**Žilinská univerzita v Žiline,**

**Fakulta riadenia a informatiky**

**Dokumentácia BGP**

Marek Buček

Branislav Juriš

Cvičiaci: Peter Palúch

Obsah

[Zadanie ISP konektivita a preering 3](#_Toc450061862)

[Zadanie ISP politika 3](#_Toc450061863)

[Topológia zapojenia a tabuľka adries 4](#_Toc450061864)

[Topológia 4](#_Toc450061865)

[Smerovacia tabuľka 5](#_Toc450061866)

[A. ISP konektivita a peering 6](#_Toc450061867)

[1. Použiť IGP OSPF alebo IS-IS -IS (L2 only) single area dizajn, priame p2p prepojenia - ISP1, ISP2 6](#_Toc450061868)

[ISP1 6](#_Toc450061869)

[ISP2 8](#_Toc450061870)

[2. Distribúcia internetových statických smerovacích záznamov 9](#_Toc450061871)

[3. Zabezpečiť plnú konektivitu prostredníctvom iBGP alebo eBGP 10](#_Toc450061872)

[Kontrola, či interné ISP adresy nie sú propagované 10](#_Toc450061873)

[Prepísať privátne AS65001 13](#_Toc450061874)

[Sumarizácia 15](#_Toc450061875)

[B. ISP politika 16](#_Toc450061876)

[1. Vlastná politka 16](#_Toc450061877)

[2. Kontrola primárnej linky medzi R3-R8, R4-R10 20](#_Toc450061878)

[R3-R8 20](#_Toc450061879)

[R4-R10 21](#_Toc450061880)

[3. Distribuovať iba default route 22](#_Toc450061881)

[4. AS5005 nesmie byť nikdy transit 24](#_Toc450061882)

[5. Kontrola ISP1 a ISP2 cez PEERING 24](#_Toc450061883)

[6. Overiť funkčnosť nastavenia politiky vhodnými výpadkami liniek a smerovačov 24](#_Toc450061884)

[7. Odklonenie prevádzky z primárnej linky R4-R10 25](#_Toc450061885)

# Zadanie ISP konektivita a preering

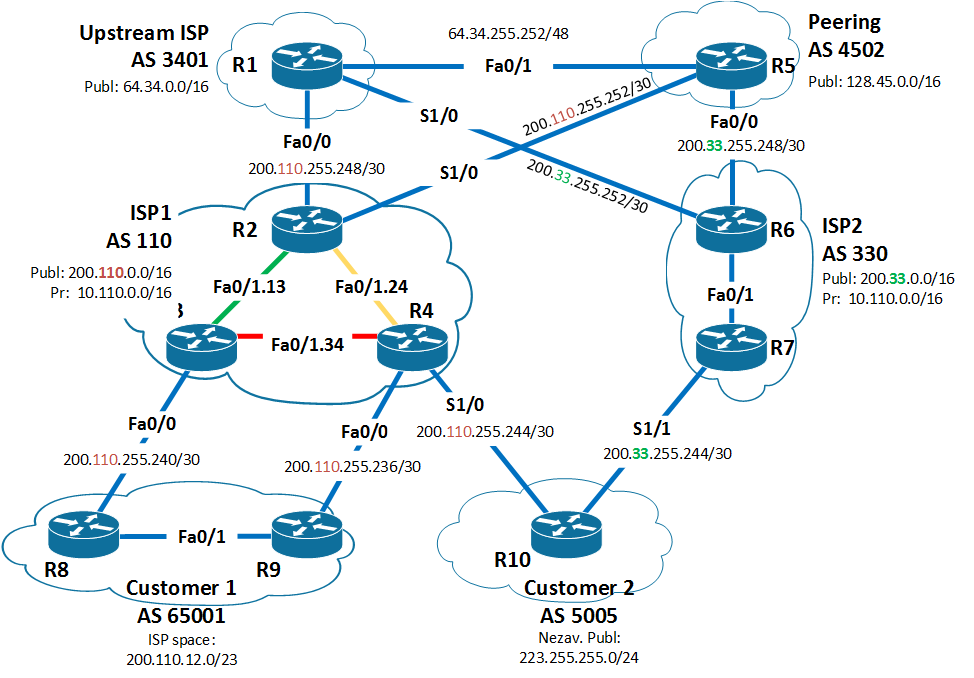
1. Použiť IGP OSPF alebo IS-IS -IS (L2 only) single area dizajn, priame p2p prepojenia
   1. ISP1, ISP2
2. Distribúcia internetových statických smerovacích záznamov z AS3401, AS4502 a zákaznických smerovacích záznamov z AS65001, AS5005, AS330
3. Zabezpečiť plnú konektivitu prostredníctvom iBGP alebo eBGP protokolov pre zákaznícké a internetové smer. Záznamy
   1. Kontrola, či interné ISP adresy nie sú propagované
   2. Prepísať privátne AS65001
   3. Sumarizácia
4. Kontrola konektivity medzi zákazníckymi a internetovými smerovacími záznamami

# Zadanie ISP politika

1. Definovať vlastnú politiku - použiť community, community alter LP, AS-PATH filtering, prepending, atď
2. Primárne linky R3-R8, R4-R10
3. Distribuovať iba default, AS5005 a peering prefixy do AS65001
4. AS5005 nesme byť nikdy transit
5. Peering iba pre ISP1 a ISP2, nie pre prefixy naučené z Upstream ISP
6. Overiť funkčnosť nastavenia politiky vhodnými výpadkami liniek a smerovačov
7. Overiť, či je možné odkloniť celú prevádzku (upstream, downstream) na linke R4-R10 v prípade plánovanej údržby (linka musí byť plne funkčna a BGP spojenie propaguje všetky prefixy)
8. Zdokumentovať (topo, adresácia, dizajn, úlohy)

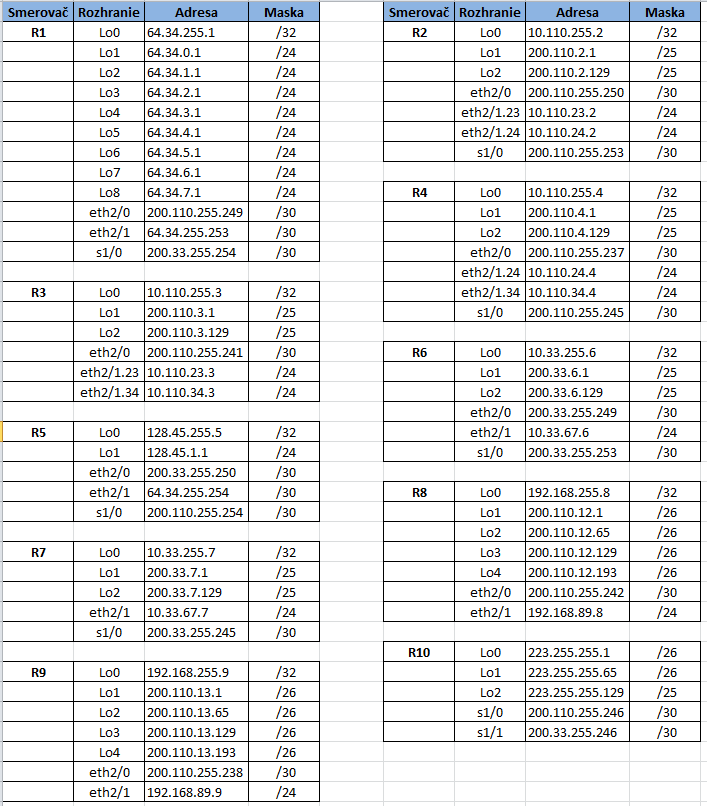
# Topológia zapojenia a tabuľka adries

### Topológia



Smerovacia tabuľka

Medzi našou smerovacou tabuľku z cvičení a tabuľkou zo zapojenia z domu je rozdiel medzi „linkami“ kde linky Eth2/X sú nahradene linkami Fa0/X (eth2/0 => Fa0/0)



# ISP konektivita a peering

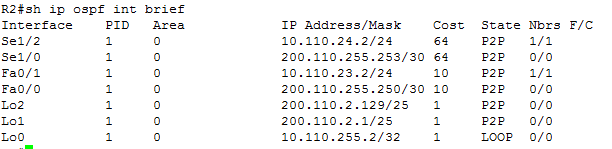
## Použiť IGP OSPF alebo IS-IS -IS (L2 only) single area dizajn, priame p2p prepojenia - ISP1, ISP2

### ISP1

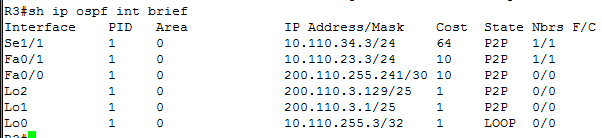
V autonómnom systéme AS 110 ISP1 bol nakonfigurovaný smerovací protokol OSPF 1 area 0. Customer 1 (AS 65001) bol nakonfigurovaný smerovacím protokolom ISIS level 2.

Kontrola prebehla výpisom „show ip ospf interface brief“, kde v stĺpci State sú označené všetky linky typu P2P.

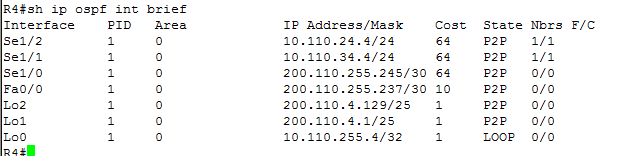
Výpis pre R2



Výpis pre R3

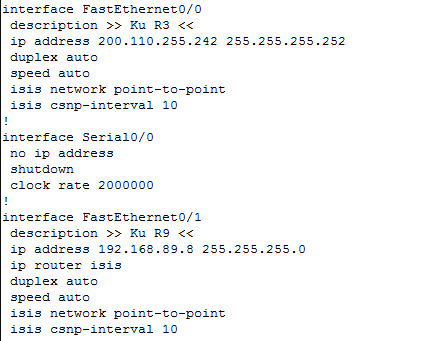


Výpis pre R4

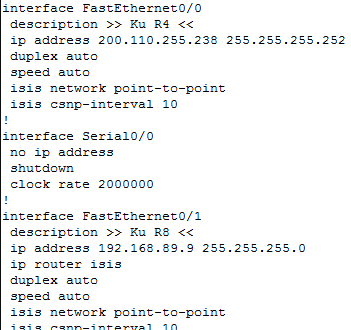


Na rozhraniach typu FastEthernet bol zadaný príkaz „isis network point-to-point“, ktorým sme zabezpečili priame P2P prepojenia medzi smerovačmi. Tento príkaz bol zadaný v smerovacom protokole ISIS v AS 65001.

Výpis pre R8



Výpis pre R9

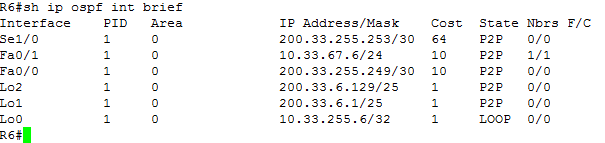


### ISP2

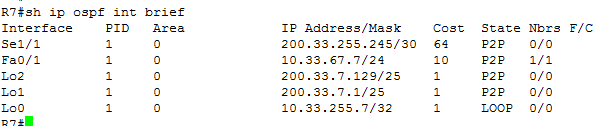
V autonómnom systéme AS 330 ISP2 bol nakonfigurovaný smerovací protokol OSPF 1 area 0.

Kontrola prebehla výpisom „show ip ospf interface brief“, kde v stĺpci State sú označené všetky linky typu P2P.

Výpis pre R6



Výpis pre R7



## Distribúcia internetových statických smerovacích záznamov

Distribúcia statický internetových smerovacích záznamov prebehla pomocou príkazu „redistribute connected“, ktorý bol zadaný po router bgp 3401 a následne address-family ipv4 (analogicky aj pre AS4502).

Distribúcia smerovacích záznamov pre AS110, AS330 a AS65001 je stavená pomocou route-map a tým je zabezpečené aby interné adresy jednotlivých AS neboli propagované.

Prvým krokom bolo vytvorenie prefix-listu, ktorý povoľuje verejné adresy AS, príkazom:

ip prefix-list as110 permit 200.110.0.0/16 le 32

Následne bola vytvorená route-mapa, ktorá povoľuje prefix-list a zároveň nastavuje origin na IGP.

route-map OSPF1 permit 10

match ip address prefix-list as110

set origin igp

exit

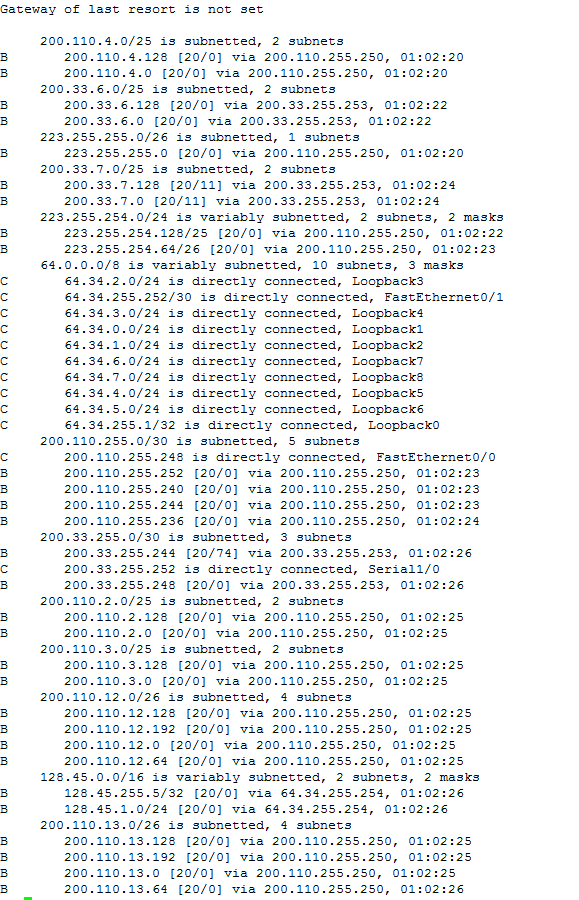
Pomocou prikazov „redistribute ospf 1 route-map OSPF1“ (prevzaté z ostatných OSPF záznamov) a „redistribute connected route-map OSPF1“ (priamo pripojené siete v OSPF), ktorý bol zadaný po router bgp 110 a následne address-family ipv4 (analogicky aj pre AS330 a AS65001).

Na smerovači R10 bol zadaný iba príkaz „redistribute connected“, pretože tam nebeží iný smerovací protokol.

## Zabezpečiť plnú konektivitu prostredníctvom iBGP alebo eBGP

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

Kontrola pomocou príkazu „show ip route“ na smerovači R1(Upstream ISP)



Kvôli praktickosti a prehľadnosti sme zaviedli prefix-list ktorý obsahuje všetky privátne adresy.

ip prefix-list RFC1918 permit 10.0.0.0/8 le 32

ip prefix-list RFC1918 permit 172.16.0.0/12 le 32

ip prefix-list RFC1918 permit 192.168.0.0/16 le 32

Následná kontrola nepropagácie privátnych adries pomocou „show ip bgp prefix-list RFC1918“.

**R1(Upstream ISP)**



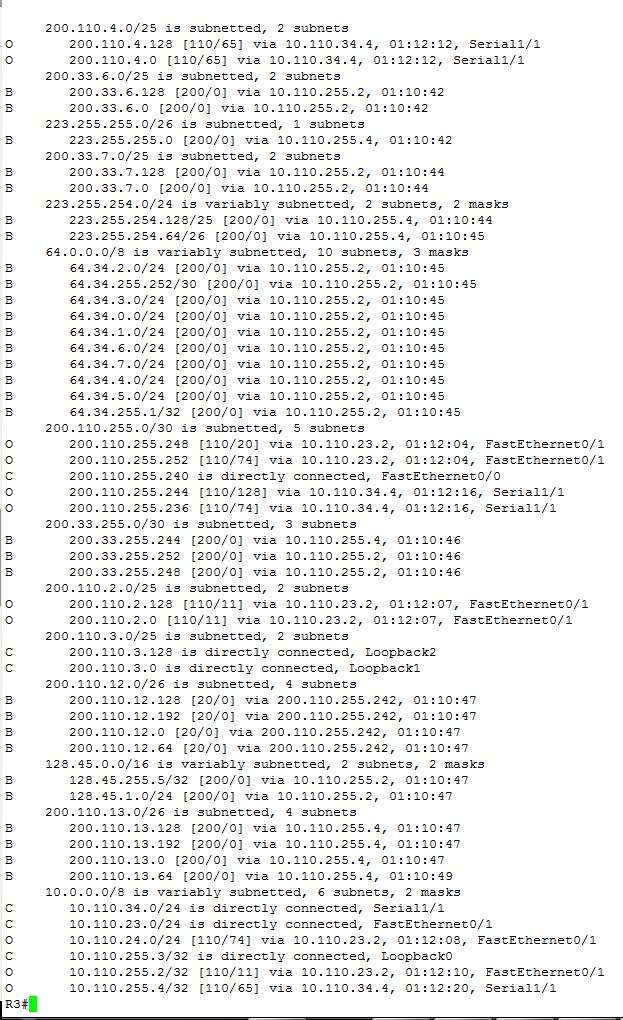
**R5(Peering)**



**R3(ISP1)**



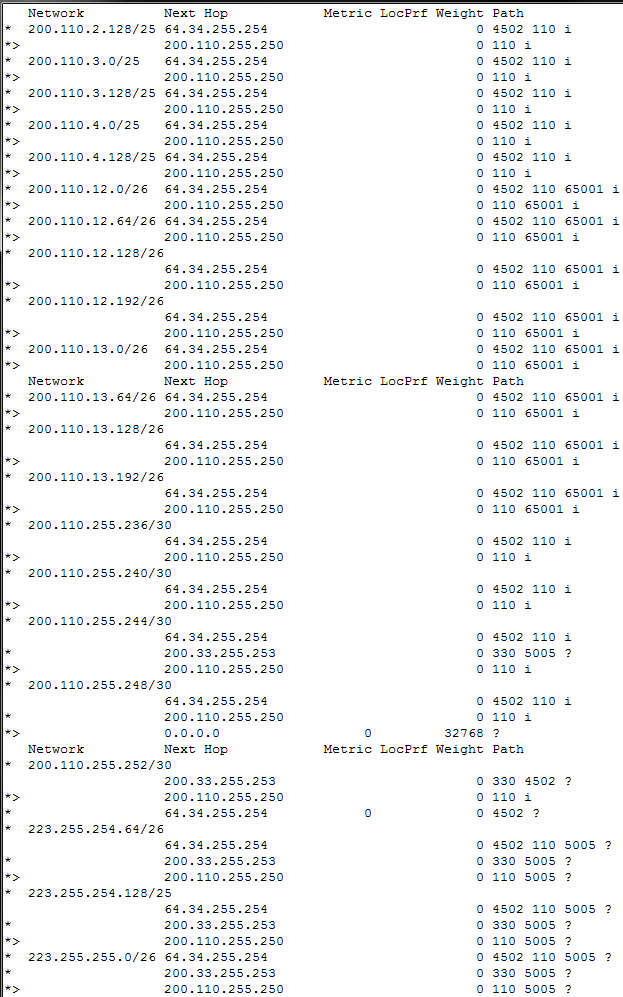
R3 – „show ip route“



Na konci tabuľky sa nachádzajú záznamy o privátnych sieťach priamo pripojených alebo naučených z OSPF. Nenachádza sa tam adresný priestor 192.168.0.0/16, ktorý bol pridelený do AS 65001. Tento sme tiež zakázali zobrazovať pomocou route-mapy.(nie je potrebné aby AS 110 videla privátne adresy z iného AS).

### Prepísať privátne AS65001

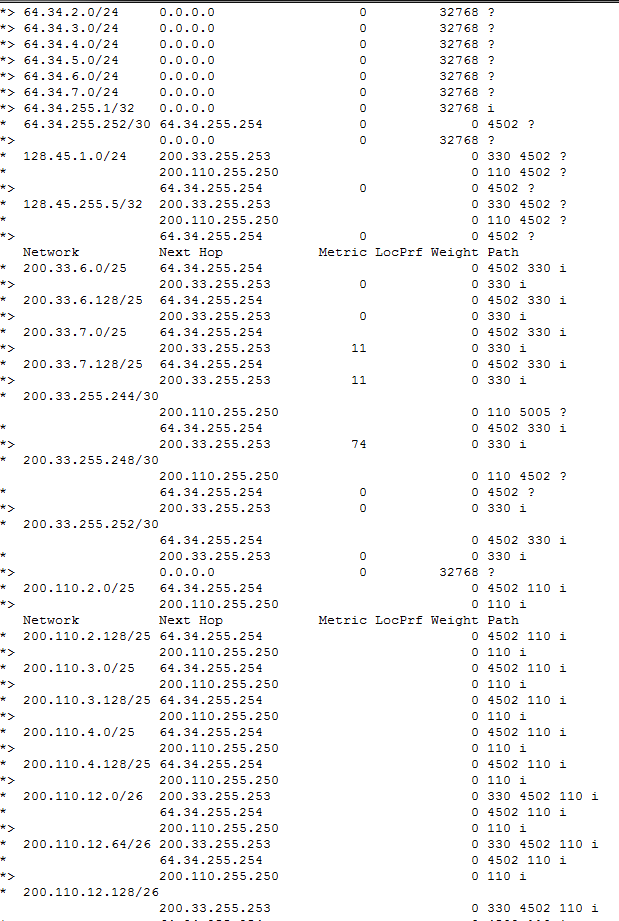
Pred odstránením privátnych AS výpis zo smerovača R1 „show ip bgp“ zobrazuje v atribúte Path aj privátny AS 65001.



Následne sme zadali príkaz „nei 200.110.255.246 remove-private-as“ (adresa je eBGP smerovača v inom AS) na smerovači R4 v „address-family ipv4“

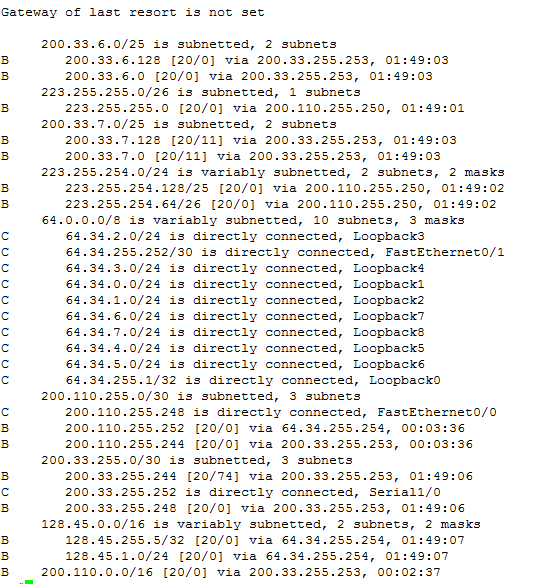
obdobne aj na smerovači R2.

Po „úprave“ už výpis zo smerovača R1 neobsahuje v atribúte Path privátne AS ale bolo nahradené verejným AS cez ktorý sa dá do cieľa dostať.



### Sumarizácia

Sumarizovali sme adresy z AS 110 pomocou príkazu “aggregate-address 200.110.0.0 255.255.0.0 as-set“ na smerovači R2 a R4 v „address-family ipv4“. Následný výpis smerovacej tabuľky na R1 ukázal sumarizovaný záznam. Celý adresný priestor 200.110.0.0/16 bol zlúčený do jedného záznamu.



# ISP politika

## Vlastná politka

U ISP1 a ISP2 došlo k zmene jedného zo základných rozhodovacích parametrov, local-preference kde sme zmenili hodnotu zo 100 na 60 pomocou príkazu „bgp default local-preference 60“ v režime smerovaču „router BGP“.

**Pre zabezpečenie primárnej linky R3-R8 sme použili nastavenie parametra Multi-Exit Discriminator a Local Preference.**

Na smerovači R9, vytvorená route-mapa pre zabezpečenie toku dát od zákazníka 1 smerom k ISP1:

route-map R9Metrika permit 10

set metric 20

MED sme nastavili na hodnotu 20 smerom na R4 (nižšia hodnota = lepšia), zaistili sme si tím (záložnú)back-up linku. Následné použitie v “address-family ipv4“ príkazom „neighbor 200.110.255.237 route-map R9Metrika out“ (200.110.255.237 - adresa rozhrania smerovača R4) pre použitie MED na vytvorenie back-up linky.

Pre smerovač R8, sme si vytvorili route-mapu pre zabezpečenie toku dát od zákazníka 1, smerom k ISP1:

route-map R8Metrika permit 10

set metric 10

ktorá bola následne použitá príkazom „neighbor 200.110.255.241 route-map R8Metrika out“ pre všetky záznamy smerom od R8.

Ďalej bolo ešte potrebné nastaviť local-preference pre smerovacie dáta z externého BGP. Na smerovači R8 sme preto vytvorili prefix-list:

ip prefix-list R4R9 permit 200.110.255.236/30 (adresa linky medzi R4-R9).

Následne sme vytvorili route-mapu z použitím prefix-listu (local-preference menšia = horšia):

route-map PreferR3R8 permit 10

match ip address prefix-list R4R9

set local-preference 50

route-map PreferR3R8 permit 20

set local-preference 150

Následne sme ich použili smerom dnu pre AS65001 v „address-family ipv4“ príkazom

„neighbor 200.110.255.241 route-map PreferR3R8 in“

**Pre zabezpečenie primárnej linky R4-R10 sme použili nastavenie parametra Weight a použili sme aj komunity.**

U ISP1, ISP2 a Zákazníka2 sme povolili nový formát komunít pomocou príkazu „ip bgp-community new-format“.

**Smerovač R10**

Najprv sme si vytvorili route-map(u) v ktorej sme nastavili parameter weight (väčší = lepší)

route-map fromR10toR4 permit 10

set weight 20

túto RouteMapu sme následne použili smerom dnu pre všetky siete preposielané od R4 príkazom „neighbor 200.110.255.245 route-map fromR10toR4 in“

v „address-family ipv4“. Táto úprava zabezpečí posielanie paketov primárne na R4.

Vytvorenie „as-path access-listu“ , ktorým zabezpečíme aby AS5005 nebol tranzitívny uzol prebehlo pomocou príkazov kde sme využívali regulárne výrazy:

ip as-path access-list 1 deny ^$

ip as-path access-list 1 permit .\*

Následné sme vytvorili route-map:

route-map ToR7c deny 1

match as-path 1

route-map ToR4c deny 1

match as-path 1

A pridali sme posielanie komunít:

route-map ToR4c permit 10

set community 110:1100

Následne sme použili príkazy na rozosielanie komunít v „address-family ipv4“:

nei 200.110.255.245 send-community standard

nei 200.33.255.245 send-community standard

a nastavením route-map smerom von:

neighbor 200.110.255.245 route-map ToR4c out

neighbor 200.33.255.245 route-map ToR7c out

Nastavili sme si vlastné comunity-listy:

ISP1 (R2,R3,R4)

ip community-list 1 permit 110:1050

ip community-list 2 permit 110:1090

ip community-list 3 permit 110:1100

ISP2 - R7

ip community-list 1 permit 330:1050

ip community-list 2 permit 330:1090

ip community-list 3 permit 330:1100

Na smerovačoch R4 a R7 sme vytvorili route-mapy, ktoré na základe komunít nastavujú local-preference:

route-map FromR10 permit 10

match community 1

set local-preference 50

route-map FromR10 permit 20

match community 2

set local-preference 90

route-map FromR10 permit 30

match community 3

set local-preference 100

route-map FromR10 permit 65535

**Preposielanie 5005 a 4502 do AS65001**

Využili sme AS-PATH ACCESS-LIST, ktorý sme použili na smerovačoch R3 a R4 , ktorý povoľuje AS 5005 (posledný AS v AS-PATH – zabraňuje tranzitivnosti) a AS 4502.

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

ip as-path access-list 1 permit \_4502\_

Následne sme vytvorili route-mapy pre R3 a R4:

Pre R3:

route-map ToR8 permit 10

match as-path 1

Route-map bola použita príkazom “neighbor 200.110.255.242 route-map ToR8 out“ v address-family ipv4.

Pre R4:

route-map ToR9 permit 10

match as-path 1

Route-map bola použita príkazom “neighbor 200.110.255.238 route-map ToR9 out“ v address-family ipv4.

**Preferecia Peering-u pred UpStream** bola riešena na smerovači R5 pomocou dvoch AS-PATH ACCESS-LISTov. Prvý zakazuje rozosielať informácie o AS 3401 a druhý povoľuje pre Upstream posielať iba priamo pripojene siete z AS 4502.

.

ip as-path access-list 1 deny \_3401\_

ip as-path access-list 1 permit .\*

ip as-path access-list 2 permit ^$

Následne sme tieto access-listy použili v address-family ipv4 príkazmi:

neighbor 64.34.255.253 filter-list 2 out

!smerom na AS3401

neighbor 200.33.255.249 filter-list 1 out

!smerom na R6 v AS330

neighbor 200.110.255.253 filter-list 1 out

!smerom na R2 v AS110

Vytvorili sme ešte route-mapy pre R2 a R6 aby preferovali Peering, v ktorých sme nastavili local-preference aby boli preferované linky do Peeringu pre UpStreamom.

route-map PreferPeering permit 10

set local-preference 150

route-map PreferUpStream permit 10

set local-preference 50

Príkazmi sme ich aplikovali smerom dnu aby túto local-preference oznamoval ostatným BGP

smerovačom v AS.

Pre R2 v address-family ipv4:

neighbor 200.110.255.249 route-map PreferUpStream in

neighbor 200.110.255.254 route-map PreferPeering in

Pre R6 v address-family ipv4:

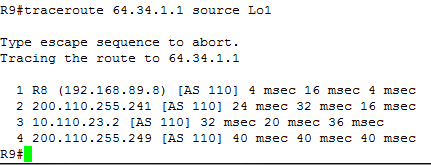
neighbor 200.33.255.250 route-map PreferPeering in

neighbor 200.33.255.254 route-map PreferUpStream in

## Kontrola primárnej linky medzi R3-R8, R4-R10

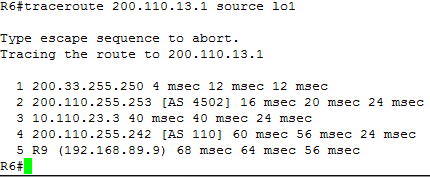
### R3-R8

Kontrola primárnej linky bola odskúšaná pomocou príkazu „traceroute 64.34.1.1 source Lo1“ (Lo1= 200.110.13.1), z R9 na R1



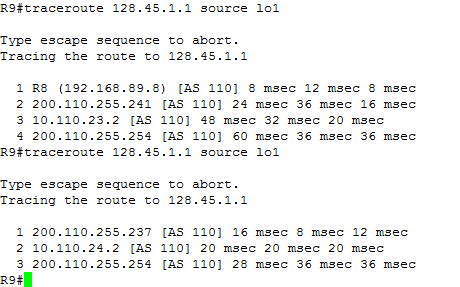
Adresa 200.110.255.241 je na rozhraní smerovača R3 ktorý je pomocou tejto linky pripojený k smerovaču R8.

Pre kontrolu sme vyskúšali aj „traceroute 200.110.12.1 source Lo1“ (Lo1 = 200.33.6.1) opačným smerom teraz z R6 na R9



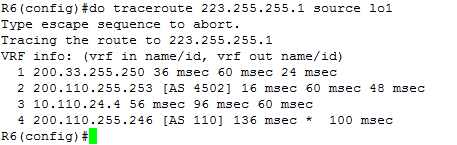
Tak isto prešiel traceroute cez R3 a R8 lebo 200.110.255.242 je adresa rozhrania na smerovači R8 smerom k R3.

Pridávame aj overenie záložnej trasy po vypnutí linky medzi R3-R8. Traceroute bol vyslaný na Loopback smerovača R5

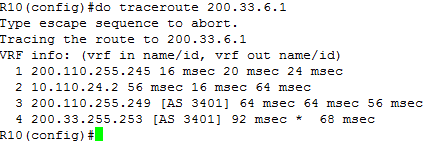


### R4-R10

Podobne sme skontrolovali funkčnosť primárnej linky medzi R4 a R10. Pomocou príkazu „traceroute 223.255.255.1 source Lo1“ (Lo1= 200.33.6.1) sme skúsil primárnu linku. Loopback smerovača R6 sme si zvolili schválne, pretože by si bez manipulácie z linkami vybral najkratšiu trasu cez R7.



Na základe traceroute vidno že prešiel cez smerovač R4 (10.110.24.4), takže manipuláciia z linkami funguje. Skúsili sme ešte traceroute smerom na R6 z R10 či si aj v tomto prípade vyberie primárnu linku. Pýtali sme sa na Loopback smerovača R6.



Opäť bola použitá linka medzi R4 a R10.

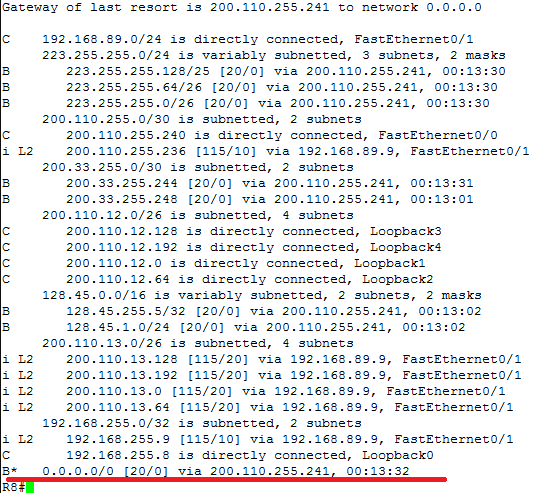
## Distribuovať iba default route

Na distribúciu default-route pre AS 65001 sme použili príkazy :   
neighbor 200.110.255.242 default-originate pre R3

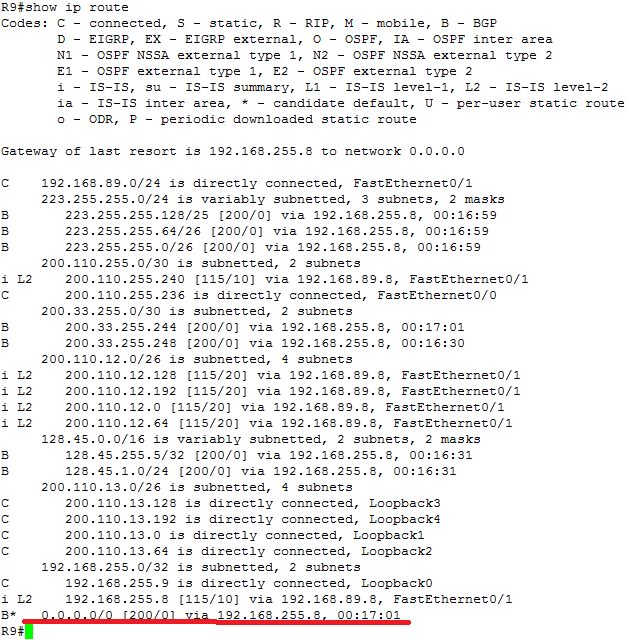
neighbor 200.110.255.238 default-originate pre R4.

Kontrola pomocou “show ip route“ na R8 aj R9

Smerovač R8:



Smerovač R9:

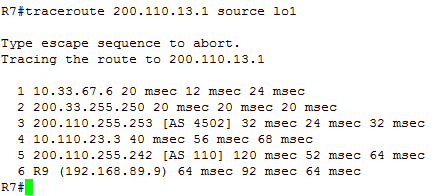


## AS5005 nesmie byť nikdy transit

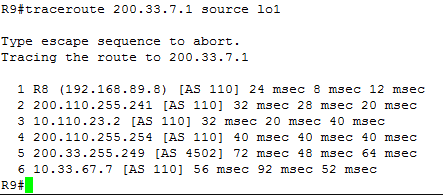
Za účelom dosiahnutia cieľa aby AS5005 nikdy nebol tranzitívny sme si vytvorili ASPATH ACCESS LIST. Pomocou tohto access-listu si zabezpečíme aby AS5005 nebol tranzitívny uzol, vzor konfigurácie je možný nájsť na str.17 tejto dokumentácie.

## Kontrola ISP1 a ISP2 cez PEERING

Kontrola prebehla pomocu príkazu traceroutezo smerovača R7 na loopback smerovača R9, traceroute prešiel cez AS 4501 - Peering



Kontrola prebehla pomocu príkazu traceroutezo smerovača R9 na loopback smerovača R7, traceroute prešiel cez AS 4501 - Peering

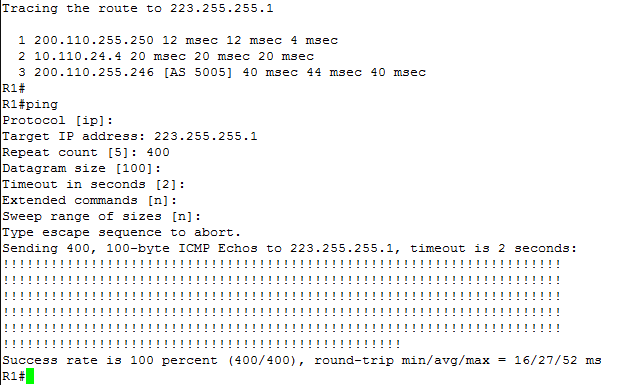


## Overiť funkčnosť nastavenia politiky vhodnými výpadkami liniek a smerovačov

Funkčnosť nastavenia politiky vhodnými výpadkami liniek a smerovačov sme priebežne kontrolovali počas konfigurácie a následne aj po konfigurácii kde sme sledovali odklonenie prevádzky, či je schopný smerovač pri “vyhodení” jednej cesty smerovať data inou cestou do cieľa, a podobne.

## Odklonenie prevádzky z primárnej linky R4-R10

Skúška odklonenia prebehla pomocou pingu o veľkosti 400 opakovaní. Ping bol vyslaný na loopback R10. Výsledok boli samé výkričníky naznačujúce, že nedošlo k výpadku spojenia väčšieho než 2 sekundy. Kontrola prebehla pomocou príkazu traceroute a ip adresou loopbacku UpStream providera na ktorom je zobrazené presunutie trasy do ISP2.



Pred a po odklonení bol vyskušaný traceroute či prebehlo správne. Na odklonenie prevádzky boli zamenené politky v AS 5005 tak ,že boli uplatnené na opačné rozhrania pomocou príkazov:

no neighbor 200.110.255.245 route-map fromR10toR4 in

no neighbor 200.110.255.245 route-map ToR4c out

no neighbor 200.33.255.245 route-map ToR7c out

neighbor 200.33.255.245 route-map fromR10toR4 in

neighbor 200.110.255.245 route-map ToR7c out

neighbor 200.33.255.245 route-map ToR4c out

do clear ip bgp \* out

do clear ip bgp \* in

