

Configurar a opção C MPLS VPN entre AS com Cisco IOS e Cisco IOS-XR

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Explicação](#)

[Verificar](#)

[Ping de CE1 para CE2 e vice-versa](#)

[Explicação das atualizações trocadas e etiquetas MPLS](#)

[Verificação via Traceroutes](#)

[Traceroute de CE1 para CE2](#)

[Traceroute de CE2 para CE1](#)

[Troubleshoot](#)

Introduction

Este documento descreve como configurar e verificar a VPN MPLS (Multiprotocol Label Switching) da Camada 3 entre AS, recurso C da opção C. As plataformas Cisco IOS® e Cisco IOS-XR são usadas para explicação e verificação. Um exemplo de cenário de rede e sua configuração e resultados são mostrados para um melhor entendimento.

Prerequisites

Requirements

Não existem requisitos específicos para este documento. No entanto, o conhecimento básico do MPLS e um conhecimento funcional da plataforma Cisco IOS-XR serão úteis.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

O MPLS é amplamente implantado em provedores de serviços de Internet (ISPs) em todo o mundo. Os ISPs oferecem uma grande variedade de serviços aos clientes e um desses serviços é a VPN MPLS de Camada 3. As VPNs de Camada 3 do MPLS esticam principalmente os limites de roteamento de um cliente de uma localização geográfica para outra. O ISP é usado principalmente como trânsito. A correspondência com o ISP em uma localização geográfica e na outra localização geográfica é concluída, então as rotas específicas do cliente são recebidas no dispositivo Customer Edge (CE) do PE (Provider Edge/ISP).

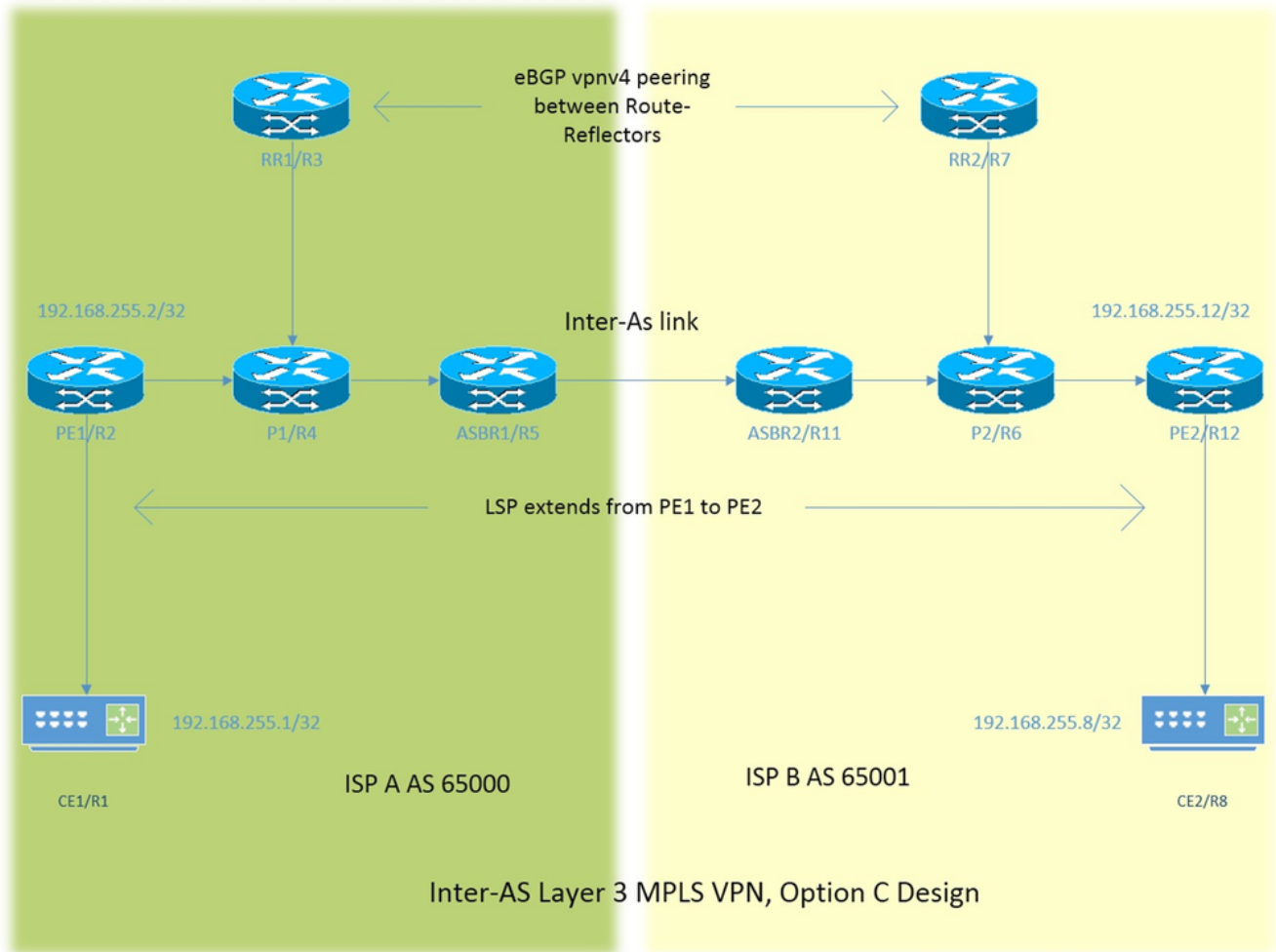
Se o requisito é estender os limites de roteamento para um cliente para dois locais geográficos diferentes onde dois ISPs diferentes têm presença, então os dois ISPs precisam coordenar para que a VPN MPLS de Camada 3 seja fornecida ao cliente final. Essa solução é chamada de VPN MPLS de Camada 3 entre AS.

As VPNS MPLS de Camada 3 entre AS podem ser implantadas de quatro maneiras diferentes, conhecidas como Opção A, Opção B, Opção C e Opção D. A implementação com a Opção C é explicada neste documento.

Configurar

Diagrama de Rede

A topologia para a troca da Opção C entre AS, como mostrado nesta imagem.



O esquema de endereçamento é muito simples. Cada roteador tem uma interface loopback1 descrita como 192.168.255.X, onde X=1 quando o roteador 1 está em questão. O endereçamento da interface é do tipo 192.168.XY.X. Suponha que R1 e R2 estejam em consideração, a configuração da interface no roteador R1 é 192.168.12.1 (aqui X =1, Y = 2).

CE - Borda do cliente

PE - Borda do provedor

RR - Refletor de Rota

ASBR - roteador de limite de sistema autônomo

Em todo o documento, o termo CE denota ambos os dispositivos de Borda do cliente. Se for necessário fazer uma referência específica a um dispositivo específico, ele será referenciado como CE1. Isso também se aplica a PE, RR e ASBR.

Todos os dispositivos executam o Cisco IOS, no entanto ASBR2/R11 e PE2/R12 executam o Cisco IOS-XR.

Dois ISPs são referenciados com o sistema autônomo (AS) 65000 e o AS 65001. O ISP com AS 65000 está no lado esquerdo da topologia e é referenciado como ISP A e ISP com AS 65001 está no lado direito da topologia e é referenciado como ISP B.

Configurações

As configurações dos dispositivos são descritas.

CE1

```
interface Loopback1                                #Customer Edge configuration.
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                                    #Provider Edge Configuration.
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                                  #EIGRP is PE-CE routing
!                                                    #protocol.
address-family ipv4 vrf A autonomous-system 1
redistribute bgp 65000 metric 10000 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                                #Advertising vpnv4 routes
neighbor 192.168.255.3 activate                    #from PE1 to RR1.
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                                #P router configuration.  
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  
!
```

RR1

```
interface Loopback1                                #Route-Reflector configuration.  
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  
neighbor 192.168.255.2 remote-as 65000  
neighbor 192.168.255.2 update-source Loopback1  
neighbor 192.168.255.7 remote-as 65001  
neighbor 192.168.255.7 ebgp-multihop 255          #EBGP-Multihop vpnv4  
neighbor 192.168.255.7 update-source Loopback1 #peering with RR2.  
  
!  
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 192.168.255.7 activate  
neighbor 192.168.255.7 send-community both  
neighbor 192.168.255.7 next-hop-unchanged  
exit-address-family  
!
```

ASBR1

```
interface Loopback1                                #Autonomous-System boundary-
ip address 192.168.255.5 255.255.255.255 #router configuration.
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
redistribute bgp 65000 subnets route-map REDISTRIBUTE_IN_IGP
!
router bgp 65000                                #Redistributing the loopbacks of
bgp log-neighbor-changes                        #RR2 and PE2 in AS 65000.
network 192.168.255.2 mask 255.255.255.255
network 192.168.255.3 mask 255.255.255.255
neighbor 192.168.115.11 remote-as 65001
neighbor 192.168.115.11 send-label
!
ip prefix-list FOREIGN_PREFIXES seq 5 permit 192.168.255.12/32
ip prefix-list FOREIGN_PREFIXES seq 10 permit 192.168.255.7/32
!
route-map REDISTRIBUTE_IN_IGP permit 10
match ip address prefix-list FOREIGN_PREFIXES
!
```

ASBR2

```
interface Loopback1                                #Autonomous System boundary
ipv4 address 192.168.255.11 255.255.255.255 #configuration.
!
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
!
prefix-set FOREIGN_PREFIXES
192.168.255.2/32,
192.168.255.3/32
end-set
!
route-policy DEFAULT
pass
end-policy
!
route-policy REDISTRIBUTE_IN_IGP
if destination in FOREIGN_PREFIXES then
pass
endif
end-policy
!
router static
address-family ipv4 unicast
```

```

192.168.115.5/32 GigabitEthernet0/0/0/0
!
router ospf 1
redistribute bgp 65001 route-policy REDISTRIBUTE_IN_IGP
area 0 #Redistributing the loopback
interface Loopback1 #of RR1 and PE1 in AS 65001.
!
interface GigabitEthernet0/0/0/1
!
router bgp 65001
address-family ipv4 unicast
network 192.168.255.7/32
network 192.168.255.12/32
allocate-label all
!
neighbor 192.168.115.5
remote-as 65000
address-family ipv4 labeled-unicast
route-policy DEFAULT in
route-policy DEFAULT out
!
mpls ldp
address-family ipv4
!
interface GigabitEthernet0/0/0/1
!

```

RR2

```

interface Loopback1 #Route-Reflector Configuration.
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
neighbor 192.168.255.3 remote-as 65000 #EBGP-Multihop vpnv4 peering
neighbor 192.168.255.3 ebgp-multihop 255 #with RR1 in AS 65000.
neighbor 192.168.255.3 update-source Loopback1
neighbor 192.168.255.12 remote-as 65001
neighbor 192.168.255.12 update-source Loopback1
!
address-family vpnv4
neighbor 192.168.255.3 activate
neighbor 192.168.255.3 send-community both
neighbor 192.168.255.3 next-hop-unchanged
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
!

```

P2

```

interface Loopback1 #P router configuration.

```

```
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
!
```

PE2

```
vrf A                                     #Provider Edge Configuration.
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 192.168.128.2 255.255.255.0
!
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                   #Advertising vpnv4 routes from
remote-as 65001                          #PE2 to RR2.
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                               #EIGRP as PE-CE protocol
vrf A
address-family ipv4
autonomous-system 1
redistribute bgp 65001
interface GigabitEthernet0/0/0/1
!

```

CE2

```

interface Loopback1                               #Customer-Edge Configuration.
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
!

```

Explicação

- EIGRP (Enhanced Interior Gateway Routing Protocol) à medida que o protocolo de roteamento PE-CE está sendo implantado.
- O OSPF (Open Shortest Path First) é usado como IGP (Interior Gateway Protocol) para o núcleo do ISP. Em ambos os ISPs em todos os links físicos, o Label Distribution Protocol (LDP) + IGP é implantado. O LDP + IGP não está configurado no link Inter-AS entre ASBR1 e ASBR2.
- A redistribuição do EIGRP em VRF A no Border Gateway Protocol (BGP) e vice-versa é executada no PE.
- Essas rotas redistribuídas são anunciadas como rotas VPNv4 para o refletor de rota (RR).
- O refletor de rota RR1 peers com PE1 e reflete essas rotas aprendidas via PE1 para RR2 via peering de eBGP VPNv4 de vários saltos.
- Esse peering de eBGP VPNv4 de vários saltos está entre dois RRs em ASs distintos.
- É importante que o LSP (Label Switch Path) exista entre os dois RR.
- Para obter um LSP entre os dois RR localizados em um AS diferente, é necessário vazar as rotas específicas entre os ASs.
- O ASBR1 e o ASBR2 vazam as rotas específicas, basicamente o loopback1 do PE e RR de seu próprio AS. O vazamento é feito por meio do anúncio da rota no peering normal do eBGP entre os ASBRs.
- Os ASBRs recebem mutuamente os prefixos loopback1 anunciados de roteadores RR e PE. Em seguida, as rotas recebidas são redistribuídas no IGP (OSPF aqui). A redistribuição é específica por natureza, apenas os dois prefixos, ou seja, o loopback1 de RR e PE remotos são redistribuídos.
- A redistribuição de rotas do BGP para o OSPF e a correspondência das rotas a serem redistribuídas no OSPF é ligeiramente diferente no Cisco IOS-XR e precisa do conhecimento das configurações do prefix-set e da política de rotas. O prefix-set é semelhante à lista de prefixos no Cisco IOS e a política de rota é equivalente ao mapa de rota.
- Agora existe um LSP entre RR1 e RR2 e também PE1 e PE2.

- O próximo salto inalterado para peers VPNv4 eBGP é usado em RRs. Deve-se observar que o próximo salto da rota VPNv4 define o LSP. Agora, se uma atualização for originada do PE2 e enviada para o próximo salto RR2 (iBGP peering) será preservada. Quando o RR2 reflete essa atualização para o RR1, já que esse é um peering eBGP, por cenário normal o RR2 se definirá como o salto seguinte para a atualização e a anunciará para o RR1. RR1 refletirá essa atualização para PE1. Portanto, o PE1 instalará a atualização e verá o próximo salto da atualização como RR2. Como já mencionado, o próximo salto da rota VPNv4 define o LSP. Assim, para que PE1 chegue a PE2, RR2 é o salto seguinte. Portanto, dois LSPs são necessários, um de PE1 a RR2 e outro de RR2 a PE2. A desvantagem em tal projeto é que o tráfego pode atravessar o mesmo link duas vezes (como nesta topologia) e os RR também estão no caminho de trânsito do tráfego.
- Para superar tal problema de design, o próximo salto é inalterado. Quando o RR2 recebe uma atualização do PE2 e reflete a atualização para o RR1, o próximo salto na atualização ainda será PE2 e quando o RR1 refletir isso em PE1, o PE1 instala a atualização com o próximo salto de PE2. Isso significa um único LSP de PE1 para PE2 e nenhum RR em trânsito.
- Deve-se observar que no link entre AS, nenhum MPLS ou LDP é implantado. Os ASBRs usavam o BGP para enviar rótulos. O XR precisa habilitar a família de endereços unicast rotulada IPv4.
- Quando o peering unicast rotulado eBGP surge no ASBR1 (Cisco IOS) com o dispositivo Cisco IOS-XR, o "encaminhamento de BGP MPLS" automaticamente é configurado no link Inter-AS. A troca de rótulos com ASBR2 é realizada, não via LDP, mas via BGP. O Cisco IOS também adiciona automaticamente uma rota /32 conectada à interface do ASBR2 de modo que o rótulo MPLS esteja vinculado a uma rota /32 e a comutação de rótulo está feita corretamente.
- Para o link Cisco IOS-XR sobre Inter-AS, há uma lógica diferente em comparação com a do Cisco IOS. É necessário configurar uma rota estática /32 para a interface do ASBR1, de modo que o rótulo MPLS seja vinculado a um prefixo /32. Se isso não for feito, o plano de controle será ativado, mas o tráfego não será encaminhado.

Verificar

Ping de CE1 para CE2 e vice-versa

A saída do ping de CE1 para CE2 com a interface loopback1 como origem é:

```
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
```

A saída do ping de CE2 para CE1 com a interface loopback1 como origem é:

```
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

Explicação das atualizações trocadas e etiquetas MPLS

- No CE1, o comando **show ip route** fornece a rota para loopback1 do CE2 na outra extremidade.

```
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
```

- O fluxo de tráfego com rótulos MPLS impostos/descartados ao longo do caminho CE1 para CE2 é discutido aqui, juntamente com a forma como a alcançabilidade é obtida quando ele vai do loopback1 da origem de CE1 para o loopback1 de CE2.
- Nos projetos de VPN de Camada 3 do MPLS, deve-se lembrar que durante a operação do switch de rótulo o rótulo de transporte é trocado e o rótulo de VPN é intocado. O rótulo da VPN é exposto quando ocorre Penúltimo Hop Popping (PHP) e o tráfego chega ao PE ou quando um Label Switched Path (LSP) é encerrado.
- No PE1, o loopback1 do CE2 é aprendido através da atualização do BGP VPNv4 e redistribuído para o EIGRP sensível a VRF. O loopback1 aprendido via CE1 via EIGRP é redistribuído no BGP e também se torna uma rota 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           24/nolabel(A)
192.168.128.0     192.168.255.12   nolabel/24000
192.168.255.1/32  192.168.12.1     25/nolabel
192.168.255.8/32  192.168.255.12  nolabel/24007
```

- A partir da saída anterior, pode concluir-se que para alcançar 192.168.255.8/32; ou seja, o loopback1 do CE2, um rótulo de saída de 24007 é aprendido através da atualização do BGP VPNv4. Da mesma forma, o PE1 anuncia a acessibilidade ao loopback1 de CE1 via rótulo de VPN de 25.

```
R2#show mpls forwarding-table
Local   Outgoing Prefix          Bytes Label   Outgoing Next Hop
Label   Label    or Tunnel Id    Switched      interface
22      20       192.168.255.12/32  0             Fa1/0       192.168.24.4
25      No Label 192.168.255.1/32[V]5976             Fa0/0       192.168.12.1
```

- O próximo salto para acessar 192.168.255.8/32 é 192.168.255.12 e o próximo salto decide o LSP. A tabela de encaminhamento MPLS mostra 20 como o rótulo de saída para acessar 192.168.255.12. Portanto, o tráfego de CE1 indo para o loopback 1 do CE2 terá 20 como rótulo de transporte e 24007 como rótulo de VPN.
- Para o tráfego de retorno destinado ao loopback1 de CE1 a operação do PHP já teria ocorrido em P1 como 192.168.255.1/32 pertence a CE1. O tráfego destinado a 192.168.255.1/32 atingirá o PE1 com um rótulo de VPN 25 e esse rótulo será removido e esse pacote será enviado para a interface fa0/0; ou seja, para CE1.

- Os rótulos de VPNv4 em RR1 reconfirmam o mesmo.

```
R3#show bgp vpnv4 unicast all labels
Network          Next Hop          In label/Out label
Route Distinguisher: 192.168.255.2:65000
192.168.255.1/32  192.168.255.2   nolabel/25
Route Distinguisher: 192.168.255.12:65001
192.168.255.8/32  192.168.255.12 nolabel/24007
```

- Em P1, o tráfego do CE1 destinado ao CE2 será atingido com um rótulo de transporte de 20.

```
R4#show mpls forwarding-table
```

Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Switched	Label	Outgoing interface	Next Hop
20	22	192.168.255.12/32	5172		Fa1/1	192.168.45.5

- Agora, o tráfego do CE1 destinado ao CE2 atingirá o ASBR1 com um rótulo de transporte de 22.

```
R5#show mpls forwarding-table
```

Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Switched	Label	Outgoing interface	Next Hop
22	24002	192.168.255.12/32	5928		Fa1/0	192.168.115.11

- Agora, o tráfego do CE1 destinado ao CE2 atingirá o ASBR2 com um rótulo de transporte de 24002.

```
RP/0/0/CPU0:ios#show mpls forwarding
```

Local Label	Outgoing Label	Prefix or ID	Outgoing Interface	Next Hop	Bytes Switched
24002	19	192.168.255.12/32	Gi0/0/0/1	192.168.116.6	7092

- Agora, o tráfego do CE1 destinado ao CE2 atingirá P2 com um rótulo de transporte de 19.

```
R6#show mpls forwarding-table
```

Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Switched	Label	Outgoing interface	Next Hop
19	Pop Label	192.168.255.12/32	9928		Fa1/1	192.168.126.12

- É observado no roteador P2 que a operação do PHP ocorre e o rótulo de transporte é aberto. Quando o tráfego atingir o PE2, ele será atingido com o rótulo VPN 24007, conforme discutido anteriormente. Também deve ser observado que o PE2 estaria anunciando acessibilidade ao loopback1 do CE2 através do rótulo de VPN 24007.

```
RP/0/0/CPU0:ios#show mpls forwarding
```

Local Label	Outgoing Label	Prefix or ID	Outgoing Interface	Next Hop	Bytes Switched
24007	Unlabelled	192.168.255.8/32 [V]	Gi0/0/0/1	192.168.128.6	7992
24008	18	192.168.255.2/32	Gi0/0/0/0	192.168.126.6	673200

```
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)			
*>i192.168.255.1/32	192.168.255.2	25	no-label
*> 192.168.255.8/32	192.168.128.8	no-label	24007

- Pode ser observado aqui que o tráfego de CE1 para CE2 atinge PE2 com um rótulo de VPN para 24007, o tráfego é enviado para Gi/0/0/1, onde CE2 está localizado e o rótulo de VPN está desligado. Também se observa que o PE2 anuncia a acessibilidade para 192.168.255.8/32 através do rótulo VPN 24007. Essas mesmas informações foram aprendidas no PE1 antes. Da mesma forma, a acessibilidade a 192.168.255.1/32 foi anunciada por PE1 através do rótulo VPN de 25 e as mesmas informações são aprendidas aqui. Para acessar 192.168.255.1/32 no CE1 a partir do CE2, um rótulo de VPN 25 e rótulo de transporte de 18 serão usados, já que o salto seguinte 192.168.255.2 pode ser alcançado através do rótulo 18.

Verificação via Traceroutes

- Os rótulos podem ser vistos no traceroute e são exatamente os mesmos como discutido.
- O próximo salto na atualização do VPNv4 controla o caminho do switch de rótulo e, portanto, o rótulo de transporte.
- Em ambos os traceroutes mostrados a seguir, pode-se observar que o rótulo VPN permanece consistente em todos os saltos no LSP. Somente o rótulo de transporte é trocado.
- Quando o PE1 aprende uma atualização originada do PE2, o próximo salto é PE2, não

qualquer RR ou ASBR. Isso faz com que o LSP seja terminado em PE2, o que resulta em um único LSP durante o caminho de trânsito do AS 65000 para o AS 65001 e vice-versa.

Traceroute de CE1 para 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 36 msec 16 msec
2 192.168.24.4 [MPLS: Labels 20/24007 Exp 0] 828 msec 628 msec 2688 msec
3 192.168.45.5 [MPLS: Labels 22/24007 Exp 0] 1456 msec * 1528 msec
4 192.168.115.11 [MPLS: Labels 24002/24007 Exp 0] 1544 msec 2452 msec 2164 msec
5 192.168.116.6 [MPLS: Labels 19/24007 Exp 0] 1036 msec 908 msec 1648 msec
6 192.168.126.12 [MPLS: Label 24007 Exp 0] 2864 msec 1676 msec 1648 msec
7 192.168.128.8 2008 msec 400 msec 572 msec
```

O rótulo VPN 24007 permanece consistente em todo o LSP.

Traceroute de CE2 para CE1

```
R8#traceroute 192.168.255.1 source lo1
```

```
Type escape sequence to abort.
```

```
Tracing the route to 192.168.255.1
```

```
VRF info: (vrf in name/id, vrf out name/id)
```

```
1 192.168.128.2 1228 msec 68 msec 152 msec
2 192.168.126.6 [MPLS: Labels 18/25 Exp 0] 1188 msec 816 msec 1316 msec
3 192.168.116.11 [MPLS: Labels 24007/25 Exp 0] 1384 msec 1816 msec 504 msec
4 192.168.115.5 [MPLS: Labels 23/25 Exp 0] 284 msec 900 msec 972 msec
5 192.168.45.4 [MPLS: Labels 17/25 Exp 0] 436 msec 608 msec 292 msec
6 192.168.12.2 [MPLS: Label 25 Exp 0] 292 msec 108 msec 536 msec
7 192.168.12.1 224 msec 212 msec 620 msec
```

O rótulo VPN 25 permanece consistente em todo o LSP.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.