Services et fonctionnalités de l'IOS XR L2VPN

Table des matières

Introduction

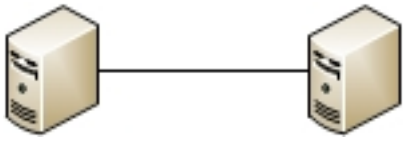
Ce document décrit les topologies de base L2 (Layer 2) VPN (L2VPN). Il est utile de présenter des exemples de base afin de démontrer la conception, les services, les fonctionnalités et la configuration. Pour plus d'informations, reportez-vous au document Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide, Release 4.3.x.

1. Services point à point et multipoint

La fonctionnalité L2VPN permet de fournir des services point à point et multipoint.

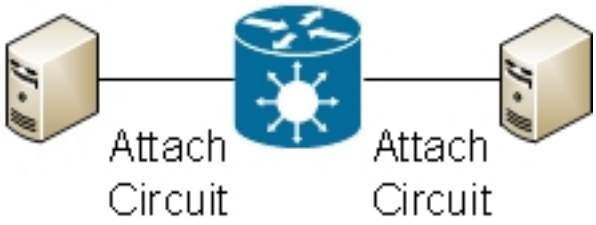
1.1 Service point à point

Le service point à point émule essentiellement un circuit de transport entre deux noeuds d'extrémité de sorte que les noeuds d'extrémité semblent être connectés directement sur une liaison point à point. Il peut être utilisé pour connecter deux sites.

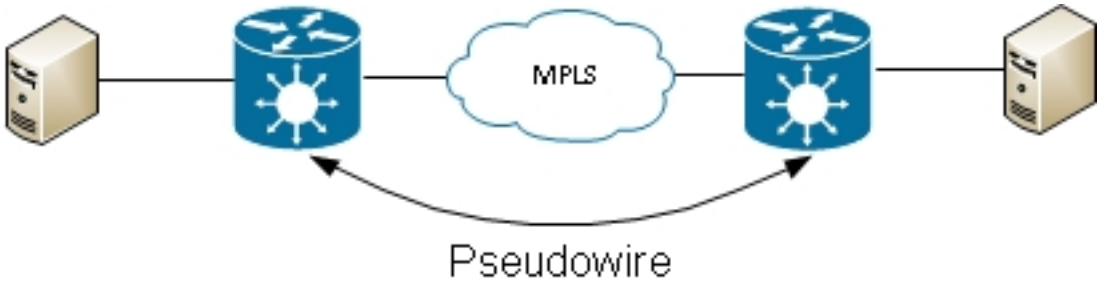


En réalité, il peut y avoir plusieurs routeurs entre les deux noeuds d'extrémité et plusieurs conceptions pour fournir le service point à point.

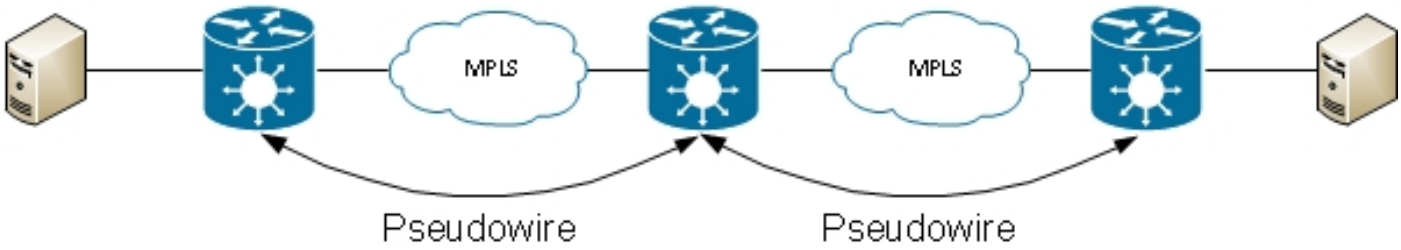
Un routeur peut effectuer une commutation locale entre deux de ses interfaces :



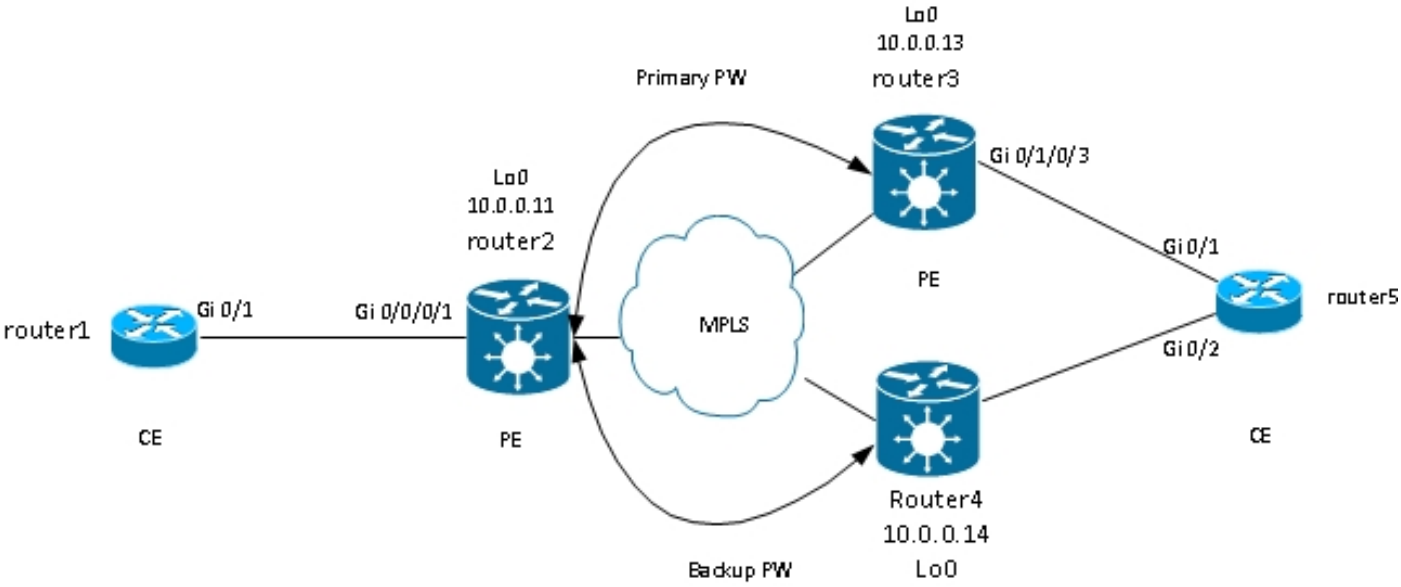
Il peut également y avoir un pseudo-fil MPLS (Multiprotocol Label Switching) entre deux routeurs :



Un routeur peut commuter des trames entre deux PW ; dans ce cas, il s'agit d'un PW multisegment :



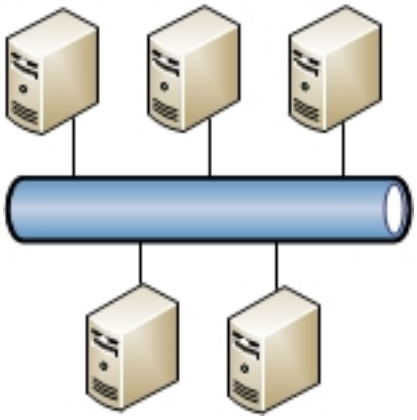
La redondance est disponible via la fonction de redondance des PW :



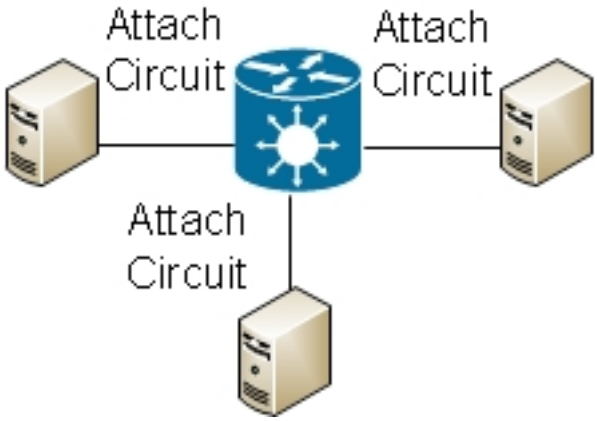
D'autres conceptions sont disponibles, mais elles ne peuvent pas toutes être répertoriées ici.

1.2 Service multipoint

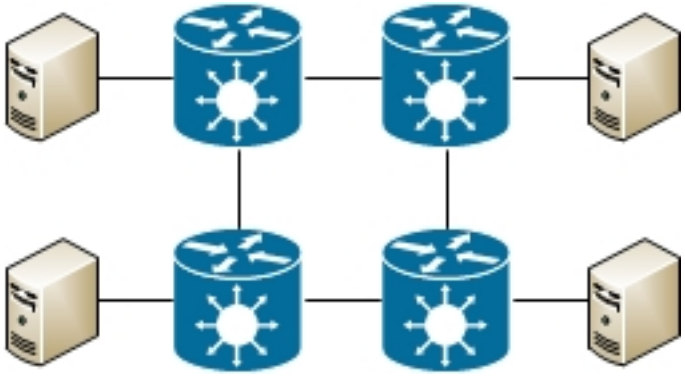
Le service multipoint émule un domaine de diffusion de sorte que tous les hôtes connectés dans ce domaine-pont semblent être connectés logiquement au même segment Ethernet :



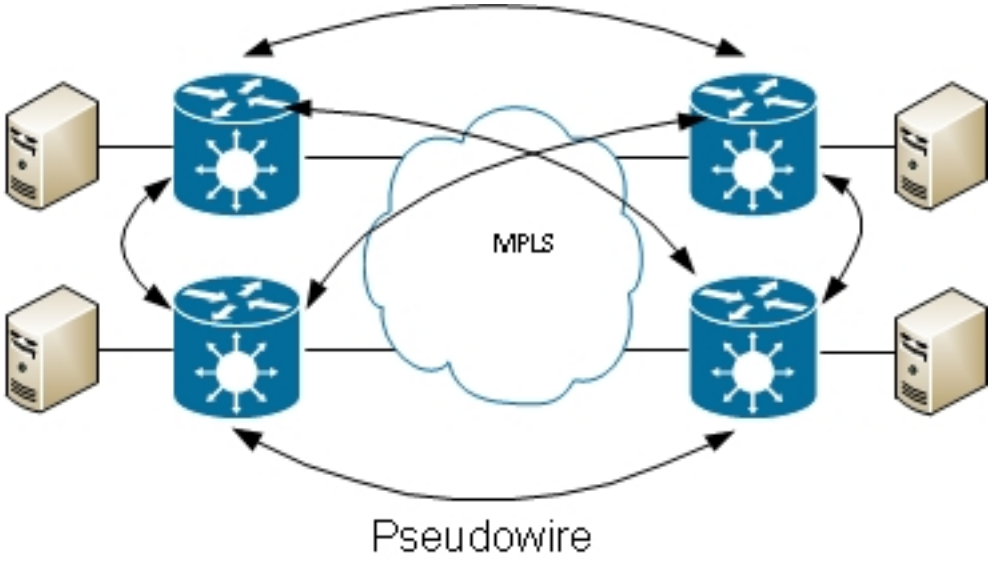
Tous les hôtes peuvent être connectés au même routeur/commutateur :



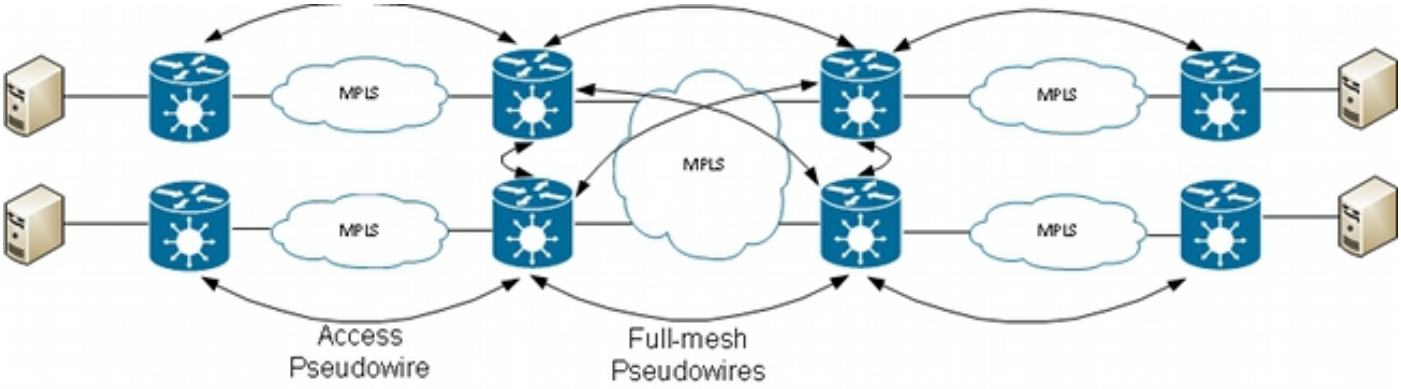
Plusieurs commutateurs peuvent effectuer une commutation Ethernet traditionnelle ; le protocole STP doit être utilisé pour rompre les boucles :



Les services VPLS (Virtual Private LAN Services) vous permettent d'étendre le domaine de diffusion entre plusieurs sites à l'aide de PC MPLS :



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



2. Circuits de fixation

2.1 Circuit virtuel Ethernet ASR 9000

2.1.1 Correspondance des interfaces entrantes

Les règles de base pour les circuits de connexion (CA) sont les suivantes :

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

    1. La trame entrante comporte deux étiquettes dot1q et correspond à une sous-interface configurée avec les mêmes deux étiquettes dot1q (tunneling 802.1Q, ou QinQ). C'est la

plus longue correspondance possible.
2. La trame entrante comporte deux étiquettes dot1q et correspond à une sous-interface configurée avec la même première étiquette dot1q et *toute autre* pour la seconde étiquette.
3. La trame entrante a une balise dot1q et correspond à une sous-interface configurée avec la même balise dot1q et le mot clé *exact*.
4. La trame entrante comporte une ou plusieurs étiquettes dot1q et correspond à une sous-interface configurée avec l'une des étiquettes dot1q.
5. La trame entrante n'a pas d'étiquettes dot1q et correspond à une sous-interface configurée avec la commande **encapsulation untagged**.
6. La trame entrante ne correspond à aucune autre sous-interface, donc elle correspond à une sous-interface configurée avec la commande **encapsulation default**.
7. La trame entrante ne correspond à aucune autre sous-interface, donc elle correspond à l'interface principale qui est configurée pour *l2transport*.

- Sur les routeurs traditionnels qui n'utilisent pas le modèle de connexion virtuelle Ethernet (EVC), les balises VLAN configurées sous la sous-interface sont supprimées (éclatées) de la trame avant d'être transportées par la fonctionnalité L2VPN.
- Sur un routeur à services d'agrégation de la gamme Cisco ASR 9000 qui utilise l'infrastructure EVC, l'action par défaut consiste à conserver les balises existantes. Utilisez la commande **rewrite** pour modifier la valeur par défaut.
- S'il y a une interface virtuelle de pont (BVI) dans le domaine de pont, toutes les balises entrantes doivent être affichées car l'interface virtuelle de pont (BVI) est une interface routée sans balise. Consultez la section BVI pour plus de détails.

Voici quelques exemples qui illustrent ces règles :

1. Un exemple de base est lorsque tout le trafic reçu sur un port physique doit être transporté, qu'il ait ou non une étiquette VLAN. Si vous configurez **l2transport** sous l'interface principale, tout le trafic reçu sur ce port physique est transporté par la fonctionnalité L2VPN :

```
interface GigabitEthernet0/0/0/2
l2transport
```

S’il existe des sous-interfaces de cette interface principale, l’interface principale intercepte toute trame qui n’a été mise en correspondance par aucune sous-interface ; il s’agit de la règle de correspondance la plus longue.

2. Les interfaces et sous-interfaces du bundle peuvent être configurées comme l2transport :

```
interface Bundle-Ether1
l2transport
```

3. Utilisez l'**encapsulation default** sous une sous-interface l2transport pour faire correspondre tout trafic étiqueté ou non étiqueté qui n'a pas été mis en correspondance par une autre sous-interface avec une correspondance la plus longue. (Voir l'exemple 4). Le mot-clé *l2transport* est configuré dans le nom de la sous-interface, et non sous la sous-interface comme sur l'interface principale :

```
interface GigabitEthernet0/1/0/3.1 l2transport
```

encapsulation default

Configurez l'**encapsulation non balisée** si vous voulez faire correspondre uniquement les trames non balisées.

4. Lorsqu'il existe plusieurs sous-interfaces, exécutez le test de correspondance le plus long 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 que :

- Une trame QinQ avec une étiquette VLAN externe 2 et une étiquette VLAN interne 3 peut correspondre aux sous-interfaces .1, .2 ou .3, mais elle est attribuée à la sous-interface .3 en raison de la règle de correspondance la plus longue. Deux balises sur .3 sont plus longues qu'une balise sur .2 et qu'aucune balise sur .1.
- Une trame QinQ avec une étiquette VLAN externe 2 et une étiquette VLAN interne 4 est attribuée à la sous-interface .2 parce que l'**encapsulation dot1q 2** peut correspondre aux trames dot1q avec seulement l'étiquette VLAN 2 mais peut également correspondre aux trames QinQ avec une étiquette externe 2. Reportez-vous à l'exemple 5 (le mot clé *exact*) si vous ne voulez pas correspondre aux trames QinQ.
- Une trame QinQ avec une étiquette VLAN externe 3 correspond à la sous-interface .1.
- Une trame dot1q avec une balise VLAN 2 correspond à la sous-interface .2.
- Une trame dot1q avec une étiquette VLAN 3 correspond à la sous-interface .1.

5. Pour faire correspondre une trame dot1q et non une trame QinQ, utilisez le mot clé *exact* :

```
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2 exact
```

Cette configuration ne correspond pas aux trames QinQ avec une étiquette VLAN externe 2, car elle ne correspond qu'aux trames avec exactement une étiquette VLAN.

6. Utilisez le mot clé *untagged* afin de faire correspondre uniquement les trames non étiquetées telles que les paquets CDP (Cisco Discovery Protocol) ou les unités BPDU (Multiple Spanning Tree) :

```
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 que :

- Les trames Dot1q avec une balise VLAN 3 ou les trames QinQ avec une balise externe 3 correspondent aux sous-interfaces .3.
- Toutes les autres trames dot1q ou QinQ correspondent à la sous-interface .1.
- Les trames sans étiquette VLAN correspondent à la sous-interface .2.

7. Le mot clé *any* peut être utilisé comme caractère générique :

```
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 sous-interfaces .4 et .5 peuvent correspondre aux trames QinQ avec les balises 4 et 5, mais les trames sont attribuées aux sous-interfaces .5 car elles sont plus spécifiques. C'est la règle de correspondance la plus longue.

8. Les plages de balises VLAN peuvent être utilisées :

```
interface GigabitEthernet0/1/0/3.6 l2transport
encapsulation dot1q 6-10
```

9. Plusieurs valeurs ou plages de balises VLAN peuvent être répertoriées pour la première ou la 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 d'autres valeurs sont requises, elles doivent être attribuées à une autre sous-interface. Regroupez les valeurs dans une plage afin de raccourcir la liste.

10. La commande **encapsulation dot1q second-dot1q** utilise l'Ethertype 0x8100 pour les balises externe et interne parce qu'il s'agit de la méthode Cisco pour encapsuler les trames QinQ. Selon IEEE, cependant, l'Ethertype 0x8100 devrait être réservé pour les trames 802.1q avec une étiquette VLAN, et une étiquette externe avec l'Ethertype 0x88a8 devrait être utilisée pour les trames 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 l'ancien Ethertype 0x9100 ou 0x9200 pour les balises externes QinQ, utilisez la commande **dot1q tunneling ethertype** sous l'interface principale de la sous-interface 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 0x9200, et la balise interne a le Ethertype dot1q 0x8100.

12. Une trame entrante peut être attribuée à une sous-interface, en fonction de l'adresse MAC source :

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

2.1.2 Manipulation de VLAN

Le comportement par défaut d'une plate-forme EVC consiste à conserver les balises VLAN sur la trame entrante.

```
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
```

Dans cette configuration, une trame dot1q entrante avec une étiquette VLAN 3 conserve son étiquette VLAN 3 lorsque la trame est transférée. Une trame QinQ entrante avec une étiquette VLAN externe 3 et une étiquette interne 100 maintient les deux étiquettes inchangées lorsque la trame est transférée.

Mais, l'infrastructure EVC vous permet de manipuler les balises avec la commande **rewrite**, de sorte que vous pouvez pop (supprimer), traduire, ou pousser (ajouter) les balises à la pile de balises VLAN entrantes.

En voici quelques exemples :

- Le mot clé *pop* vous permet de supprimer une balise QinQ d'une trame dot1q entrante. Cet exemple supprime l'étiquette externe 13 de la trame QinQ entrante et transfère la trame avec l'étiquette dot1q 100 au-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, ce qui signifie que l'étiquette extérieure 13 est soufflée dans le sens de l'entrée et poussée dans le sens de la sortie.

- Le mot-clé *translate* vous permet de remplacer une ou deux balises entrantes par une 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 *symmetric* est ajouté automatiquement car c'est le seul mode pris en charge.

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

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

Une étiquette QinQ externe (100) est ajoutée à la trame entrante avec une étiquette dot1q (4). Dans le sens de la sortie, l'étiquette QinQ apparaît.

2.2 Comportement des routeurs non EVC Cisco IOS XR (CRS et XR12000)

La syntaxe pour la correspondance VLAN sur les plates-formes non-EVC n'utilise pas le mot clé *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 des balises VLAN ne peut pas être configurée, car le seul comportement possible est d'afficher toutes les balises qui sont spécifiées dans les commandes **dot1q** ou **dot1ad**. Cette opération est effectuée par défaut, de sorte qu'il n'y a pas de commande **rewrite**.

3. Service point à point

Remarques :

Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus

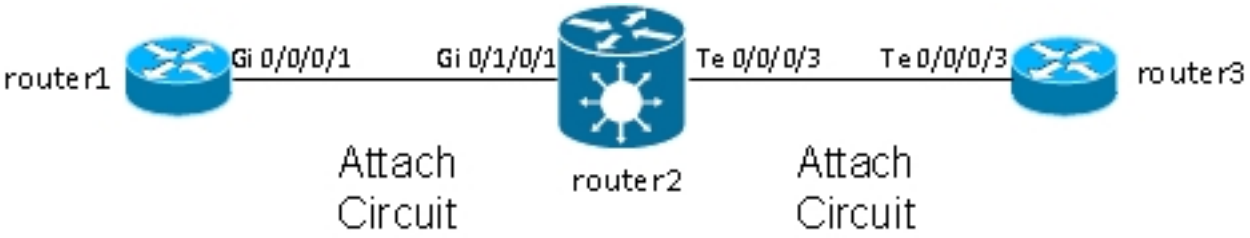
d'informations sur les commandes utilisées dans cette section.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

3.1 Commutation locale

3.1.1 Interface principale

La topologie de base est une interconnexion locale entre deux interfaces principales :



Le routeur 2 prend tout le trafic reçu sur Gi 0/1/0/1 et le transfère à Te 0/0/0/3 et vice versa.

Bien que les routeurs 1 et 3 semblent avoir un câble direct dos à dos dans cette topologie, ce n'est pas le cas, car le routeur 2 effectue en fait la traduction entre les interfaces TenGigE et GigabitEthernet. Router2 peut exécuter des fonctionnalités sur ces deux interfaces ; une liste de contrôle d'accès (ACL), par exemple, peut abandonner des types spécifiques de paquets ou une carte de stratégie afin de mettre en forme ou de limiter le débit du trafic de faible priorité.

Une interconnexion point à point de base est configurée entre deux interfaces principales configurées en tant que l2transport sur le routeur 2 :

```
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 les routeurs 1 et 3, les interfaces principales sont configurées avec le protocole CDP et une adresse IPv4 :

```
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
```

Le routeur 1 voit le routeur 3 comme un voisin CDP et peut envoyer une requête ping à 10.1.1.2 (l'adresse d'interface du routeur 3) comme si les deux routeurs étaient directement connectés.

Étant donné qu'aucune sous-interface n'est configurée sur le routeur 2, les trames entrantes avec une étiquette VLAN sont transportées de manière transparente lorsque les sous-interfaces dot1q sont configurées sur les routeurs 1 et 3 :

```
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 requêtes ping du routeur 1 vers le routeur 3, vous pouvez utiliser les commandes **show interface** et **show l2vpn** afin de vous assurer que les requêtes ping reçues par le routeur 2 sur un CA sont transférées sur l'autre CA et que les réponses ping sont traitées de la même manière en sens inverse.

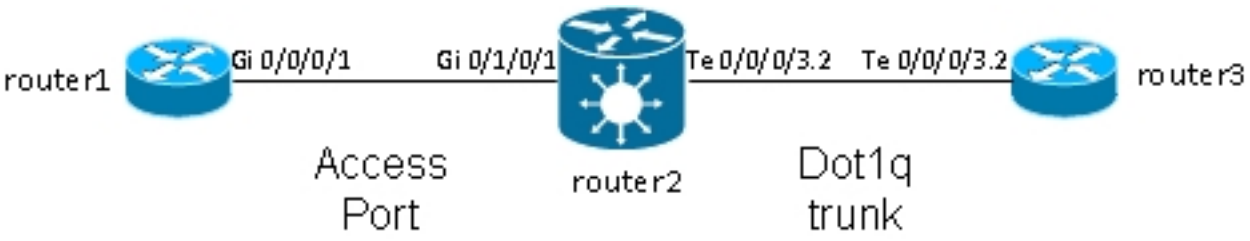
```
RP/0/RSP0/CPU0:router2#sh int gig 0/1/0/1
GigabitEthernet0/1/0/1 is up, line protocol is up
Interface state transitions: 1
Hardware is GigabitEthernet, address is 0024.986c.63f1 (bia 0024.986c.63f1)
Description: static lab connection to acdc 0/0/0/1 - dont change
Layer 2 Transport Mode
MTU 1514 bytes, 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 de VLAN

Dans la terminologie du logiciel Cisco IOS®, cet exemple a une CA semblable à une interface d'accès en mode port de commutation et une sous-interface dot1q semblable à une agrégation :



Généralement, cette topologie utilise un domaine de pont car il y a généralement plus de deux ports dans le VLAN, bien que vous puissiez utiliser une interconnexion point à point s'il n'y a que deux ports. Cette section décrit comment des fonctionnalités de réécriture flexibles vous permettent de manipuler le VLAN de plusieurs façons.

3.1.2.1 Interface principale et sous-interface Dot1q

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

Il s'agit de l'interface principale sur le routeur 1 :

```
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
!
```

Voici la sous-interface dot1q sur le routeur 2 :

```
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
```

Le nom de sous-interface TenGigE0/0/0/3.2 contient maintenant un mot clé *l2transport*. Le routeur 3 envoie des trames dot1q avec la balise 2, qui correspondent à la sous-interface TenGigE0/0/0/3.2 sur le routeur 2.

La balise entrante 2 est supprimée dans le sens d'entrée par la commande **rewrite ingress tag pop**

1 symmetric. Comme l'étiquette a été supprimée en entrée sur l'interface TenGigE0/0/0/3.2, les paquets sont envoyés sans étiquette en sortie sur l'interface GigabitEthernet0/1/0/1.

Le routeur 1 envoie des trames non étiquetées, qui correspondent à l'interface principale GigabitEthernet0/1/0/1.

Il n'y a pas de commande **rewrite** sur GigabitEthernet0/1/0/1, donc aucune balise n'est ajoutée, poussée ou traduite.

Lorsque des paquets doivent être transférés à partir de TenGigE0/0/0/3.2, la balise dot1q 2 est poussée en raison du mot clé *symmetric* dans la commande **rewrite ingress tag pop 1**. La commande affiche une balise dans la direction d'entrée, mais pousse symétriquement une balise dans la direction de sortie. Voici un exemple sur le routeur 3 :

```
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 les mêmes commandes **show interface** et **show 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 reçus sur TenGigE0/0/0/3.2 correspond au nombre de paquets envoyés sur GigabitEthernet0/1/0/1 et vice versa.

3.1.2.2 Sous-interface avec encapsulation

Au lieu de l'interface principale sur GigabitEthernet0/1/0/1, vous pouvez utiliser une sous-interface avec **encapsulation default** afin d'attraper toutes les trames ou avec **encapsulation untagged** afin de correspondre uniquement aux trames non étiquetées :

```
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
```

3.1.2.3 Sens d'entrée sur GigabitEthernet0/1/0/1.1

Plutôt que de faire apparaître la balise 2 dans le sens d'entrée sur TenGigE0/0/0/3.2, vous pouvez pousser la balise 2 dans le sens d'entrée sur GigabitEthernet0/1/0/1.1 et ne rien faire 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
```

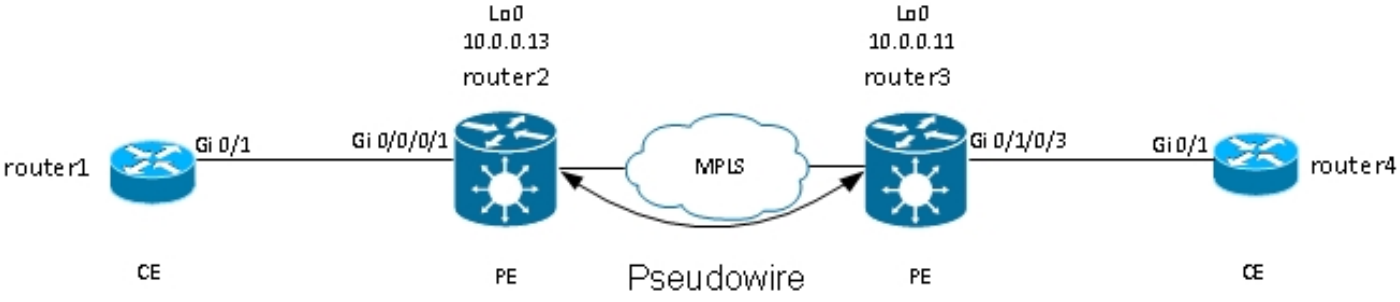
Ainsi, vous pouvez voir que le modèle EVC avec les commandes **encapsulation** et **rewrite** vous

donne une grande flexibilité pour faire correspondre et manipuler les balises VLAN.

3.2 Services de câblage privé virtuel

3.2.1 Vue d'ensemble

Les services VPWS (Virtual Private Wire Services), également connus sous le nom d'Ethernet sur MPLS (EoMPLS), permettent à deux périphériques L2VPN Provider Edge (PE) de tunneler le trafic L2VPN sur un cloud MPLS. Les deux PE L2VPN sont généralement connectés sur deux sites différents avec un coeur MPLS entre eux. Les deux CA connectés à chaque PE L2VPN sont reliés par un PW sur le réseau MPLS, qui est le PW MPLS.



Chaque PE doit avoir une étiquette MPLS afin d'atteindre le bouclage du PE distant. Cette étiquette, généralement appelée étiquette IGP (Interior Gateway Protocol), peut être apprise via le protocole LDP (MPLS Label Distribution Protocol) ou l'ingénierie de trafic MPLS (TE).

Les deux PE établissent entre eux une session LDP MPLS ciblée afin de pouvoir établir et contrôler l'état du PW. Un PE annonce à l'autre PE l'étiquette MPLS pour l'identification PW.

> **Remarque** : bien que le protocole BGP puisse être utilisé pour la signalisation, il n'est pas traité dans ce document.

Le trafic reçu par le routeur 2 sur son CA local est encapsulé dans une pile d'étiquettes MPLS :

- L'étiquette MPLS externe est l'étiquette IGP permettant d'atteindre le bouclage du routeur 3. Il peut s'agir de l'étiquette implicit-null si les étiquettes sont directement connectées ; cela signifie qu'aucune étiquette IGP ne sera ajoutée.
- L'étiquette MPLS interne est l'étiquette PW annoncée par le routeur 3 via la session LDP ciblée.
- Il peut y avoir un mot de contrôle PW après les étiquettes MPLS, selon la configuration et le type d'encapsulation. Le mot de contrôle n'est pas utilisé par défaut sur les interfaces Ethernet et doit être explicitement configuré si nécessaire.
- La trame L2 transportée suit le paquet.
- Certaines balises VLAN sont transportées sur le PW, en fonction de la configuration et du type de PW.

L'avant-dernier saut, juste avant le routeur 3 dans le coeur MPLS, affiche l'étiquette IGP ou la remplace par une étiquette null explicite. Par conséquent, l'étiquette significative supérieure sur la trame reçue par le routeur 3 est l'étiquette PW que le routeur 3 a signalée au routeur 2 pour le

PW. Ainsi, le routeur 3 sait que le trafic reçu avec cette étiquette MPLS doit être commuté vers le CA connecté au routeur 4.

Dans l'exemple précédent, vous devez d'abord vérifier si chaque L2VPN a une étiquette MPLS pour le bouclage du PE distant. Voici un exemple de vérification des étiquettes sur le routeur 2 :

```
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 CA est toujours la même :

```
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
```

Comme il n'y a pas de commande **rewrite ingress pop**, l'étiquette VLAN entrante 2 est transportée sur le PW. Voir PW de type 4 et 5 pour plus de détails.

La configuration L2VPN spécifie l'AC local et le PE L2VPN distant avec un ID de PW qui doit correspondre de chaque côté et doit être unique 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 le routeur 3 est la suivante :

```
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
```

Utilisez la commande **show l2vpn xconnect detail** afin d'afficher les détails sur l'interconnexion :

```
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 que :

- L'unité de transmission maximale (MTU) du courant alternatif est 1504, car l'étiquette entrante sur le courant alternatif n'apparaît pas. Le MTU doit correspondre de chaque côté, sinon le PW ne s'affiche pas.
- 186 paquets ont été reçus sur le contrôleur d'accès et envoyés sur le PW comme prévu.
- 38448 paquets ont été reçus sur le PW et envoyés sur le CA comme prévu.
- L'étiquette locale sur le routeur 2 est 16026 et est l'étiquette que le routeur 3 utilise comme étiquette interne. Les paquets sont reçus sur le routeur 2 avec cette étiquette MPLS comme étiquette supérieure parce que l'étiquette IGP a été sautée par l'avant-dernier saut MPLS. Le routeur 2 sait que les trames entrantes avec cette étiquette PW doivent être commutées vers l'interface graphique AC Gi 0/0/0/1.2 :

```
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 État couplé PW et CA

Dans une interconnexion point à point, l'alimentation CA et l'alimentation électrique sont couplées. Ainsi, si le courant alternatif tombe en panne, le PE L2VPN signale via LDP au PE distant que

l'état du PW doit être en panne. Cela déclenche la convergence lorsque la redondance PW est configurée. Consultez la section Redondance pour plus de détails.

Dans cet exemple, le courant alternatif est en panne sur le routeur 2 et envoie l'état de l'alimentation en courant alternatif en panne au routeur 3 :

```
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
```

Le routeur 3 sait que le PW doit être hors service, car le CA distant est hors service :

```
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 PV de type 4 et 5

Deux types d'PG peuvent être utilisés : le type 4 et le type 5.

- Un PW de type 4 est connu sous le nom de PW basé sur VLAN. Le PE d'entrée n'est pas censé supprimer les balises VLAN entrantes qui doivent être transportées sur le PW.

  Sur les plates-formes basées sur EVC telles que l'ASR 9000, le problème est que les AC entrants peuvent avoir une commande de **réécriture** qui affiche les balises VLAN entrantes, donc il peut y avoir aucune balise VLAN à transporter sur le PW. Afin de répondre à cette possibilité, les plates-formes EVC insèrent une étiquette VLAN factice 0 au-dessus de la trame pour les PW de type 4. Les PW de type 4 sont configurés avec la commande **transport-mode vlan**. Le PE distant doit être basé sur EVC et doit comprendre que la balise VLAN supérieure est la balise factice à supprimer.

  Cependant, si vous utilisez un PW de type 4 entre une plate-forme EVC et une plate-forme non EVC, cela peut entraîner des problèmes d'interopérabilité. La plate-forme non-EVC ne considère pas l'étiquette VLAN supérieure comme l'étiquette VLAN factice et transfère la trame avec l'étiquette VLAN factice 0 comme étiquette externe. Les plates-formes EVC ont la

capacité de manipuler les balises VLAN reçues sur la trame entrante avec la commande **rewrite**. Les résultats de cette manipulation de VLAN sont transportés sur le PW de type 4 avec la balise factice supplémentaire 0 au-dessus.

Les versions récentes du logiciel Cisco IOS XR offrent la possibilité d'utiliser un PW de type 4 sans utiliser la balise factice 0 avec la commande **transport-mode vlan passthrough**. La manipulation de l'étiquette VLAN sur le point de flux Ethernet (EFP) doit garantir qu'au moins une étiquette reste car il doit y avoir une étiquette VLAN transportée sur un PW de type 4 et parce que, dans ce cas, il n'y a pas d'étiquette factice qui répond à cette exigence. Les étiquettes qui restent sur la trame après la réécriture de l'étiquette d'interface entrante sont transportées de manière transparente à travers le PW.

- Un PW de type 5 est appelé PW basé sur un port Ethernet. Le PE d'entrée transporte les trames reçues sur une interface principale ou après que les balises de sous-interface ont été supprimées lorsque le paquet est reçu sur une sous-interface. Il n'est pas nécessaire d'envoyer une trame étiquetée sur un PW de type 5, et aucune étiquette factice n'est ajoutée par les plates-formes basées sur EVC. Les plates-formes basées sur EVC ont la capacité de manipuler les balises VLAN reçues sur la trame entrante avec la commande **rewrite**. Les résultats de cette manipulation de VLAN sont transportés sur le PW de type 5, étiqueté ou non.

Par défaut, les PE L2VPN tentent de négocier un PW de type 5, comme le montre 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
```

Le type de PW Ethernet indique un PW de type 5.

Il s'agit d'une capture de renifleur d'une requête ARP envoyée par le routeur 1 et encapsulée par le routeur 2 sur le PW vers le routeur 3 :

```
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)
```

L'étiquette MPLS 16031 est l'étiquette PW annoncée par le routeur 3. La capture du renifleur a été effectuée entre l'avant-dernier saut et le routeur 3, il n'y a donc pas d'étiquette IGP.

La trame Ethernet encapsulée commence immédiatement après l'étiquette PW. Il peut y avoir un mot de contrôle PW, mais il n'est pas configuré dans cet exemple.

Même s'il s'agit d'un PW de type 5, l'étiquette VLAN 2 entrante reçue sur le CA par le routeur 2 est transportée parce qu'il n'y a aucune commande **rewrite** qui l'affiche sur le CA. Les résultats qui proviennent de l'AC après le traitement de réécriture sont transportés car il n'y a pas d'apparition automatique d'étiquette sur les plates-formes basées sur EVC. Notez qu'il n'y a pas de balise VLAN 0 factice avec un PW de type 5.

Si vous avez configuré avec la commande **rewrite ingress tag pop 1 symmetric**, il n'y aurait aucune balise VLAN transportée sur le PW.

Voici un exemple d'un PW de type 4 avec la configuration d'une pw-class sur router2 et router3.

> **Remarque** : si vous configurez un type 4 sur un seul côté, le PW reste inactif et signale 'Erreur : type de PW incompatible.'

```
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 PW indique un PW de type 4.

```
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
```

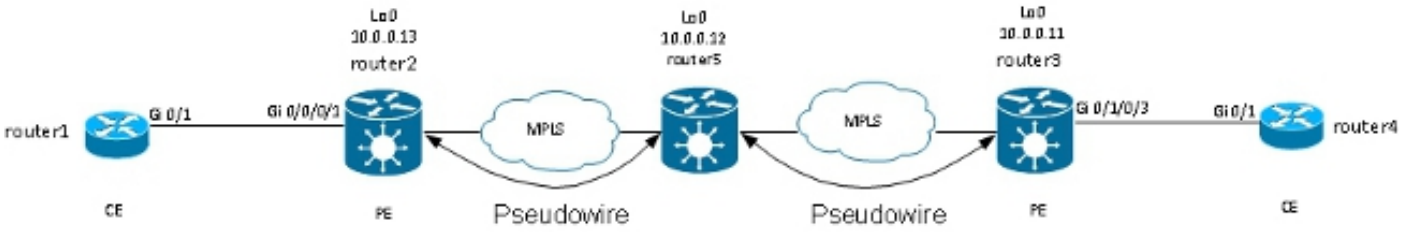
Une étiquette factice 0 est maintenant insérée au-dessus de la trame transportée :

```
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 supprime l'étiquette factice et transfère la trame avec l'étiquette 2 sur son CA local. Le PE de sortie applique la manipulation d'étiquette locale configurée sur son CA sur la trame reçue sur le PW. Si son CA local est configuré comme **symétrique de rewrite ingress tag pop 1**, la balise configurée doit être poussée dans la direction de sortie, de sorte qu'une nouvelle balise est poussée au-dessus de la balise 2 reçue sur le PW. La commande rewrite est très flexible, mais vous devez évaluer soigneusement ce que vous voulez réaliser de chaque côté du PW.

3.2.4 PW multisegment

Il est possible d'avoir un PE L2VPN qui a un PW, au lieu d'une interface physique, comme un AC :



Le routeur 5 reçoit des paquets sur le PW du routeur 2 et commute les paquets sur son autre PW vers le routeur 3. Ainsi, le routeur5 commute entre les PW afin de créer un PW multisegment entre le routeur2 et le routeur3.

La configuration sur le routeur 2 pointe désormais vers le routeur 5 en tant que 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 le routeur 5 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 dans une valeur TLV (Type Length Value) de commutation PW qui est envoyée par le routeur 5 à chaque PE distant (routeurs 2 et 3). La **description** est utile lorsque vous devez dépanner un problème de PW quand il y a un routeur au milieu qui fait la commutation de PW.

Entrez la commande **sh l2vpn xconnect** afin de passer en revue le TLV de commutation PW :

```
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)
```

Le routeur 5 envoie un TLV de commutation PW au routeur 3 avec les détails de son PW au routeur 2 et envoie un TLV de commutation PW au routeur 2 avec les détails de son PW au routeur 3.

3.2.5 Redondance

Un PW point à point peut être utilisé pour connecter deux sites, mais ces deux sites doivent rester connectés en cas de défaillance d'un PE ou d'un CA.

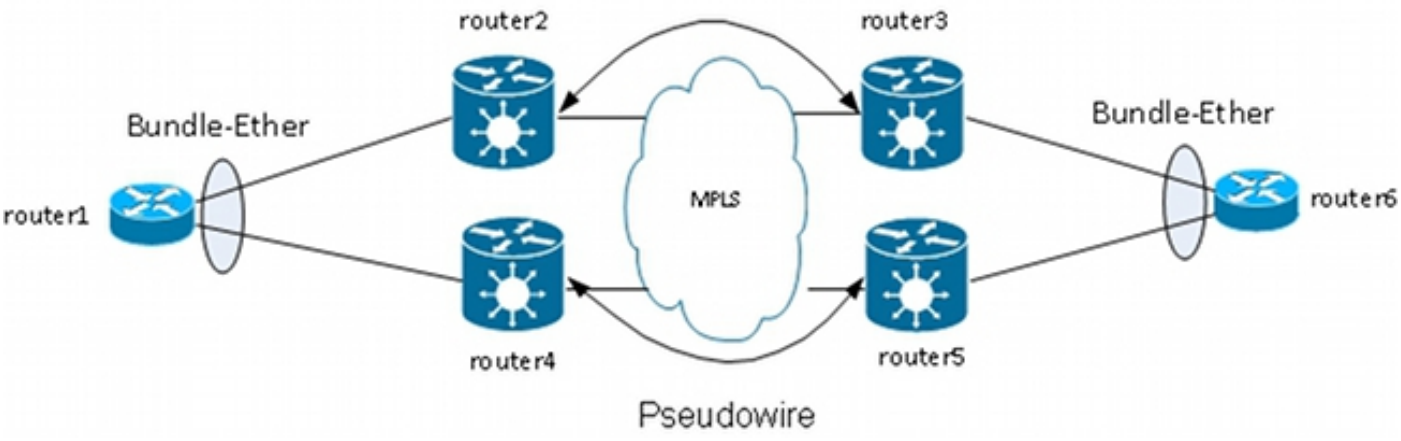
3.2.5.1 Redondance du coeur de réseau

Si vous apportez une modification à la topologie qui affecte le réacheminement dans le coeur MPLS, le PW MPLS hérite immédiatement du nouveau chemin.

3.2.5.2 Bundle sur PW

Un périphérique de périphérie client (CE) peut être connecté au PE via un bundle Ethernet afin de fournir une redondance de liaison en cas de défaillance d'une liaison membre du bundle entre le CE et le PE. Le bundle reste actif même si un membre de liaison du bundle tombe en panne. Notez que cela n'offre pas de redondance PE, car une défaillance PE entraîne l'arrêt de l'ensemble.

Une méthode de redondance consiste à transporter plusieurs circuits par des PW point à point. Chaque circuit fait partie d'un faisceau Ethernet entre deux CE :



Le PE ne termine pas le bundle et transporte les trames de manière transparente sur le PW, y compris les trames LACP (Link Aggregation Control Protocol) que les CE échangent entre eux.

Avec cette conception, la perte d'un CA ou d'un PE entraîne la chute d'un membre de l'offre groupée, mais l'offre groupée reste active.

> **Remarque** : les BPDU LACP n'ont pas été transportés sur L2VPN par l'ASR 9000 dans des versions antérieures au logiciel Cisco IOS XR version 4.2.1.

Le CE reste un point de défaillance unique dans cette conception. D'autres fonctionnalités de

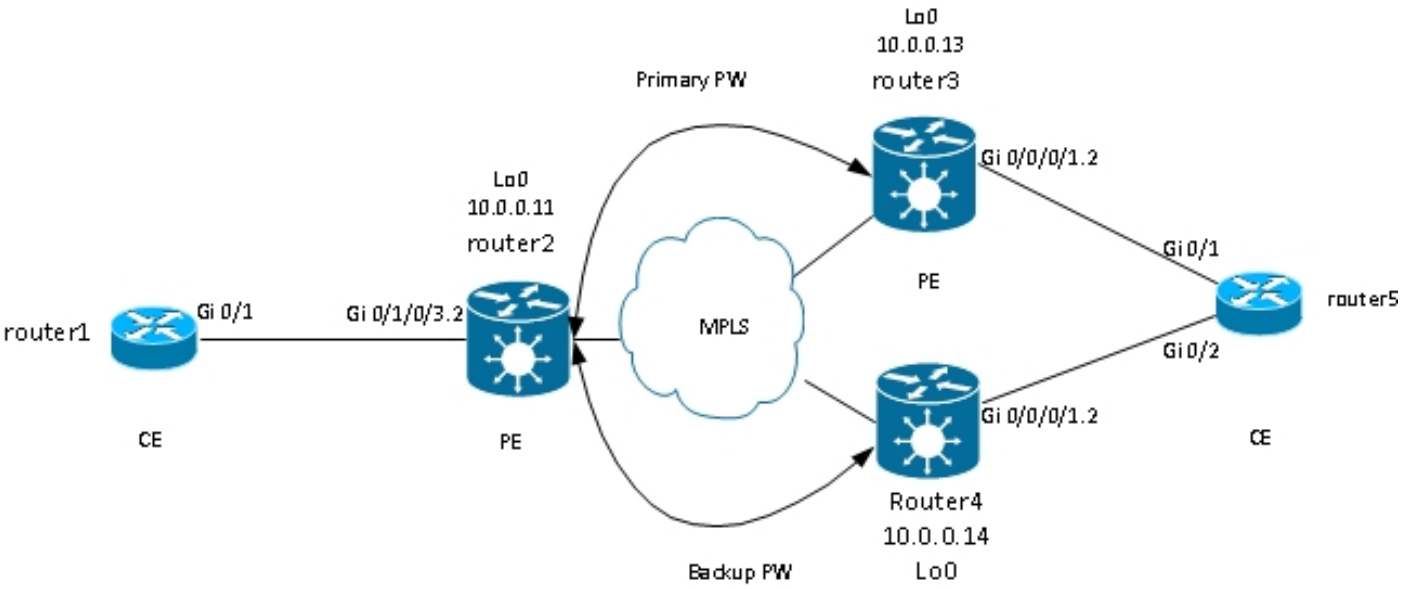
redondance peuvent être utilisées sur le CE, notamment :

- Groupe d'agrégation de liens multichâssis (MC-LAG)
- Mise en grappe de la virtualisation du réseau (nV) ASR 9000
- Système de commutation virtuel (VSS) sur les commutateurs Cisco IOS
- Virtual Port Channel (vPC) sur les commutateurs Cisco Nexus

Du point de vue du PE, il existe une connexion point à point simple entre un PC CA et un PC MPLS.

3.2.5.3 Redondance du matériel

Les PE peuvent également fournir une redondance grâce à une fonctionnalité appelée redondance PW.



Le routeur 2 dispose d'un PW principal vers le routeur 3. Le trafic entre le routeur 1 et le routeur 6 transite sur ce PW principal dans des circonstances normales. Le routeur 2 dispose également d'un PW de secours vers le routeur 4 en veille automatique, mais, dans des circonstances normales, aucun trafic ne circule sur ce PW.

En cas de problème avec le PW principal, avec le PE distant du PW principal (routeur3) ou avec le CA du PE distant (routeur3), le routeur2 active immédiatement le PW de secours et le trafic commence à le traverser. Le trafic revient au PW principal lorsque le problème est résolu.

La configuration sur le routeur 2 est la suivante :

```
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 les routeurs 3 et 4 est la suivante :

```
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 PW vers le routeur 3 est actif et le PW vers le routeur 4 est en veille :

```
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#
```

Comme l'état CA et l'état PW sont couplés, le routeur 3 signale « CA hors service » au routeur 2 lorsque le CA du routeur 3 tombe en panne. Router2 désactive son PW principal et active le PW de secours :

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

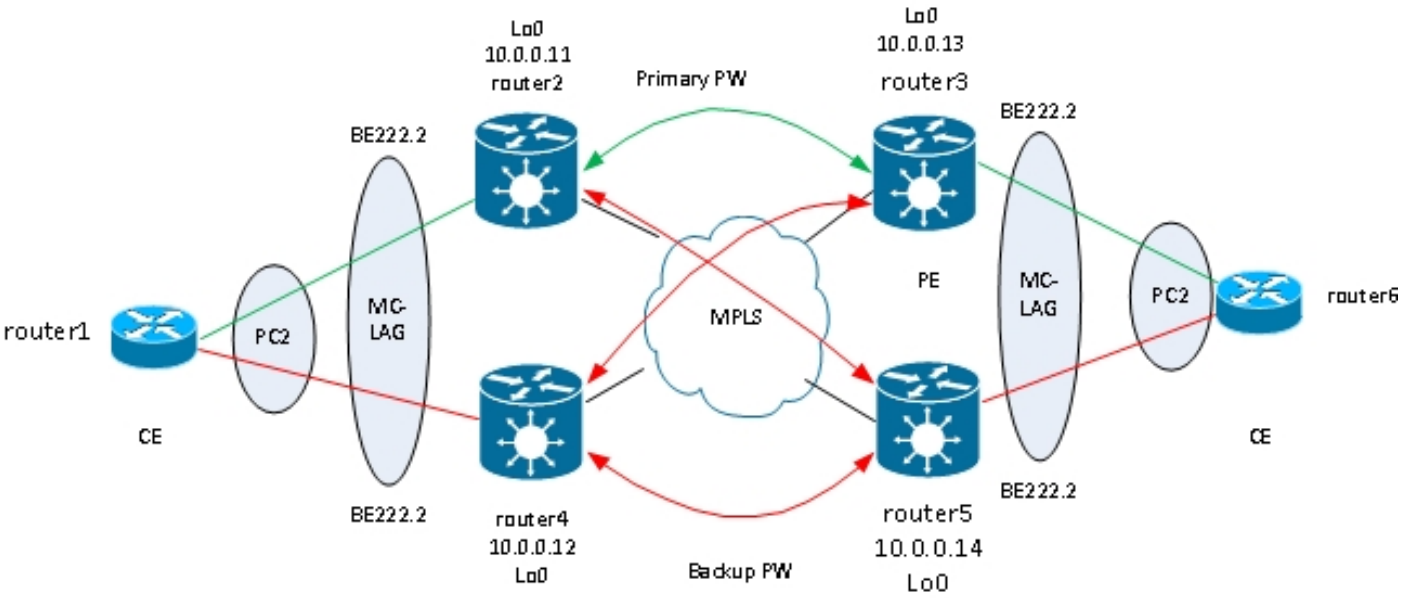
```
test p2p6 UP Gi0/1/0/3.2 UP 10.0.0.13 222 DN
Backup
10.0.0.14 222 UP
------------------------------------------------------------------------------
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test det

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#
```

Lorsque l'alimentation CA du routeur 3 est rétablie, le routeur 2 réactive l'alimentation principale vers le routeur 3 et l'alimentation vers le routeur 4 revient à l'état de veille.

Le PW de secours est également activé lorsque le routeur 3 tombe en panne et que le routeur 2 perd la route vers son bouclage.

L'étape logique suivante consiste à introduire une redondance PW bidirectionnelle avec deux PE sur chaque site :



Cependant, ce maillage complet de PW rencontre un problème lorsque deux PW sont actifs en même temps qu'une boucle est introduite dans le réseau. La boucle doit être rompue, généralement à l'aide du protocole STP (Spanning Tree Protocol). Cependant, vous ne voulez pas que l'instabilité du Spanning Tree d'un site se propage à l'autre site. Par conséquent, il est préférable de ne pas exécuter le Spanning Tree sur ces PW et de ne pas fusionner le Spanning Tree entre les deux sites . Il est plus simple d'établir une seule liaison logique entre les deux sites, de sorte qu'aucun Spanning Tree n'est requis.

Une solution consiste à utiliser un bundle MC-LAG entre les deux PE sur un site et leur CE local. Un seul des deux PE a ses membres de groupement actifs, de sorte que son PW vers le site distant est actif. L'autre PE a ses membres de groupement en état de veille et son PW vers le site

distant est arrêté. Avec un seul PW actif entre les deux sites, aucune boucle n'est introduite. Le PE avec le PW actif dispose également d'un PW de secours vers le second PE sur le site distant.

Dans des conditions stables, les membres actifs du faisceau se trouvent sur les routeurs 2 et 3, et le PW actif se trouve entre eux. Voici la configuration sur le routeur 3 :

```
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 le routeur5, le membre du groupe local et l'alimentation principale vers le routeur2 sont en veille et l'alimentation de secours vers le routeur4 est hors service :

```
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 le routeur6, le membre du groupement vers le routeur3 est actif, tandis que le membre du groupement vers le routeur5 est en veille :

```
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)
```

Lorsque le membre de l'offre groupée sur le routeur 3 tombe en panne, le membre actif du routeur 6 est connecté au routeur 5 :

```
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 inactif sur le routeur5, l'alimentation couplée au routeur2 s'arrête 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 routeur 2 détecte que son PW vers le routeur 3 est en panne et active son PW de secours vers le routeur 5 :

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

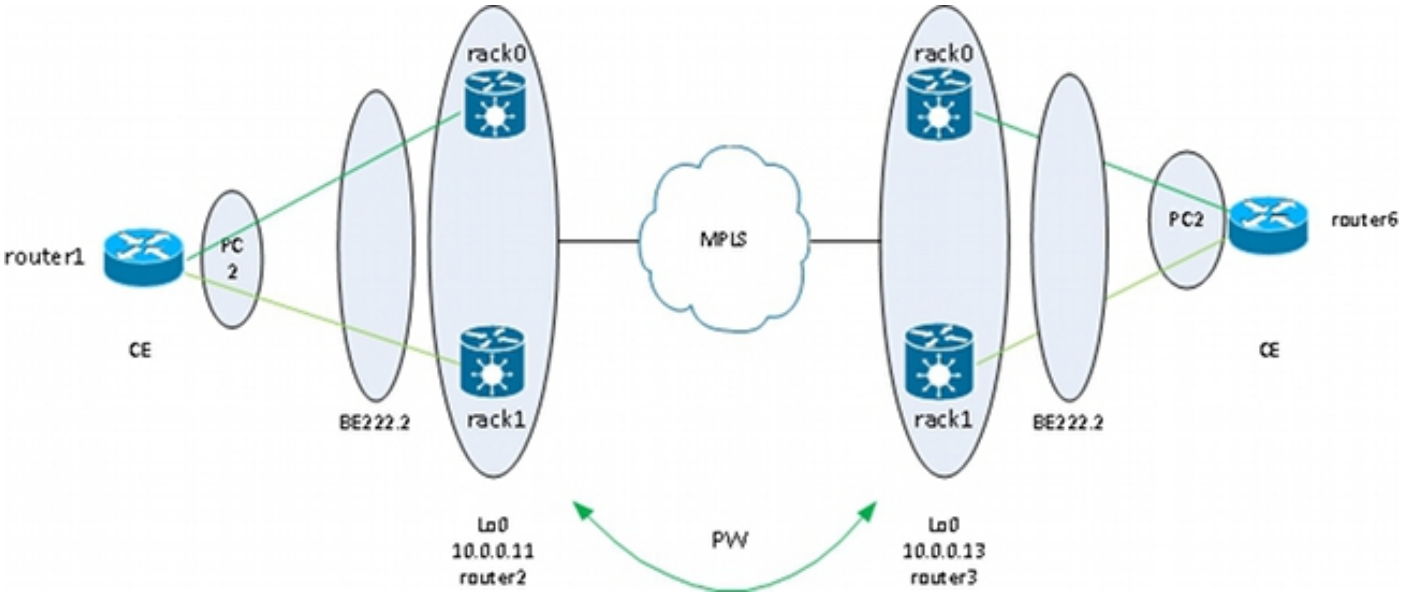
Le membre de l'offre groupée du routeur 5 est actif, ainsi que son PW principal vers le routeur 2 :

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

3.2.5.4 Cluster de périphérie nV ASR 9000

La conception précédente basée sur la redondance MC-LAG et PW fonctionne correctement pour la redondance, mais, comme certains membres de l'offre groupée sont en veille, ils ne transportent pas le trafic en conditions stables.

Si vous souhaitez que tous les membres du bundle soient actifs, même dans des conditions stables, vous pouvez utiliser un cluster ASR 9000 avec des membres du bundle CE connectés à chaque rack du PE :



Cette conception offre une redondance contre une défaillance de liaison d'un membre de l'offre groupée entre le CE et le PE, une défaillance de rack et une défaillance de liaison de coeur de réseau, tant que le cluster est relié au coeur MPLS et qu'il y a redondance dans le coeur de réseau. Les deux racks n'ont pas besoin d'être colocalisés et peuvent se trouver à des emplacements différents. Les liaisons entre les racks ne sont pas représentées dans ce schéma.

Si vous souhaitez une redondance sur le CE, vous pouvez utiliser une solution multichâssis pour le CE :

- MC-LAG
- Mise en grappe ASR 9000 nV
- VSS
- vPC

La configuration du cluster ASR 9000 est très basique :

```
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 de configurer une adresse MAC système LACP statique et une adresse MAC d'ensemble afin d'éviter un changement d'adresse MAC provoqué par un basculement de contrôleur d'étagère désigné. Cet exemple montre comment rechercher les adresses :

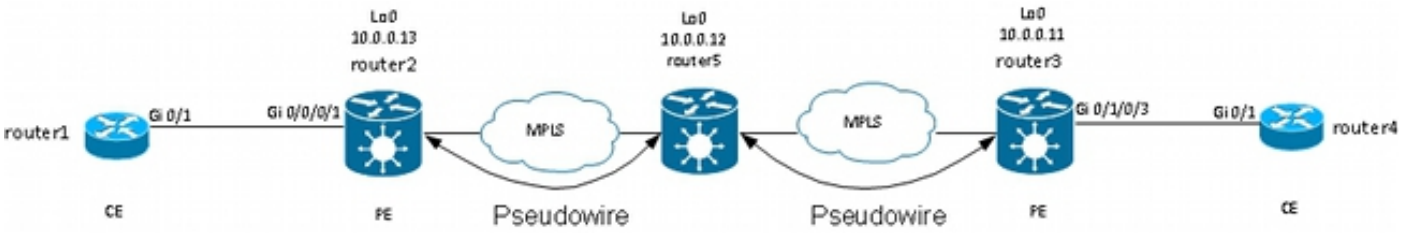
```
RP/1/RSP0/CPU0:router2#sh int bundle-ether 222 | i address is
Hardware is Aggregated Ethernet interface(s), address is 0024.f71e.d309
Internet address is Unknown
RP/1/RSP0/CPU0:router2#
RP/1/RSP0/CPU0:router2#conf
RP/1/RSP0/CPU0:router2(config)#int bundle-ether 222
RP/1/RSP0/CPU0:router2(config-if)#mac-address 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, il s'agit de l'éther de faisceau 222 avec un membre sur chaque rack (dix 0/0/0/8 sur le rack 0 et dix 1/0/0/8 sur le rack 1) et la sous-interface de faisceau configurée pour une interconnexion point à point :

```
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 commutateurs Cisco envoient généralement des paquets CDP sans balises dot1q. Il existe plusieurs scénarios qui déterminent ce qui arrive à ces paquets CDP lorsqu'ils sont reçus par un routeur IOS XR configuré pour une interconnexion :



Dans cette topologie, le routeur 1 peut voir son routeur PE local 2 comme un voisin CDP ou le routeur CE distant 4, selon la configuration.

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

Les paquets CDP provenant du CE L2VPN sont transportés via l'interconnexion. Les deux CE L2VPN se voient (avec l'utilisation de la commande **show cdp neighbors**) si l'interface principale est configurée comme l2transport ou s'il y a une sous-interface correspondant aux trames CDP non étiquetées.

Voici 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
!
!
!
!
```

Voici un exemple de sous-interface non étiquetée :

```
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 CDP sont transportés sur l'interconnexion, et les CE se voient mutuellement comme des voisins CDP. Le CE ne voit pas le PE comme un voisin 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 de L2VPN PE

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

Notez que :

- Vous ne pouvez pas configurer le protocole CDP sur une interface principale configurée comme l2transport.
- Le PE intercepte les paquets CDP lorsque le CDP est configuré sur l'interface de transport non-l2 principale. Cela se produit même si une sous-interface l2transport est configurée pour correspondre aux paquets CDP non balisés (avec l'utilisation des commandes **encapsulation untagged** ou **encapsulation default**). Dans ce cas, les paquets CDP ne sont pas transportés vers le site distant.

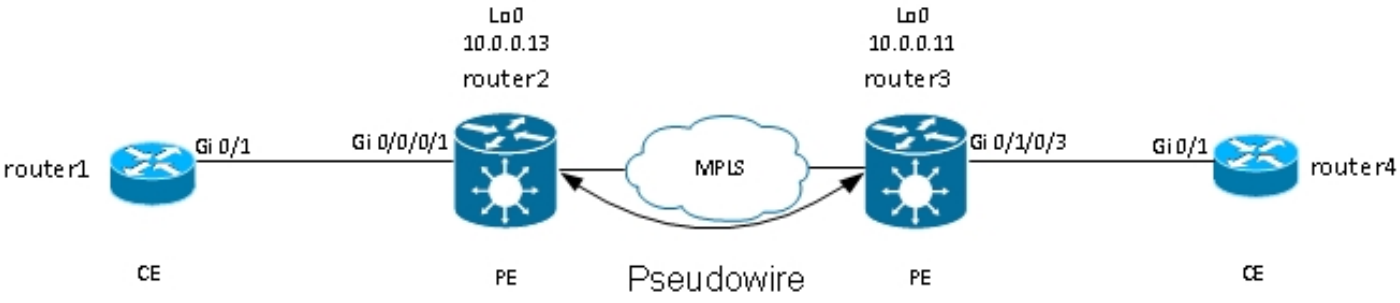
3.4 Spanning Tree

Si le CE L2VPN est un commutateur Ethernet et envoie des BPDU Spanning Tree au PE L2VPN, ces BPDU sont traitées comme du trafic régulier et sont transportées selon la configuration L2VPN.

Les BPDU STP ou MST sont envoyées sans étiquette et sont transportées via l'interconnexion point à point si l'interface principale est configurée comme l2transport ou si une sous-interface l2transport est configurée avec les commandes **encapsulation untagged** ou **encapsulation default**.

Par VLAN, Spanning Tree Plus (PVST+) ou Rapid PVST+ (PVRST+) envoient des BPDU étiquetées qui sont transportées s'il existe une sous-interface l2transport qui correspond à l'étiquette dot1q des BPDU.

Voici un exemple de topologie :



Les routeurs 2 et 3 transportent des trames non étiquetées et des trames avec l'étiquette dot1q 2 :

```
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
!
```

```
!
!
!
```

Le commutateur 1 reçoit les BPDU non étiquetées dans le VLAN 1 et les BPDU étiquetées dans le VLAN 2 du commutateur 4 ; son port racine est sur Gi0/1 vers le commutateur 4 :

```
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 Spanning Tree du site A est fusionné avec le domaine Spanning Tree du côté B. Un problème potentiel est que l'instabilité Spanning Tree d'un site peut se propager à l'autre site.

Si vous êtes certain qu'un site est connecté uniquement par l'intermédiaire d'un PW à un autre site et qu'il n'existe pas de lien de porte dérobée susceptible d'introduire une boucle physique, il est conseillé de ne pas exécuter le protocole Spanning Tree sur les deux sites. Les deux domaines Spanning Tree restent ainsi isolés. Pour ce faire, configurez un spanning tree bpdufilter sur les CE, ou configurez une liste d'accès ethernet-services sur les PE pour supprimer les trames avec l'adresse MAC de destination utilisée par les BPDU. Une liste de contrôle d’accès ethernet-services sur les PE peut être utilisée pour supprimer des trames avec l’adresse MAC de destination BPDU ou d’autres types de protocoles L2 que vous ne souhaitez pas transférer sur le PW.

Il s'agit d'une liste d'accès que vous pouvez utiliser sous chaque (sous-)interface l2transport

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
!
```

La liste de contrôle d’accès ethernet-services commence à supprimer les unités 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)
```

Le commutateur Switch1 ne reçoit plus les unités BPDU du commutateur Switch4. Le commutateur Switch1 est donc à présent 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 protocole Spanning Tree sur une liaison est le suivant : si une connexion de porte dérobée est créée entre les sites, elle introduit une boucle physique et le protocole Spanning Tree ne peut pas rompre la boucle. Ainsi, lorsque vous désactivez le protocole STP sur un PC, assurez-vous qu'il n'y a pas de liaisons redondantes entre les sites et que le PC reste la seule connexion entre les sites.

S'il existe plusieurs connexions entre les sites, utilisez une solution telle que VPLS avec une version de passerelle d'accès du Spanning Tree, telle que MST Access Gateway (MSTAG) ou PVST+ Access Gateway (PVSTAG). Reportez-vous à la section sur le service multipoint pour plus de détails.

4. Service multipoint

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

Reportez-vous à Implémentation de services de couche 2 multipoint pour une description complète des fonctionnalités de couche 2 multipoint.

Avec seulement deux interfaces dans une interconnexion point à point, un commutateur L2VPN prend tout ce qui est reçu sur le côté et le transfère sur l'autre côté.

Lorsqu'il y a plus de deux interfaces dans un domaine de pont, un commutateur Ethernet doit prendre une décision de commutation afin de déterminer où transférer les trames en fonction de leur adresse MAC de destination. Le commutateur effectue l'apprentissage MAC en fonction de l'adresse MAC source des trames qu'il reçoit et crée une table d'adresses MAC.

Le commutateur transfère les trames selon la méthode suivante :

- Les trames de diffusion sont diffusées sur tous les ports. Utilisez le contrôle des tempêtes afin de limiter le taux d'inondation de diffusion.
- Les trames de multidiffusion sont diffusées sur tous les ports du domaine de pont, sauf lorsque le protocole IGMP (Internet Group Management Protocol) ou la surveillance MLD (Multicast Listener Discovery) est configuré. Utilisez le contrôle des tempêtes afin de limiter le taux d'inondation de multidiffusion.
- Les trames de monodiffusion dont l’adresse MAC de destination ne fait pas partie de la table d’adresses MAC du domaine de pont (monodiffusion inconnue) sont diffusées sur tous les ports du domaine de pont. Utilisez le contrôle des tempêtes afin de limiter le taux d'inondation de monodiffusion inconnue.
- Les trames de monodiffusion dont l’adresse MAC de destination fait partie de la table d’adresses MAC du domaine de pont sont transmises au port où l’adresse MAC de destination a été apprise.

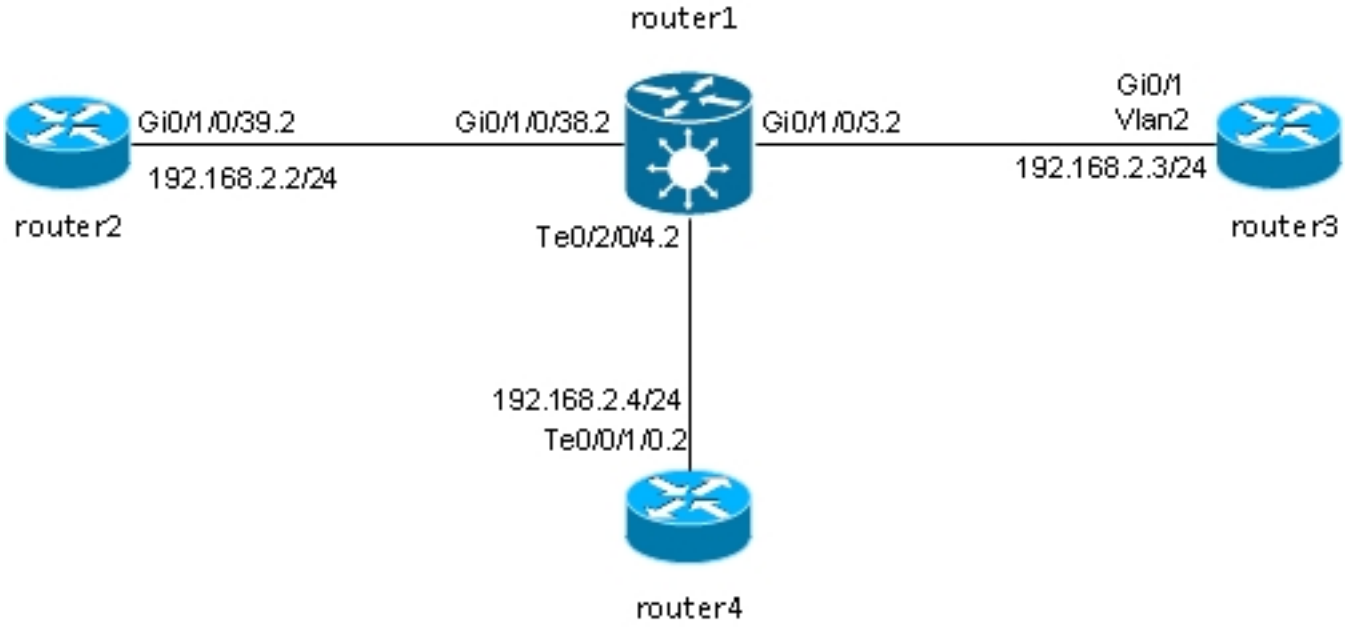
Dans le logiciel Cisco IOS XR, un domaine de diffusion ou un réseau local émulé est appelé domaine de pont. Ceci est similaire à un VLAN dans la terminologie du logiciel Cisco IOS, sauf qu'un VLAN dans IOS est lié à un numéro de VLAN qui est utilisé comme balise dot1q sur les agrégations. Un domaine de pont dans le logiciel Cisco IOS XR n'est pas lié à un numéro d'étiquette VLAN dot1q. Vous pouvez utiliser le modèle EVC afin de manipuler les balises dot1q et avoir des sous-interfaces dot1q avec différents numéros de VLAN dot1q dans le même domaine de pont ou avoir des interfaces non étiquetées.

Un domaine de pont est essentiellement un domaine de diffusion dans lequel les diffusions et les trames de multidiffusion sont diffusées. Une table d’adresses MAC est associée à chaque domaine de pont (sauf si l’apprentissage MAC est désactivé manuellement par la configuration, ce qui est très rare). Cela correspond généralement à un sous-réseau IPv4 ou IPv6 dans lequel tous les hôtes du domaine de pont sont directement connectés.

Les domaines de pont peuvent être regroupés au sein d'un groupe de ponts. C'est un moyen pratique de vérifier la configuration. Vous pouvez exécuter une commande show pour un groupe de ponts au lieu d'une commande show pour chaque domaine-pont. Un groupe de pontage n’a pas de table d’adresses MAC ou d’autres associations ; il est uniquement utilisé pour la configuration et les commandes show.

4.1 Commutation locale

Voici un exemple très simple :



Les routeurs 2, 3 et 4 sont connectés via un routeur ASR 9000, qui simule un réseau local entre ces trois routeurs.

Voici 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
!
```

Les paquets sont reçus par le routeur 1 avec l'étiquette dot1q 2 et sont transférés aux autres routeurs avec l'étiquette dot1q 2.

Dans ce scénario de base, il existe deux options sur les adaptateurs secteur :

1. Puisque tous les CA utilisent la balise dot1q 2, vous pouvez la conserver sur la trame et la transférer sur l'interface de sortie avec la même balise dot1q que celle reçue sur l'interface d'entrée. La commande **rewrite ingress tag pop 1 symmetric** n'est pas requise.

2. Vous pouvez faire sauter l'étiquette dot1q 2 entrante dans la direction d'entrée et pousser symétriquement l'étiquette dot1q 2 dans la direction de sortie. Bien que cela ne soit pas nécessaire dans ce scénario de base, il est recommandé de configurer le domaine de pont de cette manière au début, car cela offre plus de flexibilité pour l'avenir. Voici deux exemples de modifications susceptibles de se produire après la configuration initiale :

   - Si une interface BVI routée est introduite ultérieurement dans le domaine de pont, les paquets doivent être traités sur l'interface BVI sans balises. Reportez-vous à la section pour plus de détails.
   - Un nouveau contrôle d'accès, qui utilise une balise dot1q différente, est ajouté ultérieurement. L'étiquette dot1q 2 serait déplacée dans la direction d'entrée, et l'autre étiquette dot1q serait poussée sur la nouvelle interface dans la direction de sortie et vice versa.BVI

Placez les balises dot1q sur chaque CA du routeur 1 :

```
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
!
```

Affichez la configuration du domaine de pont avec les trois contrôleurs d'accès suivants :

```
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 domaine de pont doit être configuré sous un groupe de ponts. Si d'autres domaines de pont de ce client sont nécessaires, ils peuvent être configurés sous le même groupe de ponts, client1. Si de nouveaux domaines de pont appartiennent à un autre client, vous pouvez créer un nouveau groupe de ponts. Ces exemples utilisent le client afin de regrouper les domaines de pont, mais les domaines de pont peuvent être regroupés selon n'importe quel critère.

Utilisez la commande **show run l2vpn bridge group customer1 bridge-domain engineering** afin d'afficher la configuration du bridge-domain.

Utilisez la commande **show run l2vpn bridge group customer1** afin d'afficher la configuration de tous les domaines de pont.

Utilisez la commande **show l2vpn bridge-domain bd-name engineering** ou la commande **show l2vpn bridge-domain group customer1** 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 **show l2vpn bridge-domain group customer1 bd-name engineering det** si vous voulez vérifier que les paquets sont reçus et envoyés sur chaque CA.

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

```
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
```

L’apprentissage MAC est exécuté dans le matériel par les cartes de ligne chaque fois qu’une trame est reçue dans le domaine de pontage. Il existe également un cache logiciel de la table d'adresses MAC, mais cette table logicielle ne peut pas être mise à jour en continu afin de correspondre aux entrées matérielles. Lorsque la commande **show** est entrée dans le code récent, elle tente de resynchroniser la table logicielle avec la table matérielle. Après un maximum de 15 secondes, il imprime l'état actuel de la table d'adresses MAC du logiciel, même si la resynchronisation n'est pas terminée (par exemple, si la table est volumineuse). Utilisez la commande **l2vpn resynchronize forwarding mac-address-table** afin de resynchroniser manuellement les tables du logiciel et du matériel.

```
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 syslog indique que le processus de resynchronisation est terminé. Il est donc utile d'activer le **moniteur de terminal** pour afficher le message.

La colonne Resync Age indique la dernière fois que l'adresse MAC a été resynchronisée à partir de la table matérielle.

Le mot clé *location* est l'emplacement d'une carte de ligne entrante ou sortante. Les adresses MAC sont échangées entre les cartes de ligne dans le matériel, de sorte que les adresses MAC doivent être connues sur chaque carte de ligne où il y a un CA ou un PW. Le mot-clé *detail* peut fournir une version plus à jour de la table logicielle :

```
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 indique le nombre total d'adresses MAC apprises dans le domaine de pont, ainsi que le nombre d'adresses MAC apprises sous chaque CA.

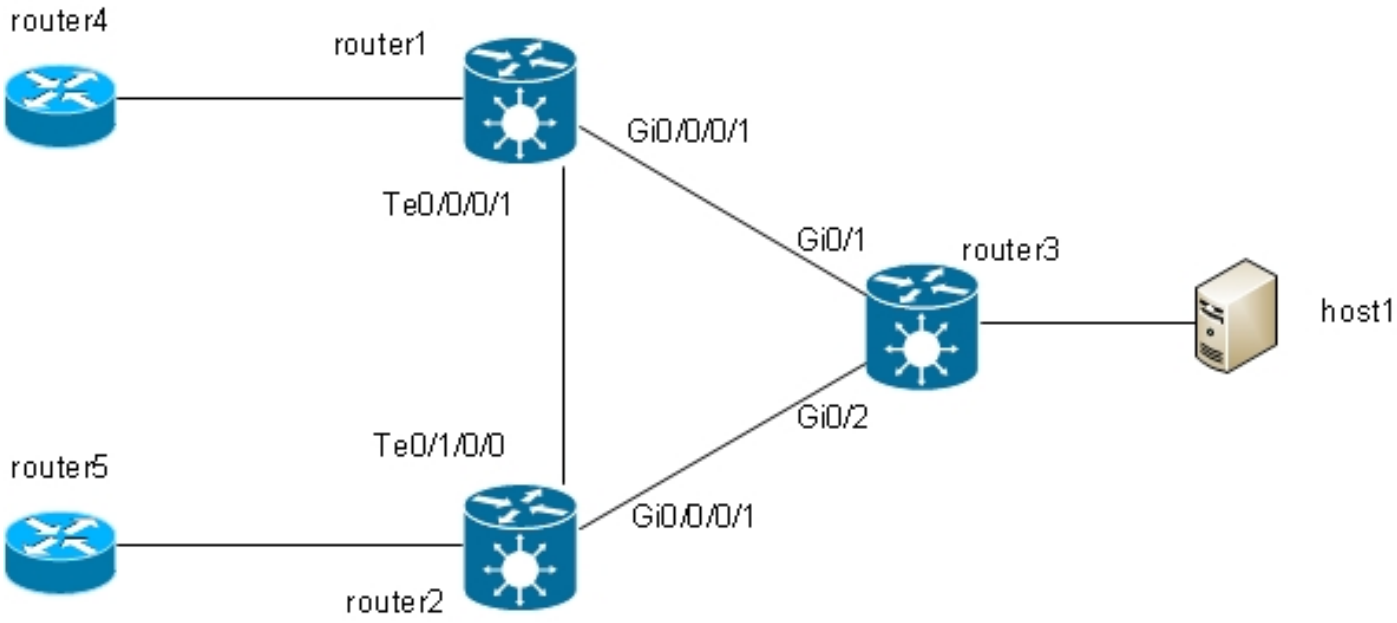
Le mot-clé *hardware* interroge la table d'adresses MAC matérielle directement à partir des moteurs de transfert d'entrée ou de sortie :

```
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 MST complet

Les exemples précédents de commutation locale étaient de base car seuls les routeurs étaient connectés au domaine de pont. Cependant, une fois que vous commencez à connecter des commutateurs L2, vous pouvez introduire une boucle et avoir besoin du protocole STP afin de rompre la boucle :



Dans cette topologie, les routeurs 1, 2 et 3 sont chacun configurés avec un domaine de pont avec toutes leurs interfaces dans le schéma. Si le routeur 4 envoie une diffusion, telle qu'une requête ARP, au routeur 1, le routeur 1 la diffuse vers les routeurs 2 et 3, le routeur 2 la diffuse vers le routeur 3 et le routeur 3 la diffuse vers le routeur 2. Il en résulte une boucle et une tempête de diffusion.

Pour rompre la boucle, utilisez un protocole STP. Il existe plusieurs types de STP, mais le logiciel Cisco IOS XR n'offre qu'une seule implémentation complète, le MST.

Il existe également des versions de passerelle d'accès des protocoles pris en charge dans le logiciel Cisco IOS XR, tels que PVSTAG et MSTAG. Il s'agit de versions statiques et limitées du protocole à utiliser dans des topologies spécifiques, généralement avec VPLS, et elles sont décrites dans les sections MSTAG et PVSTAG. Dans le logiciel Cisco IOS XR, MST est la seule option si une topologie comporte plusieurs commutateurs et si une implémentation Spanning Tree complète est requise.

Deux sous-interfaces sont configurées sur chaque routeur et ajoutées à un domaine de pont. Pour le routeur 1, la configuration est la suivante :

```
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 attribué à l'instance 1 et tous les autres VLAN restent l'instance 0 par défaut. (Une configuration plus réaliste diviserait les VLAN de manière égale entre les instances.)

La sélection du pont racine dans un réseau STP est déterminée par la priorité configurée et l'ID de pont intégré de chaque périphérique. Le périphérique avec la priorité la plus basse, ou avec la priorité la plus basse mais l'ID de pont le plus bas, est sélectionné comme pont racine. Dans cet exemple, le routeur 3 est configuré avec une priorité inférieure à celle du routeur 1 pour l’instance 0, de sorte que le routeur 3 est la racine pour l’instance 0. Le routeur 1 a une priorité inférieure à celle du routeur 3 pour l’instance 1, de sorte que le routeur 1 est la racine pour l’instance 1.

Voici la configuration du routeur 1 :

```
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
!
!
```

Voici la configuration sur le routeur 3 :

```
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 VLAN à instance doivent être identiques sur tous les commutateurs.

Vérifiez maintenant l'état du Spanning Tree sur le routeur 1 :

```
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
```

Le routeur 3 est la racine de l'instance 0, de sorte que le routeur 1 a son port racine sur Gi0/0/0/1 vers le routeur 3. Le routeur 1 est la racine de l'instance 1, de sorte que le routeur 1 est le pont désigné sur toutes les interfaces de cette instance.

Le routeur 2 est bloqué pour l'instance 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#
```

L'interface Te0/1/0/0.2 est en cours de transmission tandis que l'interface Te0/1/0/0.3 est bloquée. Lorsque la valeur STP Blocked est 0x0, la condition est false, de sorte que l'interface est en transfert ; lorsque la valeur STP Blocked est 0x1, la condition est true, de sorte que l'interface est bloquée.

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

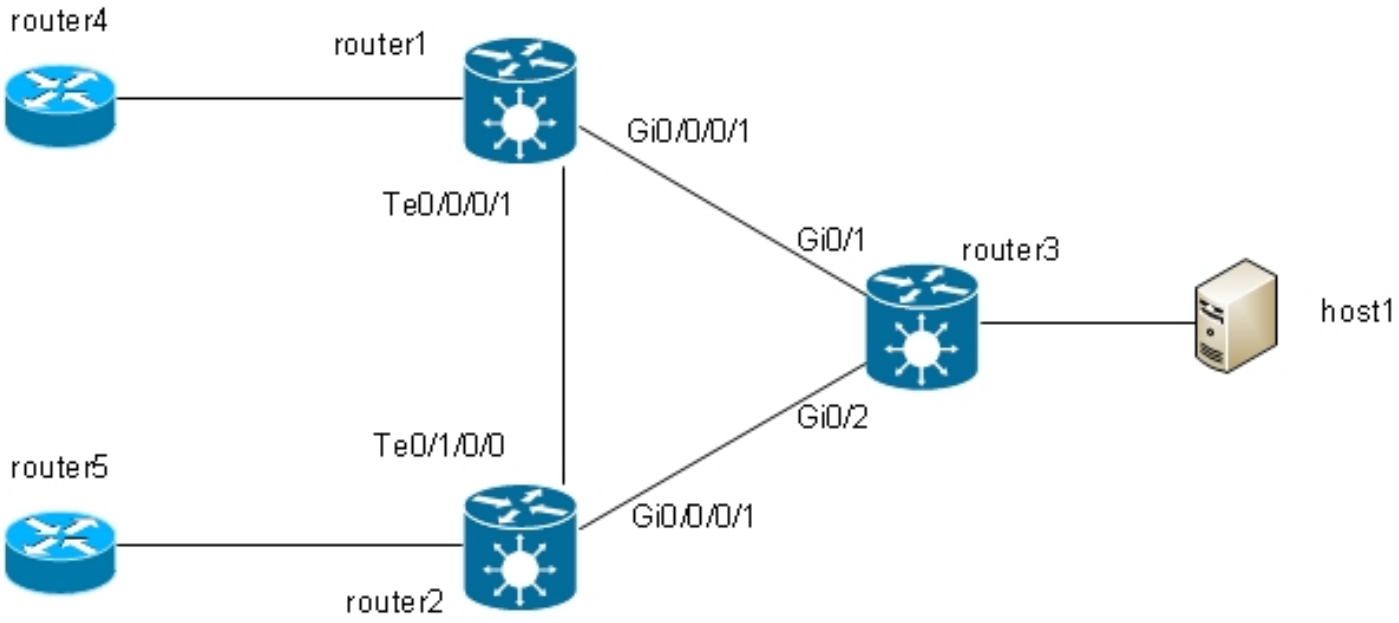
```
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.2
ingress | i Blocked
STP Blocked                      0x0
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.3
ingress | i Blocked
STP Blocked                      0x1
```

4,3 BVI

La configuration d'un domaine de pont crée un domaine L2. Afin de quitter ce domaine de couche 2, connectez les routeurs de couche 3 qui routent entre les hôtes à l'intérieur du domaine de pont et le monde extérieur. Dans le schéma précédent, l'hôte 1 pouvait utiliser le routeur 4 ou le routeur 5 afin de quitter le sous-réseau local et d'accéder à Internet.

Les routeurs 1 et 2 sur lesquels les domaines de pont sont configurés sont des routeurs ASR 9000, qui peuvent acheminer le trafic IPv4 et IPv6. Ainsi, ces deux routeurs pourraient prendre le trafic IP hors du domaine de pont et l'acheminer vers Internet eux-mêmes, au lieu de s'appuyer sur des routeurs de couche 3. Pour ce faire, vous devez configurer une interface BVI, qui est une interface de couche 3 qui se connecte à un domaine de pont afin d'acheminer les paquets en entrée et en sortie du domaine de pont.

Voici à quoi ça ressemble 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
!
```

Une interface BVI est une interface de couche 3 non étiquetée. Par conséquent, si vous souhaitez que l'interface BVI traite les paquets reçus sur les adaptateurs de domaine du pont, les adaptateurs de domaine doivent être configurés pour afficher toutes les étiquettes entrantes.

Sinon, l'interface BVI ne peut pas comprendre l'étiquette et abandonne les paquets. Il n'y a aucun moyen de configurer une sous-interface dot1q sur une interface BVI, donc les balises doivent être placées en entrée sur les adaptateurs secteur comme cela a été fait sur Gi0/0/0/1.2 dans l'exemple précédent.

Comme une interface BVI est une interface virtuelle, il existe certaines restrictions sur les fonctionnalités qui peuvent être activées. Ces restrictions sont documentées dans Configuration du routage et du pontage intégrés sur le routeur de la gamme Cisco ASR 9000 : Restrictions for Configuring IRB. Ces fonctionnalités ne sont pas prises en charge sur les interfaces BVI de l'ASR 9000 :

- Listes de contrôle d'accès (ACL). Cependant, les listes de contrôle d'accès L2 peuvent être configurées sur chaque port L2 du domaine de pont.
- Reroutage rapide IP (FRR)
- Netflow
- MoFRR (multidiffusion uniquement, réacheminement rapide)
- commutation d'étiquettes MPLS
- mVPNv4
- Qualité de service (QoS)
- Mise en miroir du trafic
- Interface non numérotée pour BVI
- Surveillance vidéo (Vidmon)

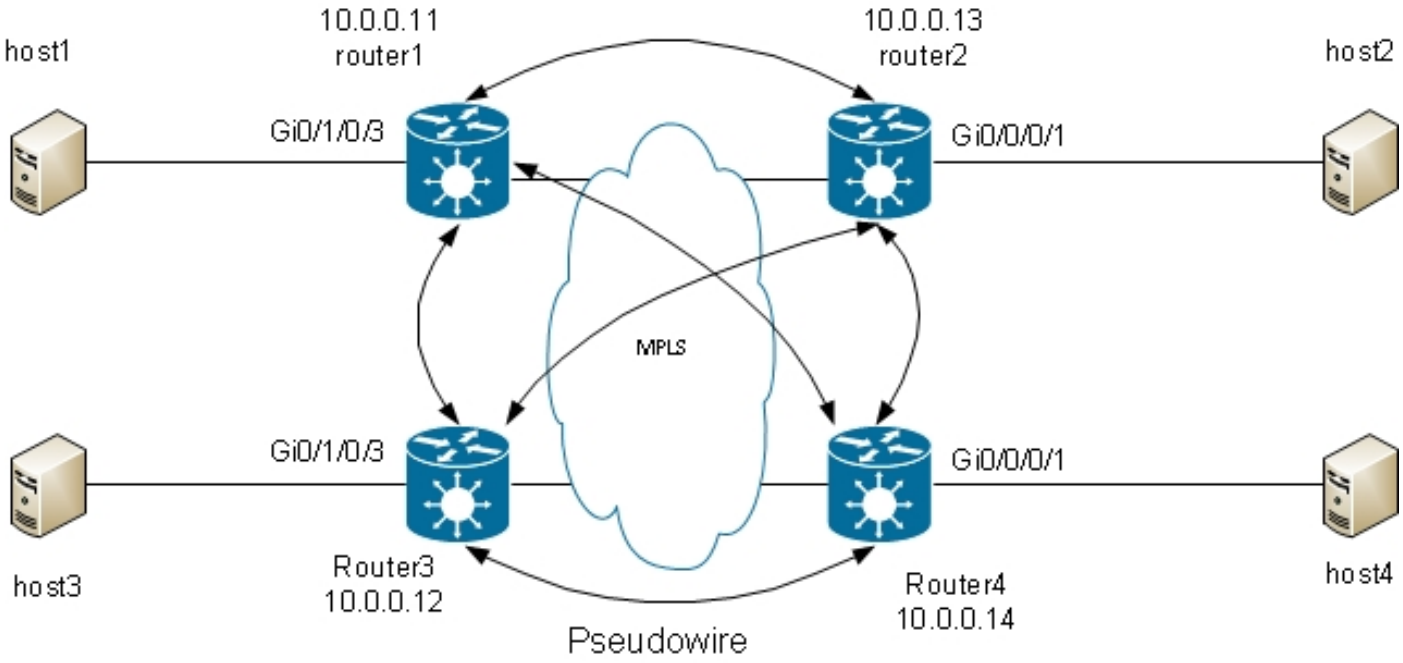
L'interface BVI peut être dans une configuration VRF (Virtual Routing and Forwarding), de sorte que le trafic reçu sur l'interface BVI est transféré sur MPLS, mais *par VRF label-allocation-mode* doit être utilisé.

Si l'une de ces fonctions restreintes est requise, vous ne pouvez pas utiliser une interface BVI. Une autre solution consiste à utiliser un câble de bouclage externe entre deux ports sur le routeur, où un port se trouve dans le domaine du pont et un port est configuré comme une interface routée normale où toutes les fonctionnalités peuvent être configurées.

4.4 VPLS

4.4.1 Vue d'ensemble

VPLS offre la possibilité de combiner des domaines de pont sur plusieurs sites en un grand domaine de pont via des PW MPLS. Les hôtes des différents sites semblent être directement connectés au même segment L2, car leur trafic est encapsulé de manière transparente sur le maillage complet des PW MPLS entre les PE L2VPN :



Un maillage complet des PW est requis afin de s'assurer que chaque hôte peut recevoir le trafic de tous les autres hôtes. La conséquence est qu'un PE L2VPN ne transfère pas une trame reçue sur un PW VPLS sur ses autres PW VPLS. Il doit y avoir un maillage complet des PW, de sorte que chaque PE reçoit le trafic directement et n'a pas besoin de transférer le trafic entre les PW puisque le transfert entraînerait une boucle. C'est ce qu'on appelle la règle du découpage d'horizon.

Le routeur exécute l'apprentissage MAC. Une fois qu'une adresse MAC est présente dans la table d'adresses MAC, vous ne transférez que la trame de cette adresse MAC de destination sur le PW vers le PE L2VPN à partir duquel cette adresse MAC a été apprise. Cela évite la duplication inutile du trafic dans le coeur. Les diffusions et les multidiffusions sont diffusées sur tous les PW afin de garantir que tous les hôtes peuvent les recevoir. Une fonctionnalité telle que la surveillance IGMP est utile car elle permet d'envoyer des trames de multidiffusion aux PE uniquement là où il y a des récepteurs ou des routeurs de multidiffusion. Cela réduit la quantité de trafic dans le coeur, bien qu'il y ait encore plusieurs copies des mêmes paquets qui doivent être envoyées à chaque PE quand il y a un intérêt pour ce groupe.

Le maillage complet des PW 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
!
!
!
!
!
```

Les PW configurés sous le VFI sont ceux qui sont entièrement maillés dans le coeur. Ils font partie du même groupe de découpage d'horizon (SHG) afin de s'assurer que les trames reçues sur un PW ne sont pas transmises à un autre PW.

Il est possible de configurer des PW d'accès, qui sont considérés comme un type de CA et ne sont pas configurés sous le VFI. Reportez-vous à la section pour plus de détails.

La configuration sur les routeurs 2, 3 et 4 est très similaire et tous les routeurs 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 de l'IPW vers 10.0.0.12 est 16049, ce qui signifie que les trames Ethernet sont reçues avec l'étiquette 16049. La décision de commutation est basée sur cette étiquette MPLS car l'avant-dernier saut MPLS aurait dû sauter l'étiquette IGP. Il peut toujours y avoir une étiquette Null explicite, mais la décision de commutation est basée sur l'étiquette PW :

```
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
```

La commande **show mpls forwarding labels** pour l'étiquette donne le numéro de domaine de pont, que vous pouvez utiliser afin de trouver l'adresse MAC de destination et le PW (neighbor et pw-id) où le paquet a été reçu. Vous pouvez ensuite créer des entrées dans la table d'adresses MAC qui pointent vers 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
```

4.4.2 Types de PW et balises transportées

Les PW VPLS sont négociés en tant que PW de type 5 (Ethernet) par défaut. Tout ce qui arrive dans le contrôle d'accès après une manipulation d'étiquette VLAN (quand la commande **rewrite** est configurée) est envoyé sur le PW.

La version 4.1.0 du logiciel Cisco IOS XR pour la signalisation LDP et la version 4.3.1 avec BGP vous permettent de configurer une classe pw sous un voisin et de configurer le **mode de transport vlan passthrough** sous la classe pw. Ceci négocie un PW de connexion virtuelle (VC) de type 4 (VLAN Ethernet), qui transporte tout ce qui sort du CA après la manipulation de l'étiquette VLAN lorsque la commande **rewrite** est configurée.

La manipulation de l'étiquette VLAN sur l'EFP garantit qu'il reste au moins une étiquette VLAN sur la trame, car vous avez besoin d'une étiquette dot1q sur la trame s'il existe des PW de type VC-4. Aucune balise factice 0 n'est ajoutée à la trame lorsque vous utilisez le mode **transport vlan passthrough**.

Une combinaison de PW de type 4 et de type 5 sous le même VFI n'est pas prise en charge. Tous les PW doivent 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 Détection automatique et signalisation

Ils étaient basés sur la configuration manuelle de tous les voisins sous le VFI. MPLS LDP a été utilisé pour la signalisation du PW avec le voisin.exemples précédents

Lorsque vous ajoutez un nouveau PE VPLS au réseau, configurez le PE afin d'avoir un PW pour tous les PE existants dans chacun de ses domaines de pont locaux. Tous les PE existants doivent ensuite être reconfigurés afin d'avoir un PW vers le nouveau PE, car tous les PE doivent être entièrement maillés. Cela pourrait devenir un défi opérationnel à mesure que le nombre de PE et de domaines de pont augmente.

Une solution consiste à demander aux PE de découvrir d'autres PE automatiquement via BGP. Bien qu'il existe également une exigence de maillage global pour l'IBGP, elle peut être levée en utilisant des réflecteurs de route. Ainsi, un nouveau PE est généralement configuré afin d'être homologue avec un petit nombre de réflecteurs de route, tous les autres PE reçoivent ses mises à jour, et le nouveau PE reçoit les mises à jour des autres PE.

Afin de découvrir d'autres PE via BGP, chaque PE est configuré pour la *famille d'adresses vpls-vpws* et annonce dans BGP les domaines de pont auxquels ils veulent participer. Une fois que les autres PE qui font partie du même domaine de pont sont découverts, un PW est établi pour chacun d'eux. BGP est le protocole utilisé pour cette détection automatique.

Il existe deux options pour la signalisation du PW aux PE détectés automatiquement : BGP et LDP. Dans ces exemples, vous convertissez la topologie précédente en découverte automatique BGP avec la signalisation BGP et la signalisation LDP.

4.4.3.1 Détection automatique BGP et signalisation BGP

Configurez la **famille d'adresses l2vpn vpls-vpws** sous le routeur bgp et les voisins, qui sont d'autres PE ou les réflecteurs de route :

```
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
!
```

La nouvelle famille d'adresses devient active avec les voisins, mais aucun PE n'a encore annoncé sa participation à un domaine de pont :

```
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 **autodiscovery bgp** et **signaling-protocol bgp** sous le mode de configuration L2VPN bridge-domain. La configuration sur le routeur 1 est la suivante :

```
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 le routeur 2 est la suivante :

```
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
!
!
!
!
!
!
```

L'ID de vpn et la cible de route sont identiques sur les différents PE pour chaque domaine de pont, mais chaque PE a un identifiant de périphérie virtuel (VE-ID) unique. Chaque PE découvre les autres PE dans le VPN via BGP et utilise BGP afin de signaler les PW. Le résultat est un maillage complet de PW :

```
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
```

Il s’agit des préfixes annoncés par le routeur 3 (10.0.0.13), tels qu’ils apparaissent sur le routeur 1. Les préfixes sont reçus via les deux réflecteurs de route, 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
```

Le routeur 1 a établi quelques PW :

```
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
```

4.4.3.2 Détection automatique BGP et signalisation LDP

La configuration BGP avec la commande **address-family l2vpn vpls-vpws** est exactement la même qu'avec la signalisation BGP. La configuration L2VPN est modifiée afin d'utiliser la signalisation LDP avec la commande **signaling-protocol ldp**.

La même configuration est utilisée sur les quatre PE :

```
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 constitué du numéro de système autonome BGP (AS) et du vpn-id.

Trois commandes show du routeur 1 illustrent que les PW ont été établis avec les PW détectés :

```
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 Vidages et retraits MAC

Le transfert dans VPLS est basé sur la table d'adresses MAC, qui est construite dynamiquement en apprenant les adresses MAC source des trames reçues. En cas de modification de topologie dans un domaine de pont, un hôte peut devenir accessible via un autre voisin AC ou VPLS. Le trafic de cet hôte risque de ne pas atteindre sa destination si les trames continuent d'être transmises conformément à la table d'adresses MAC existante.

Pour un PE L2VPN, il existe plusieurs façons de détecter une modification de topologie :

- Un port dans le domaine de pont est actif ou inactif.
- Une unité BPDU TCN (Topology Change Notification) d'arbre recouvrant est traitée lorsque le PE L2VPN exécute l'implémentation MST complète ou un protocole de passerelle d'accès d'arbre recouvrant. La liaison défaillante n'est peut-être pas locale sur le PE, mais peut être plus éloignée dans la topologie. Le PE intercepte le TCN.

Lorsqu'un PE L2VPN détecte une modification de topologie, il effectue deux actions :

1. Le PE vide la table d'adresses MAC des domaines de pont affectés par la modification de topologie. Lorsque le PE est configuré pour PVSTAG ou PVRSTAG (Per-VLAN Rapid Spanning Tree Access Gateway), une trame BPDU TCN détectée dans une sous-interface VLAN affecte tous les VLAN et domaines de pont sur cette interface physique.
2. Le PE signale aux voisins VPLS par le biais d'un message de retrait MAC MPLS LDP qu'ils doivent vider leur table d'adresses MAC. Tous les PE L2VPN distants recevant le message LDP de retrait MAC vident leurs tables d'adresses MAC et le trafic est à nouveau inondé. Les tables d'adresses MAC sont reconstruites en fonction de la nouvelle topologie.

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

- Traditionnellement, dans le logiciel Cisco IOS XR, un PE L2VPN envoyait des messages de retrait MAC lorsqu'un CA était en panne. L'intention était d'avoir des PE distants vidant leurs tables d'adresses MAC pour le domaine de pont affecté afin que les adresses MAC pointant derrière le port désactivé soient apprises à partir d'un autre port.
- Cependant, cela a créé un problème d'interopérabilité avec certains PE distants qui suivent la RFC 4762 et purgent les adresses MAC qui pointent vers tous les PE, à l'exception de celui qui envoie le message de retrait MAC. Le document RFC 4762 suppose qu'un PE envoie un message de retrait MAC lorsqu'un CA s'allume, mais pas lorsqu'un CA s'arrête. Après la version 4.2.1 du logiciel Cisco IOS XR, le comportement par défaut est d'envoyer des messages de retrait MAC LDP uniquement lorsqu'un port de domaine de pont s'active afin de mieux se conformer à la RFC. Une commande de configuration a été ajoutée afin de revenir à l'ancien comportement.

Il s'agit d'une commande show avec le comportement par défaut après la version 4.2.1 du 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:
```

La ligne importante est « MAC remove sent on bridge port down », qui est maintenant désactivé par défaut après la version 4.2.1 du logiciel Cisco IOS XR. La commande indique également le nombre de messages de retrait MAC envoyés et reçus dans le domaine de pont. Un nombre élevé de messages de retrait indique une instabilité dans le domaine de pontage.

Voici la configuration qui revient à l'ancien comportement :

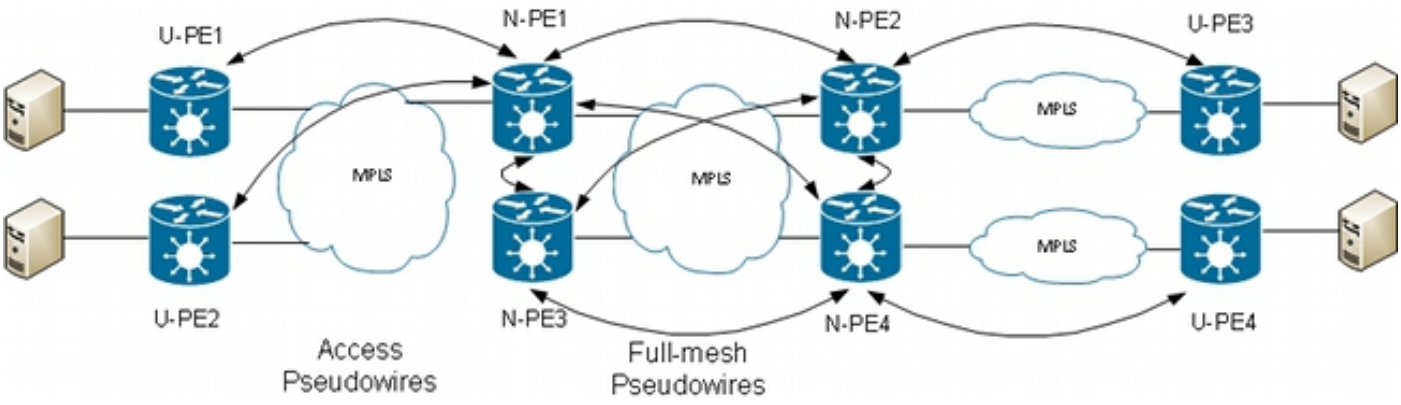
```
l2vpn
bridge group customer1
bridge-domain finance
mac
withdraw state-down
!
!
!
!
```

4.4.5 H-VPLS

VPLS nécessite un maillage complet des PW entre les PE L2VPN afin de garantir que tout PE peut atteindre, dans un saut, un hôte derrière tout autre PE sans qu'un PE ait besoin de refléter les trames d'un PW à un autre PW. C'est la base de la règle de découpage d'horizon, qui empêche un PE de transférer des trames d'un PW à un autre. Même dans des cas particuliers, lorsque l'adresse MAC de destination dans la table d'adresses MAC pointe vers un autre PW, la trame est abandonnée.

Un maillage complet des PW signifie que le nombre de PW peut devenir très élevé à mesure que le nombre de PE augmente, ce qui peut entraîner des problèmes d'évolutivité.

Vous pouvez réduire le nombre d'ordinateurs personnels dans cette topologie avec une hiérarchie d'ordinateurs personnels :



Dans cette topologie, notez que :

- Un périphérique utilisateur Provider Edge (U-PE) est doté de contrôleurs d'accès aux CE.
- Le périphérique U-PE transporte le trafic CE sur un PW point à point MPLS vers un périphérique N-PE (Provider Edge) du réseau.
- Le N-PE est un PE VPLS principal qui est entièrement maillé avec d'autres N-PE.
- Sur le N-PE, le PW provenant du U-PE est considéré comme un PW d'accès, tout comme un CA. Le U-PE ne fait pas partie du maillage avec les autres N-PE, de sorte que le N-PE peut considérer le PW d'accès comme un CA et transférer le trafic de ce PW d'accès aux PW principaux qui font partie du maillage VPLS complet.
- Les PW principaux entre les N-PE sont configurés sous une VFI afin de garantir que la règle de découpage d'horizon est appliquée à tous les PW principaux configurés sous la VFI.
- Les PW d'accès des PE-U ne sont pas configurés sous un VFI, ils n'appartiennent donc pas au même SHG que les PW VFI. Le trafic peut être transféré d'un PW d'accès à un PW VFI et vice versa.
- Les PE-U peuvent utiliser la fonctionnalité de redondance des PG afin d'avoir une PG principale vers un PE-N principal et une PG de secours vers un PE-N de secours. Le mode veille prend le relais lorsque l'alimentation principale tombe en panne.

Voici un exemple où U-PE1 (10.0.0.15) est configuré avec une redondance PW vers N-PE1 (10.0.0.11) et 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 PW vers 10.0.0.12 est en état de veille. Sur N-PE1, il y a un PW d'accès à 10.0.0.15 et un AC qui ne sont pas sous le VFI.

N-PE1 apprend certaines adresses MAC sur les PW d’accès et les PW VFI :

```
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), le PW d'accès est en état de veille :

```
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 à horizon divisé (SHG)

La règle de découpage d'horizon stipule qu'une trame reçue sur une PW VFI ne peut pas être transférée sur une autre PW VFI. Les N-PE VFI doivent être entièrement maillés.

Ce découpage d'horizon est imposé par un SHG :

- Les membres d'un SHG ne peuvent pas se transférer des trames entre eux, mais peuvent transférer des trames aux membres d'autres SHG.
- Tous les PW VFI sont affectés à SHG 1 par défaut. Cela garantit qu'il n'y a pas de transfert entre les PW VFI, de sorte que la règle de découpage d'horizon est appliquée. Les paquets reçus sur un PW VFI peuvent être transférés vers des AC et des PW d'accès, car ils ne font pas partie du même SHG.
- Par défaut, tous les AC et les PW d'accès ne font pas partie d'un groupe SHG, ce qui signifie que les paquets reçus sur un AC ou un PW d'accès peuvent être transférés vers un autre AC ou un PW d'accès dans le même domaine de pont.
- Les AC et les PW d'accès peuvent être assignés au SHG 2 avec la commande **split-horizon group** si le but est d'empêcher le transfert 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
```

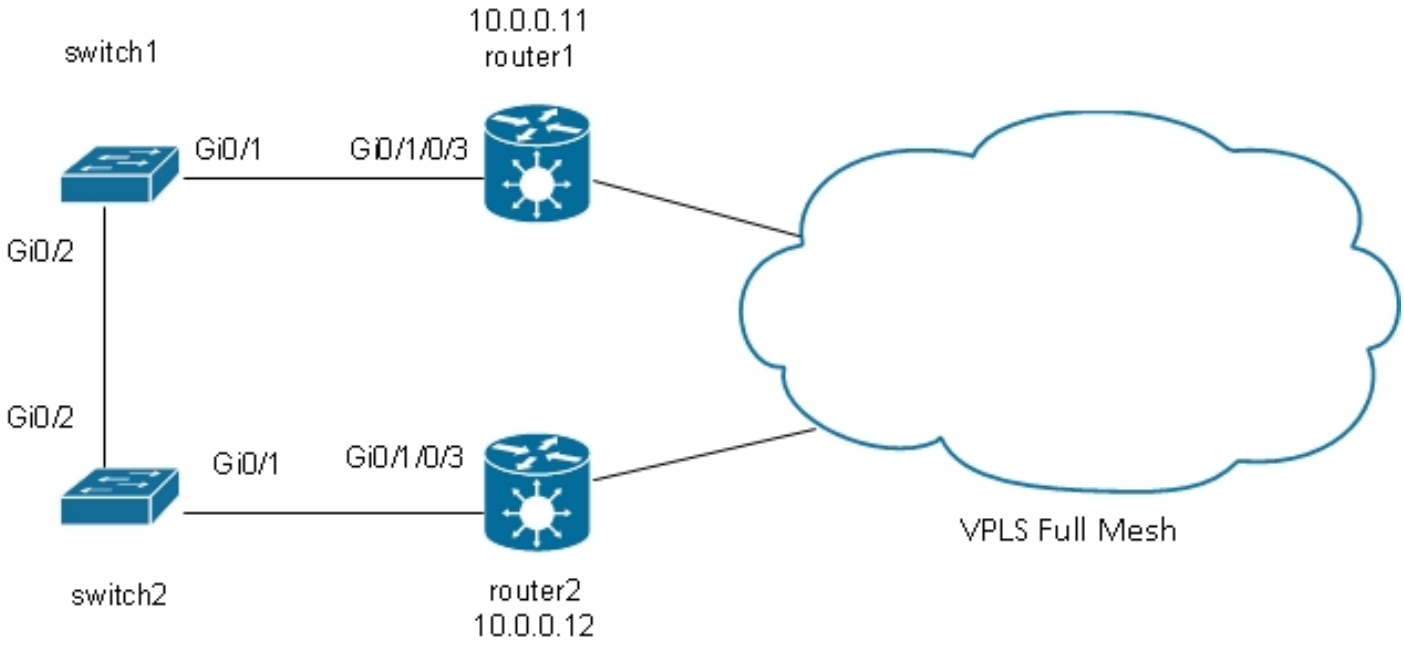
```
!
neighbor 10.0.0.15 pw-id 15
split-horizon group
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
```

Dans cette configuration, il n'y a pas de transfert entre Gi 0/0/0/1.2 et Gi 0/1/0/3.2, Gi 0/0/0/1.2 et 10.0.0.15, ou Gi 0/1/0/3.2 et 10.0.0.15. Mais il peut toujours y avoir un transfert de trafic entre les AC et les PW VFI parce qu'ils font partie de SHG différents (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

Pour tenter d'introduire la redondance, vous pouvez avoir un site qui est attaché en double au domaine VPLS :



Si un hôte connecté au commutateur 1 envoie une diffusion, le commutateur 1 la transfère au routeur 1 et au commutateur 2. Le routeur 1 a un maillage complet de PW, il y a donc un PW vers le routeur 2, et le routeur 1 transfère la diffusion sur ce PW. Le routeur 2 transfère la diffusion au commutateur 2, qui la transfère au commutateur 1. Il en résulte une boucle physique.

4.4.7.1 Spanning Tree

L'implémentation MST complète ne fonctionne pas avec VPLS parce que cette implémentation envoie des BPDU MST sur une interface principale afin de contrôler l'état de transmission de tous les VLAN sur cette interface. Avec VPLS, il existe des VFI pour chaque domaine de pont, de sorte que vous ne pouvez pas envoyer de BPDU sur une interface principale pour toutes ces VFI.

Par défaut, les unités BPDU Spanning Tree sont transportées sur des VPLS et des PW point à point.

Si le commutateur 1 et le commutateur 2 envoient des BPDU par VLAN ou des BPDU MST non balisées et si les BPDU correspondent aux sous-interfaces de transport l2 sur les routeurs 1 et 2, les BPDU sont transportées via VPLS. Les commutateurs voient leurs BPDU respectifs sur les interfaces Gi 0/1, et le protocole Spanning Tree rompt la boucle et bloque un port.

Le commutateur 2 est la racine du 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)
```

Le commutateur Switch1 a son port racine sur Gi 0/1 et bloque 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 unités BPDU sont également transportées vers des sites distants et que l'instabilité du Spanning Tree dans un site se propage à tous les sites connectés au domaine VPLS. Il est plus sûr d'isoler chaque site et de ne pas transporter de BPDU sur VPLS.

Une solution consiste à utiliser une version de passerelle d'accès du protocole STP. Il s'agit d'une implémentation limitée du protocole, où les PE L2VPN sont configurés pour envoyer des BPDU statiques afin d'apparaître connectés à la racine du Spanning Tree. Le PE L2VPN ne transporte pas les BPDU reçues des CE vers les sites distants, de sorte que chaque site possède son propre domaine Spanning Tree.

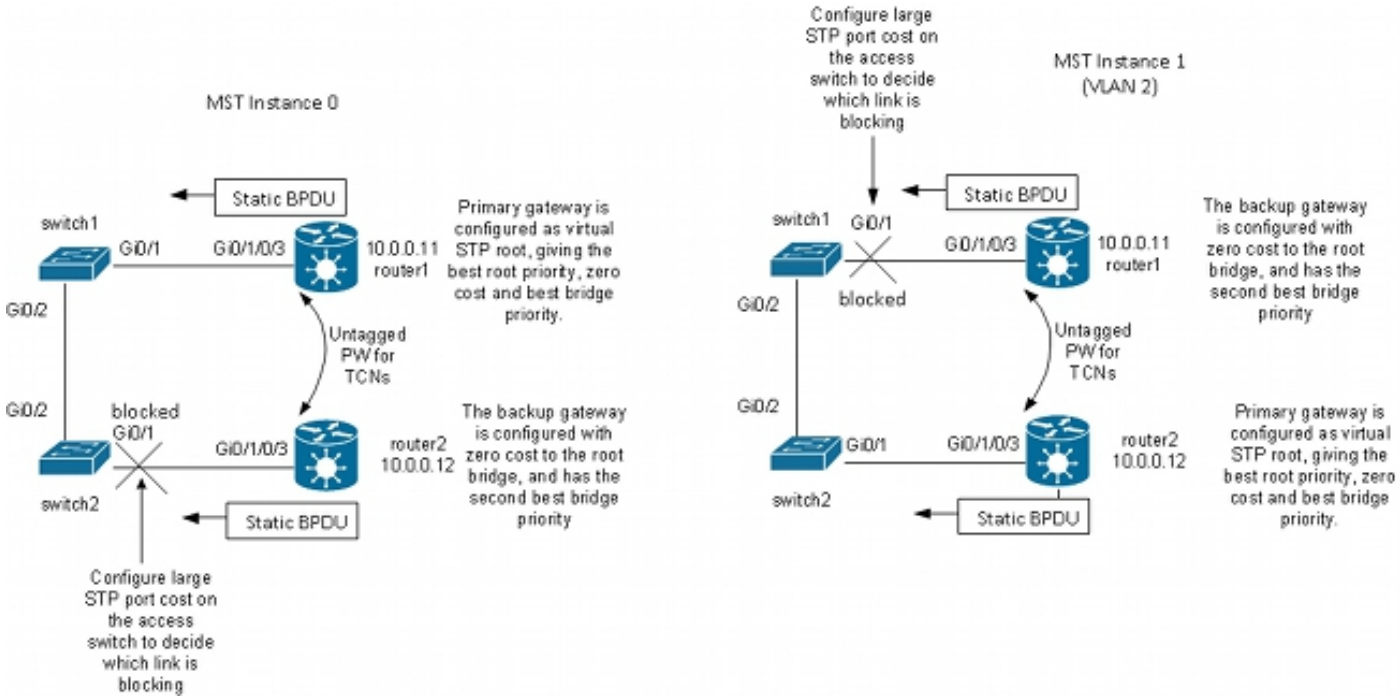
4.4.7.2 MSTAG

Comme expliqué dans la section Spanning Tree, MST envoie des BPDU non balisées, mais ces BPDU contrôlent l'état de transmission de tous les VLAN sur l'interface.

Les VLAN peuvent être regroupés en plusieurs instances et chaque instance possède son propre état de transmission.

Les VLAN sont généralement regroupés de sorte que le trafic puisse être réparti uniformément entre plusieurs chemins. Lorsqu'il y a deux chemins, la moitié du trafic appartient à une instance qui transfère sur le premier chemin et bloque sur le second chemin. L'autre moitié du trafic appartient à une instance qui bloque sur le premier chemin et qui transfère sur le second chemin. Cela permet un équilibrage de charge entre les deux chemins dans des conditions stables. Sinon, vous avez un chemin qui est normalement complètement bloqué et qui devient actif uniquement lorsque le chemin principal est inactif.

Voici une topologie MSTAG type :



Dans cet exemple de travaux pratiques, l'instance 1 a le VLAN 2 et l'instance 0 a les autres VLAN. (Dans un scénario plus réaliste, les VLAN sont répartis entre plusieurs instances afin d'obtenir un bon équilibrage de charge de trafic entre les instances.) Comme certains VLAN ont beaucoup plus de trafic que d'autres, il n'y a pas toujours le même nombre de VLAN dans chaque instance.

Voici la configuration pour l'instance 0 de MST :

- Les routeurs 1 et 2 envoient des unités BPDU statiques en fonction de la configuration MSTAG. Ils ne traitent pas les trames BPDU entrantes du réseau ou ne tentent pas d'exécuter une implémentation complète. Avec MSTAG, les deux PE L2VPN envoient simplement des BPDU statiques en fonction de leur configuration MSTAG.
- Le routeur 1 est configuré afin d'attirer le trafic de l'instance 0 en apparaissant comme étant la racine de cette instance.
- Le routeur 2 est configuré avec la deuxième meilleure priorité racine pour l'instance 0, de sorte qu'il devienne la nouvelle racine en cas de panne du routeur 1 ou de la prise en charge CA entre le commutateur 1 et le routeur 1.
- Le commutateur 2 est configuré avec un coût Spanning Tree élevé sur le port Gi 0/1 vers le routeur 2 afin de s'assurer que son chemin principal vers la racine est sur Gig 0/2 via le commutateur 1 et le routeur 1.
- Le commutateur 2 sélectionne Gi 0/2 comme port racine pour l'instance 0 et Gi 0/1 comme port alternatif en cas de perte de la racine.
- Ainsi, le trafic provenant de ce site dans les VLAN appartenant à l'instance 0 atteint d'autres sites via VPLS via le routeur 1.

Pour l'instance MST 1 (VLAN 2), la configuration est inversée :

- Le routeur 2 est configuré afin d'attirer le trafic de l'instance 1 en apparaissant comme étant la racine de cette instance.
- Le routeur 1 est configuré avec la deuxième meilleure priorité racine pour l'instance 1, de sorte qu'il devienne la nouvelle racine en cas de panne du routeur 2 ou de la prise en charge CA entre le commutateur 2 et le routeur 2.

- Le commutateur Switch1 est configuré avec un coût Spanning Tree élevé sur le port Gi 0/1 vers le routeur Router1 afin de s'assurer que son chemin principal vers la racine est sur Gig 0/2 via le commutateur Switch2 et le routeur Router2.
- Switch1 sélectionne Gi 0/2 comme port racine pour l'instance 1 et sélectionne Gi 0/1 comme port alternatif en cas de perte de la racine.
- Ainsi, le trafic provenant de ce site dans les VLAN appartenant à l'instance 1 (VLAN 2 dans cet exemple) atteint d'autres sites via VPLS via le routeur 2.
- Il doit y avoir une sous-interface sur les routeurs 1 et 2 afin d'attraper les TCN non balisés et de les transférer via un PW point à point à l'autre routeur. Étant donné que les commutateurs 1 et 2 peuvent perdre leurs liaisons directes et être isolés l'un de l'autre, les routeurs 1 et 2 doivent transférer les TCN entre eux via ce PW point à point.
- Les PE interceptent également les TCN, vident leurs tables d'adresses MAC et envoient le retrait MAC LDP aux PE distants.

Voici la configuration sur le routeur 1 :

```
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 que :

- Dans l’instance MST 0, le pont racine est 0000.0000.0001, qui est l’ID de pont du routeur 1.
- Dans l’instance MST 1, le pont racine est 0000.0000.0002, qui est l’ID de pont du routeur 2.
- La priorité de pont du routeur 1 est 4096 dans l’instance 0 (pour devenir la racine) et 8192 dans l’instance 1 (pour devenir la meilleure racine).
- La priorité de pont du routeur 1 est 8192 dans l’instance 0 (pour devenir la deuxième meilleure racine) et 4096 dans l’instance 1 (pour devenir la racine).
- L'interconnexion point à point sur GigabitEthernet0/1/0/3.1 transporte les TCN MST non étiquetés vers l'autre routeur.

Une liste de contrôle d’accès de sortie a été configurée sur les sous-interfaces dot1q afin de supprimer les BPDU par VLAN qui pourraient être envoyées par un autre site qui n’a pas encore été migré vers MST. Cette configuration empêche le commutateur CE de déclarer que l'interface est incohérente lorsqu'il reçoit une trame BPDU par VLAN sur une interface configurée pour MST.

La configuration du routeur 2 est très similaire :

```
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
```

Voici 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 de l'instance 0 est transféré via le routeur 1 et le trafic de l'instance 1 est transféré via le commutateur 2 et le routeur 2.

La configuration du commutateur 2 utilise les mêmes commandes que celle du commutateur 1 :

```
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
```

Le commutateur 2 passe par le commutateur 1 et le routeur 1 pour l'instance 0 et par le routeur 2 pour l'instance 1.

Le trafic est équilibré en charge, car une instance quitte le site via le routeur 1 et l'autre instance quitte le site via le routeur 2.

Si la liaison entre le routeur 1 et le commutateur 1 est interrompue, les deux instances passent par le routeur 2.

```
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
```

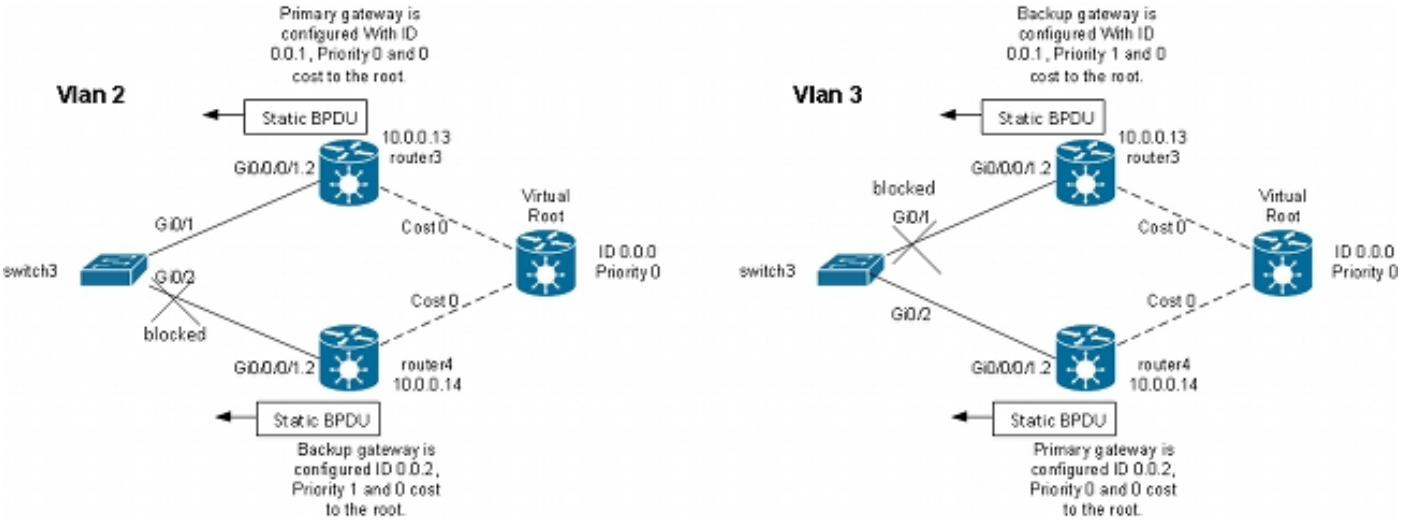
```
Interface Role Sts Cost Prio.Nbr Type
------------------ ---- --- --------- -------- ------------------------------
Gi0/1 Root FWD 20000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p
```

Une convergence rapide peut être obtenue dans ce type de défaillance, car le chemin par la racine de deuxième choix a déjà été sélectionné comme chemin alternatif. Avec MSTAG, les BPDU MST ne sont pas transportées sur VPLS, de sorte que les sites sont isolés de l'instabilité dans d'autres sites.

4.4.7.3 PVSTAG ou PVRSTAG

MSTAG est le protocole de passerelle d'accès préféré pour VPLS, car il utilise le protocole Rapid Spanning Tree et parce qu'il est évolutif avec l'utilisation d'instances plutôt que de BPDU sur chaque VLAN.

Si un site ne peut pas être migré vers MST et que 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 ne peut y avoir qu'un seul commutateur CE. Vous ne pouvez pas avoir deux commutateurs comme dans la topologie MSTAG. Dans MSTAG, vous pouvez configurer un PW point à point afin de transporter le trafic non étiqueté (y compris les TCN BPDU) d'un PE à l'autre lorsque le site est divisé en deux parties. Avec PVST et PVRST, les TCN sont envoyés étiquetés de sorte qu'ils correspondent à la même sous-interface que le trafic de données à transporter sur VPLS. Le routeur doit identifier les unités BPDU en fonction de l'adresse MAC et du type de protocole afin de transmettre les TCN à l'autre extrémité. Comme cette fonctionnalité n'est pas prise en charge actuellement, un seul périphérique CE est requis.

Une autre exigence des versions antérieures au logiciel Cisco IOS XR version 4.3.0 est que les interfaces du bundle ne peuvent pas être utilisées comme CA. Cette restriction a été levée dans le logiciel Cisco IOS XR version 4.3.0.

Le principe est sensiblement le même qu'avec MSTAG. Le routeur PVSTAG envoie des BPDU statiques de sorte que le CE semble être connecté à des commutateurs qui sont directement connectés à la racine (virtuelle) avec un coût 0. Afin d'équilibrer la charge du trafic, certains VLAN

peuvent être configurés avec la racine sur le routeur 3 et d'autres avec la racine sur le routeur 4.

Voici un exemple de configuration sur le routeur 3 :

```
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
```

Voici un exemple de configuration sur le routeur 4 :

```
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
```

Voici un exemple de configuration sur le commutateur CE3 :

```
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 de PVSTAG est très similaire à celle de MSTAG, à ceci près que la priorité racine et la priorité de la passerelle principale sont configurées comme 4096 et la priorité de la passerelle de secours est configurée comme 8192 dans l'exemple de MSTAG.

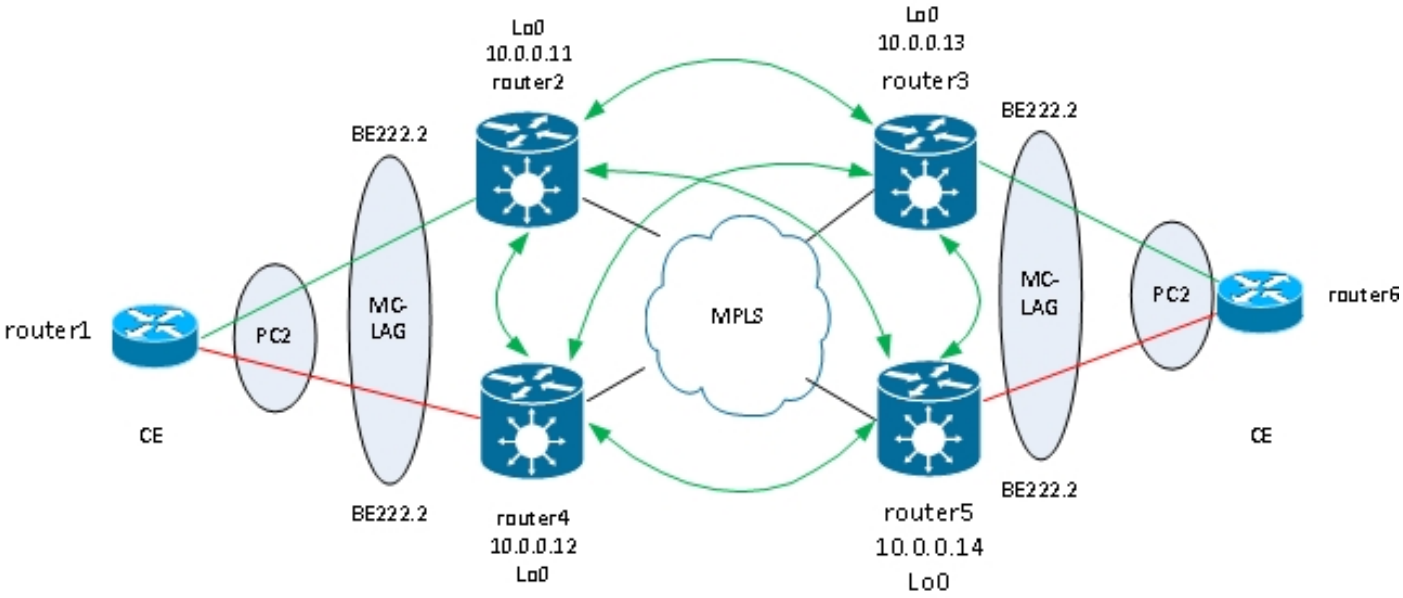
Tous les autres commutateurs des domaines doivent avoir des priorités supérieures à celles configurées dans PVSTAG ou PVRSTAG.

Vous pouvez régler le coût d'interface sur les commutateurs CE afin d'influencer quel port devient le port racine et quel port est bloqué.

4.4.7.4 MC-LAG

La configuration MC-LAG avec VPLS est plus simple que les PW point à point avec redondance des PW bidirectionnels. Au lieu d'un PW principal et de trois PW de secours, les PE n'ont besoin

que d'un maillage complet de PW VPLS, standard avec VPLS :



Dans cette topologie, notez que :

- MC-LAG fonctionne entre les deux PE VPLS de gauche : router2 et router4.
- Dans des conditions normales, les membres du groupement sont actifs entre le routeur 1 et le routeur 2 et en veille entre le routeur 1 et le routeur 4.
- Les sous-interfaces de l'ensemble du routeur 2 sont configurées sous les domaines de pont VPLS, de sorte que le routeur 2 transfère le trafic vers les PE VPLS distants. Deux sites sont illustrés dans le schéma de topologie, mais il pourrait y en avoir bien d'autres.
- Les PE distants apprennent les adresses MAC du routeur 1 et des périphériques derrière via le routeur 2, de sorte que les PE transfèrent le trafic pour ces adresses MAC de destination via le routeur 2.
- Lorsque la liaison entre le routeur 1 et le routeur 2 est interrompue ou lorsque le routeur 2 est interrompu, le membre de l'ensemble entre le routeur 1 et le routeur 4 devient actif.
- Comme le routeur 2, le routeur 4 a ses sous-interfaces de groupe configurées sous les domaines de pont VPLS.
- Lorsque les sous-interfaces du groupe sont activées sur le routeur 4, ce dernier envoie des messages de retrait MAC LDP aux PE VPLS distants afin de les informer d'une modification de topologie.

Voici la configuration sur le routeur 3 :

```
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 le bundle MC-LAG configuré, ajoutez-le sous la configuration VPLS comme n'importe quel autre CA.

Voici la configuration correspondante sur le routeur 5 :

```
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
!
!
!
!
!
```

Dans des circonstances normales, le membre de groupement entre le routeur 3 et le routeur 6 est actif et le membre entre le routeur 5 et le routeur 6 est en veille :

```
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 en provenance du CE est reçu sur le routeur 3 et transféré vers des PE distants :

```
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 montre que le routeur 3 apprend certaines adresses MAC sur son groupe et que les membres actifs se trouvent sur le routeur 3. Sur le routeur 5, il n'y a aucune adresse MAC apprise sur l'ensemble, car le membre local est en état de veille :

```
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
```

Lorsque le membre de l'offre groupée entre les routeurs 3 et 6 tombe en panne, il devient actif sur le routeur 5. Les PE VPLS MC-LAG envoient un message de retrait MAC LDP afin que les PE distants purgent leurs tables d'adresses MAC et apprennent l'adresse MAC via le nouveau routeur PE MC-LAG actif5.

Le routeur 2 reçoit un message de retrait MAC du routeur 3 et du routeur 5 lorsque le membre actif du groupe MC-LAG passe du routeur 3 au routeur 5 :

```
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 le routeur 2 se déplacent du routeur 3 (10.0.0.13) vers le routeur 5 (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
```

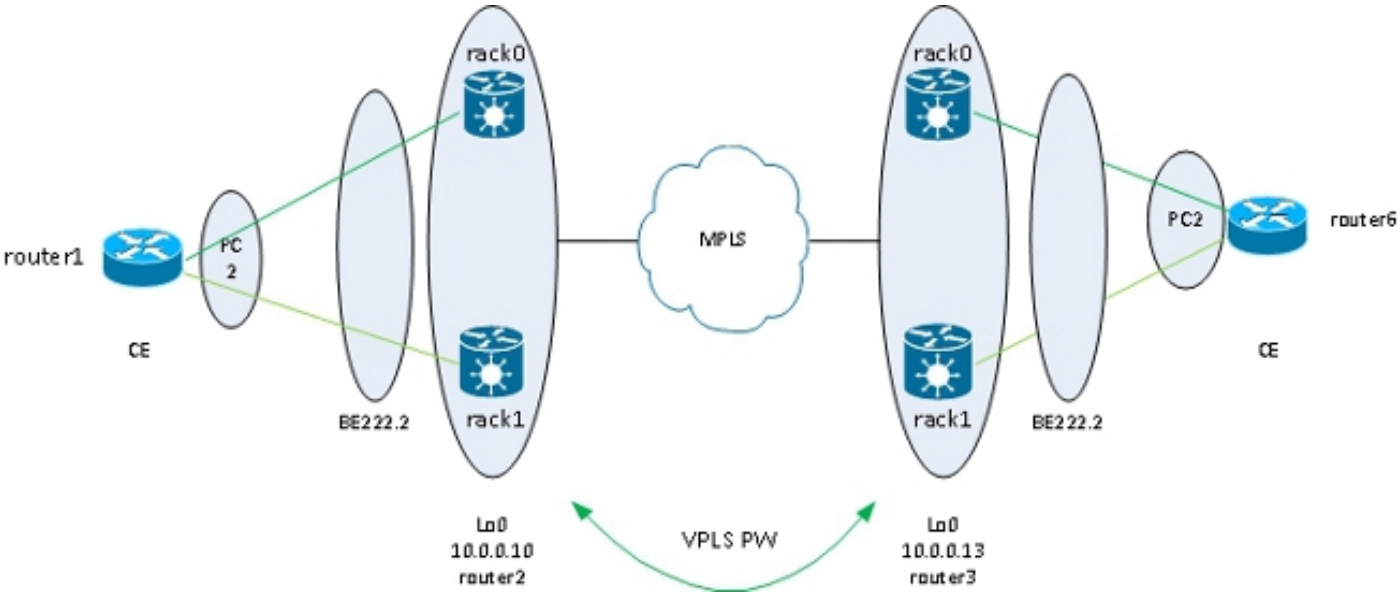
Avec MC-LAG, un site peut utiliser un seul bundle à relier aux autres sites via VPLS. MC-LAG fournit la liaison et la redondance PE, mais logiquement, il s'agit toujours d'une interface groupée pour atteindre d'autres sites. Le Spanning Tree n'est pas requis sur ce bundle, et un filtre BPDU pourrait être configuré sur le CE afin de s'assurer que les BPDU ne sont pas échangés entre les sites sur VPLS.

Une autre option est la configuration d'une liste de contrôle d'accès ethernet-services sur les adaptateurs de contrôle d'accès du bundle afin de supprimer les adresses MAC de destination des BPDU afin que les BPDU ne soient pas transportées entre les sites. Cependant, si une liaison de porte dérobée est introduite entre les sites, le protocole Spanning Tree ne peut pas rompre la boucle, car il ne fonctionne pas sur le bundle MC-LAG. Par conséquent, évaluez soigneusement s'il faut désactiver le protocole Spanning Tree sur le bundle MC-LAG. Si la topologie entre les sites est soigneusement entretenue, il est agréable d'avoir une redondance via MC-LAG sans avoir besoin de Spanning Tree.

4.4.7.5 Cluster de périphérie nV ASR 9000

La solution MC-LAG assure la redondance sans avoir à utiliser le protocole Spanning Tree. Un inconvénient est que les membres de l'offre groupée d'un PE MC-LAG sont à l'état de veille. Il s'agit donc d'une solution de veille active qui n'optimise pas l'utilisation de la liaison.

Une autre option de conception est l'utilisation d'un cluster ASR 9000 nV Edge afin que les CE puissent avoir des membres de groupement à chaque rack de cluster qui sont tous actifs en même temps :



Un autre avantage de cette solution est que le nombre d'PV est réduit car il n'y a qu'un PV par cluster pour chacun des clusters sur chaque site. Lorsqu'il y a deux PE par site, chaque PE doit disposer d'un PW pour chacun des deux PE de chaque site.

La simplicité de la configuration est un autre avantage. La configuration ressemble à une configuration VPLS de base avec un domaine de pont avec des blocs d'alimentation CA et des blocs d'alimentation VFI :

```
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 assurée par le double hébergement CA du bundle sur les deux racks, de sorte que le bundle reste actif en cas de défaillance de l'élément de bundle ou du rack.

Lorsqu'un site est connecté au domaine VPLS uniquement via un cluster, la topologie est similaire à celle de MC-LAG en ce qui concerne le Spanning Tree. Le protocole Spanning Tree n'est donc pas requis sur ce bundle et un filtre BPDU pourrait être configuré sur le CE afin de garantir que les BPDU ne sont pas échangées entre les sites sur VPLS.

Une autre option est la configuration d'une liste de contrôle d'accès ethernet-services sur les adaptateurs de contrôle d'accès du bundle afin de supprimer les adresses MAC de destination des BPDU afin que les BPDU ne soient pas transportées entre les sites. Cependant, si une liaison de porte dérobée est introduite entre les sites, le protocole Spanning Tree ne peut pas rompre la boucle, car il ne fonctionne pas sur le bundle CE-PE. Par conséquent, évaluez soigneusement s'il faut désactiver le protocole Spanning Tree sur ce bundle CE-PE. Si la topologie entre les sites est soigneusement mise à jour, il est préférable d'avoir une redondance via le cluster sans avoir besoin de Spanning Tree.

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

Il y a une nouvelle fonctionnalité introduite dans la version 4.3.1 afin de surmonter la limitation de MC-LAG, où certaines liaisons de bundle sont inutilisées car elles restent en mode veille. Dans la nouvelle fonctionnalité, appelée *Pseudo MCLAG*, toutes les liaisons du DHD vers les points d'attache (PoA) sont en cours d'utilisation, mais les VLAN sont divisés entre les différents ensembles :

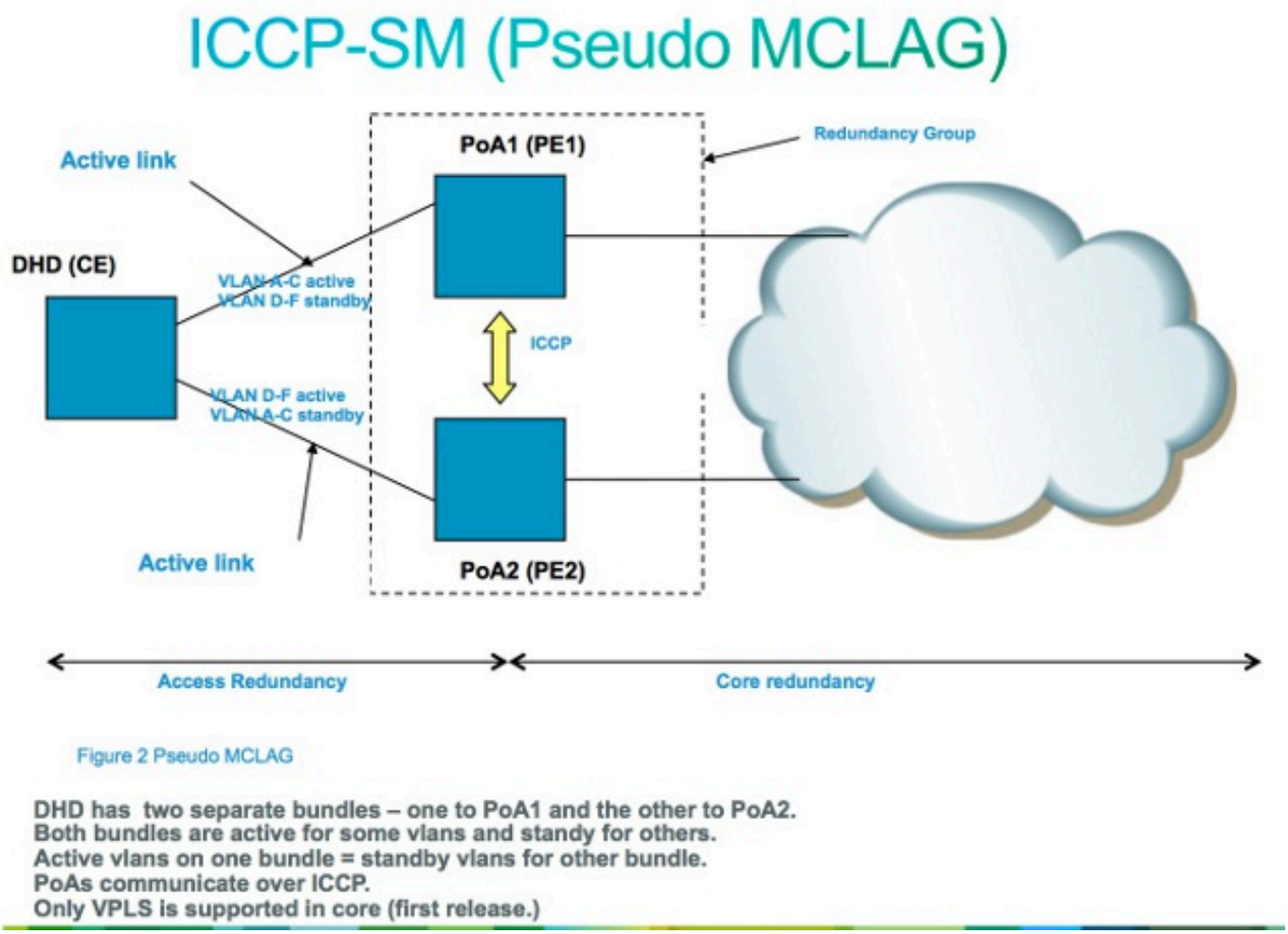


Figure 2 Pseudo MCLAG

4.5 Contrôle des tempêtes de trafic

Dans un domaine de diffusion de couche 2, il existe un risque qu'un hôte se comporte mal et envoie un taux élevé de trames de diffusion ou de multidiffusion qui doivent être diffusées partout dans le domaine de pont. Un autre risque est la création d'une boucle L2 (qui n'est pas interrompue par le Spanning Tree), qui entraîne des diffusions et des multidiffusions en boucle des paquets. Un taux élevé de diffusions et de paquets de multidiffusion affecte les performances des hôtes dans les domaines de diffusion.

Les performances des périphériques de commutation du réseau peuvent également être affectées par la réplication d'une trame d'entrée (diffusion, multidiffusion ou trame de monodiffusion inconnue) vers plusieurs ports de sortie dans le domaine de pontage. La création de plusieurs copies du même paquet peut être gourmande en ressources, en fonction de l'emplacement à l'intérieur du périphérique où le paquet doit être répliqué. Par exemple, la réplication d'une diffusion vers plusieurs emplacements différents n'est pas un problème en raison des capacités de réplication multidiffusion du fabric. Les performances d'un processeur réseau peuvent être affectées lorsqu'il doit créer plusieurs copies du même paquet à envoyer sur certains ports que le processeur réseau gère.

Afin de protéger les périphériques en cas de tempête, la fonctionnalité de contrôle de tempête de trafic vous permet de configurer un taux maximal de diffusions, de multidiffusion et de monodiffusions inconnues à accepter sur un domaine de pont AC. Pour plus d'informations, reportez-vous au Guide de configuration de la sécurité du système du routeur à services d'agrégation de la gamme Cisco ASR 9000, version 4.3.x : Mise en oeuvre du contrôle des

tempêtes de trafic sous un pont VPLS.

Le contrôle des tempêtes de trafic n'est pas pris en charge sur les interfaces CA ou les PW VFI groupés, mais il est pris en charge sur les PW d'accès et les PW non groupés. La fonctionnalité est désactivée par défaut ; à moins que vous ne configuriez le contrôle des tempêtes, vous acceptez tout taux de diffusions, de multidiffusion et de monodiffusions inconnues.

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 d'abandon du contrôle d'orage sont toujours présents dans le résultat de la commande **show l2vpn bridge-domain detail**. Étant donné que la fonctionnalité est désactivée par défaut, les compteurs commencent à signaler les abandons uniquement lorsque la fonctionnalité a été configurée.

Les débits configurés peuvent varier selon le modèle de trafic d'un réseau à l'autre. Avant de configurer un débit, Cisco vous recommande de comprendre le débit des trames de diffusion, de multidiffusion ou de monodiffusion inconnue dans des circonstances normales. Ajoutez ensuite une marge dans le débit configuré au-dessus du débit normal.

4.6 Déplacements MAC

En cas d'instabilité du réseau, telle qu'une défaillance d'interface, une adresse MAC peut être acquise à partir d'une nouvelle interface. Il s'agit d'une convergence réseau normale et la table d'adresses MAC est mise à jour dynamiquement.

Cependant, des déplacements MAC constants indiquent souvent une instabilité du réseau, telle qu'une instabilité grave au cours d'une boucle L2. La fonction de sécurité des adresses MAC vous

permet de signaler les déplacements MAC et de prendre des mesures correctives, telles que la fermeture d'un port incriminé.

Même si une action corrective n'est pas configurée, vous pouvez configurer la commande **logging** afin d'être alerté de l'instabilité du réseau par le biais des messages MAC move :

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

Dans cet exemple, l'action est configurée sur aucune, de sorte que rien n'est fait lorsqu'un déplacement MAC est détecté, sauf qu'un message syslog est consigné. Voici un exemple de message :

```
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 Surveillance IGMP et MLD

Par défaut, les trames de multidiffusion sont diffusées vers tous les ports d'un domaine de pont. Lorsque vous utilisez des flux à haut débit comme des services de télévision sur IP (IPTV), il peut y avoir une quantité importante de trafic transféré sur tous les ports et répliqué sur plusieurs PW. Si tous les flux TV sont transférés sur une interface, cela peut congestionner les ports. La seule option est la configuration d'une fonctionnalité telle que la surveillance IGMP ou MLD, qui intercepte les paquets de contrôle de multidiffusion afin de suivre les récepteurs et les routeurs de multidiffusion et de transférer les flux sur les ports uniquement lorsque cela est approprié.

Pour plus d'informations sur ces fonctionnalités, reportez-vous au document Cisco ASR 9000 Series Aggregation Services Router Multicast Configuration Guide, Release 4.3.x.

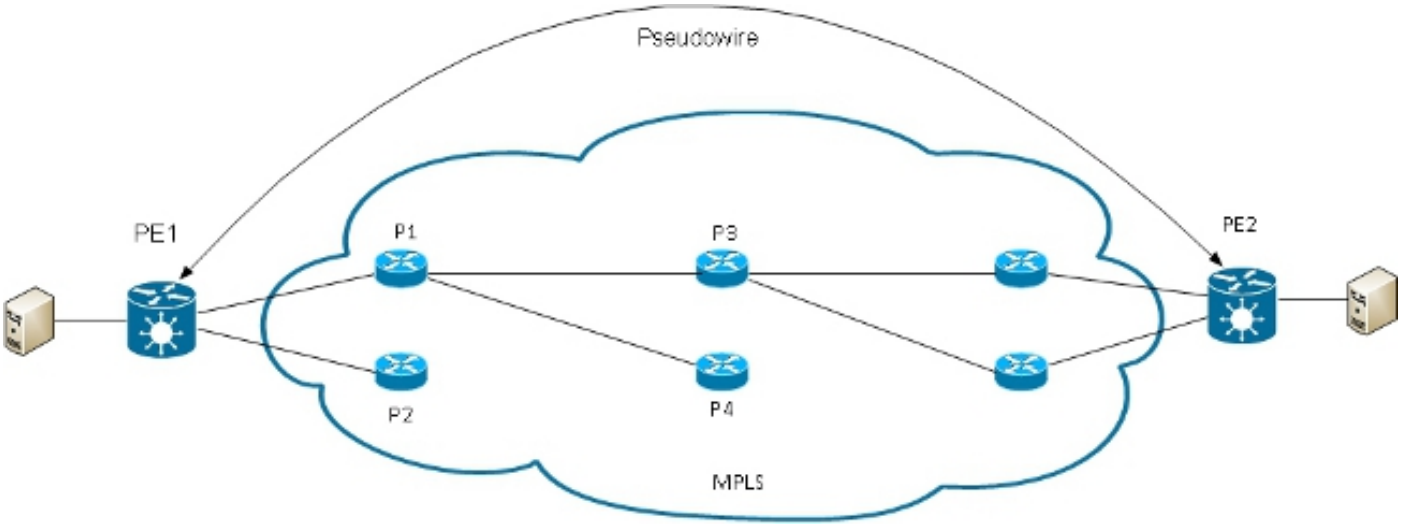
5. Rubriques supplémentaires sur L2VPN

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

5.1 Équilibrage de charge

Lorsqu'un PE L2VPN doit envoyer une trame sur un PW MPLS, la trame Ethernet est encapsulée dans une trame MPLS avec une ou plusieurs étiquettes MPLS ; il y a au moins une étiquette PW et peut-être une étiquette IGP afin d'atteindre le PE distant.

La trame MPLS est transportée par le réseau MPLS vers le PE L2VPN distant. Il existe généralement plusieurs chemins pour atteindre le PE de destination :



Remarque : tous les liens ne sont pas représentés dans ce schéma.

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

Les fournisseurs de services MPLS préfèrent que toutes les liaisons soient utilisées de la même manière plutôt qu'une liaison encombrée avec d'autres liaisons sous-utilisées. Cet objectif n'est pas toujours facile à atteindre car certains PW transportent beaucoup plus de trafic que d'autres et parce que le chemin emprunté par un trafic PW dépend de l'algorithme de hachage utilisé dans le coeur. Plusieurs PW à bande passante élevée peuvent être hachés sur les mêmes liaisons, ce qui crée un encombrement.

Une exigence très importante est que tous les paquets d'un flux doivent suivre le même chemin. Dans le cas contraire, les trames sont désordonnées, ce qui peut avoir un impact sur la qualité ou les performances des applications.

L'équilibrage de charge dans un réseau MPLS sur des routeurs Cisco est généralement basé sur les données qui suivent l'étiquette MPLS inférieure.

- Si les données immédiatement après l'étiquette inférieure commencent par 0x4 ou 0x6, un routeur IP MPLS suppose qu'il y a un paquet IPv4 ou IPv6 à l'intérieur du paquet MPLS et tente d'équilibrer la charge en fonction d'un hachage des adresses IPv4 ou IPv6 source et de destination extraites de la trame. En théorie, cela ne devrait pas s'appliquer à une trame Ethernet encapsulée et transportée sur un PW, car l'adresse MAC de destination suit l'étiquette inférieure. Mais récemment, certaines plages d'adresses MAC commençant par 0x4 et 0x6 ont été attribuées. Le routeur IP MPLS peut considérer à tort que l'en-tête Ethernet est en fait un en-tête IPv4 et hacher la trame en fonction de ce qu'il suppose être les adresses source et de destination IPv4. Les trames Ethernet d'un PW peuvent être hachées sur

différents chemins dans le coeur MPLS, ce qui entraîne des trames hors séquence dans le PW et des problèmes de qualité des applications. La solution est la configuration d'un mot de contrôle sous une pw-class qui peut être attaché à un PW point à point ou VPLS. Le mot de contrôle est inséré immédiatement après les étiquettes MPLS. Le mot de contrôle ne commençant pas par 0x4 ou 0x6, 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 immédiatement après le bas de la pile d'étiquettes MPLS ne commencent pas par 0x4 ou 0x6, le routeur IP équilibre la charge en fonction de l'étiquette du bas. Tout le trafic provenant d'un PW suit le même chemin, de sorte que les paquets dans le désordre ne se produisent pas, mais cela peut entraîner un encombrement sur certaines liaisons en cas de PW à bande passante élevée. Avec le logiciel Cisco IOS XR version 4.2.1, l'ASR 9000 prend en charge la fonction de transport Flow Aware Transport (FAT) PW. Cette fonctionnalité s'exécute sur les PE L2VPN, où elle est négociée entre les deux extrémités d'un PW point à

point ou VPLS. Le PE L2VPN d'entrée détecte les flux sur la configuration AC et L2VPN et insère une nouvelle étiquette de flux MPLS sous l'étiquette MPLS PW au bas de la pile d'étiquettes MPLS. Le PE d'entrée détecte les flux en fonction des adresses MAC source et de destination (par défaut) ou des adresses IPv4 source et de destination (configurables). L'utilisation des adresses MAC est la valeur par défaut ; l'utilisation des adresses IPv4 est recommandée, mais elle doit être configurée manuellement.

Avec la fonctionnalité FAT PW, le PE L2VPN d'entrée insère une étiquette MPLS inférieure par src-dst-mac ou par src-dst-ip. Les routeurs MPLS P (entre les PE) hachent les trames sur les chemins disponibles, puis atteignent le PE de destination en fonction de cette étiquette de flux FAT PW au bas de la pile MPLS. Cela permet généralement une bien meilleure utilisation de la bande passante dans le coeur, à moins qu'un PW ne transporte qu'un petit nombre de conversations src-dst-mac ou src-dst-ip. Cisco recommande d'utiliser un mot de contrôle pour éviter d'avoir des adresses MAC commençant par 0x4 et 0x6 immédiatement après l'étiquette de flux. Cela garantit que le hachage est correctement basé sur les pseudo-adresses IP et non sur l'étiquette de flux.

Avec cette fonctionnalité, le trafic d'un PW est réparti sur plusieurs chemins dans le coeur de réseau, lorsqu'il est disponible. Le trafic d'application ne souffre pas de paquets dans le désordre, car tout le trafic de la même source (MAC ou IP) vers la même destination (MAC ou IP) suit le même chemin.

Voici 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 Journalisation

Différents types de messages de journalisation peuvent être configurés en mode de configuration L2VPN. Configurez la journalisation l2vpn afin de recevoir des alertes Syslog pour les événements L2VPN, et configurez la journalisation pseudowire afin de déterminer quand un état PW change :

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

Si de nombreux PW sont configurés, les messages peuvent inonder le journal.

5.3 liste d'accès ethernet-services

Vous pouvez utiliser une liste d'accès ethernet-services afin de supprimer le trafic provenant d'hôtes spécifiques ou de vérifier si un routeur reçoit des paquets d'un hôte sur une interface 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 matérielles ne sont visibles qu'avec le mot clé *hardware*. Utilisez le mot clé

ingress ou *egress* selon la direction du groupe d'accès. L'emplacement de la carte de ligne de l'interface à laquelle la liste d'accès est appliquée est également spécifié.

Vous pouvez également appliquer une liste d'accès ipv4 sur une interface l2transport en tant que fonctionnalité 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)
```

5.4 ethernet egress-filter

Dans le sens de sortie d'un CA, supposons qu'il n'existe aucune commande **symétrique rewrite ingress tag pop <>** qui détermine les balises VLAN de sortie. Dans ce cas, il n'y a pas de vérification afin de s'assurer que la trame sortante a les balises VLAN correctes selon la commande **encapsulation**.

Voici 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 que :

- Une diffusion reçue avec une balise dot1q 2 sur GigabitEthernet0/1/0/39.2 conserve sa balise entrante car il n'y a pas de commande **rewrite ingress**.
- Cette diffusion est diffusée hors de GigabitEthernet0/1/0/3.2 avec sa balise dot1q 2, mais cela ne pose pas de problème car GigabitEthernet0/1/0/3.2 est également configuré avec la balise dot1q 2.
- Cette diffusion est également diffusée hors de GigabitEthernet0/1/0/3.3, qui conserve sa balise d'origine 2 car il n'y a pas de commande de **réécriture** sur GigabitEthernet0/1/0/3.3. La commande **encapsulation dot1q 3** sur GigabitEthernet0/1/0/3.3 n'est pas vérifiée dans le sens de la sortie.
- Le résultat est que, pour une diffusion reçue avec l'étiquette 2 sur GigabitEthernet0/1/0/39, il y a deux diffusions avec l'étiquette 2 sortant de GigabitEthernet0/1/0/3. Ce trafic dupliqué peut entraîner des problèmes au niveau des applications.
- La solution est la configuration de *ethernet egress-filter strict* afin de s'assurer que les paquets quittent la sous-interface avec les balises VLAN correctes. Sinon, les paquets ne sont pas transférés et sont abandonnés.

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

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

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