ZAVOD ZA ELEKTRONIKU, MIKROELEKTRONIKU, RAČUNALNE I INTELIGENTNE SUSTAVE
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA
SVEUČILIŠTE U ZAGREBU

DIPLOMSKI RAD BR. 1888

# ODREĐIVANJE REPUTACIJE AUTONOMNIH SUSTAVA TEMELJENO NA PRAĆENJU UPRAVLJAČKOG PROMETA RUBNIH USMJERNIKA

TOMISLAV DEJDAR

U Zagrebu, listopad 2011.

# Sadržaj

# 1. Uvod

Internet se sastoji od mnoštva međusobno nezavisnih autonomnih sustava koji su mahom usmjereni na podršku komercijalnim aktivnostima. Kako je stoga prvenstveni cilj povećanje dobiti, administratori autonomnih sustava nisu potaknuti na ulaganja u poboljšanja koja bi koristila Internetu kao cjelini, već samo na kratkoročno maksimiziranje profita. Uočljivo je da je ovakvo stanje prvenstveno posljedica nepostojanja središnjeg autoriteta koji bi jamčio za autonomne sustave i pratio njihov rad. Jedan od mogućih pristupa razrješavanju navedenog problema korištenje je primjerenog reputacijskog sustava za određivanje kvalitete autonomnih sustava temeljeći se na mjerenju izvjesnih parametara, između kojih se ističe upravljački promet koji generiraju rubni usmjernici. Cilj je ovog rada proučiti postojeće rezultate, predložiti način praćenja prometa autonomnih sustava, predložiti model izračuna reputacije te implementirati prototip reputacijskog sustava.

U drugom poglavlju opisan je sam protokol rubnih usmjernika (engl. *Border Gateway Protocol*, *BGP*). Nakon početnog opisa samog protokola, načina na koji radi i njegove primjene, detaljno je opisana UPDATE poruka. Razlog tome je što se upravo tom porukom prenose usmjerničke informacije između rubnih usmjernika te se kroz snimanje informacija iz tih poruka prikupljaju podaci potrebni za izračun reputacije. Kao poseban naglasak opisan je atribut AS Path, dio UPDATE poruke koji prenosi najbitnije informacije o samom usmjeravanju i čini srž podataka za vrednovanje autonomnih sustava i izračun njihove reputacije. Nadalje se opisuje struktura Interneta sastavljenog od autonomnih sustava. Nakon opisa autonomnih sustava i registratora, slijedi dio koji opisuje usmjeravanje na Internetu i BGP kao protokol usmjeravanja na Internetu. Opisuje se atribut AS Path i njegova važnost za usmjeravanje na Internetu, za odabir najboljeg puta i određivanje politike usmjeravanja. Opisane su različite razine autonomnih sustava te odnosi među njima. Na kraju poglavlja detaljno je opisan postupak konvergencije BGP-a te njegov utjecaj na opterećenje usmjernika, slabljenje ili prekid veza.

Treće poglavlje opisuje pogreške konfiguracije BGP-a. Uvršten je u ovaj rad jer veliki dio problema koji nastaju pri usmjeravanju na Internetu nisu uzrokovani namjernim ponašanjem, već jednostavno propustima u konfiguraciji BGP-a i lošim odlukama politika usmjeravanja autonomnih sustava. U ovom su poglavlju dani rezultati mjerenja pogrešaka i njihov utjecaj na usmjeravanje BGP-om što se pokazalo kao bitan faktor prilikom odabira načina i metoda izračuna reputacije.

Četvrto poglavlje opisuje pretpostavke ponašanja, odnosno dobru praksu usmjeravanja na Internetu. Navedeni su različiti načini kršenja dobre prakse usmjeravanja. Navedeni su i načini korištenja informacija iz usmjerničkog prometa koje će poslužiti za evaluaciju autonomnih sustava i izračun reputacije. Zatim su, prvo kvalitativno, a potom i kvantitativno opisana dva modela predložena za izračun reputacija autonomnih sustava na temelju kojih je izvedena praktična implementacija reputacijskog sustava.

Peto poglavlje opisuje samu arhitekturu reputacijskog sustava i njegovu praktičnu izvedbu korištenjem programskog jezika Python. Dan je popis dodatnih modula korištenih u izradi programskog rješenja implementacije, opisana je sama implementacija te su dane upute za njeno korištenje.

U šestom poglavlju opisana su praktična mjerenja reputacijskog sustava. Inicijalna su mjerenja bila potrebna kako bi se provjerila ispravnost empirijski izvedenih formula i funkcija za izračun reputacije. Daljnja su mjerenja vršena kako bi se izabrali ispravni parametri funkcija te kako bi se pokazao utjecaj parametara na rezultate mjerenja. Na kraju su dani primjeri slučajeva koji su se dogodili u bliskoj povijesti, a koji su uzrokovali probleme s usmjeravanjem na Internetu.

Primijenjen je implementirani reputacijski sustav na te slučajeve, izmjereni su dobiveni rezultati te je dan prijedlog načina kojim bi, u budućnosti, reputacijski sustav mogao pomoći u predviđanju, izbjegavanju ili ublažavanju posljedica sličnih incidenata. Rad završava zaključkom i popisom literature.

# 2. Arhitektura i usmjeravanje na Internetu

U ovom će poglavlju biti opisan Border Gateway Protocol. Naglasak će biti stavljen na BGP Update poruku koju razmjenjuju usmjernici koji koriste ovaj protokol i informacije koje se prenose tom porukom, atributi puta jer se upravo kroz Update poruku ostvaruje sama srž protokola. Najveći će naglasak biti na AS Path atributu budući da je on odgovoran za selekciju puta te je iznimno bitan za kasniju evaluaciju pojedinih autonomnih sustava koji čine Internet te za izračun njihove reputacije. Objašnjeni su različiti tipovi AS Path atributa te je dana interpretacija raznih slučajeva što je bitno za kasnije razumijevanje problematike reputacije autonomnih sustava.

U nastavku će poglavlja bit objašnjeno što su to autonomni sustavi, što su to registri te koja je njihova uloga u ustrojstvu Interneta. Dalje ćemo vidjeti kako se ostvaruje usmjeravanje između autonomnih sustava te koja je uloga BGP-a u tome. Objasnit ćemo razne tipove AS-ova, odnose među njima te putove kojima promet prolazi od početnog prema krajnjem AS-u. Objasnit ćemo neke probleme koji pritom mogu nastati te objasniti zašto je BGP protokol usmjeravanja drugačiji od drugih usmjerničkih protokola. Dat ćemo kratak uvod u opterećenje usmjernika koji sudjeluju u BGP-u, problem i vrijeme konvergencije samog protokola. Materija ovog poglavlja važna je za kasnije razumijevanje pogrešaka u konfiguraciji BGP-a, bilo onih slučajnih, bilo namjernih kao dio usmjerničke politike pojedinog AS-a, koje otežavaju, onemogućavaju, destabiliziraju ili poskupljuju održavanje komunikacije. To će nas dovesti do problematike određivanja reputacija pojedinih AS-ova na temelju njihovog ponašanja, posebno na temelju njihove usmjerničke politike i konfiguracije BGP-a, koja može pomoći drugim AS-ovima koji se ponašaju „prihvatljivije“ kako bi smanjili negativne utjecaje koje mogu nastati uslijed propusta te slučajno ili namjerno pogrešnih politika usmjeravanja drugih AS-ova.

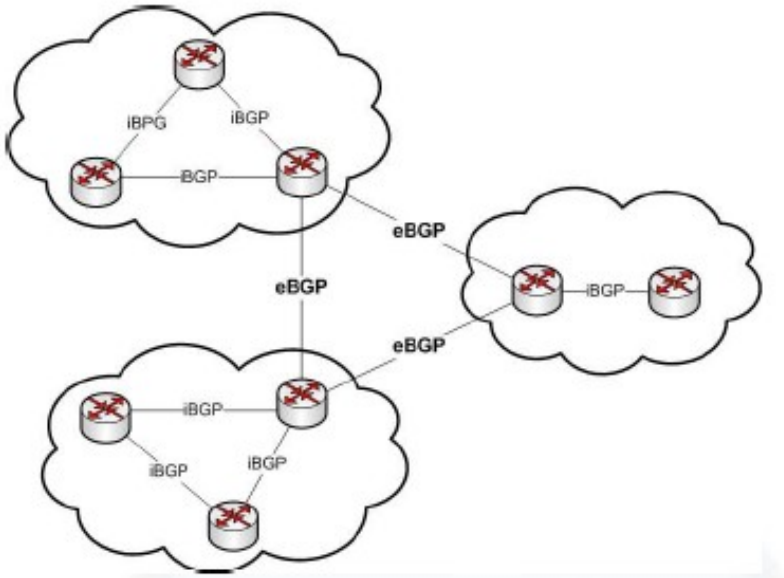
## 2.1 Općenito o BGP-u

Border Gateway Protocol usmjernički je protokol koji se upotrebljava za usmjeravanje u samoj okosnici Interneta. Internet je sastavljen od mnoštva zasebnih mreža koje se nazivaju autonomni sustavi ili AS-ovi (engl. *Autonomous System*). Za usmjeravanje unutar pojedinog autonomnog sustava koriste se protokoli unutarnjeg usmjeravanja ili IGP-ovi (engl. *Interior Gateway Protocol*). Za usmjeravanje između autonomnih sustava koriste se protokoli vanjskog usmjeravanja EGP-ovi (engl. *Exterior Gateway Protocol*). Trenutno je BGP jedini protokol vanjskog usmjeravanja koji se koristi na cijelom Internetu. Za odluke usmjeravanja i odabir puta BGP se za razliku od protokola unutarnjeg usmjeravanja oslanja na veći set informacija koje se nazivaju atributi puta. Sam se odabir puta vrši algoritmom odabira, međutim velik utjecaj na odabir puta imaju pravila zadana od strane administratora u vidu filtriranja usmjerničkih informacija i određivanjem pravila i politika usmjeravanja. Organizacije koje posjeduju autonomne sustave određuju pravila i politike usmjeravanja te mrežni administratori konfiguriraju BGP usmjernike u skladu s tim pravilima. Zbog toga možemo reći da se odabir najboljeg puta manje svodi na puko izvršavanje samog algoritma odabira puta, a više se bazira na specifičnom politički baziranom usmjeravanju.

Trenutno je u uporabi verzija 4 BGP-a koji omogućuje besklasno međudomensko usmjeravanje ili CIDR (engl. *Classless Inter-Domain Routing*) i agregaciju ruta. Zadnja inačica BGP-a opisana je u dokumentu RFC 4271 [18] koji je ispravio mnoge nedostatke RFC-a 1771. Budući da se BGP koristi za usmjeravanje između autonomnih sustava, BGP usmjernici se smještaju na granice autonomnog sustava te se nazivaju granični usmjernici, a sam se protokol naziva protokol graničnih usmjernika. Po prirodi veza koje BGP usmjernik ostvaruje sa svojim susjedima, protokol se može podijeliti na dvije inačice:

- iBGP (engl. *Internal BGP*) - veza između BGP usmjernika koji se nalaze u istom autonomnom sustavu
- eBGP (engl. *External BGP*) - veza između BGP usmjernika koji se nalaze u različitim autonomnim sustavima

Na slici 2.1 prikazan je način rada ove dvije inačice. Unutarnji BGP koristi se za razmjenu informacija između usmjernika u istom autonomnom sustavu koje je pojedini usmjernik naučio od svog susjeda iz nekog drugog autonomnog sustava. Njegova je zadaća stvaranje identične BGP tablice usmjeravanja za sve BGP usmjernike unutar jednog AS-a kako bi se održala jedinstvenost politike usmjeravanja na razini cijelog AS-a. Ne treba koristiti BGP za usmjeravanja unutar jednog autonomnog sustava; za to postoje protokoli unutarnjeg usmjeravanja, a ne iBGP. Eksterni BGP koristi se za razmjenu usmjerničkih informacija između usmjernika u različitim autonomnim sustavima. Ova su dva načina jako slična te se razlikuju samo u nekim detaljima. Prije svega tu je pravilo koje zabranjuje usmjerniku slanje informacija svom internom susjedu koje je saznao od svog drugog internog susjeda.




*Slika 2.1. Unutrašnji i vanjski BGP*

Kako bi BGP usmjernici mogli razmjenjivati informacije o usmjeravanju i usmjeravati promet, potrebno je u konfiguraciji usmjernika eksplicitno definirati susjedski odnos. Za razmjenu poruka susjedni se usmjernici koriste TCP-om na pristupu 179. Nakon početne uspostave susjedskog odnosa usmjernici razmjenjuju sve informacije o BGP rutama koje sami imaju. Poslije nisu više potrebne periodičke razmjene svih ruta već se nove informacije razmjenjuju inkrementalnim objavama. Postojanost BGP susjedskog odnosa mora se stoga provjeravati periodičkim jednostavnim porukama kako bi usmjernici mogli otkriti naprasan prekid veze sa susjedom. U svom radu BGP usmjernici razmjenjuju 4 vrste poruka:

- **OPEN**

  se koristi za inicijalnu uspostavu susjedskog odnosa među usmjernicima. Sadrži osnovne informacije poput identifikatora usmjernika, korištene verzije BGP-a, broja autonomnog sustava i sl.

- **UPDATE**

  služi za razmjenu informacija o mrežama za koje se vrši usmjeravanje. U njoj se nalazi popis novoobjavljenih mreža te sve informacije o putu prema tim mrežama. Također sadrži i popis mreža za koje se prekida usmjeravanje.

- **KEEPALIVE**

  služi održavanju sjednice aktivnom. U slučaju neprimitka nekoliko uzastopnih KEEPALIVE poruka, susjedski se odnos prekida.

- **NOTIFICATION**

  poruka koristi se za prekid veze uslijed pogreške.

Srž samog BGP-a upravo je poruka UPDATE te je ona detaljno opisana u sljedećem potpoglavlju.

## 2.2 BGP Update poruka

UPDATE poruke koriste se za razmjenu usmjerničkih informacija između BGP susjednih usmjernika. Jedna UPDATE poruka služi za oglašavanje samo jedne dohvatljive rute svome susjedu, ili za povlačenje jedne ili više ranije objavljenih ruta koje su postale nedohvatljive, ili više nisu u uporabi. UPDATE poruka može također istovremeno oglašavati jednu rutu i povlačiti više prethodno oglašenih ruta. Svaka UPDATE poruka obavezno sadržava zaglavlje fiksne veličine od 19 okteta, dva kasnije opisana polja svako od 2 okteta te po potrebi i druga polja kako je prikazano na slici 2.2.

| SECTIONS | FRAME FORMAT | |
|---|---|---|
| Unreachable Routes | Unfeasible Routes Length (2bytes) | |
| | Withdrawn Routes (variable) | |
| Path Attributes | Total Path Attribute Length (2 bytes) | |
| | Path Attributes (variable length) | |
| NLRI | Length (1 byte) | Prefix (variable length) |
| | Length (1 byte) | Prefix (variable length) |
| | *additional length/prefix pairs* | |

*Slika 2.2. Format BGP UPDATE poruke*

- Polje *Unfeasible Routes Length*:

Ovo polje od 2 okteta sadržava ukupnu duljinu u oktetima sljedećeg polja *Withdrawn Routes*. Iz ove se vrijednosti kasnije također mora moći izračunati vrijednost duljine polja *Network Layer Reachability Information*. Ukoliko je vrijednost ovoga polja 0, UPDATE poruka ne sadrži rute koje su postale nedohvatljive te u skladu s tim ne postoji niti polje *Withdrawn Routes*.

- Polje *Withdrawn Routes*:

  Ovo je polje promjenjive duljine koje sadrži listu IP prefiksa za rute koje se povlače iz uporabe. Svaki IP prefiks kodiran je parom sastavljenim od duljine mrežne maske prefiksa (*length*) i samog prefiksa (*prefix*).

  a) Polje *Length* sadrži duljinu u bitovima IP prefiksa, odnosno duljinu mrežne maske dotičnog prefiksa; fiksne je veličine od 1 okteta.

  b) Polje *Prefix* sadrži IP prefiks na kojeg slijedi popuna do granice okteta. Vrijednost je pratećih bitova irelevantna.

- Polje *Total Path Attribute Length*:

  Polje od 2 okteta koje sadržava ukupnu duljinu u oktetima sljedećeg polja *Path Atributes*. Iz ove se vrijednosti kasnije također mora moći izračunati vrijednost duljine polja *Network Layer Reachability Information*. Ukoliko je vrijednost ovoga polja 0, UPDATE poruka ne sadrži polje *Network Layer Reachability Information*.

- Polje *Path Attributes*:

  Sekvenca varijabilne duljine atributa puta (*Path Attributes*) prisutna je u svakoj UPDATE poruci. Svaki atribut puta sastavljen je od tri člana: tipa atributa (*attribute type)*, duljine atributa (*attribute length*) i vrijednosti samog atributa (*attribute value*) te kao takav može biti varijabilne duljine.

  a) Tip atributa je polje od dva okteta koje se sastoji od polja zastavica (*Attribute Flags*) duljine jednog okteta i od polja koda tipa atributa (*Attribute Type Code*) također duljine jednog okteta.

  Najviši bit okteta (bit 0) polja zastavica je opcionalni bit. On određuje je li atribut opcionalan, ako mu je vrijednost 1 ili je atribut općepoznat, ako mu je vrijednost 0.

  Drugi najviši bit okteta (bit 1) polja zastavica je bit tranzitivnosti. On određuje je li opcionalni atribut tranzitivan ako mu je vrijednost 1 ili je netranzitivan, ako mu je vrijednost 0. Za općepoznate atribute tranzitivni bit mora biti postavljen na vrijednost 1.

  Treći najviši bit okteta (bit 2) polja zastavica je bit djelomičnosti. On određuje jesu li informacije sadržane u opcionalnom tranzitivnom atributu djelomične, ako mu je vrijednost 1 ili potpune, ako mu je vrijednost 0. Za dobro znane atribute kao i za opcionalne netranzitivne atribute bit djelomičnosti mora biti postavljen na 0.

  Četvrti najviši bit okteta (bit 3) polja zastavica je bit produljene duljine. On određuje je li član duljina atributa dugačak jedan oktet, ako mu je vrijednost 0 ili dva okteta, ako mu je vrijednost 1. Produljena duljina smije se koristiti samo, ako

je duljina člana vrijednosti atributa dulja od 255 okteta.

Niža četiri bita okteta (bitovi 4-7) polja zastavica se ne koriste. Oni moraju biti nula i moraju biti ignorirani po primitku.

Drugi oktet polja tipa atributa je polje koda tipa atributa (*Attribute Type Code*). Trenutno definirani kodovi tipa atributa opisani su u sljedećim odlomcima.

b) Ukoliko je bit produljene duljine (*Extended Length bit*) u oktetu zastavica atributa (*Attribute Flags*) postavljen na 0, treći oktet polja atributa puta, odnosno drugi član ranije navedenog polja, polje duljine atributa je duljine jednog okteta i sadrži vrijednost duljine trećeg člana, odnosno vrijednosti atributa u oktetima.

Ukoliko je bit produljene duljine u oktetu zastavica atributa postavljen na 1, treći i četvrti oktet polja atributa puta, odnosno drugi član ranije navedenog polja, polje duljine atributa je duljine dva okteta i sadrži vrijednost duljine trećeg člana, odnosno vrijednosti atributa u oktetima.

c) Preostali okteti polja atributa puta predstavljaju vrijednost atributa i oni se interpretiraju u skladu s vrijednošću polja zastavica atributa i polja koda tipa atributa. Podržane vrijednosti polja koda tipa atributa, vrijednosti samih atributa i njihova uporaba opisane su u sljedećim odlomcima.

- Polje *Network Layer Reachability Information*:

Ovo polje varijabilne duljine sadrži listu IP prefiksa. Duljina ovog polja u oktetima nije posebno nigdje zapisana, ali se može posredno izračunati iz duljine ostalih polja formulom:

*len(UPDATE) - 23 - len(Total Path Attribute) - len(Unfeasible Routes)*

gdje je *UPDATE message Length* vrijednost zapisana u zaglavlju bilo koje BGP poruke koja je uvijek fiksne veličine, *Total Path Attribute Length* i *Unfeasibile Routes Length* su vrijednosti zapisane u promjenjivom dijelu UPDATE poruke, a 23 je ukupna duljina zaglavlja BGP poruka koje je uvijek fiksne duljine (19), polja *Total Path Attribute Length* (2) i polja *Unfeasibile Routes Length* (2).

*Network Layer Reachability Information* polje sastoji se od jednog ili više parova sastavljenih od 2 člana, duljine i prefiksa. Ova dva člana jednako su formatirana kao i članovi polja *Withdrawn Routes*.

a) Polje Length sadrži duljinu u bitovima IP prefiksa, odnosno duljinu mrežne maske dotičnog prefiksa.

a) Polje Prefix sadrži IP prefiks kojem slijedi dovoljan broj pratećih bitova da bi se dostigla granica okteta. Vrijednost je pratećih bitova irelevantna.

Minimalna duljina UPDATE poruke iznosi 23 okteta; 19 okteta za zaglavlje BGP poruke, 2 okteta za polje *Unfeasible Routes Length* i 2 okteta za polje *Total Path Attribute Length*. U tom su slučaju zadnja dva polja jednaka 0 te time označavaju da nema drugih polja. UPDATE poruka može oglašavati samo jednu rutu koja može biti opisana s više atributa, dok su neki atributi uvijek obavezni. Svi atributi u jednoj UPDATE poruci odnose se na sve mreže, odnosno sve prefikse oglašene u toj poruci kroz polje NLRI. Osim toga UPDATE poruka može sadržavati više prefiksa koji se povlače iz uporabe, a koji su navedeni u polju Withdrawn Routes. Budući da susjedni BGP

usmjernici razmjenjuju samo po jednu rutu za svaki prefiks, ovakav način povlačenja jednoznačno određuje kombinciju rute i prefiksa koji se povlači. Naravno da UPDATE poruka može sadržavati i samo oglašenu novu rutu i samo povučene prefikse, odnosno ne mora nužno sadržavati oboje, ali i može. Ukoliko UPDATE poruka samo povlači prefikse, tada neće biti polja atributa puta kao niti polja NLRI. Ako pak UPDATE poruka samo oglašava rutu, tada neće biti polja s povučenim prefiksima. Slijedi popis i objašnjenje atributa o putu.

- **Origin**

Izvor je opće poznati obvezni atribut koji sadrži izvor informacije o ruti. Može imati sljedeće vrijednosti:

- 0 IGP – Prefiks ili prefiksi unutrašnji su prefiksi od izvorišnog AS-a
- 1 EGP – Prefiks je naučen putem EGP-a
- 2 INCOMPLETE – Prefiks je naučen nekom drugom metodom

Vrijednost koda tipa (*Type Code*) za ovaj je atribut 1.

- **AS Path**

AS Path je općepoznat obvezan atribut koji je sastavljen od sekvence AS Path segmenata. Svaki AS Path segment je predstavljen trojkom: tip segmenta (*path segment type*), duljina segmenta (*path segment length*) i vrijednost (*path segment value*).

Tip segmenta je polje duljine jedan oktet sa sljedećim vrijednostima:

- 1 AS_SET – neporedan set AS-ova koji vode prema prefiksu
- 2 AS_SEQUENCE – poredan set AS-ova koji vode prema prefiksu

Duljina segmenta je polje duljine jedan oktet koje sadrži broj AS-ova u sljedećem polju vrijednosti (*path segment value field*).

Polje vrijednosti sadrži jedan ili više brojeva AS-a, svaki kodiran kao sa 2 okteta (za 16-bitne brojeve AS-ova).

Vrijednost koda tipa za ovaj je atribut 2.

- **Next Hop**

Sljedeći skok je općepoznat obvezni atribut koji definira IP adresu rubnog usmjernika koja bi se trebala koristiti kao sljedeći skok prema mreži, prefiksu ili prefiksima, navedenoj u polju NLRI te UPDATE poruke.

Vrijednost koda tipa za ovaj je atribut 3.

- **Multi Exit Discriminator**

Atribut višestrukih izlaza je opcionalni netranzitivni atribut koji je prikazan pozitivnom cjelobrojnom vrijednošću od četiri okteta. Vrijednost ovog atributa može poslužiti BGP usmjerniku prilikom odlučivanja između višestrukih izlaznih točaka prema susjednom autonomnom sustavu.

Vrijednost koda tipa za ovaj je atribut 4.

- **Local Preference**

Atribut lokalne preferencije je općepoznati neobvezan atribut koji je prikazan pozitivnom cjelobrojnom vrijednošću od četiri okteta. Koristi ga BGP usmjernik da bi obavijestio druge usmjernike u svom autonomnom sustavu o svom stupnju preferencije prema oglašenoj ruti.

Vrijednost koda tipa za ovaj je atribut 5.

- **Atomic Aggregate**

Atribut *Atomic Aggregate* je općepoznati neobvezan atribut duljine 0. Koristi ga BGP usmjernik kako bi informirao druge BGP usmjernike da je lokalni sustav izabrao rutu kraće mrežne maske bez slanja objave o ruti dulje mrežne maske koja je sadržana u prvoj.

Vrijednost koda tipa za ovaj je atribut 6.

- **Aggregator**

Atribut Aggregator je opcionalni tranzitivni atribut duljine 6. Ovaj atribut sadrži broj AS-a posljednjeg sustava koji je stvorio agregiranu rutu, zapisano u 2 okteta te IP adresu BGP usmjernika koji je tu agregiranu rutu stvorio, 4 okteta.

Vrijednost koda tipa za ovaj je atribut 7.

## 2.3 AS Path atribut

AS Path je općepoznati obvezan atribut. Sadrži brojeve autonomnih sustava kroz koje je UPDATE poruka prošla. Na početku je liste broj posljednjeg AS-a kroz koji je prošla informacija o tom prefiksu, odnosno broj AS-a koji je našem AS-u objavio taj prefiks. Na začelju je liste broj AS-a koji je izvor navedenog prefiksa. Izvor prefiksa je autonomni sustav u kojem se nalazi mreža ili mreže koje su sadržane u navedenom prefiksu. Iznimka ovom pravilu slučaj je agregacije prefiksa gdje AS agregator ne mora sadržavati sve ili neke mreže koje su sadržane u prefiksu. Osnovna je namjena atributa AS Path osiguravanje usmjeravanja bez petlji; naime svaki usmjernik koji primi objavu prefiksa s atributom AS Path u kojem se nalazi i njegov broj AS-a, zanemarit će tu objavu jer će u suprotnom stvoriti petlju. Druga namjena atributa AS Path odabir je najboljeg puta. Sam algoritam ima više kriterija, a duljina AS Path atributa, odnosno broj autonomnih sustava u atributu predstavlja svojevrsnu metriku udaljenosti u jednom od koraka algoritma. Treća je namjena atributa implementacija politika usmjeravanja i filtriranje objava; poznavajući kroz koje je autonomne sustave prošla pojedina objava, usmjernik može tu objavu propustiti, zanemariti, promijeniti ili je vrednovati na razne načine već u skladu sa svojom konfiguracijom postavljenom od strane mrežnih administratora u cilju ostvarivanja zacrtane politike usmjeravanja dotičnog autonomnog sustava. Također pomoću ovog atributa možemo skicirati položaj i odnose autonomnih sustava, možemo snimati i bilježiti statističke informacije te nam na kraju ovaj atribut predstavlja ključnu informaciju prilikom vrednovanja reputacije autonomnih sustava što je opisano u 4. poglavlju.

AS Path atribut sastavljen je od jednog ili više segmenata. U općoj formi BGP-a, ovi segmenti mogu biti u obliku dva različita tipa:

- 1 AS_SET – neporedan set AS-ova kroz koje prolazi prefiks u UPDATE poruci
- 2 AS_SEQUENCE – poredan set AS-ova kroz koje prolazi prefiks u UPDATE poruci

Kada BGP usmjernik objavljuje prefiks koji je naučio od svojih susjeda, modificira atribut AS Path ovisno o lokaciji BGP susjeda kojem šalje taj prefiks. AS Path atribut ne mijenja se kada se prefiks

objavljuje iBGP susjedu koji se nalazi u istom autonomnom sustavu. AS Path se mijenja kada se prefiks objavljuje eBGP susjedu koji se nalazi u drugom autonomnom sustavu na sljedeće načine:

1) Kada je prvi segment AS Path atributa tipa *AS Sequence*, usmjernik dodaje na početak liste svoj vlastiti broj AS-a. Sekvenca je uvijek u obrnutom poretku tako da je posljednji element sekvence zapravo posljednji dodani element te se nalazi na početku same liste, odnosno sekvence.

1) Kada je prvi segment AS Path atribut tipa *AS Set*, usmjernik dodaje novi segment tipa AS Sequence ispred već postojećeg segmenta u atribut AS Path stavljajući svoj vlastiti broj autonomnog sustava u novi segment.

2) Ako je atribut AS Path prazan, usmjernik stvara *AS Sequence* segment, stavlja u njega svoj vlastiti broj autonomnog sustava i stavlja taj novi segment u AS Path atribut.

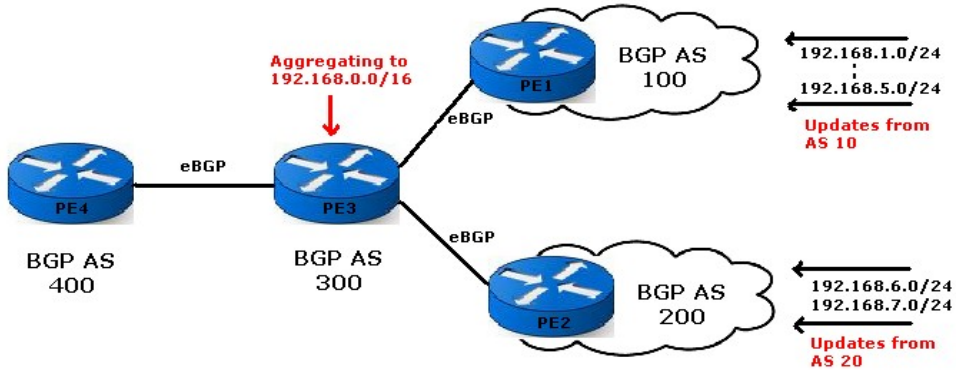
Kada BGP usmjernik objavljuje prefiks koji sam posjeduje:

1) Izvorišni BGP usmjernik stavlja svoj vlastiti broj autonomnog sustava u segment tipa *AS Sequence* koji stavlja u AS Path atribut UPDATE poruka koje šalje svojim eBGP susjedima. Tako će AS Path atribut imati samo jedan segment te će taj segment sadržavati samo jedan broj AS-a.

2) Izvorišni BGP usmjernik postavlja prazan AS Path atribut u sve UPDATE poruke koje šalje svojim iBGP susjedima.

Neporedani skup brojeva AS-ova koji se nalazi u segmentu tipa AS Set predstavlja popis svih AS-ova kroz koje se dolazi do nekog od prefiksa sadržanih u superprefiksu objavljenom tom UPDATE porukom. Budući da je globalna BGP tablica velika te sve više raste, agregacija je prefiksa uvedena kao postupak smanjivanja unosa u BGP tablicama. Agregacija je postupak smanjivanja broja prefiksa obuhvaćanjem više pojedinačnih prefiksa jednim superprefiksom. Pri tome je nužno da su svi agregirani prefiksi sadržani u superprefiksu, ali nije nužno da se prefiksi nastali deagregiranjem superprefiksa zaista mogu doseći. Tako primjerice prefikse 141.29.4.0/24, 141.29.5.0/24 i 141.29.6.0/24 možemo agregirati u superprefiks 141.29.4.0/22. Taj superprefiks također sadržava svoj potprefiks 141.29.7.0/24. Takva je agregacija i oglašavanje superprefiksa dozvoljena premda potprefiks 141.29.7.0/24 možda nije dohvatljiv putom navedenim uz superprefiks 141.29.4.0/22. Potprefiksi koji sudjeluju u agregaciji mogu potjecati iz različitih AS-ova ili imati različite atribute AS Path. Tada usmjernik koji obavlja agregaciju sve te brojeve AS-ova iz svih atributa AS Path koji sudjeluju u agregaciji stavlja u neporedani skup u segment tipa AS Set. Njega pak stavlja na začelje segmenata atributa AS Path prilikom objave UPDATE porukama svojim susjedima. Navedena se pojava lijepo može opisati sljedećim primjerom sa slike 2.3.

Na slici 2.3 usmjernik PE1 dobiva prefikse 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24, 192.168.4.0/24 i 192.168.5.0/24 iz AS-a 10. Usmjernik PE2 dobiva prefikse 192.168.6.0/24 i 192.168.7.0/24 iz AS-a 20. Oba ta usmjernika, PE1 i PE2 objavljuju te prefikse usmjerniku PE3 u autonomnom sustavu 300. Pritom PE1 usmjernik dodaje na početak liste AS Path svoj broj AS-a 100 dok usmjernik PE2 dodaje svoj broj AS-a 200. Tako usmjernik PE3 koristi AS-ove [100, 10] da dođe do prefiksa u AS-u 10, a AS-ove [200, 20] da dođe do prefiksa u AS-u 20. Uglatim zagradama označavamo segment tipa AS Sequence. U njemu se točno zna poredak AS-ove kojima se dolazi do određenog prefiksa. Usmjernik PE3 objavljuje navedene prefikse dalje usmjerniku PE4 u AS 400 te na početak liste dodaje svoj broj autonomnog sustava 300. Tako da BGP tablica usmjernika PE4 izgleda kao na ispisu 2.1, a vrijednost atributa AS Path u UPDATE porukama došlima usmjerniku PE4 iznosi [300, 100, 10], odnosno [300, 200, 20].




*Slika 2.3. Agregiranje i AS Set segment*

```
   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      34.1.1.1                               0 300 100 10 i
*> 192.168.2.0      34.1.1.1                               0 300 100 10 i
*> 192.168.3.0      34.1.1.1                               0 300 100 10 i
*> 192.168.4.0      34.1.1.1                               0 300 100 10 i
*> 192.168.5.0      34.1.1.1                               0 300 100 10 i
*> 192.168.6.0      34.1.1.1                               0 300 200 20 i
*> 192.168.7.0      34.1.1.1                               0 300 200 20 i
```

*Ispis 2.1. Neagregirani ispis BGP tablice usmjernika PE4*

Agregiranjem prefiksa dobivenih od usmjernika PE1 i PE2, usmjernik PE3 stvara agregiranu rutu koja dalje objavljuje usmjerniku PE4. BGP tablica usmjernika PE4 tada izgleda kao na ispisu 2.2.

```
   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.0.0/16   34.1.1.1                 0             0 300 i
*> 192.168.1.0      34.1.1.1                               0 300 100 10 i
*> 192.168.2.0      34.1.1.1                               0 300 100 10 i
*> 192.168.3.0      34.1.1.1                               0 300 100 10 i
*> 192.168.4.0      34.1.1.1                               0 300 100 10 i
*> 192.168.5.0      34.1.1.1                               0 300 100 10 i
*> 192.168.6.0      34.1.1.1                               0 300 200 20 i
*> 192.168.7.0      34.1.1.1                               0 300 200 20 i
```

*Ispis 2.2. Agregirani ispis BGP tablice usmjernika PE4*

Budući da su sada pojedinačne rute za potprefikse nepotrebne, moguće je na usmjerniku PE3 izostaviti ih iz objavljivanja dalje usmjerniku PE4 te ostaviti objavljivanje samo zajedničke agregirane rute. Tada se na usmjerniku PE4 dobiva tablica kao u ispisu 2.3.

```
   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.0.0/16   34.1.1.1                 0             0 300 i
```

*Ispis 2.3. Samo agregirani ispis BGP tablice usmjernika PE4*

Vidimo da su u oba slučaja u atributu AS Path koji se objavljuje usmjerniku PE4 prisutni samo brojevi AS-a 300. Čini se kao da je on izvorišni AS prefiksa 192.168.0.0/16. To tako i jest jer je upravo AS 300 agregiranjem stvorio taj prefiks premda on sam nema mrežu ili podmreže koje pripadaju navedenom prefiksu. U ovom slučaju stvarni izvorišni AS-ovi 10 i 20 kao i tranzitni AS-ovi 100 i 200 ostaju skriveni te usmjernik PE4 nema saznanja o njima. To se može ispraviti stvaranjem segmenta AS Set i postavljanjem takvog segmenta na početak atributa AS Path od strane agregirajućeg usmjernika. U segmentu AS Set pobrojani su neporedano svi izvorišni i tranzitni AS-ovi za sve potprefikse agregiranog prefiksa. Tada će BGP tablica na usmjerniku PE4 izgledati kao na ispisu 2.4.

```
   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.0.0/16   34.1.1.1                 0             0 300 {100,10,200,20} i
```

*Ispis 2.4. Agregirani ispis BGP tablice usmjernika PE4 sa segmentom AS Set*

## 2.4 Autonomni sustavi

Na Internetu, autonomni sustav je skup mreža, odnosno adresnih prefiksa pod upravljanjem jednog ili više operatera koji predstavlja jedinstvenu jasno definiranu politiku usmjeravanja. Sam je Internet stoga podijeljen na autonomne sustave te svako računalo s IP adresom na Internetu mora biti dio nekog autonomnog sustava. Budući da održavanje svake mreže zahtijeva financijska sredstva, tako i održavanje samog Interneta zahtijeva značajna ulaganja. Iako je Internet globalna mreža, osim načelnih pravila komunikacije definiranih standardima, brigu oko financijskog aspekta rada Interneta ne može preuzeti niti jedna globalna organizacija. S druge pak strane to nije ni potrebno jer po svojoj prirodi Internet nije ništa više od skupa mreža povezanih zajedno. Iza apstraktnog pojma autonomnog sustava zapravo se skriva stručni termin za ono što svaka od tih mreža koje zajedno povezane čine Internet zapravo i jesu, svaka od njih je sustav za sebe, svaka od njih ima jasno određene granice te sama određuje politiku svojih odnosa s drugim sustavima. Kako se poslovna ili financijska korist ostvaruje zbog ostvarivanja komunikacije, tako i sami autonomni sustavi određuju s kime će i pod kojim uvjetima komunicirati. U skladu s time, autonomni sustavi sami stvaraju veze prema drugim sustavima i u međusobnom dogovoru usmjeravaju promet prema njima kako bi zadovoljili potrebe za komunikacijom. Iza pojedinog autonomnog sustava nalazi se jedna organizacija, najčešće su to tvrtke za davanje pristupa Internetu (ISP-ovi), velike tvrtke koje imaju velike mreže za svoje potrebe, razne velike ustanove i slično. Zaista je zapanjujuće kako dobro funkcionira povezanost na cijelom Internetu kada vidimo koliko je slobodno i decentralizirano sam Internet ustrojen.

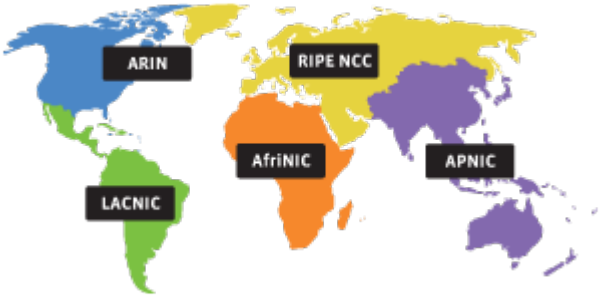
## 2.5 Brojevi autonomnih sustava

Definicija autonomnog sustava iz dokumenta RFC 1771 zahtijevala je da on bude upravljan od

strane jednog entiteta, organizacije, najčešće davatelja pristupa Internetu (ISP-a) s neovisnim vezama prema raznim mrežama koji ima jasno definiranu politiku usmjeravanja. Kasnije u RFC-u 1930 [19] uvedena je mogućnost korištenja privatnih autonomnih sustava kojima se onda organizacije povezuje prema ISP-ovima. Taj je način analogan korištenju privatnog IP adresnog prostora za korisnike koji se onda povezuje na ISP-ove od kojih dobivaju pristup na Internet. Jedna organizacija može isto tako imati više autonomnih sustava kojima upravlja koji onda zajednički održavaju jedinstvenu politiku usmjeravanja. Svaki AS mora imati jedinstveni broj autonomnog sustava. Jedinstvenost ovog broja nužna je zbog njegove uporabe u samom BGP-u. Također svaki broj autonomnog sustava na jedinstven način određuje taj sustav na Internetu. Do 2007. brojevi AS-ova bili su 16-bitne cjelobrojne vrijednosti što je dozvoljavalo ukupno 65536 dodjela brojeva. Glavna međunarodna organizacija za dodjelu brojeva IANA (*Internet Assigned Numbers Authority*) odredila je da se brojevi od 64512 do 65534 koriste za privatne mreže. Također, brojevi 0, 56320-64511 te 65535 ostavljeni su rezervirani i ne bi trebali biti korišteni za potrebe usmjeravanja. Neki su pak brojevi rezervirani za buduće potrebe. Svi ostali brojevi autonomnih sustava (1-54271) dodjeljuju se od strane IANA-e pojedinim autonomnim sustavima. Zaista, organizacija postaje autonomni sustav dodjelom jedinstvenog broja autonomnog sustava. RFC 4893 [20] uveo je 32-bitne AS brojeve koje je IANA počela alocirati. Sredinom 2010. u globalnoj BGP tablici nalazilo se oko 35000 jedinstvenih brojeva autonomnih sustava.

## 2.6 Registratori

IANA ne dodjeljuje izravno brojeve pojedinim autonomnim sustavima već to radi posredstvom područnih Internetskih registratora ili RIR-ova (Regional Internet Registry). Svakom RIR-u dodijeli se raspon AS brojeva koje on onda poslije dodjeljuje AS-ovima u području za koje je zadužen. Kada neka organizacija želi postati autonomni sustav i dobiti broj, mora ga zatražiti od svog lokalnog registratora. Na slici 2.4 vidimo zemljopisni raspored pet registratora koji pokrivaju svaki svoj dio svijeta. Za područje cijele Europe, a tako i Hrvatske zadužen je RIPE.




*Slika 2.4. Zemljopisni raspored registratora*

Zadaće samih registratora nisu samo puko dodjeljivanje brojeva, već donošenje globalnih pravila ponašanja autonomnih sustava i njihov nadzor. Međutim to se često pokazalo teškom zadaćom. Mnogi AS-ovi zbog poslovne odluke i poslovnih tajni često ne otkrivaju svoj odnos s drugim AS-ovima te je zbog toga teško pratiti globalno ponašanje, usmjeravanje i politike usmjeravanja pojedinih AS-ova. Unatoč postojanju IANA-e i pet registratora, Internet nije hijerarhijski organiziran, točnije, samo ustrojstvo Interneta i veze među pojedinim AS-ovima povode se za trenutnim stanjem i poslovnim odlukama, a ne za nekom globalno utvrđenom i predefiniranom shemom.

## 2.7 Usmjeravanje na Internetu

Usmjeravanje je postupak odabira puta kroz mrežu kojim će se slati promet. Svaka mreža mora imati riješeno usmjeravanje pa tako i mreže koje koriste preklapanje paketa. Za male, jednostavne mreže gdje promjene nisu česte, koristi se statičko usmjeravanje u kojem su unaprijed dogovoreni i uneseni putevi u konfiguraciju usmjernika. Pri statičkom usmjeravanju sami se usmjernici ne mogu prilagođavati promjenama topologije mreže. Zbog toga je za usmjeravanje na većini mreža potrebno implementirati usmjerničke protokole koji omogućuju automatsku i samostalnu razmjenu podataka o mreži i putovima između usmjernika te odabir puta za prosljeđivanje prometa. Time se postiže dinamičko prilagođavanje trenutnom stanju i promjenama na mreži bez uplitanja ljudskog faktora te se omogućava neprestano funkcioniranje i povezanost same mreže. Usmjernički protokoli dijele se u dvije grupe:

- Protokoli vektora udaljenosti

  koriste se Bellman-Fordovim alogritmom za razmjenu podataka o mreži i odabir puta. Ovaj algoritam dodjeljuje brojčanu vrijednost (cijenu) svakoj vezi između čvorova na mreži. Tako će se promet usmjeravati od ishodišta do odredišta putem koji ima najmanju cijenu. U početku svaki čvor vidi samo svoje susjede i cijene slanja prometa prema njima. Razmjenom informacija među čvorovima, svaki čvor od susjeda dobiva imformacije o njihovim susjedima zajedno s pripadajućom cijenom. Pomoću algoritma vrši se odabir najboljeg puta prema pojedinom odredištu, onog puta s najmanjom cijenom te se taj put sprema u tablicu i prosljeđuje dalje svojim susjedima. Niti jedna točka u mreži ne poznaje izgled cijele mreže, već samo zna koja je sljedeća točka na koju treba poslati promet, ako želi postići najmanju cijenu slanja tog prometa prema odredištu. Tako se uz svaki prefiks veže ukupna cijena slanja prema odredištu i samo adresa sljedećeg čvora u mreži, odnosno usmjernika.

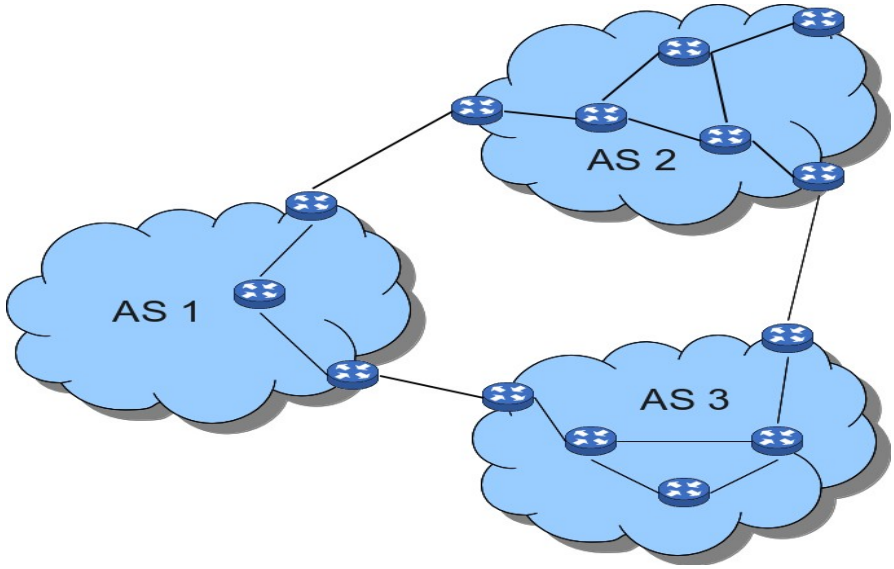
- Protokoli stanja veze

  koriste se Dijkstrinim algoritmom za razmjenu podataka o mreži i odabir najboljeg puta. Svaki čvor u mreži šalje podatke o sebi svim ostalim čvorovima odnosno preplavljuje cijelu mrežu. Na taj će način svaki čvor u mreži imati iste informacije te će imati saznanje o cjelokupnoj topologiji mreže. Svaki će čvor, odnosno usmjernik samostalno izračunati najbolje puteve prema svim odredištima; budući da svi rade istim algoritmom, ti će podaci biti koncizni odnosno najbolji putovi na pojedinim usmjernicima neće biti proturječni stvarajući tako petlje u mreži. Na taj način svaki usmjernik stvara stablo cijele mreže sa sobom u korijenu stabla te iz toga stabla za svaki prefiks izvlači adresu sljedećeg usmjernika kroz koji će odabrani put imati najmanju cijenu.

Protokoli vektora udaljenosti poput RIP-a i EIGRP-a te protokoli stanja veze poput OSPF-a i IS-IS-a zahtijevaju puno razmjene informacija između usmjernika na mreži. To ih ne čini pogodnima za usmjeravanje na Internetu koji se sastoji od tisuća i tisuća usmjernika. Navedeni se protokoli koriste unutar zatvorenih mreža i autonomnih sustava te se stoga i nazivaju protokoli unutrašnjeg usmjeravanja (IGP). Nasuprot njima za usmjeravanje između pojedinih autonomnih sustava koriste se protokoli vanjskog usmjeravanja (EGP). Danas se koristi samo jedan protokol vanjskog usmjeravanja i to je upravo BGP.

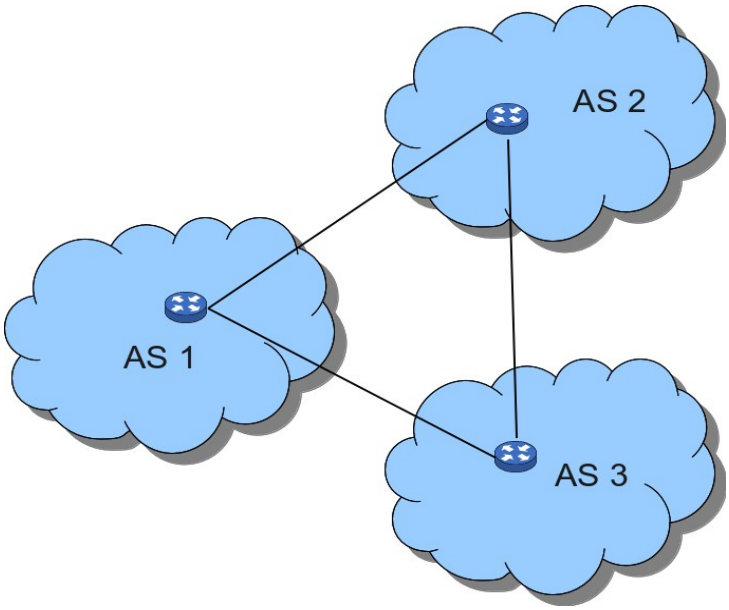
### 2.7.1 BGP kao protokol usmjeravanja na Internetu

Za usmjeravanje u velikim mrežama koje bi bile sastavljene od više autonomnih sustava bilo bi teško koristiti protokole vektora udaljenosti i stanja veze. Ovi prvi bili bi uzrok čestih nestabilnosti i dugih vremena konvergencije za mreže koje imaju više od nekoliko skokova, dok bi ovi drugi zahtijevali puno resursa usmjernika za pohranu cijele topologije mreže te bi opterećivali same veze prilikom preplavljivanja cijele mreže svojim upravljačkim informacijama. Servisne su informacije svi podaci koje usmjernici razmjenjuju u okviru nekog usmjerničkog protokola. BGP je po svojoj prirodi modificirana verzija protokola vektora udaljenosti koji se naziva protokol vektora puta. Za razliku od protokola vektora udaljenosti, BGP ne promatra sve usmjernike već samo neke. Na slici 2.5 prikazana su 3 autonomna sustava s pripadajućim usmjernicima. Budući da je Internet sastavljen od tisuća takvih sustava s velikim brojem usmjernika, protokoli unutrašnjeg usmjeravanja radili bi iznimno opterećeno, sporo i zagušeno ako bi uopće i mogli savladati cijelu silu servisnih informacija.




*Slika 2.5. BGP između autonomnih sustava*

Za potrebe usmjeravanja između pojedinih autonomnih sustava nije potrebno poznavati unutrašnju topologiju samog sustava, već je dovoljno predstaviti svaki sustav kao jednu točku te vršiti usmjeravanje između tih točaka kao što je prikazano na slici 2.6. Sa stajališta drugih autonomnih sustava nije bitno na kojem se usmjerniku nalazi spojena koja mreža, već sve te mreže smatra internim mrežama drugog autonomnog sustava. Kada se primjerice šalje promet iz autonomnog sustava 1 u mrežu koja je spojena na jedan usmjernik u autonomnom sustavu 2, usmjernici AS-a 1 ne moraju znati na kojem je usmjerniku unutar AS-a 2 ta mreža zapravo spojena niti ne moraju znati kojim će se putem unutar samog AS-a 2 taj promet usmjeravati. Za njih je samo bitno da se tražena mreža nalazi negdje unutar AS-a 2 te da se do njega dolazi putem rubnog usmjernika na kojem se izvodi BGP. Tako je adresa rubnog usmjernika AS-a 2 prema AS-u 1 zapravo adresa sljedećeg skoka za sve mreže unutar AS-a 2 koji je sam prikazan kao samo jedan čvor na slici 2.6.



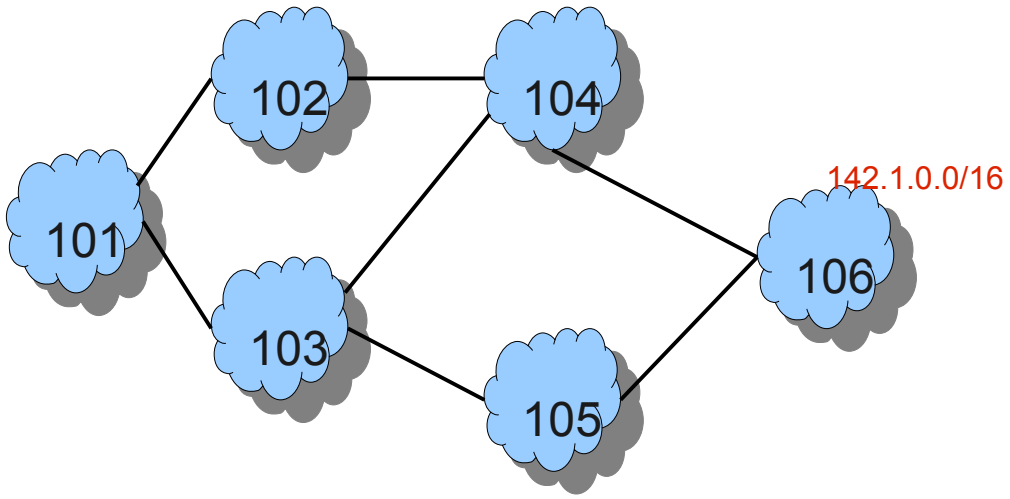

*Slika 2.6. Kako BGP vidi autonomne sustave*

Naravno da situacija nije uvijek ovako jednostavna. Često postoji više točaka povezivanja između pojedinih AS-ova ili se različitim točkama pojedini AS povezuje s različitim susjednim AS-ovima. Kako onda možemo promatrati pojedini AS kao samo jednu točku? Naime svi usmjernici unutar AS koji rade na BGP-u međusobno razmjenjuju usmjerničke informacije i imaju identične tablice s identičnim podacima. Zbog toga svi BGP usmjernici jednog AS-a imaju istu točku sljedećeg skoka za pojedini prefiks. Sam je protokol dizajniran kako bi usmjeravanje bilo jedinstveno za sve granične usmjernike jednog AS-a. Iz toga proizlazi da će usmjeravanje prema mrežama u drugim AS-ovima biti neovisno o točnoj lokaciji izvora prometa unutar pojedinog AS-a. Također će biti neovisno o putu kojim prolazi tranzitni promet unutar pojedinog AS-a. To je u skladu sa zahtjevom da se usmjeravanje između autonomnih sustava vrši na temelju unaprijed dogovorenih politika gdje se cijeli autonomni sustav ponaša kao jedna cjelina te svi njegovi rubni usmjernici usmjeravaju promet na identičan način, odnosno prema identičnim susjednim autonomnim sustavima na temelju odabira prema odredišnom prefiksu. Iz svega ovoga je jasno zašto pojedini autonomni sustav možemo s pravom promatrati kao jednu točku sa stajališta BGP-a, a ne kao skup mnoštva pojedinačnih usmjernika. U slučaju višestrukih veza između dva autonomna sustava u odabiru puta pomažu atributi BGP-a poput lokalne preferencije i višeizlaznog diskriminatora. Jasno je da pritom susjedni AS promatramo kao više međusobno povezanih usmjernika, a ne kao jednu točku, no i tih nekoliko usmjernika svejedno ima jedinstvenu politiku usmjeravanja. Odstupanje od pojednostavljenog prikaza autonomnih sustava samo jednom točkom tako ostaje relevantno samo između susjednih AS-ova i to samo za one usmjernike pomoću kojih ta dva AS-a uspostavljaju susjedski odnos. Za sve ostale AS-ove svejedno možemo koristiti pojednostavljen prikaz.

### 2.7.2 Atribut AS Path i njegova važnost

Atribut AS Path predstavlja poredani popis AS-ova kroz koje promet treba proći na svom putu do određenog odredišta. Atribut AS Path obvezatan je prilikom objavljivanja svakog prefiksa. Početni ili izvorišni AS za pojedini prefiks prilikom objavljivanja prefiksa i slanja obavijesti svojim susjednim AS-ovima stavlja svoj broj AS-u u atribut AS Path. Njemu susjedni AS-ovi prilikom

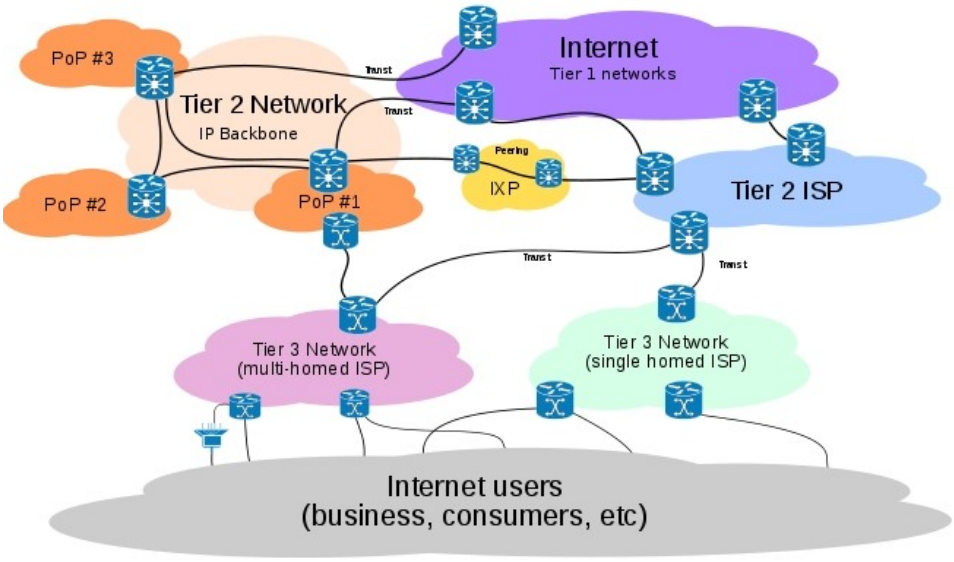
slanja objava za taj prefiks svojim susjedima stavljaju svoj broj AS-a na početak liste, odnosno ispred postojećeg broja izvorišnog AS-a. Tako redom svaki AS prilikom objave prefiksa svojim susjedima stavlja svoj broj na početak liste koja se nalazi u atributu AS Path. Primjerice na slici 2.7 autonomni sustav 106 objavljuje prefiks 142.1.0.0/16 svom susjednom AS-u 104 koji prima objavu s vrijednošću atributa AS Path 106. Autonomni sustav 102 primit će pak objavu za taj prefiks 142.1.0.0/16 od svog susjeda 104 dok će u atributu AS Path biti zapisane redom vrijednosti 104, 106 jer će promet koji se iz AS-a 102 šalje prema tom prefiksu redom prolaziti kroz autonomne sustave 104 pa potom 106. Autonomni sustav 101 dobit će vrijednost atributa 102, 104, 106. Kod BGP-a u izboru najboljeg puta prema odredištu sudjeluju razni atributi. Od svih atributa koji se prenose BGP porukama i koji sudjeluju u procesu odabira najboljeg puta, jedino je atribut AS Path sličan informaciji o cijeni do odredišta koju jedan usmjernik koji radi na protokolu vektora udaljenosti šalje svojim susjedima. Tako atribut AS Path sadrži popis AS-ova kojima taj promet mora proći do odredišta. Nije teško zaključiti da će manji broj AS-ova biti bolji kriterij prilikom odabira najboljeg puta. Za razliku od protokola vektora udaljenosti gdje usmjernik svojim susjedima šalje samo informaciju o cijeni, odnosno ukupnoj udaljenosti do odredišta, BGP šalje točan put kojim taj promet treba proći. Dok se kod prvih možemo ravnati samo po ukupnoj udaljenosti ili cijeni, kod BGP-a možemo u obzir uzeti značajke pojedinog puta te AS-ove kojima promet treba proći prema odredištu, a ne samo puku udaljenost izraženu kao broj AS-ova do odredišta. Istina, sam algoritam odabira puta među raznim kriterijima uzima i u obzir atribut AS Path, ali samo kao ukupnu udaljenost, odnosno broj AS-ova do odredišta. Zapravo se dobar dio usmjeravanja, odnosno odabira puta te daljnjeg prosljeđivanja informacija susjedima ne odvija pod samim algoritmom BGP-a, već vlasnici pojedinih AS-ova na temelju ranije dogovorene politike usmjeravanja primjenjuju filtere na dolazne i odlazne obavijesti te na taj način aktivno utječu na odabir puta i prosljeđivanje informacija susjednim AS-ovima. Zbog toga se BGP naziva protokolom vektora puta, a ne udaljenosti jer je sam naprednija verzija protokola vektora udaljenosti. Usmjeravanje protokolima vektora udaljenosti usmjeravanje je po glasini. Pojedini usmjernik od svoga susjeda dobije ukupnu udaljenost do pojedinog prefiksa, ali sam ne zna kojim će putem dalje taj promet krenuti prema odredištu. Naš usmjernik samo zna kolika je ukupna cijena do tog prefiksa, ako kao sljedeći skok izabere upravo taj susjedni usmjernik. On vjeruje svom susjedu, premda ne zna stvaran put te će isto tako tu informaciju proslijediti svojim susjedima kao glasinu. Za složene tržišne odnose koji vladaju među pojedinim AS-ovima, odnosno ISP-ovima, usmjeravanje na temelju glasine bez stvarnog poznavanja točnog puta prema odredištu je u potpunosti neprihvatljivo. Poznavanje cijelog puta do odredišta, a ne samo sljedećeg skoka tako postaje instrument odabira puta na temelju ranije dogovorenih politika usmjeravanja implementacijom filtera i konfiguriranjem BGP usmjernika. Vrijednost atributa AS Path zapravo ne mora nužno biti točan put prema odredištu, odnosno ne mora predstavljati obrnuti poredak AS-ova kroz koje je prošla objava pojedinog prefiksa. Istina, tako bi trebalo biti, međutim u praksi neki AS-ovi znaju namjerno promijeniti stvarnu vrijednost tog atributa šaljući tako svojim susjedima pogrešne informacije o putu kako bi ostvarili zacrtane politike usmjeravanja. Isto tako je potrebno naglasiti da čak i ako vrijednost atributa AS Path predstavlja stvaran put, odnosno obrnuti poredak propagacije objave prefiksa, samo promet prema tom prefiksu može zbog raznih razloga u konačnici biti usmjeren drugim putem.




*Slika 2.7. Propagacija prefiksa i promjena atributa AS Path*

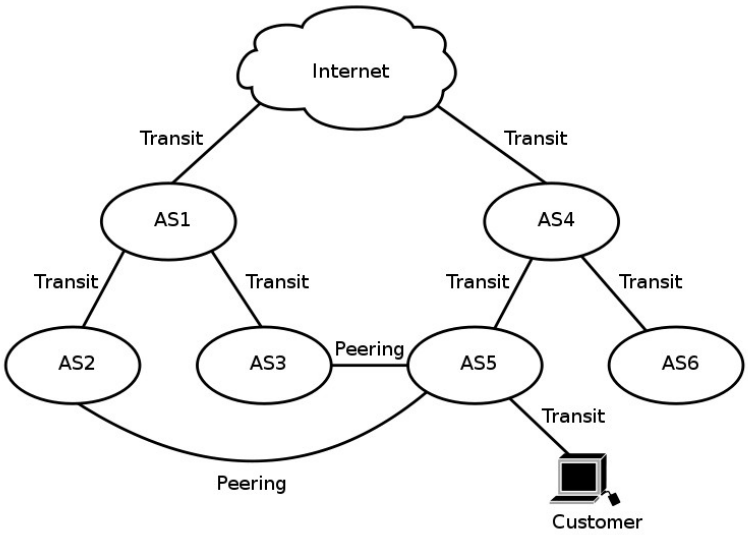
### 2.7.3 Razine autonomnih sustava

Kako bismo lakše razumjeli odnose između pojedinih autonomnih sustava, svrstavamo ih u pojedine razine. Ne postoji univerzalni niti općeprihvaćeni način određivanja koje je razine pojedini autonomni sustav. Samo se svrstavanje provodi empirijski te nikada nema oštre granice. AS-ovi više razine daju pristup ostatku Interneta AS-ovima niže razine. I obrnuto, AS-ovi niže razine obraćaju se AS-ovima više razine kako bi ih povezali s ostatkom Interneta. AS-ovi iste razine također mogu biti povezani zajedno. Uobičajeno je svrstavati AS-ove u tri razine gdje je razina 1 najveća te obuhvaća samo najveće AS-ove s razvijenom globalnom infrastrukturom. Autonomni sustavi druge razine služe kao davatelji pristupa za regionalne i manje nacionalne ISP-ove te služe povezivanju ISP-ova na koje se spajaju krajnji korisnici s velikim autonomnim sustavima koji služe tranzitu prometa preko velikih zemljopisnih udaljenosti.
Na slici 2.8 prikazan je odnos između AS-ova pojedinih razina. Vidimo da se većina korisnika Interneta za pružanje usluge pristupa Internetu obraća ISP-ovima čiji su autonomni sustavi na najnižoj trećoj razini. Na taj način takav ISP može povezati korisnike samo s drugim korisnicima koji su spojeni na taj isti ISP. Za povezivanje s korisnicima koji su spojeni na druge ISP-ove, potrebno je da prvi ISP zatraži uslugu tranzitnog prometa od ISP-a više razine. Alternativno se dva ISP-a čiji su AS-ovi na trećoj razini mogu direktno povezati za usmjeravanje prometa između njih, no to je rješenje primjenjivo u pravilu samo za manja zemljopisna područja. Autonomne sustave razine 2 obično posjeduju veći ISP-ovi koji usluge pristupa Internetu uglavnom pružaju manjim ISP-ovima ili većim korisnicima. Na taj je način njihov skup klijenata veći te imaju veće mogućnosti povezivanja svojih korisnika, s jednim širim dijelom Interneta nego što to mogu neposredno ISP-ovi AS-ova treće razine. Sami korisnici svoj pristup Internetu plaćaju svom ISP-u koji u većini slučajeva radi na trećoj razini. Oni pak plaćaju povezivanje s ostatkom Interneta AS-u druge razine. Ako taj AS druge razine ovaj promet prosljeđuje svojim korisnicima ili AS-u najviše razine te taj promet samo prolazi kroz navedeni AS, a nema u njemu izvor ili odredište, takav je promet tranzitni promet za navedeni AS. Tranzitni se promet naravno naplaćuje svojim korisnicima.




*Slika 2.8. Prikaz razina autonomnih sustava*

Za povezivanje pak svojih korisnika s cijelim Internetom, ISP-ovi razine 2 obraćaju se vlasnicima autonomnih sustava najveće razine, razine 1. Ukoliko odredište prometa nije neki od korisnika AS-a druge razine, on se mora obratiti AS-u najviše razine te njemu platiti za uslugu tranzita prema udaljenim AS-ovima. U praksi je sasvim jednostavno, AS više razine naplaćuje AS-u niže razine uslugu pristupa i tranzita. Na taj način dolazimo do uobičajene definicije AS-ova prve razine: oni se, naime, moraju moći povezati sa svim drugim autonomnim sustavima bez plaćanja usluge tranzita. U praksi to znači da svi AS-ovi prve razine moraju biti povezani međusobno sa svim ostalim AS-ovima prve razine. AS-ovi iste razine koji su međusobno izravno spojeni nazivaju se partnerski AS-ovi (*peer*s) kao što je prikazano na slici 2.9. U pravilu si oni međusobno ne naplaćuju usluge tranzita [15].




*Slika 2.9. Odnosi između autonomnih sustava*

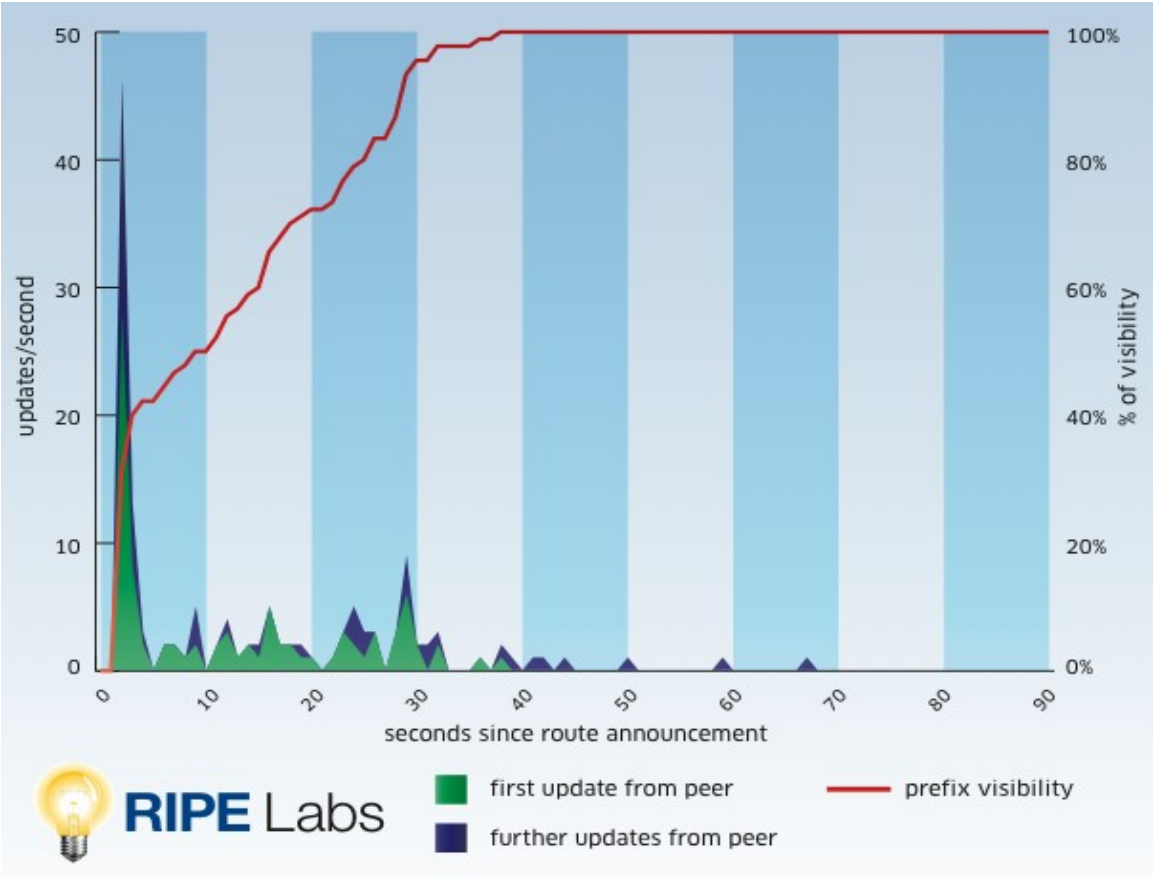
### 2.7.4 Konvergencija BGP-a

Prilikom objave ili povlačenja nekog prefiksa potrebno je određeno vrijeme da se ta informacija proširi kroz Internet. Sama propagacija zahtijeva neko vrijeme. Međutim prilikom primitka novih informacija BGP tablice na usmjernicima mogu se promijeniti te one generiraju nove UPDATE poruke s novim rutama. Taj se postupak iterativno ponavlja sve dok svi usmjernici ne dođu u ciljno stanje usmjeravanja. Tada kažemo da je mreža konvergirala. Za ispunjenje uvjeta konvergencije nužno je da ponovljeno slanje ikoje informacije iz usmjerničkih tablica bilo kojeg usmjernika na mreži neće uzrokovati daljnju propagaciju tih informacija. Vrijeme konvergencije vremenski je interval od slanja početne UPDATE poruke za promatranu informaciju, objavu prefiksa, povlačenje prefiksa ili promjenu atributa puta na nekom usmjerniku do primitka i primjene te informacije na svim ostalim relevantnim usmjernicima. Budući da je globalna BGP tablica jako velika te se neprestano razmjenjuje velik broj UPDATE poruka, možemo reći da Internet nikada u potpunosti ne uđe u stabilno stanje, već uvijek promatramo je li Internet konvergirao za pojedini prefiks. Također prilikom propagacije usmjerničkih informacija dolazi do multiplikacije UPDATE poruka što dodatno opterećuje usmjernike i veze između njih. Kako bismo bolje shvatili navedene fenomene u nastavku je opisan pokus te su navedeni rezultati pokusa koji je proveo registrator RIPE 2. veljače 2011 [4].

Prefiks 84.205.67.0/24 nije bio vidljiv u usmjerničkim tablicama 2. veljače 2011. u 8.00 po univerzalnom vremenu. Tada je prefiks oglašen svakom od 61 direktno spojenog susjeda. Točno 2 sata poslije prefiks je povučen slanjem UPDATE poruka opet svakom od 61 direktno spojenog susjeda. Pritom je mjeren BGP promet koji je generiran ovim dvama događajima putem RIS kolektora promatrajući dolazne UPDATE poruke za njihovih 90 susjeda na cijelom svijetu. RIS je projekt RIPE-a koji skuplja i sprema usmjerničke podatke iz nekoliko lokacija širom svijeta. Na RIPE-ovoj stranici mogu se pogledati prikupljeni podaci. Podaci se prikupljaju usmjernicima koji imaju formirane susjedske odnose s mnogim usmjernicima širom svijeta, ali sami ne usmjeravaju promet. Oni ne šalju susjednim usmjernicima nikakve informacije, već ih od njih samo skupljaju u svrhu istraživanja i dokumentiranja. Prefiks 84.205.67.0/24 jedan je od prefiksa kojima se RIS služi u testne i istraživačke svrhe.

Za objavu prefiksa slika 2.10 [4] prikazuje broj UPDATE poruka po sekundi, plavi i zeleni graf te vidljivost prefiksa odnosno broj usmjernika koji vide navedeni prefiks kao postotna vrijednost u odnosu na ukupan broj promatranih usmjernika, crvena linija. U 0 sekundi na grafu je došlo do inicijalne objave prefiksa. Vidljivost je izračunata kao postotak nastao dijeljenjem broja promatranih usmjernika koji u datom trenutku vide taj prefiks s ukupnim brojem promatranih usmjernika (90). Zelenom površinom prikazan je broj prvih UPDATE poruka koje su poslali usmjernici. Plavom je pak bojom na grafu prikazan broj naknadnih UPDATE poruka na usmjernicima. Ove su druge rezultat slanja boljeg puta svojim susjedima uslijed ponovnog izračuna najboljeg puta nakon primitka novih informacija i predstavljaju normalan tijek konvergencije.

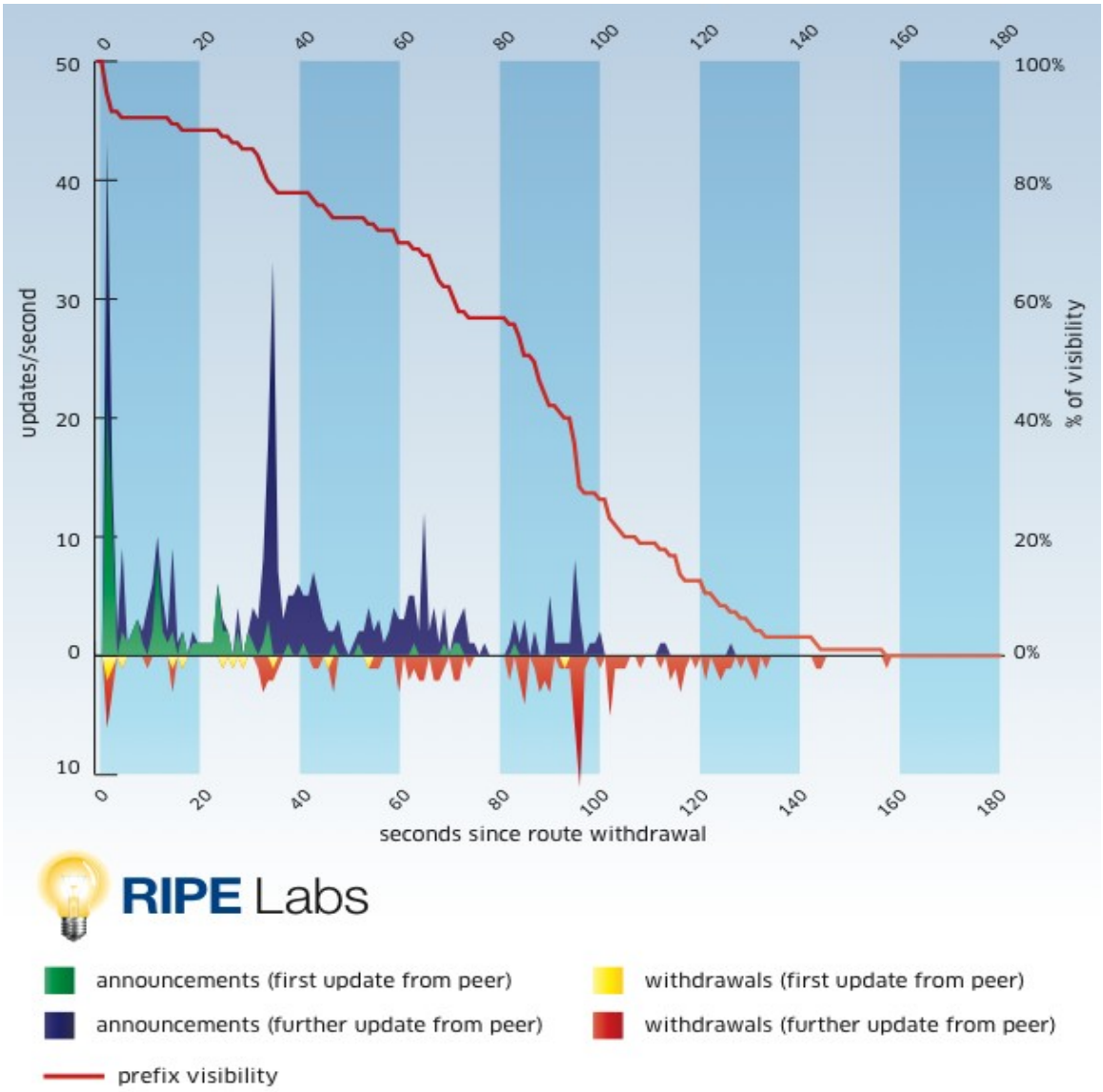
Sav BGP generiran promet dogodio se u vremenu nešto duljem od jedne minute, dok se čak 90% ukupnog prometa odvio u prvih 30 sekundi. Potpuna vidljivost postignuta je nakon 38 sekundi. Gotovo polovica od ukupnog broja UPDATE poruka (46%) su naknadne UPDATE poruke te predstavljaju nekoristan promet postupka konvergencije.




*Slika 2.10. Objava prefiksa - UPDATE poruke i propagacija*

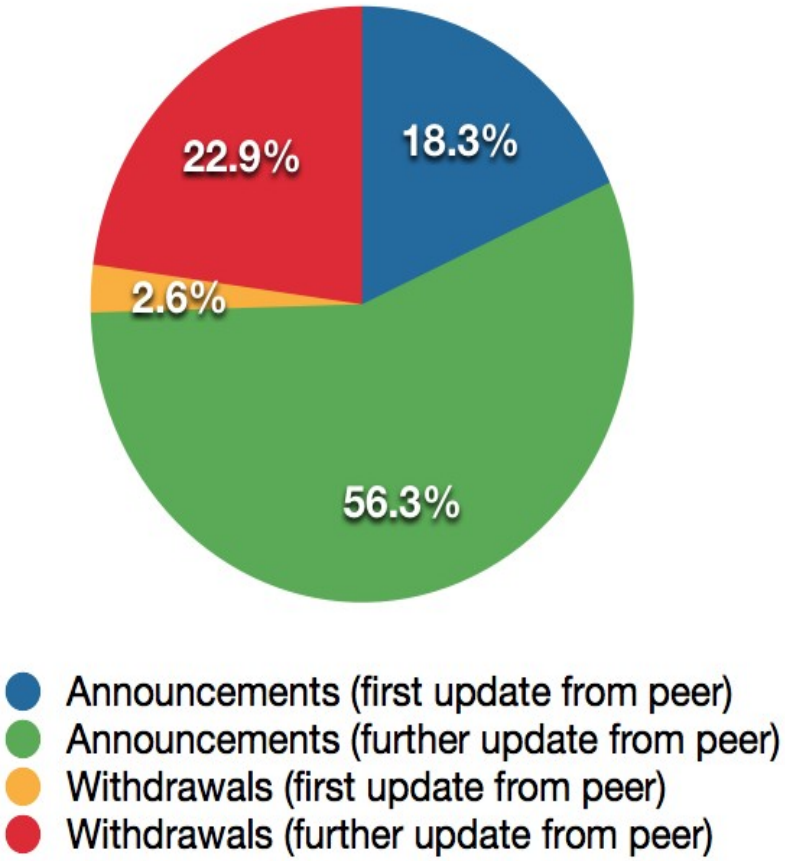
Slika 2.11 [4] prikazuje aktivnost UPDATE poruka za povlačenje prefiksa koje je započelo u 10.00. Na grafu je u pozitivnoj ordinati zelenom bojom prikazan broj prvih objava UPDATE poruka, dok je plavom bojom prikazan broj naknadnih objava. Na negativnoj ordinati prikazan je žutom bojom broj prvih povlačenja UPDATE porukama, dok je crvenom bojom prikazan broj sukcesivnih povlačenja. Generiran obujam prometa za povlačenje prefiksa dosta je veći nego za objavu prefiksa. Ukupan broj UPDATE poruka gotovo je četiri puta veći prilikom povlačenja prefiksa. Ukupna aktivnost mreže, odnosno vrijeme konvergencije, iznosi gotovo 3 minute.

79% svih UPDATE poruka predstavljaju naknadne poruke. To znači da na svaku prvu UPDATE poruku po usmjerniku prosječno se generiraju 4 nove UPDATE poruke koje su nekoristan dio konvergencije. Također samo 25% svih UPDATE poruka su poruke povlačenja prefiksa, što znači da je prosjek po usmjerniku 3 dodatne ponovne objave prije stvarnog povlačenja prefiksa. Većina poruka za povlačenje javlja se jednu minutu nakon početnog povlačenja prefiksa, dok je vidljivost prefiksa još uvijek oko 80%. Tek 90 sekundi nakon početnog povlačenja dolazi do brže konvergencije mreže i naglog pada vidljivosti prefiksa. Potrebno je gotovo 3 minute do nastupa potpune konvergencije.




*Slika 2.11. Povlačenje prefiksa - UPDATE poruke i propagacija*

Usmjernik ne zna je li se povlačenje rute dogodilo zbog povlačenja rute na samom izvoru ili je ruta povučena od strane njegovog susjeda jer je susjed izgubio vezu prema tom autonomnom sustavu. Stoga usmjernik traži u svojoj BGP tablici alternativni put prema povučenom prefiksu. Ako ga nađe, poslat će objavu svojim susjedima s tim drugim putem kojeg je našao u svojoj tablici produljujući na taj način vrijeme konvergencije. Tek kada naposljetku usmjernik ostane bez svih alternativnih putova, izbacit će tu rutu iz BGP tablice i poslat će poruku povlačenja svojim susjedima. Tako nastaje fenomen puno većeg broja UPDATE poruka prilikom povlačenja prefiksa nego li prilikom objave. Štoviše, prilikom povlačenja prefiksa broj UPDATE poruka tipa objave višestruko premašuje broj UPDATE poruka tipa povlačenja. Raspodjela UPDATE poruka po tipu prilikom povlačenja prefiksa prikazana je na slici 2.12 [4].




*Slika 2.12. Raspodjela UPDATE poruka po tipu prilikom povlačenja prefiksa*

Globalno se konvergencija odvija u svega nekoliko minuta. Propagacija novoobjavljenog prefiksa je dosta brza; 50% vidljivosti postiže se za 10 sekundi. Povlačenje prefiksa konvergira kroz nešto dulji vremenski period uz početnu zadršku od 90-ak sekundi velike vidljivosti. Također povlačenje generira 4 puta više BGP prometa nego objava prefiksa. Suvišan promet, pogotovo kod čestih povlačenja, dosta je čest na Internetu. To je posljedica loših konfiguracija usmjernika i politika usmjeravanja autonomnih sustava koji stvaraju puno nepotrebnih objava i povlačenja prefiksa koji su se mogli izbjeći. Takve nepotrebne objave i povlačenja opterećuju usmjernike u susjednim autonomnim sustavima usporavajući konvergenciju te stvaraju veći vremenski prozor kada promet postaje neoptimalno usmjeravana, prefiks privremeno nevidljiv ili nepotrebno dugo vidljiv kada ne bi smio biti. Kako bi se naš autonomni sustav mogao uspješnije nositi s izazovima usmjeravanja na Internetu, u reputacijski je sustav potrebno uvrstiti komponentu koja će kažnjavati autonomne sustave koji uslijed loše konfiguracije generiraju suviše nepotrebnog prometa.

# 3. Pogreške konfiguracije BGP-a

Poznato je da male te čak većim dijelom i slučajne konfiguracijske pogreške kod BGP-a mogu uzrokovati probleme povezanosti na Internetu. Malo se zna o učestalosti pogrešaka ili o njihovim uzrocima osim u slučajevima ispada povezanosti na Internetu širokih razmjera. U radu "Understanding BGP Misconfiguration" [7] proučavane su pogreške konfiguracije te je uočeno da svakodnevno 0,2-1,0% prefiksa iz globalne BGP tablice prolazi kroz konfiguracijske pogreške. Štoviše, 75% svih novoobjavljenih prefiksa posljedica je pogrešaka u konfiguraciji BGP usmjernika. Nasreću, većina tih pogrešaka ne utječe na mogućnost povezivanja krajnjih korisnika. To je također uzrok što većina pogrešaka prođe nezamjećeno jednostavno iz razloga što ih nitko nije mogao zamijetiti. Korisnici u pravilu svojim davateljima usluga prijavljuju greške samo pri gubitku veze. Pod pojmom korisnika smatra se svaki korisnik usluge pristupa Internetu. Sa stajališta globalnih tranzitnih AS-ova to su razni AS-ovi ISP-ova ili drugi tranzitni AS-ovi niže razine. Sa stajališta ISP-ova to su mali korisnici ili drugi manji ISP-ovi. Samo oko 4% svih pogrešaka utječu na gubitak ili probleme prilikom povezivanja, tako da je lako zaključiti da većina grešaka prođe nezamjećeno. Međutim sve pogreške, neovisno uzrokuju li one samo gubitak veze ili ne, dodatno i nepotrebno opterećuju BGP usmjernike što neposredno može uzrokovati druge probleme. Prije svega tu je problem samog opterećenja usmjernika koje u pojedinim slučajevima može dovesti do maksimalnog opterećenja te sporije komunikacije sa susjednim BGP usmjernicima. Samim će time ažuriranje usmjerničkih tablica biti sporije, kao i konvergencija cijele mreže.

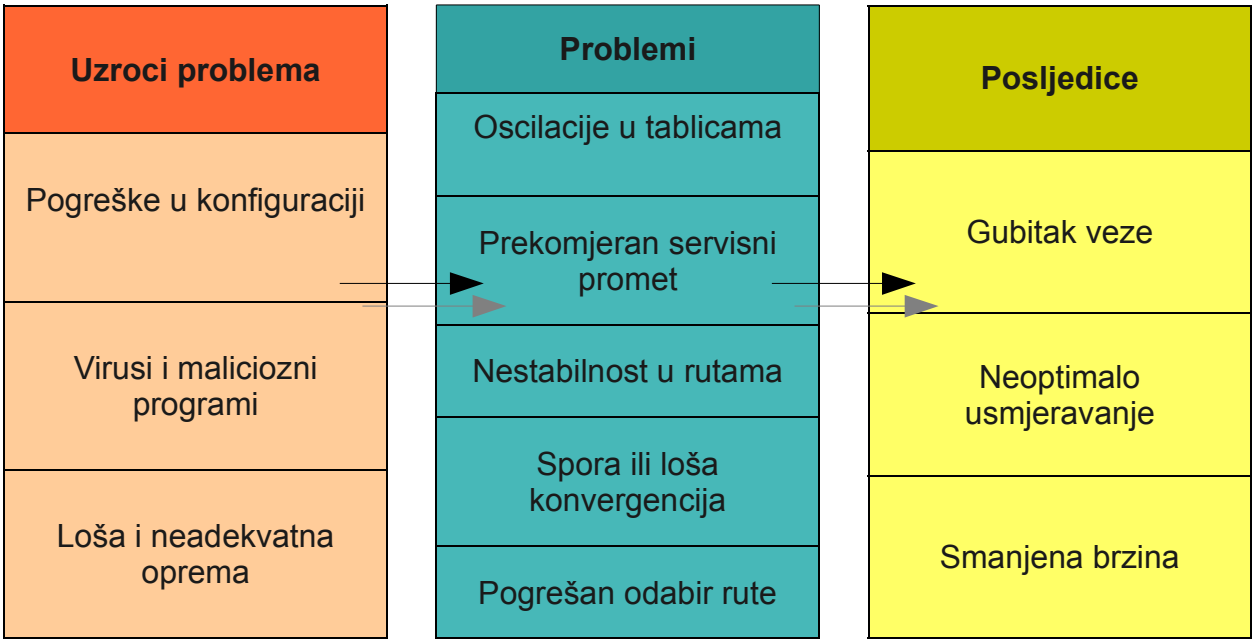
U ovom se poglavlju govori o pogreškama konfiguracije BGP-a. Prvo se iznosi podjela pogrešaka koje mogu nastati zbog loše konfiguracije usmjernika. Zatim se analiziraju pogreške kako bi se vidjelo kako pojedine pogreške nastaju. Nadalje su navedeni rezultati mjerenja pogrešaka koje su provedene u radu "Understanding BGP Misconfiguration" [7] te njihov utjecaj na opterećenje rubnih usmjernika.

## 3.1 Važnost razumijevanja pogrešaka pri konfiguraciji BGP-a

Kao jedini međudomenski usmjernički protokol, BGP je važan za sveukupnu pouzdanost Interneta. Pogreške u implementaciji BGP-a mogu dovesti do ispada povezanosti na velikim dijelovima Interneta. Razni se problemi mogu nametnuti koji ugrožavaju ispravno i stabilno funkcioniranje BGP-a poput oscilacija u usmjerničkim tablicama, prekomjernog servisnog prometa između usmjernika, spore ili loše konvergencije ili nestabilnosti u samim rutama. Pod pojmom servisnog prometa podrazumijevaju se podaci koje razmjenjuju BGP usmjernici kako bi uspostavili i održavali vezu te kako bi razmjenjivali usmjerničke podatke. Uzroci ovih problema koji mogu dovesti do gubitka veze ili neoptimalnog usmjeravanja također mogu biti razni: neispravana ili loša oprema, virusi, pogreške u konfiguraciji i sl. Odnos uzroka problema, manifestacije samih problema i njihovih posljedica prikazan je na slici 3.1. U ovom se poglavlju fokusiramo na pogreške u konfiguraciji usmjernika, bilo slučajne bilo namjerne, koje mogu uzrokovati ranije navedene probleme. Razumijevanje pogrešaka u konfiguraciji ključno je za kasnije osmišljavanje metode otkrivanja pogrešaka te evaluacije reputacije pojedinog autonomnog sustava što je opisano u sljedećim poglavljima.

## 3.2 Podjela pogrešaka pri konfiguraciji BGP-a

Pogreška se definira kao greška u konfiguraciji koja uzrokuje neželjeno stvaranje novih ili povlačenje postojećih BGP usmjerničkih objava. Same greške u konfiguraciji mogu biti jednostavno propusti ili mogu biti greške u samom dizajnu. Ponekad je teško razlučiti je li nešto greška ili nije. Pojedini AS može primjenjivati određenu konfiguraciju, naprimjer uvoditi dodatne petlje u objavljenom putu kako bi postigao određenu politiku usmjeravanja. Dok je za taj AS takva konfiguracija jednostavno način postizanja određenog cilja, odnosno određene politike usmjeravanja, drugi AS-ovi to mogu smatrati pogreškom. Mnoge je pogreške također teško otkriti, pogotovo kada nije došlo do prekida veze ili kada udaljenom promatraču u drugom AS-u sve izgleda regularno. Budući da je teško razlikovati pogreške od stvarne, ali sa stajališta udaljenog promatrača loše konfiguracije, ponajprije zbog odsutnosti uvriježene i univerzalno prihvaćene operativne prakse, svaki AS samostalno može procjenjivati je li pojedina praksa i konfiguracija susjednih ili udaljenih AS-ova za njega dobra ili loša te u skladu s tim određivati reputaciju drugih AS-ova. Za početak je potrebno pogledati koje pogreške pri konfiguraciji BGP-a mogu nastati kako bismo ih kasnije analizirali i predložili rješenja za promatranje, bilježenje i evaluaciju pogrešaka.




*Slika 3.1. Uzroci i posljedice problema kod BGP-a*

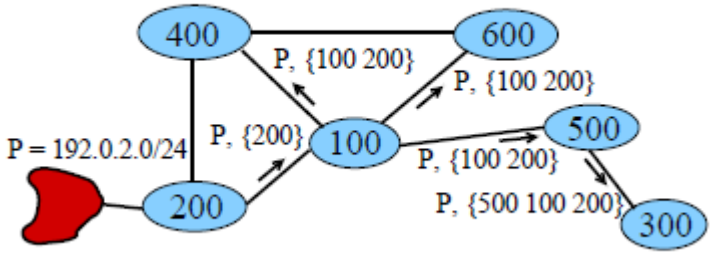
### 3.2.1 Pogreške izvora prefiksa

Pogreške izvora prefiksa (engl. *Origin Misconfiguration*) nastaju kada AS ubaci prefiks u globalnu BGP tablicu. Naravno da je globalna BGP tablica nastala upravo tako što su pojedini AS-ovi ubacivali svoje prefikse u tablicu. Međutim jednom kada se pojedinom AS-u dodijeli određeni prefiks, taj će prefiks dugo vremena, u pravilu godinama, ostati kod tog AS-a. U slučaju kvara i ispada pojedinih veza, prefiks će ili postati privremeno nedostupan, ili će dobiti novi put prema odredištu koji vodi manje dobrim, no ispravnim putem. Pojavljivanje novih prefiksa u globalnoj BGP tablici u većini je slučajeva posljedica pogreške, dok je samo ponekad posljedica promjene

vlasništva nad pojedinim prefiksom ili dijelom prefiksa ili je pak privremena nedostupnost nekog prefiksa.

### 3.2.2 Pogreške izvoza prefiksa

Pogreške izvoza prefiksa (engl. *Export Misconfiguration*) nastaju kada je AS-put u suprotnosti s pravilom politike nekog AS-a na tom putu. Pod pojmom izvoza prefiksa smatra se objava prefiksa BGP susjedu u drugom AS-u oblikovana politikom usmjeravanja. Najčešće se događaju kada usmjernik izveze određenu rutu koju je trebao filtrirati. Naprimjer na slici 3.2 [7] AS 400 može izvesti rutu prema P AS-u 600 protivno njegovoj politici. Takav pogrešan izvoz ruta ili curenje ne samo da može stvoriti suboptimalne puteve ili dodatno opteretiti druge usmjernike stvarajući nepotrebne objave i šaljući ih svojim BGP partnerima, već može stvoriti probleme u konekciji ako drugi AS-ovi na tom putu navedene rute filtriraju.




*Slika 3.2. Izvoz prefiksa iz AS-ova*

### 3.2.3 Druge pogreške u konfiguraciji i posljedice pogrešaka

Pogreške izvora prefiksa i pogreške izvoza prefiksa imaju najveći potencijal da ugroze povezanost na širem području Interneta. Osim ovih postoje i druge pogreške pri konfiguraciji BGP-a, međutim njih uglavnom nije lagano identificirati promatrajući globalnu BGP tablicu. Ako jedan AS, naprimjer filtrira prefiks koji je trebao propustiti, udaljenom promatraču će se ta pogreška činiti jednakom kao i najobičniji gubitak konekcije prema tom prefiksu. Pogreške kod MED atributa bit će vidljive samo susjednim AS-ovima te će za druge promatrače proći nezamjećeno premda mogu utjecati na brzinu veze pa čak i na postojanje same veze. Za potpuno otkrivanje i bilježenje pogrešaka bilo bi potrebno snimati stanje unutar svakog pojedinog AS-a. Ne samo što bi takva metoda bila isuviše složena, već je zbog naravi ustrojstva samog Interneta koji je podijeljen na AS-ove čija je interna politika usmjeravanja tajna, takvo što nemoguće izvesti.

Posljedice pogrešne konfiguracije mogu među ostalim biti sljedeće:

- Opterećivanje usmjernika:

  Pogreške u konfiguraciji povećavaju opterećenje usmjernika stvarajući nepotrebne BGP Update poruke. Mnogi BGP usmjernici su već pod velikim opterećenjem kako zbog obrađivanja puno Update poruka koje dobivaju od svojih susjednih usmjernika, tako i zbog potrebe za pohranom i manipuliranjem velikim BGP tablicama, te je svako dodatno nepotrebno opterećenje potrebno izbjeći.

- Poremećaji u konekciji:

Pogreške u konfiguraciji mogu uzrokovati gubitak ili otežati konekciju prema nekom prefiksu s dijela ili s cijelog Interneta. Protiv poremećaja konekcije treba biti iznimno oprezan te odmah reagirati u slučaju gubitka konekcije.

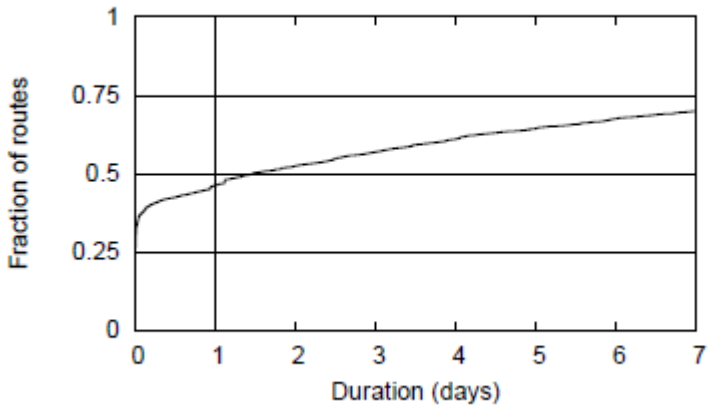
- Povreda politike usmjeravanja:

  Po definiciji, pogreške u konfiguraciji krše predviđenu politiku usmjeravanja pojedinog AS-a; iznimka su regularne politike usmjeravanja koje drugi AS-ovi doživljavaju kao neuvriježene metode konfiguracije te ih smatraju pogreškama. Naprimjer prefiksi mogu pogrešno procuriti prema cijelom Internetu, pogrešno objavljene rute mogu dobiti prioritet u odnosu na željene, AS može pogrešno dozvoliti tranzit drugim AS-ovima.

## 3.3 Analiza pogrešaka pri konfiguraciji BGP-a

Otkriti pogrešku u konfiguraciji u toku BGP Update poruka nije lagan zadatak zbog toga što pogreške izgledaju slično ili jednako kao i obični ispadi ili promjene politike usmjeravanja. U praksi se stoga često pretpostavlja da promjene politike uzrokuju promjene u prefiksima ili rutama koje traju dulji period vremena, dok promjene uzrokovane pogreškama u konfiguraciji najčešće traju kraće vremensko razdoblje.

Na slici 3.3 [7] prikazan je graf ukupne distribucije novih ruta kroz vrijeme izraženo u danima. Iz ovog grafa vidimo da većina novih ruta traju ili manje od jednog dana ili više od tjedan dana; 45% ruta traje manje od jednog dana, dok 30% ruta traju dulje od jednog tjedna. Za pretpostaviti je da prve predstavljaju pogreške izvora prefiksa, dok druge vjerovatno predstavljaju promjene politike usmjeravanja, migraciju prefiksa ili širenje Interneta. Za otkrivanje pogrešaka potrebno se stoga usredotočiti na kratkotrajne promijene koje traju kraće od jednog dana. Međutim i one same mogu biti posljedica legitimnih događaja, poput gubitka veze s dijelom prefiksa koji onda uzrokuju objavljivanje novih ruta ili prefiksa.




*Slika 3.3. Frakcija novih ruta koje traju manje ili jednako x dana*

### 3.3.1 Analiza pogrešaka izvora

Pogreška izvora neželjeno je ubacivanje rute u globalnu BGP tablicu. Ukoliko se takva greška brzo otkrije od strane operatera pojedinog AS-a, ona će trajati samo kratak period vremena te će se

pojaviti kao kratkotrajna nova ruta u tablici. Ispadi pojedinih prefiksa imaju sličnu manifestaciju drugačijeg predznaka, oni uzrokuju kratkotrajne gubitke pojedinih ruta. Pojavljivanje novih ruta zbog promjene politike poput višestrukih veza prema ISP-ovima, upravljanja prometom i promjene davatelja usluge imaju karakteristiku duljeg trajanja u odnosu na one uzrokovane pogreškama u konfiguraciji. Ponekad se legitimni događaji poput balansiranja prometom ili ispada glavnog, a pojavljivanja pomoćnog puta, mogu pokazati kao kratkotrajne nove rute. No takve se pojave događaju rjeđe od samih pogrešaka u konfiguraciji.

Za razjašnjavanje pogrešaka u konfiguraciji klasificiramo nove rute u različite kategorije u odnosu na njihov odnos prema postojećim rutama kao što je prikazano u tablici 3.1 [7]. Za svaku su kategoriju u tablici navedene stara ruta te jedna od mogućih novih ruta.

*Tablica 3.1. Klasifikacija pogrešaka izvora*

| | **Stara ruta** | **Nova ruta** |
|---|---|---|
| *Vlastita deagregacija* | a.b.0.0/16 XYZ | a.b.c.0/24 XYZ |
| *Srodan izvor* | a.b.0.0/16 XYZ | a.b.0.0/16 XY<br>a.b.0.0/16 XYZO<br>a.b.c.0/24 XY<br>a.b.c.0/24 XYZO |
| *Strani izvor* | a.b.0.0/16 XYZ | a.b.0.0/16 XYO<br>a.b.c.0/24 XYO<br>e.f.g.h/i XYO |

- Vlastita deagregacija:

  Kod vlastite deagregacije izvor sam deagregira vlastiti prefiks. Vidimo da je mrežna maska novog prefiksa dulja od mrežne maske starog prefiksa, dok je atribut AS-put ostao neprimijenjen.

- Srodan izvor:

  Kod srodnog izvora, postojeći prefiks ili njegova podmreža objavljen je s novim atributom AS-put gdje je izvorišni AS drugačiji, a sam je novi AS-put sadržan u starom AS-putu ili je pak stari AS-put sadržan u novom. Naprimjer prijašnji prefiks a.b.0.0/16 s putom XYZ je povučen, a objavljen je novi prefiks a.b.c.0/24 koji predstavlja podmrežu starog prefiksa s novim putem XYZO, gdje je stari put sadržan u novome (XYZ je podskup XYZO), ali im je izvorišni AS drugačiji (iz Z sada je postao O).

- Strani izvor:

  Kod stranog je izvora prefiks ili njegova mreža objavljen od strane drugoga izvora koji nije u korelaciji sa starim izvorom (niti je XYO podskup XYZ, niti je XYZ podskup XYO). Nove rute za prefikse koji još nisu bili prisutni u tablici ili koji nemaju manje specifičan prefiks u tablici, dakle prefiks s kraćom mrežnom maskom, također se klasificiraju kao strani izvor.

Budući da sa stajališta udaljenog promatrača nemamo pred sobom sliku cijelog Interneta, može se dogoditi da pogrešno klasificiramo pojedini slučaj. Moguće je da se neki slučajevi srodnog izvora zbog nepotpune slike klasificiraju kao pogreške stranog izvora.

### 3.3.2 Analiza pogrešaka izvoza

Pogreška izvoza, odnosno curenje rute, neželjeni je izvoz rute BGP susjedu u suprotnosti s politikom AS-a koji je napravio izvoz rute. Same politike AS-ova na kojima se bazira izvoz pojedinih ruta proizlazi iz komercijalnih odnosa između AS-ova.

Tablica 3.2 [7] pokazuje uobičajene odnose između AS-ova i pravila za izvoz ruta između njih. Bratski AS-ovi izvoze sve rute svojim bratskim AS-ovima isto kao što i davatelji usluge izvoze sve rute svojim korisnicima. Korisnici pak svojim davateljima usluge pristupa izvoze samo vlastite rute, rute svojih bratskih AS-ova ili svojih korisnika. Jednakovrijedni AS-ovi, AS-ovi na istoj razini ili partnerski AS-ovi, razmjenjuju rute koje imaju izvor u njihovom AS-u, u AS-ovima njihovih korisnika ili u svojim bratskim AS-ovima, ali nikada ne bi smjeli razmjenjivati rute svojih partnerskih AS-ova s drugim svojim partnerskim AS-ovima. Primjer pogrešne konfiguracije bio bi slučaj kada bi AS svom davatelju usluge (Provider) izvezao rutu koju je naučio od drugog davatelja usluge. Na taj bi način dotični AS mogao postati tranzitni AS za dio prometa između ta dva davatelja usluge.

*Tablica 3.2. Izvozna pravila za uobičajene komercijalne odnose između AS-ova*

| Izvoz rute | Izvozna politika |
|---|---|
| Korisnik → Davatelj usluge | Samo rute dobivene od korisnika ili bratskih AS-ova |
| Partnerski AS → Partnerski AS | Samo rute dobivene od korisnika ili bratskih AS-ova |
| Davatelj usluge → Korisnik | Sve rute |
| Bratski AS → Bratski AS | Sve rute |

Kada bismo znali odnose između pojedinih AS-ova, lako bismo mogli uočiti izvozne pogreške konfiguracije BGP-a. Međutim odnosi između AS-ova smatraju se poslovnom tajnom što otežava uočavanje pogrešaka. Često se ti odnosi mogu zaključiti promatrajući BGP tablice. Svi AS-putovi morali bi se pokoravati pravilu slobodne doline (engl. *valley free*). Ako smjer od davatelja usluge prema korisniku smatramo padajućim smjerom, a promet između bratskih AS-ova (engl. *siblings*) i partnerskih AS-ova (*peer*) prometom na istoj razini, pravilo slobodne doline zahtijeva da ruta koja je krenula padajućim smjerom više ne smije krenuti suprotnim rastućim smjerom. Također na cijelom putu smije postojati samo jedan prijelaz između partnerskih AS-ova i on stoga nužno mora biti na najvišoj točki puta.

U skladu s tim, rute koje krše pravilo slobodne doline ili koje u sebi sadrže više od jedne veze između partnerskih AS-ova (*peer-peer* veze), vjerojatno predstavljaju pogreške u konfiguraciji. Navedena metoda otkrivanja pogrešaka nije sasvim precizna te ponekad stvarne pogreške mogu proći nezamijećene, dok se s druge strane legitimne rute mogu shvatiti kao pogreške.

U tablici 3.3 [7] kategorizirane su pogreške prilikom izvoza ruta. U svakom od ovih slučajeva AS pruža tranzitni promet od svog davatelja usluge ili partnerskog AS-a prema svom drugom davatelju usluge ili partnerskom AS-u. Bratski AS-ovi ovdje nisu navedeni jer se, zbog jednostavnosti, lanac bratskih AS-ova promatra kao jedan AS, što kao rezultat daje gore navedenu klasifikaciju.

*Tablica 3.3. Klasifikacija pogrešaka pri izvozu ruta*

| Izvoz | Kršenje pravila politike |
|---|---|
| Davatelj usluge → AS → Davatelj usluge | Ruta izvezena davatelju usluge je uvezena od davatelja usluge |
| Davatelj usluge → AS → Partnerski AS | Ruta izvezena partnerskom AS-u je uvezena od davatelja usluge |
| Partnerski AS → AS → Davatelj usluge | Ruta izvezena davatelju usluge je uvezena od partnerskog AS-a |
| Partnerski AS → AS → Partnerski AS | Ruta izvezena partnerskom AS-u je uvezena od partnerskog AS-a |

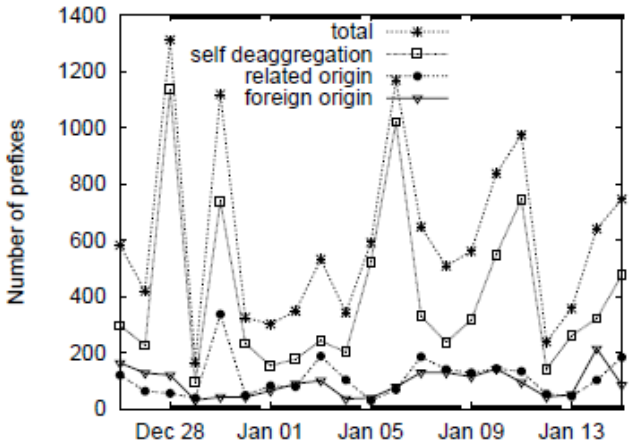
## 3.4 Rezultati mjerenja

U radu "Understanding BGP Misconfiguration" [7] dani su rezultati mjerenja pogrešaka kod BGP-a za jedno promatrano razdoblje, analizirane su same pogreške te utjecaj tih pogrešaka na gubitak veza i opterećenje usmjernika.

### 3.4.1 Rezultati mjerenja pogrešaka izvora

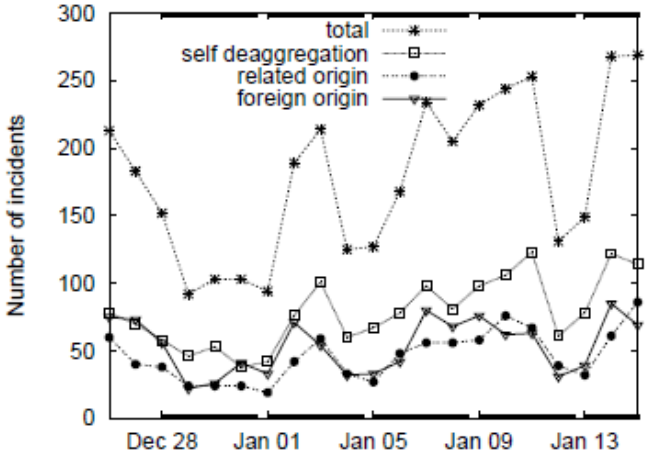
Vjerojatne pogreške koje mogu biti klasificirane kao pogreške izvora variraju na dnevnoj osnovi. Raščlanjivanjem tih pogrešaka u kategorije opisane u odjeljku 3.3.1 ustanovilo se da većina novih ruta dolazi od vlastite deagregacije dok je manji postotak došao kao srodan ili strani izvor. Točnije, do takvih rezultata dolazimo ako pogledamo broj novih prefiksa po pojedinim danima kao što je prikazano na slici 3.4 [7]. Međutim kako bi se bolje razaznali uzroci pogrešaka tako ubačeni, novi su prefiksi grupirani u skupine nazvane incidentima. Pojedini incident obuhvaća cijeli skup prefiksa koji potječu iz istog AS-a čije se pojavljivanje i nestanak dogodio u kratkom vremenskom razdoblju. Za trajanje vremenskog razdoblja uzet je interval od 15 minuta, budući da se to smatra gornjom granicom konvergencije kod BGP-a.

Na slici 3.5 [7] prikazana je raspodjela incidenata po danima. U ovom prikazu više ne dominira vlastita deagregacija kao u prikazu po prefiksima. Tako prosječan broj pogrešaka vlastite deagregacije, premda samo nešto veći od preostale dvije grupe pogrešaka, srodnog izvora i stranog izvora, predstavlja veliki broj prefiksa koji sudjeluju u pogrešci. To je samo po sebi i razumljivo jer je upravo proces deagregacije taj koji stvara veliki broj novih prefiksa iz manjeg broja već postojećih. Dok je prilično lako uočiti novonastale prefikse kod vlastite deagregacije i klasificirati ih kao pogreške, to nije slučaj s druga dva tipa. Kod srodnog ili stranog izvora često se može dogoditi da se ne radi o pogreški konfiguracije, nego o namjernoj politici usmjeravanja koja do izražaja dolazi kod ispada krajnjih korisnika. Često davatelji usluga imaju spremne rezervne rute za pojedine prefikse u slučaju njihovog ispada koje se aktiviraju u slučaju ispada primarnih ruta. Najčešći je slučaj redundantne veze korisnika na dva davatelja usluge pristupa gdje se druga veza aktivira u slučaju kada prva zakaže. Dok takve stanja nisu uzrokovana pogreškama u konfiguraciji, ona svejedno dodatno opterećuju usmjernike te mogu dovesti do ranije opisanih problema i posljedica prikazanih na slici 3.1 te ih kao takve treba svesti na najmanju moguću mjeru.




*Slika 3.4. Broj pogrešaka izvora po danima*

Ako pogledamo kako pogreške izvora utječu na gubitak veze iz tablice 3.4 [7] u zadnjem retku vidimo da je u 13% slučajeva incident doveo do gubitka veze. Međutim tih je 13% incidenata obuhvatilo samo 4% od ukupnog broja prefiksa. Takav se rezultat objašnjava time što najveći broj pogrešaka nastaje vlastitom deagregacijom koje generiraju veliki broj novih prefiksa, no malen broj tih prefiksa uzrokuje stvaran gubitak veze. Veliki incidenti, incidenti u kojima sudjeluje velik broj prefiksa, generiraju veliki servisni promet, ali ne uzrokuju gubitak veze jer su dio legitimne politike usmjeravanja i najčešće nastaju kao odgovor na ispad veza na nekom dijelu Interneta kako bi alternativnim rutama održali povezanost s tim prefiksima. S druge pak strane, gotovo polovica (44%) incidenata kategoriziranih kao strani izvor uzrokuju gubitak veze. Ove rezultate treba uzeti s dozom opreza jer je u mnogim slučajevima teško uočiti gubitak veze, pogotovo ako je takav ispad trajao kraće vremensko razdoblje. Najčešće su sami korisnici ti koji svojim davateljima usluga prijavljuju gubitak veze prema određenim IP adresama. Također mnogi prefiksi koji sudjeluju u incidentima spadaju pod manje ili rjeđe korištene poslužitelje ili rubne dijelove Interneta te se stoga gubitak veze prema njima teže uočava.



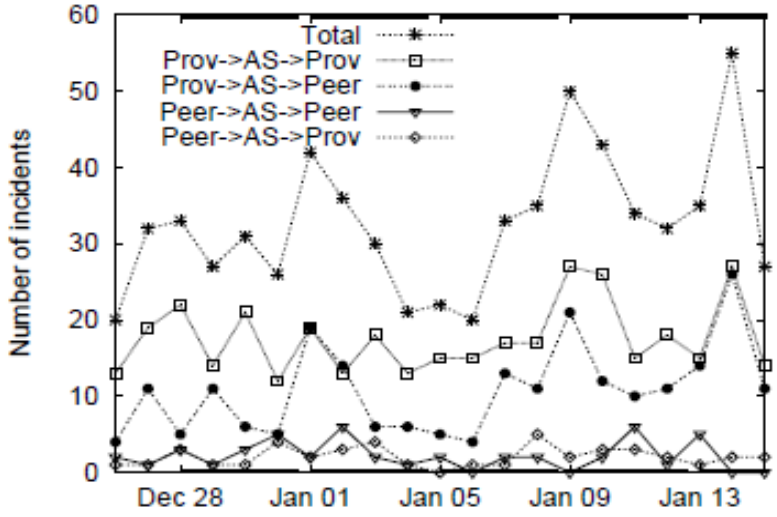

*Slika 3.5. Incidenti pogrešaka izvora po danima*

*Tablica 3.4. Postotna raspodjela pogrešaka izvora*

| Type | Prefixes (top) Incidents (bottom) | Classified (% of total) | Misconfigurations All (% of classified) | Misconfigurations Connectivity (% of misconfigs) | Non-misconfigurations (% of classified) |
|---|---|---|---|---|---|
| Self deaggregation | 8424 | 5598 (66%) | 5519 (99%) | 74 (01%) | 79 (01%) |
| | 1648 | 616 (37%) | 563 (91%) | 13 (02%) | 53 (09%) |
| Related Origin | 2341 | 1153 (49%) | 1068 (93%) | 54 (05%) | 85 (07%) |
| | 969 | 229 (24%) | 188 (82%) | 25 (13%) | 41 (18%) |
| Foreign origin | 1951 | 642 (33%) | 535 (83%) | 142 (27%) | 107 (17%) |
| | 1131 | 257 (23%) | 194 (75%) | 85 (44%) | 63 (25%) |
| Total | 12716 | 7393 (58%) | 7122 (96%) | 270 (04%) | 271 (04%) |
| | 3748 | 1102 (29%) | 945 (86%) | 123 (13%) | 157 (14%) |

## 3.4.2 Rezultati mjerenja pogrešaka izvoza

Svaka pogreška izvoza nastala je objavom AS puta koji nije u skladu s izvoznim politikama objava. Ona se detektira sekvencom od tri AS-a čiji poredak nije u skladu s ranije dogovorenom politikom ili ustaljenom praksom. Pogreške izvoza također se mogu grupirati u incidente. Pojedini incident sadrži sve objave koje imaju istu sekvencu AS-ova te su objavljene, a kasnije i povučene u približno isto vrijeme. Na slici 3.6 [7] prikazana je raspodjela incidenata uzrokovanih pogreškama kod izvoza po danima za različite tipove sekvenci AS-ova. Budući da je većina veza između AS-ova između davatelja usluga i korisnika, a ne između partnerskih AS-ova, postotak prvih je veći. Pogreške izvoza ne uzrokuju izravno gubitak veze. One prije svega donose dodatni upravljački promet i opterećuju usmjernike. Često se kao posljedica može uočiti zagušenje veza ili gašenje pojedinih veza, a samo u pojedinim slučajevima potpuni ispad veze.




*Slika 3.6. Incidenti pogrešaka izvoza po danima*

### 3.4.3 Opterećenje usmjernika

Svaki dinamički protokol zahtijeva razmjenu upravljačkih informacija između usmjernika koji sudjeluju u samom protokolu. Količina razmjenjenih informacija ovisi o dinamici same mreže kao i o promjenama u konfiguraciji usmjernika. Dok su ove druge uzrokovane izravnim ljudskim utjecajem te se odvijaju samo povremeno, dinamika mreže je ta koja uzrokuje generiranje puno servisnog usmjerničkog prometa. Usmjernik, kao i svako računalo, treba određeno vrijeme da bi te informacije obradio što uzrokuje stanovito kašnjenje u propagaciji informacija drugim usmjernicima; pogotovo kada u kratkom vremenskom roku dođe puno informacija na obradu. Također velika količina informacija može uzrokovati zagušenje samog usmjernika koji tako privremeno gubi mogućnost obrade informacija te ažuriranje usmjerničkih tablica i pravodobnu propagaciju informacija što dodatno komplicira situaciju u samoj mreži. U slučaju izrazito velikog opterećenja usmjernik može čak privremeno prestati usmjeravati promet jer je cijelo vrijeme zauzet obradom servisnih informacija. Stoga lako zaključujemo da izravne posljedice opterećenja usmjernika mogu biti:

- Sporo ažuriranje usmjerničkih tablica
- Spora propagacija usmjerničkih informacija susjedima
- Odbacivanje dijela prometa uslijed nemogućnosti obrade

Iz izravnih se posljedica razvijaju neizravne posljedice po cijelu mrežu:

- Spora konvergencija mreže
- Neoptimalno usmjeravanje
- Privremeni gubitak povezanosti prema nekim mrežama

Stoga je iznimno važno opterećenje usmjernika svesti na najmanju moguću mjeru. Ključ je u ispravnoj konfiguraciji samih usmjernika koji će uspjeti ublažiti nepotreban servisni promet generiran dinamikom same mreže. Budući da Internet nije hijerarhijski ustrojen te nema autoriteta koji propisuje pravila ispravne konfiguracije, teško je utjecati na konfiguraciju rubnih usmjernika u tuđim autonomnim sustavima i na njihovu politiku usmjeravanja. Ali možemo prilagoditi naše usmjernike kako bi se što bolje nosili s pretjeranim servisnim prometom. Kako on nastaje dinamikom same mreže, reputacijski sustav koji će pratiti ponašanja drugih autonomnih sustava može nam pritom biti od velike pomoći. Na temelju ocjene reputacije susjednih ili udaljenih AS-ova, možemo izgraditi sustav koji će dinamički filtrirati servisni usmjernički promet i selektivno propuštati informacije drugim autonomnim sustavima. Time ćemo zaštiti ne samo sebe, već i druge sustave od malicioznih ili loše konfiguriranih tuđih AS-ova. Tako nam sam reputacijski sustav ne bi trebao pomoći samo u otkrivanju lažnih objava prefiksa ili u pronalasku optimalnog puta, odnosno u odbacivanju nestabilnih putova, već bi nam trebao pomoći i u suzbijanju nepotrebnog servisnog usmjerničkog prometa.

# 4. Usmjernički promet i reputacija

Internet je sačinjen od autonomnih sustava koji predstavljaju mreže davatelja usluge ili velikih organizacija. Za usmjeravanje između autonomnih sustava koristi se usmjernički protokol rubnih usmjernika (BGP). Rubni usmjernici BGP-om razmjenjuju informacije o mrežama odnosno adresnim blokovima koje posjeduju šaljući si međusobno UPDATE poruke u kojima objavljuju ili povlače raniju objavu dohvatljivosti pojedine mreže, odnosno prefiksa iz svog autonomnog sustava. Autonomni sustavi objavljuju prefikse koje posjeduju šaljući informacije o tome svojim susjedima; ti su autonomni sustavi izvorišni za te prefikse. Svi ostali AS-ovi prosljeđuju te informacije dalje propagacijom svojih UPDATE poruka kojima pak obavještavaju svoje susjede da je i kroz njih dohvatljiv taj prefiks. U toj se poruci nalaze informacije o dohvatljivosti: sam prefiks koji se objavljuje, atribut AS Path u kojem su zabilježeni poredano svi AS-ovi kroz koje se treba proći na putu do tog prefiksa te razni drugi atributi koji nose dodatne informacije ili mogu utjecati na odabir puta. To se prvenstveno odnosi na odabir puta između usmjernika u susjednim AS-ovima.

BGP je napravljen kako bi bio što efikasniji, međutim ima jedan veliki inherentni nedostatak: BGP naime implicitno vjeruje svim autonomnim sustavima, vjeruje da su informacije koje se prenose između susjeda točne te vjeruje da se svi autonomni sustavi drže dobre prakse usmjeravanja BGP-om i dobre prakse politika usmjeravanja. Pod pojmom dobre prakse misli se na pretpostavke ponašanja koje nisu nužne niti su igdje protokolom ili zakonom propisane, no o kojima uvelike ovisi optimalno funkcioniranje usmjeravanja i veza na Internetu. Stoga se nameće problem vrednovanja drugih autonomnih sustava u smislu vjerovanja njihovim usmjerničkim informacijama, vjerovanja da se služe dobrom praksom usmjeravanja BGP-om, postojanosti njihove opreme i veza te ne posezanja drugih autonomnih sustava za zlonamjernim radnjama i postupcima. U svrhu vrednovanja vjerovanja drugim autonomnim sustavima kao rješenje predlaže se snimanje usmjerničkog prometa kako bi se prikupile informacije o ponašanju drugih autonomnih sustava te iz tih informacija izračun vrijednosti vjerovanja drugim sustavima. Numerička vrijednost vjerovanja drugim autonomnim sustavima naziva se reputacija. Na temelju tako izračunate reputacije pojedinih autonomnih sustava mogu se bazirati kasniji odnosi između AS-ova, mogu se donositi politike usmjeravanja i filtriranja prometa iz pojedinih AS-ova, može se utjecati na odabir najboljeg puta ili na prihvaćanje ili neprihvaćanje usmjerničkih informacija dobivenih iz AS-ova s lošom reputacijom kao vjerodostojnih.

U ovom je poglavlju prvo opisana dobra praksa usmjeravanja BGP-om koje bi se trebali držati AS-ovi. Dalje su opisana razna ponašanja koja mogu uzrokovati kršenje takve dobre prakse. Potom su navedene informacije koje se snimaju iz usmjerničkog prometa iz kojih se mogu saznati ponašanja AS-ova te njihovo kršenje dobre prakse usmjeravanja. Kvalitativno je opisano uočavanje kršenja dobre prakse te je predložena evaluacija dobivenih informacija u svrhu izračuna reputacije. Detaljno su opisani slučajevi koji mogu biti naznaka nepoštivanja uobičajenih pretpostavki ponašanja koji će se potom koristiti u izračunu reputacije autonomnih sustava. Dok je u prvom dijelu poglavlja dana kvalitativna analiza ponašanja autonomnih sustava koja se razmatra prilikom njihovog vrednovanja, u drugom je dijelu poglavlja dana kvantitativna analiza gdje su prikazane metode prikupljanja informacija iz kojih se potom izračunava kažnjavanje autonomnih sustava na osnovu njihovog kršenja dobre prakse usmjeravanja na Inernetu te se naposljetku razvija matematički model izračuna reputacije.

## 4.1 Pretpostavke dobrog ponašanja

Pretpostavke ponašanja očekivana su ponašanja autonomnih sustava koja se povode za dobrom praksom usmjeravanja BGP-om. Takva praksa nije nigdje izrijekom propisana: niti je uvrštena u ikakav protokol niti je zakonski uvjetovana. Ona je naprosto izraz očekivanog ponašanja autonomnih sustava koji drže do što boljeg, ispravnog, preciznog i konciznog usmjeravanja na Internetu. Tri su glavne pretpostavke ponašanja koje se smatraju dobrom praksom usmjeravanja BGP-om:

- Legalnost i točnost usmjerničkih informacija

  pretpostavka koja traži da su sve usmjerničke informacije legalne, odnosno da se nigdje ne pojavljuju nelegalne informacije o prefiksima, autonomnim sustavima ili putovima koje treba preći. Ne smiju se pojavljivati rezervirane adrese, odnosno prefiksi koje se ne koriste na Internetu, rezervirani brojevi autonomnih sustava koji se ne koriste za usmjeravanje na Internetu, ne smiju se pojaviti nedozvoljene kombinacije puta poput petlji i sl.

- Stabilnost rute

  oglašena ruta treba biti stabilna odnosno treba izbjeći oglašavanje ruta koje su podložne čestim promjenama jer one mogu uzrokovati smanjenu propusnost, potpuni gubitak povezanosti i nepotrebno opterećivanje rubnih usmjernika.

- Bezdolinsko usmjeravanje

  ruta se treba pokoravati putanji između autonomnih sustava u kojoj neće nastati dolina.

Kršenje ovih pretpostavki ponašanja može dovesti do ozbiljnih posljedica na usmjeravanje na Internetu. Osim blagog kršenja pretpostavki ponašanja koje se neprestano događa, često svjedočimo velikim kršenjima koji prerastaju u incidente s globalnim posljedicama. Najveći je problem otimanje prefiksa gdje autonomni sustav oglašava prefiks koji zapravo ne posjeduje ili do kojega ne može doći oglašenom rutom, a tvrdi da može. Također je veliki problem usmjeravanje s dolinama koje može usporiti, otežati ili spriječiti konvergenciju BGP-a. Prisutno je i ubacivanje nestabilnih veza te oglašavanje ruta preko tih veza kao i ubacivanje lažnih veza za rute inače dosezljive, ali lošijim putom, kako bi se učinile atraktivnijima.

## 4.2 Kršenje pretpostavki dobrog ponašanja

Već je navedeno da je BGP dizajniran samo za što efikasnije usmjeravanje. Implicitno pretpostavlja da se svim autonomnim sustavima može vjerovati da će slijediti dobru prakse, odnosno da će se ponašati u skladu s određenim pretpostavkama ponašanja. Te pretpostavke nisu generalno određene niti propisane već su samo izraz nastojanja da se omogući što bolje i postojanije usmjeravanje na Internetu. Dok su neka ponašanja okarakterizirana kao manje problematična poput prevelikog nepotrebnog slanja UPDATE poruka, druga su iznimno problematična poput otimanje tuđeg prefiksa. Tri glavne pretpostavke dobre prakse usmjeravanja na Internetu navedene su u potpoglavlju 4.1. Autonomni sustav na Internetu krši neku od ovih pretpostavki, ako pokaže bilo koje od sljedećih ponašanja:

1) **Ilegalnost**

   Vrijednosti broja autonomnog sustava ili prefiksi oglašeni UPDATE porukom su iz zabranjenog raspona. Ono obuhvaća brojeve AS-ova i prefikse rezervirane za uporabu u lokalnim mrežama, rezervirane za testne i druge namjene kao i one koji se ne smiju pojaviti na Internetu.

2) **Otimačina**

   Autonomni sustav tvrdi da posjeduje prefiks koji mu nije dodijeljen od strane registratora. On taj prefiks objavljuje svojim susjedima koji ga dalje propagiraju na Internet, onemogućujući pritom vezu prema traženom prefiksu s dijela ili s cijelog Interneta te uzrokuje preusmjeravanje prometa za taj prefiks prema AS-u koji je stvorio lažnu objavu.

3) **Kolebanje**

   Kolebanje nastaje naizmjeničnim objavljivanjem pa potom povlačenjem prefiksa od strane autonomnog sustava koji posjeduje taj prefiks uzrokovano unutarnjim previranjem samog autonomnog sustava.

4) **Dolinska ruta**

   Dolinska ruta nastaje kada UPDATE poruka ima jedan ili više autonomnih sustava koji tvore dolinu. Dolina nastaje kada korisnik usluge propagira svom davatelju usluge rutu koju je dobio od svog drugog davatelja usluge ili kada AS propagira svom partnerskom susjedu (peer) rutu koju je dobio od svog drugog partnerskog susjeda. Većina AS-ova na Internetu nastoje prilagoditi svoje politike izvoza ruta kako bi poštovali pravilo bezdolinskih ruta. Upravo se ovo pravilo pokazalo kao dovoljan uvjet konvergencije BGP-a.

5) **Nestabilne veze između AS-ova**

   Nestabilne veze između autonomnih sustava postaju problem kada pojedini AS propagira rutu koju prolazi kroz takvu nestabilnu vezu. Pravodobno otkrivanje nestabilnih veza i ruta te filtriranje takvih ruta je nužno kako bismo smanjili vrijeme konvergencije, kako bismo uopće smanjili izmjene ruta, kako ne bismo stvarali nepotreban upravljački promet te kako bismo spriječili potencijalne napade iz AS-ova koji preusmjeravaju promet preko sebe koristeći se kratkovjekima vezama.

### 4.2.1 Ilegalnost

Od cijelog skupa IP adresa većina se nalazi na Internetu, što znači da se one dodjeljuju autonomnim sustavima koji ih poslije dodjeljuju svojim računalima, poslužiteljima, usmjernicima ili ih daju na korištenje svojim korisnicima. Takve se IP adrese i prefiksi kojima one pripadaju mogu naći u globalnoj BGP tablici, smiju se usmjeravati na Internetu te ih autonomni sustavi smiju oglašavati, naravno samo ako su vlasnici tih prefiksa. Jedan dio IP adresa i njima pripadajućih prefiksa koristi se za uporabu u lokalnim mrežama i kao takav nikada se ne smije naći u globalnoj usmjerničkoj tablici. Takvi se prefiksi ne smiju oglašavati. Slično vrijedi i za većinu adresa i prefiksa rezerviranih za buduće namjene kao i za višeodredišne adrese (engl. *Multicast*). Neke se pak adrese i prefiksi smiju naći u globalnoj usmjerničkoj tablici, ali služe samo za testne svrhe te ih većina autonomnih sustava ne smije oglašavati. Oglašavanje prefiksa namijenjenih uporabi u lokalnim mrežama i nekih

testnih prefiksa zabranjena je ne samo u obliku gdje bi AS koji oglašava takav prefiks bio njemu izvorišni AS, već je zabranjeno i prosljeđivanje rute prema tim prefiksima koje su došle iz drugih AS-ova. Tako svaki AS koji dobije od susjeda prefiks koji ne smije biti usmjeravan na Internetu, mora taj prefiks filtrirati i odbaciti, a ne se zamarati pitanjima kako se taj prefiks uopće tu isprva i našao. Začudo, ali mnogi ISP-ovi zaborave staviti opisane filtere na usmjernike u svojim AS-ovima. Takvi se prefiksi, ukoliko se nađu na Internetu, nazivaju lažnima (engl. Bogon) ili marsovskim prefiksima (engl. Martians). U širem se smislu pod lažnim prefiksima smatraju ne samo ovdje navedeni prefiksi koji se ne smiju usmjeravati na Internetu, već i svi oni prefiksi koji su oglašeni s izvorom u AS-u kojem ne pripadaju odnosno kojemu ih nije dodijelio lokalni registrator. U ovom radu takve prefikse ne nazivamo lažnima, već jednostavno otetima. Također se u dijelu literature lažnim prefiksima smatraju samo oteti, dok se ovi prvi jednostavno nazivaju prefiksima koji se ne usmjeravaju na Internetu. Definirani su u dokumentima RFC 1918 [21] i RFC 5735 [22] te se njihov popis i namjena nalaze u tablici 4.1.

*Tablica 4.1. Prefiksi s ograničenom uporabom*

| Prefiks | Namjena |
|---|---|
| 0.0.0.0/8 | Ova mreža |
| 10.0.0.0/8 | Lokalne mreže |
| 127.0.0.0/8 | Povratna veza |
| 169.254.0.0/16 | Lokalna veza |
| 172.16.0.0/12 | Lokalne mreže |
| 192.0.0.0/24 | Dodijeljeno za IETF protokole |
| 192.0.2.0/24 | Test |
| 192.88.99.0/24 | Ipv6 na IPv4 |
| 192.168.0.0/16 | Lokalne mreže |
| 198.18.0.0/15 | Međumrežno povezivanje - test |
| 198.51.100.0/24 | Test |
| 203.0.113.0/24 | Test |
| 224.0.0.0/4 | Višeodredišne |
| 240.0.0.0/4 | Rezervirano za buduće potrebe |
| 255.255.255.255/32 | Ograničena sveodredišna adresa |

Slično vrijedi i za brojeve autonomnih sustava. Dio brojeva autonomnih sustava ostavljen je za uporabu u lokalnim mrežama, dio brojeva je rezerviran i ne smije se koristiti za usmjeravanje na Internetu dok se velika većina brojeva dodjeljuje od strane IANA-e te se koristi za usmjeravanje na Internetu i za identificiranje autonomnih sustava. Također postoji i dio brojeva koji su namijenjeni usmjeravanju na Internetu, ali još nisu dodijeljeni niti jednom AS-u. Popis brojeva AS-ova nalazi se u tablici 4.2.

*Tablica 4.2. Raspodjela brojeva autonomnih sustava*

| Raspon brojeva autonomnih sustava | Namjena |
|---|---|
| 0 | Za mreže koje se ne usmjeravaju |
| 1-59391 | Za dodjelu autonomnim sustavima |
| 59392-64495 | Rezervirano za IANA-u |
| 64496-64511 | Rezervirano za testnu uporabu |
| 64512-65534 | Rezervirano za lokalnu uporabu |
| 65535 | Rezervirano |

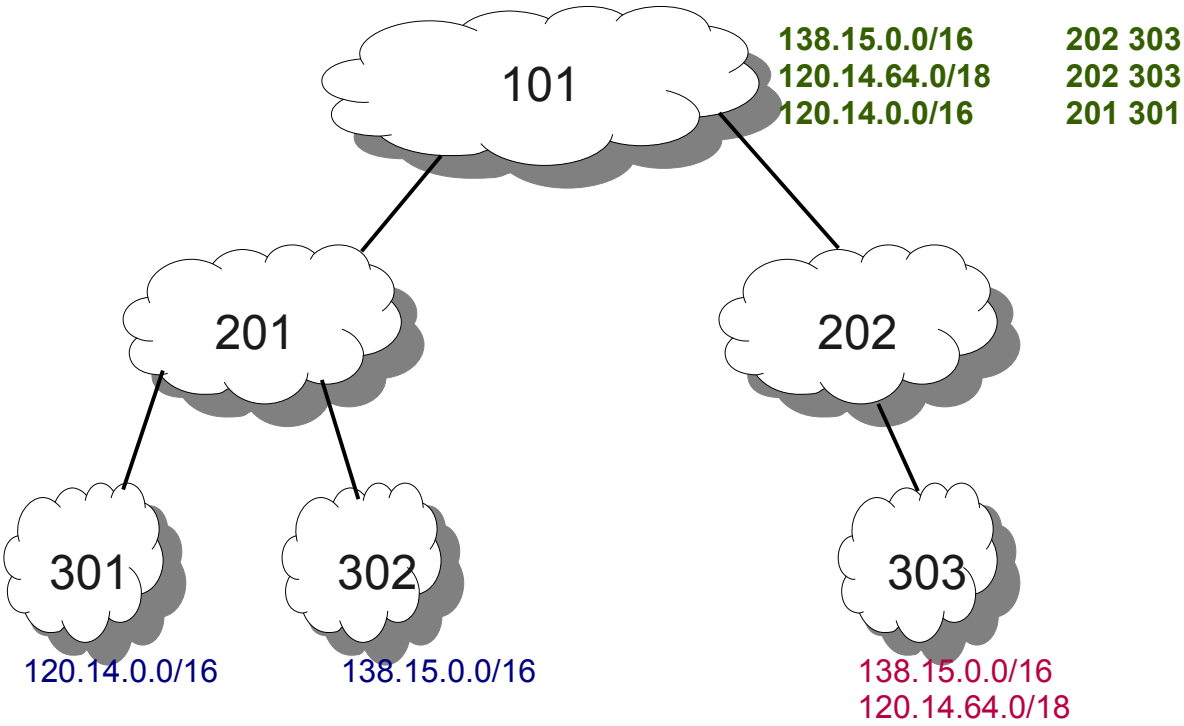
### 4.2.2 Otimačina

Otimačina nastaje kada autonomni sustav tvrdi da posjeduje prefiks koji mu nije dodijeljen od strane registratora te taj prefiks objavi u UPDATE poruci svojim susjedima. Njegovi susjedi vjerojatno nisu svjesni činjenice da taj AS ne bi trebao oglašavati taj prefiks te propagiraju objavu dalje susjedima. Na taj način dio Interneta ili čak cijeli Internet neće moći pristupiti tom prefiksu jer će promet biti preusmjeren otimaču.

Na slici 4.1 prikazan je slučaj otimačine prefiksa. Autonomni sustavi 301 i 302 stvarni su vlasnici redom prefiksa 120.14.0.0/16 i 138.15.0.0/16. Oni te prefikse u objavi šalju svom davatelju usluge, AS-u 201, koji ih potom propagira tranzitnom AS-u 101 koji ih zatim propagira ostatku Interneta. U jednom trenutku AS 303 objavi da on posjeduje prefikse 138.15.0.0/16 i 120.14.64.0/18. Oba prefiksa objavljuje svom davatelju usluge AS-u 202 koji ih prosljeđuje tranzitnom AS-u 101. Ukradeni prefiks 138.15.0.0/16 od strane AS-a 303 u potpunosti se poklapa s ispravnim prefiksom AS-a 301 koji mu je stvarni vlasnik. Ovisno o politikama usmjeravanja mogući su različiti ishodi. Najvjerojatnije je da će iz AS-a 202 te drugih AS-ova kojima je AS 202 davatelj usluge promet prema tom prefiksu biti pogrešno usmjeren prema AS-u 303. AS 201 vjerojatno će ispravno usmjeravati promet prema AS-u 301. U ovisnosti o politici usmjeravanja, neizravno ovisno o drugim atributima, stanje na tranzitnom AS-u može biti nepromijenjeno ili se može promijeniti u korist lažnog objavljenog prefiksa kao što je prikazano na slici. Budući da je AS 101 tranzitni AS, takva je situacija opasna jer će on proslijediti pogrešnu rutu ostatku Interneta te će promet iz većine Interneta prema prefiksu 138.15.0.0/16 biti pogrešno usmjeren prema AS-u 303.

Sljedeća situacija još je opasnija. Isti AS koji je već napravio probleme, AS 303, sada objavljuje prefiks 120.14.64.0/18. Taj je prefiks sadržan u prefiksu 120.14.0.0/16 čiji je stvarni vlasnik AS 301. Budući da je lažni prefiks 120.14.64.0/18, objavljen od strane već dokazano problematičnog AS-a 303, specifičniji, upravo će on biti proslijeđen cijelom Internetu. Tablica usmjernika u autonomnom sustavu 101 tada će imati oba unosa, jedan ispravan za prefiks 120.14.0.0/16 i jedan lažan za prefiks 120.14.64.0/18. Istu će tablicu vjerojatno imati i svi usmjernici na Internetu. Usmjernici prilikom odabira puta uvijek odabiru specifičniji prefiks ispred općenitijeg tako da će sav promet namijenjen onom dijelu prefiksa 120.14.0.0/16 koji je sadržan i u prefiksu 120.14.64.0/18 (dakle točno 25% IP adresa početnog prefiksa) uvijek biti usmjeravan prema AS-u 303 umjesto prema pravom vlasniku tih adresa, AS-u 301. Specifičniji od dva ili više prefiksa je onaj koji ima najdulju mrežnu masku te time određuje najmanji broj pojedinačnih IP adresa. Specifičniji je prefiks uvijek preferiran za usmjeravanje prometa neovisno o tipu usmjeravanja i usmjerničkom protokolu. Navedena je situacija izrazito opasna jer će svi usmjernici uvijek prvo

odabrati specifičniji prefiks tako da nikakve metrike niti odabiri najboljeg puta tu neće pomoći. Jedino što može pomoći u ovom slučaju je detekcija i filtriranje lažnog prefiksa. Potrebno je saznati koji prefiks pripada kojem AS-u što je teško znati za cijeli Internet, neprecizno je, a i protivno je politici dinamičkog Interneta. Zatim je potrebno filtrirati lažne objave. Alternativa tom rješenju korištenje je reputacijskog sustava koji će na temelju ranijih lažnih objava dodijeliti lošu reputaciju problematičnom AS-u 303 te će se sve njegove kasnije objave uzimati s dozom opreza. Upravo su ovakve lažne objave specifičnijeg prefiksa uzrok mnogih široj javnosti poznatih otimačina IP adresa i gubitka veze prema dijelu Interneta. Najpoznatiji je takav slučaj ispad popularnog servisa YouTube koji se zbio 24. veljače 2008. uzrokovan upravo objavom specifičnijeg prefiksa koji je pokrio dio adresnog prostora servisa YouTube od strane jednog pakistanskog davatelja usluge.

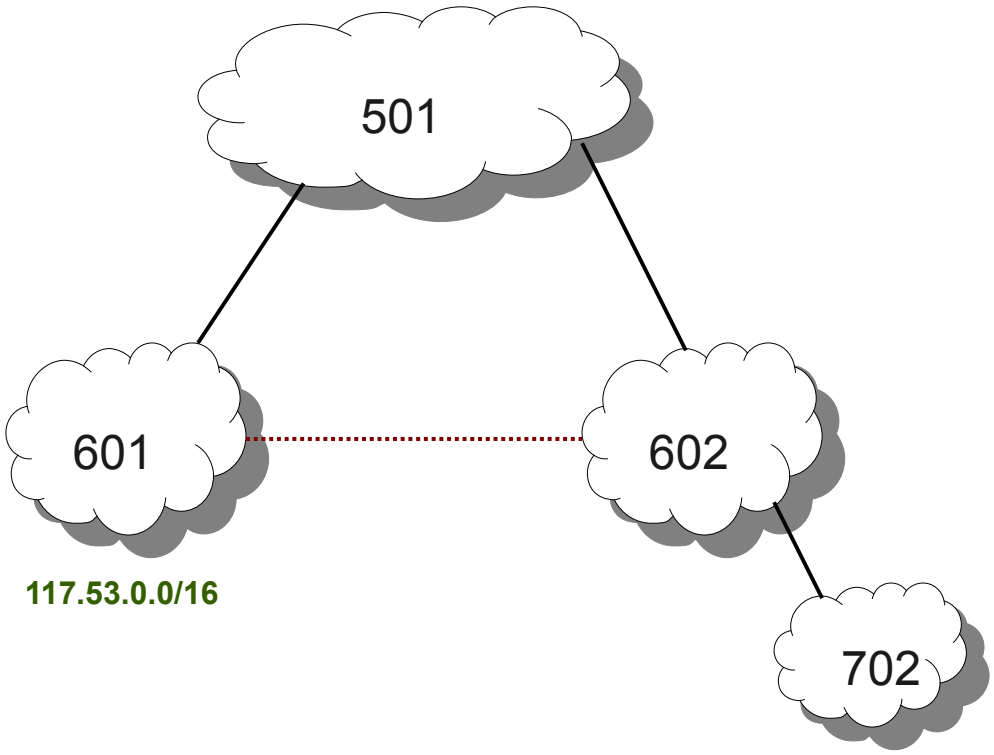



*Slika 4.1. Otimačina prefiksa*

### 4.2.3 Kolebanje

Više uzastopnih UPDATE poruka kojima se naizmjenično objavljuje pa potom povlači isti prefiks uzrokuje problem kolebanja. On je najčešće uzrokovan unutarnjim problemima u autonomnom sustavu koji se potom manifestiraju dalje preko BGP-a drugim autonomnim sustavima. Unutarnji problemi mogu biti nevezani za BGP. Sam prefiks postaje na trenutke vidljiv unutar samog autonomnog sustava. Redistribucijom takav prefiks može završiti u BGP koji ga objavljuje svojim susjedima, a ovi ga dalje prosljeđuju ostatku Interneta. Čestim uzastopnim prestankom vidljivosti tog prefiksa unutar samog autonomnog sustava pa potom ponovne vidljivosti, smijenjuju se putem BGP-a objave i povlačenja dotičnog prefiksa. Takvo ponašanje uzrokuje kolebanje prefiksa. Kolebanje može biti i na izlaznim vezama kao što je prikazano na slici 4.2. AS 601 vezan je postojanom vezom na tranzitni AS 501 i nepostojanom vezom na njegov susjedni partnerski (peer) AS 602. Budući da je veza između AS-ova 601 i 602 nepostojana, kolebanje prefiksa 117.53.0.0/16 koji objavljuje AS 601 uzrokuje česta mijenjanja rute prema tom prefiksu u AS-u 602. Ovakva kolebanja izlaznih veza mogu se također klasificirati kao nepostojanost veza između autonomnih

sustava što se često klasificira kao druga vrsta kršenja pretpostavki ponašanja, odnosno kao nestabilnost veze između AS-ova.




*Slika 4.2. Kolebanje rute*

### 4.2.4 Dolinska ruta

Dobra praksa usmjeravanja zahtijeva usmjeravanje između autonomnih sustava koje neće stvoriti udoline na svome putu. Crtajući graf usmjeravanja na ispravno posloženoj shemi gdje se autonomni sustavi više razine nalaze iznad sustava niže razine, lagano se može uočiti postojanje doline pri usmjeravanju. Na slici 4.3 prikazana su dva načina nastanka doline. Zelenom je bojom označen put bez doline. Ako AS 1001 želi objaviti prefiks promatramo kako bi put trebao ići od AS-a 1001 do AS-a 1004. AS 1001 nema izravnu vezu prema AS-u 1004 te će stoga objaviti prefiks svom davatelju usluge, AS-u 101. On pak nema izravnu vezu prema AS-u 1004, niti sustav 102, partner sustavu 101, nema izravnu vezu na AS 1004, tako da će AS 101 objaviti tu rutu svom davatelju usluge, tranzitnom AS-u 11. Tranzitni će AS tu rutu objaviti drugom tranzitnom AS-u koji je potom treba propagirati prema dolje sve do AS-a 1004. Naravno da će AS 101 objaviti taj prefiks u pravilu svim svojim susjedima te će se formirati razni putovi koji će se onda natjecati kroz algoritam za odabir najboljeg puta od AS-a 1004 do AS-a 1001. Cilj svih autonomnih sustava trebao bi biti filtriranjem, odnosno pravilima o izvozu, ruta kao što je opisano u poglavlju 3., spriječiti nastanak dolina na grafu usmjeravanja. Doline nastaju u 2 slučaja:

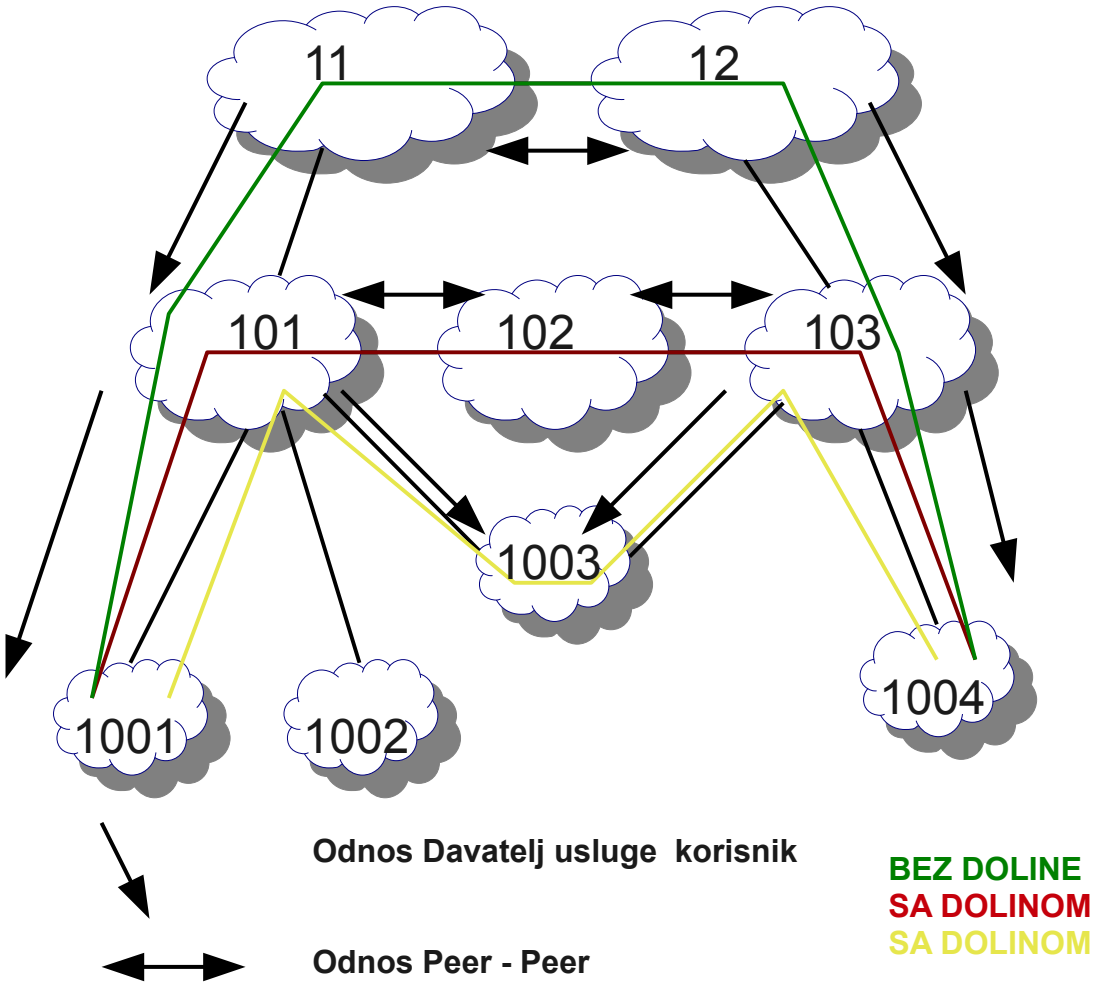
- Usmjeravanje preko korisnika usluge:

  korisnik usluge rute dobivene od svog davatelja usluge nikada ne smije prosljeđivati drugom davatelju.

- Uzastopno usmjeravanje preko više partnerskih autonomnih sustava:

  autonomni sustav koji je dobio rutu od sebi partnerskog susjednog sustava (*peer*) ne

smije tu rutu proslijediti svom drugom partnerskom sustavu.



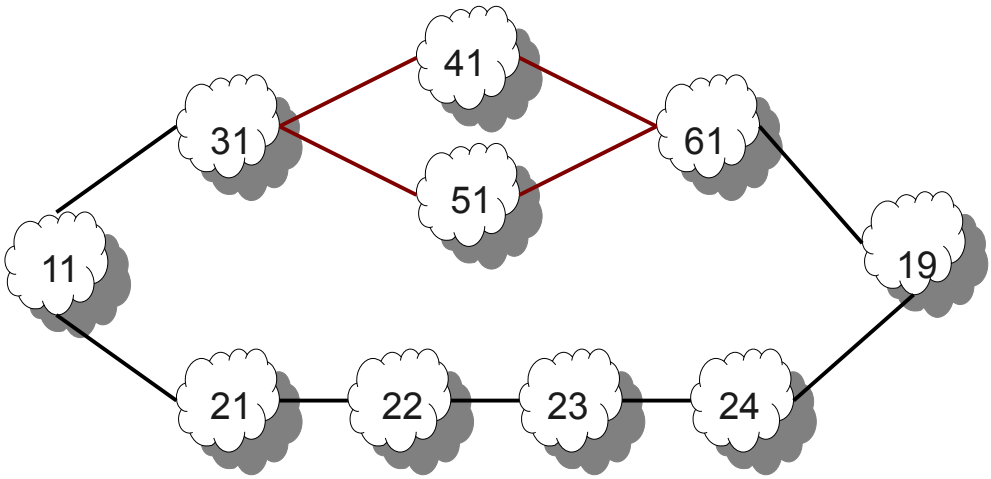

*Slika 4.3. Dolinske rute*

Na slici 4.3 AS 1003 dobio je od svog davatelja usluge, AS-a 101, rutu prema AS-u 1001. On je tu rutu proslijedio svom drugom davatelju usluge AS-u 103 te je time prekršio pravilo bezdolinskog usmjeravanja. Time se formirao put (označen žutom bojom) koji u sebi ima udolinu na mjestu AS-a 1003. Drugi je primjer s AS-om 102; on je dobio rutu prema AS-u 1001 od svog partnerskog susjeda, AS-a 101 te ju je potom proslijedio svom drugom partnerskom susjedu, AS-u 103. Time se može formirati put koji ima dvije uzastopne veze između partnerskih sustava te na tom mjestu (vezi između AS-ova 101-102-103) može nastati dolina i time prekršiti drugo pravilo bezdolinskog usmjeravanja. Ispravan bi put bio taj koji bi imao samo jednu dolinu ili niti jednu dolinu, koja se nalazi na vrhu puta (označen zelenom bojom). Ukoliko put ide preko AS-ova najviše razine tada se niti ta dolina neće formirati. Upravo je to najtočnija definicija AS-ova najviše razine; oni naime moraju imati mogućnost izravnog pristupa svim drugim AS-ovima bez slanja prometa preko bilo kojeg drugog AS-a najviše razine. Osim ova dva pravila kojima se definiraju putovi bez formiranih dolina postoji još jedno pravilo. Ono zahtijeva postojanje najviše jednog prelaska između partnerskih susjednih AS-ova na cijelom putu koje se, ako uopće postoji, mora onda nužno dogoditi na najvišoj točki grafa. Po tom pravilu nije dozvoljeno imati više takvih prijelaza makar oni i ne bili nužno slijedni.

### 4.2.5 Nestabilnost veza između autonomnih sustava

Prilikom međusobnog spajanja mnoge veze između autonomnih sustava nemaju trajan karakter. Neke su namijenjene samo kao rezervna opcija, neke su namijenjene da služe samo za lokalnu razmjenu prometa između susjednih AS-ova, neke pak nisu niti dizajnirane za velike količine prometa koje mogu naići te se u tom slučaju gase ili se nastoji naći mehanizam prebacivanja prometa na druge veze. Često se događa da takve veze koje nisu namijenjene za tranzit prometa budu uključene u propagaciju ruta te time postaju kandidati u procesu odabira najboljeg puta. Premda se taj put naoko čini optimalnim, sam nestabilan karakter takve veze nikako ga ne čini dobrim izborom. U svakom bi slučaju bilo korisno izbjeći algoritam odabira najboljeg puta te filtriranjem izbaciti rute koje prolaze nestabilnim vezama između pojedinih autonomnih sustava ili u potpunosti izbaciti rute koje prolaze kroz autonomne sustave koji mahom imaju nestabilne veze prema svojim susjedima.

Na slici 4.4 prikazane su četiri nestabilne veze označene crvenom bojom. To su veze između autonomnih sustava 31-41, 31-51, 41-61 i 51-61. Kada AS 19 objavljuje svoj prefiks, šalje UPDATE poruke svojim susjedima, AS-ovima 24 i 61. U konačnici ta se objava propagira sve do AS-a 11. On tada ima rutu prema prefiksu u AS-u 19 s vrijednošću atributa AS Path [21, 22, 23, 24, 19] te će upravo tim redoslijedom autonomnih sustava prolaziti promet prema objavljenom prefiksu AS-a 19 s izvorištem prometa u AS-u 11. Kada nestabilne veze postanu aktivne, usmjernici AS-a 11 dobit će nove objave s drugačijim putom. Nakon aktiviranja veza 31-51 i 51-61 pojavit će se u autonomnom sustavu 11 ruta prema istom prefiksu sustava 19, ali ovaj puta s drugačijom vrijednosti atributa AS Path koja će iznositi [31, 51, 61, 19]. Ako nismo ranije prepoznali te veze kao potencijalno nestabilne te ih nismo filtriranjem odbacili, ovaj drugi put bit će izabran na štetu onog prvog, duljeg ali stabilnijeg. AS 11 mora prilagoditi svoje usmjerničke tablice, te mora dalje propagirati tu bolju rutu. Međutim, kako te veze oko AS-a 51 nisu postojane, ta ruta brzo puca te se AS 11 mora vratiti na usmjeravanje starom rutom [21, 22, 23, 24, 19]. Ponovno usmjernici AS-a 11 moraju prilagoditi svoje usmjerničke tablice te moraju propagirati ponovno staru prethodno povučenu rutu. Ako ubrzo prorade veze oko AS-a 41 slična se procedura ponavlja. Posljedice takvog ponašanja su razne: prije svega generira se puno upravljačkog prometa čime se zagušuje u manjoj mjeri veze, a u većoj mjeri sami usmjernici koji moraju obraditi novopristigle usmjerničke informacije. Taj proces traje neko vrijeme kako se ruta propagira te se to vrijeme naziva vremenom konvergencije. Za vrijeme trajanja konvergencije povezanost prema prefiksu u AS-u 19 može biti privremeno otežana ili u potpunosti prekinuta s dijela, a ponekad i s cijelog Interneta. Nameće se zaključak kako bi bilo bolje da je cijelo vrijeme ruta išla putem [21, 22, 23, 24, 19], makar se on tada po kriteriju duljine puta činio kao lošiji izbor, umjesto da su se nakratko javile naoko kraće, ali nestabilnije rute. Takvo ponašanje AS-ova 41 i 51 krši pravila dobre prakse te bi trebalo biti kažnjeno. U tome nam može pomoći reputacijski sustav koji će snimati prethodno loše ponašanje AS-ova 41 i 51, koji su u više navrata propuštali rute svojim vezama koje nisu bile stabilne i davati im loše ocjene koje će utjecati na budući odabir ili odbacivanje ruta koje prolaze navedenim AS-ovima.

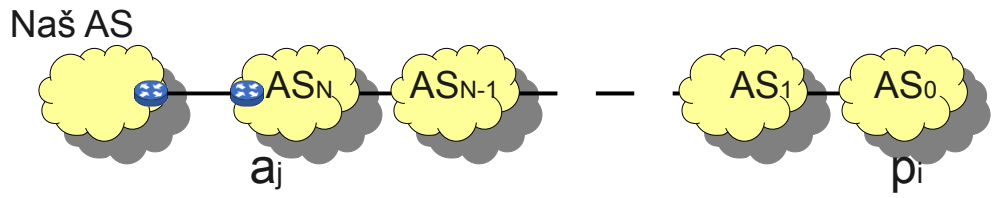



*Slika 4.4. Nestabilnost veza između autonomnih sustava*

## 4.3 Izvor informacija za evaluaciju autonomnih sustava

Promatrajući iz perspektive usmjernika koji se nalazi u našem autonomnom sustavu, dobivamo razne UPDATE poruke od usmjernika u susjednim autonomnim sustavima. Naš sustav može i sam imati više rubnih usmjernika, no praksa je da se u svrhe prikupljanja informacija koriste kolektorski usmjernici. Oni ne služe usmjeravanju prometa, već samo kreiraju susjedske odnose s drugim usmjernicima u drugim autonomnim sustavima u svrhu prikupljanja usmjerničkih informacija od njih. Upravljački promet koji dolazi od rubnih usmjernika u drugim autonomnim sustavima nimalo se ne razlikuje od stvarnog prometa namijenjenoga usmjernicima koji aktivno sudjeluju u usmjeravanju. Radi lakše analize prikupljenih podataka, informacije koje nose UPDATE poruke obrađujemo te iz njih izdvajamo podatke potrebne za evaluaciju reputacije drugih autonomnih sustava.

Na slici 4.5 imamo primjer usmjernika u našem autonomnom sustavu koji je kreirao susjedski odnos s usmjernikom u autonomnom sustavu $AS_N$. On je kroz niz autonomnih sustava povezan s autonomnim sustavom $AS_0$. Prefiks $p_i$ je dodijeljen autonomnom sustavu $AS_0$ te ga on objavljuje svom susjedu. Kada taj prefiks naposljetku dođe do našeg usmjernika sadržavat će vrijednost atributa AS Path [$AS_N$, $AS_{N-1}$, ..., $AS_1$, $AS_0$].




*Slika 4.5. Informacijski set*

Taj je prefiks objavljen našem usmjerniku putem njegovog susjednog usmjernika čija je adresa sljedećeg skoka jednaka $a_j$. Na taj način dobivamo podatak koji je sastavljen od informacija koje se nalaze u UPDATE poruci, a koji će nam kasnije koristiti za razne evaluacije i izračun reputacije:

$$Iij = a_j, p_i, [AS_N, AS_{N-1}, \cdots, AS_1, AS_0]$$

## 4.4 Postojanost veza

Kao što je ranije objašnjeno, nepostojane veze između autonomnih sustava mogu dovesti do niza problema. Prije svega tu je nepotrebno opterećenje usmjernika upravljačkim prometom koji se generira prilikom slanja UPDATE poruka uslijed promjene puta. Same rute koje prolaze kroz nestabilne veze time i same postaju nestabilne, često pucaju, spore su te mogu dovesti do privremenog gubitka povezanosti. Također putevi kroz nestabilne veze mogu biti namjerno stvoreni kao vrsta napada u kojoj se promet namjerno preusmjerava određenim putem kroz određeni AS u svrhu ostvarenja dodatne zarade prolaskom prometa ili u svrhu snimanja prometa. Sama arhitektura Interneta neprestano je u sukobu između dvije opcije: jedne opcije nepromijenjene arhitekture sa stalnim, uvijek prisutnim vezama između autonomnih sustava i svima znanom stalnom topologijom te druge opcije dinamičkog Interneta koji se prilagođava promjenama kako na kratkoročnoj vremenskoj razini, uzrokovanih opterećenjem veza, promjenama putova zbog pucanja veza i sl., tako i na dugoročnoj vremenskoj razini, promjenama u politikama usmjeravanja između autonomnih sustava, stvaranju novih autonomnih sustava i slično. BGP kao i svaki dinamički protokol omogućuje stvaranje dinamičkog Interneta, međutim nedostaje mehanizam koji će limitirati opseg te dinamičnosti jer prevelika dinamičnost, pogotovo stvaranje ruta kroz spore, neoptimalne i nestabilne veze, može uzrokovati ranije opisane probleme. U tu svrhu potrebno je stvoriti reputacijski sustav koji će pratiti kvalitetu pojedinih autonomnih sustava promatrajući postojanost i stabilnost veza između njih te na taj način rangirati same autonomne sustave. Tako će reputacija predstavljena brojčanom ocjenom pojedinog autonomnog sustava moći pomoći drugim autonomnim sustavima prilikom kasnijeg odlučivanja, odabira puta ili filtriranja određenih ruta koje prolaze kroz ranije dokazane nestabilne veze. Promatrajući upravljački promet rubnih usmjernika predlaže se reputacijski model koji će snimati postojanost veza između autonomnih sustava te iz te statistike izračunavati reputaciju. Iz UPDATE poruka dobivenih iz susjednih usmjernika ekstrahiraju se podaci te se spremaju u informacijski set:

$$Iij = a_j, p_i, [AS_N, AS_{N-1}, \cdots, AS_1, AS_0]$$

Informacijski set sadržava adresu susjednog usmjernika od koga je primljena UPDATE poruka s tim informacijskim setom $a_j$, sadržava sam prefiks koji je objavljen $p_i$ te put AS-ova kroz koji je prošla objava tog prefiksa $P_{ij}$ koji je predstavljen poredanom listom [$AS_N$, $AS_{N-1}$, ..., $AS_1$, $AS_0$] u kojoj je $AS_N$ broj posljednjeg autonomnog sustava u nizu, dok je $AS_0$ prvi autonomni sustav u nizu.

Dolaskom nove UPDATE poruke koja stvara istu oznaku informacijskog seta, dakle poruke od istog susjednog usmjernika s objavom ili povlačenjem istog prefiksa (isti $a_j$ i $p_i$) stvara se novi informacijski set $I_{ij}$'. Odnos između informacijskih setova $I_{ij}$ i $I_{ij}$' može imati 3 različita karaktera:

(1) Novi informacijski set ima promijenjeni atribut AS Path, odnosno $P_{ij}' \neq P_{ij}$. Posljedica je isključivo primitka objave u UPDATE poruci. Tada se vrši usporedba starog i novog puta te na temelju promjena kažnjavaju određeni autonomni sustavi. Stari informacijski set se briše te na njegovo mjesto dolazi novi informacijski set ($I_{ij}$').

(2) Novi informacijski set ima nepromijenjeni atribut AS Path odnosno $P_{ij}' = P_{ij}$. Posljedica je isključivo primitka objave u UPDATE poruci. Takva naoko ponovljena objava u praksi najčešće nosi neki drugi promijenjeni atribut ili je posljedica nepravilnog rada implementacije BGP-a. Jasno je da se tada informacijski set nije promijenio, odnosno $I_{ij} = I_{ij}'$, te se takva poruka neće uzimati u obzir prilikom izračuna postojanosti puteva.

(3) U UPDATE poruci povučen je prefiks $p_i$, s pripadajućim putem $P_{ij}$ bez da je objavljen novi

put za taj prefiks. Informacijski set $I_{ij}$ se zbog toga briše. Kasnija objava istog prefiksa, od strane istog susjeda tretirat će se kao potpuno nova objava s novim informacijskim setom.

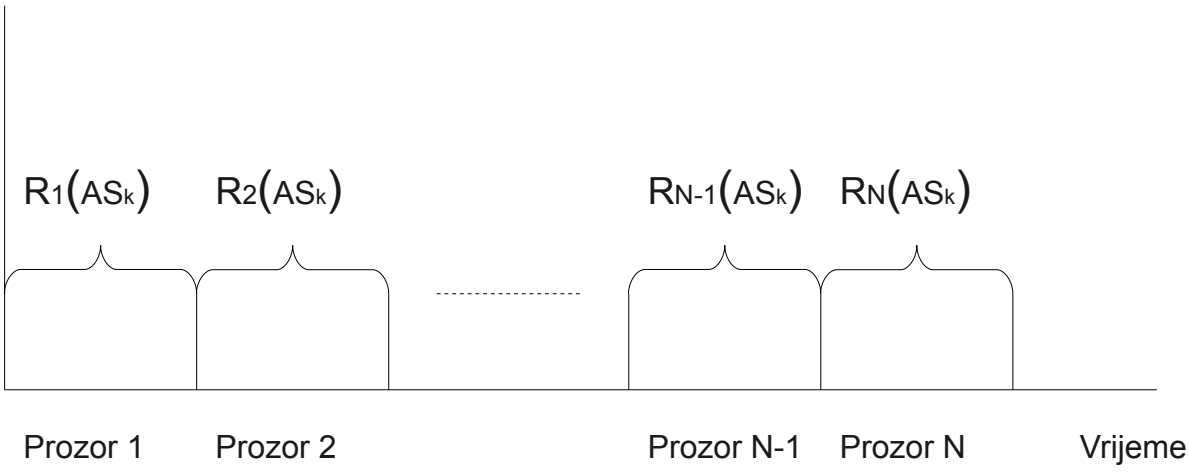
U slučaju (2) nije došlo do promjene puta te ne treba vršiti kažnjavanje autonomnih sustava na tome putu. Naravno da postoji mogućnost da je jedan od autonomnih sustava iz objavljenog puta uzrokovao ponovno slanje objave od strane našeg susjednog usmjernika, međutim to ne možemo sa sigurnošću znati.

Prilikom slučaja (1) potrebno je izvršiti usporedbu starog i novog puta. Novu objavu i promjenu rute uzrokovao je najvjerojatnije jedan od autonomnih sustava čija se veza nalazila u starom putu, a ne nalazi se u novom ili obrnuto. Naravno da je promjena mogla biti uzrokovana i drugim faktorima. Primjerice, moglo se dogoditi da je konfiguracija BGP-a upravo u tom trenutku promijenjena na jednom usmjerniku u nekom autonomnom sustavu na putu te je zbog novog pravila usmjeravanja odnosno nove politike usmjeravanja odabran novi put. Takve se situacije događaju rijetko odnosno na ljudskoj razini vremena jer su posljedice ljudske intervencije u samoj konfiguraciji te je njihov broj zanemariv u odnosu na ukupan broj situacija. Stoga je potrebno kazniti sve autonomne sustave koji su izgubili svoje veze u novoobjavljenom putu.

Kada dolazi do povlačenja starog puta kao u situaciji (3), također možemo imati više uzroka. Kao logičan uzrok nameće se povlačenje samog prefiksa od strane izvorišnog autonomnog sustava. Međutim, većina povlačenja uzrok ima u gubitku veze koja se može dogoditi bilo gdje na putu. Tada je potrebno kazniti sve autonomne sustave koji su imali međusobne veze na povučenom putu.

### 4.4.1 Izračun reputacije postojanosti veza

Izračun reputacije postojanosti veza odvija se u vremenskim prozorima. Tijekom trajanja svakog vremenskog prozora bilježe se sve nepostojanosti veza između autonomnih sustava koje dovode do njihovih kažnjavanja. Svaka promjena pridonosi povećanju reputacijskog inkrementa za promatrani prozor. Na kraju svakog prozora vrši se izračun ukupne reputacije za promatrani prozor.




*Slika 4.6. Prozori izračuna reputacije*

Ukupna se reputacija na kraju prozora dobiva kao kombinacija prijašnje reputacije i reputacije za promatrani prozor koristeći faktor zaboravljanja $\gamma$. Na taj se način reputacija nakon prozora N računa kao kombinacija reputacije izračunate u samom prozoru N i prijašnje reputacije. Ako je reputacija u koraku N-1 iznosila vrijednost $r_{N-1}$, tada će reputacija nakon prozora N ($r_N$) biti sljedeća:

$$r_N = (1-\gamma)\cdot r_{N-1} + \gamma \cdot R_N$$

*Formula 4.1. Izračun reputacije nakon N-tog prozora*

Slijedi objašnjenje izračuna reputacije za pojedini prozor.

Put $P_{ij}$ informacijskog seta $I_{ij}$ možemo raščlaniti na skup pojedinačnih veza između autonomnih sustava $S_{ij}$.

$$P_{ij} = [AS_N, AS_{N-1}, \cdots, AS_1, AS_0,]$$

$$S_{ij} = [(AS_N, AS_{N-1}), (AS_{N-1}, AS_{N-2}), \cdots, (AS_2, AS_1), (AS_1, AS_0)]$$

Budući da je put imao broj od N+1 autonomnih sustava u sebi dobit ćemo listu od N dvočlanih elemenata koji predstavljaju veze između autonomnih sustava. Promjenom puta $P_{ij}$ novom objavom u put $P_{ij}'$, formirat će se novi skup veza između autonomnih sustava $S_{ij}'$. Potrebno je napraviti razliku između ta dva skupa, odnosno naći elemente koji su prisutni u prvom skupu, ali nisu u drugom, kako bismo pronašli veze između AS-ova koje su se promijenile novom objavom. Takva razlika je također skup sastavljen od dvočlanih elemenata brojeva autonomnih sustava koji predstavljaju veze između njih. Skup promijenjenih veza označit ćemo sa $S_{ijP}$.

$$S_{ijP} = S_{ij} / S'_{ij}$$

Potom je potrebno pobrojati pojavljivanja autonomnih sustava u novonastalom skupu. Budući da u atributu AS Path ne smiju postojati petlje, svaki AS može se naći najviše 2 puta u tom skupu i to najviše jedan puta kao lijevi i najviše jedanput kao desni element dvočlanog para.

Ako sa $C(AS_t)$ označimo broj pojavljivanja autonomnog sustava *t* u skupu $S_{ijP}$, taj će broj predstavljati broj promijenjenih veza za autonomni sustav $AS_t$. Budući da je više autonomnih sustava moglo uzrokovati pucanje veze, potrebno je reducirati kaznu pojedinog autonomnog sustava na način da se njegova kazna dijeli s ukupnim brojem kazni svih T autonomnih sustava koji su mogli uzrokovati promjenu puta. Tako dobivamo reduciranu kaznu $C_r(AS_t)$ t-tog autonomnog sustava koja iznosi:

$$C_r(AS_t) = \frac{C(AS_t)}{\sum_{t=1}^{T} C(AS_t)}$$

Ukupna će kazna za t-ti autonomni sustav na kraju promatranog prozora iznositi $C_U(AS_t)$ te se računa kao zbroj svih reduciranih kazni autonomnih sustava koje je zaradio kroz sve od ukupno F prefiksa čije su objave prolazile kroz njega, za ukupno G susjednih usmjernika koji su slali te objave, za svih H promjena informacijskog seta $I_{ij}$ na $I_{ij}'$.

$$C_U(AS_t) = \sum_{i=1,j=1,k=1}^{F,G,H} C_r(AS_t)$$

Odmah se uočava da će upravo najveći autonomni sustavi koji su odgovorni za većinu tranzitnog prometa imati najviše promjena u svojim putovima. To nastaje kao posljedica koncentriranja prometa iz svih manjih rubnih sustava kroz njih same te će dovesti do lažnih očitanja. Stoga je potrebno ukupne kazne autonomnih sustava normalizirati s faktorom kojim će se u obzir uzimati ukupan broj ruta koje prolaze kroz autonomne sustave. Veliki tranzitni autonomni sustav ima jako puno ruta od kojih su velika većina stabilnih ruta. Zbog tako velikog broja ruta koje prolaze kroz njega, sam će mu normalizacijski faktor biti velik. Upravo će veliki normalizacijski faktor smanjiti efekt koji doživljavaju veliki autonomni sustavi kada im se gomilaju kazne zbog toga što su mijenjali putove prema manjim autonomnim sustavima koji imaju nestabilnije veze. Na taj način neće više biti relevantan ukupan broj puknutih, odnosno promijenjenih veza između autonomnih sustava u izračunu njihove reputacije, već će reputacija autonomnog sustava ovisiti o relativnom broju puknutih ili promijenjenih veza u odnosu na ukupan broj prefiksa koji kroz njega prolaze:

$$\sum_{i=1,j=1}^{F,G} N(p_i) : uz\ uvjet\ AS_t \in P_{ij}$$

Ukupnu kaznu za t-ti autonomni sustav podijelit ćemo s brojem svih prefiksa koji su na svom putu prošli kroz autonomni sustav $AS_t$ pomnožen s faktorom ε, koji predstavlja koeficijent normalizacije, i uvećan za 1 odnosno:

$$\frac{C_U(AS_t)}{1+\varepsilon \cdot \sum_{i=1,j=1}^{F,G} N(p_i) : uz\ uvjet\ AS_t \in P_{ij}}$$

Tako dobivenu vrijednost potrebno je dodatno skalirati na raspon [0,1] uporabom eksponencijalne funkcije. Na taj se način sprječava nepotreban prevelik rasap vrijednosti reputacije i izbjegavaju se, koliko je to moguće, ekstremne vrijednosti. Odmah je lakše uočiti lošije, odnosno bolje vrijednosti reputacije i u skladu s time grupirati autonomne sustave kao bolje, odnosno lošije. Skaliranje vrijednosti kazne vrši se dakle obrnutom eksponencijalnom funkcijom uz faktor δ:

$$R_N(AS_t) = \mathrm{e}^{-\delta \cdot \frac{1}{C_U(AS_t)/\left(1+\varepsilon \cdot \sum_{i=1,j=1}^{F,G} N(p_i)\right)}}$$

*Formula 4.2. Inkrement reputacije postojanosti veza*

Dobivena je vrijednost reputacije izračunate u N-tom prozoru za t-ti autonomni sustav kako je navedeno formulom 4.2. Ona predstavlja inkrement reputacije koji se uz faktor zaboravljanja korišten u formuli 4.1 koristi za izračun ukupne reputacije t-tog AS-a nakon N prozora. Time se dobiva ukupna vrijednost reputacije koja se ponovno izračunava nakon svakog prozora za sve autonomne sustave, a njena se vrijednost uvijek nalazi u okviru [0,1].

## 4.5 Postojanost veze prefiks – izvorišni autonomni sustav

Dodjeljivanje IP adresa i prefiksa autonomnim sustavima vrši se pod nadzorom IANA-e i lokalnih registratora. Tim se postupkom svakom AS-u daju određeni opsezi IP adresa pokriveni određenim prefiksima koji ostaju permanentno vezani za dotični autonomni sustav. Za razliku od prethodnog slučaja gdje su promatrane veze između AS-ova i putovi koji su podložni češćim promjenama, sama veza između prefiksa i njegovog izvorišnog autonomnog sustava prilično je čvrsta. Iznimke od ovog pravila agregirani su prefiksi, gdje autonomni sustav više razine, davatelj usluge, spaja više prefiksa svojih korisnika u superprefiks te njega objavljuje svojim susjedima. Promjene vlasništva prefiksa između autonomnih sustava su rijetke. Svode se uglavnom na dogovorene prijenose koji su iznimno rijetki (primjerice kada jedna tvrtka ili ISP kupi od drugoga prefiks ili prefikse) i na dodjele istog prefiksa od strane davatelja usluge različitim korisnicima ili korisničkim AS-ovima u različito vrijeme. U ovom se drugom slučaju sam postupak najčešće izvodi transparentno za ostatak Interneta gdje samo AS davatelja usluge ostaje vidljiv ostatku Interneta kao izvorišni AS tog prefiks, a samo on sam zna kojem AS-u od njegovih korisnika usluge pripada pojedini prefiks u kojem trenutku. Stoga je realno očekivati da će se, premda se putovi mogu mijenjati, uvijek isti prefiks biti objavljen od strane istog autonomnog sustava. Takva veza naziva se veza prefiks – autonomni sustav. Pojavom objave prefiksa od strane drugog autonomnog sustava ta veza biva narušena. To može biti posljedica ranije opisanih slučajeva ili posljedica otimačine. Sama otimačina ili prisvajanje tuđeg prefiksa, suprotno popularnom mišljenu, rjeđe je posljedica zle namjere, a češće je samo zapravo pogreška u konfiguraciji rubnih usmjernika. No ipak i takva nenamjerna pogreška može uzrokovati gubitak veza s dijela ili čak s cijelog Interneta prema otetim prefiksima. Kod zlonamjernih otimačina situacija je ista prethodno opisanoj s razlikom što zlonamjerni otimač ima svrhu ili spriječiti pristup otetim prefiksima ili, još gore, prisluškivati tuđi promet. Svaka otimačina generira dodatni servisni promet koji nepotrebno opterećuje druge usmjernike i stvara nepotreban promet. Kao posljedica može se pojaviti zagušenje veza uslijed pogrešno usmjeravanog prometa. Budući da su istraživanja opisana u radu "Understending BGP Misconfiguration" [7] pripisali većinu otimačina pogreškama u konfiguraciji kao što je opisano u poglavlju 3., pri vrednovanju autonomnih sustava možemo se poslužiti postojanošću veza između prefiksa i njegovog izvorišnog sustava. U skladu s time razvija se obrazac pretpostavki ponašanja za set veza prefiks – autonomni sustav. Od autonomnog sustava u vezi prefiks - autonomni sustav zahtijeva se da ne pokazuje sljedeća ponašanja:

- **Ilegalnost:** autonomni sustav ne smije objavljivati prefikse kojima je zabranjeno ili ograničeno objavljivanje na Internetu. Također ne smije u atribut AS Path uključivati brojeve autonomnih sustava koji se ne smiju koristiti na Internetu.
- **Otimačina:** autonomni sustav ne smije objavljivati prefikse koji mu ne pripadaju, odnosno koji mu nisu dodijeljeni od strane registratora. Postupak suprotan ovome izaziva krađu prefiksa što može dovesti do djelomičnog ili potpunog gubitka veze s Internetom pravog vlasnika ukradenog prefiksa.
- **Nestalnost**[1]**:** autonomni sustav trebao bi se suzdržati od čestih objava i povlačenja prefiksa. Također bi se trebao suzdržati od čestih promjena prefiksa postupcima agregacija i deagregacija. Navedeni slučajevi uzrokuju nepotreban usmjernički promet, stvaraju nestabilnost usmjeravanja prema zahvaćenim prefiksima te mogu dovesti do drugih grešaka.

Ilegalnost danas ne predstavlja veliki problem. Većina administratora autonomnih sustava filtrira

1 Nestalnost prefiksa često se naziva kolebanjem (engl. vacillation)

sve objave koje sadrže ilegalne IP adrese ili ilegalne brojeve autonomnih sustava tako da će se oni rijetko naći u usmjerničkim tablicama BGP usmjernika. S druge je strane ipak malo teže odrediti je li neki prefiks otet ili nije. Premda postoje podaci kod registratora kojem autonomnom sustavu pripada koji prefiks te se ti podaci mogu saznati uvidom u bazu ili direktnim upitom (*whois* upit), često su ti podaci neažurirani te ne prikazuju dobro stvarno stanje na terenu. Također bi postojanje neraskidivih veza između prefiksa i AS-ova ugrozilo dinamiku samog Interneta što bi se posebice osjetilo pri objavljivanju agregiranih ruta, gdje bi upit u centralnu bazu za pripadnošću agregiranog prefiksa autonomnom sustavu koji ga objavljuje stvorio mnogobrojna lažna pozitivna očitanja, odnosno takve bi se objave mogle okvalificirati kao otimačina prefiksa makar to stvarno nisu. Pri našem izračunu reputacije poslužit ćemo se pak mjerenjem nestalnosti objavljenih prefiksa koja se može prikazati faktorima prevalencije i perzistencije što je opisano u sljedećem odjeljku.

### 4.5.1 Izračun reputacije postojanosti veze prefiks – izvorišni autonomni sustav

Kao i pri izračunu reputacije postojanosti veza, pri izračunu reputacije postojanosti veze prefiks – izvorišni autonomni sustav mjerenja vršimo u vremenskim prozorima prikazanima na slici 4.6. Tijekom trajanja svakog vremenskog prozora bilježe se sve nepostojanosti veze prefiks – izvorišni AS koje dovode do kažnjavanja izvorišnog AS-a. Svaka nepostojanost pridonosi povećanju reputacijskog inkrementa za promatrani prozor. Na kraju svakog prozora vrši se izračun ukupne reputacije za promatrani prozor. Ukupna se reputacija na kraju prozora dobiva kao kombinacija prijašnje reputacije i reputacije za promatrani prozor koristeći faktor zaboravljanja $\gamma$. Na taj se način reputacija nakon prozora N računa kao kombinacija reputacije izračunate u samom prozoru N i prijašnje reputacije kao što je prikazano formulom 4.1.

Za izračun reputacije ponovno ćemo se koristiti informacijskim setom $I_{ij}$. Slijedi objašnjenje izračuna reputacije za pojedini prozor.

$$\exists a_j \, za \, koji \, \exists I_{ij} \rightarrow I_i(AS_k)$$

gdje je $I_i(AS_k)$ pojavljivanje objave prefiksa $p_i$ od strane izvorišnog autonomnog sustava $AS_k$ unutar N-tog prozora duljine trajanja $T_{WN}$ za sve informacijske setove $I_{ij}$:

$$Iij = a_j, p_i, [AS_N, AS_{N-1}, \cdots, AS_1, AS_0]$$

Tada je ukupan broj različitih prefiksa u N-tom prozoru objavljenih od strane izvorišnog AS-a $AS_k$, $Q(AS_k)$ jednak:

$$Q(AS_k) = \sum_{i=1}^{Q} I_i(AS_k)$$

gdje je Q jednak ukupnom broju svih različitih prefiksa objavljenih od strane svih autonomnih sustava unutar N-tog prozora.

Ako je $t_{ikm}$ vremensko trajanje m-te objave prefiksa $p_i$ od strane AS-a $AS_k$ u N-tom prozoru, onda je ukupno trajanje objave tog prefiksa od strane tog AS-a u N-tom prozoru jednako:

$$T_{ik} = \sum_{m=1}^{M_{ik}} t_{ikm}$$

gdje je $M_{ik}$ ukupan broj različitih pojavljivanja prefiksa $p_i$ objavljenog od strane autonomnog sustava $AS_k$.

Tada je prevalencija prefiksa $p_i$ za $AS_k$, $P_{sik}$ iznositi:

$$P_{sik} = \frac{T_{ik}}{T_W}$$

gdje Tw iznosi vremenski interval trajanja N-tog prozora. Prevalencija zapravo predstavlja frakcijski dio prozora u kojem je bila aktivna objava prefiksa $p_i$ od strane izvorišnog AS-a $AS_k$. Iz izračuna je jasno da perzistencija može poprimiti vrijednosti samo iz intervala [0,1]. Vrijednost 0 poprima kada dotični prefiks nije bio uopće objavljen od strane promatranog AS-u u tom intervalu, dok vrijednost 1 poprima kada je prefiks bio objavljen cijelo vrijeme trajanja intervala[2]. Namijenjena je kažnjavanju autonomnih sustava koji objavljuju nepostojane prefikse (prefikse koji nisu stalno prisutni u globalnoj usmjerničkoj tablici.

Perzistencija predstavlja prosječno trajanje objave prefiksa $p_i$ od strane AS-a $AS_k$ kao frakciju promatranog intervala te se računa na sljedeći način:

$$P_{rik} = \frac{T_{ik}}{M_{ik} \cdot T_W}$$

Perzistencija također poprima vrijednosti u intervalu [0,1] te je namijenjena kažnjavanju većeg broja objava i povlačenja prefiksa unutar promatranog prozora za k-ti AS.

Ukupna se prevalencija i perzistencija k-tog autonomng sustava računaju kao zbroj prevalencija i perzistencija svih prefiksa koji su imali objave od strane k-tog AS-a u N-tom prozoru:

$$P_{sk} = \sum_{i=1}^{Q(AS_k)} P_{sik}$$

i

$$P_{rk} = \sum_{i=1}^{Q(AS_k)} P_{rik}$$

Kombinacijom ukupne prevalencije i perzistencije dobiva se reputacijski inkrement k-tog AS-a za N-ti prozor sljedećom formulom:

$$R_N(AS_k) = \frac{P_{sk} + P_{rk}}{2 \cdot Q(AS_k)}$$

*Formula 4.3. Inkrement reputacije veze prefiks - izvorišni AS*

Dobivena je vrijednost reputacije izračunate u N-tom prozoru za t-ti autonomni sustav kako je prikazano formulom 4.3. Ona predstavlja inkrement reputacije koji se uz faktor zaboravljanja korišten u formuli 4.1 koristi za izračun ukupne reputacije t-tog AS-a nakon N prozora. Time se dobiva ukupna vrijednost reputacije koja se ponovno izračunava nakon svakog prozora za sve autonomne sustave, a njena se vrijednost uvijek nalazi u okviru [0,1].

2 Da bi prefiks bio objavljen od strane nekog autonomnog sustava u nekom intervalu, nije nužno da postoji i objava u UPDATE poruci u promatranom intervalu. Jednostavno taj je prefiks mogao biti objavljen u nekom prijašnjem intervalu ili je mogao biti u RIB tablici prije samog početka izračuna reputacije te poslije nije nikada povučen. Tada kažemo da je prefiks u stanju aktivne objave za taj interval.

# 5. Arhitektura reputacijskog sustava

Prototip reputacijskog sustava izrađen je u programskom jeziku Python. Po automatskoj memorijskoj alokaciji, Python je sličan programskim jezicima kao što su Perl, Ruby, Smalltalk itd. Python dopušta programerima korištenje nekoliko stilova programiranja. Objektno orijentirano, strukturno i aspektno orijentirano programiranje dopušteni su stilovi korištenjem Pythona te ova fleksiblinost čini Python programski jezik sve popularnijim.

Prednosti su korištenja Pythona pri praktičnoj implementaciji postavljenog zadatka velike. Prije svega sam je programski jezik Python lagan za savladavanje, jednostavan za korištenje i omogućuje lagano povezivanje više dijelova programa u cjelinu. Prilikom izvođenja programa pokazala se potreba za intenzivnom manipulacijom i obradom tekstualnih podataka za što Python pruža dobru podršku. Manipulacija datotečnim sustavom također je jednostavna i brza u programskom jeziku Python. Naposljetku, velika prednost Pythona je veliki izvor raznih modula i gotovih rješenja za razne podzadaće koje su se koristile prilikom izrade programske implementacije prototipa reputacijskog sustava u okviru teme ovog diplomskog rada.

Program je pisan za izvođenje na verziji Pythona 2.7.1 te nije provjeravana kompatibilnost sa starijim verzijama. Kao pomoć pri pisanju samog programa korišteno je nekoliko dodatnih paketa otvorenog koda:

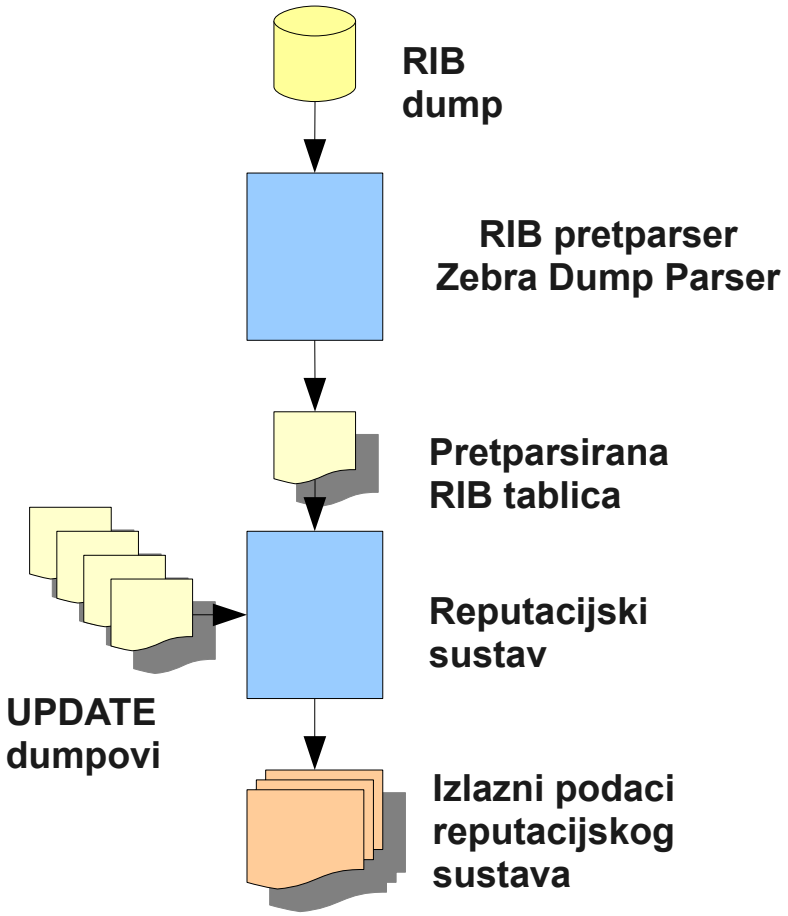
- dpkt-1.7 [9]
- mdmft-0.2 [8]
- pybgpdump-0.2 [10]

Paket dpkt sadrži veliki broj dodatnih modula namijenjenih podršci stvaranja programa koji koriste razne mrežne protokole. Ovaj je paket bitan jer kroz svoj modul *bgp.py* omogućava laganu obradu i manipulaciju poruka koje se koriste za rad protokola rubnih usmjernika (BGP-a). Nadalje tu je paket mdmft u čijem se sastavu nalazi zakrpa za sam paket dpkt čime se on proširuje za mogućnosti korištenja više ulaznih formata BGP poruka pohranjenih u datotekama. Naposljetku tu je i paket pybgpdump koji kroz svoj modul *pybgpdump.py* daje mogućnosti laganog parsiranja BGP UPDATE poruka te izdvajanje ključnih dijelova iz samih poruka koji su potrebni za daljnju obradu prilikom izračuna reputacije. Svi ovi dodatni paketi u potpunosti imaju licencu slobodnog korištenja otvorenog koda (engl. *open source*).

Za pretparsiranje datoteka s RIB tablicama usmjernika napravljen je parser baziran također na programu otvorenog koda napisanog u programskom jeziku Perl pod nazivom Zebra Dump Parser. On se koristi za pretparsiranje podataka iz RIB tablica usmjernika u oblik pogodan za daljnu obradu programskim jezikom Python. Sam postupak pretparsiranja ubrzava izvođenje same implementacije reputacijskog sustava te također pomaže standardizaciji samog sustava s obzirom na ulazne podatke. Naime ulazni podaci, pogotovo RIB tablice, mogu doći u više formata što može stvoriti određene poteškoće prilikom njihove obrade. Sam program testiran je na nekoliko ulaznih formata te se uz korištenje Zebra Dump Parsera lagano može prilagoditi za možebitne druge formate, kao i za formate koji se možda tek pojave u budućnosti.

## 5.1 Tijek izvođenja programa

Cijeli sustav za izračun reputacija sastoji se od RIB pretparsera i reputacijskog sustava. RIB pretparser zadužen je za pretparsiranje RIB dump usmjerničkih datoteka u format pogodan za daljnju obradu reputacijskim sustavom. Sam reputacijski sustav, koji je izveden u dvije varijante, kao ulazne podatke uzima pretparsiranu RIB tablicu te listu datoteka u kojoj su pohranjeni dumpovi UPDATE poruka. Tijekom izvršavanja programa izlazni se rezultati, same reputacije i dodatne informacije ispisuju u datoteke. Izgled sustava za izračun reputacija shematski je prikazan na slici 5.1.




*Slika 5.1. Arhitektura reputacijskog sustava*

RIB pretparser ima zadaću pretparsiranja RIB dump datoteka u jednostavniji format pogodan za daljnju obradu reputacijskom sustavom. RIB dump datoteke sadrže ispise cjelokupne RIB tablice usmjernika. Oni su zapisani u MRT formatu (engl. Multithreaded Routing Toolkit) napravljenom prvenstveno za pohranu usmjerničkih informacija. Datoteke u MRT formatu binarne su datoteke te postoji više podformata MRT-a. Danas je najčešće korišteni format za BGP dump datoteke "IPV4 MRT RIB table dump v2". Takve binarne datoteke u MRT formatu dodatno su komprimirane, najčešće u gzip ili bzip2 sustavu komprimiranja te ih je prvo potrebno dekomprimirati. Zatim je potrebno promijeniti parametre, ime ulazne i izlazne datoteke te pozvati Zebra Dump Parser kako bi izvršio pretparsiranje RIB datoteke kao što je prikazano primjerom na ispisu 5.1.

```
open(INPUT, 'rib') or die "Could not open INPUT $!\n";
open(MYOUTFILE, ">rib.parsed");
.....
perl zebra-dump-parser.pl
```

*Ispis 5.1. Ispis konfiguracije i pozivanja pretparsera*

Pretparsiranjem RIB datoteka dobivaju se jednostavne tekstualne datoteke, čitljive ljudima, samo s izdvojenim podacima potrebnima za kasniji izračun reputacija. Izgled pretparsirane RIB tablice prikazan je na ispisu 5.2. Sadrži podatke o objavljenom prefiksu, atributu AS Path te o oznaci susjednog usmjernika od kojeg je došao taj podatak u obliku IP adrese.

```
PREFIX: 91.212.154.0/24
FROM: 202.249.2.86
AS_PATH: 7500 2516 3549 21219 49139
PREFIX: 91.212.155.0/24
FROM: 202.249.2.169
AS_PATH: 2497 3549 5588 8246 49141
PREFIX: 91.212.155.0/24
FROM: 202.249.2.86
AS_PATH: 7500 2497 3549 5588 8246 49141
```

*Ispis 5.2. Pretparsirana RIB tablica*

## 5.2 Izvor informacija usmjerničkog prometa

Reputacijski sustav u svojoj bi primijenjenoj izvedbi trebao biti izveden na poslužitelju koji će ostvarivati susjedske veze s velikim brojem BGP usmjernika u raznim autonomnim sustavima te bi od njih trebao dobivati usmjerničke informacije. Taj bi se poslužitelj u susjedskom odnosu ponašao kao i svaki drugi usmjernik uz tri iznimke:

- Samo bi primao usmjerničke podatke, a ne bi ih slao svojim susjedima
- Ne bi usmjeravao promet
- Održavao bi susjedske odnose i s usmjernicima koji se ne nalaze u autonomnim sustavima izravno spojenima matičnom sustavu ovakvog poslužitelja

Takvi se poslužitelji nazivaju usmjernički kolektori te ih održavaju veliki davatelji usluga, registratori, obrazovne ustanove i sl., u svrhu prikupljanja usmjerničkog prometa. Za prototip reputacijskog sustava napravljen u okviru ovog diplomskog rada poslužit ćemo se upravo takvim usmjerničkim kolektorima koji prikupljaju usmjerničke informacije te ih pohranjuju u datoteke.

Dva su osnovna tipa datoteka u kojima kolektori pohranjuju informacije:

- RIB datoteke
- UPDATE datoteke

U RIB datotekama pohranjuje se ispis cjelokupne RIB tablice usmjernika (kolektora) u određenom trenutku. To su binarne datoteke u jednoj od verzija MRT formata dodatno komprimirane. Kolektori ih pohranjuju u pravilnim vremenskim razmacima, obično svakih 2 sata. Drugi je tip također binarnih UPDATE datoteka u koje kolektori pohranjuju sve UPDATE poruke dobivene od svojih susjeda u određenom vremenskom intervalu. One se pohranjuju najčešće u pravilnim vremenskim razmacima od 15 ili 20 minuta. Imena datoteka su tako složena da se iz njih može lagano iščitati vrijeme nastanka; za RIB datoteke to je točan trenutak RIB tablice, a za UPDATE datoteke je početni trenutak od kojeg se pohranjuju UPDATE poruke. Iz imena sljedeće datoteke saznaje se početni trenutak sljedećeg prozora prikupljanja i pohrane UPDATE poruka što se poklapa sa zaključnim trenutkom prethodnog prozora.

Za potrebe ovog rada korišteni su podaci s kolektora pohranjeni na web stranici održavanoj od strane Oregonskog sveučilišta u okviru projekta pod vodstvom Davida Meyera [3].

## 5.3 Reputacijski sustav

Reputacijski sustav odgovoran je za učitavanje ulaznih podataka o usmjerničkom prometu, ekstrakciju informacija potrebnih za izračun reputacije, obradu informacija, izračune relevantnih podataka i same reputacije te za pohranu dobivenih vrijednosti u izlazne datoteke. Izveden je u tri modula:

- *classes.py*
- *link_bindings.py*
- *pref_bindingy.py*

Prvi modul, *classes.py*, sadrži razrede objekata. Dva glavna razreda u kojima se vrši obrada podataka, izračun i pohrana reputacija prije ispisa su *PrefixPath* i *PrefixAS0Binding*. Prvi razred služi pri izračunu reputacija metodom postojanosti veza između autonomnih sustava dok se drugi razred koristi za izračun reputacija metodom postojanosti veze prefiks – izvorišni autonomni sustav. Sljedeća dva modula izvršavaju program za te dvije metode izračuna reputacija; modul *link_bindings.py* za izračun metodom postojanosti veza, a modul *pref_bindings.py* za izračun metodom postojanosti veze prefiks – izvorišni AS. Samo pozivanje i prilagodba parametara programa vrlo je jednostavno. U oba modula potrebno je navesti samo sljedeće podatke:

- ime pretparsirane RIB datoteke
- putanju direktorija s pohranjenim UPDATE dump datotekama
- početno vrijeme prvog prozora
- trajanje pojedinog prozora

Sama promjena parametara prikazana je na ispisu 5.3.

```
os.chdir(dircur + "/UP")      #directory containing UPDATE dumps
...
f0Name = dircur + '/RIB/RIB.parsed'          #preparsed RIB
...
time_win = 4*60*60  #duration of computation window in seconds
hours x minutes x seconds
...
time_start = time.mktime(time.strptime("14 Jan 11 CET 06 00
00", "%d %b %y %Z %H %M %S")) #start time of first dump
```

*Ispis 5.3. Parametri u kodu*

Opcionalni parametri izračuna reputacija nalaze se u datoteci *classes.py* te ih je također lagano prilagoditi kao što je prikazano na ispisu 5.4.

```
alpha = float(0.8)
beta = float(0.5)
gama = float(0.5)
delta = float(0.25)
```

*Ispis 5.4. Postavljanje parametara izračuna reputacije*

### 5.3.1 Izlazni podaci reputacijskog sustava

Prilikom izvođenja programa na konzolnom se izlazu ispisuje trenutna datoteka koja se obrađuje kao i kraj svakog prozora obrade. Svi se ostali podaci ispisuju u izlazne datoteke. Pri pozivanju modula izračuna reputacija metodom postojanosti veza između autonomnih sustava nastaju datoteke gdje je sa N označen redni broj prozora nakon kojega je nastao ispis:

- *RIB_Prefixes_Source_AS_information*
- *Prefixes_Source_AS_information_N*
- *Ases_prefix_percentage_N*
- *Ases_reputation_N*

Datoteka *RIB_Prefixes_Source_AS_information* i datoteke *Prefixes_Source_AS_information_N* su istog formata i sadrže informacije o objavljenim prefiksima. U datoteci *RIB_Prefixes_Source_AS_information* to je informacija o objavljenim prefiksima učitanima iz RIB tablice. U slučaju datoteka *Prefixes_Source_AS_information_N* to su kumulativne informacije o prefiksima na kraju N-tog prozora. Za svaki od objavljenih prefiksa dane su sljedeće informacije:

- Source AS: Izvorišni autonomni sustav za taj prefiks

- Time of Activation: Vrijeme prve objave ovog prefiksa u N-tom prozoru
- Total Active Time: Ukupno vrijeme koje je prefiks bio objavljen u N-tom prozoru
- Repetition: Broj ponovnih objava prefiksa (u slučaju da je bilo više objava i povlačenja)
- Update from Router(s): Susjedni usmjernici od kojih je ova objava stigla

U slučaju da ima više izvorišnih AS-ova za isti prefiks, što se događa iznimno rijetko, uglavnom u stanju greške, svi se podaci ispisuju ponovno, po jedanput za svaki izvorišni AS. Vrijeme aktivacije prikazano je kao broj sekundi od 1. 1. 1970. Ako je vrijeme aktivacije 0, prefiks trenutno nije aktivan s izvorištem u navedenom AS-u. Ukupno aktivno vrijeme zbroj je svih intervala u kojima je prefiks bio aktivan u N-tom prozoru. Ukoliko je to vrijeme jednako 0, a vrijeme aktivacije nije 0, znači da je prefiks još uvijek aktivan sa svojom prvom objavom u N-tom prozoru. Tada će se i to vrijeme pribrojiti prilikom izračuna na kraju prozora. Broj ponavljanja označava ukupan broj puta koliko je prefiks objavljen u promatranom prozoru nakon što je bio povučen. Objava prefiksa naslijeđena iz prethodnog prozora također se broji kao jedna objava. I naposljetku je tu popis susjednih usmjernika od koji je stigla objava tog prefiksa. Ukoliko je taj popis prazan, prefiks je povučen i njegovo je vrijeme aktivacije 0. Prefiks je aktivan dok postoji barem jedan susjedni usmjernik koji je objavio taj prefiks. Izgled navedenih datoteka prikazan je na ispisu 5.5.

```
Prefix:  66.17.158.0/23
    Source AS:                6517
    Time of Activation:       1203805320.0
    Total Active Time:        0
    Repetition:               1
    Update from Router(s):
                              202.249.2.86
                              202.249.2.20
                              202.249.2.169
```

*Ispis 5.5. Informacije o prefiksima*

Datoteka *Ases_prefix_percentage_N* također nastaje nakon svakog prozora te sadrži tekuće podatke na kraju N-tog prozora. Sastoji se od sljedećih informacija:

- AS-Num: Broj autonomnog sustava
- Number of Prefixes Broj prefiksa kojima je ovaj sustav izvorišni
- Total Active Percentage Time Prevalencija
- Average Active Percentage Time Perzistencija

Izgled datoteke dan je ispisom 5.6.

```
    AS-Num:     3

    Number of Prefixes                  19
    Total Active Percentage Time        1.0
    Average Active Percentage Time      1.0
-----------------------------------
    AS-Num:     4

    Number of Prefixes                  7
    Total Active Percentage Time        1.0
    Average Active Percentage Time      1.0
-----------------------------------
```

*Ispis 5.6. Informacije o autonomnim sustavima*

Datoteke *Ases_reputation_N* ispisuju iznos ukupne reputacije autonomnih sustava nakon N-tog prozora. Ispis sadrži redni broj autonomnog sustava, počevši od najlošije rangiranog prema najboljem, sam broj AS-a te pripadajuće izračunate reputacije nakon N-tog prozora kao što je prikazano ispisom 5.7.

```
Order num.: 33      AS 36889:     Reputation: 0.603430555556
Order num.: 34      AS 32334:     Reputation: 0.607611111111
Order num.: 35      AS 13789:     Reputation: 0.607873294347
Order num.: 36      AS 32226:     Reputation: 0.616166666667
Order num.: 37      AS 44154:     Reputation: 0.621388888889
Order num.: 38      AS 38927:     Reputation: 0.626944444444
Order num.: 39      AS 22284:     Reputation: 0.627846978558
```

*Ispis 5.7. Reputacije autonomnih sustava*

Identičan ispis reputacija po autonomnim sustavima kao u prethodnom primjeru koristi i modul za izračun reputacija metodom postojanosti veza između autonomnih sustava ispisom u datoteku *Reputations_N* za ukupnu izračunatu reputaciju nakon N-tog prozora.

# 6. Mjerenja reputacija

Prema modelima predloženima u poglavlju 4., izrađena su dva reputacijska sustava. Jedan ima zadaću mjeriti postojanost veza između autonomnih sustava, uočavati nestabilne veze, česta pucanja veza i promjene putova te na temelju dobivenih mjerenja evaluirati ponašanje autonomnih sustava i izračunati im reputaciju. Drugi reputacijski sustav mjeri povezanost veze prefiks – izvorišni autonomni sustav; kroz izračun prevalencije i perzistencije prefiksa i autonomnog sustava u kojem ima izvorište, izračuna se reputacija tog autonomnog sustava. Na temelju uočenih ponašanja rubnih usmjernika i autonomnih sustava izvedene su metode izračuna oba reputacijska modela opisane u poglavlju 4. Budući da su navedene metode i formule izračuna reputacije izvedene pretpostavkom, potrebno je bilo izvršiti razna mjerenja kako bi se potvrdila ispravnost predloženih metoda izračuna za dobivanje reputacija autonomnih sustava. Pri raznim mjerenjima mijenjani su parametri izračuna i prilagođavane su same formule izračuna reputacije kako bi što bolje predstavljale stvarnu reputaciju autonomnih sustava. Tu se nametnuo prvi problem nepoznavanja referentne reputacije. Budući da ne postoji izrađen i javno dostupan reputacijski sustav koji bi poslužio kao orijentir pri kalibriranju ovog reputacijskog sustava, mjerenja su vršena za neke poznate povijesne slučajeve većih incidenata na samom mjerenju. Iskušavani su razni parametri, što je i prikazano u nastavku poglavlja, ne bi li se sustav što bolje prilagodio stvarnim uvjetima i ne bi li što bolje i točnije izračunavao reputacije AS-ova. Dokumentirano je kako odabir različitih vrijednosti parametara može potencirati identifikaciju određenih problema, poput krađe prefiksa te su predložene vrijednosti parametara u ovisnosti o stvarnoj primjeni reputacijskog sustava.

Pri samom mjerenju uočeni su neki nedostaci u reputacijskom sustavu. Pri izradi modela i implementaciji uzeta je u obzir potreba za normalizacijom izmjerenih vrijednosti. Normalizacija je potrebna zbog različitog opsega mjerenja za različite veličine i razine autonomnih sustava. Primjerice, veliki tranzitni sustav imat će iznimno velika očitanja pri mjerenju promjena putova, odnosno nestalnosti veza između AS-ova. To se događa jer takav veliki tranzitni AS kroz sebe usmjerava i prosljeđuje objave velikog broja manjih autonomnih sustava. Ako se veliki broj manjih autonomnih sustava ponaša protivno dobroj praksi usmjeravanja, veliki će tranzitni autonomni sustav zbog toga neopravdano biti kažnjen lošijom reputacijom. Zbog toga je u sam izračun reputacije obavezno uvršten postupak normalizacije. U ovom slučaju gdje se mjere promjene putova, očitanje samog mjerenja normalizira se s ukupnim brojem putova koji prolaze kroz navedeni sustav. Tako će tranzitni AS, premda ima veliki broj promjena putova, imati malen relativan broj promjena u odnosu na ukupan broj objava putova. Normalizacija stoga uspješno rješava navedeni problem.

Drugi je problem uočen pri samim apsolutnim vrijednostima reputacije. Kod više manjih istodobnih ili jednog većeg incidenta, usmjernički promet na kojem se bazira izračun reputacije propagira se diljem Interneta. Stoga će se reputacija pogoršavati ne samo sustavima koji su grešku i uzrokovali, već će se u manjoj mjeri pogoršavati i drugim autonomnim sustavima obrnuto proporcionalno udaljenosti od sustava koji je grešku prouzročio i njegova utjecaja. Stoga je ponekad umjesto apsolutne vrijednosti reputacije bolje promatrati relativne vrijednosti reputacije pojedinog autonomnog sustava, odnosno njegov položaj u odnosu na druge autonomne sustave. Tako primjerice s velikom sigurnošću možemo reći da je problematičan AS kojemu je reputacija među 5% najlošije rangiranih autonomnih sustava neovisno o apsolutnoj vrijednosti njegove reputacije. U sljedećim su primjerima dane uz apsolutne vrijednosti reputacije i relativne vrijednosti, odnosno položaj prema drugim AS-ovima za koje se mjeri reputacija.

## 6.1 Krađa YouTubea

Jedan od velikih incidenta u globalnoj usmjerničkoj tablici neslavna je krađa popularnog Internetskog servisa YouTube od strane jednog pakistanskog davatelja pristupa Internetu. Događaj se zbio u nedjelju, 24. veljače 2008. kada je ISP Pakistan Telecom odlučio zabraniti svojim korisnicima pristup servisu YouTube [4]. Pakistanska je vlada, naime odredila blokadu pristupa YouTubeu zbog navodno uvredljivog sadržaja prisutnog na njihovim stranicama. Kada je Pakistanska regulatorna agencija za elektroničke medije proslijedila zabranu ISP-ovima, navedeni ISP odabrao je metodu zabrane pristupa YouTubeu koja je uzrokovala incident. Umjesto da filtriraju promet prema IP adresama YouTubeovih poslužitelja ili da prestanu redistribuirati prefikse YouTubea u svoju mrežu, odlučili su se za drugačiji pristup. Sami su oglasili posjedovanje tih prefiksa želeći tako postati lažno odredište prometa prema YouTubeu za sve svoje korisnike. Slučajno ili namjerno, ti su se prefiksi našli na Internetu te su brzo proslijeđeni drugim autonomnim sustavima. Tako je ISP Pakistan Telecom postao lažno odredište prometa namijenjenog YouTubeovim serverima ne samo za svoje korisnike, već i za veliku većinu Interneta [17]. Tako se autonomni sustav pakistanskog ISP-a, AS 17557, neko vrijeme našao kao izvor prefiksa YouTubea u većini usmjerničkih tablica BGP usmjernika. Slijedi vremenski tijek događaja koji su doveli do ispada YouTubea pri čemu su sva vremena prikazana kao UTC vremena:

- **Prije, tijekom i poslije nedjelje, 24. veljače 2008.:** YouTubeov AS (AS 36561) objavljuje prefiks 208.65.152.0/22 koji pokriva poslužitelje servisa YouTube. Također objavljuje i neke druge prefikse, međutim oni nisu relevantni za promatrani slučaj.

- **Nedjelja, 24. veljače 2008., 18:47:** AS Pakistan Telecoma (AS 17557) objavljuje prefiks 208.65.153.0/24. PCCW Global (AS 3491) – davatelj usluge pristupa pakistanskom ISP-u propagira objavu tog prefiksa. U roku od svega nekoliko minuta ta se objava proširila cijelim Internetom te je sav promet prema YouTubeu preusmjeren u Pakistan.

- **Nedjelja, 24. veljače 2008, 20:07:** YouTubeov AS počinje objavljivati prefiks 208.65.153.0/24. Budući da su se sada u globalnoj BGP tablici našla dva identična prefiksa, algoritam odabira najboljeg puta odlučuje koja će ruta biti izabrana. Sada dio Interneta još uvijek vidi pakistanski ISP kao izvor prefiksa koji pripada YouTubeu.

- **Nedjelja, 24. veljače 2008, 20:18:** YouTube počinje objavljivati još specifičnije prefikse 208.65.153.0/25 i 208.65.153.128/25. Po pravilu duljeg prefiksa sada se sav promet prema YouTubeu zaista usmjerava na pravo mjesto.

- **Nedjelja, 24. veljače 2008, 20:51:** Sve objave prefiksa s izvorištem u AS-u 17557 koje su proslijeđene od strane PCCW Globala (AS 3491) imaju atribut AS Path uvećan za jedan dodatni broj AS-a 17557. To je bio nespretan pokušaj suzbijanja usmjeravanja prometa prema YouTubeovim prefiksima kroz AS 3491 prema AS-u 17557.

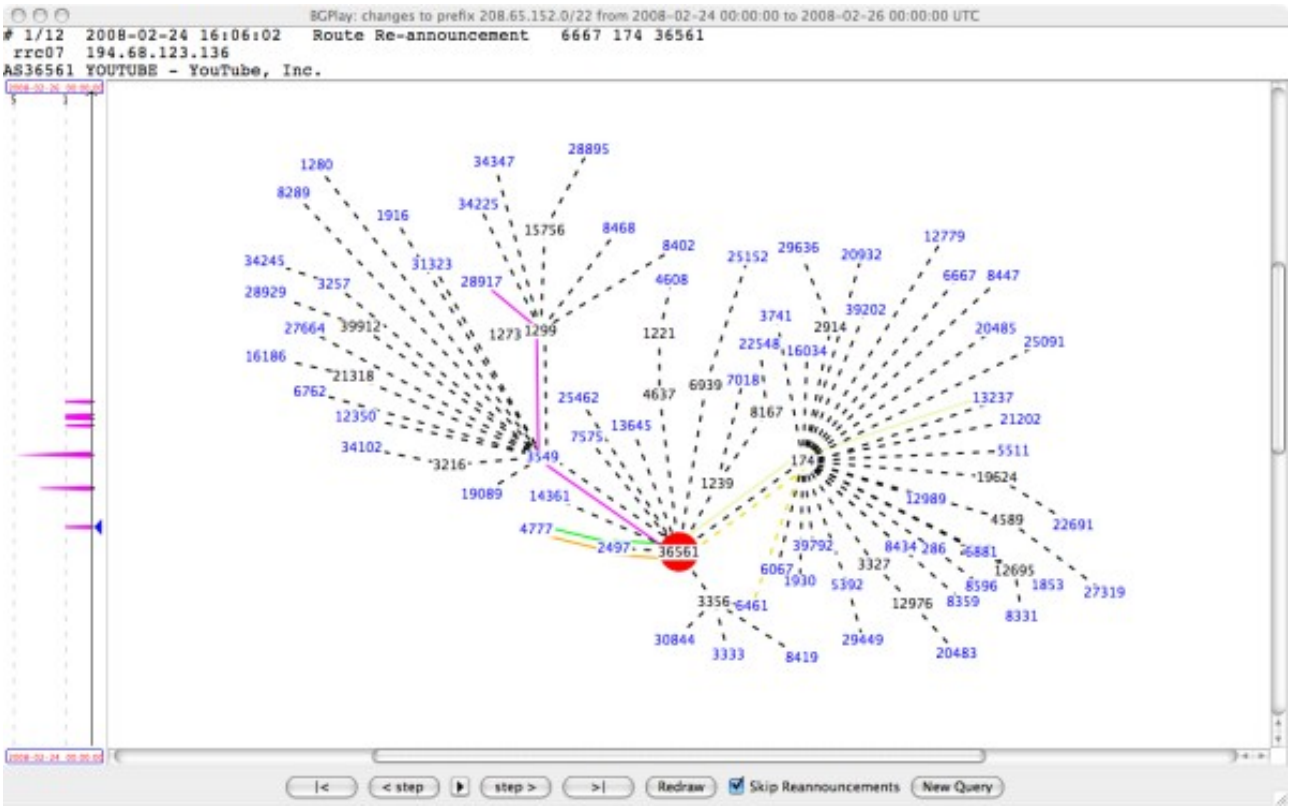
- **Nedjelja, 24. veljače 2008, 21:01:** PCCW Global (AS 3491) povlači sve prefikse s izvorištem u AS-u 17557 te na taj način konačno u potpunosti sprječava krađu prefiksa 208.65.153.0/24.

Što se zapravo dogodilo da je uzrokovalo globalni ispad servisa YouTube? U želji da spriječe pristup YouTubeu, pakistanski telekom objavio je specifičniji prefiks. Budući da svi usmjernici neovisno o tipu usmjeravanja (statičkim rutama ili dinamičkom usmjerničkom protokolu) ili o izabranom dinamičkom usmjerničkom protokolu uvijek preferiraju mrežu s duljom mrežnom maskom odnosno specifičniji prefiks, bez obzira na sve druge vrijednosti, atribute koji se vežu za taj prefiks pri objavljivanju BGP-om te činjenice koliko zapravo ta ruta za promatrani prefiks bila lošija od rute za njegov superprefiks, uvijek će biti izabran specifičniji prefiks ispred onog manje specifičnog. Prije samog incidenta na Internetu bio je objavljen samo prefiks 208.65.152.0/22. Za grafičko praćenje događaja možemo se poslužiti RIS-ovim alatom BGPlay koji grafički prikazuje smjer objava prefiksa. Za razdoblje koje je prethodilo samom incidentu, na Internetu je objavljen samo prefiks 208.65.152.0/22 kao što je prikazano na slici 6.1 gdje svi putevi prema navedenom prefiksu vode prema crveno označenom AS-u 36561, dok prefiks 208.65.153.0/24 nije nigdje objavljen kao što se vidi na slici 6.2 gdje se ne mogu uočiti putevi za taj prefiks.

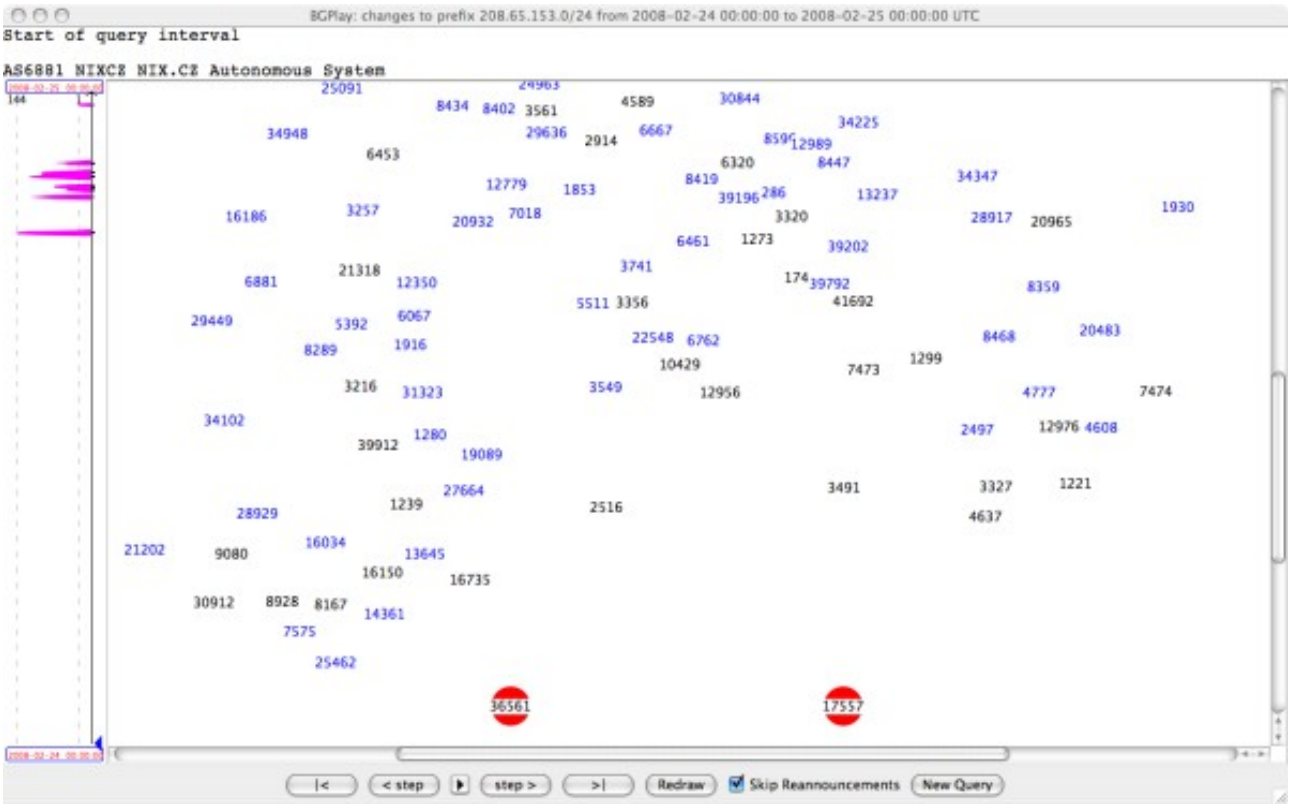
Pakistanski ISP je pogriješio što je dozvolio da prefiks 208.65.153.0/24 koji mu ne pripada bude objavljen na Internet. Ispravan način za sprječavanje pristupa nekim adresama svojim korisnicima bio bi filtriranje prometa ili neprosljeđivanje stvarnog prefiksa s Interneta u vlastiti autonomni sustav. Metoda kojom se poslužio pakistanski ISP iznimno je opasna i teško ju je suzbiti zbog pravila duljeg prefiksa koji preferira dulje prefikse ispred kraćih. U tom slučaju preostaju dva moguća rješenja:

- **Filtriranje objava:** kojim se sprječava propagacija objava za ukradene prefikse. AS3491 (PCCW Global) upravo je to naposljetku i napravio kako bi suzbio krađu prefiksa. No u početku AS3491 (PCCW Global) nije mogao znati da taj prefiks ne pripada pakistanskom ISP-u. Mogla se dogoditi legitimna situacija u kojoj je YouTube prebacio svoje poslužitelje u pakistanski AS (doduše malo vjerovatna situacija). Uostalom tranzitni AS (PCCW Global) ne mora znati koji AS na Internetu posjeduje koji prefiks. Takvu bi tablicu bilo teško održavati i pratiti te bi i sama bila u suprotnosti s dinamičkim ponašanjem Interneta.
- **Objava specifičnijeg prefiksa:** kojom se poslužio sam YouTube kako bi preusmjerio promet nazad u svoj AS. Takva metoda generira dosta upravljačkog prometa, opterećuje usmjernike na Internetu i povećava usmjerničke tablice. Naposljetku ne mora niti biti previše efikasna budući da drugi AS ponovno može objaviti još specifičniji prefiks.

Budući da je iznimno trivijalno ukrasti nečiji prefiks na Internetu i predstaviti ga kao svoj, nameće se pitanje kako spriječiti takve slučajeve ili ograničiti opseg istih. Jedna od mogućih metoda sprječavanja i ograničavanja krađe prefiksa ostvaruje se kroz reputacijski sustav. Kroz njega, promatranjem usmjerničkog prometa i ponašanja autonomnih sustava, vrednujemo njihovu vjerodostojnost. Na temelju numeričke vrijednosti vjerodostojnosti koja se naziva reputacija, možemo utjecati na odluke pri usmjeravanju. U slučaju krađe prefiksa to se prije svega odnosi na filtriranje objava koje nose ukradene prefikse. Međutim kako znati je li neki prefiks ukraden? U okviru ovog diplomskog rada napravljen je reputacijski sustav čija jedna komponenta upravo prati možebitne lažne objave prefiksa. Kreće se od osnovne premise da je većina prefiksa na Internetu fiksno vezana. Ta se fiksna veza ne odnosi na putove kojima prolazi objava prefiksa i kojima se usmjerava promet, već na stalnu pripadnost svakog prefiksa točno određenom autonomnom sustavu. Kao što znamo, autonomni sustavi dobivaju na korištenje IP adrese, odnosno prefikse od svog lokalnog registratora te se očekuje da se alocirane adrese pojedinom AS-u ne mijenjaju često. Također se očekuje od autonomnih sustava da cijelo ili većinu vremena objavljuju svoje prefikse uz što je moguće manje promjena ili povlačenja objava.




*Slika 6.1. Stanje usmjeravanja prije incidenta za prefiks 208.65.152.0/22*




*Slika 6.2. Stanje usmjeravanja prije incidenta za prefiks 208.65.153.0/24*

Na temelju algoritma opisanog ranije, izračunavamo reputaciju autonomnih sustava. Svaki autonomni sustav izračunava reputacije za sve ostale (ili većinu) autonomnih sustava te mu ta izračunata reputacija pomaže pri donošenju odluka. Na koji će način reputacija pomoći autonomnim sustavima nije implementirano u okviru ovog diplomskog rada. Pod objavama novih prefiksa ne misli se na potpuno nove prefikse, već na prefikse koje to tada nije objavljivao promatrani AS. Za potrebe presretanja i suzbijanja ukradenih prefiksa objave novih prefiksa od strane autonomnih sustava s lošijom reputacijom mogu se filtrirati na određeno vrijeme dok se ne utvrdi legitimnost objave tog prefiksa.
U svrhu testiranja promatran je upravljački promet između rubnih usmjernika u vrijeme prije i tijekom opisanog incidenta. Kao kolektor upravljačkog prometa poslužio je usmjernik-kolektor "Dixie" čiji su podaci spremljeni na stranici Oregonskog sveučilišta [3]. Tamo su spremljeni svi podaci koje usmjernik koristi i koje je dobivao od svojih susjeda u obliku takozvanih *dump* datoteka u kojima se bilježe logovi. Prvo je potrebno učitati datoteku s podacima iz RIB tablice usmjernika, a potom je potrebno redom parsirati datoteke u kojima su pohranjene sve UPDATE poruke kroz promatrano razdoblje. UPDATE poruke su grupirane također u *dump* datoteke po vremenskoj osnovi.

Snimanje prometa i izračun reputacije pokrenut je od trenutka 23. veljače 2008. u 23:22 (UTC). Promet se skupljao te se reputacija računala u prozorima - vremenskim intervalima od 4 sata. Budući da je ukupno trajanje promatranja bilo kratko, za očekivati je da će većina autonomnih sustava pokazati dobro ponašanje dok će samo nekolicina najlošijih imati niske vrijednosti reputacije. To su upravo oni autonomni sustavi koji su u promatranom razdoblju imali najviše nepostojanih prefiksa, prefiksa kojima su oni sami izvor. Ukoliko je autonomni sustav pakistankog ISP-a problematičan, trebao bi na temelju mjerenja pokazati lošu reputaciju. Ona se potom može iskoristiti za neprihvaćanje novih objava za nove prefikse koji imaju izvorište u pakistanskom AS-u što je moglo spriječiti preuzimanje YouTubeovog prefiksa.

U tablici 6.1 prikazani su izračuni reputacija za autonomni sustav 17557 (Pakistani Telecom) koji je uzrokovao ispad YouTubea. Prikazana je izračunata reputacija nakon svakog vremenskog intervala. Reputacije su prikazane u intervalu [0, 1) gdje su niže vrijednosti reputacija lošije. Početna je vrijednost reputacije za sve autonomne sustave 0. Velike promjene u reputaciji nisu posljedica velikih skokova već su jednostavno odraz konvergencije budući da je sam algoritam koncipiran tako da od početne vrijednosti reputacija konvergira za autonomne sustave koji ne rade probleme. Također se isto zbiva s reputacijama problematičnih sustava poput ovog promatranog. Zbog toga je bitnije promatrati relativan položaj reputacije promatranog autonomnog sustava u odnosu na ostale autonomne sustave. U stupcu "Poredak" dan je redni broj promatranog AS-a gdje niži redni broj označava lošije rangiran AS. U stupcu "Ukupno AS-ova" dan je ukupan broj autonomnih sustava koji su do tada uočeni i za koje se računa reputacija. Posljednji stupac prikazuje postotni poredak gdje se vidi relativan poredak promatranog autonomnog sustava u odnosu na sve uočene autonomne sustave. Vidimo da je pakistanski autonomni sustav 17557 pokazao dosta problematično ponašanje te da je konstantno unutar 2% najlošije rangiranih autonomnih sustava. U posljednjem retku mu je reputacija dodatno pala što je izravna posljedica incidenta s YouTubeom. Na temelju reputacije koja je za pakistanski AS iznimno loša, moglo se predvidjeti njegovo otimanje tuđeg prefiksa te se moglo filtrirati i odbaciti njegovu objavu ili je barem odgoditi na određeno vrijeme. Kada prefiksi nisu isti, kao što je upravo ovaj slučaj, obje objave bi došle do našeg autonomnog sustava budući da nose različite prefikse (doduše jedan je superprefiks drugoga). Kada bismo na temelju loše reputacije filtriranjem odbacili objavu pakistanskog AS-a, ostao bi nam samo ispravan prefiks YouTubea prema kojem bismo ispravno usmjeravali promet.

*Tablica 6.1. Reputacija autonomnog sustava 17557 počevši od 23:22*

| Prozor / 4h | Reputacija | Poredak | Ukupno AS-ova | Postotni poredak |
|---|---|---|---|---|
| 1 | 0.791615234456 | 174 | 27384 | 0,6354% |
| 2 | 0.957370380921 | 399 | 27396 | 1,4564% |
| 3 | 0.988032686234 | 450 | 27409 | 1,6418% |
| 4 | 0.995210784598 | 459 | 27413 | 1,6744% |
| 5 | 0.987974626982 | 295 | 27420 | 1,0759% |

## 6.2 Slučaj Indosata

U petak, 14. siječnja 2011., ISP INDOSAT-INP-AP (AS 4761) počeo je objavljivati veliki broj novih prefiksa [1]. Njihov autonomni sustav poslao je objave u kojima se prikazao kao izvorište za otprilike 2800 prefiksa koji su inače u vlasništvu 824 različita AS-a. Inače je Indosat izvorišni AS za stotinjak prefiksa. Neki od ovih prefiksa bili su vidljivi na manjem zemljopisnom području samo manjem broju susjednih sustava, dok su neki preuzeli velika područja raspršena preko cijelog svijeta. Neke od mreža na koje su utjecale ove pogrešne objave pripadaju Googleu, Amazonu, American Expressu, Ciscu, Ministarstvu obrane SAD-a i sl. Premda pogrešne objave, bilo one slučajne ili namjerne nisu trajale predugo, svega oko jedan sat, uzrokovale su mnogo problema u komunikaciji i odsjekli su neke od ovih mreža ili njihove dijelove od ostatka Interneta.

U svrhu testiranja reputacijskog sustava promatran je i sniman upravljački promet rubnih usmjernika prije, tijekom i poslije ovog incidenta. Isprobane su razne kombinacije s različitim parametrima snimanja i izračuna reputacije kako bi se utvrdilo koji bi parametri najbolje odgovarali ovom slučaju. To nam može pomoći u predviđanju budućih sličnih događaja ili barem u promptnom reagiranju ubuduće čim se primijete anomalije u usmjerničkom prometu. Za razliku od prethodnog primjera gdje je korištena metoda postojanosti veze između prefiksa i izvorišnog autonomnog sustava, ovdje je korištena metoda postojanosti veza između autonomnih sustava. Ovaj reputacijski mehanizam snima usmjernički servisni promet te iz njega bilježi sve promjene u putevima na razini veza između susjednih AS-ova. Veliki broj promijenjenih veza u kratkom vremenu signal je za nestabilnost koja može imati razne uzroke. No bez obzira na uzroke nestabilnosti, ona svakako nije dobra niti poželjna te će za ostatak Interneta biti najbolje uzrokujući autonomni sustav ili sustave zaobići ili odstraniti na neko vrijeme. U tome nam naravno može pomoći upravo reputacija izračunata na temelju snimljenoga prometa.

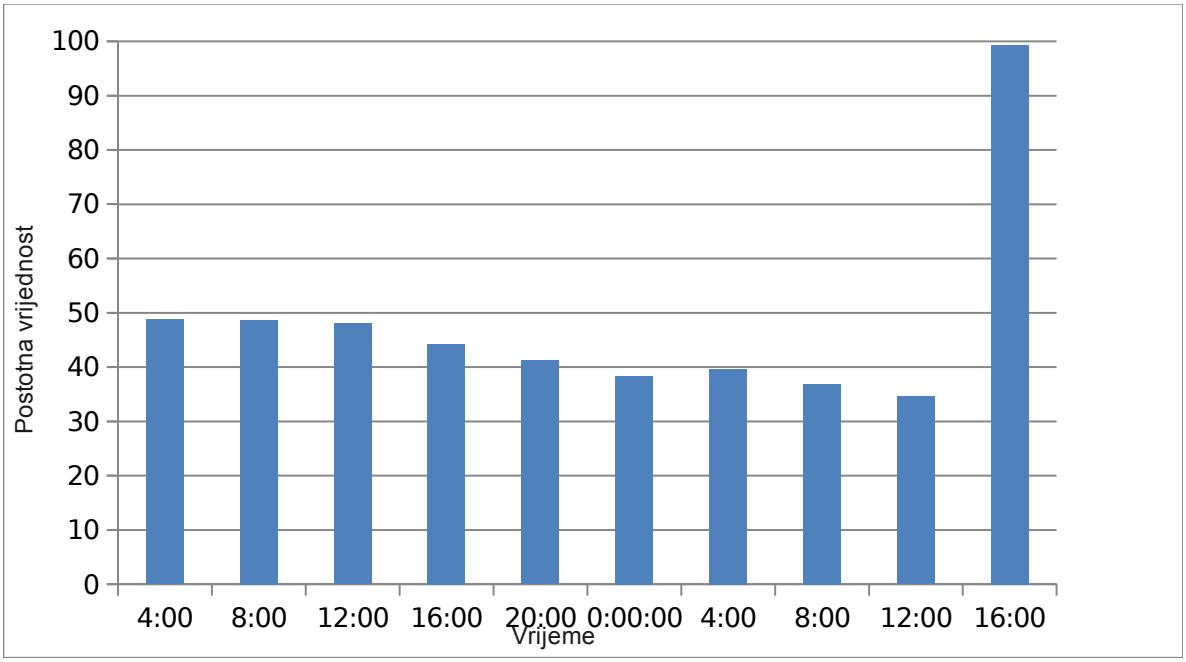
Same promjene u vezama i putovima normalna su pojava, naposljetku zbog njih i postoje dinamičko usmjeravanje i usmjernički protokoli. Međutim promatrajući Internet u globalu, nakon što se autonomnim sustavima dodijele prefiksi te se definiraju veze, samih bi naknadnih promjena

trebalo biti relativno malo. Premda Internet nije hijerarhijski organiziran niti je statičan, priroda dodjele prefiksa AS-ovima te veze između AS-ova i njihovih međusobnih dogovora usmjeravanja čine Internet relativno statičnom mrežom gdje promjene nisu poželjne i treba ih ograničiti na najmanju moguću mjeru. Upravo je to razlog što su ekcesni promet, česte promjene veza i općenito nestabilnost, u pravilu pokazatelj problema s pojedinim autonomnim sustavima, problema s njihovim politikama usmjeravanja, njihovim vezama s drugim autonomnim sustavima ili legitimnosti njihovih objava mreža koje im pripadaju.

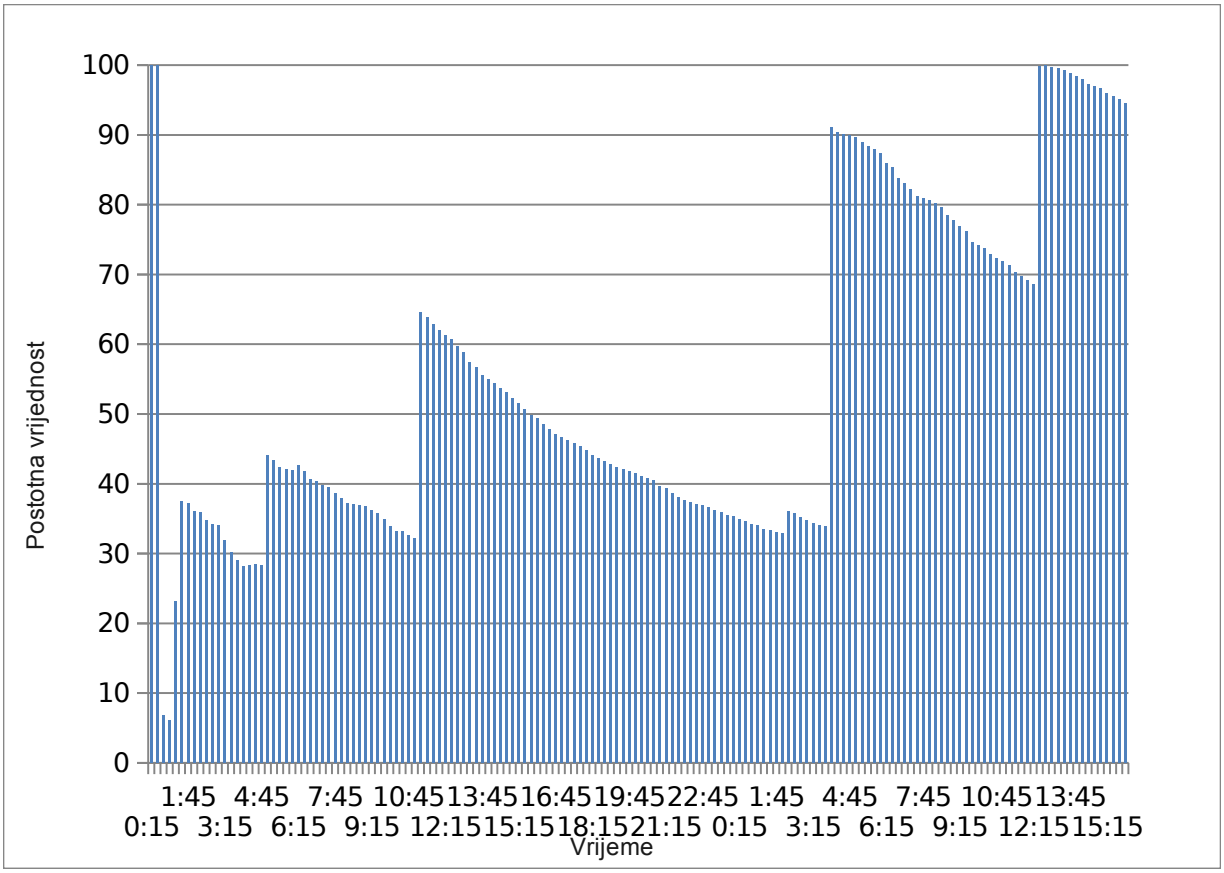
Budući da je početak incidenta zabilježen u petak, 14. siječnja 2011., u 12:19 (UTC), kao početak snimanja usmjerničkog prometa izabran je 13. siječanj u 0:00, dakle nešto više od 36 sati prije samog incidenta. Promet je sniman u prozorima trajanja 4 sata te uz faktor zaboravljanja $\gamma = 0,5$. Ovaj faktor znači da se po završetku svakog prozora točno polovica nove reputacije bazira na reputaciji promatranog prozora, dok se druga polovica uzima iz reputacije koja je prethodila početku promatranog prozora. Prilikom mjerenja postojanosti veza između AS-ova također je potrebno izvršiti normalizaciju dobivenih vrijednosti već u skladu s ukupnim brojem prefiksa čije objave prolaze kroz pojedini AS. U suprotnom, najlošije vrijednosti reputacija uvijek bi imali veliki tranzitni sustavi makar sami nisu odgovorni za nestabilnosti. Kako promjene putova na Internetu često nisu izoliran slučaj, prilikom velikog broja novih objava i njihove propagacije opterećuje se veliki broj usmjernika u također velikom broju autonomnih sustava. Premda faktor normalizacije smanjuje pogoršanje reputacije za udaljene autonomne sustave kojima promjene utječu samo na malu frakciju ukupnih ruta, svejedno će i njihova reputacija trpiti. Stoga je često umjesto apsolutne vrijednosti reputacije bolje promatrati njenu relativnu vrijednost, odnosno položaj autonomnog sustava na temelju njegove izračunate reputacije u odnosu na druge autonomne sustave. Ukupan je broj promatranih autonomnih sustava u ovom slučaju iznosio 5753. Tako se, pogotovo za predočavanje ljudskom oku, čini zgodno rangirati autonomne sustave na skali od 0 do 100. Time bi pozicija vrijednosti 75 značila da od ukupnog broja promatranih autonomnih sustava njih 75% ima bolju reputaciju od tog AS-a, dok 25% sustava ima lošiju reputaciju. Grafovi koji slijede prikazuju upravo relativnu reputaciju našeg malicioznog indijskog AS-a 4761 na skali od 0 do 100. Stvarna reputacija kreće od vrijednosti 0 koja je najbolja vrijednost pri ovoj metodi izračuna.

Promatrajući graf na slici 6.3 vidimo da se reputacija AS-a 4761 Indosata kreće u rasponu od 35-50%. Takve vrijednosti ne svrstavaju ga niti među ekstremno dobre, niti među ekstremno loše autonomne sustave. S velikom sigurnošću mogli bismo reći da je ovaj autonomni sustav nešto lošiji od prosjeka, no ne prelazi granice normale. Međutim u 12:19 drugog dana promatranja došlo je do početka incidenta. Objavljeni su mnogi tuđi prefiksi, dakle dogodila se klasična otimačina prefiksa od strane indijskog AS-a. To je uzrokovalo promjenu velikog broja putova čime su mnoge veze indijskog i okolnih sustava proglašene nestabilnima. Naravno, sam je indijski sustav, koji je prouzročio incident, dobio najveću kaznu. Već na kraju sljedećeg reputacijskog prozora postotna mu je reputacija narasla na 99,32% što ga je svrstalo u 1% najgorih AS-ova. Nažalost, taj je prozor završio u 16:00 što je dobrih 3,5 sati prekasno da nam informacije o promjeni reputacije mogu biti od pomoći pri filtriranju i odbacivanju lažnih objava.

Budući da mjerenja s prozorom duljine 4 sata nisu dala dobre rezultate, mjerenje je ponovljeno uz osjetno smanjenu veličinu prozora od 15 minuta. Rezultati prikazani grafom na slici 6.4 više su nego zanimljivi. Iz grafa je vidljivo da je AS 4761 u prethodnih 36 sati imao nekoliko ekscesa koji su mu osjetno pogoršali reputaciju u tim trenucima. Najveći takav eksces zbio se u prozoru koji je prethodio vremenu od 4:00, dakle nešto više od 8 sati prije velikog incidenta, kada mu je reputacija porasla i svrstala ga među 10% najlošije rangiranih autonomnih sustava.

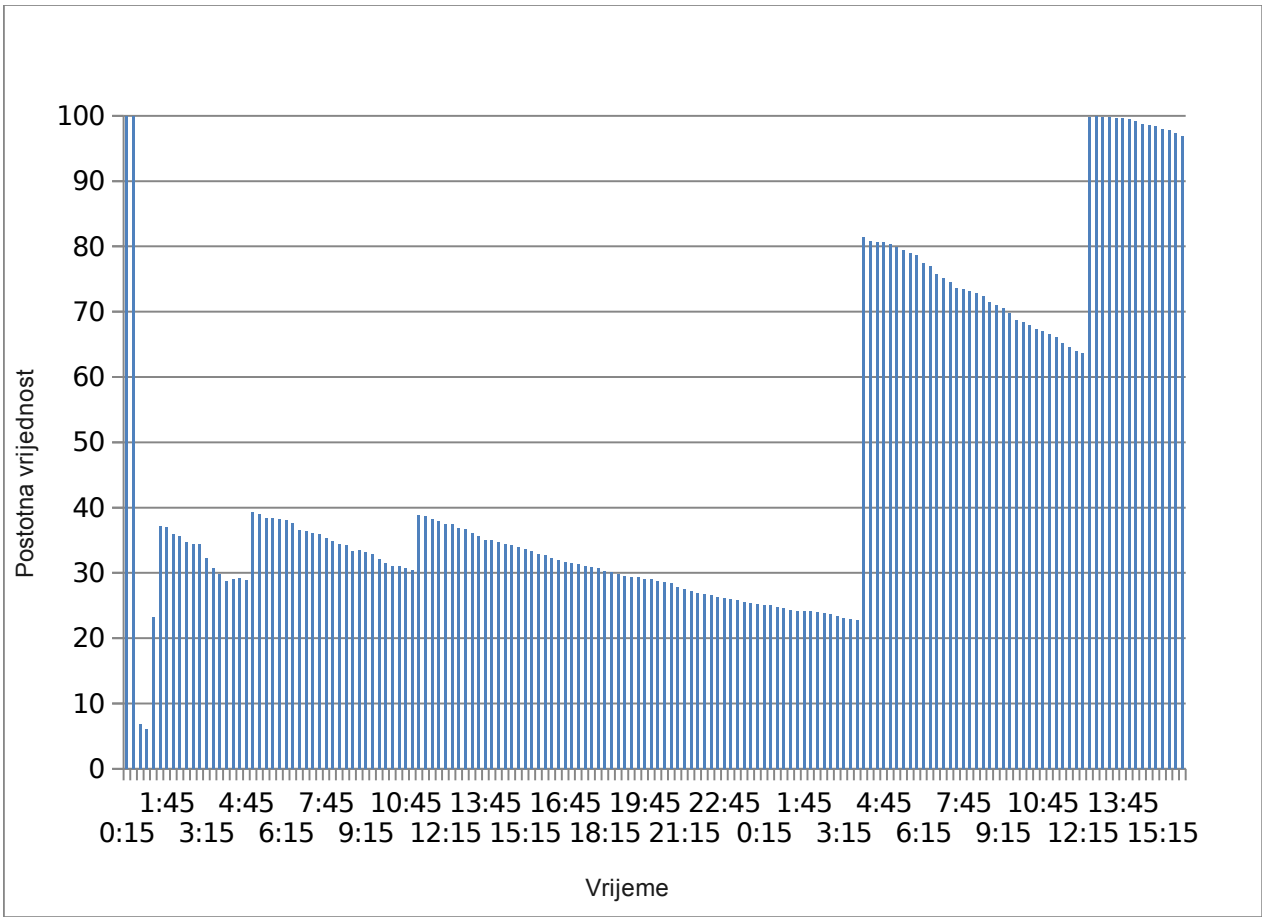



*Slika 6.3. Postotna vrijednost reputacije za prozore od 4 sata*



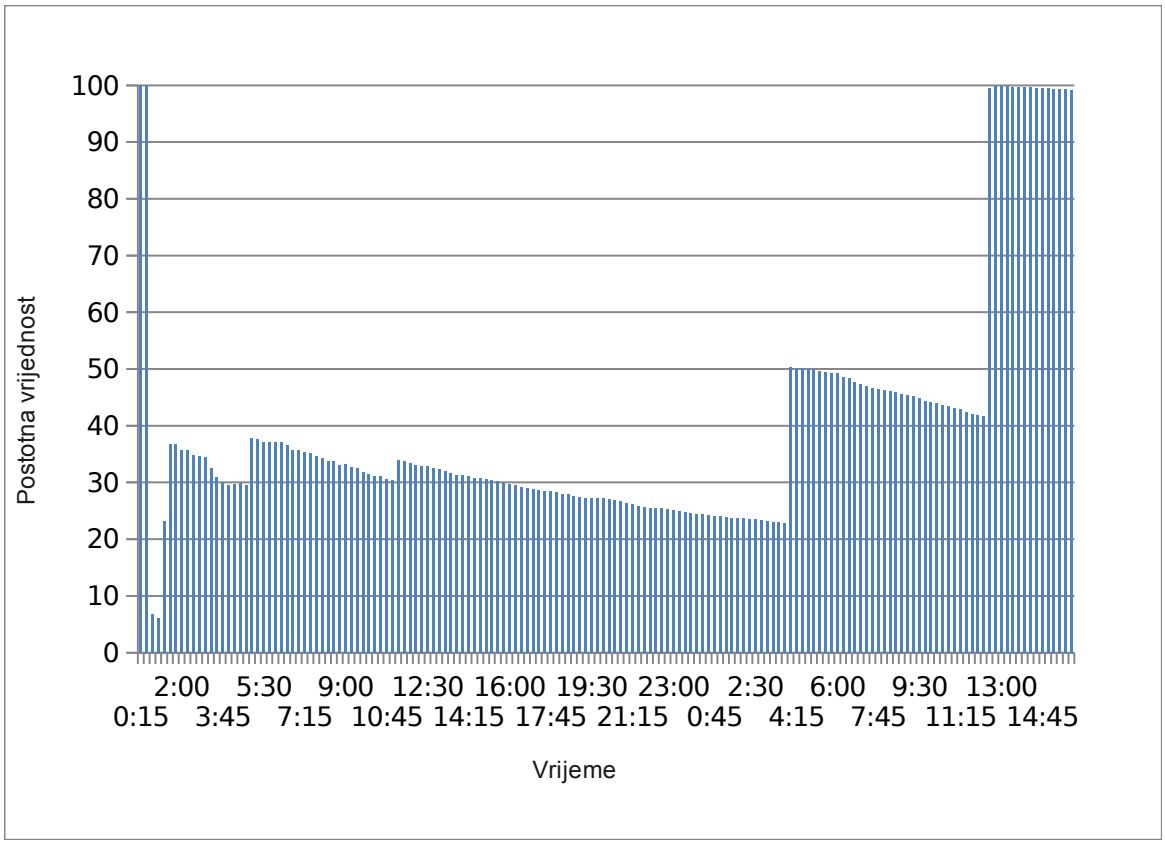

*Slika 6.4. Postotna vrijednost reputacije za prozore od 15 minuta i faktor zaboravljanja od 0,5*

Kod sljedećeg su mjerenja, prikazanog na slici 6.5, korišteni također prozori u trajanju od 15 minuta dok je faktor zaboravljanja smanjen na 0,25. Uz takvu vrijednost faktora zaboravljanja izračunata vrijednost reputacije svakog prozora sudjeluje samo sa 25% u izračunu ukupne reputacije, dok se 75% nasljeđuje od prije. Na taj način ćemo bolje razlučiti manje od većih ekscesa. I zaista, tri manja ekscesa koja su se dogodila prvoga dana mjerenja, puno su manje utjecala na porast reputacije nego pri prethodnom mjerenju. Međutim eksces koji se zbio u 4:00 drugoga dana, uistinu se pokazao kao veći eksces jer je reputacija tada osjetno skočila unatoč manjem faktoru zaboravljanja. Manji faktor zaboravljanja također smanjuje brzinu povratka reputacije na uobičajene vrijednosti.




*Slika 6.5. Postotna vrijednost reputacije za prozore od 15 minuta i faktor zaboravljanja od 0,25*

Pri posljednjem mjerenju korišteni su prozori vremenskog trajanja također 15 minuta kao i u prethodna dva slučaja, ali je ovaj puta vrijednost faktora zaboravljanja smanjena dodatno na svega 0,1. Stoga će svaki novi prozor u ukupnoj reputaciji utjecati sa svega 10%. Dobiveni graf prikazan je na slici 6.6. Odmah je vidljivo da je manji faktor zaboravljanja dodatno smanjio efekte svih ekscesa međutim napravio je vidljiviju podjelu između manjih i većih ekscesa. Tako su manji ekscesi neznatno utjecali na promjenu reputacije, dok je veći eksces koji se dogodio oko 4:00 sljedećeg dana svejedno jače utjecao na porast reputacije, a samim time i na rangiranje AS-a 4761 u odnosu na ostale promatrane AS-ove.




*Slika 6.6. Postotna vrijednost reputacije za prozore od 15 minuta i faktor zaboravljanja od 0,1*

Razmatrajući mjerenja može se zaključiti da je izračunata reputacija mogla biti od koristi pri filtriranju lažnih objava od strane AS-a 4761. U ovom slučaju dugački vremenski prozori mjerenja reputacije nemaju učinka jer je reputacija ovog autonomnog sustava uglavnom stalna kao što se vidi na slici 6.3. Međutim smanjivanje vremenskih prozora otkriva nam da je ovaj AS za razliku od većine drugih sklon povremenim ekscesima što nam daje za pretpostavku da je samo pitanje trenutka kada će ovi manji ekscesi prerasti u incident većih razmjera poput ovog što se zbio 14. siječnja 2011. Posebno je indikativno naglo povećanje reputacije svega 8 sati prije velikog incidenta koji je mogao poslužiti kao nagovještaj budućih događaja. Naravno da sama reputacija nije dovoljna jer ne možemo zabraniti primanje objava primjerice 20% najlošije rangiranih sustava. Ali možemo uzeti reputaciju u obzir kada primijetimo nagli porast objava od strane jednog autonomnog sustava. Umjesto uzimanja svih tih objava zdravo za gotovo, rubni se usmjernici mogu za pomoć obratiti reputacijskom poslužitelju zaduženom za izračun reputacija koji će na temelju reputacije i prethodnih ekscesa savjetovati usmjernik hoće li prihvatiti nagli veliki broj novih objava ili će ipak pričekati određeno vrijeme i filtrirati dobivene objave kako bi sačuvao ispravna usmjeravanja u slučaju greške ili krađe prefiksa ili pak u slučaju čestog pucanja nestabilnih veza. Čak i da na temelju prijašnje izračunate reputacije nije moguće donijeti takvu odluku, može se iskoristiti nova reputacija izračunata neposredno nakon početka incidenta. Koliko će se to brzo dogoditi, odnosno koliko će se brzo reputacija povećati nakon početka incidenta ovisi o faktoru, posebice faktoru zaboravljanja, o položaju incidenata unutar promatranog prozora, ali ponajviše o samoj duljini prozora. Pogledom na sva četiri prikazana grafa, uočavamo da je reputacija nesretnog sustava skočila do krajnjih vrijednosti poslije samog incidenta pri sva četiri mjerenja, neovisno o faktorima

i duljini samog prozora, što je samo po sebi i razumljivo. Uzimajući dulje vremenske prozore promatramo prevladavajući trend reputacije. Uzimajući pak kraće vremenske prozore, brže ćemo moći uočiti nagle promjene reputacije te primijetiti incidente dok su još u ranoj fazi. Uz početak incidenta u 12:19, već je nakon prvog prozora u kojem se zbio početak incidenta (prozor koji je počeo u 12:15, a završio u 12:30) bilo razvidno da je u pitanju zaista veliki problem. Iako je tih 11 minuta bilo dovoljno da se nanese dosta štete u obliku gubitka veze prema inkriminiranim prefiksima, opterećenja usmjernika i sl., automatizacijom usmjernika koji bi za savjet pitali središnji reputacijski server nastavak incidenta mogao je biti prekinut već tada. Potrebno je također naglasiti da primjena reputacijskog sustava na velikim tranzitnim autonomnim sustavima može dovesti do značajnih poboljšanja sigurnosti i konzistentnosti usmjeravanja na cijelom Internetu.

# 7. Zaključak

Današnji se Internet nalazi pod mnogim sigurnosnim prijetnjama. Jedna od njih svakako se odnosi na problem sigurnosti usmjeravanja protokolom rubnih usmjernika između autonomnih sustava na Internetu. Jedno od predloženih rješenja povećanja sigurnosti izrada je reputacijskog mehanizma koji bi vrednovao pojedine autonomne sustave te im davao određene reputacije. U sklopu ovog rada izrađen je reputacijski sustav kroz dva različita modela koji na temelju prometa rubnih usmjernika određuje reputacije autonomnih sustava. Izvršena su razna mjerenja te je njima pokazano da se mnogi problemi prilikom usmjeravanja na Internetu mogu izbjeći ili ublažiti uporabom ovakvog reputacijskog sustava. No zbog same prirode protokola rubnih usmjernika nije dovoljno da neki autonomni sustavi imaju razvijen mehanizam reputacije, već bi većina sustava, ili barem veliki tranzitni sustavi, trebali imati ovakav ili sličan reputacijski sustav temeljen na praćenju prometa rubnih usmjernika. Zajedno s drugim reputacijskim mehanizmima koji vrednuju autonomne sustave na osnovi drugih kriterija tako se može složiti kompleksan zajednički sustav koji bi mogao uvelike pridonijeti ovom aspektu sigurnosti Interneta.

# 8. Literatura


[1] BGP monitoring and analyses tool

URL: http://bgpmon.net/ (23/8/2011)

[2] BGP: the Border Gateway Protocol Advanced Internet Routing Resources

URL: http://www.bgp4.as/ (8/4/2011)

[3] Route Views Project Page

URL: http://www.routeviews.org/ (28/6/2011)

[4] RIPE Network Coordination Centre

URL: http://www.ripe.net/ (18/7/2011)

[5] BGP AS_PATH Attribute – Knowledge Base

URL: http://sites.google.com/site/amitsciscozone/home/bgp/bgp-as_path-attribute (18/5/2011)

[6] Jian Chang, Krishna K. Venkatasubramanian, Andrew G. West, Sampath Kannan, Boon Thau Loo, Oleg Sokolsky, and Insup Lee, *AS-TRUST: A Trust Quantication Scheme for Autonomous Systems in BGP*, Department of Computer and Information Science, University of Pennsylvania, 2011

URL: http://www.seas.upenn.edu/~vkris/papers/Tech-Report-MS-CIS-10-25.pdf

[7] Ratul Mahajan, David Wetherall, Tom Anderson, *Understanding BGP Misconfiguration*, Computer Science and Engineering, University of Washington, 2011

URL: http://djw.cs.washington.edu//papers/sigcomm2002-misconfigs.pdf

[8] Mattia Rossi, *MRT dump file manipulation toolkit (MDFMT) - version 0.2*, Centre for Advanced Internet Architectures, Swinburne University of Technology, Melbourne, 2009

URL: http://caia.swin.edu.au/reports/090730B/CAIA-TR-090730B.pdf

[9] DPKT v1.7, Python Packet

URL: http://code.google.com/p/dpkt/ (13/3/2011)

[10] Oberheide, J., jon.oberheide.org – pybgpdump, 2007

URL: http://jon.oberheide.org/pybgpdump/ (13/3/2011)

[11] BGP Reports

URL: http://bgp.potaroo.net/ (8/3/2011)

[12] *COS 561 Assignment #3: Internet Measurement*, 2011

URL: http://www.cs.princeton.edu/courses/archive/fall10/cos561/assignments/ps3.pdf

[13] Barry Greene, *The Bogon Reference – Team Cymru*

URL: http://www.team-cymru.org/Services/Bogons/ (15/8/2011)

[14] Centar informacijske sigurnosti, *BGP protokol*, 2011

URL: http://www.cis.hr/files/dokumenti/CIS-DOC-2011-03-006.pdf

[15] Wikipedia, *Tier 1 Network*

URL: http://en.wikipedia.org/wiki/Tier_1_network (23/8/2011)

[16] Hyun, Y., *Bogons*

URL: http://www.caida.org/~youngh/bogons.html (3/3/2004)

[17] McCullagh, D., *How Pakistan knocked YouTube offline*

URL: http://news.cnet.com/8301-10784_3-9878655-7.html (25/2/2008)

[18] Y. Rekhter, T. Li, S. Hares, *A Border Gateway Protocol 4 (BGP-4)*, The Internet Engineering Task Force (IETF), RFC 4271

URL: http://www.ietf.org/rfc/rfc4271 (11/8/2011)

[19] J. Hawkinson, BBN Planet, T. Bates, *Guidelines for creation, selection, and registration of an Autonomous System (AS)*, The Internet Engineering Task Force (IETF), RFC 1930

URL: http://www.ietf.org/rfc/rfc1930 (11/8/2011)

[20] Q. Vohra, Juniper Networks, E. Chen, Cisco Systems, *BGP Support for Four-octet AS Number Space*, The Internet Engineering Task Force (IETF), RFC 4893

URL: http://www.ietf.org/rfc/rfc4893 (11/8/2011)

[21] Y. Rekhter, Cisco Systems, B. Moskowitz, Chrysler Corp., D. Karrenberg, RIPE NCC, G. J. de Groot, RIPE NCC, E. Lear, Silicon Graphics, Inc., *Address Allocation for Private Internets*, The Internet Engineering Task Force (IETF), RFC 1918

URL: http://www.ietf.org/rfc/rfc1918 (11/8/2011)

[22] M. Cotton, L. Vegoda, ICANN, *Special Use IPv4 Addresses*, The Internet Engineering Task Force (IETF), RFC 5735

URL: http://tools.ietf.org/html/rfc5735 (11/8/2011)

[23] Python v2.7.2 documentation

URL: http://docs.python.org/index.html (14/6/2011)

[24] Malhotra, R., *IP Routing*, O'Reilly & Associates, Inc., Sebastopol, 2002