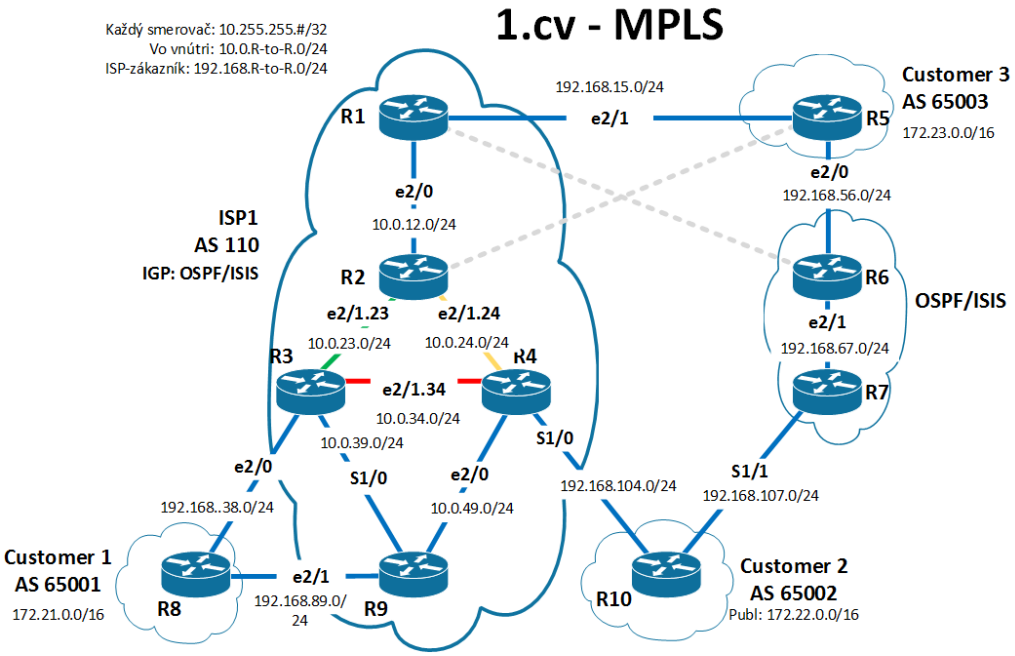
MPLS

Andrej Šišila, Marián Vachalík

Obsah

1.1 Topológia

Budeme konfigurovať smerovacie protokoly MPLS a IS-IS na topológií, ktorá je znázornená na obrázku 1. V rámci autonómnych systémov sme konfigurovali smerovacie protokoly IS-IS (pokiaľ má autonómny systém viac ako 2 smerovače) a BGP (iBGP). Medzi autonómnymi systémami sme konfigurovali len BGP (eBGP). IP adresácia je uvedená v tabuľke 1 a dopĺňa grafické znázornenie topológie na obrázku 1. Smerovače R6 a R7 sme nekonfigurovali.



Obr. 1: Topológia MPLS + L3VPN

Tabuľka 1: IP adresácia

Smerovač	Rozhranie	IP adresa	Maska
R1	E2/0	10.0.12.1	255.255.255.0
	E2/1	192.168.15.1	255.255.255.0
	Lo0	10.255.255.1	255.255.255.255
R2	E2/0	10.0.12.2	255.255.255.0
	E2/1.23	10.0.23.2	255.255.255.0
	E2/1.24	10.0.24.2	255.255.255.0
	Lo0	10.255.255.2	255.255.255.255
R3	E2/0	192.168.38.3	255.255.255.0
	E2/1.23	10.0.23.3	255.255.255.0
	E2/1.34	10.0.34.3	255.255.255.0
	Lo0	10.255.255.3	255.255.255.255
R4	S1/0	192.168.104.4	255.255.255.0
	E2/0	10.0.49.4	255.255.255.0
	E2/1.24	10.0.24.4	255.255.255.0
	E2/1.34	10.0.34.4	255.255.255.0
	Lo0	10.255.255.4	255.255.255.255
R5	E2/0	192.168.56.5	255.255.255.0
	E2/1	192.168.15.5	255.255.255.0
	Lo0	10.255.255.5	255.255.255.255
	Lo1	172.23.0.1	255.255.0.0
R6	E2/0	192.168.56.6	255.255.255.0
	E2/1	192.168.67.6	255.255.255.0
	Lo0	10.255.255.6	255.255.255.255
R7	E2/1	192.168.67.7	255.255.255.0
	S1/1	192.168.107.7	255.255.255.0
	Lo0	10.255.255.7	255.255.255.255
R8	E2/0	192.168.38.8	255.255.255.0
	E2/1	192.168.89.8	255.255.255.0
	Lo0	10.255.255.8	255.255.255.0
	Lo1	172.21.0.1	255.255.0.0
R9	E2/0	10.0.49.9	255.255.255.0
	E2/1	192.168.89.9	255.255.255.0
	Lo0	10.255.255.9	255.255.255.255
	Lo1	172.21.0.1	255.255.0.0
R10	S1/0	192.168.104.10	255.255.255.0
	S1/1	192.168.107.10	255.255.255.0
	Lo0	10.255.255.10	255.255.255.255
	Lo1	172.22.0.1	255.255.0.0

1.2 Úlohy

1.2.1 IS−IS alebo OSPF

Popis

Ako vnútorný smerovací protokol sme zvolili IS-IS, ktorý sme konfigurovali na smerovačoch R1, R2, R3, R4, R6, R7 a R9. Základná konfigurácia protokolu IS-IS spočívala z vytvorenia dvoch oblastí: jednu pre chrbticovú oblasť (R1, R2, R3, R4, R9) a oblasť ďalšieho providera (R6, R7), nastavenia broadcast spojení pre R2, R3 a R4 a nastavenia zvyšku spojení ako P2P a vytvorenia NSAP identifikátorov. Podobne ako pri OSPF sme do základnej konfigurácie zahrnuli aj nastavenie adresácie, vzdialeného prístupu a úpravu vypisovania konzoly.

Konfigurácia

Nižšie uvádzame základnú konfiguráciu IS-IS pre R1. Rozhranie pridáme do IS-IS protokolu príkazom "ip router isis". V nastaveniach procesu IS-IS ("router isis") sme definovali Lo0 a eth2/1 ako pasívne rozhranie (neposielajú sa Hello pakety) príkazom "passive-interface". Nastavili sme NSAP identifikátor príkazom "net". Typ priľahlosti pre smerovače R1, R2, R3, R4, R6, R7 a R9 sme nastavili ako typ L2 príkazom "is-type level-2", a nakoniec sme nastavili rozšírenú metriku pre R1 príkazom "metric-style wide". Rozšírená metrika je novšou implementáciou počítania metriky pre IS-IS. Pokiaľ sa rozhodneme použiť takúto metriku, musíme ju nastaviť na všetkých smerovačoch v IS-IS doméne.

```
!R1
ena
conf t
hostname R1
no ip domain-lookup
username admin privil 15 secret admin
line con 0
  login local
  logging syn
  exec-time 120
line vty 0 15
  privilege level 15
  no login
int e2/0
  ip addr 10.1.12.1 255.255.255.0
  ip router isis
  isis network point-to-point
int e2/1
  ip addr 10.100.15.1 255.255.255.0
  no shut
int lo0
  ip addr 10.255.255.1 255.255.255.255
  ip router isis
  no shut
router isis
```

```
 net 49.0001.0102.5525.5001.00
 passive-interface lo0
 passive-interface e2/1
 is-type level-2
 metric-style wide
```

Overenie

Konfiguráciu IS-IS sme overovali zobrazením IS-IS databázy. Nižšie uvádzame výpis príkazu "show isis database" zo smerovača R1.

```
R1#sh isis database

Tag null:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00            * 0x000004BE   0x23C9        944               0/0/0
R2.00-00              0x000004BD   0x5254        619               0/0/0
R3.00-00              0x000004C3   0x3539        945               0/0/0
R3.01-00              0x000004BE   0x0B18        733               0/0/0
R4.00-00              0x000004C2   0x4758        420               0/0/0
R4.01-00              0x000004BB   0x170D        465               0/0/0
R4.02-00              0x000004BC   0x27F9        900               0/0/0
R9.00-00              0x000004C0   0x0BD0        1084              0/0/0
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00            * 0x000004C6   0x7857        787               0/0/0
R2.00-00              0x000004C1   0x9FB1        1186              0/0/0
R3.00-00              0x000004C8   0xE562        973               0/0/0
R3.01-00              0x000004BE   0x9A11        1157              0/0/0
R4.00-00              0x000004CB   0x89ED        973               0/0/0
R4.01-00              0x000004BE   0xA009        1146              0/0/0
R4.02-00              0x000004B6   0xC2EC        1122              0/0/0
R9.00-00              0x000004C2   0xAE2A        768               0/0/0
```

Z výpisu vyplýva, že protokol IS-IS na R1 je spustený. IS-IS databáza na R1 obsahuje aj záznamy o smerovačoch, ktoré sa nacáhádzajú v IS-IS oblasti 1 t.j. R2, R3, R4 a R9. Z toho vyplýva, že IS-IS je spustený v celej oblasti 1.

1.2.2 MPLS

Popis

Aby sme zabezpečili konektivitu medzi jednotlivými zákazníkmi R5, R8 a R10, bolo potrebné nakonfigurovať BGP a MPLS v sieti providera ISP1. Vďaka tomu bude pre zákazníka sieť **za** Provider Edge smerovačom transparentná. Providerské smerovače ohlasujú požadovanú sieť zákazníka, v našom prípade Lo0. Na smerovači R2 nekonfigurujeme BGP, pretože sa nachádza vnútri providerovej siete a nie na jej okraji. Najprv zapneme "Cisco express forwarding" príkazom "ip cef". Nakoniec zapneme MPLS príkazom "mpls ip". Príkaz "mpls ip" sme

použili iba na rozhraniach vnútri providerskej siete, nie na PE smerovačoch smerom k zákazníkom (R2).

Konfigurácia

```
R1 (config)#ip cef
mpls ip
int serial1/0
  mpls ip
router bgp 65001
  neighbor 192.168.15.1 remote-as 110
  address-family ipv4 unicast
  neighbor 192.168.15.1 activate
  network 10.255.255.5 mask 255.255.255.255
```

Overenie

```
R10#sh ip bgp ipv4 unicast
...

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.255.255.5/32  192.168.104.4                       0 110 110 i
 *>  10.255.255.8/32  192.168.104.4                       0 110 110 i
 *>  10.255.255.10/32 0.0.0.0                  0         32768 i
 *>  172.21.0.0       192.168.104.4                       0 110 110 ?
 *>  172.22.0.0       0.0.0.0                  0         32768 ?
 *>  172.23.0.0       192.168.104.4                       0 110 110 ?
...
```

```
R10#traceroute 10.255.255.8 source l0
Type escape sequence to abort.
Tracing the route to 10.255.255.8
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.104.4 24 msec 16 msec 16 msec
  2 192.168.38.3 [AS 110] [MPLS: Label 26 Exp 0] 16 msec 36 msec 36 msec
  3 192.168.38.8 [AS 110] 68 msec *  52 msec
R10#
```

Z výpisu "show ip bgp ipv4 unicast" z klientského smerovača R10 vyplýva, že vidíme zákaznícke siete aj zo smerovačov R5 a R8. Na výpise "traceroute 10.255.255.8 source l0" vidíme, že paketu bola priradená MPLS značka.

1.2.3 LDP alebo RSVP

Popis

Dohodli sme sa, že aktivujeme LDP (Label Distribution Protocol), aby si smerovače mohli MPLS značky posielať medzi sebou.

Konfigurácia

Na každom providerskom smerovači sme v globálnom konfiguračnom režime aktivovali LDP príkazom:

```
mpls label protocol ldp
```

Overenie

Funkčnosť LDP sme overovali príkazom "show mpls ldp discovery" na providerských smerovačoch. Nižšie je uvedený výpis z R3.

```
R3#show mpls ldp discovery
 Local LDP Identifier:
    10.255.255.3:0
    Discovery Sources:
    Interfaces:
Serial1/0 (ldp): xmit/recv
    LDP Id: 10.255.255.9:0
Ethernet2/1.23 (ldp): xmit/recv
    LDP Id: 10.255.255.2:0
Ethernet2/1.34 (ldp): xmit/recv
    LDP Id: 10.255.255.4:
```

Z výpisu vyplýva, že R3 vidí aktívne LDP na susedných providerských smerovačoch R2, R4 a R9.

1.2.4 Router Reflector alebo konfederácie

Popis

V tomto prípade sme sa dohodli o nastavení Route Reflectora (RR) na smerovač R1. RR je BGP smerovač, ktorý obchádza pravidlo, že iBGP topológia musí byť "full-mesh" t.j. iBGP smerovač v jednej oblasti nešíri prefixy, ktoré sa naučil cez iBGP smerovač z inej oblasti.

Konfigurácia

Smerovače R3, R4 a R9 sme nakonfigurovali tak, aby používali R1 ako RR.

```
!R3, R4, R9
router bgp 110
  neighbor 10.255.255.1 remote-as 110
  neighbor 10.255.255.1 update-source Loopback0
  address-family ipv4 unicast
```

```
    neighbor 10.255.255.1 activate
    neighbor 10.255.255.1 next-hop-self
  network 10.255.255.3 mask 255.255.255.255
```

Potom sme nakonfigurovali R1 ako RR.

```
!R1
router bgp 110
  neighbor 10.255.255.3 remote-as 110
  neighbor 10.255.255.3 update-source l0
  neighbor 10.255.255.4 remote-as 110
  neighbor 10.255.255.4 update-source l0
  neighbor 10.255.255.9 remote-as 110
  neighbor 10.255.255.9 update-source l0
  address-family ipv4 unicast
    neighbor 10.255.255.3 route-reflector-client
    neighbor 10.255.255.3 send-community extended
    neighbor 10.255.255.3 next-hop-self
    neighbor 10.255.255.3 activate
    neighbor 10.255.255.4 route-reflector-client
    neighbor 10.255.255.4 send-community extended
    neighbor 10.255.255.4 next-hop-self
    neighbor 10.255.255.4 activate
    neighbor 10.255.255.9 route-reflector-client
    neighbor 10.255.255.9 send-community extended
    neighbor 10.255.255.9 next-hop-self
    neighbor 10.255.255.9 activate
```

Overenie

Konektivita by mala byť v tomto prípade už všade. Presvedčíme sa pomocou tcl skriptu.

```
R1#tclsh
R1(tcl)#foreach address
+>(tcl)#10.255.255.1
+>(tcl)#10.255.255.2
+>(tcl)#10.255.255.3
+>(tcl)#10.255.255.4
+>(tcl)#10.255.255.5
+>(tcl)#10.255.255.6
+>(tcl)#10.255.255.7
+>(tcl)#10.255.255.8
+>(tcl)#10.255.255.9
+>(tcl)#10.255.255.10
+>(tcl)#
+>(tcl)#ping $address source 10.255.255.1
Sending 5, 100-byte ICMP Echos to 10.255.255.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms
Sending 5, 100-byte ICMP Echos to 10.255.255.2, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/22/28 ms
Sending 5, 100-byte ICMP Echos to 10.255.255.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/39/68 ms
Sending 5, 100-byte ICMP Echos to 10.255.255.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/33/52 ms
Sending 5, 100-byte ICMP Echos to 10.255.255.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/26/40 ms
Sending 5, 100-byte ICMP Echos to 10.255.255.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/88/100 ms
Sending 5, 100-byte ICMP Echos to 10.255.255.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/63/80 ms
Sending 5, 100-byte ICMP Echos to 10.255.255.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/79/100 ms
```

```
R4#ping vrf GREEN 172.21.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.21.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/31/40 ms
R4#ping vrf GREEN 172.22.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.22.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/23/36 ms
R4#ping vrf GREEN 172.23.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.23.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/56/72 ms
```

Z výpisov z R1 vyplýva, že konektivita zostala zachovaná ku všetkým smerovačom v oblasti 110. S použitím VRF pingu z R4 sme zistili, že aj zákaznícke siete sú stále dostupné.

1.2.5 Multiprotocol BGP

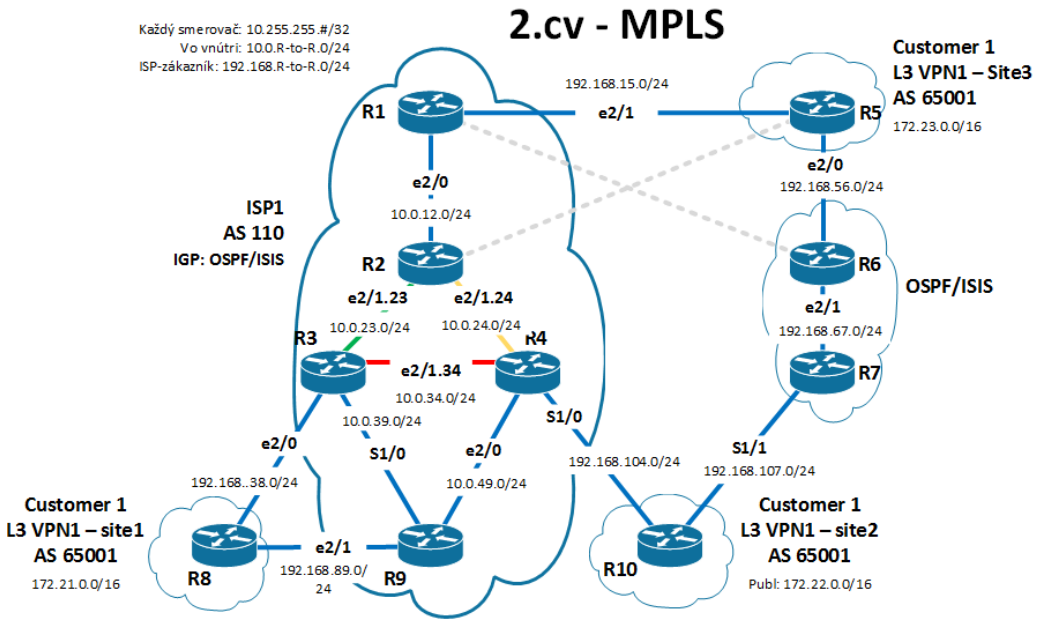
Popis

Multiprotokolové BGP (MP-BGP) je kombinácia BGP s MPLS. Tak možeme poskytovať L3VPN službu viacerým zákazníkom. Naši zákazníci sú nazvaní RED a GREEN.

Zákazník RED mal loopback rozhrania s IP adresami 172.[21/22/23].0.1 /16 na smerovačoch v AS 65001. Zákazník GREEN mal dve loopback rozhrania: jedno na R1, druhé na R9 s IP adresami 172.[21/22].0.1 /16.

Problémom je, že siete zákazníka GREEN sa prekrývali so sieťami zákazníka RED. V takom prípade by PE smerovač nevedel určiť, komu pakety patria. Riešením je vytvorenie VRF tabuliek na PE smerovačoch. Každý zákazník má na PE smerovači vlastnú VRF tabuľku. VRF tabuľka je definovaná atribútmi Route Target a Route Distinguisher. Tieto atribúty musia byť unikátne pre každého zákazníka. PE smerovač pomocoutakto definovanej VRF zistí, ktorý smerovací záznam patrí do ktorej VRF tabuľky. Následne sa podľa spomenutých atribútov, ktorú smerovaciu tabuľku použiť na preposielanie paketov, aby boli doručené tomu správnemu zákazníkovi.

Topológia pre MP-BGP je znázornená na obr. 2.



Obr. 2: Topológia MP-BGP

Konfigurácia

MP-BGP sme konfigurovali na **všetkých PE smerovačoch** t.j. R1, R3, R4 a R9. Nižšie je uvedená konfigurácia pre R1. Zapneme "Cisco express forwarding" príkazom ""ip cef" a MPLS príkazom "mpls ip". Definujeme jednotlivé VRF tabuľky príkazom "ip vrf ¡názov_zákazníka¿" napr. "ip vrf RED". V rámci VRF konfigurácie nastavíme Route Distinguisher, Route Target (pre import aj export - both); napr. pre zákazníka RED sú to príkazy "rd 110:1" pre Route Distinguisher a " route-target export 110:1", " route-target import 110:1" pre Route Target. Následne pripojíme vytvorenú VRF tabuľku ku príslušným rozhraniam konkrétneho zákazníka príkazom "ip vrf forwarding RED" pre RED zákazníka resp. "ip vrf forwarding GREEN" pre GREEN zákazníka.

V rámci BGP konfigurácie sme na R1 potrebovali pridať ako susedov providerské hraničné smerovače ISP1 (R3, R4 a R9) príkazmi (napr. pre R3) "neighbor 10.255.255.3 remote-as 110" a "neighbor 10.255.255.3 update-source Loopback0".

Ďalej sme na R1 zadali príkaz "address-family vpnv4", kde sme jednotlivých susedov aktivovali, zapli sme odosielanie indentifikátorov komunity ostatným smerovačom vnútri ISP1 a nastavili ich ako klientov pre Route Reflector, ktorý sa nachádzal na R1. Na to slúžia príkazy (pre R3) "neighbor 10.255.255.3 activate", "neighbor 10.255.255.3 send-community extended" a "neighbor 10.255.255.3 route-reflector-client".

Nakoniec sme potrebovali redistribuovať siete od jednotlivých zákazníkov cez providera ISP1. Do módu na konfiguráciu VRF pre zákazníka zadáme príkaz "address-family ipv4 vrf ¡názov_zákazníka¿". Pre zákazníka GREEN stačilo zadať príkaz "redistribute connected", pomocou ktorého príkazov sa VRF naučí siete patriace zákazníkovi GREEN zo všetkých ostatných PE smerovačov v ISP1.

Zákazníkovi RED sme do VRF konfigurácie v BGP zadali príkaz "redistribute connected", ktorý má vyššie uvedený účinok. Ďalej sme pripojili oblasť 65001 ku VRF RED príkazmi "neighbor 192.168.15.5 remote-as 65001" a "neighbor 192.168.15.5 activate". Lenže vzniká tu jeden problém: pokiaľ by chcela pobočka 1 komunikovať napr. s pobočkou 3, pobočka 3 tieto pakety zahodí, pretože v BGP platí pravidlo, že pokiaľ prijatý paket má rovnaké číslo AS ako má prijímajúci smerovač, tento paket sa zahodí, aby sa predišlo slučke. V tomto prípade je takéto správanie nežiadúce a dá sa ošetriť príkazom "neighbor 192.168.15.5 as-override", ktorý zabezpečí prijatie paketu s rovnakým číslom AS.

```
R1(config)#ip cef
mpls label protocol ldp

ip vrf GREEN
 rd 100:2
 route-target export 110:2
 route-target import 110:2
 exit
ip vrf RED
 rd 110:1
 route-target export 110:1
 route-target import 110:1
 exit

interface Loopback0
 ip address 10.255.255.1 255.255.255.255
 ip router isis

interface Loopback1
 ip address 172.21.0.1 255.255.0.0
 ip vrf forwarding GREEN
```

```
interface Ethernet2/0
 ip address 10.0.12.1 255.255.255.0
 ip router isis
 duplex half
 mpls ip
 isis network point-to-point

interface Ethernet2/1
 ip vrf forwarding RED
 ip address 192.168.15.1 255.255.255.0
 duplex half

router bgp 110
 bgp log-neighbor-changes
 neighbor 10.255.255.3 remote-as 110
 neighbor 10.255.255.3 update-source Loopback0
 neighbor 10.255.255.4 remote-as 110
 neighbor 10.255.255.4 update-source Loopback0
 neighbor 10.255.255.9 remote-as 110
 neighbor 10.255.255.9 update-source Loopback0

 address-family vpnv4
  neighbor 10.255.255.3 activate
  neighbor 10.255.255.3 send-community extended
  neighbor 10.255.255.3 route-reflector-client
  neighbor 10.255.255.4 activate
  neighbor 10.255.255.4 send-community extended
  neighbor 10.255.255.4 route-reflector-client
  neighbor 10.255.255.9 activate
  neighbor 10.255.255.9 send-community extended
  neighbor 10.255.255.9 route-reflector-client
 exit-address-family

 address-family ipv4 vrf GREEN
  redistribute connected
 exit-address-family

 address-family ipv4 vrf RED
  redistribute connected
  neighbor 192.168.15.5 remote-as 65001
  neighbor 192.168.15.5 activate
  neighbor 192.168.15.5 as-override
 exit-address-family
```

Overenie

Funkčnosť BGP sme overovali príkazmi "show ip bgp vpnv4 vrf RED", "show ip bgp vpnv4 vrf GREEN" a "show ip bgp vpnv4 vrf RED 172.21.0.0" na PE smerovačoch a príkazom "show ip bgp" na Customer Edge (CE) smerovačoch.

```
R1#show ip bgp vpnv4 vrf RED
BGP table version is 144, local router ID is 10.255.255.1
```

```
...

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 110:2 (default for vrf RED)
 * i 172.21.0.0       10.255.255.9             0    100      0 65001 ?
 *>i                  10.255.255.3             0    100      0 65001 ?
 *>i 172.22.0.0       10.255.255.4             0    100      0 65002 ?
 *>  172.23.0.0       192.168.15.5             0             0 65003 ?
...
```

```
R1#show ip bgp vpnv4 vrf GREEN
BGP table version is 144, local router ID is 10.255.255.1
...

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 110:2 (default for vrf RED)
 * i 172.21.0.0       0.0.0.0                  0    100      0 65004 ?
 *>i 172.22.0.0       10.255.255.9             0    100      0 65005 ?
...
```

```
R8#show ip bgp
BGP table version is 47, local router ID is 10.255.255.8
...

     Network          Next Hop            Metric LocPrf Weight Path
...
 *>  172.21.0.0       0.0.0.0                  0         32768 ?
 *   172.22.0.0       192.168.89.9                           0 110 110 ?
 *>                   192.168.38.3                           0 110 110 ?
 *   172.23.0.0       192.168.89.9                           0 110 110 ?
 *>                   192.168.38.3                           0 110 110 ?
...
```

```
R1#show ip bgp vpnv4 vrf RED 172.21.0.0
BGP routing table entry for 110:2:172.21.0.0/16, version 142
Paths: (2 available, best #2, table RED)
  Advertised to update-groups:
     9          3
  Refresh Epoch 10
  65001, (Received from a RR-client)
    10.255.255.9 (metric 40) from 10.255.255.9 (10.255.255.9)
```

```
    Origin incomplete, metric 0, localpref 100, valid, internal
    Extended Community: RT:110:2
    Connector Attribute: count=1
     type 1 len 12 value 110:2:10.255.255.9
    mpls labels in/out nolabel/24
    rx pathid: 0, tx pathid: 0
Refresh Epoch 10
65001, (Received from a RR-client)
  10.255.255.3 (metric 30) from 10.255.255.3 (10.255.255.3)
    Origin incomplete, metric 0, localpref 100, valid, internal, best
    Extended Community: RT:110:2
    Connector Attribute: count=1
     type 1 len 12 value 110:2:10.255.255.3
    mpls labels in/out nolabel/22
    rx pathid: 0, tx pathid: 0x0
```

Z výpisov uvedených vyššie vyplýva, že pre zákazníkov GREEN a RED sme vytvorili L3VPN. Tak sme oddelili siete jednotlivých zákazníkov. To, že obaja zákazníci používajú rovnaký adresný rozsah, neprekáža, pretože na PE smerovačoch boli vytvorené VRF tabuľky (každému zákazníkovi sa vytvorila jedna VRF tabuľka), ktoré na základe "route target" parametra vedia, o ktorého zákazníka ide, a na základe toho smerujú premávku do sietí rovnakého zákazníka. O tom, že napr. zákazník RED sa môže dostať aj do ďalších svojich sietí, ktoré sú na opačných koncoch providerovej siete, svedčí aj BGP tabuľka zákazníka, kde sú uvedené prefixy z jeho pobočiek.

1.2.6 Hub & Spoke VPN

Popis

Topológia bola pozmenená tak, že namiesto dvoch rôznych zákazníkov RED a GREEN budeme mať iba jedného, ktorý má tri pobočky s rovnakým ASN 65001.

Adresovanie ostáva rovnaké, len pobočkám sme pridali nové siete na rozhraní Loopback1.

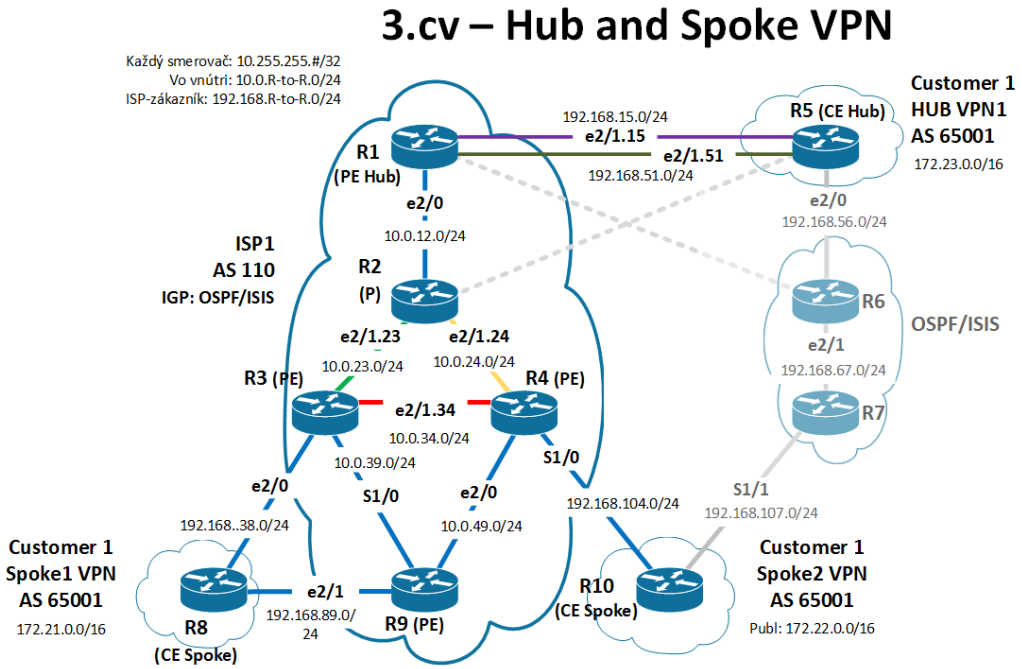
R5	lo1	172.23.0.1 /16
R8	lo1	172.21.0.1 /16
R10	lo1	172.22.0.1 /16

Na prepojenie týchto pobočiek sme využili VPN. V prvom kroku bolo potrebné na smerovačoch R5, R8 a R10 vypnúť bežiaci BGP (no router bgp 65001/2/3), keďže nastala zmena AS oproti pôvodnému zadaniu.

Ďalším krokom bola aktivácia VRF (Virtual Routing Instance) pre pobočky na každom provider edge (PE) smerovači v AS 110 (R1, R3, R4 a R9). Aby sa vytvorila unikátna VPN cesta pre daného zákazníka, bolo potrebné definovať Route Distingusher (RD) a následne aj Route Target (RT).

Potom danú VRF treba priradiť rozhraniam, ktoré smerujú k zákazníkom. Následne bolo potrebné nadviazať BGP susedstvá medzi PE smerovačmi a CE smerovačmi v zákazníckom AS 65001 vytvorením VRF tabuľky.

Úlohou bolo zmeniť predošlú konfiguráciu tak, aby smerovač R1 bol hubom pre ostatné PE smerovače a R5 hubom pre zákaznícke CE smerovače (viď obr. 3). Medzi týmito dvomi smerovačmi v topológii tiež pribudla linka, avšak fyzickú máme k dispozícii len jednu, preto sme museli vytvoriť pre jedného dve podrozhrania: jedno pre odosielanie dát "spoke" smerovačom, druhé pre príjem správ od nich. Tým pádom je nutné fyzické rozhranie e2/1 rozdeliť na dve subrozhrania a na nich vytvoriť dve samostatné VRF pre import a export (viď obr. 4). Predtým sme však museli odstrániť staré VRF z predošlých cvičení, príkazom no ip vrf z1.

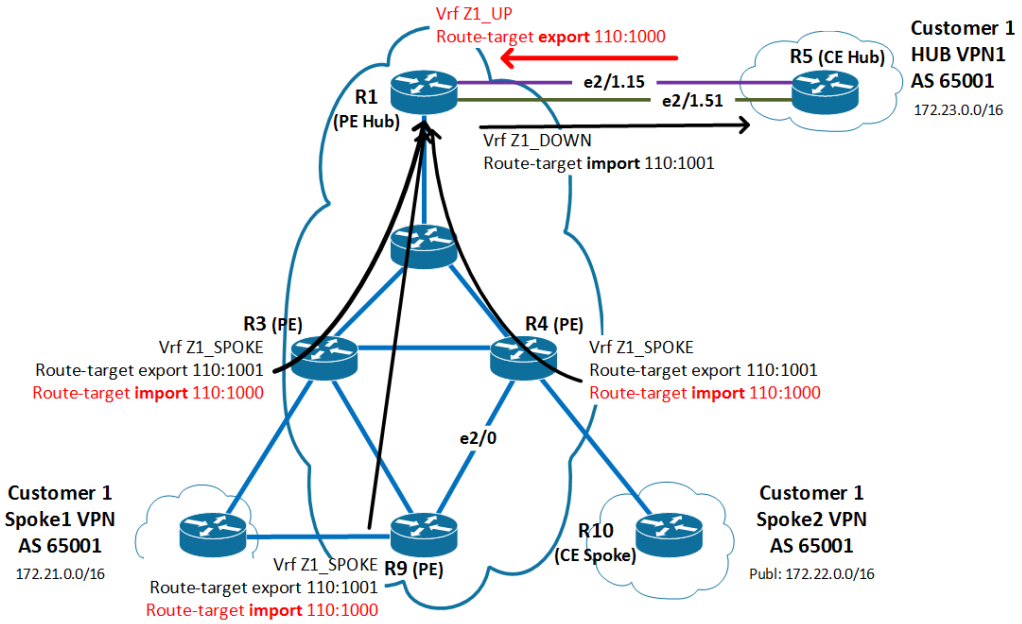


Obr. 3: Topológia MPLS Hub & Spoke

Konfigurácia

```
R5 (CE smerovač)
router bgp 65001
  address-family ipv4 unicast
    network 10.255.255.5 mask 255.255.255.255
    network 172.23.0.0 mask 255.255.255.0
    neighbor 192.168.15.1 activate
```

Pokračovali sme konfiguráciou VRF tabuliek pre providerské smerovače.



Obr. 4: Topológia MPLS Hub & Spoke s Route Target

```
R1
no ip vrf RED

ip vrf Z1_DOWN
 rd 110:1001
 route-target import 110:1001

ip vrf Z1_UP
 rd 110:1000
 route-target export 110:1000

interface Ethernet2/1
 no ip address
 duplex half

interface Ethernet2/1.15
 encapsulation dot1Q 15
 ip vrf forwarding Z1_UP
 ip address 192.168.15.1 255.255.255.0

interface Ethernet2/1.51
 encapsulation dot1Q 51
 ip vrf forwarding Z1_DOWN
 ip address 192.168.51.1 255.255.255.0

router bgp 110
 address-family ipv4
  neighbor 10.255.255.3 activate
  neighbor 10.255.255.4 activate
  neighbor 10.255.255.9 activate
```

```
 exit-address-family

 address-family ipv4 vrf Z1_DOWN
  redistribute connected
  neighbor 192.168.51.5 remote-as 65001
  neighbor 192.168.51.5 activate
  neighbor 192.168.51.5 as-override
 exit-address-family

 address-family ipv4 vrf Z1_UP
  redistribute connected
  redistribute static
  neighbor 192.168.15.5 remote-as 65001
  neighbor 192.168.15.5 activate
  neighbor 192.168.15.5 as-override
  default-information originate
 exit-address-family

ip route vrf Z1_UP 0.0.0.0 0.0.0.0 192.168.15.5
mpls ldp router-id Loopback0
=============================================
R3#
no ip vrf RED

int eth2/0
 ip addr 192.168.38.3

ip vrf Z1_SPOKE
 rd 110:1001
 route-target export 110:1001
 route-target import 110:1000

interface Ethernet2/0
 ip vrf forwarding Z1_SPOKE

router bgp 110
 address-family ipv4 vrf Z1_SPOKE
  redistribute connected
  neighbor 192.168.38.8 remote-as 65001
  neighbor 192.168.38.8 activate
  neighbor 192.168.38.8 as-override
 exit-address-family
=======================================
R4#sh run
!ip brf GREEN a RED zmazal a dal:

int s1/0
 ip addr 192.168.104.4 255.255.255.0

int e2/0
 ip addr 10.0.49.4 255.255.255.0
```

```
ip vrf Z1_SPOKE
 rd 110:1001
 route-target export 110:1001
 route-target import 110:1000

interface Serial1/0
 ip vrf forwarding Z1_SPOKE

router bgp 110
!namiesto RED a GREEN dal:

 address-family ipv4 vrf Z1_SPOKE
  redistribute connected
  neighbor 192.168.104.10 remote-as 65001
  neighbor 192.168.104.10 activate
  neighbor 192.168.104.10 as-override
 exit-address-family
================================================
R9#
!ip vrf RED zmenil na:

ip vrf Z1_SPOKE
 rd 110:1001
 route-target export 110:1001
 route-target import 110:1000

interface Ethernet2/1
 ip addr 192.168.89.9 255.255.255.0
 ip vrf forwarding Z1_SPOKE

router bgp 110
!namiesto RED dal:

 address-family ipv4 vrf Z1_SPOKE
  redistribute connected
  neighbor 192.168.38.8 remote-as 65001
  neighbor 192.168.38.8 activate
  neighbor 192.168.38.8 as-override
 exit-address-family
============
R5

interface Ethernet2/1
 no ip address

interface Ethernet2/1.15
 encapsulation dot1Q 15
 ip address 192.168.15.5 255.255.255.0

interface Ethernet2/1.51
```

```
 encapsulation dot1Q 51
 ip address 192.168.51.5 255.255.255.0

router bgp 65001
 network 10.255.255.5 mask 255.255.255.255
 neighbor 192.168.15.1 remote-as 110
 neighbor 192.168.51.1 remote-as 110
```

Parameter as-override zabezpečí, aby smerovače nezahadzovali siete, ktoré prechádzajú do rovnakého AS (65001). Príkaz redistribute connected distribuuje všetky pripojené siete zákazníka v rámci BGP. Tieto príkazy zadáme na smerovačoch R1 smerom k R5, na R9 k R8 a na R4 k R10.

Konfigurácia CE smerovačov je podobná, využíva však address-family, pretože zákazníci sa o VRF nezaujímajú. Na smerovačoch R5, R8 a R10 musíme zmeniť predošlú konfiguráciu BGP, teda pôvodné AS nahradíme AS 65001, ohlásime ich vlastné siete a aktivujeme spojenie na suseda.

```
R5 (CE smerovač)
router bgp 65001
  address-family ipv4 unicast
    network 10.255.255.5 mask 255.255.255.255
    network 172.23.0.0 mask 255.255.255.0
    neighbor 192.168.15.1 activate
```

Overenie

Zadaním tohto príkazu sa presunie záznam z globálnej smerovacej tabuľky do smerovacej tabuľky vrf z1. Po zadaní príkazu je takisto potrebné na ňom nanovo zadať IP adresu. Overenie, že sa rozhranie pridalo do danej VRF, vykonáme príkazom "sh ip vrf".

```
R1#show ip vrf
  Name                                     Default RD          Interfaces
  Z1_DOWN                                  110:2               Et2/1.15
  Z1_UP                                    110:2               Et2/1.51
```

Po správnej konfigurácii by sa na CE smerovačoch v BGP tabuľke pre ipv4 unicast mali objaviť všetky ohlasované siete smerovačov R5, R8 a R10 (Lo0 aj Lo1).

```
R8#
...
     Network          Next Hop            Metric LocPrf Weight Path
 *   10.255.255.5/32  192.168.89.9                         0 110 110 i
 *>                   192.168.38.3                         0 110 110 i
 *>  10.255.255.8/32  0.0.0.0                  0         32768 i
 *   10.255.255.10/32 192.168.89.9                         0 110 110 i
 *>                   192.168.38.3                         0 110 110 i
 *>  172.21.0.0       0.0.0.0                  0         32768 ?
```

```
 *   172.22.0.0       192.168.89.9                           0 110 110 ?
 *>                   192.168.38.3                           0 110 110 ?
 *   172.23.0.0       192.168.89.9                           0 110 110 ?
 *>                   192.168.38.3                           0 110 110 ?
...
```

Rovnako sme použili traceroute z R8 (lo1) na R10 (lo1):

```
R8#traceroute 172.22.0.1 source lo0
Type escape sequence to abort.
Tracing the route to 172.22.0.1
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.38.3 16 msec 52 msec 16 msec
  2 192.168.15.1 [AS 110] [MPLS: Label 34 Exp 0] 13 msec 19 msec 66 msec
  3 192.168.51.1 [AS 110] [MPLS: Label 21 Exp 0] 16 msec 20 msec 60 msec
  4 192.168.104.4 [AS 110] [MPLS: Label 29 Exp 0] 18 msec 25 msec 40 msec
  5 192.168.104.10 [AS 110] 60 msec *  72 msec
```

Z výpisu "show ip vrf" vyplýva, že obidve subrozhrania medzi R1 a R5 (pre odoslanú a prijatú premávku) patria do VRF s názvom Z1_SPOKE. Výpis príkazu "sh ip bgp ipv4 unicast" ukazuje naučené lo0 a lo1 rozhrania od R5, R8 a R10. Nakoniec vo výpise príkazu traceroute z R8 na R10 vidíme, že premávka smeruje zo spoke smerovača najprv na hub R5 a odtiaľ späť na spoke R10.

1.2.7 Draft Rosen

Popis

Draft Rosen je multicastová MPLS technológia pre VPN, ktorá na riadenie multicastovej premávky používa BGP. Topológiu môžeme vidieť na obr. 5.

Konfigurácia

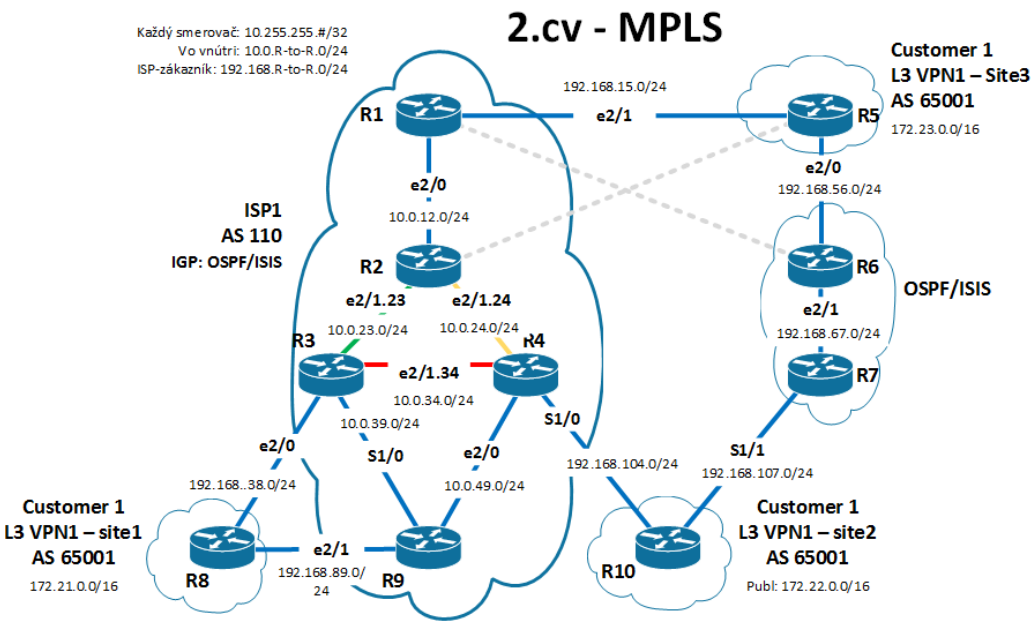
Najprv zrušíme všetko, čo sme nakonfigurovali pri Hub & Spoke:

Zrušíme subrozhrania medzi R1 a R5 a urobíme medzi nimi iba jednu linku.

```
no int eth2/1.15
no int eth2/1.51
int eth2/1
ip addr 192.168.15.# 255.255.255.0
```

Vymažeme IPčku druhého spätného subinterfejsu eth2/1.51 "192.168.51.1" z neighbrov v BGP na R5.

```
R5(config)#router bgp 65001
  no neighbor 192.168.51.1 remote-as 110
```



Obr. 5: Topológia Draft Rosen

Vymažeme VRF z Hub & Spoke.

```
!R1
no ip vrf Z1_DOWN
no ip vrf Z1_UP

!R3, R4, R9
no ip vrf Z1_SPOKE
```

Vytvoríme novú VRF pre klienta GREEN. Route target import a export pre ne bude rovnaký. Novú VRF nastavíme na R1, R3, R4 a R9.

```
ip vrf GREEN
  rd 110:2
  route-target both 110:2
```

VRF GREEN aplikujeme na rozhrania R1, R3, R4 a R9 a nanovo nastavíme IP adresy na na rozhraniach, pretože tým, že sme zrušili pôvodné VRF, odstránili sa zároveň IP adresy z rozhraní, na ktorých boli nastavené.

```
!R1
R1(config)#int eth2/1
R1(config-if)#ip vrf forwarding GREEN
% Interface Ethernet2/1 IPv4 disabled and address(es) removed due to enabling
R1(config-if)#ip addr 192.168.15.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#router bgp 110
R1(config-router)#address-family ipv4 vrf GREEN
R1(config-router-af)#redistribute connected
```

```
R1(config-router-af)#neighbor 192.168.15.5 remote-as 65001
R1(config-router-af)#neighbor 192.168.15.5 activa
*May 16 10:10:08.158: %BGP-5-ADJCHANGE: neighbor 192.168.15.5 vpn vrf GREEN Up
R1(config-router-af)#neighbor 192.168.15.5 activate
R1(config-router-af)#neighbor 192.168.15.5 as-ov
R1(config-router-af)#neighbor 192.168.15.5 as-override
```

Teraz môžeme začať konfigurovať Draft Rosen. IP adresa multicastovej skupiny (MDT ID) pre zákaznika GREEN je 239.10.10.10. V sieti zákaznika je potrebné nastaviť PIM sparse mode. RP bude R1, v sieti zakaznika to bude R5. konfigurujeme zákaznicke routre R5, R8 a R10. Zákaznícke smerovače potom staticky pripojíme do multicastovej skupiny a overíme funkčnosť.

Na všetkých smerovačoch zadáme nižšie uvedený príkaz, aby sme aktivovali multicastové smerovanie.

```
ip multicast-routing
```

Na PE smerovačoch (R1, R3, R4, R9) aktivujeme multicastové smerovanie aj pre VRF GREEN.

```
ip multicast-routing vrf GREEN
```

Na všetkých providerských smerovačoch zadáme pre všetky rozhrania, ktoré sa podieľajú na multicastovom prenose (aj na loopback0), príkaz:

```
ip pim sparse-mode
```

Tým aktivujeme PIM Sparse Mode, ktorý bude prenášať dátový multicastový tok. V trojuholníku stačí dávať príkaz iba na subrozhrania. Tento príkaz vykonáme aj na CE routroch, ale iba pre rozhrania smerujúce ku PE smerovačom.

Nastavíme RP pre providera na R1 a pre zakaznika na R5.

PE smerovače:

```
R3(config)#ip pim rp-address 10.255.255.1
```

Zákaznicke CE smerovače:

```
R8(config)#ip pim rp-address 172.23.0.1
```

PE smerovače priradíme do multicastovej skupiny.

```
R1(config)#ip vrf GREEN
  mdt default 239.10.10.10
```

Na PE smerovačoch nastavíme zákaznicky RP pre VRF GREEN na R5.

```
R9(config)#ip pim vrf GREEN rp-address 172.23.0.1
```

Na CE smerovačoch priradíme loopback1 do multicastovej skupiny

```
int lo1
  ip igmp join-group 239.10.10.10
```

Overenie MP-BGP konektivity

Najprv sme overovali základnú MP−BGP konektivitu príkazmi "sh ip route vrf GREEN" z R4, "show ip bgp ipv4 unicast" z R8, "ping 172.22.0.1 source 172.21.0.1" z R8 a "ping vrf GREEN 172.23.0.1" z R4.

```
R4(config-router-af)#do sh ip route vrf GREEN

Routing Table: GREEN
...

Gateway of last resort is not set

      10.0.0.0/32 is subnetted, 3 subnets
B        10.255.255.5 [200/0] via 10.255.255.1, 00:08:23
B        10.255.255.8 [200/0] via 10.255.255.3, 00:03:21
B        10.255.255.10 [20/0] via 192.168.104.10, 00:00:23
B     172.21.0.0/16 [200/0] via 10.255.255.3, 00:03:21
B     172.22.0.0/16 [20/0] via 192.168.104.10, 00:00:23
B     172.23.0.0/16 [200/0] via 10.255.255.1, 00:08:23
B     192.168.15.0/24 [200/0] via 10.255.255.1, 00:08:53
B     192.168.38.0/24 [200/0] via 10.255.255.3, 00:04:05
B     192.168.56.0/24 [200/0] via 10.255.255.1, 00:08:23
B     192.168.89.0/24 [200/0] via 10.255.255.3, 00:03:21
      192.168.104.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.104.0/24 is directly connected, Serial1/0
L        192.168.104.4/32 is directly connected, Serial1/0
B     192.168.107.0/24 [20/0] via 192.168.104.10, 00:00:23
```

```
R8#show ip bgp ipv4 unicast
BGP table version is 42, local router ID is 10.255.255.8
Status codes: s suppressed, d damped, h history, * valid, > best, i - interna
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *   10.255.255.5/32  192.168.89.9                         0 110 110 i
 *>                   192.168.38.3                         0 110 110 i
 *>  10.255.255.8/32  0.0.0.0                  0         32768 ?
 *   10.255.255.10/32 192.168.89.9                         0 110 110 ?
 *>                   192.168.38.3                         0 110 110 ?
```

```
 *>  172.21.0.0       0.0.0.0                  0         32768 i
 *   172.22.0.0       192.168.89.9                           0 110 110 i
 *>                   192.168.38.3                           0 110 110 i
 *   172.23.0.0       192.168.89.9                           0 110 110 i
 *>                   192.168.38.3                           0 110 110 i
 *   192.168.15.0     192.168.89.9                           0 110 ?
 *>                   192.168.38.3                           0 110 ?
 *   192.168.38.0     192.168.89.9                           0 110 ?
 *                    192.168.38.3             0             0 110 ?
     Network          Next Hop            Metric LocPrf Weight Path
 *>                   0.0.0.0                  0         32768 ?
 *   192.168.56.0     192.168.89.9                           0 110 110 ?
 *>                   192.168.38.3                           0 110 110 ?
 *   192.168.89.0     192.168.89.9             0             0 110 ?
 *                    192.168.38.3                           0 110 ?
 *>                   0.0.0.0                  0         32768 ?
 *   192.168.104.0    192.168.89.9                           0 110 ?
 *>                   192.168.38.3                           0 110 ?
 *   192.168.107.0    192.168.89.9                           0 110 110 ?
 *>                   192.168.38.3                           0 110 110 ?
```

```
R8#ping 172.22.0.1 source 172.21.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.22.0.1, timeout is 2 seconds:
Packet sent with a source address of 172.21.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/56/60 ms
```

```
R4(config-router-af)#do ping vrf GREEN 172.23.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.23.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/59/72 ms
```

Z výpisov uvedených vyššie vyplýva, že privátne siete 172.2X.0.0 sa rozšírili medzi všetky PE aj CE smerovače. Výpisy príkazu "ping" ukazujú vzájomnú konektivitu medzi pobočkami zákazníka GREEN.

Overenie Draft Rosen a multicastových tunelov

Draft Rosen sme overovali príkazmi "ip pim rp-address 10.255.255.1" z R1 a "ping 239.10.10.10 repeat 2" z R5.

```
R1(config)#ip pim rp-address 10.255.255.1
R1(config)#
*May 16 10:59:35.306: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0
*May 16 10:59:35.474: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1
```

```
R5#ping 239.10.10.10 repeat 2
Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 239.10.10.10, timeout is 2 seconds:

Reply to request 0 from 172.23.0.1, 32 ms
Reply to request 0 from 172.21.0.1, 84 ms
Reply to request 0 from 172.22.0.1, 80 ms
Reply to request 1 from 172.23.0.1, 8 ms
Reply to request 1 from 172.21.0.1, 80 ms
Reply to request 1 from 172.22.0.1, 80 ms
```

Po vykonaní príkazu "ip pim rp-address 10.255.255.1" sa zobrazili správy, ktoré hovoria o vytvorení tunelových rozhraní ku smerovačom, ktoré sa nachádzajú v multicastovej doméne. Na ping zákazníckej multicastovej skupiny odpovedali všetky smerovače nachádzajúce sa v zákazníckej multicastovej doméne t.j. R5, R8 a R10.

1.2.8 Otázky MPLS

1. Podľa čoho sa MPLS rozhoduje pri preposielaní paketov?
A. Static Route
B. BGP
C. L2 label +
D. smerovací protokol

2. Ako sa nazýva akcia pridávania a odoberania labelov v MPLS?
A. Plug and Play
B. Wipe on / Wipe off
C. Push and Pop +
D. Take / Drop

3. Kde sa nachádza MPLS label v data L2 rámci?
A. medzi IP a data
B. medzi IP a MAC +
C. v rámci vrstvy IP
D. ani jedna z odpovedí nie je správna

4. Kolko bitov má MPLS label value v MPLS hlavičke?
A. 10
B. 16
C. 20 +
D. 21

5. Na ktorom UDP porte sú LDP posielané?
A. 22
B. 464
C. 502
D. 646 +

1.2.9 Otázky L3VPN, Hub and Spoke, Draft Rosen

1. Konfigurácia L3 VPN sa uskutočňuje na:
A. Customer Edge smerovačoch
B. Provider Edge smerovačoch +
C. Customer Edge aj Provider Edge smerovačoch
D. Route Reflector smerovači

2. Ako vieme zabezpečiť situáciu, kedy viacerí zákazníci používajú rovnaké privátne rozsahy?
A. Nastavíme každému zákazníkovi rôzny Route Target pre export
B. Nastavíme každému zákazníkovi rôzny Route Target pre import
C. Nastavíme každému zákazníkovi rôzny Route Target pre import aj export +
D. Nastavíme každému zákazníkovi rôzny Route Distinguisher

3. Čo potrebujeme spraviť pri L3 VPN na Customer Edge smerovačoch, pokiaľ má zákazník pripojené ku providerovi viaceré pobočky s rovnakým číslom AS?
A. Vypnúť LDP
B. Nastaviť odlišný Route Target pre každú pobočku
C. Zmeniť Route Distinguisher
D. Nastaviť AS-Override +

4. Prečo pri Hub & Spoke VPN musíme mať odlišné Route Targety pre import a export?
A. Aby sme zbytočne nezahlcovali linky
B. Aby sa privátne adresy importovali na Hub smerovač +
C. Aby Hub smerovač mohol plniť funkciu Route Reflectora
D. Aby sme vytvorili záložnú cestu v prípade výpadku primárnej linky

5. Aký typ PIM módu sa používa pri Draft Rosen?

A. Sparse Mode +
B. Dense Mode
C. Sparse-Dense Mode
D. BSR