**ŽILINSKÁ UNIVERZITA V ŽILINE**

**Fakulta riadenia a informatiky**

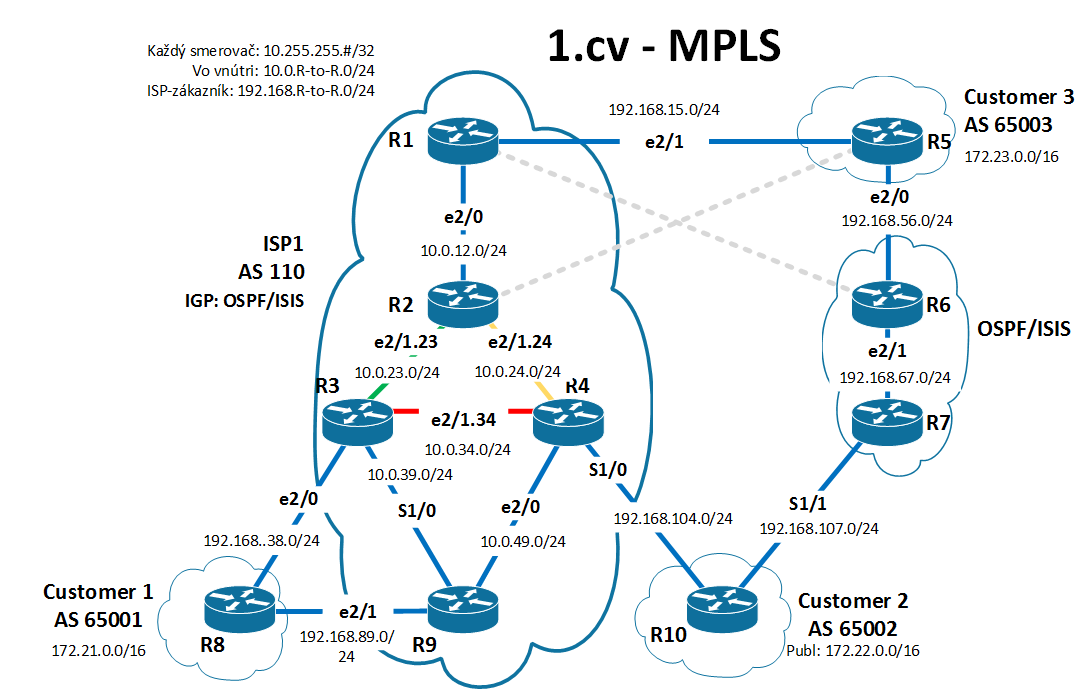
**Projektovanie sietí 1**

**MPLS**

**Akademický rok Andrej Kováč 2015/2016 Pavol Tuka 5ZKS11**

**Cvičenie 1 – Protokol MPLS**

**Topológia a adresovanie**

**** V tejto topológii sme smerovače R6 a R7 vôbec nepoužívali. Vo vnútri AS 110 sme použili smerovací protokol IS-IS.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **R1** | lo0 | 10.255.255.1 | **R4** | e2/1.34 | 10.0.34.4 |
| e2/0 | 10.0.12.1 | s1/0 | 192.168.104.4 |
| e2/1 | 192.168.15.1 | **R5** | lo0 | 10.255.255.5 |
| **R2** | lo0 | 10.255.255.2 | e2/0 | 192.168.56.5 |
| e2/0 | 10.0.12.2 | e2/1 | 192.168.15.5 |
| e2/1.23 | 10.0.23.2 | **R8** | lo0 | 10.255.255.8 |
| e2/1.24 | 10.0.24.2 | e2/0 | 192.168.38.8 |
| **R3** | lo0 | 10.255.255.3 | e2/1 | 192.168.89.8 |
| e2/0 | 192.168.38.3 | **R9** | lo0 | 10.255.255.9 |
| e2/1.23 | 10.0.23.3 | e2/0 | 10.0.49.9 |
| e2/1.34 | 10.0.34.3 | e2/1 | 192.168.89.9 |
| s1/0 | 10.0.39.3 | s1/0 | 10.0.39.9 |
| **R4** | lo0 | 10.255.255.4 | **R10** | lo0 | 10.255.255.10 |
| e2/0 | 10.0.49.4 | s1/0 | 192.168.104.10 |
| e2/1.24 | 10.0.24.4 | s1/1 | 192.168.107.10 |

**Konfigurácia IS-IS**

Tento protokol sme už konfigurovali a zdokumentovali na predošlom cvičení, takže uvedieme len stručný popis konfigurácie.

Bolo potrebné vypracovať L2 adresovanie, ktoré podľa už známych pravidiel obsahuje:

* AFI – hodnota 49 pre privátne domény
* AREA\_ID – číslo oblasti
* SYSTEM\_ID – je vypočítané z ip adresy rozhrania loopback0 na smerovači
* NSEL – defaultne 00

Adresy smerovačov v našej topológii:

|  |  |
| --- | --- |
| **R1** | 49.0001.0102.5525.5001.00 |
| **R2** | 49.0001.0102.5525.5002.00 |
| **R3** | 49.0001.0102.5525.5003.00 |
| **R4** | 49.0001.0102.5525.5004.00 |
| **R9** | 49.0001.0102.5525.5009.00 |

Konfiguračné príkazy pre IS-IS (na smerovačoch R1, R2, R3, R4, R9):

R1(config)#router isis

R1(config-router)#net 49.0002.0102.5525.5001.00

R1(config)#interface e2/0

R1(config-if)#ip router isis

R1(config-if)#isis network point-to-point

R1(config)#interface l0

R1(config-if)#ip router isis

Správnu konfiguráciu overíme zobrazením IS-IS databázy – vidíme v nej všetky smerovače, na ktorých beží protokol IS-IS.

R1#sh isis database

IS-IS Level-2 Link State Database:

LSPID LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL

**R1**.00-00 \* 0x000005AE 0xD719 1187 0/0/0

**R2**.00-00 0x000005B0 0x1457 754 0/0/0

**R3**.00-00 0x000005AF 0x154B 617 0/0/0

**R4**.00-00 0x000005AD 0xDF7E 1177 0/0/0

**R9**.00-00 0x000005AB 0xF0A9 381 0/0/0

**MPLS a LDP**

Konfigurácia MPLS pozostáva len z nasledujúcich 4 príkazov na smerovačoch v AS 110 (R1, R2, R3, R4, R9):

R1(config)#ip cef !cisco express forwarding

R1(config)#mpls label protocol ldp !LDP pre výmenu návestí

R1(config)#mpls ip !globálne zapnutie MPLS

R1(config-if)#mpls ip !zapnutie MPLS na rozhraniach

Príkaz mpls ip sa použije len na na rozhraniach smerujúcich na susedné smerovače vo vnútri AS 110, na loopbackoch nie. Ešte bolo potrebné nastaviť LDP router-id na loopback každého smerovača:

R1(config-if)#mpls ldp router-id lo0 force

Konfiguráciu overíme výpisom *sh mpls ldp discovery*, kde je vidieť, že LDP router-id sa nastavil ako adresa loopback0 (tak isto vidíme aj suseda R2) a *sh mpls forwarding-table*, kde je značkovanie jednotlivých trás:

R1#sh mpls ldp discovery

Local LDP Identifier:

**10.255.255.1**:0

Discovery Sources:

Interfaces:

Ethernet2/0 (ldp): xmit/recv

LDP Id: **10.255.255.2**:0

R1#sh mpls forwarding-table

Local Outgoing Prefix Bytes Label Outgoing Next Hop

Label Label or Tunnel Id Switched interface

**16 Pop Label** 10.255.255.2/32 0 Et2/0 10.0.12.2

**17 Pop Label** 10.0.23.0/24 0 Et2/0 10.0.12.2

**18 Pop Label** 10.0.24.0/24 0 Et2/0 10.0.12.2

**19 17** 10.255.255.3/32 0 Et2/0 10.0.12.2

**20 18** 10.0.34.0/24 0 Et2/0 10.0.12.2

**21 19** 10.0.39.0/24 0 Et2/0 10.0.12.2

**22 20** 10.255.255.9/32 0 Et2/0 10.0.12.2

**23 21** 10.0.49.0/24 0 Et2/0 10.0.12.2

**24 22** 10.255.255.4/32 0 Et2/0 10.0.12.2

Aby sme zabezpečili konektivitu zákazníkov R5, R8 a R10, je potrebné na týchto smerovačoch nakonfigurovať BGP a spojiť ich s poskytovateľom ISP1, teda AS 110. Tak isto je potrebné ohlasovať siete zákazníkov, ktoré sú v našej topológii na loopbackoch týchto smerovačov. Konfigurácia na R5 vyzerá nasledovne (na R8 a R10 je obdobná):

R5(config)#router bgp 65003

R5(config-router)#neighbor 192.168.15.1 remote-as 110

R5(config-router)#address-family ipv4 unicast

R5(config-router-af)#neighbor 192.168.15.1 activate

R5(config-router-af)#network 10.255.255.5 mask 255.255.255.255

Teraz by v BGP tabuľke malo byť vidieť všetky smerovače. Na výpis je potrebné použiť správny príkaz *sh ip bgp ipv4 unicast*.

R1#sh ip bgp ipv4 unicast

Network Next Hop Metric LocPrf Weight Path

\*> 10.255.255.1/32 0.0.0.0 0 32768 i

r>i 10.255.255.2/32 10.255.255.2 0 100 0 i

r>i 10.255.255.3/32 10.255.255.3 0 100 0 i

r>i 10.255.255.4/32 10.255.255.4 0 100 0 i

\*> **10.255.255.5/32 192.168.15.5 0 0 65003 i**

\*>i **10.255.255.8/32 10.255.255.3 0 100 0 65001 i**

r>i 10.255.255.9/32 10.255.255.9 0 100 0 i

\*>i **10.255.255.10/32 10.255.255.4 0 100 0 65002 i**

Overiť konektivitu zákazníkov môžeme prostredníctvom traceroute-u, ktorý zobrazí aj MPLS značku. Otestovali sme trasu zo smerovača R5 na R8.

R5#traceroute 10.255.255.8 source l0

Tracing the route to 10.255.255.8

1 192.168.15.1 24 msec 56 msec 12 msec

2 10.0.12.2 **[MPLS: Label 17 Exp 0]** 88 msec 76 msec 80 msec

3 10.0.23.3 48 msec 38 msec 64 msec

4 192.168.38.8 88 msec \* 96 msec

**Konfigurácia Route reflectora**

V rámci AS 110 sme sa rozhodli ako Route reflector nakonfigurovať smerovač R2. To zabezpečí, že z full-mesh topológie sa stane hup-and-spoke, kde R2 bude vystupovať ako hub a R1, R3, R4 a R9 ako spoke-y. Route reflector je BGP smerovač, ktorý obchádza pravidlo, že cez iBGP sa nesmie odovzdávať informácia, ktorá bola naučená práve cez iBGP.

Na smerovačoch R1, R3, R4 a R9 bolo treba najprv nadviazať BGP susedstvo s R2:

R1(config)#router bgp 110

R1(config-router)#neighbor 10.255.255.2 remote-as 110

R1(config-router)#neighbor 10.255.255.2 update-source Loopback0

R1(config-router)#address-family ipv4 unicast

R1(config-router-af)#neighbor 10.255.255.2 activate

R1(config-router-af)#neighbor 10.255.255.2 next-hop-self

R1(config-router-af)#network 10.255.255.1 mask 255.255.255.255

Následne smerovač R2 nastavíme ako Route reflector. Pre zjednodušenie konfigurácie susedstiev sme použili peer-group.

R2(config)#router bgp 110

R2(config-router)#neighbor PEERS peer-group

R2(config-router)#neighbor PEERS remote-as 110

R2(config-router)#neighbor PEERS update-source l0

R2(config-router)#neighbor 10.255.255.1 peer-group PEERS

R2(config-router)#neighbor 10.255.255.3 peer-group PEERS

R2(config-router)#neighbor 10.255.255.4 peer-group PEERS

R2(config-router)#neighbor 10.255.255.9 peer-group PEERS

R2(config-router)#address-family ipv4 unicast

R2(config-router-af)#neighbor PEERS **route-reflector-client**

R2(config-router-af)#neighbor PEERS next-hop-self

Susedov v peer-group už aktivovať nemusíme, sú aktivovaní automaticky.

Správnosť konfigurácie a plnú konektivitu overíme pingom na všetky aktívne smerovače v topológii (z R1) 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

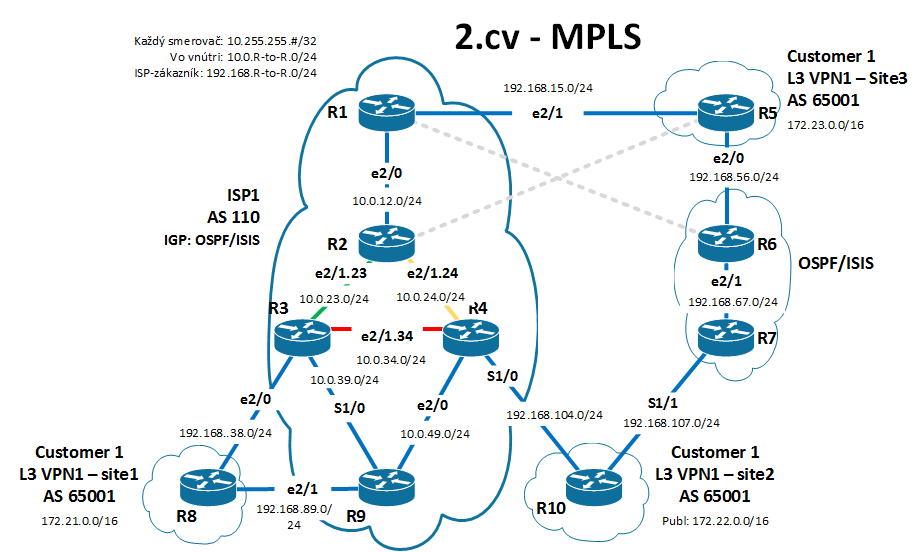
Sending 5, 100-byte ICMP Echos to 10.255.255.10, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 72/79/100 ms

**Cvičenie 2 – Protokol MPLS**

**Topológia a adresovanie**

Topológia bola pozmenená tak, že všetci traja zákazníci sa nachádzajú v tom istom AS 65001.

Adresovanie ostáva rovnaké, len zákazníkom 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 |

**Konfigurácia VRF**

Na prepojenie týchto zákazníkov sme použili VPN. Preto sme na smerovačoch v rámci AS 110 (R1, R3, R4, R9) zapli VRF (Virtual Routing Instance) pre všetkých zákazníkov. Na vytvorenie unikátnej VPN cesty bolo potrebné definovať Route Distingusher (RD) a Route Target (RT).

R1(config)#ip vrf z1

R1(config-vrf)#rd 110:1

R1(config-vrf)#route-target 110:1

Túto VRF je potom potrebné priradiť všetkým rozhraniam, ktoré smerujú k zákazníkom, teda na R1 smerom k R5, na R9 k R8 a na R4 k R10.

R1(config)#interface Ethernet2/1

R1(config-if)#ip vrf forwarding z1

Zadaním tohto príkazu sa presunie záznam z globálnej smerovacej tabuľky do smerovacej tabuľky vrf z1 ale zároveň sa z rozhrania odstráni IP adresa, takže po jeho zadaní je potrebné na ňom ju nanovo zadať. Pridanie rozhrania do danej VRF overíme príkazom *sh ip vrf*.

R1#sh ip vrf

Name Default RD Interfaces

**z1 110:1 Et2/1**

Smerovač R1 bude slúžiť ako route reflector, pričom tentoraz použijeme address-family vpnv4. Konfigurácia teda bude vyzerať takto:

R1(config)#router bgp 110

R1(config-router)#no bgp default ipv4-unicast

R1(config-router)#neighbor PEERS peer-group

R1(config-router)#neighbor PEERS remote-as 110

R1(config-router)#neighbor PEERS update-source Loopback0

R1(config-router)#neighbor 10.255.255.2 peer-group PEERS

R1(config-router)#neighbor 10.255.255.3 peer-group PEERS

R1(config-router)#neighbor 10.255.255.4 peer-group PEERS

R1(config-router)#neighbor 10.255.255.9 peer-group PEERS

R1(config-router)#neighbor 192.168.15.5 remote-as 65001

R1(config-router)#address-family vpnv4

R1(config-router-af)#neighbor PEERS send-community extended

R1(config-router-af)#neighbor PEERS route-reflector-client

R1(config-router-af)#neighbor 10.255.255.3 activate

R1(config-router-af)#neighbor 10.255.255.4 activate

R1(config-router-af)#neighbor 10.255.255.9 activate

R1(config-router-af)#neighbor 10.255.255.2 activate

Na smerovačoch R2, R3, R4, R9 použijeme tieto príkazy:

R3(config)#router bgp 110

R3(config-router)#no bgp default ipv4-unicast

R3(config-router)#neigbor 10.255.255.1 remote-as 110

R3(config-router)#neigbor 10.255.255.1 update-source Lo0

R3(config-router)#address-family vpnv4

R3(config-router-af)#neighbor 10.255.255.1 activate

Následne bolo potrebné nadviazať BGP susedstvá medzi PE smerovačmi v AS 110 a CE smerovačmi v zákazníckom AS 65001 a to pomocou VRF nasledovne:

R1(config)#router bgp 110

R1(config-router)#address-family ipv4 vrf z1

R1(config-router-af)#neighbor 192.168.15.5 remote-as 65001

R1(config-router-af)#neighbor 192.168.15.5 activate

R1(config-router-af)#neighbor 192.168.15.5 as-override

R1(config-router-af)#redistribute connected

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 všetkých troch (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(config)#no router bgp 65003

R8(config)#no router bgp 65001

R10(config)#no router bgp 65002

R5(config)#router bgp 65001

R5(config-router)#address-family ipv4 unicast

R5(config-router-af)#network 10.255.255.5 mask 255.255.255.255

R5(config-router-af)#network 172.23.0.0 mask 255.255.255.0

R5(config-router-af)#neighbor 192.168.15.1 activate

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

R5#sh ip bgp ipv4 unicast

Network Next Hop Metric LocPrf Weight Path

**\*> 10.255.255.5/32 0.0.0.0 0 32768 i**

**\*> 10.255.255.8/32 192.168.15.1 0 110 110 i**

**\*> 10.255.255.10/32 192.168.15.1 0 110 110 i**

**\*> 172.21.0.0 192.168.15.1 0 110 110 i**

**\*> 172.22.0.0 192.168.15.1 0 110 110 i**

**\*> 172.23.0.0 0.0.0.0 0 32768 i**

r> 192.168.15.0 192.168.15.1 0 0 110 ?

\*> 192.168.38.0 192.168.15.1 0 110 ?

\*> 192.168.89.0 192.168.15.1 0 110 ?

\*> 192.168.104.0 192.168.15.1 0 110 ?

Ďalším spôsobom overenia je traceroute, napr. z loopbackovej zákazníckej siete smerovača R5 na zákaznícku sieť R10.

R5#traceroute 172.22.0.1 source 172.23.0.1

Type escape sequence to abort.

Tracing the route to 172.22.0.1

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

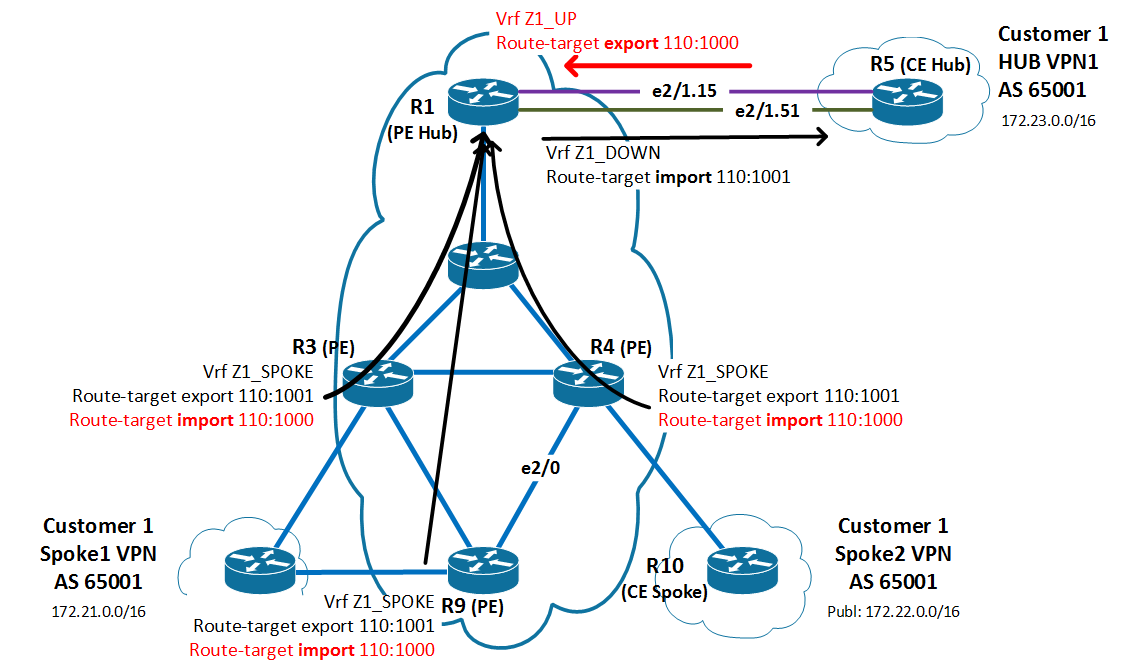
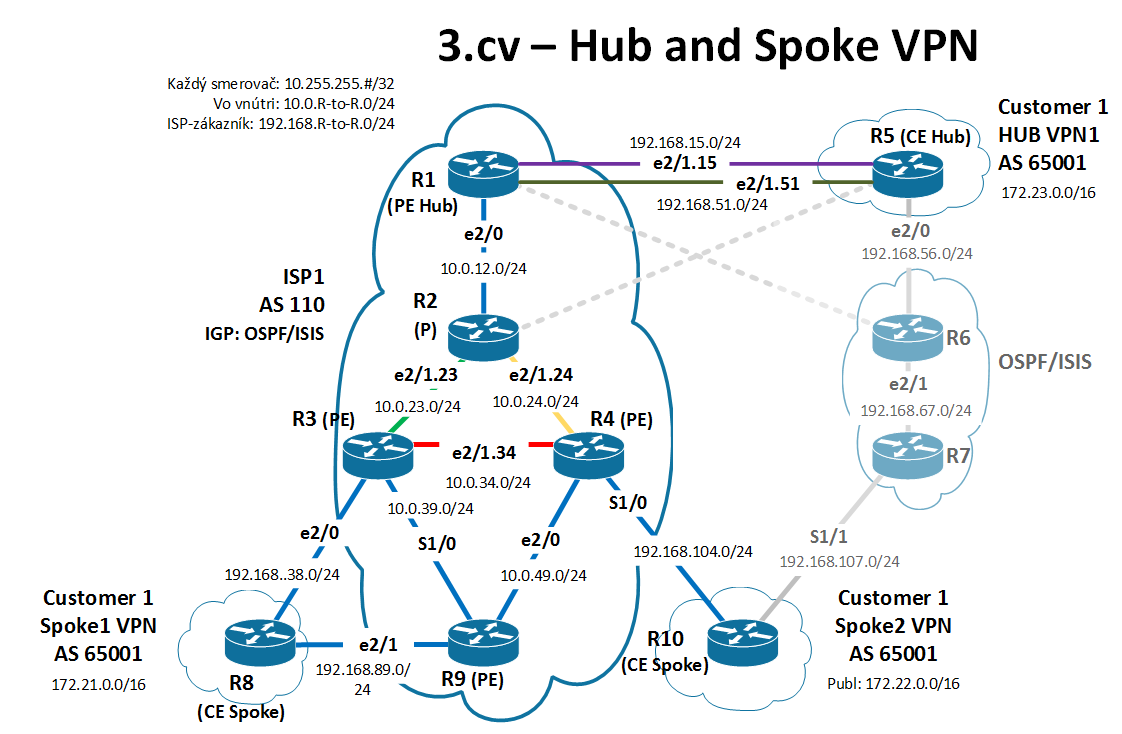
1 192.168.15.1 [AS 110] 60 msec 28 msec 20 msec

2 10.0.12.2 [MPLS: Labels 22/24 Exp 0] 84 msec 100 msec 84 msec

3 192.168.104.4 [AS 110] [MPLS: Label 24 Exp 0] 56 msec 44 msec 56 msec

4 192.168.104.10 [AS 110] 96 msec 100 msec \*

**Cvičenie 3 – Hub and Spoke VPN**

**Topológia**

**Konfigurácia**

Úlohou bolo zmeniť predošlú konfiguráciu tak, aby smerovač R1 bol hubom pre ostatné PE smerovače a R5 hubom pre zákaznícke CE smerovače. Medzi týmito dvomi smerovačmi v topológii tiež pribudla linka, avšak fyzickú máme k dispozícii len jednu. Tým pádom je nutné fyzické rozhranie e2/1 rozdeliť na dve subrozhrania a na nich vytvoriť dve samostatné VRF pre import a export. Predtým sme však museli odstrániť staré VRF z predošlých cvičení, príkazom *no ip vrf z1*.

Zákaznícke vrf pre export a import:

R1(config)#ip vrf z1\_DOWN

R1(config-vrf)#rd 110:2

R1(config-vrf)#route-target import 110:1001

R1(config)#ip vrf z1\_UP

R1(config-vrf)#rd 110:1

R1(config-vrf)#route-target export 110:1000

Konfigurácia subrozhraní:

R1(config)#interface Ethernet2/1

R1(config-if)#no ip address

R1(config)#interface Ethernet2/1.15

R1(config-subif)#encapsulation dot1Q 15

R1(config-subif)#ip vrf forwarding z1\_DOWN

R1(config-subif)#ip address 192.168.15.1 255.255.255.0

R1(config-subif)#interface Ethernet2/1.51

R1(config-subif)#encapsulation dot1Q 51

R1(config-subif)#ip vrf forwarding z1\_UP

R1(config-subif)#ip address 192.168.51.1 255.255.255.0

Konfigurácia BGP, address-family vrf pre import a export:

R1(config)#router bgp 110

R1(config-router)#address-family ipv4 vrf z1\_DOWN

R1(config-router-as)#neighbor 192.168.51.5 remote-as 65001

R1(config-router-as)#neighbor 192.168.51.5 activate

R1(config-router-as)#neighbor 192.168.51.5 as-override

R1(config-router)#address-family ipv4 vrf z1\_UP

R1(config-router-as)#redistribute static

R1(config-router-as)#neighbor 192.168.15.5 remote-as 65001

R1(config-router-as)#neighbor 192.168.15.5 activate

R1(config-router-as)#neighbor 192.168.15.5 as-override

R1(config-router-as)#default-information originate

Treba nastaviť aj defaultnú cestu, aby komunikácia smerovala na hub. Distribuovať sa bude príkazmi *redistribute static* a *default-information originate*.

R1(config)#ip route vrf z1\_UP 0.0.0.0 0.0.0.0 192.168.15.5

Subrozhrania sme zamozrejme podobne nastavili aj na smerovači R5.

Zákaznícku VRF pre spoke smerovače bolo potrebné nakonfigurovať na ostatných okrajových PE smerovačoch (R3, R4, R9) a to nasledovne:

R4(config)#ip vrf z1\_spoke

R4(config-vrf)#rd 110:1

R4(config-vrf)#route-target export 110:1001

R4(config-vrf)#route-target import 110:1000

R4(config)#interface Ethernet2/0

R4(config-if)#ip vrf forwarding z1\_spoke

R4(config-if)#ip address 192.168.38.3 255.255.255.0

R4(config)#router bgp 110

R4(config-router)#address-family ipv4 vrf z1\_spoke

R4(config-router-af)#neighbor 192.168.38.8 remote-as 65001

R4(config-router-af)#neighbor 192.168.38.8 activate

R4(config-router-af)#neighbor 192.168.38.8 as-override

Konfiguráciu overíme traceroute-om zo smerovača R8 na R10 kde vidíme, že prevádzka je smerovaná cez hub smerovač R5.

R8#traceroute 172.22.0.1 source 172.21.0.1

Type escape sequence to abort.

Tracing the route to 172.22.0.1

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

1 192.168.89.9 [AS 110] 42 msec 38 msec 32 msec

2 10.0.39.3 [AS 110] [MPLS: Labels 20/24 Exp 0] 224 msec 82 msec 112 msec

3 10.0.23.2 [AS 110] [MPLS: Labels 21/24 Exp 0] 86 msec 224 msec 148 msec

4 **192.168.15.1** [AS 110] [MPLS: Label 24 Exp 0] 182 msec 216 msec 86 msec

5 **192.168.15.5** [AS 110] 120 msec 112 msec 136 msec

6 **192.168.51.1** [AS 110] 84 msec 114 msec 124 msec

7 10.0.12.2 [AS 110] [MPLS: Labels 22/25 Exp 0] 252 msec \* 220 msec

8 \*

192.168.104.4 [AS 110] [MPLS: Label 25 Exp 0] 222 msec 236 msec

9 192.168.104.10 [AS 110] 208 msec \* 242 msec

**Cvičenie 4 – Draft Rosen**

V rámci tohto cvičenia bolo potrebné nastaviť multicast cez VPN, tzv. Draft Rosen koncept. Pre lepšiu viditeľnosť a komunikáciu uzlov v sieti sme sa rozhodli vrátiť do stavu z druhého cvičenia, kde sme nemali Hub and Spoke topológiu ale mali sme troch zákazníkov z AS 65001 prepojených pomocou VPN.

Ukážka konfigurácie na smerovači R1:

R1(config)#ip multicast-routing

R1(config)#interface Loopback0

R1(config-if)#ip pim sparse-mode

R1(config)#interface Ethernet2/0

R1(config-if)#ip pim sparse-mode

R1(config)#interface Ethernet2/1

R1(config-if)#ip pim sparse-mode

R1(config)#ip pim rp-address 10.255.255.1

Rovnakú konfiguráciu treba aplikovať aj na ostatné smerovače s tým, že adresa RP (Randevous Point) bude pre smerovače PE adresa smerovača R1 10.255.255.1 a pre smerovače CE to bude adresa Lo1 smerovača R5 172.23.0.1.

Na okrajových PE smerovačoch (R1, R3, R4) bolo potrebné zadať nasledovný príkaz pre smerovanie na VRF:

R1(config)#ip multicast-routing vrf z1

A taktiež bolo treba pridať do zákazníckej VRF z1 nasledovný príkaz pre vyhradenie multicastovej skupiny:

R1(config)#ip vrf z1

R1(config-vrf)#mdt default 233.3.3.3

Na týchto okrajových smerovačoch bolo taktiež treba zadať nasledovný príkaz pre nastavenie RP zákazníckej VRF:

R1(config)#ip pim vrf Z1 rp-address 172.23.0.1

Následne bolo potrebné pre overenie funkčnosti, požiadať o pridelenie smerovača do multicastovej skupiny. Na smerovači R8 sme požiadali o vstup do multicastovej skupiny 239.1.1.1 nasledovne:

R8(config)#interface Lo10

R8(config-if)#ip igmp join-group 239.1.1.1

R8#sh ip igmp groups

IGMP Connected Group Membership

Group Address Interface Uptime Expires Last Reporter Group Accounted

**239.1.1.1 Loopback1 1w0d never 172.21.0.1**

224.0.1.40 Ethernet2/1 1w0d 00:02:58 192.168.89.9

224.0.1.40 Ethernet2/0 1w0d 00:02:35 192.168.38.8

Následné overenie bolo riešené pingom zo strany zákazníka na multicastovú skupinu. Do multicastovej skupiny sme priradili smerovač R8 aj smerovač R10, preto vo výpise vidíme dve odpovede.

R5#ping 239.1.1.1 source Lo1 repeat 5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 239.1.1.1, timeout is 2 seconds:

**Reply to request 0 from 172.21.0.1, 84 ms**

**Reply to request 0 from 172.22.0.1, 88 ms**

Reply to request 1 from 172.22.0.1, 88 ms

Reply to request 1 from 172.21.0.1, 88 ms

Reply to request 2 from 172.22.0.1, 88 ms

Reply to request 2 from 172.21.0.1, 88 ms

Reply to request 3 from 172.22.0.1, 88 ms

Reply to request 3 from 172.21.0.1, 88 ms

Reply to request 4 from 172.22.0.1, 88 ms

Reply to request 4 from 172.21.0.1, 88 ms

Na nasledovnom výpise môžeme vidieť zdroj pre danú multicastovú skupinu (239.1.1.1) je smerovač R5 s IP adresou rozhrania 192.168.15.5. Následná komunikácia prebieha cez rozhranie Tunnel3, pretože Draft-Rosen využíva GRE tunelovanie.

R1#sh ip route vrf z1 239.1.1.1

IP Multicast Routing Table

Flags: D - Dense, S - Sparse, ...

Outgoing interface flags: H - Hardware switched, A - Assert winner

Timers: Uptime/Expires

Interface state: Interface, Next-Hop or VCD, State/Mode

**(\*, 239.1.1.1)**, 00:16:42/00:02:46, RP 172.23.0.1, flags: S

Incoming interface: Ethernet2/1, RPF nbr 192.168.15.5

Outgoing interface list:

**Tunnel3, Forward/Sparse**, 00:11:58/00:02:50

**(192.168.15.5, 239.1.1.1)**, 00:13:25/00:03:29, flags: T

Incoming interface: Ethernet2/1, RPF nbr 192.168.15.5

Outgoing interface list:

**Tunnel3, Forward/Sparse**, 00:10:24/00:02:32