

УНИВЕРЗИТЕТ СИНГИДУНУМ

**ДЕПАРТМАН ЗА ПОСЛЕДИПЛОМСКЕ СТУДИЈЕ И
МЕЂУНАРОДНУ САРАДЊУ**

Студијски програм: Савремене информационе технологије

МАСТЕР РАД

**ИМПЛЕМЕНТАЦИЈА VGR КОНЕКЦИЈЕ СА ИНТЕРНЕТ
СЕРВИС ПРОВАЈДЕРОМ И АНАЛИЗА МОГУЋИХ
НАПАДА**

Ментор:
Проф. др Младен Веиновић

Студент:
Жарко Грујић 410204/2014

Београд, 2015. године

Садржај

Увод.....	4
1. Концепти BGP протокола.....	5
1.1. Аутономни систем.....	5
1.2. BGP конекција мрежа са ISP.....	6
1.2.1. Употреба статичких рута при конекцији са ISP.....	7
1.2.2. Начини BGP конекција са ISP.....	7
1.3. <i>Path Vector</i> карактеристике BGP протокола.....	10
1.4. BGP карактеристике.....	11
1.5. Везе између BGP суседа.....	12
1.6. BGP табела.....	13
1.7. Типови BGP порука.....	13
2. Појам и улога BGP атрибута.....	15
2.1. <i>AS-path</i> атрибут.....	16
2.2. <i>Next-hop</i> атрибут.....	17
2.3. <i>Origin</i> атрибут.....	17
2.4. <i>Local preference</i> атрибут.....	17
2.5. Атрибут <i>community</i>	18
2.6. MED атрибут.....	18
2.7. <i>Weight</i> атрибут.....	19
2.8. BGP процес одабира рута.....	20
2.9. Манипулација BGP атрибутима коришћењем мапа рутирања.....	20
3. Имплементација BGP решења.....	24
4. Рањивости BGP протокола и ризици од могућих напада.....	35
4.1. Безбедносни напади на BGP рутер и BGP конекцију.....	35
4.2. <i>Spoofing</i>	35
4.3. Преузимање сесије (<i>Session hijacking</i>).....	37
4.4. <i>Route flapping</i>	37
4.5. <i>Route de-aggregation</i>	38
4.6. <i>Unallocated route injection</i>	39
4.7. <i>Denial of service (DoS)</i>	39
4.8. Погрешна конфигурација.....	40

5.	Концепти заштите од појединих напада на BGP конекцију.....	41
5.1.	Заштита BGP рутера	41
5.2.	Заштита од напада на BGP конекцију	42
5.3.	Заштита од импортовања и пропагације погрешних рута	44
5.4.	Заштита од преузимања сесије (<i>session hijacking</i>)	45
5.5.	Secure BGP (S-BGP).....	45
6.	Закључак.....	48
7.	Литература	50
8.	Списак слика	51

Увод

У данашње време Интернет представља витални ресурс за већину организација. Стога, редувантни Интернет линкови ка Интернет сервис провајдерима (у даљем тексту ISP) постају неопходни за велики број организација. *Border Gateway Protocol* (у даљем тексту BGP) представља протокол, који се користи при селекцији путање Интернет саобраћаја код присутних редувантних Интернет линкова са једним или више ISP. BGP је настао из потребе контроле рутирања и пропагације Интернет саобраћаја од стране ISP.

Када је настао, BGP је био једноставан *path-vector* протокол [1]. Временом, вршене су бројне модификације BGP протокола, које су дозвољавале контролу Интернет саобраћаја од стране ISP. Усложњавањем BGP протокола настаје неколико кључних проблема, укључујући и сигурносне пропусте, велики број грешака при конфигурацији, као и конфликте између политика различитих ISP.

У **првом** делу рада описани су концепти BGP протокола и његова намена при повезивању мреже неке организације са ISP.

У **другом** одељку обухваћен је преглед BGP атрибута и њихово коришћење од стране BGP протокола.

Трећи одељак би приказао решење једног од начина повезивања сопственог AS са ISP. Представљен је пример повезивања једног AS са ISP преко две конекције, како би постојала редувантност.

У **четвртном** и **петом** одељку извршена је анализа могућих напада на BGP конекцију, као и мере које треба предузети да поменути напади не доведу до нежељених последица.

1. Концепти BGP протокола

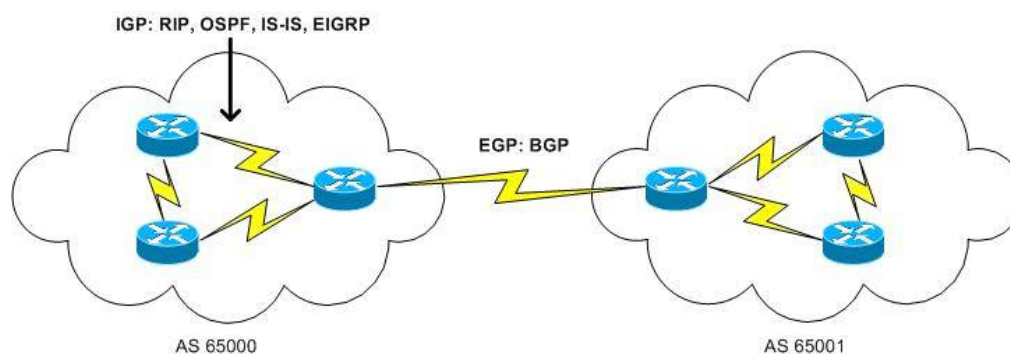
1.1. Аутономни систем

Да би се разумели концепти BGP протокола, потребно је разумети и појам Аутономног система (у даљем тексту AS).

Једна од подела протокола рутирања јесте подела на интерне (*interior*) и екстерне (*exterior*):

- **Interior Gateway Protocol (IGP)** – протокол рутирања, који врши размену информација рутирања унутар једног AS. Примери интерних протокола рутирања су *Routing Information Protocol (RIP)*, *Open Shortest Path First (OSPF)*, *Intermediate System – to – Intermediate System (IS – IS)* и *Enhanced Interior Gateway Routing Protocol (EIGRP)*.
- **Exterior Gateway Protocol (EGP)** – протокол рутирања, који врши размену информација рутирања између AS. BGP је пример EGP протокола.

Слика 1 приказује концепт IGP и EGP.



Слика 1: Примена IGP и EGP у односу на AS

Унутар једног AS може се користити и више од једног IGP протокола. Једна од основних, а вероватно и најважнија, карактеристика AS, са становишта BGP протокола, јесте та да се један AS представља другим AS са јединственим логичким планом рутирања. [2]

Екстерни протоколи рутирања настали су ради контроле експанзије табела рутирања, и како би се постигао структурирани изглед Интернет мреже дељењем домена рутирања у одвојене AS. Сваки AS има своју независну политику рутирања и јединствен IGP протокол. [1]

BGP протокол омогућава транзицију пакета како би пакети стигли до одредишног AS (нпр. AS Интернет сервис провајдера). Улога BGP протокола се највише огледа када један AS има више конекција, ка више суседних AS. У том случају сваки AS има могућност примене различитих политика рутирања. Самим тим врши и селекцију рута за саобраћај који напушта AS.

BGP протокол не представља увек најприкладније решење за конекцију између два AS. Уколико постоји само једна конекција неког AS ка другом AS, онда је најбоље

користити *default* или статичко рутирање. У том случају, коришћењем BGP протокола не може се ништа остварити осим оптерећења процесора и заузетости меморије рутера. Једини случај када ће се користити BGP протокол у овој топологији јесте када се разликује локална политика AS од политике ISP. [3]

Internet Assigned Numbers Authority (IANA) представља организацију, која врши додељивање бројева AS. *Regional Internet Registry* (RIR) представља непрофитабилну организацију за администрирање опсега IP адреса и бројева AS. Постоји пет RIR организација у свету:

- *African Network Information Centre* (AfriNIC) – одговорна за афрички континент.
- *Asia Pacific Network Information Centre* (APNIC) – одговорна за пацифички део азијског континента.
- *American Registry for Internet Numbers* (ARIN) – одговорна за САД, Канаду и нека острва у Карипском мору и Северном Атлантском океану
- *Latin American and Caribbean IP address Regional Registry* (LACNIC) – одговорна за Јужну Америку и део Кариба.
- *Reseaux IP Europeens Network Coordination Centre* (RIPE NCC) – одговорна за Европу, Блиски Исток и централни део Азије. [2]

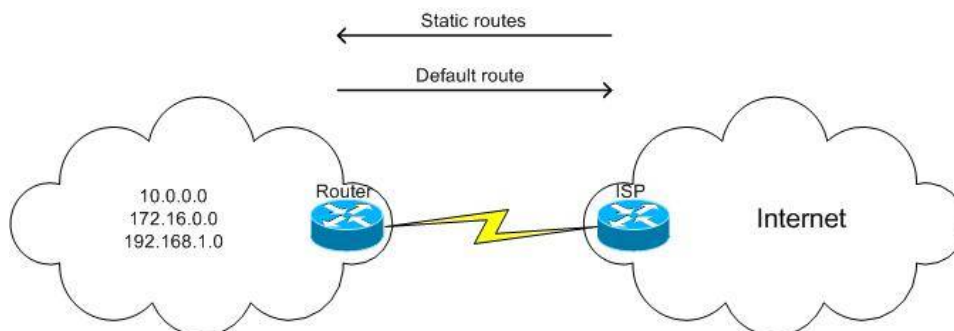
AS број је број у опсегу од 1 до 65535. Опсег AS бројева од 64512 до 65535 резервисан је за приватну употребу. Ако нека организација одлучи да користи EGP као везу са ISP, онда је потребно користити IANA AS број, а не AS број резервисан за приватну употребу. [4]

1.2. BGP конекција мрежа са ISP

За повезивање рачунарских мрежа са ISP користи се BGP протокол. Потребно је испунити неке одређене услове, како би се могла реализовати конекција мреже неке организације са ISP. Први од услова је да организација поседује најмање једну јавну IP адресу. У овом случају клијентски рачунари, као и мрежна опрема, у мрежи једне такве организације, треба да поседују приватне IP адресе. Тада је потребно реализовати *Network Address Translation* (NAT). Јавне IP адресе користе се за транслацију приватних адреса клијената, који желе да приступе Интернету. У тренутку размене саобраћаја приватне мреже ка Интернет мрежи, приватни корисници мреже се Интернет свету представљају јавном IP адресом (или адресама), што је омогућио NAT. Јавне адресе се, такође користе за сервере, који треба да буду доступни са Интернет мреже. Сервери могу имати и приватне IP адресе, које се статички транслирају у јавне IP адресе. Други услов је да постоји линк између приватне и мреже ISP. Сваки такав линк треба да задовољи неке услове што се тиче капацитета. Типови таквих линкова могу бити различити, као што су *leased line*, *ethernet* линк, затим различити типови DSL (*digital subscriber line*) конекција, итд... Трећи услов је реализација статичког или динамичког рутирања. Опциони услов јесте постојање редундантне конекције са истим или другим ISP. У овом случају треба да постоје редундантни *edge* рутер, редундантни линк, као и редундантни ISP. Редундантни линк се може реализовати ка истом ISP, са којим је реализован и примерни линк.

1.2.1. Употреба статичких рута при конекцији са ISP

Најједноставнији начин имплементације конекције са ISP јесте конфигурацијом статичких рута. Сама промена статичких рута не врши се често. Ако би се којим случајем вршила промена статичких рута долазило би и до прекида логичке конекције са ISP. Статичко рутирање се најчешће користи када приватна мрежа поседује само једну конекцију ка једном ISP. У том случају клијентска мрежа, односно *edge* рутер те мреже, може користити *default* руту ка ISP, као што је приказано на Слици 2. *Edge* рутер на страни ISP треба поседовати статичке руте ка свим приватним IP мреже, које користи клијентска мрежа.

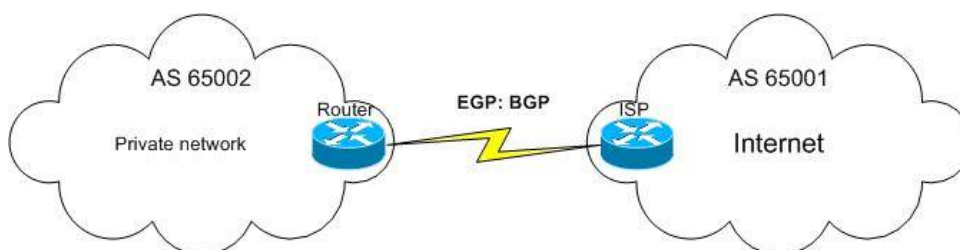


Слика 2: Статичке руте у конекцији са ISP

Статичко рутирање има и мане, посебно у погледу флексибилности и адаптивности. У случају било какве промене топологије мреже, статичке руте се не могу адаптирати на настале промене. [2]

1.2.2. Начини BGP конекција са ISP

Приликом промене топологије мреже, BGP протокол размењује информације рутирања. Слика 3 приказује једноставан пример конекције корисничког *edge* рутера и *edge* рутера на страни ISP.



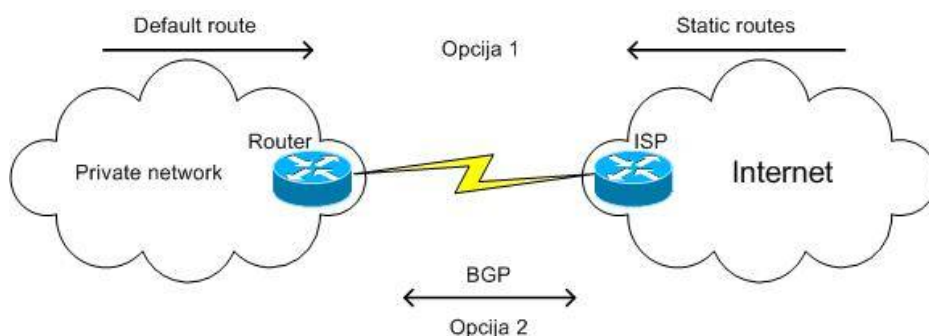
Слика 3: ISP конекција коришћењем BGP протокола

Конекцијом *enterprise* мреже са ISP, редундантност се постиже реализацијом редундантних линкова и постојањем редундантних мрежних уређаја. Може постојати и редундантни ISP. Корисничка *enterprise* мрежа може бити конектована са једним или више ISP. Постоји више типова конекција са ISP:

- **single-homed** - конекција са једним ISP без редундантности линка. Уколико дође до прекида линка, корисничка мрежа остаје без могућности коришћења Интернет сервиса.

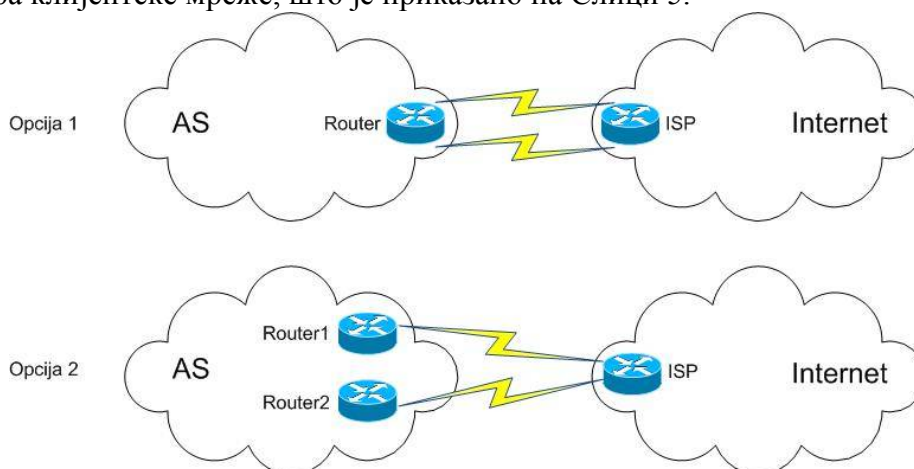
- **dual-homed** -конекција са једним ISP, али са постојањем редундантног линка ка истом ISP.
- **multihomed** - конекција корисничке мреже са два или више ISP.
- **dual multihomed** - конекција корисничке мреже са два или више ISP, уз постојање редундантних линкова са сваким од ISP. [2]

Слика 4 приказује *single-homed* конекцију са ISP. *Single-homed* конекција не захтева употребу BGP протокола. Углавном се користи статичко рутирање.



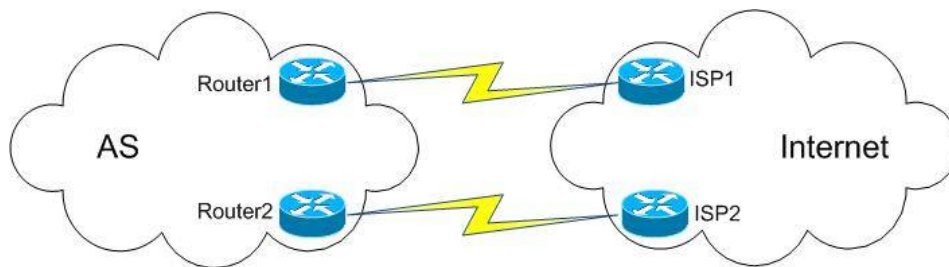
Слика 4: *single-homed* конекција са ISP

Постоје два начина повезивања код *dual-homed* конекције. Код оба начина приватна мрежа поседује две конекције ка истом ISP. У једном случају оба линка се терминирају на истом *edge* рутеру клијентске мреже, а у другом се терминирају на два различита *edge* рутера клијентске мреже, што је приказано на Слици 5.



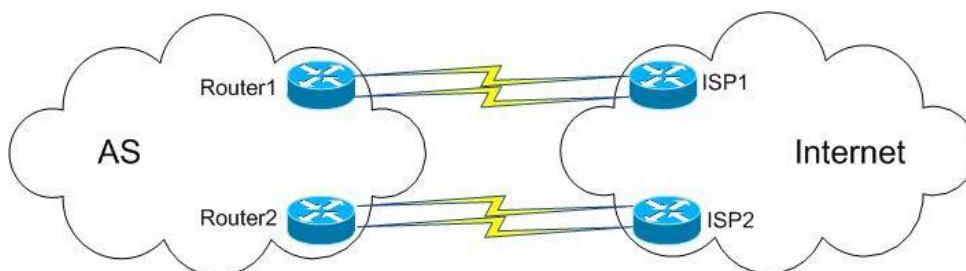
Слика 5: *dual-homed* конекција са ISP

Multihomed конекција представља везу клијентске мреже са два различита ISP. Конекције од оба ISP могу се терминирати на један исти или два различита *edge* рутера клијентске мреже, као што је приказано на Слици 6.



Слика 6: *multi-homed* конекција са ISP

Dual multi-homed конекција представља везу клијентске мреже са два или више ISP, са двоструким линковима ка сваком ISP, као што је приказано на Сlici 7.



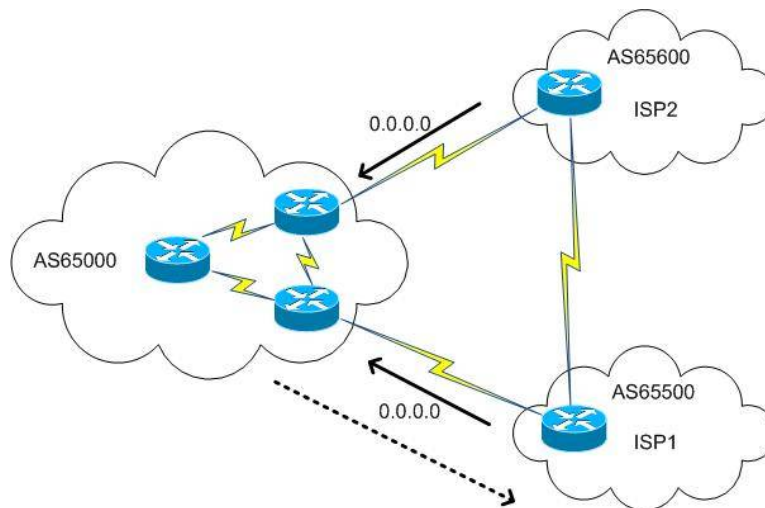
Слика 7: *dual multi-homed* конекција са ISP

Интернет представља велики број AS, који су међусобно повезани и омогућавају међусобну комуникацију. Рутирање међу AS остварује се помоћу BGP протокола. Предности BGP протокола најбоље се показују када један AS има више EBGP конекција ка једном или више ISP. Поседовање вишеструких конекција једне организације са ISP омогућава постојање редундантних линкова ка Интернет мрежи, тако да ако се догоди да један од линкова не функционише, други ће остати у функцији. Поседовање конекција са више ISP за организацију доноси више предности. Једна од њих јесте да ће постојати редундантност линкова. Затим, организација неће бити везана за политику само једног ISP. Постојаће више путања ка истим мрежама, тако да ће постојати могућност бољег манипулисања полисама.

Уколико се једна организација одлучи за реализацију *multi-homed* конекције са ISP, постоји три начина за то:

- Сваки ISP прослеђује само *default* руту ка корисничком AS. Та рута се затим прослеђује и до интерних рутера.
- Сваки ISP прослеђује само *default* руту и своје специфичне руте. Ове руте могу бити прослеђене ка свим интерним рутерима или интерни рутери могу сами разменити те руте коришћењем интерног BGP протокола.
- Сваки ISP прослеђује све руте ка AS организације. Код овог случаја сви интерни рутери на путањи користе BGP протокол и међусобно размењују руте. [2]

Код првог начина *multi-homed* конекције са ISP, оба *edge* рутера уче *default* руту од свог директно конектованог ISP, и те руте прослеђују у свој AS коришћењем локалног IGP протокола. Уколико неки интерни рутер једног AS научи више *default* рута, он у своју табелу рутирања уписује најбољу *default* руту. То је рута са најмањом ценом коштања по метрици IGP протокола. Пример оваквог начина функционисања представљен је на Сlici 8.



Слика 8: *default* руте добијене од суседних ISP

Организације које користе други начин *multihomed* конекције са ISP, од ISP добијају *default* руту и још неке специфичне руте. Тада AS организације може добити руте AS других организација. Редистрибуција великог броја BGP рута унутар IGP може проузроковати бројне проблеме и не препоручује се.

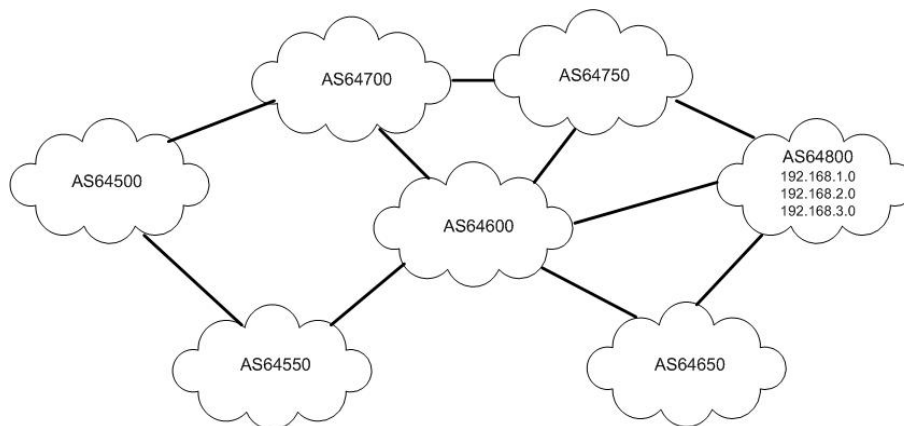
Реализација трећег начина реализације *multihomed* конекције са ISP изискује много ресурса унутар једног AS зато што рутери тог AS морају процесуирати све екстерне руте. У овом случају AS шаље и све своје руте суседном ISP, који процесуира те руте и прослеђује својим суседним AS.

1.3. *Path Vector* карактеристике BGP протокола

BGP рутери размењују информације о доступности мрежа, и те информације се називају **вектори путања** (*path vectors*). Информација о вектору путање садржи листу целокупне путање бројева BGP аутономних система, неопходних да би се дошло до дестинационе мреже (хоп по хоp).

Информација о путањи AS користи се за конструкцију графа аутономних система без петљи и да идентификује полису рутирања. Путања BGP аутономних система је увек без петљи. Рутер, који на себи има покренут BGP, не прихвата *update* рутирања, који већ садржи његов број AS у путањи, зато што је *update* већ прошао кроз његов AS. Уколико би рутер прихватио тај *update* дошло би до креирања петље рутирања. [2]

На Слици 9 приказане су неке од могућих путања од AS 64500 до AS 64800, а да притом на свом путу има AS 64700.



Слика 9: Вектор путање

Неке од могућих путања су:

- 64700 64750 64800
- 64700 64750 64600 64650 64800
- 64700 64600 64750 64800
- 64700 64600 64650 64800

AS 64700 оглашава ка AS 64500 само најбољу путању, која је у овом случају 64700 64750 64800. На исти начин и IGP бира руту са најмањом ценом коштања. AS 64700 не оглашава друге путање већ само најбољу путању, што је путања са најмањим бројем хопова. AS 64500 не учи друге путање, већ само путању са најмањим бројем хопова, све док та најбоља путања не постане недоступна.

1.4. BGP карактеристике

BGP протокол користи TCP порт 179 за комуникацију. Пошто TCP омогућава поуздану комуникацију у смислу ретрансмисије, BGP не мора имати имплементиран било какав механизам ретрансмисије или *error-recovery* механизам. OSPF и EIGRP функционишу директно изнад IP слоја. IS-IS функционише на мрежном слоју, док RIP користи UDP протокол на транспортном слоју.

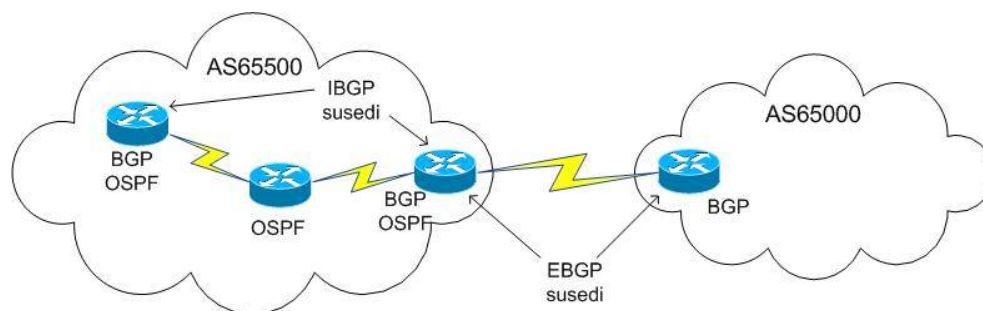
При BGP комуникацији два рутера, успоставља се TCP конекција међу њима, и размењују поруке којима отварају и потврђују параметре конекције. Оваква два рутера називају се BGP *peer* рутери или BGP *neighbors* (суседи). Након успостављања конекције, рутери међусобно размењују комплетне табеле рутирања. Након тога, размењују само настале промене у табели рутирања. BGP протокол шаље *keepalive* поруке, слично као *hello* поруке код OSPF, EIGRP и IS-IS протокола.

BGP протокол функционише на Интернет мрежи, где има више од 300.000 мрежа, а тај број се свакодневно повећава. Самим тим, BGP користи TCP за *acknowledgment*. TCP има динамички *window*, који омогућава и до 65.576 бајтова, који чекају на свој *acknowledgment*.

1.5. Везе између BGP суседа

Један BGP рутер формира директну суседску везу са одређеним бројем других BGP рутера. Преко ових BGP суседа рутер учи AS путање на Интернет мрежи, како би стигао до одређених дестинационих мрежа. Сваки рутер, на коме функционише BGP протокол, назива се BGP *speaker*. Два BGP суседа директно размењују информације BGP рутирања међу собом. [1]

BGP *speaker* има ограничени број BGP суседа, са којима формира TCP конекцију. BGP конекција може бити интерна или екстерна у односу на аутономни систем, као што је приказано на Слици 10.



Слика 10: BGP суседи

BGP *peer* конфигурише се у BGP процесу ***neighbor*** командом. Ова команда налаже BGP процесу да оствари конекцију са суседом, чија је адреса наведена у команди, и да са тим суседом размењује промене у BGP табели рутирања. BGP који се остварује међу рутерима различитих AS назива се EBGP. За два рутера који су BGP суседи, TCP нивои на обе стране морају проћи кроз TCP *three-way handshake* пре него остваре BGP сесију. Управо због тога, адреса из ***neighbor*** команде мора бити доступна без коришћења IBGP, тј. да постоји у табели рутирања. То може бити директно конектована мрежа или да рутирање буде статички остварено.

Постоји неколико предуслова за остваривање EBGP конекције. Један од њих је да AS бројеви буду различити. Други услов је да TCP сесија мора бити остварена пре саме размене информација о BGP рутирању. Трећи услов је да постоји доступност (*reachability*) IP адресе, која се наводи у ***neighbor*** команди. EBGP суседи обично су директно конектовани.

BGP који се остварује међу рутерима унутар истог AS назива се IBGP. IBGP се покреће ради размене информација о BGP рутирању, тако да сви BGP рутери садрже исте информације о спољашњем AS и да се ове информације могу прослеђивати другим AS. Постоји неколико предуслова за остваривање IBGP конекције. Један од њих је да буде исти AS број, тј. да рутери припадају истом AS. Други услов је да TCP сесија мора бити остварена пре саме размене информација о BGP рутирању. Трећи услов је да IBGP суседи морају бити доступни један другом. IBGP суседи не морају бити директно конектовани. IBGP сусед може бити директно конектован или доступан путем статичких рута или неког од динамичких протокола рутирања.

1.6. BGP табела

Рутер, који користи BGP, своју табелу користи и за смештање BGP информација добијених од других BGP рутера. Исту табелу шаље другим рутерима, који користе BGP. Табела BGP информација садржи следеће елементе:

- *BGP table* (BGP табела)
- *BGP topology table* (BGP табела топологије)
- *BGP topology database* (BGP база топологија)
- *BGP routing table* (BGP табела рутирања)
- *BGP forwarding database* (BGP база прослеђивања)

Потребно је знати да је код рутера BGP табела одвојена од IP табеле рутирања. Само најбоље руте из BGP табеле улазе у састав IP табеле рутирања. Размена информација између две табеле врши се редистрибуцијом. BGP такође садржи и табелу суседа, са којима је остварена BGP конекција. Током остварене BGP конекције суседи један другом периодично шаљу BGP/TCP *keepalive* поруке. По *default*-у ове поруке се шаљу сваких 60 секунди.

Након остваривања BGP конекције, суседи размењују своје најбоље BGP руте. Сваки BGP рутер сакупља најбоље руте од свих својих BGP суседа, и смешта их у своју BGP *forwarding database*. Затим следи процес селекције BGP рута и оне се нуде IP табели рутирања. Сваки рутер пореди понуђене BGP руте са осталим рутама истих дестинационих мрежа, и најбоље руте, базирано на административној дистанци, смешта у IP табелу рутирања. EBGP руте имају административну дистанцу 20, док IBGP руте имају административну дистанцу 200 [3]. Рутер може имати најбољу BGP руту ка дестинацији, али да се та рута не може наћи у IP табели рутирања, зато што има већу административну дистанцу од неке друге руте.

1.7. Типови BGP порука

BGP дефинише следеће типове порука, које размењују BGP суседи:

- *Open*
- *Keepalive*
- *Update*
- *Notification*

Након успоставе TCP конекције *open* порука је прва коју шаљу обе стране конекције. Ако се *open* порука прихвати, онда следи порука *keepalive*, која се шаље као потврда од стране оног ко је примио *open* поруку. Тада је BGP конекција успостављена. Након тога се могу размењивати *update*, *keepalive* и *notification* поруке. Иницијално, BGP рутери (суседи) размењују комплетне BGP табеле рутирања. Након тога се размењују само промене настале у BGP табелама рутирања. *Keepalive* поруке се шаљу ради провере да ли конекција још увек постоји међу BGP суседима. *Notification* поруке се шаљу као одговор на грешке у комуникацији. [2]

Open порука садржи следеће информације:

- **Верзија BGP поруке.** На пример, верзија BGP је 4.

- **Број AS**, коме припада. Овај број се шаље суседу, а сусед затим верификује број аутономног система. Ако се не очекује порука из тог аутономног система, прекида се BGP сесија.
- **Hold time**, који означава максималан број секунди који протекне између две *keepalive* или *update* поруке пошиљаоца. *Hold time* информација се прима у *open* поруци, и по *default*-у је 180 секунди.
- **BGP router identifier (router id)** означава пошиљаоца. *Router id* је највећа активна IP адреса на рутеру, или се може статички дефинисати. Препоручује се да највећа IP адреса рутера буде управо *loopback* интерфејс, јер је он увек активан.
- **Опциони параметри**. Пример опционог параметра је аутентикација сесије. [1]

Update порука садржи информацију о једној путањи. Информације о више путања шаљу се кроз више *update* порука. Једна *update* порука садржи информације о рутама, које више нису у оптицају. Затим садржи атрибуте путање, и *network layer reachability information* (NLRI), што представља листу мрежа, које могу бити доступне коришћењем те путање. BGP рутер шаље и *notification* поруке када детектује неку грешку. Чим се појави грешка, шаље се *notification* порука. Одмах након тога BGP рутер прекида конекцију. *Notification* порука садржи код грешке и податке везане за грешку.

2. Појам и улога BGP атрибута

BGP протокол користи атрибуте путање (*path attributes*) за селекцију најбоље путање ка дестинационој мрежи. Атрибути путање сврставају се у четири категорије:

- ***Well-known mandatory*** (обавезни)
- ***Well-known discretionary*** (дискрециони)
- ***Optional transitive*** (опциони прелазани)
- ***Optional non-transitive*** (опциони непрелазни)

Well-known mandatory (добро познати, обавезни) атрибути су обавезни и морају бити део сваке *update* поруке. Остали су дискрециони и могу, али и не морају, бити део *update* поруке. Сви *well-known* атрибути морају бити пренети на BGP *peer* рутер. Поред *well-known* атрибута, свака путања може садржати један или више опционих атрибута. Не захтева се, нити очекује, да свака имплементација BGP протокола садржи све опционе атрибуте. Пошиљалац *update* поруке треба захтевати да атрибути унутар поруке буду поређани по типу атрибута. Прималац поруке мора бити спреман да успешно прими поруку чак и ако атрибути нису поређани по типу атрибута. Исти атрибут не може се појавити више од једног пута унутар *Path Attributes* поља унутар *update* поруке. [5]

Атрибути дефинисани од стране BGP протокола су следећи:

- *Well-known mandatory*
 - AS-path
 - Next hop
 - Origin
- *Well-known discretionary*
 - Local preference
 - Atomic aggregate
- *Optional transitive*
 - Aggregator
 - Community
- *Optional non-transitive*
 - Multiexit-discriminator

Поред горе наведених, BGP протокол је дефинисао и *weight* атрибут. Он се креира локално на рутеру и не пропагира се другим BGP рутерима.

У Табели 1 дати су кодови типова атрибута, које користи BGP протокол.

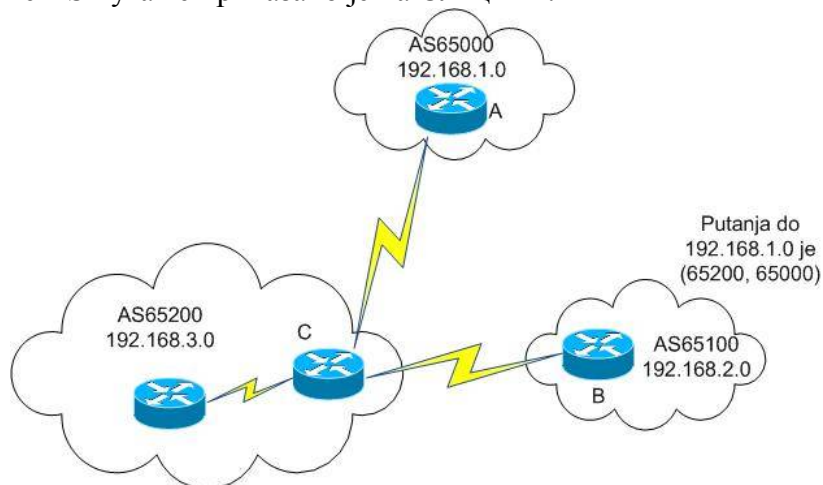
Атрибут	Код типа атрибута
Origin	1
AS-path	2
Next-hop	3
MED	4
Local preference	5
Atomic aggregate	6
Aggregator	7
Community	8
Originator-ID	9
Cluster list	10

Табела 1: Кодови типова BGP атрибута

2.1. *AS-path* атрибут

AS-path атрибут садржи листу бројева аутономних система, који чине путању до одредишта. Сваки AS додаје свој број AS на почетак AS путање. *AS-path* приказује све аутономне системе, кроз које би пакет требало да прође да би дошао до дестинационе мреже. *AS-path* атрибут даје сигурност да у путањи не постоје петље. Када један AS бира путању, бира се путања са најмањим бројем AS хопова. [6]

Функционисање AS путање приказано је на Слици 11.

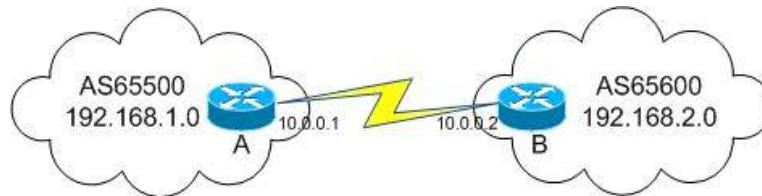


Слика 11: Функционисање AS путање

Рутер В у својој табели рутирања, за мрежу 192.168.1.0, поседује AS путању (65200,65000). Уколико пакет жели да стигне до одредишне мреже, мора проћи кроз листу аутономних система. Уколико BGP рутер прими руту са сопственим AS бројем у AS путањи, тада рутер не прихвата руту, одбацује је. AS путања се мења само уколико руту рекламира EBGP рутер свом суседу. Уколико рутер оглашава руту ка IBGP суседу, онда се AS путања не мења.

2.2. *Next-hop* атрибут

Next-hop атрибут представља *next-hop* IP адресу, која ће се користити како би се стигло до дестинационе мреже. Овај атрибут спада у *well-known mandatory* групу атрибута. *Next-hop* IP адреса за мрежу из другог AS јесте IP адреса улазне тачке наредног AS дуж путање која води ка дестинационој мрежи. Слика 12 приказује употребу *next-hop* атрибута. [6]



Слика 12: BGP *next-hop* атрибут

Рутер А рекламира рутеру В мрежу 192.168.1.0 са *next-hop* адресом 10.0.0.1, док рутер В рекламира рутеру А мрежу 192.168.2.0 са *next-hop* адресом 10.0.0.2. Стога, рутер А користи адресу 10.0.0.2 као *next-hop* атрибут како би дошао до мреже 192.168.2.0, док рутер В користи адресу 10.0.0.1 као *next-hop* атрибут како би дошао до мреже 192.168.1.0.

2.3. *Origin* атрибут

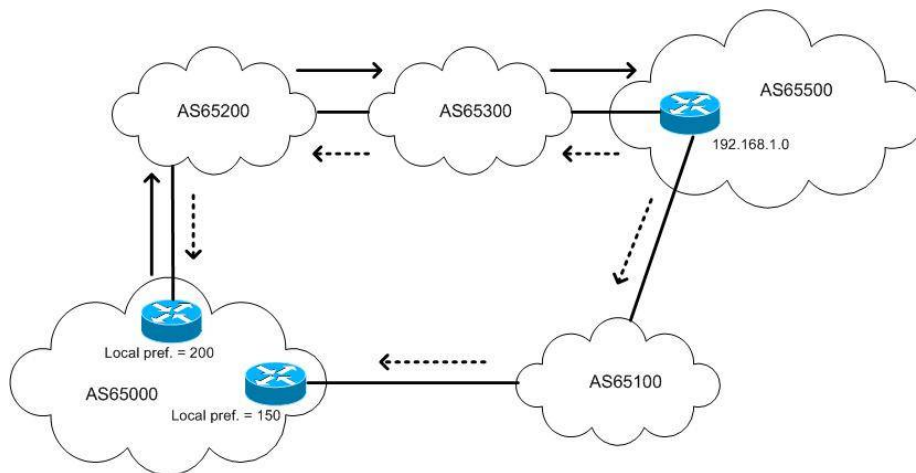
Origin атрибут дефинише порекло информације о путањи. *Origin* атрибут може имати једну од три вредности:

- IGP - означена је са *i* у BGP табели. Порекло означене мреже је исти аутономни систем, а рута може бити научена преко IGP протокола.
- EGP - рута је научена преко EGP протокола. Ова рута означена је ознаком *e* у BGP табели.
- некомплетна - означена је знаком питања (?) у BGP табели. Овај случај се најчешће дешава ако се користи редистрибуција рута.

2.4. *Local preference* атрибут

Local preference атрибут одређује која путања ће се користити за излаз из аутономног система. Овај атрибут се користи између IBGP *peer* рутера и не прослеђује се екстерним BGP *peer* рутерима. Default вредност овог атрибута је 100. Увек предност има већа вредност *local preference* атрибута. [6]

Начин функционисања поменутог атрибута приказан је на Слици 13.



Слика 13: BGP *local preference* атрибут

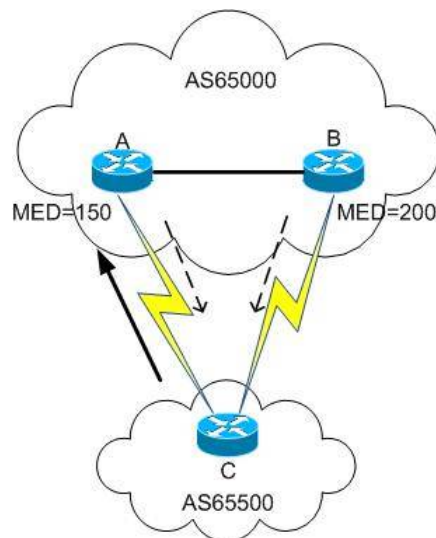
AS 65000 добија информације о мрежи 192.168.1.0 са две различите стране. Рутери у AS 65000 су IBGP суседи. На једном рутеру је за мрежу 192.168.1.0 намештен атрибут *local preference* на вредност 200, а на другом рутеру на вредност 150. *Local preference* атрибут се размењује међу рутерима унутар AS 65000. Сав саобраћај из AS 65000 намењен мрежи 192.168.1.0 биће послат преко рутера са *local preference* атрибутом 200 ка AS 65200. У овом случају је тај рутер излазна тачка аутономног система AS 65000.

2.5. Атрибут *community*

Спада у групу *Optional transitive* атрибута. Не представља атрибут који утиче у процесу доношења одлуке рутирања. Овај атрибут групише руте и примењује полисе и одлуке (*accept, prefer*) везане за те руте. То су групе дестинација, које деле неке заједничке особине. *Community* атрибут омогућава рутеру да означава (*tag*) руте индикатором и омогућава осталим рутерима да на основу њега доносе своје одлуке. BGP рутер може филтрирати руте или одабирати најбоље руте на основу индикатора *community*. Уколико рутер не разуме концепт *community* атрибута, он препушта то наредном рутеру. Ако рутер разуме концепт *community* атрибута, он мора бити конфигурисан да пропагира овај атрибут. У супротном, *community* атрибут биће одбачен. [2]

2.6. MED атрибут

MED атрибут назначавља екстерном BGP суседу коју путању радије да користи, када има више путањи ка истом аутономном систему. Ово је динамички начин да један AS утиче на други AS тако што ће му предложити коју путању да користи. Мањом вредношћу MED атрибута означава се боља путања. За разлику од *local preference* атрибута, MED атрибут се размењује између AS. MED се шаље екстерном BGP суседу. MED атрибут утиче на улазни саобраћај једног AS, док атрибут *local preference* утиче на излазни саобраћај једног AS. *Default* вредност MED атрибута је 0. [6]



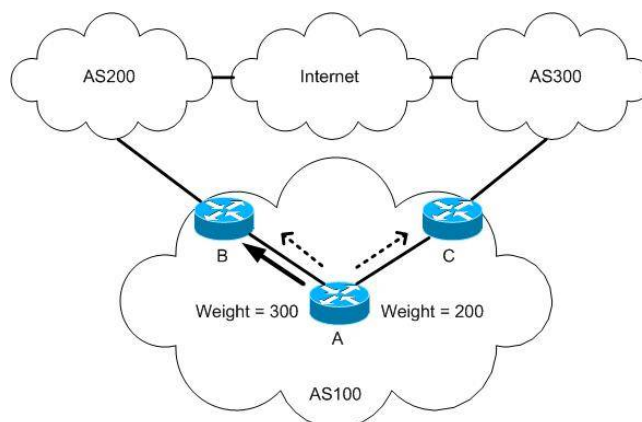
Слика 14: Улога MED атрибута

На Слици 14 представљена је улога MED атрибута. Рутер А поставља MED атрибут на вредност 150 и кроз *update* поруку га шаље ка рутеру С. Рутер В поставља MED атрибут на вредност 200 и кроз *update* поруку га шаље ка рутеру С. Када рутер С прими те поруке, он бира рутер А као *next-hop* како би дошао до AS 65000, зато што је MED атрибут вредности 150 мање од 200.

2.7. *Weight* атрибут

Weight атрибут је локални атрибут на рутеру, који служи за одабир најбоље путање уколико постоји више могућих путања ка дестинационој мрежи. Овај атрибут је специфичан само за CISCO рутере и не преноси се на остале рутере у мрежи. Вредност овог атрибута креће се од 0 до 65535. Рутери са већом вредношћу овог атрибута имају предност уколико постоји више рута ка дестинационој мрежи. *Default* вредност овог атрибута јесте 32768. [6]

Радије се користи овај атрибут него *local preference* атрибут зато што је *weight* атрибут локалног типа, док се *local preference* атрибут размењује између IBGP рутера.



Слика 15: Улога BGP *weight* атрибута

На Слици 15 приказан је начин функционисања *weight* атрибута. Рутер А учи преко рутера В и С о некој мрежи, која је на Интернет мрежи. Рутер А има постављен *weight* атрибут вредности 300 за руте коју учи преко рутера В, док је *weight* атрибута вредности 200 постављен за руте које учи од рутера С. Рутер А ће изабрати путању преко рутера В зато што је пут ка рутеру В има већи *weight* атрибут.

2.8. BGP процес одабира рута

Процес одабира најбоље руте врши се на основу BGP атрибута, које смо описали у претходном делу текста. Уколико постоји више рута ка истој дестинационој мрежи, BGP бира најбољу руту за слање саобраћаја ка самој дестинацији. У одабиру најбоље руте, BGP разматра само синхронизоване руте, тј. руте без AS петљи и са валидном *next-hop* адресом. Процес одабира руте од стране BGP протокола на CISCO рутеру, одвија се следећим корацима:

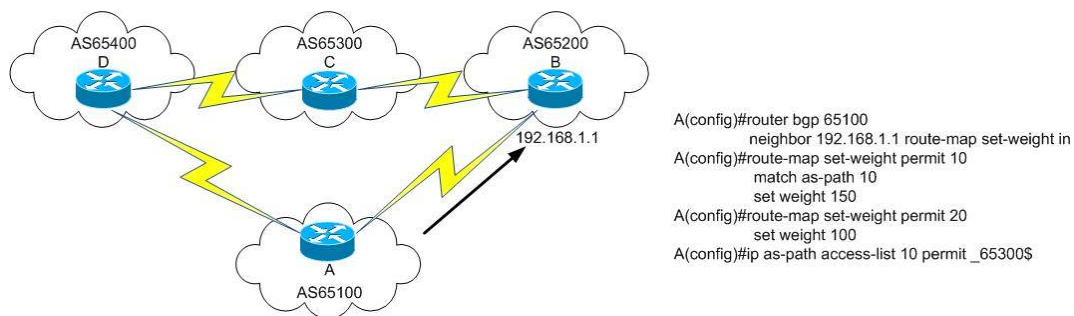
1. Бира се рута са највећим *weight* атрибутом.
2. Уколико *weight* атрибут није подешен, бира се рута са највећим *local preference* атрибутом.
3. Бира се рута коју је створио сам рутер на коме се врши процес одабира руте.
4. Бира се путања са најкраћом AS путањом.
5. Бира се путања са најмањим кодом порекла (*origin code*) ("*i*" је најмањи, "*e*" је наредни, и последњи је "?").
6. Бира се рута са најмањим MED атрибутом, ако исти AS оглашава могуће руте.
7. Бира се EBGP рута пре IBGP руте.
8. Бира се рута преко најближег IGP суседа, као рута са најмањом метриком.
9. Бира се најстарија рута.
10. Бира се путања преко суседа са најмањим *router-ID*.
11. Бира се путања преко суседа са најмањом IP адресом. [7]

Уколико се одабир руте не реализује једним кораком, онда се прелази на следећи корак, и све тако док се не одабере најбоља рута.

2.9. Манипулација BGP атрибутима коришћењем мапа рутирања

Манипулацијом и променом BGP атрибута може се утицати на одабир најбоље путање. BGP протокол никада није био дизајниран са циљем одабира најбрже путање, већ да се управља мрежним саобраћајем како би се смањио или повећао проток на одређеном линку. Све ово је, наравно, могуће уколико постоји две или више конекција ка другим аутономним системима. Коришћењем мапа рутирања (*route maps*) и променама BGP атрибута регулише се који ће саобраћај бити послат на који излазни линк из аутономног система, као и преко ког рутера ће који саобраћај улазити у аутономни систем.

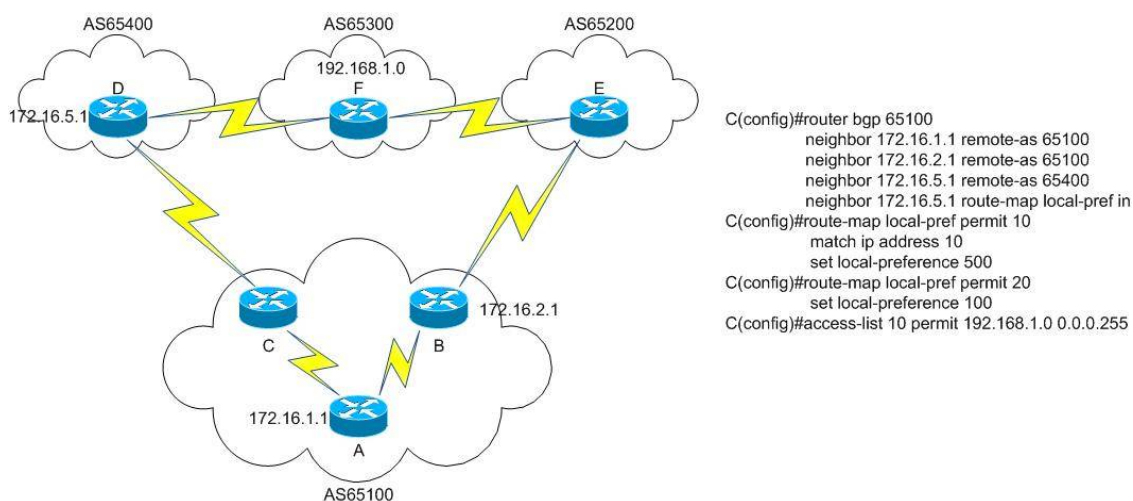
Употребом мапа рутирања могуће је утицати на вредност *weight* атрибута и мењати га по потреби. На Слици 16 приказан је пример како је могуће подесити вредност поменутог атрибута у зависности од саобраћаја.



Слика 16: Употреба мапе рутирања при промени *weight* атрибута

Мапом рутирања, приказаном на горњој слици, врши се промена вредности *weight* атрибута за саобраћај, који је намењен било којој мрежи, која се налази у AS65300. У овом случају се суседни рутер B, из AS 65200, узима као примарни рутер за излазни саобраћај из AS 65100, а који је намењен некој мрежи из AS 65300. Ово се постиже постављањем вредности *weight* атрибута на 150 за све објављене руте од AS 65200, а које носе информације о мрежи из AS 65300. Као резултат, сваки саобраћај намењен мрежи из AS 65300 биће послат преко AS 65200.

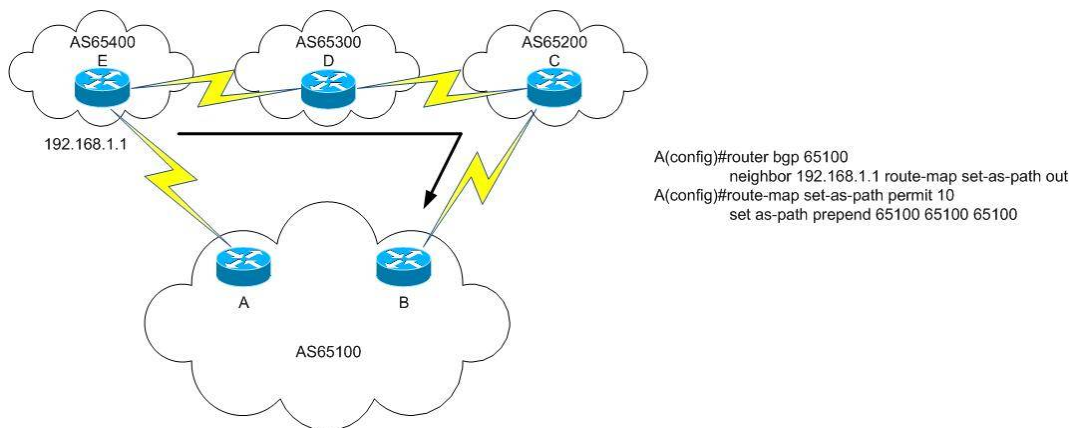
Атрибут *local preference* користи се искључиво унутар једног AS, између BGP рутера, како би се одабрала најбоља излазна путања из AS за саобраћај намењен некој мрежи, која је ван AS.



Слика 17: Употреба мапе рутирања при промени атрибута *local preference*

На Слици 17 приказана је мапа рутирања, у којој се врши промена вредности атрибута *local preference*. Рутер C остварује BGP конекцију са рутерима A, B и D. Овом мапом рутирања се на рутеру C подешава атрибут *local preference* на свим рутама ка дестинационој мрежи 192.168.1.0, а које су добијене од рутера D. Руте за мрежу 192.168.1.0 рутер C размењује унутар AS 65100 са осталим рутерима, тако да ће саобраћај намењен овој мрежи, из AS 65100 бити прослеђиван преко рутера C ка рутеру D (AS 65400) зато што руте имају подешену већу вредност атрибута *local preference*. У овом случају је то вредност 500.

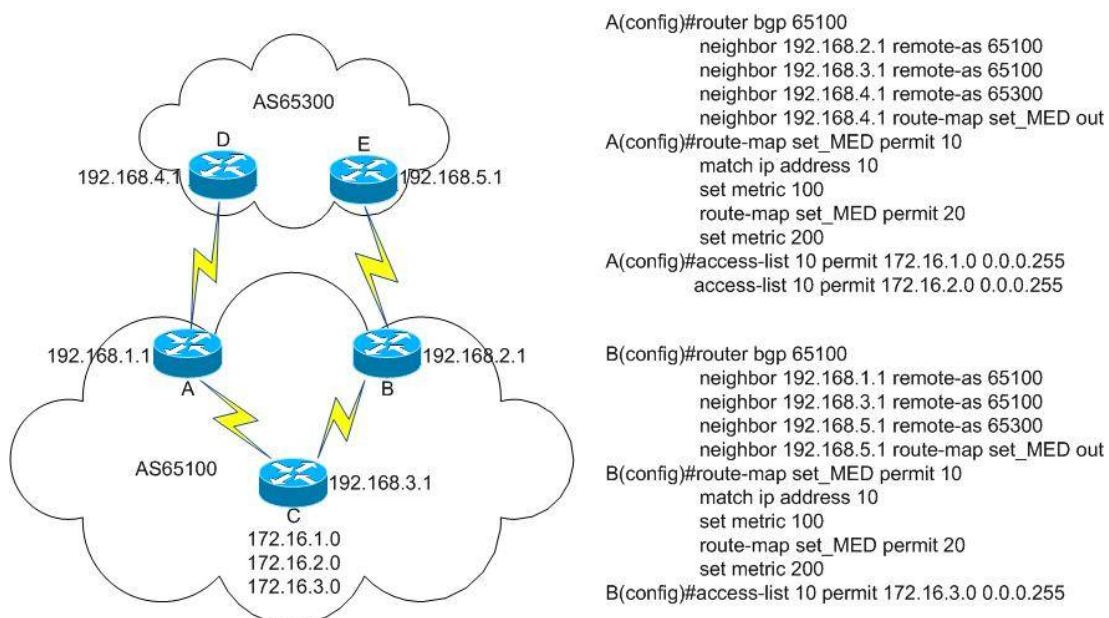
Такође, подешавањем *AS-path* атрибута, може се утицати на путању мрежног саобраћаја. На Сlici 18 приказан је пример подешавања *AS-path* атрибута, чиме се мења ток саобраћаја у мрежи.



Слика 18: Подешавање и употреба *AS-path* атрибута

Рутер А шаље *update* поруке ка суседном рутеру Е, тако што их процесуира излазном мапом рутирања, којом подешава *AS-path* атрибут, тако што у путањи додаје три пута број АS пошиљаоца, чиме ту путању чини мање прихватљивом. Стога, рутер Е ће за сваки саобраћај намењен за АS 65100, користити путању АS65300-АS65200-АS65100.

Подешавањем вредности MED атрибута може се утицати на то која ће бити улазна путања саобраћаја у неки АS, када тај АS има бар две конекције са другим АS. Тиме АS утиче на путању саобраћаја који њему шаље други АS. MED атрибут се може подешавати и на нивоу појединачне руте.



Слика 19: Подешавање и употреба MED атрибута

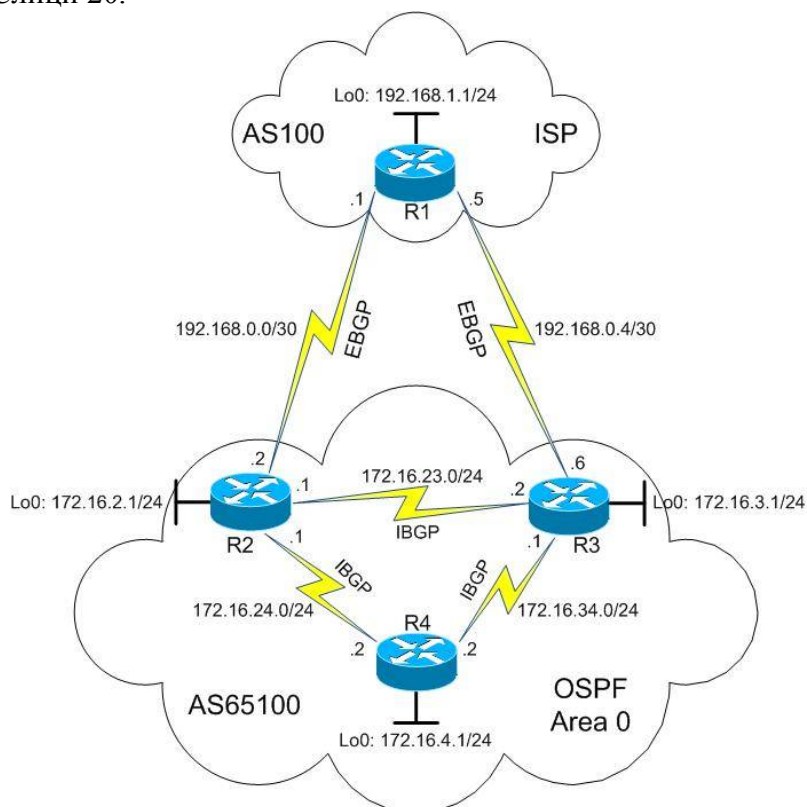
Датим примером са Сlike 19, приказано је подешавање вредности MED атрибута. Рутер А подешава MED атрибут на вредност 100 код рута за мреже 172.16.1.0 и 172.16.2.0. Обзиром да је у сваком другом случају вредност MED атрибута 200, онда ће

сваки саобраћај намењен мрежама 172.16.1.0 и 172.16.2.0, ући у AS 65100 преко рутера А. Рутер В подешава MED атрибут на вредност 100 код руте за мрежу 172.16.3.0. Обзиром да је у сваком другом случају вредност MED атрибута 200, онда ће сваки саобраћај намењен мрежи 172.16.3.0, ући у AS 65100 преко рутера В.

3. Имплементација BGP решења

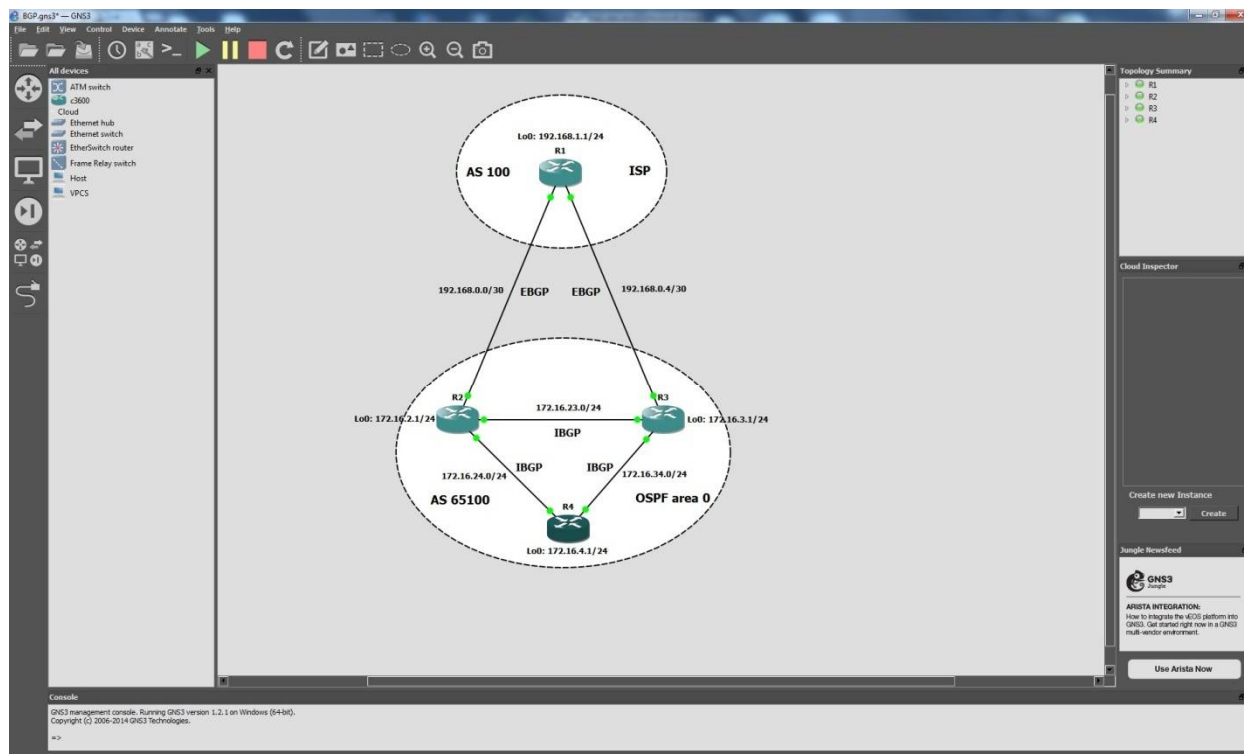
Као пример имплементације биће обрађено повезивање једног AS са ISP, коришћењем и редувантне конекције, што представља *dual-homed* конекцију. У имплементацији биће обрађен пример повезивања AS са једним ISP, што је веома слично и реализацији *multi-homed* конекције са два ISP. У том случају би два ISP међусобно комуницирала путем Интернет мреже, коришћењем неког од протокола рутирања.

Имплементација је реализована на конекцији приватног AS са ISP, чија је топологија приказана на Слици 20.



Слика 20: Топологија мреже практичног решења

Практично решење реализовано је у програмском пакету GNS3, верзије 1.2.1. У имплементацији, коришћени су рутери CISCO серије 3600. Мрежна топологија и поменутом програму изгледа на следећи начин:



Слика 21: Приказ топологије мреже из програмског пакета GNS3

Као што је приказано на претходној слици топологије практичног решења, приватни AS65100 чине три рутера CISCO серије 3600, који међу собом размењују табеле рутирања коришћењем динамичког протокола рутирања OSPF. Обзиром да се сва три рутера налазе у истом AS, међу њима је реализован и IBGP. Приватни AS65100 повезан је са ISP коришћењем две конекције. ISP је у овом решењу приказан као један рутер CISCO серије 3600. Са становишта приватног AS65100 не би се променила логика чак и да је ISP представљен са два рутера.

Да би се реализовала EBGП конекција између приватног AS и ISP, потребно је претходно извршити потребну конфигурацију свих уређаја. Прво, неопходно је конфигурисати потребне интерфејсе на свим рутерима. Конфигурација интерфејса рутера R1 (ISP) приказана је на Слици 22:

```
interface Loopback0
description LAN
ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/0
description Link ka R2
ip address 192.168.0.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
description Link ka R3
ip address 192.168.0.5 255.255.255.252
duplex auto
speed auto
!
```

Слика 22: Конфигурација интерфејса на рутеру R1

Конфигурација интерфејса рутера R2 приказана је на Слици 23:

```

interface Loopback0
  description LAN
  ip address 172.16.2.1 255.255.255.0
!
interface FastEthernet0/0
  description Link ka R1(ISP)
  ip address 192.168.0.2 255.255.255.252
  duplex auto
  speed auto
!
interface FastEthernet1/0
  description Link ka R3
  ip address 172.16.23.1 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet2/0
  description Link ka R4
  no switchport
  ip address 172.16.24.1 255.255.255.0
!

```

Слика 23: Конфигурација интерфејса на рутеру R2

Конфигурација интерфејса рутера R3 приказана је на Слици 24:

```

interface Loopback0
  description LAN
  ip address 172.16.3.1 255.255.255.0
!
interface FastEthernet0/0
  description Link ka R1(ISP)
  ip address 192.168.0.6 255.255.255.252
  duplex auto
  speed auto
!
interface FastEthernet1/0
  description Link ka R2
  ip address 172.16.23.2 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet2/0
  description Link ka R4
  no switchport
  ip address 172.16.34.1 255.255.255.0
!

```

Слика 24: Конфигурација интерфејса на рутеру R3

Конфигурација интерфејса рутера R4 приказана је на Слици 25:

```

interface Loopback0
description LAN
ip address 172.16.4.1 255.255.255.0
!
interface FastEthernet0/0
description Link ka R2
ip address 172.16.24.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/0
description Link ka R3
ip address 172.16.34.2 255.255.255.0
duplex auto
speed auto
!

```

Слика 25: Конфигурација интерфејса на рутеру R4

Након основних подешавања рутера, потребно је подесити протокол рутирања на рутерима у AS65100. Конфигурација OSPF протокола рутирања на рутеру R2 приказана је на слици 26:

```

router ospf 1
log-adjacency-changes
network 172.16.2.0 0.0.0.255 area 0
network 172.16.23.0 0.0.0.255 area 0
network 172.16.24.0 0.0.0.255 area 0
!

```

Слика 26: Конфигурација OSPF протокола на рутеру R2

Конфигурација OSPF протокола рутирања на рутеру R3 приказана је на слици 27:

```

router ospf 1
log-adjacency-changes
network 172.16.3.0 0.0.0.255 area 0
network 172.16.23.0 0.0.0.255 area 0
network 172.16.34.0 0.0.0.255 area 0
!

```

Слика 27: Конфигурација OSPF протокола на рутеру R3

Конфигурација OSPF протокола рутирања на рутеру R4 приказана је на слици 28:

```

router ospf 1
log-adjacency-changes
network 172.16.4.0 0.0.0.255 area 0
network 172.16.24.0 0.0.0.255 area 0
network 172.16.34.0 0.0.0.255 area 0
!

```

Слика 28: Конфигурација OSPF протокола на рутеру R4

Функционисање OSPF протокола рутирања на рутерима у AS65100, омогућава несметано функционисање IBGP унутар AS. Да би IBGP функционисао унутар AS65100, потребно је подесити одређене параметре BGP протокола на рутерима R2, R3 и R4.

Између два аутономна система, у овом случају AS65100 и AS100 (ISP), потребно је извршити конфигурацију параметара везаних за BGP протокол.

Код подешавања, потребно је навести IP адресу суседа, са којим се остварује BGP конекција, број AS у коме се сусед налази, као и мреже које се оглашавају кроз BGP протокол. Конфигурација параметара BGP протокола на рутеру R1, приказана је на Слици 29.

```
router bgp 100
  no synchronization
  bgp log-neighbor-changes
  network 192.168.1.0
  neighbor 192.168.0.2 remote-as 65100
  neighbor 192.168.0.6 remote-as 65100
  no auto-summary
!
```

Слика 29: Конфигурација BGP протокола на рутеру R1

Конфигурација параметара BGP протокола на рутеру R2, приказана је на Слици 30.

```
router bgp 65100
  no synchronization
  bgp log-neighbor-changes
  network 172.16.2.1 mask 255.255.255.255
  network 172.16.3.1 mask 255.255.255.255
  network 172.16.4.1 mask 255.255.255.255
  network 172.16.23.0 mask 255.255.255.0
  network 172.16.24.0 mask 255.255.255.0
  network 172.16.34.0 mask 255.255.255.0
  neighbor 172.16.3.1 remote-as 65100
  neighbor 172.16.3.1 update-source Loopback0
  neighbor 172.16.4.1 remote-as 65100
  neighbor 172.16.4.1 update-source Loopback0
  neighbor 192.168.0.1 remote-as 100
  no auto-summary
!
```

Слика 30: Конфигурација BGP протокола на рутеру R2

Конфигурација параметара BGP протокола на рутеру R3, приказана је на Слици 31.

```
router bgp 65100
  no synchronization
  bgp log-neighbor-changes
  network 172.16.2.1 mask 255.255.255.255
  network 172.16.3.1 mask 255.255.255.255
  network 172.16.4.1 mask 255.255.255.255
  network 172.16.23.0 mask 255.255.255.0
  network 172.16.24.0 mask 255.255.255.0
  network 172.16.34.0 mask 255.255.255.0
  neighbor 172.16.2.1 remote-as 65100
  neighbor 172.16.2.1 update-source Loopback0
  neighbor 172.16.4.1 remote-as 65100
  neighbor 172.16.4.1 update-source Loopback0
  neighbor 192.168.0.5 remote-as 100
  no auto-summary
!
```

Слика 31: Конфигурација BGP протокола на рутеру R3

Конфигурација параметара BGP протокола на рутеру R4, приказана је на Слици 32.

```
router bgp 65100
  no synchronization
  bgp log-neighbor-changes
  network 172.16.4.1 mask 255.255.255.255
  neighbor 172.16.2.1 remote-as 65100
  neighbor 172.16.2.1 update-source Loopback0
  neighbor 172.16.3.1 remote-as 65100
  neighbor 172.16.3.1 update-source Loopback0
  no auto-summary
!
```

Слика 32: Конфигурација BGP протокола на рутеру R4

Након успоставе BGP конекција међу рутерима, долази до размене информација између BGP суседа. Тиме долази и до промена у табелама рутирања рутера, који учествују у конекцији. На Слици 33 приказан је изглед табеле рутирања рутера R1 (ISP).

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
B       172.16.34.0/24 [20/0] via 192.168.0.6, 00:52:56
B       172.16.24.0/24 [20/0] via 192.168.0.2, 00:53:23
B       172.16.23.0/24 [20/0] via 192.168.0.2, 00:53:23
B       172.16.4.1/32 [20/2] via 192.168.0.2, 00:53:23
B       172.16.3.1/32 [20/2] via 192.168.0.2, 00:53:23
B       172.16.2.1/32 [20/2] via 192.168.0.6, 00:52:56
    192.168.0.0/30 is subnetted, 2 subnets
C       192.168.0.0 is directly connected, FastEthernet0/0
C       192.168.0.4 is directly connected, FastEthernet1/0
C       192.168.1.0/24 is directly connected, Loopback0
R1#
```

Слика 33: Табела рутирања рутера R1

Из претходне табеле види се које је руте рутер R1 научио од BGP суседа. Те руте означене су словом B испред руте у табели рутирања. На Слици 34, као пример, приказана је табела рутирања рутера R2.

```

R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
O       172.16.34.0/24 [110/2] via 172.16.24.2, 00:58:50, FastEthernet2/0
        [110/2] via 172.16.23.2, 00:58:50, FastEthernet1/0
C       172.16.24.0/24 is directly connected, FastEthernet2/0
C       172.16.23.0/24 is directly connected, FastEthernet1/0
O       172.16.4.1/32 [110/2] via 172.16.24.2, 00:58:50, FastEthernet2/0
O       172.16.3.1/32 [110/2] via 172.16.23.2, 00:58:50, FastEthernet1/0
C       172.16.2.0/24 is directly connected, Loopback0
    192.168.0.0/30 is subnetted, 1 subnets
C       192.168.0.0 is directly connected, FastEthernet0/0
B       192.168.1.0/24 [20/0] via 192.168.0.1, 00:58:22
R2#

```

Слика 34: Табела рутирања рутера R2

У табели рутирања рутера R2 примећујемо да постоји само једна рута научена путем BGP протокола, и то путем EBGP. Административна дистанца EBGP протокола је 20. Руте унутар AS65100 нису научене и уписане у табелу рутирања путем IBGP јер административна дистанца IBGP износи 200, док административна дистанца OSPF износи 110. У том случају, приоритет имају руте OSPF протокола због ниже вредности административне дистанце.

На Слици 35 и Слици 36 приказани су неки од BGP параметара, где се могу видети и суседи рутера R1 и R2, верзија BGP протокола коју рутери користе, као и AS коме њихови суседи припадају.

```

R1#sh ip bgp summary
BGP router identifier 192.168.1.1, local AS number 100
BGP table version is 9, main routing table version 9
7 network entries using 819 bytes of memory
11 path entries using 572 bytes of memory
4/3 BGP path/bestpath attribute entries using 496 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1911 total bytes of memory
BGP activity 7/0 prefixes, 11/0 paths, scan interval 60 secs

Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.0.2    4 65100     74     77      9    0   0 01:09:55      5
192.168.0.6    4 65100     74     77      9    0   0 01:09:56      5
R1#

```

Слика 35: BGP на рутеру R1

```

R2#sh ip bgp summary
BGP router identifier 172.16.2.1, local AS number 65100
BGP table version is 7, main routing table version 7
6 network entries using 702 bytes of memory
10 path entries using 520 bytes of memory
7/3 BGP path/bestpath attribute entries using 868 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2114 total bytes of memory
BGP activity 6/0 prefixes, 10/0 paths, scan interval 60 secs

Neighbor      V    AS MsgRcvd MsgSent   TblVer   InQ OutQ Up/Down State/PfxRcd
172.16.3.1    4 65100     81      81       7    0   0 01:14:05         4
172.16.4.1    4 65100     77      81       7    0   0 01:14:07         0
192.168.0.1   4   100     82      79       7    0   0 01:14:33         1
R2#

```

Слика 36: BGP на рутеру R2

BGP руте, метрику, као и AS путање на рутерима R1 и R2, могу се видети на Слици 37, односно Слици 38.

```

R1#sh ip bgp
BGP table version is 9, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
*> 172.16.2.1/32   192.168.0.6          2             0 65100 i
*> 172.16.3.1/32   192.168.0.2          2             0 65100 i
* 172.16.4.1/32   192.168.0.6          2             0 65100 i
*>                192.168.0.2          2             0 65100 i
* 172.16.23.0/24  192.168.0.6          0             0 65100 i
*>                192.168.0.2          0             0 65100 i
* 172.16.24.0/24  192.168.0.6          2             0 65100 i
*>                192.168.0.2          0             0 65100 i
*> 172.16.34.0/24  192.168.0.6          0             0 65100 i
*                  192.168.0.2          2             0 65100 i
*> 192.168.1.0    0.0.0.0              0            32768 i
R1#

```

Слика 37: BGP руте, метрика и AS путање на рутеру R1

```

R2#sh ip bgp
BGP table version is 7, local router ID is 172.16.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
*> 172.16.3.1/32   172.16.23.2          2            32768 i
* i172.16.4.1/32  172.16.34.2          2          100    0 i
*>                172.16.24.2          2            32768 i
* i172.16.23.0/24 172.16.3.1           0          100    0 i
*>                0.0.0.0             0            32768 i
*> 172.16.24.0/24  0.0.0.0             0            32768 i
* i172.16.34.0/24 172.16.3.1           0          100    0 i
*>                172.16.23.2          2            32768 i
* i192.168.1.0    192.168.0.5          0          100    0 100 i
*>                192.168.0.1          0            0 100 i
R2#

```

Слика 38: BGP руте, метрика и AS путање на рутеру R2

На Слици 37 приказано је да рутер R1 све информације о рутама добија од суседа R2 и R3, што показује параметар *Next-hop*, а доказује и *Path* параметар где стоји да је за све руте путања (65100, i), што значи да руте настају у AS65100. На Слици 38 су приказани исти параметри за рутер R2, где видимо да информације о мрежи 192.168.1.0 добија од суседа из AS100, док су остале руте интернет, тј. учи их од рутера из сопственог AS.

На рутерима R2 и R3 у AS65100 можемо подесити *local preference* атрибут за руте, које се уче од рутера R1. У том случају за AS65100 бирамо излазни рутер када је саобраћај намењен некој од мрежа, за које информације шаље рутер R1. Као пример, за све руте које оглашава рутер R1, на рутеру R2 подешен је *local preference* атрибут на вредност 200, а на рутеру R3 на вредност 150.

```
route-map set_loc_pref permit 10
set local-preference 200
```

Слика 39: Подешавање BGP атрибута *local preference* на рутеру R2

```
route-map set_loc_pref permit 10
set local-preference 150
```

Слика 40: Подешавање BGP атрибута *local preference* на рутеру R3

Након креирања *route-map* за подешавање *local preference* атрибута на рутеру R2, командом **neighbor 192.168.0.1 route-map set_loc_pref in** примењујемо је за све информације о рутама, које стижу од суседа са адресом 192.168.0.1. Након креирања *route-map* за подешавање *local preference* атрибута на рутеру R3, командом **neighbor 192.168.0.5 route-map set_loc_pref in** примењујемо је за све информације о рутама, које стижу од суседа са адресом 192.168.0.5.

У овом случају сав саобраћај из AS65100 који је намењен мрежи 192.168.1.0, биће послат преко рутера R2, као излазном рутеру из AS65100. Ово можемо утврдити на основу BGP табела рутера R2 и R3, које су приказане на Слици 41, односно Слици 42.

```
R2#sh bgp
BGP table version is 13, local router ID is 172.16.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
* 1172.16.0.0      172.16.3.1             0    100      0 i
*>                 0.0.0.0                0           32768 i
r> 192.168.0.0/30  192.168.0.1            0    200      0 100 i
*> 192.168.0.4/30  192.168.0.1            0    200      0 100 i
*> 192.168.1.0     192.168.0.1            0    200      0 100 i
R2#
```

Слика41: BGP табела рутера R2

```
R3#sh bgp
BGP table version is 927, local router ID is 172.16.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
* 1172.16.0.0      172.16.2.1             0    100      0 i
*>                 0.0.0.0                0           32768 i
*>i192.168.0.0/30  172.16.2.1             0    200      0 100 i
*                  192.168.0.5            0    150      0 100 i
r>i192.168.0.4/30  172.16.2.1             0    200      0 100 i
r                  192.168.0.5            0    150      0 100 i
*>i192.168.1.0     172.16.2.1             0    200      0 100 i
*                  192.168.0.5            0    150      0 100 i
R3#
```

Слика 42: BGP табела рутера R3

На Слици 41 и Слици 42 приказано је да рутери R2 и R3 одабирају руте са већим атрибутом *local preference* као најбоље и њих уводе у табеле рутирања, тако да ће се саобраћај намењен дестинационим мрежама кретати преко адреса означених као *Next*

Нор. Ово је приказано примером на Слици 43, где је приказана *traceroute* команда и путања кретања пакета насталим на рутеру R3, а који су намењени дестинационој адреси 192.168.1.1.

```
R3#traceroute 192.168.1.1

Type escape sequence to abort.
Tracing the route to 192.168.1.1

 1 172.16.23.1 68 msec 68 msec 32 msec
 2 192.168.0.1 [AS 100] 124 msec 92 msec 96 msec
R3#
```

Слика 43: Путања пакета од R3 ка адреси 192.168.1.1

На основу Слике 43, види се која је путања одлазних пакета, али није засигурно којом се путањом ти пакети враћају до рутера R3. Повратна путања се може утврдити на основу табеле рутирања рутера R1. Табела рутирања рутера R1 приказана је на Слици 44.

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B    172.16.0.0/16 [20/0] via 192.168.0.6, 02:44:32
     192.168.0.0/30 is subnetted, 2 subnets
C      192.168.0.0 is directly connected, FastEthernet0/0
C      192.168.0.4 is directly connected, FastEthernet1/0
C      192.168.1.0/24 is directly connected, Loopback0
R1#
```

Слика 44: Табела рутирања рутера R1

На основу табеле рутирања рутера R1, повратни пакети се шаљу директно рутеру R3. Да бисмо искориговали повратну путању пакета, тј. да би се пакети враћали истом путањом, потребно је подесити MED атрибут BGP протокола, који дефинише путању улазног саобраћаја у приватни AS.

На рутерима R2 и R3 у AS65100 може се подесити *MED* атрибут за руте, које рутери R2 и R3 шаљу ка рутеру R1 (ISP). У том случају за AS65100 бирамо улазну путању, односно улазни рутер када је саобраћај намењен некој од мрежа у AS65100. Као пример, за све руте које оглашава рутер R2 ка рутеру R1, подешен је *MED* атрибут на вредност 50, а на рутеру R3 ка рутеру R1 на вредност 70. Овим ће рутер R1 саобраћај намењен за AS65100 увек прослеђивати преко рутера R2, јер руте које стижу од рутера R2 имају мању вредност *MED* атрибута, у односу на рутер R3.

```
route-map set_med permit 10
 set metric 50
```

Слика 45: Подешавање MED атрибута на рутеру R2

```
route-map set_med permit 10
set metric 70
```

Слика 46: Подешавање MED атрибута на рутеру R3

Након креирања *route-map* за подешавање *MED* атрибута на рутеру R2, командом **neighbor 192.168.0.1 route-map set_med out** примењујемо је за све информације о рутама, које се шаљу ка суседу R1 са адресом 192.168.0.1. Након креирања *route-map* за подешавање *MED* атрибута на рутеру R3, командом **neighbor 192.168.0.5 route-map set_med out** примењујемо је за све информације о рутама, које се шаљу ка суседу R1 са адресом 192.168.0.5. Овим конфигурацијама се подешава преко ког рутера ће повратни пакети ући у приватни AS. У овом случају ће то бити преко рутера R2, што се види по BGP табели рутера R1, на Слици 47.

```
R1#sh bgp
BGP table version is 10, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
*> 172.16.0.0      192.168.0.2             50           0 65100 i
*                  192.168.0.6             70           0 65100 i
*> 192.168.0.0/30  0.0.0.0                 0           32768 i
*> 192.168.0.4/30  0.0.0.0                 0           32768 i
*> 192.168.1.0    0.0.0.0                 0           32768 i
```

Слика 47: BGP табела рутера R1

4. Рањивости BGP протокола и ризици од могућих напада

Уколико се коришћење Интернет мреже у једној организацији повећава, оно уједно постаје и најкритичнији део активности саме организације. Ове активности захтевају од обичног слања и пријема електронске поште па све до хостовања комплексних веб сајтова и употребе Интернет сервиса. Иако се грешке и проблеми могу јавити у било ком сегменту Интернет мреже, код многих организације најчешћи проблем се јавља на физичком линку ка ISP.

У неким случајевима ISP даје поједине гаранције како би могућност финансијских губитака била веома мала. Организација повећава своју сигурност додавањем редувантног линка. Многи ISP нуде редувантне линкове и мрежну опрему, па чак и редувантни линк ка различитој прикључној тачки њихове мреже. Ово може бити врло скупо, а уколико дође до прекида линка ISP ка остатку Интернет мреже, онда и мрежа организације остаје без Интернет приступа. Решење овог појединачног проблема може бити и реализација Интернет конекције ка два различита ISP. Овај начин повезивања штити организацију од проблема са конекцијама. Тада би организација користила BGP протокол за рутирање саобраћаја, као и свој сопствени адресни опсег. Уколико би дошло до прекида једне BGP конекције, не би дошло до прекида TCP/IP сесије, већ би BGP рутер прерутирао саобраћај на конекцију, која је у функцији. Конвергенција BGP рута је мања и од 30 секунди. Не би се приметиле промене и прекиди приликом преласка на секундарну конекцију. [8]

4.1. Безбедносни напади на BGP рутер и BGP конекцију

BGP рутер за конекцију са ISP налази се са спољне стране *firewall* уређаја, и самим тим има мањи ниво заштите у односу на уређаје унутар мреже. Рутер на оваквој позицији представља најкритичнији уређај, који је уједно и најподложнији нападима јер кроз њега пролази сав улазни и излазни саобраћај једног AS. Уколико се на рутеру не филтрирају руте пажљиво, могу се створити проблеми на тој али и другим мрежама Интернета. [8]

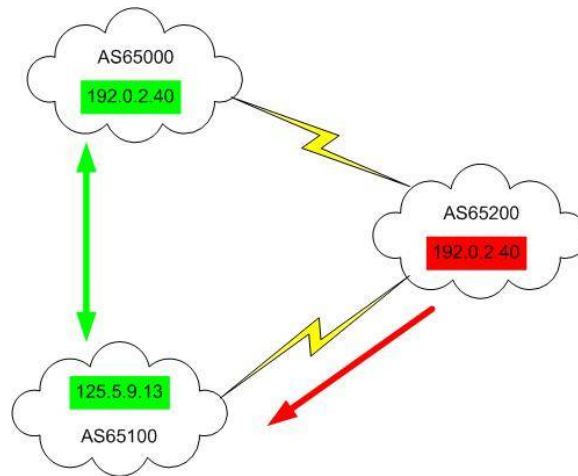
BGP протоколу рутирања углавном недостају поједине провере како би се дошло до одређених безбедносних гаранција. Неке од њих су:

- Непостојање аутентикације од самог старта
- BGP нема могућност провере да ли је порука, примљена у оквиру *update* поруке, модификована
- Непостојање механизма провере да ли оглашени префикси у оквиру поруке припадају оглашивачу или су ауторизоване од стране оглашивача
- Непостојање механизма за проверу исправности атрибута путање, који су придружени *update* поруци
- У случају повлачења рута мора постојати могућност потврде да је исти BGP рутер ту руту претходно и огласио. [11]

4.2. *Spoofing*

Оваква врста напада јавља се тамо где се имитира BGP сусед. Много Интернет напада се деси у којима нападач користи лажну IP адресу. Да би нападач користио IP адресу

мреже коју напада, прво врши скенирање мреже, да би скенирао сервисе преко којих може да ући у мрежу. Коришћење маскиране IP адресе даје нападачу могућност неауторизованог приступа уређају или некој апликацији. Чак су и неке BGP рањивости у овој категорији напада.



Слика 48: *Spoofing* напад

На Слици 48 дат је пример регуларне комуникације између два аутономна система. Нападач, који је конектован на другу мрежу, може слати пакете са изворишном IP адресом једног од учесника у комуникацији. У овакве врсте напада спадају и следећи:

- Напади на апликације, које су базиране само на ауторизацији по изворишној IP адреси долазног пакета
- Rsh, rlogin, NFS, Xwindows...
- Напади где може бити експлоатисана недоступност извора
- TCP SYN плављење које исцрпљује ресурсе на серверу
- Напади где се нападач представља као жртва
- Мали DNS и SNMP захтеви, који узрокују асиметрични ток података ка жртви
- Увредљив саобраћај, који узрокује да легитиман корисник буде блокиран од стране сервера или мреже [9]

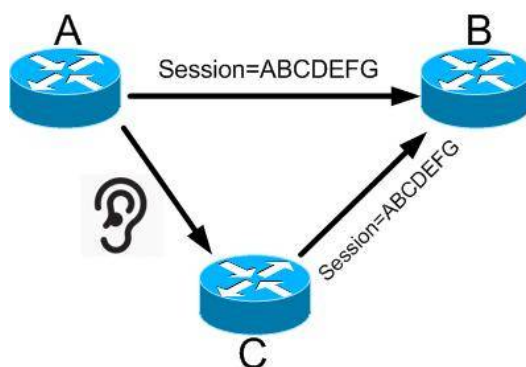
Променом IP адресе, хост рутер нападача може остварити BGP сесију са другим рутером и тиме са њим размењивати BGP *update* поруке. Кроз ове поруке хост BGP рутер може послати дестинационом BGP рутеру погрешан запис што би узроковало нестабилност рута. *Time to live* (TTL) представља важну компоненту пакета и пакет треба достићи дестинацију у оквиру тог времена. Обзиром да су BGP суседи директно конектовани, онда је TTL=1. Хост BGP рутер може у свом нападу променити и TTL на већу вредност, што би довело до одбацивања тих пакета, а самим тим и до прекида BGP сесије између рутера. [10]

Да би се *spoofing* успешно реализовао над TCP сесијом два BGP рутера, потребно је имитирати изворишну IP адресу и изворишни порт. Адреса се обично одреди на основу ICMP *traceroute* пакета са различитих Интернет локација ка одређеном BGP рутеру. Ова врста мапирања је напреднија, и захтева разумевање како рутирање и BGP суседи функционишу на Интернет мрежи. BGP сусед обично шаље захтев са дестинационим портом 179, што значи да ће тај порт користити BGP рутер који напада, као изворишни

порт. Поред изворишне адресе и порта, потребно је да се поклопи и TCP *sequence number* и TTL. [12]

4.3. Преузимање сесије (*Session hijacking*)

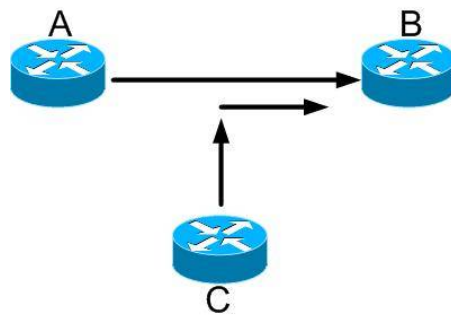
Session hijacking представља једну од првих BGP напада, чију тачку напада представља уствари сама сесија између два BGP рутера, који остварују BGP конекцију. BGP сесија заснована је на TCP протоколу, где се преносе и веб странице, фајлови и друге информације. Код оваквих напада, *host* може преузети постојећу сесију између два BGP суседа. До овога може доћи ако сесија није криптована. Самим преузимањем сесије, *host* може убацивати нове или мењати постојеће информације рутирања. Чак се може понашати и као “*man-in-the-middle*” и тако мењати информације рутирања, које размењују BGP суседи. Тополошки приказ *session hijacking* напада дат је на Слици 49. [9]



Слика 49: Тополошки приказ *session hijacking* напада

4.4. *Route flapping*

Код овог типа напада AS постаје *man-in-the-middle* између два BGP суседа и успешно оглашава модификоване или погрешне информације кроз BGP поруку, која пролази кроз аутономни систем суседног рутера, што је приказано на Слици 50. Поруке рутера C узрокују нестабилност рута код рутера B, што може довести и до привременог престанка исправног функционисања. Тада се јављају и велика кашњења у достављању порука.



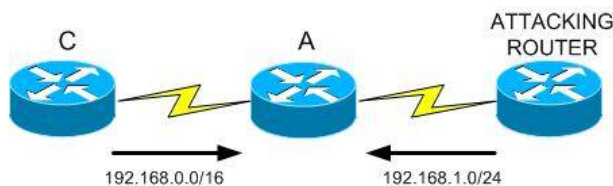
Слика 50: Рутер С изазива *flapping*

Route flapping може довести и до проблема у глобалним табелама рутирања на Интернет мрежи. Може се догодити да нека рута нестане из табела рутирања или чак да се и додају неке нове, погрешне, руте. Тада долази до непрестаног прерачунавања најбољих рута од стране рутера, што доводи до оптерећења рутера и кашњења доставе порука. У неким тренуцима пакети не могу ни стићи до дестинационе мреже, чиме се ствара ефекат “црних рупа”. [10]

4.5. *Route de-aggregation*

Представља оглашавање специфичнијих BGP рута, са дужим префиксом, уместо сумарних рута од стране суседног AS. *De-aggregation* саме табеле рутирања пропагира се веома брзо преко Интернет мреже, узрокујући велике проблеме код рутера, па чак и престанак њиховог рада. [10]

Када рутер прими специфичнију руту, радије ће користити ту информацију рутирања од било ког другог начина одабира путање рутирања. Као што је приказано на Слици 51, легитимни рутер С оглашава руту 192.168.0.0/16 ка рутеру А, док рутер са кога се врши напад оглашава специфичнију руту 192.168.1.0/24 ка рутеру А. Рутер А ће у овом случају инсталирати обе руте у табелу рутирања, али ће пре користити руту 192.168.1.0/24 због правила поклапања дужег префикса.



Слика 51: Пример *de-aggregation* напада

Оглашавање специфичнијих рута, уз погрешну конфигурацију, представља највећи узрок већине прекида у функционисању у историји BGP протокола. [11]

4.6. *Unallocated route injection*

Ови типови напада односе се на трансмисију рута, које садрже неауторизоване префиксе. Ови специфични префикси представљају сетове IP адреса, које су резервисане за специјалне намене и не би требало да се пропагирају и оглашавају у сврху јавног рутирања. [10]

Опсежи адреса, који не би требало да се појаве у глобалном рутирању Интернет мреже су следећи:

- 0.0.0.0/8 i 0.0.0.0/32 – *default* и *broadcast*
- 127.0.0.0/8 – *host loopback*
- 192.0.2.0/24 – TEST-NET за документацију
- 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16 – приватне IP адресе
- 169.254.0.0/16 – DHCP аутоконфигурација крајњег уређаја
- 192.88.99.0/24 – *anycast* префикс за 6to4 рутере

Један од најважнијих задатака сваког ISP-а је да филтрира ове скупове адреса, како оне не би ушле или изашле из њихове мреже.

IP адресе издвојене су у документу RFC2050 – *Internet Registry IP Allocation Guidelines*. Нико на Интернет мрежи није власник IP адреса, већ су оне додељене на коришћење *Regional Internet Registries* (RIR), ISP и корисницима, као привремени ресурс. Корисници, који врше пресељење са једног на други ISP, не могу задржати исте IP адресе, већ ће код новог ISP добити нове IP адресе на коришћење. У овом случају, нападач који се конектује за BGP рутер може на основу табеле рутирања и BGP табеле сазнати локације појединих блокова IP адреса на Интернет мрежи.

4.7. *Denial of service (DoS)*

Пошто су рутери, на неки начин, специјализовани хостови, изложени су *Denial-of-Service* (DoS) нападима, као и други хостови или сервери. Ови напади се још зову и “SYN flood”. Код овог типа напада, нападач иницира велики број TCP/IP конекција, користећи SYN пакете. Овиме шаље велики број лажног саобраћаја суседним рутерима. Постоје три врсте оваквих напада. Једни настоје да исцрпе сав проток доступних интерфејса, чиме се смањује проток легитимног саобраћаја. Овим нападима се узрокује да рутери не успевају да приме информације рутирања или *keepalive* поруке од својих BGP суседа. У оваквим ситуацијама долази до прекида BGP сесије између два BGP суседа. Овакви су UDP плавање и рефлективни напади. Затим постоје напади који за циљ имају да исцрпе све ресурсе, као што су нпр. процесор, меморија или портови, тако да систем постаје све више заузет за одговоре. Овакви су TCP SYN напади. Трећу врсту представљају напади, који користе специјално креиране пакете, којима покушавају да сруше систем или га наведу да ради неочекивано. Овде спадају напади преоптерећења бафера. У оваквим ситуацијама може доћи до искључења или

рестарта процесора. Већина произвођача мрежне опреме не зна како да се носи са овом врстом напада. [9]

4.8. Погрешна конфигурација

Конфигурисање BGP рутера је веома комплексан и посао склон грешкама. Администратори мрежа тестирају све конфигурације у тестној мрежи пре саме примене у продукционој мрежи. Тиме се проверава утицај тих конфигурација на стабилност мреже. На пример, мала грешка у конфигурационом коду може довести до нестабилности рута.

Постоје грешке иницијализације, које узрокују грешке унутар самог софтвера BGP рутера. Рутери са оваквим грешкама оглашавају специфичније руте, а затим их сами обришу из табела рутирања након рестартовања рутера. Други вид грешака се јавља када, приликом уношења било каквих промена у конфигурацији рутера, администратор заборави да сачува нову конфигурацију рутера. Након рестартовања рутер учитава стару конфигурацију. Такође, грешка се може догодити приликом редистрибуције рута. Погрешном редистрибуцијом рута, може се десити оглашавање великог броја погрешних рута. Поједине грешке се јављају приликом погрешне сумаризације адреса. Погрешном сумаризацијом адреса може доћи до оглашавања већег скупа (опсега) IP адреса. Један AS може направити грешку уколико огласи руте, које припадају неком другом AS. У овом случају погрешно оглашене мреже постају *unreachable* (недостижне). [13]

5. Концепти заштите од појединих напада на BGP конекцију

Када говоримо о концептима заштите од напада описаних у претходној секцији, треба поменути да постоје технике заштите самог BGP рутера, али и заштите BGP протокола, односно саме BGP конекције.

5.1. Заштита BGP рутера

У данашње време, администраторима у великим организацијама, веома битну ствар чини креирање заштитних полиса на рутерима, који су изложени могућим нападима са Интернет мреже. Саму улогу рутера данас играју за то специјално креирани уређаји, док неки администратори врше инсталацију оперативног система рутера на рачунарима. У сваком случају, постоје неке основне ствари које треба да задовољи сам уређај, који има улогу рутера. Прво је потребно одредити начин на који ће администратор приступати рутеру. Затим је битно дефинисати начин аутентикације између администратора и рутера, као и начин на који ће се чувати приступне шифре на рутеру.

Традиционално, рутером се управља даљинским приступом путем *telnet* алата, али проблем представља што сама комуникација путем *telnet* алата није криптована и приступне шифре се шаљу конекцијом у отвореном тексту. Због овога, сви удаљени приступи рутеру треба да буду *secure shell* (SSH), а *telnet* треба бити деактивиран. Поред приступне шифре, треба да постоји и *enable* шифра. Ова шифра је најприближнија *root* налогу на *Linux* оперативном систему, и тако се треба поставити према њој. Према томе, сама приступна и *enable* шифра морају бити веома јаке. По *default*-у, IOS шифре се не складиште криптоване, и зато их треба криптовати посебном командом **service password-encryption** у глобалном конфигурационом моду.

У мрежи се BGP рутер налази ван главног *firewall*-а и његове заштите, те је потребно да се он посебно штити од скенирања и разних напада са Интернет мреже. Један од видова одбране BGP рутера јесу *Access Control Lists* (ACL). Оне представљају главно оружје за одбрану BGP рутера. Од саобраћаја ка овим рутерима треба дозволити искључиво SSH приступ са одређене радне станице, SNMP приступ од стране мрежних монитора за надзор, и евентуално ICMP саобраћај ради детекције и решавања проблема у мрежи. Поред овога, треба дозволити BGP комуникацију искључиво са IP адресе BGP суседа.

Поред горе наведених мера, постоје још неке мере заштите рутера. Потребно је да он буде инсталиран у заштићеној просторији, где само ауторизовани администратори имају приступ. Рутер треба бити конфигуриран са највише подржане меморије да би постојала могућност да се избегне DoS напад. Због могућности појаве проблема са напајањем електричном енергијом, потребно је да рутер буде прикључен на UPS уређај. Рутер на себи треба да има најновије верзије фирмвера и софтвера, који су на њему инсталирани.

5.2. Заштита од напада на BGP конекцију

Уколико мрежа једне организације има више конекција ка ISP и уједно користи BGP протокол да би остварила редувантни Интернет приступ, рутер мреже оглашава свој адресни опсег мреже и очекује да остале руте добије од својих BGP суседа. У овом случају не постоји транзитни саобраћај кроз мрежу те организације, и њихов рутер никада неће оглашавати друге мрежне IP опсеге.

Постоји могућност да BGP сусед огласи погрешну руту (*invalid route*) ка BGP рутеру, тако да рутер више неће бити у могућности да шаље саобраћај ка тој одређеној мрежи. Исти случај ће бити ако BGP сусед погрешно оглашава руту неке организације ка другим својим суседима, тако да тада мрежа те организације неће бити достижна (*reachable*).

Основна заштита против овакве врсте злоупотребе јесте филтрирање рута које BGP рутер једне организације треба да огласи ка свом BGP суседу, и обрнуто. Ови проблеми се првенствено решавају договором двеју страна о њиховим политикама и на тај начин се долази до одговора ком то саобраћају треба дозволити улаз и излаз у и из мреже. Поменути начин стопираће већину напада од стране нападача, који имитирају IP адресу BGP суседа и покушавају намерно да огласе погрешне руте.

Други начин заштите саме BGP конекције и комуникације између два BGP јесте аутентикација BGP *peer* рутера. Аутентикација између рутера конфигурише се коришћењем команде **neighbor 11.11.11.11 password cisco** унутар *router BGP* мода конфигурације. BGP протокол користи TCP уместо UDP и тиме је мање склон преузимању сесије (*session hijacking*) и *spoofing*-у од стране нападача. И поред аутентикације, и даље постоји могућност да се нападач претвара да је BGP коме се верује. Један од таквих напада је *man-in-the-middle*, где нападач поставља себе између два BGP суседа. Оно што представља предност нападачу јесте што рутери BGP суседа нису на истим физичким локацијама. Пошто различите организације имају различите политике и циљеве, обично се договор заврши на успостави најосновније аутентикације и енкрипције. Јака аутентикација и енкрипција могу да допринесу заштити BGP сесије од највећег броја напада. Уколико нека организација плаћа остваривање BGP *peer* сесије ка ISP, онда се налази и у позицији да може захтева да се користе јаки аутентикација и енкрипција. [8]

Једна од најбржих и најсигурнијих криптографских *hash* метода јесте аутентикација поруке. Ово се најчешће користи у комуникацији између два суседна BGP рутера. MD5 *key digest* у TCP заглављу и BGP подаци додају се у сваки пакет који се размењује у BGP комуникацији два суседа. Тиме се сваки сегмент TCP сесије проверава и верификује како би се порука заштитила од модификовања. Сесија између два BGP рутера неће се успоставити док се лозинке не подударе.



Слика 52: Криптована сесија

MD5 на BGP сесији ублажава највећи број *sniffing* претњи и онемогућава *spoofing* код BGP сесије. Коришћењем различитих кључева смањује се могућност “цурења” MD5 кључа.

Када се оствари BGP конекција, кључ сесије (тајни кључ) и *sequence* порука додају се како би се потврдило да је порука достављена BGP суседу у тачном редоследу. Размена тајног кључа између BGP суседа омогућује поузданост и интегритет BGP поруке (*keepalive* и *notification*).



Слика 53: Криптована порука у сесији

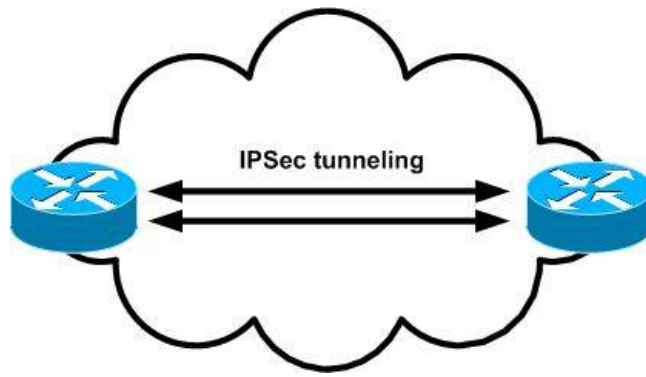
Број атрибута путање, који се налази у *update* поруци, размењује се приликом слања суседном BGP рутеру. Како би се заштитила ова *update* порука, она садржи *update sequence number*, нову и претходну AS_Path информацију и дигитални потпис.



Слика 54: Криптовање *update* поруке у сесији

Hop Integrity Protocol обезбеђује заштиту на IP слоју (трећем слоју OSI модела) чиме се остварује интегритет и редослед у пристизању пакета поруке. Овај протокол омогућује BGP *peer* рутерима да детектују модификовану поруку примљену од BGP суседа.

IPSec (*Internet Protocol Security*) представља *network layer* протокол који се користи за заштиту IP сесије између рутера, криптовањем и аутентикацијом криптографских сервиса заштите. Омогућава *end-to-end* сервисе заштите тако што врши криптовање IP заглавља и поља *payload*. За аутентикацију користи се *Authentication Header* (AH), који врши заштиту на IP слоју, док *Encapsulating Security Payload* (ESP) служи за криптовање података између BGP *peer* рутера. IPSec се примарно користи за обезбеђивање сервиса заштите у *Virtual Private Networks* (VPNs) и гарантује сигурност BGP сесија, али има ограничену заштиту када су у питању DoS напади. IPSec обезбеђује аутентикацију између BGP *peer* рутера, поверљивост и интегритет поруке. [10]



Слика 55: IPSec tunneling

Hashing алгоритми обезбеђују интегритет података на сесији између два рутера. *Standard Hashing Algorithm* (SHA-1) и *Message Digest* (MD5) представљају најчешће *hash* функције. Деле тајни кључ, који је ручно конфигурисан на обе стране сесије. Сесија између два BGP суседа неће бити остварена ако се ти кључеви не подударају. Енкрипција се заснива на вредности *hash*. Ова вредност се рачуна од улазног броја, који се затим користи за *hash* алгоритам. Скоро да је немогуће да се добије оригинални улазни број, који се транслира у исту *hash* вредност без познавања података који се користе за креирање *hash* вредности.

Message Authentication Code (MAC) се генерише комбинацијом тајног кључа и поруке. Такође је познат као *hash* функција са кључем. MAC вредност се прилаже уз поруку и обезбеђује интегритет поруке и аутентикацију. Страна која прима поруку познаје тајни кључ и биће у могућности да дође до оригиналне функције, како би верификовала аутентичност информације, која је генерисана од стране пошиљача.

Diffie-Hellman размена кључева представља криптографску методу, која користи два кључа: јавни, који је познат обема странама у комуникацији, и тајни, који је познат примаоцу поруке. Обе стране добијају резултат, који даље користе као *shared key*. *Diffie-Hellman* енкрипција се још назива и асиметрична енкрипција јер користи два кључа уместо један.

Public Key Infrastructure (PKI) омогућава да две стране сигурно деле информацију преко незаштићене јавне мреже. PKI обезбеђује дигитални сертификат за сваког појединца или организацију, који касније може бити опозван за валидирање интегритета поруке. У BGP сваки AS дели свој јавни кључ са другим AS, а тајни кључ са AS којима се верује. Тајни кључ се размењује преко заштићене комуникације коришћењем *Diffie-Hellman* алгоритма. Уколико AS хоће да валидира кључ другог AS, он опозива сертификат нивоа изнад, а уколико сертификат није доступан онда опозива сертификат нивоа изнад претходног. [10]

5.3. Заштита од импортовања и пропагације погрешних рута

Кључна заштита од уласка и пропагације нелегитимних рута и информација о рутирању у систем рутирања јесте филтрирање на нивоу префикса. Обично се филтери постављају на граничним рутерима ISP и корисничког AS. Овај метод подразумева листу рута и AS-ова, за које се очекује да буду достижни кроз конекцију са ISP.

Валидност информација у овој листи је веома битна, али постоји могућност да корисник намерно или случајно унесе погрешан префикс (руту). Овим се види да и филтер листа префикса остаје рањива уколико дође до вештачког импортовања рута. Ручна провера филтера, који имају и по неколико хиљада линија записа, са више стотина промена недељно, је веома тешка и дуготрајна. Уколико транзитни ISP филтрира оглашене префиксе својих корисника, као и префиксе свих других транзитних ISP којима се верује, онда се проблем настајања и пропагације погрешних рута скоро и елиминише. Ако се деси да неко приликом одржавања или конфигурисања филтера направи неку грешку, резултат је недоступност сервера или неких сервиса, што траје све док се грешка не пронађе и исправи.

Уместо префикс филтера неки ISP користе и AS_PATH филтере. Ово је још један вид одбране од импортовања и пропагације нелегалних рута. Као и сваки вид филтрирања, и овај је неадекватан за заштиту од погрешне конфигурације администратора. Раније је било доста проблема у процесу редистрибуције BGP рута у друге протоколе рутирања и обрнуто. AS_PATH филтери представљају веома користан вид заштите од “озбиљних цурења” рута. Код *update* порука корисничког AS, ISP у AS_PATH не очекује појаву AS бројева неких виших IPS. Мануално одржавање листи, које садрже очекиване записе, којима се верује, може бити склоно грешкама и некомплетно. Када се достигне праг максималног броја префикса, долази до прекида сесије, и потребна је ручна интервенција да би се сесија опет остварила. Уколико AS има конекције ка више ISP, долази до прекида свих сесија. Креирање и примена ових мера мора бити добро промишљена. Некада се може догодити да неке *update* поруке BGP суседа садрже и до 300.000 рута што узрокује заузеће меморије рутера. Уколико ти суседи шаљу велике сетове рута, од којих су многе *flapping* руте, онда и лимитирање максималног броја префикса доноси неки вид заштите.

Најбољи вид заштите од оваквих врста напада представљају улазна филтрирања рута ISP на својим граничним рутерима, као и излазна филтрирања рута на граничним рутерима корисничких мрежа. Као други вид заштите ISP и корисничке мреже треба да користе AS_PATH филтере, као и максималан број размењених префикса у сесији.

5.4. Заштита од преузимања сесије (*session hijacking*)

Пошто је ISP тај који је одговоран за линк ка корисничкој мрежи, потребно је да ISP обезбеди сигурност инфраструктуре, како не би дошло до физичког конектовања треће стране на остварени линк. Поред овога, потребно је и додатно обезбедити сервере. ISP је, такође, потребно да обезбеди механизме и методе у пословању самог ISP, које би се огледале у реаговању на нападе детектоване као успешна убацивања и пропагације рута. Сваки ISP треба размотрити имплементацију провере интегритета података, који су генерисани као извештај од стране рутера.

Употреба IPSec протокола у BGP комуникацији са ISP отежава појаву *hijacking*, тј. појаву преузимања сесије од треће стране. [12]

5.5. Secure BGP (S-BGP)

S-BGP представља верзију BGP протокола, која обухвата веома јаку аутентикацију и енкрипцију коришћењем PKI инфраструктуре. S-BGP верификује следеће:

- да је *update* порука примљена од легитимног BGP *peer* рутера и да није модификована
- да оглашавач поседује или је ауторизован од стране власника да оглашава руте, чије се информације налазе у *update* поруци
- ако се уклањање руте захтева у *update* поруци, иста рута би требало да је претходно оглашена од стране тог рутера.

Структура S-BGP има четири главна елемента, који омогућавају горе наведене поузданости:

- *Public Key Infrastructure* (PKI), која представља власништво рута и AS броја
- *Address Attestation* (AA) прописана AS-у од стране власника руте; овлашћење одређеног AS
- *Route Attestation* (RA), где сваки рутер дуж AS путање издаје потврду руте *peer* рутеру о претходним путањама
- предлаже се да IPSec буде коришћен у S-BGP за сигурност сесије. [11]

S-BGP захтева PKI за ауторизацију префикса и алокацију AS бројева различитим организацијама. У овој структури, сваки AS са придодатим јавним префиксом, биће придружен јавном сертификатом, који повезује префикс и AS број са јавним кључем организације. Постоје две потврде, потврда руте (*Route Attestation* - RA) и потврда адресе (*Address Attestation* - AA). Власник блока IP адреса даје AA групи AS, која ће бити овлашћена да их оглашава. AA се користи за верификацију овлашћења оглашавања руте или блока рута. RA се постиже од стране сваког рутера пре оглашавања *update* поруке свом *peer* рутеру. Ова потврда верификује да је последњи AS у AS_Path путањи овлашћен од стране претходног AS да оглашава одређене префиксе. RA се користи за верификацију интегритета AS путање. Рутери који примају префиксе, користе те потврде и дигиталне сертификате, како би се уверили у поузданост примљених *update* порука. S-BGP потврђује да је власник префикса овластио оглашивача да оглашава префиксе, коришћењем адресних поврда придодатих *update* поруци и јавном кључу власника. Ово такође верификује да су сви AS дуж путање овлашћени да оглашавају префиксе својим BGP *peer* рутерима. S-BGP користи IPSec да обезбеди потврду идентитета, поверљивост и интегритет поруке. IPSec користи различите протоколе заштите. *Encapsulation Security Payload* (ESP), *Authentication Header* (AH) и *Internet Key Exchange* (IKE) су главни протоколи заштите у IPSec. IPSec користи алгоритме енкрипције *data-encryption-standard* (DES), 3DES, *advanced-encrypted-standard* (AES) и *rivest-shamir-adleman* (RSA). За интегритет, IPSec користи *hashing* алгоритме MD5, Hash Based Message Authentication Code (HMAC) и Secure Hash Algorithm (SHA).

S-BGP користи четири различита типа података: сертификате, *Certificate Revocation List* (CRL), RA и AA. S-BGP не пропагира сертификате, CRL и AA у *update* порукама. Слање ових података може изазвати већу потрошњу протока и унети додатно кашњење. S-BGP користи репозиторијуме за пропагацију сертификата, CRL и AA. Репозиторијуми периодично размењују своје информације међусобно и шаљу их ка ISP. S-BGP шаље RA у BGP *update* поруци. Рутери примају информацију о RA и смештају је у локалној *routing information base*. Сви мањи Интернет сервис провајдери се конектују на репозиторијуме и постављају податке као што су сертификати, CRL и AA. Интернет сервис провајдери од RIR добијају сертификате везане за префиксе и AS, и постављају све потребне информације за друге AS на репозиторијуме. [13]

S-BGP може решити бројне проблеме заштите BGP протокола, али се није раширила његова употреба из следећа три разлога:

- захтева већу снагу процесора
- предуслов за S-BGP је креирање PKI инфраструктуре
- S-BGP није имплементиран код многих произвођача и Интернет сервис провајдера. [11]

6. Закључак

За повезивање рачунарских мрежа са ISP користи се BGP протокол. За реализацију конекције са ISP потребно је испунити неке одређене услове, као што су поседовање једне или више јавних IP адреса, линк између рачунарске мреже организације и ISP, и реализовано рутирање. Опциони услов јесте постојање редундантне конекције са истим или другим ISP. У овом случају треба да постоје редундантни *edge* рутер, редундантни линк, као и редундантни ISP. У данашње време компаније углавном реализују и редундантне линкове ка једном или више ISP, јер би у случају прекида јединог Интернет линка компанија могла да изгуби доста профита.

Организације, које имају редундантне Интернет линкове ка ISP, треба да поседују одређене политике о реализацији и функционисању Интернет линкова и саобраћаја, који се остварује преко тог линка. Контрола и управљање саобраћајем, тј. одређивање улазне и излазне путање из AS, одабир путање одређеног саобраћаја и још многи начини вршења контроле Интернет саобраћаја, врше се употребом BGP атрибута. Најчешће коришћени BGP атрибути јесу *weight*, *local preference* и MED, којима се утиче на излазну и улазну путању Интернет саобраћаја у AS. Поменуте путање Интернет саобраћаја могу се контролисати на основу одређених IP опсега. Такође, линкови ка ISP могу се паралелно користити, све у зависности од потреба и захтева саме организације. Коришћењем и подешавањем BGP атрибута може се реализовати растерећење линкова ка ISP, распоређивањем Интернет саобраћаја на више линкова.

У раду је, као пример имплементације, обрађено повезивање једног AS са ISP, коришћењем *dual-homed* конекције. Што се имплементације тиче, са становишта AS неке организације, ова врста конекције је веома слична *multi-homed* конекцији са два ISP, што је најчешћи случај повезивања неког AS са ISP.

У данашње време, коришћење Интернет мреже у једној организацији представља најкритичнији део активности саме организације. Разлог томе је што саобраћај, који размењује AS организације са ISP, није криптован. Саме BGP конекције AS и ISP тиме постају подложне безбедносим нападима од стране нападача. Пошто се два BGP *peer* рутера не налазе на истој локацији, потребно је обезбедити заштиту самих BGP рутера, као и BGP конекције. Поред физичког обезбеђења самих рутера, потребно је подесити да се рутерима приступа искључиво путем SSH, и да *telnet* опција приступа буде забрањена. Наравно, уз ово је потребно имплементирати и ACL на рутерима, да би приступ рутерима имали само одређени хостови, као и да саобраћај који рутери размењују буде филтриран. Филтрирање рута је директно повезано са политикама које воде организација и ISP, а чије занемаривање може довести до импортовања и оглашавања погрешних рута. Ово би могло створити проблеме и у глобалним Интернет табелама рутирања. Аутентикација између рутера представља, такође, један од битнијих елемената, који је пожељно имати имплементиран. Једна од најбржих и најсигурнијих криптографских *hash* метода јесте аутентикација поруке. Ово се најчешће користи у комуникацији између два суседна BGP рутера. Тиме се сваки сегмент TCP сесије проверава и верификује како би се порука заштитила од модификовања. Сесија између два BGP рутера се неће успоставити док се не поклопе лозинке. MD5 на BGP сесији ублажава највећи број *sniffing* претњи и онемогућује *spoofing* код BGP сесије. Сесија између два BGP рутера може се заштитити и коришћењем IPSec протокола, којим се врши криптовање и аутентикација

криптографских сервиса заштите. IPSec се примарно користи за обезбеђивање сервиса заштите у *Virtual Private Networks* (VPNs) и гарантује сигурност BGP сесија, али има ограничену заштиту када су у питању DoS напади. IPSec обезбеђује аутентикацију између BGP *peer* рутера, поверљивост и интегритет поруке. Имплементацијом IPSec протокола, умногоме би се смањила могућност реализације свих врста напада на BGP сесију између два рутера.

Као најбољи вид заштите комплетне комуникације између два BGP рутера јавља се S-BGP протокол, који користи IPSec протокол, којим се обезбеђује потврда идентитета, поверљивост и интегритет поруке, а за чију је имплементацију потребно реализовати PKI. И поред свега наведеног, S-BGP није имплементиран код многих произвођача и Интернет сервис провајдера због различитости политике и приступа према BGP комуникацијама са суседним AS. Тренутно у свету, у великој већини случајева, ISP или AS организација препуштен су сами себи око вођења безбедносне политике, где свако за себе имплементира различите видове заштите на BGP рутерима, који им представљају везу са другим AS.

7. Литература

- [1] Sam Halabi, Danny McPherson, "Internet routing architectures", Cisco Press, 2000.
- [2] Diane Teare, "Implementing Cisco IP routing", Cisco Press, 2010.
- [3] Aaron Balchunas, "Cisco CCNP routing study guide", 2012.
- [4] http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/border-gateway-protocol-bgp/white_paper_C11_516823.html
- [5] Yakov Rekhter, Tony Li, "RFC 1771 - A Border Gateway Protocol 4 (BGP-4)", Cisco Systems, 1995.
- [6] Anthony Bruno, Steve Jordan, "CCDA 640-864 Official Certification Guide", Cisco Press, 2011.
- [7] Denise Donohue, Brent Stewart, "CCNP routing and switching quick reference", Cisco Press, 2010.
- [8] Sargon Elias, "Is the Border Gateway Protocol safe?", SANS Institute, 2003.
- [9] "BGP security best practices", Communications Security, Reliability and Interoperability Council, 2013.
- [10] Muhammad Mutjaba, "Analysis of Intrusion Detection System in Border Gateway Protocol", University of technology, Sydney, 2012.
- [11] Akhtar Zeb, Muhammad Farooq, "BGP threats and practical security", University of Technology, Gothenburg, 2011.
- [12] Barry Raveendran Greene, Philip Smith, "The ISP Essentials", Cisco Press, 2002.
- [13] Muhammad Adnan Khalid, Qamar Nazir, "Security Issues of BGP in Complex Peering and Transit Networks", Halmstad University, 2008.

8. Списак слика

Слика 1: Примена IGP и EGP у односу на AS	5
Слика 2: Статичке руте у конекцији са ISP.....	7
Слика 3: ISP конекција коришћењем BGP протокола.....	7
Слика 4: <i>single-homed</i> конекција са ISP.....	8
Слика 5: <i>dual-homed</i> конекција са ISP.....	8
Слика 6: <i>multihomed</i> конекција са ISP	9
Слика 7: <i>dual multihomed</i> конекција са ISP	9
Слика 8: <i>default</i> руте добијене од суседних ISP.....	10
Слика 9: Вектор путање.....	11
Слика 10: BGP суседи.....	12
Слика 11: Функционисање AS путање.....	16
Слика 12: BGP <i>next-hop</i> атрибут.....	17
Слика 13: BGP <i>local preference</i> атрибут	18
Слика 14: Улога MED атрибута.....	19
Слика 15: Улога BGP <i>weight</i> атрибута	19
Слика 16: Употреба мапе рутирања при промени <i>weight</i> атрибута	21
Слика 17: Употреба мапе рутирања при промени атрибута <i>local preference</i>	21
Слика 18: Подешавање и употреба <i>AS-path</i> атрибута.....	22
Слика 19: Подешавање и употреба MED атрибута.....	22
Слика 20: Топологија мреже практичног решења	24
Слика 21: Приказ топологије мреже из програмског пакета GNS3	25
Слика 22: Конфигурација интерфејса на рутеру R1	25
Слика 23: Конфигурација интерфејса на рутеру R2.....	26
Слика 24: Конфигурација интерфејса на рутеру R3	26
Слика 25: Конфигурација интерфејса на рутеру R4.....	27
Слика 26: Конфигурација OSPF протокола на рутеру R2	27
Слика 27: Конфигурација OSPF протокола на рутеру R3	27
Слика 28: Конфигурација OSPF протокола на рутеру R4	27
Слика 29: Конфигурација BGP протокола на рутеру R1	28
Слика 30: Конфигурација BGP протокола на рутеру R2.....	28
Слика 31: Конфигурација BGP протокола на рутеру R3.....	28

Слика 32: Конфигурација BGP протокола на рутеру R4	29
Слика 33: Табела рутирања рутера R1	29
Слика 34: Табела рутирања рутера R2	30
Слика 35: BGP на рутеру R1	30
Слика 36: BGP на рутеру R2	31
Слика 37: BGP руте, метрика и AS путање на рутеру R1	31
Слика 38: BGP руте, метрика и AS путање на рутеру R2	31
Слика 39: Подешавање BGP атрибута <i>local preference</i> на рутеру R2	32
Слика 40: Подешавање BGP атрибута <i>local preference</i> на рутеру R3	32
Слика 41: BGP табела рутера R2	32
Слика 42: BGP табела рутера R3	32
Слика 43: Путања пакета од R3 ка адреси 192.168.1.1	33
Слика 44: Табела рутирања рутера R1	33
Слика 45: Подешавање MED атрибута на рутеру R2	33
Слика 46: Подешавање MED атрибута на рутеру R3	34
Слика 47: BGP табела рутера R1	34
Слика 48: <i>Spoofing</i> напад	36
Слика 49: Тополошки приказ <i>session hijacking</i> напада	37
Слика 50: Рутер C изазива <i>flapping</i>	38
Слика 51: Пример <i>de-aggregation</i> напада	38
Слика 52: Криптована сесија	42
Слика 53: Криптована порука у сесији	43
Слика 54: Криптовање <i>update</i> поруке у сесији	43
Слика 55: IPSec tunneling	44