Servizi e funzionalità di IOS XR L2VPN

Sommario

Introduzione

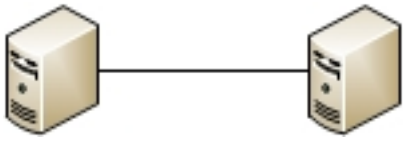
In questo documento vengono descritte le topologie VPN di base di layer 2 (L2). È utile presentare esempi di base per illustrare progettazione, servizi, funzionalità e configurazione. Per ulteriori informazioni, vedere la guida alla configurazione di Cisco ASR 9000 Aggregation Services Router L2VPN e Ethernet Services, versione 4.3.x.

1. Servizi punto-punto e multipunto

La funzionalità L2VPN consente di fornire servizi point-to-point e multipoint.

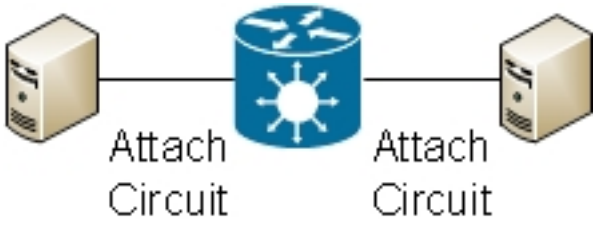
1.1 Servizio point-to-point

Il servizio point-to-point in pratica emula un circuito di trasporto tra due nodi finali in modo che i nodi finali sembrino essere connessi direttamente tramite un collegamento point-to-point. Può essere utilizzato per connettere due siti.

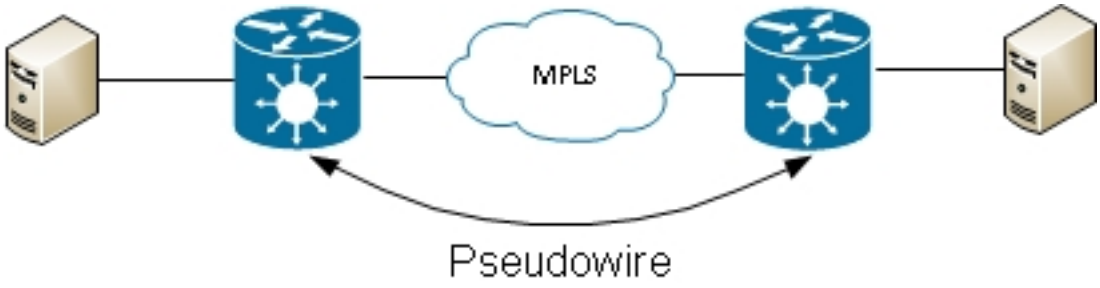


In realtà, possono esistere più router tra i due nodi finali e possono esistere più progetti per fornire il servizio point-to-point.

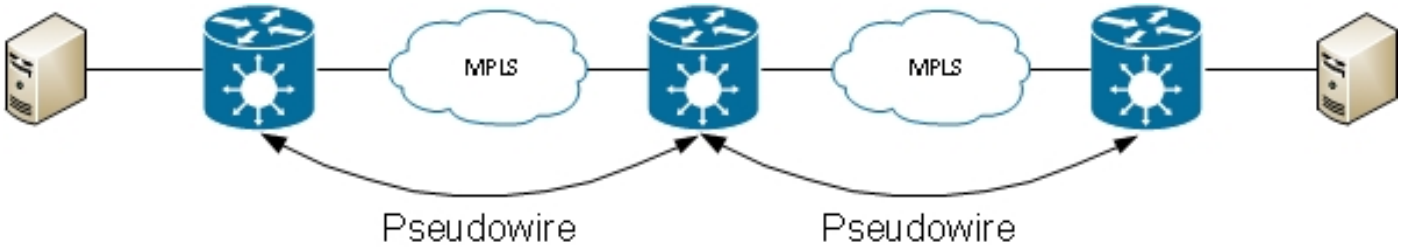
Un router può effettuare la commutazione locale tra due delle sue interfacce:



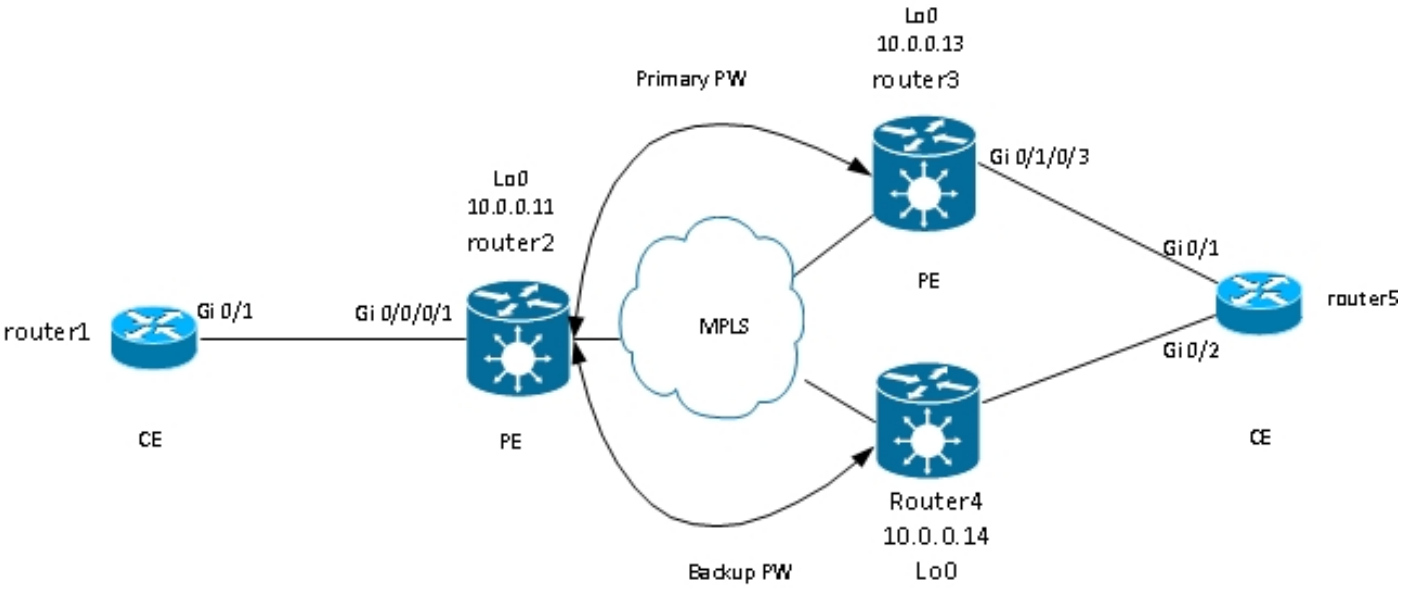
Tra due router può inoltre essere presente uno pseudofilo (PW) Multiprotocol Label Switching (MPLS):



Un router può commutare i frame tra due PW; in questo caso, si tratta di un PW multisegmento:



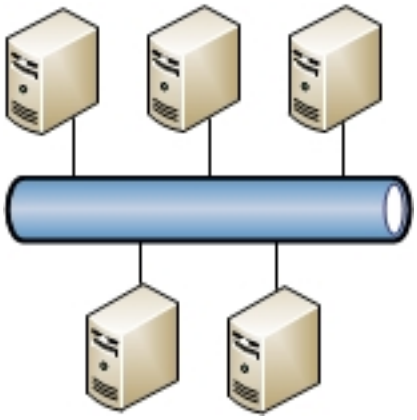
La ridondanza è disponibile tramite la funzione di ridondanza PW:



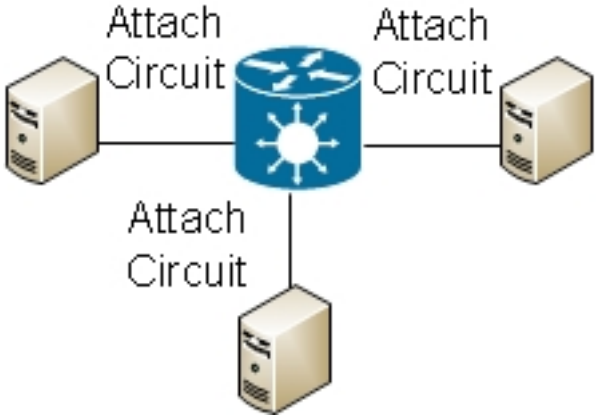
Sono disponibili altri schemi, ma non è possibile elencarli tutti.

1.2 Servizio multipunto

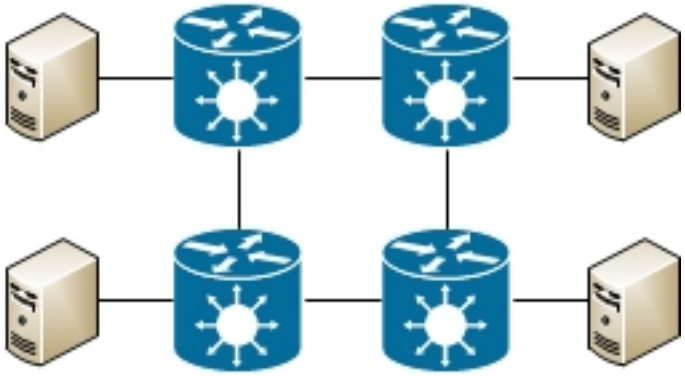
Il servizio multipunto emula un dominio broadcast in modo che tutti gli host connessi in tale dominio bridge appaiano connessi logicamente allo stesso segmento Ethernet:



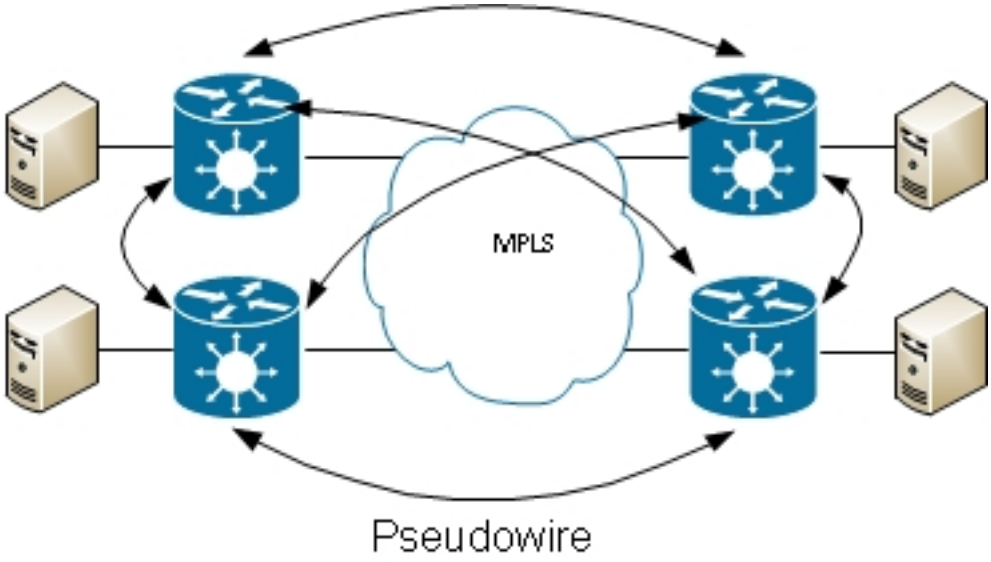
Tutti gli host possono essere collegati allo stesso router/switch:



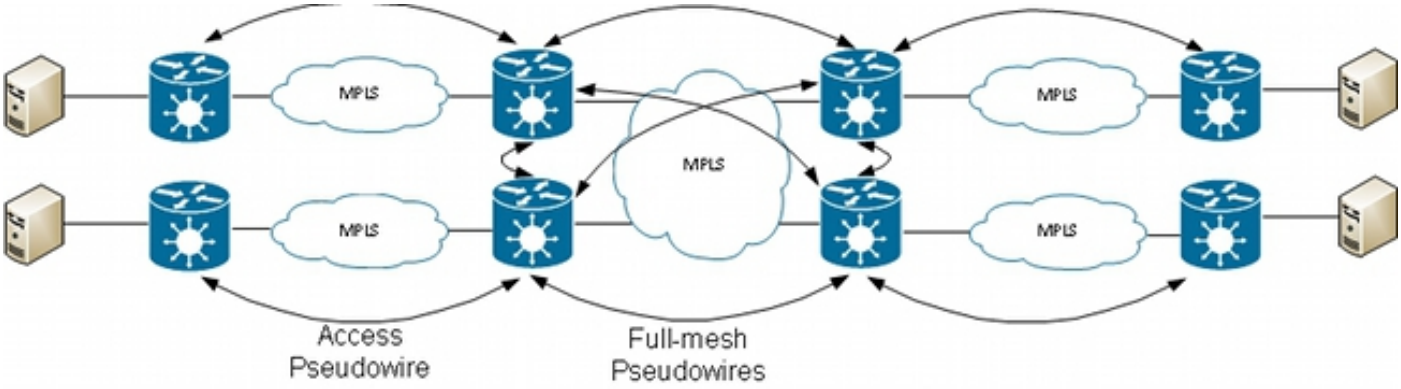
La commutazione Ethernet tradizionale può essere eseguita da più switch. Per interrompere i loop, è necessario usare lo spanning tree:



I servizi VPLS (Virtual Private LAN Services) consentono di estendere il dominio di broadcast tra più siti utilizzando i PW MPLS:



Èpossibile utilizzare VPLS gerarchico per aumentare la scalabilità:



2. Circuiti di collegamento

2.1 ASR 9000 Ethernet Virtual Circuit

2.1.1 Corrispondenza interfaccia in ingresso

Le regole di base per i circuiti di collegamento (CA) comprendono:

- Per essere elaborato dalla funzionalità L2VPN, un pacchetto deve essere ricevuto su un'interfaccia configurata con la parola chiave *l2transport*.
- Questa interfaccia può essere principale, con il comando **l2transport** configurato in modalità di configurazione interfaccia, o secondaria, con la parola chiave *l2transport* configurata dopo il numero della sottointerfaccia.
- L'interfaccia in ingresso del pacchetto è determinata da una ricerca di corrispondenze più lunga. La ricerca di corrispondenze più lunga controlla queste condizioni in modo da far corrispondere il pacchetto in arrivo a una sottointerfaccia:

    1. Il frame in ingresso ha due tag dot1q e corrisponde a una sottointerfaccia configurata con gli stessi due tag dot1q (tunneling 802.1Q o QinQ). Questa è la corrispondenza più lunga

possibile.

2. Il frame in ingresso ha due tag dot1q e corrisponde a una sottointerfaccia configurata con lo stesso tag dot1q first e *qualsiasi* per il secondo tag.
3. Il frame in ingresso ha un tag dot1q e corrisponde a una sottointerfaccia configurata con lo stesso tag dot1q e la parola chiave *esatta*.
4. Il frame in ingresso ha uno o più tag dot1q e corrisponde a una sottointerfaccia configurata con uno dei tag dot1q.
5. Il frame in arrivo non ha tag dot1q e corrisponde a una sottointerfaccia configurata con il comando **encapsulation untagged**.
6. Il frame in ingresso non corrisponde a nessuna altra sottointerfaccia, quindi corrisponde a una sottointerfaccia configurata con il comando **encapsulation default**.
7. Il frame in ingresso non corrisponde a nessuna altra sottointerfaccia, quindi corrisponde all'interfaccia principale configurata per *l2transport*.

- Sui router tradizionali che non utilizzano il modello Ethernet Virtual Connection (EVC), i tag VLAN configurati nella sottointerfaccia vengono rimossi (estratti) dal frame prima di essere trasportati dalla funzionalità L2VPN.
- Su un Cisco ASR serie 9000 Aggregation Services Router che utilizza l'infrastruttura EVC, l'azione predefinita è quella di mantenere i tag esistenti. Utilizzare il comando **rewrite** per modificare l'impostazione predefinita.
- Se nel bridge-domain è presente un'interfaccia BVI (Bridge Virtual Interface), tutti i tag in ingresso devono essere saltati perché il BVI è un'interfaccia di routing senza alcun tag. Per ulteriori informazioni, vedere la sezione BVI.

Di seguito sono riportati diversi esempi che illustrano queste regole:

1. Un esempio di base si ha quando tutto il traffico ricevuto su una porta fisica deve essere trasportato, con o senza tag VLAN. Se si configura **l2transport** con l'interfaccia principale, tutto il traffico ricevuto su quella porta fisica viene trasportato dalla funzionalità L2VPN:

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

   Se esistono sottointerfacce dell'interfaccia principale, l'interfaccia principale rileva tutti i frame a cui non corrisponde alcuna sottointerfaccia. Si tratta della regola di corrispondenza più lunga.

2. Le interfacce bundle e le sottointerfacce possono essere configurate come l2transport:

```
interface Bundle-Ether1
l2transport
```

3. Utilizzare l'**incapsulamento predefinito** in una sottointerfaccia l2transport per trovare la corrispondenza con qualsiasi traffico con o senza tag a cui non sia stata trovata una corrispondenza con un'altra sottointerfaccia con una corrispondenza più lunga. (Vedere Esempio 4). La parola chiave *l2transport* viene configurata nel nome della sottointerfaccia e non nella sottointerfaccia come nell'interfaccia principale:

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

Configurate l'**incapsulamento senza tag** se desiderate trovare solo i fotogrammi senza tag.

4. Se sono presenti più sottointerfacce, eseguire il test di corrispondenza più lungo sul frame in ingresso per determinare l'interfaccia in ingresso:

```
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
```

In questa configurazione, tenere presente che:

- Un frame QinQ con tag VLAN esterno 2 e tag VLAN interno 3 può corrispondere alle sottointerfacce .1, .2 o .3, ma viene assegnato alla sottointerfaccia .3 a causa della regola di corrispondenza più lunga. Due tag su .3 sono più lunghi di un tag su .2 e più lunghi di nessun tag su .1.
- All'interfaccia .2 viene assegnato un frame QinQ con tag VLAN esterno 2 e tag VLAN interno 4 perché l'**incapsulamento dot1q 2** può abbinare i frame dot1q solo al tag VLAN 2, ma può anche abbinare i frame QinQ con tag esterno 2. Fate riferimento all'esempio 5 (la parola chiave *esatta*) se non desiderate che i fotogrammi QinQ corrispondano.
- Un frame QinQ con un tag VLAN esterno 3 corrisponde all'interfaccia secondaria .1.
- Un frame dot1q con tag VLAN 2 corrisponde alla sottointerfaccia 0,2.
- Un frame dot1q con tag VLAN 3 corrisponde alla sottointerfaccia 0,1.

5. Per far corrispondere un fotogramma dot1q e non un fotogramma QinQ, usate la parola chiave *esatta*:

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

Questa configurazione non corrisponde ai frame QinQ con tag 2 della VLAN esterna perché corrisponde solo ai frame con esattamente un tag VLAN.

6. Utilizzare la parola chiave *untagged* per cercare solo i frame senza tag, ad esempio i pacchetti Cisco Discovery Protocol (CDP) o le unità 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
```

In questa configurazione, tenere presente che:

- I frame Dot1q con tag VLAN 3 o i frame QinQ con tag esterno 3 corrispondono alle

sottointerfacce .3.
- Tutti gli altri frame dot1q o QinQ corrispondono alla sottointerfaccia .1.
- I frame senza tag VLAN corrispondono alla sottointerfaccia .2.

7. La parola chiave *any* può essere utilizzata come carattere jolly:

```
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
```

Entrambe le sottointerfacce .4 e .5 possono far corrispondere i frame QinQ con i tag 4 e 5, ma i frame vengono assegnati alle sottointerfacce .5 perché sono più specifiche. Regola di corrispondenza più lunga.

8. Èpossibile usare intervalli di tag VLAN:

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

9. Èpossibile elencare più valori o intervalli di tag VLAN per il primo o il secondo tag 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
```

Èpossibile elencare un massimo di nove valori. Se sono richiesti più valori, è necessario assegnarli a un'altra sottointerfaccia. Raggruppare i valori in un intervallo per abbreviare l'elenco.

10. Il comando **encapsulation dot1q secondo-dot1q** usa l'Ethertype 0x8100 per i tag esterno e interno perché è il metodo Cisco per incapsulare i frame QinQ. In base allo standard IEEE, tuttavia, l'Ethertype 0x8100 deve essere riservato ai frame 802.1q con un tag VLAN, e un tag esterno con Ethertype 0x88a8 deve essere utilizzato per i frame QinQ. Il tag esterno con Ethertype 0x88a8 può essere configurato con la parola chiave *dot1ad*:

```
interface GigabitEthernet0/1/0/3.12 l2transport
encapsulation dot1ad 12 dot1q 100
```

11. Per usare il vecchio Ethertype 0x9100 o 0x9200 per i tag router QinQ, usare il comando **dot1q tunneling ethertype** nell'interfaccia principale della sottointerfaccia QinQ:

```
interface GigabitEthernet0/1/0/3
 dot1q tunneling ethertype [0x9100|0x9200]
!
interface GigabitEthernet0/1/0/3.13 l2transport
encapsulation dot1q 13 second-dot1q 100
```

Il tag esterno ha un Ethertype di 0x9100 o 0x9200 e il tag interno ha il dot1q Ethertype

0x8100.

12. È possibile assegnare un frame in ingresso a una sottointerfaccia, in base all'indirizzo MAC di origine:

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

2.1.2 Manipolazione della VLAN

Il comportamento predefinito di una piattaforma basata su EVC è quello di mantenere i tag VLAN sul frame in ingresso.

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

In questa configurazione, un frame dot1q in ingresso con tag VLAN 3 mantiene il tag VLAN 3 quando il frame viene inoltrato. Un frame QinQ in arrivo con tag VLAN esterno 3 e tag interno 100 mantiene entrambi i tag invariati quando il frame viene inoltrato.

Tuttavia, l'infrastruttura EVC consente di modificare i tag con il comando **rewrite**, in modo da poter inserire (rimuovere), tradurre o aggiungere tag allo stack di tag VLAN in arrivo.

Ecco alcuni esempi:

- La parola chiave *pop* consente di rimuovere un tag QinQ da un fotogramma dot1q in ingresso. Questo esempio rimuove il tag esterno 13 del frame QinQ in arrivo e lo inoltra con il tag dot1q 100 in cima:

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

Il comportamento è sempre simmetrico, il che significa che il tag esterno 13 viene aperto nella direzione in entrata e spinto nella direzione in uscita.

- La parola chiave *translate* consente di sostituire uno o due tag in arrivo con uno o due nuovi tag:

```
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
```

La parola chiave *symmetric* viene aggiunta automaticamente perché è l'unica modalità supportata.

- La parola chiave *push* consente di aggiungere un tag QinQ a un frame dot1q in ingresso:

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

Un tag QinQ esterno 100 viene aggiunto al frame in arrivo con un tag dot1q 4. Nella direzione di uscita, viene aperto il tag QinQ.

2.2 Comportamento del router Cisco IOS XR non-EVC (CRS e XR12000)

La sintassi per la corrispondenza VLAN sulle piattaforme non EVC non usa la parola chiave *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
```

Non è possibile configurare la manipolazione dei tag VLAN, perché l'unico comportamento possibile è fare clic su tutti i tag specificati nei comandi **dot1q** o **dot1ad**. Questa operazione viene eseguita per impostazione predefinita, quindi non è disponibile alcun comando **rewrite**.

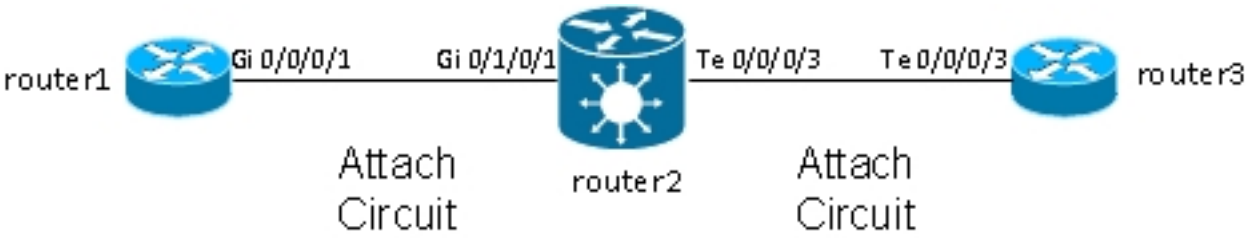
3. Servizio point-to-point

> **Note:**
>
> per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).
>
> Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

3.1 Switching locale

3.1.1 Interfaccia principale

La topologia di base è una connessione incrociata locale tra due interfacce principali:



Il router2 riceve tutto il traffico sul Gi 0/1/0/1 e lo inoltra al Gi 0/0/0/3 e viceversa.

Mentre router1 e router3 sembrano avere un cavo back-to-back diretto in questa topologia, in realtà il router2 non sta convertendo tra le interfacce TenGigE e Gigabit Ethernet. Il router2 può eseguire funzionalità su queste due interfacce; un elenco di controllo di accesso (ACL), ad esempio, può eliminare tipi specifici di pacchetti o una mappa dei criteri per definire o limitare la velocità del traffico a bassa priorità.

Una connessione incrociata point-to-point di base viene configurata tra due interfacce principali configurate come l2transport sul router2:

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

Sul router1 e sul router3, le interfacce principali sono configurate con CDP e un indirizzo 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
```

Il router1 vede il router3 come router adiacente CDP e può eseguire il ping 10.1.1.2 (indirizzo di interfaccia del router3) come se i due router fossero collegati direttamente.

Poiché non è configurata alcuna sottointerfaccia sul router2, i frame in ingresso con un tag VLAN vengono trasportati in modo trasparente quando le sottointerfacce dot1q vengono configurate sul router1 e sul router3:

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

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

Dopo 10.000 ping tra il router1 e il router3, è possibile usare i comandi **show interface** e **show l2vpn** per assicurarsi che le richieste ping ricevute dal router2 su un access point vengano inoltrate sull'altro access point e che le risposte ping vengano gestite allo stesso modo al contrario.

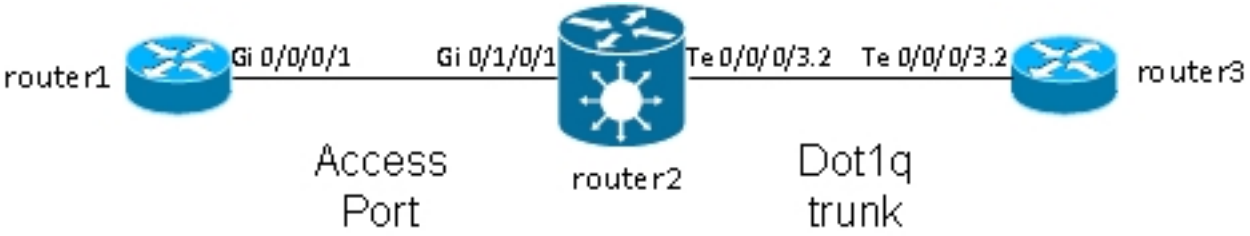
```
RP/0/RSP0/CPU0:router2#sh int gig 0/1/0/1
GigabitEthernet0/1/0/1 is up, line protocol is up
Interface state transitions: 1
Hardware is GigabitEthernet, address is 0024.986c.63f1 (bia 0024.986c.63f1)
Description: static lab connection to acdc 0/0/0/1 - dont change
Layer 2 Transport Mode
MTU 1514 bytes,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

Nella terminologia del software Cisco IOS®, questo esempio ha un ACL simile a un'interfaccia di accesso in modalità switchport e una sottointerfaccia dot1q simile a un trunk:



In genere, questa topologia utilizza un bridge-domain perché la VLAN contiene in genere più di due porte, anche se è possibile utilizzare una connessione incrociata point-to-point se le porte sono solo due. In questa sezione viene descritto come le funzionalità di riscrittura flessibili consentono di manipolare la VLAN in diversi modi.

3.1.2.1 Interfaccia principale e sottointerfaccia Dot1q

Nell'esempio, l'interfaccia principale si trova su un lato e la sottointerfaccia dot1q sull'altro lato:

Questa è l'interfaccia principale del router1:

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

Questa è la sottointerfaccia dot1q sul router2:

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

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

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

A questo punto, è disponibile una parola chiave *l2transport* nel nome della sottointerfaccia TenGigE0/0/0/3.2. Il router3 invia frame dot1q con tag 2, che corrispondono alla sottointerfaccia TenGigE0/0/3.2 sul router2.

Il tag in ingresso 2 viene rimosso nella direzione in entrata dal comando **rewrite ingress tag pop 1 symmetric**. Poiché l'etichetta è stata rimossa in direzione di entrata su TenGigE0/0/0/3.2, i pacchetti vengono inviati senza etichetta in direzione di uscita su Gigabit Ethernet0/1/0/1.

Il router1 invia frame senza tag, che corrispondono all'interfaccia principale Gigabit Ethernet0/1/0/1.

Non è disponibile alcun comando **rewrite** su Gigabit Ethernet0/1/0/1, quindi non viene eseguito il popup, il push o la conversione di alcun tag.

Quando i pacchetti devono essere inoltrati fuori da TenGigE0/0/0/3.2, il tag 2 dot1q viene premuto a causa della parola chiave *symmetric* nel comando **rewrite ingress tag pop 1**. Il comando apre un tag in entrata ma spinge simmetricamente un tag in uscita. Questo è un esempio su router3:

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

Monitorare i contatori della sottointerfaccia con la stessa **interfaccia show** e i comandi **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
```

Come previsto, il numero di pacchetti ricevuti su TenGigE0/0/0/3.2 corrisponde al numero di pacchetti inviati su Gigabit Ethernet0/1/0/1 e viceversa.

3.1.2.2 Sottointerfaccia con incapsulamento

Anziché l'interfaccia principale su Gigabit Ethernet0/1/0/1, è possibile usare una sottointerfaccia con **incapsulamento predefinito** per acquisire tutti i frame o con **incapsulamento senza tag** per abbinare solo i frame senza tag:

```
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 Direzione di ingresso su Gigabit Ethernet0/1/0/1.1

Anziché premere tag 2 in entrata nella direzione TenGigE0/0/0/3.2, è possibile premere tag 2 in entrata nella direzione Gigabit Ethernet0/1/0/1.1 e non eseguire alcuna operazione su TenGigE0/0/0/3.2:

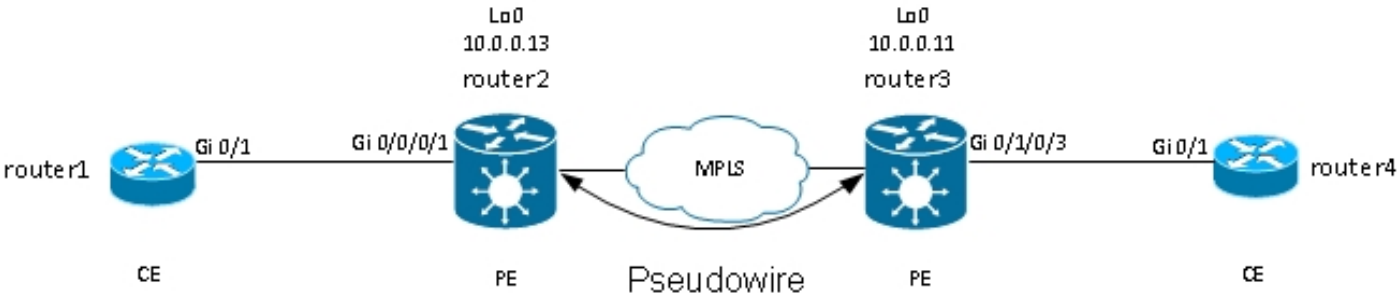
```
RP/0/RSP0/CPU0:router2#sh run int  TenGigE0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2

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
```

Pertanto, è possibile notare che il modello EVC con i comandi **encapsulation** e **rewrite** offre una grande flessibilità per abbinare e modificare i tag VLAN.

3.2 Servizi di cablaggio privati virtuali

3.2.1 Panoramica

I servizi VPN (Virtual Private Wire Services), noti anche come Ethernet over MPLS (EoMPLS), consentono a due dispositivi L2VPN Provider Edge (PE) di eseguire il tunnel del traffico L2VPN su un cloud MPLS. I due PE L2VPN sono in genere connessi a due siti diversi con un core MPLS. I due ACL connessi a ogni PE L2VPN sono collegati da un PW sulla rete MPLS, ovvero il PW MPLS.



Ogni PE deve disporre di un'etichetta MPLS per poter raggiungere il loopback del PE remoto. Questa etichetta, generalmente denominata IGP (Interior Gateway Protocol), può essere appresa tramite il protocollo MPLS Label Distribution Protocol (LDP) o MPLS Traffic Engineering (TE).

I due PE stabiliscono tra loro una sessione LDP MPLS di destinazione in modo da poter stabilire e controllare lo stato del PW. Un PE annuncia all'altro PE l'etichetta MPLS per l'identificazione del PW.

> **Nota**: il protocollo BGP può essere utilizzato per la segnalazione, ma non è trattato in questo documento.

Il traffico ricevuto dal router2 sull'access point locale è incapsulato in uno stack di etichette MPLS:

- L'etichetta MPLS esterna è l'etichetta IGP che permette di raggiungere il loopback del router3. Questa potrebbe essere l'etichetta implicita-null se le etichette sono direttamente connesse; ciò significa che non verrebbe aggiunta alcuna etichetta IGP.
- L'etichetta MPLS interna è l'etichetta PW annunciata dal router3 durante la sessione LDP di destinazione.
- Può esistere una parola di controllo PW dopo le etichette MPLS, a seconda della configurazione e del tipo di incapsulamento. La parola di controllo non viene utilizzata per impostazione predefinita sulle interfacce Ethernet e deve essere configurata in modo esplicito quando necessario.
- Il frame L2 trasportato segue nel pacchetto.
- Alcuni tag VLAN vengono trasportati sul PW, a seconda della configurazione e del tipo di PW.

Il penultimo hop, appena prima del router3 nel core MPLS, scarta l'etichetta IGP o la sostituisce con un'etichetta null esplicita. Pertanto, l'etichetta significativa superiore sul frame ricevuto dal router3 è l'etichetta PW che il router3 ha segnalato al router2 per il PW. Pertanto, il router3 sa che il traffico ricevuto con l'etichetta MPLS deve essere commutato sull'adattatore CA collegato al router4.

Nell'esempio precedente, è innanzitutto necessario verificare se ogni L2VPN dispone di un'etichetta MPLS per il loopback del server PE remoto. Questo è un esempio di come controllare le etichette sul router2:

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

La configurazione CA è la stessa:

```
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
```

Poiché non è disponibile alcun comando **rewrite in entrata pop**, il tag 2 della VLAN in arrivo viene trasportato sul PW. Vedere i Type 4 e 5 PW per i dettagli.

La configurazione L2VPN specifica l'ACL locale e il PE L2VPN remoto con un ID PW che deve corrispondere su ogni lato e deve essere univoco per ogni router adiacente:

```
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 configurazione corrispondente sul router3 è:

```
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
```

Per visualizzare i dettagli della connessione incrociata, usare il comando **show l2vpn xconnect detail**:

```
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
```

In questa configurazione, tenere presente che:

- L'MTU (Maximum Transmission Unit) dell'alimentatore CA è 1504 in quanto il tag in ingresso sull'alimentatore CA non viene scaricato. L'MTU deve corrispondere su ciascun lato, altrimenti il PW non viene visualizzato.
- 186 pacchetti sono stati ricevuti sull'AC e inviati sul PW come previsto.
- Sul PW sono stati ricevuti 38448 pacchetti, che sono stati inviati sull'AC come previsto.
- L'etichetta locale sul router2 è 16026 e è l'etichetta usata dal router3 come etichetta interna. I pacchetti vengono ricevuti sul router2 con quell'etichetta MPLS come etichetta superiore perché l'etichetta IGP è stata scaricata dal penultimo hop MPLS. Il router2 sa che i frame in ingresso con quell'etichetta PW devono essere commutati sull'interfaccia AC Gi 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 Stato PW e accoppiato CA

In una connessione incrociata point-to-point, l'AC e la PW sono accoppiati. Quindi, se l'alimentazione CA si interrompe, L2VPN PE segnala tramite LDP al dispositivo remoto che lo stato PW non dovrebbe essere attivo. Ciò attiva la convergenza quando viene configurata la ridondanza PW. Per ulteriori informazioni, vedere la sezione Ridondanza.

Nell'esempio, l'alimentazione CA è spenta sul router2 e sta inviando lo stato 'AC Down' PW al router3:

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

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

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

Il router3 sa che il PW non deve essere attivo perché l'alimentazione CA remota è inattiva:

```
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 PW di tipo 4 e 5

Èpossibile utilizzare due tipi di PW: tipo 4 e tipo 5.

- Un PW di tipo 4 è noto come PW basato su VLAN. Il file PE in entrata non deve rimuovere i tag VLAN in entrata che devono essere trasportati sul PW.

  Sulle piattaforme basate su EVC, come ASR 9000, il problema è che gli ACL in arrivo potrebbero avere un comando **rewrite** per rimuovere i tag VLAN in arrivo, quindi potrebbe non esserci alcun tag VLAN da trasportare sul PW. Per risolvere questo problema, le piattaforme EVC inseriscono un tag VLAN fittizio 0 sopra il frame per i PW di tipo 4. I PW di tipo 4 sono configurati con il comando **transport-mode vlan**. Il file PE remoto deve essere basato su EVC e deve essere consapevole che il tag VLAN superiore è il tag fittizio da rimuovere.

  Tuttavia, se si utilizza una PW di tipo 4 tra una piattaforma EVC e una non EVC, potrebbero verificarsi problemi di interoperabilità. La piattaforma non EVC non considera il tag VLAN superiore come tag VLAN fittizio e inoltra il frame con il tag VLAN fittizio 0 come tag esterno. Le piattaforme EVC possono modificare i tag VLAN ricevuti sul frame in arrivo con il comando **rewrite**. I risultati della manipolazione della VLAN vengono trasportati sul PW di tipo 4 con il tag fittizio aggiuntivo 0 nella parte superiore.

  Le recenti versioni del software Cisco IOS XR offrono la possibilità di usare un PW di tipo 4 senza usare il tag fittizio 0 con il comando **transport-mode vlan passthrough**. La manipolazione del tag VLAN sul punto di flusso Ethernet (EFP) deve garantire la presenza di almeno un tag, in quanto deve essere presente un tag VLAN trasportato su un PW di tipo 4 e,

in questo caso, non esiste un tag fittizio che soddisfi tale requisito. I tag che rimangono sul frame dopo la riscrittura del tag di interfaccia in ingresso vengono trasportati in modo trasparente attraverso il PW.

- Un PW di tipo 5 è noto come PW basato su porta Ethernet. Il pacchetto PE in entrata trasporta i frame ricevuti su un'interfaccia principale o dopo che i tag della sottointerfaccia sono stati rimossi quando il pacchetto viene ricevuto su una sottointerfaccia. Non è necessario inviare un frame con tag su un PW di tipo 5 e le piattaforme basate su EVC non aggiungono alcun tag fittizio. Le piattaforme basate su EVC possono modificare i tag VLAN ricevuti sul frame in arrivo con il comando **rewrite**. I risultati della manipolazione della VLAN vengono trasportati sulla rete PW di tipo 5, con o senza tag.

Per impostazione predefinita, i PE L2VPN tentano di negoziare un PW di tipo 5, come illustrato nell'esempio seguente:

```
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
```

Il tipo PW Ethernet indica un tipo 5 PW.

Questa è l'acquisizione di una richiesta ARP inviata dal router1 e incapsulata dal router2 sul PW al router3:

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

L'etichetta MPLS 16031 è l'etichetta PW pubblicizzata dal router3. L'acquisizione dello sniffer è stata effettuata tra il penultimo hop e il router3, quindi non esiste un'etichetta IGP.

Il frame Ethernet incapsulato inizia immediatamente dopo l'etichetta PW. È possibile che sia presente una parola del controllo PW, ma in questo esempio non è configurata.

Anche se si tratta di una PW di tipo 5, il tag VLAN in ingresso 2 ricevuto sull'appliance ASA dal router2 viene trasportato perché non è presente alcun comando **rewrite** che lo popola sull'appliance ASA. I risultati provenienti dall'alimentatore CA dopo l'elaborazione di riscrittura vengono trasportati perché non è presente alcun salto automatico dei tag sulle piattaforme basate su EVC. Si noti che non esiste un tag VLAN 0 fittizio con un PW di tipo 5.

Se la configurazione è stata eseguita con il comando **rewrite in entrata tag pop 1 symmetric**, non sarà presente alcun tag VLAN trasportato sul PW.

Di seguito è riportato l'esempio di un PW di tipo 4 con configurazione di una classe pw sul router2 e sul router3.

> **Nota**: se si configura un tipo 4 solo su un lato, il PW rimane inattivo e segnala 'Errore: mancata corrispondenza del tipo PW'.

```
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
!
!
!
!
```

Il tipo PW Ethernet VLAN indica un tipo 4 PW.

```
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
```

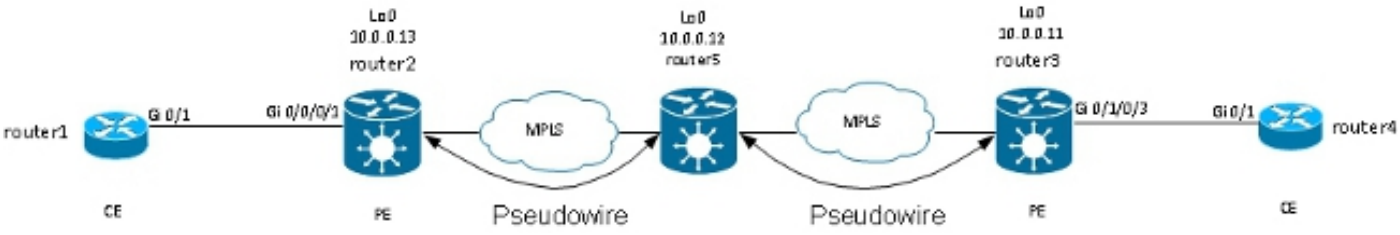
Sulla parte superiore del telaio da trasportare è ora inserito un tag fittizio 0:

```
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)
```

Il file PE basato su EVC in uscita rimuove il tag fittizio e inoltra il frame con il tag 2 sull'alimentatore CA locale. Il PE in uscita applica la manipolazione del tag locale configurata sul relativo CA sul frame ricevuto sul PW. Se l'adattatore CA locale è configurato come **riscrittura in entrata tag pop 1 simmetrico**, il tag configurato deve essere spostato in uscita, in modo che un nuovo tag venga posizionato sopra il tag 2 ricevuto sul PW. Il comando rewrite è molto flessibile, ma è necessario valutare con attenzione gli obiettivi che si desidera raggiungere su ciascun lato della PW.

3.2.4 PW multisegmento

Èpossibile avere un PE L2VPN con PW, invece di un'interfaccia fisica, come AC:



Il router5 riceve i pacchetti sul PW dal router2 e passa i pacchetti sull'altro PW al router3. Pertanto, il router5 sta commutando tra i PW in modo da creare un PW a più segmenti tra il router2 e il router3.

La configurazione sul router2 punta ora al router5 come PE remoto:

```
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 configurazione sul router5 è di 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
!
!
!
```

Il comando **description** è facoltativo e viene inserito in un TLV (Type Length Value) di switching PW inviato dal router5 a ogni PE remoto (router2 e router3). La **descrizione** è utile quando è necessario risolvere un problema relativo a PW quando al centro della rete è presente un router che esegue la commutazione di PW.

Immettere il comando **sh l2vpn xconnect** per rivedere il TLV di switching 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)
```

Il router5 invia un TLV di switching PW al router3 con i dettagli del PW al router2 e invia un TLV di switching PW al router2 con i dettagli del PW al router3.

3.2.5 Ridondanza

Èpossibile utilizzare una PW point-to-point per connettere due siti, ma questi due siti devono rimanere connessi in caso di guasto di PE o di CA.

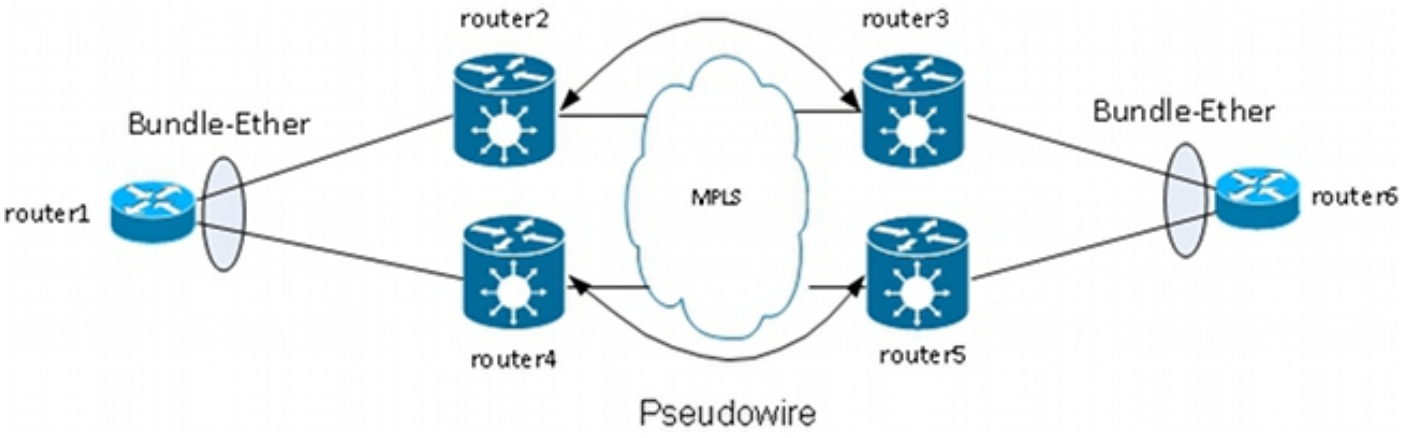
3.2.5.1 Ridondanza dei core

Se si apportano modifiche alla topologia che influiscono sul reindirizzamento nel core MPLS, il PW MPLS eredita immediatamente il nuovo percorso.

3.2.5.2 Pacchetto over PW

Un dispositivo Customer Edge (CE) può essere collegato al PE tramite un bundle Ethernet per fornire ridondanza del collegamento in caso di guasto del collegamento del componente del bundle tra CE e PE. Il bundle rimane attivo anche se un membro del collegamento del bundle diventa inattivo. Si noti che questa operazione non fornisce la ridondanza PE in quanto un errore PE comporta la disattivazione dell'intero bundle.

Un metodo per la ridondanza consiste nel far trasportare più circuiti da PW point-to-point. Ogni circuito è membro di un bundle Ethernet tra due CE:



Il PPE non termina il bundle e trasporta i frame in modo trasparente sul PW, inclusi i frame LACP (Link Aggregation Control Protocol) scambiati tra i CE.

Con questo progetto, la perdita di un CA o di un PE provoca la caduta di un membro del bundle, ma il bundle rimane attivo.

> **Nota**: le BPDU LACP non sono state trasferite su L2VPN da ASR 9000 in versioni precedenti al software Cisco IOS XR versione 4.2.1.

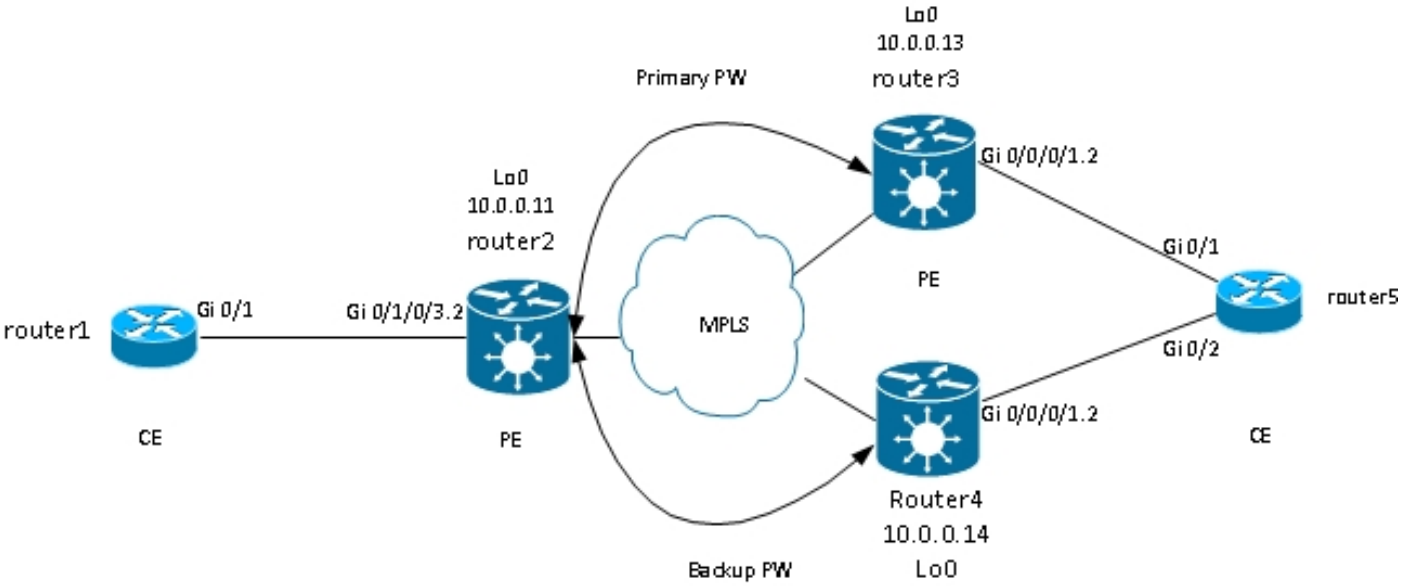
Il CE è ancora un singolo punto di errore in questo progetto. Altre funzioni di ridondanza che possono essere utilizzate sul CE sono:

- MC-LAG (Multicassis Link Aggregation Group)
- ASR 9000 Network Virtualization (nV) clustering
- Virtual Switching System (VSS) sugli switch Cisco IOS
- Virtual Port Channel (vPC) sugli switch Cisco Nexus

Dal punto di vista del PE, esiste una semplice connessione point-to-point tra un AC e un PW MPLS.

3.2.5.3 Ridondanza PW

I sistemi PE possono inoltre fornire ridondanza con una funzionalità denominata Ridondanza PW.



Il router2 ha un PW primario per il router3. Il traffico tra il router1 e il router6 passa attraverso il PW primario in circostanze normali. Il router2 dispone anche di un PW di backup per il router4 in hot standby ma, in circostanze normali, il traffico su tale PW non passa.

Se si verifica un problema con il PW primario, con il PE remoto del PW primario (router3) o con l'AC sul PE remoto (router3), il router2 attiva immediatamente il PW di backup e il traffico inizia a fluire attraverso di esso. Il traffico torna al PW primario quando il problema viene risolto.

La configurazione sul router2 è:

```
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 configurazione standard sui router3 e router4 è:

```
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
!
!
!
!
```

In condizioni stabili, il PW al router3 è attivo e il PW al router4 è in stato di standby:

```
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#
```

Poiché lo stato AC e lo stato PW sono accoppiati, il router3 invia il segnale 'AC down' al router2 quando l'AC sul router3 si spegne. Router2 interrompe il PW principale e attiva il PW di backup:

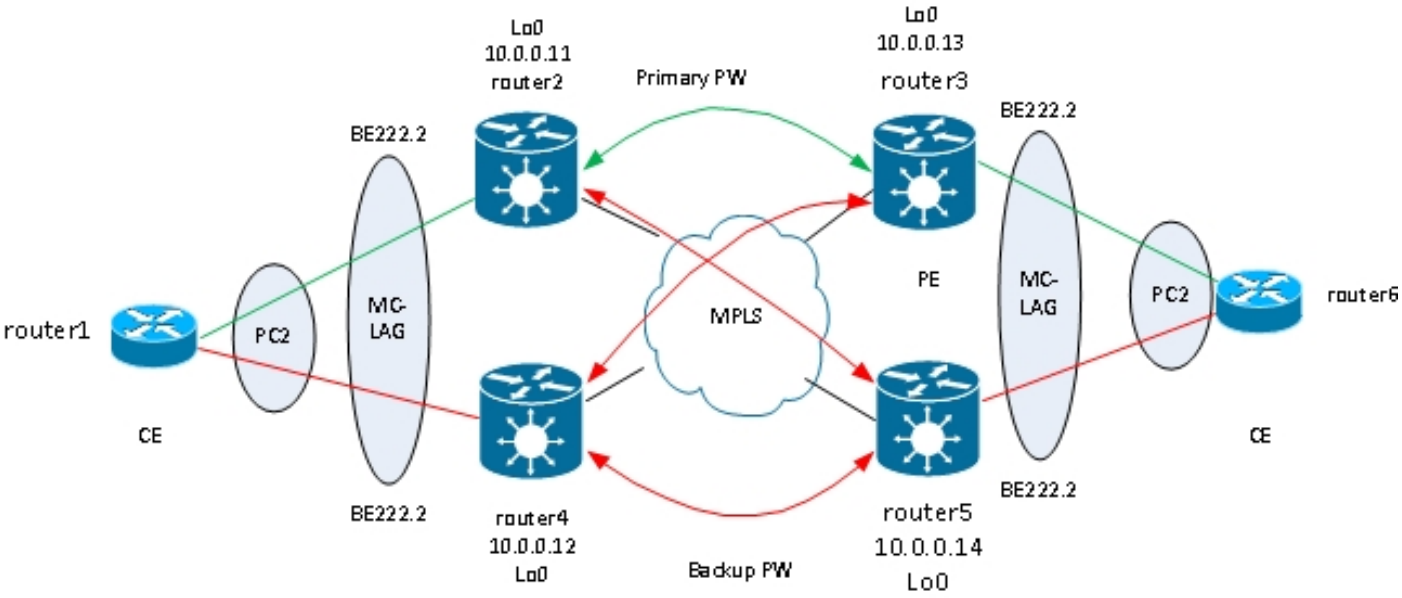
```
RP/0/RSP0/CPU0:May  3 15:34:08.772 : l2vpn_mgr[1121]: %L2-L2VPN_PW-3-UPDOWN :
Pseudowire with address 10.0.0.13, id 222, state is Down
RP/0/RSP0/CPU0:May 3 15:34:08.772 : l2vpn_mgr[1121]: %L2-L2VPN_PW-3-UPDOWN :
Pseudowire with address 10.0.0.14, id 222, state is Up

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#
```

Quando l'alimentazione CA sul router3 ritorna attiva, il router2 riattiva il PW primario sul router3 e il PW sul router4 torna allo stato di standby.

La PW di backup viene attivata anche quando il router3 si blocca e il router2 perde il percorso verso il loopback.

Il passaggio logico successivo consiste nell'introdurre la ridondanza PW bidirezionale con due PE in ogni sito:



Tuttavia, questa rete completa di PW incontra un problema quando due PW sono attivi contemporaneamente quando viene introdotto un loop nella rete. Il loop deve essere interrotto, generalmente utilizzando il protocollo Spanning Tree Protocol (STP). Non si desidera tuttavia che l'instabilità dello Spanning Tree in un sito venga propagata all'altro sito. Pertanto, è meglio non eseguire Spanning Tree su questi PW e non unire lo Spanning Tree tra i due siti . È più semplice se esiste un solo collegamento logico tra i due siti in modo che non sia richiesto spanning tree.

Una soluzione consiste nell'utilizzare un bundle MC-LAG tra i due PE in un unico sito e il CE locale. Solo uno dei due PE dispone di membri bundle attivi in modo che il relativo PW al sito remoto sia attivo. L'altro sistema PE ha i suoi membri bundle in stato di standby e il suo PW al sito remoto è inattivo. Con un solo PW attivo tra i due siti, non viene introdotto alcun loop. Il sistema PE con il PW attivo dispone inoltre di un PW in standby al secondo sistema PE sul sito remoto.

In condizioni stabili, i membri del bundle attivi si trovano sui router2 e sui router3 e il PW attivo si trova tra di essi. Questa è la configurazione sul router3:

```
RP/0/RSP1/CPU0:router3#sh run redundancy
redundancy
iccp
group 2
mlacp node 1
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.14
!
```

```
backbone
interface TenGigE0/0/0/0
interface TenGigE0/0/0/1
!
isolation recovery-delay 300
!
!
!

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

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

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

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

Bundle-Ether222
Status: Up
Local links : 1 / 0 / 1
Local bandwidth : 1000000 (1000000) kbps
MAC address (source): 0000.0000.0002 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 1
Wait while timer: Off
Load balancing: Default
LACP: Operational
Flap suppression timer: 100 ms
Cisco extensions: Disabled
mLACP: Operational
ICCP Group: 2
Role: Active
```

```
Foreign links : 0 / 1
Switchover type: Revertive
Recovery delay: 40 s
Maximize threshold: 1 link
IPv4 BFD: Not configured

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

Sul router5, il membro del bundle locale e il PW primario al router2 sono in stato standby e il PW di backup al router4 è inattivo:

```
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
```

Su router6, il membro del bundle su router3 è attivo, mentre il membro del bundle su router5 è in stato standby:

```
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)
```

Quando il membro del bundle sul router3 si blocca, il router6 ha il suo membro attivo sul router5:

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

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


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

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

Poiché il bundle-ther22 non è attivo sul router5, il PW al router2 accoppiato si interrompe contemporaneamente:

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

Il router2 rileva che il PW al router3 è inattivo e attiva il PW di backup sul router5:

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

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

Il router5 ha il suo membro di bundle attivo così come il suo PW primario verso il router2:

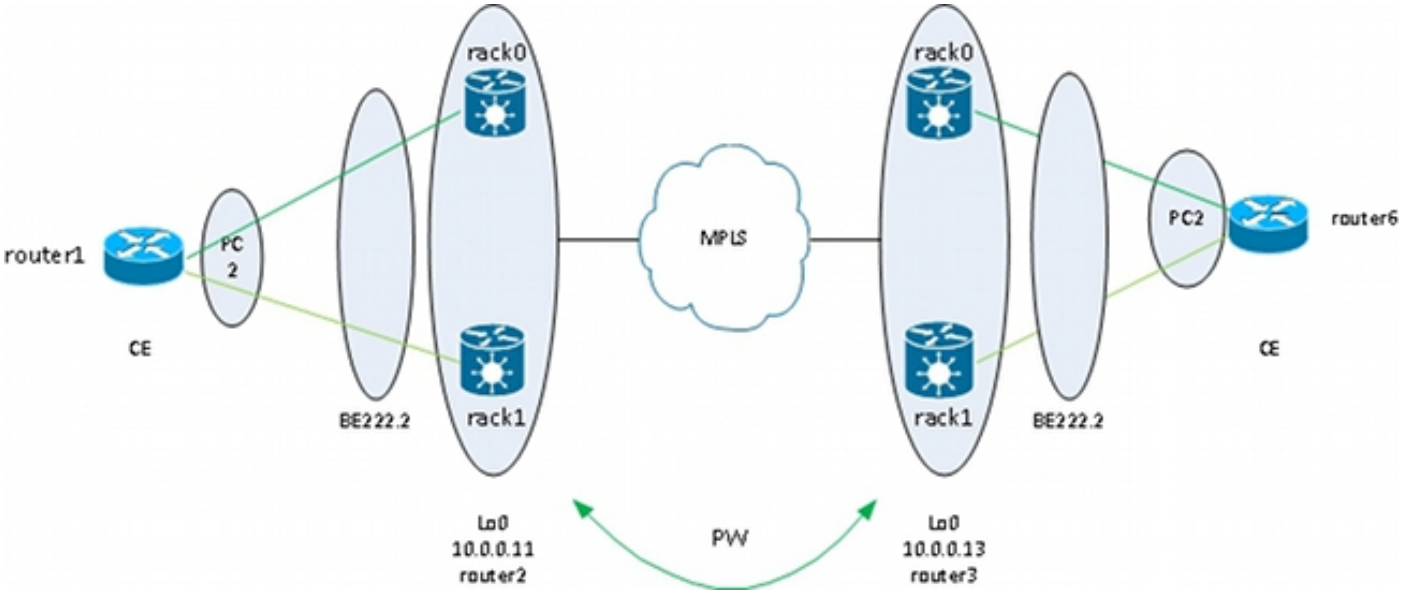
```
RP/0/RSP1/CPU0:router5#sh bundle bundle-ether 222

Bundle-Ether222
Status: Up
Local links : 1 / 0 / 1
Local bandwidth : 1000000 (1000000) kbps
MAC address (source): 0000.0000.0002 (Configured)
```

```
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 1
Wait while timer: Off
Load balancing: Default
LACP: Operational
Flap suppression timer: 100 ms
Cisco extensions: Disabled
mLACP: Operational
ICCP Group: 2
Role: Active
Foreign links : 0 / 1
Switchover type: Revertive
Recovery delay: 40 s
Maximize threshold: 1 link
IPv4 BFD: Not configured

Port Device State Port ID B/W, kbps
-------------------- ----------- ----------- -------------- ----------
Gi0/0/0/1 Local Active 0x8002, 0xa002 1000000
Link is Active
Gi0/0/0/1 10.0.0.13 Configured 0x8003, 0x9001 1000000
Link is down
RP/0/RSP1/CPU0:router5#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

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

3.2.5.4 ASR 9000 nV Edge Cluster

Il progetto precedente basato sulla ridondanza MC-LAG e PW funziona bene per la ridondanza ma, poiché alcuni membri del bundle sono in stato di standby, non trasportano il traffico in condizioni stabili.

Se si desidera che tutti i membri del bundle siano attivi, anche in condizioni stabili, è possibile utilizzare un cluster ASR 9000 con membri del bundle dal CE collegati a ciascun rack del PE:



Questo design offre ridondanza in caso di guasto del collegamento di un componente del bundle tra il CE e il PE, di guasto del rack e di guasto del collegamento del core, a condizione che il cluster sia collegato due volte al core MPLS e che il core sia ridondante. I due rack non devono necessariamente essere collocati nello stesso luogo e possono trovarsi in posizioni diverse. I collegamenti tra rack non sono rappresentati in questo diagramma.

Se si desidera ottenere la ridondanza sul CE, è possibile utilizzare una soluzione a più chassis per il CE:

- MC-LAG
- ASR 9000 nV Clustering
- VSS
- vPC

La configurazione sul cluster ASR 9000 è molto semplice:

```
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 consiglia di configurare un indirizzo MAC di sistema LACP statico e un indirizzo MAC del bundle in modo da evitare che l'indirizzo MAC cambi a causa di uno switchover del controller dello scaffale designato. Nell'esempio viene mostrato come trovare gli indirizzi:

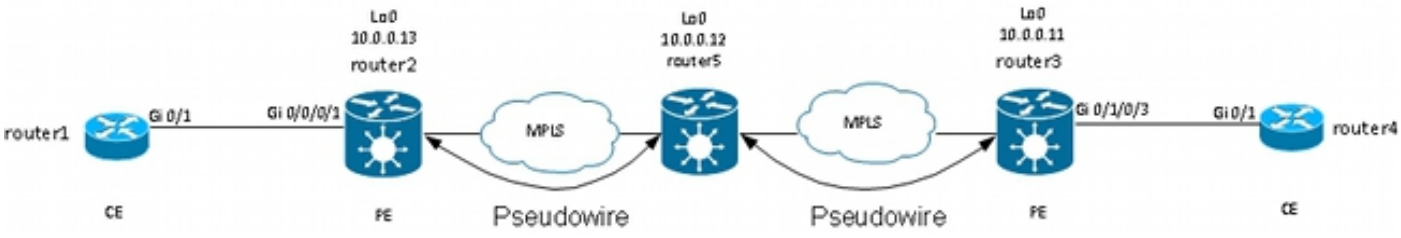
```
RP/1/RSP0/CPU0:router2#sh int bundle-ether 222 | i address is
Hardware is Aggregated Ethernet interface(s), address is 0024.f71e.d309
Internet address is Unknown
RP/1/RSP0/CPU0:router2#
RP/1/RSP0/CPU0:router2#conf
RP/1/RSP0/CPU0:router2(config)#int bundle-ether 222
RP/1/RSP0/CPU0:router2(config-if)#mac-address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

In sintesi, questo è il bundle-ther 222 con un membro su ciascun rack (dieci 0/0/0/8 sul rack 0 e dieci 1/0/0/8 sul rack 1) e la sottointerfaccia del bundle configurata per una connessione incrociata point-to-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

I router e gli switch Cisco inviano in genere pacchetti CDP senza tag dot1q. Esistono diversi scenari per determinare cosa succede a questi pacchetti CDP quando vengono ricevuti da un router IOS XR configurato per una connessione incrociata:



In questa topologia, il router1 può visualizzare il router PE locale router2 come router adiacente CDP o il router CE remoto router4, a seconda della configurazione.

3.3.1 CDP non abilitato sull'interfaccia principale di L2VPN PE

I pacchetti CDP provenienti da L2VPN CE vengono trasportati attraverso la connessione incrociata. I due L2VPN CE si vedono (con l'uso del comando **show cdp neighbors**) se l'interfaccia

principale è configurata come l2transport o se esiste una sottointerfaccia che corrisponde ai frame CDP senza tag.

Questo è un esempio dell'interfaccia 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
!
!
!
!
```

Questo è un esempio di sottointerfaccia senza tag:

```
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
!
!
!
!
```

In questi due esempi, i pacchetti CDP vengono trasportati attraverso la connessione incrociata e gli EC si vedono a vicenda come vicini CDP. Il CE non vede il PE come un CDP adiacente:

```
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 abilitato sull'interfaccia principale di L2VPN PE

Il sistema PE elabora i pacchetti CDP senza tag e il sistema PE e il sistema CE si vedono reciprocamente come router adiacenti. Tuttavia, il CE remoto non viene visualizzato quando CDP è abilitato sull'interfaccia principale del PE L2VPN.

Si noti che:

- Non è possibile configurare CDP su un'interfaccia principale configurata come l2transport.
- Il PPE intercetta i pacchetti CDP quando il CDP è configurato sull'interfaccia principale diversa da l2transport. Questo si verifica anche se esiste una sottointerfaccia l2transport configurata

per corrispondere ai pacchetti CDP senza tag (con l'uso dei comandi **incapsulation untagged** o **encapsulation default**). In questo caso, i pacchetti CDP non vengono trasportati sul sito remoto.

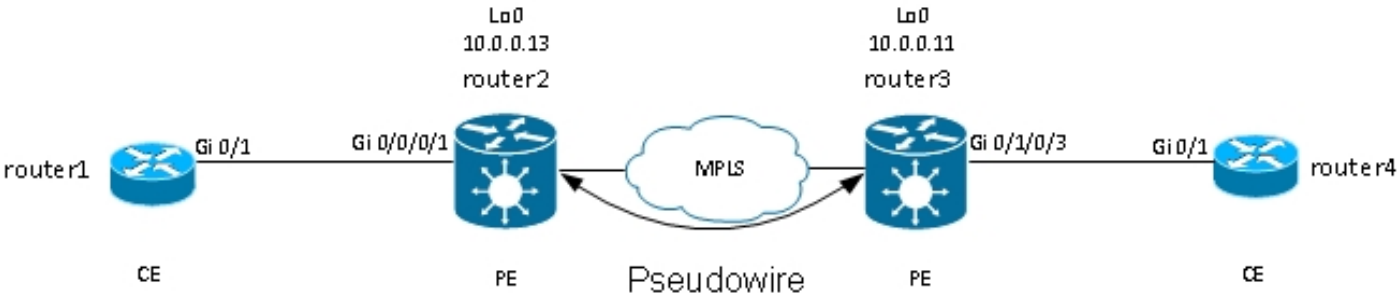
3.4 Spanning Tree

Se L2VPN CE è uno switch Ethernet e invia Spanning Tree BPDU a L2VPN PE, queste BPDU vengono gestite come traffico normale e trasportate in base alla configurazione L2VPN.

I pacchetti BPDU STP o MST vengono inviati senza tag e vengono trasportati tramite la connessione incrociata point-to-point se l'interfaccia principale è configurata come l2transport o se esiste una sottointerfaccia l2transport configurata con i comandi **incapsulation untagged** o **encapsulation default**.

PVST+ (Per VLAN Spanning Tree Plus) o PVST+ (Rapid PVST+) inviano BPDU con tag che vengono trasportati se esiste una sottointerfaccia l2transport che corrisponde al tag dot1q delle BPDU.

Questa è una topologia di esempio:



Router2 e router3 stanno trasportando frame e frame senza tag con tag dot1q tag 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
!
!
!
!
```

Lo switch 1 riceve le BPDU senza tag nella VLAN 1 e le BPDU con tag nella VLAN 2 dallo switch 4; la sua porta radice è su Gi0/1 verso lo switch 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
```

Con questa configurazione, il dominio Spanning Tree del sito A viene unito al dominio Spanning Tree del lato B. Un potenziale problema è che l'instabilità dello Spanning Tree di un sito potrebbe propagarsi all'altro sito.

Se si è certi che un sito è connesso solo tramite un PW a un altro sito e che non esiste alcun collegamento backdoor che potrebbe introdurre un loop fisico, è consigliabile non eseguire Spanning Tree sui due siti. In questo modo i due domini Spanning Tree rimangono isolati. A tale scopo, configurare uno spanning tree bpdufilter sugli EC oppure configurare un elenco degli accessi ai servizi Ethernet sui PE in modo che rilasci i frame con l'indirizzo MAC di destinazione utilizzato dagli BPDU. Un elenco degli accessi ai servizi Ethernet sui sistemi PE può essere utilizzato per rilasciare frame con l'indirizzo MAC di destinazione BPDU o altri tipi di protocolli L2 che non si desidera inoltrare sul PW.

Questo è un elenco degli accessi che può essere utilizzato sotto ciascuna (sotto)interfaccia l2transport che viene trasportata tra i due siti:

```
ethernet-services access-list block-invalid-frames
10 deny any 0180.c200.0000 0000.0000.000f
20 deny any host 0180.c200.0010
30 deny any host 0100.0c00.0000
40 deny any host 0100.0ccc.cccc
```

```
50 deny any host 0100.0ccc.cccd
60 deny any host 0100.0ccd.cdce
70 permit any any
!

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

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

L'ACL dei servizi Ethernet inizia a eliminare i 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)
```

Lo switch 1 non riceve più le BPDU dallo switch 4, quindi lo switch 1 è ora la radice:

```
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
```

Il rischio di disabilitare lo Spanning Tree su un collegamento è questo: se viene creata una connessione backdoor tra i siti, viene introdotto un loop fisico e lo Spanning Tree non può interrompere il loop. Quindi, quando si disabilita lo Spanning Tree su un PW, verificare che non vi siano collegamenti ridondanti tra i siti e che il PW rimanga l'unica connessione tra i siti.

Se sono presenti più connessioni tra i siti, utilizzare una soluzione come VPLS insieme a una versione gateway di accesso dello Spanning Tree, ad esempio MST Access Gateway (MSTAG) o PVST+ Access Gateway (PVSTAG). Per ulteriori informazioni, vedere la sezione relativa a Multipoint Service.

4. Multipoint Service

> **Note:**
>
> per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).
>
> Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

Vedere Implementazione dei servizi Multipoint Layer 2 per una descrizione completa delle funzionalità Multipoint L2.

Con solo due interfacce in una connessione incrociata point-to-point, uno switch L2VPN porta tutto ciò che riceve da un lato e lo inoltra dall'altro.

Quando ci sono più di due interfacce in un dominio-bridge, uno switch Ethernet deve prendere una decisione di switching per determinare dove inoltrare i frame in base all'indirizzo MAC di destinazione. Lo switch esegue l'apprendimento MAC in base all'indirizzo MAC di origine dei frame ricevuti e crea una tabella mac-address-table.

Lo switch inoltra i frame con questo metodo:

- I frame di trasmissione vengono trasmessi a tutte le porte. Usate il controllo della tempesta per limitare la velocità di trasmissione.
- I frame multicast vengono trasmessi a tutte le porte nel dominio bridge, ad eccezione del caso in cui sia configurato lo snooping IGMP (Internet Group Management Protocol) o MLD (Multicast Listener Discovery). Usare il controllo temporale per limitare la velocità di flooding multicast.
- I frame unicast con un indirizzo MAC di destinazione che non fa parte della tabella mac-address-table del dominio bridge (unicast sconosciuto) vengono trasmessi a tutte le porte nel dominio bridge. Usate il controllo temporale per limitare la velocità di allagamento unicast

sconosciuta.
- I frame unicast con un indirizzo MAC di destinazione che fa parte della tabella mac-address-table del dominio bridge vengono inoltrati alla porta dove è stato appreso l'indirizzo MAC di destinazione.

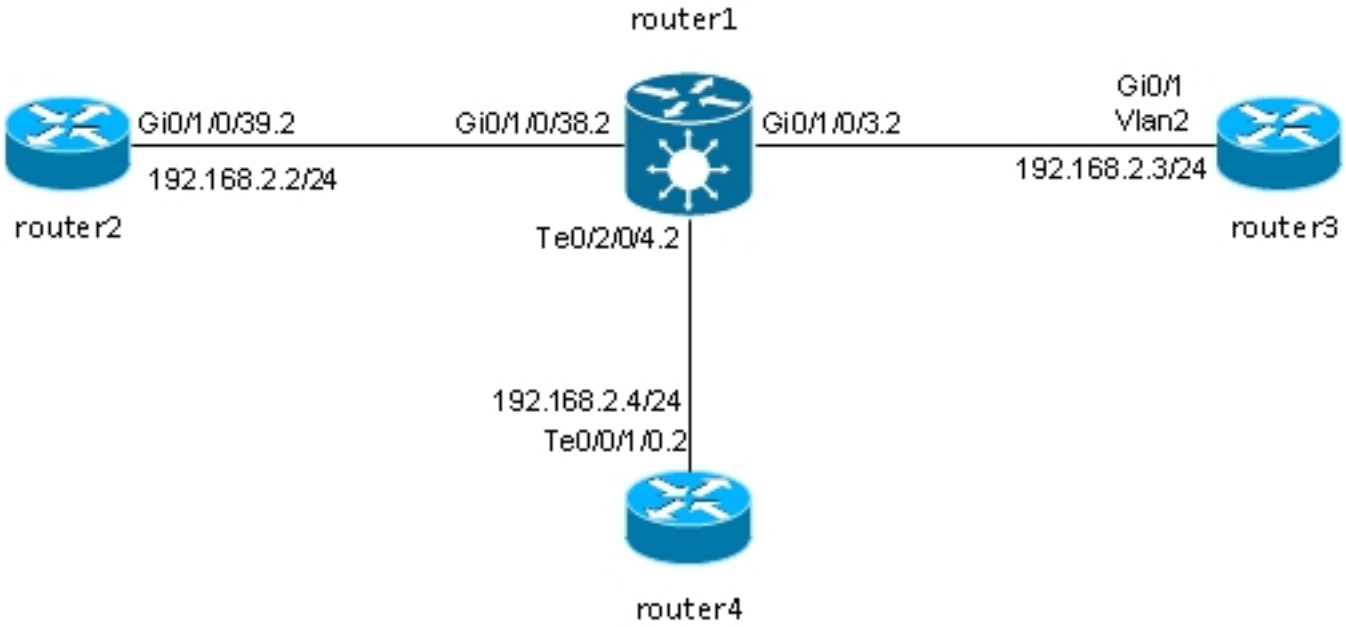
Nel software Cisco IOS XR, un dominio di broadcast o una LAN emulata è detto dominio-bridge. Questa è simile a una VLAN nella terminologia del software Cisco IOS, con la differenza che una VLAN in IOS è collegata a un numero VLAN che viene usato come tag dot1q sui trunk. Un dominio bridge nel software Cisco IOS XR non è collegato a un numero di tag VLAN dot1q. Il modello EVC può essere usato per manipolare i tag dot1q e per avere sottointerfacce dot1q con numeri VLAN diversi nello stesso dominio bridge o interfacce senza tag.

Un dominio bridge è fondamentalmente un dominio broadcast in cui le trasmissioni e i frame multicast vengono trasmessi a tutti i livelli. A ogni bridge-domain è associata una mac-address-table (a meno che l'apprendimento degli indirizzi MAC non venga disabilitato manualmente dalla configurazione, cosa molto rara). In genere corrisponde a una subnet IPv4 o IPv6 in cui tutti gli host nel dominio bridge sono connessi direttamente.

I domini bridge possono essere raggruppati all'interno di un gruppo bridge. Questo è un modo pratico per controllare la configurazione. È possibile eseguire un comando show per un gruppo bridge anziché un comando show per ogni dominio bridge. Un gruppo bridge non dispone di una tabella mac-address-table o di altre associazioni; viene utilizzato solo per i comandi configuration e show.

4.1 Switching locale

Questo è un esempio molto semplice:



Il router2, il router3 e il router4 sono connessi tramite un'ASR 9000, che simula una LAN tra i tre router.

Di seguito sono riportate le configurazioni dell'interfaccia sui tre router:

```
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
!
```

I pacchetti vengono ricevuti dal router1 con il tag 2 dot1q e inoltrati agli altri router con il tag 2 dot1q.

In questo scenario di base, sono disponibili due opzioni per gli ACL:

1. Poiché tutti gli ACL utilizzano il tag 2 dot1q, è possibile mantenerlo sul frame e inoltrarlo sull'interfaccia in uscita con lo stesso tag dot1q ricevuto sull'interfaccia in entrata. il comando **rewrite ingress tag pop 1 symmetric** non è richiesto.

2. Èpossibile inserire il tag 2 dot1q in entrata nella direzione in entrata e spingere simmetricamente il tag 2 dot1q nella direzione in uscita. Anche se questo non è richiesto in questo scenario di base, è buona norma configurare il dominio-ponte in questo modo all'inizio perché fornisce una maggiore flessibilità per il futuro. Di seguito sono riportati due esempi di modifiche che possono verificarsi dopo la configurazione iniziale:

   - Se un'interfaccia BVI indirizzata viene introdotta successivamente nel dominio bridge, i pacchetti devono essere elaborati sulla BVI senza tag. Per ulteriori informazioni, vedere la sezione.
   - Un nuovo ACL, che utilizza un diverso tag dot1q, viene aggiunto in seguito. Il tag 2 dot1q verrebbe inserito nella direzione in entrata e l'altro tag dot1q verrebbe inserito nella nuova interfaccia in uscita e viceversa.BVI

Posizionare i tag dot1q su ciascun CA del router1:

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

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

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

Visualizzare la configurazione del bridge-domain con questi tre ACL:

```
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
!
!
!
!
```

Il dominio bridge deve essere configurato in un gruppo bridge. Se sono necessari altri domini bridge di questo cliente, è possibile configurarli nello stesso gruppo bridge, ovvero il cliente1. Se nuovi domini bridge appartengono a un cliente diverso, è possibile creare un nuovo gruppo bridge. In questi esempi viene utilizzato il cliente per raggruppare i domini bridge, che possono tuttavia essere raggruppati in base a qualsiasi criterio.

Usare il comando **show run l2vpn bridge group customer1 bridge-domain engineering** per visualizzare la configurazione del bridge-domain.

Usare il comando **show run l2vpn bridge group customer1** per visualizzare la configurazione di tutti i domini bridge.

Per visualizzare le informazioni sul bridge-domain, usare il comando **show l2vpn bridge-domain bd-name engineering** o il comando **show l2vpn bridge-domain group customer1**.

```
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:
```

Per controllare che i pacchetti vengano ricevuti e inviati su ciascun access point, usare il comando **show l2vpn bridge-domain group customer1 bd-name engineering det**.

Aggiungere la parola chiave *mac-address* al comando **show l2vpn forwarding bridge-domain** per controllare la tabella degli indirizzi 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'apprendimento MAC viene eseguito nell'hardware dalle linecard ogni volta che un frame viene ricevuto nel dominio bridge. Esiste anche una cache software della tabella mac-address-table, ma questa tabella software non può essere aggiornata continuamente per corrispondere alle voci hardware. Quando il comando **show** viene immesso nel codice recente, tenta di risincronizzare la tabella software con la tabella hardware. Dopo un massimo di 15 secondi, stampa lo stato corrente della mac-address-table del software, anche se la risincronizzazione non è completa (ad esempio, se la tabella è grande). Usare il comando **l2vpn resynchronize forwarding mac-address-table** per risincronizzare manualmente le tabelle software e hardware.

```
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 messaggio syslog indica quando il processo di risincronizzazione è completato, quindi è utile avere **terminal monitor** abilitato per visualizzare il messaggio.

La colonna Durata risincronizzazione visualizza l'ultima volta in cui l'indirizzo MAC è stato risincronizzato dalla tabella hardware.

La parola chiave *location* indica la posizione di una scheda di linea in entrata o in uscita. Gli indirizzi MAC vengono scambiati tra le schede di linea nell'hardware, quindi gli indirizzi MAC devono essere noti su ciascuna scheda di linea in cui è presente un ACL o un PW. La parola chiave *detail* potrebbe fornire una versione più aggiornata della tabella software:

```
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
```

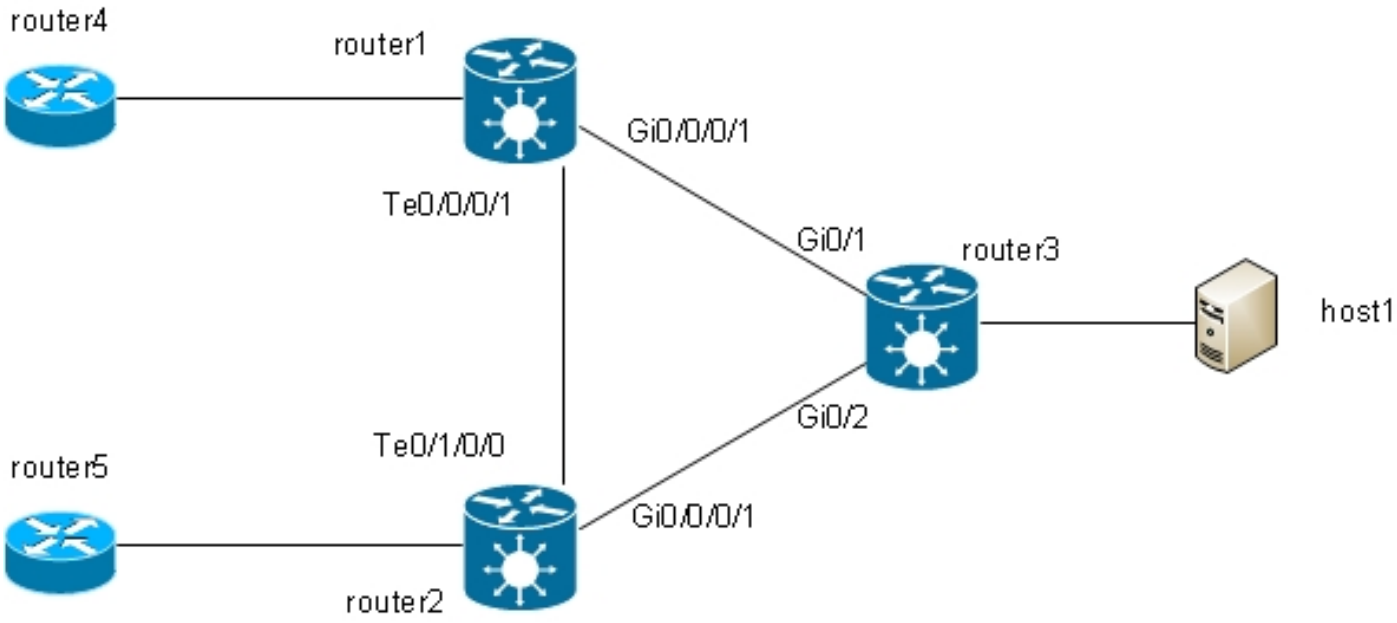
La versione dettagliata del comando fornisce il numero totale di indirizzi MAC appresi nel dominio bridge, nonché il numero di indirizzi MAC appresi in ciascun ACL.

La parola chiave *hardware* esegue il polling della tabella degli indirizzi MAC dell'hardware direttamente dai motori di inoltro in entrata o in uscita:

```
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 TGV completo

Gli esempi precedenti di switching locale erano di base perché solo i router erano connessi al dominio bridge. Tuttavia, quando si inizia a collegare gli switch L2, è possibile introdurre un loop e usare il protocollo STP per interrompere il loop:



In questa topologia, router1, router2 e router3 sono configurati ciascuno con un dominio bridge con tutte le relative interfacce nel diagramma. Se il router4 invia una trasmissione, ad esempio una richiesta ARP, al router1, il router1 la invia al router2 e il router3, il router2 la invia al router3 e il router3 al router2. Ciò si traduce in un loop e in una tempesta radiofonica.

Per interrompere il ciclo continuo, utilizzare un STP. Sono disponibili diversi tipi di STP, ma il software Cisco IOS XR offre un'unica implementazione completa, l'MST.

Inoltre, sono disponibili versioni gateway di accesso dei protocolli supportati nel software Cisco IOS XR, ad esempio PVSTAG e MSTAG. Si tratta di versioni statiche limitate del protocollo da utilizzare in topologie specifiche, in genere con VPLS, descritte nelle sezioni MSTAG e PVSTAG. Nel software Cisco IOS XR, l'opzione MST è l'unica opzione disponibile se è presente una topologia con più switch e se è richiesta un'implementazione Spanning Tree completa.

Su ciascun router vengono configurate due sottointerfacce che vengono aggiunte a un dominio bridge. Per il router1, la configurazione è:

```
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 è configurato sull'interfaccia principale. Nell'esempio, la VLAN 2 è assegnata all'istanza 1 e tutte le altre VLAN rimangono l'istanza predefinita 0. (Una configurazione più realistica consente di suddividere le VLAN in modo uniforme tra le istanze.)

La selezione del bridge radice all'interno di una rete STP è determinata dalla priorità configurata e dall'ID bridge incorporato di ogni dispositivo. Come bridge radice viene selezionato il dispositivo con la priorità più bassa o con la priorità più bassa ma con l'ID bridge più basso. Nell'esempio, il router3 è configurato con una priorità inferiore rispetto al router1 per l'istanza 0, quindi il router3 è la radice per l'istanza 0. Router1 ha una priorità inferiore rispetto a router3 per l'istanza 1, quindi router1 è la radice per l'istanza 1.

Questa è la configurazione del router1:

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

Questa è la configurazione sul router3:

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

Il nome, la revisione e il mapping tra VLAN e istanza devono essere gli stessi su tutti gli switch.

A questo punto, controllare lo stato dello spanning tree sul router1:

```
RP/0/RSP1/CPU0:router1#sh spanning-tree mst customer1
Role: ROOT=Root, DSGN=Designated, ALT=Alternate, BKP=Backup, MSTR=Master
```

```
State: FWD=Forwarding, LRN=Learning, BLK=Blocked, DLY=Bringup Delayed

Operating in dot1q mode


MSTI 0 (CIST):

VLANS Mapped: 1,3-4094

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

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


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


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


MSTI 1:

VLANS Mapped: 2

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


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


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

Il router3 è la radice dell'istanza 0, quindi il router1 ha la porta radice su Gi0/0/0/1 verso il router3. Router1 è la radice dell'istanza 1, quindi router1 è il bridge designato su tutte le interfacce per quell'istanza.

Il router2 è bloccato, ad esempio, 0 sul router Te0/1/0/0:

```
RP/0/RSP1/CPU0:router2#sh spanning-tree mst customer1
```

```
Role: ROOT=Root, DSGN=Designated, ALT=Alternate, BKP=Backup, MSTR=Master
State: FWD=Forwarding, LRN=Learning, BLK=Blocked, DLY=Bringup Delayed

Operating in dot1q mode


MSTI 0 (CIST):

VLANS Mapped: 1,3-4094

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

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


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


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


MSTI 1:

VLANS Mapped: 2

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


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


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

Te0/1/0/0.2 sta inoltrando mentre Te0/1/0/0.3 è bloccato. Quando il valore di STP Blocked è 0x0, la condizione è false, quindi l'interfaccia sta inoltrando; quando il valore di STP Blocked è 0x1, la condizione è true, quindi l'interfaccia è bloccata.

Per verificare questa condizione, usare il comando **show uidb data** e visualizzare i dati di interfaccia presenti nel processore di rete:

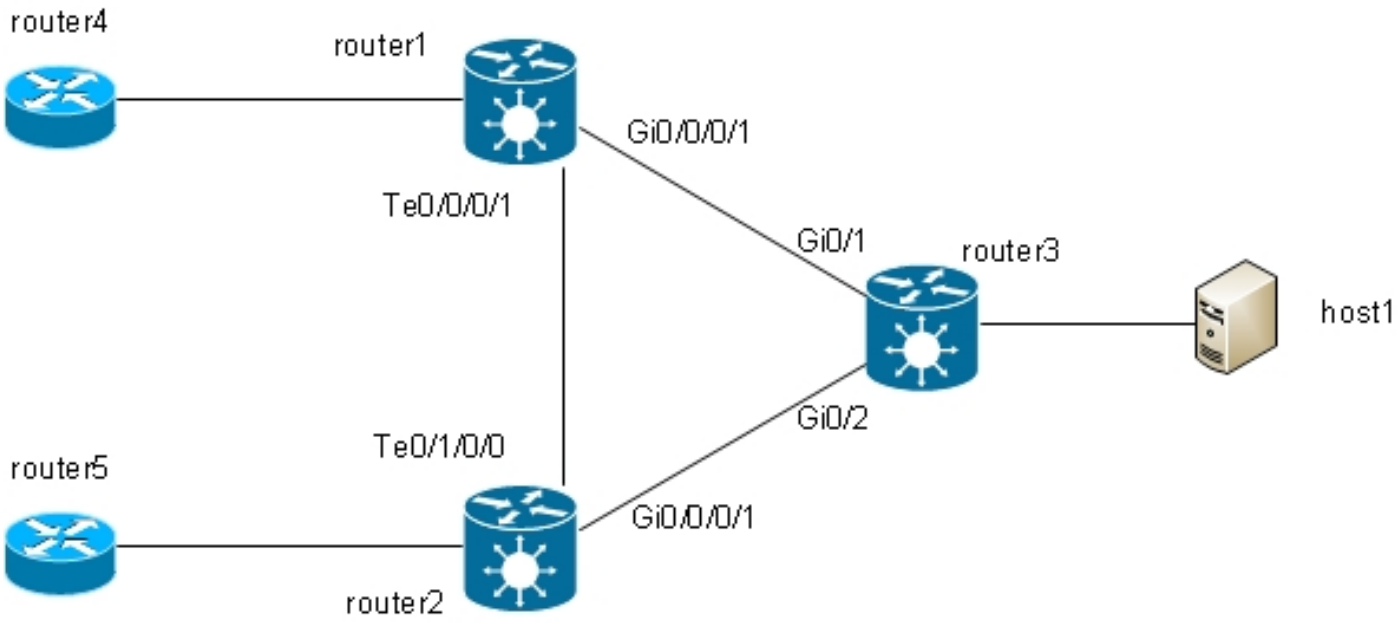
```
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.2
ingress | i Blocked
STP Blocked                         0x0
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.3
ingress | i Blocked
STP Blocked                         0x1
```

4,3 BVI

La configurazione di un dominio bridge crea un dominio L2. Per uscire da tale dominio L2, connettere i router L3 che eseguono il routing tra gli host all'interno del dominio bridge e il mondo esterno. Nel diagramma precedente, l'host 1 poteva utilizzare il router4 o il router5 per uscire dalla subnet locale e raggiungere Internet.

Il router1 e il router2 in cui i domini bridge sono configurati sono router ASR 9000, che possono instradare il traffico IPv4 e IPv6. Questi due router potrebbero prendere il traffico IP dal dominio-ponte e indirizzarlo verso Internet direttamente, invece di affidarsi a router L3. A tale scopo, è necessario configurare una BVI, ossia un'interfaccia L3 che si collega a un dominio bridge per indirizzare i pacchetti in entrata e in uscita dal dominio bridge.

L'aspetto logico è il seguente:



Questa è la configurazione:

```
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
!
```

Una BVI è un'interfaccia L3 senza tag, quindi se si desidera che la BVI elabori i pacchetti ricevuti sugli ACL del dominio di bridge, gli ACL devono essere configurati in modo da eliminare tutti i tag in arrivo. In caso contrario, la BVI non è in grado di capire il tag e scarta i pacchetti. Non è possibile configurare una sottointerfaccia dot1q su un BVI, quindi le etichette devono essere inserite sugli AC come è stato fatto su Gi0/0/0/1.2 nell'esempio precedente.

Poiché un'interfaccia BVI è un'interfaccia virtuale, esistono alcune restrizioni alle funzionalità che è possibile abilitare. Queste restrizioni sono documentate in Configurazione del routing e del bridging integrato su Cisco ASR serie 9000 Router: restrizioni per la configurazione di IRB. Le seguenti funzioni non sono supportate sulle interfacce BVI di ASR 9000:

- Access Control Lists (ACLs). Tuttavia, gli ACL L2 possono essere configurati su ciascuna porta L2 del dominio bridge.
- IP Fast Reroute (FRR)
- NetFlow
- MoFRR (Fast Re-Route solo multicast)
- Commutazione etichette MPLS
- mVPNv4
- QoS (Quality of Service)
- Mirroring del traffico
- Interfaccia senza numero per BVI
- Monitoraggio video (Vidmon)

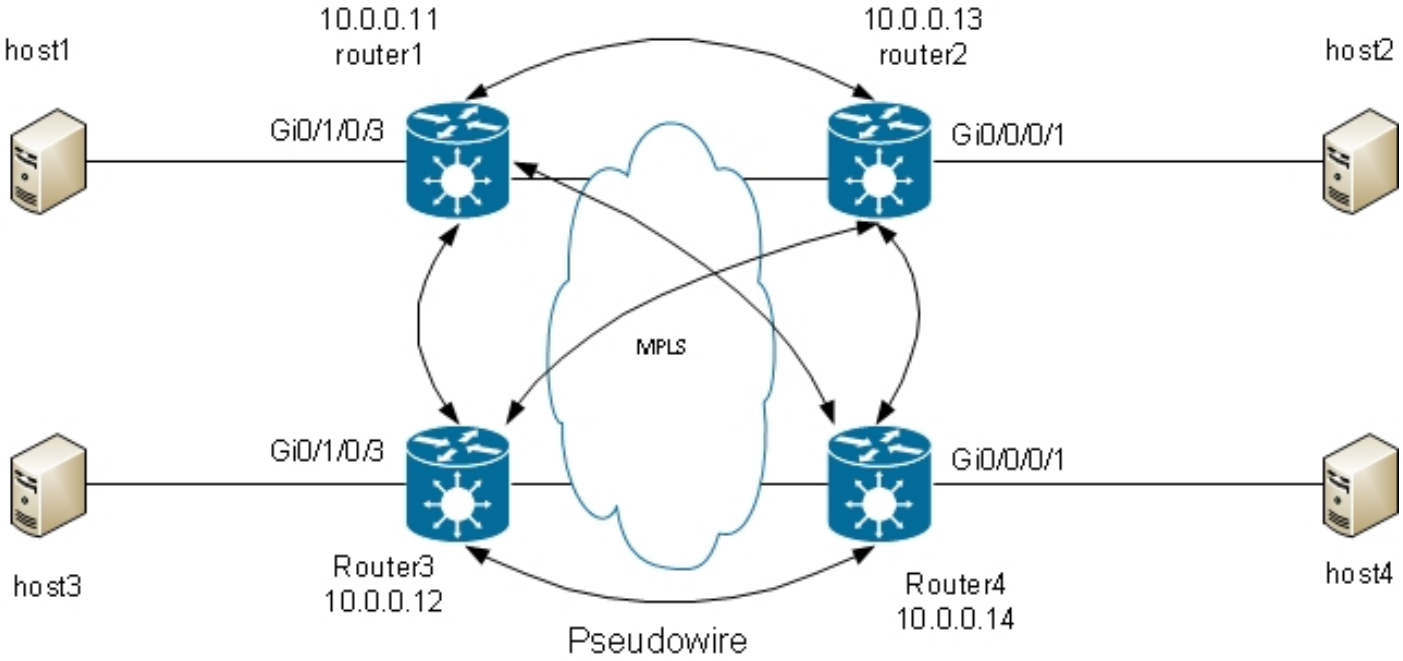
Il BVI può essere in una configurazione VRF (Virtual Routing and Forwarding), in modo che il traffico ricevuto sul BVI venga inoltrato su MPLS, ma deve essere utilizzata la *modalità di allocazione etichette per ogni VRF*.

Se è necessaria una di queste funzionalità limitate, non è possibile utilizzare un BVI. In alternativa, è possibile utilizzare un cavo di loopback esterno tra due porte del router, dove una porta si trova nel dominio-bridge e una porta è configurata come una normale interfaccia di routing in cui è possibile configurare tutte le funzionalità.

4,4 VPLS

4.4.1 Panoramica

VPLS consente di combinare domini bridge in più siti in un unico grande dominio bridge tramite PW MPLS. Gli host nei diversi siti sembrano essere connessi direttamente allo stesso segmento L2 perché il loro traffico è incapsulato in modo trasparente sull'intera rete di PW MPLS tra i PE L2VPN:



Per garantire che ciascun host possa ricevere il traffico da tutti gli altri, è necessario disporre di una rete completa di PW. Di conseguenza, un PE L2VPN non inoltra un frame ricevuto su un PW VPLS rispetto agli altri PW VPLS. Dovrebbe esistere una rete completa di PW, in modo che ogni PW riceva il traffico direttamente e non debba inoltrare il traffico tra PW poiché l'inoltro causerebbe un loop. Questa regola è denominata regola dell'orizzonte diviso.

Il router esegue l'apprendimento MAC. Una volta che un indirizzo MAC è presente nella tabella mac-address-table, si inoltra solo il frame per l'indirizzo MAC di destinazione attraverso il PW al PE L2VPN da cui è stato appreso questo indirizzo MAC. In questo modo si evitano inutili duplicazioni del traffico nel core. Le trasmissioni e i multicast vengono trasmessi su tutti i PW in modo da garantire che tutti gli host possano riceverli. Una funzione come lo snooping IGMP è utile perché consente l'invio di frame multicast a PE solo in presenza di ricevitori o router multicast. In questo modo si riduce la quantità di traffico nel core, anche se esistono ancora più copie degli stessi pacchetti che devono essere inviate a ciascun PE quando vi è interesse per quel gruppo.

La rete completa dei PW deve essere configurata in una VFI (Virtual Forwarding Instance):

```
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
!
!
!
!
!
```

I PW configurati in VFI sono quelli con mesh completa nel core. Fanno parte dello stesso gruppo di orizzonti divisi (SHG) per essere certi che i frame ricevuti su un PW non vengano inoltrati a un altro PW.

Èpossibile configurare i PW di accesso, che sono considerati un tipo di alimentazione CA e non sono configurati nel VFI. Per ulteriori informazioni, vedere la sezione.

La configurazione sui router2, router3 e router4 è molto simile e tutti gli altri tre router sono router adiacenti sotto il filtro 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'etichetta locale per PW su 10.0.0.12 è 16049, quindi i frame Ethernet vengono ricevuti con l'etichetta 16049. La decisione di commutazione si basa su questa etichetta MPLS perché il penultimo hop MPLS deve aver aperto l'etichetta IGP. È possibile che sia ancora presente un'etichetta Null esplicita, ma la decisione di commutazione si basa sull'etichetta 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
```

Il comando **show mpls forwarding labels** per l'etichetta fornisce il numero di dominio-bridge, che è possibile usare per trovare l'indirizzo MAC di destinazione e il PW (adiacente e pw-id) dove il pacchetto è stato ricevuto. È quindi possibile creare nella tabella mac-address-table voci che puntino a tale router adiacente:

```
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 Tipi di PW e tag trasportati

I PW VPLS vengono negoziati come PW di tipo 5 (Ethernet) per impostazione predefinita. Tutti gli elementi che entrano nell'alimentatore CA dopo la manipolazione del tag VLAN (quando è configurato il comando **rewrite**) vengono inviati al PW.

Il software Cisco IOS XR versione 4.1.0 per la segnalazione LDP e la versione 4.3.1 con BGP consentono di configurare una classe pw in un router adiacente e la **modalità di trasporto** della **vlan in** una classe pw. Questa procedura consente di negoziare una connessione virtuale (VC) di tipo 4 (VLAN Ethernet) PW, che trasferisce tutto ciò che esce dall'access point dopo la manipolazione del tag VLAN quando viene configurato il comando **rewrite**.

La manipolazione del tag VLAN sull'EFP assicura che sul frame sia presente almeno un tag VLAN, in quanto è necessario un tag dot1q sul frame se sono presenti PW VC di tipo 4. Quando si usa la modalità **trasporto** vlan **passthrough** mode, al frame non viene aggiunto alcun tag fittizio 0.

Non è supportata la combinazione di PW di tipo 4 e 5 nello stesso VFI. Tutti i PW devono essere dello stesso tipo.

```
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 Rilevamento e segnalazione automatici

I modelli erano basati sulla configurazione manuale di tutti i vicini sotto il VFI. MPLS LDP è stato utilizzato per la segnalazione del PW con il router adiacente.esempi precedenti

Quando si aggiunge un nuovo VPLS PE alla rete, configurare il PE in modo che disponga di una PW per tutti i PE esistenti in ciascuno dei relativi domini bridge locali. Tutti i PE esistenti devono quindi essere riconfigurati in modo da avere una PW per il nuovo PE, in quanto tutti i PE devono avere una mesh completa. Ciò potrebbe diventare una sfida operativa con l'aumento del numero di PE e di domini-ponte.

Una soluzione consiste nell'individuare automaticamente altri PE tramite BGP. Sebbene vi sia anche un requisito di rete completa per l'IBGP, esso può essere sollevato mediante l'uso di catadiottri di rotta. Di conseguenza, un nuovo PE viene in genere configurato per eseguire il peer con un numero ridotto di riflettori di route, tutti gli altri PE ricevono i relativi aggiornamenti e il nuovo PE riceve gli aggiornamenti dagli altri PE.

Per individuare altri PE tramite BGP, ogni PE è configurato per la *famiglia di indirizzi vpls-vpws* e annuncia in BGP i domini di bridge a cui desiderano partecipare. Una volta individuati gli altri PE

che fanno parte dello stesso dominio-ponte, viene stabilito un PW per ciascuno di essi. BGP è il protocollo utilizzato per questa individuazione automatica.

Per la segnalazione della PW ai PE con rilevamento automatico sono disponibili due opzioni: BGP e LDP. In questi esempi, la topologia precedente viene convertita in individuazione automatica BGP con segnalazione BGP e segnalazione LDP.

4.4.3.1 Rilevamento automatico BGP e segnalazione BGP

Configurare la famiglia di indirizzi **l2vpn vpls-vpws** sotto il router bgp e i router adiacenti, ossia altri PE o riflettori di routing:

```
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 nuova famiglia di indirizzi diventa attiva con i vicini, ma nessun PE ha ancora annunciato la sua partecipazione in un dominio-ponte:

```
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
```

Configurare **autodiscovery bgp** e **signaling-protocol bgp** in modalità di configurazione L2VPN bridge-domain. La configurazione sul router1 è:

```
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 configurazione sul router2 è:

```
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-vpn e la destinazione-route sono gli stessi nei diversi PE di ogni dominio bridge, ma ogni PE dispone di un ID del perimetro virtuale (VE-ID) univoco. Ogni PE individua gli altri PE nella VPN tramite BGP e utilizza BGP per segnalare i PW. Il risultato è una maglia completa di 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
```

Questi sono i prefissi annunciati dal router3 (10.0.0.13) come visualizzati sul router1; i prefissi vengono ricevuti tramite i due catadiottri, 10.0.0.3 e 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
```

Il router1 ha stabilito alcuni 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 Rilevamento automatico BGP e segnalazione LDP

La configurazione BGP con il comando **l2vpn vpls-vpws** della famiglia di indirizzi è esattamente la stessa della segnalazione BGP. La configurazione L2VPN viene modificata in modo da utilizzare la segnalazione LDP con il comando **signaling-protocol ldp**.

La stessa configurazione viene utilizzata in tutti e quattro i 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
!
!
!
!
!
!
```

Il vpls-id è costituito dal numero BGP Autonomous System (AS) e dal vpn-id.

Tre comandi show del router1 indicano che i PW sono stati stabiliti con i PE rilevati:

```
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 Svuotamenti e ritiri MAC

L'inoltro in VPLS si basa sulla tabella mac-address-table, che viene creata dinamicamente imparando gli indirizzi MAC di origine dei frame ricevuti. In caso di modifica della topologia in un dominio-bridge, un host potrebbe diventare raggiungibile tramite un ACL o un VPLS adiacente diverso. Il traffico per l'host potrebbe non raggiungere la destinazione se i frame continuano ad essere inoltrati in base alla tabella mac-address-table esistente.

Per un PE L2VPN, sono disponibili diversi modi per rilevare una modifica alla topologia:

- Una porta nel dominio-ponte si solleva o si abbassa.
- Una BPDU Spanning Tree Topology Change Notification (TCN) viene elaborata quando il PE L2VPN esegue l'implementazione MST completa o un protocollo Spanning Tree Access Gateway. È possibile che il collegamento che causa l'errore non sia locale nel PE, ma più lontano nella topologia. Il PE intercetta il TCN.

Quando un PE L2VPN rileva una modifica della topologia, vengono eseguite due azioni:

1. Il file PE scarica la tabella degli indirizzi MAC dei domini bridge interessati dalla modifica della topologia. Quando il PVSTAG o il PVRSTAG (Rapid Spanning Tree Access Gateway) sono configurati per il PVSTAG o per VLAN, un BPDU TCN rilevato in una sottointerfaccia VLAN influisce su tutte le VLAN e i domini bridge su quell'interfaccia fisica.
2. Il PE invia un segnale ai router adiacenti VPLS tramite un messaggio di ritiro MAC LDP MPLS per segnalare che devono scaricare la tabella degli indirizzi MAC. Tutti i PE L2VPN remoti che ricevono il messaggio LDP di ritiro MAC scaricano le tabelle degli indirizzi MAC e il traffico viene nuovamente inondato. Le tabelle mac-address-table vengono ricostruite in base alla nuova topologia.

Il comportamento predefinito del messaggio di ritiro MAC in caso di flap della porta è cambiato nel tempo:

- Tradizionalmente nel software Cisco IOS XR, un PE L2VPN ha inviato messaggi di ritiro MAC quando un CA stava per scendere. L'intento era quello di far scaricare dai PE remoti le tabelle degli indirizzi MAC per il dominio di bridge interessato in modo che gli indirizzi MAC che puntano dietro la porta abbattuta venissero appresi da un'altra porta.
- Tuttavia, ciò ha creato un problema di interoperabilità con alcuni PE remoti che seguono la RFC 4762 ed eliminano gli indirizzi MAC che puntano a tutti i PE tranne quello che sta inviando il messaggio di ritiro MAC. La RFC 4762 presume che un dispositivo PE invii un messaggio di disattivazione dell'indirizzo MAC quando viene attivato un alimentatore CA, ma non quando quest'ultimo si disattiva. Dopo la versione 4.2.1 del software Cisco IOS XR, per impostazione predefinita i messaggi di ritiro degli indirizzi MAC LDP vengono inviati solo quando viene visualizzata una porta di dominio-bridge per conformarsi meglio all'RFC. È stato

aggiunto un comando di configurazione per ripristinare il comportamento precedente. Questo è un comando show con il comportamento predefinito dopo il software Cisco IOS XR versione 4.2.1:

```
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 riga importante è il messaggio 'MAC Ritiro inviato sulla porta bridge Giù', che ora è disabilitato per impostazione predefinita dopo il software Cisco IOS XR versione 4.2.1. Il comando fornisce anche il numero di messaggi MAC di ritiro inviati e ricevuti nel dominio bridge. Un numero elevato di messaggi di ritiro indica instabilità nel dominio-ponte.

Questa è la configurazione che ripristina il comportamento precedente:

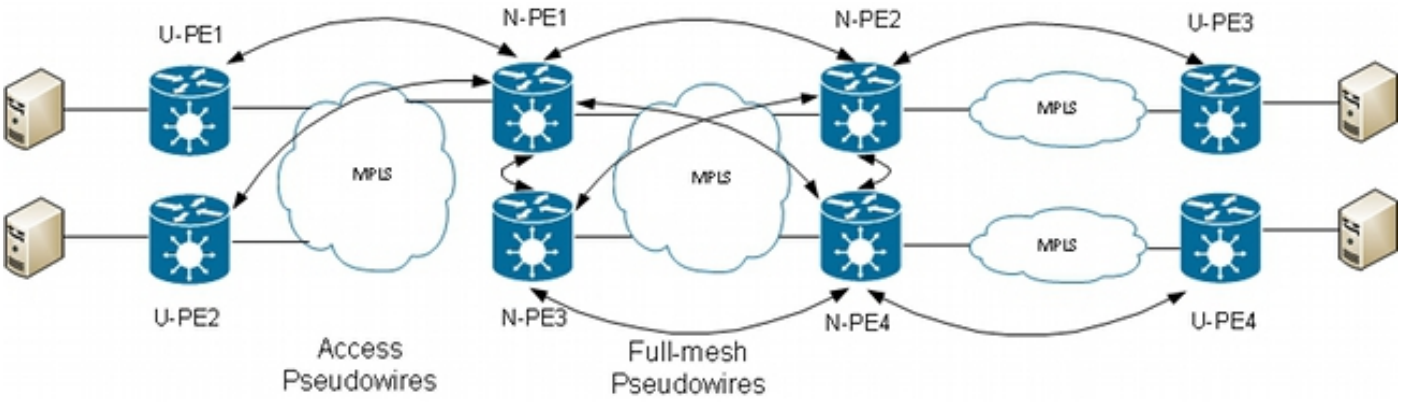
```
l2vpn
bridge group customer1
bridge-domain finance
mac
withdraw state-down
!
!
!
!
```

4.4.5 H-VPLS

VPLS richiede una mesh completa di PW tra i PE L2VPN per garantire che ogni PE possa raggiungere, in un hop, un host dietro qualsiasi altro PE senza la necessità che un PE rifletta i frame da un PW a un altro PW. Questa è la base per la regola dell'orizzonte di divisione, che impedisce a un PE di inoltrare i frame da un PW a un altro PW. Anche in casi speciali, in cui l'indirizzo MAC di destinazione nella tabella mac-address-table punta a un altro PW, il frame viene scartato.

Una mesh completa di PW significa che il numero di PW potrebbe diventare molto elevato con l'aumento del numero di PW, e questo potrebbe introdurre problemi di scalabilità.

Èpossibile ridurre il numero di PW in questa topologia con una gerarchia di PW:



In questa topologia, tenere presente che:

- Un dispositivo U-PE (User Provider Edge) dispone di CA per gli EC.
- Il dispositivo U-PE trasporta il traffico CE su un PW point-to-point MPLS su un dispositivo Network Provider Edge (N-PE).
- L'N-PE è un VPLS PE di base completamente mesh con altri N-PE.
- Sulla N-PE, il PW proveniente dall'U-PE è considerato un PW di accesso molto simile a un AC. L'U-PE non fa parte della mesh con gli altri N-PE, quindi l'N-PE può considerare il PW di accesso come un CA e inoltrare il traffico da quel PW di accesso ai PW core che fanno parte della mesh completa del VPLS.
- I PW di base tra N-PE sono configurati in una VFI in modo da assicurare che la regola dell'orizzonte di divisione sia applicata a tutti i PW di base configurati in base alla VFI.
- I PW di accesso dagli U-PE non sono configurati in una VFI, quindi non appartengono allo stesso SHG dei PW VFI. Il traffico può essere inoltrato da un PW di accesso a un PW VFI e viceversa.
- Gli U-PE possono utilizzare la funzione di ridondanza PW per disporre di una PW primaria in una N-PE primaria e di una PW di standby in una N-PE di standby. Lo standby prende il sopravvento quando la PW principale si interrompe.

Questo è un esempio di configurazione di U-PE1 (10.0.0.15) con ridondanza PW su N-PE1 (10.0.0.11) e 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
------------------------------------------------------------------------------
```

Il PW su 10.0.0.12 è in stato di standby. In N-PE1, sono presenti un access PW a 10.0.0.15 e un alimentatore CA non incluso nel VFI.

N-PE1 sta apprendendo alcuni indirizzi MAC sul PW di accesso e sui 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
```

In N-PE2 (10.0.0.12), il PW di accesso è in stato di standby:

```
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 Gruppi di orizzonti divisi (SHG)

La regola dell'orizzonte di divisione stabilisce che un frame ricevuto su una PW VFI non può essere inoltrato su un'altra PW VFI. Le VFI N-PE devono avere una rete completa.

Questo orizzonte di divisione viene imposto tramite un SHG:

- I membri di un gruppo di SHG non possono inoltrare frame l'uno all'altro, ma possono inoltrare frame ai membri di altri gruppi di SHG.
- Per impostazione predefinita, tutte le PW VFI vengono assegnate a SHG 1. Ciò garantisce che non vi sia inoltro tra PW VFI in modo che la regola dell'orizzonte di divisione venga applicata. I pacchetti ricevuti su una PW VFI possono essere inoltrati agli ACL e accedere ai PW perché non fanno parte dello stesso SHG.
- Per impostazione predefinita, tutti gli ACL e i PW di accesso non fanno parte di un gruppo SHG, il che significa che i pacchetti ricevuti su un ACL o su un PW di accesso possono essere inoltrati a un altro ACL o a un PW di accesso nello stesso dominio bridge.

- Gli ACL e i PW di accesso possono essere assegnati all'SHG 2 con il comando **split-horizon group** se l'obiettivo è quello di impedire l'inoltro tra di essi.

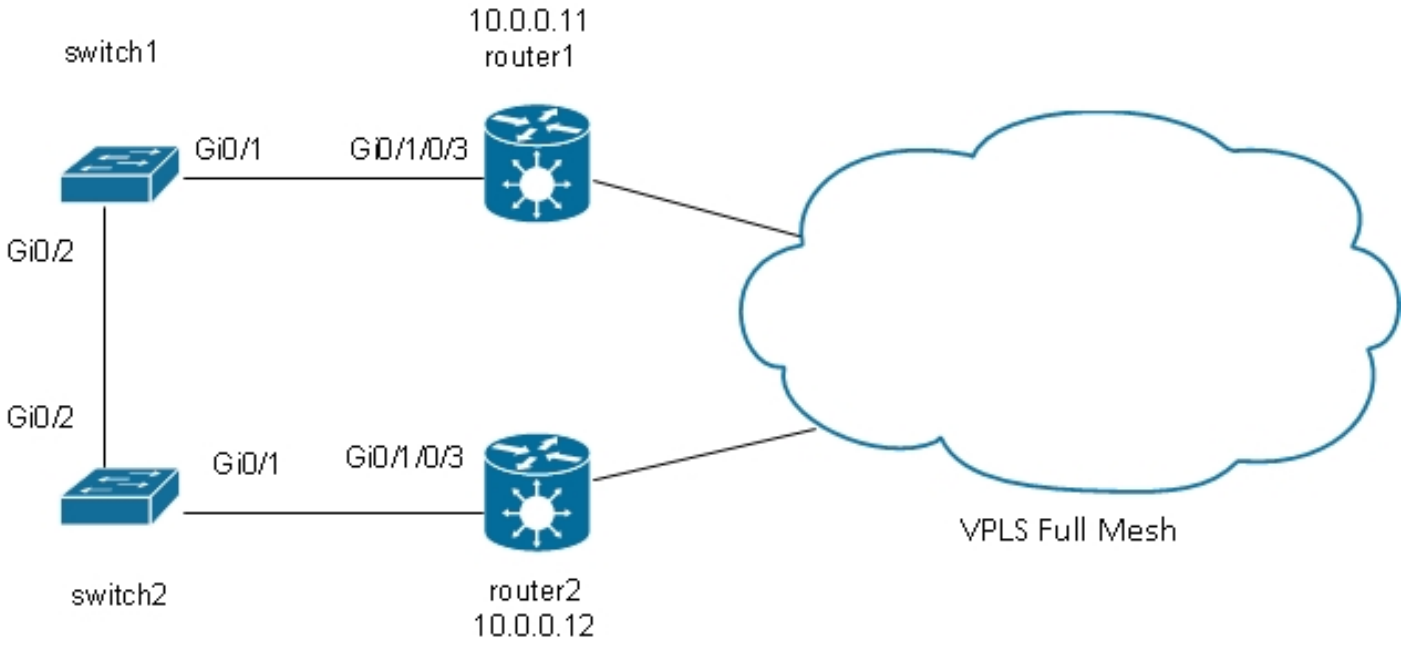
```
RP/0/RSP0/CPU0:N-PE1#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
split-horizon group
!
interface GigabitEthernet0/1/0/3.2
split-horizon group
!
neighbor 10.0.0.15 pw-id 15
split-horizon group
!
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
!
!
!
!
!
```

In questa configurazione, non è possibile eseguire l'inoltro tra Gi 0/0/0/1.2 e Gi 0/1/0/3.2, Gi 0/0/0/1.2 e 10.0.0.15 o Gi 0/1/0/3.2 e 10.0.0.15. Tuttavia, è possibile che vi sia ancora un inoltro del traffico tra gli ACL e i POW VFI in quanto fanno parte di SHG diversi (1 e 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 Ridondanza

Nel tentativo di introdurre la ridondanza, è possibile avere un sito a doppio collegamento al dominio VPLS:



Se un host collegato allo switch1 invia una trasmissione, lo switch1 la inoltra al router1 e allo switch2. Poiché il router1 ha una rete completa di PW, è presente un PW al router2 e il router1 inoltra la trasmissione su tale PW. Il router2 inoltra la trasmissione allo switch2, che la inoltra allo switch1. Il risultato è un loop fisico.

4.4.7.1 Spanning Tree

L'implementazione MST completa non funziona con VPLS perché quell'implementazione invia BPDU MST su un'interfaccia principale per controllare lo stato di inoltro di tutte le VLAN su quell'interfaccia. Con i VPLS, sono presenti VFI per ciascun bridge-domain, quindi non è possibile inviare BPDU su un'interfaccia principale per tutte queste VFI.

Per impostazione predefinita, le BPDU dello Spanning Tree vengono trasportate su VPLS e su PW point-to-point.

Se lo switch 1 e lo switch 2 inviano BPDU per VLAN o MST senza tag e se le BPDU corrispondono alle sottointerfacce l2transport sul router1 e sul router2, le BPDU vengono trasportate tramite VPLS. Gli switch vedono le rispettive BPDU sulle interfacce Gi 0/1 e lo Spanning Tree interrompe il loop e blocca una porta.

Lo switch 2 è la directory principale della 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)
```

Lo switch 1 ha la porta radice su Gi 0/1 e sta bloccando 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
```

Il problema è che le BPDU vengono anche trasferite su siti remoti e l'instabilità dello spanning tree in un sito si propaga a tutti i siti connessi al dominio VPLS. È più sicuro isolare ciascun sito e non trasportare le BPDU su VPLS.

Una soluzione è l'uso di una versione gateway di accesso dell'STP. Si tratta di un'implementazione limitata del protocollo, in cui i PE L2VPN sono configurati per inviare alcuni BPDU statici in modo che appaiano connessi alla radice dello spanning tree. L2VPN PE non trasferisce le BPDU ricevute dagli EC ai siti remoti, quindi ogni sito ha il proprio dominio Spanning Tree.

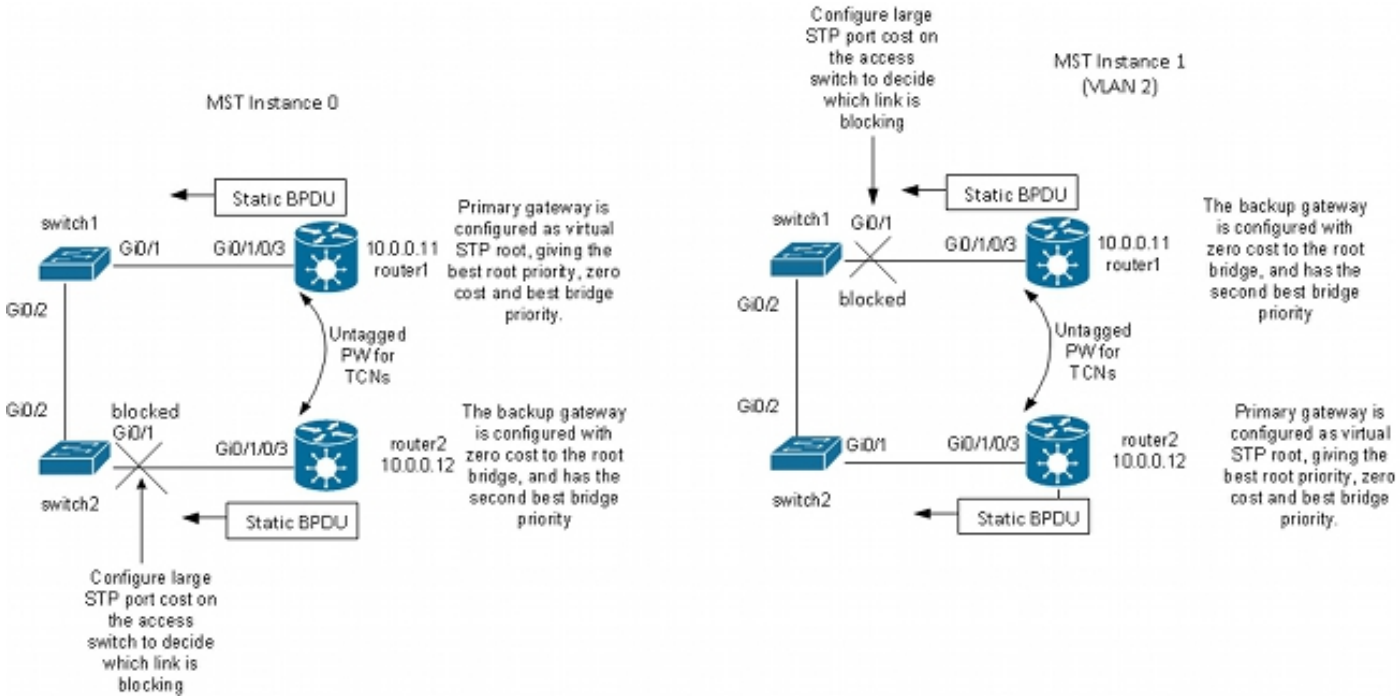
4.4.7.2 MSTAG

Come spiegato nella sezione Spanning Tree, l'MST invia pacchetti BPDU senza tag, ma questi pacchetti BPDU controllano lo stato di inoltro di tutte le VLAN sull'interfaccia.

Le VLAN possono essere raggruppate in più istanze e ogni istanza ha il proprio stato di inoltro.

Le VLAN sono in genere raggruppate in modo che il traffico possa essere distribuito uniformemente su più percorsi. Quando sono presenti due percorsi, metà del traffico appartiene a un'istanza che sta inoltrando sul primo percorso e blocca sul secondo percorso. L'altra metà del traffico appartiene a un'istanza che sta bloccando il primo percorso e inoltrando il secondo percorso. Ciò consente il bilanciamento del carico tra i due percorsi in condizioni stabili. In caso contrario, si dispone di un percorso che in genere è completamente bloccato e diventa attivo solo quando il percorso primario è inattivo.

Di seguito è riportata una topologia MSTAG tipica:



Nell'esempio di laboratorio, l'istanza 1 ha la VLAN 2 e l'istanza 0 ha le altre VLAN. In uno scenario più realistico, le VLAN vengono distribuite tra più istanze per ottenere un buon bilanciamento del carico del traffico tra le istanze. Poiché alcune VLAN includono molto più traffico di altre, non sempre lo stesso numero di VLAN è presente in ciascuna istanza.

Questa è la configurazione per l'istanza MST 0:

- Il router1 e il router2 stanno inviando alcuni BPDU statici basati sulla configurazione MSTAG. Non stanno elaborando le BPDU in arrivo dalla rete o stanno tentando di eseguire un'implementazione completa. Con MSTAG, i due PE L2VPN inviano semplicemente BPDU statici in base alla configurazione MSTAG.
- Il router1 è configurato in modo da attirare il traffico dell'istanza 0 apparendo come la radice di quell'istanza.
- Il router2 è configurato con la seconda priorità radice migliore, ad esempio 0, in modo che diventi la nuova radice in caso di errore del router1 o di errore dell'alimentazione CA tra lo switch1 e il router1.
- Lo switch 2 è configurato con un costo elevato per lo spanning tree sulla porta da Gi 0/1 a router 2 in modo da garantire che il percorso primario alla radice si trovi su Gig 0/2 attraverso lo switch 1 e il router 1.
- Lo switch 2 seleziona Gi 0/2 come porta radice per instance0 e seleziona Gi 0/1 come porta alternativa in caso di perdita della porta radice.
- Pertanto, il traffico proveniente da quel sito nelle VLAN appartenenti all'istanza 0 raggiunge altri siti tramite VPLS e passa per il router1.

Per l'istanza MST 1 (VLAN 2), la configurazione viene invertita:

- Il router2 è configurato in modo da attirare il traffico dell'istanza 1, apparendo come la radice di tale istanza.
- Il router1 è configurato con la priorità principale secondaria per l'istanza 1, in modo che diventi la nuova radice in caso di errore del router2 o di errore dell'alimentazione CA tra lo switch2 e il router2.

- Lo switch 1 è configurato con un costo elevato per lo Spanning Tree sulla porta Gi 0/1 al router1 in modo da garantire che il suo percorso primario alla radice sia su Gig 0/2 attraverso lo switch2 e il router2.
- Lo switch 1 seleziona Gi 0/2 come porta radice per l'istanza 1 e seleziona Gi 0/1 come porta alternativa in caso di perdita della porta radice.
- Pertanto, il traffico proveniente da quel sito nelle VLAN che appartengono all'istanza 1 (la VLAN 2 in questo esempio) raggiunge altri siti tramite VPLS e passa per il router2.
- Deve essere presente una sottointerfaccia sui router1 e sui router2 per catturare i TCN senza tag e inoltrarli tramite un PW point-to-point all'altro router. Poiché lo switch1 e lo switch2 potrebbero perdere i loro collegamenti diretti e rimanere isolati l'uno dall'altro, il router1 e il router2 devono inoltrare i TCN tra di loro attraverso il PW point-to-point.
- I PE intercettano inoltre i TCN, scaricano le tabelle degli indirizzi MAC e inviano il ritiro degli indirizzi MAC LDP ai PE remoti.

Questa è la configurazione sul router1:

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

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

```
!

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

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

RP/0/RSP0/CPU0:router1#sh spanning-tree mstag customer1-0-1-0-3
GigabitEthernet0/1/0/3.1
Pre-empt delay is disabled
Name: customer1
Revision: 1
Max Age: 20
Provider Bridge: no
Bridge ID: 0000.0000.0001
Port ID: 1
External Cost: 0
Hello Time: 2
Active: yes
BPDUs sent: 3048
MSTI 0 (CIST):
VLAN IDs: 1,3-4094
Role: Designated
Bridge Priority: 4096
Port Priority: 128
Cost: 0
Root Bridge: 0000.0000.0001
Root Priority: 4096
Topology Changes: 369
MSTI 1
VLAN IDs: 2
Role: Designated
Bridge Priority: 8192
Port Priority: 128
Cost: 0
Root Bridge: 0000.0000.0002
Root Priority: 4096
Topology Changes: 322
```

In questa configurazione, tenere presente che:

- Nella MST istanza 0, il bridge radice è 0000.0000.0001, che è l'ID del bridge del router1.
- Nella MST istanza 1, il bridge radice è 0000.0000.0002, che è l'ID del bridge del router2.
- La priorità bridge del router1 è 4096 nell'istanza 0 (per diventare la radice) e 8192 nell'istanza 1 (per diventare la seconda radice migliore).
- La priorità del bridge del router1 è 8192 nell'istanza 0 (per diventare la seconda radice migliore) e 4096 nell'istanza 1 (per diventare la radice).
- La connessione incrociata point-to-point su Gigabit Ethernet0/1/0/3.1 porta gli MST TCN senza tag sull'altro router.

Sulle sottointerfacce dot1q è stato configurato un ACL di uscita per eliminare le BPDU per VLAN che potrebbero essere inviate da un altro sito che non è stato ancora migrato alla MST. Questa configurazione impedisce allo switch CE di dichiarare che l'interfaccia è incoerente quando riceve una BPDU per VLAN su un'interfaccia configurata per MST.

La configurazione sul router2 è molto simile:

```
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
```

Questa è la configurazione base dello switch 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
```

Pertanto, il traffico nell'istanza 0 viene inoltrato tramite il router1 e il traffico nell'istanza 1 viene inoltrato tramite lo switch2 e il router2.

La configurazione sullo switch2 utilizza gli stessi comandi dello switch1:

```
switch2#sh run | b spanning
spanning-tree mode mst
```

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

switch2#sh spanning-tree

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

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

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



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

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

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

Lo switch 2 passa attraverso lo switch1 e il router1, ad esempio instance0, e attraverso il router2, ad esempio instance1.

Il traffico viene bilanciato perché un'istanza esce dal sito tramite router1 e l'altra esce dal sito tramite router2.

Se il collegamento tra il router1 e lo switch1 è inattivo, entrambe le istanze passano attraverso il router2.

```
switch1#sh spanning-tree

MST0
Spanning tree enabled protocol mstp
Root ID Priority 4096
```

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

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

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



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

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

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


switch2#sh spanning-tree

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

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

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



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

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

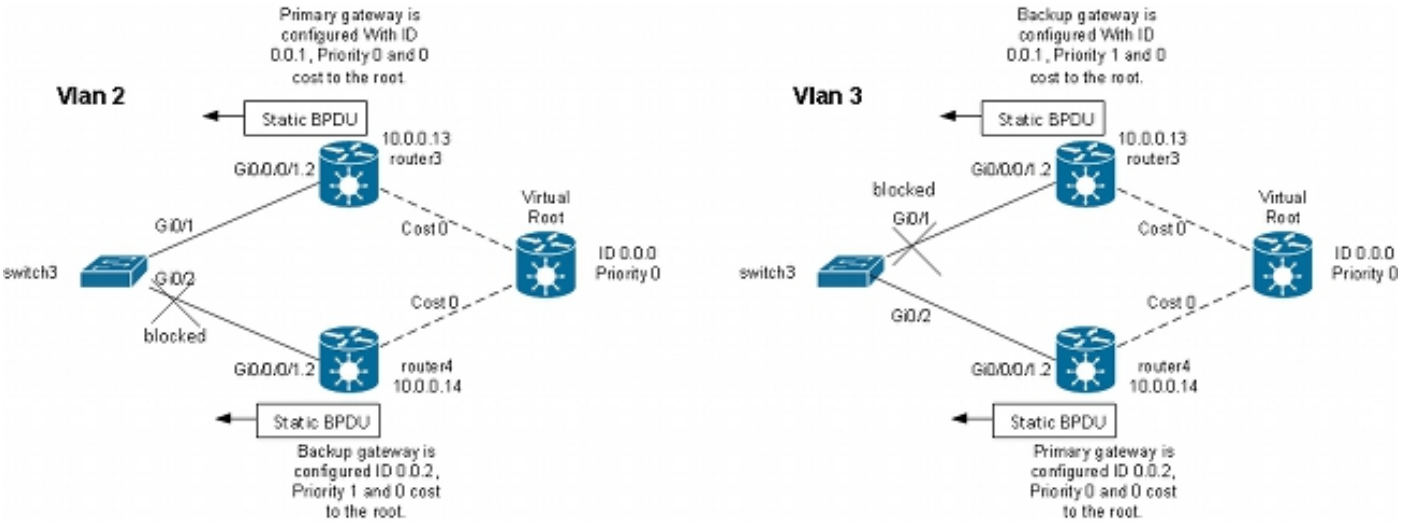
```
Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- ------------------------------
Gi0/1 Root FWD 20000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p
```

In questo tipo di errore è possibile ottenere una rapida convergenza in quanto il percorso che passa attraverso la seconda radice migliore è già stato selezionato come percorso alternativo. Con MSTAG, la maggior parte delle BPDU non viene trasportata su VPLS, quindi i siti sono isolati dall'instabilità di altri siti.

4.4.7.3 PVSTAG o PVRSTAG

MSTAG è il protocollo gateway di accesso preferito per VPLS perché usa lo Spanning Tree rapido e perché è scalabile con il suo uso di istanze anziché di BPDU su ciascuna VLAN.

Se non è possibile eseguire la migrazione di un sito a MST e l'unica soluzione consiste nel mantenere in esecuzione PVST+ o PVRST, è possibile utilizzare PVSTAG o PVRSTAG, ma l'implementazione è limitata a una topologia specifica:



In questa topologia, la restrizione più importante è che può esistere un solo switch CE. Non è possibile avere due switch come nella topologia MSTAG. In MSTAG, è possibile configurare un PW point-to-point in modo da trasportare il traffico non codificato (inclusi i TCN BPDU) da un PE all'altro quando il sito viene suddiviso in due parti. Con PVST e PVRST, i TCN vengono inviati con tag in modo che corrispondano alla stessa sottointerfaccia del traffico dati da trasportare su VPLS. Per inoltrare i TCN all'altro lato, il router deve identificare i BPDU in base all'indirizzo MAC e al tipo di protocollo. Poiché questa funzionalità non è attualmente supportata, è necessario disporre di un solo dispositivo CE.

Un altro requisito delle versioni precedenti al software Cisco IOS XR versione 4.3.0 è che le interfacce del bundle non possono essere utilizzate come ACL. Questa restrizione è stata eliminata nel software Cisco IOS XR versione 4.3.0.

Il principio è molto simile a quello del MSTAG. Il router PVSTAG invia pacchetti BPDU statici in modo che il CE sembri essere connesso agli switch direttamente alla radice (virtuale) con un costo di 0. Per bilanciare il carico del traffico, alcune VLAN possono essere configurate con la radice sul router3 e altre con la radice sul router4.

Questo è un esempio di configurazione sul router3:

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

RP/0/RSP1/CPU0:router3#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/0/0/1.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!

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

```
RP/0/RSP1/CPU0:router3#sh spanning-tree pvstag customer1-0-0-0-1
GigabitEthernet0/0/0/1
VLAN 2
Pre-empt delay is disabled
Sub-interface: GigabitEthernet0/0/0/1.2 (Up)
Max Age: 20
Root Priority: 0
Root Bridge: 0000.0000.0000
Cost: 0
Bridge Priority: 0
Bridge ID: 0000.0000.0001
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202821
Topology Changes: 0
VLAN 3
Pre-empt delay is disabled
Sub-interface: GigabitEthernet0/0/0/1.3 (Up)
Max Age: 20
Root Priority: 0
Root Bridge: 0000.0000.0000
Cost: 0
Bridge Priority: 1
Bridge ID: 0000.0000.0001
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202821
Topology Changes: 0
```

Questo è un esempio di configurazione sul router4:

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

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

```
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
!
!
!
!

RP/0/RSP1/CPU0:router4#sh run spanning-tree pvstag customer1-0-0-0-1
spanning-tree pvstag customer1-0-0-0-1
interface GigabitEthernet0/0/0/1
vlan 2
root-priority 0
root-id 0000.0000.0000
root-cost 0
priority 1
bridge-id 0000.0000.0002
!
vlan 3
root-priority 0
root-id 0000.0000.0000
root-cost 0
priority 0
bridge-id 0000.0000.0002
!
!
!

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

Questo è un esempio di configurazione dello switch 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
```

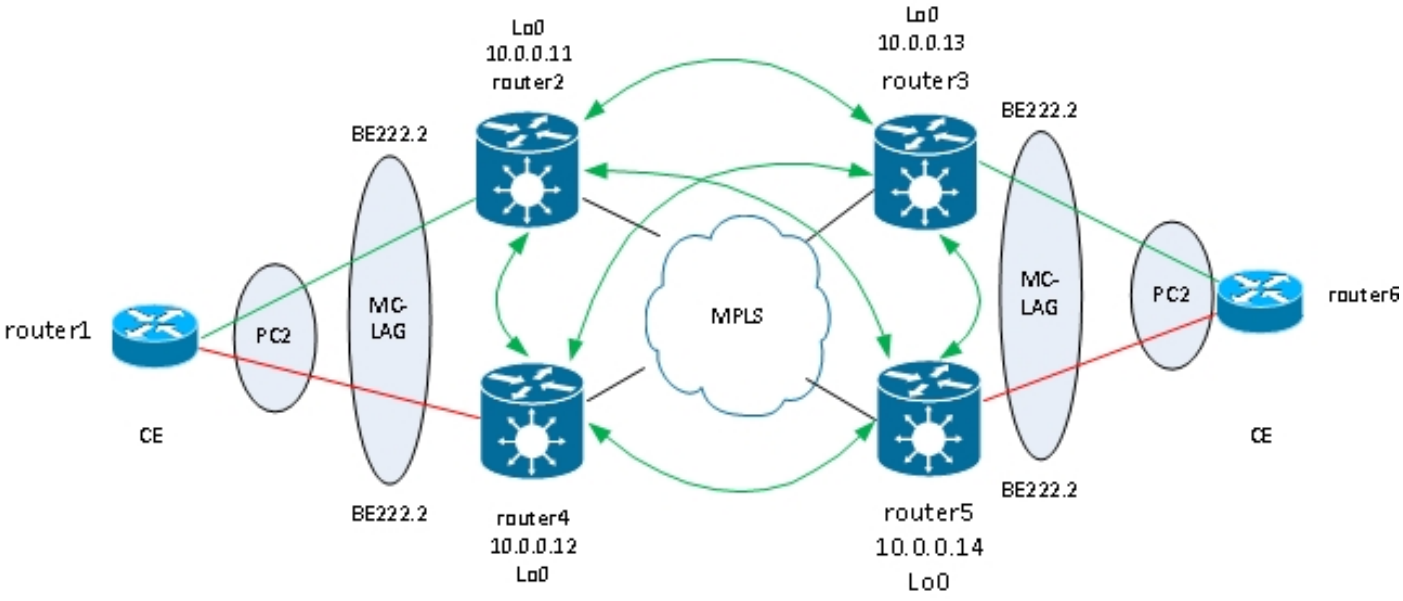
La configurazione di PVSTAG è molto simile a quella di MSTAG, ad eccezione del fatto che la priorità principale e la priorità del gateway primario sono configurate come 4096 e la priorità del gateway di backup è configurata come 8192 nell'esempio di MSTAG.

Tutti gli altri switch nei domini devono avere priorità più alte di quelle configurate in PVSTAG o PVRSTAG.

Èpossibile regolare il costo dell'interfaccia sugli switch CE in modo da influenzare la porta che diventa la porta principale e la porta che è bloccata.

4.4.7.4 LAG MC

La configurazione MC-LAG con VPLS è più semplice rispetto ai PW point-to-point con ridondanza PW bidirezionale. Anziché un PW primario e tre PW in standby, i PE richiedono solo una rete completa di PW VPLS, come standard con VPLS:



In questa topologia, tenere presente che:

- MC-LAG viene eseguito tra i due VPLS PE a sinistra: router2 e router4.
- In condizioni normali, i membri del bundle sono attivi tra il router1 e il router2 e in stato di standby tra il router1 e il router4.
- Il router2 ha le sottointerfacce del bundle configurate nei domini bridge VPLS, quindi il router2 inoltra il traffico ai VPLS PE remoti. Nel diagramma della topologia sono illustrati due siti, ma potrebbero essercene molti altri.
- I PE remoti apprendono gli indirizzi MAC dal router1 e i dispositivi dietro attraverso il router2, quindi i PE inoltrano il traffico per questi indirizzi MAC di destinazione attraverso il router2.
- Quando il collegamento tra router1 e router2 si interrompe o quando il router2 si interrompe, il membro del bundle tra router1 e router4 diventa attivo.
- Come il router 2, il router4 ha le sue sottointerfacce del bundle configurate nei domini bridge VPLS.
- Quando le sottointerfacce del bundle compaiono sul router4, il router4 invia messaggi di ritiro dell'indirizzo MAC LDP ai VPLS PE remoti per avvisarli che è presente una modifica della topologia.

Questa è la configurazione sul router3:

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

```
!
!
!

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

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

RP/0/RSP1/CPU0:router3#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface Bundle-Ether222.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface Bundle-Ether222.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
```

Una volta configurato il bundle MC-LAG, aggiungerlo alla configurazione VPLS come per qualsiasi altro alimentatore CA.

Questa è la configurazione corrispondente sul router 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
!
!
!
!
!
```

In circostanze normali, il membro del bundle tra il router3 e il router6 è attivo e il membro tra il router5 e il router6 è in stato di standby:

```
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#
```

Il traffico proveniente dal CE viene ricevuto sul router3 e inoltrato ai PE remoti:

```
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
```

L'ultimo comando mostra che il router3 sta imparando alcuni indirizzi MAC sul suo bundle e i membri attivi si trovano sul router3. Sul router5, non è presente alcun indirizzo MAC appreso sul bundle perché il membro locale è in stato standby:

```
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
```

Quando il membro del bundle tra router3 e router6 diventa inattivo, il membro del bundle diventa attivo sul router5. I PE VPLS MC-LAG inviano un messaggio di ritiro MAC LDP in modo che i PE

remoti rimuovano le proprie tabelle degli indirizzi MAC e apprendano l'indirizzo MAC tramite il nuovo router 5 attivo.

Il router2 riceve un messaggio di rifiuto MAC dal router3 e dal router5 quando il membro attivo del bundle MC-LAG si sposta dal router3 al router5:

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

Gli indirizzi MAC sul router2 vengono spostati dal router3 (10.0.0.13) al router5 (10.0.0.14):

```
RP/0/RSP0/CPU0:router2#sh l2vpn forwarding bridge-domain customer1:
engineering mac-address location 0/0/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

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

Con MC-LAG, un sito può utilizzare un singolo bundle da collegare agli altri siti tramite VPLS. MC-LAG fornisce il collegamento e la ridondanza PE, ma logicamente è ancora un'interfaccia di bundle per raggiungere altri siti. Lo Spanning Tree non è richiesto su quel bundle e un filtro BPDU potrebbe essere configurato sul CE per assicurare che i BPDU non vengano scambiati tra i siti su VPLS.

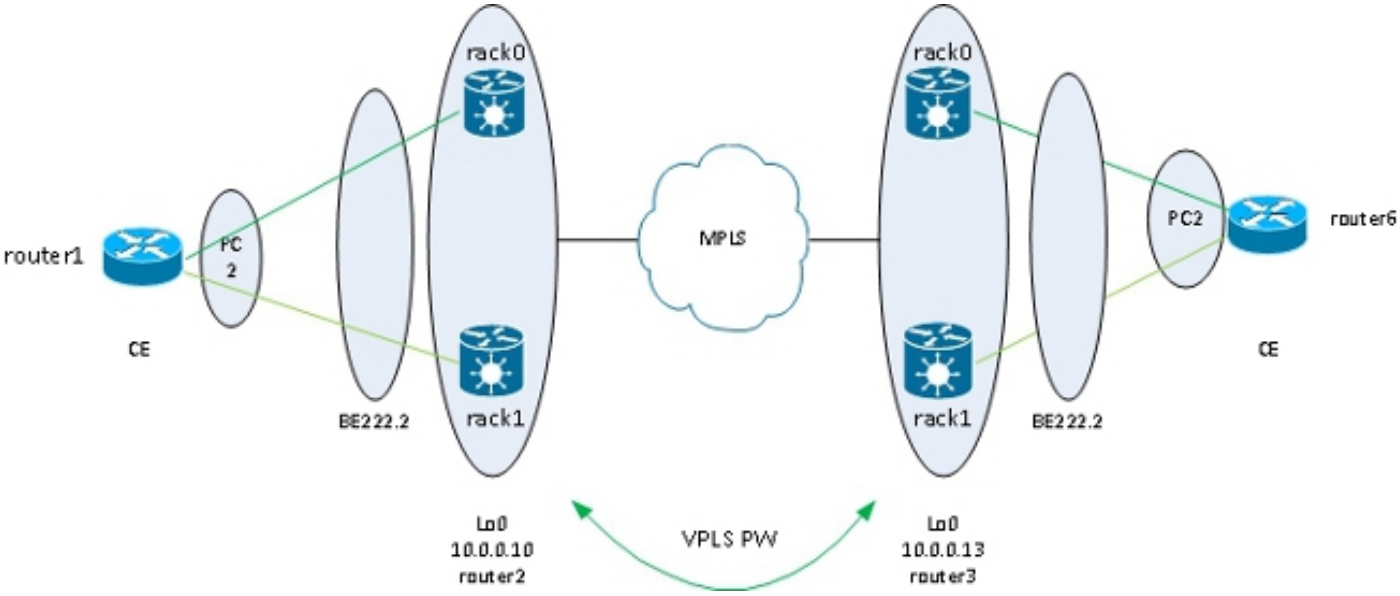
Un'altra opzione è la configurazione di un elenco degli accessi ai servizi Ethernet sugli ACL del bundle in modo da eliminare gli indirizzi MAC di destinazione dei BPDU in modo che i BPDU non vengano trasportati tra i siti. Tuttavia, se viene introdotto un collegamento backdoor tra i siti, lo

spanning tree non può interrompere il loop perché non è in esecuzione sul bundle MC-LAG. Valutare attentamente se disabilitare Spanning Tree sul pacchetto MC-LAG. Se la topologia tra i siti è accuratamente mantenuta, è preferibile avere ridondanza tramite MC-LAG senza la necessità di spanning tree.

4.4.7.5 ASR 9000 nV Edge Cluster

La soluzione MC-LAG fornisce ridondanza senza la necessità di utilizzare Spanning Tree. Uno svantaggio è che i membri del bundle di un MC-LAG PE sono in stato di standby, quindi si tratta di una soluzione in standby attivo che non massimizza l'utilizzo del collegamento.

Un'altra opzione di progettazione è l'uso di un cluster ASR 9000 nV Edge in modo che i CE possano avere membri bundle per ogni rack di cluster tutti attivi contemporaneamente:



Un altro vantaggio di questa soluzione è la riduzione del numero di PW, in quanto esiste un solo PW per cluster in ogni sito. Quando sono presenti due PE per sito, ciascun PE deve disporre di una PW per ciascuno dei due PE in ciascun sito.

La semplicità della configurazione è un altro vantaggio. La configurazione è simile a una configurazione VPLS di base con un bridge-domain con bundle AC e VFI PW:

```
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 ridondanza viene fornita dal sistema di alimentazione CA in dotazione a due rack, in modo che il bundle rimanga attivo in caso di guasto del componente o di guasto del rack.

Quando un sito è collegato al dominio VPLS solo tramite un cluster, la topologia è simile a MC-LAG per quanto riguarda lo Spanning Tree. Pertanto, lo Spanning Tree non è richiesto su quel bundle e un filtro BPDU potrebbe essere configurato sul CE in modo da garantire che i BPDU non vengano scambiati tra i siti su VPLS.

Un'altra opzione è la configurazione di un elenco degli accessi ai servizi Ethernet sugli ACL del bundle in modo da eliminare gli indirizzi MAC di destinazione dei BPDU in modo che i BPDU non vengano trasportati tra i siti. Tuttavia, se viene introdotto un collegamento backdoor tra i siti, lo spanning tree non può interrompere il loop perché non è in esecuzione sul bundle CE-PE. Quindi, valutare attentamente se disabilitare Spanning Tree su quel pacchetto CE-PE. Se la topologia tra i siti viene gestita con attenzione, è preferibile disporre di ridondanza attraverso il cluster senza la necessità di spanning tree.

4.4.7.6 Multi-homing (ICCP-SM) basato su ICCP (PMCLAG (Pseudo MCLAG) e attivo/attivo)

Nella versione 4.3.1 è stata introdotta una nuova funzionalità per superare la limitazione di MC-LAG, dove alcuni collegamenti del bundle sono inutilizzati in quanto rimangono in modalità standby. Nella nuova funzione, denominata *Pseudo MCLAG*, vengono utilizzati tutti i collegamenti dal DHD ai punti di attacco (PoA), ma le VLAN vengono suddivise tra i diversi pacchetti:

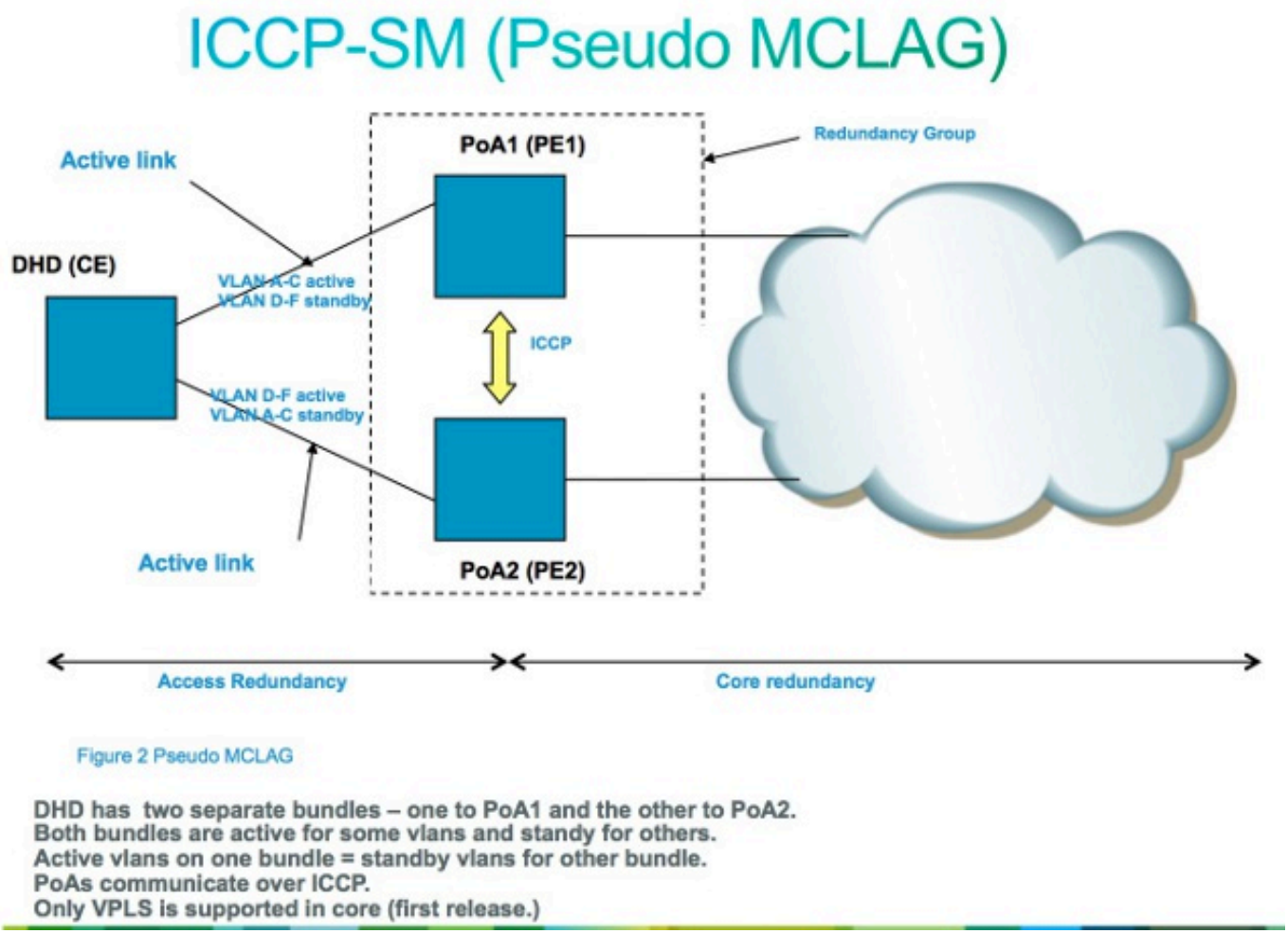


Figure 2 Pseudo MCLAG

4.5 Controllo delle tempeste di traffico

In un dominio di broadcast L2, esiste il rischio che un host possa comportarsi in modo errato e inviare un'elevata velocità di frame broadcast o multicast che devono essere trasmessi ovunque nel dominio bridge. Un altro rischio è la creazione di un loop L2 (che non viene interrotto dallo spanning tree), che si traduce in un loop di pacchetti broadcast e multicast. Un elevato tasso di pacchetti broadcast e multicast influisce sulle prestazioni degli host nei domini di broadcast.

Le prestazioni dei dispositivi di commutazione nella rete possono essere influenzate anche dalla replica di un frame di input (broadcast, multicast o un frame unicast sconosciuto) su più porte di uscita nel dominio bridge. La creazione di più copie dello stesso pacchetto può richiedere molte risorse, a seconda della posizione all'interno del dispositivo in cui il pacchetto deve essere replicato. Ad esempio, replicare una trasmissione su più slot diversi non è un problema a causa delle funzionalità di replica multicast della struttura. Le prestazioni di un processore di rete potrebbero risentirne quando è necessario creare più copie dello stesso pacchetto da inviare su alcune porte gestite dal processore di rete.

Per proteggere i dispositivi in caso di uragani, la funzione di controllo della tempesta di traffico consente di configurare una velocità massima di trasmissioni, multicast e unicast sconosciuti da accettare su un adattatore CA di dominio-ponte. Per ulteriori informazioni, vedere Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide, release 4.3.x: Implementing Traffic Storm Control under a VPLS Bridge.

Il controllo dell'urto del traffico non è supportato sulle interfacce CA del bundle o sui PW VFI, ma è

supportato sugli ACL non del bundle e sui PW di accesso. La funzione è disattivata per impostazione predefinita; se non si imposta il controllo temporale, è possibile accettare qualsiasi frequenza di trasmissioni, multicast e unicast sconosciuti.

Di seguito è riportato un esempio di configurazione:

```
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>
```

I contatori di rilascio del controllo della temporizzazione sono sempre presenti nell'output del comando **show l2vpn bridge-domain detail**. Poiché la funzionalità è disattivata per impostazione predefinita, i contatori iniziano a segnalare la perdita di dati solo quando la funzionalità è stata configurata.

Le velocità configurate possono variare a seconda del modello di traffico tra le reti. Prima di configurare una velocità, Cisco consiglia di comprendere la velocità dei frame broadcast, multicast o unicast sconosciuti in circostanze normali. Aggiungere quindi un margine nella velocità configurata superiore alla velocità normale.

4.6 Mosse MAC

In caso di instabilità di rete come in un flap di interfaccia, è possibile imparare un indirizzo MAC da una nuova interfaccia. Si tratta di una normale convergenza di rete e la tabella degli indirizzi MAC viene aggiornata dinamicamente.

Tuttavia, gli spostamenti MAC costanti spesso indicano l'instabilità della rete, come una grave instabilità durante un loop L2. La funzione di sicurezza dell'indirizzo MAC consente di segnalare gli spostamenti MAC e di intraprendere azioni correttive, ad esempio la chiusura di una porta che causa problemi.

Anche se non è configurata un'azione correttiva, è possibile configurare il comando **logging** in modo da essere avvisati dell'instabilità della rete tramite i messaggi di spostamento MAC:

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

Nell'esempio, l'azione è configurata su none (nessuno), quindi non viene eseguita alcuna operazione quando viene rilevato uno spostamento MAC, tranne che quando viene registrato un messaggio syslog. Questo è un messaggio di esempio:

```
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 Snooping IGMP e MLD

Per impostazione predefinita, i frame multicast vengono trasmessi a tutte le porte di un dominio bridge. Quando si utilizzano flussi ad alta velocità come i servizi di televisione IP (IPTV), potrebbe essere presente una quantità significativa di traffico inoltrato su tutte le porte e replicato su più PW. Se tutti i flussi TV vengono inoltrati su un'interfaccia, è possibile che vengano congestionate le porte. L'unica opzione è la configurazione di una funzione come lo snooping IGMP o MLD, che intercetta i pacchetti di controllo multicast per tenere traccia dei ricevitori, dei router multicast e dei flussi di inoltro sulle porte solo quando appropriato.

Per ulteriori informazioni su queste funzionalità, consultare la guida alla configurazione del multicast del router Cisco ASR serie 9000 Aggregation Services, versione 4.3.x.

5. Argomenti aggiuntivi L2VPN

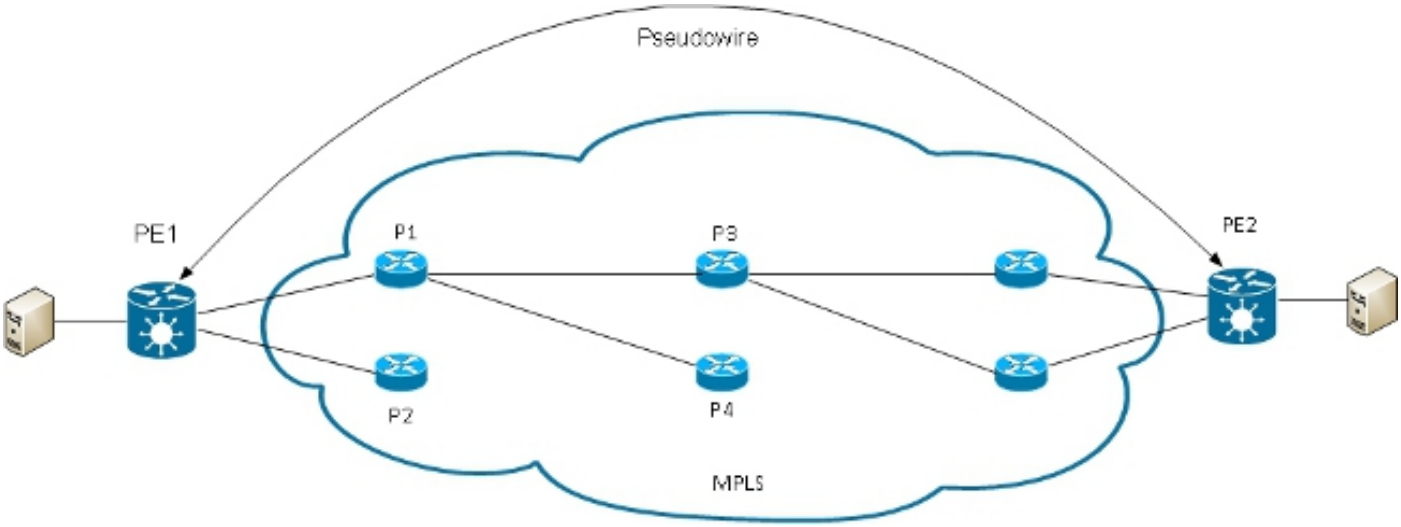
> **Note:**
>
> per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).
>
> Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

5.1 Bilanciamento del carico

Quando un PE L2VPN deve inviare un frame su un PW MPLS, il frame Ethernet viene incapsulato in un frame MPLS con una o più etichette MPLS. Per raggiungere il PE remoto, sono presenti

almeno un'etichetta PW e forse un'etichetta IGP.

Il frame MPLS viene trasportato dalla rete MPLS al PE L2VPN remoto. In genere esistono più percorsi per raggiungere il file PE di destinazione:



Nota: in questo diagramma non sono rappresentati tutti i collegamenti.

PE1 può scegliere tra P1 e P2 come primo router MPLS P verso PE2. Se si seleziona P1, PE1 sceglierà tra P3 e P4 e così via. I percorsi disponibili sono basati sulla topologia IGP e sul percorso del tunnel MPLS TE.

I provider di servizi MPLS preferiscono utilizzare tutti i collegamenti in modo uguale anziché un collegamento congestionato con altri collegamenti sottoutilizzati. Questo obiettivo non è sempre facile da raggiungere perché alcuni PW trasportano molto più traffico di altri e perché il percorso seguito da un traffico PW dipende dall'algoritmo di hashing usato nel core. È possibile che più PW con larghezza di banda elevata vengano hashati sugli stessi collegamenti, con conseguente congestione.

Un requisito molto importante è che tutti i pacchetti da un flusso devono seguire lo stesso percorso. In caso contrario, si verificheranno frame non ordinati che potrebbero influire sulla qualità o sulle prestazioni delle applicazioni.

Il bilanciamento del carico in una rete MPLS sui router Cisco si basa in genere sui dati che seguono l'etichetta MPLS inferiore.

- Se i dati immediatamente successivi all'etichetta inferiore iniziano con 0x4 o 0x6, un router MPLS IP presume che il pacchetto MPLS contenga un pacchetto IPv4 o IPv6 e tenta di eseguire il bilanciamento del carico in base a un hash degli indirizzi IPv4 o IPv6 di origine e destinazione estratti dal frame. In teoria, ciò non dovrebbe applicarsi a un frame Ethernet incapsulato e trasportato su un PW perché l'indirizzo MAC di destinazione segue l'etichetta in basso. Di recente sono stati assegnati alcuni intervalli di indirizzi MAC che iniziano con 0x4 e 0x6. Il router MPLS IP potrebbe erroneamente considerare che l'intestazione Ethernet sia in realtà un'intestazione IPv4 e incapsulare il frame in base a ciò che presuppone siano gli indirizzi di origine e di destinazione IPv4. I frame Ethernet da un PW possono essere sottoposti a hashing su percorsi diversi nel core MPLS, il che porta a frame fuori sequenza nel PW e a problemi di qualità delle applicazioni. La soluzione consiste nella configurazione di

una parola di controllo in una classe pw che può essere collegata a un punto-punto o a un PW VPLS. La parola del controllo viene inserita immediatamente dopo le etichette MPLS. La parola di controllo non inizia con 0x4 o 0x6 quindi il problema viene evitato.

```
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)
------------ ------------------------------ ------------------
```

- Se i dati immediatamente successivi alla parte inferiore dello stack di etichette MPLS non iniziano con 0x4 o 0x6, il router P esegue il bilanciamento del carico in base all'etichetta inferiore. Tutto il traffico proveniente da un PW segue lo stesso percorso, quindi non si verificano pacchetti non in ordine, ma ciò potrebbe portare a congestione su alcuni collegamenti in caso di PW con larghezza di banda elevata. Con il software Cisco IOS XR versione 4.2.1, ASR 9000 supporta la funzione PW Flow Aware Transport (FAT). Questa funzionalità viene eseguita sui PE L2VPN, dove viene negoziata tra le due estremità di un PW point-to-point o VPLS. L2VPN PE in entrata rileva i flussi sulla CA e sulla configurazione L2VPN e inserisce una nuova etichetta di flusso MPLS sotto l'etichetta MPLS PW nella parte

inferiore dello stack di etichette MPLS. Il PE in entrata rileva i flussi in base agli indirizzi MAC di origine e di destinazione (impostazione predefinita) o agli indirizzi IPv4 di origine e di destinazione (configurabile). L'impostazione predefinita prevede l'utilizzo degli indirizzi MAC. È consigliabile utilizzare indirizzi IPv4, ma questi devono essere configurati manualmente.

Con la funzione FAT PW, l'interfaccia L2VPN PE in entrata inserisce un'etichetta MPLS inferiore per src-dst-mac o per src-dst-ip. I router MPLS IP (tra i PE) eseguono l'hash dei frame sui percorsi disponibili, quindi raggiungono il PE di destinazione in base all'etichetta di flusso PW FAT nella parte inferiore dello stack MPLS. In genere, questo consente un migliore utilizzo della larghezza di banda nel core, a meno che un PW non supporti solo un numero ridotto di conversazioni src-dst-mac o src-dst-ip. Cisco consiglia di utilizzare una parola di controllo in modo da evitare di avere indirizzi MAC che iniziano con 0x4 e 0x6 subito dopo l'etichetta di flusso. Ciò assicura che l'hash sia correttamente basato sugli pseudo indirizzi IP e non sull'etichetta di flusso.

Con questa funzione, il traffico proveniente da una PW viene bilanciato su più percorsi nel core, quando disponibile. Il traffico delle applicazioni non risente di pacchetti non ordinati perché tutto il traffico proveniente dalla stessa origine (MAC o IP) e diretto alla stessa destinazione (MAC o IP) segue lo stesso percorso.

Di seguito viene riportata una configurazione di esempio:

```
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 Registrazione

In modalità di configurazione L2VPN è possibile configurare diversi tipi di messaggi di registrazione. Configurare la registrazione l2vpn in modo da ricevere gli avvisi syslog per gli eventi L2VPN e configurare lo pseudonimo di registrazione in modo da determinare quando cambia lo stato di un PW:

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

Se sono configurati molti PW, è possibile che il log venga inondato dai messaggi.

5.3 ethernet-services access-list

Èpossibile usare un elenco degli accessi ai servizi ethernet per eliminare il traffico da determinati host o verificare se un router riceve pacchetti da un host su un'interfaccia 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)
```

Le corrispondenze hardware possono essere visualizzate solo con la parola chiave *hardware*. Utilizzare la parola chiave *in entrata* o *in uscita* a seconda della direzione del gruppo di accesso. Viene inoltre specificata la posizione della scheda di linea dell'interfaccia a cui si applica l'elenco

degli accessi.

èpossibile anche applicare un elenco degli accessi ipv4 all'interfaccia l2transport come funzionalità di sicurezza o risoluzione dei problemi:

```
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 filtro di uscita ethernet

Nella direzione di uscita di un'appliance ASA, si supponga che non vi sia alcun comando **riscrittura tag in entrata pop <>simmetrico** che determina i tag VLAN in uscita. In questo caso, non viene eseguito alcun controllo per verificare che il frame in uscita abbia i tag VLAN corretti in base al comando **encapsulation**.

Di seguito viene riportata una configurazione di esempio:

```
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
!
!
!
!
```

In questa configurazione, tenere presente che:

- Una trasmissione ricevuta con un tag 2 dot1q su Gigabit Ethernet0/1/0/39.2 conserva il tag in

ingresso perché non è presente alcun comando **rewrite ingress**.

- La trasmissione viene propagata da Gigabit Ethernet0/1/0/3.2 con il tag 2 dot1q, ma ciò non causa problemi in quanto Gigabit Ethernet0/1/0/3.2 è configurato anche con il tag 2 dot1q.
- La trasmissione viene inoltre trasmessa da Gigabit Ethernet0/1/0/3.3, che conserva il tag 2 originale perché non è disponibile il comando **rewrite** su Gigabit Ethernet0/1/0/3.3. Il comando **encapsulation dot1q 3** su Gigabit Ethernet0/1/0/3.3 non viene controllato nella direzione di uscita.
- Il risultato è che, per una trasmissione ricevuta con tag 2 su Gigabit Ethernet0/1/0/39, ci sono due trasmissioni con tag 2 che escono da Gigabit Ethernet0/1/0/3. Il traffico duplicato potrebbe causare problemi all'applicazione.
- La soluzione è la configurazione del *filtro di uscita Ethernet strict* per garantire che i pacchetti lascino la sottointerfaccia con i tag VLAN corretti. In caso contrario, i pacchetti non vengono inoltrati e vengono scartati.

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

Informazioni su questa traduzione

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