**ŽILINSKÁ UNIVERZITA V ŽILINE**

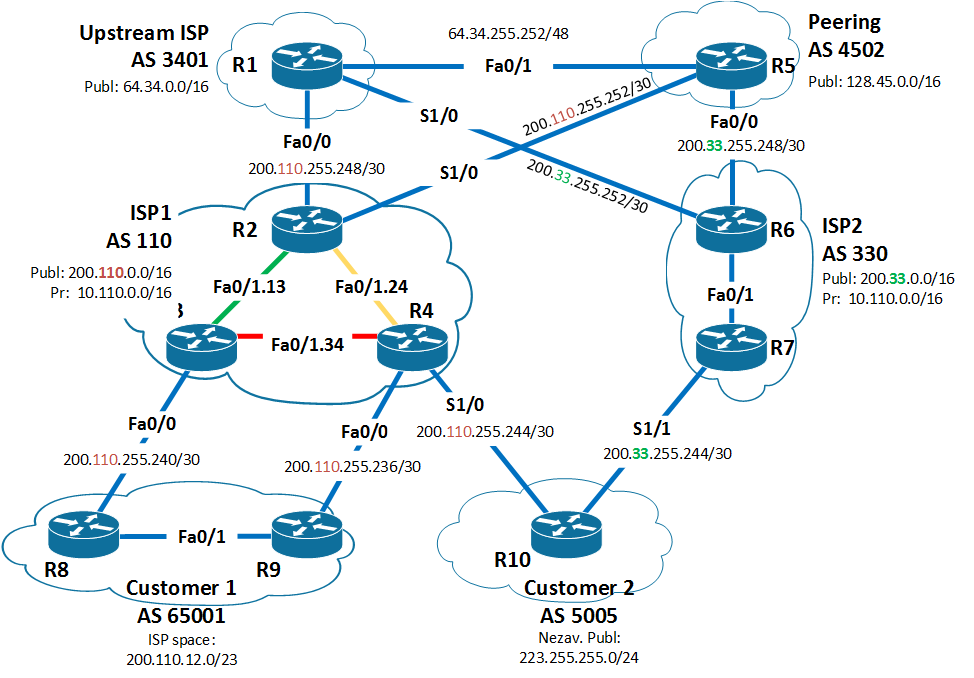
**Fakulta riadenia a informatiky**

**Projektovanie sietí 1**

**BGP**

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

**Topológia a adresovanie**



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **R1** | lo0 | 10.255.255.1 | **R6** | lo0 | 10.255.255.6 |
| lo1 | 64.34.1.1 | lo1 | 200.33.6.1 |
| fa0/0 | 200.110.255.249 | fa0/0 | 200.33.255.250 |
| fa0/1 | 64.34.255.253 | fa0/1 | 10.110.67.6 |
| s1/0 | 200.33.255.253 | s1/0 | 200.33.255.254 |
| **R2** | lo0 | 10.255.255.2 | **R7** | lo0 | 10.255.255.7 |
| lo1 | 200.110.2.1 | lo1 | 200.33.7.1 |
| fa0/0 | 200.110.255.250 | fa0/1 | 10.110.67.7 |
| fa0/1.23 | 10.110.23.2 | s1/1 | 200.33.255.245 |
| fa0/1.24 | 10.110.24.2 | **R8** | lo0 | 10.255.255.8 |
| s1/0 | 200.110.255.253 | lo1 | 200.110.12.1 |
| **R3** | lo0 | 10.255.255.3 | fa0/0 | 200.110.255.242 |
| lo1 | 200.110.3.1 | fa0/1 | 10.110.89.8 |
| fa0/0 | 200.110.255.241 | **R9** | lo0 | 10.255.255.9 |
| fa0/1.23 | 10.110.23.3 | lo1 | 200.110.13.1 |
| fa0/1.34 | 10.110.34.3 | fa0/0 | 200.110.255.238 |
| **R4** | lo0 | 10.255.255.4 | fa0/1 | 10.110.89.9 |
| lo1 | 200.110.4.1 | **R10** | lo0 | 10.255.255.10 |
| fa0/0 | 200.110.255.237 | lo1 | 223.255.255.1 |
| fa0/1.24 | 10.110.24.4 | s1/0 | 200.110.255.246 |
| fa0/1.34 | 10.110.34.4 | s1/1 | 200.33.255.246 |
| s1/0 | 200.110.255.245 |  | | |
| **R5** | lo0 | 10.255.255.5 |
| lo1 | 128.45.5.1 |
| fa0/0 | 200.33.255.249 |
| fa0/1 | 64.34.255.254 |
| s1/0 | 200.110.255.254 |

**Použiť IGP OSPF single area dizajn, priame p2p prepojenia – ISP1, ISP2**

Ako IGP sme použili protokol OSPF so single area dizajnom - area 0. Všetky priame linky v sieti ISP1 a ISP2 sme nastavili ako bod-bod pomocou príkazu ip ospf network point-to-point na príslušných rozhraniach smerovačov R2-R3-R4, R6-R7, R8-R9. Z nasledujúcich výpisov sme odstránili nadbytočné riadky - sériové rozhrania, ktoré sú vždy typu bod-bod a loopbacky.

R2#sh ip ospf interface brief

Interface PID Area IP Address/Mask Cost State Nbrs F/C

Fa0/0 1 0 200.110.255.250/30 10 **P2P**  0/0

Fa0/1.24 1 0 10.110.24.2/24 10 **P2P**  1/1

Fa0/1.23 1 0 10.110.23.2/24 10 **P2P**  1/1

R3#sh ip ospf interface brief

Interface PID Area IP Address/Mask Cost State Nbrs F/C

Fa0/0 1 0 200.110.255.241/30 10 **P2P**  0/0

Fa0/1.34 1 0 10.110.34.3/24 10 **P2P**  1/1

Fa0/1.23 1 0 10.110.23.3/24 10 **P2P**  1/1

R4#sh ip ospf interface brief

Interface PID Area IP Address/Mask Cost State Nbrs F/C

Fa0/0 1 0 200.110.255.237/30 10 **P2P**  0/0

Fa0/1.34 1 0 10.110.34.4/24 10 **P2P**  1/1

Fa0/1.24 1 0 10.110.24.4/24 10 **P2P**  1/1

R6#sh ip ospf interface brief

Interface PID Area IP Address/Mask Cost State Nbrs F/C

Fa0/0 1 0 200.33.255.250/30 10 **P2P**  0/0

Fa0/1 1 0 10.110.67.6/24 10 **P2P** 1/1

R7#sh ip ospf interface brief

Interface PID Area IP Address/Mask Cost State Nbrs F/C

Fa0/1 1 0 10.110.67.7/24 10 **P2P**  1/1

R8#sh ip ospf interface brief

Interface PID Area IP Address/Mask Cost State Nbrs F/C

Fa0/0 1 0 200.110.255.242/30 10 **P2P**  0/0

Fa0/1 1 0 10.110.89.8/24 10 **P2P**  1/1

R9#sh ip ospf interface brief

Interface PID Area IP Address/Mask Cost State Nbrs F/C

Fa0/0 1 0 200.110.255.238/30 10 **P2P**  0/0

Fa0/1 1 0 10.110.89.9/24 10 **P2P**  1/1

**Zabezpečiť plnú konektivitu prostredníctvom iBGP alebo eBGP protokolov pre zákaznícké a internetové smerovacie záznamy**

Ako IGP sme použili OSPF, ktorý ohlasoval privátne siete v rámci svojho autonómneho systému a takisto verejné siete smerujúce von/dnu z/do AS. Pre konektivitu medzi AS sme použili externý protokol eBGP.

Príkaz na aktivovanie BGP je *router bgp <číslo AS>*, susedov pridáme príkazom *neighbor <IP adresa susedovho rozhrania> remote-as <číslo susedného AS>*. Tie príkazy bolo potrebné zadať na všetkých smerovačoch. V rámci jedného AS je protokol automaticky iBGP, avšak ako IP adresu suseda použijeme adresu jeho Loopbacku a pridáme príkaz *neighbor <IP adresa susedovho Loopbacku> update-source Loopback0*. Ohlasovanie vlastných sietí zabezpečíme príkazom *network <IP siete> mask <maska siete>*. Ako príklad uvedieme konfiguráciu na smerovačoch R10 a R2 (len v rámci AS 110):

R10(config)#router bgp 5005

R10(config-router)#network 223.255.255.0 mask 255.255.255.0

R10(config-router)#neighbor 200.110.255.245 remote-as 110

R10(config-router)#neighbor 200.33.255.245 remote-as 330

R2(config)#router bgp 110

R2(config-router)#network 200.110.2.0 mask 255.255.255.0

R2(config-router)#neighbor 10.255.255.3 remote-as 110

R2(config-router)#neighbor 10.255.255.3 update-source Loopback0

R2(config-router)#neighbor 10.255.255.4 remote-as 110

R2(config-router)#neighbor 10.255.255.4 update-source Loopback0

Plná konektivita bola overená - výpisy nižšie v časti *Kontrola konektivity*.

**Kontrola, či interné ISP adresy nie sú propagované**

Aby sme zabránili propagovaniu interných IP adries mimo vlastných AS, nastavili sme v OSPF pomocou príkazu passive-interface id\_rozhrania všetky rozhrania, ktoré smerujú von/dnu z/do AS ako pasívne. Ako overenie poskytneme výpis sh ip route zo smerovačov R4, R6 a R10, na ktorých si môžete všimnúť, že všetky interné siete (napr. 10.110.0.0/16, ktoré používa ISP1 aj ISP2) sú viditeľné iba s označením C - teda priamo pripojené a teda nikde nie sú šírené pomocou nejakého smerovacieho protokolu.

R4#sh ip route

C 200.110.4.0/24 is directly connected, Loopback1

B 223.255.255.0/24 [20/0] via 200.110.255.246, 3d12h

64.0.0.0/24 is subnetted, 1 subnets

B 64.34.1.0 [200/0] via 200.110.255.249, 03:47:46

200.110.255.0/30 is subnetted, 5 subnets

O 200.110.255.248 [110/20] via 10.110.24.2, 03:32:52, FastEthernet0/1.24

O 200.110.255.252 [110/74] via 10.110.24.2, 03:32:52, FastEthernet0/1.24

O 200.110.255.240 [110/20] via 10.110.34.3, 03:32:52, FastEthernet0/1.34

C 200.110.255.244 is directly connected, Serial1/0

C 200.110.255.236 is directly connected, FastEthernet0/0

200.110.2.0/32 is subnetted, 1 subnets

O 200.110.2.1 [110/11] via 10.110.24.2, 03:32:54, FastEthernet0/1.24

200.110.3.0/32 is subnetted, 1 subnets

O 200.110.3.1 [110/11] via 10.110.34.3, 03:33:03, FastEthernet0/1.34

128.45.0.0/24 is subnetted, 1 subnets

B 128.45.5.0 [200/0] via 200.110.255.254, 03:47:19

10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks

O 10.255.255.2/32 [110/11] via 10.110.24.2, 03:33:03, FastEthernet0/1.24

O 10.255.255.3/32 [110/11] via 10.110.34.3, 03:33:03, FastEthernet0/1.34

C 10.255.255.4/32 is directly connected, Loopback0

C 10.110.34.0/24 is directly connected, FastEthernet0/1.34

O 10.110.23.0/24 [110/20] via 10.110.34.3, 03:33:03, FastEthernet0/1.34

[110/20] via 10.110.24.2, 03:33:03, FastEthernet0/1.24

C 10.110.24.0/24 is directly connected, FastEthernet0/1.24

B 200.33.6.0/23 [20/0] via 200.110.255.246, 3d10h

B 200.110.0.0/21 [200/0] via 0.0.0.0, 3d10h, Null0

B 200.110.12.0/23 [20/0] via 200.110.255.238, 3d10h

R6#sh ip route

C 200.33.6.0/24 is directly connected, Loopback1

B 223.255.255.0/24 [20/0] via 200.33.255.249, 1d18h

200.33.7.0/32 is subnetted, 1 subnets

O 200.33.7.1 [110/11] via 10.110.67.7, 00:29:58, FastEthernet0/1

64.0.0.0/24 is subnetted, 1 subnets

B 64.34.1.0 [20/0] via 200.33.255.253, 1d22h

200.33.255.0/30 is subnetted, 3 subnets

O 200.33.255.244 [110/74] via 10.110.67.7, 00:29:58, FastEthernet0/1

C 200.33.255.252 is directly connected, Serial1/0

C 200.33.255.248 is directly connected, FastEthernet0/0

128.45.0.0/24 is subnetted, 1 subnets

B 128.45.5.0 [20/0] via 200.33.255.249, 1d22h

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks

C 10.255.255.6/32 is directly connected, Loopback0

O 10.255.255.7/32 [110/11] via 10.110.67.7, 00:30:01, FastEthernet0/1

C 10.110.67.0/24 is directly connected, FastEthernet0/1

B 200.33.6.0/23 [200/0] via 0.0.0.0, 1d20h, Null0

B 200.110.0.0/21 [20/0] via 200.33.255.249, 1d20h

B 200.110.12.0/23 [20/0] via 200.33.255.249, 1d20h

R10#sh ip route

C 223.255.255.0/24 is directly connected, Loopback1

64.0.0.0/24 is subnetted, 1 subnets

B 64.34.1.0 [20/0] via 200.33.255.245, 1d21h

200.110.255.0/30 is subnetted, 1 subnets

C 200.110.255.244 is directly connected, Serial1/0

200.33.255.0/30 is subnetted, 1 subnets

C 200.33.255.244 is directly connected, Serial1/1

128.45.0.0/24 is subnetted, 1 subnets

B 128.45.5.0 [20/0] via 200.33.255.245, 1d21h

10.0.0.0/32 is subnetted, 1 subnets

C 10.255.255.10 is directly connected, Loopback0

B 200.33.6.0/23 [20/0] via 200.33.255.245, 1d20h

B 200.110.0.0/21 [20/0] via 200.110.255.245, 1d20h

B 200.110.12.0/23 [20/0] via 200.110.255.245, 1d20h

**Prepísať privátne AS65001**

Keďže zákazník 1 patrí pod ISP1, ktorý mu pridelil číslo autonómneho systému 65001, ktoré patrí medzi privátne, je potrebné zaručiť, aby neboli cesty do tohoto AS propagované cez BGP. Preto sme na smerovači R2 na všetky linky smerujúce mimo AS 110 (teda na smerovače R1 a R5) nakonfigurovali odstránenie privátnych AS pomocou prepínača *remove-private-as* na spomínaných susedov. Rovnako sme nakonfigurovali aj linku z prepínača R4 na smerovač R10.

R2(config)#router bgp 110

R2(config-router)#neighbor 200.110.255.249 remove-private-as

R2(config-router)#neighbor 200.110.255.254 remove-private-as

R4(config)#router bgp 110

R4(config-router)#neighbor 200.110.255.246 remove-private-as

Overenie sme urobili pomocou príkazu *show ip bgp* na smerovačoch mimo AS 110 (napr. R5). Privátny AS 65001 sa potom v AS-PATH nenachádza, ako môžeme vidieť v tomto výpise:

|  |
| --- |
| R5#sh ip bgp 200.110.12.0  BGP routing table entry for 200.110.12.0/23, version 14  Paths: (2 available, best #2, table Default-IP-Routing-Table)  Advertised to update-groups:  1  **3401 110**  64.34.255.253 from 64.34.255.253 (64.34.0.1)  Origin IGP, localpref 100, valid, external  **110**  200.110.255.253 from 200.110.255.253 (200.110.2.1)  Origin IGP, localpref 100, valid, external, best |

**Sumarizácia**

Sumarizáciu sme urobili na smerovačoch R2-R3-R4, kde sme agregovali do jednej adresy priestor 200.110.0.0/21. Ďalej na smerovačoch R6-R7 priestor 200.33.6.0/23. A nakoniec aj na smerovačoch R8-R9, kde sme agregovali priestor 200.110.12.0/23. Následne sme na smerovači R10 pozreli smerovacie záznamy, kde sme videli všetky tri agregované/sumarizované cesty. Pri konfigurácii agregácie sme použili aj parameter summary-only, aby sme zabránili šíreniu parciálnych aj sumarizovaných ciest. Znenie príkazu: *aggregate-address <IP siete> <maska siete> summary-only*.

R10#sh ip route

**B 200.33.6.0/23 [20/0] via 200.33.255.245, 1d20h**

**B 200.110.0.0/21 [20/0] via 200.110.255.245, 1d20h**

**B 200.110.12.0/23 [20/0] via 200.110.255.245, 1d20h**

**Kontrola konektivity medzi zákazníckymi a internetovými smerovacími záznamami**

Overenie funkčnosti konektivity v celej sieti sme overili pomocou tcl shell skriptu, ktorým sme poslali ping na IP adresy rozhraní *loopback1* uvedené v adresnej tabuľke zo smerovačov R3, R5 a R8 so zdrojovou IP adresou rozhrania *loopback1*.

R3#tclsh

R3(tcl)#foreach address {

+>(tcl)#64.34.1.1

+>(tcl)#200.110.2.1

+>(tcl)#200.110.3.1

+>(tcl)#200.110.4.1

+>(tcl)#128.45.5.1

+>(tcl)#200.33.6.1

+>(tcl)#200.33.7.1

+>(tcl)#200.110.12.1

+>(tcl)#200.110.13.1

+>(tcl)#223.255.255.1

+>(tcl)#} {ping $address source lo1 timeout 1 repeat 3}

Sending 3, 100-byte ICMP Echos to 64.34.1.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.3.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 40/46/56 ms

Sending 3, 100-byte ICMP Echos to 200.110.2.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.3.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 12/14/16 ms

Sending 3, 100-byte ICMP Echos to 200.110.3.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.3.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 1/1/1 ms

Sending 3, 100-byte ICMP Echos to 200.110.4.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.3.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 16/24/36 ms

Sending 3, 100-byte ICMP Echos to 128.45.5.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.3.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 32/48/76 ms

Sending 3, 100-byte ICMP Echos to 200.33.6.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.3.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 32/85/152 ms

Sending 3, 100-byte ICMP Echos to 200.33.7.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.3.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 84/104/116 ms

Sending 3, 100-byte ICMP Echos to 200.110.12.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.3.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 16/25/32 ms

Sending 3, 100-byte ICMP Echos to 200.110.13.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.3.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 40/52/64 ms

Sending 3, 100-byte ICMP Echos to 223.255.255.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.3.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 36/44/56 ms

R5#tclsh

R5(tcl)#foreach address {

+>(tcl)#64.34.1.1

+>(tcl)#200.110.2.1

+>(tcl)#200.110.3.1

+>(tcl)#200.110.4.1

+>(tcl)#128.45.5.1

+>(tcl)#200.33.6.1

+>(tcl)#200.33.7.1

+>(tcl)#200.110.12.1

+>(tcl)#200.110.13.1

+>(tcl)#223.255.255.1

+>(tcl)#} {ping $address source lo1 timeout 1 repeat 3}

Sending 3, 100-byte ICMP Echos to 64.34.1.1, timeout is 1 seconds:

Packet sent with a source address of 128.45.5.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 8/17/24 ms

Sending 3, 100-byte ICMP Echos to 200.110.2.1, timeout is 1 seconds:

Packet sent with a source address of 128.45.5.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 8/22/32 ms

Sending 3, 100-byte ICMP Echos to 200.110.3.1, timeout is 1 seconds:

Packet sent with a source address of 128.45.5.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 52/53/56 ms

Sending 3, 100-byte ICMP Echos to 200.110.4.1, timeout is 1 seconds:

Packet sent with a source address of 128.45.5.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 52/73/92 ms

Sending 3, 100-byte ICMP Echos to 128.45.5.1, timeout is 1 seconds:

Packet sent with a source address of 128.45.5.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 4/5/8 ms

Sending 3, 100-byte ICMP Echos to 200.33.6.1, timeout is 1 seconds:

Packet sent with a source address of 128.45.5.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 4/26/56 ms

Sending 3, 100-byte ICMP Echos to 200.33.7.1, timeout is 1 seconds:

Packet sent with a source address of 128.45.5.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 24/50/84 ms

Sending 3, 100-byte ICMP Echos to 200.110.12.1, timeout is 1 seconds:

Packet sent with a source address of 128.45.5.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 68/70/72 ms

Sending 3, 100-byte ICMP Echos to 200.110.13.1, timeout is 1 seconds:

Packet sent with a source address of 128.45.5.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 80/110/136 ms

Sending 3, 100-byte ICMP Echos to 223.255.255.1, timeout is 1 seconds:

Packet sent with a source address of 128.45.5.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 56/76/88 ms

R8#tclsh

R8(tcl)#foreach address {

+>(tcl)#64.34.1.1

+>(tcl)#200.110.2.1

+>(tcl)#200.110.3.1

+>(tcl)#200.110.4.1

+>(tcl)#128.45.5.1

+>(tcl)#200.33.6.1

+>(tcl)#200.33.7.1

+>(tcl)#200.110.12.1

+>(tcl)#200.110.13.1

+>(tcl)#223.255.255.1

+>(tcl)#} {ping $address source lo1 timeout 1 repeat 3}

Sending 3, 100-byte ICMP Echos to 64.34.1.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.12.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 80/96/128 ms

Sending 3, 100-byte ICMP Echos to 200.110.2.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.12.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 32/50/60 ms

Sending 3, 100-byte ICMP Echos to 200.110.3.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.12.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 16/40/56 ms

Sending 3, 100-byte ICMP Echos to 200.110.4.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.12.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 36/42/48 ms

Sending 3, 100-byte ICMP Echos to 128.45.5.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.12.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 56/88/116 ms

Sending 3, 100-byte ICMP Echos to 200.33.6.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.12.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 80/88/92 ms

Sending 3, 100-byte ICMP Echos to 200.33.7.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.12.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 108/125/152 ms

Sending 3, 100-byte ICMP Echos to 200.110.12.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.12.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 1/3/4 ms

Sending 3, 100-byte ICMP Echos to 200.110.13.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.12.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 20/22/24 ms

Sending 3, 100-byte ICMP Echos to 223.255.255.1, timeout is 1 seconds:

Packet sent with a source address of 200.110.12.1 !!!

Success rate is 100 percent (3/3), round-trip min/avg/max = 64/77/84 ms

**Primárne linky R3-R8, R4-R10**

Primárnu linku medzi R3 a R8 sme zabezpečili nastavením local preference na hodnotu 150 medzi smerovačom R3 a R8 (set local-preference 150). Následne sme vytvorili *route-map* na smerovačoch R8 a R9, ktorá “zafarbí” prevádzku z AS 65001 na “farbu” 1100 príkazom set community 65001:1100 additive. Túto komunitu sme následne aplikovali v BGP na smerovači R8 smerom k susedovi R3 a na smerovači R9 smerom na R4. V poslednom kroku bolo potrebné na R3 vytvoriť *community-list*, ktorý rozpozná “farbu” 1100 (ip community-list 1 permit 65001:1100) a zhodujúcu sa prevádzku na linke R3-R8 zvýhodní nastavením *local preference* na 150. Overenie sme vykonali príkazom *traceroute* zo smerovača R9 na smerovač R1.

R9#traceroute 64.34.1.1 source lo1

Tracing the route to 64.34.1.1

1 **10.110.89.8** 20 msec 44 msec 64 msec

2 200.110.255.241 52 msec 56 msec 36 msec

3 10.110.23.2 116 msec 100 msec 76 msec

4 200.110.255.249 76 msec \* 96 msec

Primárnu linku R4-R10 sme vyriešili na smerovači R10 pomocou *route-map* a *as-path access-list*, prepending predstrčí číslo AS 5005 tri krát (set as-path prepend 5005 5005 5005). Tým povieme, že z R7 do R10 je cesta o 3 *hopy* dlšia ako v skutočnosti. Potvrdia nám to nasledujúce riadky výpisu sh ip bgp na R7:

R7#sh ip bgp

Network Next Hop Metric LocPrf Weight Path

\*>i 223.255.255.0 200.33.255.253 0 100 0 3401 110 5005 i

\* **200.33.255.246** 0 0 **5005 5005 5005 5005** i

**Distribuovať iba default, AS5005 a peering prefixy do AS65001**

1. **Riešenie cez *route-map***

Keďže smerovače R8 a R9 zákazníka sú pripojené len na ISP 1 môžeme ich BGP databázu zredukovať tak, že prebytočné záznamy nahradíme príkazom *defaultnou* cestou. Na smerovači R2 sme teda vytvorili *route-map*, ktorá prepustí len záznamy, ktorých *as-path* začína 5005 alebo 4502, ktoré smerujú k zákazníkovi 2 alebo na *peering* centrum. Následne sme túto *route-map* pridali na BGP susedov R3 a R4 vo výstupnom smere. Postupnosť príkazov:

R2(config)#ip as-path access-list 2 permit \_5005$, \_4502$

R2(config)#route-map PEERING permit 10

R2(config-route-map)#match as-path 2

R2(config)#router bgp 110

R2(config-router)#neighbor 10.255.255.4 route-map PEERING out

R2(config-router)#neighbor 10.255.255.4 default-originate

R2(config-router)#neighbor 10.255.255.3 route-map PEERING out

R2(config-router)#neighbor 10.255.255.3 default-originate

Overenie:

R8#sh ip bgp

Network Next Hop Metric LocPrf Weight Path

**\*> 0.0.0.0 200.110.255.241 150 0 110 i**

**\*> 128.45.5.0/24 200.110.255.241 150 0 110 4502 i**

\*> 200.110.0.0/21 200.110.255.241 0 150 0 110 i

s> 200.110.12.0 0.0.0.0 0 32768 i

\*> 200.110.12.0/23 0.0.0.0 32768 i

\* i 10.255.255.9 0 100 0 i

**\*> 223.255.255.0 200.110.255.241 150 0 110 5005 i**

R9#sh ip bgp

Network Next Hop Metric LocPrf Weight Path

**\*>i0.0.0.0 200.110.255.241 0 150 0 110 i**

\* 200.110.255.237 0 110 i

**\*>i128.45.5.0/24 200.110.255.241 0 150 0 110 4502 i**

\* 200.110.255.237 0 110 4502 i

\* 200.110.0.0/21 200.110.255.237 0 0 110 i

\*>i 200.110.255.241 0 150 0 110 i

\* i200.110.12.0/23 10.255.255.8 0 100 0 i

\*> 0.0.0.0 32768 i

s> 200.110.13.0 0.0.0.0 0 32768 i

**\*>i223.255.255.0 200.110.255.241 0 150 0 110 5005 i**

\* 200.110.255.237 0 110 5005 i

1. **Riešenie cez *community***

Predchádzajúce riešenie sme zrušili, ale ponechali sme distribuovanie *default route*.

Na smerovači R5 sme zafarbili cesty z AS 4502 “farbou” 2222. Na smerovači R10 sme zafarbili cesty z AS 5005 “farbou” 3333. Nakoniec sme na smerovači R2 povolili prechod BGP záznamov z AS 4502 a AS 5005. (Pozn.: Bolo potrebné nastaviť *send-community* pozdĺž celej cesty.)

R2#sh ip bgp 64.34.1.0 255.255.255.0

BGP routing table entry for 64.34.1.0/24, version 15

Paths: (2 available, best #2, table Default-IP-Routing-Table)

Flag: 0x820

Advertised to update-groups:

2

4502 3401

200.110.255.254 from 200.110.255.254 (128.45.5.1)

Origin IGP, localpref 100, valid, external

3401

200.110.255.249 from 200.110.255.249 (64.34.1.1)

Origin IGP, metric 0, localpref 100, valid, external, best

Community: **3401:2222**

R2#sh ip bgp 223.255.255.0 255.255.255.0

BGP routing table entry for 223.255.255.0/24, version 8

Paths: (2 available, best #1, table Default-IP-Routing-Table)

Advertised to update-groups:

1

5005

200.110.255.246 (metric 74) from 10.255.255.4 (200.110.4.1)

Origin IGP, metric 0, localpref 100, valid, internal, best

3401 330 5005

200.110.255.249 from 200.110.255.249 (64.34.1.1)

Origin IGP, localpref 100, valid, external

Community: **5005:3333**

Na výpisoch zo smerovačov R8 a R9 vidíme, že sú tu len záznamy o sieťach z AS 4502 a z AS 5005 a ostatné sú nahradené *defaultnou* cestou.

R8#sh ip bgp

Network Next Hop Metric LocPrf Weight Path

**\*> 0.0.0.0 200.110.255.241 150 0 110 i**

**\*> 128.45.5.0/24 200.110.255.241 150 0 110 4502 i**

\*> 200.110.0.0/21 200.110.255.241 0 150 0 110 i

s> 200.110.12.0 0.0.0.0 0 32768 i

\* i200.110.12.0/23 10.255.255.9 0 100 0 i

\*> 0.0.0.0 32768 i

**\*> 223.255.255.0 200.110.255.241 150 0 110 5005 i**

R9#sh ip bgp

Network Next Hop Metric LocPrf Weight Path

**\* 0.0.0.0 200.110.255.237 0 110 i**

\*>i 200.110.255.241 0 150 0 110 i

**\*>i128.45.5.0/24 200.110.255.241 0 150 0 110 4502 i**

\* 200.110.255.237 0 110 4502 i

\*>i200.110.0.0/21 200.110.255.241 0 150 0 110 i

\* 200.110.255.237 0 0 110 i

\* i200.110.12.0/23 10.255.255.8 0 100 0 i

\*> 0.0.0.0 32768 i

s> 200.110.13.0 0.0.0.0 0 32768 i

**\*>i223.255.255.0 200.110.255.241 0 150 0 110 5005 i**

\* 200.110.255.237 0 110 5005 i

**AS5005 nesmie byť nikdy transit**

Na smerovači R4 sme vytvorili *route-map*, ktorá povolí smerom dnu smerovacie BGP záznamy, ktoré majú na prvom mieste v *as-path* číslo 5005. Ostatné sú zakázané (*defaultným deny any*). Na nasledujúcom výpise vidíme, stav pred aplikovaním *route-map* s názvom NO\_TRANSIT - R4 pozná cesty k R1, R5 a R6 cez R10, čomu chceme zabrániť.

R4#sh ip bgp

BGP table version is 11, local router ID is 200.110.4.1

Network Next Hop Metric LocPrf Weight Path

\* 64.34.1.0/24 200.110.255.246 0 **5005** 330 3401 i

\* 128.45.5.0/24 200.110.255.246 0 **5005** 330 4502 i

\*> 200.33.6.0/23 200.110.255.246 0 **5005** 330 i

Použité príkazy na R4:

ip as-path access-list 1 permit \_5005$

route-map NO\_TRANSIT permit 10

match as-path 1

neighbor 200.110.255.246 route-map NO\_TRANSIT in

Po aplikovaní spomínanej *route-map* ostali cesty do spomínaných sietí v BGP tabuľke ale už nebudú prechádzať cez R10 (v *path* nemajú AS 5005). A teda R10 už viac nebude slúžiť ako transit. Po aplikovaní tohto pravidla u ISP1 je vhodné nastaviť podobnú politiku aj u ISP2 na smerovači R7 a takisto u zákazníka 2 na smerovači R10.

R4#sh ip bgp

BGP table version is 12, local router ID is 200.110.4.1

Network Next Hop Metric LocPrf Weight Path

\*>i64.34.1.0/24 200.110.255.249 0 100 0 3401 i

\*>i128.45.5.0/24 200.110.255.254 0 100 0 4502 i

\*>i200.33.6.0/23 200.110.255.249 0 100 0 3401 330 i

**Peering iba pre ISP1 a ISP2, nie pre prefixy naučené z Upstream ISP**

Chceme zabezpečiť, aby komunikáciu z Upstream ISP nebolo možné prevádzkovať cez R5 v AS 4502, iba z ISP1 a ISP2. Na R1 (Upstream ISP) použijeme nasledujúce príkazy:

R1(config)#route map NO\_UPS permit 10

R1(config-route-map)#set community 3401:20

R1(config)#router bgp 3401

R1(config-router)#neighbor 200.110.255.250 route-map NO\_UPS out

R1(config-router)#neighbor 200.110.255.250 send-community

R1(config-router)#neighbor 200.33.255.254 route-map NO\_UPS out

R1(config-router)#neighbor 200.33.255.254 send-community

Smerovače R2 a R6 (ISP1 a ISP2) nakonfigurujeme pomocou komunít takto:

R2(config)#ip community-list 1 permit 5401:30

R2(config)#route-map NO-UPS deny 10

R2(config-route-map)#match community 1

R2(config)#router bgp 110

R2(config-router)#neighbor 200.110.255.254 route-map NO\_SIX out

R6(config)#ip community-list 1 permit 5401:30

R6(config)#route-map NO-UPS deny 10

R6(config-route-map)#match community 1

R6(config)#router bgp 330

R6(config-router)#neighbor 200.33.255.249route-map NO\_SIX out

Vďaka tomu sa z R5 dostaneme na R1 len pomocou priamej linky a nikdy nie cez R2 alebo R6.

R5#sh ip bgp 64.34.0.0/24

BGP routing table entry for 64.34.0.0/24, version 15

Paths: (1 available, best #1, table Default-IP-Routing-Table)

Advertised to update-groups:

1

3401

**64.34.255.253** from 64.34.255.253 (64.34.0.1)

**Overiť funkčnosť nastavenia politiky vhodnými výpadkami liniek a smerovačov**

Otestujeme konektivitu v prípade výpadku linky medzi R5 a R6 a tiež medzi R2 a R5. Na výpisoch je vidieť, že v oboch prípadoch bola nájdená a použitá záložná trasa.

Traceroute z R2 na R10:

R2#traceroute 223.255.255.1 source 200.110.2.1

1 200.110.255.249 24 msec 32 msec 42 msec

2 200.33.255.254 32 msec 26 msec 30 msec

3 10.110.67.7 38 msec 46 msec 36 msec

4 200.33.255.246 50 msec 58 msec \*

Traceroute z R6 na R8:

R6#traceroute 200.110.12.1 source 200.33.6.1

1 200.33.255.253 0 msec 20 msec 16 msec

2 200.110.255.250 22 msec 34 msec 12 msec

3 10.110.13.3 74 msec 60 msec 52 msec

4 200.110.255.242 84 msec \* 62 msec

**Overiť, či je možné odkloniť celú prevádzku na linke R4-R10 v prípade údržby**

Toto overíme pomocou traceroutu z R8 na R10. Za normálnych okolností by bola prevádzka smerovaná cez smerovače R3 a R4 priamo na R10, pri výpadku linky R4-R10 sa využije (horná) záložná trasa cez Peeringové centrum (R3 – R2 – R5 – R6 – R7 – R10).

R8#traceroute 223.255.255.1 source 200.110.12.1

1 200.110.255.241 8 msec 56 msec 24 msec

2 10.110.23.2 40 msec 72 msec 72 msec

3 200.110.255.254 92 msec 88 msec 100 msec

4 200.33.255.250 88 msec 60 msec 120 msec

5 10.110.67.7 104 msec 144 msec 88 msec

6 200.33.255.246 124 msec \* 104 msec