Services et caractéristiques de L2VPN IOS XR

Contenu

Introduction

Ce document décrit des topologies de base de la couche 2 (L2) VPN (L2VPN). Il est utile de présenter des exemples de base afin d'expliquer la conception, les services, les caractéristiques, et la configuration. Voyez le L2VPN de routeur de services d'agrégation de gamme 9000 de Cisco ASR et le guide de configuration de services Ethernet, libérez 4.3.x pour des informations supplémentaires.

1. Services point par point et multipoints

La caractéristique de L2VPN fournit la capacité de fournir des services point par point et multipoints.

1.1 Service point par point

Le service point par point émule fondamentalement un circuit de transport entre deux Noeuds d'extrémité ainsi les Noeuds d'extrémité semblent être directement connectés au-dessus d'un lien point par point. Ceci peut être utilisé pour connecter deux sites.

En réalité, il peut y avoir des plusieurs routeurs entre les deux Noeuds d'extrémité, et il peut y avoir de plusieurs conceptions pour fournir le service point par point.

Un routeur peut faire la commutation locale entre deux de ses interfaces :

Il peut également y a un pseudowire de Commutation multiprotocole par étiquette (MPLS) (picowatt) entre deux Routeurs :

Un routeur peut des trames de commutateur entre deux PWs ; dans ce cas, c'est un multi-segment picowatt :

La Redondance est disponible par la caractéristique de Redondance picowatt :

D'autres conceptions sont disponibles, mais ne peuvent pas tous être répertoriées ici.

1.2 Service multipoint

Le service multipoint émule un domaine d'émission de sorte que tous les hôtes connectés dans ce bridge-domain semblent être logiquement connectés au même segment d'Ethernets :

Tous les hôtes peuvent être connectés au mêmes routeur/commutateur :

Les plusieurs commutateurs peuvent faire la commutation Ethernet traditionnelle ; le spanning-tree doit être utilisé afin de casser des boucles :

Les services privés virtuels de RÉSEAU LOCAL (VPLS) vous permettent d'étendre le domaine d'émission entre les plusieurs sites utilisant MPLS PWs :

VPLS hiérarchique peut être utilisé afin d'augmenter l'évolutivité :

2. Circuits de connexion

2.1 Circuit virtuel d'Ethernets ASR 9000

2.1.1 Apparier d'interface entrante

Les principes de base pour des circuits de connexion (ACs) incluent :

- Un paquet doit être reçu sur une interface configurée avec le mot clé de *l2transport* afin de pour être traité par la caractéristique de L2VPN.
- Cette interface peut être une interface principale, où la commande de **l2transport** est configurée sous le mode de configuration d'interface, ou une sous-interface, où le mot clé de *l2transport* est configuré après le numéro de sous-interface.
- Une consultation de correspondance plus longue détermine l'interface entrante du paquet. La consultation de correspondance plus longue vérifie ces conditions dans cette commande pour apparier le paquet entrant à une sous-interface :

    1. La trame entrante a deux balises dot1q et apparie une sous-interface configurée avec les mêmes deux balises dot1q (802.1Q perçant un tunnel, ou QinQ). C'est la plus longue possible correspondance.
    2. La trame entrante en a deux balises dot1q et apparie une sous-interface configurée avec le même dot1q les étiquettent d'abord et pour la deuxième balise.
    3. La trame entrante a une balise dot1q et apparie une sous-interface configurée avec la même balise dot1q et le mot clé *précis*.
    4. La trame entrante a un ou plusieurs balises dot1q et apparie une sous-interface configurée avec une des balises dot1q.
    5. La trame entrante n'a aucune balise dot1q et apparie une sous-interface configurée avec la commande d'**encapsulation untagged**.
    6. La trame entrante échoue au match any l'autre sous-interface, ainsi elle apparie une sous-interface configurée avec la commande d'**encapsulation default**.
    7. La trame entrante échoue au match any l'autre sous-interface, ainsi il apparie l'interface principale qui est configurée pour le *l2transport*.

- Sur les Routeurs traditionnels qui n'utilisent pas le modèle de la connexion virtuelle d'Ethernets (EVC), les balises VLAN configurées sous la sous-interface sont retirées (sauté) de la trame avant qu'elles soient transportées par la caractéristique de L2VPN.
- Sur la gamme 9000 de Cisco ASR une agrégation entretient le routeur qui utilise l'infrastructure EVC, l'action par défaut est de préserver les étiquettes existantes. Utilisez la commande de **réécriture** de modifier le par défaut.
- S'il y a une interface virtuelle de passerelle (BVI) dans le bridge-domain, toutes les balises entrantes devraient être sautées parce que le BVI est une interface conduite sans n'importe quelle balise. Voyez la section BVI pour des détails.

Voici plusieurs exemples qui montrent ces règles :

1. Un exemple de base est quand tout le trafic reçu sur un port physique doit être transporté, s'il a une balise VLAN. Si vous configurez le **l2transport** sous l'interface principale, tout le trafic reçu sur ce port physique est transporté par la caractéristique de L2VPN :

   ```
   interface GigabitEthernet0/0/0/2
   l2transport
   ```
   S'il y a des sous-interfaces de cette interface principale, l'interface principale attrape n'importe quelle trame qui n'a été appariée par aucune sous-interface ; c'est la règle de correspondance plus longue.

2. Des interfaces et les sous-interfaces de paquet peuvent être configurées comme l2transport :

   ```
   interface Bundle-Ether1
   l2transport
   ```
3. **Encapsulation default d'**utilisation sous une sous-interface de l2transport au trafic étiqueté ou non-marqué de match any qui n'a pas été apparié par une autre sous-interface avec une correspondance plus longue. (Voir l'exemple 4). Le mot clé de *l2transport* est configuré dans le nom de sous-interface, pas sous la sous-interface comme sur l'interface principale :

   ```
   interface GigabitEthernet0/1/0/3.1 l2transport
   encapsulation default
   ```
   Configurez l'**encapsulation untagged** si vous voulez apparier seulement des trames non marquées.

4. Quand il y a de plusieurs sous-interfaces, exécutez le test de correspondance plus longue sur la trame entrante afin de déterminer l'interface entrante :

   ```
   interface GigabitEthernet0/1/0/3.1 l2transport
   encapsulation default
   !
   interface GigabitEthernet0/1/0/3.2 l2transport
   encapsulation dot1q 2
   !
   interface GigabitEthernet0/1/0/3.3 l2transport
   encapsulation dot1q 2 second-dot1q 3
   ```
   Dans cette configuration, notez cela :

   - Une trame de QinQ avec une balise externe 2 VLAN et une balise intérieure 3 VLAN pourrait apparier la .1, .2, ou .3 sous-interface mais elle est assignée à la .3 sous-interface en raison de la règle de correspondance plus longue. Deux balises sur .3 sont plus longues qu'une balise sur .2 et plus longues qu'aucune balise sur .1.
   - Une trame de QinQ avec une balise externe 2 VLAN et une balise intérieure 4 VLAN est

assignée à la .2 sous-interface parce que l'**encapsulation dot1q 2** peut apparier des trames dot1q avec juste la balise 2 VLAN mais peut également apparier des trames de QinQ avec une balise externe 2. se rapportent à l'exemple 5 (le mot clé *précis*) si vous ne voulez pas apparier les trames de QinQ.
- Une trame de QinQ avec une balise externe 3 VLAN apparie la .1 sous-interface.
- Une trame dot1q avec une balise 2 VLAN apparie la .2 sous-interface.
- Une trame dot1q avec une balise 3 VLAN apparie la .1 sous-interface.

5. Pour apparier une trame dot1q et pas une trame de QinQ, utilisez le mot clé *précis* :

   ```
   interface GigabitEthernet0/1/0/3.2 l2transport
   encapsulation dot1q 2 exact
   ```
   Cette configuration n'apparie pas des trames de QinQ avec une balise externe 2 VLAN parce qu'elle apparie seulement des trames avec exactement une balise VLAN.

6. Employez le mot clé *non-marqué* afin d'apparier seulement des trames non marquées telles que les paquets de Protocole CDP (Cisco Discovery Protocol) ou les Bridges Protocol Data Unit de protocole MSTP (Multiple Spanning Tree Protocol) (BPDU) :

   ```
   interface GigabitEthernet0/1/0/3.1 l2transport
   encapsulation default
   !
   interface GigabitEthernet0/1/0/3.2 l2transport
   encapsulation untagged
   !
   interface GigabitEthernet0/1/0/3.3 l2transport
   encapsulation dot1q 3
   ```
   Dans cette configuration, notez cela :

   - Les trames Dot1q avec un VLAN étiquettent 3 ou les trames de QinQ avec une balise externe 3 apparient la .3 sous-interface.
   - Tout autre dot1q ou QinQ encadre la correspondance la .1 sous-interface.
   - Vues sans correspondance de balise VLAN la .2 sous-interface.

7. *Le n'importe quel* mot clé peut être utilisé comme masque :

   ```
   interface GigabitEthernet0/1/0/3.4 l2transport
   encapsulation dot1q 4 second-dot1q any
   !
   interface GigabitEthernet0/1/0/3.5 l2transport
   encapsulation dot1q 4 second-dot1q 5
   ```
   Les deux sous-interfaces .4 et .5 pourraient apparier des trames de QinQ avec les balises 4 et 5, mais les trames sont assignées à la .5 sous-interface parce qu'il est plus spécifique. C'est la règle de correspondance plus longue.

8. Des plages des balises VLAN peuvent être utilisées :

   ```
   interface GigabitEthernet0/1/0/3.6 l2transport
   encapsulation dot1q 6-10
   ```
9. Des valeurs ou les plages de balise du multiple VLAN peuvent être répertoriées pour la première ou deuxième balise dot1q :

   ```
   interface GigabitEthernet0/1/0/3.7 l2transport
   encapsulation dot1q 6 , 7 , 8-10
   ```

```
!
interface GigabitEthernet0/1/0/3.11 l2transport
encapsulation dot1q 11 second-dot1q 1 , 2 , 3 , 4-6 , 10
```
Vous pouvez répertorier un maximum de neuf valeurs. Si plus de valeurs sont exigées, elles doivent être assignées à une autre sous-interface. Valeurs de groupe dans une plage afin de raccourcir la liste.

10. La commande d'**encapsulation dot1q second-dot1q** utilise l'Ethertype 0x8100 pour les balises externes et intérieures parce que c'est la méthode de Cisco pour encapsuler des trames de QinQ. Selon IEEE, cependant, l'Ethertype 0x8100 devrait être réservé des trames de 802.1Q avec une balise VLAN, et une balise externe avec Ethertype 0x88a8 devrait être utilisée des trames de QinQ. La balise externe avec Ethertype 0x88a8 peut être configurée avec le mot clé *dot1ad* :

```
interface GigabitEthernet0/1/0/3.12 l2transport
encapsulation dot1ad 12 dot1q 100
```
11. Afin d'utiliser le vieil Ethertype 0x9100 ou 0x9200 pour les balises externes de QinQ, utilisez la commande de **dot1q tunneling ethertype** sous l'interface principale de la sous-interface de QinQ :

```
interface GigabitEthernet0/1/0/3
dot1q tunneling ethertype [0x9100|0x9200]
!
interface GigabitEthernet0/1/0/3.13 l2transport
encapsulation dot1q 13 second-dot1q 100
```
La balise externe a un Ethertype de 0x9100 ou de 0x9200, et la balise intérieure a le dot1q Ethertype 0x8100.

12. Une trame entrante peut être assignée à une sous-interface, basée sur l'adresse MAC source :

```
interface GigabitEthernet0/1/0/3.14 l2transport
encapsulation dot1q 14 ingress source-mac 1.1.1
```

2.1.2 Manipulation VLAN

Le comportement par défaut d'une plate-forme basée sur EVC est de garder les balises VLAN sur la trame entrante.

```
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
```
Dans cette configuration, une trame entrante dot1q avec une balise 3 VLAN garde sa balise 3 VLAN quand la trame est expédiée. Une trame entrante de QinQ avec une balise externe 3 VLAN et une balise intérieure 100 maintient les deux balises inchangées quand la trame est expédiée.

Mais, l'infrastructure EVC te permet pour manipuler les balises avec la commande de **réécriture**, ainsi vous pouvez sauter (retirer), se traduire, ou des balises de pousser (ajoutez) à la pile entrante de balise VLAN.

Voici plusieurs exemples :

- Le mot clé *pop* vous permet de retirer une balise de QinQ d'une trame entrante dot1q. Cet exemple retire la balise externe 13 de la trame entrante de QinQ et en avant de la trame avec la balise 100 dot1q sur le dessus :

```
interface GigabitEthernet0/1/0/3.13 l2transport
encapsulation dot1q 13 second-dot1q 100
rewrite ingress tag pop 1 symmetric
```

Le comportement est toujours symétrique, ainsi il signifie que la balise externe 13 est sautée dans la direction d'entrée et enfoncée la direction de sortie.

- Le mot clé de *traduire* vous permet de remplacer un ou deux balises entrantes par un ou deux nouvelles balises :

```
RP/0/RSP0/CPU0:router2(config-subif)#interface GigabitEthernet0/1/0/3.3
l2transport
RP/0/RSP0/CPU0:router2(config-subif)# encapsulation dot1q 3
RP/0/RSP0/CPU0:router2(config-subif)#rewrite ingress tag translate ?
1-to-1 Replace the outermost tag with another tag
1-to-2 Replace the outermost tag with two tags
2-to-1 Replace the outermost two tags with one tag
2-to-2 Replace the outermost two tags with two other tags
RP/0/RSP0/CPU0:router2(config-subif)#rewrite ingress tag translate 1-to-1 ?
dot1ad Push a Dot1ad tag
dot1q Push a Dot1Q tag
RP/0/RSP0/CPU0:router2(config-subif)#rewrite ingress tag translate 1-to-1
dot1q 4
RP/0/RSP0/CPU0:router2(config-subif)#show config
Building configuration...
!! IOS XR Configuration 4.3.0
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
rewrite ingress tag translate 1-to-1 dot1q 4 symmetric
!
end
```

Le mot clé *symétrique* est ajouté automatiquement parce que c'est le seul mode pris en charge.

- Le mot clé de *pousser* vous permet d'ajouter une balise de QinQ à une trame entrante dot1q :

```
interface GigabitEthernet0/1/0/3.4 l2transport
encapsulation dot1q 4
rewrite ingress tag push dot1q 100 symmetric
```

Une balise externe 100 de QinQ est ajoutée à la trame entrante avec une balise 4. dot1q. Dans la direction de sortie, la balise de QinQ est sautée.

2.2 Comportement de routeur de Non-EVC de Cisco IOS XR (CRS et XR12000)

La syntaxe pour le VLAN s'assortissant sur les Plateformes de non-EVC n'utilise pas le mot clé d'*encapsulation* :

```
RP/0/RP0/CPU0:router1#config
RP/0/RP0/CPU0:router1(config)#int gig 0/0/0/2.3 l2transport
RP/0/RP0/CPU0:router1(config-subif)#dot1q ?
vlan Configure a VLAN ID on the subinterface
RP/0/RP0/CPU0:router1(config-subif)#dot1q vlan ?
<1-4094> Configure first (outer) VLAN ID on the subinterface
RP/0/RP0/CPU0:router1(config-subif)#dot1q vlan 3 ?
<1-4094> Configure second (inner 802.1Q) VLAN ID on the subinterface
any Match frames with any second 802.1Q VLAN ID

RP/0/RP0/CPU0:router1(config-subif)#dot1q vlan 3 100
```

La manipulation de balise VLAN ne peut pas être configurée, parce que le seul comportement possible est de sauter toutes les balises qui sont spécifiées dans les commandes **dot1q** ou

dot1ad. Ceci est fait par défaut, tellement là n'est aucune commande de **réécriture**.

3. Service point par point

Remarques :

Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

3.1 Commutation locale

3.1.1 Interface principale

La topologie de base est une croix locale se connectent entre deux interfaces principales :

Le Router2 prend tout le trafic reçu sur le Gi 0/1/0/1 et en avant lui à Te 0/0/0/3 et vice versa.

Tandis que router1 et router3 semblent avoir un câble dos à dos direct dans cette topologie, ce n'est pas le cas parce que router2 se traduit réellement entre les interfaces de TenGigE et de GigabitEthernets. Le Router2 peut exécuter des caractéristiques sur ces deux interfaces ; une liste de contrôle d'accès (ACL), par exemple, peut relâcher les types spécifiques des paquets ou d'un policy-map afin de former ou de trafic de faible priorité de rate-limit.

Une croix point par point de base se connectent est configurée entre deux interfaces principales qui sont configurées comme l2transport sur router2 :

```
interface GigabitEthernet0/1/0/1
l2transport
!
!
interface TenGigE0/0/0/3
l2transport
!
!
l2vpn
xconnect group test
p2p p2p1
interface TenGigE0/0/0/3
interface GigabitEthernet0/1/0/1
!
```

Sur router1 et router3, les interfaces principales sont configurées avec le CDP et un ipv4 addres :

```
RP/0/RP0/CPU0:router1#sh run int Gi 0/0/0/1
interface GigabitEthernet0/0/0/1
cdp
```

```
ipv4 address 10.1.1.1 255.255.255.0
!

RP/0/RP0/CPU0:router1#
RP/0/RP0/CPU0:router1#sh cdp nei Gi 0/0/0/1
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater

Device ID Local Intrfce Holdtme Capability Platform Port ID
router3.cisco.c Gi0/0/0/1 132 R ASR9K Ser Te0/0/0/3
RP/0/RP0/CPU0:router1#ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/8/32 ms
```

Router1 voit router3 en tant que voisin de CDP et peut cingler 10.1.1.2 (l'adresse d'interface de router3) comme si les deux Routeurs ont été directement connectés.

Puisqu'il n'y a aucune sous-interface configurée sur router2, des trames entrantes avec une balise VLAN sont transportées d'une manière transparente quand des sous-interfaces dot1q sont configurées sur router1 et router3 :

```
RP/0/RP0/CPU0:router1#sh run int gig 0/0/0/1.2
interface GigabitEthernet0/0/0/1.2
ipv4 address 10.1.2.1 255.255.255.0
dot1q vlan 2
!

RP/0/RP0/CPU0:router1#ping 10.1.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/5 ms
```

Après 10,000 pings de router1 à router3, vous pouvez employer l'**interface d'exposition** et les commandes de **l2vpn d'exposition** afin de s'assurer que des requêtes pings reçues par router2 sur un courant alternatif sont expédiées sur l'autre courant alternatif et que des réponses pings sont traitées la même manière à l'envers.

```
RP/0/RSP0/CPU0:router2#sh int gig 0/1/0/1
GigabitEthernet0/1/0/1 is up, line protocol is up
Interface state transitions: 1
Hardware is GigabitEthernet, address is 0024.986c.63f1 (bia 0024.986c.63f1)
Description: static lab connection to acdc 0/0/0/1 - dont change
Layer 2 Transport Mode
MTU 1514 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
reliability 255/255, txload 0/255, rxload 0/255
Encapsulation ARPA,
Full-duplex, 1000Mb/s, SXFD, link type is force-up
output flow control is off, input flow control is off
loopback not set,
Last input 00:00:00, output 00:00:00
Last clearing of "show interface" counters 00:01:07
5 minute input rate 28000 bits/sec, 32 packets/sec
5 minute output rate 28000 bits/sec, 32 packets/sec
10006 packets input, 1140592 bytes, 0 total input drops
0 drops for unrecognized upper-level protocol
Received 0 broadcast packets, 6 multicast packets
0 runts, 0 giants, 0 throttles, 0 parity
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
10007 packets output, 1140832 bytes, 0 total output drops
Output 0 broadcast packets, 7 multicast packets
```

```
0 output errors, 0 underruns, 0 applique, 0 resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions


RP/0/RSP0/CPU0:router2#sh int ten 0/0/0/3
TenGigE0/0/0/3 is up, line protocol is up
Interface state transitions: 3
Hardware is TenGigE, address is 0024.98ea.038b (bia 0024.98ea.038b)
Layer 1 Transport Mode is LAN
Description: static lab connection to putin 0/0/0/3 - dont change
Layer 2 Transport Mode
MTU 1514 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
reliability 255/255, txload 0/255, rxload 0/255
Encapsulation ARPA,
Full-duplex, 10000Mb/s, LR, link type is force-up
output flow control is off, input flow control is off
loopback not set,
Last input 00:00:00, output 00:00:06
Last clearing of "show interface" counters 00:01:15
5 minute input rate 27000 bits/sec, 30 packets/sec
5 minute output rate 27000 bits/sec, 30 packets/sec
10008 packets input, 1140908 bytes, 0 total input drops
0 drops for unrecognized upper-level protocol
Received 0 broadcast packets, 8 multicast packets
0 runts, 0 giants, 0 throttles, 0 parity
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
10006 packets output, 1140592 bytes, 0 total output drops
Output 0 broadcast packets, 6 multicast packets
0 output errors, 0 underruns, 0 applique, 0 resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions


RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
---------------------- ------------------------- -------------------------
test p2p1 UP Te0/0/0/3 UP Gi0/1/0/1 UP
------------------------------------------------------------------------------
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test det

Group test, XC p2p1, state is up; Interworking none
AC: TenGigE0/0/0/3, state is up
Type Ethernet
MTU 1500; XC ID 0x1080001; interworking none
Statistics:
packets: received 10008, sent 10006
bytes: received 1140908, sent 1140592
AC: GigabitEthernet0/1/0/1, state is up
Type Ethernet
MTU 1500; XC ID 0x1880003; interworking none
Statistics:
packets: received 10006, sent 10008
bytes: received 1140592, sent 1140908

RP/0/RSP0/CPU0:router2#sh l2vpn forwarding interface gigabitEthernet 0/1/0/1
hardware ingress detail location 0/1/CPU0
Local interface: GigabitEthernet0/1/0/1, Xconnect id: 0x1880003, Status: up
Segment 1
AC, GigabitEthernet0/1/0/1, Ethernet port mode, status: Bound
```

```
Statistics:
packets: received 10022, sent 10023
bytes: received 1142216, sent 1142489
packets dropped: PLU 0, tail 0
bytes dropped: PLU 0, tail 0
Segment 2
AC, TenGigE0/0/0/3, Ethernet port mode, status: Bound

Platform AC context:
Ingress AC: Local Switch, State: Bound
Flags: Remote is Simple AC
XID: 0x00580003, SHG: None
Ingress uIDB: 0x0003, Egress uIDB: 0x0003, NP: 3, Port Learn Key: 0
NP3
Ingress uIDB:
Flags: L2, Status
Stats Ptr: 0x0d842c, uIDB index: 0x0003, Wire Exp Tag: 0
BVI Bridge Domain: 0, BVI Source XID: 0x01000000
VLAN1: 0, VLAN1 etype: 0x0000, VLAN2: 0, VLAN2 etype: 0x0000
L2 ACL Format: 0, L2 ACL ID: 0, IPV4 ACL ID: 0, IPV6 ACL ID: 0
QOS ID: 0, QOS Format ID: 0
Local Switch dest XID: 0x00000001
UIDB IF Handle: 0x00000000, Source Port: 1, Num VLANs: 0
Xconnect ID: 0x00580003, NP: 3
Type: AC, Remote type: AC
Flags: Learn enable
uIDB Index: 0x0003, LAG pointer: 0x0000
Split Horizon Group: None

RP/0/RSP0/CPU0:router2#sh l2vpn forwarding interface Te 0/0/0/3 hardware egress
detail location 0/0/CPU0
Local interface: TenGigE0/0/0/3, Xconnect id: 0x1080001, Status: up
Segment 1
AC, TenGigE0/0/0/3, Ethernet port mode, status: Bound
Statistics:
packets: received 10028, sent 10027
bytes: received 1143016, sent 1142732
packets dropped: PLU 0, tail 0
bytes dropped: PLU 0, tail 0
Segment 2
AC, GigabitEthernet0/1/0/1, Ethernet port mode, status: Bound

Platform AC context:
Egress AC: Local Switch, State: Bound
Flags: Remote is Simple AC
XID: 0x00000001, SHG: None
Ingress uIDB: 0x0007, Egress uIDB: 0x0007, NP: 0, Port Learn Key: 0
NP0
Egress uIDB:
Flags: L2, Status, Done
Stats ptr: 0x000000
VPLS SHG: None
L2 ACL Format: 0, L2 ACL ID: 0, IPV4 ACL ID: 0, IPV6 ACL ID: 0
VLAN1: 0, VLAN1 etype: 0x0000, VLAN2: 0, VLAN2 etype: 0x0000
UIDB IF Handle: 0x04000240, Search VLAN Vector: 0
QOS ID: 0, QOS format: 0
Xconnect ID: 0x00000001, NP: 0
Type: AC, Remote type: AC
Flags: Learn enable
uIDB Index: 0x0007, LAG pointer: 0x0000
Split Horizon Group: None
```

3.1.2 Sous-interfaces et manipulation VLAN

En terminologie de logiciel de Cisco IOS®, cet exemple a un courant alternatif qui est comme une interface de switchport mode access et une sous-interface dot1q qui est comme un joncteur réseau :

Typiquement cette topologie utilise un bridge-domain parce qu'il y a habituellement plus de deux ports dans le VLAN, bien que vous puissiez utiliser une croix point par point connectez s'il y a seulement deux ports. Cette section décrit comment les capacités flexibles de réécriture te donnent de plusieurs manières de manipuler le VLAN.

Interface principale de 3.1.2.1 et sous-interface Dot1q

Dans cet exemple, l'interface principale est d'un côté, et la sous-interface dot1q est de l'autre côté :

C'est l'interface principale sur router1 :

```
RP/0/RP0/CPU0:router1#sh run int gig 0/0/0/1
interface GigabitEthernet0/0/0/1
description static lab connection to router2 0/1/0/1
cdp
ipv4 address 10.1.1.1 255.255.255.0
!
```

C'est la sous-interface dot1q sur router2 :

```
RP/0/RSP0/CPU0:router2#sh run int gig 0/1/0/1
interface GigabitEthernet0/1/0/1
description static lab connection to router1 0/0/0/1
l2transport

RP/0/RSP0/CPU0:router2#sh run int ten 0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric

RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p2
interface TenGigE0/0/0/3.2
interface GigabitEthernet0/1/0/1
```

Il y a maintenant un mot clé de *l2transport* dans le nom de sous-interface de TenGigE0/0/0/3.2. Envoie Routeur3 les trames dot1q avec la balise 2, qui apparient la sous-interface TenGigE0/0/0/3.2 sur router2.

La balise entrante 2 est retirée dans la direction d'entrée par la commande **symétrique du bruit 1 de rewrite ingress tag**. Puisque la balise a été retirée dans la direction d'entrée sur le TenGigE0/0/0/3.2, les paquets sont envoyés à non-marqué dans la direction de sortie sur GigabitEthernet0/1/0/1.

Router1 envoie les trames non marquées, qui apparient l'interface principale GigabitEthernet0/1/0/1.

Il n'y a aucune commande de **réécriture** sur GigabitEthernet0/1/0/1, ainsi aucune balise n'est sautée, est poussée, ou traduite.

Quand des paquets doivent être expédiés hors de TenGigE0/0/0/3.2, la balise 2 dot1q est due poussé au mot clé *symétrique* dans la commande du **bruit 1 de rewrite ingress tag**. La commande saute une balise dans la direction d'entrée mais pousse symétriquement une balise dans la direction de sortie. C'est un exemple sur router3 :

```
RP/0/RSP0/CPU0:router3#sh run int ten 0/0/0/3.2
interface TenGigE0/0/0/3.2
ipv4 address 10.1.1.2 255.255.255.0
encapsulation dot1q 2
```

Surveillez les compteurs de sous-interface avec la même **interface d'exposition** et **affichez les** commandes de **l2vpn** :

```
RP/0/RSP0/CPU0:router2#clear counters
Clear "show interface" counters on all interfaces [confirm]
RP/0/RSP0/CPU0:router2#clear l2vpn forwarding counters
RP/0/RSP0/CPU0:router2#
RP/0/RSP0/CPU0:router2#
RP/0/RSP0/CPU0:router2#sh int TenGigE0/0/0/3.2
TenGigE0/0/0/3.2 is up, line protocol is up
Interface state transitions: 1
Hardware is VLAN sub-interface(s), address is 0024.98ea.038b
Layer 2 Transport Mode
MTU 1518 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
reliability Unknown, txload Unknown, rxload Unknown
Encapsulation 802.1Q Virtual LAN,
Outer Match: Dot1Q VLAN 2
Ethertype Any, MAC Match src any, dest any
loopback not set,
Last input 00:00:00, output 00:00:00
Last clearing of "show interface" counters 00:00:27
1000 packets input, 122000 bytes
0 input drops, 0 queue drops, 0 input errors
1002 packets output, 122326 bytes
0 output drops, 0 queue drops, 0 output errors


RP/0/RSP0/CPU0:router2#sh l2vpn xconnect detail

Group test, XC p2p2, state is up; Interworking none
AC: TenGigE0/0/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0x1080001; interworking none
Statistics:
packets: received 1001, sent 1002
bytes: received 118080, sent 118318
drops: illegal VLAN 0, illegal length 0
AC: GigabitEthernet0/1/0/1, state is up
Type Ethernet
MTU 1500; XC ID 0x1880003; interworking none
Statistics:
packets: received 1002, sent 1001
bytes: received 114310, sent 114076
```

Comme prévu, le nombre de paquets a reçu sur TenGigE0/0/0/3.2 apparie le nombre de paquets envoyés sur GigabitEthernet0/1/0/1 et vice versa.

Sous-interface de 3.1.2.2 avec l'encapsulation

Au lieu de l'interface principale sur GigabitEthernet0/1/0/1, vous pouvez employer une sous-

interface avec l'**encapsulation default** afin d'attraper toutes les trames ou avec l'**encapsulation untagged** afin d'apparier seulement des trames non marquées :

```
RP/0/RSP0/CPU0:router2#sh run interface GigabitEthernet0/1/0/1.1
interface GigabitEthernet0/1/0/1.1 l2transport
encapsulation untagged

RP/0/RSP0/CPU0:router2#sh run int TenGigE0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric

RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p3
interface TenGigE0/0/0/3.2
interface GigabitEthernet0/1/0/1.1
```

Direction d'entrée de 3.1.2.3 sur GigabitEthernet0/1/0/1.1

Plutôt que la balise pop 2 dans la direction d'entrée sur TenGigE0/0/0/3.2, vous pouvez pousser la balise 2 dans la direction d'entrée sur GigabitEthernet0/1/0/1.1 et ne pas faire n'importe quoi sur TenGigE0/0/0/3.2 :

```
RP/0/RSP0/CPU0:router2#sh run int  TenGigE0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2

RP/0/RSP0/CPU0:router2#sh run interface GigabitEthernet0/1/0/1.1
interface GigabitEthernet0/1/0/1.1 l2transport
encapsulation untagged
rewrite ingress tag push dot1q 2 symmetric

RP/0/RSP0/CPU0:router2#sh run int TenGigE0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2

RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p3
interface TenGigE0/0/0/3.2
interface GigabitEthernet0/1/0/1.1
```

Ainsi, vous pouvez voir que le modèle EVC avec les commandes d'**encapsulation** et de **réécriture** te donne la grande flexibilité d'apparier et manipuler des balises VLAN.

3.2 Agences de presse privées virtuelles

3.2.1 Aperçu

Les agences de presse privées virtuelles (VPWS), également connues sous le nom de Fonction Ethernet over MPLS (EoMPLS), permettent à deux périphériques de Provider Edge de L2VPN (PE) pour percer un tunnel le trafic de L2VPN au-dessus d'un nuage MPLS. Le siège potentiel d'explosion du L2VPN deux sont typiquement connectés à deux sites différents à un noyau MPLS

entre eux. Les deux ACs connecté à chaque PE de L2VPN sont joints par un picowatt au-dessus du réseau MPLS, qui est le MPLS picowatt.

Chaque PE doit avoir des mpls label afin d'atteindre le bouclage du PE distant. Cette étiquette, habituellement appelée l'étiquette de Protocole IGP (Interior Gateway Protocol), peut être apprise par le protocole de distribution de mpls label (LDP) ou l'Ingénierie de trafic MPLS (TE).

Le siège potentiel d'explosion deux établissent une session visée MPLS LDP entre eux-mêmes ainsi ils peuvent établir et contrôler le statut du picowatt. Un PE annonce à l'autre PE les mpls label pour l'identification picowatt.

> Remarque: Tandis que le BGP peut être utilisé pour la signalisation, il n'est pas couvert dans ce document.

Le trafic reçu par router2 sur son courant alternatif de gens du pays est encapsulé dans une pile de mpls label :

- Les mpls label externes sont l'étiquette d'IGP pour atteindre le bouclage de router3. Ceci pourrait être l'étiquette d'implicite-null si les étiquettes sont directement connectées ; ceci signifie qu'aucune étiquette d'IGP ne serait ajoutée.
- Les mpls label intérieurs sont l'étiquette picowatt annoncée par router3 par la session visée LDP.
- Il peut y a un mot de commande picowatt après les mpls label, selon la configuration et le type d'encapsulation. Le mot de commande n'est pas utilisé par défaut sur des interfaces Ethernet et doit être explicitement configuré une fois nécessaire.
- La trame L2 transportée suit dans le paquet.
- Quelques balises VLAN sont transportées au-dessus du picowatt, selon la configuration et le type picowatt.

Le saut pénultième, juste avant que router3 dans le noyau MPLS, saute l'étiquette d'IGP ou la remplace par une étiquette d'Étiqette Explicit Null. Ainsi, l'étiquette signicative supérieure sur la trame reçue par router3 est l'étiquette picowatt que router3 a signalée à router2 pour le picowatt. Ainsi, router3 sait que le trafic reçu avec ces mpls label devrait être commuté au courant alternatif connecté à router4.

Dans l'exemple précédent, vous devriez d'abord vérifier si chaque L2VPN a des mpls label pour le bouclage du PE distant. C'est un exemple de la façon vérifier des étiquettes sur router2 :

```
RP/0/RSP1/CPU0:router2#sh mpls forwarding prefix 10.0.0.11/32
Local Outgoing Prefix Outgoing Next Hop Bytes
Label Label or ID Interface Switched
------ ----------- ------------------ ------------ --------------- ------------
16008 16009 10.0.0.11/32 Te0/0/0/1 10.0.23.2 681260
```

La configuration à C.A. est toujours identique :

```
RP/0/RSP1/CPU0:router2#sh run int gig 0/0/0/1.2
Wed May 1 13:56:07.668 CEST
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
```

Puisqu'il n'y a aucune commande de **bruit d'entrée de réécriture**, la balise entrante 2 VLAN est transportée au-dessus du picowatt. Voir le type 4 et 5 PWs pour des détails.

La configuration de L2VPN spécifie le courant alternatif de gens du pays et le PE de L2VPN distant avec un ID picowatt qui doit s'assortir de chaque côté et doit être seul pour chaque voisin :

```
RP/0/RSP1/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p4
interface GigabitEthernet0/0/0/1.2
neighbor 10.0.0.11 pw-id 222
```

La configuration correspondante sur router3 est :

```
RP/0/RSP0/CPU0:router3#sh run int gig 0/1/0/3.2
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
!

RP/0/RSP0/CPU0:router3#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p4
interface GigabitEthernet0/1/0/3.2
neighbor 10.0.0.13 pw-id 222
```

Employez la commande de **détail de show l2vpn xconnect** afin de visualiser des détails sur la croix se connectent :

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test xc-name p2p4 detail

Group test, XC p2p4, state is up; Interworking none
AC: GigabitEthernet0/0/0/1.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0x840006; interworking none
Statistics:
packets: received 186, sent 38448
bytes: received 12644, sent 2614356
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.11, PW ID 222, state is up ( established )
PW class not set, XC ID 0xc0000004
Encapsulation MPLS, protocol LDP
Source address 10.0.0.13
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------------------
Label 16026 16031
Group ID 0x4000280 0x6000180
Interface GigabitEthernet0/0/0/1.2 GigabitEthernet0/1/0/3.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
```

```
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225476
Create time: 30/04/2013 16:30:58 (21:31:00 ago)
Last time status changed: 30/04/2013 16:36:42 (21:25:16 ago)
Statistics:
packets: received 38448, sent 186
bytes: received 2614356, sent 12644
```

Dans cette configuration, notez cela :

- Le Maximum Transmission Unit (MTU) du courant alternatif est 1504 parce que la balise entrante sur le courant alternatif n'est pas sautée. Le MTU doit s'assortir de chaque côté, ou le picowatt n'est pas soulevé.
- 186 paquets ont été reçus sur le courant alternatif et ont été envoyés sur le picowatt comme prévus.
- 38448 paquets ont été reçus sur le picowatt et ont été envoyés sur le courant alternatif comme prévus.
- L'étiquette locale sur router2 est 16026 et est l'étiquette que router3 utilise comme étiquette intérieure. Les paquets sont reçus sur router2 avec ces mpls label comme étiquette supérieure parce que l'étiquette d'IGP a été sautée par le saut pénultième MPLS. Le Router2 sait que des trames entrantes avec cette étiquette picowatt devraient être commutées au Gi 0/0/0/1.2 à C.A. :

```
RP/0/RSP1/CPU0:router2#sh mpls forwarding labels 16026
Local Outgoing Prefix Outgoing Next Hop Bytes
Label Label or ID Interface Switched
------ ----------- ----------------- ------------ --------------- ------------
16026 Pop PW(10.0.0.11:222) Gi0/0/0/1.2 point2point 2620952
```

3.2.2 picowatts et courant alternatif ont couplé l'état

Dans une croix point par point connectez, le courant alternatif et le picowatt sont couplés. Ainsi, si le courant alternatif descend, le PE de L2VPN signale par l'intermédiaire du LDP au PE distant que l'état picowatt devrait être en baisse. Ceci déclenche la convergence quand la Redondance picowatt est configurée. Voyez la section de Redondance pour des détails.

Dans cet exemple, le courant alternatif est en baisse sur router2 et envoie l'état « à C.A. vers le bas » picowatt à router3 :

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test xc-name p2p4 detail
Wed May 1 23:38:55.542 CEST

Group test, XC p2p4, state is down; Interworking none
AC: GigabitEthernet0/0/0/1.2, state is down
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0x840006; interworking none
Statistics:
packets: received 186, sent 38544
bytes: received 12644, sent 2620884
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.11, PW ID 222, state is down ( remote standby )
PW class not set, XC ID 0xc0000004
Encapsulation MPLS, protocol LDP
Source address 10.0.0.13
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
```

```
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------------------
Label 16026 16031
Group ID 0x4000280 0x6000180
Interface GigabitEthernet0/0/0/1.2 GigabitEthernet0/1/0/3.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x6 (AC Down) in Notification message
MIB cpwVcIndex: 3221225476
Create time: 30/04/2013 16:30:58 (1d07h ago)
Last time status changed: 01/05/2013 14:05:07 (09:33:47 ago)
Statistics:
packets: received 38544, sent 186
bytes: received 2620884, sent 12644
```

Sait Routeur3 que le picowatt devrait être en baisse parce que le courant alternatif de distant est en baisse :

```
RP/0/RSP0/CPU0:router3#sh l2vpn xconnect group test xc-name p2p4 detail

Group test, XC p2p4, state is down; Interworking none
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0xc40003; interworking none
Statistics:
packets: received 38545, sent 186
bytes: received 2620952, sent 12644
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.13, PW ID 222, state is down ( local ready )
PW class not set, XC ID 0xc0000005
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------------------
Label 16031 16026
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
```

```
------------ ------------------------------ ----------------------------
Incoming Status (PW Status TLV):
Status code: 0x6 (AC Down) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225477
Create time: 30/04/2013 16:37:57 (1d07h ago)
Last time status changed: 01/05/2013 14:11:33 (09:35:50 ago)
Statistics:
packets: received 186, sent 38545
bytes: received 12644, sent 2620952
```

3.2.3 Type 4 et type 5 PWs

Deux types de PWs peuvent être utilisés - le type 4 et le type 5.

- Un type 4 picowatts est connu comme picowatt basé sur VLAN. Le PE d'entrée n'est pas censé retirer les balises entrantes VLAN qui doivent être transportées au-dessus du picowatt.

  Sur les Plateformes basées sur EVC telles que l'ASR 9000, le problème est que l'ACs entrant pourrait avoir une commande de **réécriture** qui saute les balises entrantes VLAN, tellement là ne pourrait pas être n'importe quelle balise VLAN à transporter au-dessus du picowatt. Afin d'adresser cette possibilité, les Plateformes EVC insèrent une balise factice 0 VLAN sur la trame pour le type 4 PWs. Le type 4 PWs sont configurés avec la commande de **VLAN de transport-mode**. Le PE distant devrait être basé sur EVC et devrait comprendre que la balise du dessus VLAN est la balise factice à éliminer.

  Cependant, si vous utilisez un type 4 picowatts entre une plate-forme EVC et une plate-forme de non-EVC, ceci pourrait mener aux problèmes d'interopérabilité. La plate-forme de non-EVC ne considère pas la balise du dessus VLAN comme balise factice VLAN et à la place en avant la trame avec la balise factice 0 VLAN comme balise externe. Les Plateformes EVC ont la capacité de manipuler les balises VLAN reçues sur la trame entrante avec la commande de **réécriture**. Les résultats de cette manipulation VLAN sont transportés au-dessus du type 4 picowatts avec la balise factice supplémentaire 0 sur le dessus.

  Les releases récentes de Logiciel Cisco IOS XR offrent la capacité d'utiliser un type 4 picowatts sans utilisation de la balise factice 0 avec la commande de **fonction émulation de VLAN de transport-mode**. La manipulation de balise VLAN sur les Ethernets circulent le point (EFP) doit s'assurer qu'au moins une balise reste parce qu'il doit y a une balise VLAN transportée sur un type 4 picowatts et parce que, dans ce cas, il n'y a aucune balise factice qui répond à cette exigence. Les balises qui restent sur la trame après que la réécriture de balise d'interface entrante soient transportées d'une manière transparente par le picowatt.

- Un type 5 picowatts est connu comme Ethernet picowatt basé sur port. Les trames de transports de PE d'entrée reçues sur une interface principale ou après que les balises de sous-interface aient été retirées quand le paquet est reçu sur une sous-interface. Il n'y a aucune condition requise d'envoyer à une trame marquée au-dessus d'un type 5 picowatts, et aucune balise factice n'est ajoutée en les Plateformes basées sur EVC. Les Plateformes basées sur EVC ont la capacité de manipuler les balises VLAN reçues sur la trame entrante avec la commande de **réécriture**. Les résultats de cette manipulation VLAN sont transportés au-dessus du type 5 picowatts, si étiqueté ou non-marqué.

Par défaut, l'essai de siège potentiel d'explosion de L2VPN pour négocier un type 5 picowatts, comme vu dans cet exemple :

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test det | i " PW type"
PW type Ethernet, control word disabled, interworking none
PW type Ethernet Ethernet
```

L'Ethernet de type picowatt indique un type 5 picowatts.

C'est une capture de renifleur d'une requête envoyée d'ARP par router1 et encapsulée par router2 au-dessus du picowatt à router3 :

```
Frame 38: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
Ethernet II, Src: Cisco_2f:dc:04 (00:0b:60:2f:dc:04), Dst: Cisco_1e:93:50
(00:24:f7:1e:93:50)
MultiProtocol Label Switching Header, Label: 16031, Exp: 0, S: 1, TTL: 251
Ethernet II, Src: Cisco_03:1f:46 (00:1d:46:03:1f:46), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2
Address Resolution Protocol (request)
```

Les mpls label 16031 sont l'étiquette picowatt annoncée par router3. La capture de renifleur a été prise entre le saut pénultième et router3, tellement là n'est aucune étiquette d'IGP.

Les débuts encapsulés de trame Ethernet juste après l'étiquette picowatt. Il peut y a un mot de commande picowatt, mais il n'est pas configuré dans cet exemple.

Même si c'est un type 5 picowatts, la balise entrante 2 VLAN reçue sur le courant alternatif par router2 est transportée parce qu'il n'y a aucune commande de **réécriture** qui le saute sur le courant alternatif. Les résultats que provenu le courant alternatif après que le traitement de réécriture soient transportés parce qu'il n'y a aucune balise automatique sautant sur les Plateformes basées sur EVC. Notez qu'il n'y a aucune balise factice 0 VLAN avec un type 5 picowatts.

Si vous configuriez avec la commande **symétrique du bruit 1 de rewrite ingress tag**, il n'y aurait aucune balise VLAN transportée au-dessus du picowatt.

Voici un exemple d'un type 4 picowatts avec la configuration d'une picowatt-classe sur router2 et router3.

> Remarque: Si vous configurez un type 4 d'un côté seulement, le picowatt reste vers le bas et signale la « erreur : Type picowatt mal adapté. »

```
l2vpn
pw-class VLAN
encapsulation mpls
transport-mode vlan
!
!
xconnect group test
p2p p2p4
neighbor 10.0.0.11 pw-id 222
pw-class VLAN
!
!
!
!
```

Le VLAN Ethernet de type picowatt indique un type 4 picowatts.

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test det | i " PW type"
PW type Ethernet VLAN, control word disabled, interworking none
PW type Ethernet VLAN Ethernet VLAN
```

Il y a maintenant une balise factice 0 insérée sur la trame étant transportée :

```
Frame 15: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Cisco_2f:dc:04 (00:0b:60:2f:dc:04), Dst: Cisco_1e:93:50
(00:24:f7:1e:93:50)
MultiProtocol Label Switching Header, Label: 16031, Exp: 0, S: 1, TTL: 251
Ethernet II, Src: Cisco_03:1f:46 (00:1d:46:03:1f:46), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 0
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2
Address Resolution Protocol (request)
```

Le PE basé sur EVC de sortie retire la balise factice et en avant la trame avec la balise 2 sur son courant alternatif de gens du pays. Le PE de sortie applique la manipulation locale de balise configurée sur son courant alternatif sur la trame reçue sur le picowatt. Si son courant alternatif de gens du pays est configuré comme **bruit 1 de rewrite ingress tag symétrique**, la balise configurée doit être enfoncée la direction de sortie, ainsi une nouvelle balise est poussée sur la balise 2 reçue sur le picowatt. La commande de réécriture est très flexible mais vous devriez soigneusement évaluer ce que vous voulez réaliser sur chaque côté du picowatt.

3.2.4 Multisegment picowatt

Il est possible d'avoir un PE de L2VPN qui a un picowatt, au lieu d'une interface physique, comme courant alternatif :

Router5 reçoit des paquets sur le picowatt de router2 et commute les paquets sur son autre picowatt à router3. Ainsi router5 commute entre PWs afin de créer un multisegment picowatt entre router2 et router3.

La configuration sur router2 se dirige maintenant à router5 comme PE distant :

```
RP/0/RSP1/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p5
interface GigabitEthernet0/0/0/1.2
neighbor 10.0.0.12 pw-id 222
!
!
!
!
```

La configuration sur router5 est de base :

```
RP/0/RSP0/CPU0:router5#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p5
neighbor 10.0.0.11 pw-id 223
!
neighbor 10.0.0.13 pw-id 222
!
description R2-R5-R3
!
!
!
```

La commande description est facultative et est insérée en valeur de longueur de type de commutation picowatt (TLV) qui est envoyée par router5 à chaque PE distant (router2 et router3). La description est utile quand vous devez dépanner un problème picowatt quand il y a un routeur au milieu qui fait la commutation picowatt.

Sélectionnez la commande SH de xconnect de l2vpn afin de passer en revue le picowatt commutant la TLV :

```
RP/0/RSP0/CPU0:router5#sh l2vpn xconnect group test det

Group test, XC p2p5, state is down; Interworking none
Description: R2-R5-R3
PW: neighbor 10.0.0.11, PW ID 223, state is down ( provisioned )
PW class not set, XC ID 0xc0000002
Encapsulation MPLS, protocol LDP
Source address 10.0.0.12
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------------------
Label 16042 unknown
Group ID 0x4000280 0x0
Interface GigabitEthernet0/0/0/1.2 unknown
MTU 1504 unknown
Control word disabled unknown
PW type Ethernet unknown
VCCV CV type 0x2 0x0
(none)
(LSP ping verification)
VCCV CC type 0x4 0x0
(none)
(TTL expiry)
------------ ------------------------------ ------------------------------
Outgoing PW Switching TLVs (Label Mapping message):
Local IP Address: 10.0.0.12, Remote IP Address: 10.0.0.13, PW ID: 222
Description: R1-R5-R3
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Statistics for MS-PW:
packets: received 0
bytes: received 0
MIB cpwVcIndex: 3221225474
Create time: 02/05/2013 15:37:53 (00:34:43 ago)
Last time status changed: 02/05/2013 16:12:30 (00:00:06 ago)
Last time PW went down: 02/05/2013 16:12:30 (00:00:06 ago)
PW: neighbor 10.0.0.13, PW ID 222, state is up ( established )
PW class not set, XC ID 0xc0000001
Encapsulation MPLS, protocol LDP
Source address 10.0.0.12
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------------------
Label 16043 16056
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
```

```
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x4 0x6
(router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing PW Switching TLVs (Label Mapping message):
Local IP Address: 10.0.0.12, Remote IP Address: 10.0.0.11, PW ID: 223
Description: R2-R5-R3
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Statistics for MS-PW:
packets: received 0
bytes: received 0
MIB cpwVcIndex: 0
Create time: 02/05/2013 15:37:53 (00:34:43 ago)
Last time status changed: 02/05/2013 16:12:35 (00:00:01 ago)
Last time PW went down: 02/05/2013 16:12:30 (00:00:06 ago)
```

Router5 envoie un picowatt commutant la TLV à router3 avec les détails de son picowatt à router2 et envoie un picowatt commutant la TLV à router2 avec les détails de son picowatt à router3.

3.2.5 Redondance

Un Point à point picowatt peut être utilisé pour connecter deux sites, mais ces deux sites devraient rester connectés en cas de panne de PE ou à C.A.

Redondance centrale de 3.2.5.1

Si vous apportez n'importe quelle modification de topologie qui affecte le réacheminement dans le noyau MPLS, le MPLS picowatt hérite du nouveau chemin immédiatement.

Paquet de 3.2.5.2 au-dessus de PWs

Un périphérique de Customer Edge (CE) peut être connecté au PE par un paquet d'Ethernets afin de fournir la Redondance de lien s'il y a une panne de liaison membre de paquet entre le CE et le PE. Le paquet reste même si un membre de lien de paquet descend. Notez que ceci ne fournit pas la Redondance de PE parce qu'une panne de PE réduit le paquet entier.

Une méthode pour la Redondance est de faire transporter de plusieurs circuits par PWs point par point. Chaque circuit est un membre d'un paquet d'Ethernets entre deux ces :

Le PE ne termine pas le paquet et à la place les trames de transports d'une manière transparente au-dessus du picowatt, y compris les trames du Control Protocol d'agrégation de liaisons (LACP) qui échange de ces entre elles.

Avec cette conception, la perte d'un courant alternatif ou un PE entraîne un membre de paquet descend, mais le paquet reste.

Remarque: LACP BPDU n'ont pas été transportés au-dessus du L2VPN par l'ASR 9000 dans les versions plus tôt que la version 4.2.1 de Logiciel Cisco IOS XR.

Le CE est toujours un point de défaillance unique dans cette conception. D'autres caractéristiques de Redondance qui peuvent être utilisées sur le CE incluent :

- Groupe d'agrégation de liaisons de Multichassis (MC-LAG)
- Groupement de la virtualisation de réseau ASR 9000 (nanovolt)
- Système de commutation virtuelle (VSS) sur des commutateurs de Cisco IOS
- Le Port canalisé virtuel (vpc) sur Cisco Nexus commute

De la perspective du PE, il y a une connexion point-à-point simple entre un courant alternatif et un MPLS picowatt.

Redondance de 3.2.5.3 picowatt

Le siège potentiel d'explosion peut également fournir à la Redondance une configuration appelée la Redondance picowatt.

Le Router2 a un picowatt primaire à router3. Le trafic de router1 à router6 circule sur ce picowatt primaire sous des circonstances normales. Le Router2 a également une sauvegarde picowatt à router4 dans des circonstances de secours immédiat mais, sous normales, aucune circulation au-dessus de ce picowatt.

S'il y a un problème avec le picowatt primaire, avec le PE distant du picowatt primaire (router3), ou avec le courant alternatif sur le PE distant (router3), router2 lance immédiatement la sauvegarde picowatt, et les débuts du trafic la traversant. Le trafic se déplace de nouveau au picowatt primaire quand le problème est résolu.

La configuration sur router2 est :

```
RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p6
interface GigabitEthernet0/1/0/3.2
neighbor 10.0.0.13 pw-id 222
backup neighbor 10.0.0.14 pw-id 222
!
!
!
!
!
```

La configuration standard sur router3 et router4 est :

```
RP/0/RSP1/CPU0:router3#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p6
interface GigabitEthernet0/0/0/1.2
neighbor 10.0.0.11 pw-id 222
!
!
!
!
```

Dans des conditions stables, le picowatt à router3 est en activité, et le picowatt à router4 est dans un état de réserve :

```
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
---------------------- ------------------ --------------------------
test p2p6 UP Gi0/1/0/3.2 UP 10.0.0.13 222 UP
Backup
10.0.0.14 222 SB
------------------------------------------------------------------------
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test det

Group test, XC p2p6, state is up; Interworking none
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0xc40003; interworking none
Statistics:
packets: received 51412, sent 25628
bytes: received 3729012, sent 1742974
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.13, PW ID 222, state is up ( established )
PW class not set, XC ID 0xc0000005
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------ --------------------------
Label 16049 16059
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------ --------------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225477
Create time: 03/05/2013 15:04:03 (00:21:26 ago)
Last time status changed: 03/05/2013 15:17:34 (00:07:55 ago)
MAC withdraw message: send 0 receive 0
Statistics:
packets: received 25628, sent 51412
bytes: received 1742974, sent 3729012

Backup PW:
PW: neighbor 10.0.0.14, PW ID 222, state is standby ( all ready )
Backup for neighbor 10.0.0.13 PW ID 222 ( inactive )
```

```
PW class not set, XC ID 0xc0000006
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ -------------------------- -------------------------
Label 16050 289971
Group ID 0x6000180 0x4000100
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ -------------------------- -------------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x20 (Standby) in Notification message
MIB cpwVcIndex: 3221225478
Create time: 03/05/2013 15:04:03 (00:21:26 ago)
Last time status changed: 03/05/2013 15:17:34 (00:07:55 ago)
MAC withdraw message: send 0 receive 0
RP/0/RSP0/CPU0:router2#
```

Puisque l'état à C.A. et l'état picowatt sont couplés, router3 signale le « courant alternatif vers le bas » à router2 quand le courant alternatif sur router3 descend. Le Router2 réduit son picowatt primaire et lance la sauvegarde picowatt :

```
RP/0/RSP0/CPU0:May  3 15:34:08.772 : l2vpn_mgr[1121]: %L2-L2VPN_PW-3-UPDOWN :
Pseudowire with address 10.0.0.13, id 222, state is Down
RP/0/RSP0/CPU0:May 3 15:34:08.772 : l2vpn_mgr[1121]: %L2-L2VPN_PW-3-UPDOWN :
Pseudowire with address 10.0.0.14, id 222, state is Up

RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
------------------------ --------------------- --------------------------
test p2p6 UP Gi0/1/0/3.2 UP 10.0.0.13 222 DN
Backup
10.0.0.14 222 UP
------------------------------------------------------------------------------
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test det

Group test, XC p2p6, state is up; Interworking none
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0xc40003; interworking none
Statistics:
packets: received 51735, sent 25632
bytes: received 3752406, sent 1743230
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.13, PW ID 222, state is down ( local ready )
PW class not set, XC ID 0xc0000005
```

```
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ --------------------------
Label 16049 16059
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ --------------------------
Incoming Status (PW Status TLV):
Status code: 0x6 (AC Down) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225477
Create time: 03/05/2013 15:04:03 (00:30:14 ago)
Last time status changed: 03/05/2013 15:34:08 (00:00:09 ago)
MAC withdraw message: send 0 receive 0

Backup PW:
PW: neighbor 10.0.0.14, PW ID 222, state is up ( established )
Backup for neighbor 10.0.0.13 PW ID 222 ( active )
PW class not set, XC ID 0xc0000006
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------ ----------------------------
Label 16050 289971
Group ID 0x6000180 0x4000100
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------ ----------------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225478
Create time: 03/05/2013 15:04:03 (00:30:14 ago)
Last time status changed: 03/05/2013 15:34:08 (00:00:09 ago)
MAC withdraw message: send 0 receive 0
Statistics:
packets: received 25632, sent 51735
```

```
bytes: received 1743230, sent 3752406
RP/0/RSP0/CPU0:router2#
```

Quand le courant alternatif sur router3 se réactive, router2 réactive le picowatt primaire à router3, et le picowatt à router4 retourne à un état de réserve.

La sauvegarde picowatt est également lancée quand router3 descend, et router2 perd l'artère à son bouclage.

La prochaine étape logique est d'introduire la Redondance bi-directionnelle picowatt avec le siège potentiel d'explosion deux à chaque site :

Cependant, ce maillage complet de PWs rencontre un problème quand deux PWs sont en activité en même temps une boucle est introduits dans le réseau. La boucle doit être cassée, généralement au moyen du Protocole Spanning Tree (STP). Cependant, vous ne voulez pas que l'instabilité de spanning-tree à un site propage à l'autre site. Ainsi, il vaut mieux de ne pas exécuter le spanning-tree sur des ces PWs et de ne pas fusionner le spanning-tree entre les deux sites. Il est plus simple s'il y a juste un lien logique entre les deux sites de sorte qu'aucun spanning-tree ne soit exigé.

Une solution est d'utiliser un paquet MC-LAG entre le siège potentiel d'explosion deux à un site et à leur CE local. Seulement un du siège potentiel d'explosion deux a son active de membres de paquet de sorte que son picowatt au site distant soit en activité. L'autre PE a ses membres de paquet dans l'état de réserve et a son picowatt au site distant vers le bas. Avec seulement un active picowatt entre les deux sites, aucune boucle n'est introduite. Le PE avec le picowatt actif a également un standby picowatt au deuxième PE au site distant.

Dans des conditions stables, les membres actifs de paquet sont sur router2 et router3, et le picowatt actif est entre eux. C'est la configuration sur router3 :

```
RP/0/RSP1/CPU0:router3#sh run redundancy
redundancy
iccp
group 2
mlacp node 1
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.14
!
backbone
interface TenGigE0/0/0/0
interface TenGigE0/0/0/1
!
isolation recovery-delay 300
!
!
!

RP/0/RSP1/CPU0:router3#sh run int bundle-ether 222
interface Bundle-Ether222
lacp switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mlacp port-priority 1
mac-address 0.0.2
```

```
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!

RP/0/RSP1/CPU0:router3#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p7
interface Bundle-Ether222.2
neighbor 10.0.0.11 pw-id 222
backup neighbor 10.0.0.12 pw-id 222
!
!
!
!
!
RP/0/RSP1/CPU0:router3#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
------------------------ --------------------- --------------------------
test p2p7 UP BE222.2 UP 10.0.0.11 222 UP
Backup
10.0.0.12 222 DN
------------------------------------------------------------------------------

RP/0/RSP1/CPU0:router3#sh bundle bundle-ether 222

Bundle-Ether222
Status: Up
Local links : 1 / 0 / 1
Local bandwidth : 1000000 (1000000) kbps
MAC address (source): 0000.0000.0002 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 1
Wait while timer: Off
Load balancing: Default
LACP: Operational
Flap suppression timer: 100 ms
Cisco extensions: Disabled
mLACP: Operational
ICCP Group: 2
Role: Active
Foreign links : 0 / 1
Switchover type: Revertive
Recovery delay: 40 s
Maximize threshold: 1 link
IPv4 BFD: Not configured

Port Device State Port ID B/W, kbps
-------------------- --------------- -------- -------------- ----------
Gi0/0/0/1 Local Active 0x8001, 0x9001 1000000
Link is Active
Gi0/0/0/1 10.0.0.14 Standby 0x8002, 0xa002 1000000
Link is marked as Standby by mLACP peer
```

Sur router5, le membre local de paquet et le picowatt primaire à router2 sont dans l'état de réserve, et la sauvegarde picowatt à router4 est en baisse :

```
RP/0/RSP1/CPU0:router5#sh run redundancy
```

```
redundancy
iccp
group 2
mlacp node 2
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.13
!
backbone
interface TenGigE0/1/0/0
interface TenGigE0/1/0/1
!
isolation recovery-delay 300
!
!
!

RP/0/RSP1/CPU0:router5#sh run int bundle-ether 222
interface Bundle-Ether222
lacp switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mac-address 0.0.2
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!

RP/0/RSP1/CPU0:router5#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p7
interface Bundle-Ether222.2
neighbor 10.0.0.11 pw-id 222
backup neighbor 10.0.0.12 pw-id 222
!
!
!
!
!

RP/0/RSP1/CPU0:router5#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
------------------------ ---------------------- -------------------------
test p2p7 DN BE222.2 UP 10.0.0.11 222 SB
Backup
10.0.0.12 222 DN
------------------------------------------------------------------------------
RP/0/RSP1/CPU0:router5#sh bundle bundle-ether 222

Bundle-Ether222
Status: mLACP hot standby
Local links : 0 / 1 / 1
Local bandwidth : 0 (0) kbps
MAC address (source): 0000.0000.0002 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
```

```
Maximum active links: 1
Wait while timer: Off
Load balancing: Default
LACP: Operational
Flap suppression timer: 100 ms
Cisco extensions: Disabled
mLACP: Operational
ICCP Group: 2
Role: Standby
Foreign links : 1 / 1
Switchover type: Revertive
Recovery delay: 40 s
Maximize threshold: 1 link
IPv4 BFD: Not configured

Port Device State Port ID B/W, kbps
-------------------- ------------ ----------- -------------- ----------
Gi0/0/0/1 Local Standby 0x8002, 0xa002 1000000
mLACP peer is active
Gi0/0/0/1 10.0.0.13 Active 0x8001, 0x9001 1000000
Link is Active
```

Sur router6, le membre de paquet à router3 est en activité, alors que le membre de paquet à router5 est dans l'état de réserve :

```
router6#sh etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port


Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+-----------------------------------------------
2 Po2(SU) LACP Gi0/1(P) Gi0/2(w)
```

Quand le membre de paquet sur router3 descend, router6 a son membre actif à router5 :

```
router6#sh etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port


Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
```

```
------+-------------+-----------+---------------------------------------------
2 Po2(SU) LACP Gi0/1(D) Gi0/2(P)
```

Puisque le bundle-ether222 est vers le bas sur router5, le picowatt couplé à router2 descend en même temps :

```
RP/0/RSP1/CPU0:router3#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
------------------------ ------------------- -------------------------
test p2p7 DN BE222.2 DN 10.0.0.11 222 DN
Backup
10.0.0.12 222 DN
------------------------------------------------------------------------------
```

Le Router2 détecte que son picowatt à router3 est en baisse et lance sa sauvegarde picowatt à router5 :

```
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
------------------------ ------------------- -------------------------
test p2p7 UP BE222.2 UP 10.0.0.13 222 DN
Backup
10.0.0.14 222 UP
------------------------------------------------------------------------------
```

Router5 a son membre de paquet actif aussi bien que son picowatt primaire à router2 :

```
RP/0/RSP1/CPU0:router5#sh bundle bundle-ether 222

Bundle-Ether222
Status: Up
Local links : 1 / 0 / 1
Local bandwidth : 1000000 (1000000) kbps
MAC address (source): 0000.0000.0002 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 1
Wait while timer: Off
Load balancing: Default
LACP: Operational
Flap suppression timer: 100 ms
Cisco extensions: Disabled
mLACP: Operational
ICCP Group: 2
Role: Active
Foreign links : 0 / 1
Switchover type: Revertive
Recovery delay: 40 s
Maximize threshold: 1 link
IPv4 BFD: Not configured

Port Device State Port ID B/W, kbps
-------------------- ----------- ----------- ------------- ----------
Gi0/0/0/1 Local Active 0x8002, 0xa002 1000000
Link is Active
Gi0/0/0/1 10.0.0.13 Configured 0x8003, 0x9001 1000000
Link is down
```

```
RP/0/RSP1/CPU0:router5#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
------------------------ ---------------------- --------------------------
test p2p7 UP BE222.2 UP 10.0.0.11 222 UP
Backup
10.0.0.12 222 DN
------------------------------------------------------------------------------
```

Batterie de périphérie de 3.2.5.4 ASR 9000 nanovolt

La conception précédente basée sur la Redondance MC-LAG et picowatt fonctionne bien pour la Redondance mais, parce que quelques membres de paquet sont dans l'état de réserve, ils ne portent pas le trafic dans des conditions régulières.

Si vous voulez tout l'active de membres de paquet, même dans des conditions stables, vous pouvez utiliser une batterie ASR 9000 avec des membres de paquet du CE connecté à chaque étagère du PE :

Cette conception offre la Redondance contre une panne de liaison membre de paquet entre le CE et le PE, une panne d'étagère, et une principale panne de lien - tant que la batterie est double reliée au noyau MPLS et il y a Redondance au centre. Les deux étagères ne doivent pas être coïmplantées et pourraient être aux endroits différents. des liens d'Inter-étagère ne sont pas représentés dans ce diagramme.

Si vous voulez la Redondance sur le CE, vous pouvez utiliser une solution de multichassis pour le CE :

- MC-LAG
- Groupement ASR 9000 nanovolt
- VSS
- vpc

La configuration sur la batterie ASR 9000 est très de base :

```
interface TenGigE0/0/0/8
bundle id 222 mode on
!
interface TenGigE1/0/0/8
bundle id 222 mode on
!
interface Bundle-Ether222
!
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
l2vpn
xconnect group test
p2p p2p8
interface Bundle-Ether222.2
neighbor 10.0.0.13 pw-id 8
!
!
!
```

```
!
```

Cisco vous recommande configurent une adresse MAC statique de système LACP et une adresse MAC de paquet afin d'éviter une modification d'adresse MAC provoquée par un basculement indiqué de contrôleur de module. Cet exemple affiche comment trouver les adresses :

```
RP/1/RSP0/CPU0:router2#sh int bundle-ether 222 | i address is
Hardware is Aggregated Ethernet interface(s), address is 0024.f71e.d309
Internet address is Unknown
RP/1/RSP0/CPU0:router2#
RP/1/RSP0/CPU0:router2#conf
RP/1/RSP0/CPU0:router2(config)#int bundle-ether 222
RP/1/RSP0/CPU0:router2(config-if)#mac-address 0024.f71e.d309
RP/1/RSP0/CPU0:router2(config-if)#commit
RP/1/RSP0/CPU0:router2(config-if)#end
RP/1/RSP0/CPU0:router2#
RP/1/RSP0/CPU0:router2#sh lacp system-id

Priority MAC Address
-------- -----------------
0x8000 00-24-f7-1e-d3-05
RP/1/RSP0/CPU0:router2#
RP/1/RSP0/CPU0:router2#conf
RP/1/RSP0/CPU0:router2(config)#lacp system mac 0024.f71e.d305
RP/1/RSP0/CPU0:router2(config)#commit
RP/1/RSP0/CPU0:router2(config)#end
```

En résumé, c'est le paquet-Ether 222 avec un membre sur chaque étagère (dix 0/0/0/8 sur 1/0/0/8 de l'étagère 0 et dix sur l'étagère 1) et la sous-interface de paquet configurée pour une croix point par point se connectent :

```
RP/1/RSP0/CPU0:router2#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
------------------------ ---------------------- --------------------------
test p2p8 UP BE222.2 UP 10.0.0.13 8 UP
------------------------------------------------------------------------------
```

3.3 CDP

Les Routeurs et les Commutateurs de Cisco envoient habituellement des paquets de CDP sans balises dot1q. Il y a de plusieurs scénarios qui déterminent ce qui arrive à ces paquets de CDP quand elles sont reçues par un routeur IOS XR configuré pour une croix se connectent :

Dans cette topologie, router1 peut voir son PE local router2 comme voisin ou CE distant router4 de CDP, selon la configuration.

3.3.1 CDP non activé sur l'interface principale du PE de L2VPN

Les paquets de CDP du CE de L2VPN sont transportés au-dessus de la croix se connectent. Les deux ces de L2VPN se voient (avec l'utilisation de l'ordre de **show cdp neighbors**) si l'interface principale est configurée comme l2transport ou s'il y a une sous-interface appariant les trames CDP non-marquées.

C'est un exemple de l'interface principale :

```
interface GigabitEthernet0/0/0/1
l2transport
!
!
l2vpn
xconnect group test
p2p p2p8
interface GigabitEthernet0/0/0/1
neighbor 10.0.0.11 pw-id 8
!
!
!
!
```

C'est un exemple d'une sous-interface non-marquée :

```
interface GigabitEthernet0/0/0/1.1 l2transport
encapsulation untagged
!
l2vpn
xconnect group test
p2p p2p8
interface GigabitEthernet0/0/0/1.1
neighbor 10.0.0.11 pw-id 8
!
!
!
!
```

Dans ces deux exemples, les paquets de CDP sont transportés au-dessus de la croix se connectent, et le ces se voient comme voisins de CDP. Le CE ne voit pas le PE en tant que voisin de CDP :

```
router1#sh cdp nei gigabitEthernet 0/1
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID Local Intrfce Holdtme Capability Platform Port ID
router4 Gig 0/1 168 R S ME-3400G- Gig 0/1
```

3.3.2 CDP activé sur l'interface principale du PE de L2VPN

Le PE traite les paquets non-marqués de CDP, et le PE et le CE se voient comme voisins. Cependant, le CE ne voit pas le CE distant quand le CDP est activé sur l'interface principale du PE de L2VPN.

Notez cela :

- Vous ne pouvez pas configurer le CDP sur une interface principale qui est configurée comme l2transport.
- Le PE intercepte les paquets de CDP quand le CDP est configuré sur l'interface principale non-l2transport. Ceci se produit même s'il y a une sous-interface de l2transport configurée pour apparier les paquets non-marqués de CDP (avec l'utilisation des commandes d'**encapsulation untagged** ou d'**encapsulation default**). Des paquets de CDP ne sont pas transportés au site distant dans ce cas.

3.4 Spanning-tree

Si le CE de L2VPN est un commutateur ethernet et envoie le spanning-tree BPDU au PE de L2VPN, ces BPDU sont manipulés comme trafic habituel et sont transportés selon la configuration de L2VPN.

STP ou MST BPDU sont envoyés à non-marqué et sont transportés par la croix point par point se connectent si l'interface principale est configurée comme l2transport ou s'il y a une sous-interface de l2transport configurée avec les commandes d'**encapsulation untagged** ou d'**encapsulation default**.

Le Per VLAN Spanning Tree Plus (PVST+) ou les PVST+ rapides (PVRST+) envoient les BPDU étiquetés qui sont transportés s'il y a une sous-interface de l2transport qui apparie la balise dot1q des BPDU.

C'est un exemple de topologie :

Le Router2 et les router3 sont des trames non marquées et des trames de transport avec la balise 2 dot1q :

```
interface GigabitEthernet0/0/0/1.1 l2transport
encapsulation untagged
!
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
l2vpn
xconnect group test
p2p p2p8
interface GigabitEthernet0/0/0/1.2
neighbor 10.0.0.11 pw-id 8
!
!
p2p p2p9
interface GigabitEthernet0/0/0/1.1
neighbor 10.0.0.11 pw-id 9
!
!
!
!
```

Switch1 reçoit les BPDU non-marqués dans le VLAN 1 et les BPDU étiquetés dans VLAN2 de switch4 ; son port de racine est sur Gi0/1 vers switch4 :

```
switch1#sh spanning-tree vlan 1

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32768
Address 0024.985e.6a00
Cost 8
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
```

```
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Root FWD 4 128.1 P2p

switch1#sh spanning-tree vlan 2

VLAN0002
Spanning tree enabled protocol ieee
Root ID Priority 32770
Address 0019.552b.b580
Cost 4
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Root FWD 4 128.1 P2p
```

Avec cette configuration, le domaine de spanning-tree au site A est fusionné avec le domaine de spanning-tree sur le côté B. Un problème potentiel est que l'instabilité de spanning-tree à un site pourrait propager à l'autre site.

Si vous êtes sûr qu'un site soit connecté seulement par un picowatt à un autre site et qu'il n'y a aucun lien secret qui pourrait introduire une boucle physique, c'est une bonne idée de ne pas exécuter le spanning-tree au-dessus des deux sites. Ceci maintient les deux domaines de spanning-tree d'isolement. Pour faire ceci, configurer un spanning-tree bpdufilter sur le ces, ou configurer une liste d'accès d'Ethernet-services sur le siège potentiel d'explosion pour relâcher des trames avec l'adresse MAC de destination utilisée par des BPDU. Une liste d'accès d'Ethernet-services sur le siège potentiel d'explosion peut être utilisée pour relâcher des trames avec le MAC de destination BPDU ou d'autres genres de protocoles L2 que vous ne voulez pas expédier au-dessus du picowatt.

C'est une liste d'accès que vous pourriez utiliser sous chaque sous) interface de l2transport (qui est transportée entre les deux sites :

```
ethernet-services access-list block-invalid-frames
10 deny any 0180.c200.0000 0000.0000.000f
20 deny any host 0180.c200.0010
30 deny any host 0100.0c00.0000
40 deny any host 0100.0ccc.cccc
50 deny any host 0100.0ccc.cccd
60 deny any host 0100.0ccd.cdce
70 permit any any
!

RP/0/RSP1/CPU0:router2#sh run int GigabitEthernet0/0/0/1.1
interface GigabitEthernet0/0/0/1.1 l2transport
encapsulation untagged
ethernet-services access-group block-invalid-frames ingress
ethernet-services access-group block-invalid-frames egress
!

RP/0/RSP1/CPU0:router2#sh run int GigabitEthernet0/0/0/1.2
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ethernet-services access-group block-invalid-frames ingress
```

```
ethernet-services access-group block-invalid-frames egress
!
```

L'ACL d'Ethernet-services commence à relâcher les BPDU :

```
RP/0/RSP1/CPU0:router2#sh access-lists ethernet-services block-invalid-frames
hardware ingress location 0/0/CPU0
ethernet-services access-list block-invalid-frames
10 deny any 0180.c200.0000 0000.0000.000f (41 hw matches)
20 deny any host 0180.c200.0010
30 deny any host 0100.0c00.0000
40 deny any host 0100.0ccc.cccc
50 deny any host 0100.0ccc.cccd (63 hw matches)
60 deny any host 0100.0ccd.cdce
70 permit any any (8 hw matches)
```

Switch1 ne reçoit plus les BPDU de switch4, ainsi switch1 est maintenant la racine :

```
switch1#sh spanning-tree vlan 1

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 001d.4603.1f00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- ----------------------
Gi0/1 Desg FWD 4 128.1 P2p

switch1#sh spanning-tree vlan 2

VLAN0002
Spanning tree enabled protocol ieee
Root ID Priority 32770
Address 001d.4603.1f00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- ----------------------
Gi0/1 Desg FWD 4 128.1 P2p
```

Le risque de désactiver le spanning-tree sur un lien est ceci : si une connexion secrète est créée entre les sites, elle introduit une boucle physique, et le spanning-tree ne peut pas casser la boucle. Ainsi, quand vous désactivez le spanning-tree au-dessus d'un picowatt, assurez-vous qu'il n'y a aucun lien redondant entre les sites et que le picowatt demeure la seule connexion entre les sites.

S'il y a de plusieurs connexions entre les sites, utilisez une solution comme VPLS avec une version de passerelle d'accès du spanning-tree, tel que la passerelle MST Access (MSTAG) ou la passerelle PVST+ Access (PVSTAG). Voyez la section au service multipoint pour des détails.

4. Service multipoint

> Remarques :
>
> Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.
>
> L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Voyez mettre en application des services multipoints de la couche 2 pour une description complète des caractéristiques L2 multipoints.

Avec seulement deux interfaces dans une croix point par point connectez, un commutateur de L2VPN prend tout reçu là-dessus le côté et en avant de l'autre côté.

Quand il y a plus de deux interfaces dans un bridge-domain, un commutateur ethernet doit prendre une décision de commutation afin de déterminer où expédier des trames basées sur leur adresse MAC de destination. Le commutateur fait apprendre de MAC basé sur l'adresse MAC source des trames qu'elle reçoit et construit une MAC-adresse-table.

De commutateur les trames en avant dans cette méthode :

- Des trames d'émission sont inondées à tous les ports. Contrôle de tempête d'utilisation afin de limiter le débit d'inondation d'émission.
- Des trames de Multidiffusion sont inondées à tous les ports dans le bridge-domain, à moins que quand le Protocole IGMP (Internet Group Management Protocol) ou le Multicast Listener Discovery (MLD) pillant est configuré. Contrôle de tempête d'utilisation afin de limiter le débit d'inondation de Multidiffusion.
- Des trames de monodiffusion avec une adresse MAC de destination qui n'est pas une partie de la MAC-adresse-table du bridge-domain (unicast inconnu) sont inondées sur tous les ports dans le bridge-domain. Contrôle de tempête d'utilisation afin de limiter le débit d'inondation d'UNKNOWN-unicast.
- Des trames de monodiffusion avec une adresse MAC de destination qui fait partie de la MAC-adresse-table du bridge-domain sont expédiées au port où l'adresse MAC de destination a été apprise.

Dans le Logiciel Cisco IOS XR, un domaine d'émission ou un LAN émulé s'appelle un bridge-domain. C'est semblable à un VLAN en terminologie de logiciel de Cisco IOS, sauf qu'un VLAN dans l'IOS est lié à un nombre VLAN qui est utilisé comme balise dot1q sur les joncteurs réseau. Un bridge-domain dans le Logiciel Cisco IOS XR n'est pas lié à un nombre de balise de dot1q vlan. Vous pouvez employer le modèle EVC afin de manipuler les balises dot1q et avoir des sous-interfaces dot1q avec différents nombres de dot1q vlan dans le même bridge-domain ou avoir les interfaces non-marquées.

Un bridge-domain est fondamentalement un domaine d'émission où des émissions et les trames de Multidiffusion sont inondées. Une MAC-adresse-table est associée avec chaque bridge-domain (à moins qu'apprendre de MAC est désactivé manuellement par la configuration, qui est très rare).

Ceci correspond habituellement à un sous-réseau d'ipv4 ou d'IPv6 où tous les hôtes dans le bridge-domain sont directement connectés.

Des bridges-domain peuvent être groupés dans un groupe de passerelle. C'est un moyen pratique de vérifier la configuration. Vous pouvez exécuter une commande show pour un groupe de passerelle au lieu d'une commande show pour chaque bridge-domain. Un groupe de passerelle n'a pas une MAC-adresse-table ou d'autres associations ; il est juste utilisé pour la configuration et les commandes show.

4.1 Commutation locale

C'est un exemple très de base :

Le Router2, les router3, et les router4 sont connectés par un ASR 9000, qui simule un RÉSEAU LOCAL entre ces trois Routeurs.

Ce sont les configurations d'interface sur ces trois Routeurs :

```
RP/0/RSP0/CPU0:router2#sh run int gig 0/1/0/39.2
interface GigabitEthernet0/1/0/39.2
ipv4 address 192.168.2.2 255.255.255.0
encapsulation dot1q 2
!

router3#sh run int gig 0/1
Building configuration...

Current configuration : 203 bytes
!
interface GigabitEthernet0/1
port-type nni
switchport access vlan 2
switchport trunk allowed vlan 1,2
switchport mode trunk
end

router3#sh run int vlan 2
Building configuration...

Current configuration : 61 bytes
!
interface Vlan2
ip address 192.168.2.3 255.255.255.0
end

router3#

RP/0/RSP0/CPU0:router4#sh run int ten 0/0/1/0.2
interface TenGigE0/0/1/0.2
ipv4 address 192.168.2.4 255.255.255.0
encapsulation dot1q 2
!
```

Des paquets sont reçus par router1 avec la balise 2 dot1q et sont expédiés aux autres Routeurs avec la balise 2. dot1q.

Dans ce scénario de base, il y a deux options sur l'ACs :

1. Puisque tout l'ACs utilisent la balise 2 dot1q, vous pouvez la garder sur la trame et en avant la trame sur l'interface de sortie avec la même balise dot1q que reçue sur l'interface d'entrée. La commande **symétrique du bruit 1 de rewrite ingress tag** n'est pas exigée.

2. Vous pouvez sauter la balise entrante 2 dot1q dans la direction d'entrée et symétriquement pousser la balise 2 dot1q dans la direction de sortie. Tandis que ceci n'est pas exigé dans ce scénario de base, c'est une bonne idée de configurer le bridge-domain de cette fa4con au début parce qu'il fournit plus de flexibilité à l'avenir. Voici deux exemples des modifications qui pourraient se produire après configuration initiale :

   - Si une interface BVI conduite est introduite plus tard dans le bridge-domain, des paquets doivent être traités sur le BVI sans balises. Voyez la section pour des détails.
   - Un nouveau courant alternatif, qui utilise une balise différente dot1q, est ajouté plus tard. La balise 2 dot1q serait sautée dans la direction d'entrée, et l'autre balise dot1q serait poussée sur la nouvelle interface dans la direction de sortie et vice versa le .BVI

Sautez les balises dot1q sur chaque courant alternatif sur router1 :

```
RP/0/RSP0/CPU0:router1#sh run int GigabitEthernet0/1/0/3.2
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!

RP/0/RSP0/CPU0:router1#sh run int GigabitEthernet0/1/0/38.2
interface GigabitEthernet0/1/0/38.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!

RP/0/RSP0/CPU0:router1#sh run int TenGigE0/2/0/4.2
interface TenGigE0/2/0/4.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

Visualisez la configuration du bridge-domain avec ces trois ACs :

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain engineering
interface TenGigE0/2/0/4.2
!
interface GigabitEthernet0/1/0/3.2
!
interface GigabitEthernet0/1/0/38.2
!
!
!
!
```

Le bridge-domain doit être configuré sous un groupe de passerelle. Si d'autres bridges-domain de ce client sont nécessaires, ils peuvent être configurés sous le même groupe de passerelle, customer1. Si les nouveaux bridges-domain appartiennent à un client différent, vous pouvez créer un nouveau groupe de passerelle. Ces exemples utilisent le client afin de grouper des bridges-domain, mais des bridges-domain peuvent être groupés par tous les critères.

Employez la commande d'**ingénierie de bridge-domain du groupe customer1 de passerelle de**

l2vpn de passage d'exposition afin d'afficher la configuration du bridge-domain.

Employez la commande du **groupe customer1 de passerelle de l2vpn de passage d'exposition** afin de visualiser la configuration de tous les bridges-domain.

Employez la commande d'**ingénierie de BD-nom de bridge-domain de l2vpn d'exposition** ou la commande du **groupe customer1 de bridge-domain de l2vpn d'exposition** afin d'afficher des informations sur le bridge-domain.

```
RP/0/RSP0/CPU0:router1#show l2vpn bridge-domain group customer1 bd-name
engineering
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 3 (3 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
Gi0/1/0/38.2, state: up, Static MAC addresses: 0
Te0/2/0/4.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
RP/0/RSP0/CPU0:router1#show l2vpn bridge-domain group customer1 bd-name
engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (00:18:06 ago)
No status change since creation
ACs: 3 (3 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40003; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
```

```
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 185066, sent 465
bytes: received 13422918, sent 34974
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
AC: GigabitEthernet0/1/0/38.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40005; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 8, sent 12287
bytes: received 770, sent 892418
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
AC: TenGigE0/2/0/4.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0x1040001; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
```

```
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 463, sent 11839
bytes: received 35110, sent 859028
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
```

Utilisez la commande de **det d'ingénierie de BD-nom du groupe customer1 de bridge-domain de l2vpn d'exposition** si vous voulez vérifier que des paquets sont reçus et envoyés en fonction chaque courant alternatif.

Ajoutez le mot clé de *mac-address à la* commande de **bridge-domain de show l2vpn forwarding** si vous voulez vérifier la MAC-adresse-table :

```
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address location 0/1/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0024.986c.6417 dynamic Gi0/1/0/38.2 0/1/CPU0 0d 0h 0m 0s N/A
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 0s N/A
```

Apprendre de MAC est exécuté dans le matériel par les linecards chaque fois que une trame est reçue dans le bridge-domain. Il y a également un cache de logiciel de la MAC-adresse-table, mais cette table de logiciel ne peut pas être mise à jour continuellement afin d'apparier les entrées de matériel. Quand la **commande show** est sélectionnée en code récent, elle essaye de resynchroniser la table de logiciel avec la table de matériel. Après un maximum de 15 secondes, il imprime l'état actuel de la MAC-adresse-table de logiciel, même si la resynchronisation n'est pas complète (par exemple, si la table est grande). Utilisez le **l2vpn resynchronisent la** commande de MAC-adresse-**table d'expédition** afin de resynchroniser les tables de logiciel et de matériel manuellement.

```
RP/0/RSP0/CPU0:router1#term mon
RP/0/RSP0/CPU0:router1#l2vpn resynchronize forwarding mac-address-table
location 0/1/CPU0
RP/0/RSP0/CPU0:router1#LC/0/1/CPU0:May 28 18:25:35.734 : vkg_l2fib_mac_cache[357]
%PLATFORM-
PLAT_L2FIB_MAC_CACHE-6-RESYNC_COMPLETE : The resynchronization of the MAC
address table is complete
0/1/CPU0

RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:engineering
mac-address location 0/1/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location
```

```
Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 0s N/A
```

Un message de Syslog indique quand le processus de resyncronisation est complet, ainsi il est utile pour faire activer le **terminal monitor** afin de voir le message.

La colonne d'âge de resync affiche la dernière fois que l'adresse MAC a été resynchronisée de la table de matériel.

Le mot clé d'*emplacement* est l'emplacement d'un linecard entrant ou sortant. Les adresses MAC sont permutées entre les linecards dans le matériel, ainsi des adresses MAC devraient être connues sur chaque linecard où il y a un courant alternatif ou un picowatt. Le mot clé de *détail* pourrait fournir une version plus à jour de la table de logiciel :

```
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address detail location 0/1/CPU0

Bridge-domain name: customer1:engineering, id: 5, state: up
MAC learning: enabled
MAC port down flush: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC Secure: disabled, Logging: disabled
DHCPv4 snooping: profile not known on this node
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
IGMP snooping: disabled, flooding: enabled
Bridge MTU: 1500 bytes
Number of bridge ports: 3
Number of MAC addresses: 4
Multi-spanning tree instance: 0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location


GigabitEthernet0/1/0/3.2, state: oper up
Number of MAC: 2
Statistics:
packets: received 187106, sent 757
bytes: received 13571342, sent 57446
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic arp inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0

Mac Address: 0019.552b.b581, LC learned: 0/1/CPU0
Resync Age: 0d 0h 0m 0s, Flag: local


Mac Address: 0019.552b.b5c3, LC learned: 0/1/CPU0
Resync Age: 0d 0h 0m 0s, Flag: local
```

```
GigabitEthernet0/1/0/38.2, state: oper up
Number of MAC: 1
Statistics:
packets: received 18, sent 14607
bytes: received 1950, sent 1061882
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic arp inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0

Mac Address: 0024.986c.6417, LC learned: 0/1/CPU0
Resync Age: 0d 0h 0m 0s, Flag: local


TenGigE0/2/0/4.2, state: oper up
Number of MAC: 1
Statistics:
packets: received 0, sent 0
bytes: received 0, sent 0
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic arp inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0

Mac Address: 6c9c.ed3e.e484, LC learned: 0/2/CPU0
Resync Age: 0d 0h 0m 0s, Flag: remote
```

La version détaillée de la commande fournit le nombre total d'adresses MAC apprises dans le bridge-domain, aussi bien que le nombre d'adresses MAC apprises sous chaque courant alternatif.

Le mot clé de *matériel* vote la MAC-adresse-table de matériel directement des engines d'expédition d'entrée ou de sortie :

```
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address hardware ingress location 0/1/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0024.986c.6417 dynamic Gi0/1/0/38.2 0/1/CPU0 0d 0h 0m 0s N/A
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 0s N/A
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address hardware egress location 0/2/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 14s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 1s N/A
0024.986c.6417 dynamic Gi0/1/0/38.2 0/1/CPU0 0d 0h 0m 10s N/A
```

```
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 13s N/A
RP/0/RSP0/CPU0:router1#
```

4.2 Plein MST

Les exemples précédents de la commutation locale étaient de base parce que seulement des Routeurs ont été connectés au bridge-domain. Une fois que vous commencez à connecter les Commutateurs L2, cependant, vous pourriez introduire une boucle et avoir besoin du STP afin de casser la boucle :

Dans cette topologie, router1, router2, et router3 chacun sont configurés avec un bridge-domain avec toutes leurs interfaces dans le diagramme. Si router4 envoie une émission, telle qu'une demande d'ARP, à router1, router1 l'inonde à router2 et à router3, router2 l'inonde à router3, et router3 l'inonde à router2. Ceci a comme conséquence une boucle et une saturation de diffusion.

Pour casser la boucle, utilisez un STP. Il y a de plusieurs types de STPs, mais offres de Logiciel Cisco IOS XR seulement une implémentation complète, le MST.

Il y a également des versions de passerelle d'accès des protocoles pris en charge dans le Logiciel Cisco IOS XR, tel que PVSTAG et MSTAG. Ce sont des versions statiques et limitées du protocole pour les utiliser dans des topologies spécifiques, typiquement avec VPLS, et sont décrites dans les sections MSTAG et PVSTAG. Dans le Logiciel Cisco IOS XR, MST est la seule option s'il y a une topologie avec des plusieurs commutateurs et si une implémentation intégrale de spanning-tree est exigée.

Deux sous-interfaces sont configurées sur chaque routeur et ajoutées à un bridge-domain. Pour router1, la configuration est :

```
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface GigabitEthernet0/0/0/1.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/0/0/1.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!
l2vpn
bridge group customer1
bridge-domain finance
interface TenGigE0/0/0/1.3
!
interface GigabitEthernet0/0/0/1.3
!
!
bridge-domain engineering
interface TenGigE0/0/0/1.2
!
interface GigabitEthernet0/0/0/1.2
!
!
```

```
!
!
```

MST est configuré sur l'interface principale. Dans cet exemple, le VLAN 2 est assigné pour citer 1, et tous autres VLAN restent l'exemple par défaut 0. (une configuration plus réaliste A séparerait des VLAN même entre les exemples.)

La sélection de la passerelle de racine dans un réseau STP est déterminée par la priorité configurée et l'ID inclus de passerelle de chaque périphérique. Le périphérique avec la priorité la plus basse, ou avec la priorité la plus basse égale mais le plus bas ID de passerelle, est sélectionné comme passerelle de racine. Dans cet exemple, router3 est configuré avec une priorité plus basse puis router1 par exemple 0, ainsi router3 est la racine par exemple que 0. Router1 ont une priorité plus basse puis router3 par exemple 1, ainsi router1 est la racine par exemple 1.

C'est la configuration pour router1 :

```
spanning-tree mst customer1
name customer1
revision 1
instance 0
priority 28672
!
instance 1
vlan-ids 2
priority 24576
!
interface TenGigE0/0/0/1
!
interface GigabitEthernet0/0/0/1
!
!
```

C'est la configuration sur router3 :

```
spanning-tree mode mst
spanning-tree extend system-id
!
spanning-tree mst configuration
name customer1
revision 1
instance 1 vlan 2
!
spanning-tree mst 0 priority 24576
spanning-tree mst 1 priority 28672
```

Le nom, la révision, et le mappage de VLAN-à-exemple doivent être identique sur tous les Commutateurs.

Maintenant, vérifiez l'état de spanning-tree sur router1 :

```
RP/0/RSP1/CPU0:router1#sh spanning-tree mst customer1
Role: ROOT=Root, DSGN=Designated, ALT=Alternate, BKP=Backup, MSTR=Master
State: FWD=Forwarding, LRN=Learning, BLK=Blocked, DLY=Bringup Delayed

Operating in dot1q mode


MSTI 0 (CIST):

VLANS Mapped: 1,3-4094
```

```
CIST Root Priority 24576
Address 001d.4603.1f00
Ext Cost 0

Root ID Priority 24576
Address 001d.4603.1f00
Int Cost 20000
Max Age 20 sec, Forward Delay 15 sec


Bridge ID Priority 28672 (priority 28672 sys-id-ext 0)
Address 4055.3912.f1e6
Max Age 20 sec, Forward Delay 15 sec
Max Hops 20, Transmit Hold count 6


Interface Port ID Role State Designated Port ID
Pri.Nbr Cost Bridge ID Pri.Nbr
------------ ------- --------- ---- ----- -------------------- -------
Gi0/0/0/1 128.2 20000 ROOT FWD 24576 001d.4603.1f00 128.1
Te0/0/0/1 128.1 2000 DSGN FWD 28672 4055.3912.f1e6 128.1


MSTI 1:

VLANS Mapped: 2

Root ID Priority 24576
Address 4055.3912.f1e6
This bridge is the root
Int Cost 0
Max Age 20 sec, Forward Delay 15 sec


Bridge ID Priority 24576 (priority 24576 sys-id-ext 0)
Address 4055.3912.f1e6
Max Age 20 sec, Forward Delay 15 sec
Max Hops 20, Transmit Hold count 6


Interface Port ID Role State Designated Port ID
Pri.Nbr Cost Bridge ID Pri.Nbr
------------ ------- --------- ---- ----- -------------------- -------
Gi0/0/0/1 128.2 20000 DSGN FWD 24576 4055.3912.f1e6 128.2
Te0/0/0/1 128.1 2000 DSGN FWD 24576 4055.3912.f1e6 128.1
```

Est Routeur3 la racine par exemple 0, ainsi router1 a son port de racine sur Gi0/0/0/1 vers router3. Router1 est la racine par exemple 1, ainsi router1 est le pont désigné sur toutes les interfaces pour cet exemple.

Le Router2 est bloqué par exemple 0 sur Te0/1/0/0 :

```
RP/0/RSP1/CPU0:router2#sh spanning-tree mst customer1
Role: ROOT=Root, DSGN=Designated, ALT=Alternate, BKP=Backup, MSTR=Master
State: FWD=Forwarding, LRN=Learning, BLK=Blocked, DLY=Bringup Delayed

Operating in dot1q mode


MSTI 0 (CIST):

VLANS Mapped: 1,3-4094
```

```
CIST Root Priority 24576
Address 001d.4603.1f00
Ext Cost 0

Root ID Priority 24576
Address 001d.4603.1f00
Int Cost 20000
Max Age 20 sec, Forward Delay 15 sec


Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address f025.72a7.b13e
Max Age 20 sec, Forward Delay 15 sec
Max Hops 20, Transmit Hold count 6


Interface Port ID Role State Designated Port ID
Pri.Nbr Cost Bridge ID Pri.Nbr
------------ ------- --------- ---- ----- -------------------- -------
Gi0/0/0/1 128.2 20000 ROOT FWD 24576 001d.4603.1f00 128.2
Te0/1/0/0 128.1 2000 ALT BLK 28672 4055.3912.f1e6 128.1


MSTI 1:

VLANS Mapped: 2

Root ID Priority 24576
Address 4055.3912.f1e6
Int Cost 2000
Max Age 20 sec, Forward Delay 15 sec


Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address f025.72a7.b13e
Max Age 20 sec, Forward Delay 15 sec
Max Hops 20, Transmit Hold count 6


Interface Port ID Role State Designated Port ID
Pri.Nbr Cost Bridge ID Pri.Nbr
------------ ------- --------- ---- ----- -------------------- -------
Gi0/0/0/1 128.2 20000 DSGN FWD 32768 f025.72a7.b13e 128.2
Te0/1/0/0 128.1 2000 ROOT FWD 24576 4055.3912.f1e6 128.1
RP/0/RSP1/CPU0:router2#
```

Te0/1/0/0.2 expédie tandis que Te0/1/0/0.3 est bloqué. Quand la valeur bloquée par STP est 0x0, la condition est fausse, ainsi l'interface expédie ; quand la valeur bloquée par STP est 0x1, la condition est vraie, ainsi l'interface est bloquée.

Employez la commande de **show uidb data** afin de confirmer ceci et afficher les données d'interface qui sont présentes dans le processeur de réseau :

```
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.2
ingress | i Blocked
STP Blocked 0x0
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.3
ingress | i Blocked
STP Blocked 0x1
```

4.3 BVI

La configuration d'un bridge-domain crée un domaine L2. Afin de quitter ce domaine L2, connectez les Routeurs L3 qui conduisent entre les hôtes à l'intérieur du bridge-domain et le monde extérieur. Dans le diagramme précédent, host1 a pu employer router4 ou router5 afin de quitter le sous-réseau local et atteindre l'Internet.

Router1 et router2 où les bridges-domain sont configurés sont des Routeurs ASR 9000, qui peuvent route ipv4 et trafic d'IPv6. Ainsi ces deux Routeurs pourraient prendre le trafic IP hors du bridge-domain et le conduire à l'Internet eux-mêmes, au lieu de compter sur les Routeurs L3. Pour faire ceci, vous devez configurer un BVI, qui est une interface L3 qui branche à un bridge-domain afin de conduire des paquets dans et hors du bridge-domain.

C'est à quoi il ressemble à logiquement :

Voici la configuration :

```
RP/0/RSP1/CPU0:router1#sh run int bvi 2
interface BVI2
ipv4 address 192.168.2.1 255.255.255.0
!

RP/0/RSP1/CPU0:router1#sh run int bvi 3
interface BVI3
ipv4 address 192.168.3.1 255.255.255.0
!


RP/0/RSP1/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface TenGigE0/0/0/1.3
!
interface GigabitEthernet0/0/0/1.3
!
routed interface BVI3
!
bridge-domain engineering
interface TenGigE0/0/0/1.2
!
interface GigabitEthernet0/0/0/1.2
!
routed interface BVI2
!
!
!
RP/0/RSP1/CPU0:router1#sh run int gig 0/0/0/1.2
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

Un BVI est une interface L3 non-marquée, ainsi si vous voulez avoir le processus BVI les paquets reçus sur l'ACs du bridge-domain, l'ACs doit être configuré pour sauter toutes les balises entrantes. Autrement, le BVI ne peut pas comprendre la balise et relâche les paquets. Il n'y a aucune manière de configurer une sous-interface dot1q sur un BVI, ainsi les balises doivent être d'entrée sauté sur l'ACs comme a été fait sur Gi0/0/0/1.2 dans l'exemple précédent.

Puisqu'une interface BVI est une interface virtuelle, il y a quelques restrictions sur les caractéristiques qui peuvent être activées. Ces restrictions sont documentées en configurant

l'Integrated Routing and Bridging sur le routeur de gamme 9000 de Cisco ASR : Restrictions pour configurer IRB. Ces caractéristiques ne sont pas prises en charge sur les interfaces BVI sur l'ASR 9000 :

- Listes de contrôle d'accès (ACL). Cependant, L2 ACLs peut être configuré sur chaque port L2 du bridge-domain.
- L'IP rapide reroutent (FRR)
- NetFlow
- MoFRR (la Multidiffusion seulement rapide reroutent)
- Commutation de mpls label
- mVPNv4
- Qualité de service (QoS)
- Mise en miroir du trafic
- Interface non numérotée pour BVI
- Surveillance vidéo (Vidmon)

Le BVI peut être dans une configuration de Virtual Routing and Forwarding (VRF), de sorte que le trafic reçu sur le BVI soit expédié au-dessus du MPLS, mais le *label-allocation-mode de par-vrf* doit être utilisé.

Si une de ces caractéristiques restreintes est exigée, vous ne pouvez pas utiliser un BVI. Une autre solution est d'utiliser un câble de bouclage externe entre deux ports sur le routeur, où un port est dans le bridge-domain et un port est configuré comme interface conduite par normale où toutes les caractéristiques peuvent être configurées.

4.4 VPLS

4.4.1 Aperçu

VPLS fournit la capacité de combiner des bridges-domain aux plusieurs sites dans un grand bridge-domain par MPLS PWs. Des hôtes aux différents sites semblent être directement connectés au même segment L2 parce que leur trafic est d'une manière transparente encapsulé au-dessus du maillage complet de MPLS PWs entre le siège potentiel d'explosion de L2VPN :

Un maillage complet de PWs est exigé afin de s'assurer que chaque hôte peut recevoir le trafic de tous autres hôtes. La conséquence est qu'un PE de L2VPN n'expédie pas une trame reçue sur un VPLS picowatt au-dessus de son autre VPLS PWs. Il devrait y a un maillage complet de PWs, ainsi chaque PE reçoit le trafic directement et n'a pas besoin d'expédier le trafic entre PWs puisque la transmission entraînerait une boucle. Ceci s'appelle la règle fendue d'horizon.

Le routeur est apprendre courant de MAC. Une fois qu'une adresse MAC est présente dans la MAC-adresse-table, vous expédiez seulement la trame pour cette adresse MAC de destination au-dessus du picowatt au PE de L2VPN d'où cette adresse MAC a été apprise. Ceci évite la duplication inutile du trafic au centre. Des émissions et les Multidiffusions sont inondées au-dessus de tout le PWs afin de s'assurer que tous les hôtes peuvent les recevoir. Une caractéristique telle que la surveillance IGMP est utile parce qu'elle permet des trames de Multidiffusion à envoyer au siège potentiel d'explosion seulement où il y a des récepteurs ou des routeurs multidiffusion. Ceci réduit le niveau de trafic au centre, bien qu'il y ait les copies encore

plusieurs des mêmes paquets qui doivent être envoyés à chaque PE quand il y a intérêt pour ce groupe.

Le maillage complet de PWs doit être configuré sous une instance de transfert virtuelle (VFI) :

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
```

Le PWs configuré sous le VFI sont ceux qui sont entièrement engrenés au centre. Ils font partie du même groupe fendu d'horizon (SHG) afin de s'assurer que des trames reçues sur un picowatt ne sont pas expédiées à un autre picowatt.

Il est possible de configurer l'accès PWs, qui sont considérés un type de courant alternatif et ne sont pas configurés sous le VFI. Voyez la section pour des détails.

La configuration sur router2, router3, et router4 est très semblable, et tous ont les trois autres Routeurs comme voisins sous le VFI.

```
RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain bd-name engineering detail
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
```

```
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (23:06:02 ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is upH-VPLS
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40003; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 234039, sent 7824
bytes: received 16979396, sent 584608
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc0000009
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ----------------------
Label 16049 16042
Group ID 0x5 0x1
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
```

```
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ----------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225481
Create time: 29/05/2013 15:36:17 (00:46:49 ago)
Last time status changed: 29/05/2013 15:57:36 (00:25:29 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 555, sent 285
bytes: received 36308, sent 23064
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc000000a
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ----------------------
Label 16050 16040
Group ID 0x5 0x3
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ----------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225482
Create time: 29/05/2013 15:36:17 (00:46:49 ago)
Last time status changed: 29/05/2013 16:00:56 (00:22:09 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 184, sent 158
bytes: received 12198, sent 14144
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc000000b
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ----------------------
Label 16051 289974
```

```
Group ID 0x5 0x6
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ----------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225483
Create time: 29/05/2013 15:36:17 (00:46:49 ago)
Last time status changed: 29/05/2013 16:02:38 (00:20:27 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 137
bytes: received 0, sent 12064
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
```

L'étiquette locale pour le picowatt à 10.0.0.12 est 16049, ainsi il signifie que des trames Ethernet sont reçues avec l'étiquette 16049. La décision de commutation est basée sur ces mpls label parce que le saut pénultième MPLS devrait avoir sauté l'étiquette d'IGP. Il pourrait encore y a une étiquette d'Étiqette Explicit Null, mais la décision de commutation est basée sur l'étiquette picowatt :

```
RP/0/RSP0/CPU0:router1#sh mpls forwarding labels 16049
Local Outgoing Prefix Outgoing Next Hop Bytes
Label Label or ID Interface Switched
------ ----------- ----------------- ------------ --------------- ----------
16049 Pop PW(10.0.0.12:2) BD=5 point2point 58226
```

Les étiquettes de show mpls forwarding commandent pour l'étiquette donne le nombre de bridge-domain, que vous pouvez utiliser afin de trouver le mac-address de destination et le picowatt (voisin et picowatt-id) où le paquet a été reçu. Vous pouvez alors créer les entrées dans la MAC-adresse-table qui se dirigent à ce voisin :

```
RP/0/RSP0/CPU0:router1#sh l2vpn forwarding bridge-domain customer1:
engineering mac-address location 0/1/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0024.985e.6a01 dynamic (10.0.0.12, 2) 0/1/CPU0 0d 0h 0m 0s N/A
0024.985e.6a42 dynamic (10.0.0.12, 2) 0/1/CPU0 0d 0h 0m 0s N/A
001d.4603.1f42 dynamic (10.0.0.13, 2) 0/1/CPU0 0d 0h 0m 0s N/A
```

Types 4.4.2 picowatts et balises transportées

VPLS PWs sont négociés comme type 5 (des Ethernets) PWs par défaut. Celui qui entre dans le courant alternatif après n'importe quelle manipulation de balise VLAN (quand la commande de **réécriture** est configurée) est envoyé au-dessus du picowatt.

La version 4.1.0 de Logiciel Cisco IOS XR pour la signalisation LDP et relâchent 4.3.1 avec le BGP vous a permis de configurer une picowatt-classe sous un voisin et de configurer la **fonction émulation de VLAN de mode de transport** sous la picowatt-classe. Ceci négocie une connexion virtuelle (circuit virtuel) 4 (VLAN Ethernet) picowatts de type, qui transporte celui qui sorte du courant alternatif après la manipulation de balise VLAN quand la commande de **réécriture** est configurée.

La manipulation de balise VLAN sur l'EFP s'assure qu'il y a au moins une balise VLAN laissée sur la trame parce que vous avez besoin d'une balise dot1q sur la trame s'il y a Circuit virtuel-type 4 PWs. Aucune balise factice 0 n'est ajoutée à la trame quand vous utilisez le mode de **fonction émulation de VLAN de mode de transport**.

Un mélange du type 4 et du type 5 PWs sous le même VFI n'est pas pris en charge. Tout le PWs doit être du même type.

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
pw-class VC4-PT
!
neighbor 10.0.0.13 pw-id 2
pw-class VC4-PT
!
neighbor 10.0.0.14 pw-id 2
pw-class VC4-PT
!
!
!
!
!

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain bd-name engineering detail |
i "PW:|PW type"
MAC withdraw for Access PW: enabled
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
PW type Ethernet VLAN, control word disabled, interworking none
PW type Ethernet VLAN Ethernet VLAN
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
PW type Ethernet VLAN, control word disabled, interworking none
PW type Ethernet VLAN Ethernet VLAN
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
PW type Ethernet VLAN, control word disabled, interworking none
PW type Ethernet VLAN Ethernet VLAN
```

4.4.3 Autodiscovery et signalisation

Ont été basés sur la configuration manuelle de tous les voisins sous le VFI. MPLS LDP a été utilisé pour la signalisation du picowatt avec les [exemples neighbor.previous]

Quand vous ajoutez un nouveau PE VPLS au réseau, configurez le PE afin d'avoir un picowatt à tout le siège potentiel d'explosion existant dans chacun de ses bridges-domain locaux. Tout le siège potentiel d'explosion existant doit alors être modifié afin d'avoir un picowatt au nouveau PE

parce que tout le siège potentiel d'explosion doit être entièrement engrené. Ceci pourrait devenir un défi opérationnel à mesure que le nombre de siège potentiel d'explosion et les bridges-domain augmentent.

Une solution est de faire découvrir le siège potentiel d'explosion l'autre siège potentiel d'explosion automatiquement par le BGP. Tandis qu'il y a également une condition requise de maillage global pour IBGP, il peut être soulevé en employant des artère-réflecteurs. Ainsi, un nouveau PE est typiquement configuré afin de scruter avec un nombre restreint d'artère-réflecteurs, tout autre siège potentiel d'explosion reçoivent ses mises à jour, et le nouveau PE reçoit les mises à jour de l'autre siège potentiel d'explosion.

Afin de découvrir l'autre siège potentiel d'explosion par le BGP, chaque PE est configuré pour l'*address-family de vpls-vpws* et annonce dans le BGP les bridges-domain en lesquels ils veulent participer. Une fois que l'autre siège potentiel d'explosion qui font partie du même bridge-domain sont découverts, un picowatt est établi à chacun d'eux. Le BGP est le protocole utilisé pour cet autodiscovery.

Il y a deux options pour la signalisation du picowatt au siège potentiel d'explosion autodiscovered : BGP et LDP. Dans ces exemples, vous convertissez la topologie précédente en autodiscovery BGP avec la signalisation BGP et la signalisation LDP.

Autodiscovery BGP de 4.4.3.1 et signalisation BGP

Configurez les **vpls-vpws d'address-family l2vpn** sous le BGP de routeur et les voisins, qui sont l'autre siège potentiel d'explosion ou les artère-réflecteurs :

```
router bgp 65000
address-family l2vpn vpls-vpws
!
neighbor-group IOX-LAB-RR
address-family l2vpn vpls-vpws
!
neighbor 10.0.0.3
use neighbor-group IOX-LAB-RR
!
neighbor 10.0.0.10
use neighbor-group IOX-LAB-RR
!
```

Le nouvel address-family devient actif avec les voisins, mais aucun PE n'a encore annoncé sa participation à un bridge-domain :

```
RP/0/RSP0/CPU0:router1#sh bgp neighbor 10.0.0.3 | i Address family L2VPN
Address family L2VPN VPLS: advertised and received

P/0/RSP0/CPU0:router1#sh bgp l2vpn vpls summary
BGP router identifier 10.0.0.11, local AS number 65000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0 RD version: 3890838096
BGP main routing table version 77
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.


Process RcvTblVer bRIB/RIB LabelVer ImportVer SendTblVer StandbyVer
```

```
Speaker 77 77 77 77 77 77

Neighbor Spk AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down St/PfxRcd
10.0.0.3 0 65000 252950 53252 77 0 0 1w0d 0
10.0.0.10 0 65000 941101 47439 77 0 0 00:10:18 0
```

Configurez le **BGP d'autodiscovery** et le **BGP de protocole de signalisation** sous le mode de configuration de bridge-domain de L2VPN. La configuration sur router1 est :

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
vpn-id 3
autodiscovery bgp
rd auto
route-target 0.0.0.1:3
signaling-protocol bgp
ve-id 11
!
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
vpn-id 2
autodiscovery bgp
rd auto
route-target 0.0.0.1:2
signaling-protocol bgp
ve-id 11
!
!
!
!
!
!
```

La configuration sur router2 est :

```
RP/0/RSP1/CPU0:router2#sh run l2vpn bridge group customer1
Thu May 30 15:25:55.638 CEST
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/0/0/1.3
!
vfi customer1-finance
vpn-id 3
autodiscovery bgp
rd auto
route-target 0.0.0.1:3
signaling-protocol bgp
ve-id 13
!
!
!
!
bridge-domain engineering
```

```
interface GigabitEthernet0/0/0/1.2
!
vfi customer1-engineering
vpn-id 2
autodiscovery bgp
rd auto
route-target 0.0.0.1:2
signaling-protocol bgp
ve-id 13
!
!
!
!
!
!
```

Le vpn id et le route-target sont identique sur le siège potentiel d'explosion différent pour chaque bridge-domain, mais chaque PE a un seul identifiant virtuel de périphérie (VE-ID). Chaque PE découvre l'autre siège potentiel d'explosion dans le VPN par le BGP et emploie le BGP afin de signaler le PWs. Le résultat est un maillage complet de PWs :

```
RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls summary
BGP router identifier 10.0.0.11, local AS number 65000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0 RD version: 3890838096
BGP main routing table version 103
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.


Process RcvTblVer bRIB/RIB LabelVer ImportVer SendTblVer StandbyVer
Speaker 103 103 103 103 103 103

Neighbor Spk AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down St/PfxRcd
10.0.0.3 0 65000 254944 53346 103 0 0 1w0d 6
10.0.0.10 0 65000 944859 47532 103 0 0 01:40:22 6

RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls
BGP router identifier 10.0.0.11, local AS number 65000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0 RD version: 3890838096
BGP main routing table version 103
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
i - internal, r RIB-failure, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Rcvd Label Local Label
Route Distinguisher: 10.0.0.11:32769 (default for vrf customer1:finance)
*> 11:10/32 0.0.0.0 nolabel 16060
*>i12:10/32 10.0.0.12 16060 nolabel
*>i13:10/32 10.0.0.13 16060 nolabel
*>i14:10/32 10.0.0.14 289959 nolabel
Route Distinguisher: 10.0.0.11:32770 (default for vrf customer1:engineering)
*> 11:10/32 0.0.0.0 nolabel 16075
*>i12:10/32 10.0.0.12 16075 nolabel
*>i13:10/32 10.0.0.13 16075 nolabel
*>i14:10/32 10.0.0.14 289944 nolabel
Route Distinguisher: 10.0.0.12:32768
*>i12:10/32 10.0.0.12 16060 nolabel
* i 10.0.0.12 16060 nolabel
```

```
Route Distinguisher: 10.0.0.12:32769
*>i12:10/32 10.0.0.12 16075 nolabel
* i 10.0.0.12 16075 nolabel
Route Distinguisher: 10.0.0.13:32769
*>i13:10/32 10.0.0.13 16060 nolabel
* i 10.0.0.13 16060 nolabel
Route Distinguisher: 10.0.0.13:32770
*>i13:10/32 10.0.0.13 16075 nolabel
* i 10.0.0.13 16075 nolabel
Route Distinguisher: 10.0.0.14:32768
*>i14:10/32 10.0.0.14 289959 nolabel
* i 10.0.0.14 289959 nolabel
Route Distinguisher: 10.0.0.14:32769
*>i14:10/32 10.0.0.14 289944 nolabel
* i 10.0.0.14 289944 nolabel

Processed 14 prefixes, 20 paths
```

Ce sont les préfixes annoncés par router3 (10.0.0.13) comme vu sur router1 ; les préfixes sont reçus par les deux artère-réflecteurs, 10.0.0.3 et 10.0.0.10 :

```
RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls rd 10.0.0.13:32770 13:10/32
BGP routing table entry for 13:10/32, Route Distinguisher: 10.0.0.13:32770
Versions:
Process bRIB/RIB SendTblVer
Speaker 92 92
Last Modified: May 30 15:10:44.100 for 01:23:38
Paths: (2 available, best #1)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
10.0.0.13 (metric 5) from 10.0.0.3 (10.0.0.13)
Received Label 16075
Origin IGP, localpref 100, valid, internal, best, group-best,
import-candidate, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 1, version 92
Extended community: RT:0.0.0.1:2 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.3
Block Size:10
Path #2: Received by speaker 0
Not advertised to any peer
Local
10.0.0.13 (metric 5) from 10.0.0.10 (10.0.0.13)
Received Label 16075
Origin IGP, localpref 100, valid, internal, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 0, version 0
Extended community: RT:0.0.0.1:2 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.10
Block Size:10
RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls rd 10.0.0.13:32769 13:10/32
BGP routing table entry for 13:10/32, Route Distinguisher: 10.0.0.13:32769
Versions:
Process bRIB/RIB SendTblVer
Speaker 93 93
Last Modified: May 30 15:10:44.100 for 01:25:02
Paths: (2 available, best #1)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
10.0.0.13 (metric 5) from 10.0.0.3 (10.0.0.13)
Received Label 16060
Origin IGP, localpref 100, valid, internal, best, group-best,
```

```
import-candidate, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 1, version 93
Extended community: RT:0.0.0.1:3 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.3
Block Size:10
Path #2: Received by speaker 0
Not advertised to any peer
Local
10.0.0.13 (metric 5) from 10.0.0.10 (10.0.0.13)
Received Label 16060
Origin IGP, localpref 100, valid, internal, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 0, version 0
Extended community: RT:0.0.0.1:3 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.10
Block Size:10
```

Router1 a établi un certain PWs :

```
RP/0/RSP0/CPU0:router1#sh l2vpn discovery bridge-domain

Service Type: VPLS, Connected
List of VPNs (2 VPNs):
Bridge group: customer1, bridge-domain: finance, id: 3, signaling
protocol: BGP
List of Local Edges (1 Edges):
Local Edge ID: 11, Label Blocks (1 Blocks)
Label base Offset Size Time Created
---------- ------ ---- -------------------
16060 10 10 05/30/2013 15:07:39
List of Remote Edges (3 Edges):
Remote Edge ID: 12, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created
---------- ------ ---- ------------ -------------------
16060 10 10 10.0.0.12 05/30/2013 15:09:53
Remote Edge ID: 13, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created
---------- ------ ---- ------------ -------------------
16060 10 10 10.0.0.13 05/30/2013 15:10:43
Remote Edge ID: 14, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created
---------- ------ ---- ------------ -------------------
289959 10 10 10.0.0.14 05/30/2013 15:11:22

Bridge group: customer1, bridge-domain: engineering, id: 5, signaling
protocol: BGP
List of Local Edges (1 Edges):
Local Edge ID: 11, Label Blocks (1 Blocks)
Label base Offset Size Time Created
---------- ------ ---- -------------------
16075 10 10 05/30/2013 15:08:54
List of Remote Edges (3 Edges):
Remote Edge ID: 12, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created
---------- ------ ---- ------------ -------------------
16075 10 10 10.0.0.12 05/30/2013 15:09:53
Remote Edge ID: 13, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created
---------- ------ ---- ------------ -------------------
16075 10 10 10.0.0.13 05/30/2013 15:10:43
Remote Edge ID: 14, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created
---------- ------ ---- ------------ -------------------
289944 10 10 10.0.0.14 05/30/2013 15:11:22
```

```
RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain autodiscovery bgp
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain group customer1
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.3, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain group customer1 detail
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
```

```
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 4
Filter MAC addresses:
Create time: 29/05/2013 15:36:17 (1d01h ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.3, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [3, 3]
MTU 1500; XC ID 0xc40006; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 10120, sent 43948
bytes: received 933682, sent 2989896
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
VPN-ID: 3, Auto Discovery: BGP, state is Provisioned
(Service Connected)
Route Distinguisher: (auto) 10.0.0.11:32769
Import Route Targets:
0.0.0.1:3
Export Route Targets:
0.0.0.1:3
Signaling protocol: BGP
Local VE-ID: 11 , Advertised Local VE-ID : 11
VE-Range: 10
PW: neighbor 10.0.0.12, PW ID 3, state is up ( established )
PW class not set, XC ID 0xc000000c
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
```

```
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote
------------ ------------------------------ ------------------
Label 16062 16061
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 12
------------ ------------------------------ ------------------
MIB cpwVcIndex: 3221225484
Create time: 30/05/2013 15:09:52 (01:29:44 ago)
Last time status changed: 30/05/2013 15:09:52 (01:29:44 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 2679, sent 575
bytes: received 171698, sent 51784
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 3, state is up ( established )
PW class not set, XC ID 0xc000000e
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote
------------ ------------------------------ ------------------
Label 16063 16061
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 13
------------ ------------------------------ ------------------
MIB cpwVcIndex: 3221225486
Create time: 30/05/2013 15:10:43 (01:28:54 ago)
Last time status changed: 30/05/2013 15:10:43 (01:28:54 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 11, sent 574
bytes: received 1200, sent 51840
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 3, state is up ( established )
PW class not set, XC ID 0xc0000010
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote
------------ ------------------------------ ------------------
Label 16064 289960
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 14
------------ ------------------------------ ------------------
```

```
MIB cpwVcIndex: 3221225488
Create time: 30/05/2013 15:11:22 (01:28:15 ago)
Last time status changed: 30/05/2013 15:11:22 (01:28:15 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 561
bytes: received 0, sent 50454
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (1d23h ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40007; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 243532, sent 51089
bytes: received 17865888, sent 3528732
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
```

```
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
VPN-ID: 2, Auto Discovery: BGP, state is Provisioned
(Service Connected)
Route Distinguisher: (auto) 10.0.0.11:32770
Import Route Targets:
0.0.0.1:2
Export Route Targets:
0.0.0.1:2
Signaling protocol: BGP
Local VE-ID: 11 , Advertised Local VE-ID : 11
VE-Range: 10
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc000000d
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote
------------ ------------------------------ ------------------
Label 16077 16076
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 12
------------ ------------------------------ ------------------
MIB cpwVcIndex: 3221225485
Create time: 30/05/2013 15:09:52 (01:29:45 ago)
Last time status changed: 30/05/2013 15:09:52 (01:29:45 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 2677, sent 574
bytes: received 171524, sent 51670
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc000000f
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote
------------ ------------------------------ ------------------
Label 16078 16076
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 13
------------ ------------------------------ ------------------
MIB cpwVcIndex: 3221225487
Create time: 30/05/2013 15:10:43 (01:28:54 ago)
Last time status changed: 30/05/2013 15:10:43 (01:28:54 ago)
MAC withdraw message: send 0 receive 0
```

```
Static MAC addresses:
Statistics:
packets: received 17, sent 572
bytes: received 1560, sent 51636
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc0000011
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote
------------ ------------------------------ ------------------
Label 16079 289945
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 14
------------ ------------------------------ ------------------
MIB cpwVcIndex: 3221225489
Create time: 30/05/2013 15:11:22 (01:28:16 ago)
Last time status changed: 30/05/2013 15:11:22 (01:28:16 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 559
bytes: received 0, sent 50250
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
```

Autodiscovery BGP de 4.4.3.2 et signalisation LDP

La configuration BGP avec la commande de **vpls-vpws d'address-family l2vpn** est exactement identique qu'avec la signalisation BGP. La configuration de L2VPN est modifiée afin d'utiliser la signalisation LDP avec la commande de **LDP de protocole de signalisation**.

La même configuration est utilisée sur chacun des siège potentiel d'explosion quatre :

```
router bgp 65000
address-family l2vpn vpls-vpws
!
neighbor-group IOX-LAB-RR
address-family l2vpn vpls-vpws
!
neighbor 10.0.0.3
use neighbor-group IOX-LAB-RR
!
neighbor 10.0.0.10
use neighbor-group IOX-LAB-RR
!
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
```

```
vpn-id 3
autodiscovery bgp
rd auto
route-target 0.0.0.1:3
signaling-protocol ldp
vpls-id 65000:3
!
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
vpn-id 2
autodiscovery bgp
rd auto
route-target 0.0.0.1:2
signaling-protocol ldp
 vpls-id 65000:2
!
!
!
!
!
!
```

Le vpls-id est fait du nombre de système autonome (AS) BGP et du vpn id.

Trois commandes show de router1 illustrent que le PWs ont été établis avec le siège potentiel d'explosion découvert :

```
RP/0/RSP0/CPU0:router1#sh l2vpn discovery

Service Type: VPLS, Connected
List of VPNs (2 VPNs):
Bridge group: customer1, bridge-domain: finance, id: 3,
signaling protocol: LDP
VPLS-ID: 65000:3
Local L2 router id: 10.0.0.11
List of Remote NLRI (3 NLRIs):
Local Addr Remote Addr Remote L2 RID Time Created
--------------- --------------- --------------- -------------------
10.0.0.11 10.0.0.12 10.0.0.12 05/30/2013 17:10:18
10.0.0.11 10.0.0.13 10.0.0.13 05/30/2013 17:10:18
10.0.0.11 10.0.0.14 10.0.0.14 05/30/2013 17:11:46

Bridge group: customer1, bridge-domain: engineering, id: 5,
signaling protocol: LDP
VPLS-ID: 65000:2
Local L2 router id: 10.0.0.11
List of Remote NLRI (3 NLRIs):
Local Addr Remote Addr Remote L2 RID Time Created
--------------- --------------- --------------- -------------------
10.0.0.11 10.0.0.12 10.0.0.12 05/30/2013 17:10:18
10.0.0.11 10.0.0.13 10.0.0.13 05/30/2013 17:10:18
10.0.0.11 10.0.0.14 10.0.0.14 05/30/2013 17:11:46

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain group customer1
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
```

```
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.3, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.12 pw-id 65000:3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 65000:3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 65000:3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.12 pw-id 65000:2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 65000:2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 65000:2, state: up, Static MAC addresses: 0

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain group customer1 det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 4
Filter MAC addresses:
Create time: 29/05/2013 15:36:17 (1d01h ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.3, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [3, 3]
MTU 1500; XC ID 0xc40006; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
```

```
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 10362, sent 45038
bytes: received 956240, sent 3064016
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
VPN-ID: 3, Auto Discovery: BGP, state is Provisioned
(Service Connected)
Route Distinguisher: (auto) 10.0.0.11:32769
Import Route Targets:
0.0.0.1:3
Export Route Targets:
0.0.0.1:3
Signaling protocol: LDP
AS Number: 65000
VPLS-ID: 65000:3
L2VPN Router ID: 10.0.0.11
PW: neighbor 10.0.0.12, PW ID 65000:3, state is up ( established )
PW class not set, XC ID 0xc0000003
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------
Label 16006 16033
BGP Peer ID 10.0.0.11 10.0.0.12
LDP ID 10.0.0.11 10.0.0.12
AII 10.0.0.11 10.0.0.12
AGI 65000:3 65000:3
Group ID 0x3 0x0
Interface customer1-finance customer1-finance
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225475
Create time: 30/05/2013 17:10:18 (00:06:32 ago)
Last time status changed: 30/05/2013 17:10:24 (00:06:25 ago)
```

```
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 190, sent 40
bytes: received 12160, sent 3600
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 65000:3, state is up ( established )
PW class not set, XC ID 0xc0000004
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------
Label 16016 16020
BGP Peer ID 10.0.0.11 10.0.0.13
LDP ID 10.0.0.11 10.0.0.13
AII 10.0.0.11 10.0.0.13
AGI 65000:3 65000:3
Group ID 0x3 0x4
Interface customer1-finance customer1-finance
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225476
Create time: 30/05/2013 17:10:18 (00:06:32 ago)
Last time status changed: 30/05/2013 17:10:27 (00:06:22 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 40
bytes: received 0, sent 3600
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 65000:3, state is up ( established )
PW class not set, XC ID 0xc0000009
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------
Label 16049 289970
BGP Peer ID 10.0.0.11 10.0.0.14
LDP ID 10.0.0.11 10.0.0.14
AII 10.0.0.11 10.0.0.14
AGI 65000:3 65000:3
Group ID 0x3 0x4
Interface customer1-finance customer1-finance
```

```
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225481
Create time: 30/05/2013 17:11:46 (00:05:04 ago)
Last time status changed: 30/05/2013 17:11:51 (00:04:59 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 31
bytes: received 0, sent 2790
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (1d23h ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40007; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
```

```
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 243774, sent 52179
bytes: received 17888446, sent 3602852
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
VPN-ID: 2, Auto Discovery: BGP, state is Provisioned (Service Connected)
Route Distinguisher: (auto) 10.0.0.11:32770
Import Route Targets:
0.0.0.1:2
Export Route Targets:
0.0.0.1:2
Signaling protocol: LDP
AS Number: 65000
VPLS-ID: 65000:2
L2VPN Router ID: 10.0.0.11
PW: neighbor 10.0.0.12, PW ID 65000:2, state is up ( established )
PW class not set, XC ID 0xc0000005
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------
Label 16027 16042
BGP Peer ID 10.0.0.11 10.0.0.12
LDP ID 10.0.0.11 10.0.0.12
AII 10.0.0.11 10.0.0.12
AGI 65000:2 65000:2
Group ID 0x5 0x1
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 0
Create time: 30/05/2013 17:10:18 (00:06:33 ago)
Last time status changed: 30/05/2013 17:10:24 (00:06:26 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
```

```
packets: received 190, sent 41
bytes: received 12160, sent 3690
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 65000:2, state is up ( established )
PW class not set, XC ID 0xc0000006
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------
Label 16043 16021
BGP Peer ID 10.0.0.11 10.0.0.13
LDP ID 10.0.0.11 10.0.0.13
AII 10.0.0.11 10.0.0.13
AGI 65000:2 65000:2
Group ID 0x5 0x3
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 0
Create time: 30/05/2013 17:10:18 (00:06:33 ago)
Last time status changed: 30/05/2013 17:10:27 (00:06:23 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 40
bytes: received 0, sent 3600
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 65000:2, state is up ( established )
PW class not set, XC ID 0xc000000a
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------
Label 16050 289974
BGP Peer ID 10.0.0.11 10.0.0.14
LDP ID 10.0.0.11 10.0.0.14
AII 10.0.0.11 10.0.0.14
AGI 65000:2 65000:2
Group ID 0x5 0x6
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
```

```
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225482
Create time: 30/05/2013 17:11:46 (00:05:05 ago)
Last time status changed: 30/05/2013 17:11:51 (00:05:00 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 31
bytes: received 0, sent 2790
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
```

4.4.4 Annulations et retraits de MAC

L'expédition dans VPLS est basé sur la MAC-adresse-table, qui est dynamiquement construite en apprenant les adresses MAC sources des trames étant reçues. S'il y a un changement de topologie d'un bridge-domain, un hôte pourrait devenir accessible par un voisin différent à C.A. ou VPLS. Trafiquez pour cet hôte ne pourrait pas atteindre sa destination si des trames continuent à être expédiées selon la MAC-adresse-table existante.

Pour un PE de L2VPN, il y a de plusieurs manières de détecter une modification de topologie :

- Un port dans le bridge-domain va en haut ou en bas.
- Une notification de modification de topologie de spanning tree (TCN) BPDU est traitée quand le PE de L2VPN exécute l'implémentation intégrale MST ou un protocole de passerelle d'accès de spanning-tree. Le lien manquant ne pourrait pas être local sur le PE mais pourrait être plus loin parti dans la topologie. Le PE intercepte le TCN.

Quand un PE de L2VPN détecte une modification de topologie, il prend deux mesures :

1. Le PE vide la MAC-adresse-table des bridges-domain affectés par la modification de topologie. Quand le PE est configuré pour la passerelle PVSTAG ou Par-VLAN Rapid Spanning Tree Access (PVRSTAG), un TCN BPDU détecté dans une sous-interface VLAN affecte tous les VLAN et bridges-domain sur cette interface physique.
2. Le PE signale aux voisins VPLS par un message de retrait de MAC MPLS LDP qu'ils devraient vider leur MAC-adresse-table. Tout le siège potentiel d'explosion distant de L2VPN recevant l'annulation de message du retrait LDP de MAC leurs MAC-adresse-tables, et trafic est inondé de nouveau. Les mac-adresse-tables sont reconstruites ont basé sur la nouvelle topologie.

Le comportement par défaut du message de retrait de MAC en cas d'instabilité de port a changé au fil du temps :

- Traditionnellement dans le Logiciel Cisco IOS XR, un PE de L2VPN a envoyé des messages de retrait de MAC quand un courant alternatif allait vers le bas. L'intention était de faire vider le siège potentiel d'explosion distant leurs tables d'adresse MAC pour le bridge-domain

affecté de sorte que les adresses MAC se dirigeant derrière le port avalé soient apprises d'un autre port.

- Cependant, ceci a créé un problème d'interopérabilité avec un certain siège potentiel d'explosion distant qui suivent RFC 4762 et purge les adresses MAC qui se dirigent à tout le siège potentiel d'explosion excepté celui qui envoie le message de retrait de MAC. RFC 4762 suppose qu'un PE enverrait un message de retrait de MAC quand un courant alternatif est soulevé mais pas quand un courant alternatif descend. Après que la version 4.2.1 de Logiciel Cisco IOS XR, le comportement par défaut soit d'envoyer des messages de retrait de MAC LDP seulement quand un port de bridge-domain monte afin d'être conforme mieux au RFC. Une commande de configuration a été ajoutée afin de retourner au vieux comportement.

C'est une commande show avec le comportement par défaut après que la version 4.2.1 de Logiciel Cisco IOS XR :

```
RP/0/RSP1/CPU0:router3#sh l2vpn bridge-domain bd-name engineering det |
i "PW:|VFI|neighbor|MAC w"
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.11, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 0
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 4
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 2
VFI Statistics:
```

L'importante ligne est le « MAC retirent vers le bas en fonction envoyé le port de passerelle, » qui est maintenant désactivé par défaut après que la version 4.2.1 de Logiciel Cisco IOS XR. La commande donne également le nombre de messages de retrait de MAC envoyés et reçus dans le bridge-domain. Un nombre élevé de messages de retrait indique l'instabilité dans le bridge-domain.

C'est la configuration qui retourne au vieux comportement :

```
l2vpn
bridge group customer1
bridge-domain finance
mac
withdraw state-down
!
!
!
!
```

4.4.5 H-VPLS

VPLS exige d'un maillage complet de PWs entre le siège potentiel d'explosion de L2VPN afin de s'assurer que n'importe quel PE peut atteindre, en un saut, un hôte derrière n'importe quel autre PE sans besoin d'un PE de refléter des trames d'un picowatt à un autre picowatt. Ce sert de base à la règle fendue d'horizon, qui empêche un PE des trames d'expédition d'un picowatt à un autre picowatt. Même dans des cas particuliers, où l'adresse MAC de destination dans la MAC-adresse-table se dirige à un autre picowatt, la trame est abandonnée.

Un maillage complet de PWs signifie que le nombre de PWs pourrait devenir très tout élevé que le nombre de siège potentiel d'explosion se développe, ainsi ceci pourrait introduire des problèmes d'évolutivité.

Vous pouvez diminuer le nombre de PWs dans cette topologie avec une hiérarchie de siège potentiel d'explosion :

Dans cette topologie, notez cela :

- Un périphérique du Provider Edge d'utilisateur (U-PE) a ACs au ces.
- Le périphérique U-PE transporte le trafic de la CE au-dessus d'un Point à point picowatt MPLS à un périphérique de la périphérie de fournisseur de services réseau (N-PE).
- Le N-PE est un PE du noyau VPLS qui est entièrement engrené avec l'autre N-siège potentiel d'explosion.
- Sur le N-PE, le picowatt provenant l'U-PE est considéré un accès picowatt tout comme un courant alternatif. L'U-PE n'est pas une partie de la maille avec l'autre N-siège potentiel d'explosion, ainsi le N-PE peut considérer l'accès picowatt comme courant alternatif et le trafic en avant de cet accès picowatt au noyau PWs qui font partie du maillage complet VPLS.
- Le principal PWs entre le N-siège potentiel d'explosion sont configurés sous un VFI afin de s'assurer que la règle fendue d'horizon est appliquée à tout le principal PWs configuré sous le VFI.
- Access PWs d'U-siège potentiel d'explosion ne sont pas configurés sous un VFI, ainsi ils n'appartiennent pas au même SHG que le VFI PWs. Le trafic peut être expédié d'un accès picowatt à un VFI picowatt et vice versa.
- L'U-siège potentiel d'explosion peut employer la caractéristique de Redondance picowatt afin d'avoir un picowatt primaire à un N-PE primaire et avoir un standby picowatt à un standby N-PE. Le standby succède quand le picowatt primaire descend.

C'est un exemple où U-PE1 (10.0.0.15) est configuré avec la Redondance picowatt à N-PE1 (10.0.0.11) et à N-PE2 (10.0.0.12) :

```
RP/0/RP0/CPU0:U-PE1#sh run int ten 0/1/0/5.2
interface TenGigE0/1/0/5.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!

RP/0/RP0/CPU0:U-PE1#sh run l2vpn xconnect group customer1
l2vpn
xconnect group customer1
p2p engineering-0-1-0-5
interface TenGigE0/1/0/5.2
neighbor 10.0.0.11 pw-id 15
backup neighbor 10.0.0.12 pw-id 15
!
!
!
!
!

RP/0/RP0/CPU0:U-PE1#sh l2vpn xconnect group customer1
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
```

```
---------------------- ---------------------- ----------------------------
customer1 engineering-0-1-0-5
UP Te0/1/0/5.2 UP 10.0.0.11 15 UP
Backup
10.0.0.12 15 SB
--------------------------------------------------------------------------------
```

Le picowatt à 10.0.0.12 est dans l'état de réserve. Sur N-PE1, il y a un accès picowatt à 10.0.0.15 et un courant alternatif qui ne sont pas sous le VFI.

N-PE1 apprend quelques adresses MAC au-dessus de l'accès picowatt et le VFI PWs :

```
RP/0/RSP0/CPU0:N-PE1#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
neighbor 10.0.0.15 pw-id 15
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
RP/0/RSP0/CPU0:N-PE1#sh l2vpn bridge-domain bd-name engineering
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 4 (4 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
List of Access PWs:
Neighbor 10.0.0.15 pw-id 15, state: up, Static MAC addresses: 0
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
RP/0/RSP0/CPU0:N-PE1#sh l2vpn forwarding bridge-domain customer1:engineering
mac-address location 0/0/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
--------------------------------------------------------------------------------
6c9c.ed3e.e46d dynamic (10.0.0.15, 15) 0/0/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
0024.985e.6a42 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f42 dynamic (10.0.0.13, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

Sur N-PE2 (10.0.0.12), l'accès picowatt est dans l'état de réserve :

```
RP/0/RSP0/CPU0:N-PE2#sh run l2vpn bridge group customer1 bridge-domain
engineering
```

```
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
neighbor 10.0.0.15 pw-id 15
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
RP/0/RSP0/CPU0:N-PE2#sh l2vpn bridge-domain bd-name engineering
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 1, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 4 (3 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
List of Access PWs:
Neighbor 10.0.0.15 pw-id 15, state: standby, Static MAC addresses: 0
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.11 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
```

4.4.6 Groupes fendus d'horizon (SHGs)

La règle fendue d'horizon dicte qu'une trame reçue sur un VFI picowatt ne peut pas être expédiée au-dessus d'un autre VFI picowatt. Le N-siège potentiel d'explosion VFI devrait être entièrement engrené.

Cet horizon fendu est imposé par un SHG :

- Les membres d'un SHG ne peuvent pas expédier des trames entre eux, mais peuvent expédier des trames aux membres de l'autre SHGs.
- Tous les VFI PWs sont assignés au par défaut de 1par SHG. Ceci s'assure qu'il n'y a aucun expédition entre VFI PWs de sorte que la règle fendue d'horizon soit imposée. Des paquets reçus sur un VFI picowatt peuvent être expédiés à ACs et à accès PWs parce qu'ils ne sont pas une partie du même SHG.
- Tous les ACs et accès PWs ne sont pas une partie d'un groupe SHG par défaut, ainsi il signifie que des paquets reçus sur un courant alternatif ou un accès picowatt peuvent être expédiés à un courant alternatif ou à un accès différent picowatt dans le même bridge-domain.
- ACs et accès PWs peuvent être assignés au SHG 2 avec l'ordre de **groupe de fractionnement-horizon** si le but est d'empêcher expédier entre eux.

```
RP/0/RSP0/CPU0:N-PE1#sh run l2vpn bridge group customer1 bridge-domain
```

```
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
split-horizon group
!
interface GigabitEthernet0/1/0/3.2
split-horizon group
!
neighbor 10.0.0.15 pw-id 15
split-horizon group
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
```

Dans cette configuration, il n'y a aucun expédition entre le Gi 0/0/0/1.2 et le Gi 0/1/0/3.2, le Gi 0/0/0/1.2 et le 10.0.0.15, ou le Gi 0/1/0/3.2 et le 10.0.0.15. Mais il peut encore y avoir d'expédition du trafic entre l'ACs et le VFI PWs parce qu'ils font partie de SHGs différent (1 et 2).

```
RP/0/RSP0/CPU0:N-PE1#sh l2vpn bridge-domain bd-name engineering detail  |
i "state is|List of|VFI|Split"
Split Horizon Group: none
ACs: 2 (1 up), VFIs: 1, PWs: 4 (4 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/0/0/1.2, state is unresolved
Split Horizon Group: enabled
AC: GigabitEthernet0/1/0/3.2, state is up
Split Horizon Group: enabled
List of Access PWs:
PW: neighbor 10.0.0.15, PW ID 15, state is up ( established )
Split Horizon Group: enabled
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
VFI Statistics:
```

4.4.7 Redondance

Afin d'essayer d'introduire la Redondance, vous pourriez avoir un site qui est double relié au domaine VPLS :

Si un hôte connecté à switch1 envoie une émission, switch1 en avant il à router1 et à switch2. Router1 a un maillage complet de PWs, tellement il y a un picowatt à router2, et de router1 en avant l'émission au-dessus de ce picowatt. Router2 en avant l'émission à switch2, qui en avant il à switch1. Ceci a comme conséquence une boucle physique.

Spanning-tree de 4.4.7.1

L'implémentation intégrale MST ne fonctionne pas avec VPLS parce que cette implémentation envoie MST BPDU sur une interface principale afin de contrôler l'état d'expédition de tous les VLAN sur cette interface. Avec VPLS, il y a de VFIs pour chaque bridge-domain, ainsi vous ne pouvez pas envoyer à des BPDU sur une interface principale pour tous les ces VFIs.

Le spanning-tree BPDU sont transportés au-dessus de VPLS et de PWs point par point par défaut.

Si switch1 et switch2 envoient par-VLAN BPDU ou MST non-marqué BPDU et si les BPDU apparient des sous-interfaces de l2transport sur router1 et router2, les BPDU sont transportés par VPLS. Les Commutateurs voient les BPDU de chacun sur les interfaces du Gi 0/1, et le spanning-tree cassent la boucle et bloquent un port.

Est Comm2 la racine pour le VLAN 2 :

```
switch2#sh spanning-tree vlan 2

MST0
Spanning tree enabled protocol mstp
Root ID Priority 32768
Address 0024.985e.6a00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Desg FWD 20000 128.1 P2p Bound(PVST)
Gi0/2 Desg FWD 20000 128.2 P2p Bound(PVST)
```

Switch1 a son port de racine sur le Gi 0/1 et bloque le Gi 0/2 :

```
switch1#sh spanning-tree vlan 2

VLAN0002
Spanning tree enabled protocol ieee
Root ID Priority 32768
Address 0024.985e.6a00
Cost 4
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Root FWD 4 128.1 P2p
Gi0/2 Altn BLK 4 128.2 P2p
```

Le problème est que les BPDU sont également transportés aux sites distants, et instabilité de spanning-tree dans des propagations d'un site à tous les sites connectés au domaine VPLS. Il est plus sûr d'isoler chaque site et de ne pas transporter des BPDU au-dessus de VPLS.

Une solution est utilisation d'une version de passerelle d'accès du STP. C'est une implémentation limitée du protocole, où le siège potentiel d'explosion de L2VPN sont configurés pour envoyer quelques BPDU statiques afin de sembler connecté à la racine de spanning-tree. Le PE de L2VPN ne transporte pas les BPDU reçus du ces aux sites distants, ainsi chaque site a son propre domaine de spanning-tree.

4.4.7.2 MSTAG

Comme expliqué dans la section de spanning-tree, MST envoie le contrôle BPDU non-marqués, mais ces BPDU l'état d'expédition de tous les VLAN sur l'interface.

Des VLAN peuvent être groupés dans des multiples instances, et chaque exemple a son propre état d'expédition.

Des VLAN sont habituellement groupés de sorte que le trafic puisse être propagé même entre les plusieurs chemins. Quand il y a deux chemins, la moitié du trafic appartient à un exemple qui expédie sur le premier chemin et bloque sur le deuxième chemin. L'autre moitié du trafic appartient à un exemple qui bloque sur le premier chemin et expédie sur le deuxième chemin. Ceci tient compte de loadbalancing entre les deux chemins dans des conditions stables. Autrement, vous avez un chemin qui d'habitude est complètement bloqué et devient actif seulement quand le chemin primaire est vers le bas.

Voici une topologie typique MSTAG :

Dans cet exemple de laboratoire, l'exemple 1 a le VLAN 2, et l'exemple 0 a les autres VLAN. (Dans un scénario plus réaliste, des VLAN sont propagés entre la multiple instance afin de réaliser le bon trafic loadbalancing entre les exemples.) Puisque quelques VLAN ont beaucoup plus de trafic que d'autres, il n'y a pas toujours le même nombre de VLAN dans chaque exemple.

C'est la configuration pour l'exemple 0 MST :

- Router1 et router2 envoient quelques BPDU statiques basés sur la configuration MSTAG. Ils ne traitent pas les BPDU entrants du réseau ou les essayent d'exécuter une implémentation complète. Avec MSTAG, le siège potentiel d'explosion du L2VPN deux envoient juste des BPDU statiques basés sur leur configuration MSTAG.
- Router1 est configuré afin d'attirer le trafic de l'exemple 0 en apparaissant à être la racine pour cet exemple.
- Le Router2 est configuré avec la priorité racine de tous les jours par exemple 0, de sorte que ce devienne la nouvelle racine en cas de panne router1 ou de panne à C.A. entre switch1 et router1.
- Comm2 est configuré avec un spanning-tree cost élevé sur le Gi 0/1 de port à router2 afin de s'assurer que son chemin primaire à la racine est sur la yole 0/2 switch1 et router1 traversants.
- Comm2 sélectionne le Gi 0/2 comme port de racine pour instance0 et sélectionne le Gi 0/1 comme port de remplacement au cas où la racine serait perdue.
- Ainsi, le trafic de ce site dans les VLAN appartenant pour citer 0 accède d'autres sites au-dessus de VPLS par router1.

Pour l'exemple 1 MST (VLAN 2), la configuration est renversé :

- Le Router2 est configuré afin d'attirer le trafic du 1par d'exemple semblant être la racine pour cet exemple.
- Router1 est configuré avec la priorité racine de tous les jours par exemple 1, de sorte que ce devienne la nouvelle racine en cas de panne router2 ou de panne à C.A. entre switch2 et router2.
- Switch1 est configuré avec un spanning-tree cost élevé sur le Gi 0/1 de port à router1 afin de s'assurer que son chemin primaire à la racine est sur la yole 0/2 switch2 et router2 traversants.
- Switch1 sélectionne le Gi 0/2 comme port par exemple 1 de racine et sélectionne le Gi 0/1 comme port de remplacement au cas où la racine serait perdue.
- Ainsi, le trafic de ce site dans les VLAN appartenant pour citer 1 (VLAN 2 dans cet exemple) accède d'autres sites au-dessus de VPLS par router2.
- Il doit y a une sous-interface sur router1 et router2 afin d'attraper les TCN non-marqués et les expédier par un Point à point picowatt à l'autre routeur. Puisque switch1 et switch2 pourraient perdre leurs liens directs et devenir d'isolement entre eux, router1 et router2 doivent expédier les TCN entre eux par ce Point à point picowatt.
- Le siège potentiel d'explosion également interceptent les TCN, vident leurs MAC-adresse-tables, et envoient le retrait de MAC LDP au siège potentiel d'explosion distant.

C'est la configuration sur router1 :

```
RP/0/RSP0/CPU0:router1#sh run int gigabitEthernet 0/1/0/3.*
interface GigabitEthernet0/1/0/3.1 l2transport
encapsulation untagged
!
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!

RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
```

```
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!

RP/0/RSP0/CPU0:router1#sh run l2vpn xconnect group customer1
l2vpn
xconnect group customer1
p2p mstag-gi-0-1-0-3
interface GigabitEthernet0/1/0/3.1
neighbor 10.0.0.13 pw-id 103
!
!
!
!

RP/0/RSP0/CPU0:router1#sh run spanning-tree mstag customer1-0-1-0-3
spanning-tree mstag customer1-0-1-0-3
interface GigabitEthernet0/1/0/3.1
name customer1
revision 1
bridge-id 0000.0000.0001
instance 0
root-id 0000.0000.0001
priority 4096
root-priority 4096
!
instance 1
vlan-ids 2
root-id 0000.0000.0002
priority 8192
root-priority 4096
!
!
!

RP/0/RSP0/CPU0:router1#sh spanning-tree mstag customer1-0-1-0-3
GigabitEthernet0/1/0/3.1
Pre-empt delay is disabled
Name: customer1
Revision: 1
Max Age: 20
Provider Bridge: no
Bridge ID: 0000.0000.0001
Port ID: 1
External Cost: 0
Hello Time: 2
Active: yes
BPDUs sent: 3048
MSTI 0 (CIST):
VLAN IDs: 1,3-4094
Role: Designated
Bridge Priority: 4096
Port Priority: 128
Cost: 0
Root Bridge: 0000.0000.0001
Root Priority: 4096
Topology Changes: 369
MSTI 1
VLAN IDs: 2
Role: Designated
```

```
Bridge Priority: 8192
Port Priority: 128
Cost: 0
Root Bridge: 0000.0000.0002
Root Priority: 4096
Topology Changes: 322
```

Dans cette configuration, notez cela :

- Dans l'exemple 0 MST, la passerelle de racine est 0000.0000.0001, qui est l'ID de passerelle de router1.
- Dans l'exemple 1 MST, la passerelle de racine est 0000.0000.0002, qui est l'ID de passerelle de router2.
- La priorité de passerelle de router1 est 4096 dans l'exemple 0 (pour devenir la racine) et 8192 dans l'exemple 1 (pour devenir la racine de tous les jours).
- La priorité de passerelle de router1 est 8192 dans l'exemple 0 (pour devenir la racine de tous les jours) et 4096 dans l'exemple 1 (pour devenir la racine).
- La croix point par point se connectent sur GigabitEthernet0/1/0/3.1 porte le MST non-marqué TCN à l'autre routeur.

Un ACL de sortie a été configuré sur les sous-interfaces dot1q afin de relâcher par-VLAN BPDU qui pourrait être envoyé par un autre site qui n'a pas été migré vers MST encore. Cette configuration empêche le commutateur de la CE de déclarer que l'interface en tant que contradictoire quand elle reçoit un par-VLAN BPDU sur une interface configurée pour MST.

La configuration sur router2 est très semblable :

```
RP/0/RSP0/CPU0:router2#sh run int gig 0/1/0/3.*
interface GigabitEthernet0/1/0/3.1 l2transport
encapsulation untagged
!
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!

RP/0/RSP0/CPU0:router2#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
```

```
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!

RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group customer1
l2vpn
xconnect group customer1
p2p mstag-gi-0-1-0-3
interface GigabitEthernet0/1/0/3.1
neighbor 10.0.0.13 pw-id 103
!
!
!
!

RP/0/RSP0/CPU0:router2#sh run spanning-tree mstag customer1-0-1-0-3
spanning-tree mstag customer1-0-1-0-3
interface GigabitEthernet0/1/0/3.1
name customer1
revision 1
bridge-id 0000.0000.0002
instance 0
root-id 0000.0000.0001
priority 8192
root-priority 4096
!
instance 1
vlan-ids 2
root-id 0000.0000.0002
priority 4096
root-priority 4096
!
!
!

RP/0/RSP0/CPU0:router2#sh spanning-tree mstag customer1-0-1-0-3
GigabitEthernet0/1/0/3.1
Pre-empt delay is disabled
Name: customer1
Revision: 1
Max Age: 20
Provider Bridge: no
Bridge ID: 0000.0000.0002
Port ID: 1
External Cost: 0
Hello Time: 2
Active: yes
BPDUs sent: 3186
MSTI 0 (CIST):
VLAN IDs: 1,3-4094
Role: Designated
Bridge Priority: 8192
Port Priority: 128
Cost: 0
Root Bridge: 0000.0000.0001
Root Priority: 4096
```

```
Topology Changes: 365
MSTI 1
VLAN IDs: 2
Role: Designated
Bridge Priority: 4096
Port Priority: 128
Cost: 0
Root Bridge: 0000.0000.0002
Root Priority: 4096
Topology Changes: 177
```

C'est la configuration de base sur le commutateur 1 :

```
switch1#sh run | b spanning-tree
spanning-tree mode mst
spanning-tree extend system-id
!
spanning-tree mst configuration
name customer1
revision 1
instance 1 vlan 2
!
switch1#sh run int gig 0/1 | i spanning
spanning-tree mst 1 cost 100000

switch1#sh spanning-tree

MST0
Spanning tree enabled protocol mstp
Root ID Priority 4096
Address 0000.0000.0001
Cost 0
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Root FWD 20000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p



MST1
Spanning tree enabled protocol mstp
Root ID Priority 4097
Address 0000.0000.0002
Cost 40000
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Altn BLK 100000 128.1 P2p
Gi0/2 Root FWD 20000 128.2 P2p
```

Ainsi, le trafic dans l'exemple 0 est expédié par router1 et le trafic dans l'exemple 1 est expédié par switch2 et router2.

La configuration sur switch2 utilise les mêmes commandes que switch1 :

```
switch2#sh run | b spanning
spanning-tree mode mst
spanning-tree extend system-id
!
spanning-tree mst configuration
name customer1
revision 1
instance 1 vlan 2
!
switch2#sh run int gig 0/1 | i spanning
spanning-tree mst 0 cost 100000

switch2#sh spanning-tree

MST0
Spanning tree enabled protocol mstp
Root ID Priority 4096
Address 0000.0000.0001
Cost 0
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Altn BLK 100000 128.1 P2p
Gi0/2 Root FWD 20000 128.2 P2p



MST1
Spanning tree enabled protocol mstp
Root ID Priority 4097
Address 0000.0000.0002
Cost 20000
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Root FWD 20000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p
```

Passe Comm2 par switch1 et router1 pour instance0 et par router2 pour instance1.

Le trafic loadbalanced parce qu'un exemple quitte le site par router1 et l'autre exemple quitte le site par router2.

Si le lien entre router1 et switch1 est en baisse, les deux exemples passent par router2.

```
switch1#sh spanning-tree

MST0
Spanning tree enabled protocol mstp
```

```
Root ID Priority 4096
Address 0000.0000.0001
Cost 0
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/2 Root FWD 20000 128.2 P2p



MST1
Spanning tree enabled protocol mstp
Root ID Priority 4097
Address 0000.0000.0002
Cost 40000
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/2 Root FWD 20000 128.2 P2p


switch2#sh spanning-tree

MST0
Spanning tree enabled protocol mstp
Root ID Priority 4096
Address 0000.0000.0001
Cost 0
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Root FWD 100000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p



MST1
Spanning tree enabled protocol mstp
Root ID Priority 4097
Address 0000.0000.0002
Cost 20000
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0024.985e.6a00
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- ------------------------------
Gi0/1 Root FWD 20000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p
```

La convergence rapide peut être réalisée dans ce type de panne parce que le chemin à travers la racine de tous les jours a été déjà sélectionné comme voie de déroutement. Avec MSTAG, MST BPDU ne sont pas transportés au-dessus de VPLS ainsi de sites sont isolés dans l'instabilité dans d'autres sites.

4.4.7.3 PVSTAG ou PVRSTAG

MSTAG est le protocole de passerelle préféré d'accès pour VPLS parce qu'il utilise le spanning-tree rapide et parce qu'il est extensible avec son utilisation des exemples plutôt que des BPDU sur chaque VLAN.

Si un site ne peut pas être migré vers MST et la seule solution est de continuer à exécuter PVST+ ou PVRST, vous pouvez utiliser PVSTAG ou PVRSTAG, mais l'implémentation est limitée à une topologie spécifique :

Dans cette topologie, la restriction la plus importante est qu'il peut y avoir seulement un commutateur de la CE. Vous ne pouvez pas avoir deux Commutateurs comme dans la topologie MSTAG. Dans MSTAG, vous pouvez configurer un Point à point picowatt afin de transporter le trafic non-marqué (BPDU y compris TCN) d'un PE à l'autre quand le site est coupé en deux parts. Avec PVST et PVRST, les TCN sont envoyés étiquetés ainsi ils apparient la même sous-interface que le trafic de données à transporter au-dessus de VPLS. Le routeur devrait identifier les BPDU basés sur le type d'adresse MAC et de protocole afin d'expédier les TCN à l'autre côté. Puisque ceci n'est pas actuellement pris en charge, il y a une condition requise d'avoir seulement un périphérique de la CE.

Une autre condition requise dans les versions plus tôt que la version 4.3.0 de Logiciel Cisco IOS XR est que des interfaces de paquet ne peuvent pas être utilisées comme ACs. Cette restriction a été levée dans la version 4.3.0 de Logiciel Cisco IOS XR.

Le principe est vraiment beaucoup d'identique qu'avec MSTAG. Le routeur PVSTAG envoie des BPDU statiques de sorte que le CE semble être connecté aux Commutateurs qui sont directement connectés à la racine (virtuelle) à un loadbalance du coût 0. le trafic, quelques VLAN peut être configuré avec la racine sur router3 et d'autres avec la racine sur router4.

C'est un exemple de configuration sur router3 :

```
RP/0/RSP1/CPU0:router3#sh run int gigabitEthernet 0/0/0/1.*
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface GigabitEthernet0/0/0/1.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!

RP/0/RSP1/CPU0:router3#sh run l2vpn bridge group customer1
l2vpn
```

```
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/0/0/1.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!

RP/0/RSP1/CPU0:router3#sh run spanning-tree pvstag customer1-0-0-0-1
spanning-tree pvstag customer1-0-0-0-1
interface GigabitEthernet0/0/0/1
vlan 2
root-priority 0
root-id 0000.0000.0000
root-cost 0
priority 0
bridge-id 0000.0000.0001
!
vlan 3
root-priority 0
root-id 0000.0000.0000
root-cost 0
priority 1
bridge-id 0000.0000.0001
!
!
!

RP/0/RSP1/CPU0:router3#sh spanning-tree pvstag customer1-0-0-0-1
GigabitEthernet0/0/0/1
VLAN 2
Pre-empt delay is disabled
Sub-interface: GigabitEthernet0/0/0/1.2 (Up)
Max Age: 20
Root Priority: 0
Root Bridge: 0000.0000.0000
Cost: 0
Bridge Priority: 0
Bridge ID: 0000.0000.0001
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202821
```

```
Topology Changes: 0
VLAN 3
Pre-empt delay is disabled
Sub-interface: GigabitEthernet0/0/0/1.3 (Up)
Max Age: 20
Root Priority: 0
Root Bridge: 0000.0000.0000
Cost: 0
Bridge Priority: 1
Bridge ID: 0000.0000.0001
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202821
Topology Changes: 0
```

C'est un exemple de configuration sur router4 :

```
RP/0/RSP1/CPU0:router4#sh run int gig 0/0/0/1.*
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface GigabitEthernet0/0/0/1.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!

RP/0/RSP1/CPU0:router4#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/0/0/1.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
!
!
!
!

RP/0/RSP1/CPU0:router4#sh run spanning-tree pvstag customer1-0-0-0-1
spanning-tree pvstag customer1-0-0-0-1
interface GigabitEthernet0/0/0/1
vlan 2
root-priority 0
```

```
root-id 0000.0000.0000
root-cost 0
priority 1
bridge-id 0000.0000.0002
!
vlan 3
root-priority 0
root-id 0000.0000.0000
root-cost 0
priority 0
bridge-id 0000.0000.0002
!
!
!

RP/0/RSP1/CPU0:router4#sh spanning-tree pvstag customer1-0-0-0-1
GigabitEthernet0/0/0/1
VLAN 2
Pre-empt delay is disabled
Sub-interface: GigabitEthernet0/0/0/1.2 (Up)
Max Age: 20
Root Priority: 0
Root Bridge: 0000.0000.0000
Cost: 0
Bridge Priority: 1
Bridge ID: 0000.0000.0002
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202799
Topology Changes: 0
VLAN 3
Pre-empt delay is disabled
Sub-interface: GigabitEthernet0/0/0/1.3 (Up)
Max Age: 20
Root Priority: 0
Root Bridge: 0000.0000.0000
Cost: 0
Bridge Priority: 0
Bridge ID: 0000.0000.0002
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202799
Topology Changes: 0
```

C'est un exemple de configuration sur le CE switch3 :

```
switch3#sh spanning-tree vlan 2

VLAN0002
Spanning tree enabled protocol ieee
Root ID Priority 0
Address 0000.0000.0000
Cost 4
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- ------------------------------
Gi0/1 Root FWD 4 128.1 P2p
Gi0/2 Altn BLK 4 128.2 P2p

switch3#sh spanning-tree vlan 3

VLAN0003
Spanning tree enabled protocol ieee
Root ID Priority 0
Address 0000.0000.0000
Cost 4
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32771 (priority 32768 sys-id-ext 3)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- ------------------------------
Gi0/1 Altn BLK 4 128.1 P2p
Gi0/2 Root FWD 4 128.2 P2p
```

La configuration pour PVSTAG est très semblable à MSTAG sauf que la priorité racine et la priorité de la passerelle principale sont configurées pendant que 4096 et la priorité de la passerelle de sauvegarde est configurés en tant que 8192 dans l'exemple MSTAG.

Tous autres Commutateurs dans les domaines devraient avoir le supérieur à prioritaires que celui a configuré dans PVSTAG ou PVRSTAG.

Vous pouvez accorder le coût d'interface sur les Commutateurs de la CE afin d'influencer que le port devient le port de racine et que le port est bloqué.

4.4.7.4 MC-LAG

La configuration MC-LAG avec VPLS est plus simple que PWs point par point avec la Redondance bi-directionnelle picowatt. Au lieu d'un picowatt et trois standby primaires PWs, le besoin de siège potentiel d'explosion seulement un maillage complet de VPLS PWs, qui est standard avec VPLS :

Dans cette topologie, notez cela :

- MC-LAG fonctionne entre le siège potentiel d'explosion deux VPLS du côté gauche : router2 et router4.
- Le dans des conditions normales, les membres de paquet sont en activité entre router1 et router2 et dans l'état de réserve entre router1 et router4.
- Le Router2 a les sous-interfaces de paquet configurées sous des bridges-domain VPLS, ainsi router2 en avant le trafic au siège potentiel d'explosion distant VPLS. Il y a deux sites illustrés dans le diagramme de topologie mais il pourrait y avoir beaucoup plus.
- Le siège potentiel d'explosion distant apprennent les adresses MAC de router1 et de périphériques derrière par router2, ainsi le trafic en avant de siège potentiel d'explosion pour ces adresses de MAC de destination par router2.

- Quand le lien entre router1 et router2 descend ou quand router2 descend, le membre de paquet entre router1 et router4 va l'active.
- Comme le routeur 2, router4 a ses sous-interfaces de paquet configurées sous des bridges-domain VPLS.
- Quand les sous-interfaces de paquet sont soulevées sur router4, router4 envoie des messages de retrait de MAC LDP au siège potentiel d'explosion du distant VPLS afin de les faire savoir qu'il y a une modification de topologie.

C'est la configuration sur router3 :

```
RP/0/RSP1/CPU0:router3#sh run redundancy
redundancy
iccp
group 2
mlacp node 1
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.14
!
backbone
interface TenGigE0/0/0/0
interface TenGigE0/0/0/1
!
isolation recovery-delay 300
!
!
!

RP/0/RSP1/CPU0:router3#sh run int bundle-ether 222
interface Bundle-Ether222
lacp switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mlacp port-priority 1
mac-address 0.0.2
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!

RP/0/RSP1/CPU0:router3#sh run int bundle-ether 222.*
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface Bundle-Ether222.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!

RP/0/RSP1/CPU0:router3#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface Bundle-Ether222.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
```

```
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface Bundle-Ether222.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
```

Une fois que le paquet MC-LAG est configuré, ajoutez-le sous la configuration VPLS comme n'importe quel autre courant alternatif.

C'est la configuration correspondante sur router5 :

```
RP/0/RSP1/CPU0:router5#sh run redundancy
redundancy
iccp
group 2
mlacp node 2
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.13
!
backbone
interface TenGigE0/1/0/0
interface TenGigE0/1/0/1
!
isolation recovery-delay 300
!
!
!

RP/0/RSP1/CPU0:router5#sh run int bundle-ether 222
interface Bundle-Ether222
lacp switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mac-address 0.0.2
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!

RP/0/RSP1/CPU0:router5#sh run int bundle-ether 222.*
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface Bundle-Ether222.3 l2transport
```

```
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!

RP/0/RSP1/CPU0:router5#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface Bundle-Ether222.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
!
!
bridge-domain engineering
interface Bundle-Ether222.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
!
!
!
!
```

Sous des circonstances normales, le membre de paquet entre router3 et router6 est en activité, et le membre entre router5 et router6 est dans l'état de réserve :

```
RP/0/RSP1/CPU0:router3#sh bundle bundle-ether 222

Bundle-Ether222
Status: Up
Local links : 1 / 0 / 1
Local bandwidth : 1000000 (1000000) kbps
MAC address (source): 0000.0000.0002 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 1
Wait while timer: Off
Load balancing: Default
LACP: Operational
Flap suppression timer: 100 ms
Cisco extensions: Disabled
mLACP: Operational
ICCP Group: 2
Role: Active
Foreign links : 0 / 1
Switchover type: Revertive
Recovery delay: 40 s
Maximize threshold: 1 link
IPv4 BFD: Not configured

Port Device State Port ID B/W, kbps
------------------- ------------ ----------- ------------- ----------
Gi0/0/0/1 Local Active 0x0001, 0x9001 1000000
```

```
Link is Active
Gi0/0/0/1 10.0.0.14 Standby 0x8000, 0xa002 1000000
Link is marked as Standby by mLACP peer
RP/0/RSP1/CPU0:router3#

router6#sh etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port


Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+-----------------------------------------------
2 Po2(SU) LACP Gi0/1(P) Gi0/2(w)

router6#
```

Le trafic du CE est reçu sur router3 et expédié au siège potentiel d'explosion distant :

```
RP/0/RSP1/CPU0:router3#sh l2vpn bridge-domain group customer1
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 4, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
BE222.3, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.11 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 3, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
BE222.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.11 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0

RP/0/RSP1/CPU0:router3#sh l2vpn forwarding bridge-domain customer1:
engineering mac location 0/0/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
```

```
------------------------------------------------------------------------------
001d.4603.1f01 dynamic BE222.2 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f42 dynamic BE222.2 0/0/CPU0 0d 0h 0m 0s N/A
6c9c.ed3e.e46d dynamic (10.0.0.11, 2) 0/0/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

La dernière commande illustre que router3 apprend quelques adresses MAC sur son paquet et les membres actifs sont sur router3. Sur router5, il n'y a aucune adresse MAC apprise au-dessus du paquet car le membre local est dans l'état de réserve :

```
RP/0/RSP1/CPU0:router5#sh l2vpn forwarding bridge-domain customer1:engineering
mac location 0/0/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
6c9c.ed3e.e46d dynamic (10.0.0.11, 2) 0/0/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f01 dynamic (10.0.0.13, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

Quand le membre de paquet entre router3 et router6 descend, le membre de paquet devient actif sur router5. Le siège potentiel d'explosion MC-LAG VPLS envoient un message de retrait de MAC LDP de sorte que purge distante de siège potentiel d'explosion leurs MAC-adresse-tables et apprennent l'adresse MAC par le nouveau PE router5 de l'active MC-LAG.

Le Router2 reçoit des messages d'un retrait de MAC de router3 et de router5 quand le membre actif de paquet MC-LAG se déplace de router3 à router5 :

```
RP/0/RSP0/CPU0:router2#sh l2vpn bridge-domain group customer1 detail |
i "state is|withd|bridge-domain"
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
AC: GigabitEthernet0/1/0/3.3, state is up
PW: neighbor 10.0.0.12, PW ID 3, state is up ( established )
MAC withdraw message: send 0 receive 0
PW: neighbor 10.0.0.13, PW ID 3, state is up ( established )
MAC withdraw message: send 0 receive 1
PW: neighbor 10.0.0.14, PW ID 3, state is up ( established )
MAC withdraw message: send 0 receive 1
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
AC: GigabitEthernet0/0/0/1.2, state is unresolved
AC: GigabitEthernet0/1/0/3.2, state is up
PW: neighbor 10.0.0.15, PW ID 15, state is up ( established )
MAC withdraw message: send 2 receive 0
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 0
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 1
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 1
```

Les adresses MAC sur router2 se déplacent de router3 (10.0.0.13) à router5 (10.0.0.14) :

```
RP/0/RSP0/CPU0:router2#sh l2vpn forwarding bridge-domain customer1:
engineering mac-address location 0/0/CPU0
```

```
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
-------------------------------------------------------------------------------
6c9c.ed3e.e46d dynamic (10.0.0.15, 15) 0/0/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f02 dynamic (10.0.0.14, 2) 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f42 dynamic (10.0.0.14, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

Avec MC-LAG, un site peut utiliser un seul paquet à relier aux autres sites par VPLS. MC-LAG fournit le lien et la Redondance de PE, mais logiquement c'est toujours une interface de paquet pour atteindre d'autres sites. Le spanning-tree n'est pas exigé sur ce paquet, et un filtre BPDU pourrait être configuré sur le CE afin de s'assurer que des BPDU ne sont pas permutés entre les sites au-dessus de VPLS.

Une autre option est configuration d'une liste d'accès d'Ethernet-services sur l'ACs sur le paquet afin de relâcher les adresses de MAC de destination des BPDU ainsi les BPDU ne sont pas transportés entre les sites. Cependant, si un lien secret est introduit entre les sites, le spanning-tree ne peut pas casser la boucle parce qu'il ne s'exécute pas sur le paquet MC-LAG. Ainsi, évaluez soigneusement si désactiver le spanning-tree sur le MC-LAG empaquettent. Si la topologie entre les sites est soigneusement mise à jour, il fait beau d'avoir la Redondance par MC-LAG sans besoin de spanning-tree.

Batterie de périphérie de 4.4.7.5 ASR 9000 nanovolt

La solution MC-LAG a fourni la Redondance sans nécessité d'utiliser le spanning-tree. Un inconvénient est que les membres de paquet à un PE MC-LAG sont dans l'état de réserve, ainsi c'est une solution d'actif-standby qui ne maximise pas l'utilisation de lien.

Une autre option de conception est utilisation d'une batterie de périphérie ASR 9000 nanovolt de sorte que le ces puisse avoir des membres de paquet à chaque étagère de batterie qui sont tous en activité en même temps :

Un autre avantage de cette solution est que le nombre de PWs est réduit parce qu'il y a seulement un picowatt par batterie pour chacune des batteries à chaque site. Quand il y a le siège potentiel d'explosion deux par site, chaque PE doit avoir un picowatt à chacun du siège potentiel d'explosion deux à chaque site.

La simplicité de la configuration est un autre avantage. La configuration ressemble à une configuration très de base VPLS avec un bridge-domain avec le paquet ACs et VFI PWs :

```
RP/1/RSP0/CPU0:router2#sh bundle bundle-ether 222

Bundle-Ether222
Status: Up
Local links : 2 / 0 / 2
Local bandwidth : 20000000 (20000000) kbps
MAC address (source): 0024.f71e.d309 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 64
Wait while timer: 2000 ms
Load balancing: Default
LACP: Not operational
Flap suppression timer: Off
Cisco extensions: Disabled
```

```
mLACP: Not configured
IPv4 BFD: Not configured

Port Device State Port ID B/W, kbps
------------------- ------------ ----------- -------------- ----------
Te0/0/0/8 Local Active 0x8000, 0x0005 10000000
Link is Active
Te1/0/0/8 Local Active 0x8000, 0x0001 10000000
Link is Active

RP/1/RSP0/CPU0:router2#sh run int bundle-ether 222.2
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!

RP/1/RSP0/CPU0:router2#sh run int bundle-ether 222.3
interface Bundle-Ether222.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!

RP/1/RSP0/CPU0:router2#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface Bundle-Ether222.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface Bundle-Ether222.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!

RP/1/RSP0/CPU0:router2#sh l2vpn bridge-domain group customer1
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 4 (4 up), PBBs: 0 (0 up)
List of ACs:
```

```
BE222.3, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.11 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 4, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 4 (4 up), PBBs: 0 (0 up)
List of ACs:
BE222.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.11 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
```

La Redondance est fournie par le courant alternatif de paquet dual-homed aux deux étagères de sorte que le paquet reste en cas de panne de membre de paquet ou de panne d'étagère.

Quand un site est relié au domaine VPLS seulement par une batterie, la topologie est semblable à MC-LAG quant au spanning-tree. Ainsi le spanning-tree n'est pas exigé sur ce paquet, et un filtre BPDU pourrait être configuré sur le CE afin de s'assurer que des BPDU ne sont pas permutés entre les sites au-dessus de VPLS.

Une autre option est configuration d'une liste d'accès d'Ethernet-services sur l'ACs sur le paquet afin de relâcher les adresses de MAC de destination des BPDU ainsi les BPDU ne sont pas transportés entre les sites. Cependant, si un lien secret est introduit entre les sites, le spanning-tree ne peut pas casser la boucle parce qu'il ne s'exécute pas sur le paquet CE-PE. Ainsi, évaluez soigneusement si désactiver le spanning-tree sur que cela CE-PE empaquettent. Si la topologie entre les sites est soigneusement mise à jour, il fait beau d'avoir la Redondance par la batterie sans besoin de spanning-tree.

Multihébergement ICCP basé sur de service de 4.4.7.6 (ICCP-SM) (PMCLAG (pseudo MCLAG) et Active/Active)

Il y a une nouvelle fonctionnalité introduite dans la version 4.3.1 afin de surmonter la limite de MC-LAG, où quelques liens de paquet sont tout inutilisés qu'ils demeurent dans le mode 'attente'. Dans la nouvelle caractéristique, appelée *Pseudo MCLAG*, tous les liens du DHD aux points des connexions (PoAs) sont en service, mais les VLAN sont séparés entre les différents paquets :

4.5 Contrôle de tempête du trafic

Dans un domaine de l'émission L2, il y a le risque qu'un hôte pourrait se conduire mal et envoyer un haut débit de trames d'émission ou de Multidiffusion qui doivent être inondées partout dans le bridge-domain. Un autre risque est création d'une boucle L2 (qui n'est pas à dire cassé par le spanning-tree), qui a comme conséquence le bouclage d'émissions et de paquets de Multidiffusions. Un haut débit d'émissions et de paquets de Multidiffusions affecte la représentation des hôtes dans les domaines d'émission.

La représentation des périphériques de commutation dans le réseau pourrait également être affectée par la réplication d'une trame entrée (émission, Multidiffusion ou une trame de monodiffusion inconnue) à de plusieurs ports de sortie dans le bridge-domain. La création de plusieurs copies du même paquet peut être ressource-intensive, selon l'endroit à l'intérieur du périphérique où le paquet doit être répliqué. Par exemple, répliquer une émission vers de plusieurs différents emplacements n'est pas un problème en raison des capacités de réplication de Multidiffusion de la matrice. La représentation d'un processeur de réseau pourrait être affectée quand elle doit créer de plusieurs copies du même paquet à envoyer sur quelques ports que le processeur de réseau manipule.

Afin de protéger des périphériques en cas de tempête, la caractéristique de contrôle de tempête du trafic vous permet de configurer un débit maximum d'émissions, de Multidiffusion et d'unicasts inconnus à recevoir sur un courant alternatif de bridge-domain. Voir le guide de configuration de Sécurité de système de routeur de services d'agrégation de gamme 9000 de Cisco ASR, libérez 4.3.x : En mettant en application le trafic fulminez le contrôle sous une passerelle VPLS pour des détails.

Le contrôle de tempête du trafic n'est pas pris en charge sur des interfaces ou VFI PWs à C.A. de paquet, mais est pris en charge sur le non-paquet ACs et l'accès PWs. La caractéristique est désactivée par défaut ; à moins que vous installiez le contrôle de tempête, vous recevez n'importe quel débit d'émissions, de Multidiffusion, et d'unicasts inconnus.

Voici un exemple de configuration :

```
RP/0/RSP0/CPU0:router2#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
storm-control unknown-unicast pps 10000
storm-control multicast pps 10000
storm-control broadcast pps 1000
!
neighbor 10.0.0.15 pw-id 15
storm-control unknown-unicast pps 10000
storm-control multicast pps 10000
storm-control broadcast pps 1000
!
vfi customer1-engineering
neighbor 10.0.0.10 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!

RP/0/RSP0/CPU0:router2#sh l2vpn bridge-domain bd-name engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
```

```
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (1w1d ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 5 (5 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40007; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control:
 Broadcast: enabled(1000)
 Multicast: enabled(10000)
 Unknown unicast: enabled(10000)
Static MAC addresses:
Statistics:
packets: received 251295, sent 3555258
bytes: received 18590814, sent 317984884
Storm control drop counters:
 packets: broadcast 0, multicast 0, unknown unicast 0
 bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
<snip>
```

Les compteurs de baisse de contrôle de tempête sont toujours présents dans la sortie de la commande de **détail de bridge-domain de l2vpn d'exposition**. Puisque la caractéristique est désactivée par défaut, le début de compteurs pour signaler des baisses seulement quand la caractéristique a été configurée.

Les débits configurés pourraient varier sur la structure de trafic d'un réseau à un autre réseau. Avant de configurer un débit, Cisco vous recommande comprennent le débit d'émission, de Multidiffusion ou de trames de monodiffusion inconnues sous des circonstances normales. Ajoutez alors une marge dans le débit configuré au-dessus du débit normal.

4.6 Mouvements de MAC

En cas d'instabilité de réseau comme une instabilité d'interface, une adresse MAC pourrait être apprise d'une nouvelle interface. C'est convergence normale de réseau, et la MAC-adresse-table est mise à jour dynamiquement.

Cependant, les mouvements constants de MAC indiquent souvent l'instabilité de réseau, telle que l'instabilité grave pendant une boucle L2. La fonctionnalité de sécurité d'adresse MAC vous permet de signaler des mouvements de MAC et d'agir des actions correctives telles qu'arrêter un port offensant.

Même si une action corrective n'est pas configurée, vous pouvez configurer la commande **se connectante** ainsi vous êtes alerté de l'instabilité de réseau par les messages de mouvement de MAC :

```
l2vpn
bridge group customer1
bridge-domain engineering
mac
secure
action none
logging
!
!
```

Dans cet exemple, l'action est configurée à aucun, ainsi rien n'est fait quand un mouvement de MAC est détecté sauf qu'un message de Syslog est enregistré. C'est un message d'exemple :

```
LC/0/0/CPU0:Dec 13 13:38:23.396 : l2fib[239]:
%L2-L2FIB-5-SECURITY_MAC_SECURE_VIOLATION_AC : MAC secure in AC
GigabitEthernet0_0_0_4.1310 detected violated packet - source MAC:
0000.0000.0001, destination MAC: 0000.0001.0001; action: none
```

4.7 Piller IGMP et MLD

Par défaut, des trames de Multidiffusion sont inondées à tous les ports dans un bridge-domain. Quand vous utilisez le haut débit coule comme des services de la télévision IP (IPTV), il pourrait y avoir une importante quantité de trafic expédié sur tous les ports et répliqué au-dessus de plusieurs PWs. Si tous les flots TV sont expédiés plus d'une interface, ceci pourrait congestionner des ports. La seule option est configuration d'une caractéristique telle qu'IGMP ou MLD pillant, qui interceptent des paquets de contrôle de Multidiffusion afin de dépister les récepteurs et les routeurs multidiffusion et les flots en avant sur les ports seulement si appropriés.

Voyez le guide de configuration de Multidiffusion de routeur de services d'agrégation de gamme 9000 de Cisco ASR, libérez 4.3.x pour plus d'informations sur ces caractéristiques.

5. Thèmes supplémentaires de L2VPN

Remarques :

Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

5.1 Loadbalancing

Quand un PE de L2VPN doit envoyer une trame au-dessus d'un MPLS picowatt, la trame Ethernet est encapsulée dans une trame MPLS avec un ou plusieurs mpls label ; il y a au moins une étiquette picowatt et peut-être une étiquette d'IGP afin d'atteindre le PE distant.

La trame MPLS est transportée par le réseau MPLS au PE de L2VPN distant. Il y a typiquement des plusieurs chemins pour atteindre le PE de destination :

Remarque: Non tous les liens sont représentés dans ce diagramme.

PE1 peut choisir entre P1 et P2 en tant que premier routeur MPLS P vers PE2. Si P1 est sélectionné, PE1 alors choisit entre P3 et P4, et ainsi de suite. Les chemins disponibles sont basés sur la topologie d'IGP et le chemin de tunnel MPLS TE.

Les fournisseurs de services MPLS préfèrent avoir tous les liens également utilisés plutôt qu'une liaison encombrée avec d'autres liens peu employés. Il n'est pas toujours facile réaliser ce but parce qu'un certain PWs portent beaucoup plus de trafic que d'autres et parce que le chemin emprunté par un trafic picowatt dépend de l'algorithme de hachage utilisé au centre. La plusieurs bande passante élevée PWs pourrait être hachée aux mêmes liens, qui crée l'encombrement.

Une condition requise très importante est que tous les paquets d'un écoulement devraient suivre le même chemin. Autrement, ceci mène aux trames en panne, qui pourraient affecter la qualité ou l'interprétation des applications.

Loadbalancing dans un réseau MPLS sur des Routeurs de Cisco est typiquement basé sur les données qui suivent les mpls label inférieurs.

- Si les données juste après les débuts d'étiquette inférieure avec 0x4 ou 0x6, un routeur MPLS P supposent qu'il y a un paquet d'ipv4 ou d'IPv6 à l'intérieur du paquet et des essais MPLS au loadbalance basé sur des informations parasites des adresses de source et d'ipv4 ou d'IPv6 de destination extraites de la trame. Dans la théorie, ceci ne devrait pas appliquer à une trame Ethernet qui est encapsulée et transportée au-dessus d'un picowatt parce que l'adresse MAC de destination suit l'étiquette inférieure. Mais récemment quelques chaînes d'adresse MAC qui commencent par 0x4 et 0x6 ont été assignées. Le routeur MPLS P pourrait inexactement considérer que l'en-tête Ethernet est réellement une en-tête d'ipv4 et hacher la trame en fonction sur ce qu'il assume est la source et les adresses de destination d'ipv4. Des trames Ethernet d'un picowatt pourraient être hachées au-dessus des différents chemins dans le noyau MPLS, qui mène des trames de -de-ordre dans les questions de qualité picowatt et

d'application. La solution est configuration de contrôle-Word sous une picowatt-classe qui peut être reliée à un Point à point ou à un VPLS picowatt. Le mot de commande est inséré juste après les mpls label. Le mot de commande ne commence pas par 0x4 ou 0x6 ainsi le problème est évité.

```
RP/1/RSP0/CPU0:router#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
pw-class control-word
encapsulation mpls
control-word
!
!
bridge group customer1
bridge-domain engineering
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
pw-class control-word
!
<snip>
RP/1/RSP0/CPU0:router#sh l2vpn bridge-domain bd-name engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 4, state: up,
ShgId: 0, MSTi: 0
<snip>
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.11, PW ID 2, state is up ( established )
PW class control-word, XC ID 0xc000000a
Encapsulation MPLS, protocol LDP
Source address 10.0.0.10
PW type Ethernet, control word enabled, interworking none
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------
Label 281708 16043
Group ID 0x4 0x5
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word enabled enabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x7 0x7
(control word) (control word)
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------
```

- Si les données juste après que le bas de la pile de mpls label ne commence pas par 0x4 ou 0x6, les loadbalances de routeur P ont basé sur l'étiquette inférieure. Tout le trafic d'un picowatt suit le même chemin, ainsi les paquets en panne ne se produisent pas, mais ceci pourrait mener à l'encombrement sur quelques liens en cas de bande passante élevée PWs. Avec le Logiciel Cisco IOS XR libérez 4.2.1, l'ASR 9000 prend en charge la caractéristique avertie picowatt du transport d'écoulement (FAT). Cette caractéristique fonctionne sur le siège potentiel d'explosion de L2VPN, où elle est négociée entre les deux fins d'un Point à point ou d'un VPLS picowatt. Le PE de L2VPN d'entrée détecte des écoulements sur le courant alternatif et la configuration de L2VPN et insère une nouvelle étiquette d'écoulement MPLS

au-dessous des mpls label picowatt au bas de la pile de mpls label. Le PE d'entrée détecte des écoulements basés sur la source et les adresses de MAC de destination (par défaut) ou les adresses de source et d'ipv4 de destination (configurables). L'utilisation des adresses MAC est le par défaut ; l'utilisation des adresses d'ipv4 est recommandée, mais doit être configurée manuellement.

Avec la configuration FAT picowatt, les insertions de PE de L2VPN d'entrée un mpls label inférieurs par src-dst-MAC ou par src-dst-IP. Les Routeurs MPLS P (entre le siège potentiel d'explosion) hachent des trames au-dessus des chemins disponibles, puis atteignent le PE de destination basé sur cette étiquette d'écoulement FAT picowatt au bas de la pile MPLS. Ceci fournit généralement une utilisation de bande passante bien meilleure au centre à moins qu'un picowatt porte seulement un nombre restreint de src-dst-MAC ou de conversations src-dst-IP. Cisco recommande que vous utilisiez un mot de commande ainsi vous pouvez éviter d'avoir des adresses MAC qui commencent par 0x4 et 0x6 juste après que l'étiquette d'écoulement. Ceci s'assure que les informations parasites sont correctement basées sur les pseudo adresses IP et pas basées sur l'étiquette d'écoulement.

Avec cette configuration, le trafic d'un picowatt loadbalanced au-dessus des plusieurs chemins au centre si disponible. Le trafic de l'application ne souffre pas des paquets en panne parce que tout le trafic de la même source (MAC ou IP) à la même destination (MAC ou IP) suit le même chemin.

C'est un exemple de configuration :

```
l2vpn
pw-class fat-pw
encapsulation mpls
control-word
load-balancing
flow-label both
!
!
!
bridge group customer1
bridge-domain engineering
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
pw-class fat-pw


RP/1/RSP0/CPU0:router#sh l2vpn bridge-domain bd-name engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 4, state: up,
ShgId: 0, MSTi: 0
<snip>
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.11, PW ID 2, state is up ( established )
PW class fat-pw, XC ID 0xc000000a
Encapsulation MPLS, protocol LDP
Source address 10.0.0.10
PW type Ethernet, control word enabled, interworking none
Sequencing not set
Load Balance Hashing: src-dst-ip
Flow Label flags configured (Tx=1,Rx=1), negotiated (Tx=1,Rx=1)

PW Status TLV in use
```

```
MPLS Local Remote
------------ ------------------------------ ------------------
Label 281708 16043
Group ID 0x4 0x5
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word enabled enabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x7 0x7
(control word) (control word)
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------
```

5.2 Se connecter

Différents types de messages de journalisation peuvent être configurés dans le mode de configuration de L2VPN. Configurez la commande logging on de l2vpn pour recevoir des alertes de Syslog pour des événements de L2VPN, et configurez se connecter le pseudowire afin de déterminer quand des changements d'état picowatt :

```
l2vpn
logging
bridge-domain
pseudowire
nsr
!
```

Si beaucoup PWs sont configurés, les messages pourraient inonder le log.

liste d'accès des Ethernet-services 5.3

Vous pouvez employer une liste d'accès d'Ethernet-services afin de relâcher le trafic des hôtes spécifiques ou le vérifier si un routeur obtient des paquets d'un hôte sur une interface de l2transport :

```
RP/0/RSP0/CPU0:router#sh run ethernet-services access-list count-packets
ethernet-services access-list count-packets
10 permit host 001d.4603.1f42 host 0019.552b.b5c3
20 permit any any
!

RP/0/RSP0/CPU0:router#sh run int gig 0/1/0/3.2
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ethernet-services access-group count-packets egress
!

RP/0/RSP0/CPU0:router#sh access-lists ethernet-services count-packets
hardware egress location 0/1/CPU0
ethernet-services access-list count-packets
10 permit host 001d.4603.1f42 host 0019.552b.b5c3 (5 hw matches)
20 permit any any (30 hw matches)
```

Les correspondances de matériel peuvent être vues seulement avec le mot clé de *matériel*. Utilisez le mot clé d'*entrée* ou de *sortie* selon la direction de l'access-group. L'emplacement de linecard de l'interface où la liste d'accès est appliquée est également spécifié.

Vous pouvez également appliquer un ipv4 access-list sur une interface de l2transport comme caractéristique de Sécurité ou de dépannage :

```
RP/0/RSP0/CPU0:router#sh run ipv4 access-list count-pings
ipv4 access-list count-pings
10 permit icmp host 192.168.2.1 host 192.168.2.2
20 permit ipv4 any any
!

RP/0/RSP0/CPU0:router#sh run int gig 0/1/0/3.2
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ipv4 access-group count-pings ingress
!

RP/0/RSP0/CPU0:router#sh access-lists ipv4 count-pings hardware ingress
location 0/1/CPU0
ipv4 access-list count-pings
10 permit icmp host 192.168.2.1 host 192.168.2.2 (5 hw matches)
20 permit ipv4 any any (6 hw matches)
```

de sortie-filtre de 5.4 Ethernets

Dans la direction de sortie d'un courant alternatif, supposez qu'il n'y a aucune commande **symétrique de <> de bruit de rewrite ingress tag** qui détermine les balises du de sortie VLAN. Dans ce cas, il n'y a aucun contrôle afin de s'assurer que la trame sortante a les balises correctes VLAN selon la commande d'**encapsulation**.

C'est un exemple de configuration :

```
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
!
interface GigabitEthernet0/1/0/39.2 l2transport
encapsulation dot1q 2
!
l2vpn
bridge group customer2
bridge-domain test
interface GigabitEthernet0/1/0/3.2
!
interface GigabitEthernet0/1/0/3.3
!
interface GigabitEthernet0/1/0/39.2
!
!
!
!
```

Dans cette configuration, notez cela :

- Une émission reçue avec une balise 2 dot1q sur GigabitEthernet0/1/0/39.2 garde sa balise entrante parce qu'il n'y a aucune commande d'**entrée de réécriture**.
- Cette émission est inondée hors de GigabitEthernet0/1/0/3.2 avec sa balise 2 dot1q, mais cela ne pose pas un problème parce que GigabitEthernet0/1/0/3.2 est également configuré

avec la balise 2. dot1q.

- Cette émission est également inondée hors de GigabitEthernet0/1/0/3.3, qui garde sa balise d'origine 2 parce qu'il n'y a aucune commande de **réécriture** sur GigabitEthernet0/1/0/3.3. La commande de l'**encapsulation dot1q 3** sur GigabitEthernet0/1/0/3.3 n'est pas signée la direction de sortie.
- Le résultat est que, parce que une émission reçue avec la balise 2 sur GigabitEthernet0/1/0/39, là sont deux émissions avec l'extinction de la balise 2 de GigabitEthernet0/1/0/3. Que le trafic reproduit pourrait entraîner une certaine application émet.
- La solution est configuration de sortie-*filtre d'Ethernets stricte* afin de s'assurer que les paquets partent de la sous-interface avec les balises correctes VLAN. Autrement, les paquets ne sont pas expédiés et sont lâchés.

```
interface GigabitEthernet0/1/0/3.2 l2transport
ethernet egress-filter strict
!
interface GigabitEthernet0/1/0/3.3 l2transport
ethernet egress-filter strict
!
```