Konfigurieren der Inter-AS-Option C MPLS VPN mit Cisco IOS und Cisco IOS-XR

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie das MPLS-VPN (Multiprotocol Label Switching) für Layer 3 (Inter-AS), Option C, konfiguriert und verifiziert wird. Zur Erläuterung und Verifizierung werden Cisco IOS® und Cisco IOS-XR-Plattformen verwendet. Für ein besseres Verständnis werden ein Beispiel-Netzwerkszenario sowie dessen Konfiguration und Ausgaben angezeigt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen. Grundlegende Kenntnisse von MPLS und ein funktionsfähiges Wissen über die Cisco IOS-XR-Plattform sind jedoch hilfreich.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

MPLS wird weltweit häufig bei Internetdienstanbietern (ISPs) eingesetzt. ISPs bieten Kunden eine breite Palette von Services an, zu denen auch MPLS Layer 3 VPN gehört. MPLS-Layer-3-VPNs erstrecken sich hauptsächlich über die Routing-Grenzen eines Kunden von einem geografischen Standort zu einem anderen. ISP wird hauptsächlich als Transit verwendet. Das Peering mit dem ISP an einem geografischen Standort und am anderen geografischen Standort ist abgeschlossen. Anschließend werden die kundenspezifischen Routen vom PE-Gerät (Provider Edge/ISP) auf dem Customer Edge (CE)-Gerät empfangen.

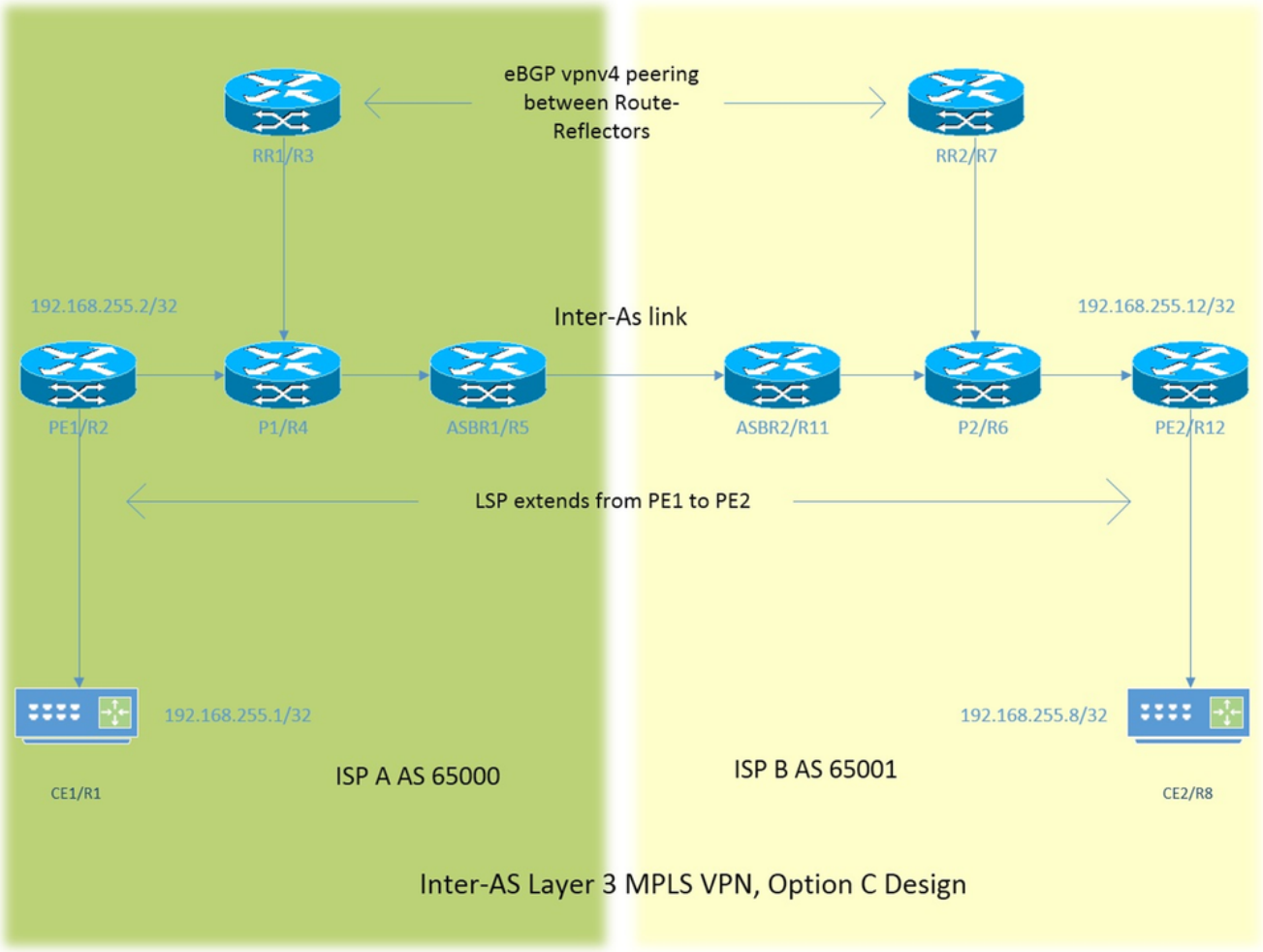
Wenn die Anforderung besteht, die Routing-Grenzen für einen Kunden für zwei verschiedene geografische Standorte zu erweitern, an denen zwei unterschiedliche ISPs vertreten sind, müssen sich die beiden ISPs abstimmen, sodass das MPLS-Layer-3-VPN für den Endkunden bereitgestellt wird. Eine solche Lösung wird als Inter-AS Layer 3 MPLS VPN bezeichnet.

Layer-3-MPLS-VPNS für die AS-Verbindung können auf vier verschiedene Arten bereitgestellt werden, die als Option A, Option B, Option C und Option D bezeichnet werden. Die Implementierung mit Option C wird in diesem Dokument erläutert.

Konfigurieren

Netzwerkdiagramm

Die Topologie für den Austausch der Option C für die AS-Verbindung, wie in diesem Bild gezeigt.



Das Adressierungsschema ist sehr einfach. Jeder Router verfügt über eine Loopback1-Schnittstelle, die als 192.168.255.X beschrieben wird, wobei X=1 steht, wenn der Router 1 betroffen ist. Die Schnittstellenadressierung ist vom Typ 192.168.XY.X . Angenommen, R1 und R2 werden in Betracht gezogen, die Konfiguration der Schnittstelle unter Router R1 ist 192.168.12.1 (hier X = 1, Y = 2).

CE = Customer Edge

PE = Provider Edge

RR = Route Reflector

ASBR = Autonomous System Boundary Router

Im gesamten Dokument bezeichnet der Begriff CE sowohl die Customer Edge-Geräte. Wenn für ein bestimmtes Gerät ein spezifischer Verweis erforderlich ist, wird auf dieses als CE1 verwiesen. Dies gilt auch für PE, RR und ASBR.

Auf allen Geräten wird Cisco IOS ausgeführt, jedoch wird Cisco IOS-XR auf ASBR2/R11 und PE2/R12 ausgeführt.

Zwei ISPs werden mit AS 6500 und AS 65001 als Autonomous System (AS) referenziert. ISP mit AS 65000 befindet sich auf der linken Seite der Topologie und wird als ISP A und ISP referenziert, wobei AS 65001 auf der rechten Seite der Topologie liegt und als ISP B bezeichnet wird.

Konfigurationen

Die Konfigurationen der Geräte werden beschrieben.

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
!                                           #Redistributing the loopbacks of
router bgp 65000                            #RR2 and PE2 in AS 65000.
bgp log-neighbor-changes
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-Refector 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
!
```

Erläuterung

- Enhanced Interior Gateway Routing Protocol (EIGRP) wird als PE-CE-Routing-Protokoll bereitgestellt.
- Open Shortest Path First (OSPF) wird als Interior Gateway Protocol (IGP) für den ISP-Core verwendet. Auf beiden ISPs aller physischen Verbindungen wird das Label Distribution Protocol (LDP) + IGP bereitgestellt. LDP + IGP ist für die Inter-AS-Verbindung zwischen ASBR1 und ASBR2 nicht konfiguriert.
- Die Neuverteilung des EIGRP unter VRF A in das Border Gateway Protocol (BGP) und umgekehrt erfolgt auf dem PE.
- Diese neu verteilten Routen werden als VPNv4-Routen zum Routen-Reflektor (RR) angekündigt.
- Der Routen-Reflektor RR1 Peers mit PE1 reflektiert diese Routen, die über PE1-RR2 über eBGP VPNv4 Multihop Peering gelernt wurden.
- Dieses eBGP-VPNv4-Multihop-Peering besteht zwischen zwei RRs in unterschiedlichen ASs.
- Es ist wichtig, dass zwischen den beiden RRs ein LSP (Label Switch Path) vorhanden ist.
- Um einen LSP zwischen den beiden RRs in einem anderen AS zu erreichen, müssen die spezifischen Routen zwischen den ASs durchlaufen werden.
- Die ASBR1 und ASBR2 überlassen die spezifischen Routen, im Wesentlichen das Loopback1 des PE und des RR des eigenen AS. Das Leaking erfolgt über die Werbung für die Route in normalem eBGP-Peering zwischen den ASBRs.
- Die ASBRs empfangen gegenseitig die Loopback1-Präfixe der jeweils anderen Partei für die RR- und PE-Router. Anschließend werden die empfangenen Routen im IGP (OSPF hier) neu verteilt. Die Neuverteilung ist spezifisch. Nur die beiden Präfixe, d. h. das Loopback1 des Remote-RR und des PE, werden neu verteilt.
- Die Neuverteilung von Routen vom BGP zum OSPF und die Anpassung der in OSPF neu zu verteilenden Routen unterscheiden sich in Cisco IOS-XR geringfügig und erfordern die Kenntnis von Konfigurationen für Präfixe und Routingrichtlinien. Das Präfixset ähnelt der Präfixliste in Cisco IOS, und die Routingrichtlinie entspricht der Routing-Map.

- Nun existiert ein LSP zwischen RR1 und RR2 sowie zwischen PE1 und PE2.
- Der Next-Hop-unveränderte für eBGP VPNv4-Peers wird in RRs verwendet. Der nächste Hop der VPNv4-Route definiert den LSP. Wenn ein Update von PE2 stammt und an RR2 (iBGP-Peering) gesendet wird, wird der nächste Hop beibehalten. Wenn RR2 dieses Update auf RR1 reflektiert, da es sich um ein eBGP-Peering handelt, wird RR2 im normalen Szenario als nächster Hop für das Update festgelegt und an RR1 weitergegeben. RR1 spiegelt dieses Update auf PE1 wider. Daher installiert PE1 das Update und sieht den nächsten Hop des Updates als RR2. Wie bereits erwähnt, definiert der nächste Hop der VPNv4-Route den LSP. Daher ist für PE1 der nächste Hop RR2 für PE2. Daher werden zwei LSP benötigt, einer von PE1 bis RR2 und einer andere von RR2 bis PE2. Der Nachteil eines solchen Designs besteht darin, dass der Datenverkehr zweimal die gleiche Verbindung durchqueren kann (wie in dieser Topologie), und die RRs befinden sich auch im Transit-Pfad des Datenverkehrs.
- Um ein solches Designproblem zu überwinden, wird next-hop-unverändert verwendet. Wenn RR2 ein Update von PE2 erhält und das Update auf RR1 wiedergibt, ist der nächste Hop im Update weiterhin PE2, und wenn RR1 dies auf PE1 widerspiegelt, installiert PE1 das Update mit dem nächsten Hop von PE2. Dies bedeutet, dass ein einziger LSP von PE1 zu PE2 und kein RR bei der Übertragung vorhanden ist.
- Es ist zu beachten, dass auf der Inter-AS-Verbindung kein MPLS oder LDP bereitgestellt wird. ASBRs senden Labels über BGP. XR muss die IPv4-markierte Unicast-Adressfamilie aktivieren.
- Wenn das mit Unicast-Peering gekennzeichnete eBGP auf dem ASBR1 (Cisco IOS) mit dem Cisco IOS-XR-Gerät auftaucht, wird automatisch "MPLS BGP Forwarding" auf der Inter-AS-Verbindung konfiguriert. Der Austausch der Labels mit ASBR2 erfolgt nicht über LDP, sondern über BGP. Cisco IOS fügt der ASBR2-Schnittstelle außerdem automatisch eine verbundene /32-Route hinzu, sodass das MPLS-Label an eine /32-Route gebunden ist und das Label-Switching ordnungsgemäß durchgeführt wird.
- Für Cisco IOS-XR-Verbindungen über Inter-AS gibt es eine andere Logik als für Cisco IOS. Es ist erforderlich, eine statische /32-Route zur Schnittstelle von ASBR1 zu konfigurieren, sodass das MPLS-Label für ein /32-Präfix gebunden ist. Ist dies nicht der Fall, wird die Steuerungsebene aktiviert, der Datenverkehr wird jedoch nicht weitergeleitet.

Überprüfen

Ping von CE1 an CE2 und umgekehrt

Die Ausgabe von Ping von CE1 zu CE2 mit der Loopback1-Schnittstelle als Quelle lautet:

```
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
```

Die Ausgabe von Ping von CE2 zu CE1 mit der Loopback1-Schnittstelle als Quelle lautet:

```
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
```

Erläuterung von ausgetauschten Updates und MPLS-Labels

- Auf CE1 gibt der Befehl **show ip route** die Route für Loopback1 des CE2 am anderen Ende an.
```
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
```
- Der Datenverkehrsfluss mit MPLS-Labels, der über den Pfad CE1 zu CE2 durchgesetzt/entsorgt wird, wird hier besprochen. Außerdem wird erläutert, wie die Erreichbarkeit beim Wechsel vom Quell-Loopback1 von CE1 zu Loopback1 von CE2 erreicht wird.
- Bei MPLS-Layer-3-VPN-Designs sollte beachtet werden, dass beim Betrieb des Label-Switches das Transportlabel ausgetauscht wird und das VPN-Label nicht berührt wird. Das VPN-Label wird verfügbar gemacht, wenn Penultimate Hop Popping (PHP) auftritt und der Datenverkehr den PE erreicht oder ein Label Switched Path (LSP) beendet wird.
- Auf PE1 wird das Loopback1 von CE2 über das BGP VPNv4-Update erfasst und an das VRF-kompatible EIGRP umverteilt. Das über CE1 über EIGRP erfasste Loopback1 wird in das BGP umverteilt und wird zu einer VPNv4-Route.
```
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
```
- Aus der vorherigen Ausgabe kann der Schluss gezogen werden, dass die Adresse 192.168.255.8/32 erreicht wird. Das heißt, das Loopback1 von CE2, ein ausgehendes Label von 24007 wird über das BGP VPNv4-Update erfasst. Auf ähnliche Weise kündigt PE1 die Erreichbarkeit dem Loopback1 von CE1 über das VPN-Label 25 an.
```
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
```
- Der nächste Hop, der 192.168.255.8/32 erreicht, ist 192.168.255.12, und der nächste Hop entscheidet über den LSP. Die MPLS-Weiterleitungstabelle zeigt 20 als ausgehendes Label, das 192.168.255.12 erreicht. Daher wird der von CE1 an das Loopback 1 von CE2 weitergeleitete Datenverkehr 20 als Transportlabel und 24007 als VPN-Label aufweisen.
- Für den Rückgabeverkehr, der für das Loopback1 von CE1 bestimmt ist, wäre der PHP-Vorgang bereits auf P1 aufgetreten, da 192.168.255.1/32 zu CE1 gehört. Der für 192.168.255.1/32 bestimmte Datenverkehr erreicht PE1 mit einem VPN-Label von 25. Dieses Label wird entfernt und an die Schnittstelle fa0/0 gesendet. also CE1.

- Die VPNv4-Labels auf RR1 bestätigen dies erneut.
```
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
```

- Auf P1 wird der für CE2 bestimmte Datenverkehr von CE1 mit einem Transportlabel von 20 gekennzeichnet.

```
R4#show mpls forwarding-table
 Local  Outgoing  Pefix            Bytes Label Outgoing   Next Hop
 Label  Label     or Tunnel Id     Switched    interface
 20     22        192.168.255.12/32 5172        Fa1/1      192.168.45.5
```

- Der für CE2 bestimmte Datenverkehr von CE1 erreicht jetzt ASBR1 mit dem Transportlabel 22.

```
R5#show mpls forwarding-table
 Local  Outgoing  Prefix           Bytes Label Outgoing   Next Hop
 Label  Label     or Tunnel Id     Switched    interface
 22     24002     192.168.255.12/32 5928        Fa1/0      192.168.115.11
```

- Der für CE2 bestimmte Datenverkehr von CE1 erreicht jetzt ASBR2 mit dem Transportlabel 24002.

```
 RP/0/0/CPU0:ios#show mpls forwarding
 Local    Outgoing   Prefix            Outgoing   Next Hop       Bytes
 Label    Label      or ID             Interface                 Switched
 24002    19         192.168.255.12/32  Gi0/0/0/1  192.168.116.6  7092
```

- Der für CE2 bestimmte Datenverkehr von CE1 erreicht P2 mit einem Transportlabel von 19.

```
 R6#show mpls forwarding-table
 Local   Outgoing  Prefix           Bytes Label  Outgoing  Next Hop
 Label   Label     or Tunnel Id     Switched     interface
 19      Pop Label 192.168.255.12/32 9928         Fa1/1     192.168.126.12
```

- Auf dem P2-Router wird beobachtet, dass PHP ausgeführt wird und das Transportetikett gestoppt wird. Wenn der Datenverkehr auf PE2 trifft, wird er, wie bereits erwähnt, mit dem VPN-Label 24007 erreicht. Es sollte auch beachtet werden, dass PE2 über das VPN-Label 24007 die Erreichbarkeit des Loopback1 von CE2 meldet.

```
 RP/0/0/CPU0:ios#show mpls forwarding
 Local   Outgoing    Prefix             Outgoing   Next Hop      Bytes
 Label   Label       or ID              Interface                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           nolabel
 *> 192.168.255.8/32    192.168.128.8      nolabel      24007
```

- Hier ist zu beobachten, dass der Datenverkehr von CE1 zu CE2 mit einem VPN-Label auf 24007 trifft, der Datenverkehr an Gi/0/0/0/1 gesendet wird, wo CE2 sich befindet und das VPN-Label deaktiviert ist. Es wird außerdem beobachtet, dass PE2 die Erreichbarkeit über das VPN-Label von 24007 an 192.168.255.8/32 meldet. Dieselben Informationen wurden zuvor auf PE1 erfasst. Ebenso wurde die Erreichbarkeit auf 192.168.255.1/32 von PE1 über das VPN-Label von 25 angekündigt, und hier werden dieselben Informationen abgerufen. Um 192.168.255.1/32 auf CE1 von CE2 zu erreichen, wird ein VPN-Label von 25 und ein Transportlabel von 18 verwendet, da der nächste Hop 192.168.255.2 über Label 18 erreichbar ist.

Verifizierung über Traceroutes

- Die Labels sind in der Traceroute sichtbar und entsprechen exakt der beschriebenen.
- Der Next Hop im VPNv4-Update steuert den Label-Switch-Pfad und damit das Transportlabel.
- In beiden nachfolgend gezeigten Tracerouten ist zu beachten, dass das VPN-Label bei allen

Hops im LSP konsistent bleibt. Nur das Transportlabel wird ausgetauscht.
- Wenn PE1 eine Aktualisierung von PE2 erfährt, ist der nächste Hop PE2, kein RR oder ASBR. Dadurch wird der LSP an PE2 terminiert, was zu einem einzigen LSP im gesamten Transitpfad von AS 65000 zu AS 65001 und umgekehrt führt.

Traceroute von CE1 zu 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
```

Das VPN-Label 24007 bleibt im gesamten LSP konsistent.

Traceroute von CE2 zu 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
```

Das VPN-Label 25 bleibt im gesamten LSP konsistent.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.