Centar Informacijske Sigurnosti

BGP protokol

CIS-DOC-2011-03-006

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Jedni od najvažnijih protokola u Internetu su protokoli za usmjeravanje paketa koji omogućuju dostavljanje paketa s jednog računala na drugo. Pri tome se pokušava pakete prenijeti optimalnim putom (optimalan je onaj put koji će najbrže dostaviti pakete na odredište uz minimalno kašnjenje, a najčešće je to upravo najkraći put). Svaki put se sastoji od niza usmjeritelja kroz koje paketi prolaze. Kako bi znao kojim putem treba usmjeriti pakete, svaki usmjeritelj održava svoju tablicu usmjeravanja na temelju koje donosi odluku o putu kojim će slati pojedine pakete. Tablice usmjeravanja se stalno moraju osvježavati jer često dolazi zbog promjena putova (npr. ispadanje pojedinih usmjeritelja, zagušenje mreže, dodavanje novih usmjeritelja itd.). Zbog toga usmjeritelji moraju komunicirati sa susjednim usmjeriteljima. Protokoli za usmjeravanje se razlikuju prema informacijama koje se nalaze u tablicama usmjeravanja, načinu dobivanja tih informacija i po algoritmu prema kojem donose odluku. Jasno je zašto je ispravan rad ovih protokola vrlo važan. Greške u radu mogu uzrokovati prestanak rada nekih servisa na Internetu te razne napade poput čitanja ili preusmjeravanja paketa.

Protokoli za usmjeravanje mogu se podijeliti u dvije glavne skupine s obzirom na područje djelovanja. To su IGP (eng. *Interior gateway protocol*) i EGP (eng. *Exterior Gateway Protocol*) protokoli usmjeravanja. Primjeri IGP protokola su RIP (eng. *Routing Information Protocol*) i OSPF (eng. *Open Shortest Path First*) protokol. Jedini EGP protokol koji se koristi u Internetu je upravo BGP (eng. Border Gateway *Protocol*) protokol i on je tema ovog dokumenta.

Na početku dokumenta je objašnjeno u kojim slučajevima se koristi BGP protokol i zašto je on jedan od najvažnijih protokola u Internetu. Zatim je opisano na koji način radi BGP protokol, kako donosi odluku o usmjeravanju, kako BGP usmjeritelji komuniciraju i koje su to poruke koje izmjenjuju. Opisani su i nedostaci BGP protokola te razlog zbog kojeg je BGP protokol ranjiv. Predstavljena su i neka rješenja kojima se mogu ublažiti neki nedostaci protokola. Na kraju su spomenute neke od implementacija, kao i budućnost BGP protokola.

2. Upotreba BGP protokola

BGP (eng. *Border Gateway Protocol*) protokol je jedan od najvažnijih protokola usmjeravanja, a koristi se za komunikaciju usmjeritelja između autonomnih sustava. Autonomni sustav (AS) je skup mreža i usmjeritelja koji imaju zajedničku politiku usmjeravanja prema drugim autonomnim sustavima, a obično su pod upravom ISP-a (eng. *Internet Service Provider*) ili veće organizacije. Važno je napomenuti da svaki AS dobiva svoj jedinstveni broj koji ga označava. Usmjeritelji u AS-u koriste neki od IGP (eng. *Interior gateway protocol*) protokola za usmjeravanje, dok rubni (vanjski) usmjeritelji, koji se koriste u komunikaciji s drugim AS-ovima, koriste EGP (eng. *Exterior Gateway Protocol*) protokol usmjeravanja (Slika 1).

Danas postoji samo jedan EGP protokol na Internetu i to je upravo BGP protokol. BGP inačice 4 koristi se u Internetu od 1994. godine. Ova inačica je uvela novosti poput podrške za CIDR[1] i združivanje putova kako bi se smanjile veličine tablica za usmjeravanje. U siječnju 2006. izdan je dokument RFC 4271 [1] kojim su ispravljene brojne greške i dvoznačnosti u prethodnoj definiciji BGP protokola (dokument RFC 1771).

BGP koristi algoritam vektora puta koji je sličan algoritmu vektora udaljenosti kojeg koriste IGP protokoli, ali uzima u obzir putove kao niz AS-ova na putu do odredišta. To znači da će se u pravilu dužina puta mjeriti po broju AS-ova koje paketi prolaze dok ne dođu do odredišnog AS-a (kod IGP protokola broje se usmjeritelji) Pri tome je odluku od odabranom putu moguće prilagoditi politici usmjeravanja pojedinog AS-a.

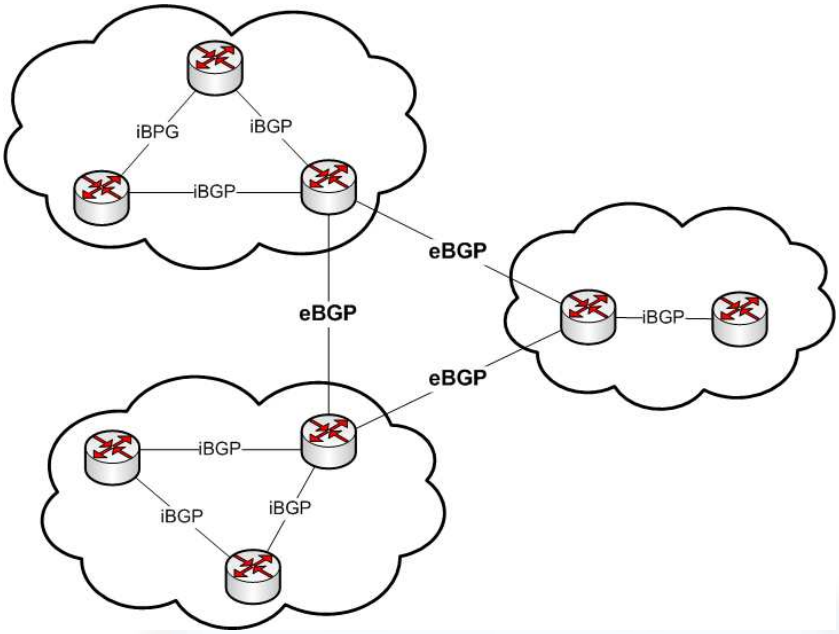
BGP može raditi kao:

- iBGP (eng. *Internal BGP*) – između usmjeritelja u istom AS-u ili
- eBGP (eng. *External BGP*) – između usmjeritelja u različitim AS-ovima.

Upotreba pojedinog načina rada je prikazana na slici u nastavku (Slika 1), koja pokazuje tri autonomna sustava i njihove BGP usmjeritelje. Rubni BGP usmjeritelji sa susjednim BGP usmjeriteljima u drugim AS-ovima rade u eBGP načinu rada, a s usmjeriteljima u istom AS-u komuniciraju u iBGP načinu rada. BGP usmjeritelji u AS-u se mogu koristiti kao rubni usmjeritelji za manje AS-ove koji su dio glavnog AS-a. Potrebno je napomenuti da iBGP nije isto što i IGP. Također, BGP protokol u iBGP načinu rada se u pravilu ne koristi umjesto nekog IGP protokola za usmjeravanje paketa.

Ova dva načina rada BGP protokola se razlikuju samo u pravilima za usmjeravanja, ali poruke koje se izmjenjuju su istog oblika, i bit će objašnjene u sljedećem poglavlju.

[1] CIDR (eng. *Classless Inter-Domain Routing*) – metoda koja omogućuje usmjeravanja paketa prema odredišnoj adresi na temelju mrežnog prefiksa (prvih nekoliko bitova IP adrese određuje mrežni prefiks). Ušteda se ostvaruje zbog toga što se nekoliko različitih IP adresa može objediniti s njihovim mrežnim prefiksom i pakete usmjeravati do usmjeritelja odredišne mreže. Dostavu paketa do odredišnog računala obavlja mrežni usmjeritelj.



Slika 1. Upotreba BGP protokola u autonomnim sustavima

3. Način rada BGP protokola

Kao transportni protokol OSI modela[2] BGP koristi TCP protokol koji podrazumijeva uspostavljanje TCP veze između usmjeritelja na priključnici (eng. *port*) 179. Dodavanje usmjeritelja s kojim će se komunicirati obavlja se ručno zbog čega nije potrebno definirati postupke otkrivanja susjeda koji se koriste u IGP protokolima. BGP usmjeritelj u svojem radu uspostavlja TCP veze sa svim svojim susjedima, te zatim razmjenjuje cijele tablice usmjeravanja u kojima se nalaze informacije o putovima (NLRI, eng. *Network Layer Reachability Information*) prema AS-u u kojem se nalazi odredišna mreža. U nastavku je prikazan isječak tablice usmjeravanja BGP usmjeritelja za jedno odredište.

```
BGP routing table entry for 129.6.0.0/16, version 8302807
Paths: (9 available, best #3)
  Advertised to non peer-group peers:
    64.62.142.154 64.71.128.254 128.223.60.102 128.223.60.103
    128.223.60.108 206.223.137.126 206.223.137.254 209.51.163.34
    216.66.3.10 216.218.185.238
  6453 UUNET/ALTERNET (701) 49
    63.243.149.105 from 63.243.149.105 (207.45.223.13)
      Origin IGP, metric 48, localpref 100, valid, external
      Community: 6939:2000
  6453 UUNET/ALTERNET (701) 49
    195.219.67.201 (metric 180) from 216.218.252.157 (216.218.252.157)
      Origin IGP, metric 60, localpref 100, valid, internal
      Community: 6939:2000
  WCG (7911) UUNET/ALTERNET (701) 49
    64.200.86.153 (metric 100) from 216.66.23.99 (216.66.23.99)
      Origin IGP, metric 47, localpref 100, valid, internal, best
      Community: 6939:2000 7911:999 7911:7307
```

Kao što je već spomenuto, BGP put se sastoji od niza autonomnih sustava koje treba proći do odredišta. Pri tome može postojati nekoliko putova s istim odredištem, a dopušta se i primjena različitih politika usmjeravanja, definiranih sa skupom parametara (atributa). Put kojim se usmjeravaju paketi prema nekom odredištu odabire se na temelju:

[2] OSI model (eng. *Open Systems Interconnection model*) definira podjelu komunikacijskog sustava na razine (http://en.wikipedia.org/wiki/OSI_model)

- parametara puta,
- dostupnosti puta,
- dodatnih pravila o prihvaćanju paketa,
- pravila o propuštanju paketa,
- ugovora između AS-ova i
- atributa (više u poglavlju 3.3).

Svaki usmjeritelj sadrži bazu putova RIB (eng. *BGP Routing Information Base*) na temelju koje određuje putove usmjeravanja pojedinih paketa. Baza RIB se sastoji od tri vrste popisa:

- ***Adj-RIBs-In***: popis neobrađenih putova koji su primljeni od susjednih usmjeritelja. Ovi putovi se uzimaju u obzir prilikom odabira puta. Za svakog susjeda postoji zasebni *Adj-RIBs-In* popis.
- ***Loc-RIB***: popis putova s lokalnim informacijama o usmjeravanju do kojih se dolazi primjenom vlastitih pravila usmjeravanja i provođenjem procesa odluke nad popisom neobrađenih ruta.
- ***Adj-RIBs-Out***: popis putova koji se šalju susjednim usmjeriteljima slanjem UPDATE poruka. Kao i kod *Adj-RIBs-In* popisa, zasebni *Adj-RIBs-Out* popis se čuva za svakog susjeda.

3.1. BGP poruke

BGP protokol koristi četiri vrste poruka u komunikaciji s drugim usmjeriteljima. To su:

- OPEN,
- UPDATE,
- KEEPALIVE i
- NOTIFICATION.

Sve poruke se šalju putem ostvarene TCP veze na priključnici 179 između dva usmjeritelja.

3.1.1. Poruka OPEN

Poruka OPEN je prva poruka koju usmjeritelji šalju nakon uspostavljanja TCP veze. Potvrdni odgovor na poruku OPEN je poruka KEEPALIVE kojom se potvrđuje da je primljena poruka OPEN. To znači da će nakon uspostavljana TCP veze oba usmjeritelja poslati po jednu OPEN i KEEPALIVE poruku. Porukom OPEN se usmjeritelji predstavljaju i pregovaraju o parametrima sjednice. U poruci se šalju sljedeći parametri:

- *version* – informacija o inačici protokola BGP (trenutno je aktualna inačica 4).
- *my autonomous system* – broj AS-a u kojem se nalazi pošiljatelj poruke.
- *hold time* – vremenski nadzor koji definira vrijeme čekanja. Predstavlja najveći broj sekundi koji može proći između prijama dvaju uzastopnih poruka KEEPALIVE ili UPDATE od pošiljatelja. Kada vrijeme istekne, sjednica se prekida (brojač se ponovo pokreće kada dođe poruka KEEPALIVE ili UPDATE).
- *BGP identifier* – identifikator usmjeritelja (najčešće IP adresa usmjeritelja koji je poslao poruku).
- *Optional parameters length* – veličina polja *optional parameters* .
- *Optional parameters* – popis izbornih parametara.

3.1.2. Poruka UPDATE

Poruka UPDATE služi za razmjenjivanje informacija o putevima (NLRI). Usmjeritelj s porukom UPDATE šalje usmjeriteljima s kojima ima uspostavljenu TCP vezu putove iz *Ajd-RIBs-Out* popisa. Ovom porukom je moguće objaviti nove putove i odjaviti stare putove koji više nisu aktivni. Polja UPDATE poruke su sljedeća:

- *Withdrawn routes length* – duljina polja *withdrawn routes*. Ukoliko je vrijednost polja 0, polje *withdrawn routes* ne postoji u poruci.
- *Withdrawn routes* – polje promjenjive duljine koja je definirana u polju *withdrawn routes length*. Sadrži popis prefiksa IP adresa za putove koji više nisu valjani.
- *Total path attribute length* – duljina polja *path attributes.*
- *Path attributes* – popis atributa koji se ažuriraju za određene putove. Atributi se zapisuju kao trojka: vrsta atributa, duljina atributa i vrijednost atributa.
- *Network layer reachability information* – popis putova koji se najavljuju za ažuriranje. Na njih se odnose navedeni atributi puta.

U poruci UPDATE se istovremeno može objaviti samo jedna vrsta atributa, ali je zato taj atribut moguće objaviti za više odredišta (pod uvjetom da sva odredišta koriste taj atribut).

3.1.3. Poruka KEEPALIVE

Poruka KEEPALIVE se koristi za održavanje sjednice. Usmjeritelji razmjenjuju KEEPALIVE poruke onoliko često koliko je potrebo kako ne bi isteklo vrijeme definirano u *hold time* polju poruke OPEN koja se slala na početku uspostavljanja sjednice, najčešće 1/3 vremena definiranog u polju *hold time*.

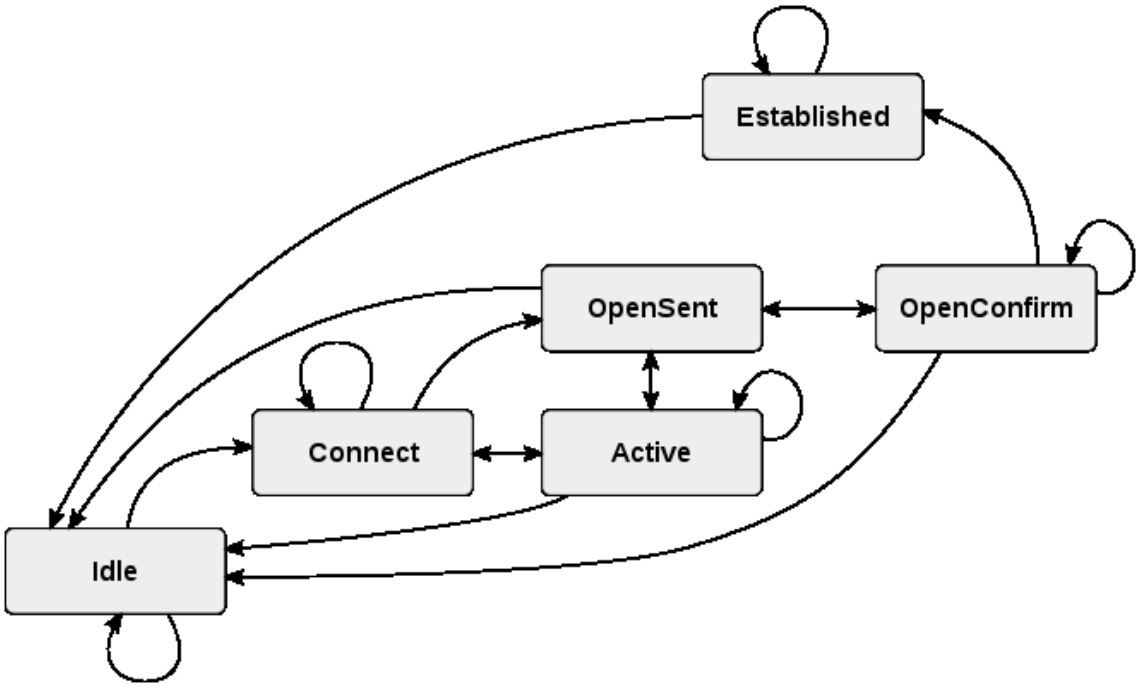
3.1.4. Poruka NOTIFICATION

Poruka NOTIFICATION se koristi kada je utvrđena neka greška. Nakon primitka ove poruke, BGP veza se odmah prekida. Neke od pogrešaka su: istek vremenskog nadzora (definiranog u *hold time* polju), primitak nepoznatog atributa, primitak pogrešnog AS broja itd.

3.2. Konačni automat

Rad BGP usmjeritelja se opisuje konačnim automatom sa šest stanja: *Idle*, *Connect*, *Active*, *OpenSent*, *OpenConfirm* i *Established* (Slika 2). Za svaku ostvarenu vezu s nekim drugim BGP usmjeriteljem stvara se poseban automat stanja i bilježi se stanje u kojem se usmjeritelj nalazi za tu vezu. Stanja konačnog automata i događaji koji uzrokuju promjenu stanja su detaljno objašnjeni u dokumentu RFC 4271 [1].

Početno stanje BGP usmjeritelja je stanje *Idle*. U tom stanju usmjeritelj odbija sve dolazne BGP veze. Kao odgovor na događaje *ManualStart* i *AutomaticStart*, sustav inicijalizira sve BGP resurse, pokreće se brojač *ConnectRetry*, pokušava se uspostaviti TCP veza sa susjednim usmjeriteljem i prelazi u stanje *Connect*. U slučaju greške (zatvorena priključnica 179, kriva konfiguracija adrese usmjeritelja ili broja AS-a), TCP veza se ne uspostavlja i usmjeritelj se zadržava u stanju *Idle* određeni period vremena.



Slika 2. Konačni automat BGP protokola
Izvor: Wikipedia

Sljedeće stanje je *Connect*, u kojem usmjeritelj čeka na uspostavu TCP veze. Ukoliko je veza uspješno uspostavljena, šalje se poruka OPEN i prelazi se u sljedeće stanje - *OpenSent*. U suprotnom, prelazi se u stanje *Active*.

Usmjeritelj se može naći u stanju *Active* ukoliko nije uspio uspostaviti TCP vezu zbog grešaka poput: zatvorena priključnica 179, kriva adresa ili AS broj na nekom od usmjeritelja. U ovom stanju, usmjeritelj još jednom pokušava uspostaviti TCP vezu s drugim usmjeriteljem. Ako uspije, šalje poruku OPEN i prelazi u stanje *OpenState*. Ako i drugi puta ne uspije uspostaviti TCP vezu, prelazi u početno stanje *Idle*. Ovdje može doći do situacije u kojoj usmjeritelj stalno prelazi iz stanja *Active* u stanje *Idle* zbog pogreška s priključnicom, pogrešne konfiguracije BGP usmjeritelja, zagušenja mreže itd. Iz stanja *Active* moguće je prijeći u stanje *Connect* ukoliko istekne vrijeme brojača *ConnectRetry*, nakon čega usmjeritelj odustaje od uspostave ove TCP veze i pokreće uspostavu TCP veze s nekim drugim usmjeriteljem.

U stanju *OpenState* usmjeritelj čeka poruku OPEN od drugog usmjeritelja s kojim je uspostavio vezu. Nakon primitka poruke OPEN, provjerava se njena valjanost. Ako se otkrije greška u poruci, usmjeritelj šalje poruku NOTIFICATION i prelazi u stanje *Idle* čime se raskida TCP veza. Ukoliko nije otkrivena nikakva greška, usmjeritelj šalje poruku KEEPALIVE kao potvrdni odgovor na primljenu OPEN poruku, postavlja brojač *hold timer* i prelazi u stanje *OpenConfirm*.

U stanju *OpenConfirm* usmjeritelj čeka poruke KEEPALIVE od drugog usmjeritelja kojom se potvrđuje ispravan primitak usmjeriteljeve poruke OPEN. Ukoliko drugi usmjeritelj umjesto KEEPALIVE pošalje poruku NOTFICATION znači da je došlo do greške pa usmjeritelj zatvara vezu i prelazi u stanje *Idle*. U početno stanje može prijeći i ako istekne vrijeme definirano u *hold timeru*. U tom slučaju usmjeritelj šalje drugom usmjeritelju poruku NOTIFICATION, zatvara vezu i prelazi u stanje *Idle*. Ako sve prođe u redu i usmjeritelj zaista dobije KEEPALIVE poruku od drugog usmjeritelja u vremenu definiranom s *hold time*, usmjeritelj prelazi u stanje *Established*.

Tek u stanju *Established* usmjeritelji mogu slati poruke UPDATE i izmjenjivati svoje tablice usmjeravanja. Iz ovog stanja moguće je prijeći samo u stanje *Idle* i to ukoliko usmjeritelj otkrije pogrešku, dobije poruku NOTIFICATION ili ne dobije poruke UPDATE ili KEEPALIVE u razdoblju definiranom s poljem *hold time* (tj. istekne brojač *hold timer*).

3.3. Atributi puta

U uvodu ovog poglavlja spomenuto je kako BGP usmjeritelj odluku od putu kojim će usmjeravati pakete prema odredišnom AS-u donosi na temelju atributa. Atributi se nalaze u poruci UPDATE i omogućavaju usmjeriteljima primjenu vlastite politike usmjeravanja. Dijele se u četiri skupine:

- dobro poznati obavezni (eng. *Well-known mandatory*),
- dobro poznati neobavezni (eng. *Well-known discretionary*),
- izborni tranzitni (eng. *Optional transitive*) i
- izborni lokalni (eng. *Optional non-transitive*) atributi.

Usmjeritelj koji implementira BGP protokol mora moći prepoznati sve dobro poznate (obavezne i neobavezne) atribute. Dobro poznati obavezni atributi se moraju nalaziti u svakoj UPDATE poruci koja sadrži NLRI. Dodatno, kada BGP usmjeritelj dobije nove informacije o dobro poznatim obaveznim atributima, te informacije mora proslijediti svim usmjeriteljima s kojima ima ostvarenu vezu.

Svi izborni atributi ne moraju biti podržani u implementaciji, ali se mora voditi računa da se izborni tranzitni atributi prenesu dalje (čak i ako nisu prepoznati, jer se odnose na sve AS-ove i svi AS-ovi bi ih trebali dobiti, neovisno o tome mogu li ih oni prepoznati ili ne), a neprepoznati izborni lokalni atributi se moraju ignorirati i ne prenositi dalje (jer se odnose samo na lokalni AS i drugi AS-ovi ne bi trebali dobiti taj atribut). U oba slučaja, poruka s putem koji sadrži izborni atribut mora se prihvatiti (i u slučajevima neprepoznavanja atributa) jer put i dalje sadrži dobro poznate atribute.

Atributi koji se koriste u BGP protokolu su:

- ORIGIN,
- AS_PATH,
- NEXT_HOP,
- MULTI_EXIT_DISC ,
- LOCAL_PREF,
- ATOMIC_AGGREGATE i
- AGGREGATOR.

3.3.1. ORIGIN

Atribut ORIGIN je dobro poznati obavezni atribut i definira porijeklo puta. Generira ga usmjeritelj od kojeg put potječe. Njegovu vrijednost ne bi smjeli mijenjati drugi usmjeritelji. Dodatno, sadrži polje kojim se usmjeritelja obavještava nalazi li se izvorišni usmjeritelj u istom AS-u kao i usmjeritelj koji je dobio ovaj atribut u UPDATE poruci.

3.3.2. AS_PATH

Atribut AS_PATH je još jedan dobro poznati obavezni atribut puta koji definira put kao listu AS-ova (segmenata puta) koje treba proći do odredišta. Svaki odsječak puta AS-a je zapisan trojkom:

- tip (skup AS-ova koje je poruka UPDATE prošla),
- duljina (broj prijeđenih AS-ova) i
- vrijednost (brojevi AS-ova).

Kada usmjeritelj dobije informaciju o putu s ovim atributom, prije prosljeđivanja informacije svojim susjedima mora izmijeniti vrijednost atributa ovisno o tome gdje se nalazi (susjed je u istom ili različitom AS-u) i koji usmjeritelj je izvorni za taj put.

Ovaj atribut je koristan kod višestrukih putova, za izbjegavanje petlji, zabranu usmjeravanja paketa kroz određeni AS i preferiranje određenog puta.

3.3.3. NEXT_HOP

Atribut NEXT_HOP je zadnji dobro poznati obavezni atribut puta, a definira IP adresu usmjeritelja na koji prvo treba usmjeriti paket kako bi se došlo do odredišta. Uobičajeno se

za vrijednost atributa uzima adresa usmjeritelja koji se nalazi na početku najkraćeg puta prema nekom odredištu. U implementaciji je potrebno postaviti ograničenje kojim usmjeritelj ne može sebe postaviti kao NEXT_HOP u nekom putu. Vrijednost atributa se smije (i mora) promijeniti samo ako je sljedeći usmjeritelj u drugom AS-u.

3.3.4. MULTI_EXIT_DISC

Atribut MULTI_EXIT_DISC (ili MED) je izborni lokalni atribut koji služi za odabir jednog od više ponuđenih putova prema istom AS-u. Na taj način usmjeritelj daje savjete svojim susjedima kojim putem poslati pakete prema njemu. Na ovaj način se provodi politika usmjeravanja dolaznog prometa pojedinog AS-a. Pri donošenju odluke o odabiru puta, kada prema AS-u postoji više mogućih putova i odluka se ne može donijeti na temelju ostalih atributa, odabire se onaj put koji ima najmanju vrijednost atributa MED.

3.3.5. LOCAL_PREF

Atribut LOCAL_PREF je dobro poznati neobavezni atribut puta koji određuje politiku usmjeravanja odlaznog prometa. Atribut se izmjenjuje samo između usmjeritelja istog AS-a (odatle i ime „*local*“), a ako greškom dođe do usmjeritelja izvan AS-a, potrebno ga je ignorirati. Atribut se koristi kada postoji više izlaznih putova iz AS-a, a odabire se onaj put koji ima veću vrijednost atributa LOCAL_PREF.

3.3.6. ATOMIC_AGGREGATE

Atribut ATOMIC_AGGREGATE je još jedan dobro poznati neobavezni atribut puta koji omogućuje združivanje putova prema odredištu. Združivanje putova je omogućilo smanjivanje broja putova jer se više putova združuje i objavljuje kao jedan u UPDATE poruci. Vrijednost koja se nalazi u atributu ATOMIC_AGGREGATE je najčešće polje „tip“ iz atributa AS_PATH i sastoji se od liste AS-ova od kojih je napravljen združeni put. Treba imati na umu da se mogu združivati samo oni putevi koji imaju iste atribute.

3.3.7. AGGREGATOR

Atribut AGGREGATOR je izborni tranzitni atribut i vezan je uz prethodno opisani atribut kojim se ostvaruje združivanje putova. Ovim atributom se daje do znanja da je usmjeritelj združio rutu. Dodatno, usmjeritelj zapisuje svoj AS broj i IP adresu.

3.4. Algoritam usmjeravanja

U BGP protokolu ne postoji točno određen način na koji se donosi odluka o odabiru puta, nego to ovisi o politici usmjeravanja pojedinog AS-a koja se nalazi u PIB-u (eng. *Policy Information Base*). U algoritmu se odlučuje o najboljem putu za neko odredište na temelju procesa odluke (eng. *decision process*).

Neki od prije navedenih atributa se uopće ne moraju koristiti pri donošenju odluke. Ipak, postoje neka osnovna pravila i navedena su u nastavku.

- Put za koji nije poznat usmjeritelj u NEXT_HOP (nije poznat put kojem je odredište usmjeritelj naveden u NEXT_HOP) se ne uzima u obzir.
- Gleda se najveća težina (vrijednost koja se postavlja u pojedinom usmjeritelju, nije povezana uz atribute BGP protokola).
- Najveća vrijednost LOCAL_PREF.
- Najkraći AS_PATH.
- Najmanji ORIGIN.
- Najmanji MED.
- Preferiranje eBGP puta naspram iBGP puta.
- Najmanja metrika do NEXT_HOP usmjeritelja .

Primjer jednog od mogućih algoritama usmjeravanja je sljedeći:

1. Prvo se provjerava dohvatljivost usmjeritelja navedenog u atributu NEXT_HOP.
    a. Ako je on dohvatljiv, provjerava se nalazi li se on u istom AS-u.
        i. Ako je i to točno, gleda se atribut LOCAL_PREF.
2. Ukoliko ima više putova za isto odredište, traži se onaj s najvećom vrijednosti u LOCAL_PREF.
    a. Ako su sve vrijednosti jednake, potrebno je gledati druge atribute. U tom slučaju, najčešće se gledaju atributi AS_PATH, ORIGIN i MED, tim redoslijedom.
        i. Prvo se traži put s najkraćim AS_PATH atributom,
        ii. zatim put s manjom vrijednosti u atributu ORIGIN, te na kraju, ako se ne može donijeti odluka na temelju prethodna dva,
        iii. gleda se put s najmanjim atributom MED.

Na temelju informacija koje dobije od susjednih usmjeritelja (spremljenih u popisu Adj-RIBs-In) i vlastitih saznanja (u popisu Loc-RIB), koristeći neki od algoritama usmjeravanja, BGP usmjeritelj za svako odredište odredi **jedan najbolji put** kojeg koristi za usmjeravanje.

4. Nedostaci BGP protokola

BGP protokol ima nekoliko nedostataka koji se uglavnom javljaju zbog velikog broja čvorova (usmjeritelja, odredišnih poslužitelja, AS-ova itd.) u današnjem Internetu. Ovi nedostaci nisu bili jako izraženi u vremenu kada se BGP protokol razvijao upravo iz razloga što Internet nije bilo tako velik kao danas. S povećanjem Interneta prijašnji manji nedostaci su počeli sve više smetati i bilo je potrebno smisliti način kako ih ukloniti ili barem ublažiti.

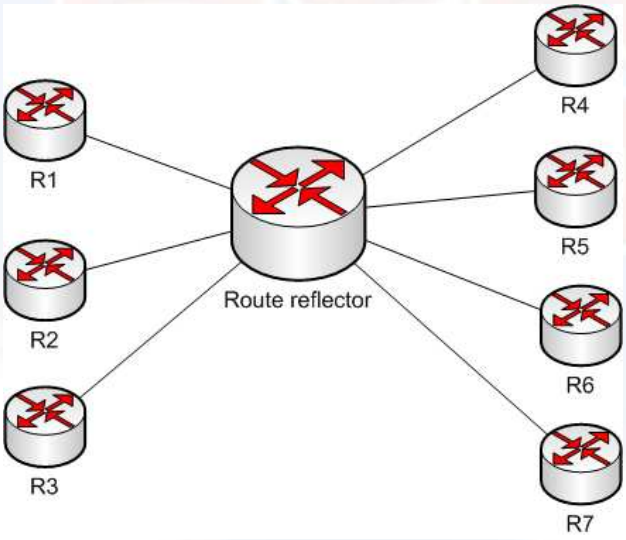
4.1. Potpuna povezanost BGP usmjeritelja

Jedan od najvećih nedostataka BGP protokola je zahtjev da svi usmjeritelji u AS-u međusobno moraju biti povezani izravno kako bi se izbjegle petlje (eng. *loop prevention*). Ovo nije toliki problem u manjim mrežama, ali kod velikih AS-ova, može doći do smanjenja performansi zbog velikog broja poruka koje usmjeritelji izmjenjuju.

Ovaj problem se rješava s dvije metode koje se međusobno ne isključuju nego se mogu koristiti zajedno:

- **reflektori putova** (eng. *route reflectors*) i
- **konfederacije** (eng. *confederations*).

Prva metoda (detaljno opisana dokumentom RFC 4456 [3]) koristi jedan usmjeritelj (ili dva zbog redundancije) kao reflektor puta kako bi se smanjio broj veza između usmjeritelja u AS-u (Slika 3). Reflektor puta je u vezi s nekoliko BGP usmjeritelja (na primjer usmjeritelji R4-R7) koji mu šalju svoje tablice. Zbog toga se ostali BGP usmjeritelji (usmjeritelji R1-R3 na slici) ne moraju povezivati s njima, nego je dovoljno povezati se s reflektorom kako bi dobili sve informacije koje imaju usmjeritelji „s druge strane“ (oni s kojima nisu izravno povezani).



Slika 3. Reflektor puta

Drugi način kojim se rješava prije opisani problem su konfederacije. Ovom metodom se veliki AS dijeli u nekoliko manjih AS-ova koje je lakše nadgledati. Manji AS-ovi se prema drugim AS-ovima predstavljaju kao matični AS kojem pripadaju.

Iako ove metode smanjuju problem koji može nastati zbog zahtjeva za izravnom povezanošću svih usmjeritelja, njihovom upotrebom nastaju novi problemi, a to su:

- oscilacije putova,
- neoptimalno usmjeravanje i
- sporija konvergencija.

4.2. Route flapping

Još jedan nedostatak BGP protokola je velika osjetljivost na greške u usmjeritelju zbog koje on često prelazi između aktivnog i neaktivnog stanja (eng. *route flapping*). Ova pojava može biti rezultat pogrešno konfiguriranog usmjeritelja ili namjernog napada (napadač bi na neki način izvodio učestale DoS[3] napade, a posljedice napada bi se propagirale kroz mrežu i uzrokovale *route flapping*). U svakom slučaju, putevi koji koriste taj usmjeritelj naizmjence se izuzimaju iz tablice usmjeravanja i ponovo dodaju u kratkim razmacima (20-50 puta u sekundi). Zbog toga što BGP usmjeritelj mora svaku promjenu puta odmah dojaviti svojim susjedima, dolazi do velikog broja UPDATE poruka koje usmjeritelji izmjenjuju. Ovo zagušuje cijelu mrežu nepotrebnim porukama koje su rezultat kvara samo jednog usmjeritelja. Još je veći problem ako je mreža konfigurirana tako da se pri izmjeni UPDATE poruka između usmjeritelja ne izmjenjuju podatkovni paketi.

Utjecaj *route flappinga* se smanjuje metodom opisanom u dokumentu RFC 2439 [4], a ona se naziva *route flap damping*. Ideja metode je unošenje vremenske zadrške kod opetovane promjene dostupnosti, odnosno nedostupnosti nekog puta. Prvih nekoliko puta (po preporuci četiri puta) kada se neki put izuzme i ponovo doda u tablicu usmjeravanja, poruke se obrađuju kao i inače. Nakon toga, kada se dogodi isti slučaj (ispadanje puta, a zatim ubrzo ponovo dodavanje) s ponovim dodavanjem puta u tablicu usmjeravanja se pričeka određeni period vremena. Sljedeći puta će se taj period još malo povećati i tako dalje. Parametri kojima se određuje period čekanja ovise o mreži u kojoj se nalazi BGP usmjeritelj (broj susjednih usmjeritelja, vjerojatnosti da će se u susjednim usmjeriteljima dogoditi *route flapping* i sl.). U RFC dokumentu 2439 [4] preporuča se maksimalni period čekanja od jednog sata. Očigledno, nedostatak metode je spora konvergencija.

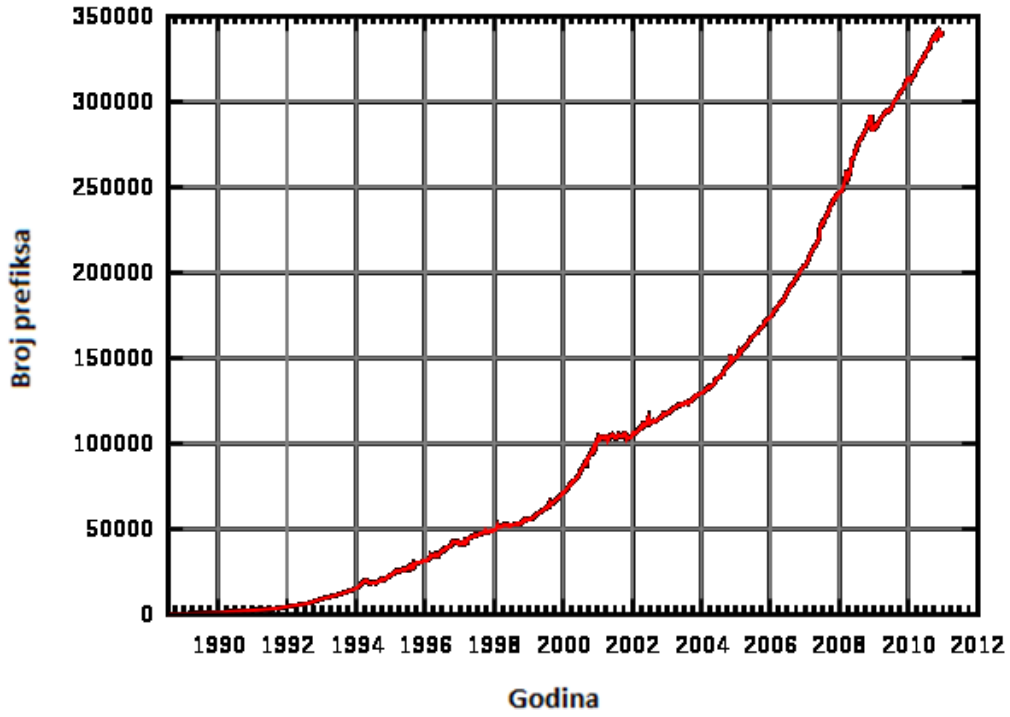
Danas se sve više savjetuje izbjegavanje korištenja *route flap damping* metode. Razlog je sve veći napredak usmjeritelja koji imaju dovoljno procesorske snage za smanjenje utjecaja *route flapping* pojave. Smatra se da danas *route flap damping* može napraviti više štete nego koristi, zbog čega se administratore upozorava da dobro odvagnu prednosti i nedostatke korištenja ove metode prije nego ju odluče primijeniti.

4.3. Veličina tablica usmjeravanja

Ipak, najveći problem BGP protokola je rast tablica usmjeravanja (Slika 4). Kako se povećava broj autonomnih sustava, povećava se i broj BGP usmjeritelja. Svaki BGP usmjeritelj mora biti povezan sa svim ostalim BGP usmjeriteljima i bilježiti sve informacije koje posjeduju i drugi usmjeritelji. Zbog toga dolazi do eksponencijalnog rasta tablica usmjeravanja, što predstavlja problem za starije BGP usmjeritelje (koji najčešće nemaju dovoljno memorije ili procesorske snage za upravljanje s novim putovima). Velike tablice mogu povećati nestabilnost sustava u smislu reakcije na velike promjene u sustavu kada je potreban određen vremenski period dok svi usmjeritelji ne izračunaju nove puteve.

Rast tablica usmjeravanja se djelomično usporio korištenjem CIDR (eng. *Classless Inter-Domain Routing*) i agregacije putova, ali ove metode nisu dovoljne. Zbog velikog broja puteva, dolazi do razmjene velike količine poruka kojima se informacije o putevima izmjenjuju između usmjeritelja putem UPDATE poruka.

[3] DoS napad (eng. *Denial of Service*) je napad uskraćivanjem usluga. Najčešće rezultira rušenjem aplikacije.



Slika 4. Veličina tablica usmjeravanja
Izvor:Wikipedia

4.4. Sigurnost

Kao što je već spomenuto, BGP protokol, u svojoj osnovnoj inačici ne donosi rješenja koja bi pomogla u sigurnosti protokola. Zbog toga se nedostaci u BGP protokolu mogu iskoristiti za razne napade poput napada uskraćivanjem usluga (DoS napad), neovlašteni pristup, prisluškivanje, upravljanje paketima, upad u sjednice itd. Napadi mogu izravno iskorištavati nedostatke u BGP protokolu, ali budući da on koristi TCP protokol, napadači mogu iskorištavati i propuste u TCP ili IP protokolu.

Najveći problem je zasigurno gubitak veze između ključnih dijelova sustava zbog čega neki ključni servisi (elektronička pošta, VoIP servisi i sl.) mogu prestati s radom. Drugi rizik je povjerljivost podataka (eng. *confidentiality*) koja može biti narušena ako su podaci pogrešno preusmjereni što može biti rezultat krivih informacija u poruci UPDATE. U sljedećem poglavlju će se razmatrati načini kojima se mogu spriječiti ili barem ublažiti napadi na BGP protokol.

5. Sigurnosne preporuke

U razvoju BGP protokola nije se vodilo računa o sigurnosti, te stoga BGP u osnovnoj inačici nema ugrađen mehanizam autentikacije kojim se provjerava odgovara li izvor poruke naveden u poruci zaista AS-u odakle je poruka poslana. Napadači mogu iskoristiti ove propuste kako bi, primjerice, slali lažne UPDATE poruke s krivim putovima usmjeravanja, zbog čega paketi neće dolaziti na svoje odredište. Drugi oblik napada je zagušenje usmjeritelja slanjem velikog broja poruka. Ranjivosti BGP protokola pokušavaju se ispraviti raznim dodacima.

Tokom godina jer razvijeno nekoliko preporuka čijom primjenom se može povećati sigurnost BGP protokola. Problem je što preporuke dolaze iz raznih izvora i često se rješenja koja nude preklapaju tako da korištenje jednog isključuje korištenje drugog. Jedna od takvih preporuka (čije se korištenje preporuča) je dokument RFC 2385 koji uvodi oblik zaštite BGP sjednice koristeći jednu mogućnost TCP protokola. Temelji se na dodavanju 16 bitnog MD5 sažetka u TCP zaglavlje. Na taj način se čuva integritet poslanog paketa i onemogućuje dobar dio napada. Nedostaci su povećano vrijeme obrade BGP poruke (zbog provjere sažetka) i povećanje veličine paketa. Preporuka uvodi jedan relativno jednostavan mehanizam zaštite, ali on ipak nije dovoljan kako bi se važni BGP usmjeritelji očuvali od napada.

U nastavku slijedi nekoliko preporuka kojima se još može povećati sigurnost BGP protokola.

5.1. Predložak za sigurni BGP

Predložak za sigurni BGP je skup postavki za Cisco usmjeritelje kojima je moguće povećati sigurnost BGP protokola, ali ovi postupci se mogu koristiti i na drugim usmjeriteljima. Postavke je odredio Team-Cymru [2], a upotreba ovih preporuka je široko rasprostranjena. U nastavku će biti opisane sve preporuke, a uz neke će biti priložen odgovarajući programski kod za Cisco usmjeritelje koji ih ostvaruje. Mogućnost primjene određene preporuke ovisi o proizvođaču usmjeritelja.

Preporuke su sljedeće:

- **Nije potrebna sinkronizacija s IGP protokolom**. U prvim inačicama implementacije protokola, BGP usmjeritelji su čekali dok su IGP usmjeritelji širili informaciju o novom putu u svom AS-u. Tek nakon što je informacija proširena kroz cijeli AS, rubni BGP usmjeritelji su tu informaciju podijelili sa svojim susjedima. Danas se ovakav način razmjene informacija uglavnom ne koristi zbog toga što su tablice usmjeravanja postale izuzetno velike pa zauzimaju velik dio računalnih resursa.
- **Isključiti mogućnost *fast external failover.*** Ova mogućnost se prvotno koristila kada bi došlo do prekida neke poveznice, a omogućavala je brzo prebacivanje na drugu poveznicu. Bez ove mogućnosti, do prebacivanja ne bi došlo prije isteka vremena između slanja dvije KEEPALIVE poruke. Budući da je vrijeme između dvije KEEPALIVE poruke najčešće 60 sekundi, moguća je situacija u kojoj cijelu minutu paketi ne mogu prolaziti putem koji su poslani jer BGP usmjeritelj ne zna da je njegov susjed postao nedostupan. *Fast external failover* je u takvim slučajevima dosta koristan, ali njegova upotreba se ne preporuča zbog pojave situacije opisane u poglavlju 4.2 (*route flapping*). Kako bi se ublažile posljedice *route flappinga* koristi se već opisana metoda *route flap damping* koja unosi vremensku zadršku. Zbog nje, usporava se i *fast external failover* što dovodi do nestabilnosti cjelokupnog sustava. Kod za Cisco usmjeritelje koji isključuje ovu opciju je:

```
no bgp fast-external-fallover
```

- **Preporuča se zapisivanje promjena kod BGP susjeda.** Zapisivanje kada koji susjed uđe ili izađe iz *Established* stanja se pokazalo korisnim prilikom traženja mogućih sigurnosnih problema. Naredba za Cisco usmjeritelje je sljedeća:

```
bgp log-neighbor-changes
```

- **Niz IP adresa (eng. *netblock*) je potrebno najaviti** tako da se ne zauzima puno procesorskog vremena. Također, adrese se ne bi smjele povezivati s IGP protokolom

kako eventualne nestabilnosti u njemu ne bi utjecale i na BGP protokol. Primjer za Cisco usmjeritelje koji zadovoljava ove zahtjeve je sljedeći:

```
network 192.0.2.0 mask 255.255.255.0
```

- **Korištenje „mekane rekonfiguracije“** (eng. *soft reconfiguration*)**.** Uobičajeno, kako bi se promijenile postavke (poput politika usmjeravanja), BGP sjednicu je potrebno prvo zatvoriti što jako utječe na kvalitetu usmjeravanja. Naime, nakon promjene postavki potrebno je ponovo izgraditi cijelu tablicu usmjeravanja što može potrajati (zbog današnjih velikih tablica usmjeravanja). Ovo se može iskoristiti za zlonamjerni napad korištenjem lažne poruke o promjeni postavki, a napad može rezultirati uskraćivanjem usluga ili DoS stanjem (eng. *Denial of Service*). Korištenjem „mekane rekonfiguracije“, promjene se mogu izvesti i tokom trajanja sjednice zbog čega nema potrebe za nepotrebnim prekidanjem sjednice. U dokumentu RFC 2918 definirano je unaprjeđenje „mekane rekonfiguracije“ koje se naziva *Route Refresh* (definirana dokumentom RFC 2918). Ova metoda uvodi nove poruke (*route refresh request* poruke) kojima je moguće ponovno objavljivanje popisa *Adj-RIBs-Out*. Naredba koja uključuje korištenje mekane rekonfiguracije za Cisco usmjeritelje:

```
neighbor 10.10.5.1 soft-reconfiguration inbound
```

- **Korištenje autentikacije**. Jasno je koliko je korištenje autentikacije važno u sprječavanju zlonamjernih aktivnosti. Preporuča se korištenje IPSec protokola ili MD5, odnosno SHA-1 algoritma za kriptografsku zaštitu BGP poruka koje usmjeritelji izmjenjuju tokom sjednice (preporuka RFC 2385).
- **Onemogućiti pregovore o BGP inačici**. BGP usmjeritelji na početku svake veze pregovaraju o inačici BGP protokola koja će se koristiti. Pokazalo se kako je ovakvo pregovaranje nepotrebno jer se usmjeriteljevi susjedi uglavnom ne mijenjaju kroz dulje razdoblje i najčešće se koristi BGP inačice 4, te je moguće podatke o inačici statički upisati za svaku vezu. Na ovaj način se ubrzava povezivanje dva BGP usmjeritelja:

```
neighbor 10.10.5.1 version 4
```

- **Zabraniti poruke i informacije o neispravnim IP prefiksima** (eng. *bogon IP address*). Radi se o prefiksima IP adresa koji su rezervirani za javnu upotrebu, ali za koje je poznato da nisu nikome dodijeljeni. Jasno je kako sve poruke s ovakvih IP adresa treba ignorirati jer sigurno ne nose valjanu poruku. Također, putevi koji koriste ovakve IP adrese nisu valjani i potrebno je takve puteve izbaciti iz popisa mogućih puteva. Ovakvim filtriranjem se olakšava donošenje odluke o najkraćem putu, a napadačima se onemogućuje izvođenje DoS napada korištenjem lažnih adresa. Filtriranje neispravnih (*bogon*) IP adresa može značajno povećati sigurnost BGP protokola. Jedno istraživanje je pokazalo kako je 60% paketa s *bogon* IP adresa korišteno u nekom obliku napada. Potrebno je često provjeravati IP adrese koje se filtriraju kako ne bi došlo do zabrane valjanih IP adresa kojima je nedavno dodijeljena IP adresa koja je prije bila *bogon*. Popis *bogon* IP adresa nalazi se na nekoliko web stranica poput onog na:

http://www.team-cymru.org/Services/Bogons/bogon-bn-nonagg.txt

- **Filtriranje IP prefiksa.** Na ovaj način je moguće spriječiti AS da postane tranzitni AS (da prenosi pakete između dva AS-a). Temelji se na propuštanju samo određenih prefiksa koji su unaprijed najavljeni, a potrebno je filtrirati i dolaze i odlazne prefikse. Ova metoda povećava sigurnost BGP protokola i onemogućuje neke napade, a zapravo je slična vatrozidu (eng. *firewall*). Može se koristiti na dva načina: zabraniti određene prefikse, a dopustiti sve ostale ili dopustiti samo određene prefikse, a sve ostale zabraniti. Potonji način pruža veću sigurnost, ali manju fleksibilnost. Odabir koji će se način rada koristiti ovisi o mrežnom administratoru. Kod ove metode korisno je ako susjedni usmjeritelji imaju iste filtre prefiksa. Na taj način se sprječava napad u kojem se napadač predstavlja kao susjedni usmjeritelj i šalje lažnu IP adresu. BGP usmjeritelj odmah može prepoznati

napadača znajući da tu IP adresu njegov susjed nikada ne šalje jer se nalazi u zajedničkom popisu prefiksa koje filtriraju. Sljedeći programski kod uključuje filtriranje IP prefiksa definiranih u *prefix-list*:

```
neighbor 10.10.5.1 prefix-list announce out
```

- **Postaviti granicu koja određuje najveći broj prefiksa** koje usmjeritelj može primiti od svog susjeda. U slučaju dobivanja velikog broja prefiksa, usmjeritelj treba biti postavljen tako da odmah prekine sjednicu sa susjedom i pošalje poruku upozorenja administratoru. Postavljanje granice za Cisco usmjeritelje se radi na sljedeći način:

```
bgp maxas-limit 10
```

- **Koristiti sučelje povratne adrese** (eng. *loopback*) za iBGP najave. Pokazalo se kako se na ovaj način povećava stabilnost u iBGP načinu rada.
- Susjedima je potrebno **omogućiti spajanje samo na priključnicu 179.** Pokušaj spajanja na bilo koju drugu priključnicu se treba tretirati kao loše postavljen BGP susjed ili pokušaj zlonamjerne aktivnosti.

Detaljan programski kod kojim se ostvaruju sve prethodno opisane preporuke na Cisco usmjeriteljima može se pronaći na web stranici:

http://www.team-cymru.org/ReadingRoom/Templates/secure-bgp-template.html

Odgovarajući programski kod za Juniper usmjeritelje nalazi se na:

http://www.cymru.com/gillsr/documents/junos-bgp-appnote.htm

5.2. S-BGP

BGP protokol u svojoj osnovnoj inačici nema podržanu autentikaciju zbog čega može jednostavno postati metom raznih napada (jer zapravo ne provjerava valjanost poruka). S-BGP (eng. *Secure BGP*) arhitektura je jedan od prvih prijedloga kojima bi se trebala povećati sigurnost BGP protokola. Razvoj S-BGP arhitekture je 1996. započeo BBN Technologies iz SAD-a. S-BGP bi trebao pokriti nedostatke BGP protokola uvođenjem tri sigurnosna mehanizma.

Kao prvi sigurnosni mehanizam, uvedena je **infrastruktura javnog ključa** ili PKI (eng. *Public Key Infrastructure*) kojom se utvrđuje:

- autentičnost vlasništva nad blokom IP adresa,
- autentičnost broja AS-a (identitet AS-a) i
- identitet BGP usmjeritelja i provjera njegove ovlaštenosti da zastupa AS.

Kao drugi sigurnosni mehanizam uveden je novi **izborni tranzitni atribut puta** (*Attestation*) kojim se prenose digitalni potpisi u UPDATE poruci. Pomoću ovog atributa i certifikata iz PKI, usmjeritelj može provjeriti prefikse adresa i informacije o putu koje je dobio u poruci UPDATE.

Posljednji sigurnosni mehanizam je **korištenje IPSec protokola** kako bi se provjerio integritet podataka. Dodatno, on omogućuje i međusobnu autentikaciju BGP usmjeritelja.

Uvedeni sigurnosni mehanizmi pružaju jako dobru zaštitu u smislu provjere ispravnosti IP prefiksa i integriteta AS_PATH atributa (koji se štiti s atributom *Attestation* i javnim ključevima).

Pokazano je da S-BGP ipak ima nekoliko nedostataka. Najveći nedostatak je uključivanje nekoliko organizacija (Internet registri, prodavači usmjeritelja i pružatelji Internet usluga) u razvoj i uvođenje S-BGP protokola. Naime, kako bi S-BGP mogao ispravno raditi, sve navedene organizacije ga moraju primijeniti (nije dovoljna samo jedna), a troškovi mogu biti veliki i organizacijama se ne isplati uvoditi ako nisu sigurne da će ga i ostale uvesti.

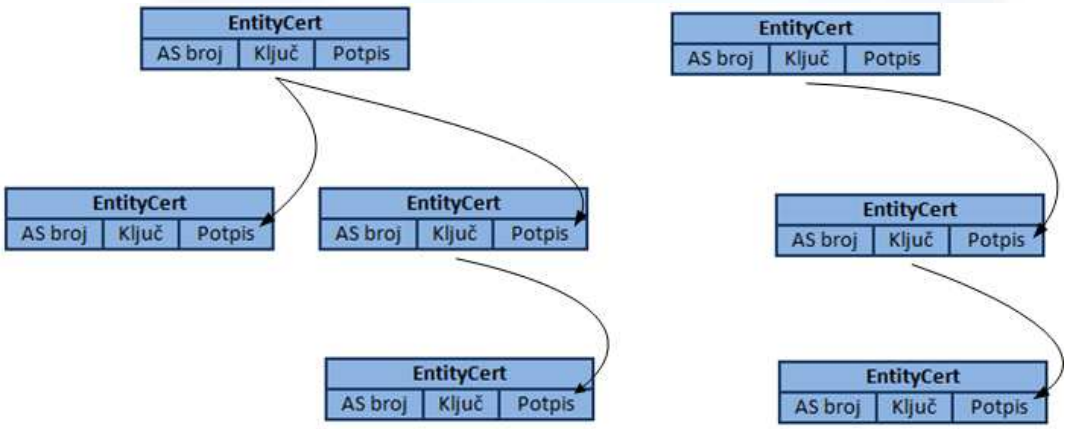
Ostali nedostaci se odnose na predloženu strukturu javnih ključeva i provjere atributa AS_PATH. Naime, predložena struktura javnih ključeva je dosta složena, a provjera AS_PATH atributa

zahtjevna za procesore. Ipak, korist upotrebe S-BGP arhitekture nadmašuje ove nedostatke, te kao jedini pravi nedostatak ostaje problem uvođenja S-BGP-a u postojeću Internet strukturu.

5.3. soBGP

Kao alternativu S-BGP arhitekturi, Cisco i nekoliko pružatelja usluga predložili su soBGP (eng. *secure origin BGP*). Ova arhitektura bi također trebala riješiti sigurnosne probleme BGP protokola, ali na način koji je jednostavniji za uvođenje od S-BGP arhitekture.

U soBGP arhitekturi koristi se hijerarhijska struktura javnih ključeva (Slika 5) koji se kasnije mogu koristiti za izradu raznih certifikata kojima se potvrđuje da AS upravlja određenim blokom IP adresa, zatim da je put objavljen u poruci UPDATE valjan itd. Svaki AS dobiva svoj javni ključ koji je povezan s brojem AS-a. Ova veza je zapisana u *EntityCert*. Ispravnu dodjelu javnog ključa je provjerila druga (viša na hijerarhiji) organizacija, a ključ je potpisan s javnim ključem te više organizacije koja je provjerila njegovu ispravnost. Javni ključ organizacije je potpisala organizacija na još višoj razini sa svojim javnim ključem i tako dalje. Dva AS-a koji se nalaze na dnu hijerarhije na slici 5 mogu vjerovati jedan drugom iako su njihove ključeve potpisali različiti viši AS-ovi. Razlog je što su njihove ključeve potpisali AS-ovi na vrhu strukture kojima se uvijek može vjerovati. Na vrhu strukture se nalazi samo nekoliko organizacija, a tu ulogu mogu preuzeti najveći ISP-ovi (eng. *Internet Service Provider*). Ovakav model dopušta jednostavno dodavanje novih AS-a u strukturu jer njihov javni ključ može potpisati i AS koji se nalazi na dnu strukture. Zbog toga je i jednostavniji za uvođenje u postojeću Internet arhitekturu od prije opisanog S-BGP rješenja.



Slika 5. Hijerarhijska struktura javnih ključeva

Ključ koji je zapisan u *EntityCert* je javni ključ. On dolazi u paru s privatnim ključem koji se nigdje ne otkriva, a zapisuje se na nekom sigurnom uređaju u AS-u. Privatni ključ se može koristiti za izradu certifikata (*AuthCert*) kojim će se potvrđivati da određeni AS ima dozvolu nad nekim blokom IP adresa. Dodatno, s ključevima je moguće potpisati certifikat *ASPolicyCert* u kojem se nalazi popis susjeda izdavatelja certifikata. Ovim certifikatom moguće je provjeriti podatke u atributu AS_PATH, odnosno može li zaista usmjeritelj koji objavio taj put provoditi pakete tim putem ili mu je put zapravo nedohvatljiv (u tom slučaju se može zaključiti da je ta poruka dio napada kojim se pokušava pakete skrenuti na krivi put i sl.).

U soBGP-u se uvodi nova vrsta poruka (poruka SECURITY) koja se koristi za prijenos certifikata, ali postoji mogućnost da se ovaj način prijenosa certifikata zamijeni nekim drugim načinom što istražuje IETF (eng. *Internet Engineering Task Force*).

5.4. psBGP

Arhitektura psBGP (eng. *Pretty Secure BGP*) kombinira najbolje od prethodne dvije arhitekture: sigurnost S-BGP i jednostavnost uvođenja soBGP. Za provjeru autentičnosti AS broja koristi se središnja agencija kojoj se može vjerovati, a provjera vlasništva nad IP prefiksima se provodi

decentralizirano. Svaki AS uz jedinstveni broj dobije i javni ključ od središnjeg certifikacijskog agenta čime se javni ključ poveže s brojem AS-a. Pokazalo se kako je ovo najbolji način za obranu od napada u kojima napadač lažno oponaša neki AS. Provjera vlasništva nad IP adresama se radi s posebnim popisima prefiksa koji povezuju blokove IP adresa s brojevima AS-ova. Svaki AS ovakav popis radi za sebe i za nekoliko susjednih AS-ova. Popis je valjan ako isti popis (nezavisno napravljen) imaju dva susjedna AS-a.

Arhitektura psBGP je nešto manje sigurna od S-BGP arhitekture (zbog manjeg broja certifikata koji se koriste i nepostojanja središnjeg certifikacijskog tijela), ali zato bolja od soBGP. S druge strane, jednostavnija je za uvođenje od S-BGP (ali ipak ne toliko kao soBGP).

6. Implementacije

Postoji nekoliko implementacija BGP protokola, a mnoge su i otvorenog koda. Najčešće su prilagođene za rad na Unix operacijskim sustavima.

Jedna od njih je **Quagga**, programski paket koji podržava nekoliko protokola za usmjeravanje, između ostalog i BGP protokol. Quagga podržava BGP protokol inačice 4, a dodatno omogućuje višeodredišno razašiljanje i IPv6 adrese. Algoritam za usmjeravanje je jako sličan primjeru algoritma usmjeravanja koji je predstavljen u poglavlju 3.4, a omogućeno je provođenje različite politike usmjeravanja prema različitim susjednim BGP usmjeriteljima (odnosno AS-ovima). Od naprednijih metoda, podržani su reflektori puta (opisani u poglavlju 4.1) i filtriranje IP adresa u dolaznim porukama u obliku provjere dolazi li neka od poruka od BGP susjeda ili je to lažna poruka koju treba odbaciti. Dokumentacija Quagga programskog paketa koja sadrži sve upute za postavljanje BGP usmjeritelja nalazi se na sljedećoj poveznici:

http://www.quagga.net/docs.php

XORP (eng. *eXtensible Open Router Platform*) je programski paket sličan prije opisanom Quagga paketu koji uz IGP protokole usmjeravanja podržava i BGP protokol inačice 4. Također, omogućuje rad s IPv6 adresama i reflektorima puta. Dodatno, podržava *route flap damping*, konfederacije te nadgledanje stanja veza sa susjednim BGP usmjeriteljima. Promjene algoritma za usmjeravanje nisu omogućene. Više informacija o XORP programskom paketu može se naći na sljedećoj poveznici:

http://www.xorp.org/design_docs.html

U programskom paketu **OpenBGPD** (također otvorenog koda) za BGP usmjeritelj može poslužiti bilo koje osobno računalo s operacijskim sustavom OpenBSD ili FreeBSD, a predstavlja alternativu za programski paket Quagga. On implementira BGP protokol definiran u starijoj inačici RFC dokumenta (dokument RFC 1771), ali podržava jednostavan sigurnosni mehanizam temeljen na MD5 sažetku u TCP zaglavlju. Također, podržava i IPSec protokol za autentikaciju i filtriranje prefiksa IP adresa. U razvoju ovog programskog paketa naglasak je stavljen na brzinu i učinkovito iskorištavanje računalnih resursa. Upute za OpenBGPD se nalaze na:

http://www.openbgpd.org/manual.html

7. Budućnost

U prijašnjim poglavljima opisana je važnost BGP protokola, ali i njegovi brojni nedostaci. Stalno se javljaju nove preporuke i rješenja koja bi ispravila njegove nedostatke, ali ta rješenja još uvijek nisu dovoljno dobra. Dva su glavna problema koja se trebaju riješiti:

- rast tablica usmjeravanja i
- povećanje sigurnosti.

Za prvi problem već postoje primjenjiva rješenja, ali stalni rast Interneta uvjetuje stalni razvoj novih rješenja ovog problema. Drugi problem je zapravo veći jer osjetljivost BGP usmjeritelja na napade izravno utječe na samu infrastrukturu Interneta. U poglavlju 5. opisano je nekoliko rješenja kojima se može povećati sigurnost BGP protokola. Ipak, ta rješenja ili nisu primjenjiva (poput S-BGP zbog zahtjeva za nekoliko certifikacijskih tijela) ili imaju presloženu strukturu certifikata ili ne pružaju dovoljnu zaštitu kakva bi bila zadovoljavajuća za tako ključan dio Interneta. Područje sigurnosti BGP protokola će se i dalje nastaviti intenzivno istraživati.

Drugi smjer istraživanja kojim bi se riješili problemi u BGP protokolu je zamjena novim protokolom za usmjeravanje između AS-ova. Rasprava o mogućoj zamjeni je započeta s **HLP protokolom**. HLP protokol bi trebao biti bolji od BGP protokola u konvergenciji, izoliranju greške, skalabilnosti te bi trebao slati manje poruka za promjenu putova. Svojstvo BGP protokola koje se trebalo žrtvovati kako bi se ostvarila ova poboljšanja je čuvanje informacije o politici usmjeravanja. Naime, BGP protokol nikako ne otkriva algoritam kojim određuje put kojim će usmjeravati pakete, te tako ne otkriva politiku usmjeravanja u AS-u. Ideja iza HLP protokola je u najvećem dijelu koristiti zajedničku politiku usmjeravanja u svim AS-ovima, ali ostaviti AS-u na izbor nekoliko manjih parametara kojima bi mogli prilagoditi tu opću politiku usmjeravanja svojim pravilima. Pri tome se koristi pretpostavka da je Internet najvećim dijelom organiziran kao hijerarhija AS-ova. Navodi se da korištenje ovakve metode može smanjiti količinu poruka za promjenu putova (kod BGP-a su to bile UPDATE poruke) za oko 400 puta.

HLP protokol je daleko od stvarne upotrebe, ali je pokrenuo neka zanimljiva razmišljanja o mogućem rješenju problema s BGP protokolom.

8. Zaključak

BGP protokol je zaista jedan od najvažnijih protokola u Internetu, a prekid rada samo nekoliko BGP usmjeritelja mogu osjetiti tisuće korisnika. Zbog toga može začuditi da, iako je BGP protokol već jako dugo u upotrebi kao jedini EGP protokol u Internetu, nisu napravljeni veliki pomaci u njegovoj sigurnosti. Istina, tokom godina su izdane brojne nadopune osnovnog RFC dokumenta kojim se definira BGP protokol (čak je i početni dokument RFC 1771 potpuno zamijenjen novim dokumentom RFC 4271), ali nadopunama nije ostvarena željena sigurnost BGP protokola i dobiva se dojam da su one samo zakrpe kojima se osnovni problem samo ublažava. Zbog toga BGP i dalje ostaje podložan raznim napadima.

Ovaj protokol koristi brojne parametre na temelju kojih usmjeritelj donosi odluku o putu kojim će slati pakete. Ovo je svakako prednost jer se omogućuje korištenje različitih politika usmjeravanja AS-a koje se još k tome ne otkrivaju ostalim AS-ovima. U tom smislu je BGP dobro razrađen protokol, ali ovakvo rješenje donosi probleme ako ga koristi jako veliki broj usmjeritelja, što je i slučaj u današnjem Internetu. Problem je što usmjeritelji moraju biti povezani s velikim brojem drugih BGP usmjeritelja kako bi se informacije o promjenama u mreži što brže proširile. Ovo ima za posljedicu iznimno velike tablice usmjeravanja od nekoliko tisuća zapisa. Pretraživanje tih zapisa kako bi se odabrao put za usmjeravanje paketa zahtjeva puno procesorskog vremena s čim se „stari“ BGP usmjeritelji ne mogu nositi. Dodatni problem je i iznimno brzi rast broja zapisa (eksponencijalni).

U dokumentu je opisano nekoliko metoda kojima se ublažuju nedostaci BGP protokola: reflektori puta, konfederacije, *route flap damping*, agregacije putova, MD5 sažetak TCP zaglavlja, korištenje IPsec protokola, filtriranje IP adresa, te nekoliko prijedloga koji koriste ključeve za autentikaciju usmjeritelja, AS-ova, vlasništva AS-ova nad blokom IP adresa itd. Korištenje ovih metoda svakako povećava sigurnost BGP protokola i njihova primjena je svakako preporučljiva.

9. Reference

[1] RFC 4271: A Border Gateway Protocol 4 (BGP-4), http://tools.ietf.org/html/rfc427, siječanj 2006.

[2] R.Thomas, Secure BGP Template, http://www.cymru.com/Documents/secure-bgp-template.html, veljača 2011.

[3] RFC 4456: BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP), http://tools.ietf.org/html/rfc4456, travanj 2006.

[4] RFC 2439: BGP Route Flap Damping, http://tools.ietf.org/html/rfc2439, studeni 1998.

[5] Evangelos Kranakis, P.C. van Oorschot, Tao Wan: Security Issues in the Border Gateway Protocol (BGP), ožujak 2005.

[6] R. White. Securing BGP Through Secure Origin BGP (soBGP). In The Internet Protocol Journal, 6(3): 15-22, September 2003.

[7] RFC 2385: Protection of BGP Sessions via the TCP MD5 Signature Option, http://tools.ietf.org/html/rfc2385, kolovoz 1998.

[8] Lakshminarayanan Subramanian, Matthew Caesar, Cheng Tien Ee, Mark Handley, Morley Mao, Scott Shenker, Ion Stoica: HLP: A Next Generation Inter-domain Routing Protocol, kolovoz 2005.

[9] Wikipedia: Border Gateway Protocol , http://en.wikipedia.org/wiki/Bgp