: ricezione 35647330, invio 0

    pacchetti in transito scartati: ricezione 0, errore seq 0, invio 0
```

Si può vedere la corrispondenza nei pacchetti tra l'invio da un lato e la ricezione dall'altro.

Per cancellare i contatori MPLS, usare il comando "clear mpls counters".

Un altro modo per verificare le statistiche consiste nell'utilizzare la funzione SPAN per replicare il traffico EFP in entrata su una porta di riserva sul nodo CPT e quindi cercare le statistiche su questa porta per monitorare i pacchetti ricevuti dall'interfaccia cliente.

Infine, è possibile eseguire i comandi della shell BCM su diversi fabric e schede di linea per tenere traccia dei pacchetti internamente, ma questo esula dall'ambito di questo articolo.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).