Comprendre MPLS L2VPN Pseudowire

Table des matières

Introduction

Ce document décrit les pseudofils du réseau privé virtuel de couche 2 (L2VPN) basés sur la commutation multiprotocole par étiquette (MPLS, pour Multiprotocol Label Switching).

Informations générales

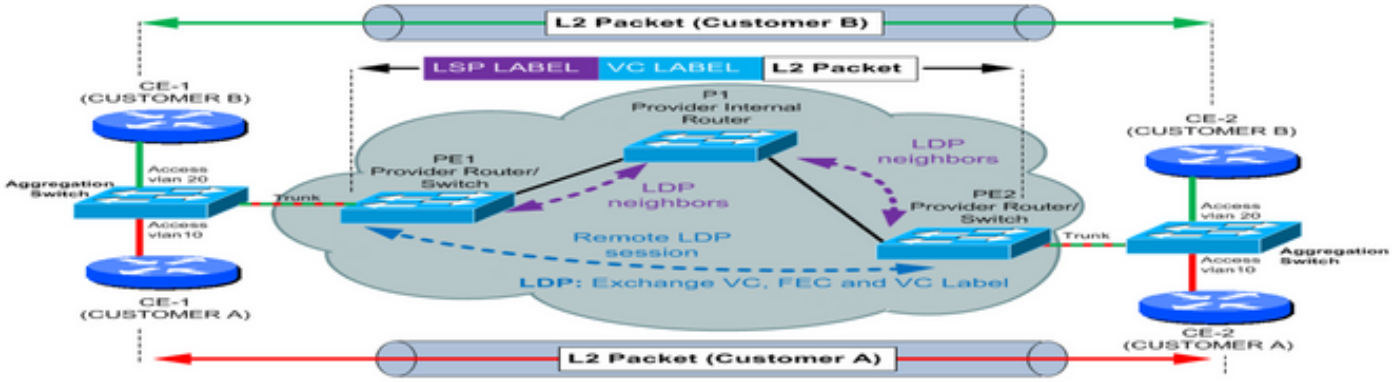
La signalisation du pseudo-fil et l'analyse de paquets dans Cisco IOS®, IOS®-XE afin d'illustrer le comportement est traitée.

Présentation de L2VPN

Le transport de couche 2 (L2) sur MPLS et IP existe déjà pour les circuits de connexion similaires, tels qu'Ethernet-vers-Ethernet, PPP-vers-PPP, HDLC (High-Level Data Link Control), etc

Les L2VPN utilisent des services L2 sur MPLS afin de construire une topologie de connexions point à point qui connectent vos sites finaux dans un VPN. Ces L2VPN offrent une alternative aux réseaux privés qui ont été provisionnés au moyen de lignes louées dédiées ou au moyen de circuits virtuels L2 qui utilisent ATM ou Frame Relay. Le service fourni avec ces L2VPN est appelé Virtual Private Wire Service (VPWS).

- Les L2VPN sont construits avec la technologie Pseudowire (PW).
- Les PW fournissent un format intermédiaire commun pour transporter plusieurs types de services réseau sur un réseau à commutation de paquets (PSN), un réseau qui transfère les paquets : IPv4, IPv6, MPLS, Ethernet.
- La technologie PW permet le transport de type à type et l'interfonctionnement (IW).
- Les trames reçues au niveau du routeur PE sur le CA sont encapsulées et envoyées via le PSW au routeur PE distant.
- Le routeur PE de sortie reçoit le paquet du PSW et supprime son encapsulation.
- Le PE de sortie extrait et transfère la trame au CA.

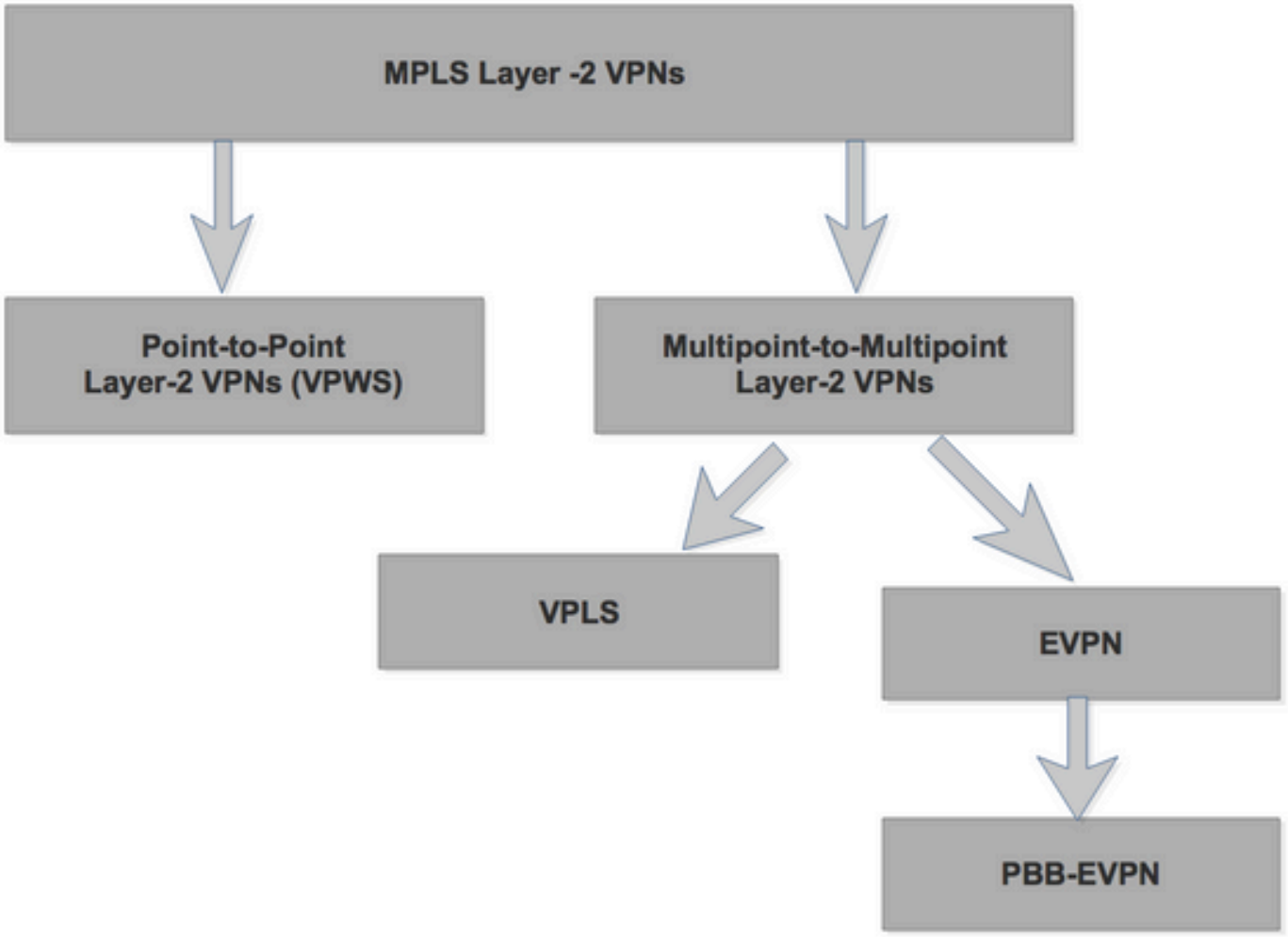


Pourquoi L2VPN est-il nécessaire ?

- Permet au SP de disposer d'une infrastructure unique pour les services IP et hérités.
- Migrer les services ATM et Frame Relay existants vers le coeur MPLS/IP sans interrompre les services existants.
- La mise en service de nouveaux services L2VPN est incrémentielle (pas de zéro) dans le coeur MPLS/IP existant.
- Économies de capital et d'exploitation du réseau IP/MPLS convergent.
- SP fournit de nouveaux services point-2-point ou point-2-multipoint. Vous pouvez disposer de leurs propres politiques de routage, de qualité de service, de mécanismes de sécurité, etc.

Modèles VPN L2 MPLS

Options technologiques



1. Services VPWS

· Point à point · Appelé Pseudo-fils (PW)

2. Services VPLS

· Multipoint

3. EVPN

· La gamme xEVPN présente des solutions de nouvelle génération pour les services Ethernet

a. Plan de contrôle BGP pour la distribution et l'apprentissage MAC et de segments Ethernet sur le coeur MPLS

b. Mêmes principes et expérience opérationnelle des VPN IP

· Pas d'utilisation de pseudo-fils

a. Utilise des tunnels MP2P pour la monodiffusion

b. Livraison de trames multidestinations via la réplication en entrée (via les tunnels MP2P) ou LSM

· Solutions multifournisseurs dans le cadre de la normalisation IETF

4. PBB-EVPN

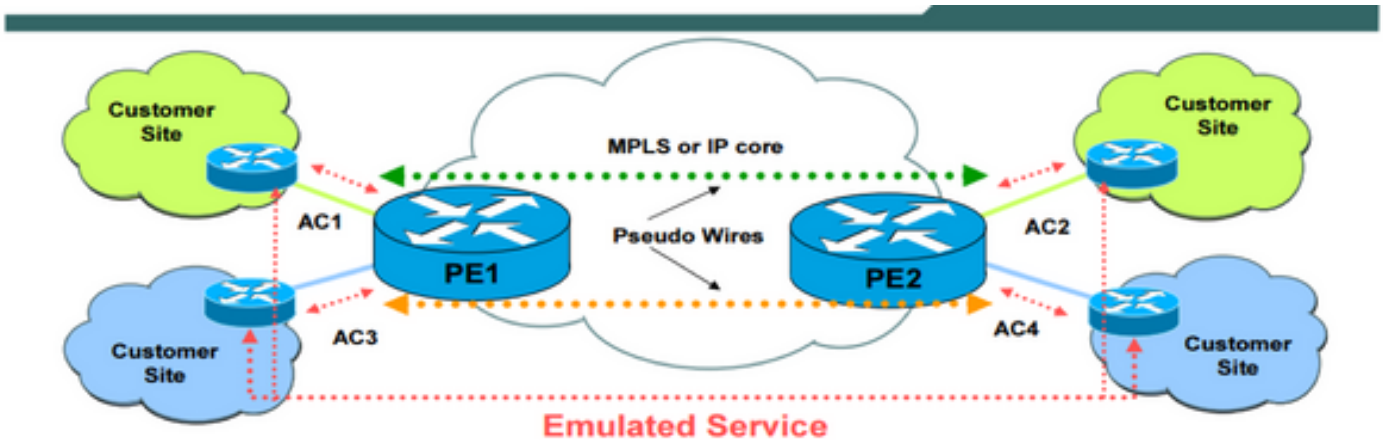
· Combine les outils d'évolutivité de PBB (alias MAC-in-MAC) avec l'apprentissage MAC basé sur BGP à partir d'EVPN

EVPN et Provider Backbone Bridging EVPN (PBB-EVPN) sont des solutions L2VPN de nouvelle génération basées sur le plan de contrôle BGP pour la distribution/l'apprentissage MAC sur le coeur, conçues pour répondre à ces exigences :

- Redondance par flux et équilibrage de charge
- Provisionnement et fonctionnement simplifiés
- Acheminement optimal
- Convergence rapide
- Évolutivité des adresses MAC

VPWS - Modèle de référence de pseudo-fil

1. PW est une connexion entre deux périphériques PE qui connecte deux adaptateurs secteur, qui transportent des trames L2.
2. Any Transport Over MPLS (AToM) est la mise en oeuvre par Cisco de VPWS pour les réseaux IP/MPLS.
3. Le circuit d'attache (CA) est le circuit physique ou virtuel qui attache un CE à un PE. Il peut s'agir d'un circuit ATM, Frame Relay, HDLC, PPP, etc.
4. Votre équipement de périphérie (CE) perçoit un PW comme une liaison ou un circuit non partagé.



L'activateur VPN de couche 2 : le pseudo-fil

Les L2VPN sont construits avec la technologie Pseudowire (PW)

- Les PW fournissent un format intermédiaire commun pour transporter plusieurs types de services réseau sur un réseau à commutation de paquets (PSN), un réseau qui transfère les paquets : IPv4, IPv6, MPLS, Ethernet.

- La technologie PW permet le transport de type à type et l'interfonctionnement (IW).
- Les trames reçues au niveau du routeur PE sur le CA sont encapsulées et envoyées via le PSW au routeur PE distant.
- Le routeur PE de sortie reçoit le paquet du Pseudowire et a supprimé son encapsulation.
- Le PE de sortie extrait et transfère la trame au CA.

Architecture AToM

- Dans un réseau AToM, tous les routeurs du SP exécutent MPLS et le routeur PE dispose d’un CA vers le routeur CE.
- Dans le cas d'AToM, le tunnel PSN n'est rien d'autre qu'un LSP à chemin commuté par étiquette entre les deux routeurs PE.
- En tant que tel, l'étiquette associée à ce LSP est appelée étiquette de tunnel dans le contexte de l'AToM.
- Tout d’abord, les signaux LDP saut par saut entre les PE.
- Deuxièmement, le LSP peut être un tunnel TE MPLS que le RSVP signale avec les extensions nécessaires pour TE.
- Avec cette étiquette de tunnel, vous pouvez identifier à quel tunnel PSN la trame transportée appartient.
- Cette étiquette de tunnel obtient également les trames du PE local ou d'entrée vers le PE distant ou de sortie à travers le backbone MPLS.
- Pour multiplexer plusieurs Pseudowire sur un tunnel PSN, le routeur PE utilise une autre étiquette pour identifier le Pseudowire.
- Cette étiquette est appelée étiquette VC ou PW car elle identifie le VC ou PW dans lequel la trame est multiplexée.

Transport L2 sur MPLS

Control Connection

- Targeted LDP session / BGP session / Static
  - Used for VC-label negotiation, withdrawal, error notification

The "emulated circuit" has three (3) layers of encapsulation

Tunnelling Component

- Tunnel header (Tunnel Label)
  - To get PDU from ingress to egress PE
  - MPLS LSP derived through static configuration (MPLS-TP) or dynamic (LDP or RSVP-TE)

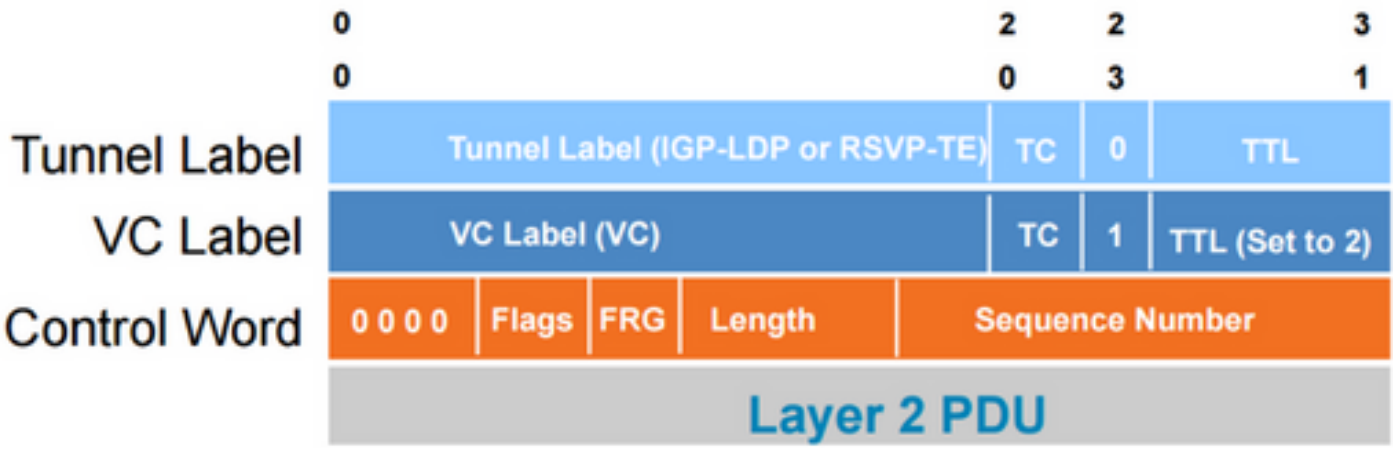
Demultiplexing Component

- Demultiplexer field (VC Label)
  - To identify individual circuits within a tunnel
  - Could be an MPLS label, L2TPv3 header, GRE key, etc.

Layer 2 Encapsulation

- Emulated VC encapsulation (Control Word)
  - Information on enclosed Layer 2 PDU
  - Implemented as a 32-bit control word

Encapsulation du trafic VPWS



1. Encapsulation à trois niveaux
2. Paquets commutés entre des PE utilisant l'étiquette de tunnel
3. L'étiquette VC identifie PW
4. Étiquette de circuit virtuel signalée entre PE
5. Le mot de contrôle facultatif (CW) transporte les bits de contrôle de couche 2 et active le séquencement

Control Word	
Encap.	Required
ATM N:1 Cell Relay	No
ATM AAL5	Yes
Ethernet	No
Frame Relay	Yes
HDLC	No
PPP	No
SAToP	Yes
CESoPSN	Yes

Signalisation du Pseudofil

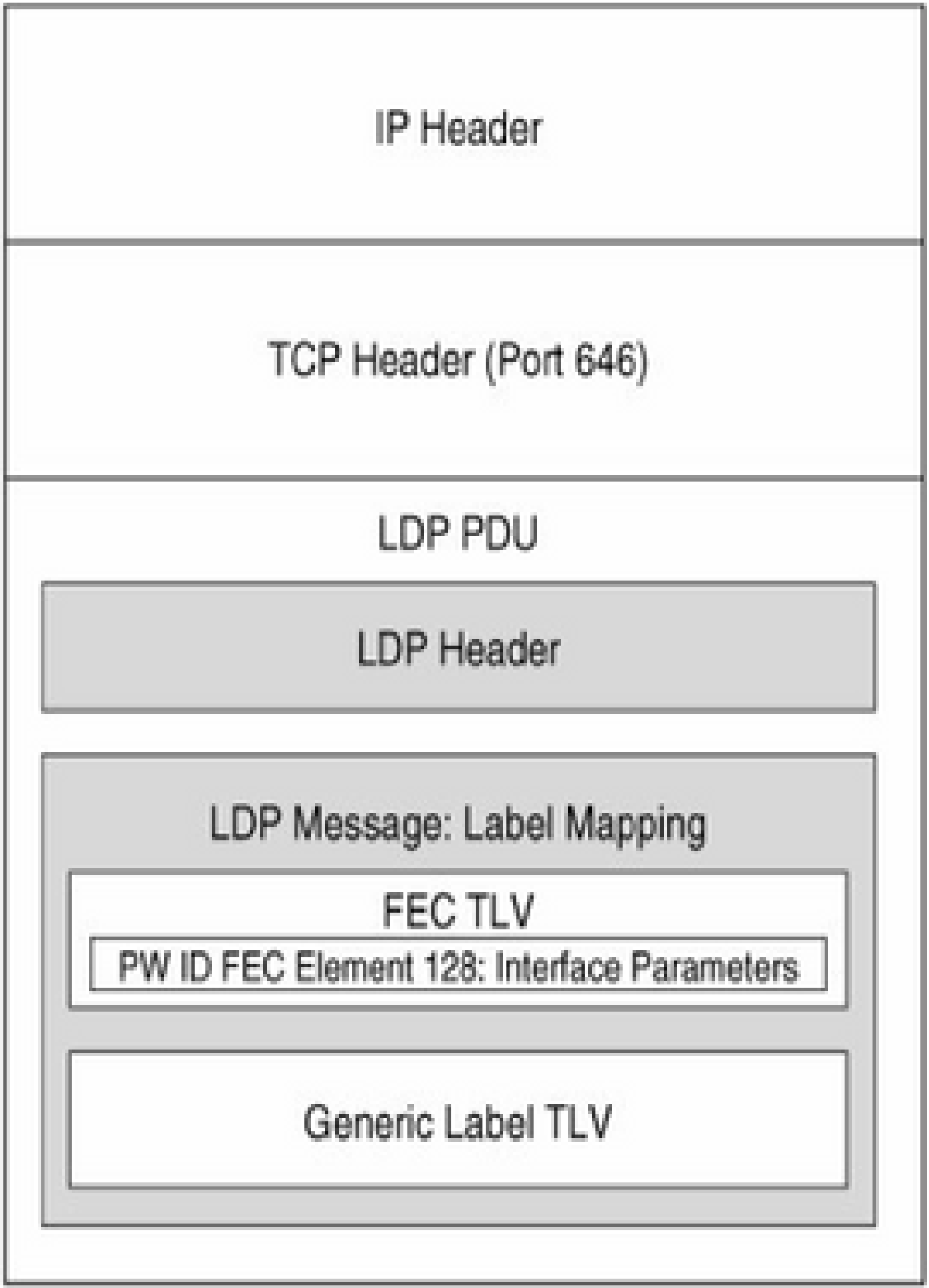
- Une session TLDP entre le routeur PE signale le Pseudowire.
- Une session T-LDP entre les routeurs PE sert à annoncer l'étiquette VC associée au PSW.
- Cette étiquette est annoncée dans un message de mappage d'étiquette qui utilise le mode d'annonce d'étiquette non sollicitée en aval.
- Étiquette de circuit virtuel annoncée par le PE de sortie au PE d'entrée pour le CA sur la

session TLDP. # Étiquette VC par TLDP
- Libellé de tunnel annoncé pour le routeur PE de sortie vers le PE d’entrée par LDP. # Libellé de tunnel par LDP

Notez que le PE de sortie annonce l'étiquette 3, qui indique que PHP est utilisé.

Le message de mappage d’étiquette qui est annoncé sur la session TLDP contient une certaine valeur TLV :

LDP Label Mapping message:



Le routeur PE d’entrée commence par pousser l’étiquette VC sur la trame. Et puis pousse l'étiquette du tunnel.

Étape 2. L'étiquette de tunnel est l'étiquette associée au préfixe IGP qui identifie le PE distant. Le préfixe est un bit spécifié dans la configuration AToM.

Étape 3. Le paquet MPLS est ensuite transféré conformément à l'étiquette de tunnel, saut par saut jusqu'à ce que le paquet atteigne le PE2 de sortie.

Étape 4. Lorsque le paquet atteint le PE de sortie, l'étiquette du tunnel a déjà été supprimée. Ceci est dû au comportement de PHP entre le dernier routeur P et le PE de sortie.

Étape 5.

Le PE de sortie recherche alors le circuit virtuel étiquette de la base de données de transmission dévêtir hors de la circuit virtuel et transfère la trame sur le bloc d'alimentation approprié.

Signalisation de l'état de PW

Une fois que les routeurs PE ont configuré le pseudo-fil, le PE peut signaler l'état du pseudo-fil au PE distant. Il existe deux méthodes :

1. Retrait de l'étiquette (plus de 2)

- Un routeur PE peut retirer le mappage d'étiquette soit en envoyant le message de retrait d'étiquette, soit en envoyant les messages de libération du mappage d'étiquette.
- Si le CA est en panne, le routeur PE le signale en envoyant un message de retrait d'étiquette au PE distant
- Si une interface physique tombe en panne, le message de retrait d'étiquette contient l'ID de groupe pour signaler que tout le courant alternatif de l'interface est en panne

2. TLV d'état PW

- Le TLV d'état de PW suit le TLV de mappage d'étiquette LDP lorsque le pseudo-fil est isolé. Cela indique que le routeur PE souhaite utiliser la deuxième méthode.
- Si l'autre routeur PE ne prend pas en charge la méthode TLV d'état de l'équipement physique, les deux routeurs PE reviennent à la méthode de retrait d'étiquette.
- Une fois le pseudo-fil isolé, le TLV d'état de l'onde entretenue est transporté dans un message de notification LDP. La valeur TLV de l'état du PW contient le champ de code d'état 32 bits.

Configuration AToM de base

Étape 1. Sélectionnez le type d’encapsulation.

Étape 2. Activez la spécification de la commande connect sur l'interface CE.

xconnect peer-router-id encapsulation vcid mpls

Peer-router-id : ID de routeur LDP pour le routeur PE distant.

VCID : identifiant que vous avez attribué au PW.

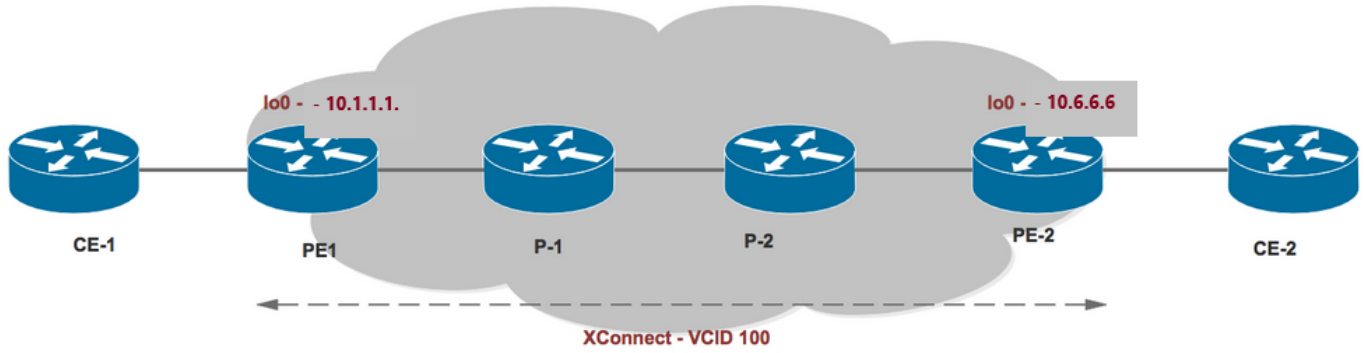
Étape 3. Dès que xconnect est configuré dans le routeur PE, la session LDP ciblée est établie entre le routeur PE.

Analyse des paquets pseudo-filaires

Lancons une requête ping Pseudowire de PE en entrée vers PE en sortie.

Paquets MPLS de requête et de réponse d'écho envoyés sur un pseudo-fil point à point.

Topologie



Envoyez une requête ping de PE1 vers PE2 :

```
R1#ping mpls pseudowire 10.6.6.6 100

Sending 5, 100-byte MPLS Echos to 10.6.6.6,

     timeout is 2 seconds, send interval is 0 msec:

Type escape sequence to abort.

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 48/61/80 ms
```

Observations formulées :

1. Demande ECHO :

Porte 2 étiquettes - VPN et transport

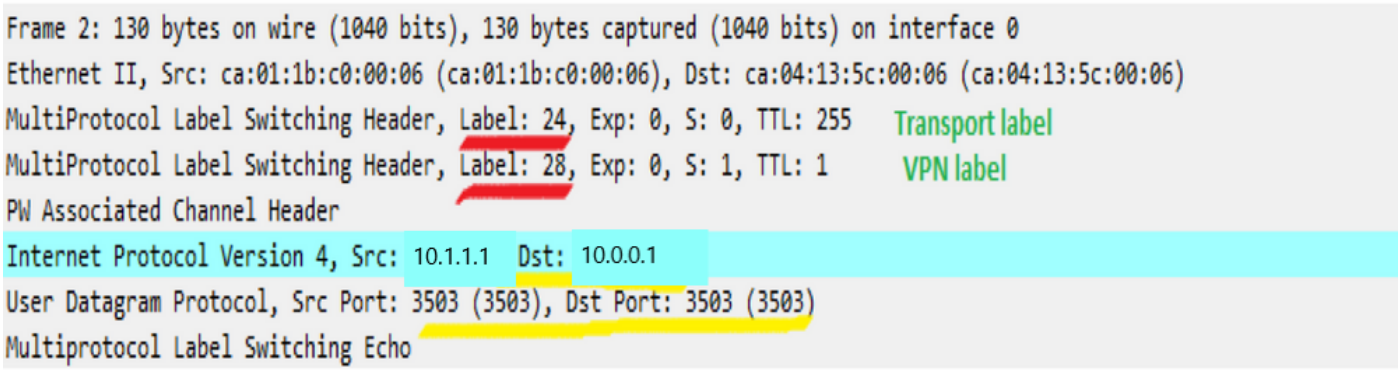
Envoyé en tant que paquet étiqueté portant l'étiquette PW. Il peut être basculé par étiquette (avec étiquette de transport)

ÉTIQUETTES : 2
SRC IP : LOOPBACK IP (UTILISÉ DANS LE VOISINAGE LDP CIBLÉ)
DST IP : 127.0.0.1
TYPE L4 : UDP
PORT SRC : 3503
PORT DST : 3505
OCTET TOS : DÉSACTIVÉ
EXP MPLS : DÉSACTIVÉ
BIT DF : ACTIVÉ

Le champ IPv4 OPTIONS est en cours d'utilisation : CHAMP ROUTER ALERT OPTIONS (Punt to CPU)

UDP PAYLOAD peut être MPLS LABEL SWITCHING ECHO REQUEST

Aperçu:



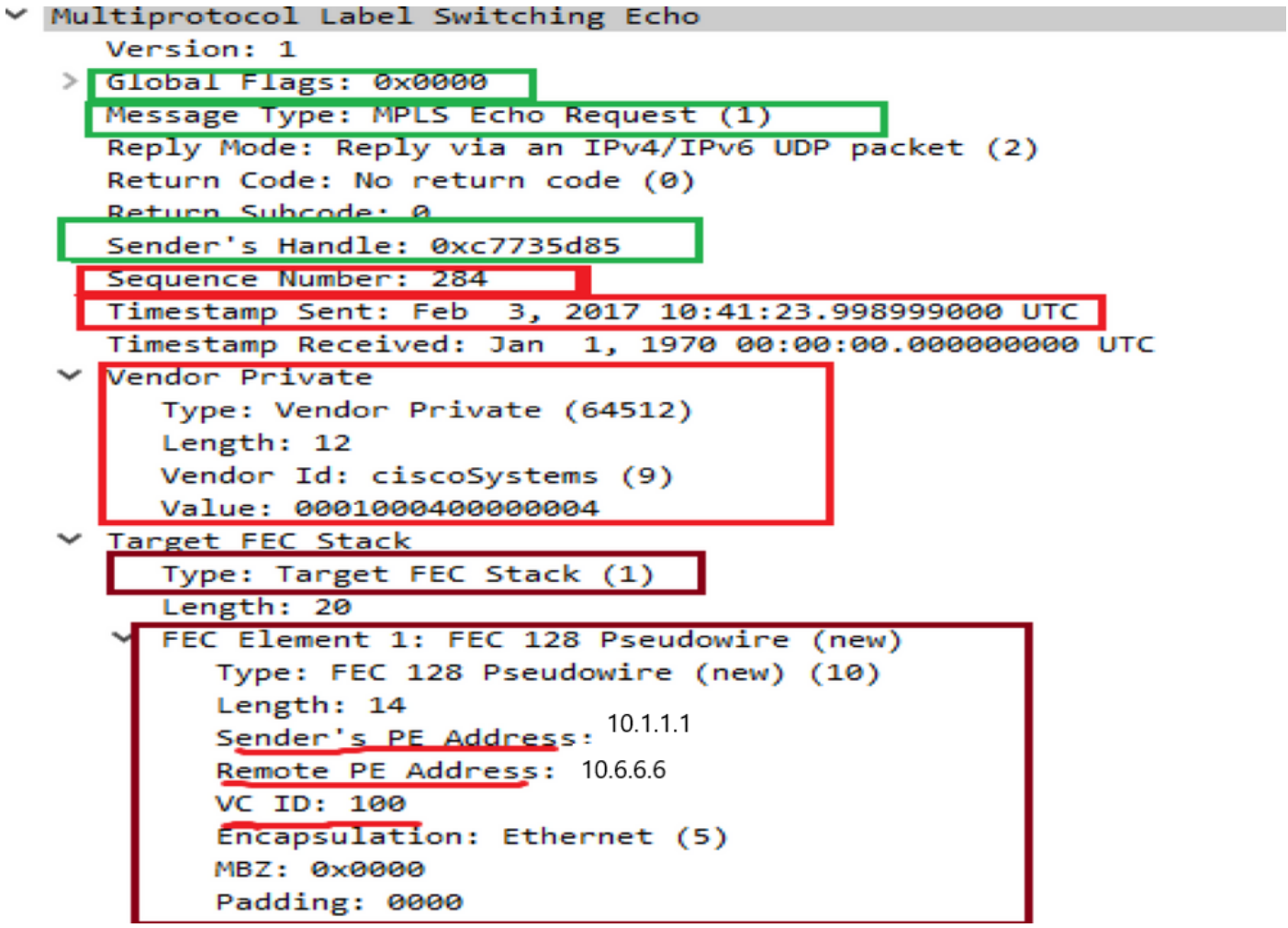
Couche 2/Étiquettes :

```
> Frame 4: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface 0
v Ethernet II, Src: ca:01:1b:c0:00:06 (ca:01:1b:c0:00:06), Dst: ca:04:13:5c:00:06 (ca:04:13:5c:00:06)
  > Destination: ca:04:13:5c:00:06 (ca:04:13:5c:00:06)
  > Source: ca:01:1b:c0:00:06 (ca:01:1b:c0:00:06)
    Type: MPLS label switched packet (0x8847)
v MultiProtocol Label Switching Header, Label: 24, Exp: 0, S: 0, TTL: 255
    0000 0000 0000 0001 1000 .... .... .... = MPLS Label: 24
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...0 .... .... = MPLS Bottom Of Label Stack: 0
    .... .... .... .... .... .... 1111 1111 = MPLS TTL: 255
v MultiProtocol Label Switching Header, Label: 28, Exp: 0, S: 1, TTL: 1
    0000 0000 0000 0001 1100 .... .... .... = MPLS Label: 28
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
    .... .... .... .... .... .... 0000 0001 = MPLS TTL: 1
v PW Associated Channel Header
    .... 0000 = Channel Version: 0
    Reserved: 0x00
    Channel Type: IPv4 packet (0x0021)
> Internet Protocol Version 4, Src: 10.1.1.1, Dst: 10.0.0.1
> User Datagram Protocol, Src Port: 3503 (3503), Dst Port: 3503 (3503)
> Multiprotocol Label Switching Echo
```

C3/C4 :

```
v PW Associated Channel Header
    .... 0000 = Channel Version: 0
    Reserved: 0x00
    Channel Type: IPv4 packet (0x0021)
v Internet Protocol Version 4, Src: 10.1.1.1, Dst: 10.0.0.1
    0100 .... = Version: 4
    .... 0110 = Header Length: 24 bytes
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 104
    Identification: 0xfd8f (64911)
  v Flags: 0x02 (Don't Fragment)
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
  > Time to live: 1
    Protocol: UDP (17)
  > Header checksum: 0x65ee [validation disabled]
    Source: 10.1.1.1
    Destination: 10.0.0.1
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  v Options: (4 bytes), Router Alert
    v Router Alert (4 bytes): Router shall examine packet (0)
      > Type: 148
        Length: 4
        Router Alert: Router shall examine packet (0)
v User Datagram Protocol, Src Port: 3503 (3503), Dst Port: 3503 (3503)
    Source Port: 3503
    Destination Port: 3503
    Length: 80
  > Checksum: 0x029f [validation disabled]
    [Stream index: 0]
> Multiprotocol Label Switching Echo
```

La charge utile MPLS réelle :



2. Réponse d'écho :

peut transporter 1 étiquette - Transport

Envoyé en tant que PAQUET UNICAST. Il peut être commuté par étiquette (avec étiquette de transport) en raison du protocole LDP dans un coeur.

ÉTIQUETTES : 1
SRC IP : EXIT INTERFACE IP ADDRESS (10.1.6.2 dans notre cas)
DST IP : IP SOURCE VUE DANS LA REQUÊTE D'ÉCHO - BOUCLAGE DU ROUTEUR SOURCE
TYPE L4 : UDP
PORT SRC : 3503
PORT DST:3505
OCTET TOS : DÉSACTIVÉ
EXP MPLS : DÉSACTIVÉ
BIT DF : ACTIVÉ

UDP PAYLOAD peut être MPLS LABEL SWITCHING ECHO REPLY

MPLS EXP est activé et défini sur 6

BIT DF activé

Détails VC pour référence :

<#root>

```
R1#sh mpls l2transport vc detail
Local interface: Fa2/0 up, line protocol up, Ethernet up
  Destination address: 10.6.6.6
,
VC ID: 100, VC status: up
    Output interface: Fa0/1, imposed label stack {24 28}
    Preferred path: not configured
    Default path: active
    Next hop: 10.1.1.2
  Create time: 2d17h, last status change time: 2d17h
    Last label FSM state change time: 2d17h
  Signaling protocol: LDP, peer 10.6.6.6:0 up
    Targeted Hello: 10.1.1.1(LDP Id) -> 10.6.6.6, LDP is UP
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: No fault
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 28, remote 28
```

```
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive enabled, send enabled
  Sequencing resync disabled
  Control Word: On (configured: autosense)
  Dataplane:
    SSM segment/switch IDs: 4097/4096 (used), PWID: 1
  VC statistics:
    transit packet totals: receive 1027360, send 1027358
    transit byte totals:   receive 121032028, send 147740215
    transit packet drops:  receive 0, seq error 0, send 0
```

Interopérabilité L2VPN

L'interconnexion L2VPN s'appuie sur cette fonctionnalité en permettant la connexion de circuits de connexion disparates. Une fonction d'interfonctionnement facilite la traduction entre différentes encapsulations de couche 2. Dans les versions précédentes, les routeurs de la gamme Cisco prenaient uniquement en charge l'interconnexion par pont, également appelée interconnexion Ethernet.

Jusqu'à présent, le contrôle d'accès des deux côtés était du même type d'encapsulation, également appelé fonctionnalité « like-to-like ».

L'interfonctionnement L2VPN est une fonctionnalité AToM qui permet différents types d'encapsulation des deux côtés du réseau AToM

- Il est nécessaire d'interconnecter deux circuits de connexion hétérogènes (CA).
- Les deux principales fonctions d'interconnexion L2VPN (IW) prises en charge dans le logiciel Cisco IOS sont les suivantes :

1. IP/Routed : l'en-tête MAC est supprimé (et remplacé par des étiquettes MPLS) à une extrémité du nuage MPLS et un nouvel en-tête MAC est construit à l'autre PE. L'en-tête IP est conservé tel quel.

2. Ethernet/Bridged : l'en-tête MAC n'est pas du tout supprimé. Les étiquettes MPLS sont imposées au-dessus de l'en-tête MAC et l'en-tête MAC est livré tel quel à l'autre extrémité du nuage MPLS.

Possibilités d'interfonctionnement

a. FR vers Ethernet

b. FR à PPP

c. FR vers ATM

d. Ethernet vers VLAN

e. Ethernet vers PPP

Informations connexes

- RFC Editor 4664
- RFC Editor 4667
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.