

Configurazione e verifica dell'opzione VPN MPLS INTER-AS di layer 3 con IOS e IOS-XR

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Ping da CE1 a CE2 e viceversa](#)

[Spiegazione degli aggiornamenti scambiati e delle etichette MPLS](#)

[Verifica tramite Traceroute](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritta la configurazione e la verifica della funzione vpn mpls, opzione B, del layer 3 di Inter-As. Le piattaforme IOS e IOS-XR vengono utilizzate per la spiegazione e la verifica. Illustra uno scenario di rete di esempio con la relativa configurazione e i relativi output per una migliore comprensione.

Prerequisiti

Requisiti

Non sono previsti requisiti di questo tipo, tuttavia la conoscenza di base di MPLS (Multi Protocol Label Switching) e la conoscenza operativa della piattaforma IOS-XR sono certamente utili.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware. Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

MPLS è ampiamente implementato sui provider di servizi Internet (ISP) in tutto il mondo. Uno di

questi servizi è MPLS layer 3 VPN (Virtual Private Network). Le VPN MPLS di layer 3 estendono principalmente i confini di routing di un cliente da una posizione geografica a un'altra. L'ISP è utilizzato principalmente come transito. Viene eseguito il peer con l'ISP in una posizione geografica e nell'altra, quindi i percorsi specifici del cliente vengono ricevuti sul dispositivo CE (Customer Edge) dal dispositivo PE (Provider Edge/ISP).

Ora, se il requisito è estendere i confini di routing per un cliente, per due diverse posizioni geografiche in cui sono presenti due diversi ISP. Quindi i due ISP devono coordinarsi in modo che la VPN MPLS layer 3 venga fornita al cliente finale. Questa soluzione è chiamata VPN MPLS Inter-As Layer 3.

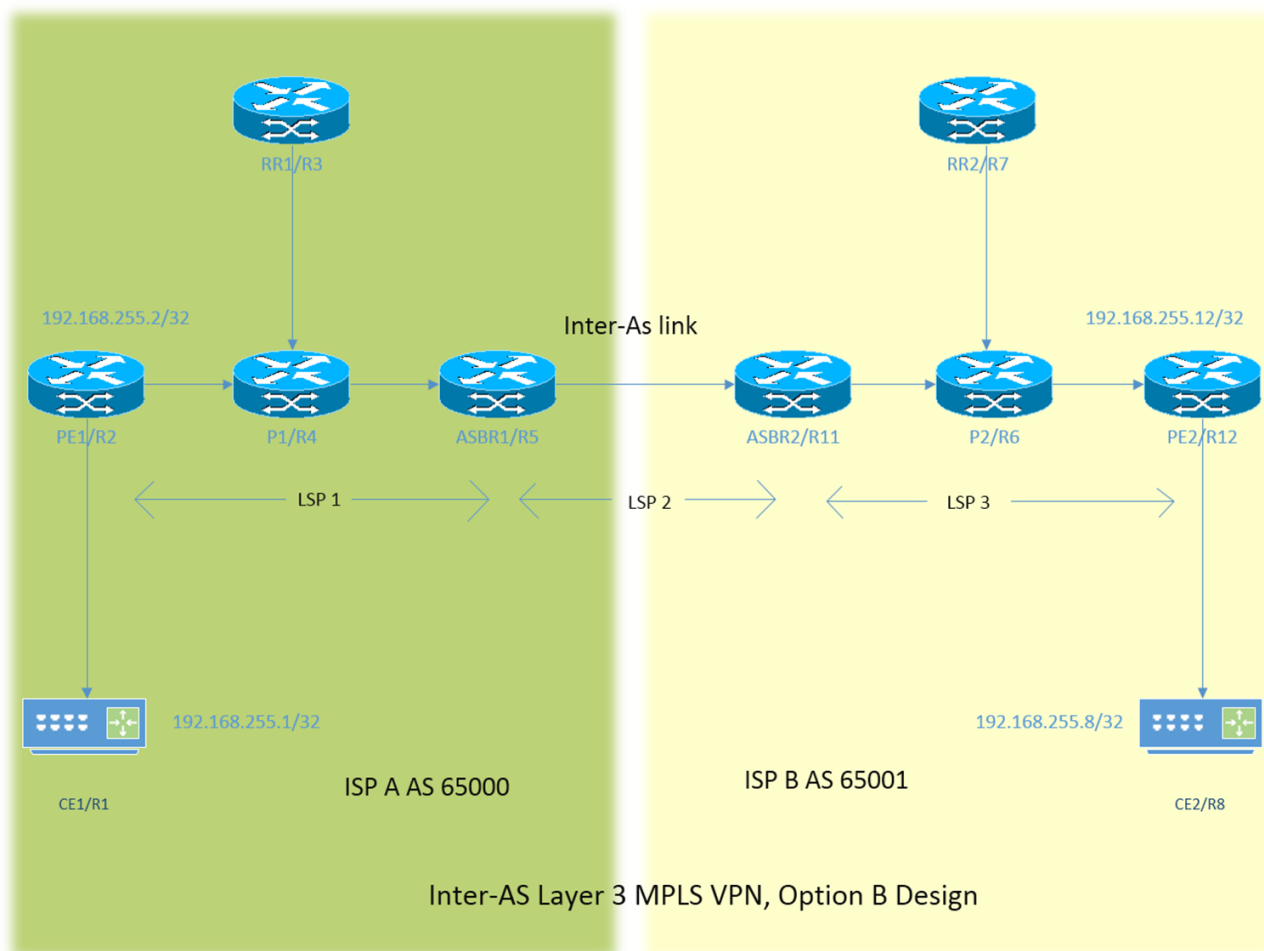
Le VPN MPLS di livello 3 inter-As possono essere distribuite in 4 modi diversi, denominati opzione A, opzione B, opzione C e opzione D.

In questo documento viene illustrata l'implementazione tramite l'opzione B.

Configurazione

Esempio di rete

Di seguito è riportata la topologia per lo scambio dell'opzione B tra appliance ASA.



Lo schema di indirizzamento è molto semplice. Ogni router ha un'interfaccia loopback1 descritta come 192.168.255.X dove X=1 quando il router 1 è in dubbio. L'indirizzo di interfaccia è del tipo

192.168.XY.X . Si supponga che R1 e R2 siano in fase di analisi e che la configurazione dell'interfaccia sul router R1 sia 192.168.12.1 (qui X =1 , Y = 2).

CE - Customer Edge

PE - Provider Edge

RR - Reflector route

ASBR - Autonomous System Boundary Router

In tutto il documento, il termine CE indica entrambi i dispositivi Customer Edge; se è necessario fare un riferimento specifico per un particolare dispositivo, verrà indicato come CE1. Questo vale anche per PE, RR e ASBR.

Tutti i dispositivi eseguono IOS, tuttavia ASBR2/R11 e PE2/R12 eseguono IOS-XR.

A due ISP viene fatto riferimento con AS (Autonomous System) 6500 e AS 65001. L'ISP con AS 65000 si trova sul lato sinistro della topologia e viene indicato come ISP A e l'ISP con AS 65001 si trova sul lato destro della topologia e viene indicato come ISP B.

Configurazioni

Le configurazioni dei dispositivi sono descritte di seguito.

CE1

```
interface Loopback1
ip address 192.168.255.1 255.255.255.255
!
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
!
router eigrp 1
network 0.0.0.0
```

PE1

```
vrf definition A
rd 192.168.255.2:65000
!
address-family ipv4
route-target export 99:99
route-target import 99:99
exit-address-family
!
interface Loopback1
ip address 192.168.255.2 255.255.255.255
ip ospf 1 area 0
!
interface FastEthernet0/0
vrf forwarding A
ip address 192.168.12.2 255.255.255.0
!
interface FastEthernet1/0
ip address 192.168.24.2 255.255.255.0
```

```
ip ospf 1 area 0
mpls ip
!
router eigrp 65000
!
address-family ipv4 vrf A autonomous-system 1
redistribute bgp 65000 metric 1500 10 255 1 1500
network 192.168.12.2 0.0.0.0
exit-address-family
!
router ospf 1
!
router bgp 65000
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 192.168.255.3 remote-as 65000
neighbor 192.168.255.3 update-source Loopback1
!
address-family ipv4
exit-address-family
!
address-family vpnv4
neighbor 192.168.255.3 activate
neighbor 192.168.255.3 send-community both
exit-address-family
!
address-family ipv4 vrf A
redistribute eigrp 1
exit-address-family
!
```

P1

```
interface Loopback1
ip address 192.168.255.4 255.255.255.255
ip ospf 1 area 0
!
interface FastEthernet0/0
ip address 192.168.24.4 255.255.255.0
ip ospf 1 area 0
duplex half
mpls ip
!
interface FastEthernet1/0
ip address 192.168.34.4 255.255.255.0
ip ospf 1 area 0
mpls ip
!
interface FastEthernet1/1
ip address 192.168.45.4 255.255.255.0
ip ospf 1 area 0
mpls ip
!
router ospf 1
!
```

R1

```
interface Loopback1
ip address 192.168.255.3 255.255.255.255
ip ospf 1 area 0
!
```

```

interface FastEthernet0/0
ip address 192.168.34.3 255.255.255.0
ip ospf 1 area 0
mpls ip
!
router ospf 1
!
router bgp 65000
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 192.168.255.2 remote-as 65000
neighbor 192.168.255.2 update-source Loopback1
neighbor 192.168.255.5 remote-as 65000
neighbor 192.168.255.5 update-source Loopback1
!
address-family ipv4
exit-address-family
!
address-family vpnv4
neighbor 192.168.255.2 activate
neighbor 192.168.255.2 send-community both
neighbor 192.168.255.2 route-reflector-client
neighbor 192.168.255.5 activate
neighbor 192.168.255.5 send-community both
neighbor 192.168.255.5 route-reflector-client
exit-address-family
!

```

ASBR1

```

interface Loopback1
ip address 192.168.255.5 255.255.255.255
ip ospf 1 area 0
!
interface FastEthernet0/0
ip address 192.168.45.5 255.255.255.0
ip ospf 1 area 0
mpls ip
!
interface FastEthernet1/0
ip address 192.168.115.5 255.255.255.0
mpls bgp forwarding
!
router ospf 1
!
router bgp 65000
bgp log-neighbor-changes
no bgp default ipv4-unicast
no bgp default route-target filter
neighbor 192.168.115.11 remote-as 65001
neighbor 192.168.255.3 remote-as 65000
neighbor 192.168.255.3 update-source Loopback1
!
address-family ipv4
exit-address-family
!
address-family vpnv4
neighbor 192.168.115.11 activate
neighbor 192.168.115.11 send-community both
neighbor 192.168.255.3 activate
neighbor 192.168.255.3 send-community both
neighbor 192.168.255.3 next-hop-self
exit-address-family

```

!
ASBR2

```
interface Loopback1
ipv4 address 192.168.255.11 255.255.255.255
!
interface GigabitEthernet0/0/0/0
ipv4 address 192.168.115.11 255.255.255.0
!
interface GigabitEthernet0/0/0/1
ipv4 address 192.168.116.11 255.255.255.0
!
route-policy DEFAULT
pass
end-policy
!
router static
address-family ipv4 unicast
192.168.115.5/32 GigabitEthernet0/0/0/0
!
router ospf 1
area 0
interface Loopback1
!
interface GigabitEthernet0/0/0/1
!
router bgp 65001
address-family vpnv4 unicast
retain route-target all
!
neighbor 192.168.115.5
remote-as 65000
address-family vpnv4 unicast
route-policy DEFAULT in
route-policy DEFAULT out
!
neighbor 192.168.255.7
remote-as 65001
update-source Loopback1
address-family vpnv4 unicast
next-hop-self
!
mpls ldp
address-family ipv4
!
interface GigabitEthernet0/0/0/1
!
```

P2

```
interface Loopback1
ip address 192.168.255.6 255.255.255.255
ip ospf 1 area 0
!
interface FastEthernet0/0
ip address 192.168.116.6 255.255.255.0
ip ospf 1 area 0
mpls ip
!
```

```
interface FastEthernet1/0
ip address 192.168.67.6 255.255.255.0
ip ospf 1 area 0
mpls ip
!
interface FastEthernet1/1
ip address 192.168.126.6 255.255.255.0
ip ospf 1 area 0
mpls ip
!
router ospf 1
!
```

R2

```
interface Loopback1
ip address 192.168.255.7 255.255.255.255
ip ospf 1 area 0
!
interface FastEthernet0/0
ip address 192.168.67.7 255.255.255.0
ip ospf 1 area 0
mpls ip
!
router ospf 1
!
router bgp 65001
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 192.168.255.11 remote-as 65001
neighbor 192.168.255.11 update-source Loopback1
neighbor 192.168.255.12 remote-as 65001
neighbor 192.168.255.12 update-source Loopback1
!
address-family ipv4
exit-address-family
!
address-family vpnv4
neighbor 192.168.255.11 activate
neighbor 192.168.255.11 send-community both
neighbor 192.168.255.11 route-reflector-client
neighbor 192.168.255.12 activate
neighbor 192.168.255.12 send-community both
neighbor 192.168.255.12 route-reflector-client
exit-address-family
!
```

PE2

```
vrf A
address-family ipv4 unicast
import route-target
99:99
!
export route-target
99:99
!
interface Loopback1
ipv4 address 192.168.255.12 255.255.255.255
!
interface GigabitEthernet0/0/0/0
ipv4 address 192.168.126.12 255.255.255.0
```

```

!
interface GigabitEthernet0/0/0/1
vrf A
ipv4 address 192.168.128.12 255.255.255.0
!
router ospf 1
address-family ipv4
area 0
interface Loopback1
!
interface GigabitEthernet0/0/0/0
!
router bgp 65001
address-family vpnv4 unicast
!
neighbor 192.168.255.7
remote-as 65001
update-source Loopback1
address-family vpnv4 unicast
!
vrf A
rd 192.168.255.12:65001
address-family ipv4 unicast
redistribute eigrp 1
!
mpls ldp
address-family ipv4
!
interface GigabitEthernet0/0/0/0
!
router eigrp 65001
vrf A
address-family ipv4
autonomous-system 1
redistribute bgp 65001
interface GigabitEthernet0/0/0/1
!

```

CE2

```

interface Loopback1
ip address 192.168.255.8 255.255.255.255
!
interface FastEthernet1/0
ip address 192.168.128.8 255.255.255.0
!
router eigrp 1
network 0.0.0.0
!

```

Spiegazione

- Distribuzione di EIGRP come protocollo di routing PE-CE in corso.
- OSPF viene utilizzato come IGP per il core ISP. Su entrambi gli ISP su tutti i collegamenti fisici viene implementato LDP + IGP. LDP + IGP non è configurato sul collegamento Inter-As tra ASBR1 e ASBR2.
- La redistribuzione dell'EIGRP in base alla vrf A in BGP e viceversa viene eseguita su PE.
- Solo la famiglia di indirizzi VPNv4 in PE viene attivata con il riflettore di route. Il comando "no bgp default ipv4-unicast" disabilita il peering della famiglia di indirizzi ipv4 predefinita in IOS.

Per IOS-XR questo comando non è richiesto in quanto forma solo il peering, in relazione alla famiglia di indirizzi in cui è configurato il router adiacente.

- Queste route ridistribuite vengono pubblicizzate come route VPNv4 al reflector di route (RR).
- Il riflettore di route riflette queste route verso il dispositivo ASBR. Poiché è necessario riflettere le route vpn4, viene attivata solo la famiglia di indirizzi vpnv4. Il riflettore della route non si troverà nel percorso di transito.
- Il dispositivo P sta semplicemente cambiando le etichette e sta per passare il traffico.
- Sul dispositivo ASBR sono stati configurati "no bgp default route-target filter" per IOS e "keep route-target all" per IOS-XR. Questo è importante perché i dispositivi ABBR non sono reflector di routing e non hanno alcun vrf con RT (route target) configurato, quindi elimineranno implicitamente l'aggiornamento di routing inviato loro dai reflector di route. Si tratta di un comportamento previsto, in quanto IOS e IOS-XR tendono a ottimizzare le informazioni della tabella di routing e a eliminare gli aggiornamenti per le VFR con RT non configurate localmente.
- Sugli ASBR il peering VPNv4 eBGP è configurato. MPLS non è abilitato con ldp sul collegamento che connette gli ASBR.
- Quando il peering eBGP VPNv4 si attiva sull'ASBR1 (IOS) con il dispositivo IOS-XR, sul collegamento Inter-As viene configurato automaticamente il "mpls bgp forwarding". Lo scambio delle etichette con ASBR2 non avviene tramite ldp ma tramite BGP. IOS aggiunge inoltre automaticamente la route /32 statica all'interfaccia ASBR2 in modo che l'etichetta mpls sia associata a una route /32 e che la commutazione dell'etichetta sia eseguita correttamente.
- Per IOS-XR su Inter-As link esiste una logica diversa rispetto a quella di IOS. È necessario configurare una route /32 statica all'interfaccia ASBR1, in modo che l'etichetta mpls sia associata al prefisso /32. In caso contrario, il control plane salirà ma il traffico non verrà inoltrato.
- IOS-XR non invia o riceve aggiornamenti del routing con peer EBGP a meno che non sia configurata una policy di route. Un criterio di route è configurato con il nome DEFAULT. L'azione consiste nel "passare", ovvero inviare/ricevere tutti gli aggiornamenti.

Verifica

Ping da CE1 a CE2 e viceversa

L'output del ping tra CE1 e CE2 utilizzando l'interfaccia loopback1 come origine è mostrato di seguito.

```
R1#ping 192.168.255.8 source lo1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.255.8, timeout is 2 seconds:
Packet sent with a source address of 192.168.255.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 104/300/420 ms
```

L'output del ping tra CE2 e CE1 utilizzando l'interfaccia loopback1 come origine è mostrato di seguito.

```
R8#ping 192.168.255.1 source lo1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.255.1, timeout is 2 seconds:
```

Packet sent with a source address of 192.168.255.8

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 168/303/664 ms

Spiegazione degli aggiornamenti scambiati e delle etichette MPLS

- In CE1 show ip route fornisce il percorso per loopback1 di CE2 sull'altra estremità.

```
R1#show ip route 192.168.255.8
Routing entry for 192.168.255.8/32
Known via "eigrp 1", distance 90, metric 156416, type internal
```

- In questa sezione viene descritto il flusso del traffico con etichette mpls applicate/eliminate lungo il percorso da CE1 a CE2, ovvero come si ottiene la raggiungibilità passando dal loopback di origine 1 di CE1 al loopback 1 di CE2. Vengono inoltre illustrate informazioni simili relative al percorso di ritorno, ad esempio da CE2 loopback1 a CE1 loopback1.
- Nelle progettazioni VPN di layer 3 MPLS, tenere presente che durante l'operazione di cambio di etichetta l'etichetta di trasporto viene scambiata e l'etichetta VPN non viene modificata. L'etichetta VPN viene esposta quando si verifica il php (Penultimate Hop Popping) e il traffico raggiunge PE o quando un LSP (Label Switch Path) viene terminato.
- In PE1, il loopback1 di CE2 viene appreso tramite BGP VPNv4 e ridistribuito in un EIGRP con riconoscimento vrf. Il loopback1 appreso tramite CE1 tramite EIGRP viene ridistribuito in BGP e diventa anche una route VPNv4.

```
R2#show bgp vpnv4 unicast all labels
Network          Next Hop          In label/Out label
Route Distinguisher: 192.168.255.2:65000 (A)
192.168.12.0     0.0.0.0           22/nolabel(A)
192.168.128.0    192.168.255.5     nolabel/26
192.168.255.1/32 192.168.12.1      23/nolabel
192.168.255.8/32 192.168.255.5     nolabel/27
```

- Dall'output di cui sopra si può capire che, per raggiungere il prefisso 192.168.255.8/32 un'etichetta vpn di 27 appreso. Questo output indica anche che l'etichetta 23 è un'etichetta vpn allocata dal BGP per pubblicizzare la raggiungibilità su 192.168.255.1/32. L'hop successivo per il prefisso VPNv4 decide l'etichetta di trasporto e il percorso del commutatore di etichetta. Quindi, "show mpls forwarding-table" per l'hop successivo 192.168.255.5 fornisce le informazioni sull'etichetta del trasporto per raggiungere 192.168.255.8/32.

```
R2#show mpls forwarding-table 192.168.255.5 255.255.255.255
Local  Outgoing  Prefix          Bytes Label  Outgoing  Next Hop
Label  Label     or Tunnel Id    Switched     interface
21     21        192.168.255.5/32  0            Fa1/0      192.168.24.4
```

- L'etichetta in uscita è 21 e si può quindi concludere che per raggiungere 192.168.255.8/32, PE1 utilizzerà un'etichetta di trasporto di 21 e un'etichetta vpn di 27.

```
R2#show mpls forwarding-table
Local  Outgoing  Prefix          Bytes Label  Outgoing  Next Hop
Label  Label     or Tunnel Id    Switched     interface
23     No Label  192.168.255.1/32[V] \
```

- Si può anche concludere che il traffico di ritorno in arrivo a 192.168.255.1/32 sarà già in possesso di PHP da parte del router P1 e quindi colpirà PE1 con etichetta vpn di 23 e la tabella di inoltro mpls invierà quel traffico a Fa0/0, cioè il CE1 dopo aver estratto l'etichetta vpn .
- L'output sul riflettore di percorso conferma le informazioni discusse finora.

```
R3#show bgp vpnv4 unicast all labels
Network          Next Hop          In label/Out label
Route Distinguisher: 192.168.255.2:65000
192.168.12.0     192.168.255.2    nolabel/22
192.168.255.1/32 192.168.255.2    nolabel/23
Route Distinguisher: 192.168.255.12:65001
192.168.128.0   192.168.255.5    nolabel/26
192.168.255.8/32 192.168.255.5    nolabel/27
```

- La parte veramente interessante è l'ASBR1, dove l'etichetta per raggiungere 192.168.255.1/32 viene inviata ad ASBR2 e ASBR2 annuncia le informazioni dell'etichetta per raggiungere 192.168.255.8/32. Come descritto in precedenza, l'hop successivo nell'aggiornamento bgp vpnv4 decide l'etichetta di trasporto, tenendo presente che l'hop successivo 192.168.255.5 (per il prefisso 192.168.255.8/32 appreso su PE1) appartiene al loopback1 di ASBR1. Così come per il processo di PHP (Penultimate hop popping) l'etichetta di trasporto sarà già stata rimossa P1 quando il traffico destinato a 192.168.255.8 raggiunge ASBR1. Quindi il traffico che raggiunge ASBR1 avrà un'etichetta vpn di 27. L'output su ASBR1 è mostrato di seguito.

```
R5#show bgp vpnv4 unicast all labels
Network          Next Hop          In label/Out label
Route Distinguisher: 192.168.255.2:65000
192.168.12.0     192.168.255.2    24/22
192.168.255.1/32 192.168.255.2    25/23
Route Distinguisher: 192.168.255.12:65001
192.168.128.0   192.168.115.11   26/24008
192.168.255.8/32 192.168.115.11   27/24009
```

- Si può ora osservare chiaramente che il traffico destinato a 192.168.255.8/32 quando colpisce l'ASBR1 con un'etichetta di 27 sarà inoltrato all'ASBR2 con un'etichetta di 24009 fino al successivo hop di ASBR2 192.168.115.11. Allo stesso modo, il traffico destinato a 192.168.255.1/32 dall'ASBR2 sarà provvisto dell'etichetta 25 e l'etichetta sarà scambiata a 23 (etichetta vpn); quindi l'etichetta di trasporto appropriata sarà incapsulata per inoltrare il traffico all'hop successivo-hop 19222229222922292229222922292229222292000000000000000 168.255.2 (PE1).

```
R5#show mpls forwarding-table
Local  Outgoing  Prefix Bytes      Label  Outgoing  Next Hop
Label  Label     or Tunnel Id      Switched Interface
21     19        192.168.255.2/32  0      Fa0/0     192.168.45.4
27     24009     192.168.255.12:65001:192.168.255.8/32 \
                                   26     Fa1/0     192.168.115.11
```

- Il traffico di ritorno prenderà l'etichetta 19 come etichetta di trasporto e la 23 come etichetta vpn per raggiungere PE1 da ASBR1.

- È importante capire che quando il traffico attraversa il collegamento Inter-As, esiste solo un'etichetta mpls, principalmente l'etichetta vpn. Quando il traffico si trova all'interno di un AS, vengono osservate due etichette mpls.
- Sull'ASBR2, ovvero il dispositivo IOS-XR, vengono osservate etichette simili.

```
RP/0/0/CPU0:ios#show bgp vpnv4 unicast labels
Network                Next Hop                Rcvd Label Local Label
Route Distinguisher:192.168.255.2:65000
*> 192.168.12.0/24      192.168.115.5          24 24006
*> 192.168.255.1/32    192.168.115.5          25 24007
Route Distinguisher: 192.168.255.12:65001
*>i192.168.128.0/24    192.168.255.12         24000 24008
*>i192.168.255.8/32    192.168.255.12         24001 24009
```

- In questo esempio si osserva che ASBR2 pubblicizza l'etichetta 24009 su ASBR1 per il prefisso 192.168.255.8/32. Questo output mostra anche che per raggiungere il prefisso 192.168.255.1/32 ASBR1 ha pubblicizzato l'etichetta 25. Ora, poiché si è visto che per raggiungere il prefisso 192.168.255.8/32 l'hop successivo è 192.168.255.12 (PE2). La tabella di inoltro mpls conterrà l'etichetta LDP o l'etichetta di trasporto per raggiungere l'hop successivo.

```
RP/0/0/CPU0:ios#show mpls forwarding
Local   Outgoing  Prefix                Outgoing   Next Hop    Bytes
Label   Label     or ID                 Interface   Interface   Switched
24004   19        192.168.255.12/32    Gi0/0/0/1  192.168.116.6 2082
```

- Per raggiungere l'etichetta 192.168.255.12 in uscita, è utilizzato 19. Il traffico da ASBR2 a PE2 avrà quindi due etichette mpls, 19 come etichetta di trasporto e 24001 come etichetta vpn.
- In modo simile a quanto descritto sopra, il traffico di ritorno, cioè da CE2 a CE1 colpirà ASBR2 con un'etichetta vpn di 24007, in quanto l'etichetta di trasporto sarebbe già stata PHP da parte del router P2. L'operazione di cambio dell'etichetta viene eseguita e l'etichetta viene sostituita con 25 e inviata all'hop successivo 192.168.115.5, ossia al collegamento ASBR1 Inter-As.

```
RP/0/0/CPU0:ios#show mpls forwarding
Local   Outgoing  Prefix                Outgoing   Next Hop    Bytes
Label   Label     or ID                 Interface   Interface   Switched
24007   25        2.255.168.192:65000:192.168.255.1/32 \
                                                Gi0/0/0/0   192.168.115.5 10146
```

- PE2 è a sua volta l'hop successivo per il prefisso 192.168.255.8/32, quindi il PHP verrà eseguito dal router P2 e il traffico destinato a 192.168.255.8/32 raggiungerà PE2 con una singola etichetta mpls, ad esempio l'etichetta VPN 24001.

```
RP/0/0/CPU0:ios#show mpls forwarding
Local   Outgoing  Prefix                Outgoing   Next Hop    Bytes
Label   Label     or ID                 Interface   Interface   Switched
24001   Unlabelled 192.168.255.8/32[V] \
                                                Gi0/0/0/1   192.168.128.8 5364
24003   20        192.168.255.11/32
```

```
RP/0/0/CPU0:ios#show bgp vpnv4 unicast labels
Network          Next Hop          Rcvd Label    Local Label
Route Distinguisher: 192.168.255.12:65001 (default for vrf A)
*>i192.168.12.0/24 192.168.255.11   24006         nolabel
*> 192.168.128.0/24 0.0.0.0         nolabel       24000
*>i192.168.255.1/32 192.168.255.11  24007         nolabel
*> 192.168.255.8/32 192.168.128.8   nolabel       24001
```

- Pertanto, quando il traffico raggiunge PE2 con etichetta vpn 24001, viene inoltrato a CE2 tramite il collegamento Gi0/0/0/1 e viene rimossa anche l'etichetta vpn. Inoltre, per inviare il traffico a 192.168.255.1/32, PE2 utilizzerà un'etichetta vpn di 24007 e un'etichetta di trasporto di 20.

Verifica tramite Traceroute

Traceroute da CE1 a CE2.

```
R1#traceroute 192.168.255.8 source lo1
Type escape sequence to abort.
Tracing the route to 192.168.255.8
VRF info: (vrf in name/id, vrf out name/id)
 1 192.168.12.2 8 msec 16 msec 20 msec
 2 192.168.24.4 [MPLS: Labels 21/27 Exp 0] 516 msec 504 msec 212 msec
 3 192.168.45.5 [MPLS: Label 27 Exp 0] 280 msec 640 msec 280 msec
---- LSP 1 ----
 4 192.168.115.11 [MPLS: Label 24009 Exp 0] 544 msec 548 msec 264 msec
---- LSP 2 ----
 5 192.168.116.6 [MPLS: Labels 19/24001 Exp 0] 748 msec 444 msec 472 msec
 6 192.168.126.12 [MPLS: Label 24001 Exp 0] 204 msec 316 msec 780 msec
---- LSP 3 ----
 7 192.168.128.8 296 msec 892 msec 496 msec
```

- Le etichette possono essere visualizzate sul traceroute e sono esattamente le stesse di cui sopra.
- è già stato detto che l'hop successivo dell'aggiornamento vpnv4 controlla il percorso del commutatore di etichetta e quindi l'etichetta di trasporto.
- L'hop successivo per un prefisso in una progettazione Option B Inter-As viene modificato 3 volte ed esistono quindi 3 provider di servizi di traduzione.
- Il prefisso 192.168.255.8/32 ha origine da PE2, quindi in AS 65001 PE2 è l'hop successivo per l'aggiornamento vpnv4.
- Questo aggiornamento raggiunge ASBR2 e ora ASBR2 annuncia questo aggiornamento ad ASBR1 tramite il collegamento Inter-As, quindi ASBR2 diventa l'hop successivo per l'aggiornamento vpnv4.
- Anche in questo caso lo stesso prefisso è ora pubblicizzato in AS 65000 tramite ASBR1 come aggiornamento vpnv4, quindi per AS 65000 ASBR1 è l'hop successivo per l'aggiornamento vpnv4.
- Poiché l'hop successivo determina l'LSP e cambia 3 volte, nel traceroute vengono evidenziati 3 LSP distinti.
- Si noti che per un provider di servizi di traduzione distinto l'etichetta vpn rimane intatta e non cambia.

Traceroute da CE2 a CE1.

```
R8#traceroute 192.168.255.1 source lol
Type escape sequence to abort.
Tracing the route to 192.168.255.1
VRF info: (vrf in name/id, vrf out name/id)
 1 192.168.128.12 172 msec 164 msec 56 msec
 2 192.168.126.6 [MPLS: Labels 20/24007 Exp 0] 472 msec 452 msec 368 msec
 3 192.168.116.11 [MPLS: Label 24007 Exp 0] 692 msec 780 msec 772 msec
---- LSP 1 ----
 4 192.168.115.5 [MPLS: Label 25 Exp 0] 484 msec 720 msec 232 msec
---- LSP 2 ----
 5 192.168.45.4 [MPLS: Labels 19/23 Exp 0] 376 msec 448 msec 336 msec
 6 192.168.12.2 [MPLS: Label 23 Exp 0] 168 msec 208 msec 432 msec
---- LSP 3 ----
 7 192.168.12.1 464 msec 468 msec 776 msec
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.