

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

STUDIMI I TRAFIKUT INTERDOMAIN BAZUAR NË PROTOKOLLIN BGP, RAST STUDIMOR NË SHQIPËRI

Ledina Karteri Hoxha

Dorëzuar
Universitetit European të Tiranës
Shkollës Doktorale

Në përmbushje të detyrimeve të programit të Doktoratës në
`Informatikë, Matematikë & Statistikë` me profil `Menaxhim i sistemeve të
Informacionit`, për marrjen e gradës shkencore “Doktor”

Udhëheqës shkencor: Prof.As Anni Dasho

Numri i fjalëve: 61655

DEKLARATA E AUTORËSISË

Deklaroj se studimi është punë origjinale e imja. Siguroj që kam dhënë kontributin tim të plotë në të gjithë punimin në përdorimin e ideve, të të dhënave, ose të gjuhës së një subjekti tjetër duke kryer citimet dhe referencat specifike.

ABSTRAKT

Border Gateway Protocol (BGP) është protokoll i aktual i rrugëzimit inter-domain i aplikuar në Internet. BGP, fillimisht një protokoll i thjeshtë path-vektor, është ndryshuar përherë në mënyrë rritëse me kalimin e kohës përmes një numri të mekanizmave për mbështetjen e politikave, duke shtuar ndjeshëm kompleksitetin. Edhe pse performanca e Border Gateway Protocol është pranuar gjithnjë, përmasat, heterogjeniteti dhe ndryshueshmëria që e karakterizojnë Internetin sot, përbëjnë një sfidë për ruajtjen e cilësisë së shërbimit (QoS) duke vendosur kërkesa gjithnjë e në rritje për BGP në trafikun e shpërndarjes së paketave të të dhënave. Analizat e fundit të sigurisë të marra nga komuniteti i kërkimit kanë raportuar qartësisht karakteristikat e pakënaqëshme të BGP si integriteti i ulët dhe konvergjenca e ngadaltë përmes analizave teorike dhe matjeve empirike. Kështu është evidentuar që infrastruktura e rrugëzimit të internetit është mjaft e cënueshme. Keqkonfigurimi i ruterave shpeshherë sjell në injektimin e tabelave të mëdha të rrugëzimit në sistemin e rrugëzimit BGP. Në këtë punim shohim mekanizmat e detajuar të përgjigjes së ruterave kundrejt tabelave të mëdha të rrugëzimit. Disa prej ruterave shfaqin oshilime që kanë potencial për të shkaktuar dështim kaskadë. Disa të tjerë kërkojnë ndërhyrjen e operatorëve për tu rikuperuar. Po ashtu vërejmë se mekanizmat e kontrollit të resurseve të aplikuara janë pjesërisht të suksesshme në zbutjen e impaktit të tabelave të mëdha të rrugëzimit. Gjithashtu dizanji dhe kudogjendja e BGP ka frustruar përpjekjet e mëparshme për sigurimin e rrugëzimit interdomain. Simulimet e kryera lejojnë eksperimente më realiste e fleksibël se metodat teorike dhe kosto më të ulët se matjet në ambjente reale. Në punim përshkruhen teorikisht karakteristikat dhe problemet që lidhen me BGP dhe gjithashtu pritshmëritë e përdoruesve të sotëm të Internetit ndaj aplikacioneve në kohë reale (psh. Voice over IP). Evidentohen dhe implementohen elementët për të krijuar një ambjent të integruar simulimi për vlerësimin e ndikimit të konvergjencës së ngadaltë të BGP në këto aplikacione. Për të kënaqur kërkesat e këtyre aplikacioneve dhe për të përfutur cilësinë e shërbimit të kushtëzuar nga SLAs, ISP të ndryshme mbështeten në një proces të quajtur Inxhinierim Trafiku (Traffic Engineering, TE). Ky i fundit mbulon vlerësimin dhe përmirësimin e performancës së rrjetave operacionale. Vëmë re se ende nuk është gjetur një balancim i përshtatshëm midis sigurisë komprehsive dhe koston së zhvillimit. Së fundmi vlerësohet saktësia e ambjentit të krijuar përmes disa simulimeve në përmasa të vogla por që modelojnë pjesë të Internetit në ditët e sotme. Së fundmi pasqyrojmë rezultatet e anketës së zhvilluar ku reflektohen vlerësimet e përdoruesve të internetit ndaj ISP-ve operuese në vendin tonë. Në anketë studiohen qëndrimet që mbajnë përdoruesit e internetit ndaj QoS së ISP-ve shqiptare duke evidentuar pikët e forta të tyre dhe pakënaqësitë ku konsistojnë për secilin ofrues interneti duke u shërbyer si një udhërrëfyes për përmirësime të mëtejshme.

Fjalë-kyçe: AS, BGP, Traffic Engineering, QoS, Simulim, NS2.

ABSTRACT

“The study of interdomain traffic based on BGP protocol”

Border Gateway Protocol (BGP) is the actual routing protocol applied in the cross-domain Internet. BGP, originally a simple protocol path-vector, changes always so incrementally over time through a number of mechanisms to support policy and complexity. Although it is agreed that the performance of Border Gateway Protocol, the size, the heterogeneity and variability that characterize the Internet today, constitute a challenge to maintain the quality of service (QoS) of the located demand ever increasing BGP traffic distribution package of the database. Recent analysis obtained by the security research community have reported clearly unsatisfactory features of BGP as low integrity and convergence slow through empirical measurements and theoretical analysis. Thus it is evident that the routing infrastructure of the Internet is vulnerable enough. Misconfiguration of routers often brings injecting billboards routing BGP routing system. In this paper, we see detailed response mechanisms SE routers versus large routing tables. Some routers exhibit oscillations that have the potential to cause failure cascade. Others call for the intervention of operators to recover. Also note that the mechanisms of control of resources applied are partially successful in mitigating the impact of large routing tables. Also design and ubiquity of BGP has frustrated previous attempts for providing interdomain routing. Completed simulations more realistic experiments allow flexible methods of theoretical and lower cost than measurements in real environments. The paper theoretically describes the characteristics and problems associated with BGP and also the expectations of today's Internet users to real-time applications (RP, Voice over IP). Also identified and implemented elements to create an integrated simulation environment impact assessment convergence BGP slower in these applications. To satisfy the requirements of these applications and quality of service obtained conditional on SLAs, different ISPs rely on a process called (Traffic Engineering, TE). The Last covers assessing and improving operational performance networking. We notice that it is still not find a suitable balance between security setting Se comprehensive and development. It used recently estimated that the environment created through several small scale simulations that model but part of the Internet nowadays. Finally we reflect the results of the survey conducted reflecting the attitudes that keep Internet users to ISPs operating in our country. The survey examines the attitudes that internet users have on QoS of Albanian ISPs, highlighting their strong points and dissatisfaction with each of the internet providers, serving as a guide for further improvements.

Keywords: AS, BGP, QoS, Simulation, NS2.

DEDIKIMI

Këtë punim ia dedikoj babait tim dhe djemve të mi.

FALENDERIME

Falenderoj pambarimisht udhëheqësen time Prof.As Anni Dasho për ndihmën e çmuar në këtë studim.

Gjithashtu kam falenderime të veçanta për vlerësuesen metodologjike Prof.As Mimoza Durrësi dhe oponenten Prof.Adriana Gjonaj që më kanë ndihmuar dhe inkurajuar në ecurinë e këtij studimi. Po ashtu gjej rastin të falenderoj koordinatoren dhe kolegët për përkrahjen në punimin tim. Sigurisht që një vend special zë familja ime të cilën e falenderoj pamasë (mamanë, vëllanë, bashkëshortin) për mbështetjen morale që asnjëherë nuk ma kanë kursyer. Një falenderim i rezervoj dhe mikeshave të mia që gjithnjë më kanë dhënë krahë për vijueshmërinë e këtij punimi.

PËRMBAJTJA E LËNDËS

Lista e figurave	8
Lista e tabelave	10
Kapitulli I	14
Hyrje.....	14
1.1 Përcaktimi i problemeve dhe nënproblemeve.....	15
1.2 Motivimi dhe kontributi i temës.....	18
1.3 Burimet e informacionit.....	20
1.4 Popullata dhe kampioni i studimit.....	21
1.5 Metodologjia.....	21
1.6 Mbledhja e të dhënave dhe përpunimi i tyre.....	22
1.7 Modeli teorik.....	23
1.8 Organizimi i kapitujve.....	24
Kapitulli II	
Border Gateway Protocol.....	27
2.1 Hyrje.....	27
2.2 Rrugëzimi në Internet.....	28
2.3 BGP: Një protokoll për rrugëzimin “inter domain”.....	31
2.3.1 Karakteristikat e funksionimit të BGP.....	32
2.3.2 Rrugëzimi i BGP.....	34
2.3.3 Konvergjencia e BGP.....	36
2.3.4 Paqëndrueshmëritë e BGP.....	38
2.4 Menaxhimi i sesionit ndërmjet `çifteve`.....	41
2.4.1 Shkëmbimi i informacionit të rrugëzimit.....	42
2.4.2 Përpunimi dhe gjetja e rrugës.....	42
2.4.3 Zhvlerësimi i një rruge.....	43
2.4.4 Reflektimi i rrugës.....	44
2.4.5 Përfundime.....	44
Kapitulli III	
Modelimi i rrugëzimit të një ISP.....	47
3.1 Modelimi i një sistemi autonom.....	47
3.1.1 Përmbledhja e konfigurimit të routerave.....	48
3.1.2 Përfaqësimi i topologjisë.....	49
3.1.3 Rrugëzimi i të dhënave.....	49
3.2 Modeli GEANT 75.....	52
3.2.1 Statistikat e trafikut.....	52
3.2.2 Modeli GEANT.....	52
3.2.3 Topologjia.....	53
3.2.4 Rrugëzimi i të dhënave.....	56
3.2.5 Statistikat e trafikut.....	49
3.3 Karakterizimi i rrugëzimit.....	57
3.3.1 Rrugëzimi Intradomain.....	57

3.3.2	Rrugëzimi Interdomain	59
3.3.3	Skenarët Çka – nëse	61
3.3.4	Peering i optimizuar	61
3.3.5	Dështimet e linqeve dhe ruterave	65
3.3.6	Ndikimi në trafik	68
3.4	Teknika TE Interdomain aktuale	71
3.4.1	Intradomain Engineering Traffic (ITE).....	72
3.4.2	Zgjidhje të bazuara në IP.....	72
3.4.3	Dështimet e linqeve dhe ruterave	72
3.4.4	Interdomain Engineering Traffic	73
3.4.5	Kufizimet e arkitekturës së rrugëzimit të Internetit të tanishëm	74
3.4.6	Karakteristikat e trafikut interdomain	75
3.4.7	Inxhinierimi i trafikut i bazuar në BGP	77
3.4.8	Kontrolli i trafikut dales	78
3.4.9	Kontrolli i trafikut në hyrje	79
3.4.10	Përhapja e rrugëzimit të kontrolluar nga komuniteti (Community)	81
3.5	Diskutimi.....	82
3.5.1	Vlerësimi i AS-Path prepending.....	83
3.5.2	Modeli i vlerësimit.....	84
3.5.3	Rëndësia e rregullave tie-breaking	86
3.5.4	Vlerësimi i AS-Path prepending.....	88
3.6	Vlerësimi i Komuniteteve	92
3.7	Qasjet duke mos u mbështetur në tweaking BGP	96
3.8	Cooperative Engineering Traffic	97
3.8.1	Peerings Virtual	98
3.8.2	Arkitektura dhe protokolli.....	100
3.8.3	Advertisement i adresave VPC.....	101
3.8.4	Krijimi dhe heqja e Peerings Virtual	101
3.8.5	Shpërndarja e rrugëve Virtual Peering brenda fushës domain	102
3.8.6	Konsiderata të sigurisë	103
3.8.7	Vendosja.....	104
3.8.8	Forca	104
3.8.9	Vlerësimi	105
	<u>Kapitulli IV</u>	
	Voice Over IP – VOIP.....	124
4.1	Hyrje	124
4.2	Pritshmëria e ndaj aplikacioneve VoIP në rrjet.....	126
4.3	Koduesit e zërit	128
4.4	Paketizimi	129
4.5	“Jitter buffer”	129
4.6	Matja e Cilësisë së VoIP	130
	<u>Kapitulli V</u>	
	Ambienti Eksperimental	133

5.1 Hyrje	133
5.2 Simulimet	134
5.2.1 Elementet e simulimit	134
5.2.2 Simulimet që varen nga koha	135
5.3 Simulimi i Rrjetit 2 (Network Simulator 2 – ns2)	135
5.3.1 Arkitektura e NS2	136
5.3.2 Direktoritë e ns2	137
5.3.3 Përdorimi i ns2	138
5.4 Modelimi i simulimit	140
5.5 Ndërtimi i modelit të rrjetit	141
5.5.1 Topologjia e rrjetit	142
5.5.2 Struktura njëdrejtimore e rrugëzimit ns2	143
5.6 Struktura njëdrejtimore e rrugëzimit ns2_BGP	145
5.6.1 Klasifikuesi IPV4.....	147
5.6.2 rtModule/BGP	147
5.6.3rtProtoBGP	147
5.6.4 TcpSockets	147
5.6.5 BGP_Timer	148
5.6.6 VecRoutes	149
5.6.6 VecRoutes	149
5.6.7 damp_reuse_timer.....	149
5.6.8 dampinfo	150
5.7 Gjeneratori i topologjisë GT-ITM.....	152
5.7.1 Modelimi i rrugëzimit	154
5.7.2 Ndërtimi I modelit të të dhënave	156
5.7.3 Gjendja e rrjetit dhe vlerësimi i performancës	156
5.7.4 Ndryshimet në model.....	156
5.8 Simulime dhe rezultate	157
5.8.1 Verifikimi i modelit të përzgjedhur të rrugëzimit	159
5.8.2 Simulimi i topologjisë Stub-Domain me trafik CBR	162
5.8.3 Rezultatet e simulimit	166
Kapitulli VI	
6.1 Realizimi dhe interpretimi i pyetësorit	168
6.2 Analiza e përgjigjeve për rastin e përdoruesve të cilët e konsiderojnë QoS në nivele maksimale në Shqipëri	178.
6.3. Analiza e përgjigjeve për rastin e përdoruesve të cilët e konsiderojnë QoS në nivele minimale në Shqipëri.....	199
Konkluzione	228
Bibliografia	238
Shtojca 1	242
Shtojca 2	244
Shtojca 3	245

Shtojca4	247
Perspektiva	253

LISTA E ILUSTRIMEVE

- Figura 2.1:** *Sistemet Autonome*
- Figura 2.2:** *Paraqitja e fushës së veprimit të protokolleve të rrugëzimit*
- Figura 2.3:** *Protokollet e rrugëzimit brenda dhe jashtë Sistemit Autonom*
- Figura 2.4:** *Protokollet e rrugëzimit në Internet*
- Figura 2.5** *Klasifikimi i AS-ve*
- Figura 2.6:** *Internal BGP (I-BGP) përkundrejt external BGP (E-BGP)*
- Figura 2.7:** *Pema e shtigjeve të AS*
- Figura 2.8:** *Funksionimi i BGP – Politikat e rrugëzimit*
- Figura 2.9:** *Shembull për përhapjen e një rifreskimi BGP*
- Figura 2.10:** *Shkëmbimi i mesazheve BGP*
- Figura 2.11:** *Zgjedhja e rrugës BGP*
- Figura 3.1:** *Përshkrimi i një modeli të një ISP-je.*
- Figura 3.2:** *Nje pamje e kufizuar e ruterave eBGP*
- Figura 3.3:** *Pamje e përgjithshme e hartës të GÉANT*
- Figura 3.4:** *Cluster-imi i prefikseve BGP*
- Figura 3.5:** *Cumulative Frekuenca e cluster-ave me numër të njëjtë prefiksesh.*
- Figura 3.6:** *Qendërzimi Betweenness i ruterave GÉANT*
- Figura 3.7:** *Qendërzimi Betweenness i linqeve GÉANT.*
- Figura 3.8:** *Ndarja e prefikseve nga numri i rrugëve të marra në GEANT .*
- Figura 3.9:** *Rëndësia e rregullave në GEANT*
- Figura 3.10:** *Ndikimi i shtimit / heqjes së peerings në shpërndarjen e trafikut përgjatë lidhjeve peering.*
- Figura 3.11:** *Ndikimi i shtimit/ largimit të peerings në koston e IGP të parë nga trafiku.*
- Figura 3.12:** *Ndikimi i shtimit / largimit të peering në vonesën e parë nga trafiku .*
- Figura 3.13:** *Analiza e dështimit të një linku të vetëm: ndikimi në BGP .*
- Figura 3.14:** *Analiza dështimi e një ruteri të vetëm : ndikimi në BGP .*
- Figura 3.15:** *Ndikimi i dështimit të R1-R3 mbi ngarkesën e lidhjeve.*
- Figura 3.16:** *Ndikimi i dështimit të R5-R6 mbi ngarkesën e lidhjeve.*
- Figura 3.17:** *Dështimi i një linku të vetëm më të ndjeshëm.*
- Figura 3.18-a:** *Shpërndarja kumulative e trafikut për secilin ISP të studiuar.*
- Figura 3.18-b:** *Shpërndarja Per-AS hop e trafikut për secilin ISP të studiuar.*
- Figura 3.19:** *Një Internet I thjeshtë*
- Figura 3.20:** *Shembull i rishpërndarjes së rrugëve të komuniteteve – kontrolluara(communities-controlled) .*
- Figura 3.21:** *Modeli i një AS me politikat.*
- Figura 3.22:** *Rëndësia e secilit rregull të procesit të vendimmarrjes BGP në nivele të ndryshme të hierarkisë së internetit .*
- Figura 3.23:** *Shpërndarja default relative e rrugëve nga ofruesit më pak të lidhur.*
- Figura 3.24:** *Përqindja e rrugëve në ofruesit më pak të lidhur për sasi të ndryshme të prepending .*
- Figura 3.25:** *Topologjia dhe politikat pengojnë efikasitetin e AS - Path prepending .*
- Figura 3.26:** *Topologjitë dhe politikat pengojnë efikasitetin e AS - Path prepending .*

Figura 3.27: Një pjesë e topologjisë interdomain parë nga YUCOM

Figura 3.28: Ndikimi i topologjisë dhe marrëdhëniet e biznesit në efikasitetin e Komuniteteve

Figura 3.29: Rëndësia e marrëdhënieve të ndryshme të biznesit në 2 AS HOPS nga multi-homed stub domains.

Figura 3.30: Skica e qasjes

Figura 3.31: Topologjia e rrjetit Interdomain

Figura 3.32: Diversiteti i rrugëve të përfuara gjatë multihoming në RouteViews ose RIPE peers.

Figura 3.33: Disbalancë e trafikut Inicializues ($\alpha = 0.5$).

Figura 3.34: Konvergenca e algoritmit evolucionarizues për stub-ë 3- dhe 4-homed.

Figura 3.35-a: Numri i Virtual Peerings për të krijuar ($\alpha = 0.5$).

Figura 3.35-b: Çekuilibri fillestar i trafikut ($\alpha = 0.25$).

Figura 3.35-c: Number of Virtual Peerings to establish ($\alpha = 0.25$).

Figura 3.36: Shpërndarja kumulative e vonesës për rrugët BGP.

Figura 3.37: Vonesa përgjatë rrugës BGP kundrejt vonesës përgjatë rrugës më të ulët.

Figura 3.38: Shpërndarja e përmirësimit të vonesës absolute

Figura 3.39: Shpërndarja kumulative e përmirësimit të vonesës absolute për stub-ët homed.

Figura 4.1: Komunikimi VoIP

Figura 4.2: Skema e aplikacionit VoIP

Figura 4.3: Skema e aplikacionit VoIP

Figura 4.4: Manaxhimi i jitter përmes jitter buffer

Figura 5.1: Arkitektura Bazë e ns-2

Figura 5.2: Struktura e direktorive të ns2

Figura 5.3: Hapat e përdorimit të ns2

Figura 5.4: Objektet e regjistrimit në një link

Figura 5.5: Diagrama rrjedhëse e metodologjisë së simulimeve

Figura 5.6: Topologjia në nivel AS dhe topologjia në nivel ruteri

Figura 5.7: Struktura njëdrejtimore e rrugëzimit në ns-2

Figura 5.8: Struktura njëdrejtimore e rrugëzimit në ns2-BGP

Figura 5.9: Struktura unicast e ns-BGP

Figura 5.10: Struktura e modulit të VoIP

Figura 5.11: Topologjia e rrjetit

Figura 5.12: Topologjia e rrjetit sipas modelit stub-domain

Figura 5.13-a: Dërgohet paketa e parë CBR

Figura 5.13-b: Dërgohet informacioni i rrugëzimit

Figura 5.13-c: Shpërndahet informacioni rrugëzimit

Figura 5.13-d: Shpërndahet informacioni rrugëzimit

Figura 5.14: Humbjet në paketa

Lista e tabelave

- Tabela 1:** *Procesi i vendimmarrjes BGP*
- Tabela 2:** *Veprimet tipike të rishpërndarjes së rrugëve në dispozicion me komunitetet*
- Tabela 3:** *Përmbledhja e RouteViews dhe RIPE datasets.*
- Tabela 4:** *Përmbledhja e metodave të inxhinierimit të trafikut*
- Tabela 5:** *Krahasimi i karakteristikave të koduesve të zërit*
- Tabela 6:** *Vlerat tipike të faktorit A*
- Tabela 7:** *Ekuivalenca midis faktorit R dhe MOS*
- Tabela 8:** *Parametrat për koduesit e ndryshëm të VoIP*
- Tabela 9 :** *Adresat IP*
- Tabela 10 :** *Karakteristikat e grafit*
- Tabela 11-48:** *Përmbledhjet e të dhënave të pyetësorit*

Kapitulli I

Hyrje

Në pak vite, interneti ka evoluar me shpejtësi nga një rrjet kërkimor që i shërben një pjese të vogël të përdoruesve në një ndërlidhje të madhe prej rreth 350 milionë hostesh [ISC05]). Në këtë mënyrë, interneti është sistemi më i madh i shpërndarë i ndërtuar ndonjëherë. Interneti është i organizuar në një numër të rrjeteve administrative të pavarur të quajtur domaine ose Sisteme autonome (AS). Për shembull, një AS mund të jetë një Internet Service Provider (ISP), një kampus universitar ose një rrjet i korporatave. Në kohën e këtij shkrimi, ka më shumë se 54.000 AS në internet [Hus06]. Gjatë kësaj infrastrukture të madhe, ka një tendencë në rritje për të vendosur aplikime të reja të tilla si transmetimin e Zërit ose video mbi IP dhe shërbime të reja të tilla si rrjetet private virtuale (VPN). Këto aplikacione dhe shërbime të reja kërkojnë garanci më të mirë apo të rrepta të cilësisë, ndërsa interneti është projektuar për të siguruar një shërbim best-effort. Ky evolucion vë shumë presion mbi ISP-të për të cilët aftësia për të ofruar më mirë se shërbimi best-effort apo mbështesin fortë marrëveshjt të nivelit të shërbimit (SLAs) [FE04] është çelësi si faktor diferencimi. Inxhinierët e rrjetit mbështeten në Inxhinierinë e Trafikut (TE) për të përshtatur konfigurimin e rrjetit të tyre për të mbështetur evolucionin e kërkesës trafikut dhe SLAs të konsumatorëve. Sot protokollin Border Gateway Protocol konsiderohet si standardi de-facto për rrugëzimin e paketave në Internet. Objektivi i tij kryesor është shkëmbimi i informacionit ndërmjet Sistemeve Autonome mbi lidhjet ekzistuese dhe aftësinë për të mbërritur një destinacion në një rrjet. Edhe pse performanca e Border Gateway Protocol është pranuar gjithnjë, përmasat, heterogjeniteti dhe ndryshueshmëria që e karakterizojnë Internetin sot, përbëjnë një sfidë për ruajtjen e cilësisë së shërbimit (QoS) duke vendosur kërkesa gjithnjë e në rritje për BGP në trafikun e shpërndarjes së paketave të të dhënave. Analizat e fundit të sigurisë të marra nga komuniteti i kërkimit kanë raportuar qartësisht karakteristikat e pakënaqëshme të BGP si integriteti i ulët dhe konvergjenca e ngadaltë përmes analizave teorike dhe matjeve empirike. Kështu është evidentuar që infrastruktura e rrugëzimit të internetit është mjaft e cënueshme. Ndaj përmes këtij punimi synohet që të vihet në dukje ndikimi që ka mbi performancën e rrjetit të internetit rifreskimi i këtij protokollin. Studiohen karakteristikat si heterogjeniteti, ndryshueshmëria dhe integriteti i ulët i këtij protokollin. Po ashtu përmes anketimit testohet kënaqshmëria e përdoruesit shqiptarë kundrejt cilësisë së shërbimit të internetit të ofruar nga ofruesit respektivë shqiptarë. Aty mund të nxirren në pah anët pozitive dhe mangësitë e QoS të internetit në Shqipëri.

Kapitulli i dytë është i natyrës teorike ku portretizohet protokollin BGP sëbashku me karakteristikat e tij të implementimit.

Kapitulli i tretë përfshin aplikimin e C-BGP që të modelojmë një domain të vetëm interneti. C-BGP lejon një operator rrjeti për të ndërtuar një model të rrjetit të tij dhe të injektojë konfigurimin, rrugëzimin dhe trafikun e të dhënave me qëllim të hetimit të skenarëve çfarë-nëse. Ne përshkruajmë çështjet teknike që lidhen me këtë modelim.

Kapitulli i katërt shtjellon elementët kryesorë VoIP dhe metodat e vlerësimit të cilësisë së thirrjeve VoIP si një aplikacion në kohë reale duke analizuar disa prej pritshmërive ndaj aplikacioneve VOIP në rrjet.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Kapitulli i pestë dhe kapitulli i gjashtë janë kapituj metodologjik që sigurojnë disa njohuri të nevojshme mbi simulimet dhe simulatorin e rrjetit ns-2. Gjithashtu në këtë kapitull përshkruhen dhe dy modulet e nevojshme për realizimin e ambjentit të integruar eksperimental dhe nga ana tjetër kapitulli i gjashtë përfshin studimin e anketës së zhvilluar, rastit studimor që është marrë në shqyrtim për vlerësimin e cilësisë së shërbimit të internetit të ofruar nga Internet service provider-at shqiptare. Së fundmi trajtohen konkluzionet e nxjerra nga realizimi i këtij punimi.

1.1 Përcaktimi i problemeve dhe nënproblemeve

Përmasat e Internetit në ditët e sotme kanë sjellë nevojën e organizimit në Sisteme Autonome (AS) ku çdo sistem nga ana e tij përfaqëson interesa biznesi të ndryshme dhe shpesh konkurruese me të tjerët. BGP konsiderohet sot si standardi *de-facto* për komunikimet ndërmjet Sistemeve Autonome dhe “ngjitësi” që e mban këtë strukturë kaq komplekse të lidhur. Duke marrë në konsideratë natyrën dinamike të Internetit, performanca e BGP mbetet një çështje e hapur studimi veçanërisht për sa i përket kohës së konvergjencës së këtij protokollit. Studime të ndryshme kanë treguar ndikimin që ka kjo çështje performance e BGP në cilësinë e shërbimit të një rrjeti. Studime të tjera janë përqëndruar në cilësinë e aplikacioneve ndërtuar mbi infrastrukturën e Internetit. Një rëndësi e veçantë i është kushtuar aplikacioneve VoIP në një kohë kur ekspertët e industrisë presin që kjo teknologji të zëvendësojë pjesën më të madhe të lidhjeve tradicionale telefonike.

Ky punim synon që përmes një ambjenti të integruar simulimi të mundësojë identifikimin dhe vlerësimin e ndikimeve që kanë faktorët e performancës së BGP në cilësinë e aplikacioneve të Internetit. Debati akademik që behet tani në vende të ndryshme të Europës dhe në USA, është integrimi i politikave të protokollit BGP (Border Gateway Protocol) Duke qenë se duhet të integrohen politika rrjetash në shtete të ndryshme implementimi i këtij protokollit has vështirësi të mëdha sidomos në nivelin e sigurisë (Imagjinoni disa e-maile nga Shtëpia e Bardhë në USA që duhet të kalojnë në disa vende të lindjes së mesme duhet të kalojnë nga vende të tilla si Iran, Irak, Siri etj).

A duhet të enkriptohet informacioni? Në ç`nivel duhet të jetë ai? Duhet të enkriptohet deri në nivele hardware informacioni? Si është raporti i BGP me TPM (Trusted Platform Module). A mund të integrojnë BGP rrjeta me platforma sigurie të ndryshme?

Këtu ne trajtojmë një anketë e cila përfshin si kampion popullatë përdorues të internetit studentët e Universitetit European të Tiranës. Ata kanë plotësuar plot 524 anketa rezultatet e të cilave janë reflektuar për të dhënë një pasqyrë të QoS të perceptuar nga kjo kategori e përdoruesve e cila na jep dhe një parashikim mbi një popullatë më të gjerë lidhur me këtë aspekt.

Ka këto kontribute kryesore në këtë tezë:

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

- Vlerësimi i një rasti studimor në Shqipëri mbi disa ISP-ë në lidhje me QoS dhe faktorët që ndikojnë në raportin kosto-performancë.
- Hartimi dhe zbatimi i një mjeti modelimi BGP, C-BGP. Është e mundur të llogariten rrugët BGP në topologjinë e rrjetit në shkallë të gjerë me anë të dy aplikimeve kryesore. Ai mund të përdoret nga operatorët e rrjetit ISP për të kuptuar më mirë rrugëzimin e tyre. Ai mund të përdoret edhe nga studiues për të studiuar karakteristikat makroskopike të rrugëzimit në internet.
- Një metodologji për të vlerësuar skenarët e rrugëzimit çfarë-nëse në rrjetet e ISP. Për shkak të ndërveprimit midis dy llojeve të protokolleve të rrugëzimit (link-state dhe path-vector), parashikimi i ndikimit në rrugëzim i një rrjeti ISP i ndryshimeve topologjike dhe të konfigurimit është një detyrë komplekse. Është treguar se si C-BGP mund të trajtojë një pjesë të madhe të këtij kompleksiteti.
- Një vlerësim i performancës në shkallë të gjerë së teknikave të tanishme të inxhinierisë së trafikut me bazë BGP. Së pari janë studiuar mekanizmat e kontrollit të rrugëzimit ekzistues të bazuar në BGP. Pastaj, duke përdorur C-BGP në një topologji Internet-shkallë, u vlerësuan dy prej këtyre mekanizmave: AS-Path prepending dhe Rishpërndarja e Komuniteteve. Është treguar se këto mekanizma janë të ashpër dhe jo-përcaktuese.
- Është propozuar Peerings virtuale, një mekanizëm të ri për inxhinierinë e trafikut të shkëmbyer në mes të dy ISP-ve bashkëpunuese, por jo të afërta. Ky mekanizëm është determinist, i shkallëzuar dhe është pothuajse gati i dislokueshëm. Është vlerësuar përdorimi i peerings virtuale për të zgjidhur dy objektivat e inxhinierisë së trafikut: ngarkesë-balancimin dhe përmirësimin e vonesave fund-më-fund.

Objektivat e studimit

Studimi ka këto objektiva:

- a) Studimi i QoS së internetit në Shqipëri.
- b) Njohja e protokollit dinamik të rrugëzimit BGP.
- c) Studimi i cilësisë së shërbimit të ISP-ve kryesore në Shqipëri.
- d) Studimi i topologjive të ndryshme të rrjetit dhe raportet e mesazheve mes kostove të ndryshme dhe cilësisë.
- e) Implementimi i politikave të sigurisë dhe rrugëzimit në nyjet e rutimit.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Hipotezat e këtij punimi janë:

1. QoS e internetit të ofruar nga ISP-të vendase në Shqipëri është në nivele optimale.
2. QoS e internetit në Shqipëri varet nga ISP e zgjedhur.
3. Interneti i cili ka heterogjenitet, përmasa shumë të mëdha, ndryshueshmëri të vazhdueshme ndikon në protokollin e rrugëzimit interdomain Border Gateway Protocol që shfaq konvergjencë të ngadaltë në nivel performance, dhe paraqet integritet të ulët.

Pyetjet kërkimore të shtruara për zgjidhje janë:

1. Varet QoS e internetit në vendin tonë nga karakteristika si besueshmëria, shpejtësia, shkëputjet e sinjalit?
2. Ka ndikim në QoS e internetit të vendit tonë operatorët dhe profesionalizmi i tyre ndaj shërbimit të klientit?
3. Ndikon lloji i ISP-së së zgjedhur në QoS e përgjithshme të internetit në Shqipëri ?
4. A do të rritet performanca e komunikimit midis kostove, pavarësisht topologjisë së lidhjes dhe fizionomisë së tyre (llojeve të paketave video, data etj)?
5. Niveli i përdorimit të një aplikacioni në kohë reale si VoIP ndikohet nga konvergjenca e ulët e BGP po aq sa ndikohet dhe nga mbingarkimi i rrjetit?
6. A ndikojnë momentet e rifreskimit të BGP në QoS e rrjetit të ISP-ve?
7. Pse ka rëndësi studimi i lidhjes që ekziston midis cilësisë së thirrjeve VoIP dhe rifreskimeve BGP, në nivel përdoruesi?

Avantazhet dhe disavantazhet

Së pari, ky studim merr përsipër të analizojë gjendjen e cilësisë së shërbimit në vendin tonë. Studimet në nivel përdoruesi mungojnë paraprakisht dhe pikërisht për këtë qëllim ky studim sjell një panoramë të përgjithshme të cilësisë së shërbimit që ofrohet në vendin tone nga ISP –të respektive.

Së dyti, krahas portretizimit të gjendjes aktuale të QoS në vend, studimi paralelisht analizon dhe një tjetër aspekt hibrid të cilësisë së shërbimit të internetit që është edhe shërbimi ndaj klientit duke parë në vija të përgjithshme evolumin e tij nga ISP-te operuese.

Së treti studimi në fjalë mund të shërbejë si një indikator për të parë cilët janë ISP-të më të parapëlqyera në vendin tone, pra kush prej tyre ka përthithur më shumë klientë-përdorues në treg.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Së katërti ky studim u vjen në ndihmë studiesve shqiptarë apo dhe atyre të huaj , për të mundësuar krijimin e perceptimit të situatës konkrete mbi gjendjen e internetit në Shqipëri, cilësinë e shërbimit të kompanive më të mëdha që mbulojnë këtë lloj shërbimi në treg sikurse është ofrimi I internetit në Shqipëri, dhe mbi këtë bazë të mbështeten për krijimin e studimeve të reja më të thelluara në të ardhmen.

Tema ka avantazhe pasi tentohet integrimi i rrjetave hibrid nën ombrellën e një protokollit të vetëm.

Avantazhi i kësaj teme është se tenton të shtojë QoS psh në transmetimet VOIP në rrjeta hibride të ndryshme si edhe shtimi i disa karakteristikave të sigurisë në të.

Element sfidues është transferimi i sistemeve video, të cilat mbështeten në QoS. Literatura për këtë është shumë e gjerë dhe fokusimi i saj është shumë i vështirë nga ana praktike.

Një sfidë tjetër është siguria, sidomos siguria duke kaluar nga niveli aplikacioni në nivelin hardware fizik.

Aktualisht ka një mungesë të theksuar të studimeve të kësaj natyre në vendin tone.

Disavantazhi apo problematika që mund të haset është implementimi i sigurisë nga niveli poshtë – lart në rrjeta hibride, për të cilën nuk ka një literaturë të mirëfilltë në botë.

1.2 Motivimi dhe kontributi i temës

Interneti përbën sot një mjet thelbësor komunikimi dhe informimi, por natyra dinamike dhe përmasat e tij bëhen shpesh shkak për degradimin e performancës. Nga ana tjetër kërkesat për shërbimet e ofruara dhe cilësinë e tyre në Internet vjen gjithnjë duke u rritur. Ky zhvillim ka hapur shtegun për studime të komponentëve të ndryshëm të tij si në nivel rrjeti ashtu dhe aplikacioni. Ndër aplikacionet që mbështeten në teknologjinë e Internetit, *Voice over IP* (VoIP) dhe *Video on Demand* (VOD) po fiton gjithnjë e më shumë interesin e përdoruesve por dhe të studiuesve të shumtë. Shpesh përdoruesit përdorin si model referimi për krahasimet e performancës së thirrjeve VoIP rrjetin tradicional telefonik, por Interneti i sotëm, i cili ofron shërbim “best effort”, duket se nuk është ende gati të ofrojë mbështetjen e duhur për cilësinë e thirrjeve VoIP dhe VOD.

BGP është protokollit “de facto” i rrugëzimit *inter – domain* në Internet sot, por ai shfaqet me një natyrë komplekse dhe me çështje performace ende të pazgjidhura. Vetë përmasat e Internetit dhe natyra heterogjene e tij i rrisin vështirësitë me të cilat duhet të përballlet ky protokoll.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Për këto arsye, realizimi i një punimi që ka si objekt kryesor studimin e trafikut në një nga aplikacionet e përhapura, VoIP, dhe protokollin BGP, si lidhësin kryesor në Internet, përbën interes në ditët e sotme.

Objektivi im është të studioj një rast në Shqipëri që përfshin aplikimin e këtij protokollin nga ISP-te respektive dhe të vlerësoj parametrat e cilësive së shërbimit dhe faktorët paralele që kontribuojnë në të duke faktuar rezultatet e përfuara nga simulimet e kryera në kushte laboratorike përmes NS-2.

Qëllimi kryesor i kësaj teze është të realizohet një studim i lidhjes që ekziston mes cilësisë së thirrjeve VOIP dhe rifreskimeve BGP si dhe të studiohet zgjedhja e gjerë e rrugëve në Internet të kryera nga BGP dhe performanca e tanishme e teknikave të kontrollit të rrugëzimit të bazuara në BGP që mund të mbështesin `interdomain Traffic Engineering`.

Në këtë punim janë përdorur simulimet si një metodë me kosto efektive për kërkimet në fushën e rrjetave kompjuterike. Një ambient eksperimental, në themel të të cilit qëndrojnë simulimet, ofron mundësinë e riprodhimit të rezultateve, për të garantuar kështu saktësinë e interpretimeve të tyre. Duke marrë parasysh që simulimet bartin kompleksitet të madh në përcaktimin e topologjive dhe modelime, ngritja e një ambienti të tillë, krijon një bazë për kërkime të mëtejshme mbi një strukturë të provuar. Në aplikojmë C-BGP që të modelojmë një domain të vetëm interneti. Në përshkruajmë çështjet teknike që lidhen me këtë modelim. Pastaj, në aplikojmë metodologjinë tonë në një rrjet ISP të vërtetë. Në vlerësojmë dy skenarë të ndryshëm çfarë-nëse.

Në ndërtojmë kërkesat për një teknikë të tillë të re: ajo duhet të jetë e parashikueshme, e shkallëzuar dhe e dislokueshme në internetin e sotëm. Në propozojmë Peerings Virtual të cilët janë një mjet për dy rrjete bashkëpunuese për të kontrolluar më mirë shtigjet mes njëri-tjetrit. Peerings Virtual kanë përparësitë e mëposhtme. Së pari, ata ofrojnë një kontroll determinist në shtigjet interdomain. Së dyti, ata mund të vendosen në internetin e tanishëm pasi ata janë transparentë në domaine të ndërmjetme.

Diskutimet rreth peshës së madhe që ka sot interneti dhe risitë dhe përparësitë që sjell përdorimi i tij janë të shumta. Pa dyshim që rëndësia e tij është e padiskutueshme. Kur flasim për internetin një aspekt tepër i çmuar është cilësia e shërbimit ose QoS. Pashmangshmërisht kjo lidhet me internetin dhe benefitet që përfitojmë prej tij. Kur gjuajmë internetin që ofrohet nga përgjegjësit përkatës sikurse janë ofruesit e tij ISP (internet service provider) pikëmbështetja është pikërisht QoS. Ky studim është fokusuar në kompanitë e mëdha që operojnë në një vend të vogël në zhvillim, siç është Shqipëria. Për këtë arsye, ky studim sjell kontribute të rëndësishme e me impakt që do t'i shërbejë jo vetëm kompanive operuese të vendit, por edhe studiuesve shqiptarë etj.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Duke qenë një shërbim dhe një drejtim I ri që po lulëzon ne treg ndeshen boshllëqe në plotësimin e studimit me element paraprijës që të kenë pararendur këtë drejtim studimi dhe për këtë arsye I gjithi studimi ka qenë një punë individuale e mirëfilltë.

Ka mjaft rëndësi që për një vend të ri në zhvillim si Shqipëria jonë, të merret në konsideratë si pjesë shembujsh dhe krahasimesh e studimesh prej sa më tepër studiuesish mbarë shqiptarë e të huaj në mënyrë të tillë që me anët positive e negative sepse në fund të fundit e gjitha kjo mund të shërbejë duke na çuar drejt zgjidhjes së problemeve ekzistuese. Duke e pare në periudhë afatgjate, rezultatet e këtij studimi e marra në konsideratë do të mund të përmirësoheshin ndjeshëm duke shtyrë në përmirësimin paraprakisht të aftësive konkurruese të kompanive të mëdha shqiptare brenda vendit si dhe do të nxitet niveli I bashkëpunimit midis bizneseve, qeverisë e universiteteve.

1.3 Burimet e informacionit

Njohuritë e përgjithshme mbi këto koncepte janë përftuar nga hulumtimi i literaturës bashkëkohore në këtë drejtim që shprehin bazat teorike mbi rrjetat, mënyrën e lidhjes mes tyre, sigurinë, protokollet e rrugëzimit të informacionit, besueshmëria në shpërndarjen e paketave etj. Kam studiuar librat me peshën më domethënëse në këtë fushë, si dhe vizituar faqet e portalet e disponueshme që ofrojnë materiale të bollshme për sfondin teorik të temës. Po ashtu një kontribut të vyer për mua kanë dhënë edhe shfletimi i artikujve mbarëbotërorë të cilët ofrojnë studimet e tyre dhe rezultatet me vlerë për zgjerimin e diapazonit të njohurive të përfshira me këtë temë. Zhvillimi i eksperimenteve praktike është realizuar në kompani private ku kam implementuar matjet ne nivel simulimi për hulumtimin e temës. Burimet ku jam mbështetur për hulumtimin e temës përfshijnë Internetin, vëllimet Tanenboun, literaturë mbi rrjetat, computer networks James Curoso, artikuj mbi protokollet BGP, konferencat me IEEE, ACM, USENIX, revista shkencore.

Pra dy burimet bazë të shfrytëzuara për hulumtimin e temës do ti gruponim në:

-Burimet parësore

a) Të dhënat e mbledhura drejtpërdrejt nga anketat e shpërndara drejt përdoruesve të internetit, të cilat janë 524 të plotësuar në total.

Këto të dhëna janë mbledhur nga një pyetësor i përgatitur online enkas për këtë studim ku secili përdorues regjistrohet automatikisht adresa e tij elektronike e kompjuterit dhe nuk kishte mundësi për një plotësim të dytë të anketës, pra të dhënat e grumbulluara janë autentike.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

b) Të dhënat e mbledhura drejtpërdrejt nga simulimet e kryera në kushte laboratorike për matjen e vonës dhe faktorëve që ndikojnë në cilësinë e shërbimit të internetit në aplikacione në kohë reale.

-Burimet dytësore

a) Të dhënat e grumbulluara nëpërmjet literaturës ku përfshihen librat, artikuj, revista shkencore.

b) Interneti dhe mediat elektronike respektive që lidhen me këtë temë.

1.4 Popullata dhe kampioni i studimit

Në fokusin e këtij studimi janë vetëm kompanitë e mëdha që operojnë në Shqipëri, qofshin ato me pronësi shqiptare, të huaj ose të përbashkët në rolin e aktorëve si ofrues të shërbimit të internetit. Lista e plotë me ISP-të operuese në vend është paraqitur në trajtë tabele në vijimësi dhe jep një përmbledhje të kompanive që gjenden në tregun shqiptar për të ofruar këtë lloj shërbimi.

Përsa i përket studimit pra janë marrë në shqyrtim liderat që dominojnë tregun në lidhje me mbulimin e shpërndarjes së internetit drejt përdoruesve vendas. Anketa i është drejtuar për plotësim studentëve të UET si përdorues të internetit.

Ata përbejnë dhe kampionin e popullatës ku prej tyre e kanë plotësuar në mënyrë të 524 prej tyre duke i dhënë përgjigje të tetë pyetjeve të parashtruara për përgjigje.

Pavarësisht nga fakti që popullata është e fundme, kampioni i këtij studimi është kampionim rasti i shtresëzuar.

Për mbledhjen e të dhënave është blerë një sistem anketimi elektronik i cili gjeneron anketat, i administron, i përpunon të dhënat në trajtat e dëshiruara për studim të mëtejshëm. Për mbledhjen e të dhënave janë shfrytëzuar databaza me kontaktet e studentëve të cilët kanë plotësuar anketën në fjalë.

Përsa i përket simulimeve në kushtet laboratorike në shqyrtim si kampion është marrë moduli BGP i instaluar në simulatorin elektronik të rrjetit NS-2. Përmes këtij simulatori është evidentuar efektshmëria që ka updatimi i protokollit BGP të internetit në cilësinë e tij si shërbim të ofruar nga ISP dhe konkretisht jemi fokusuar tek një aplikacion në kohë reale siç është VOIP.

1.5 Metodologjia

Ky punim bazohet në metodën e hulumtimit, metodën e analizës përshkruese, metodën e përpunimit matematikor të të dhënave si ngritja e algoritmave në protokollin BGP, pavarësisht hibridizimit të nënrrjetave. Qendra e temës së punimit është protokollin BGP dhe sfidat e tij. Satelitë të tij janë: QoS, Siguria në nivelin e ulët dhe të lartë, shfrytëzimi i sistemeve operative të ndryshme dhe raporti i tyre me protokollin BGP. Tematika është e gjerë pasi përfshin:

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Sistemet e rrugëzimit të paketave në sisteme hibride dhe integrimi i tyre, matja e vecorive QoS në të, siguria e informacionit, implementimi në sisteme operative të ndryshme. Po ashtu ky punim mbështetet në metodën krahasuese ku rezultatet përballen njëri-tjetrit për ti dhënë përgjigje pyetjeve kërkimore të parashtruara. Rezultatet paraqiten në trajtë grafike.

Paralelisht me anën laboratorike kemi dhe pyetësorin që perfaqëson një rast studimor konkret për vlerësimin e cilësisë së shërbimit të internetit që ofrohet në Shqipëri nga ISP-të. Duke qenë se variablat kanë natyrë përshkruese i klasifikojmë si variabla kategorikë dhe si rrjedhojë mund të kryejmë analizën respektive duke identifikuar numrin e elementeve të frekuencës së përgjigjeve të tyre për çdo pyetje, përqindjet e këtyre frekuencave të përgjigjeve, grafikët përkatës si dhe të gjykohet pavarësia midis variablave, a kanë apo jo ndikim tek njëri tjetri.

Ky punim ka karakter vlerësues përse i përket korrelacionit midis variablave. Një pjesë të rëndësishme të analizës e zë analiza përshkruese e cila krahason rezultatet dhe na jep një ide konçize mbi vërtetimin e hipotezave të parashtruara.

Padyshim që krahas metodave të lartpërmenduar kemi dhe atë që përfshin krahasimin e të dhënave sasiore që rrjedh nga rezultatet e simulimeve me analizat statistikore të raportuara me të dhënat cilësore të studimit empirik që u siguruan nga pyetësorët e shpërndarë tek lista e përdoruesve. Të dhënat janë përpunuar nëpërmjet programit të blerë SurveyMonkey, Gretl, Excel dhe me anë të NS-2.

1.6 Mbledhja e të dhënave dhe përpunimi i tyre

Pyetësori

Të dhënat i përkasin periudhës 2016-2017. Këto të dhëna janë mbledhur përmes një pyetësori i cili përbëhej prej 8 pyetjesh.

Kategoritë e pyetjeve mund ti ndanim në 3 ku përfshihen:

- pyetje të cilat lidhen me cilësinë e shërbimit të internetit,
- pyetje të cilat lidhen me cilësinë e shërbimit të operatorëve ndaj klientit,
- pyetje të cilat lidhen me shpërndarjen në zotërim të tregut prej kompanive ISP në vend.

Në pjesën më të madhe të rasteve përgjigjet e pyetësorëve janë të përshkallëzuara në 4 raste duke nisur nga shkëlqyer, shumë mirë, kënaqshëm e deri në të pakënaqur. Ky pyetësor është një kombinim i disa pyetësorëve në vendet e huaja të cilat zhvillohen me qëllim të vlerësimit të QoS të internetit.

Pyetësori jep një informacion të përgjithshëm mbi qasjen që ka përdoruesi në lidhje me cilësinë e shërbimit të internetit të ofruar nga ISP-të në Shqipëri.

Simulimi

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Të dhënat i përkasin periudhës 2015-2017. Janë zhvilluar simulime laboratorike nëpërmjet simulatorit të rrjetit NS-2 në kohë reale të cilat fokusohen në faktorët që lidhen me cilësinë e shërbimit të internetit nga updatimi i protokollit të internetit BGP.

Pra shohim konkretisht si funksionon interneti nëpërmjet ndërhyrjes që ne kryejmë në protokollin e tij të pasqyruar në aplikacion në kohë reale si VOIP.

Përpunimi i të dhënave

Të dhënat e mbledhura përmes pyetësorit janë automatikisht të përpunuara nga programi analizues i anketimit survey monkey. Më pas kalojmë në analizën përshkruese statistikore. Këtu ne përdorim programet statistikore për analizë të mëtejshme. Duke qenë se kemi të dhëna që janë variabla kategorikë , variabla cilësore, klasifikimi atëherë ne mund të vlerësojmë tre pika ku përfshihen numri i elementeve, përqindja e frekuencës së përgjigjeve për secilën kategori respektive si edhe të ndërtojmë grafikët përkatës. Kjo lloj analize përshkruese statistikore jep një vizion të përmbledhur mbi rezultatet e punimit. Këtu ne shohim përgjigjet e mbledhura të studimit në trajtë përqindjesh. Përmes saj mundësohet identifikimi paraprak i disa prej variablave më me peshë të rëndësishme si dhe shpjegimi i variablit kryesor të varur që në situatën tonë është cilësia e shërbimit të internetit, QoS. Nga përfundimet që nxjerrim mund të shohim dhe pavarësinë mes variablave. Pra a ndikon një variabël tek një tjetër. Gjithashtu mund të shohim nëse kemi apo jo variabla të kushtëzuar.

Nga ana tjetër në lidhje me simulimet laboratorike përsa i përket pjesës eksperimentale përpunimi është realizuar nga programi që ekzekuton kodet NS-2 i cili në bashkëpunim me Nam, interpretuesi vizual i topologjisë të rrjetit (Network Animator) i cili bën interpretime të rrjetit duke ofron animacion të nivelit paketë dhe grafikë (grafe) të protokolleve specifike për të ndihmuar në hartimin dhe kontrollin e gabimeve (debugging) e protokolleve të reja të punës në rrjet (net-work). Duke marrë të dhëna nga simulatorët e rrjetit (si Ns-2) ose prej rrjeteve dretpërdrejt (live), Nam ishte një nga mjetet e para për qëllimin e përgjithshëm për të siguruar vizualizimin e animuar të rrjetit dhe të nivelit të paketave. Nam tani integron subjekte të ngjarjeve në kohë tradicionale të veprimeve të protokolleve dhe aftësive redaktuese të skenarëve. Ai ofron interpretim vizual të rrjetit dhe topologjisë dhe ekzekutim të drejtpërdrejtë të skriptit Tcl. Po ashtu mjet i dytë për simulim me Ns-2 është përveç Nam edhe gjuha e skriptimit AWK e cila është një gjuhë programimi procesimi testesh duke e kthyer në një mjet ndihmës për performimin e punëve procesuese të teksteve të thjeshta e komplekse.

1.7 Modeli teorik

Performanca e BGP (si elementi kryesor lidhës për Internetin) mbetet dhe sot një çështje e hapur studimi veçanërisht për sa i përket kohës së konvergencës. Griffin *et. al* [1] e kanë cilësuar mundësinë që një grup AS-sh të shkëmbejnë pafundësisht mesazhe

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

rrugëzimi BGP, pa konvergjuar në një bashkësi rrugësh të qëndrueshme, si “*problem i konvergjencës së BGP*”. Labovitz *et. al* [2], [3] matën ndryshimet në rrugëzim në Internet dhe treguan se mund të ekzistojë një vonesë e konsiderueshme në konvergjencën e BGP dhe se një nivel i lartë i luhatjes të rrugës gjatë një konvergjence të zgjatur ka një ndikim të madh në trafikun *end-to-end*, duke shkaktuar humbje paketash dhe të lidhjes. Gjithashtu Wang *et. al* [4], [5] kanë treguar se ngjarjet e rifreskimit të BGP lidhen ngushtë me periudha humbjesh paketash dhe vonesash. Këto punime kanë studiuar ndikimin e momenteve të rifreskimit të BGP në cilësinë e rrjetit megjithatë asnjëra nuk ka patur në fokus ndikimin e “problemit të konvergjencës” në aplikacione të ndryshme.

Nga ana tjetër VoIP përbën një fushë aktive kërkimore në drejtim të cilësisë së thirrjeve “cross domain”. Tobagi *et. al* [6] shtruan një pyetje konkrete dhe ende bashkëkohore: “A është interneti gati për VoIP dhe VOD?!”. Matjet e realizuara prej tyre në rrjeta *backbone* të Internetit evidentuan se disa prej tyre shfaqin karakteristika të padëshirueshme që nuk mund të trajtoheshin me masat ekzistuese. Amir *et. al* [7] në një studim të mëvonshëm thekson nevojën për përmirësimin e aplikacioneve VoIP si rrjedhojë e faktit se modeli ekzistues i shërbimit në Internet nuk ofron garanci për cilësi shërbimi. Ky studim, si dhe të tjerë para tij [8], [9], [10], [11] ofrojnë disa zgjidhje për përmirësimin e performancës së VoIP por rezultatet e përfuara i mbështesin në vlera statistikore në nivel paketash, si vonesat dhe humbjet. Ka plot studime mbi temat që lidhen me VoIP në lidhjet “cross-domain” por ajo që synohet të realizohet në këtë punim është një studim i lidhjes që ekziston midis cilësisë së thirrjeve VoIP dhe rifreskimeve BGP, në nivel përdoruesi.

Kushman *et. al* tek [12] kanë treguar se niveli i përdorimit të VoIP ndikohet nga konvergjenca e ulët e BGP po aq sa ndikohet dhe nga mbingarkimi i rrjetit. Ky studim ndryshe nga të më sipërmir bazohet në simulime. Bacioccola *et. al* [13] kanë treguar se përlllogaritja e performancës në nivel IP (siç ndodh rëndom në ns-2) nuk rezulton gjithmonë e saktë dhe kanë ofruar një modul për ns -2 që lejon vlerësimin e performancës së VoIP në nivel përdoruesi. Nga ana tjetër në [14] tregohet se moduli ns-BGP i krijuar për simulimin e BGP në ns2 ka algoritma dhe struktura të brendshme të dhënash që janë të përshkallëzueshme në terma numri lidhjesh të palëve dhe përmasa të tabelave të rrugëzimit.

Të dy këto module dhe ambjenti i ns2 përbëjnë bazën mbi të cilën do të realizohet modelimi i sistemit.

1.8 Organizimi i kapitujve

Vazhdimi i këtij punimi është i organizuar si më poshtë vijon:

Kapitulli 2 siguron njohuritë bazë në lidhje me protokollin e rrugëzimit në Internet, BGP. Ai jep një tablo të disa nga tiparet karakterizuese me kyçe të tij duke na njohur paraprakisht me ndërtimin, strukturën dhe strategjinë e funksionimit të tij dhe Shohim tipet e rrugëzimit dhe në veçanti mënyrën si kryhet konkretisht rrugëzimi me këtë

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

protokoll specifik. Evidentojmë paqëndrueshmëritë e tij dhe gjithashtu trajton një nga çështjet kryesore të lidhura me performancën e tij, kohën e konvergencës.

Kapitulli 3 ne aplikojmë C-BGP që të modelojmë një domain të vetëm interneti. C-BGP lejon një operator rrjeti për të ndërtuar një model të rrjetit të tij dhe të injektojë konfigurimin, rrugëzimin dhe trafikun e të dhënave me qëllim të hetimit të skenarëve çfarë-nëse. Ne përshkruajmë çështjet teknike që lidhen me këtë modelim. Pastaj, ne aplikojmë metodologjinë tonë në një rrjet ISP të vërtetë. Ne vlerësojmë dy skenarë të ndryshëm çfarë-nëse. Në rastin e parë, do të hetojmë ndikimin e shtimit ose heqjes së peerings në rrugëzim. Në skenarin e dytë, ne vlerësojmë ndikimin e lidhjes së vetme dhe dështimet e routerit të vetëm në rrugëzim. Bazuar në një studim të tillë, një operator i rrjetit mund të përcaktojë se cilat lidhje duhet të mbrohen në mënyrë që të sigurojmë një shërbim elastik për dështimet. Në pjesën e tretë të tezës, ne nuk e kufizojmë modelimin në një domain të vetëm, por shtrihet tek një ndërlidhje e madhe të rrjeteve. Ne aplikojmë mjetin e modelimit në një rrjet të internetit, për të studiuar efikasitetin e teknikave aktuale të inxhinierisë së trafikut të bazuar në BGP. Ne përshkruajmë se si është kryer sot inxhinierimi i trafikut. Ne shpjegojmë se kontrollimi i trafikut që lë një ISP është i mundur meqë vetëm një kontroll lokal është i nevojshëm. Në të kundërt, kontrolli i trafikut që vjen në drejtimin e kundërt është më i vështirë pasi rrugëzimi në domain-e të largët duhet të ndikohet. Në bazë të simulimeve në shkallë të gjerë të BGP, ne tregojmë se shumë vendime rrugëzimi në modelin e internetit janë marrë rastësisht. Përveç kësaj, një rrjet në internet ka një pamje shumë të kufizuar të të gjithë topologjisë. Kjo kufizon zbatueshmërinë e teknikave inxhinierike të trafikut të tilla si AS - Path prepending ose rishpërndarja komuniteteve. Ne konkludojmë se nuk është kështu një nevojë për të zhvilluar një mekanizëm të ri inxhinierie trafiku. Ne propozojmë Peerings Virtual të cilët janë një mjet për dy rrjete bashkëpunuese për të kontrolluar më mirë shtigjet mes njëri-tjetrit.

Kapitulli 4 trajton elementët kryesorë VoIP dhe metodat e vlerësimit të cilësisë së thirrjeve VoIP. Veçanërisht, për matjen e cilësisë së VoIP, trajtohet Modeli E dhe MOS. Këtu në këtë kapitull analizohen disa prej pritshmërive ndaj aplikacioneve VOIP në rrjet, jepen disa njohuri bazë mbi koduesit e zërit, rrugën si kryhet paketizimi, po ashtu trajtohet koncepti i Jitter buffer me njohuri të përgjithshme dhe së fundmi ndalemi tek matja e cilësisë së VOIP.

Kapitulli 5 siguron disa njohuri të nevojshme mbi simulimet dhe simulatorin e rrjetit ns-2. Gjithashtu në këtë kapitull përshkruhen dhe dy modulet e nevojshme për realizimin e ambientit të integruar eksperimental. Në këtë kapitull trajtohen simulimet duke përfshirë elementet, simulimet që varen nga koha, trajtohet simulatori i rrjetit ns-2, arkitektura e tij, direktoritë e përfshira dhe po ashtu përmendet përdorimi i ns-2.

Ne përshkruajmë përpjekjet për të ofruar një model sa më të përshtatshëm simulimi dhe eksperimente sa më të plota për të treguar se trafiku i VoIP ndikohet nga koha e konvergencës së BGP. Ai trajton modelin e simulimit duke dhënë strukturimin e ndërtimit të rrjetit. Po ashtu këtu preket shkurtimisht topologjia e rrjetit, ashtu sikurse dhe struktura njëdrejtimore e rrugëzimit ns-2 si edhe struktura njëdrejtimore e rrugëzimit ns-2-BGP. Në këtë kapitull gjejmë të përmendur klasifikuesin IPV4, rmodule BGP,

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

rtProtoBGP, TcpSockets, BGPTimer, VecRoutes, dampreuse-timer, dampinfo, gjeneratorin e topologjisë GT-ITM. Këtu është trajtuar modeli i rrugëzimit, ndërtimi i modelit të të dhënave, gjendja e rrjetit dhe vlerësimet e performancës dhe së fundmi vihen në dukje ndryshimet në model.

Këtu përmbledhim rezultatet e simulimeve të realizuara dhe interpretimet përkatëse. Ne shohim që jepet verifikimi i modelit të përzgjedhur të rrugëzimit, kryhen disa simulime të topologjisë Stub-Domain me trafik CBR dhe shpalosen rezultatet e simulimit.

Kapitulli 6 përfshin studimin e anketës së zhvilluar, rastit studimor që është marrë në shqyrtim për vlerësimin e cilësisë së shërbimit të internetit të ofruar nga Internet service provider-at shqiptarë. Jepet një analizë e të dhënave të grumbulluara nga përdoruesit shqiptarë të përfshirë në pyetësor dhe listohen edhe të gjitha përgjigjet në përballjen e dy grupeve të ekstremiteteve në kategoritë e përgjigjeve. Pra kemi dhe renditjen e përgjigjeve të filtruara të grupit të shkëlqyer kundrejt atyre të pakënaqur me QoS e internetit.

Konkluzione përshkruan konkluzionet e arritura përmes këtij punimi dhe shtron disa drejtime të mundshme për punë të ardhme kërkimore, në këtë fushë.

Kapitulli II

Border Gateway Protocol – BGP

2.1 Hyrje

Që nga koha kur është krijuar interneti ose siç njihet ndryshe World Wide Web (WWW), ka pësuar ndryshime si në aspektin e topologjisë por gjithashtu edhe në shkallëzueshmërinë e tij. Në ditët e sotme mund të jenë me miliarda nje të vogla që komunikojnë me njëra-tjetrën duke shkëmbyer të dhëna. Për të përballuar gjithë këtë ngarkesë duhet të aplikohen protokolle të fuqishme rrugëzimi për të garantuar Cilësinë e Shërbimit (QoS). Ka disa mënyra komunikimi në internet: one-to-one ose *Peer2Peer*, one-to-many ose *multicast*, one-to-all ose *broadcast*. Çfarëdo protokollit rrugëzimi të përdoret 2 nga funksionalitetet kryesore të tij do të jenë: 1) Gjetja e rrugës optimale për në destinacion, si dhe 2) Dërgimi i informacionit të dëshiruar data.

Nisur nga përmasat e Internetit sot do të ishte shumë e vështirë për një autoritet të vetëm ta manaxhojë atë. Për këtë arsye Interneti është strukturuar në formën e një federate të gjërë *Sistemesh Autonome (AS)* siç paraqitet në mënyrë të thjeshtuar në figurën më poshtë:

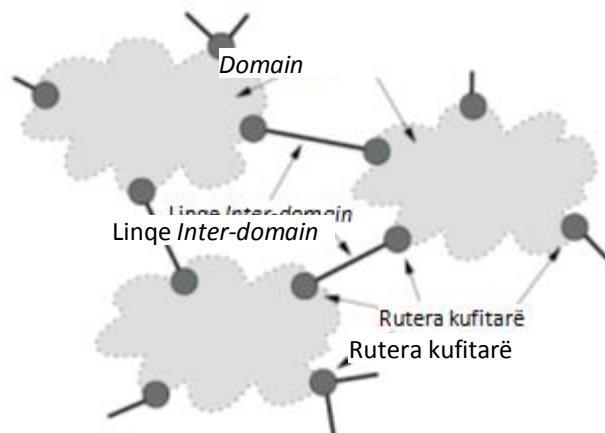


Figura 2.1: Sistemet Autonome

Çdo AS administrohet në mënyrë të pavarur nga një autoritet i vetëm, si një universitet, një kompani ose një agjenci shtetërore. Në mënyrë të përgjithëshme dhe nga këndvështrimi i kësaj teme, mund të thuhet se një AS është një bashkësi ruter-ash që ndajnë të njëjtat politika rrugëzimi dhe janë nën të njëjtin autoritet administrative.

Në ditët e sotme BGP konsiderohet si standardi de-facto për rrugëzimin e paketave në Internet. Objektivi i tij kryesor është shkëmbimi i informacionit ndërmjet Sistemeve

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Autonome mbi lidhjet ekzistuese dhe aftësinë për të mbërritur një destinacion në një rrjet. Interneti në ditët e sotme përbëhet nga mijëra Sisteme Autonome të lidhur me njëri-tjetrin, të cilat mund ti përcaktosh si një set router-ash dhe rrjetesh që ndodhen nën të njëjtin administrim. Një sistem autonom tipik është një rrjet universiteti, korporate ose një ISP. Një AS identifikohet nga një numër 16-bit. Ky numër jepet nga autoritetet e numërimit në të njëjtën mënyrë sesi shpërndahen adresat IP. Rrugëzimi në internet varet nga rrugëzimi ndërmjet AS si dhe nga rrugëzimi brenda këtyre sistemeve.

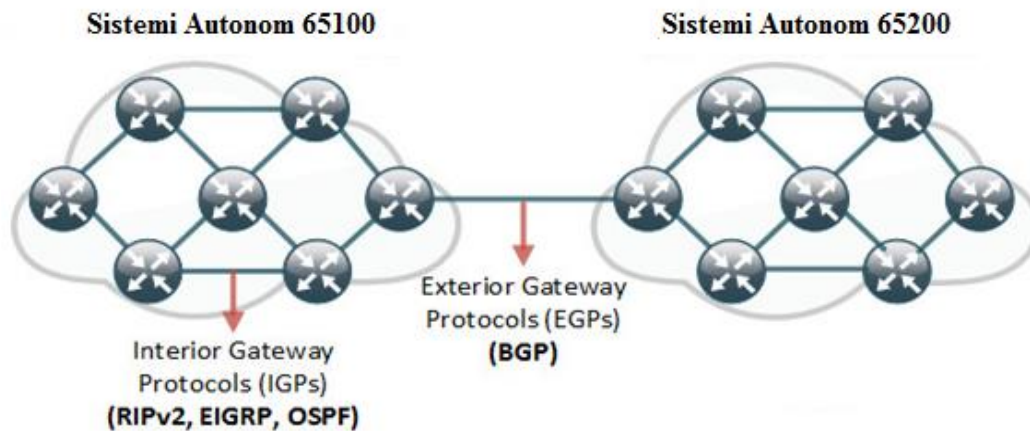


Fig 2.2 – Paraqitja e fushës së veprimit të protokolleve të rrugëzimit

Brenda të njëjtit sistem router-at aplikojnë *Interior Gateway Protocols* (IGP) për të zbuluar dhe për të shkëmbyer informacion rreth rrjeteve të brendshme me të cilat janë lidhur direkt. Router-at nga AS të ndryshme përdorin *Exterior Gateway Protocols* (EGP), për të shkëmbyer informacione mbulimi dhe për të përcaktuar rrugën nga fillimi në fund për paketa që kalojnë ndërmjet disa sistemeve. Në kufij të çdo AS, router-at fundorë të BGP shkëmbejnë informacion mbi blloqet e adresave IP, të cilat quhen ndryshe *prefikse*. Çdo prefiks konsiston nga një adresë 32-bit dhe një gjatësi maske që tregon madhësinë e rrjetit. Për shembull, 192.168.1.0/24 përfaqëson një bllok prej 256 adresash që fillojnë me 192.168.1.0 dhe mbarojnë me 192.168.1.255.

Protokolli BGP i përdorur në Internetin e ditëve të sotme është BGPv4 [15].

2.2 Rrugëzimi në Internet

Ruterat në një rrjet mbështeten në protokolle rrugëzimi për të zbuluar dhe përpunuar shtegun më të mirë për shkëmbimin e informacionit. Protokollet e rrugëzimit në Internet mund të ndahen në dy 2 kategori protokollesh rrugëzimi ku përfshihen të gjitha protokollat e sotme:

- 1) *Interior Gateway Protocols* (IGP) - mundësojnë rrugëzimin brenda një AS-je (*intra domain*), ku përfshihen Routing Information protocol (RIP),

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Open Shortest Path first (OSPF), Enhanced Interior Gateway Protocol (EIGRP) dhe Intermediate System to Intermediate System (IS-IS). Të gjitha këto protokolle funksionojnë brenda një Sistemi Autonom (AS).

2) **Exterior Gateway Protocols (EGP)** - mundësojnë rrugëzimin ndërmjet AS-ve të ndryshme (*inter domain*), ku edhe BGP bën pjesë pikërisht në këtë grup protokolle.

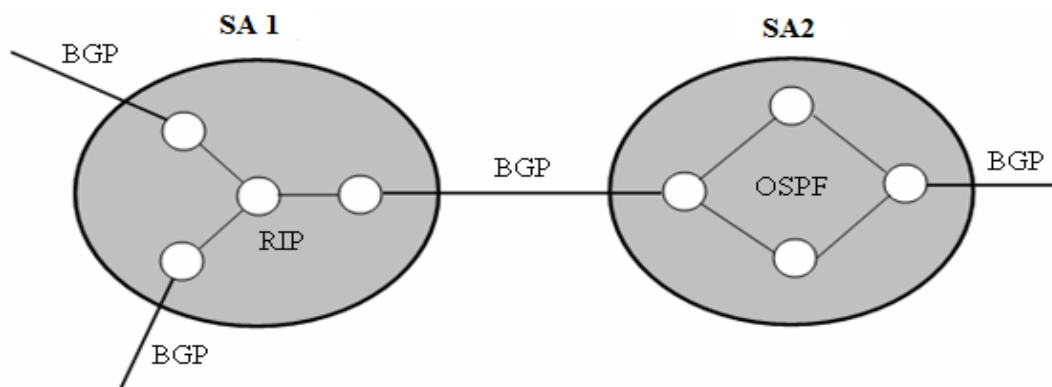


Fig 2.3 – Protokollat e rrugëzimit brenda dhe jashtë Sistemit Autonom

Më sipër paraqitet figura ku tregohen llojet e protokolleve gateway si dhe fushën e veprimit të tyre. Siç tregohet BGP është protokollin që vepron midis sistemeve autonome, të cilat zakonisht janë ISP.

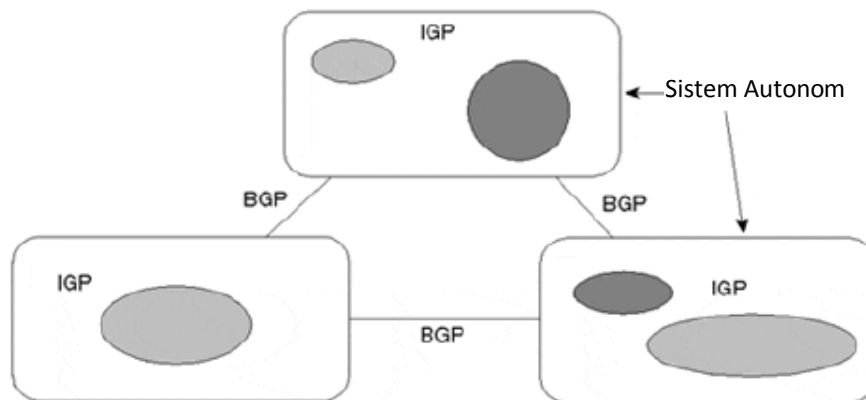


Figura 2.4: Protokollat e rrugëzimit në Internet

Rrugëzimi *inter domain* është një komponent i rëndësishëm i rrugëzimit në Internet, me që një sasi e madhe e trafikut përshkon më shumë se një AS. Për më tepër, fakti se çdo AS manaxhohet nga një autoritet i ndryshëm e komplikon situatën krahasuar

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

me rrugëzimin *intra domain*. Në këtë të fundit, të gjitha burimet administrohen nga i njëjti autoritet. Ky autoritet mund të përdorë të gjitha burimet brenda një AS-je dhe qëllimi kryesor është rrugëzimi i paketave në mënyrën më efektive të mundshme (ky rrugëzim zgjidhet përmes një protokollit IGP). Por, në rrugëzimin *inter domain*, autoritete të ndryshme mund të kenë interesa të ndryshme që mund të lidhen dhe me konkurrencën në biznes. Këto ndryshime kanë një impakt të madh në rrugëzim (për këtë arsye nevojitet një protokoll kompleks i tipit EGP –*Exterior Gateway Protocol*).

Për shembull: Zakonisht AS-të nuk duan të tregojnë topologjitë e brendshme të rrjetit apo politikat e përdorura, dhe zakonisht zgjedhin politika rrugëzimi që nga të cilat mund të përfitojnë më shumë vetë. Si rrjedhojë, rrugëzimi *inter domain* është i komplikuar me që duhet të reflektojë karakteristikat e mëposhtme:

- Çdo AS duhet të jetë në gjendje të shprehë politikat lokale që reflektojnë interesat e biznesit të saj.
- Protokollin ka nevojë të jetë i përshkallëzueshëm. Në terma përshkallëzimi, protokollin duhet të marrë në konsideratë numrin e madh të AS-ve, prefikseve IP dhe shtegjeve potenciale të pranishme në Internet. Së pari, numri i AS-ve të lajmëruara në Internet është gjithmonë në rritje. Së dyti, çdo AS mund të lajmërojë prefikse të ndryshme dhe numri i prefikseve kohët e fundit po rritet më shpejt se ai i AS-ve. Së fundmi, çdo AS mund të mësojë më shumë se një shteg për çdo prefix, kështu që numri i shtegjeve në Internet rritet edhe më shumë.
- Privatësia e çdo AS duhet respektuar. Në Internetin aktual, rrugëzimi ndahet në *intra domain* dhe *inter domain*, në mënyrë që një AS mund të shmangë ndarjen e detajve të brendshme me të jashtëmit. Kjo ndarje jo vetëm që përmirëson sigurinë por dhe ndihmon në kufizimin e efekteve të dështimeve të brendshme.

Më sipër përmendëm që Interneti është i organizuar në AS (ose *domain*-e) që mund të kenë një, dy ose qindra nyje dhe janë të lidhura me njëri tjetrin. Por një karakteristikë tjetër e Internetit është se këto nyje i nënshtrohen një hierarkie të imponuar që vjen nga klasifikimi i AS-ve në “*AS fundore*” dhe “*AS tranzit*”. Një AS është i tipit të parë nëse shtegu që lidh çdo dy nyje u ose v mbetet në atë AS vetëm nëse u ose v janë në të njëjtin AS. Qëllimi i AS tranzit është që të ndërlihdë AS fundore dhe nuk i nënshtrohen kufizimit të mëparshëm. AS tranzit përfshin një bashkësi nyjesh kryesore mbështetëse që zakonisht janë të lidhura shumë mirë menjëra-tjetrën. Secila nga këto nyje lidhet me një AS fundor përmes nyjeve ndërmjetëse (*gateway*). Disa prej këtyre nyjeve mund të lidhen dhe me AS të tjera tranzit. E gjitha kjo ilustron në figurën më poshtë:

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

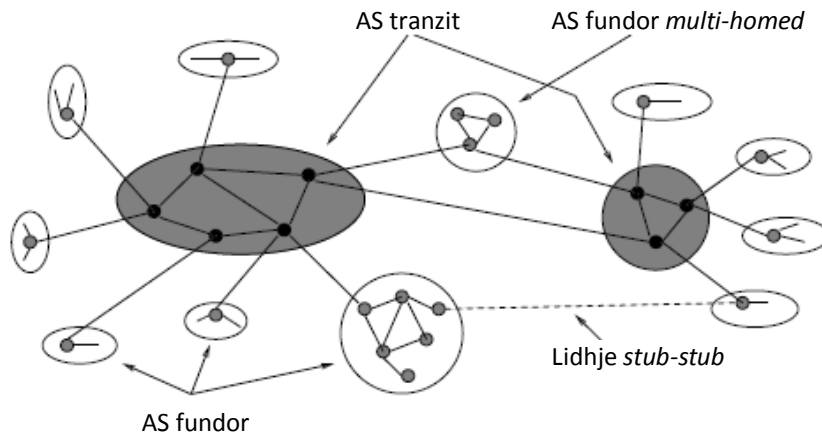


Figura 2.5 Klasifikimi i AS-ve

AS fundore mund të klasifikohen në “single homed” ose “multi-homed”. Këto të fundit kanë lidhje me më shumë se një AS tranzit ndërsa të parët lidhen vetëm me një AS tranzit. Disa fundore lidhen dhe me AS të tjera fundore.

2.3 BGP: Një protokoll për rrugëzimin “*inter domain*”

Border Gateway Protocol (BGP) është thjesht një protokoll tjetër rrugëzimi, por me një rol shumë të ndryshëm nga të tjerët me që shërben si lidhësi që mundëson funksionimin e Internetit. Për më tepër, fakti se çdo AS manaxhohet nga një autoritet i ndryshëm e komplikon situatën krahasuar me rrugëzimin *intra domain*.

BGP implementohet në ruter-a dhe mesazhet shkëmbehen përmes një lidhjeje të qëndrueshme TCP midis dy ruter-ave (duke thjeshtuar kështu kompleksitetin e implementimit të besueshmërisë së transportit).

Ruter-at që ekzekutojnë një process rrugëzimi BGP njihen si *folësa BGP*. Dy folësa BGP që krijojnë një lidhje TCP me njëri tjetrin, me qëllim shkëmbim informacion rrugëzimi, cilësohen si *fqinjë* ose *palë* në komunikim.

Trafiku që kalon nëpër një AS klasifikohet në *trafik lokal* ose *trafik tranzit*. Trafiku lokal vjen nga ose përfundon në AS ku gjendet adresa IP e burimit ose destinacionit. Çdo trafik tjetër që përshkon këtë AS përbën “trafik tranzit”. Një qëllim i rëndësishëm i BGP në Internet është pikërisht *zvogëlimi i trafikut tranzit*.

Nisur nga sa thamë për trafikun, mund të pohojmë se një ruter BGP mund të komunikojë me ruter-a të tjerë BGP që ndodhen në të njëjtën AS me të (njihet si I-BGP) ose në AS të tjera, të ndryshme (njihet si E-BGP).

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Të gjithë ruter-at që “flasin” I-BGP Brenda të njëjtit AS duhet të krijojnë lidhje me njëri-tjetrin sipas modelit “*fully connected mesh*”. Këto lidhje jo detyrimisht duhet të jenë fizike, mjafton që këto rutera të kenë të ngritur një kanal komunikimi të besueshëm, TCP, mes tyre. Me që nuk ka një mekanizëm për detektimin e cikleve të pafunda në I-BGP, ruter-at që “flasin” I-BGP nuk duhet të përcjellin informacion rrugëzimi të palëve të treta ndaj fqinjëve të tyre. Ruter-at E-BGP, ndryshe nga të mëparshmit, mund të lajmërojnë informacion të palëve të treta tek fqinjët e tyre E-BGP.

Figura në vijim tregon ruter-at R1, R2, dhe R3 që përdorin I-BGP për shkëmbimin e informacionit të rrugëzimit brenda të njëjtës AS, dhe çiftet e ruter-ave R4-R2, R3-R5, dhe R4-R5 që përdorin E-BGP për shkëmbimin e informacionit të rrugëzimit mes AS-ve.

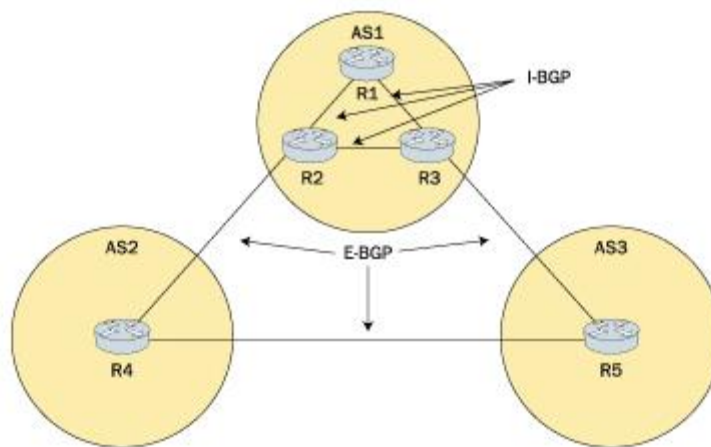


Figura 2.6: Internal BGP (I-BGP) përkundrejt external BGP (E-BGP)

Siç kemi thënë më sipër, BGP është një protokoll i përdorur për të mirëmbajtur informacionin e rrugëzimit midis AS-ve. Pjesa më e madhe e protokolleve të rrugëzimit *intra-domain* bazohen në algoritmin Dijkstra. Por BGP, është një protokoll që bazohet në “vektorin e shtegut” (*path-vector*) që nënkupton se informacioni i rrugëzimit përmban një vektor me ASN (çdo AS-je i vihet në dispozicion një numër në rendin 0 – 65535) që tregojnë shtegun e AS-ve që përshkon një prefiks i caktuar (çdo AS zotëron gjithashtu një rend adresash IP të cilat mund të vendosë ti ndajë në grupe më të vogla që përmbajnë disa adresa IP të vazhdueshme të njohura si Prefix IP.). Bazuar në informacionin e shkëmbyer mes ruter-ave BGP ndërtohet një graf Sistemesh Autonome (i njohur dhe si *pemë*).

2.3.1 Karakteristikat e funksionimit të BGP

Për sa i përket BGP:

I gjithë Interneti është një graf AS-sh, lidhjet midis dy AS-ve vормojnë një shteg, koleksioni i informacionit mbi shtegjet formon një rrugë drejt një destinacioni specific

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

dhe rrugëzimi brenda një sistemi autonom realizohet përmes IGP. Figura 2.3.2 ilustron konceptin e pemës së shtigjeve:

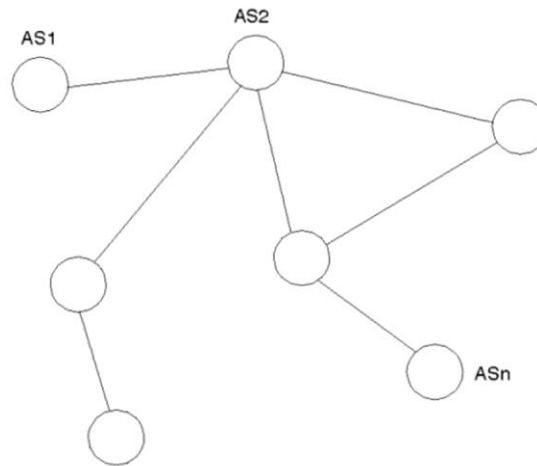


Figura 2.7: Pema e shtigjeve të AS

Katër tipa mesazhesh janë të specifikuar për BGP [16]:

- *Mesazhi i hapjes* – janë mesazhet e para që dërgohen dhe hapin një seksion komunikimi me s palëve
- *Mesazhet e rifreskimit* – sigurojnë rifreskimet mbi rrugëzimet duke lejuar ndërtimin e një pamjeje të qëndrueshme mbi topologjinë e rrjetit. Këto mesazhe bëjnë të mundur dhe shfuqizimin e rrugëve të papërshtatshme dhe lajmërimin e rrugëve të reja. Shfuqizimet e rrugëve dërgohen kur një ruter mer një vendim të ri lokal që një rrjet nuk është më i arritshëm. Një lajmërim rruge tregon që një ruter ka mësuar për lidhjen e një rrjeti të ri ose ka ndryshuar politikën duke zgjedhur një rrugë të re të preferuar për një rrjet destinacion. Pas marrjes së mesazhit çdo nyje vendos se çfarë do bëjë me të (psh. të ndryshojë tablën e rrugëzimit) dhe në se do ta përhapë më tutje këtë mesazh. Të dyja këto vendime meren në përputhje me politikat e AS
- *Mesazhet e lajmërimit* – Dërgohen në rast gabimesh për të informuar pjesmarrësit në seksionin aktiv mbi arsyet e mbylljes së këtij seksioni.
- *Mesazhi “mbaje-gjallë”* - i lajmëron palët BGP se një pajisje është active dhe seksioni nuk duhet mbyllur. Ruter-at BGP nuk kanë një pamje të plotë të topologjisë të rrjetit. Çdo ruter di vetëm si të arrijë fqinjët direkt dhe veçanërisht përmes kujt fqinji në veçanti mund të arrihet një Prefiks Rrjeti.

2.3.2 Rrugëzimi i BGP

Pjesa më e madhe e protokolleve të rrugëzimit marrin informacione rrugëzimi, e përdorin atë për të ndërtuar tabelat e rrugëzimit dhe i ndajnë këto tabela (ose pjesë të tyre) me ruter-a të tjerë në rrjet. Ajo që e bën BGP një protokoll unik është aftësia e tij për të zbatuar politika ndaj informacionit të përmbajtur në mesazhet e rifreskimit, dhe për rrjedhojë përzgjedhja e informacionit rifreskues bazuar në atributet e vetë informacionit. Politikat e rrugëzimit përcaktojnë mënyrën se si manaxhohen rrugët e mara nga nyjet BGP dhe si ja dërgon këtë informacion këtyre nyjeve. Në shumë raste, politikat e rrugëzimit konsistojnë në filtrimin e rrugëve, pranimin e disa rrugëve, pranimin dhe modifikimin e rrugëve të tjera dhe kundërshtimin e disave. Kur mesazhet e rifreskimit meren nga një ruter BGP, ato i nënshtrohen një procesi përpunimi në përputhje me një seri politikash të cilat përcaktojnë se si dhe ku do të ruhet informacioni. Në mënyrë që të lejohet ky kontroll mbi përzgjedhjen e rrugës, lajmërimeve të BGP i janë shtuar disa attribute që lejojnë ndryshimin e vendimeve në bazë të vlerave të tyre. Ruter-i krahason vlerat e këtyre attributeve për çdo rrugë, sipas një liste të renditur dhe përzgjedh rrugën që ka vlerat më të pranueshme për atributin. Nëse vlerat janë të njëjta, kalon tek atributi pauses. Rruga e përzgjedhur do jetë ajo që do përdoret për të përcjellë paketat. Përmes attributeve bëhet e mundur që një rrugë më e gjatë (që kalon nëpër më shumë AS) të përzgjidhet ndaj një më të shkurtër (këto attribute janë shumë të përdorshme në rrjetat e ISP-ve).

Koncepti i funksionimit të BGP mund të përmblihet në figurën më poshtë:

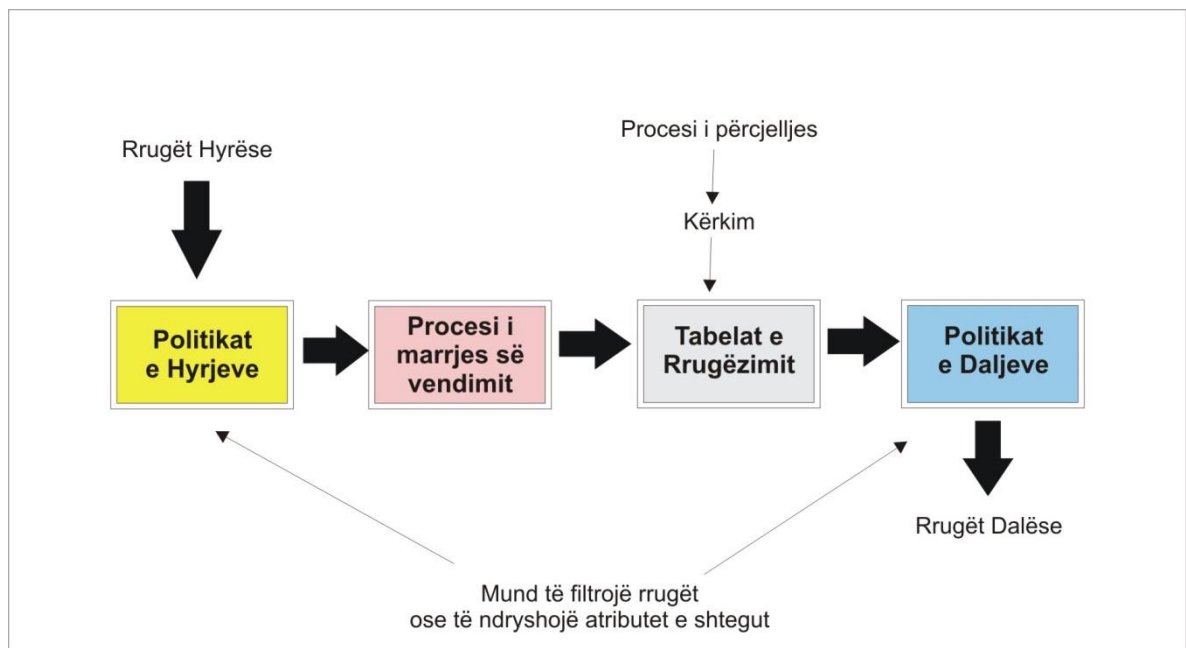


Figura 2.8: Funksionimi i BGP – Politikat e rrugëzimit

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Një folës BGP vetëm një shteg (rruga e preferuar) mund të përdoret për një destinacion dhe është e ndaluar të përhapen rrugë të ndryshme nga ajo e preferuara në përdorim. Kur merret një lajmërim i ri, shfrytëzohen politikat e implementura të rrugëzimit për të parë nëse rruga e re është më e mirë se ekzistuesja. Nëse ky është rasti, rruga e vjetër zëvendësohet me atë të marrë së fundmi. Më pas, nëse politikat e lejojnë, rruga i lajmërohet fqinjëve.

Psh. një ruter mund të ketë një politikë që përcakton se ai nuk do të aksesojë kurrë rrjetin 165.113.0.0 përmes AS 1159. Kështu që nëse një mesazh rifreskimi përmban informacion për arritshmërinë nëpër një shteg drejt 165.113.0.0 përmes AS 1159, ky informacion nuk do të lejohet nga mekanizmi i politikave që të arrijë tabelën e rrugëzimit duke shkaktuar që ruter të mos ta përdorë asnjëherë këtë shteg. Politika mund të mos jetë tërësisht diskriminuese duke e përcaktuar një rrugë jo të papërdorëshme por thjesht të pa dëshirueshme duke bërë të mundur që procesi i rrugëzimit ta konsiderojë destinacionin përmes këtij shtegu, shumë të largët. Këto që përmendëm njihen si politika të hyrjes. BGP lejon gjithashtu edhe implementimin e politikave të daljes (psh. “mos dërgë asnjë informacion mbi 165.113.0.0 tek AS47.”) ose të ndryshojnë atributet e rifreskimeve bazuar në informacionet e politikave të përcaktuara. Pra politikat mund të konsiderohen si një mënyrë për të filtruar rrugët brenda dhe jashtë sistemit.

BGP është një protokoll *rritës (inkremental)*. Kur një ruter lidhet për herë të parë me një fqinj, transmetohet tabela e plotë e rrugëzimit BGP. Pas kësaj, nuk dërgohen rifreskime të rregullta mbi informacionin e rrugëzimit përveç rastit kur ka ndryshime në rrugë. Në teori mesazhet duhet të dërgohen vetëm kur lajmërohet një rrugë e re, rifreskohet (pasqyrohen ndryshimet) apo shfuqizohet një rrugë. BGP kërkon që çdo ruter të ruajë informacionin e marrë nga çdo fqinj si dhe informacionin që i ka dërguar fqinjëve të tjerë.

Në mënyrë që të rrugëzohet një paketë të dhënash në një rrjet të caktuar, nevojitet identifikimi dhe përcaktimi i vendodhjes të rrjetit destinacion. BGP përdor *rrugëzimin me Prefiks* për të adresuar rrjetat. Prefiksi i një rrjeti bazohet në idenë e përcaktimit të një identifikuesi për çdo rrjet në mënyrë që për çdo paketë të dhënash të jetë e qartë nëse destinacioni ndodhet brenda një rrjeti të caktuar. Prefikset nuk japin asnjë informacion mbi mënyrën se si arrihet rrjeti destinacion. Ky informacion duhet të përftohet nga përdorimi i protokollit BGP. Në kontekstin e BGP, të mirëmbash informacionin mbi lidhjet do të thotë të jesh në gjendje të identifikosh mënyrën se si një paketë të dhënash rrugëzohet për në destinacion.

Përveç rrugës të paracaktuar, duhet të ruhen dhe gjithë rrugët alternative që çojnë në një prefix të caktuar rrjeti, nga fqinjët e tjerë. Arsyeja e kësaj është nevoja për të rivendosur lidhjen sa më shpejt nëse rruga e paracaktuar bëhet e padisponueshme. Kur kjo ndodh AS mund të përdorë një rrugë tjetër për të rrugëzuar paketat dhe për të mbajtur lidhjen edhe kur një link dështon ose ka ndryshuar topologjia e rrjetit.

2.3.3 Konvergjenca e BGP

BGP ekzekutohet njëkohësisht në ruter-a të vendosur në AS të ndryshme dhe për këtë arsye, procesi i zgjedhjes së një rruge në Internet plotësohet në mënyrë të shpërndarë. Rezultati i një algoritmi të shpërndarë mund të varet nga gjendja fillestare e sistemit dhe rendi i ekzekutimit gjatë procesit. Në disa raste, një algoritëm i shpërndarë mund të most arrijë një gjendje të qëndrueshme edhe pse gjendjet e qëndrueshme janë të arritshme në se një tjetër gjendje fillestare apo rend ekzekutimi do ishte zgjedhur. Kur një ruter ndryshon rrugën e tij më të mirë, mund të formohen laqe të mbyllura, të përkohëshme dhe mund të humbin paketa. Në se procesi i përzgjedhjes së rrugës në BGP nuk konvergjon, disa ruter-a mund të vazhdojnë të ndryshojnë rrugën e tyre më të mirë pafundësisht, çka mund të ketë një ndikim shkatërrues në trafikun e Internetit. Për këtë arsye, konvergjenca e protokollit është një çështje e rëndësishme në projektimin e protokolleve të rrugëzimit *inter domain*.

Si pjesa më e madhe e specifikimeve të protokolleve të rrugëzimit, BGP përfshin një “kronometër” për çdo lajmërim për të kufizuar rendin e rifreskimeve të BGP. Pa një element kufizues, një palë do ti dërgonte rifreskime fqinjëve të saj sa herë që rruga më e mirë ndryshon, edhe kur rruga për një prefix ndryshon disa herë Brenda pak sekondave.

Në BGP, ky “kronometër” quhet *Minimum Route-Advertisement Interval timer (MRAI)* [15].

Një “kronometër” i tipit *jittered* nënkupton përdorimin e vlerave që ndryshojnë në mënyrë rastësore. Vlera tipike e MRAI është 30 sekonda. Në se do përdreshin ekzaktesisht 30 sekonda për çdo ruter, do kalohej në vetë-sinkronizim të ruterave. Kjo nga ana e saj implikon dërgimin e mesazheve të rifreskimit në të njëjtën kohë, çdo 30 sekonda [19]. Ky është një efekt i padëshirueshëm për BGP. Kjo mund të evitohet pikërisht duke e modifikuar intervalin e “kronometrit” në mënyrë rastësore, për çdo ruter por duke e implementuar në mënyrë të tillë që të arrihen vlera midis 25 dhe 30 sekondave.

MRAI mund të shkaktojë dërgimin e rifreskimeve të shumëfishta në një seksion komunikimi mes palësh siç tregohet në **Figura 2.2**: AS1 ka shtuar një prefix të ri P dhe për këtë arsye po dërgon një mesazh rifreskimi BGP drejt AS2 dhe AS3 për P me shteg: AS1. Ky rifreskim meret nga AS2, shtohet në tabelat e rrugëzimit, dhe i dërgohet AS4 me që AS2 nuk ka dërguar ndonjë rifreskim drejt AS4 brenda 30 sekondave të fundit. AS4 mer rifreskimin, shton prefixin në tableë dhe ja dërgon rifreskimn AS5. Edhe AS3 e ka marë informacionin dhe ka rifreskuar tableën, por nuk ja dërgon dot AS4 për sa kohë nuk ka përfunduar intervali MRAI. Pasi AS4 mer rifreskimin nga AS3, kupton që ky është një shteg më i mirë dhe rifreskon tableën e rrugëzimit për këtë prefix me informacionin e ri e i dërgon një rifreskim tjetër për prefixin P , AS . Siç vihet re, në një shembull kaq të thjeshtë, AS1 shërbeu si burim për një rifreskim për prefixin P dhe AS4 pati nevojë të dërgojë dy rifreskime për të njëjtin prefix.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

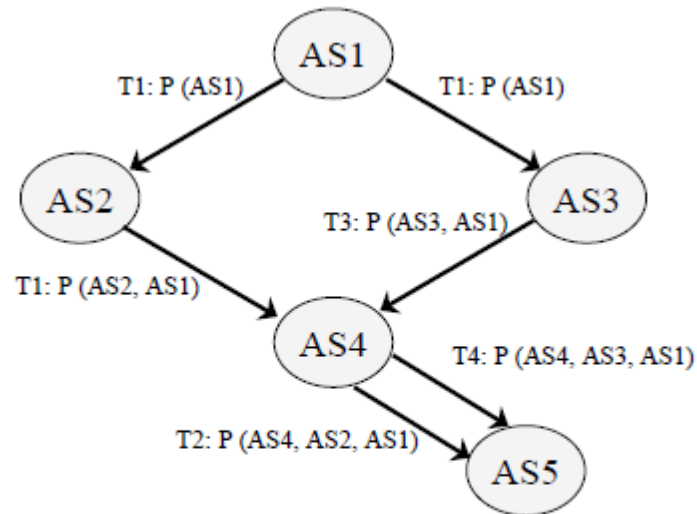


Figura 2.9: Shembull për përhapjen e një rifreskimi BGP

Shpërndarja e mesazheve të rifreskimit varet kryesisht nga topologjia dhe numri i rrugëve alternative.

Punë të mëparëshme me BGP kanë treguar se nëse nuk vihet asnjë kufizim, njëjtë tentojnë të shkëmbejnë një numër të madh rifreskimesh për rrugët e paqëndrueshme (*flapping routes*). Përmes mekanizmit *Route flap damping* [20] tentohet të evitohet që një rrugë e paqëndrueshme të bëjë mbingarkimin e Internetit me mesazhe rifreskimi. Ideja kryesore pas saj është që të mbahet një histori rifreskimesh për një prefix të caktuar dhe të refuzohet të besohen rifreskimet që kapërcejnë disa parametra të paracaktuar. Për shembull, një numër i caktuar rifreskimesh për një ore mund të jetë tepër i lartë.

BGP është një protokoll inkremental që dërgon rifreskime vetëm nëse ka ndryshime në lidhje me topologjinë dhe/ose arritshmërinë. Në teori ndryshimi ndiqet nga disa mesazhe rifreskimi dërguar mes nyjeve. Pasi palët kanë rivendosur rrugët e tyre të preferuara, bota e BGP kthehet sërisht e qetë. Koha ndërmjet ndryshimit dhe kohës kur të gjitha palët kanë zgjedhur rrugët e reja të preferuara përfaqëson konceptin e konvergencës. *Procesi i konvergimit përfundon kur të gjitha palët kanë vendosur rrugët e tyre të reja, të preferuara.*

Ky është koncepti naiv. Në realitet, si rrjedhojë e përmasave të Internetit (rreth 15 000 AS, 120 000 prefikse) dhe shumë faktorëve të tjerë, ka një zhurmë kostante në trafikun e BGP. Prandaj nevojitet që procesi i konvergimit të studiohet më në detaje.

Sa herë që aftësia për të arritur një rrjet ndryshon, duhet të ketë një arsye për këtë. Kjo njihet si *ngjarja e paqëndrueshmërisë*. Një listë e pjeshme e arsyeve të mundshme është si më poshtë:

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

- Dështim ose riparim i një linku fizik.
- Rindezja e një ruter (psh. për rifreskim softueri).
- Ndryshime në politika në AS-ve.
- Shtim/fshirje e prefikseve të rjetit.

Ngjarja e paqëndrueshmërisë mund të ndikojë në lidhjen brenda një AS-je ose midis AS-ve. Kur përfshihet lidhja e brendëshme e një AS-je, kjo trigeron procesin e konvergencës brenda AS, në protokollin IGP [21]. Lidhja e ngjarjeve IGP me BGP (rishpërndarja e IGP në BGP), është në kundërshtim me praktikat operacionale. Normalisht BGP nuk duhet të përfshihet në këtë ngjarje paqëndrueshmërie.

Kur një ngjarje paqëndrueshmërie ndikon lidhjet ndërmjet AS-ve, ajo shkakton shfuqizimin e një rruge të mëparëshme ose lajmërimin e një rruge alternative. Në se shohim efektet e paqëndrueshmërisë në BGP dallojmë momentin e ngjarjes së paqëndrueshmërisë të ndjekur nga rifreskimi i parë i BGP dërguar nga nyja BGP e prekur nga ngjarja. Ky informacion i ri arritshmërie përhapet nëpër ruter-at BGP dhe shumë mundësisht, nuk do të ketë rifreskime të tjera dhe kjo është pika ku thuhet se rrjeti ka konvergjuar për sa i përket këtij prefiksi. Parë nga këndvështrimi i një ruter, ky mund të marrë një numër rifreskimesh nga çdo palë, të përlllogarisë rrugën e re më të mirë dhe tja lajmërojë palëve të tjera. E gjitha kjo procedurë do të quhet Procesi i konvergimit në BGP.

2.3.4. Paqëndrueshmëritë e BGP

BGP ka plotësuar shumë nga kërkesat e Internetit të sotëm por ka dhe shumë dobësi. Probleme të ndryshme si gabime programimi, sulme TCP ose mbingarkimi i rrjetit mund të shkaktojnë paqëndrueshmëri në tabelat e rrugëzimit të ruter-ave BGP.

- a. Fenomeni i “vrimës së zezë” - Një nga problemet më klasike të BGP njihet me emrin fenomenin “vrimës së zezë”. Në këtë problem, një gabim, një sulmues ose një konfigurim i gabuar shkakton që një ruter BGP të lajmërojë gabimisht se përmes AS ku bën pjesë, psh AS X, ka shtegje drejt disa rrjetave me kosto të ulët. Kjo nga ana saj shkakton që shumë ruter-a BGP të rifreskojnë tabelën e tyre të rrugëzimit me këtë informacion. Si rezultat, një sasi e madhe trafiku do të kalojë përmes AS X. Ky trafik i papritur shkakton nga ana e tij paqëndrueshmëri të tabelave të rrugëzimit, sasi të mëdha paketash dhe burimesh rrjeti të humbura dhe në fund një rënie nga mbingarkesa tek AS X. Në literaturën e BGP ka disa instanca të mirëdokumentuara të fenomenit “vrima e zezë” që mund të gjenden në [16], [17], [18].
- b. Dobësitë nga TCP - Një tjetër dobësi e rëndësishme e BGP lidhet me protokollin e transportit të përdorur nga BGP, që është TCP. Ky protokoll është vulnerabël ndaj

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

disa llojeve të sulmeve DOS, gabimeve në programim dhe mbingarkesës së rrjetit në linjat e përdorura. Psh. një sulm i tipit “SYN flooding” ndaj një server, mund të shkaktojë që lidhjet e parashikuara midis palëve BGP të mos vendosen dhe ato ekzistuese të humbin, në se trafiku i krijuar nga sulmi shkakton mbingarkim të rrjetit.

- c. Mbingarkimi i rrjetit – Mbingarkimi i rrjetit mund të jetë patologjik për BGP dhe të shkaktojë paqëndrueshmëri në tabelat e rrugëzimit. Për shembull, në se një sasi shumë e madhe trafiku është paracaktuar të kalojë përmes një AS-je specifike, ka gjasa që linqet që lidhin këtë AS me botën e jashtme të jenë të mbingarkuara dhe si rrjedhojë mund të ndodhi që mesazhet KEEPALIVE që shkëmbehen përmes një lidhjeje të vendosur TCP të humbin ose dhe vetë lidhja TCP të shkëputet. Në këtë rast fqinjësia mes dy ruter-ave BGP do të humbë.
- d. Luhatja e rrugëve (*Route flapping*) - Paqëndrueshmëria e rrugëzimit mund të përshkruhet si një ndryshim i shpejtë i informacionit mbi informacionin mbi arritshmërinë e destinacionit dhe topologjisë në rrjet. Kur një rrugë lajmërohet, shfuqizohet dhe pastaj rilajmërohet thuhet se ajo luhetet. Rrugët e paqëndrueshme janë me kosto të lartë sepse ruterat duhet të përllogarisin rrugë të reja sa herë meret një mesazh i ri. Kjo shkakton ngarkesë të lartë në ruter dhe mund të {ojë deri në një dështim (*crash*) të tij.

Janë zhvilluar disa teknika për të përmirësuar paqëndrueshmëritë e BGP. Dy më kryesoret janë:

Route flap damping –Në rastin e rrugëve që luhaten, disa implementime të BGP, përdorin një mekanizëm të njohur si “shuarja e rrugës” (*route damping*) – një rrugë që luhetet i vihet në përkatësi një vlerë *ndëshkim* dhe në se kjo vlerë kapërcen një kufi të caktuar, kjo rrugë konsiderohet si e pavlefshme. Vlera e ndëshkimit zvogëlohet me kalimin e kohës. Në se rruga ndërpret luhatjet, ajo rilajmërohet dhe ndëshkimi që i ishte vendosur, shfuqizohet.

Message aggregation shpesh ka një lidhje ndërmjet mesazheve të rifreskimit dhe atyre të shfuqizimit. Zakonisht, kur një rrugë shfuqizohet, mesazhi i shfuqizimit shoqërohet direkt me një mesazh lajmërimi – rruga mund të jetë subject i ndryshimeve ose i një sjelljeje patologjike. Për të zvogëluar volumin e trafikut konsiderohet me interes që mesazhi mos përhapet menjëherë pas gjenerimit, por të ruhet për një farë kohe dhe informacioni të agregohet. Në se rruga është shfuqizuar dhe më pas rilajmërohet po njëjloj, është e saktë të anulohen të dyja mesazhet me që gjendja në përgjithësi mbetet e njëjtë. Kjo metodë zvogëlon vëllimin e trafikut dhe përpunimet në ruterat BGP.

Për fat të keq të dyja këto metoda fusin vonesa në përhapjen e rrugëve. Kështu që pavarësisht se protokollin dhe rrugët stabilizohen, koha e konvergencës vjen duke u rritur.

2.4 Menaxhimi i sesionit ndërmjet “çifteve”

Kur router-at që suportojnë BGP duan të hapin një sesion komunikimi, atëherë ata hapin një lidhje TCP në portën 179 me router-in “çift”. Pasi lidhja është krijuar, çdo entitet dërgon një mesazh *open* për të negociuar parametrat e sesionit të komunikimit. Në mënyrë që të ketë dijeni mbi vlefshmërinë e kësaj lidhjeje dhe për të monitoruar router-at komshinj, Router-at dërgojnë shpesh mesazhe *keep-alive*. Gjatë hapjes së shkëmbimit të mesazheve, router-at BGP përcaktojnë *kohën e pritjes*, maksimumi i kohës që duhet të presë para se të dërgojë mesazhin pasardhës. Mungesa e pranisë së një mesazhi brenda këtij intervali, tregon se entiteti tjetër nuk po funksionon normalisht. Nëse një entitet brenda këtij “çifti” komunikimi merr një mesazh të gabuar, të formatuar keq apo nuk merr asgjë brenda *kohës së pritje* atëherë i dërgon një mesazh të tipit *notification* entitetit fqinj, fshin të gjithë tabelën e rrugëve që ka marrë prej tij dhe me fatmirësisht mbyll sesionin TCP. Më poshtë tregohen hapat që përdoren për të arritur një sesion komunikimi BGP.

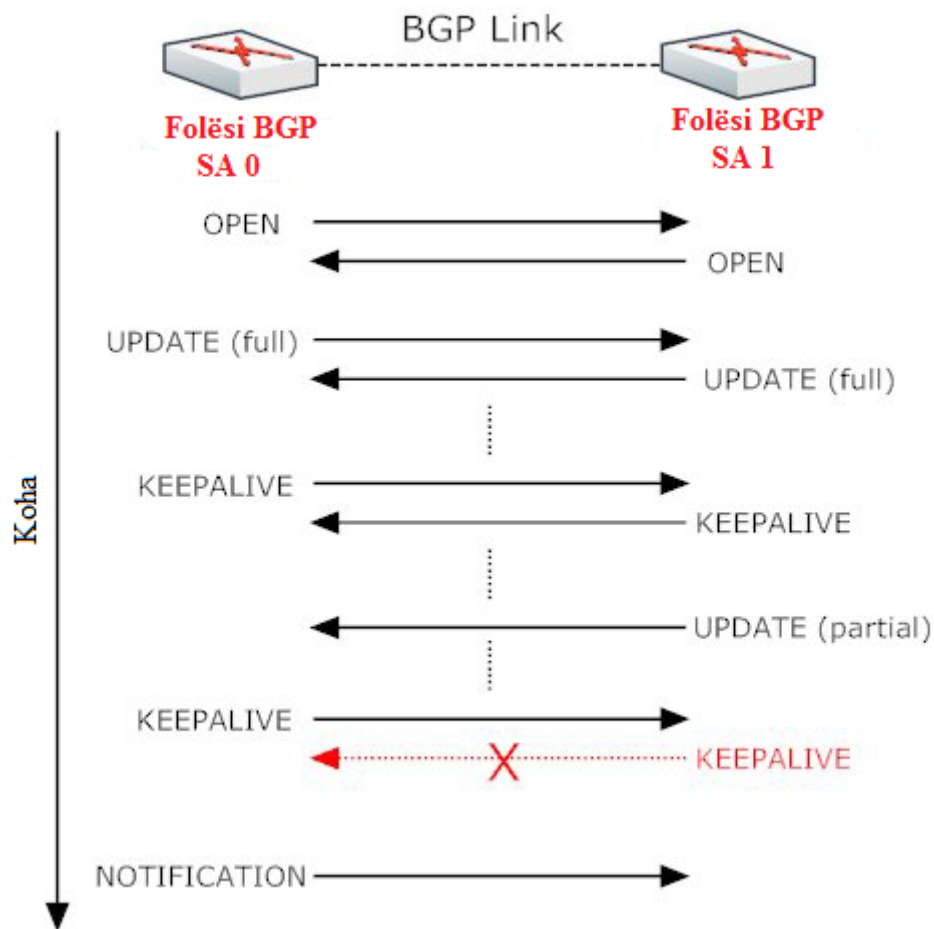


Fig 2.10 – Shkëmbimi i mesazheve BGP

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

2.4.1 Shkëmbimi i informacionit të rrugëzimit

Si fillim, para se të shkëmbejnë tabelat e rrugëzimit, 2 router-at BGP vendosin një sesion komunikimi. Më pas entitetet mund të shkëmbejnë të gjithë tabelën e rrugëzimit që disponojnë, nëpërmjet një serie mesazhesh (UPDATE). Router-at supozohet të memorizojnë të gjitha rrugët e ofruara nga entitetet e tjera në sesion. Mbasi të gjitha janë përfunduar router-at i dërgojnë njëri-tjetrit përditësime të pjesshme të rrugëve të reja në tabelat e tyre.

Mesazhet e tipit *Update* mund të mbulojnë 2 tipe informacionesh: 1) *Lajmërim* dhe 2) *Tërheqje*. Një *Lajmërim* e njofton marrësin e tij për një rrugë të re për filan prefiks destinacion, kurse një *Tërheqje* e anulon rrugën e lajmëruar më parë. Përveç informacionit të mbulimit, një mesazh *update* përmban një numër të ndryshueshëm atributesh rruge, të cilat përshkruajnë veçoritë e rrugës, nga të cilët mund të përmendim: *local preference*, *next-hop*, *origin type*, *AS path* dhe *multi-exit discriminator* (MED).

Le të shohim me rradhë se çfarë përshkruan secili prej tyre.

1) Atributi *AS path* përmban një listë të të gjitha Sistemeve Autonome që prefiksi ka përshkruar. BGP e përdor *AS path* si për të detektuar cikle ashtu edhe për të zgjedhur rrugën. Kur një router merr një BGP *update* atëherë ai ekzaminon vektorin e rrugës dhe nëse sheh numrin e Sistemit të tij Autonom atëherë ai e zhvlerëson këtë rrugë.

2) Atributi *next-hop* përfaqëson adresën IP të router-it që duhet të përdoret për të arritur rrjetin e dëshiruar.

3) Atributi *origin type* identifikon sesi Sistemi Autonom fillestar mësoi për rrugën: brenda Sistemit Autonom (konfigurimi statik), një versioni të vjetëruar *Exterior Gateway Protocol* (EGP) ose është injektuar nga një protokoll tjetër rrugëzimi. *Origin types* njihen si IGP, EGP ose e panjohur (INCOMPLETE).

4) Atributi *Multi-Exit Discriminator* inkurajon marrësin të përcaktojë se në cilën nga pikat dalje të orientojë trafikun drejt një Sistemi Autonom fqinj.

5) Atributi *local preference* mund të përfshihet në mesazhet iBGP (për të cilin do flasim më poshtë) për të ndihmuar marrësin të renditë rrugët e marra nga router-a të ndryshëm brenda të njëjtit Sistem Autonom.

2.4.2 Përpunimi dhe gjetja e rrugës

Janë dy tipe sesionesh BGP ndërmjet entiteteve: *external BGP* (eBGP) për entitete ndërmjet Sistemeve të ndryshme Autonome dhe *internal BGP* (iBGP) për entitete ndërmjet të njëjtit Sistem Autonom. Në figurën 2.3 shfaqen hapat për gjetjen e rrugës BGP.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Në fillim router-i aplikon politikat e importit për të filtruar rrugët e padëshiruara. Për shembull, një router BGP mund të pranojë lajmërimi nga një *AS path* që përmban një set të besuar Sistemesh Autonome. Më pas router-i thërret një proces vendim-marrjeje për të zgjedhur saktësisht një rrugë më të mirë për çdo prefiks destinacioni, duke krahasuar rrugën e re me të gjitha rrugët e tjera të njohura më parë për të njëjtin destinacion. Router-i aplikon një sekuençë hapash për të ngushutar setin e kandidatëve deri në 1 të vetëm. Rruga më e mirë e zgjedhur me këtë mënyrë do të instalohe në tabelën e forward-imit, ndërsa rrugët e tjera do mbahen për qëllime *backup*-i.

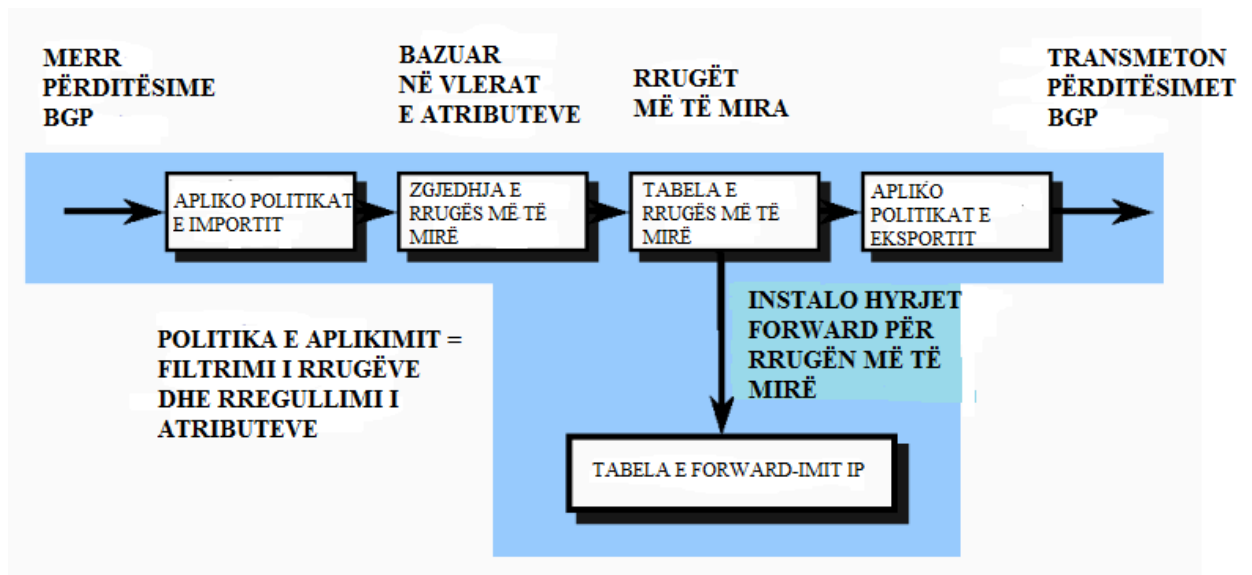


Fig 2.11 – Zgjedhja e rrugës BGP

Në përfundim, router-i aplikon politikat e eksportit për të manipuluar atributet dhe të vendosë nëse do ta lajmërojë këtë rrugë tek Sistemet Autonome fqinjë. Nëse po, router-i mund të modifikojë disa nga atributet e rrugës. Në fund do shtojë numrin AS të tij tek *AS path*.

2.4.3 Zhvlerësimi i një rruge

Nëse një router merr një informacion *tërheqjeje*, si fillim heq rrugën e zhvlerësuar nga rekordet e tij. Nëse rruga që hiqet është momentalisht rruga më e mirë, router-i kërkon në *backup*-et e tij për një rrugë të dytë më të mirë dhe nëse kjo nuk funksionon atëherë e quan destinacionin si të paarrtshëm. Nëse kjo e fundit aplikohet, një lajm zhvlerësimi *duhet* ti çohet çdo entiteti që mësoi rrugën nga lajmërimet e mëparshme.

2.4.4 Reflektimi i rrugës

Në implementimin standart iBGP, të gjithë router-at BGP brenda të njëjtit Sistemi Autonom janë të lidhur ngushtë kështu që informacioni për rrugëzim jashtë sistemit shpërndahet ndërmjet të gjithë router-ave brenda AS. Por ky model mund të krijojë problem me shkallëzueshmërinë kur AS ka një numër të madh *folësish* BGP. Reflektimi i rrugës krijon një mënyrë për të ulur kontrollin e trafikut të BGP, kjo duke minimizuar numrin e mesazheve *update* që dërgohen brenda sistemit Autonom.

Koncepti i reflektimit të rrugës është bazuar në idenë e krijimit të një nyjeje (router) përqëndrimi (reflektuese), e cila të funksionojë si një pikë kyçe për sesionet iBGP. Në reflektimin e rrugës, sistemet BGP organizohen në *tufa* (clusters). Çdo *cluster* konsiston nga të paktën një router që luan rolin e një reflektuesi rruge, së bashku me një numër çfarëdo entitetesh klientë. Entitetet që ndodhen jashtë *cluster*-it nuk quhen entitete klientë. Reflektuesit e rrugës rishpërndajnë informacionin e rrugëzimit tek çdo entitet, qoftë ai klient ose jo. Për arsye se reflektuesi i rrugës rishpërndan rrugët brenda *cluster*-it, Router-at BGP nuk është e nevojshme të jenë plotësisht të lidhur.

Kur një reflektues rruge merr një rrugë, ai zgjedh rrugën më të mirë. Më pas, nëse rruga vjen nga një entitet jo klient, reflektuesi e dërgon rrugën tek çdo entitet klient brenda *cluster*-it. Nëse rruga vjen nga një entitet klient, reflektuesi e dërgon rrugën drejt çdo entiteti jo klient si dhe entiteti klient përveç atij nga është gjeneruar. Gjatë këtij procesi, asnjë entitet klient nuk i dërgon rrugë njëri-tjetrit.

2.5 Përfundime

BGP kategorizohet si një *protokoll i vektorit të rrugës* (PV), një variant i *protokollit të vektorit të distancës* (DV). Në vend që të transferojë informacion mbi gjëndjen e lidhjes dhe koston, çon informacion mbi rrugën e plotë për të mënjeluar ciklet e tepërta. BGP përmban TCP si protokoll komunikimi në shtresën e transportit, që në anën e tij është protokoll i sigurt dhe eliminon nevojën që BGP të marrë përsipër ritransmetimin, aprovimin (ACK) dhe sekuencialitetin. Router-at që përdorin BGP si protokollin e tyre quhen BGP *folës*. Dy folës BGP që marrin pjesë në një sesion BGP quhen *fqinjë* ose *çift*. Router-at çift shkëmbejnë 4 tipe mesazhesh: *open*, *update*, *notification* dhe *keep-alive*. Nga të gjitha këto mesazhe vetëm *update* përmban informacion rrugëzimi ndërkohe që 3 të tjerët shërbejnë për menaxhimin e sesionit të komunikimit.

Duke u mbështetur nga çka përmendëm më sipër, karakteristikat e rrugëzimit në Internetin e sotëm mund të përmbledhen në parimet e përgjithshme të mëposhtme, në lidhje me shtegun midis dy nyjeve u dhe v :

- Nëse u dhe v janë në të njëjtin AS, shtegu ndërmjet tyre mbetet i gjithi brenda AS.
- Nëse u është në AS U dhe v është në AS V , shtegu mes u dhe v kalon nga U në zero ose më shumë AS tranzit.

Inicialisht, para se të shkëmbejnë tabelat e rrugëzimit, 2 router-at BGP caktojnë një sesion komunikimi. Më pas entitetet mund të shkëmbejnë të gjithë tabelën e rrugëzimit që

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

kanë, me anë të një serie mesazhesh (UPDATE). Router-at mendohet të memorizojnë të gjitha rrugët e ofruara nga entitetet e tjera në sesion. Pasi të gjitha janë përfunduar router-at i dërgojnë njëri-tjetrit përditësime të pjesshme të rrugëve të reja në tabelat e tyre.

Në fillim router-i aplikon politikat e importit për të filtruar rrugët e padëshiruara. Në vazhdim router-i thërret një proces vendim-marrjeje për të zgjedhur saktësisht një rrugë më të mirë për çdo prefiks destinacioni, duke krahasuar rrugën e re me të gjitha rrugët e tjera të njohura më parë për të njëjtin destinacion. Router-i aplikon një sekuencë hapash për të ngushtuar setin e kandidatëve deri në 1 të vetëm. Rruga më e mirë e zgjedhur me këtë mënyrë do të instalohet në tabelën e forward-imit, ndërsa rrugët e tjera do mbahen për qëllime *backup*-i.

Në përfundim, router-i aplikon politikat e eksportit për të manipuluar atributet dhe të vendosë nëse do ta lajmërojë këtë rrugë tek Sistemet Autonome fqinjë. Nëse po, router-i mund të modifikojë disa nga atributet e rrugës. Në fund do shtojë numrin AS të tij tek *AS path*.

Nëse një router merr një informacion *tërheqjeje*, si fillim heq rrugën e zhvlerësuar nga rekordet e tij. Nëse rruga që hiqet është momentalisht rruga më e mirë, router-i kërkon në *backup*-et e tij për një rrugë të dytë më të mirë dhe nëse kjo nuk funksionon atëherë e quan destinacionin si të paarrtshëm. Nëse kjo e fundit aplikohet, një lajm zhvlerësimi *duhet* ti çohet çdo entiteti që mësojë rrugën nga lajmërimet e mëparshme.

Në implementimin standart iBGP, të gjithë router-at BGP brënda të njëjtit Sistemi Autonom janë të lidhur ngushtë kështu që informacioni për rrugëzim jashtë sistemit shpërndahet ndërmjet të gjithë router-ave brënda AS. Por ky model mund të krijojë problem me shkallëzueshmërinë kur AS ka një numër të madh *folësish* BGP. Reflektimi i rrugës krijon një mënyrë për të ulur kontrollin e trafikut të BGP, kjo duke minimizuar numrin e mesazheve *update* që dërgohen brenda sistemit Autonom.

Koncepti i reflektimit të rrugës është bazuar në idenë e krijimit të një nyjeje (router) përqëndrimi (reflektuese), e cila të funksionojë si një pikë kyçe për sesionet iBGP. Në reflektimin e rrugës, sistemet BGP organizohen në *tufa* (clusters). Çdo *cluster* konsiston nga të paktën një router që luan rolin e një reflektuesi rruge, së bashku me një numër çfarëdo entitetesh klientë. Entitetet që ndodhen jashtë *cluster*-it nuk quhen entitete klientë.

Kapitulli III

Modelimi i rrugëzimit të një ISP

Hyrje

Shërbimi kryesor i ofruar nga Internet Service Providers (ISP-të) është një përpjekje e mirërealizuar best-effort. Sot, gjithsesi konsumatorët janë duke kërkuar për shumë më tepër se një shërbim best-effort s'rrugëzime do të ishte performanca dhe besueshmëria e garantuar. Shërbimet e reja të shpërndara gjerësisht të tilla si VPN ose VoIP apo VOD dhe IPTV kërkojnë rritjen e garancive të performancës nga rrjeti. Për këtë arsye, ISP- të janë shumë të ndjeshëm ndaj elasticitetit dhe performancës së rrjetit të tyre. Ata përpiqen të sigurojnë cilësitë për klientët e tyre me anë të Marrëveshjeve të Nivelit të Shërbimit (SLAs) (FE04). Prandaj, ISP-të kërkojnë të ndërtojnë rrjete që do të strehojnë ngarkesa të ndryshueshme të trafikut dhe të jenë të fuqishme për lidhjet e linqeve si dhe ndaj dështimeve të router-ave. Për të kënaqur kufizimet e shtrënguara të SLAs, ISP e planifikojnë nga pikëpamja inxhinierike rrjetin e tyre për të siguruar performancat më të mira, si minimizimin e vonesës në të gjithë rrjetin, ose parandalimin e ngjeshjes (congestion) që ndodh në lidhjet e aksesit.

Sot, kompleksiteti i rrjeteve të ISP-ve " e bën të vështirë për të hetuar implikimet e ndryshimeve të brendshme apo të jashtme në shpërndarjen e trafikut në të gjithë rrjetin e tyre. Disa studime kanë shqyrtuar kohët e fundit ndërveprimin mes protokolleve IGP dhe BGP. Bazuar në rrjetin AT & T, Teixeira et al kanë treguar (TSGR04) se ndryshimet IGP në rrjetet IP mund të shkaktojnë ndërrime në trafik dhe updates BGP të dukshme nga jashtë. Përditësime të tilla të BGP mund të mbeten më shumë se 60s pas ngjarjes përkatëse IGP, duke shkaktuar ekstra - vonesë në konvergjencën e planit të shpërndarjes. Në (ACBD04), Agarwal et al studioi ndikimin e përditësimeve BGP në matricën e trafikut intradomain të Sprint. Ata arritën në përfundimin se edhe pse janë marrë shumë prej përditësimeve BGP, matrica e trafikut ka mbetur e qëndrueshme. Kjo është parashikuar nga Uhlig et al (UMB + 04) i cili tregoi se rrugët drejt shumicës së destinacioneve të internetit janë të qëndrueshme. Në (TAR05), Teixeira et al paraqesin një pamje të konsoliduar të rezultateve të disa studimeve të matjes të kryera në AT & T dhe Sprint . Ata arrijnë në përfundimin se ndërtimi i një model të një rrjeti 1- shtresor të madh është i vështirë dhe përkrahën zhvillimin e një modeli të bashkëveprimit ndërmjet topologjisë së rrjetit, protokolleve të rrugëzimit, trafikut dhe ngjarjeve të rrjetit. Asnjë mjet modelimi nuk kap aktualisht plotësisht shumëllojshmërinë e rrugëve të njoftuara nga fushat(domain-e) fqinje as edhe detajet e konfigurimit të rrugëzimit brenda një AS. Në (FGL + 00), Feldmann et al përshkroi Netscope, si një mjet për të studiuar dhe vizualizuar rrjedhën e trafikut në një rrjet shtyllë kurrizore. Netscope fokusohet vetëm në intradomain. Në (FWR04), Feamster et al përshkroi një emulator BGP që lejon për të llogaritur vendimet e rrugëzimit BGP në një AS të vetme. Për fat të keq, ky mjet është jo në dispozicion të publikut. Kohët e fundit, Teixeira et al propozoi një model të ndryshëm të ndryshimeve hot - patate në procesin e përzgjedhjes së rrugëzimit BGP

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

(TGVS04). Megjithatë formulimi analitik i propozuar në (TGVS04) nuk riprodhon të plotë procesin e vendimmartjes së BGP dhe as kompleksitetin e punës së BGP brenda një AS (HP00). Ky model analitik nuk është në dispozicion si një mjet që mund të përdoret nga operatorët e rrjetit.

Si rrugëzime ne do të tregojmë në këtë kapitull, të kuptuarit e rrugëzimit të AS-eve të mëdhenj jo vetëm kërkon për të modeluar rrugëzimin brenda AS, por më e rëndësishmja duhet marrë në konsideratë informacioni i rutimit të marrë nga AS-et fqinj. Është përshkruar në seksionin 3.2 si të modelohet rrugëzimi i një rrjeti ISP. Sqarohen se cilat informacione janë të nevojshme për të ndërtuar një model të tillë dhe pse ai është aq i ndërlikuar. Është aplikuar metodologjia në një rrjet tranzit dhe janë siguruar dy aplikacione të modelit tonë për të studiuar sjelljen e këtij AS në Seksionin 3.5. Skenari i parë studion ndikimin e ndryshimeve në lidhjen e internetit të rrjetit transit. I dyti heton ndikimin e lidhjeve të vetme të brendshme dhe dështimet e router-ave. Së fundi, jepen përfundimet në seksionin 3.6.

3.1 Modelimi i një sistemi autonom

Në këtë seksion, është përshkruar se si të ndërtohet një model i një rrjeti ISP që është i përshtatshëm për solver rrugëzimi. Është treguar se ndërtimi i një modeli të tillë është një detyrë që përfshin disa aspekte, duke filluar nga të kuptuarit e arkitekturës së AS-ve, mbledhjen e të dhënave të rrjetit, ndërtimin e një përfaqësimit të rrjetit të AS-ve, si dhe duke i dhënë fund me një model të përshtatshëm për solver rrugëzimi.

INetscope ka një mbështetje për destinacionet e jashtme të arritshme nëpërmjet pikave të shumta të drejta për të dalë. Ai nuk e mbështet BGP gjithsesi.

Në mënyrë që të modelohet rrugëzimi i një ISP, është e nevojshme për të ndërtuar një model. Së pari, lindi nevoja për të modeluar topologji rrjeti. Në shembull, topologjia përbëhet nga routera R1 R6 dhe lidhjet (linqet) midis tyre. Meqë përbën interes rrugëzimi interdomain, gjithashtu duhet të përfshihen në topologji lidhjet interdomain që lidhin routerat kufitare të ISP-ve të routerave kufitare të ISP-ve të tjera. Në shembull, modeli përmban 7 lidhje interdomain që lidhin ISP me 5 fqinjët. Pastaj, ka nevojë për të marrë konfigurimin e protokollit të rrugëzimit intradomain që të jetë në gjendje për të llogaritur rrugët intradomain të çdo routeri. Gjithashtu duhet të përcaktoheshin sesionet BGP mes routerave. Kjo përfshin seksionet iBGP mes routerave e ISP-ve të modeluara. Këto seksione iBGP mund të organizohen në një hierarki duke përdorur reflektorët e rrugëzimit. Kjo gjithashtu përfshin seksionet eBGP mes routerave kufitare dhe respektivëve të jashtëm. Veçanërisht, këto seksione eBGP e lejojnë për të ushqyer modelin me rrugët interdomain të mësuara nga ISP. Së fundi, për të studiuar ndikimin e ndryshimit të rrugëzimit në trafik, ishte e nevojshme për të përfshirë modelin "rrjedhës" të trafikut hyrës nga një pikë hyrjeje dhe daljeje në një pikë të llogaritur drejtë për të dalë.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

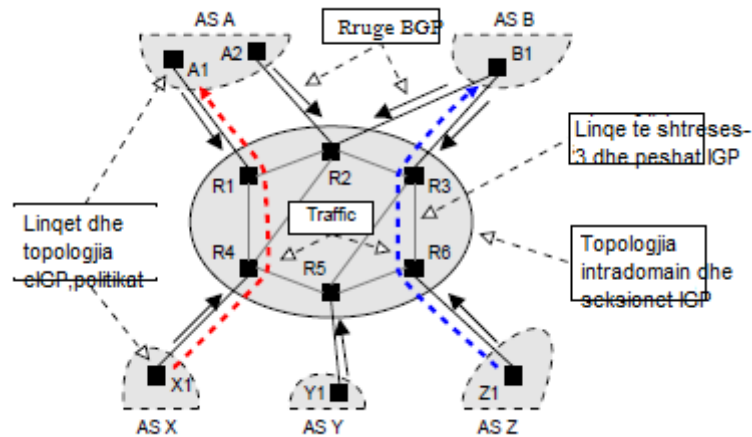


Figura 3.1 Përshkrimi i një modeli të një ISP-je.

Është diskutuar në seksionet e mëposhtme se si mund të merret informacioni i kërkuar për të ndërtuar këtë model. Gjithashtu shpjegohen se cilat janë sfidat aktuale teknike në mbledhjen e këtyre të dhënave.

3.1.1 Përmbledhja e konfigurimit të routerave

Pjesa e parë drejt ndërtimit të modelit të një AS-je konsiston në gjetjen e konfigurimit të tij. Konfigurimi i rrjetit është i përhapur në të gjithë routerat e tij. Konfigurimi i një routeri përfshin elementet e mëposhtme të cilat janë të rëndësishme për një model rrugëzimi. Së pari, ai përmban hartëzimin mes lidhjeve fizike dhe lidhjeve të shtresës së tretë. Vini re se tunelet IP janë gjithashtu të rëndësishme në praktikë dhe ato mund të shihen si lidhje shtesë të shtresës së tretë. Çdo ndërfaqe fizike (ose grup ndërfaqesh fizik në rastin e tufave lidhjesh) do të marrë një ose më shumë adresa IP identifikimin e pikës fundore endpoint të linkut. Së dyti, konfigurimi i routerit përmban metrikën IGP lidhur me një lidhje të shtresës së tretë. Nëse IGP është hierarkike, konfigurimi i një routeri gjithashtu përmban përkufizimin e zonave të cilit i përket. Së fundi, konfigurimi i routerit përmban përkufizimin e seksionit që routeri BGP ka me fqinjët e tij. Për çdo seksion BGP, konfigurimi tregon nëse është i brendshëm apo i jashtëm. Nëse routeri është një reflektor rrugëzimi, konfigurimi do të tregojë për cilin seksion është i lejuar reflektimi. Ky konfigurim zakonisht përfshin edhe politikat BGP që janë të detyrueshme në çdo seksion. Konfigurimi i routerave gjithashtu përmban shumë parametra të tjerë që nuk është e nevojshme të diskutohen këtu meqë ata nuk janë të nevojshëm për të ndërtuar modelin tonë. Trajtimi i konfigurimit të routerave në një rrjet të madh është i vështirë. Së pari, në një rrjet IP të madh, vëllimi i informacionit të gjetur në konfigurimin e routerave është shumë i madh për një njeri që të jetë në gjendje të merret me to manualisht. Së dyti, konfigurimi i routerave ndryshon dhe ka shpesh mospërputhje në mes të routerave të ndryshëm në të njëjtin rrjet (FR01, QN04, FB05). Për shembull, nuk është e rrallë për të gjetur seksione BGP gjysmë të përcaktuara, që do të thotë se seksioni është përcaktuar në

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

konfigurimin e një routeri por jo në konfigurimin e peer-ve të tij. Së fundi, shumë rrjete përdorin pajisje heterogjene. Konfigurimet janë shkruar në këtë mënyrë në gjuhë të ndryshme konfigurimi. Ndonjëherë, disa opsione madje edhe varen prej versionit e sistemit operativ të pajisjes së rrjetit. Prandaj, ekziston një nevojë për të automatizuar procesin e analizimit të konfigurimit të rrjetit dhe për të raportuar si duhet mospërputhjet. Shumicën e kohës, diskutimi me operatorin, si dhe ndër-kontrolli i dokumentave do të jetë i nevojshëm në mënyrë që të shfrytëzojmë konfigurimin e rrjetit.

3.1.2 Përfaqësimi i topologjisë

Hapi i dytë i ndërtimit të modelit konsiston në ndërtimin e një modeli të topologjisë së rrjetit. Si rrugëzime e kemi shpjeguar më parë ne nuk i përfshijmë detajet e nivelit fizik/facilitet meqënëse nuk na nevojiten në mënyrë që të jemi në gjendje të modelojmë me kujdes se si realizohet zgjedhja e rrugës në një AS. Në këtë rast nevojitet një graf të ruterave IP dhe linqeve të shtresës së tretë. Për ta ndërtuar këtë topologji, mund të mbështetemi në konfigurimin e ruterave të përshkruar më parë. Një tjetër mundësi është të braktiset databaza e topologjisë të ndërtuar nga një ruter. Me të vërtetë, derisa me protokollet e rrugëzimit si një OSPF ose IS-IS, secili ruter në domain ndërton databazën e afërsive mes ruterave, është e mundur të mbështetemi në databazën e afërsive të ndërtuar nga një ruter i vetëm. Në praktikë, një workstation i cili ekzekuton një demon IGP të tillë si Quagga (Qua03) do të përdoret për këtë qëllim dhe do të ketë një afërsi me një ruter në domain. Kjo metodë kërkon për të konfiguruar një afërsi të re në një ruter rrjeti. Në rastin e një IGP hierarkike është e nevojshme një kapje e të dhënave të topologjisë. Disa operatorë rrjetesh preferojnë të mbështeten në përgjimin e IGP në një lidhje Ethernet (Bon05) pasi ajo kërkon më pak përpjekje për konfigurimin. Kjo metodë ka të papërshtatshëm humbjen e historisë të LSPs të fundit dhe mund të marrë disa kohë që të ketë një pamje të saktë të topologjisë. Një vështirësi që mund të haset në këtë pjesë është hartëzimi i nyjeve dhe skajeve të modelit me pajisje të vërteta rrjetëzimi. Adresat e ndryshme IP mund të përdoren për të identifikuar pjesë të ndryshme të pajisjeve. Routerat mund të kenë adresa të shumëfishëta IP përkatësisht në ndërfaqe të ndryshme fizike dhe adresa loopback-e të ndryshme. Në konfigurime të caktuara, adresat IP të përdorura për të identifikuar routerin në IGP ndryshojnë nga adresa IP që identifikon routerin në protokollin BGP. Një zgjidhje për këtë konsiston në hartëzimin e të gjitha adresave të një routeri në një adresë të vetme IP (Tan06). Kjo duhet të bëhet me kujdes duke qenë se protokollet e rutimit mund të marrin vendimet e bazuara në këtë adresë. Ky është rasti për BGP, për shembull, ku adresat IP e ruterave mund të përdoren për të thyer lidhjet në hapin e fundit të procesit të vendimit.

3.1.3 Rrugëzimi i të dhënave

Pjesa e tretë e modelimit të një AS konsiston në ushqyerjen e saj me të dhënat e rrugëzimit. Lidhur me rrugëzimin intradomain, rrugët mund të llogariten në bazë të afërsive të gjetura në grafikun e modelit dhe në metrikën IGP të skajeve ekzistuese. Për

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

rrugëzimin interdomain, informacioni shtesë duhet të vendoset në model. Routerat AS do të kryejnë zgjedhjen e tyre të rrugës në bazë të rrugëve të jashtme të marra përmes BGP nga routerat kufitare. Këto rrugë janë për tu kapur dhe për tu injektuar në modelin e AS-së. Për të qenë në gjendje për të kryer parashikimet shumë të sakta me modelin, duhet të mblidhen të gjitha rrugët e eBGP të mësuar nga AS. Mbledhja e të gjitha rrugëve të BGP të mësuar nga një AS mund të jetë një problem funksional. Teknikisht, është e mundur për të kapur të gjitha rrugët e BGP që janë marrë në lidhjet peering të AS. Është gjithashtu e mundur që të hyni në të gjitha routerat kufitare dhe ti pyesim ata për të lënë të gjitha rrugët e tyre eBGP. Në praktikë megjithatë, për shkak të kufizimeve të pranishme në software-t e routerave dhe në hezitimin e operatorëve për të kryer këto veprime në routerat e prodhimit, për të mbledhur rrugët eBGP nuk është e thjeshtë. Teknika e përdorur për mbledhjen e të dhënave BGP varet në rrjetin e AS-ve, por një teknikë e zakonshme është që të mbështetet në një workstation të dedikuar i cili ekzekuton e një software zbatimi i BGP si Quagga [Qua03] që ka seksione pasive BGP me routerat BGP të AS (shih Fig. 3.2). Në një rrjet të vogël apo të mesëm me një rrjetë të plotë mesh iBGP, të gjitha routerat do të ketë një seksion iBGP me workstation dhe do të mësohen të gjitha rrugët më të mira të routerave. Në rrjetet e mëdha, çdo router nuk mund të mbajë një seksion iBGP me kolektor rrugë dhe vetëm një nëngrup i rrugëve do të mblidhen. Në mënyrë tipike, rrjete të mëdha mbështeten në një hierarki iBGP dhe rrugët do të mblidhen në reflektorë të rëndësishëm rrugësh.

Është e rëndësishme të theksohet se duke përdorur një nëngrup të rrugëve BGP mund të çojë në pasaktësi në modelin që nga daljet e mundshme për disa prefikse destinacioni do të ngelen të panjohur.

Për shembull le ti hedhim një sy figurës 3.2.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

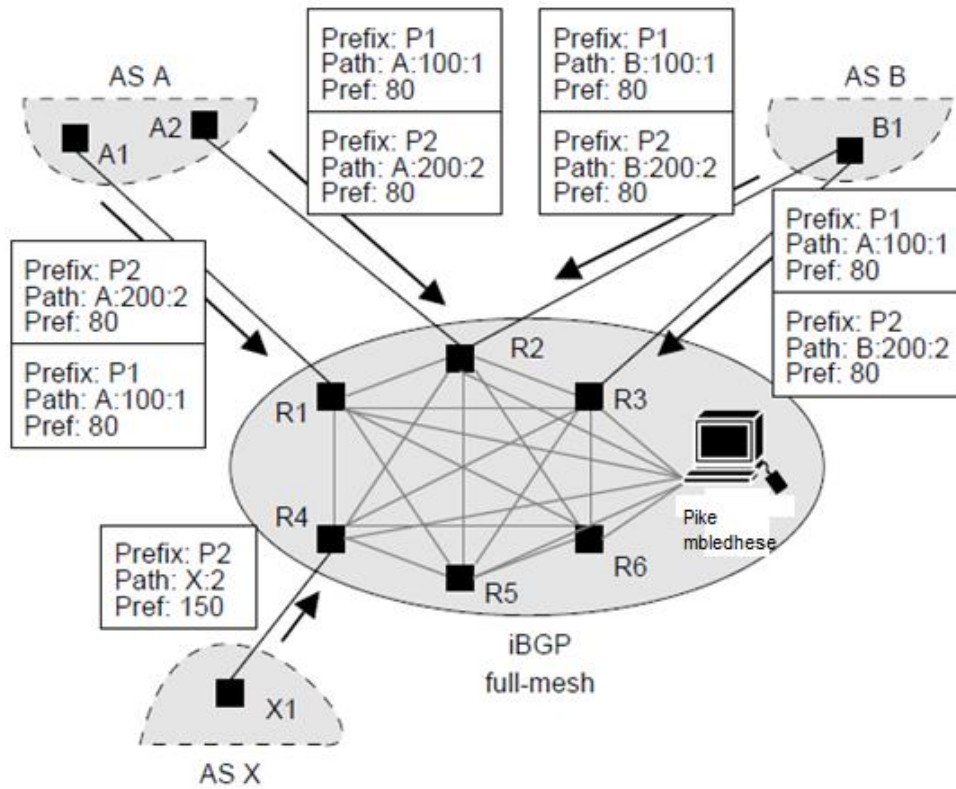


Figura 3.2: Nje pamje e kufizuar e ruterave eBGP

Në së pari është marrë në konsideratë rasti i rrugëve të mësuara drejt P1. Dy rrugët janë marrë nga R1 dhe R2 nga ASA. Dy rrugët janë pranuar edhe nga R2 dhe R3 nga ASB. Çdo router kufitar (R1, R2 dhe R3) propagandon një rrugë të vetme të mirë në iBGP. R2 ka marrë dy rrugë eBGP dhe reklamon një të vetme në iBGP. Cila është shpallur varet nga rezultati i procesit të vendimmarrjes në R2. Një rast i dytë i mundshëm ka të bëjë me P2. Rrugët drejt këtij prefixi janë marrë nga ASA, ASB dhe ASX. Por preferenca e 150 e dhënë rrugës të marrë nga ASX është më e lartë se preferenca e dhënë rrugëve të marra nga ASA dhe ASB (80). Kjo do të thotë se R4 propagandon këtë rrugë në iBGP dhe ajo është zgjedhur më pas sa më mirë nga R1, R2 dhe R3, si pasojë është që R1, R2 dhe R3 nuk ofojnë rrugët e tyre eBGP ndaj P2 në iBGP dhe pika grumbulluese në këtë mënyrë nuk është i vetëdijshme për to.

Qasje të reja të tilla si protokollin i monitorimit BGP (BMP) (Scu05) janë aktualisht diskutuar në IETF. BMP lejon një qasje më të lehtë në rrugët BGP të njohura nga një router (përfshirë Adj - RIB - in). Ruterat Juniper gjithashtu kanë një funksion të fshehur që u lejon atyre për të reklamuar në iBGP rrugën më të mirë të mësuar gjatë seksioneve eBGP në qoftë se rruga e tyre e tanishme më e mirë është mësuar nga iBGP. 3. 3The JunOS magjike është komanda për të mundësuar shpalljen e rrugës më të mirë të jashtme që është BGP reklamo –më mirë - jashtë -brenda (advertise-best-external-to-internal).

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

3.2. Modeli GEANT 75,

3.2.1 Statistikat e trafikut

Pjesa e katërt e nevojshme për të modeluar një AS ka të bëjë me trafikun. Për një AS, informacioni i trafikut ngre probleme serioze (VE04). Në një model intradomain të AS, vetëm matrica e trafikut router - router duhet të merret parasysh. Ky nivel i detajuar është i mjaftueshëm që ndryshimet në rrugëzimin intradomain do të ndryshojnë vetëm shtigjet nga ruteri në ruter, jo vëllimin e të dhënave të dërguara nga një ruter në një tjetër. Në këtë rast, ai mund të mbështetet në matjet SNMP në ndërfaqet e jashtme të AS dhe përdorimit të teknikave të tilla si Tomo - graviteti (ZR DG03) të interferojë një matricë trafiku router - router. Saktësia e këtyre teknikave është e diskutueshme (GJT04). Një tjetër teknikë që mund të përdoret në AS, ku MPLS është dislokuar është për të mbledhur statistika per-LSP.

Kur e shqyrtojmë një model të një AS që ofron shërbimin e transitit, matrica ruter-ruter nuk është e mjaftueshme. Duhet marrë në konsideratë matrica prefiks – prefiks pasi që (1) routeri i daljes i zgjedhur nga një ruter hyrjeje për të arritur një prefiks destinacioni mund të ndryshojë dhe (TGVS04) (2) routeri i hyrjes ku trafiku nga një prefiks që ishte marrë gjithashtu mund të ndryshojë. Teknikat e përshkruara më lart nuk janë të zbatueshme këtu pasi nuk japin informacion mbi burimet dhe destinacionet e trafikut që rrjedh.

Një zgjidhje është mbështetja në statistikën NetFlow (SF02) të mbledhura në ruterat kufi. Mbledhja e të dhënave të tilla është ende një çështje operative sot (VE04). Problemet me të cilat përballen operatorët e rrjetit janë si në vijim. Së pari, madhësia e një matrice prefixprefix është dukshëm më e madhe se një matricë ruter - ruter. Numri i burimeve dhe prefikset e destinacionit është në rendin e 180,000 (Hus06). Së dyti, aktivizimi i NetFlow mund të vënë një barrë të rëndësishme mbi routerat kufitare. Së fundi, ngritja e një infrastrukture të tillë të matjes kërkon një investim të rëndësishëm në kohën e konfigurimit dhe pajisjet. Si pasojë, NetFlow zakonisht do të aktivizohet vetëm në ndërfaqet peering që bartin një pjesë të konsiderueshme të trafikut. Përveç kësaj, kampionimi i NetFlow (CB05) është përdorur edhe për të ulur volumin e statistikave të mbledhura.

3.2.2 Modeli GEANT

Në këtë seksion, është përshkruar se si ne është përdorur solver-i i rrugëzimit për të modeluar rrugëzimin e një rrjeti tranzit. Është përdorur rrjeti GEANT si një rast studimi. GEANT është rrjeti kërkimor i cili është operuar nga Dante. Ai mban trafik kërkimesh nga European National Research and Education Networks (NRENs) dhe lidh universitete dhe institucione kërkimore. GEANT ka nxjerrë PoPs në të gjitha vendet e Europës. Të gjitha ruterat e GEANT janë ruterat kufitare. Fig.3.3 tregon një pasqyrë të shtyllës kurrizore GEANT.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

3.2.3 Topologjia

Është marrë topologjia e shtresës - tre e GEANT nga një gjurmë një -ditore IS – IS. Është ndër- kontrolluar topologjia e fituar me një hartë rrjeti të ofruar nga Dante. Është modeluar GEANT me një grafik të përbërë nga 23 routera, 38 lidhje kryesore bërthamë dhe 53 lidhjet anësore edge .

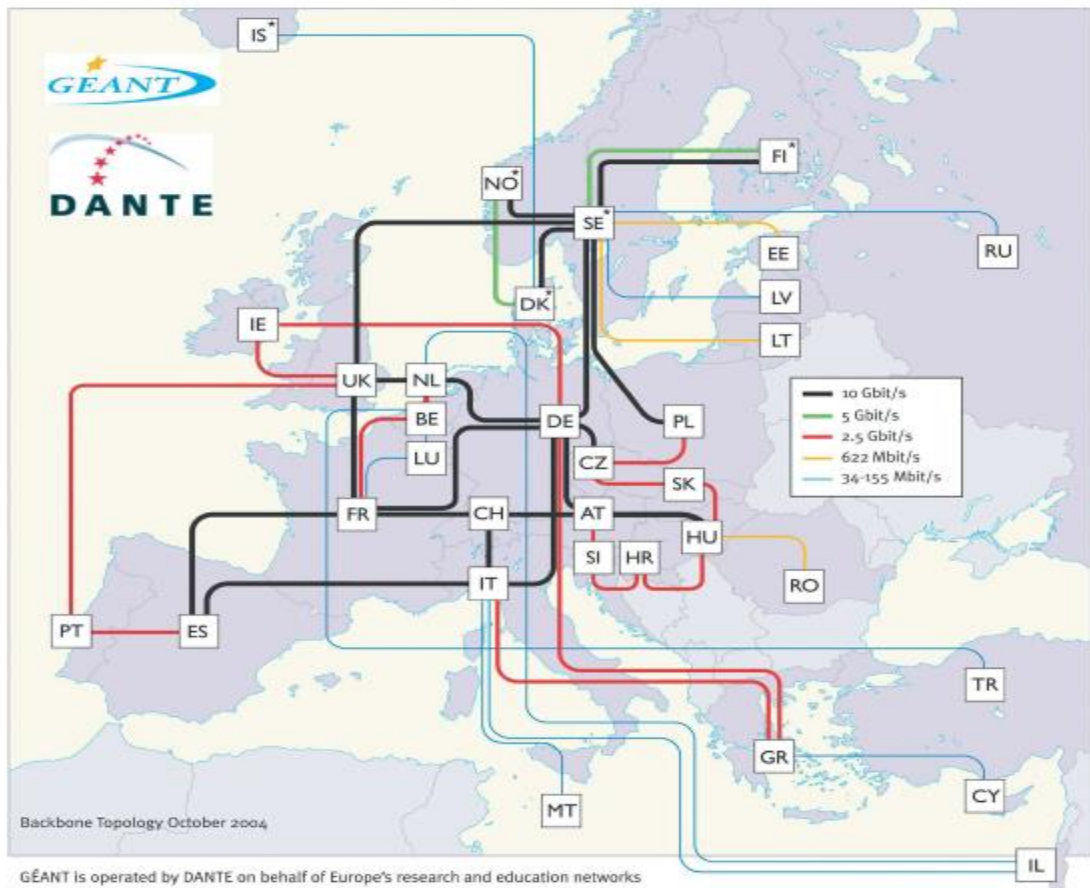


Figura 3.3: Pamje e përgjithshme e hartës të GEANT (burimi: <http://www.geant.net>).

3.2.4 Rrugëzimi i të dhënave

Në GEANT, rrugët BGP janë mbledhur duke përdorur një workstation të dedikuar që ekzekuton GNU Zebra, një software implementimi i BGP. Workstation-i ka një seksion iBGP me 22 e 23 routera kufitare të rrjetit. Duke përdorur këtë teknikë, është bërë e mundur për të mbledhur të gjitha rrugët më të mira BGP të zgjedhura nga routerat kufitare të AS. Është përdorur një fotografi dhe janë marrë 640,897 rrugë BGP të përhapura në iBGP. Kështu, janë ditur të gjitha rrugët më të mira për momentin të zgjedhura nga secili router në GEANT.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Ky është një nëngrup i të gjitha rrugëve të eBGP të mësuar nga GEANT në 53 peering e saj pasi ne nuk njihen rrugët eBGP aktualisht jo të përzgjedhura si më të mirat. Duke pasur vetëm rrugët e eBGP të zgjedhura si më të mirat mund të ndikojnë në rezultatet e eksperimenteve në rastin kur një rrugë e panjohur eBGP do të ishte zgjedhur në vend të një më të mire aktuale. Vini re se për të mbledhur të gjitha rrugët eBGP të marra nga GEANT do të ishte kërkuar kapja e mesazheve BGP të marra në 53 lidhjet peering .

Kompleksiteti kompjuterik i njëhësimi nga llogaritja e rrugëve është në proporcion me numrin e prefikseve në tabelat e rrugëzimit. Një tabelë rrugëzimi e plotë BGP mund të përmbajë më shumë se 180.000 prefikse. Megjithatë, kur duke pasur parasysh rrugët e shpallura nga të gjithë fqinjët e një domain-i , duket se shumë prefikse janë mësuar nga të njëjtët fqinjë, me të njëjtën cilësi BGP-je (Local-Pref, length of the AS-Path, MED, next-hop) (HP00).

Rezultati i procesit të vendimmarrjes në të gjithë rrjetin do të jetë i njëjtë për këto prefikse. Për shembull, në Fig 3.4, rrjeti merr rrugët eBGP ndaj 2 prefikseve të ndryshme: P1 dhe P2. Këto prefikse janë mësuar nga të tre të njëjtët fqinjë dhe për secilin, cilësia e BGP është e njëjtë për të dy prefikset. Gjatësia për P1, AS- Path të marrë nga A1 është A : 100 : 10 dhe P2 , AS- Path është A : 100 : 20. Gjatësia e rrugëve AS - Path është e njëjtë për të dyja. Kjo është e njëjtë për rrugët e marra nga A2 dhe nga Z1. Pika e daljes së zgjedhur nga routerat në rrjetin e modeluar është e njëjtë për të dy prefikset (shih shigjetat me pika në Fig. 3.4). Prandaj, është kufizuar në prefix P1, llogaritja e rezultatit të procesit të vendimmarrjes BGP në modelin meqë rezultati do të jetë i njëjtë për P2.

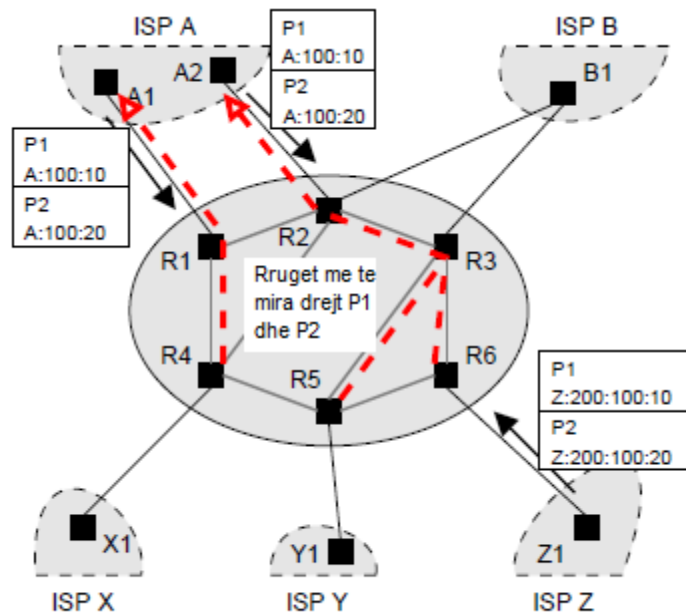


Figura 3.4: Cluster-imi i prefikseve BGP

Për të vlerësuar zbatueshmërinë e kësaj metode clustering në GEANT, është parë në rrugët eBGP të mbledhura. Janë grupuar së bashku prefikset të njoftuara me të njëjtën

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

cilësi të BGP nga të njëjtat routera fqinje. Është përfunduar me 406 grupe cluster-ash për 105,071 prefikset. Kjo paraqet një raport clustering prej 0.27%. Është treguar në Fig.3.5 shpërndarja e numrit të prefikseve në cluster-at e përfituara. 80% e tyre përmbajnë më pak se 67 prefikse. Grupet e mbetura mund të përmbajnë deri në mijëra prefikse. Gjithashtu është vëzhguar stabiliteti i numrit të grupimeve përgjatë kohës. Gjatë periudhës së shkuar nga 16 në 30 nëntor, numri i prefikseve shkonte nga 149,438 në 150,234. Për këtë periudhë, numri i grupeve ishte 405.8 mesatarisht me një standard të vogël devijimi 16.5, do të thotë se numri i grupimeve nuk ka ndryshuar shumë gjatë kësaj periudhe. Kemi vërejtur të njëjtën sjellje për të dhëna më të fundit.

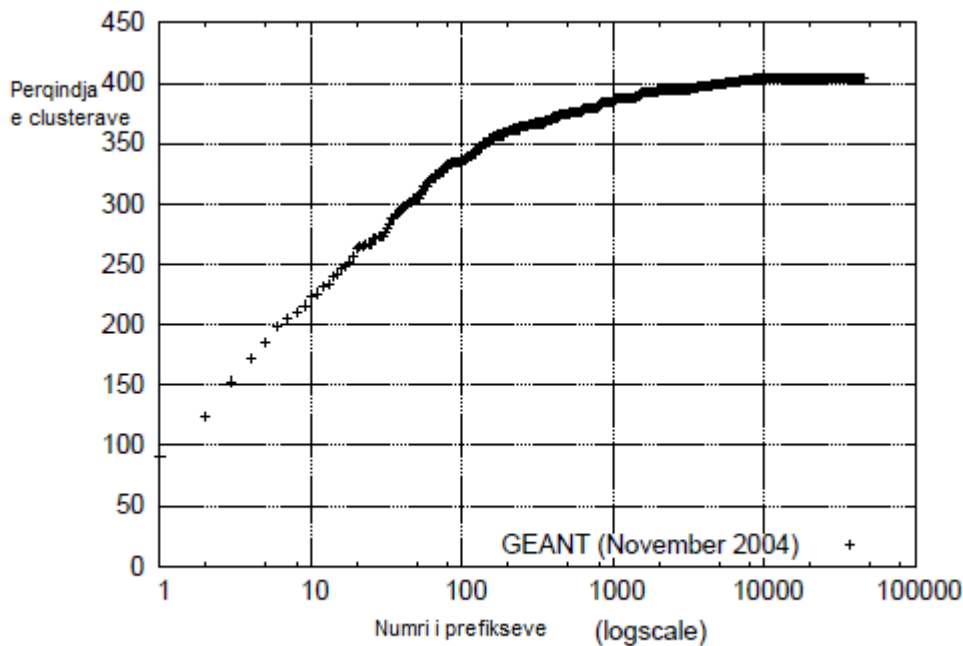


Figura 3.5: Frekuenca cumulative e cluster-ave me numër të njëjtë prefiksesh.

Kjo do të thotë se për GEANT, në vend të ndërfitjes së 105.071 prefikseve në simulator (që përfaqëson 640.897 rrugë të ndryshme), mund të ndërfiteshin vetëm 406 prefikse (që përfaqësojnë 986 rrugë) në modelin pa humbur asnjë informacion mbi rezultatin e procesit të vendimmarrjes. Njësimi i rrugëve BGP ndaj 406 grupimeve të GEANT duke përdorur C - BGP që i nevojshëm vetëm 68s në një P4 Intel i cili ekzekutohej në 2.66GHz dhe kishte gjurmë të kujtesës vetëm 69MB.

3.2.5 Statistikat e trafikut

Për të ndërtuar një model të saktë të trafikut, janë marrë statistikat e mbledhura me NetFlow në të gjitha lidhjet edge të rrjetit GEANT. Për të kufizuar volumin e gjurmëve NetFlow, është përdorur një raport NetFlow kampion prej 1/1000. Kjo ende gjeneron në

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

rendin e 150 GB të gjurmëve zipped në muaj të trafikut. Prandaj, edhe më tej është përmbledhur informacioni NetFlow duke bashkuar në një (prefiks burim, prefiks destinacion) bazë, duke e mbajtur vetëm vëllimin për çdo (prefiks burim, prefiks destinacion) palë për çdo skedar NetFlow. Është quajtur rezultati i procesit të përmbledhjes "NetFlow të grumbulluara". Është përdorur një bazë rrugëzimi të vetëm BGP Informacioni (RIB) që të mbledhë flukset e para NetFlow, pasi qëllimi është vetëm për të kufizuar madhësinë e gjurmëve.

3.3 Karakterizimi i rrugëzimit

Në këtë seksion, është karakterizuar rrugëzimin në GÉANT. Është identifikuar në nënseksionin vijues se cilët janë faktorët që ndikojnë në të dy itineraret të intra dhe interdomain. Këta faktorë do të ndihmojnë për të kuptuar rezultatet e " çfarë- nëse " skenarë të studiuar në seksionin 3.5.

3.3.1 Rrugëzimi Intradomain

Në mënyrë që të karakterizohet rrugëzimi intradomain, u mbështetën në një masë të qendrës së routerave dhe lidhjeve në grafik. Kjo masë tregon se si rrugëzimi intradomain është i ndjeshëm ndaj dështimit të një routeri ose lidhjeje. Kjo do të thotë, sa më shumë një nyje ose lidhje është në qendër, aq më shumë dështimi i saj do të shkaktojë ndryshime intradomain shtegu. Masa e përdorur zakonisht për të kryer këtë karakterizim është betweennesscentrality (BE04). Në thelb, betweenness - qendërsia llogarit sasinë e shtigjeve më të shkurtër që kalojnë nëpër një kulm ose një anë (edge). Qendërsimi i një kulmi v është llogaritur si :

$$c(v) = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}}$$

dmth shuma për të gjitha palë e burimeve dhe destinacioneve (s , t) e pjesëve të shtigjeve më të shkurtër (shortestpaths) nga s për t që kalojnë nëpër v . σ_{st} tregon numrin e shtigjeve më të shkurtër nga s për t dhe $\sigma_{st}(v)$ tregon numrin e shtigjeve më të shkurtër nga s për t që kalojnë nëpër V. Një perkufizim i ngjashëm është përdorur për të llogaritur rëndësinë e skajeve :

$$c(u, v) = \sum_{s \neq u, v} \frac{\sigma_{st}(u, v)}{\sigma_{st}}$$

ku $\sigma_{st}(u, v)$ tregon numrin e të shkurtër - shtigjet nga s për t që kalojnë nëpër anët edge (u , v). Vini re se çështja e drejtimit ka mjaft rëndësi. Është treguar qendërsia - betweenness - të ruterave GEANT në Fig 3.6 dhe betweenness - qendërsimi i lidhjeve GEANT në Fig 3.7. Vihet re se për skajet, është përmbledhur qendërsimin për të dy drejtimet. Vëzhgimi i parë që mund të bëhet është se shpërndarja e qendërsisë është

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

anuar. Kjo do të thotë se nga pikëpamja e rrugëzimit intradomain, disa nyje dhe disa lidhje janë më të rëndësishme se të tjerët. Nëse këto nyje ose lidhje mund të dështojnë, ndikimi i tyre në shtigjet intradomain do të jetë më i lartë se të tjerët. Për shembull, rreth gjysma e nyjeve kanë një qendërsi e cila është afër zeros.

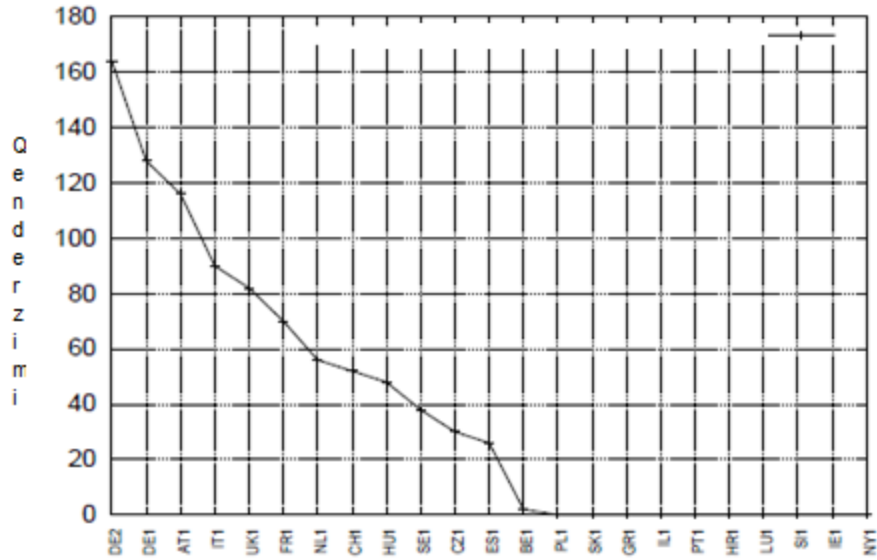


Figura 3.6: Qendërsimi Betweenness i ruterave GÉANT.

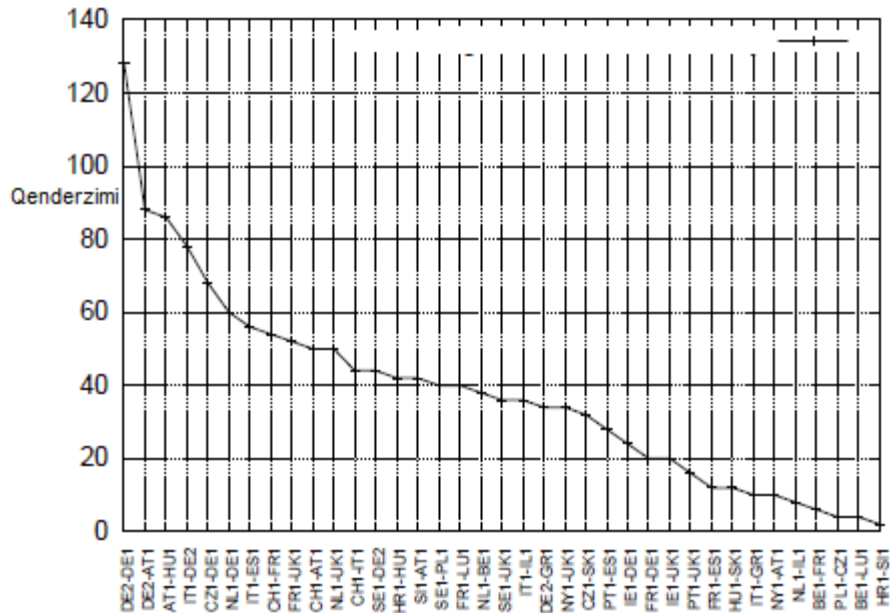


Figura 3.7: Qendërsimi Betweenness i linqeve GÉANT.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Kjo do të thotë që nga pikëpamja e rrugëzimit intradomain, këto nyje janë rrallë nyje tranziti. Gjysma tjetër mbështet një numër të ndryshueshëm të shtigjeve më të shkurtër. DE2, DE1 dhe AT1 kanë rëndësinë më të lartë. Pritet që dështimi i tyre do të ketë një ndikim të rëndësishëm në rrugëzim. Për sa i përket lidhjeve, ne gjithashtu është vërejtur se disa linqe duken më kritike se të tjerët : DE2 - DE1 , DE2 - AT1 dhe AT1 - HU1 janë lidhjet me qendërzimin më të lartë. Mund të konkludohet se rrugëzimi intradomain në **GEANT është më së shumti i ndjeshëm ndaj dështimit të një numri të vogël të nyjeve dhe lidhjeve.**

3.3.2 Rrugëzimi Interdomain

Në mënyrë që të karakterizohet rrugëzimi interdomain në GEANT, së pari është analizuar shumëllojshmëria e rrugëve interdomain. Për këtë qëllim, është marrë parasysh numri i rrugëve interdomain të mësuar nga GEANT gjatë seksioneve të tij eBGP ndaj çdo prefiksi destinacion. Kjo jep informacion në lidhje me numrin e pikëve të mundshme të daljes për secilin prefiks destinacioni. Është treguar ndarja e prefikseve kundrejt numrit të rrugëve eBGP në Fig.3.8. Informacioni i dytë i cili është paraqitur në Fig.3.8 shpreh shqetësimet e numrit të rrugëve të marra nga i njëjti fqinj AS për çdo prefiks. Rrugë të shumëfishta janë mësuar nga i njëjti fqinj AS, kur ka lidhje paralele peering me këtë AS. Është llogaritur për çdo prefiks destinacioni dhe për çdo fqinj AS numri i rrugëve të mësuar. Është marrë në konsideratë për secilin prefiks maksimumi i numrit të rrugëve të mësuar nga i njëjti AS. Është treguar ndarja e prefikseve kundrejt numrin maksimal të "rrugëve paralele" në Fig .3.8.

Një vëzhgim i parë është se GEANT ka mësuar të paktën 2 rrugë për për shumicën e parashtesave (prefiksve) destinacion (më shumë se 97 %). Për 63% të prefikseve, ka mësuar edhe 5 rrugë. Për më tepër, numri maksimal i rrugëve të mësuar nga një fqinj AS është mes 3 dhe 4 për shumicën e prefikseve destinacion. Kjo pritej meqë GEANT ka deri në 4 lidhjet peering me disa nga fqinjët e saj. Pra është kështu një diversitet i lartë rrugësh në GEANT .

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

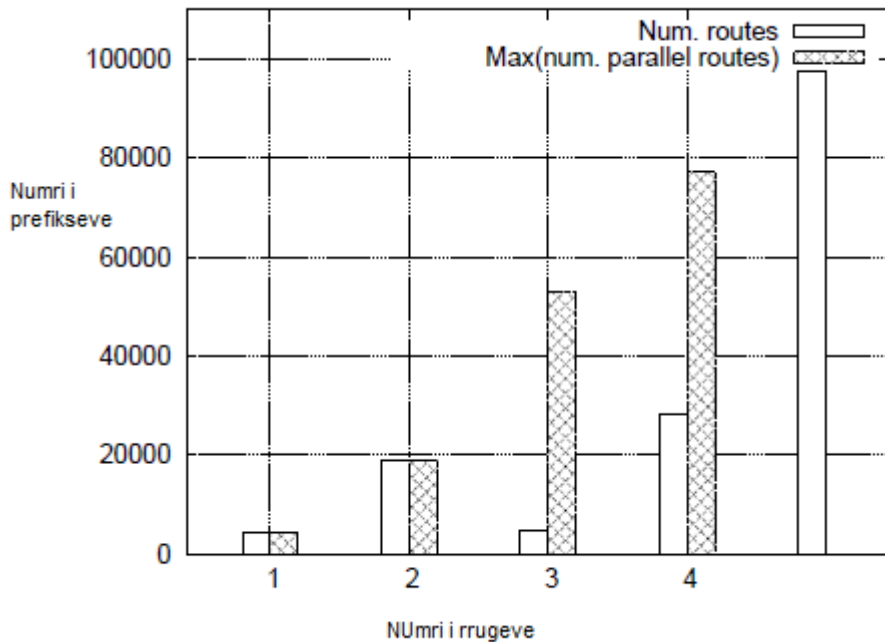


Figura 3.8 : Ndarja e prefikseve nga numri i rrugëve të marra në GEANT .

Duke pasur parasysh diversitetin rrugëve të treguar në Fig .3.8, është interesante për të pyetur se si secili router do të zgjedhë rrugën e tij më të mirë. Për këtë qëllim, është parë në secilin ruter të modeluar, çfarë ishte sundimi i procesit të vendimmarrjes BGP që është përdorur për të zgjedhur rrugën më të mirë drejt çdo prefiksi destinacion. Janë treguar rezultatet tona në Fig.3.9. Aksi x i figurës përfaqëson çdo router të modeluar të identifikuar me emrin e tij. Axi-y përfaqëson prefikset destinacion të njohur nga ky ruter . Për çdo ruter, figura tregon rregullin e procesit të vendimmarrjes BGP që është përdorur për të zgjedhur një rrugë drejt një pjesë të prefikseve. Janë treguar vetëm 4 rregullat kryesore. Rregulli i "rrugë e vetme " do të thotë se ruteri nuk ka zgjedhje, sepse ai mori vetëm një rrugë të vetme për prefiks të destinacionit. Kuptimi i rregullave të tjera është i drejtpërdrejtë. Vëmë re se ndikimi i diversitetit të rrugëve në procesin e vendimmarrjes BGP është i lartë. Në GEANT shumica e prefikseve të destinacionit (më shumë se 97 %) janë të arritshme me anë të të paktën 2 rrugë të ndryshme (shih Fig.7.8). Si pasojë, ndikimi i strukturës së brendshme të GEANT në zgjedhjen e rrugës interdomain është e rëndësishme. Pika interesante këtu është se për shumicën e parashtesave (prefikseve) destinacion, janë përdorur rregullat e lidhura me rrugëzimin hot - patate. Shihet se ruterat kufitare që marrin një pjesë të madhe të rrugëve eBGP zgjedhin rrugën më të mirë kundrejt një pjesë të madhe të prefikseve duke përdorur rregullin " eBGP mbi iBGP". Ky është rasti për IT , SE , Britania e Madhe , CH dhe DE1. Kjo do të thotë se vendi i pikave peering është i rëndësishëm për modelin. Përveç kësaj , rregulli " Nearest next hop " është përdorur për shumicën e përzgjedhjes së rrugës. Kjo do të thotë se për këto ruterat dhe për këto destinacione, zgjedhja e rrugë ishte pjesërisht e bazuar në koston IGP për të

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

arritur ruterat e daljes. Vërehet gjithashtu se 4 ruterat përdorin rregullin " Router - ID më i vogël " për të zgjedhur një pjesë të madhe të rrugëve të tyre : FR ,NL , BE dhe LU . Arsyeja është se këto ruterat janë në një distancë të barabartë IGP nga ruterat e daljes duke njoftuar një pjesë të madhe të rrugëve .

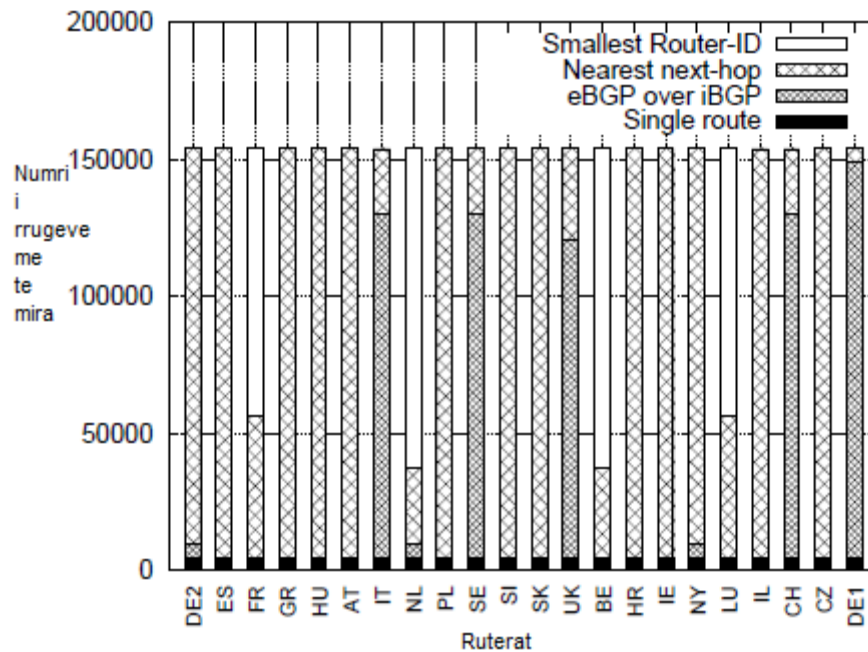


Figura 3.9: Rëndësia e rregullave në GEANT

3.3.3 Skenarët Çka – nëse

Në këtë seksion, janë paraqitur dy raste studimore që kryhen në modelin e rrjetit GEANT. I pari heton shtimin ose heqjen e peerings në rrjedhën e trafikut. Studimet e dytë mposhtin ndikimin e dështimeve të lidhjeve.

3.3.4 Peering i optimizuar

Një problem i rëndësishëm me të cilat përballen ISP-të është për të gjetur vendndodhjen optimale të pikave peering. Një ISP do të kërkojë për pikë të reja peering në mënyrë që të përmirësohet efikasiteti i trafikut të saj interdomain dhe / ose për të ulur koston e peering të saj. Zbulimi i vendndodhjes peering optimale është një problem jo i parëndësishëm (AAM98), që varet nga faktorët si teknike dhe ekonomike (Nor02). Në (AAM98), autorët u fokusuan në vendndodhjen e peerings me një fqinj të vetme AS. Me këtë mjet, mund të hetohej problemi i modifikimit të lidhjes interdomain të një AS derisa merret në konsideratë informacionin BGP. Për dijeninë tonë, qasjet ekzistuese nuk kanë marrë BGP parasysh. Në praktikë një AS mund të zgjedhë të peer me mjaft AS të ndryshme dhe në

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

zona të ndryshme. Gjithsesi, të gjitha zonat e mundshme nuk i kënaqin kërkesat e ISP-së dhe ISP duhet të vendosë i cili përshtatet më tepër qëllimeve të tij. Është marrë një shembull të provider-it tranzit. Është supozuar se rrjeti i tij është i përbërë prej n POP. Tani supozohet se provider-i shërben klientit të ri AS që lidh në disa PoPx-e. Këta klientë shkaktajnë një sasi të shtuar trafikut për të kapërcyer topologjinë përpara se të dalin në PoP-e të tjerë. Për të parandaluar trafikun për të kaluar të gjithë rrjetin përpara se të arrijnë pikat e daljes, provider-i tranzit mund të preferojë të shtojë një peering afër PoPx-it që gjeneron më shumë trafik në mënyrë që trafiku i marrë nga ky PoP të dalë nga rrjeti sa më parë që të jetë e mundur. Kështu që pritet që një sasi e dhënë trafikut të dalë nga rrjeti përmes peering-ut të ri, por është tepër e vështirë të parashikohet sasia. Shtimi i një peering ka potencialin të modifikojë rrugët më të mira të ruterit BGP të lidhura me këtë peering të ri. Ka të ngjarë që ky ruter do të selektojë rrugët e mësuara përmes peering-ut të tij të ri si rrugët më të mira. Më pas do të rishpërndajë rrugët e reja më të mira drejt ruterave të tjerë BGP nëpërmjet seksioneve iBGP. Nëse ruterat e tjerë BGP zgjedhin të përdorin disa nga rrugët e mësuara nëpërmjet peering-ut të ri, është e mundur të kalojë më shumë trafik në rrjet nga sa ishte planifikuar në fillim në peering-un e ri. Modelet e një AS që nuk e marrin në konsideratë rrugëzimin nuk mund të parashikojnë ndryshimin e saktë në matricën e trafikut në një rast të tillë. Me këtë mjet modelimi, është mundësuar të parashikohet çfarë do të ndodhë në një trafik AS-je kur shtohet apo hiqet një peering i ri. Në mënyrë që të krahasohet impakti i skenarëve të ndryshëm, do të përdoren metrika të ndryshme. Fillimisht njëhsohet shpërndarja e trafikut mbi linqet peering. Shtimi i një peering-u të ri mund të tërheqë trafik nga lidhjet peering ekzistuese tashmë dhe të ulë mundësinë e ndodhjes së kongestionit në këto lidhje. Më pas llogaritet koston IGP që trafiku merr kur i shtohet një peering i ri. Nëse kostoja ulet për një numër domethënës çiftesh hyrëse-dalëse, kjo do të thotë se trafiku ndjek path-e intradomain që janë më të shkurtër në terma peshe IGP të caktuara nga ISP.

Është kryer ky vlerësim në një rrjet GEANT. Në fakt, Dante i cili vepron në GEANT, po merret me hartimin e versionit të ardhshëm të rrjetit të tij. GÉANT2 do të ketë një rritje të numrit të konsumatorëve, kryesisht në Evropën Lindore. GÉANT2 do të sigurojë kalimin tranzit të NRENs shtesë, duke përfshirë rusen NREN, JSCC, përsëmbull. Në këtë kontekst, është e rëndësishme për Dante të dinë se cilat vende do të përfitojnë nga peerings shtesë. Në vlerësimin tonë, janë konsideruar gjashtë më të rëndësishmit peerings të rrjetit GEANT që ne i quajmë PR1, ..., PR6. Sot, të gjithë këto peerings përdorin OC - 48 lidhje me një kapacitet 2.4 Gbps. Është studiuar shtimi dhe heqja e peerings dhe ndikimi i tyre në trafikun që vjen nga të gjithë klientët GEANT.

Fig.3.10 tregon ndikimin e heqjes apo shtimit të një peering, në kuptimin e shpërndarjes së trafikut dalës mbi peerings-at që konsiderohen të GEANT. Aksi X - Fig.3.10 jep skenarë të ndryshëm të simuluar. Një prej tyre i etiketuar "Default" jep shpërndarjen e trafikut në qoftë se ne do të largohemi nga peerings aktuale i pandryshuar.

Ata të etiketuar "të hequr - X" kanë të bëjnë me skenarët ku kemi hequr peerings-at ekzistues X. Të tjerët të etiketuar me "add - PRX" janë skenarë ku një peering u shtua në PoP X. Aksi Y i Fig.3.10 tregon shpërndarjen e Përqindjes së trafikut të përgjithshëm në dalje të mbartur nga peerings-at e marrë në konsideratë.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

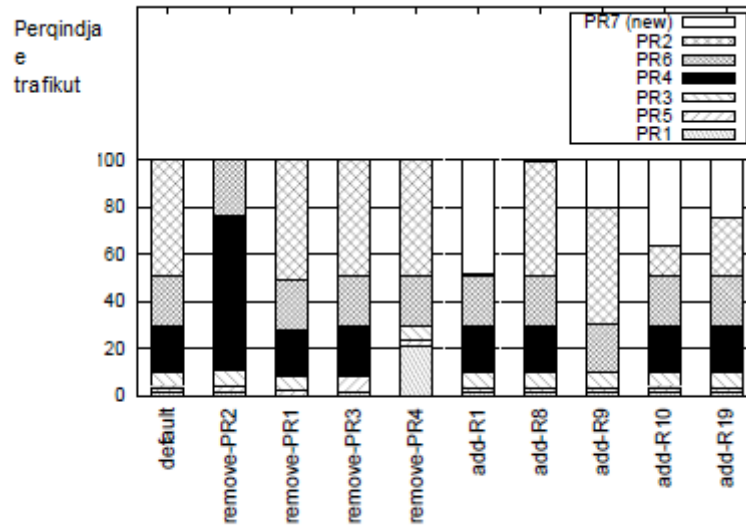


Figura 3.10 : Ndikimi i shtimit / heqjes së peerings në shpërndarjen e trafikut përgjatë lidhjeve peering.

Skenari " default" në Fig.3.10 tregon se gati 50 % e trafikut është bartur nga një peering i vetëm eBGP (PR2) dhe dy të tjerë peerings bartin secili rreth 20 % përkatësisht. Trafiku është duke balancuar në mënyrë të pabarabartë mbi lidhjet e konsideruara peering. Heqja e një peering nuk e ndryshon këtë shpërndarje të pabarabartë . Kur peering PR2 është hequr , pothuajse i gjithë trafiku del në PR4 dhe PR6 . Heqja e peerings-ve PR1 ose PR3 ka efekt të vogël . Heqja e peering PR4 shkëmben trafikun e saj drejt peering PR1 . Tani le të marrim në konsideratë shtimin e peerings në NOQ- R1 , R8 , R9 , R10 dhe R19. Shtimi i një lidhje peering në R1 absorbon të gjithë trafikun që doli më parë me PR2. Shpjegimi është se shumica e trafikut të dërguar përmes peering PR2 vinte nga Evropa Lindore. Për të arritur në peering PR2, këto paketa tani duhet të kalojnë nëpër router R1 dhe kështu të lënë rrjetin GEANT atje. Nëse qëllimi i shtimit të këtij peering është për të ndryshuar shpërndarjen e pabarabartë të trafikut përgjatë lidhjeve peering, pastaj duke shtuar një peering në R1 nuk na ndihmon. Situata është e ngjashme kur duke shtuar një peering në R9, pasi ajo thith pjesën më të madhe të trafikut që më parë doli nëpër peering PR4. Shtimi i një peering në R8 është i pavlefshëm pasi shpërndarja e trafikut është lënë e pandryshuar. Shtimi i një peering në R10 ose R19 nga ana tjetër, përmirëson ekuilibrin e trafikut mbi linjet peering e marrë në konsideratë.

Modifikimi i peerings të një AS ndryshon jo vetëm shpërndarjen e trafikut ndër peerings, por edhe se si trafiku kalon topologjinë intradomain.

Fig.3.11 tregon ndikimin e shtimit ose heqjes së një peering mbi koston IGP të vuajtur nga trafiku për të kaluar në rrjet. Në boshtin x të Fig.3.11, është treguar se dallimi mes IGP kushtëzon trafikun ti nënshtrohet në situatën e parazgjedhur dhe atë në çdo skenar.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Një ndryshim pozitiv do të thotë një përmirësim meqë kostoja IGP është ulur. Një ndryshim negativ do të thotë një përkeqësim. Në aksin Y i Fig.3.11, është treguar pjesa kumulative të trafikut që percepton një ndryshim në koston IGP.

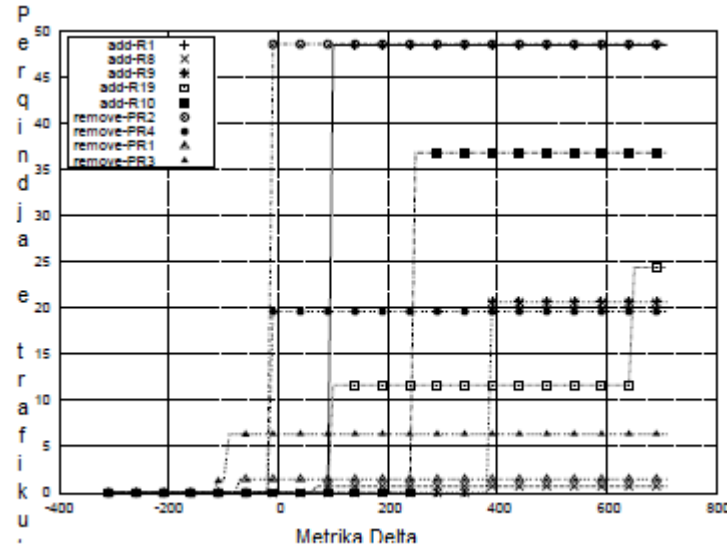


Figura 3.11: Ndikimi i shtimit/ largimit të peerings në koston e IGP të parë nga trafiku.

Është parë në Fig.3.10 se heqja e peerings PR1 dhe PR3 nuk ka ndikuar shumë në bilancin e trafikut në lidhjet peering. Megjithatë, mund të shihet se heqja e peering PR3 ka një ndikim në koston IGP e parë me 5% të trafikut. Kostoja IGP për këtë trafik është rritur me 100. Një tjetër vëzhgim është se edhe pse heqja e peering PR2 ka një ndikim të rëndësishëm në shpërndarjen e trafikut në lidhjet peering, ka një ndikim të vogël në koston IGP (= -5) e parë nga ky trafik. Skenarët më interesantë janë shtimi i peering në R10 ose R19 që përmirëson edhe koston IGP dhe shpërndarjen e trafikut ndër lidhjet peering si u tregua më sipër. Nëse qëllimi i shtimit të një lidhjeje të vetme peering është të përmirësojë shpërndarjen e trafikut mbi lidhjet peering pa përkeqësim në vonesën në gjithë rrjetin, atëherë dihet se zgjidhja është të shtohet një peering ose në R10 ose në R19. Në Fig.3.11, është treguar ndikimin e shtimit ose heqjes së një peering në vonesën e parë nga trafiku për të kaluar në rrjet. Rezultatet janë paraqitur në të njëjtën mënyrë si për diferencën e koston IGP e treguar në Fig.3.10. Në boshtin x të Fig.3.12, është treguar dallimi mes vonesës së trafikut që është subjekt në situatën e parazgjedhur dhe atij në secilin skenar. Një ndryshim pozitiv do të thotë një përmirësim derisa vonesa është ulur. Një ndryshim negativ do të thotë një përkeqësim. Në aksin Y i Fig.3.12, është treguar pjesa kumulative e trafikut që percepton një ndryshim në vonesë.

Vërehet në Fig.3.12 që shumicën e kohës përmirësimi i koston IGP është i lidhur me përmirësimin e vonesës. Ka një përjashtim me heqjen e peering PR2 i cili shkakton një përmirësim të vogël në koston IGP, por një degradim të vogël i vonesës. Kjo mund të duket e habitshme, por kjo mund të shpjegohet me mënyrën sesi peshat IGP janë caktuar në GEANT. Dante shpjegon se nga fakti që ata së pari përdorin peshat IGP që janë në përpjesëtim me kapacitetet e lidhjeve. Pastaj, caktimi manual i peshave është bërë për të

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

preferuar shtigjet me vonesën më të ulët. Së fundi, peshat IGP janë caktuar në mënyrë që të shmangen shtigjet me kosto të barabartë. Nuk është pra domosdoshmërisht një korrelacion midis vonesës dhe koston IGP. Është gjithashtu e rëndësishme të theksohet se Fig.3.12 jep vetëm vonesën intradomain. Për të matur ndikimin në vonesë fund-më-fund, shqyrtimi aktiv duhet të kryhet në një bazë për destinacion, e cila është e shtrenjtë .

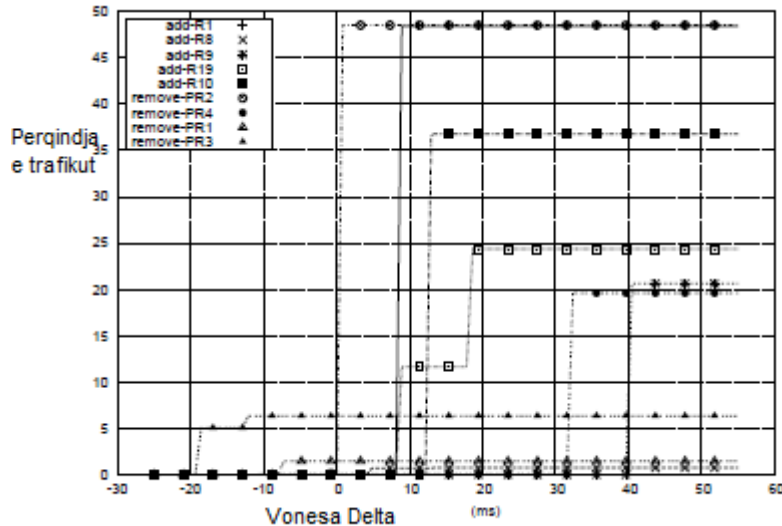


Figura 3.12 : Ndikimi i shtimit / largimit të peering në vonesën e parë nga trafiku .

3.3.5 Dështimet e linqeve dhe ruterave

Vlerësimi i ndikimit të dështimeve të lidhjeve dhe ruterave në rrjet është një problem tjetër jo banal. Në një rrjet të madh, përcaktimin se cili dështim lidhjeje apo ruteri do të ndryshojë rezultatit e zgjedhjes së daljes të kryer nga BGP është problem i vështirë. Ky është një problem i rëndësishëm pasi ndryshimet e rrugëzimit mund të shkaktojnë ndërrime trafiku dhe të çojnë në bllokime (TSGR04). Për një operator, është e rëndësishme që të kontrollohet se rrjeti do të jetë në gjendje për të akomoduar ngarkesën e trafikut, edhe në rastin e një dështimi të vetëm lidhjeje ose ruteri. Nëse jo, është e dobishme për të identifikuar lidhjet e rrjetit të cilat duhet të mbrohen me shtimin e lidhjeve paralele , mbrojtjen SONET - SDH ose përdorimin e tunele mbrojtës MPLS (VPD04). Metodologjia për të studiuar ndikimin e ndryshimeve intradomain në zgjedhjen e rrugëve është si më poshtë. Së pari, është ndërtuar një përfaqësim të rrjetit brenda solverit rrugëzues. Është lejuar solver-i të llogarisë rrugët në çdo ruter, më pas është ruajtur një fotografi snapshot të rrugëve të zgjedhura. Kjo fotografi përputhet me gjendjen e rrugëzimit kur çdo gjë është në ekzekutim. Pastaj është hequr lidhja e dështuar ose ruteri dhe i lejohet solverit rrugëzues të rillogarisë shtigjet.

Në mënyrë që të sigurohet një pamje sintetike të ndikimit të çdo dështimi, është ndarë secili grup i ndryshimeve në rrugëzim në katër klasa të ndryshme: ndryshimi Peer, ndryshimi i daljes, ndryshim brenda koston dhe ndryshimi Intra path. Klasa e ndryshimit Peer korrespondon me ndryshimet në hapin e ardhshëm AS. Nëse ai nuk ka ndryshuar,

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

por ka ndryshuar ruteri i daljes, flasim për një ndryshim *Egress change*. Kur dalja është e pandryshuar por kostoja IGP i rrugës hyrje-dalje ka ndryshuar, ndryshimi i rrugëzimit është klasifikuar si një ndryshim të koston brenda. Së fundi, në qoftë se një rrugë hyrje-dalje me të njëjtën IGP kostoja është gjetur, ndryshimi i rrugëzimit është vënë në brenda klasës *Intra path change*. Kjo mund të ndodhë vetëm nëse ka shtigje të shumta me kosto të barabartë në mes të një hyrje dhe një daljeje routeri në rrjet. Janë simuluar të gjitha dështimet e një lidhjeje të vetme në GEANT dhe vëzhguar ndikimin në rrugët BGP të zgjedhura nga secila router GEANT. Janë treguar rezultatet në Fig. 3.13. Në boshtit x, tregohen të gjitha lidhjet e brendshme të GEANT. Në aksit y, tregohet numri i ndryshimeve të rrugëzimit total në të gjitha ruterat GEANT. Ndryshimet e rrugëzimit janë klasifikuar në ndryshimin Peer, ndryshimi dalje, ndryshimit të koston brenda dhe brenda dhe ndryshimi i shtigjeve intra (*Peer change, Egress change, Intra cost change and Intra path change*) siç shpjegohet më sipër. Lidhjet në boshtin x janë të renditura sipas numrit të përgjithshëm të ndryshimeve të rrugëzimit të shkaktuara nga dështimi i tyre. Vërehet se shumicën e kohës, një dështim i një lidhjeje të vetme bën shumë ndryshime në dalje. Gati 60% e lidhjeve GEANT mund të shkaktojë më shumë se 100.000 ndryshime rrugëzimi, kur ata dështojnë.

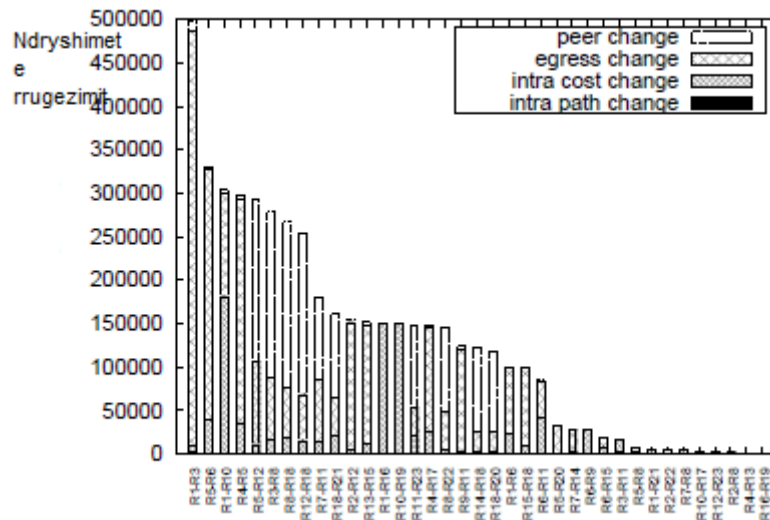


Figura 3.13 : Analiza e dështimit të një linku të vetëm: ndikimi në BGP .

Gjithashtu mund të vërehet se, në GEANT, ka pak ri-rrugëzime të pastra intradomain. Kjo do të thotë se, ka disa ndryshime rrugëzimi në klasat e ndryshimit brenda koston (Intra cost change) dhe rrugën intra (Intra path Change). Këto rezultate tregojnë se një model i pastër intradomain e rrjetit GEANT nuk do të kapë shumicën e ndryshimeve të rrugëzimit që ndodhin nën dështimet e lidhjeve të vetme. Kjo tregon qartë se për të modeluar me saktësi një rrjet tranzit si GEANT, është e nevojshme për të marrë parasysh rrugët interdomain dhe topologjinë. E njëjta metodë mund të përdoret për të kryer analiza të dështimit të një ruteri të vetëm ose për të studiuar ndikimin e ndryshimit të koston IGP në një lidhje. Janë marrë rezultate të ngjashme me ato të gjeturat për dështimet e lidhjeve.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Janë treguar ato në Fig.3.14. Në aksin x, tregohen të gjitha routerat e GEANT. Në aksin y, tregohet numri i ndryshimeve të rrugëzimit të grumbulluara në të gjitha routerat GEANT. Në routerat në boshtin x janë të renditura sipas numrit të përgjithshëm të ndryshimeve rrugët të shkaktuara nga dështimi i tyre. Vërehet se dështimi i gati gjysmës së routerave GEANT mund të shkaktojë ndryshime të rrugëzimit. Dështimi i një routeri të vetëm mund të shihet si dështim i përbashkët i të gjitha lidhjeve të tij. Pasoja është se routerat dështimi të cilëve shkakton numrin më të madh të ndryshimeve të rrugës janë routera që lidhin me lidhjet më të rëndësishme të identifikuara në Fig.3.13. Routerat R5, R3, R18, R11 dhe kolegët (peers) R15 me ofruesit komercial dhe në këtë mënyrë marrin rrugët BGP për gati të gjitha prefikset e internetit. Routerat R1 dhe R6 janë më kritike për qasjen në internet të një numri të madh të GEANT NOQ, kryesisht në vendet lindore evropiane.

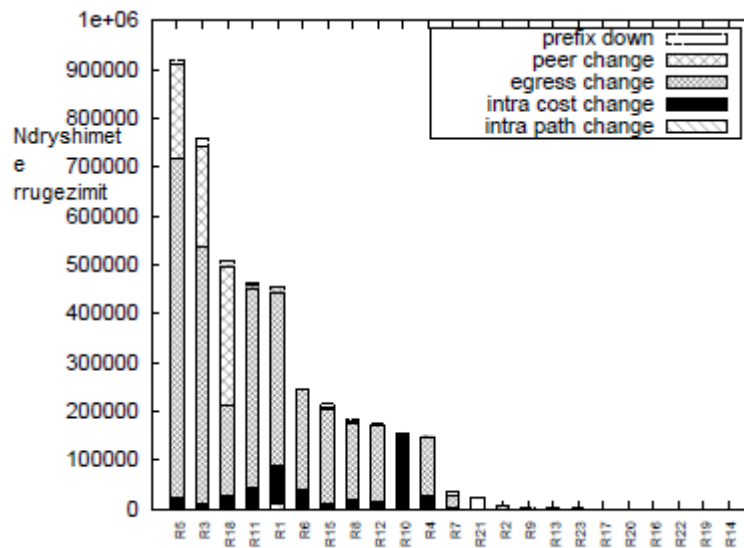


Figura 3.14 : Analiza dështimi e një ruteri të vetëm: ndikimi në BGP.

Gjithashtu mund të vëzhgohet në Fig.3.14 se klasa Prefix poshtë nuk është e zbrazët. Kjo ndodh për prefikset e destinacionit për të cilën një rrugë e vetme eBGP është e njohur në model. Kjo do të thotë se në bazë të modelit tonë, mund të konkludohet se dështimi i disa routerave mund të çojë në pakapshmeri të disa destinacioneve. Në fakt, ky përfundim është pak i nxituar. Një arsye e parë është se nuk dihen të gjithë rrugët e jashtme të pranuar nga routerat GEANT. Vetëm njihen rrugët më të mira të përzgjedhura nga secili router kufitar. Në rrjetin GEANT të vërtetë, rrugët e tjera mund të bëhen të disponueshme kur rruga më e mirë e tanishme është tërhequr, siç thamë në seksionin 3.2.3. Përveç kësaj, edhe në qoftë se një parashtesë nuk është e arritshme më, është e mundur që një prefiks më pak i veçantë është ende. Në këtë rast, destinacioni do të jetë ende i arritshëm.

3.3.6 Ndikimi në trafik

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Përveç se për të studiuar ndikimin e dështimeve në rrugëzim, është vlerësuar rëndësia e lëvizjeve të trafikut të shkaktuara nga dështimet e lidhjeve. Në të vërtetë, kur rrugët ndryshojnë disa rrjedha të trafikut mund të përcillen përgjatë rrugëve të ndryshme intradomain. Kjo do të ndodhë për rrjedhat e trafikut që janë dërguar në një rrugë që është prekur nga dështimi. Ndërrime të trafikut do të ndryshojnë shpërndarjen e trafikut brenda rrjetit dhe ngarkesën e disa lidhjeve. Si pasojë, disa lidhje mund të bëhen edhe më të tejmbushura (congested). Me qëllim vlerësimit e ndërrimeve të trafikut të shkaktuara nga dështimet e lidhjeve, është përdorur një matricë interdomain (parashtesë-prefiksin) trafiku nga GEANT siç përshkruhet në seksionin 3.3.3. Një matricë interdomain trafiku e GEANT është një grup i treshe (router hyrjeje, prefix destinacioni, volumi i trafikut). Çdo trefishtë paraqet vëllimin e trafikut që është marrë nga një router hyrje dhe për t'u dërguar në drejtim të prefiksit të destinacionit gjatë një periudhe të caktuar kohe. Për të llogaritur matricën e trafikut intradomain (router-router), ne zhvillojmë sërish rrjedhën e trafikut nëpër GEANT. Për këtë qëllim, është marrë çdo triplet nga matrica e trafikut interdomain (Parashtesë-prefix), një në një kohë. Pastaj, është kryer një longest-matching në tabelën e rrugëzimit të llogaritur nga solveri I rrugëzimit për routerin e hyrjes të marrë në konsideratë, në mënyrë që të gjeni prefiksën që përmban destinacionin. Pastaj duhet të përdoret rruga e lidhur me këtë prefiks për të rrugëzuar trafikun. Është përsëritur ky hap në një bazë hop-by-hop derisa routeri i daljes të jetë arritur. Matrica e trafikut intradomain është marrë duke mbledhur volumin e trafikut të shkëmbyer mes të gjitha palëve të routerave të hyrjes dhe daljes për periudhën kohore. Është përdorur metodologjia e mësipërme për të llogaritur matricën e trafikut intradomain pas çdo dështimi lidhjeje. Është treguar një nëngrup i rezultateve në Fig. 3.15 dhe Fig.3.16. Këto shifra tregojnë vëllimin e trafikut të kryer nga çdo lidhje, pas një dështimi të një lidhjeje të vetme (Lidhjet R1-R3 dhe R5, R6 janë treguar). Janë dalluar drejtimet e lidhjeve derisa secili drejtim mund të kryejë një volum të ndryshëm të trafikut. Në boshtin x, mund të tregohen të gjithë lidhjet të drejtuara të udhëzuara duke u bazuar në volumin e trafikut që kanë bartur para dështimit. Aksi y tregon sasinë e trafikut të bartur nga linku përkatës. Në çdo figurë, tregohen dy kurba. E para, emërtohet "default", dhe përfaqëson ngarkesën e lidhjeve, kur të gjitha lidhjet janë në ekzekutim. E dyta paraqet lidhjet e ngarkesës pas dështimit të linkut. Në situatën e parazgjedhur të treguar në Fig.3.15, mund të vëzhgohet se ngarkesa e trafikut është e shpërndarë në mënyrë të pabarabartë në lidhjet. Lidhja më e ngarkuar është R5-R6 e ndjekur nga R1-R3. Fig.3.15 tregon ngarkesën lidhjet pas dështimit të lidhjes R1-R3. Është treguar në Fig.3.13 se kjo lidhje ishte më e rëndësishme nga pikëpamja e rrugëzimit. Vërejmë që, siç pritet, trafiku I bartur fillimisht nga linku R1-R3 tani kalon përmes lidhjeve të tjera. Vërejmë gjithashtu se ngarkesa e Lidhjes së mëparshme më të ngarkuar, R5-R6, është pothuajse dyfishuar. Kjo tregon se një pjesë e madhe e trafikut fillimisht kalonte në R1-R3 tani është përcjellë përgjatë rrugëve që kalojnë nëpër R5-R6.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

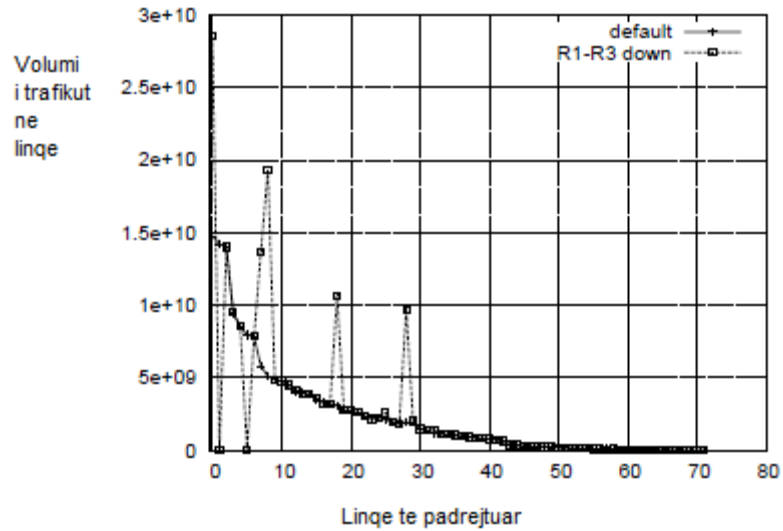


Figura 3.15: Ndikimi i dështimit të R1-R3 mbi ngarkesën e lidhjeve.

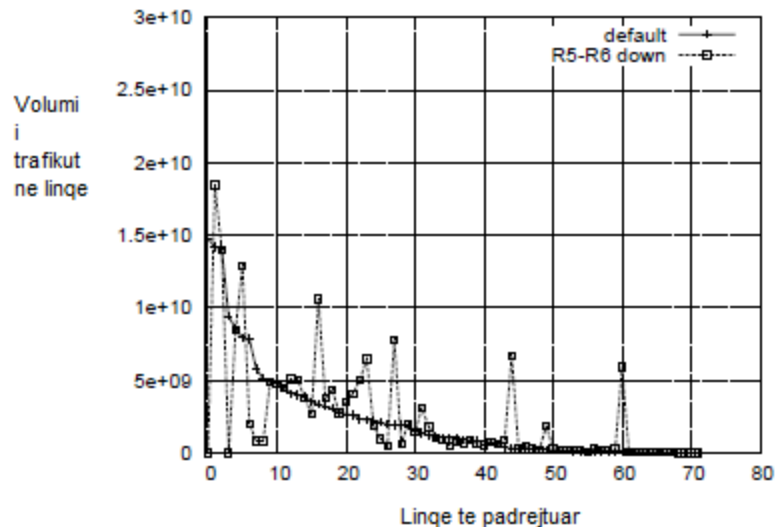


Figura 3.16: Ndikimi i dështimit të R5-R6 mbi ngarkesën e lidhjeve.

Në Fig. 3.16, është treguar ngarkesa e lidhjeve pas dështimit të lidhjes R5-R6. Është vërejtur se ndërrime të trafikut janë më pak të lokalizuara se me dështimin e R1-R3. Më shumë linqe kanë ndryshuar ngarkesën e tyre. Kjo mund të duket e habitshme që Fig. 3.13 tregon se numri i ndryshimeve të rrugëzimit për shkak të dështimit të R5-R6 është më i ulët se sa numri i ndryshimeve të rrugëzimit për shkak të dështimit të R1-R3. Siç shpjegohet në Seksionin 3.5, kjo është për shkak të ndërveprimit kompleks midis IGP, BGP dhe trafikut. Dështimi i R1-R3 dhe dështimi i R5-R6 nuk kanë të njëjtin ndikim në rrugët intradomain të llogaritura nga IGP. Këto rrugë janë përdorur nga routerat e hyrjes për të arritur routerat e daljes. Pastaj, rrugët e hyrje-daljes janë përdorur nga rrugët BGP për të kaluar GEANT. Në varësi të cilës rrugë janë përdorur për të përcjellë sasi të mëdha

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

të trafikut, ndikimi do të ndryshojë. Së fundi, Fig.3.17 tregon një përmbledhje të ndikimit të të gjitha dështimeve të lidhjes të trafikut. Aksi x tregon të gjitha dështimet e Lidhjeve të udhëzuara në bazë të ngarkesës të lidhjes më të ngarkuar. Aksi y ofron statistikën e mëposhtme: mesataren, 5- dhe 95-përqindëshin, si dhe ngarkesën mesatare dhe ngarkesa e lidhjes më të ngarkuar. Së pari, vërejmë se në GEANT, dështimi i një lidhje të vetme mund të shkaktojë një rritje të madhe të ngarkesës të linkut maksimal. Ka gjithashtu edhe një dështim lidhjeje që shkakton ngarkesën e lidhjes maksimale të pothuajse dyfishohet. Së dyti, ne vërejmë se në GEANT, forma e shpërndarjes së ngarkesës të lidhjeve nuk është ndikuar shumë nga dështimet e lidhjeve. Në të vërtetë, mesatarja dhe 5 dhe 95 përqindshi nuk ndryshon shumë.

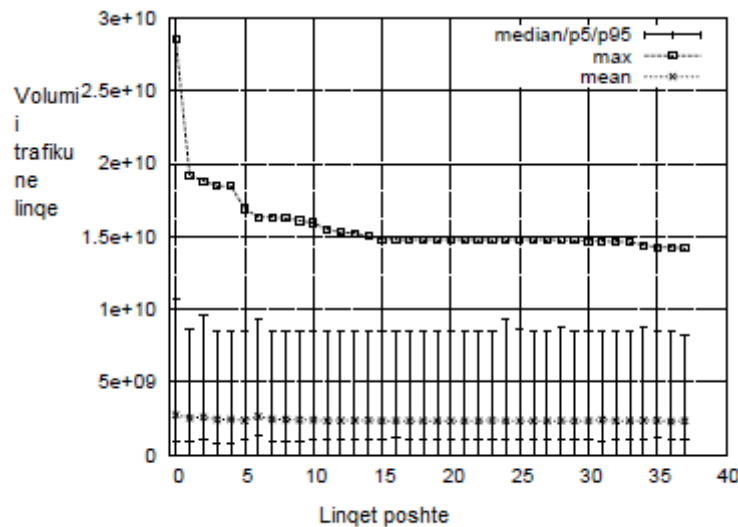


Figura 3.17: Dështimi i një linku të vetëm më të ndjeshëm.

Është treguar në këtë seksion që dështimet e lidhjeve mund të shkaktojnë ndërrime të trafikut të rëndësishme. Për shembull, dështimi i Lidhjes R1-R3 ka dyfishuar ngarkesën e Lidhjes R5-R6. Gjatë analizës të rrjetit GEANT, asnjë ngjeshje (congestion) nuk është provokuar nga dështimet e Lidhjeve. Kjo është për shkak të situatës së veçantë të GEANT që është i përbërë nga lidhjet që kanë një kapacitet shumë të lartë në krahasim me volumin e trafikut që ata zakonisht mbajnë. Megjithatë, në rrjete të tjera, kjo analizë mund të ndihmojë për të përcaktuar se cilat lidhjet janë të rëndësishme për trafikun. Është treguar se ndërvarësia mes rrugëzimit intra dhe interdomain e kombinuar me shpërndarjen e trafikut është e vështirë të kuptuar në një rrjet tranzit me madhësi të mesme. Një metodologji si ajo e përdorur në këtë kapitull mund të ndihmojë operatorët për të vlerësuar synimet e tyre apo për të vlerësuar se si rrjeti i tyre do të silllet kur të ndryshojnë kushtet e trafikut dhe / ose të rrugëzimit.

3.4 Teknika TE Interdomain aktuale

Fillimisht i zhvilluar si një rrjet kërkimor, interneti është optimizuar për të ofruar një shërbim ku rrjeti bën më të mirë e tij për të ofruar paketa në destinacionin e tyre. Në internetin kërkimor, lidhja ishte çështja më e rëndësishme. Gjatë viteve të fundit, interneti ka pësuar një rritje të shpejtë dhe është përdorur gjithnjë e më shumë për të kryer shërbime të tilla si e-commerce, Virtual Private Networks ose Voice / Video mbi IP.

Për të mbështetur me efikasitet ato shërbime, disa Internet Service Providers (ISP) mbështeten në Traffic Engineering (TE) (ACE + 02) për të kontrolluar më mirë rrjedhën e paketave brenda rrjetit të tyre. Inxhinieria e trafikut përfshin disa teknika që operatorët ISP mund të përdorin për të vlerësuar dhe përmirësuar punën e rrjetit të tyre. Objektivat e zakonshme të inxhinierisë së trafikut përbëhen nga zhvendosja e trafikut larg nga linqet e bllokuara (congested), shpërndarja e trafikut brenda rrjetit, në mënyrë për të rritur sasinë e trafikut që mund të kryhet nga rrjeti, duke reaguar me shpejtësi ndaj dështimeve duke drejtuar trafikun larg nga lidhjet e gabuara ose me efikasitet mbështesin Kërkesat e Cilësisë së Shërbimit (QoS).

Ndërsa inxhinieria e trafikut intradomain është një problem i kuptuar mirë, kryerja e inxhinierisë së trafikut në të gjithë kufijtë e fusha të shumta është komplekse. Ky kompleksitet është kryesisht për shkak të arkitekturës të rrugëzimit të Internetit aktual. BGP propagandon vetëm një nëngrup të topologjisë së internetit mes routerave. Kjo e kufizon dukshmërinë që një AS ka në topologjinë e internetit. Përveç kësaj, BGP nuk optimizon një objektiv global, por lejon çdo AS të pavarur të zgjedhë dhe rishpërndajë rrugët interdomain në mënyrë që të plotësojë objektivat e veta lokale. Kontrollimi i përzgjedhjes së rrugëve interdomain me BGP, në mënyrë për të mbështetur procesin e inxhinierisë së trafikut interdomain është i vështirë meqë BGP nuk është projektuar për këtë qëllim. Gjithsesi, disa mekanizma të kontrollit të rrugëzimit me bazë BGP primitive përdoren aktualisht nga AS-set. Këto mekanizma mbështeten në akordimin etributeve të rrugëve BGP. Në këtë kapitull, janë studiuar mekanizmat e kontrollit të rrugëzimit të bazuar në BGP të përdorura nga AS-set në ditët e sotme dhe është përshkruar funksionimi i tyre.

3.4.1 Intradomain Engineering Traffic (ITE)

Brenda një ISP të vetme (ose domain), e tërë topologjia e rrjetit është e njohur nga të gjithë routerat për shkak të përdorimit të protokolleve të rrugëzimit lidhje - gjendje. Për më tepër, protokollin e rrugëzimit intradomain zakonisht optimizon një objektiv të vetëm global. Prandaj, mund të përdoren disa teknika për të kontrolluar rrjedhën e paketave IP. Ato mund të ndahet në dy klasa. Klasa e parë përmban teknikat e përdorshme në rrjetat e pastra IP, dmth që merren me shpërndarjen në destinacion të bazuar në hop-by-hop. Klasa e dytë përmban teknikat që mund të përdoren në rrjetet me komutim qarku. Në veçanti, janë diskutuar teknikat duke u mbështetur në rivalitetin e rrjetave me komutim qarku në krye të rrjetave me komutim paketë, të tilla si me Multi-Protocol Label Switching (MPLS) (BZB+97, DR00).

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

3.4.2 Zgjidhje të bazuara në IP

Në një rrjet të pastër IP, rrjedha e paketave IP mund të kontrollohet nga akordimi i protokollit të rrugëzimit intradomain (i quajtur edhe Interior Gateway Protocol - IGP). Brenda një domaini, protokollin e rrugëzimit do të llogarisë rrugën më të mirë për të arritur çdo destinacion. Rruga më e mirë është zakonisht rruga me koston më të vogël, ku kostoja e një rruge është shuma e peshave të të gjitha hallkave që përbëjnë rrugën. Kostoja e lidhur me çdo lidhje është zakonisht e caktuar administrative nga operatorët e rrjetit në varësi me objektivin e tyre të optimizimit. Në qoftë se çdo lidhje ka një kosto unitare, atëherë protokollin e rrugëzimit do të favorizojë shtigjet me numrin më të vogël të hops (kapërcimeve). Nëse kostoja e çdo lidhjeje është një funksion i vonësës së transmetimit të linqeve, atëherë rrugëzimit protokollin do të zgjedhë rrugët me vonësë më të shkurtër. Nëse kostoja e lidhur me një lidhje është një funksion i bandwidth-it të lidhjeje, atëherë protokollin e rrugëzimit do të favorizojë shtigjet me bandwidth të lartë.

Për shembull, në figurën 8.1, nëse të gjitha lidhjet kanë një kosto unitare, rruga më e shkurtër nga burimi S1 në një destinacion D1 është rruga (S1, R8, R6, R5, D1) që ka një kosto totale prej 4. Rruga e përdorur në mes të burimit S2 dhe destinacion D2 është (S2, R1, R8, R6, R5, D2). Nëse ka një shumë të trafikut nga S1 për D1 dhe nga S2 për D2, atëherë lidhjet R8 - R6 dhe R6 - R5 mund të bëhen pengesë që këto dy lidhje janë përdorur nga të dy flukset. Një metodë e zakonshme për të përcjellë trafikun larg nga lidhjet e tejmbushura (congested) është duke akorduar koston e lidhjeve kryesore [FRT02]. Në shembullin e sipërm (figura 4.1) është e mundur të detyrohet rrjedhja e trafikut S2 - D2 (. resp S1 - D1) për të ndjekur rrugën R1 - R2 - R3 - R4 - (. resp R8 - R9 - R7 - R5) R5 duke përdorur një kosto prej 2 në vend të 1 në lidhjet R1 - R8 dhe R9 R6 - dhe 3 në vend të 1 në linkun R8 - R6. Në fakt, në qoftë se kërkesa e trafikut në mes të çdo palë burim-destinacioni në rrjet është e njohur, vendosja e shpenzimeve të lidhjeve mund të konvertohet në një problem optimizimi (FT00) që mund të zgjidhet duke përdorur metodat të përshtatshme matematikore. Megjithatë, këto metoda janë të dobishme vetëm në praktikë, nëse kërkesa e trafikut është relativisht e qëndrueshme. Nëse kërkesa e trafikut ndryshon shpesh, do të jetë e vështirë për të rillozuar dinamikisht vendosjen optimale të kostove të lidhjeve dhe për të rikonfiguruar dinamikisht të gjitha ruterat pa ndikuar në trafikun aktual brenda rrjetit. Optimizimi i fuqishëm i peshave IGP (FT03) është një zgjidhje e mundshme.

3.4.3 Teknikat e bazuara në MPLS

MPLS është përdorur shpesh për qëllime inxhinierike trafiku brenda rrjeteve ISP. MPLS mbështetet në teknikat e komutimit të etiketave (label switching technique) si në ATM apo rrjetet Relay Frame. Avantazhi kryesor i MPLS për inxhinierinë e trafikut, në krahasim me rrugëzimin klasik IP, është se MPLS mund të përdoret për të përcaktuar në mënyrë të qartë rrugën e ndjekur nga paketat brenda domainit. MPLS kështu lehtësisht mund të anashkalojë rrugën më të shkurtër të përzgjedhur nga rrugëzimi IP. Kjo është bërë duke vendosur Label Switched Paths (LSPs) mes çifteve të routerave në rrjet. Një

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

ofMPLS para shfrytëzimit është për të zgjidhur problemin e trafikut inxhinierik statistikisht. Bazuar në një kërkesë të njohur të trafikut ndërmjet të gjithë çifteve burim-destinacion, është e mundur për të llogaritur një plan urbanistik optimal të LSPs në rrjet, në mënyrë që të përhapet ngarkesa midis të gjitha lidhjeve në dispozicion. Ky shfrytëzim është i ngjashëm me vendosjen e shpenzimeve të lidhjeve në një rrjet IP të pastër edhe pse MPLS ofron një fleksibilitet më të madh. Me vetëm kostot e lidhjeve, një ndryshim në koston e një lidhjeje mund të ndikojë potencialisht në trafikun e shpërndarjes në të gjithë rrjetin. Me MPLS, është e mundur për të detyruar çdo rrjedhë paketash të ndjekë një rrugë të veçantë. Për shembull, do të ishte e mundur të detyronte paketat nga rrjedha -S1 D1 për të ndjekur rrugët R8 - R1 - R2 R3 - -R4 - R6 - R5 ndërsa paketat nga rrjedha S2 - D2 do të ndiqnin rrugët R1 -R8 -R9 -R7 -R5 në figurën 3.1. Ky lloj i shpërndarjes së trafikut nuk do të jetë i mundur duke zgjedhur shpenzimet e lidhjeve në një rrjet IP të pastër.

MPLS është gjithashtu e dobishme në një mjedis më dinamik ku kërkesat e trafikut ndryshojnë ngadalë (psh kërkesa gjatë orarit të punës nuk është e njëjtë si gjatë mbrëmjes). Në këtë rast, MPLS është përdorur në kombinim me protokollin e rrugëzimit intradomain të zgjeruara (OSPF-TE (KKY03) ose ISIS-TE (SL04)). Këto protokolle janë zgjerime të protokolleve klasike intradomain lidhje-gjendje (OSPF dhe ISIS) që janë në gjendje për tu shpërndarë të gjitha routerave së bashku me të gjithë topologjitë e informacionit të rrjetit shtesë si bandwidth dhe shfrytëzimin e secilës lidhjeje. Bazuar në këtë informacion, secili router mund të përcaktojë lidhjet brenda rrjetit më të ngarkuar rëndë. Për të kuptuar përdorimin e MPLS, le të shqyrtojmë figurën 3.1 përsëri dhe të supozojmë se ka dy flukse të rëndësishme të paketave (S1 -D1 dhe S2 - D2) dhe që lidhjet R8 - R6 dhe R6 - R5 janë duke u bërë të tejmbushura, ndërsa lidhjet e tjera janë shfrytëzuar lehtësisht. Bazuar në informacionin e shpërndarë nga protokollin e rrugëzimit të kufizuar, routerat R1 dhe R8 janë të vetëdijshëm për ngarkesën në këto linqe. Nëse këto rutera vërejnë flukse të mëdha nga S2 dhe S1, ata mund të përcjellin ato rrjedha nëpër lidhje të tjera duke krijuar LSPs të reja. Për të vendosur një LSP të tillë, R1 do të specifikojë një grup kufizimesh për LMS e re ndaj D2. Për të zgjedhur rrugën më të mirë, routeri R1 do të përcaktojë një sërë pengesa që duhet të plotësohen nga rruga e zgjedhur. Për shembull, R1 mund të kërkojë një rrugë që shmang lidhjet e ngarkuara (R8 - R6 dhe R6 - R5). Nëse R1 di se rrjedha S2 - D2 kërkon 100 Mbps mesatarisht, ai gjithashtu mund të zgjidhë një rrugë ku të gjitha lidhjet të kenë të paktën 100 Mbps bandwidth të papërdorur. Rruga e zgjedhur e kufizuar do të përdoret nga ana e protokollit të sinjalizimit RSVP-TE [ABG + 01] që do të krijojë LSP. Ky protokoll sinjalizimi gjithashtu mund të përdoret për të rezervuar burimet (p.sh. Bandwidth) në rrugën e zgjedhur nëse kërkohet. Një përparësi tjetër e MPLS është se është e mundur për të rirrugëzuar një LSP ekzistuese mbi një tjetër rrugë (psh më pak i mbushur plot) para këputjes së LSP ekzistuese.

3.4.4 Interdomain Engineering Traffic

Një pjesë e madhe e trafikut të internetit nuk do të mbetet brenda një domaini të vetëm, por ndërkohë do të kalojë kufijtë e tij interdomain. Burimi dhe destinacioni i këtij trafiku

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

interdomain mund të jetë edhe disa domaine larg. Kjo e bën inxhinierinë e trafikut interdomain një çështje të rëndësishme për ISP-të. Kërkesat e inxhinierisë së trafikut interdomain janë të ndryshme. Ato varen në lidhjet e një AS me të tjerët (shih kapitullin 1), por edhe në llojin e bizneseve që trajtohen nga ky AS. Në mënyrë tipike, ofruesit e përmbajtjes (content-providers) që presin shumë web ose serverat streaming dhe zakonisht kanë disa marrëdhënie të konsumatorëve-ofrues(customer-to-provider) me AS-ët tranzit do të përpiqen të optimizojnë rrugën që trafiku lë rrjetet e tyre. Së dyti, ofruesit e aksesit (access-providers) që u shërbejnë ndërmarrjeve të vogla dhe të mesme, përdoruesit e dial-up ose xDSL zakonisht dëshirojnë të optimizojnë se si trafiku i Internetit hyn në rrjetet e tyre. Së fundi, një AS tranzit do të përpiqet për të balancuar trafikun në lidhjet e shumta që ka me shokët e vet. Prandaj, objektivi kryesor i inxhinierisë së trafikut interdomain është për të kontrolluar përmes cilit rrjedhat e trafikut të linqeve peering do të hyjnë ose dalin nga rrjeti. Kjo mund të jetë me qëllim të balancimit të trafikut në lidhjet e shumta me AS-et e tjera, për të zhvendosur trafikun larg nga një lidhje e mbushur plot (congested) peering apo për të lëvizur një pjesë të trafikut në lidhje peering më paktë shtrenjta. Një tjetër kërkesë e inxhinierisë së trafikut interdomain është aftësia për të drejtuar trafikun drejt rrugëve alternative interdomain me veti të ndryshme. Një shembull do të jetë për të zgjedhur një rrugë më të mirë me performancë fund-më-fund (end-to-end) (latency të ulët ose me bandwidth të lartë në dispozicion), madje edhe në kosto më të lartë. Një tjetër qëllim do të jetë siguri i një rrugë backup plotësisht të shkëputur nga ai kryesor.

3.4.5 Kufizimet e arkitekturës së rrugëzimit të Internetit të tanishëm

Për fat të keq, duke arritur këto objektiva me arkitekturën e rrugëzimit të Internetit aktual është e vështirë. Ka dy çështje kryesore.

Së pari, natyra vektor - rrugë e BGP imponon kufizime në zgjedhjen e rrugëve interdomain. Çdo router BGP rishpërndan vetëm një rrugë të vetme "më të mirë" për fqinjët e saj. Edhe nëse routeri di shumë rrugë kandidate, rrugët alternative nuk janë të përhapura. Kjo e kufizon dukshmërinë e secilit router që ka mbi topologjinë e internetit dhe redukton diversitetin e rrugëve. Kjo është në kontrast me protokollet e rrugëzimit intradomain (Lidhje-gjendje) që shpërndajnë topologji të plotë për të gjithë routerat pjesëmarrës. Implikimi për inxhinierinë e trafikut është një liri e kufizuar për drejtimin e trafikut të rrugëve alternative. Përveç kësaj, nuk është e natyrshme pak kontroll në vendimet e rrugëzimit, meqë rrugët që një router pranon varen nga vendimet e tjera të drejtimit të rrymës të routerave.

Së dyti, BGP mbështetet në një proces kompleks vendimmarrjeje i cili nuk zgjedh një metrikë globale. Kjo është në kontrast me zgjedhjen e rrugëve me kosto më të paktë nga protokollet e rrugëzimit intradomain. Në vend të kësaj, operatorët e çdo AS mund të konfigurojnë në mënyrë të pavarur routerat e tyre në mënyrë që të optimizojnë objektivat lokale dhe për të zbatuar politikën e filtrimit të rrugëzimit lokale. Për shembull, çdo AS mund të konfigurojë një renditje lokale të rrugëve drejt një destinacioni të caktuar duke

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

përdorur atributin Lokale-pref. Implikimi për inxhinierimin e trafikut është se konfigurimi i një AS mund të anulohet përpjekjet e kontrollit të rrugëve të një tjetër AS-je.

3.4.6 Karakteristikat e trafikut interdomain

Një vështirësi tjetër e inxhinierisë së trafikut interdomain vjen nga një numër i madh i burimeve dhe destinacioneve të përfshirë. Në nivelin intradomain, numri i destinacioneve të shpallur nga protokollin IGP është i kufizuar në routera dhe subnet-e të domain-ve. Në varësi të madhësisë së fushës, rendi i saj i madhësisë së magnitudës varion nga dhjetëra në mijëra të destinacioneve. Në nivelin interdomain, numri i burimeve dhe destinacioneve përfshin rrjete të reklamuar në distancë. Ky numër është shumë më i madh. Për shembull, numri aktual i prefikseve të destinacionit në një tabelë rrugëzimi BGP është në rendin e 180,000 (Hus06).

Në pamje të parë vihet në dukje megjithatë është se edhe pse një AS mund të shkëmbejë trafik me një pjesë të madhe të fushave (domaineve) të internetit, nuk do të shkëmbejë të njëjtën sasi trafikut me secilin AS të largët. Në Fig.3.18, është treguar shpërndarja kumulative e trafikut interdomain të marrë ose dërguar nga tre ISP-ë. Figura ka të bëjë me trafikun e marrë nga BELNET, rrjeti belg i Kërkimeve Kombëtare dhe Arsimit (Belgian National Research and Education Network)(NREN) gjatë një javë të tërë në dhjetor 2000; trafiku i marrë nga YUCOM, një ISP belg, gjatë 5 ditëve të njëpasnjëshme në prill të vitit 2001; dhe trafiku i dërguar nga Super-Computing Center Pitsburg të (PSC) gjatë një dite në mars 2002. Më shumë detaje mbi të dhënat e mbledhura mund të gjenden në (UB02). Vihen re se 100 burimet më të mëdha të trafikut për BELNET kontribuojnë më shumë se 64% të Trafiku ka marrë gjatë një jave. Në mënyrë të ngjashme, 100 burimet më të mëdha të trafikut për YUCOM kontribuojnë më shumë se 72% e trafikut të marrë nga ky ISP. Për KDP, përqendrimi i trafikut është edhe më i rëndësishëm meqë 100 destinacionet më të mëdha marrin 78% të trafikut të përgjithshëm të dërguar nga KDP. (FBR03) përmend një shpërndarje të ngjashme për trafikun interdomain e një pjesë të madhe shtresore-1 ISP (*tier-1* ISP).

Një tjetër pikë e rëndësishme që përmendet në lidhje me trafiku interdomain e shkëmbyer nga ISP-të e studiuara është distanca (matur në SI HOPS) midis AS-ët e largët dhe çdo ISP i studiuar. Fig.3.18 tregon, për çdo ISP, përqindjen e interdomain-it të trafikut të saj që është prodhuar nga ose dërguar drejt një AS të largët si një funksion i distancës së tyre të matur në AS-HOPS. Kjo analizë tregon se ISP-të studiuara vetëm shkëmbejnë një pjesë të vogël të trafikut të tyre me kolegët e tyre të drejtpërdrejtë (AS-hop në distancë në 1). Shumica e paketave shkëmbehen me AS që janë vetëm disa AS HOPS larg. Për BELNET, shumica e trafikut është prodhuar nga burime të vendosura 3 dhe 4 AS HOPS larg ndërsa YUCOM merr trafikun nga burime që janë 2 dhe 3 AS HOPS larg. PSC në anën tjetër dërgon trafikun në AS të vendosur në deri në 4 AS HOPS larg. Kjo nënkupton se një AS i gatshëm për inxhinierim të trafikut të saj interdomain mund të lëvizë një sasi të madhe të trafikut duke ndikuar vetëm një numër të vogël AS-sh të largët, në mënyrë tipike, burimet më të popullarizuara / destinacionet. Përveç kësaj, që burimet dhe / ose destinacionet e trafikut interdomain janë të vendosura vetëm AS pak HOPS larg,

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

zgjidhjet inxhinierike të trafikut interdomain duhet të jenë në gjendje të ndikojnë në AS pak hapa (hops) larg përtej ofruesve të tyre në rrjedhën e sipërme apo peer-ve direkte.

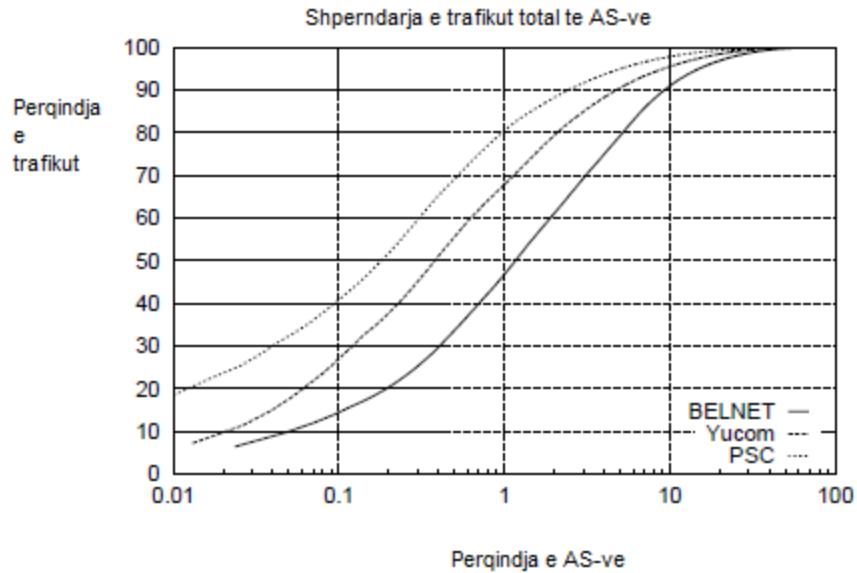


Figura 3.18-a : Shpërndarja kumulative e trafikut për secilin ISP të studiuar.

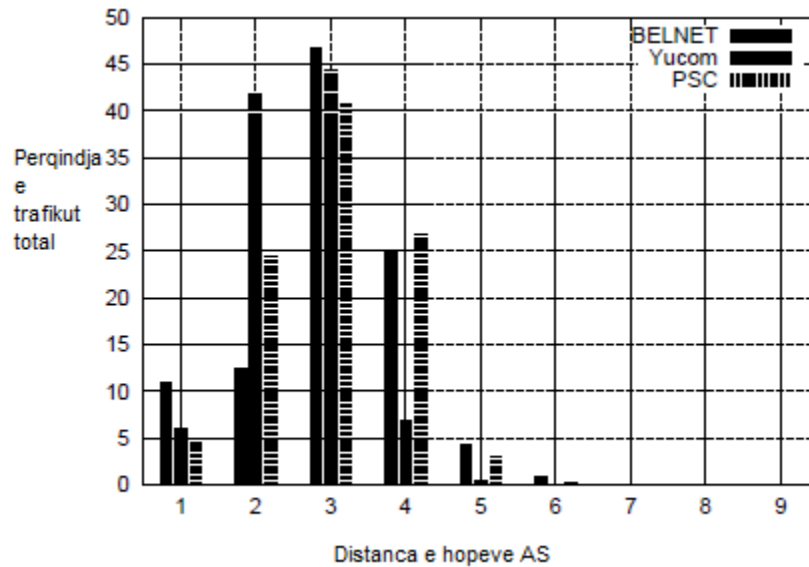


Figura 3.18-b: Shpërndarja Per-AS hop e trafikut për secilin ISP të studiuar.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

3.4.7 Inxhinierimi i trafikur i bazuar në BGP

Optimizimi i mënyrës që trafiku hyn ose del nga një rrjet do të thotë që të favorizojë një lidhje kundrejt një tjetre për të arritur një destinacion të caktuar apo për të marrë trafikun nga një burim i caktuar. Ky lloj i inxhinierisë së trafikut interdomain mund të kryhet nga heqja e konfigurimit nga routerat BGP të AS. Në të vërtetë, një tipar kryesor i BGP është procesi i vendimmarrjes i përdorur nga çdo router BGP për të zgjedhur, në mesin e të gjithë reklamave të pranuar, rruga më e mirë për të arritur çdo destinacion. Për të kuptuar se si BGP mund të përdoret për të kontrolluar rrugën e trafikut që hyn, largohet apo kalon një AS, është e nevojshme një kuptim më i mirë i procesit të vendimmarrjes së BGP. Është përsëritur procesi i vendimmarrjes BGP në Tabelën.1. Një router BGP merr një rrugë drejt çdo destinacioni nga secili prej peers-ave të saj. Për të zgjedhur rrugën më të mirë në mesin e këtij grupi të rrugëve, një router BGP mbështetet në një sërë rregullash të quajtura procesi i vendimmarrjes. Shumica e routerave BGP zbatojnë një proces vendimmarrjeje të ngjashëm në parim me atë të treguar në figurë. Tërësia e rrugëve me të njëjtin destinacion analizohen nga rregullat në rend të treguara në figurë. Këto rregulla do të veprojnë si filtra dhe rregulli N-të vlerësohet vetëm nëse më shumë se një rrugë ka kaluar rregullin e N - 1. Duhet të theksohet se shumica e implementimeve të BGP lejojnë administratorin e rrjetit të çaktivizojë opsionalisht disa nga rregullat e procesit të vendimmarrjes së BGP.

Tabela .1 : Procesi i vendimmarrjes BGP

Rank	Rule
1	Prefer highest Local-Pref
2	Prefer shortest AS-Path
Tie-breaking rules	
3	Prefer lowest Origin
4	Prefer lowest MED
5	Prefer eBGP over iBGP
6	Prefer nearest next-hop
7	Prefer lowest router-ID or oldest route

Atributet e para të përdorura për të krahasuar rrugët janë Lokale - pref dhe AS- Path (Fig.4.1). Në hartimin fillestar të procesit të vendimmarrjes BGP (RL95), qëllimi i atributit Lokale – pref ishte për të lënë operatorin e rrjetit të zgjedhin rrugën më të dëshirueshme, ndërsa AS - Path ka luajtur rolin e një metrikë rruge. Rregullat e mbetura janë përdorur kryesisht për të thyer lidhjet kur atributet e mësipërme ku janë jo të mjaftueshme për të zgjedhur një rrugë të vetme të mirë. Sot, shumë attribute përdoren për të ndikuar në vendimin e procesit të vendimmarrjes (QUP + 03 , CR05). Mekanizma të

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

ndryshëm mund të përdoren për të kontrolluar trafikun në dalje dhe trafikun hyrës në një AS. Në paragrafët në vijim, janë përshkruar teknikat inxhinierike të trafikut që mbështeten në manipulimin e attributeve BGP në mënyrë që të ndikojnë në rezultatin e procesit të vendimmarrjes BGP .

3.4.8 Kontrolli i trafikut dalës

Për të kontrolluar se si trafiku lë rrjetin e tij një AS duhet të jetë në gjendje të zgjedhë se cilat rrugë do të përdoren për të arritur një destinacion të veçantë me shokët (peers) e vet. Meqë një AS kontrollon procesin e vendimmarrjes në routerat e saj BGP, ajo lehtësisht mund të ndikojë në zgjedhjen e rrugës më të mirë. Dy teknika janë përdorur shpesh. Një teknikë e parë është që të preferojmë disa rrugë mbi të tjerat duke vendosur atributin Lokale-pref. Një shfrytëzimi i përbashkët i këtij atributi është që të preferohen rrugët e mësuara nga konsumatorët mbi rrugët e mësuara nga ofruesit (GR00). Atributi Lokale-pref është opsional dhe është i shpërndarë vetëm brenda një AS. Ai mund të përdoret për të rangëzuar rrugët dhe është rregull i parë i procesit të vendimmarrjes BGP. Për shembull, e konsiderojmë një faqe stub AS me dy lidhje drejt një ofruesi në upstream: një Lidhje Bandwidth të lartë dhe një Lidhje të ulët Bandwidth. Në këtë rast, routeri BGP i këtij AS mund të konfigurohet për të të futur një Lokal-pref të ulët për rrugët e mësuara nëpërmjet linkut të ulët Bandwidth dhe një vlerë më të lartë të rrugëve të mësuara nëpërmjet linkut të lartë Bandwidth. Një situatë e ngjashme mund të ndodhë për një faqe stub AS të lidhur me një ofrues të lirë dhe një më të shtrenjtë në rrjedhën e sipërme(upstream). Përdorimi i atributit Lokale-pref me qëllim të kontrollit të trafikut në largim i një ISP është studiuar në (UBQ03a).

Në praktikë manipulimi i atributit Lokale - pref mund të bazohet në matjet pasive ose aktive. Kohët e fundit, disa kompani kanë zbatuar zgjidhje (Bor02 , All02) që lejojnë multi- homed stub ASs dhe përmbajtje ofruesit (content-providers)për inxhinierimin e trafikut të tyre interdomain. Këto zgjidhje zakonisht masin ngarkesën në çdo lidhje interdomain dhe disa mbështeten në matjet aktive për të vlerësuar performancën e shtigjeve interdomain. Në bazë të këtyre matjeve dhe disa njohurive të topologjisë së internetit (ose marrë nëpërmjet një serveri qendror ose nga routeri BGP në të cilat ato janë bashkëngjitur) ata bashkëngjisin vlerat e përshtatshme të attributeve Lokal - PREF për të treguar cila rrugë duhet të konsiderohet si rruga më e mirë nga routerat BGP . Disa shitësa router- ash gjithashtu ofrojnë këtë lloj të zgjedhjes automatike nga outbound direkt në routera. Për shembull, CISCO propozon Routimin e tij Optimized Edge (RHA) (Sys05c).

Një teknikë e dytë, e përdorur shpesh nga ISP-ve të mëdha të tranzitit, është të mbështetet në protokollin e rrugëzimit intradomain për të ndikuar si një paketë kalon ISP-në tranzit . Siç tregohet në figurë, procesi i vendimmarrjes BGP do të zgjedhë fqinjin më të afërt IGP kur krahason disa rrugë ekuivalente të marra nëpërmjet iBGP. Për shembull, merret në konsideratë në figurën 3.19 që routeri R27 merr një paketë destinacioni i të cilit është R45. BGP Prosesi i vendimmarrjes të routerit R27 do të krahasojë dy rrugët drejt R45,

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

një të marrë përmes R28 dhe tjetra e marrë nëpërmjet R26 . Duke zgjedhur routerat R28 si router në kufirin e daljes për këtë paketë, AS2 do të sigurojë që kjo paketë do të konsumojnë sa më pak burime që të jetë e mundur brenda rrjetit të vet. Nëse një AS transit mbështetet në një akordim të peshave të protokollit të rrugëzimit të saj intradomain siç është përshkruar në (FRT02), ky akordim në mënyrë indirekte do të ndikojë në trafikun e tij dalës (TSGR04 , ANB05).

Përveç kësaj, ekzistojnë teknika të veçanta shitësish. Routerat CISCO për shembull lejojnë që të caktohet një atribut shtesë të quajtur peshë në rrugët BGP . Ky atribut mund të vendoset në një bazë për - router. Rruga me vlerën më të lartë të Peshës është preferuar nga procesi i vendimmarrjes. Atributi i peshës është marrë në konsideratë para atributit Lokale - pref. Megjithatë, në të kundërtën e atribut Lokale - pref, ai nuk është fuq mbi seksionet iBGP. Vlera e atributit të Peshës mund të vendoset bazuar në përmbajtjen e AS - Path, në bazë të autorit të rrugës dhe kështu me radhë. Vendosija mund të bëhet automatikisht bazuar në filtrat e rrugëzimit input.

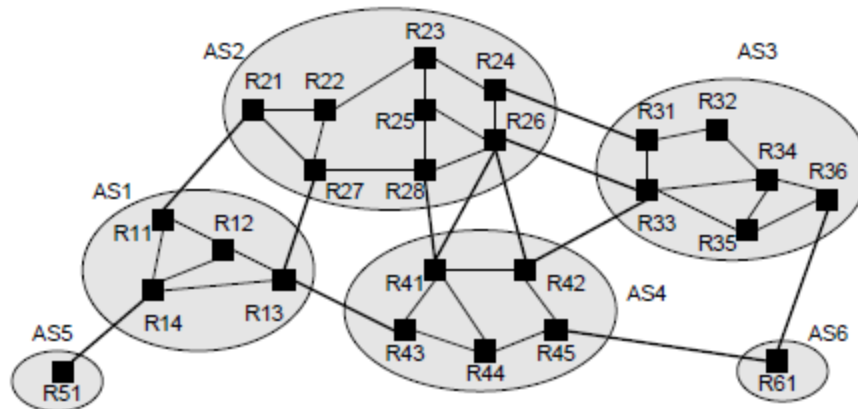


Figura 3.19: Një Internet I thjeshtë

3.4.9 Kontrolli i trafikut në hyrje

Nëse një ISP ka nevojë për të kontrolluar trafikun në drejtimin e kundërt, dmth hyrjen në rrjetin e tij, situata është shumë më komplekse. Në të vërtetë, kjo nuk është e mjaftueshme për ISP për të kontrolluar procesin e vendimmarrjes në routerat e veta. Ai ka nevojë për të ndikuar në vendimet e bëra nga routerat në fusha të tjera. Një shembull tipik ku është e nevojshme kontrolli i tillë është një ofrues aksesi i cili zakonisht ka më shumë trafik përbrenda se jashtë (outbound). Janë përshkruar në paragrafët e mëposhtëm disa teknika të bazuara në BGP për kontrollin e trafikut në hyrje.

Metoda e parë që mund të përdoret për të kontrolluar trafikun që hyn në një AS është të mbështetet në lajmërimet selektive dhe reklamojë njoftimet e ndryshme të rrugëzimit në lidhjet e ndryshme për shembull në figurën 3.19, nëse AS1 ka kërkuar për të balancuar trafikun që vjen nga AS2 mbi lidhjet R11 - R21 dhe R13 - R27, atëherë ajo mund të shpallë vetëm rrugët e brendshme në lidhjet R11 - R21 dhe vetëm rrugët e mësuara nga

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

AS5 mbi linkun R13 - R27. Meqë AS2 do të mësojë vetëm rreth AS5 përmes routerit R27, ai do të jetë i detyruar ti dërgojë paketa destinacioni të cilit i takon AS5 me anë të routerit R27. Megjithatë, një pengesë e kësaj zgjidhjeje është se në qoftë se lidhja R13 - R27 dështon, atëherë AS2 nuk do të jetë në gjendje për të arritur AS5 përmes AS1. Kjo nuk është e dëshirueshme dhe duhet të jetë e mundur për të shfrytëzuar lidhjet R11 - R21 për paketa ndaj AS5 në atë kohë pa qenë të detyruar për të ndryshuar rrugët që janë të reklamuar në këtë link.

Një variant i njoftimeve selektive është shpallja e prefikseve më specifike (e njohur edhe si ndarja e prefikseve). Ky lloj reklamimi mbështetet mbi faktin që një router IP gjithmonë do të zgjedhë në tabelën e tij të shpërndarjes rrugën më specifike për çdo paketë (dmth rruga me prefiksin përputhës më të gjatë). Për shembull, në qoftë se një tabelë shpërndarjeje përmban sëbashku një rrugë drejt 16.0.0.0/8 dhe një rrugë drejt 16.1.2.0/24, atëherë një paketë destinacioni i të cilit është 16.1.2.200 do të përcillet përgjatë rrugës së dytë. Ky fakt mund të përdoret gjithashtu për të kontrolluar trafikun në hyrje. Në shembullin e mëposhtëm, ne supozojmë se prefiksi 16.0.0.0/8 i takon AS3 dhe se disa servera të rëndësishme janë pjesë e subnet-it 16.1.2.0/24. Nëse AS3 preferon për të marrë paketa drejt serverave të saj në lidhjen R24-R31, atëherë ajo do të reklamojë si 16.0.0.0/8 dhe 16.1.2.0/24 në këtë link dhe vetëm 16.0.0.0/8 në lidhjet e saj të tjera të jashtme. Një përparësi e kësaj zgjidhjeje është se në qoftë se lidhja R24-R31 dështon, atëherë subneti 16.1.2.0/24 do të jetë ende i arritshëm nëpërmjet lidhjeve të tjera.

Një tjetër metodë është të lejojë një AS të tregojë një renditje mes reklamave të rrugëve të ndryshme që dërgon. Teknika e quajtur 'AS-Path prepending' shfrytëzon faktin se procesi i vendimmarrjes BGP përdor gjatësinë e AS-Path për të vlerësuar cilësinë e një rruge. Një mënyrë të natyrshme për të ndikuar në zgjedhjen e një routei fqinj është për të rritur artificialisht gjatësinë e AS-Path të disa rrugëve të caktuara për t'i bërë ato më pak të preferuara. Shumë operatorë rrjeti përdorin AS-Path prepending në një linjë rezervë për shembull, ose të devijojnë trafikun nga disa fqinjë pa humbur lidhjen. Duke u kthyer në figurën 3.19, supozohet se interdomain primare AS3-së është lidhja R61-R45 ndërsa Lidhja R61-R36 është përdorur vetëm si lidhje rezervë primare. Në këtë rast, AS6 do të njoftojë rrugët e saj normalisht në lidhjen primare (dmth me AS-rruga e AS6), por do të shtojë numrin AS të saj disa herë në vend të një here në atributin AS-Path (p.sh. AS6 AS6 AS6) në lidhjen R61 - R36. Rruga e reklamuar në linkun primar do të konsiderohet si rruga më e mirë nga të gjitha routerat që nuk mbështeten në parametrat e konfiguruar manualisht për atributet e Peshës dhe Localpref. Kjo teknikë mund të kombinohet me shpallje selektive.

Për shembull, një AS mund të ndajë hapësirën e adresave në dy parashitesat p1 dhe p2 dhe reklamojë prefiksin p1 pa prepending dhe prefiksin p2 me prepending në lidhjen e saj të parë dhe e kundërta në lidhjen e saj të dytë.

Metoda e fundit për të lejuar një AS të kontrollojë trafikun e tij në hyrje është që të mbështetet në atributin Multi - Exit - diskriminues (**Multi-Exit-Discriminator MED**). Ky atribut opsional mund vetëm të përdoret nga një AS të multi- lidhur me një tjetër AS për të ndikuar në lidhjen që duhet të përdoret nga AS e tjera për të dërguar paketa drejt një destinacioni të caktuar. Duhet megjithatë të theksohet se përdorimi i atributit Med

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

është zakonisht subjekt i një negociate në mes të dy peering AS-ve dhe disa AS nuk pranojnë të marrin atributin MED parasysh në procesin e tyre të vendimmarrjes . MED vetëm siguron një kontroll lokal të trafikut përbrenda inbound. Nuk studihet efikasiteti i saj në më shumë detaje në këtë tezë. Inxhinierimi i trafikut në mes të fushave fqinje është studiuar nga Winick et al në (WJR02).

3.4.10 Përhapja e rrugëzimit të kontrolluara nga komuniteti (Community)

Një tjetër teknikë që është duke u bërë shumë e popullarizuar për kontrollin e trafikut në hyrje është të mbështetet në kontrollin e Komuniteteve BGP (TCL96, BQ03). Ky atribut opsional rrugëzimi është një grup i 32 bit integer-ave, ku secili prej tyre identifikon një "komunitet" BGP. Një komunitet harton një grup të rrugëve që ndajnë attribute të përbashkëta apo që duhet të marrin të njëjtin trajtim. Vlerat e komunitetit janë përdorur shpesh për të bashkëngjitur Informacione fakultative të rrugëve të tilla si një kod që përfaqëson qytetin ku rruga ishte marrë, pranuar ose një kod që tregon nëse rruga është marrë nga një kolegë (peer) ose një konsumator. Prania e komuniteteve të caktuara BGP brenda një rruge BGP mund të ndikojë në se si kjo rrugë do të përpunohet nga routerat e largët. Në mënyrë tipike, një AS përcakton, në konfigurimin e routerave të saj, një listë të vlerave të komunitetit dhe veprimet për tu kryer kur një rrugë që përmban këto vlera të komunitetit është pranuar. Konsumatorët e këtij AS mund të bashkëngjitin komunitetet e tilla në rrugët që i njoftojnë këtij provider-i.

Disa ISP kanë përdorur atributin e Komuniteteve për tu dhënë klientëve të tyre një kontroll më të hollë në rishpërndarjen e rrugëve të tyre. Prandaj klientëve u ishte dhënë mundësia për të inxhinier-uar më mirë trafikun e tyre në hyrje duke bashkëngjitur vlera të paracaktuara Komuniteti rrugëve. Veprimet e inxhinierimit të trafikut tipik të mbështetur nga ISP-të janë të shënuara në Tabelën .2 . Këto veprime zakonisht zbatohen ndaj AS të madhe (psh tier - 1 ose tier - 2 ISP-të duke ofruar shërbime tranzit), një pikë ndërlidhjeje , një vend ose një kontinent. Vini re se edhe pse jepen emra të tillë si NO_ANNOUNCE dhe prepend të këtyre vlerave të komunitetit, nuk ekziston kodimi standard dhe çdo ISP mund të përcaktojë vlerat e veta të komunitetit.

Tabela 2 : Veprimet tipike të rishpërndarjes së rrugëve në dispozicion me komunitetet

Community	Requested action
NO_ANNOUNCE	Do not announce the route to specified peer(s)
PREPEND	Prepend the AS-Path when announcing the route to specified peer(s)
CHANGE_PREF	Set the Local-Pref value in the AS receiving the route [CB96]

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Në rastin e parë, komuniteti është i bashkangjitur në një rrugë për të treguar se kjo rrugë nuk duhet të shpallet në një peer të caktuar ose në një pikë të caktuar të interkoneksionit . Për shembull, në pjesën e majtë Fig.3.20, AS2 ka konfiguruar routerat e saj për të mos u shpallur rrugëve AS4 që përmbajnë komunitetin 2:1004. AS2 ka dokumentuar përdorimin e këtij komuniteti për peer-sët e vet në mënyrë që AS1 mund të bashkëngjijë këtë vlerë për rrugët e reklamuar për AS2 për të siguruar se ajo nuk do të marrë paketa nga AS4 nëpërmjet AS2. Në një studim të detajuar të dhënave RIPE (BQ03) , është treguar se ky lloj i komuniteteve është përdorur shpesh nga ISP .

Lloji i dytë i komunitetit është përdorur për të kërkuar në rrjedhën e sipërme(upstream) AS për të kryer AS-Path prepending për rrugët e lidhura. Pjesa e djathtë e Fig. 3.20 tregon se si AS1 përdor 2: 3003 dhe 2: 2005 të komuniteteve të dokumentuara nga AS2 për të kërkuar se AS-Path e rrugës është shpallur të paraprijë dy herë kur të shpallet për AS3 dhe AS5. Për të kuptuar më mirë dobinë e vlerave të tilla të komunitetit, le të shqyrtohet përsëri Fig. 3.20, dhe të supozohet se AS6 merr një shumë të trafikut nga AS1 dhe AS2 dhe se ajo do të donte për të marrë paketa nga AS1 (resp. AS2) në R45-R61 (resp. R36-R61) link. AS6 nuk mund të arrijë këtë lloj shpërndarje të trafikut duke kryer prepending vetë. Megjithatë, kjo do të jetë e mundur në qoftë se AS4 mund të kryejë prepending gjatë shpalljes së rrugëve AS6 peers.ave të jashtëm. AS6 kështu mund të reklamojë për AS4 rrugët e saj me komunitetin 4: 5202 (Dokumentuar nga AS4) që tregon se kjo rrugë duhet të paraprijë dy herë, kur të njoftohet AS2. Së fundi, lloji i tretë i përbashkët i komunitetit i përdorur për qëllime inxhinierike trafikut është për të vendosur atributin Lokale-pref në rrjedhën e sipërme upstream AS siç është përshkruar në (CB96).

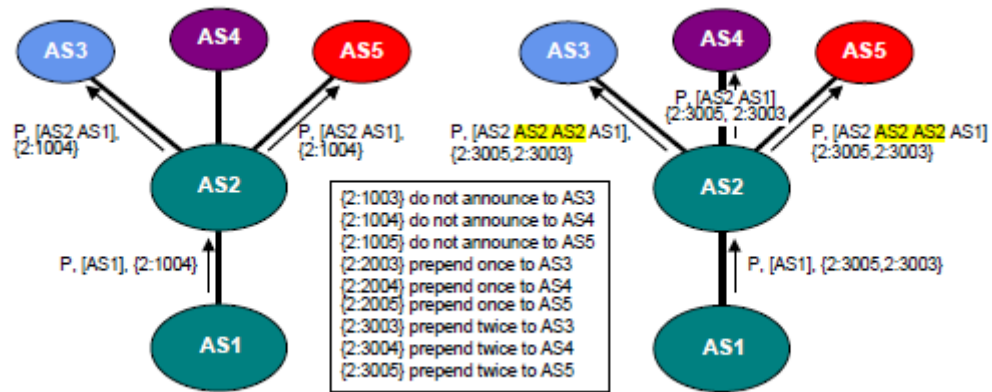


Figura 3.20 : Shembull i rishpërndarjes së rrugëve të komuniteteve – kontrolluara(communities-controlled) .

3.5 Diskutimi

Pjesët e mësipërme kanë përshkruar disa nga manipulimet e attributeve BGP që janë përdorur nga ISP-të për inxhinierimin e trafikut të tyre interdomain. Megjithatë, ka disa kufizime që duhet të merren parasysh kur vendosen këto teknika. Një pikë së pari të

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

theksohet është se kontrolli i trafikut që po largohet (outgoing) me BGP është në bazë të për zgjedhjes, midis rrugëve në dispozicion, të një rrugë të vetme më të mirë. Kjo zgjedhje mund të kryhet në bazë të parametrave të ndryshme, por ajo është e kufizuar nga diversiteti i rrugëve të marra nga ofruesit në rrjedhën e sipërme upstream e cila varet nga lidhja dhe politika e këtyre AS. Sidoqoftë, siç tregohet në (UBQ03a), inxhinieria e trafikut dalës e bazuar në manipulimin e attributeve BGP është e mundur në një kosto të arsyeshme.

Në të kundërtën, kontrolli i trafikut në hyrje është i bazuar në një akordim të kujdesshëm të reklamave të dërguara nga një AS. Ky akordim mund të shkaktojë disa probleme. Për shembull, duke njoftuar prefikset në mënyrë selektive në seksionet peering nuk garanton lidhje me prefikset kur një seksion dështon. Teknika e njoftimeve selektive nuk është pra e fuqishme. Një zgjidhje mund të jetë për të njoftuar prefikset më specifike. Megjithatë, një AS që reklamon prefikset më specifike apo që ka ndarë hapësirë në saj të adresave në prefikse të ndryshme për të njoftuar ata në mënyrë selektive do të reklamojë një numërmë të madh të prefikseve se sa është e nevojshme. Të gjitha këto prefikset do të përhapen në të gjithë internetin global dhe do të rrisin madhësinë e tabelave të rrugëzimit BGP potencialisht të të gjitha AS-ve në internet. (BNC02) raporton se rrugët më të veçanta përbëjnë më shumë se gjysmën e shënimeve në një tabelë BGP. Të ballafaquar me këtë rritje të tabelave të rrugëzimit BGP të tyre, disa ISP të mëdha kanë filluar të instalojnë reklama filtrimi rënëse për prefikset të vogla, në mënyrë për të shmangur një rritje të panevojshme të tabelave të rrugëzimit BGP (BBGR01). Në kohën e këtij shkrimi, filtrimi i prefikseve më të gjatë se 19 bit për disa klasa të adresave është një praktikë e zakonshme dhe inkurajoi praktikën në mes operatorëve të ISP, duke bërë teknika e prefikseve më specifike më pak efektive (Veg05). Atributi MED mund të përdoret vetëm kur ka lidhje të shumta fizike midis dy AS-ve dhe jo në rastin e stub ASs multi-homed për disa ofrues, një situatë shumë e zakonshme sot (ACK03). Teknikat e vetme të mbetura për kontrollimin e trafikut përbrenda një ISP-je janë AS-Path prepending dhe komunitetet BGP. Pavarësisht nga rëndësia e inxhinierisë së trafikut për ISP-të, ka pasur pak studime mbi efikasitetin e këtyre teknikave.

3.5.1 Vlerësimi i AS-Path prepending

Sipas një analize të detajuar të tabelave të rrugëzimit BGP të paraqitur në (BNC02), ASPath prepending është një teknikë e përdorur gjerësisht. Broido et al (BNC02) tregon se 6.5% e rrugëve janë prekur nga prepending. Çuditërisht, efikasiteti i kësaj teknike nuk është studiuar në një bazë në shkallë të gjerë. U krye një studim i parë me simulim të bazuar në AS-Path prepending në (BTP + 03). Më vonë, studimet e matjes janë kryer paralelisht në (QPBU05) dhe (CL05). Në (QPBU05), është studiuar AS-Path prepending nga një stub i vërtetë AS dhe kanë treguar se grimcimi i AS-Path prepending është i trashë. Prepending vetëm një herë ose dy herë tashmë mund të zhvendosë një pjesë të madhe të trafikut. Kjo do të thotë se në praktikë, AS-Path prepending mund të përdoret për të treguar se një lidhje backup duhet të shmanget kur është e mundur, por duke përdorimi i saj për qëllime të ngarkesës-balancimit është i vështirë. Në (CL05), Chang

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

dhe Lo propozoi një teknikë të automatizuar AS-Path prepending. Ata vlerësuan nga një site jo komercial. Ata arritën në përfundimin se teknika e tyre punon, por kërkon matje aktive ndërhyrëse dhe nuk është ekokrrizuar fine. Së fundi, një teknikë AS-Path prepending e optimizuar u propozua në (GDZ05). Një studim i fundit nga Yang et al (YXW + 05) ka hetuar inxhinieri të pakoordinuar të trafikut dhe ka nxjerrë udhëzimet duke siguruar stabilitet, pa koordinim global. Megjithatë, rezultatet e marra nga studime të vogla simulimi ose duke marrë parasysh një pikë të vetme të matjes mund të varet nga vendndodhja aktuale e stub-it AS dhe nuk mund të përgjithësohet lehtë për të gjithë internetin. Në këtë seksion, janë paraqitur rezultatet e një studimi simulimi të performancës AS-Path prepending në një model të topologjisë së Internetit.

3.5.2 Modeli i vlerësimit

Për të vlerësuar efikasitetin e AS- Path prepending si një teknikë inxhinierimi të trafikut, u mbështet në simulimet. Janë përdorur solver-at e rrugëzimit C-BGP të përshkruar më lart si dhe një topologji interneti të nivelit AS. Kjo topologji u nxorr nga tabela rrugëzimi të vërteta BGP të mbledhura nga pikat e shumta të favorshme nga Subramanian et al. (SARK02). Topologjia që kemi përdorur për këtë studim përmban 14695 domains dhe 30815 lidhje interdomain. Është maksimumi një lidhje mes dy fushave (domain) të ndryshme. Ne modelojmë çdo sferë me një router të vetëm BGP dhe politikat e rrugëzimit të bazuara në marrëdhëniet ekonomike, të përcaktuara me (SARK02), të cilat ekzistojnë në mes të fushave domain. Asnjë studim nuk ka qenë në gjendje simulimi për të analizuar ndikimin e politikave të rrugëzimit në rrjete të mëdha të përbëra nga mijëra routers me politika rrugëzimi. Shumica e studimeve të simulimit vetëm marrin në konsideratë disa dhjetëra apo ndonjëherë disa qindra routera. Duke pasur parasysh rëndësinë e politikave të rrugëzimit, kemi zgjedhur për të modeluar ato realisht. Kufizimet e kujtesës dhe pamundësia e dëshimit të topologjisë së brendshme të secilit-AS nga tabelat e të rrugëzimit në dispozicion (SARK02) detyruan marrjen në konsideratë të një routeri të vetëm brenda secilit AS (shih Fig. 3.21).

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

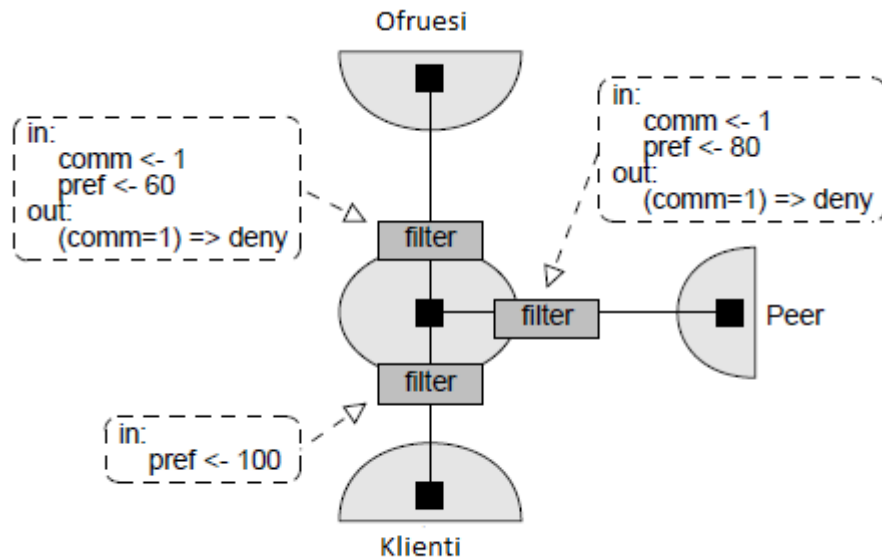


Figura 3.21: Modeli i një AS me politikat.

Këto politika mund të zbatohen lehtësisht me ndihmën e filtrave. Janë treguar detajet e këtyre filtrave në Fig.3.21. Routerat do të jenë konfiguruar për të shënuar çdo rrugë të marrë nga një peer i një ofruesi me një Komunitet. Ky Komunitet (Community) është përdorur për të parandaluar rishpërndarjen e këtyre rrugëve me peers dhe ofruesit e tjerë. Preferenca për rrugët e marra nga klientët, më pas nga kolegët dhe më në fund nga ofruesit është zbatuar në simulimet tona duke u mbështetur në lokal – pref atribut. Një vlerë Lokale - pref prej 100 është caktuar për rrugët e marra nga klientët, një vlerë prej 80 për rrugët e marra nga kolegët dhe një vlerë prej 60 për rrugët e marra nga ofruesit. Edhe pse topologjia e 9 Janarit ishte harta e internetit globale më e saktë në dispozicion të publikut, ajo ka disa kufizime. Së pari, në këtë topologji çdo AS është modeluar si një nyje e vetme e lidhur me AS fqinje. Në realitet, një AS mundet të përmbajë deri në disa qindra routera dhe nuk mund të ketë më shumë se dhjetë lidhjet fizike të ndryshme ndërmjet dy As-sh dhe pse këto lidhje mund të shfaqen si një kufi i vetëm në topologjinë e nxjerrë. Për më tepër, deduktiviteti i përdorur për të konkluduar politikat e rrugëzimit kufizohet nga dy faktorë. Së pari, ajo mbështetet në një grup të vogël të tabelave BGP, në mënyrë tipike të mbledhura në tier-1 ISPs të mëdha dhe këto tabela nuk përmbajnë të gjitha lidhjet interdomain. Së dyti, politikat e rrugëzimit e nxjerra nuk janë gjithmonë të sakta. U llogaritën rrugët interdomain për çdo prefiks të pavarur. Kjo nuk e ndryshon rezultatin e simulimit meqë nuk merret në konsideratë grumbullimi i rrugëve BGP. Përzgjedhja e rrugëve interdomain ndaj çdo prefiksi është pra e pavarur. Kjo bën të mundur të shpërndahen lehtë llogaritjet mbi CPU të ndryshme, pa shtuar shumë overhead.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

3.5.3 Rëndësia e rregullave tie-breaking

Para se të analizohen simulimet e AS-Path prepending, është e rëndësishme për të kuptuar se procesi i vendimmarrjes BGP zgjedh rrugën më të mirë drejt çdo destinacioni. Për këtë qëllim, janë kryer simulimet me modelin e përshkruar në seksionin 3.5.1. U instrumentua simulatori të regjistrojë, për çdo rrugë më të mirë të zgjedhur nga një router BGP, rregullin e veçantë të procesit të vendimmarrjes BGP që ishte në nivel lokal përgjegjës për zgjedhjen e tij. Pastaj mund të përdoret ky informacion për të përcaktuar rëndësinë e rregullave të ndryshme në zgjedhjen e rrugës BGP. U kryen 14695 simulime. Në çdo simulim, një domain tjetër njofton një prefiks të vetëm. Pastaj llogaritet për çdo domain numri i rrugëve të zgjedhura nga çdo rregull i procesit të vendimmarrjes për t'u bashkuar me prefiksin e shpallur. Për çdo domain burim dhe çdo prefix destinacion, ka 4 mundësi. Së pari, domaini ka marrë, pranuar një rrugë të vetme drejt prefiksit dhe procesi i vendimmarrjes nuk është aplikuar. Së dyti, domain ka marrë një rrugë me një preferencë më të lartë, kështu rregulli lokal pref është në rregull. Së treti, ka më shumë se një rrugë me *local-pref* më të lartë por në mesin e tyre ka një AS-rrugën më të shkurtër, kështu rregulli *shortest-path* është në rregull. Dhe së fundi, në qoftë se ka ende më shumë se një rrugë pas rregullit *shortest-path*, *tie-break* është në rregull, i llogaritur.

Ne klasifikuam këto rezultate bazuar në nivelin e domain-ve në hierarkinë e Internetit sirrugesime është identifikuar nga (SARK02). Ka 5 nivele në hierarkinë e internetit. Niveli i parë është thelbi i internetit dhe përmban një rrjetë të plotë të fushave të mëdha tranzit (Tier -1 -së). Niveli i dytë përmban rrjete të mëdha tranzit (tier - 2 -të) të ndërlidhura thellë. Nivelet e tretë dhe në vijim përmbajnë ofruesit më të vogjël rajonale dhe domain-ët stub.

Fig.3.22 paraqet rezultatet e këtyre simulimeve. Në boshtin x ne tregohen 5 nivelet e hierarkisë së Internetit të identifikuara nga (SARK02). Aksi Y tregon rëndësinë relative të rregullave, për çdo nivel të hierarkisë X. Është një barrierë për çdo rregull e marrë në konsideratë : *local-pref*, *shortest-path* dhe *tie-break*, si dhe një barrierë për rrugë të vetme. Kjo e fundit jep një ide për rëndësinë e rrjeteve të cilat mund vetëm të marrin një rrugë të vetme për të arritur një destinacion dhe që në këtë mënyrë nuk do të zbatohet procesi i vendimmarrjes .

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

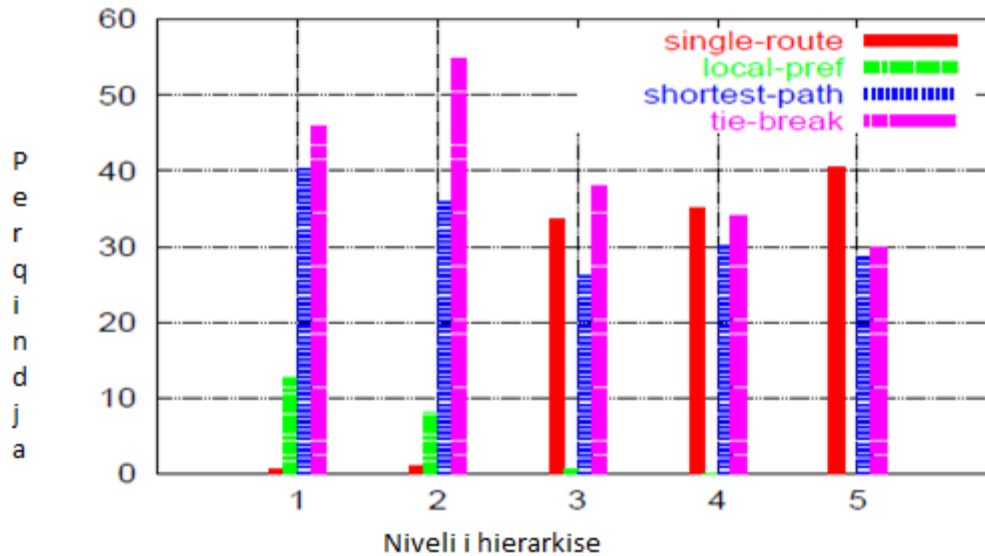


Figura 3.22 : Rëndësia e secilit rregull të procesit të vendimmarrjes BGP në nivele të ndryshme të hierarkisë së internetit .

Rezultatet e simulimit që janë paraqitur në Fig.3.7 tregojnë disa rezultate interesante. Së pari, mund të vërejmë se në mes të 30 dhe 45 % të tier-3 në tier-5 AS vetëm mund të marrë një rrugë të vetme për çdo destinacion. Këto AS janë single - homed. Për AS nga tier-3 në tier - 5, rreth 30% e rrugëve BGP janë zgjedhur në bazë të gjatësisë së AS - Paths të tyre. Pjesa e mbetur prej 30% e rrugëve janë zgjedhur në bazë të rregullave tie-breaking. Për stub AS, këto rregulla tie-breaking shpesh korrespondojnë me hapin e router ID të procesit të vendimmarrjes BGP. Vini re se në realitet, rregulli lokale pref mund të përdoret më shpesh në stub për backup ose arsye të inxhinierisë së trafikut, por kjo nuk është modeluar në simulimet.

Lidhur me AS-ët tier-1 dhe tier-2, 10% e rrugëve të zgjedhura nga ato AS janë zgjedhur në bazë të atributit të tyre lokale-pref. Pastaj, rreth 40% e rrugëve janë zgjedhur në bazë të AS-Path të tyre. Së fundi, në tier-1 -të dhe në domaine kombëtare të mëdha tranzit, rreth 50% e rrugëve janë zgjedhur në një bazë tie-break. Kjo është për shkak të numrit të madh të ndërlidhjeve që ekzistojnë në mes të gjitha këto domaineve dhe në këtë mënyrë për një numër të madh të rrugëve alternative me një gjatësi të ngjashme AS-Path. Për domainet tranzit, rregullat e tie-break korrespondojnë me hapat të tretë, të katërt dhe të pestë të procesit të vendimmarrjes BGP . Një pasojë e rëndësisë së rregullave tie-break në procesin e vendimmarrjes BGP është se është e vështirë të parashikohet se cila rrugë më e mirë do të përzgjidhet në AS e largët. Zgjedhja e rrugës më të mirë varet nga informacioni që nuk është në dispozicion jashtë AS lokale. Në të vërtetë, në rregullin e parë tie-breaking, vlera e MED është në dukje vetëm mes AS-ve fqinje. Në rregullin e dytë tie-break, nëse ekziston një rrugë eBGP, rrugët iBGP janë hequr nga shqyrtimi. Rezultati i rregullit metrikë IGP varet nga politika e brendshme e alokimit të kostos IGP i domainit në konsideratë. Ky informacion zakonisht është konfidencial. Megjithatë disa

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

studiues kanë përdorur traceroutes të konkludojnë shpenzimet IGP të lidhjeve të brendshme në ISP-të tranzit [SMW02], saktësia e tyre duket të jetë e kufizuar [TMSV03]. Në rregullin final tie-break, ne duhet të dimë Router-ID apo IP adresat e routerave të përfshirë, nëse zbatimi mbështetet në këtë informacion. Përsëri, kjo është mbajtur shpesh sekret nga operatorët e rrjetit. Nga ana tjetër, në qoftë se tie-break final mban rrugën e vjetër, ky vendim është jo-determinist.

Meqë rregullat tie-breaking janë përdorur gjerësisht në përzgjedhjen e rrugës BGP, është e vështirë për një AS për të vlerësuar se si trafiku do të hyjë në AS. Për më tepër, kjo gjithashtu tregon se AS-ë shpesh marrin rrugët me të njëjtën gjatësi AS - Path për secilin prefiks destinacioni. Tashmë mund të mendohet se kjo do të ndikojë në efikasitetin e AS - Path prepending. Duke rritur gjatësinë e AS - Path për një rrugë në një ofrues i një dual-homed stub, rruga e njoftuar përmes ofruesve të tjerë është e preferuar nga të gjithë AS që përdorin rregullat tie-breaking për këtë destinacion. Si pasojë, shumë prej rrugëve hyrëse kanë gjasa për të kaluar në ofruesin e preferuar sepse tie-breaking është përdorur për më shumë se 30% të rrugëve.

3.5.4 Vlerësimi i AS-Path prepending

Qëllimi i këtij seksioni është të përgjithësohen vërejtjet në kontrollin e rrugëve që hyjnë në AS tonë eksperimentale me AS-Path prepending. Prandaj, ne kryhen simulimet me topologji të përshkruara në seksionin 3.5.1, i cili kap një pjesë të madhe të internetit të vërtetë. Simulimet nuk kufizohen në një dualhomed të vetme stub. Mund të merren rezultate të ngjashme me (QPBU05) për çdo dual-homed stub në topologji. Për çdo dual-homed stub, studiojmë përdorimin e AS-Path prepending për të kontrolluar se si AS e tjerë arrijnë stub-in.

Është mbështetur në fusha domain dual-homed stub ku të vlerësohet lehtë ndikimi i prepending në shpërndarjen e rrugëve në dy ofruesit e tyre në rrjedhën e sipërme upstream. Këto stub-e përfaqësojnë 82% të multi-homed AS stub në topologjinë e marrë në konsideratë. 5841 dual-homed stubs përbëhen nga më shumë se 39% të AS në topologjinë e 9 janarit. Single homed stubs nuk konsiderohen meqë ata nuk kanë mundësi për të inxhinieruar trafikun e tyre në lidhje të shumta interdomain. Stub-ët me më shumë se 2 ofrues janë më pak të shpeshta. Nuk janë marrë në konsideratë ata në këtë studim, sepse është e vështirë të paraqesim grafikisht rezultatet e simulimit për të tilla multi-homed stub-e. Është përdorur modeli i simulimit të paraqitur në Seksionin 3.5.1. Për çdo stub të konsideruar, është përcaktuar se si është i bashkuar nga të gjitha fushat e tjera, kur nuk përdoret prepending. Pastaj është llogaritur për çdo faqe stub shpërndarja e rrugëve nëpërmjet dy ofruesve të tyre. Është quajtur "default" të shpërndarjes. Kjo shpërndarje është skenarizuar në Fig.3.23. Për të paraqitur rezultatet grafikisht, ne përcaktuam një urdhërimi në mes ofruesve. Secili prej stub-ve tona ka një ofrues të lidhur mirë dhe një ofrues më pak të lidhur. Për të përcaktuar se çfarë është ofruesi më i afërt i një dual-homed stub, është shoqëruar për çdo domain një renditje të bazuar në gradët e mëposhtme: numrin e ofruesit të domain, numrin e peers-ëve dhe numrin e klientëve. Kjo

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

renditje është një mënyrë leksikografike në (hnum_prov, num_peer, num_custi) për të përcaktuar rëndësinë e një domaini. Kjo renditje ka një përjashtim për domains të nivelit-1 në bërthamë që nuk kanë ofruesit. Kur dy fusha domain duhet të krahasohen, nëse një është në bërthamë dhe tjetri nuk është, domeni në bërthamë është konsideruar më i rëndësishmi. Përndryshe, domaini i cila ka më shumë ofrues është më i rëndësishmi. Nëse numri i ofruesve është i barabartë, ne e krahasojmë numrin e peers-ave, më pas numrin e konsumatorëve, nëse kërkohet. Në boshtin x të Fig.3.23, është treguar përqindja e rrugëve që kalojnë më pak providerin e lidhur. Aksi Y- i Fig.3.23 paraqet numrin e stub-ëve të cilët kanë shpërndarje të rrugëve të njëjtë. Ne mund të vërejmë se kur nuk është bërë prepending, nuk ka asnjë tendencë të qartë në favor të një prej dy ofruesve. Disa stube marrin shumicën e rrugëve të tyre interdomain nëpërmjet ofruesit të tyre më të lidhur, të tjerët marrin numrin e njëjtë të rrugëve nëpërmjet çdo ofruesi, ndërsa disa stube marrin pjesën më të madhe të shtigjeve të tyre përmes ofruesit më pak të lidhur.

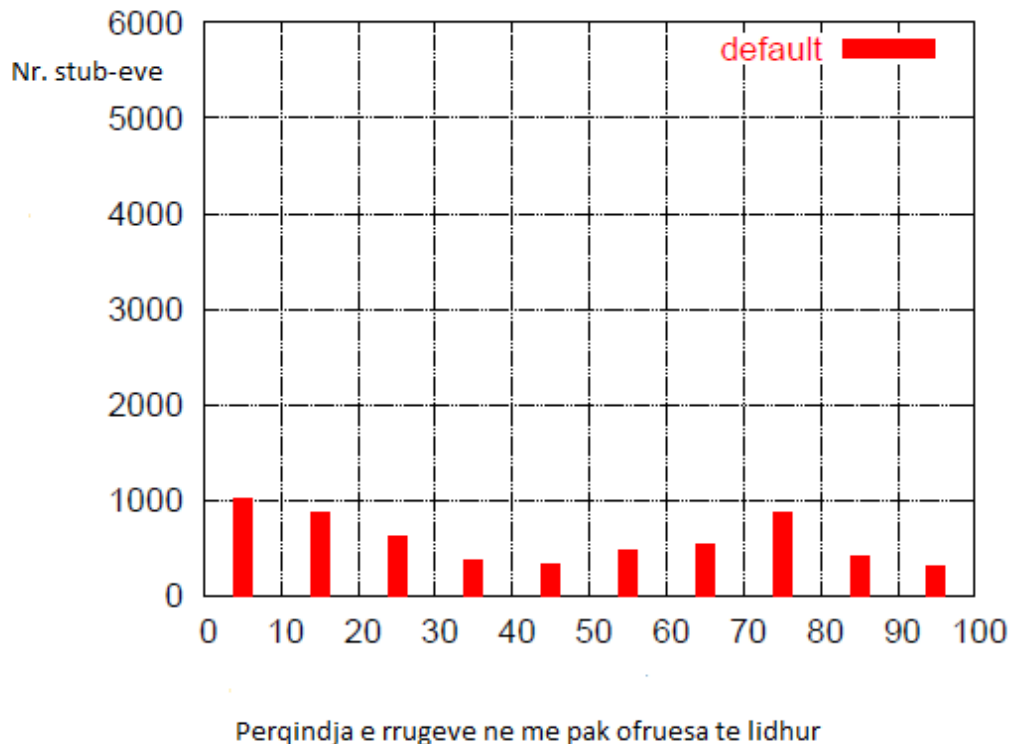


Figura 3.23 : Shpërndarja default relative e rrugëve nga ofruesit më pak të lidhur.

Pastaj mund të kryhen simulime ku çdo dual-homed stub selektive prepëndon AS- Path drejt ofruesit të tij më pak të lidhur dhe në drejtim të providerit më të lidhur. Për çdo stub dhe për secilin nga ofruesit e tyre, janë përdorur tre shuma prepënding të ndryshme: 1, 2 dhe 7. Rezultatet e këtyre simulimeve janë paraqitur në Fig.3.24. Subjekti i sipërm tregon ndikimin e prepënding drejt providerave më pak të lidhur ndërsa subjekti i poshtëm

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

tregon ndikimin e prepending drejt atyre më të lidhur. Rezultati i parë i rëndësishëm që mund të nxirret nga këto simulime është se efekti i prepending është i trashë Mesatarisht, prepending një herë në drejtim të një ofruesi tashmë lëviz një pjesë të madhe të rrugëve larg nga ky ofrues. Grimcimi i AS - Path prepending është pra shumë i kufizuar. Pra, është interesi i tij për inxhinieri trafiku .

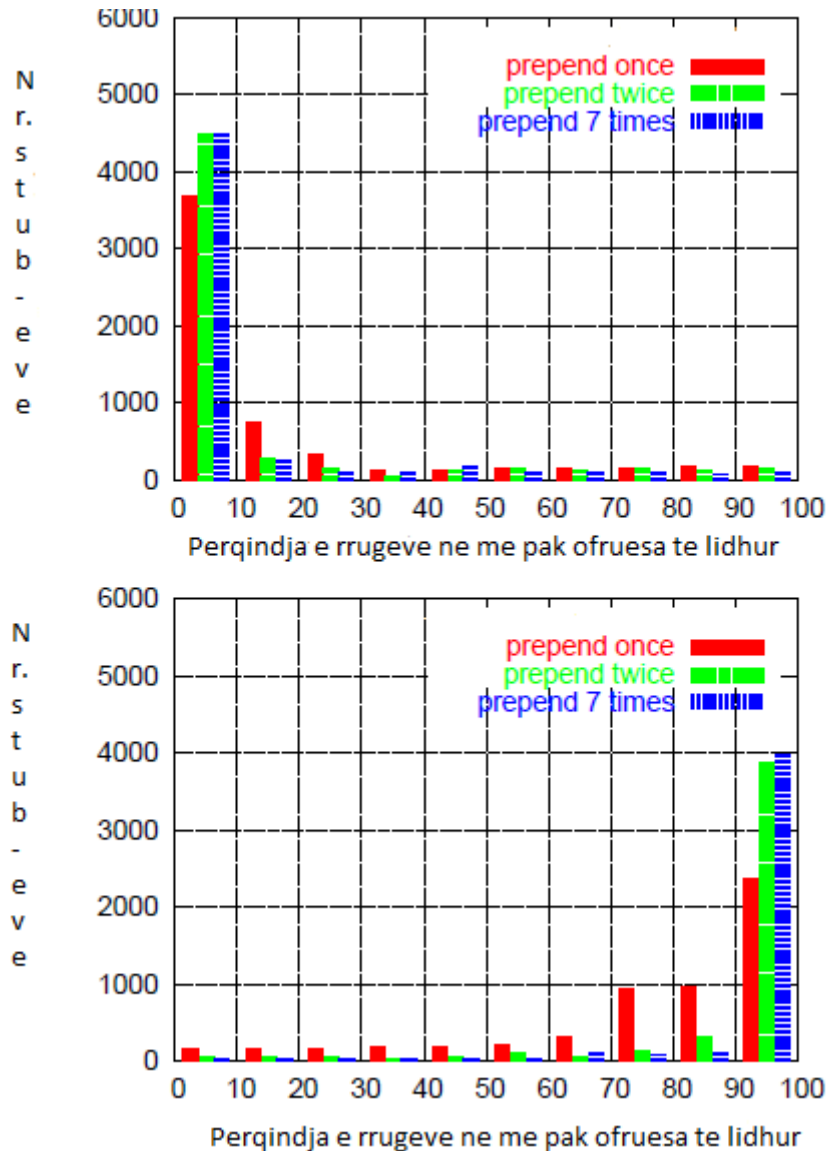


Figura 3.24 : Përqindja e rrugëve në ofruesit më pak të lidhur për sasi të ndryshme të prepending .

Përfundimi i dytë që mund të nxjerrim nga këto simulime është se përfitimi marxhinal i prepending zvogëlohet shpejt. Mund të shihni se prepending një herë lëviz shumë rrugë. Prepending dy herë ende lëviz shumë rrugë larg. Por Dallimi është i vogël në mes të

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

prepending dy herë dhe prepending 7 herë. Për më tepër, prepending shumë herë mund të jetë një problem për shkak të AS-Shtigjet të ngarkuara kërkojnë një sasi të rritur të kujtesës në routera. Së treti, efikasiteti i prepending është shumë i pasigurt dhe varet nga vendndodhja e ofruesve stub, si dhe marrëdhënieve që këto ofrues kanë me domaine të tjera. Ka stub-ë për të cilat rrugë mund të zhvendosen lehtësisht nga një ofrues në një tjetër, stub-ët e tjerë për të cilët është më e lehtë për të lëvizur rrugën nga një ofrues të tjetri se e kundërta dhe madje stub-ët për të cilët një pjesë shumë e madhe e rrugëve nuk mund të zhvendoset në mënyrë të pavarur me shumën e prepending. Më tej janë shqyrtuar disa raste që kanë ndodhur në studimin tonë të simulimit për të sqaruar si topologjia dhe marrëdhëniet e biznesit ndikojnë në efikasitetin e ASPath prepending. Fig. 3.25 paraqet dy stub-e të ndryshme nga topologjia që ne kemi përdorur dhe tregon se si lidhja e ofruesve të tyre të kufizojnë efikasitetin e prepending. Së pari, në Fig.3.25 (a), stub AS3748 ka dy ofruesit, AS3786 dhe AS4766 të cilat kanë një lidhje të ngjashme. Ata të dy kanë shumë marrëdhënie konsumator--ofrues (customer-to-provider) me domaine në bërthamë. Shpërndarja e parazgjedhur e rrugëve hyrëse në lidhjen e aksesit të stubi-it është balancuar: rreth 50% është marrë nga çdo ofrues. Kjo është për shkak të distancës të ngjashme të stubit me pjesën tjetër të internetit nëpërmjet të dy ofruesve. Kur prepending përdoret një herë drejt AS3786, përqindja e rrugëve të cilat arrijnë në faqe stub përmes saj zvogëlohet në 10%. Kjo shpjegohet nga distanca që shpejt bëhet më e gjatë nëpërmjet ofruesit AS3786 duke e bërë rrugën alternative të preferuar. Kur prepending është përdorur dy herë, kjo përqindje bie në pothuajse 0%. Sjellja është e ngjashme kur prepending përdoret drejt AS4766. Pas prepending një herë, përqindja e rrugëve përmes AS4766 ulet deri në 3%. Pas prepending dy herë, ai është i afërt me 0%.

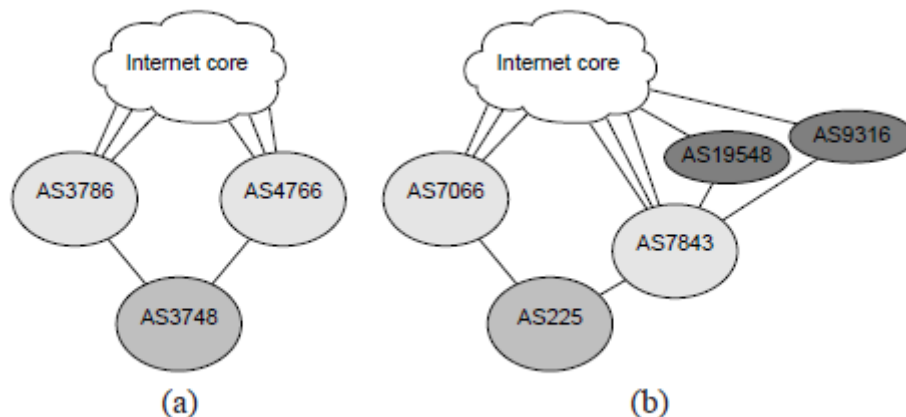


Figura 3.25 : Topologjia dhe politikat pengojnë efikasitetin e AS - Path prepending .

Shembulli i dytë, që është paraqitur në Fig. 3.25 (b), tregon një faqe stub i cili ka ofruesit me rëndësi të ndryshme. Ofruesit më pak të lidhur, AS7066 ka një lidhje customer-to-provider të vetme me AS1239 në bërthamë. Ai gjithashtu ka më pak klientë. Në të kundërt, ofruesi i dytë, AS7843 ka tre marrëdhënie klient-ofrues me AS1, AS209 dhe AS701, të gjithë në bërthamën e internetit. Ai gjithashtu ka dy marrëdhënie të tjera me

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

ofrues të vegjël dhe disa konsumatorë Këtu, në hyrjen default shpërndarja e rrugëve tashmë është e pabalancuar: 15% kalojnë nëpër AS7066, ndërsa 85% kalojnë nëpër AS7843. Kjo është për shkak të zgjedhjeve të fushave domain në bërthamë. Ato zgjedhin rrugën më të shkurtër për stub dhe e ri-reklamojnë atë për klientët e tyre dhe peers-at. Në këtë rast, efikasiteti i AS-Path prepending ndryshon kur ai është përdorur në drejtim të ofruesve më të lidhur ose drejt ofruesve më pak të lidhur. Pas prepending një herë dhe dy herë në drejtim AS7066, përqindja e rrugëve hyrëse të marra nëpërmjet këtij ofruesi bëhet respektivisht 12% dhe gati 0%. Në të kundërt, nuk është e mundur të lëvizen të gjitha shtigjet hyrëse larg nga ofruesi tjetër, AS7843. Rezultatet e prepending një herë, dy herë dhe 7 herë japin në vijim përqindjen e rrugëve: 75%, 67% dhe 50%. Një shembull tjetër është dhënë në Fig.2.26. Këtu, stub, AS17049 është i lidhur edhe me dy ofruesit të një rëndësie të ndryshme. Ofruesi më i afërt është një AS6467 prioritar për shkak se ai nuk është në bërthamë, ndërsa ofruesi tjetër, AS1239 është. Megjithatë, AS6467 ka një lidhje të shkëlqyer me domaine në bërthamë, të tillë si AS1, AS701, AS7018 dhe gjithashtu AS1239. Për më tepër, këto fusha, domaine (përveç AS1239) do të preferojnë rrugët e mësuara nga AS6467 i cili është një klient nga rrugët e marra nga AS1239 i cili është një peer pavarësisht nga gjatësia e AS-Path! Kjo është arsyeja pse pas prepending vetëm dy herë në drejtim AS1239, nuk ka më shumë rrugë duke kaluar përmes saj. Në të kundërt, prepending ndaj provider-it tjetër, AS6467, mezi lëviz shumë rrugë. Edhe pas prepending 7 herë, përqindja e rrugëve të cilat arrijnë stubin me anë të AS6467 është ende më shumë se 58%.

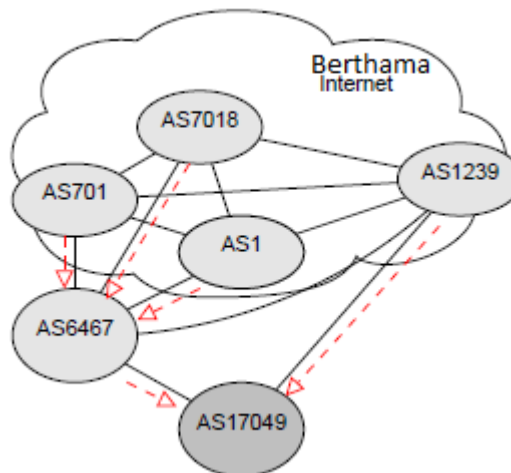


Figura 3.26 : Topologjitë dhe politikat pengojnë efikasitetin e AS - Path prepending .

3.6 Vlerësimi i Komuniteteve

Duke përdorur atributin e Komuniteteve për të kryer inxhinierinë e trafikut hvrës mund të sigurojë një grimcim më fin se sa prepending AS-Path apo njoftimet selektive. Megjithëse atributi i Komuniteteve është përdorur gjerësisht në internet sot, siç tregohet në anketat tona (BQ03), shfrytëzimi i tij për qëllime të inxhinierisë së trafikut të një ISP

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

nuk është studiuar ende. Në (QTUB04), është treguar se shfrytëzimi i Komuniteteve për qëllime inxhinierike trafiku mbështetet në një përkufizim ad hoc të vlerave të Komunitetit dhe në konfigurimin manual të filtrave BGP që e bëjnë atë vështirë për t'u përdorur dhe subjekt i gabimeve. Për të zgjidhur këto probleme janë propozuar një numër i kodimit standard për Komunitetet: Komunitetet e rishpërndarjes (BCH + 03) dhe Komunitetet Proxy (AG04).

Në praktikë, mund të pritet që këto komunitete do të përdoren për të ndikuar rishpërndarjen e rrugëve në drejtim të ISP-ve të mëdha tranzit me një numër të madh të konsumatorëve. Konsiderohet për shembull rasti i YUCOM, një të dyfishtë-homed ISP evropiane. Ashtu si shumë të tjerë ISP (SARK02), kjo ISP ka dy ofrues të mëdhenj upstream që lejojnë që ai të arrijë të gjithë internetin. Fig. 3.27 siguron një vështrim nga afër të ofruesve të nivelit-(tier-1) dhe peers-ëve në bazë të reklamave BGP të marra nga ISP e studiuar. Në këtë shifër, tregojmë një nëngrup të vogël të topologjisë interdomain dhe numri i dallueshëm i AS të reklamuar nëpër tre ISP-ve të nivelit-1 më të mëdha.

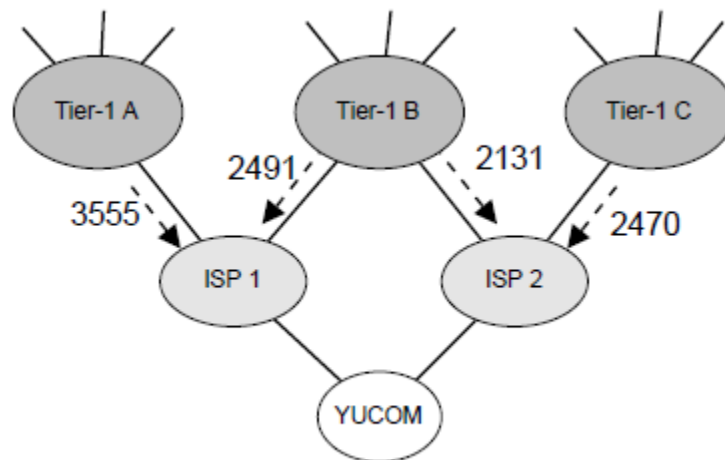


Figura 3.27 : Një pjesë e topologjisë interdomain parë nga YUCOM

Fig.3.27 tregon dy informacione interesante. Së pari, çdo tier-1 ISP siguron lidhje dhe kështu shpall rrugët drejt një numri të madh të AS. Në total, tre ofruesit më të mëdhenj tier-1 shpallin prefikset nga më shumë se 8500 AS. Së dyti, ISP e studiuar mëson rrugët për më shumë se 2000 AS bashkangjitur tier-1 B me anë të dy ofruesve të tij në rrjedhën e sipërme upstream. Duke përdorur komunitetet në shënjestër të atyre tier-1 ISP të mëdhenj, ISP e shqyrtuara mund të ndikojnë në rishpërndarjen e rrugëve të saj në një numër të madh AS-sh me vetëm disa komunitete. Për shembull, ISP e studiuar mund të përdorë një komunitet të vetëm që të kërkojë ofruesin e saj të parë në rrjedhën e sipërme për të njoftuar rrugët e saj lokale me AS-Path prepending vetëm ndaj tier-1 B. Rezultati i këtij njoftimi të modifikuar nga ofruesi i parë do të jetë që trafiku i cili vjen nga AS e

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

bashkangjitur me tier-1 B do të merret përmes ofruesit tjetër. Ky është një lajm i mirë për inxhinierinë e trafikut me bazë në Komunitet Klasike. Komunitetet BGP apo Komunitetet e rishpërndarjes duke u zhvilluar nga IETF citedraft-red-comm-grow-00: 2003 mund të përdoret për të arritur një kontroll fin në trafikun në hyrje sesa AS-Path prepending. Megjithatë, duhet të theksohet që ata vuajnë nga tre të meta të rëndësishme. Pengesë e parë është se, duke pasur parasysh njohuritë tona të kufizuara mbi topologjinë e internetit dhe politikat e rrugëzimit të përdorura nga AS e largëta, është e vështirë të parashikohet ndikimi i një vlerë të caktuar të Komunitetit. Për shembull, është konsideruar Fig. 3.28 dhe është supozuar se stub AS i bashkangjitur rrugës së saj të reklamuar për ISP2 një Komuniteti që tregon se ISP2 nuk duhet të reklamojë rrugën nivelit-1 B (tier-1B). Në këtë rast, tier-1 B nuk do të përdoret lidhjen e saj me ISP2 për të arritur në stub. Nga Fig. 3.28, tier-1 B do të dërgojë paketat e saj për tek tier-1 C ose tier-1 A. Në rastin e parë, Komuniteti i përdorur nga stub-i nuk ka ndonjë efekt në paketat të marra nga stub-i. Për më tepër, burimet që janë në drejtim të rrymës nga tier-1 B do të rillogaritin rrugën e tyre më të mirë për të arritur në stub dhe disa prej tyre mund të përdorin tier-1 C në vend të nivelit-1 B për të arritur në stub, ndërsa të tjerët do të shfrytëzojnë rrugë të tjera. Duke pasur parasysh njohuritë e kufizuara mbi topologjinë e internetit, është shumë e vështirë për të parashikuar vendimet që të gjitha këto AS do të marrin. Vini re se në qoftë se prepending drejt tier-1 B është kërkuar nga stub-i, Komuniteti nuk do të ketë ndonjë ndikim meqë tier-1 B preferon rrugët e drejtpërdrejta të marra nga klientët e saj sesa rrugët përmes peers-ëve të saj.

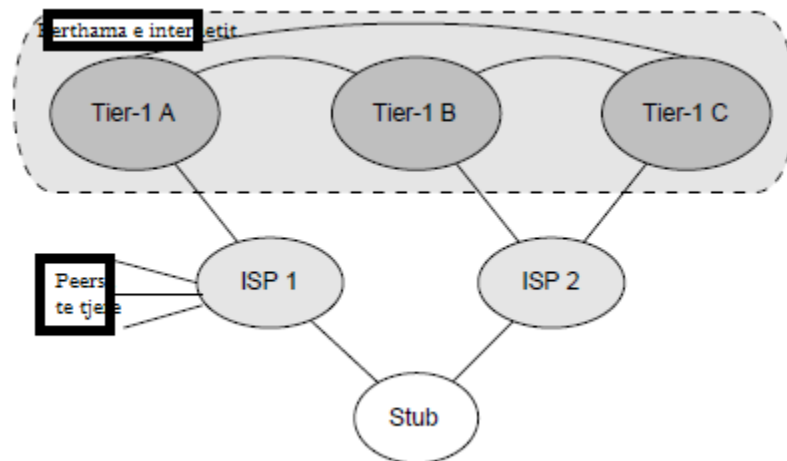


Figura 3.28 : Ndikimi i topologjisë dhe marrëdhëniet e biznesit në efikasitetin e Komuniteteve

Një pengesë e dytë e komuniteteve BGP është se ndikimi i një Komuniteti në rrjedhën e paketave hyrëse do të varet nga fakti nëse është i lidhur me komunitetet e tjera apo jo. Për shembull, merret në konsideratë pjesa e djathtë e Fig.3.10. Supozohet se AS17049 përdor një Komunitet për të kërkuar AS6467 të mos njoftojë rrugën e tij për AS701. Në këtë rast, AS701 mund të rinovojë rrugët e tij BGP dhe përdorimi i lidhjeve peering të tij me

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

AS1 për të arritur AS17049 nëpërmjet AS6467. Kështu, Komuniteti nuk ka efekt mbi rrjedhën e paketës siç shihet nga AS17049. Megjithatë, nëse ky komunitet është përdorur së bashku me një komunitet duke kërkuar AS6467 për të mos reklamuar rrugën për AS1, atëherë të dy AS701 dhe AS1 ndoshta do të përdorin AS1239 për të arritur AS17049. Së fundi, pengesa e fundit e përdorimit të Komuniteteve është se një AS tipik do të duhet të zgjedhë në mes të një numri të madh të komuniteteve të ndryshme. Për shembull, konsiderojmë Komunitetet e rishpërndarjes (BCH + 03) që lejojnë njëstub të ndikojë në shpallje të rrugëve të tij peers-ave të peers-ave të vet. Numri në dispozicion i komuniteteve të rishpërndarjes varet nga numri i AS-ve që janë dy AS-HOPS larg. Për Belnet, ka 1729 AS të dallueshme në dy AS-HOPS. Në praktikë megjithatë, mund të pritet se Komunitetet e rishpërndarjes do të përdoren kryesisht në lidhjet e konsumatorë-provider. Fig.3.29 tregon shpërndarjen kumulative të lidhjeve në 2 HOPS për AS multi-homed stub në topologji nga (SARK02). Kjo na jep një ide të numrit të Komunitetit të rishpërndarjes që mund të përdoren nga një stub multi-homed. Kurba e parë (Në të majtë) jep numrin kumulativ të multi-homed stub me një numër të caktuar lidhjesh me ofruesit në 2 HOPS. Kurba dytë lidhet me numrin e lidhjeve peer-to-peer në dy HOPS. Kurba e tretë tregon numrin e lidhjeve, në 2 HOPS, me klientët që janë të single-homed. Kthesa e fundit jep numrin e peerings me klientët e vetëm dhe multi-homed në 2 HOPS dhe numri i përgjithshëm i peerings në 2 HOPS.

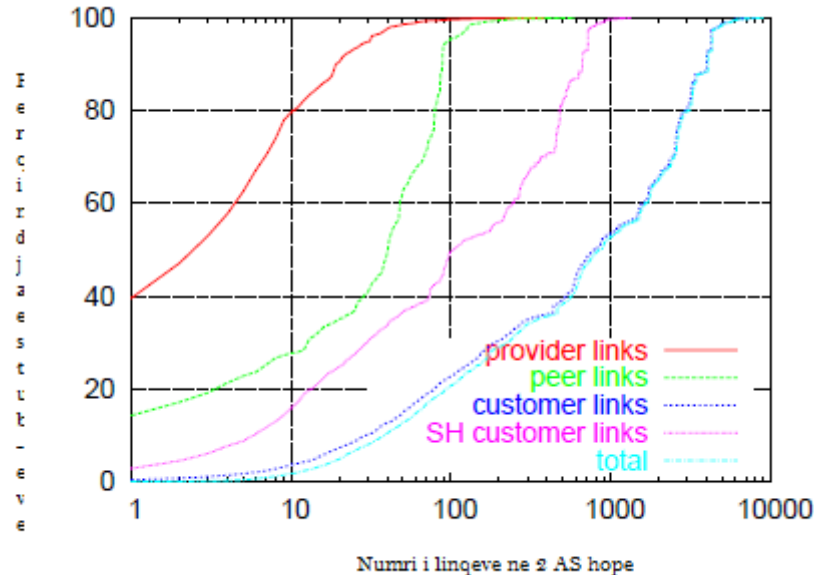


Figura 3.29 : Rëndësia e marrëdhënieve të ndryshme të biznesit në 2 AS HOPS nga multi-homed stub domains.

Njëzet për qind e stub-ve multi-homed kanë më shumë se dhjetë ofrues peerings në dy HOP-e. Këto stub-ë mund të përdorin $2_{10} = 1024$ grupe të komuniteteve për inxhinierimin

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

e tyre të trafikut në hyrje me komunitetet që ndikojnë në rishpërndarjen e rrugës së tyre drejt vetëm ofruesve. Gjashtëdhjetë për qind e stub-ve kanë më shumë se 500 lidhje në 2 HOPS. Kjo do të thotë se shumë kombinime të Komuniteteve ekzistojnë për inxhinierimin e trafikut e këtyre stub-ve edhe nëse përjashtohen komunitetet që targetojnë klientët single-homed meqë ky trafik nuk mund të zhvendoset me rishpërndarjen e Komuniteteve.

3.7 Qasjet duke mos u mbështetur në tweaking BGP

Përveç teknikave inxhinierike të trafikut që kemi diskutuar në seksionet në të kaluarën, ka propozime të tjera për të kontrolluar trafikun interdomain që jo domosdoshmërisht mbështeten në tweaking atributet BGP. Një shembull i parë është përdorimi i sistemeve fundorë me bazë rrjete mbulues të tillë si RON (ABKM01). Në ato qasje, overlay janë krijuar mes sistemeve fundore në bazë të matjeve të mbledhura. Mbulimi overlay është zbatuar duke përdorur tunelet IP. Këto qasje kërkojnë që sistemet fundorë të modifikohen. Përveç kësaj, këto qasje kërkojnë ngritjen e një numri të madh të tuneleve meqë ata punojnë në nivelin e flukseve ose çifteve burim i / e destinacionit. Një qasje e ngjashme është edhe alternativa e propozuar në (SSA + 99). Alternativa gjithashtu mbështetet në tunele të përcaktuara mes routerave dhe supozon se sistemet fundorë janë në gjendje për të zgjedhur routerat e tërthortë të e duhur. Në (GCLC04) është propozuar dhe vlerësuar, një sistem load-balancing i bazuar në përkthimin e adresave të rrjetave dinamike (NAT). Adresat burim e paketave dalëse janë përkthyer në një nga adresat e jashtme të një kutie NAT lidhur me ofruesit e shumtë. Adresat e jashtme të zgjedhura nga sistemi i ngarkesës-balancim varen nga cilët link është caktuar trafiku kthimit. Ky sistem lejon për kontrollin hyrës dhe dalës të trafikut për rrjetet e ndërmarrjeve të vogla. Kontrolli i ofruar është fine-grained pasi mund të bëhet në nivelin e flukseve të shtresës 4. Përveç kësaj, ka edhe propozime për të sjellë ndryshime drastike të rrugëzimit interdomain. Për shembull, arkitektura e kontrollit të politikave mbuluese (Opca) (ACK03) ka marrë në konsideratë përdorimin e një protokollit të veçantë për të kryer kontrollin e informacionit. Ideja që mbështetet pas Opca është për të ndarë rrugëzimin dhe politikat e tij. Kjo çon në përdorimin e një tjetër protokollit në një rrjet overlay për të trajtuar ndryshimet në politikën e rrugëzimit. Aplikacionet e një arkitekture të tillë përfshijnë përmirësimin e kohës së rrugës failover si dhe lejjimin e multi-homed stub-ve të kontrollit të trafikut në hyrje të tyre. Së fundi, (Yan03) propozon arkitekturën e rrugëzimit të internetit të re (Nira) që të lejojë hostet për të zgjedhur ISP tranzit të përdorura për të arritur një destinacion. Nira përfshin metodat që lejojnë hostet individuale për të zbuluar topologjitë, dmth rrugët ekzistuese në destinacion, si dhe për të zbuluar disponueshmërinë e këtyre rrugëve, dmth nëse ato aktualisht mund të përdoren apo jo. (Yan03) diskuton sfidat e projektimit dhe të vendosjes së një protokollit të tillë të rrugëzimit interdomain të ri. Një tjetër metodë është përshkruar në (KKW + 03), ku propozohet korniza (framework) *banane*. Kjo kornizë synon të ofrojë mjetet e shfrytëzimit të shumëllojshmërisë së rrugëve në dispozicion në Internet.

3.8 Cooperative Engineering Traffic

Është propozuar një qasje e re për të lejuar një AS stub për të kontrolluar trafikun në hyrje të saj në mënyrë deterministike. Për më tepër, ajo është e shkallëzuar dhe me pak përpjekje mund të vendoset sot në internet. Qasja mbështetet në krijimin e Peerings Virtual në mes të AS-ve bashkëpunues. Një Peering Virtual lejon një destinacion AS për të kërkuar një burim AS për të dërguar paketat e tij me anë të routerit hyrës të zgjedhur në AS-në destinacion. Zgjidhja mund të përdoret nga AS-t të gatshëm për të load-balancuar trafikun e tyre hyrës, përdorimi i rrugëve të ulët latente, shtigjet me Bandwidth të lartë apo edhe për të ulur koston e trafikut të tyre interdomain. Këtu është fokusi në AS stub-ë të tillë si përmbajtje- ofruesit(content-providers), rrjetet e ndërmarrjeve dhe ofruesve të aksesit broadband që prodhojnë shumicën e trafikut në internet. Edhe pse zgjidhja mund të përdoret në rastin e AS-ve tranzit, kontrollimi i trafikut në hyrje në AS-e të mëdhenj tranzit është një problem tjetër që është jashtë fushëveprimit të kësaj teze.

Zgjidhja e dhënë e ndryshon pak protokollin BGP. Për të siguruar që këto modifikime mund të vendosen në mënyrë rritëse, nuk do të kërkohen AS tranzit për të mbështetur shtesat. Të vetmit routera të prekur janë të vendosur brenda burimit dhe destinacionit bashkëpunues. Ky është një kontribut i rëndësishëm i zgjidhjes tonë. Peerings virtualë mund të përdoren për të arritur lloje të ndryshme objektivash të inxhinierisë së trafikut, si balancimi i ngarkesës së trafikut, duke preferuar rrugët me vonesë më të ulët, rrugët me Bandwidth më të lartë ose uljen e koston së trafikut. Është hetuar shfrytëzimi i Peerings Virtual për të zgjidhur dy probleme të ndryshme inxhinierike të trafikut. Problemi i parë i shqyrtuar, është balancimi i ngarkesës së trafikut të marrë nga një domain stub në lidhjen e tij të qasjes. Siç përkrahë në Kapitullin 2, trafiku i një multi-homed domain stub shpesh është i pabalancuar. Kur një AS stub është i lidhur me dy ofruesit tranzit ai mund të, në varësi të konfigurimit BGP të ofruesve të saj, të marrë 80 ose 90% e trafikut të tij nëpërmjet një ofruesi. Ky çekuilibër mund të çojë në kongestion dhe humbje paketash mbi lidhjet e qasjes. Për të shmangur këtë, ngjeshje AS stub kanë nevojë për të lëvizur disa rrjedhje të trafikut në hyrje në mes të ofruesve për të marrë një bilanc trafiku më të mirë.

Problemi i dytë i shqyrtuar është zgjedhja e rrugëve me një cilësi më të mirë. Meqenëse BGP nuk përdor asnjë metrikë përveç gjatësisë së AS - Path (HFP + 02 ,BNC02), zgjedhja që bën është më e mirë kur ka rëndësi një tjetër QoS metrikë. Ka raste kur janë dy AS që do të donin që të mbështeten në një metrikë tjetër të tillë si vonesa apo bandwidth në dispozicion për të kryer zgjedhjen e rrugëve të tyre. Për shembull, dy AS mund të dëshirojnë të zgjedhin rrugën interdomain me latencinë më të ulët në mes të portave VoIP. Një shembull tjetër është rasti i dy Rrjetave Kombëtare të Kërkimit dhe Edukimit(NRENs) labororët host e të cilëve që duhet të shkëmbejnë të dhëna të mëdha të tilla si imazhe teleskopi. Ata mund të dëshirojnë për të gjetur rrugën që ka Bandwidth më të madh në dispozicion për të vazhduar me transferimin e file-ve .E njëjta kërkesë e aplikuar për informatikë GRID ku duhet shpesh të shkëmbehen vëllime të mëdha të të

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

dhënave në mes të qendrave që zotërojnë fuqinë e llogaritjes. Në fund, ne fokusohemi në përzgjedhjen e rrugëve me vonesë të vogël .

3.8.1 Peerings Virtual

Sot, një metodë e zakonshme e përdorur nga AS për inxhinierimin e rrjedhës së trafikut të tyre interdomain është për të krijuar peerings me AS e tjera (Bar00). Këto peerings shitesë do të sigurojnë rrugët e ndryshme për AS, duke rritur larminë e saj të rrugëve dhe mundësinë për të marrë rrugët më të mira në drejtim të disa destinacioneve. Këto peerings janë krijuar ose me lidhje direkte private mes dy AS-ve ose mbi një pikë të interkoneksionit. Një seancë eBGP përdoret mbi linkun stub për të reklamuar prefikset që janë të arritshme nëpërmjet çdo AS. Peerings BGP krijohen manualisht duke ndryshuar konfigurimin e ruterave me dorë. Megjithatë, veprimet manuale janë të gabueshme dhe të ngadalta (MWA02). Përveç kësaj, koha e krijimit të një peering të ri është shpesh në rendin e madhësisë së disa ditëve ose javëve. Është propozuar për ti zgjidhur këto probleme me Peerings Virtual, të cilat automatizojnë krijimin e peerings BGP në mes AS-ve bashkëpunues dhe zgjerimin e tyre në Ass1 të largët. Peerings virtuale lejojnë një AS për të kontrolluar pikën e hyrjes së përdorur nga AS-të non-adjacent (të pangjitur). Prandaj, Peerings Virtual përfaqësojnë një zgjidhje deterministike për kontrollin e trafikut në hyrje të një si-së. Peerings Virtual janë themeluar nga AS-të bashkëpunues në bazë të ngarkesës së tanishme të trafikut ose në një tjetër pronë. Pritet se institucionet dhe removals të Peerings virtuale do të ndodhin në një periudhë kohore të paktën disa orë.

Një Peering Virtual është një peering i ndërtuar në një mënyrë dinamike i themeluar nga tuneli IP uni-drejtim mes dy AS-ve, por jo AS-të 'non-adjacent'. Ky tunel është përdorur nga burimi AS për të dërguar paketa në destinacionin AS nëpërmjet një routeri hyrës të zgjedhur në AS destinacion. Për të kontrolluar këto Peerings Virtuale, është propozuar për të vendosur, brenda secilit AS bashkëpunues, një Virtual Peering Controller (VPC) që do të jetë përgjegjës për krijimin dhe mirëmbajtjen e Peerings Virtual. Një VPC mund për shembull të jetë një workstation i dedikuar ose vetëm një router BGP stand-alone. Lloje të ndryshme të tuneleve IP mund të përdoren për të mbartur paketa mbi Peerings Virtual. Zgjidhja më e thjeshtë është që të përdorin IP-in-IP encapsulation (Sim95) ose tunelet Generic Routing Encapsulation (GRE) (FLH + 00). Këto zgjidhje kanë një overhead të ulët (20 bytes për IP-në-IP dhe 24 bytes për GRE) dhe janë mbështetur nga shumica e ruterave. Dy llojet e tjera të mundshme të tuneleve janë Layer Two Tunneling Protocol (L2TP) (LTG05) dhe IPSec (Ken05) në mënyrën e tunelit. L2TP është përdorur shpesh për të siguruar shërbimet Virtual Private Network (VPN), por overhead- ët e saj janë më të mëdhenj se GRE. Avantazhi kryesor i IPSec do të jetë origjinaliteti dhe facilitetet e enkriptimit që mund të përdoren për të mbrojtur Virtual Peering.

Në të kaluarën, tunelet IP shpesh janë kritikuar për shkak të kostos së enkapsulimit /dekapsulimit të paketave dhe rrezikun e fragmentimit do të duheshin për të vënë në dukje se ata nuk janë më probleme operative. High-end routerat tani janë të aftë për të mbështetur enkapsulimin dhe dekapsulimin e normë së linjës, ose në ndërfaqet normale

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

ose duke përdorur ndërfaqe të veçanta (Net04). Së dyti, me lidhjet Packet mbi SONET / SDH që janë të vendosur gjerësisht nga ISP, njësia e transmetimit maksimal (MTU) janë më pak të rrepta sesa ishin më parë. Për më tepër, pothuajse të gjitha implementimet TCP mbështesin PathMTU Discovery (PMTUD) (MD91) dhe tunelin head-end mund të kryejnë PMTUD në vetë tunelin. Një tjetër lloj i zakonshëm i tuneleve të përdorura nga ISP-të janë tunelet MPLS (DR00). Për Peerings virtuale, MPLS do të ofrojë një overhead të ulët, si dhe restaurimin të shpejtë, të rezervimit Bandwidth dhe aftësive të inxhinierimit të trafikut. Për fat të keq, ato përparësi vijnë me një çmim: domain-et tranzit duhet të suportojnë MPLS dhe duhet të lejojnë fushat të tjera për të përdorur RSVP-TE (ABG + 01) për të vendosur tunelet MPLS nëpërmjet rrjetit të tyre. Ndërsa shumë ISP-të mëdha përdorin MPLS brenda rrjetit të tyre, ata shpesh hezitojnë për të lejuar klientët e tyre apo peer-ët të dërgojnë mesazhe RSVP-te për të krijuar MPLS LSPs përmes rrjetit të tyre.

Për të kuptuar funksionimin dhe dobinë e Peerings Virtual, le të shqyrtojmë rrjetin e thjeshtë të paraqitur në Fig.3.30. Në këtë rrjet, le të supozojmë se ASD do të donte të balanconte mbi ofruesit e tij trafikun e marrë nga dy burimet AS1 dhe AS2. Meqenëse dy burimet janë të bashkangjitur në të njëjtin ofrues, asnjë ASPath prepending as komunitetet e rishpërndarjes (QTUB04) nuk do të lejojnë ASD që të kontrollojnë trafikun e saj në hyrje. Si router aksesi i ASD është i lidhur me dy ofruesit, P1 dhe P2, një tjetër zgjidhje është e mundur. Kur një ofrues krijon një lidhje me një nga klientët e saj, ai zakonisht ndan dy adresat IP në këtë link nga një prej blloqeve të veta CIDR.

I pari është për routerin e vet dhe i dyti është për routerin për krahun e konsumatorit. Një pasojë e kësaj praktike të përbashkët është se routeri i aksesit i ASD mund të arrihet me anë të dy adresave të ndryshme IP: P1.1 dhe P2.1. AS P1.1 i takon bllokut CIDR të reklamuar nga P1, cdo pakëta e dërguar në internet me P1.1 si destinacion do të arrijë ASD nëpërmjet P1. Në bazë të këtij konstatimi, ASD mund të balancojë trafikun e saj në hyrje me kusht që të mund të bindë AS1 (resp. AS2) për të dërguar të gjitha paketat destinacioni i të cilit i takon ASD brenda një tuneli IP që përfundon në P2.1 (resp. P1.1). Ky tunel mund të krijohet pa ndonjë bashkëpunim nga ofruesit tranzit. Kjo është transparente për P1, P2 dhe P3 dhe kontrollohet tërësisht nga AS1 (resp. AS2) dhe ASD.

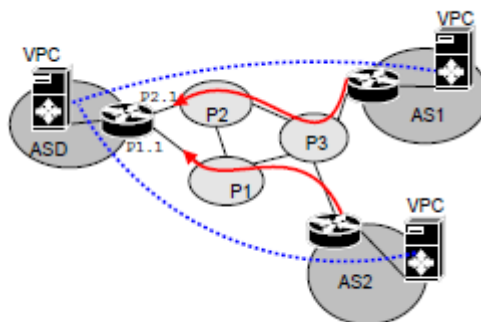


Figura 3.30: Skica e qasjes

3.8.2 Arkitektura dhe protokollin

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Komponentë të shumtë janë të përfshirë në krijimin dhe funksionimin e një Virtual Peering, siç tregohet në Fig. 3.31. Së pari, të dy sistemet autonome që do të vendosin Virtual Peering: Kërkuesi AS (RAS) dhe Burimi AS (sas). RAS është AS i cili dëshiron të kontrollojë trafikun e tij në hyrje. Një nga routerat e tij do të ndërpresë tunelin që do të ketë origjinën në një router të SAS. Si RAS dhe SAS mund të jenë rrjetet e përbërë nga disa routerat BGP. Duhet të ketë të paktën një Virtual Peering Controller (VPC) në çdo SAS dhe RAS. VPC-të janë përgjegjës për monitorimin e rrjetit dhe krijimin e Peerings të kërkuara Virtual. Në mënyrë që të monitorojnë trafikun, VPC-të janë të lidhura me një infrastrukturë matjeje të tillë si (VE04). Përveç kësaj, do të mbledhin VPCs rrugët në dispozicion eBGP nga routerat kufi. Në një rrjetë- të plotë(full-mesh) iBGP, VPC zakonisht do të ketë një seksion iBGP me të gjitha routerat në domenin. Zgjidhje të tilla si BMP (Scu05) dhe Juniper's e externalbest mund të përdoren në të ardhmen për të rritur numrin e rrugëve eBGP të mësuara. VPC-të mund të jenë workstation-a të dedikuara ose të qëndrojnë si routerat të vetëm BGP. Për shkak të pozicionit të tyre qendror në një AS, do të ishte e natyrshme për zbatimin e karakteristikave VPC në BGP rrugë - reflektorët.

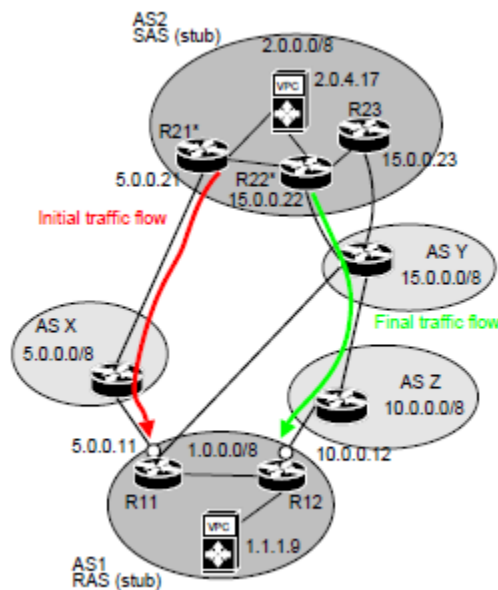


Figura 3.31: Topologjia e rrjetit Interdomain

Për të filluar krijimin e Peerings Virtual dhe për shkëmbimin e parametrave në mes të VPC-ve të përfshirë është i nevojshëm një protokoll. Në vend të përcaktimit të një protokollit të ri sinjalizimi, është propozuar në këtë kapitull mbështetja në protokollin BGP tashmë të vendosur si një mjet për të shkëmbyer kërkesat Peerings Virtual. Arsyeja për këtë zgjedhje është se një protokoll i tillë kërkon disa ndryshime në BGP dhe se ai

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

mund të vendoset në mënyrë rritëse. Zgjerimet e zgjidhin çështjet si në vijim. Së pari, VPC në një RAS duhet të mësojnë adresën IP e VPC në SAS. Së dyti, VPC në një RAS ka nevojë për një mjet të sigurt të kërkuar nga një VPC në një AS të largët krijimin dhe heqjen e Peerings Virtual. Pastaj, VPC në SAS duhet të komunikojë me routerat kufitare të AS të saj në mënyrë që të strukturojë tunelet e kërkuara. Së fundi, rrugët duhet të shpërndahen brenda SAS për të reklamuar tunelet.

3.8.3 Advertisement i adresave VPC

Virtual Peering Controller Advertisement (VPCA) është përdorur për të reklamuar adresat IP e VPCs që i shërbejnë SAS. Në të vërtetë, për të kërkuar ngritjen e Virtual Peering me SNS, RAS duhet të dijë adresën IP e VPC të Sas-së. Në qoftë se një numër i vogël i AS duan të përdorin Peerings Virtuale, këto adresa mund të shpërndahen në mënyrë offline, me e-mail ose me mjete të tjera. Megjithatë, pasi numri i pjesëmarrësve rritet, një zgjidhje automatike do të jetë e nevojshme. Është propozuar që të shpërndahen adresat VPC IP SAS-së brenda mesazheve BGP Update të krijuara nga SAS. Adresa VPC IP është e koduar në një vlerë kalimtare të zgjeruar të komunitetit. Atributi i zgjeruar i komunitetit është një atribut fakultativ i përkrahur nga të gjitha implementimet BGP. Ai është përdorur tashmë për të koduar lloje të ndryshme të informacionit opsional (STR06). Është përcaktuar komuniteti i zgjeruar Peerings Virtual që përmban adresën IP të VPC që është përgjegjës për të lidhur prefikset dhe një grup të flamujve bit që tregojnë llojet e tuneleve që mund të përdoren për të krijuar një Virtual Peering. Për arsye teprice, një AS mund të përdorë disa VPCs. Në këtë rast, ai thjesht i bashkangjit disa komunitete të zgjeruara Peerings Virtuale për rrugët BGP që kishte krijuar. Në shembullin e Fig.3.31, rrugët BGP drejt prefiksit 1.0.0.0/8 të shpallura nga RAS do të përmbajnë adresën IP 1.1.1.9 në komunitetin Virtual Peering. Rrugët BGP e reklamuar nga SAS për prefiksin 2.0.0.0/8 do të përmbajnë 2.0.4.17, adresën IP e VPC SAS-së.

3.8.4 Krijimi dhe heqja e Peerings Virtual

Për të kërkuar ngritjen e Peerings Virtual, duhet të shkëmbehen disa mesazhe mes VPC të RAS dhe VPC të SAS -së. Në vend të përcaktimit të një protokollit të ri sinjalizimi nga e para për të krijuar Peerings Virtual, është përdorur një seksion eBGP multi-hop midis dy VPCs2. Ky sesion është përdorur nga VPC të RAS për të dërguar mesazhe për VPC SAS -së. Është quajtur ky seksion Virtual Peering Session. Mesazhet e shkëmbyera gjatë një sesioni Peering Virtual nuk janë përhapur drejt routerave BGP të tjera.

Dy llojet e mesazheve BGP janë shkëmbyer gjatë një Sesioni Peering Virtual :

Krijimi Virtual Peering (Virtual Peering Establishment) dhe Shkarkimi Virtual Peering (Virtual Peering Removal). Krijimi Virtual Peering (VPE) është një mesazh BGP Update i dërguar për të kërkuar ngritjen e një Virtual Peering ose të ndryshojë parametrat e një Virtual Peering ekzistuese. VPE-të e dërguara nga VPC e RAS gjatë seancës Virtual Peering duhet të përmbajnë dy prefiksë destinacioni (1.0.0.0/8 në rastin e Fig.3.31) dhe

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

informacionin e kërkuar për të krijuar tunele, duke përfshirë tunelin tail-end. Ky informacion mund të kodohet duke përdorur tunelin Subsequent Address Family Identifier (SAFI) i propozuar në (NKTW05). Ky propozim përcakton një lloj të ri të familjes së adresave që lejon të bashkëngjiti informacionin tunel me prefikset e reklamuar. Kodimi i propozuar në (NKTW05) ju lejon të specifikoni parametrat për llojet e ndryshme të tuneleve. Për shembull, një rrugë tunel duke treguar një tunel GRE mund të përmbajë çelësin e nevojshëm dhe seksionin e ID (Dom00), ndërsa një rrugë tunel që tregon një tunel L2TPv3 do të përmbajë cookie kërkuar. Për më tepër, disa lloje të tuneleve mund të jenë bashkëngjitur në çdo rrugë të tuneleve.

Kur reklamohen rrugët tunel, një VPC mund të kërkojë Peerings Virtual të dallueshme nga reklamimi i prefikseve të ndryshme me tunele të ndryshme të lidhur 'tail-ends'. Një Virtual Peering Removal (VPR) është një mesazh BGP Withdraw i dërguar në mënyrë që të mbyllë një Virtual Peering ekzistues. VPRs i dërguar nga RAS i VPC do të përmbajnë vetëm prefiksën për të cilin Virtual Peering duhet të mbyllet dhe kanë të bëjnë me të njëjta familje adresash . Kur një VPR është marrë nga një VPC, ajo kontakton tunel head-ends që të mbyllë tunelet për prefiksën e dhënë .

3.8.5 Shpërndarja e rrugëve Virtual Peering brenda fushës domain

Shpërndarja në domainin e rrugëve të mësuar nëpërmjet Virtual Peering është bërë nga një Virtual Peering Tunnel Route (VPTR). Një VPTR është një mesazh normal BGP Update që VPC i dërgon routerave kufitare në mënyrë që të shpërndajë rrugët tunel të marra në një VPE. VPTRs janë dërguar mbi seksionet genuine iBGP që VPC ka krijuar me routerat kufitare. Çdo VPTR përmban një prefiks, një tunel tail-end dhe lloji i tunelit të kërkuar. VPTR përdorin një familje të ndryshme adresash, në mënyrë që të dy adresat e IPv4 normale dhe rrugët tunel mund të reklamohen më shumë se në një seancë të vetme BGP. Përzgjedhja e routerave më të mirë kufitarë për të shërbyer si head-end Virtual Peering në SAS mund të varet se si SAS do të optimizojë trafikun e tij interdomain. Në praktikë, ky vendim do të merret nga VPC. Dy qasje janë të mundshme. Në qasjen e parë, vetë VPC mund të mësojë rrugët eBGP e njohura nga çdo router kufi. Meqë ajo ka një sesion iBGP me çdo router kufi, kjo është e lehtë. VPC pastaj mund të masë cilësinë e çdo rrugë eBGP në bazë të kriterëve të paracaktuara duke kërkuar çdo router kufi për të kryer matje të vonesës dhe bandwidth-it duke përdorur një teknikë të tillë si (Sys04). Për shembull, ajo mund të masë vonesën e rrugëve apo bandwidth-in maksimal në dispozicion përgjatë rrugës. Bazuar në rezultatet e matura, VPC pastaj mund të zgjidhë routerin më të përshtatshëm kufitar. Qasja e dytë konsiston në krijimin e tuneleve të shumta. VPC duhet pastaj të zgjedhë routerat e shumtë kufitarë që do të shërbejnë si tunel head-tail. Kjo qasje është interesante në qoftë se SAS ka peerings të shumtë me ofruesit e saj, të vendosur në vende shumë të largët. Në këtë rast, mund të jetë interesante për të ndërtuar tunele duke u nisur në secilin prej këtyre peerings në mënyrë që të favorizojnë rrugëzimin hot-patate. Pas pranimit të një VPTR çdo router kufitar përcakton nëse ka një rrugë eBGP më të mirë për të arritur tunelin tail-end në tabelën e tij të

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

rrugëzimit BGP. Në atë rast, router kufi mund të shërbejë si një tunel head-tail për paketat të dërguara drejt këtij prefiksi. Për shembull, në shembullin e Fig. 3.31, R22 ka mësuar nga AS Y një rrugë eBGP drejt prefiksit të routerit tail-end R12. Routeri R12 ka adresën IP 10.0.0.12 që i takon prefiksit 10.0.0.0/8 të dala nga AS Z. Pasi është themeluar tuneli, routeri kufi reklamon përmes iBGP një rrugë të re që tregon se ajo mund të arrijë prefiksin destinacion, dmth 1.0.0.0/8. Kjo rrugë ka një lokale-pref më të lartë për të detyruar fqinjët e tjerë iBGP të preferojnë atë mbi rrugët e marra jashtë Virtual Peering. AS-Path e kësaj shpalljeje përmban AS-Path e rrugës që routeri kufi përdor për të arritur në tunelin tail-end, dmth Y: Z: 1. Nëse nuk ka rrugë për të arritur tunelin tail-end eBGP (kjo mund të jetë për shkak të politikave të BGP), routeri kufi nuk do të shërbejë si një tunel head-end për paketat e dërguara drejt këtij prefiksi. Në supozojmë se në një rrjet IP tipik, vetëm një pjesë e routerave kufitare do të jenë në gjendje për të shërbyer si tunele head-tail. Kjo mund për shembull, të varet nga llojin i ndërfaqeve të instaluar në çdo router. Për të lejuar VPC të dijë routerat që janë të aftë për krijimin e lidhjeve Virtuale Peering, ne supozojmë se secili router tregon në gjendjen e lidhjes IGP të paketave që ajo krijon llojet e tuneleve që mbështet, nëse ka ndonjë të tillë. Për IS-IS, kjo mund të jetë e koduar duke përdorur TLV aftësinë e përcaktuar në (VSA06). Bazuar në databazën e gjendjeve të saj të lidhjeve, VPC kështu mund të përcaktojë lehtë aftësitë e të gjitha routerave kufitare brenda AS të saj.

3.8.6 Konsiderata të sigurisë

Nga pikëpamja e sigurisë, qasja Peerings Virtual e propozuar në këtë kapitull ekspozon dy çështje të mëdha. Së pari, mesazhi VPCA reklamon në internet global adresat IP të VPC-ve të bashkangjitura në një prefiks. Nëse një sulmues mund të modifikojë përmbajtjen e komuniteteve të zgjeruara Peerings Virtual në reklamën BGP duke kaluar nëpër një (transit) router , ai mund të ripërcjellë kërkesat Virtuale Peering tek një tjetër makinë. Kjo mund të çojë në sulme ridrejtimi të trafikut. Megjithatë, duhet të theksohet se në qoftë se një sulmues është në gjendje të modifikojë mesazhet BGP, shumë lloje të sulmeve janë të mundshme me BGP standarde që është dislokuar sot. Për të shmangur këtë problem, zgjidhja më e mirë është që të përdoret një nga zgjerimet BGP të propozuara në (Whi03 , KLS00), që të lejojë autentifikimin e reklamave BGP. Nëse këto zgjerime nuk mund të përdoren, një zgjidhje e mundshme është të sigurohemi që adresat IP e VPC-ve i takojnë prefiksit të reklamuar .

Çështja e dytë është për shkak të VPEs . Kur merr një VPE , një VPC duhet të jetë në gjendje për të verifikuar se RAS është i autorizuar për të reklamuar ato prefikset dhe tunele tail-ends. Përndryshe , një sulmues lehtësisht mund të ripërcjellë paketa të dërguara nga SAS në ambientet e tij në vend të një tail-end në RAS . Ky verifikim mund të bazohet në regjistrat e ndarjes së adresave në dispozicion të publikut të tilla si Arin ose RIPE. Disa ISP- të mëdha , sidomos në Evropë, tashmë përdorin ato bazat të të dhënave për të filtruar rrugët e shpallur nga kolegët(peers) e tyre dhe konsumatorët. Këto teknika

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

mund të përdoren edhe nga VPC-të. Në afat të gjatë , shtesat e sigurisë BGP duke u zhvilluar nga IETF (Whi03 , KLS00) do të trajtojnë këtë problem .

3.8.7 Vendosja

Arsyetimi për hartimin e protokollit të përkthuar në këtë seksion është për të bërë të mundur një vendosje në rritje. Meqë protokollin nuk kërkon modifikime në AS-ët e ndërmjetëm, dy domaine mund të fillojnë të përdorin atë për të negociuar Virtual Peerings. Për më tepër, brenda një domaini të vetëm, vetëm një nëngrup routerash kufitare duhet të përditësohen në mënyrë për të mbështetur VPTRs. Përveç kësaj, VPC mund fillim të zbatohet në një workstation të veçantë dhe më vonë do të vendoset brenda një routeri të vërtetë BGP ose rrugë-reflektor. Së fundi, ndërsa zgjerimet e sigurisë BGP (Whi03, KLS00) ende nuk janë të vendosur në internetin global, do të ishte më e lehtë për t'i përdorur ato në mes të VPCs pasi do të jenë më pak VPC sesa routerat normalë BGP dhe VPC-të nuk rishpërndajnë VPE-të e marra nga seksionet Virtual Peering në AS-të e tjerë. Një skemë e mundur vendosjeje do të ishte që fillimisht të fillojë duke përdorur Peerings Virtual në mes të një numri të vogël universitete apo laboratorësh kërkimore. Më pas, zgjidhja natyrisht mund të vendoset nga ofruesit e përmbajtjes dhe qasjes po ashtu.

3.8.8 Forca

Pasi peering virtual është themeluar, ai do të përdoret për të mbartur paketa. Gjatë operacionit të peering virtuale, mund të ndodhin disa ngjarje. Së pari, burimi ose destinacioni AS mund të dëshirojë, për ndonjë arsye, për të përfunduar peering virtual. Kjo mund të arrihet duke ndërprerë seancën e Peering Virtual dhe duke treguar se arsyeja për dështimin në mesazh e dërguar BGP NOTIFY. Së dyti, dështimet dhe ndryshimet në rrugën interdomain të ndjekura nga peering virtuale nga head-end në tail-end mund të ndikojnë në funksionimin e tij. Për të përballuar ato ngjarje, tuneli (head-end)kreu-fund duhet të përdorë një protokoll zbulimi dështimesh të tilla si Bidirectional Forwarding Detection (BFD) (KW06). BFD mund të përdoret në mjedise të ndryshme dhe është në gjendje për të zbuluar të dy dështimet e lidhjeve dhe dështimet tunel. Pasi BFD në tunelin kokë-fund(head-end) ka zbuluar një dështim të peering virtuale, tuneli kokë-fund (head-end) duhet të tërhiqë rrugët iBGP që njoftoi prefikset e arritshme nëpërmjet peering virtual. Kjo tërheqje do të detyrojë routerat e tjerë e të AS oser të kalojnë në një tjetër peering virtual tail-end që është ende në gjendje për të arritur në prefiksin destinacion ose në një rrugë normale BGP.

Një tjetër ngjarje që mund të ndodhë është dështimi i seancës Peering Virtual hedhur në mes të VPC në RAS dhe VPC në SAS. Ky dështim mund të zbulohet në të njëjtën mënyrë si një seancë të vërtetë BGP, dmth duke u mbështetur në mesazhet BGP KEEP_ALIVE. Kur VPC në SAS zbulon që seanca Peering Virtual është e dështuar, ajo vepron sikur të ishte pranuar një VPR. Ai tërheq VPTR-të e reklamuar më parë brenda domainit. Një mënyrë për të qenë e fuqishme në dështimin të një seksioni Peering Virtual

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

është që të ketë të paktën dy VPC në çdo domain dhe të veçojë seksionet Peering Virtual mes tyre. Çdo VPC në SAS, pra, do të marrë një VPE për secilin prefix destinacion dhe reklamuar VPTR-të korresponduese me routerat kufitare. Çdo router kufi do të marrë dy VPTR-të. Në qoftë se një seksion Peering Virtual dështon, një nga VPTR-të do të tërhiqet, por tjera do të mbetet. Kjo punë zgjidhet në qoftë se shkak i dështimit të seancës Peering Virtual nuk ndikon seksionet e tjera Peering Virtual. Nëse të dy seksionet ndjekin të njëjtën rrugë në internet, ata ndajnë njëjtat rreze. Së fundi, për të shmangur një pikë të vetme të dështimit, një praktikë e mirë operacionale do të jetë për të vendosur dy VPC-të e tepërta në një AS.

3.8.9 Vlerësimi

Për të treguar përfitimin e mundshëm të përdorimit Peerings virtuale për të shfrytëzuar rrugët ndaj ofruesit të domain destinacion , është kryer një simulim bazuar në tabela reale rrugëzimi BGP të mbledhura nga projektet RouteViews (Mey05) dhe (RIP05). Tabela e rrugëzimit nga RouteViews të përmbajtura në 5,750,380 rrugët e marra nga 34 peer-ët e ndryshëm. Në simulim, ne konsiderojmë vetëm 32 peers-ët që shpallën një tabelë të plotë rrugëzimi , dmth më shumë se 140.000 rrugë. Tabela e rrugëzimit RIPE ishte mbledhur nga RRC00. Ajo përmbante 1,641,618 rrugët e shpallura nga 11 peers-ët. Të gjitha këta peers-ë njoftuan më shumë se 140.000 rrugë. U përmblohdën grupet e të dhënave në Tabelën 3.

Tabela 3: Përmbledhja e RouteViews dhe RIPE datasets.

Dataset	Routes	Peers	Pairs	M-h stubs	M-h prefixes
RouteViews	5,750,380	32 (34)	496	6,402	29,575
RIPE RRC00	1,641,618	11	55	6,247	29,934

Ndër të gjitha rrugët e marra, janë identifikuar, në bazë të shtigjeve AS(AS-paths), 6402 multihomed stub-ë që reklamojnë 29,575 prefixe të ndryshme për dataset-ët e RouteViews dhe 6,247 multi - homed stub-ë që reklamojnë 29,934 prefixet për dataset-ët RIPE. Më pas mund të merren në konsideratë të gjitha palët e peers-ëve të pranishëm në çdo dataset . Ka 496 palë peers-ë të ndryshme në dataset-et RouteViews dhe 55 çifte të ndryshme në dataset –et RIPE. Ne simuluar një domain të dyfishtë - homed stub të lidhur me peers-ët e përzgjedhura. Për çdo stub të simuluar, u llogaritën numri i rrugëve të ndryshme të mësuara nga BGP ndaj të gjithë prefixeve të marra në konsideatë të destinacionit. U konsideruan se dy rrugë janë të ndryshëm, nëse të paktën ofruesi në burimin AS ose ofruesi në destinacionin AS janë të ndryshëm. Vini re se në qoftë se dy rrugë janë të ndryshme , kjo nuk do të thotë se ata janë plotësisht të veçuar.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Janë tregojmë rezultatet e simulimeve në Fig.3.32. Shifrat tregon shpërndarjen e numrit të rrugëve të ndryshme në dispozicion gjatë përdorimit të rrugëve BGP drejt domainit destinacion dhe kur duke përdorur Peerings virtuale, për të gjitha prefikset e destinacionit. Në boshtit x, është treguar numrin e rrugëve të ndryshme në dispozicion dhe nga ana aksit-y, numri i prefikseve që mund të arrihen me numrin korrespondues të rrugëve. Është treguar mesatarja, përqindëshin e 10-të dhe e 90-të e numrit të prefikseve meqë kjo është një përmbledhje për 496 çifte në rastin e RouteViews dataset dhe 55 çifte në rastin e RIPE dataset. Lehtësisht mund të vërejmë se ka pasur pak ndryshim mes çifteve të ndryshme meqë përqindjet janë afër mesatares. Kur sheh në shtigjet BGP ndaj destinacionit AS, numri i dallueshëm i shtigjeve përbëhet në mes të 0 dhe 2. Nëse nuk ka shteg, do të thotë se prefikset e destinacionit nuk mund të arrihen. Kjo për fat të mirë ndodh për vetëm një nëngrup të vogël të RouteViews dataset. Kjo është ndoshta për shkak të filtrave të përdorura nga disa ISP-të. Nëse ka vetëm një rrugë, që do të thotë se prefiksi i destinacionit nuk ishte arritur me një nga ofruesit. Por pjesa më e madhe e kohës, prefikset e destinacionit ishin të arritshme nëpërmjet dy ofruesve. Numri i rrugëve në dispozicion BGP nuk mund të jetë më shumë se 2 meqë nga stub-ët e simuluar janë dual-homed. Prandaj, ata vetëm marrin një rrugë të vetme për çdo prefiks destinacioni nga çdo ofrues. Për më tepër, është e shpeshtë që këto rrugë të bashkohen në të njëjtën ofrues destinacioni AS. Diversiteti i rrugës është i ulët me BGP edhe në qoftë se ka dy rrugë të ndryshme pjesën më të madhe të kohës.

Nëse ne shikojmë në rrugët që do të merren duke përdorur Peerings Virtuale, diversiteti i rrugëve rritet shumë. Shumica e prefikseve të destinacionit (67.6% për RouteViews dhe 69.9% për RIPE) janë të arritshme nëpërmjet të paktën 4 rrugëve të ndryshme. Ka edhe një numër të konsiderueshëm AS-sh destinacion që janë të arritshme nëpërmjet 6 rrugëve (14.9% për RouteViews dhe 14.5% për RIPE) ose edhe më shumë për shkak të disa stub-ve destinacion të qenë më shumë se dual-homed.

Arsyeja për shumicën e madhe të prefikseve të destinacionit që kanë numër çift të rrugëve të ndryshme është se stub-i burim është dualhomed . Simulimet tregojnë se duke përdorur rrugët drejt ofruesve të domain-ve destinacion sjell shumë të rrugë të reja . Një rregull mund të rrjedhë nga ky vëzhgim : numri i rrugëve të nxjerra nga Virtual Peerings $ISM \times N$, me M (resp . N) numri stub i ofruesve të burimit (resp . destinacion). Një studim i ngjashëm është kryer në kuadrin e një vlerësimit të zgjidhjeve IPv6multihoming(shih (dLBL03, dLQB06). Me IPv6 multi- homing, çdo sistem fundor merr disa adresa IPv6, nga një për ofruesin e AS të saj. Duke zgjedhur adresën që ai përdor për të arritur një destinacion, çdo host në mënyrë indirekte mund të zgjedhë rrugën interdomain të përdorur. Me IPv6, është i mundur pa përdorur peerings virtuale një kontroll determinist të shtigjeve interdomain.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

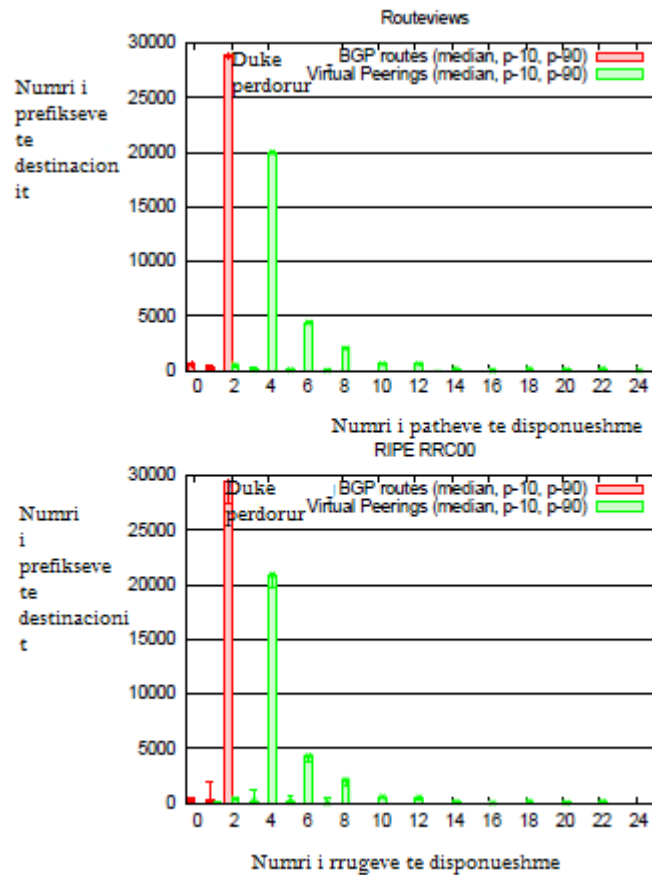


Figura 3.32: Diversiteti i rrugëve të përftuara gjatë multihoming në RouteViews ose RIPE peers.

a) Balancimi i trafikut hyrës

Në këtë seksion, është përshkruar se si Peerings Virtual mund të përdoret për të balancuar ngarkesën e trafikut në hyrje në lidhjet e aksesit të një domaini stub. Për të arritur një balancim të mirë të trafikut përbrenda inbound, stub-i AS ka nevojë për të monitoruar trafikun e marrë në çdo lidhje qasjeje. Kjo mund të bëhet duke aktivizuar NetFlow në ndërfaqet e routerave kufitare dhe duke mbledhur statistikën e trafikut në një workstation të dedikuar (VE04). Më pas, bazuar në statistikën e trafikut të kombinuar me një algoritëm optimizimi, AS stub identifikon AS-të burim që duhet të lëvizin. Për çdo burim AS përkatës, është themeluar një Peering Virtual. Nëpërmjet Peering Virtual, destinacioni i kërkon burimit AS për të përmbledhur trafikun e saj në një tunel drejt një lidhje të caktuar të qasjes.

Është treguar se kjo zgjidhje është e mundur dhe se me një numër të kufizuar Virtual Peerings, është e mundur për të arritur një ekuilibër të përsosur në afërsi të ngarkesës të

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

trafikut përbrenda inbound. Është kryer vlerësimi në dy hapa. Së pari, është simuluar çekuilibrin e trafikut në stubin që duam të optimizohet. Pastaj, për çdo stub të marrë në konsideratë, në të ekzekutohet një algoritëm optimizimi i cili përcakton Peerings Virtual që janë të nevojshme për të lëvizur burimet e trafikut të stub-it dhe të marrë një ekuilibër më të mirë të trafikut të tij inbound. Janë përshkruar këto dy hapa në seksionet pasuese, më pas janë paraqitur rezultatet.

Skenari b) Simulimi

Është përdorur një skenar simulimi të ngjashëm me atë të Kapitullit 2, bazuar në topologjinë e internetit të nxjerrë nga (SARK02) nga tabela reale rrugëzimi BGP të mbledhura nga pikat e shumta të favorshme, kryesisht në bërthamën e internetit. Topologjia daton që nga 10 shkurt, 2004 dhe përmban 16,921 domain-e dhe 37,271 lidhje interdomain. Është më së shumti një lidhje midis dy domain-eve të ndryshme dhe çdo lidhje përfaqëson marrëdhënien e biznesit që ekziston mes dy domain-eve që lidh. Marrëdhëniet e mundshme janë *customer-provider* dhe *peer-to-peer*. Është përdorur C-BGP dhe modelojmë çdo domain si një router të vetëm BGP. Ne përkthejmë marrëdhëniet e biznesit midis domain-eve në politikat e rrugëzimit e konfiguruar në çdo router. Këto politika janë të përbëra nga dy pjesë. Pjesa e parë zbaton të ashtuquajturën rregullin e ksporit selektiv (Gao00) dhe pjesa e dytë zbaton preferencën që një domain ka për rrugët e mësuara gjatë marrëdhënieve të ndryshme (Gao00). Për të siguruar një përfaqësim të mirë, simulimet janë kryer për një numër të madh të stub-ve. Janë marrë në konsideratë 1000 dual-homed stub-e, 1000 3-homed stub-e, 295 4-homed stub-e, 101 5-homed stub-e dhe 49 6-homed stub-e. Kjo korrespondon me 29% të multi-homed stub-ë në internetin e sotëm. Duke përdorur C-BGP, janë llogaritur rrugët e përdorura nga të gjitha fushat domain për të arritur në stub-ët e zgjedhur. Llogaritja është bërë në mënyrë të shpërndarë, duke e marrë në konsideratë një prefiks destinacion në një kohë, siç shpjegohet në seksionin e sipërm.

c) Çekuilibri topologjik dhe çekuilibri i trafikut

Ka dy shkaqe kryesore strukturore të çekuilibrit të trafikut inbound të marrë nga një domain stub. Ne e quajmë shkakun e parë mosbalancim topologjik. Çekuilibri topologjik është një çekuilibër në numrin e rrugëve përbrenda që arrijnë stub-in destinacion me anë të secilit prej ofruesve të saj. Ky çekuilibër është për shkak të vendimeve të marra nga rrugëzimi BGP në domain-e të largëta. Rëndësia e çekuilibrit varet nga lidhja e domain-ve stub dhe në kufizimet e rrugëzimit të politikës. Pasoja e mosbalancimit topologjik është se burimet e trafikut të arritura në stubin destinacion nëpër rrugë të ndryshme përfshijrë kështu ofrues të ndryshëm .

Është treguar çekuilibër topologjik fillestar të parë nga domain-et stub të marra në konsideratë në simulim tonë në Fig. 3.33. Është përcaktuar çekuilibri topologjik si numrin maksimal të rrugëve të marra nga një ofrues i pjesëtuar me numrin mesatar të rrugëve. Për shembull, një stub dual-homed që është arritur me 75% të rrugëve të tij të

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

brendshme (inbound) nëpërmjet një ofruesi dhe 25% nëpërmjet ofruesit tjetër ka një çekuilibër topologjik të $75/50 = 1.5$. Në boshtin x të Fig. 3.34, është treguar çekuilibri topologjik dhe, nga ana në aksin-y, tregojmë pjesë kumulative të stub-ve cung që shohin çekuilibrin përkatës. Shifra tregon pesë kthesa. Një e sipërme ka të bëjë me stub-ët 2-homed. Është vëzhguar se gati 50% e stub-ve 2-homed kanë një çekuilibër topologjik më të madh se 1.6, që do të thotë se këto stub-ë kanë një ofrues që merr më shumë se 80% të rrugëve. Për stub-ët 3-homed (kurba e dytë), 50% e tyre kanë një çekuilibër topologjik që është më i madh se 2.1, që do të thotë se këto stub-ë kanë një ofrues që merr më shumë se 70% të rrugëve. Kthesa e pasuar tregon çekuilibër topologjik për stub-ët 4-homed, stub-ët 5-homed dhe stub-ët 6-homed. Për stub-ët 4-homed, mosbalancimi mesatar topologjik është më i madh se 2.3, për stub-ët 5-homed, ai është afër 2.7 dhe për stub-ët 6-homed, ai është afër 2.8.

Mosbalancimi topologjikal duhet të kombinohet me çekuilibrin e trafikut . Kjo do të thotë se të gjitha burimet nuk do të dërgojnë të njëjtën volum trafik në stub-et destinacion . Shpërndarja e vëllimit të trafikut në burim është zakonisht shumë anuese . Në mënyrë tipike, një numër i vogël As-sh janë përgjegjëse për një pjesë të madhe të trafikut të marrë (QUP + 03 , UB02 , FBR03). Për të modeluar shpërndarjen e trafikut në këtë topologji, është caktuar trafiku në të gjitha burimet pas shpërndarjes aWeibull me parametrin e formave i _ barabartë me 0.5. Me këtë shpërndarje , rreth 1000 burime janë përgjegjëse për 95 % të trafikut të marrë nga një stub AS. Kjo i përshtatet shumë mirë me shpërndarjen e trafikut të treguar në (FBR03) dhe (UBQ03b) dhe referencat e tjera .

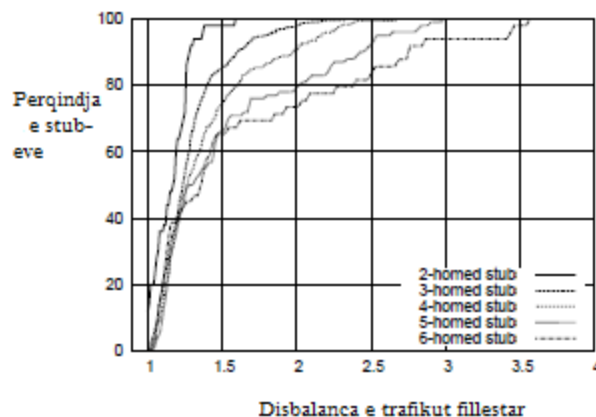


Figura 3.33: Disbalancë e trafikut Inicializues ($\alpha = 0.5$).

Janë përdorur ato shpërndarje të trafikut për të peshuar shtigjet e njehsuara nga C-BGP. Duke bërë këtë, është marrë shpërndarja e trafikut në hyrje për secilin nga 2445 domain-et stub të marra në konsideratë 2445. Fig. 3.33 tregon shpërndarjet e çekuilibrit të trafikut në mesin e të gjitha atyre domain-ëve stub. Është përkufizuar çekuilibri i trafikut si volumin e trafikut të marrë nga ofruesi më i ngarkuar i pjesëtuar me vëllimin e trafikut të dobët. Në aksin-y, tregohen fraksione kumulative të stub-ëve që kanë çekuilibër përkatës.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Fig.3.33 tregon çekuilibër trafiku për stub-et që kanë 2 deri në 6 ofrues (provider). Vërejmë në kurbën e parë se më pak se 25% e stub-eve të dual-homed kanë trafikun e tyre inbound të ekuilibruar mbi ofruesit e tyre, që është me një çekuilibër më të vogël se 1.01. Për më tepër, më shumë se 35% e stub-eve dual-homed kanë një çekuilibër më të lartë se 1.2, që do të thotë se 35% e stub-eve dual-homed kanë një ofrues që merr më shumë se 60% të trafikut. Ndër stub-et që kanë 3 ofrues, rreth 60% kanë një çekuilibër më të madh se 1.2. Diskutimet me ISP tregojnë se të tilla pabarazi të e mëdha të trafikut janë të zakonshme.

d) Përzgjedhja e Peerings Virtual

Kërkimi për një rindarje më të mirë të trafikut është një problem optimizimi i cili konsiston në ndarjen e një lidhjeje qasjeje për çdo burim të trafikut. Ky është një problem kombinatorik. Numri i detyrave të mundshme të N burimeve në M lidhje të aksesit është M^N . Për një stub dual - homed ($M = 2$) dhe në rendin e 15.000 burimeve, ky numër është tashmë i madh. Disa teknika mund të përdoren për të zgjidhur këtë problem. Ne mund të zgjedhim të përdorim teknikat Computing evolutiv (ES03) të zbatuara me ndihmën e bibliotekës Gaudi (Adc04). Ne zgjedhim një algoritëm evolucionar për të zgjidhur këtë problem, sepse ajo është e mundur për të zgjeruar atë për të mbështetur objektivat e shumta (Deb01) dhe kjo teknikë tashmë është aplikuar për të zgjidhur probleme inxhinierimi trafiku interdomain të ndryshme (UBQ03b).

Algoritmi i dhënë evolucionar (Alg. 4) mbështetet në një popullsi të individëve, që është një grup i zgjidhjeve të mundshme që zhvillohet në kohë. Në popullsinë, një individ paraqet një detyrë të veçantë të burimeve N mbi M lidhjet e aksesit të destinacionit. Një individ është kështu një vektor (l_0, \dots, l_{N-1}) të N integer-ave $0 \leq l_j < M$ ku çdo p_j është identifikuesi i lidhjes së qasjes të përdorur nga burimi j për të hyrë në rrjet. Ne inicializojmë popullatën me individë që përfaqësojnë gjendjen fillestare BGP, që është, një individ përfaqëson lidhjen e aksesit të përdorur nga burimet N. Në praktikë, një rrjet stub nuk ka nevojë të njohë rrugët interdomain të përdorura nga çdo burim AS. Pra mund të përdorim NetFlow në routerat e vet kufitare dhe të mbledhë statistikën e trafikut [VE04] për të përcaktuar se cili burim AS është marrë mbi cilën lidhje aksesit. Para fillimit të optimizimit, algoritmi pak turbullon individët fillestarë. Në këtë mënyrë, nuk do të fillohet me një popullsi prej individëve identikë. Turbullimi i një individi konsiston në zëvendësimin e lidhjes së aksesit të një burimi të zgjedhur rastësisht nga një lidhje e aksesit të zgjedhur rastësisht.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Alg. 4 Algoritmi I Optimizimit

```
Let  $N$  be the number of sources
Let  $M$  be the number of access links
Let  $(l_j)_{0 \leq j < N}$  be the initial access link used by each source
Let  $(v_j)_{0 \leq j < N}$  be the traffic volume sent by each source
1: /* Initialize population with  $2N$  individuals */
2:  $pop \leftarrow \emptyset$ 
3: for  $k = 0$  to  $2N - 1$  do
4:    $pop \leftarrow pop \cup mutate((l_0, \dots, l_{N-1}))$ 
5: end for
6: /* Evaluate fitness of individuals */
7:  $evaluate\_fitness\_pop(pop)$ 
8: /* Main loop, each generation updates the population */
9: while ( $generation < MAXGEN$ ) do
10:  /* Crossover with probability 0.1 */
11:   $crossover\_pop(pop)$ 
12:  /* Mutation of individuals with probability 0.9 */
13:   $mutate\_pop(pop)$ 
14:  /* Evaluate fitness of individuals */
15:   $evaluate\_fitness\_pop(pop)$ 
16:  /* Terminates if a good individual is found */
17:  if ( $\exists k : pop[k]$  satisfies termination criterion) then
18:    break
19:  end if
20:  /* Select best individuals based on fitness */
21:   $select(pop)$ 
22: end while
```

Alg. 5 Mutate individual (l_0, \dots, l_{N-1})

```
1: /* Choose a random access link  $i$  */
2:  $i = rand(M)$ 
3: /* Choose a random source  $j$  */
4:  $j = rand(N)$ 
5: /* The new access link used by source  $j$  is  $i$  */
6:  $l_j \leftarrow i$ 
```

U rregullua madhësia e popullsisë, në mënyrë empirike, me dyfishin e numrit të burimeve të marra në konsideratë. Numri i burimeve të marra në konsideratë varet nga shpërndarja e vëllimit të trafikut. Në këto rezultate, algoritmi konsideron burimet e nevojshme për të mbuluar 95% të vëllimit të përgjithshëm të trafikut. Kjo është, $N = 942$ burime ishin marrë parasysh. Gjatë evolucionit të popullsisë, janë kryer mutacione dhe mbikalime. Në algoritmin tonë, një mutacion konsiston në ndryshimin lidhjen e aksesit të një burimi të

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

zgjedhur rastësisht (shih ALG. 5). I referohemi lexuesit për (ES03) për një shpjegim të operacionit të mbikalesës.

Pas çdo gjenerimi të popullsisë, individët janë vlerësuar me një funksion përshtatshmërie. Funksioni i përdorur në algoritmin tonë (Alg. 6) mat për një individ devijimin që ai shkakton në terma të balancimit të ngarkesës. Formalisht, në mënyrë që të matim përshtatshmërinë e një individi x , algoritmi së pari llogarit përqindjen e trafikut L_i që do të marrë nga çdo lidhje aksesi i nëse konfiguracioni i përfaqësuar nga individi x është zbatuar me Peerings Virtual. Pastaj, funksioni llogarit distancën L_2 midis vektorit $(L_i)_{0 \leq i < M}$ dhe ekuilibrit. Ekuilibri paraqet rastin kur çdo lidhje aksesi merr një përqindje të barabartë të trafikut të $1 / M$. Së fundi, një përzgjedhje do të kryhet bazuar në përshtatshmërinë e individëve. Individët që më së miri përshtaten me objektivin mbahen, ndërsa të tjerët hiqen.

Alg. 6 Compute the fitness of individual (l_0, \dots, l_{N-1})

```
1: /* Compute the load vector  $(L_i)_{0 \leq i < M}$  */
2: for  $i = 0$  to  $M - 1$  do
3:    $L_i \leftarrow \frac{\sum_{v_j: l_i = 1} v_j}{\sum_{0 \leq j < N} v_j}$ 
4: end for
5: /* Compute the L2 distance from the equilibrium vector */
6:  $fitness \leftarrow \sum_{0 \leq i < M} (L_i - \frac{1}{M})^2$ 
```

Është treguar në Fig.9.6 konvergjenca e algoritmit evolucionar për dy domain-e të ndryshme. I pari është një 3-homed stub. Shpërndarja fillestare e ngarkesës së trafikut është si vijon: ISP1 merr 17.59 % të trafikut, ndërsa ISP2 merr 53,58 % dhe ISP3 merr 28.82 % . Pas 38 brezave të popullsisë, algoritmi ka përzgjedhur 30 tunele të përcaktuara. Këto tunele të çojë në një shpërndarje të re të ngarkesës e cila është si më poshtë: ISP1 merr 33.33 % të trafikut, ISP2 merr 33,80 % dhe ISP3 merr 32.87 % . Kjo është pranë objektivit nga më pak se 1% dhe algoritmi përfundon . Domeni i dytë është një domen 4-homed. Ngarkesa fillestare e trafikut është si vijon: 17.60 % , 51,80 % , 19,27 % dhe 11.33 % . Algoritmi konvergon në një përzgjedhje të 55 tuneleve pas 55 brezave. Shpërndarja përfundimtare e ngarkesës së trafikut është 24.80 % , 25.50 % , 25,04 % dhe 24.66 % .

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

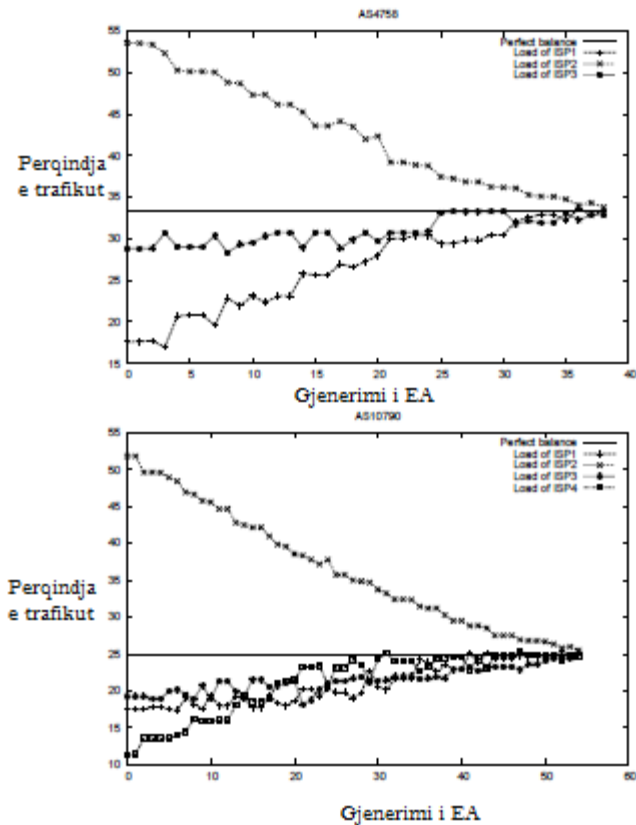


Figura 3.34: Konvergjenca e algoritmit revolucionarizues për stub-ë 3- dhe 4-homed.

e) Rezultatet

Është përdorur ky algoritëm evolutiv për të përcaktuar Peerings Virtual që secili prej 2445 stub-ët tona e marra në konsideratë do të duhet të vendosin një ekuilibër të përsosur ndër lidhjet e tij të aksesit me më pak se 1%. Kjo do të thotë se në rastin e një dual-homed stub për shembull, numri i tuneleve të nevojshme shkakton ofruesin më të ngarkuar që të mbartë më së shumti 50.9% të vëllimit të trafikut. Figura 5.7 raporton shpërndarjen kumulative të numrit të Peerings Virtual të vendosur nga të gjitha ata domain-e stub për t'iu qasur ekuilibrit të përsosur me më pak se 1%. Vëmë re se në rastin e stub-ve dual-homed, qëllimi është arritur me jo më shumë se 41 tunele për 90% të stub-ve. Në rastin e stub-ve 3-homed, jo më shumë se 42 tunele janë të nevojshme për të balancuar trafikun e 90% stub-ve. Së fundi, më pak se 50 tunele janë të nevojshme për të balancuar trafikun mes ofruesve të 90% të stub-ve 4-homed.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

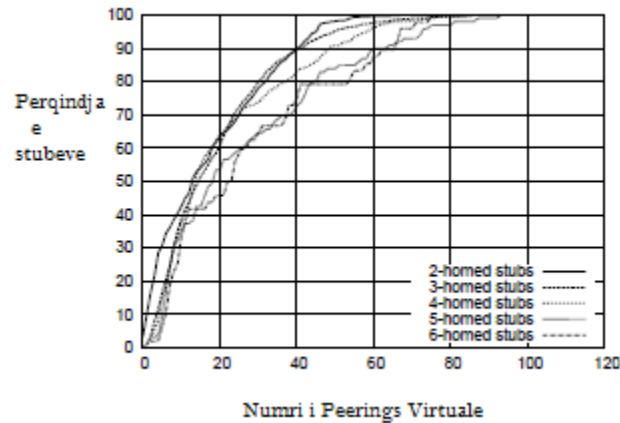


Figura 3.35-a: Numri i Virtual Peerings për të krijuar ($\alpha = 0.5$).

Është studiuar ndjeshmëria e teknikës në shpërndarjen e trafikut. U kryen të njëjtat simulime me një shpërndarje të trafikut që ndjek një Weibull me parametër $\alpha = 0.25$. Në këtë rast, situata është me të vërtetë e pafavorshme : 3000 burime As-sh prodhojnë 95% të trafikut të marrë nga një stub. Mosbalancimi i trafikut rezultat është treguar në Fig.3.36 dhe numri i tuneleve është treguar në Fig.3.37. Rezultatet e këtij simulimi tregojnë se numri i Peerings Virtual të nevojshme për të balancuar trafikun përbrenda rritet, por mbetet mjaft i ulët. Me $\alpha = 0.5$, ishte i mundur balancimi i ngarkesës thajse i përsosur me aq pak sa 43 tunele për 90% të stub-eve. Stub-ët e mbetur 10% kërkojnë mes 44 dhe 94 tunele. Me $\alpha = 0,25$, 43 tunele lejojnë një balancim të përkryer të ngarkesës prej 68% të stub-ve . Deri në 80 tunele janë të nevojshme për të mbuluar 90% të stub-ve . Pjesa e mbetur prej 10% e stub-ve ende ka vetëm nevojë për jo më shumë se 148 tunele për të balancuar trafikun e tyre përbrenda inbound .

Këto rezultate tregojnë se një inxhinierimi i trafikut inbound duke u mbështetur në Peerings Virtual është i mundur edhe me një shpërndarje të pafavorshme të trafikut . Për më tepër , me MultiObjective Computing Evolutionary (Deb01) do të ishte e mundur për të përcaktuar peerings optimale virtuale që minimizojnë të dyja dhe çekuilibrimet dhe numrin e tuneleve për të krijuar. Gjithashtu do të jetë e mundur për të kombinuar balancimin e ngarkesës me të tjera objektiva të tilla si reduktimi i vonesës por ne e lëmë këtë punë si të mëtejshme.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

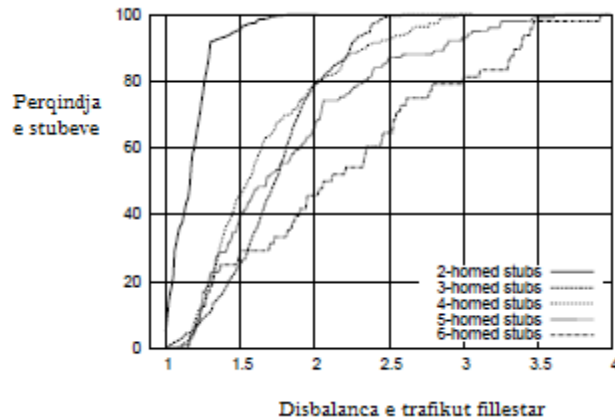


Figura 3.35-b: Çekuilibri fillestar i trafikut ($\alpha = 0.25$).

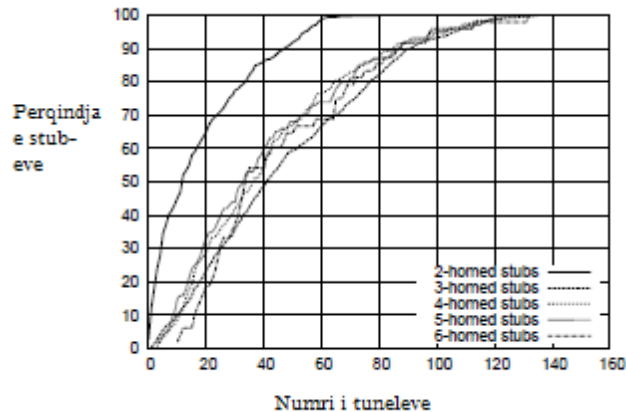


Figura 3.35-c: Number of Virtual Peerings to establish ($\alpha = 0.25$).

f) Përmirësimi i vonesës

Duke përdorur Peerings e dhura Virtuale, AS-të burim dhe destinacion mund të zgjedhin për të përcjellë trafikun mbi shtigjet që plotësojnë më mirë kërkesat e QoS së tyre. Në këtë seksion ne do të përqëndrohemi në zgjedhjen e rrugëve me vonesë më të ulët. Në mënyrë që të zgjidhni rrugën më të mirë sipas kësaj metrike, kemi nevojë për një mekanizëm që monitoron shtigjet e ndryshme në dispozicion për t'u bashkuar me peer-ët virtualë. Lind nevoja për të matur vonesën me-një-kalim për çdo rrugë në dispozicion. Matja e RTT nuk është e mjaftueshme meqenëse rrugëzimi mund të jetë asimetrik. Për fat të mirë, zgjidhjet standarde ekzistojnë për matjen e vonesës një-kalim të cilat janë diskutuar në kuadër të grupit punues Internet IP Performance Metrics (AKZ99 , ST04). Pajisjet e matjes së vonesave një-kalimshe janë gjithashtu në dispozicion në hardware të veçantë (FGK + 01), si dhe në routera (Sys04). Prandaj ne mund të konsiderojmë se matja e vonesës me një kalim e rrugëve në dispozicion është e mundur.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Në këtë seksion, vlerësohet përdorimin i Peerings virtuale për të reduktuar vonesën e rrugëve interdomain. Për këtë qëllim, është përdorur një skenar të dytë simulimi ku ne krahasojmë vonesën përgjatë rrugës BGP të zgjedhur nga një domain stub-i që të arrijë një tjetër domain stub në vonesën përgjatë rrugëve që mund të merren me peerings virtuale. Për të kryer këtë simulim, ne nuk mund të mbështetemi në të njëjtën topologji si në seksionin 2.4 pasi ajo nuk përmban vonesat përgjatë lidhjeve. Për më tepër, topologjia e përdorur në seksionin 2.4 përmban një router të vetëm per domain.

Në këtë kohë, nuk ka asnjë topologji realiste Internet- shkallë në dispozicion që përmban vonesa. Një zgjidhje e mundshme mund të jetë për të përdorur një topologji sintetike. Për shembull, Brite (MAMB01) bën të mundur gjenerimin e topologjisë me dy nivele (AS-sh dhe routerash) me vonesa. Për fat të keq, Brite nuk përmban një model të marrëdhënieve të biznesit interdomain. Një gjenerator topologjie me interes është GTITM. Autorët e tij kanë paraqitur në (CDZ97) një version të dytë të gjeneratorit të tyre që është menduar për të mbështetur politikën, por për fat të keq, ky version nuk është në dispozicion të publikut në këtë kohë. Së fundi, një tjetër gjenerator I quajtur Inet (JCJ00) ofron topologji me një shpërndarje shkallë më të saktë. Megjithatë, kjo nuk do të merret me marrëdhëniet e biznesit.

g) Një topologji me dy nivele me vonesa

Përsa i përket njohurive tona, nuk ekziston një topologji e përshtatshme plotësisht ideale në internet. Është ndërtuar realisht një topologji interneti që përmban vonesa, pesha IGP, lidhje interdomain të shumta dhe politikën BGP. Është përdorur topologji të nivelit AS të nxjerra nga Subramanian et al (SARK02) si një pikënisje. Kjo topologji përmban një pjesë të madhe të domain-ve të internetit si dhe marrëdhëniet e biznesit mes tyre. Për të ndërtuar një strukturë intradomain, kemi përdorur një bazë të dhënash komerciale (Max04), që siguron pasqyrimin gjeografik (gjerësi dhe gjatësi) në mes të blloqeve të adresave IP dhe vendeve në mbarë botën. Baza e të dhënave përmban 1,837,457 blloqe adresash IP të vendosura në 118,489 vende. Bazuar në këtë bazë të dhënash, ne ishim në gjendje të tregojmë se pikat e pranisë së domeneve gjenden në tabelën e rrugëzimit BGP. Për të identifikuar domain-in që reklamon çdo bllok, ne kemi përdorur tabela rrugëzimi të vërteta BGP të mbledhura në kuadër të projektit RouteViews (Mey05) në Universitetin e Oregon dhe daton nga 10 shkurt,2004. Këto tabela rrugëzimi përmbajnë 139,527 prefikset e krijuara nga 15,030 domaine të ndryshme. Për çdo pikë të pranisë, ne kemi vendosur një router në domain-in origjinë.

Pastaj, për të ndërtuar strukturën e brendshme për çdo domain, janë grupuar pikat më të afërta të pranisë së çdo domaini në grupe clusterash duke përdorur një metodë klasifikimi hierarkike duke përdorur metrikën Euklidiane të distancës. Më pas u lidhën të gjitha routerat e një clusteri së bashku. Pastaj, u lidhën të gjithë clusterat së bashku, duke përdorur routerat më të afërt për secilin cluster. Kështu morrëm një strukturë intradomain

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

me dy nivele. Bazuar në koordinatat e pikave fundore për çdo lidhje, ishin në gjendje për të llogaritur distancën dhe kështu vonesën e përhapjes përgjatë linkut. Përveç kësaj, pesha IGP që ne caktuam për lidhjet favorizon rrugëzimin hot-patate në kuptimin që lidhjet më të shkurtra u janë caktuar një kosto më e shkurtër se sa lidhjet e gjata. Për lidhjet interdomain, ne u mbështetëm në topologjinë e nivelit AS. Për çdo lidhje interdomain që gjendet midis dy domaineve në këtë topologji, kemi shtuar linqe interdomain të shumtë në topologjinë tonë. U caktua numri maksimal të lidhjeve(linqeve) interdomain midis dy domain-eve në $N = 5$ Pastaj, numri i lidhjeve interdomain në mes të dy domain-ve ishte llogaritur duke shumëzuar N me madhësinë e çdo domain-i dhe duke e pjestuar rezultatin nga katrori i madhësisë së domain-it më të madh në topologji. Iu shtua 1 në rezultatin për t'u siguruar se nuk ka të paktën një lidhje. Topologjia rezultuese³ përmban 39,343 routers, 103,829 lidhje dhe kërkon 400,148 seksione BGP.

Ne pastaj kryejmë simulim tonë me C - BGP për një nëngrup prej 8026 multi-homed stub-ësh të përfshira në topologji. Për të reduktuar kohën e simulimit, ne kryejmë simulimin për 2,068 stub-e multi-homed të zgjedhur rastësisht në mesin e 8,026 multihomed stub-eve. Ne tregojmë rezultatet e simulimit në shifrat pasuese. Vonesat e treguara në këto shifra mund të konsiderohen si kufijtë minimale për vonesat e vërteta, meqë ne vetëm marrim vonesën e përhapjes në konsideratë. Faktorë të tjerë mund të ndikojnë në vonesën fund-më-fund, të tilla si bandwidth të kufizuar (vonesë transmetimi), si dhe të bllokimit (vonesë radhe). Përveç kësaj, çdo hap paraqet një vonesë përpunimi i cili nuk është marrë parasysh këtu. Megjithatë, vonesat e paraqitura në Fig.3.36 dhe Fig.3.37 mund të konsiderohen si të njëjtit rend të magnitudës si vonesa të vërteta.

Së pari, në Fig.3.36, janë treguar vonesat përgjatë shtigjeve të zgjedhura nga BGP. Në aksin-x, është inskenuar vonesa e rrugëve në milisekonda (ms). Në aksin y, është inskenuar pjesa kumulative të rrugëve stub - stub që kanë vonesën përkatëse. Është vërejtur se rreth 21 % e rrugëve të zgjedhura nga BGP kanë një vonesë më të ulët se 10ms. Rreth 64 % e rrugëve të zgjedhura nga BGP kanë një vonesë të përbërë mes 10 dhe 50ms, 24 % kanë një vonesë mes 50 dhe 100ms dhe më pak se 1% kanë një vonesë më të madhe se 100ms, vonesa më e madhe duket të jetë 208ms. Vetëm për të patur një ide se çfarë vonesat përfaqësojnë, kujtojmë se vonesa për të shkuar me shpejtësinë e dritës nga një fund të një diametri të tokës të tjetri (për 20,000km) është përafërsisht 67ms.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

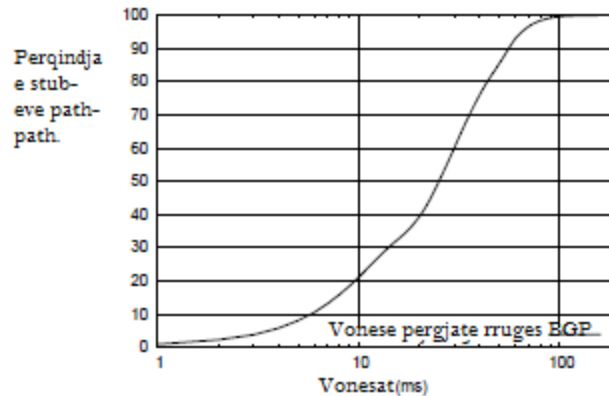


Figura 3.36: Shpërndarja kumulative e vonesës për rrugët BGP.

Në Fig.3.37, u inskenua vonesa përgjatë rrugës BGP (aksi-x) kundër vonesës së bashku me vonesën më të mirë të marrë me Peerings Virtual (aksi-y). Çdo pikë përfaqëson një çift të vlerave të vonesës. Ngjyra e pikës është një tregues se sa shumë cifte stub-esh korrespondojnë me këto vonesa. Vija diagonale, ku x është i barabartë me y paraqet rast ku nuk ka përmirësim, pasi vonesa përgjatë rrugës BGP dhe vonesa më e mirë janë të barabarta. Një vëzhgim i parë është se pikat nuk janë mbi këtë linjë. Kjo do të thotë se Peerings Virtual nuk e përkeqëson vonesën fund-më-fund. Për të gjitha pikat që shtrihen në mënyrë rigoroz sipas linjës, ekziston një rrugë alternative të shfrytëzueshme, duke përdorur Peerings Virtuale dhe kjo rrugë ka një vonesë më të ulët se rruga BGP. Vërejmë se një përmirësim i saktë në vonesë është e mundur. Për shembull, në qoftë se ne respektojmë pjesën e djathtë të Fig.3.37, vërehet se një numër i konsiderueshëm i rrugëve të zgjedhura nga BGP të ketë një vonesë që është më shumë se 100ms. Pjesa e rrugëve BGP që kanë një vonesë më të madhe se 100ms është rreth 25%. Në të kundërtën, në qoftë se respektohet pjesën e sipërme të subjektit, vërehet se shumica e rrugëve me vonesë më të ulët janë nën 100ms. Pjesa e rrugëve me vonesë më të ulët që janë më të shkurtra se 100ms është rreth 95%.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

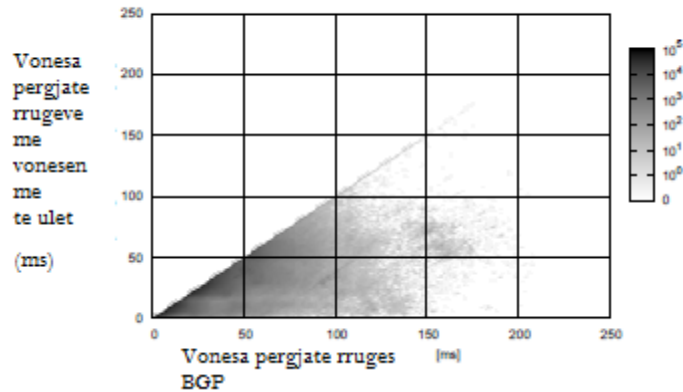


Figura 3.37: Vonesë përgjatë rrugës BGP kundrejt vonesës përgjatë rrugës më të ulët.

Kurba e Fig .3.38 jep shpërndarjen e përmirësimit absolut në vonesë, që është dallimi në mes të vonesës së rrugës BGP dhe vonesën e rrugës më të mirë alternative që lejojnë peerings virtuale. Vërejmë se për rreth 40 % të rrugëve, nuk ka asnjë përmirësim të mundur. Kjo do të thotë se, rastësisht, BGP ka zgjedhur tashmë rrugën më të mirë në terma të vonesës për këto rrugë. Megjithatë, vërehet se për më shumë se 40% të rrugëve ka një përmirësim të mundshëm përse i përket vonesës. 30% e rrugëve mund të përmirësohen deri në 5ms. 22 % e rrugëve mund të përmirësohen me 5 për 20ms dhe 8 % e rrugëve mund të përmirësohen nga më shumë se 20ms dhe deri në më shumë se 180ms .

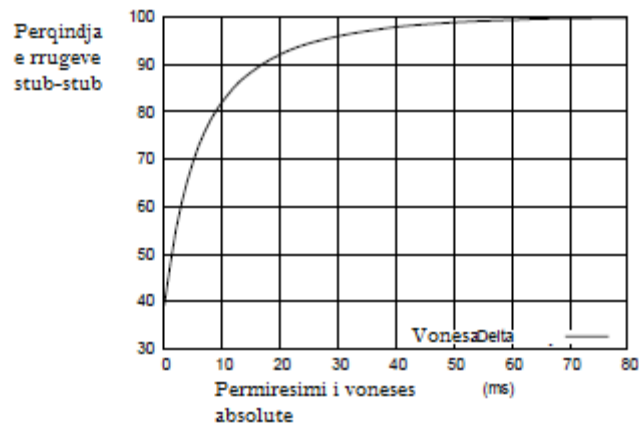


Figura 3.38: Shpërndarja e përmirësimit të vonesës absolute

Së fundi, është treguar në Fig.3.39 ndikimi i të pasurit të 2, 3, 4 ose më shumë ofruesve për një rrjet stub. Në boshtin x të Fig. 3.39, është treguar përmirësimi absolut në vonesë, që është dallimi në mes të vonesës së rrugës BGP dhe rruga më e mirë në afat të vonesës. Në aksit y, tregohen pjesë të rrugëve stub-stub. Shifra përfaqëson të njëjtën kurbë në Fig.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

3.39, përveç se kemi ndarë kurbën në varësi të numrit të ofruesve të domainit burim. Përveç kësaj, është përdorur një shkallë logaritmike për të zmadhuar përmirësimet e vogla. Vëmë re se kur një rrjet stub lidhet me shumë ofruesë, është e mundur për të gjetur rrugët më të shkurtra në afat të vonesës. Së pari, duke pasur më shumë ofrues do të thotë se një pjesë e madhe e rrugëve mund të përmirësohen. Për shembull, për stub-ët dual-homed, ka më pak se 50% të rrugëve që mund të përmirësohen. Për stub-ët që kanë 3 ofrues, më shumë se 45% mund të përmirësohen. Me stub-ët që kanë 4 ofrues, pjesa rritet me rreth 40% dhe me më shumë se 5 ofrues, deri në 30% e rrugëve mund të përmirësohen. Megjithatë, fitimi marginal në përmirësimin e mundshëm të vonesës zvogëlohet shpejt.

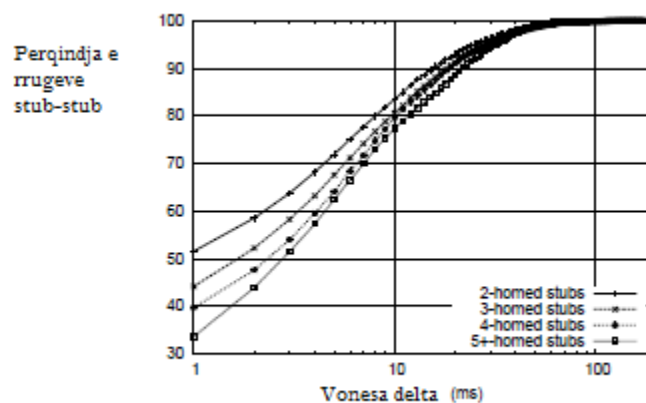


Figura 3.39: Shpërndarja kumulative e përmirësimit të vonesës absolute për stub-ët homed.

Përfundime

Në këtë kapitull është përshkruar se si të ndërtohet një model rrugëzimit të një AS të madh duke përshkruar faktorët thelbësorë që duhet të merren në konsideratë kur ndërtohet një model rrugëzimit të një AS-je. Në veçanti, është treguar se ndërtimi i një modeli të saktë të një AS kërkon topologji rrjeti, trafikut, protokollet e rrugëzimit dhe konfigurimin e tyre. Marrja e të dhënave të lidhura ende mund të jetë një çështje operative. U ilustrua përdorimi i solverit të rrugëzimit nëpërmjet dy studimeve të ndryshme të rastit. Studimi i parë i rastit ishte një analizë e ndikimit të ndryshimit të peer-save të një AS tranzit në trafikun e tij. U tregua se duke përdorur një model i një AS mundësohet shqyrtimi i zgjidhjeve peering të ndryshme. Studimi i dytë heton ndikimin e dështimeve të lidhjeve në ndryshimet e rrugëzimit brenda AS. Kjo është e rëndësishme pasi ngjarjet e rrjetit të tilla si dështimet dhe mirëmbajtjet janë të shpeshta. Dy studime të rasteve kanë treguar rëndësinë e marrjes parasysh të informacionit interdomain të rrugëzimit për të kuptuar rrugëzimin e një AS të madh. Në këtë kapitull, është marrë në konsideratë rrugëzimi në një fushë të vetme. CBGP mund të përdoret për të llogaritur

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

rezultatit e zgjedhjes së rrugës BGP kur ka domain-e të shumta. Megjithatë, kjo kërkon një njohuri të strukturës dhe të politikave nga fusha të tjera. Për të studiuar ndikimin e ndryshimeve në një domain të trafikut inbound të tij për shembull, ne duhet të kemi njohuri për gati të gjitha domain-et e internetit. Një përmirësim i mundshëm në të ardhmen konsiston në funksionimin e modelit në një ushqim të vazhdueshëm të topologjisë, rrugëzimit të të dhënave dhe të dhënat e trafikut. Besohet se qasja për të integruar topologjinë, të dhënat e rrugëzimit dhe të dhënat e trafikut mund tu shërbejë operatorëve ISP për të kuptuar më mirë sjelljen e një AS dhe të ndihmojë ata për të hetuar përmirësimet në projektimin e rrjetit të tyre. Në internetin e sotëm, AS shpesh duhet të kontrollojnë rrjedhën e trafikut të tyre interdomain, për arsye të kostos ose performancës. Në këtë kapitull, është shpjeguar se pse është e vështirë për një sistem autonom të kontrollojë rrjedhën e trafikut të tij në hyrje me arkitekturën e tanishme në Internetin të bazuar në BGP. Janë trajtuar teknikat e bazuara në inxhinierinë e trafikut BGP që mbështeten në ndikimin në procesin e vendimmarrjes së ruterave BGP. U bë dallimi i kontrollit të trafikut dalës nga kontrolli i trafikut në hyrje. Të dyja teknikat janë të ndryshme në se ata manipulojnë attribute të ndryshme të rrugëve BGP, por edhe për shkak të fushës së ndikimit të tyre. Teknikat duke u fokusuar në trafikun dalës mbështeten në vendimet e marra nga BGP në domenin lokal ndërsa teknikat duke u përpjekur për të kontrolluar nevojën e trafikut hyrës për të ndikuar në procesin e vendimmarrjes BGP në domaine të largët, e cila është shumë më e vështirë. Konkluzionet u përmbledhën në Tabelë duke treguar për çdo teknikë se cilin drejtim të trafikut mund të kontrollojë (kolona 2), si dhe qëllimin e teknikës (kolona 3). Kolonat e mbetura tregojnë cilësitë e ndryshme të teknikës. Së pari, është treguar nëse teknika është e parashikueshme, dmth nëse rrugëzimi i saj mund të parashikohet. Në të vërtetë , për të kontrolluar me saktësi rrjedhën e paketave hyrëse, një AS duhet të jetë në gjendje të parashikojnë se cila rrugë do të përzgjidhen nga AS-ët në distancë. Së dyti, është treguar nëse teknika është e shkallëzueshme, dmth në qoftë se teknika mund të përdoret duke pasur parasysh numrin e rrugëve në internet sot dhe rritjen e tij të pritshme. Së treti, është treguar nëse metoda është e fortë, që është në qoftë se ajo nuk do të pengojë fuqinë e tanishme të sistemit interdomain të rrugëzimit. Kolona e fundit jep komente mbi efikasitetin e teknikës. Teknikat e bazuara në BGP në dispozicion për të kontrolluar punën e trafikut dalës duke ndikuar në routerat në domenin lokal. Të gjitha këto teknika janë deterministe, të shkallëzuar dhe të fuqishme. Konkluzionet për teknikat e bazuara në BGP konsiderojnë trafikun në hyrje më shumë ndryshore. Së pari , njoftimet selektive nuk janë të fuqishme që nga dështimi i një lidhjeje të qasjes do të shkaktojë tërheqjen e plotë të disa prefikseve. Shpallja e më shumë prefikseve specifike nuk është përcaktuese pasi ajo është e ndjeshme ndaj filtrimit nga AS-ët e largët. Përveç kësaj, kjo teknikë nuk është e shkallëzuar pasi ajo rrit numrin e prefikseve në tabelat e rrugëzimit BGP. Atributi MED vetëm mund të përdoret për të kontrolluar trafikun e marrë mbi lidhjet e shumta me një fqinj AS. Përveç kësaj, kjo teknikë kërkon një marrëveshje me fqinjin AS . Së fundi , duke përdorur atributin MED mund të çojë në luhatjet e vështira për të korrigjuar [W02a], kështu që fuqia e saj është e diskutueshme .

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Tabela 4: Përmbledhja e metodave të inxhinierimit të trafikut

		Trafik	Shkallëzueshmeria			Eficiencia
		Qellimi	Parashikueshmeria	Robustiteti		
BGP-based approaches						
Local-Pref	Out	Domain	✓	✓	✓	
IGP weights	Out	Domain	✓	(✓)	✓	
Sel. announcements	In	Internet	✓			Not robust to access link failure.
More spec. prefixes	In	Internet			✓	Sensitive to filtering
MED	In	Neighbor(s)	✓	✓	(✓)	Requires bilateral agreement(s)
AS-Path prepending	In	Internet		✓	✓	Limited granularity (given the diameter of the Internet). Impact difficult to predict.
Communities	In	Internet		✓	✓	Impact difficult to predict. Large search space.
Non BGP-based approaches						
RON, Detours	In/Out	Internet	✓		✓	Require modifications to end-systems. Rely on a large number of IP tunnels.
NAT	In	Internet	✓			Target multi-homed enterprise networks. Poses problem when one access link fails.
New architectures	In/Out	Internet	✓	✓	✓	Difficult to deploy in the current Internet.

Nga simulimet u tregua që AS-Path prepending, edhe pse një teknikë e përdorur gjerësisht, siguron një kontroll jo të parashikueshëm për trafikun në hyrje. Ky parashikim është i vështirë për dy arsye. Së pari, njohuritë tona të topologjisë së internetit dhe politikat e rrugëzimit janë të paplota. Së dyti, edhe me një topologji të detajuar, ende do të jetë shumë e vështirë për të parashikuar rezultatin e rregullave të tie-break të procesit të vendimmarrjes BGP. Në praktikë, AS-Path prepending mund të përdoret për të treguar se një lidhje backup duhet të shmanget kur është e mundur, por është e vështirë të përdorin atë për të balancuar trafikun në hyrje. Një qasje alternative është që të mbështeten në teknikat e bazuara në komunitete të veçanta BGP (QTUB04, AG04). Këto teknika sigurojnë një kontroll fin në trafikun hyrës. Për fat të keq, ato janë të vështira për t'u përdorur në praktikë për shkak të pamjes jo të plotë të të gjithë internetit që një operator ka dhe për shpërthimin kombinator të mundësive duke pasur parasysh numrin e komuniteteve të veçanta BGP që një AS mund të përdorë. Bazuar në analizat tona, teknikat aktuale me bazë BGP nuk janë të përshtatshme për të kontrolluar flukset e paketave hyrëse. Ndryshimet në arkitekturën e internetit janë të nevojshme për të arritur një kontroll të tillë. Arkitektura të ndryshme alternative kanë qenë propozuar në literaturë si Opca, Nira dhe banane, por këto arkitektura kërkojnë që të gjitha routerat e BGP në internet të përditësohen të cilat do të të kërkojë disa ditë flamuj. I njëjti përfundim mund

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

të nxirret për alternativat më bazë end-systems të tilla si RON apo Detours, pasi ata do të kërkojnë që të gjithë endsystems të përditësohen. Përveç kësaj, këto qasje e end-sisteme të bazuara në shkallë më pak pasi ata punojnë në një grimcim fin (flukseve ose palë burim / destinacionit). Prandaj, mund të konstatohet se asnjë teknikë nuk mund të përdoret sot nga një domain stub i madh për të kontruar trafikun në hyrje të saj në mënyrë të shkëlqyer, shkallëzuar dhe të parashikueshme.

Në këtë kapitull, është prezantuar një qasje bashkëpunuese për inxhinierimin të trafikut interdomain. Kjo qasje mbështetet në Peerings Virtual. Një Peering Virtual është një tunel IP njëdrejtimësh midis një routeri kufitar e zgjedhur nga burimi AS dhe një router kufiri i zgjedhur nga AS destinacion. Zgjidhja jonë për të krijuar një Peering Virtual mbështetet në tre parime themelore. Së pari, ka një Peering Virtual Controller brenda secilit AS dhe IP adresa e tij është e bashkangjitur si komunitet i zgjeruar BGP për të gjithë reklamat BGP të krijuara nga AS. Së dyti, një seancë eBGP multi-hop është themeluar mes VPC-ve të burimit dhe AS-ve destinacion për të negociuar Virtual Peering-sët. Burimi AS zgjedh "head-end"-in e Peering Virtual në bazë të objektivave të vet të inxhinierisë së trafikut. Së treti, destinacioni AS zgjedh në mënyrë autonome "tail-end"-in e Peering Virtual. Një përparësi kryesore e qasjes sonë është se ajo mund të vendoset në mënyrë rritëse brenda AS-ve bashkëpunuese stub dhe nuk kërkon ndonjë ndryshim në AS-të tranzit. Duke pasur parasysh madhësinë e internetit global dhe numrin e rrugëve BGP, kjo vendosje në rritje është një problem kyç operativ që duhet të merret parasysh.

Ne kemi treguar se Peerings virtuale mund të përdoren për të zgjidhur problemet inxhinierike të trafikut interdomain. Ne vlerësuam ato në dy raste të veçanta, pra balancimi i ngarkesës së trafikut dhe uljen e vonesës së rrugëve interdomain. Kur përdoret për të balancuar ngarkesën e trafikut, Peerings Virtual janë një zgjidhje e shkallëzueshme meqënëse nga një numër i kufizuar i tyre do të jetë e nevojshme për të arritur një ekuilibër afër perfektës. Në mënyrë tipike, me 1000 burimet përgjegjëse për 95% të trafikut inbound, në rendin e 50 peerings virtuale janë të nevojshme për të balancuar trafikun. Në rastin e dytë, duke përdorur Peerings Virtual bëhet e mundur për të përcjellë trafikun në rrugë interdomain me një vonesë më të ulët. Ne krahasim me vonesën e marrë në rrugë të zgjedhura nga BGP të vërtetë (genuine) dhe rrugët e marra duke përdorur Peerings Virtuale tregohet se më shumë se 40% të palëve burim / destinacion ishte e mundur një përmirësim i vonesës. Kjo është në përputhje me punën paraardhëse nga Savage et al që tregojnë se 30-80% e shtigjeve fund-me-fund mund të përfitojnë nga një përmirësim i dukshëm në cilësinë e duke përdorur një rrugë alternative [SCH + 99].

Kapitulli IV

Voice Over IP – VOIP

4.1 Hyrje

Në ditët e sotme termi “Voice over IP” përfshin të gjitha mënyrat e mundëshme të realizimit të një bashkëbisedimi zanor përmes Internetit. Një bisedë e tillë mund të arrihet shumë thjesht përmes harduer dhe softuer përkates (psh. një komunikim në MSN ose Skype përmes një seti kufjesh dhe mikrofi).

Interesi mbi VoIP është rritur në mënyrë të vazhdueshme vitet e fundit por projektimi i një rrjeti VoIP kërkon një planifikim të kujdeshëm në mënyrë që të sigurohet ruatja e kualitetit të zërit në nivele të përshtatshme.

Në formën më të thjeshtë një komunikimi VoIP në ditët e sotme, mund të paraqitet si më poshtë:

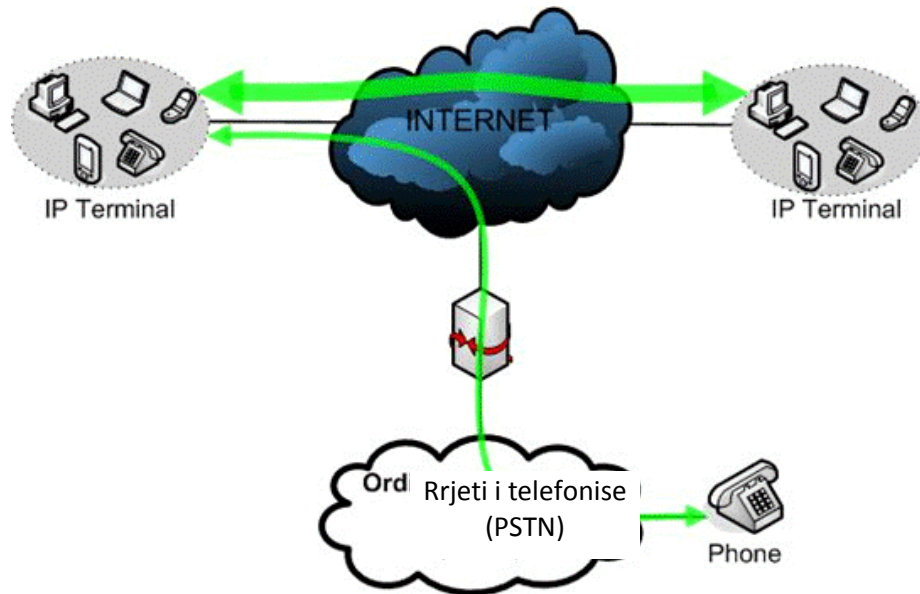


Figura 4.1: Komunikimi VoIP

Sipas figurës më sipër kompjuterat, celularët, PDA-të etj. shërbejnë si terminalë IP dhe telefonatat mund të vendosen ndërmjet dy terminaleve IP, ndërmjet një terminali IP dhe një telefoni analog tradicional dhe anasjelltas. Skenarët e mësipërm të komunikimit bëhen të mundur vetëm në se zëri konvertohet nga analog në shifror tek ana e folësit, në mënyrë që të transmetohet në rrjetat IP, dhe anasjelltas tek dëgjuesi i informacionit zanor. Konvertimi nga analog në shifror arrihet përmes një procesi kampionimi dhe kuantizimi

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

të cilët implementohen në koduesit e VoIP. Nga ana e dëgjuesit informacioni zanor kthehet nga shifror në analog përmes procesit të dekodimit.

Nisur nga sa thamë, figura e më poshtme jep në terma të përgjithëshme skemën e një aplikacioni VoIP:

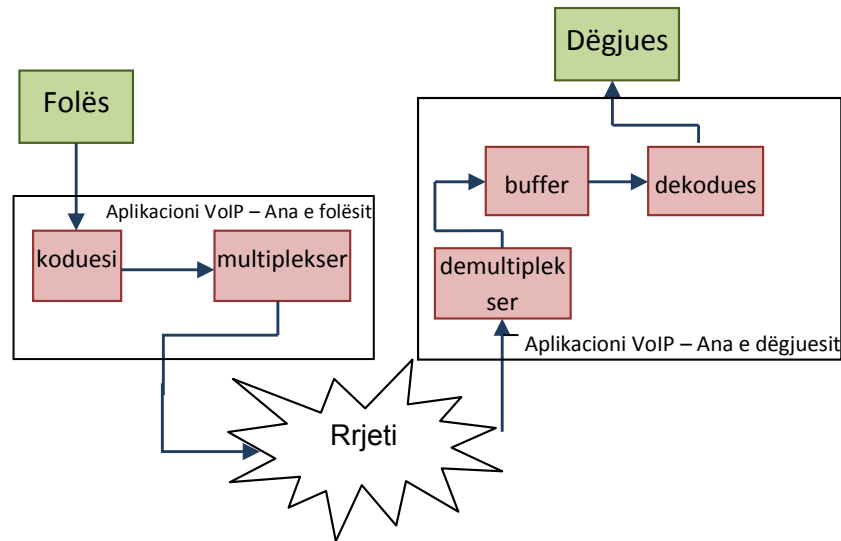


Figura 4.2: Skema e aplikacionit VoIP

Disa nga përbërësit kryesorë të VoIP mund të renditen si më poshtë:

- Nje burim audio, si psh. zëri i njeriut, një regjistrim zanor etj. dhe një konvertues i këtij informacioni zanor në një sinjal elektrik të vazhdueshëm dhe anasjelltas, si psh. një set me mikrofon dhe kufje.
- Një pajisje kampionuese dhe enkoduese në mënyrë që sinjali analog të mund të transportohet në një rrjet me të dhëna në formë paketë. Enkodimi dhe dekodimi i kampionëve të zërit ka hapur rrugën për krijimin e një sërë algoritmesh kodimi dhe dekodimi që njihen me emrin *codecs* (*kodues*) të projektuar me synimin për të përmirësuar parametra të ndryshëm si: përdorimi i kapacitetit në mënyrë efikase ose përshtatja me kushtet e ndryshueshme të kanalit.
- Media Transport Protocol (MTP) që bën të mundur transportimin e kampionëve të koduar në rrjetin e të dhënave. Në Internet, protokollin i zgjedhur për këtë qëllim është Real-time Transport Protocol (RTP) [22]. Kampionët e zërit enkapsulohen në RTP dhe UDP para se të dërgohen në formën e një *IP frame*.
- Një multipleksor që bën të mundur multipleksimin e disa *frame* në të njëjtën paketë duke reduktuar numrin e kokave MAC, të rrjetit dhe të transportit me kosto rritjen e vonës në transmetim. Pjesa e të dhënave të paketës VoIP është në thelb një enkapsulim në paketa RTP/UDP/IP.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

- Një *playout buffer* i cili detyron *frame*-t tek marrësi që të dekodohen në të njëjtin interval në të cilin janë enkoduar tek dërguesi. Për këtë arsye mund të bëjë rirenditje, vonesë ose dhe hedhje paketash që vijnë përtej kohës së pritur.
- Protokoll për manaxhimin e sesionit që nevojitet për të ngritur, negociuar dhe mbyllur seksionet ndërmjet palëve komunikuese. Një protokoll i tillë është SIP (Session Initiation Protocol) [23].
- Aplikacioni VoIP që përcakton qëllimin për të cilin informacioni zanor po transmetohet, si psh. në se kërkohet komunikimi mes dy njerëzve atëherë mund të përdoren aplikacione si Skype, MSN etj.
- Nyje të specializuara rrjeti të nevojshme për funksionimin e saktë të protokolleve të mësipërme dhe të arkitekturës komunikuese. Këto nyje kryejnë funksione të tipit: identifikimi i përdoruesve përmes identifikuesit të tyre VoIP, ruajtja e preferencave të përdoruesve, përkthimi i *codec* të përdorur nga njëra palë në atë të përdorur nga pala tjetër, etj

4.2 Pritshmëria ndaj aplikacioneve VoIP në rrjet

Përdoruesit e kanë kërkesat e tyre ndaj cilësisë në lidhje me telefonatat VoIP. Në mënyrë që këto kërkesa të vlerësohen nevojitet të përcaktohen shpjegimet e mëposhtme në lidhje me çfarë nënkupton QoS:

1. Aftësitë për, ose klasat e përcaktuara për të arritur, manaxhim preferencial të tipave të ndryshëm të trafikut në një rrjet *packet-switching*. Veçanërisht në gjuhën e Internetit QoS nënkupton përcaktimin e një klase preferenciale shërbimi të cilës i vihet në përkatësinë e transmetimit të caktuar. Klasa krijohet nga specifikimi i aftësive të veçanta të rrugëzimit që i vënë në dispozicion një tipi të caktuar trafiku prioritar përdorimin e gjerësisë së mundëshme të brezit.

2. *Cilësia vetiake e shërbimit (Intrinsic QoS)*. Kur trafiku kalon nëpër një rrjet *packet-switching*, me apo pa zbatimin e QoS, trafiku fiton një nivel të matshëm performance nën nivele të ndryshme kërkesë. Siguruesi i shërbimit mund të masë karakteristikat e trafikut pa patur nevojë ti referohet perceptimit të klientit për cilësinë. Këto karakteristika që konsiderohen vetiake janë:

- *Latenca* - koha që i duhet paketës për të arritur në destinacion
- *Jitter* – ndryshueshmëria në latencë të paketave
- *Niveli i paketave të hedhura* - frekuenca me të cilën paketat nuk e arrijnë destinacionin në kohë për tu përdorur.

Për çdo klasë trafiku këto karakteristika do të varen nga gjerësia e disponueshme e brezit dhe nga niveli i kërkesës.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

3. *Kualiteti i perceptuar i shërbimit*. Nënkupton cilat janë rezultatet pas përdorimit të rrjetit dhe përcaktohet nga çfarë shikon përdoruesi si rrjedhojë e *QoS veti*ake, gjatë aktiviteteve të komunikimit, dhe si reagojnë ndaj kësaj në përputhje me pritshmëritë e tyre.

Përcaktimi i këtij kualiteti të perceptuar fillon pikërisht nga përshkrimi i shqetësimeve të përdoruesit në lidhje me QoS. Përdoruesi diskuton kualitetin e asaj që dëgjon duke shtruar çështjet e kuptueshmërisë së fjalëve, efektit eko, natyralitetin e zërit, ruajtjen e intonacioni, etj.

Marrëdhënia ndërmjet kualitetit të perceptuar të shërbimit dhe atij veti ak përkundrejt cilësisë së lidhjes do të përcaktohet nga tre karakteristika kryesore të sistemit:

1. *Koduesi i zërit (kodues/dekodues)*, përcakton mënyrën se si sinjali zanor konvertohet në shifror për transmetim
2. Skema e paketizimit, përcakton gjatësinë e segmenteve të të dhënave zanore të transmetuara në çdo paketë dhe madhësinë në *bit*-e të kokave të paketave.
3. Madhësia e *jitter buffer*, që përcakton aftësinë për të rifituar sinjalin original kundrejt ndryshimeve në vonesat në transmetim.

Ajo çka i vështirëson punët për VoIP është se për të vlerësuar shërbimin e ofruar, kundrejt këtyre shqetësimeve, një përdorues përdor eksperiencat e mëparëshme të tija në transmetim zëri, që shpesh nënkupton se përdor si bazë krahasuese eksperiencën me telefoninë tradicionale. .

Përvç çështjeve që kanë të bënë me cilësinë e asaj që dëgjohe (cilësinë e zërit), perceptimi mbi cilësinë e shërbimit nga ana e një përdoruesi përfshin dhe karakteristikat e mëposhtme të shërbimit:

- *Aksesueshmërinë*, aftësinë për të filluar një lidhje kur dëshirohet;
- *Shpejtësia e rrugëzimit*, shpejtësia me të cilën vendoset lidhja;
- *Besueshmëria e lidhjes*, besueshmëria e procesit të vendosjes së lidhjes;
- *Besueshmëria e rrugëzimit*, besueshmëria e procesit të rrugëzimit të lidhjes në destinacionin e duhur;
- *Vazhdueshmëria e lidhjes*, aftësia për të mbajtur një lidhje me cilësi deri kur nuk është më e nevojshme;
- *Besueshmëria e shkëputjes*, besimi se përgjigja e sistemit ndaj kërkesës për të ndërprerë njëthrrje dhe gjithashtu dhe procesin e faturimit për të.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Kuptohet që përdoruesi nuk i referohet këtyre karakteristikave në formën e lartpërmendur por përmes pyetjeve të tipit: “sa kohë duhet që të kuptoj se lidhja është vendosur dhe a është kjo kohë e parashikueshme?”, “A do qëndrojë lidhja ime e ngritur deri sa të vendos unë ta mbyll?”, etj.

4.3 Koduesit e zërit

Transformimi i zërit analog në kampionë diskretë të koduar dhe që mund të transportohen në një rrjet paketash është një process i komplikuar. Një pjesë e informacionit gjatë konvertimit të informacionit original humbet dhe nuk mund të rekuperohet më (siç tregohet dhe në figuren më poshtë).

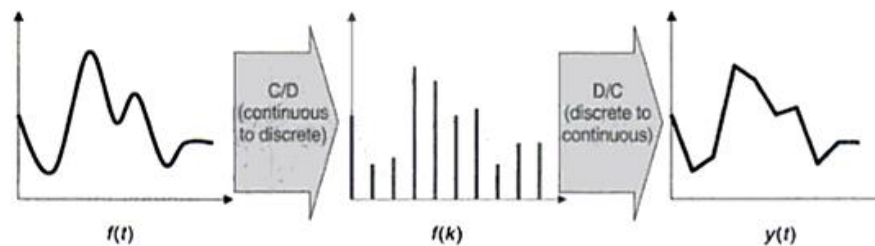


Figura 4.3: Skema e aplikacionit VoIP

Për këtë arsye është e rëndësishme që të zgjidhet rendi i përshtatshëm i kampionimit dhe shkalla e përshtatshme e kuantizimit me që ato ndikojnë në mënyrë direkte në cilësinë e sinjalit në dalje. Si rrjedhojë janë zhvilluar algoritma të ndryshëm kodimi. Në thelb secili prej tyre duhet të kalojë këto hapa kryesorë:

1. Transformimi i sinjalit të vazhdueshëm, analog në një sekuencë kampionësh diskretë me hapësirë të njëjtë. Rendi i kampionimit përcaktohet sipas Teoremës së Nyquist-it, i cili thotë se në mënyrë që të bëhet e mundur kthimi i sinjalit original nga ai i koduar duhet të kampionohet në një frekuencë të barabartë me dyfishin e gjerësisë së brezit të tij. Edhe pse zëri i njeriut përfshin brezin 0 - 20.000 Hz, zakonisht kufizohet me ndihmën e një filtri në 0-3400 Hz dhe rendi tipik i kampionimit përcaktohet 8000 Hz.
2. Amplituda e kampionëve mund të marrë vlera nga më të ndryshmet. Si rrjedhojë në mënyrë që ti vendoset një vlerë diskrete çdo kampioni e cila më pas do të kodifikohet në një fjalë binare, do të duheshin një numër gjigand bitesh. Për të kufizuar këtë numër përcaktohet një bashkësi vlerash standard dhe gjithë vlerat e ndërmjetme rrumbullakosen në to. Si rrjedhojë e kësaj futet një masë gabimi që njihet me emrin zhurma e kuantizimit. Për ta evituar përdoret kuantizimi jouniform. Kjo nënkupton se vlerat standard për vlera amplitudash të vogla zgjidhen që të kenë më pak diferencë (zhurma e kuantizimit ndjehet më shumë në rastin kur përdoren tonalitete të ulëta të zërit dhe amplitudat janë të ulët).
3. Së fundmi, vlera e kampionëve rezultues mund të dërgohen nëpër rrjet.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Koduesit e zërit projektohen sipas standardeve të International Telecommunication Union (ITU) standards, që përcaktojnë se si do të kodohen në rrjedha të dhënash shifrore sinjalet analoge zanore. Projektimi i një koduesi të tillë përfshin përcaktimin e numrit të byte-ve që mund të përfshihen në një paketë zëri dhe rendin e përshtatshëm të bit-ëve të të dhënave në mënyrë që të transmetohet sinjali zanor shifror përmes teknikave të ndryshme të kodimit.. Tabela 3.3 tregon psh. karakteristikat e 3 koduesve më të përdorur për ngritjen e shërbimeve VoIP.

Tabela 5: *Krahasimi i karakteristikave të koduesve të zërit*

Koduesi	Teknika e kodimit	Gjatësia e segmentit të zërit	Data rate (bit/s)
G.711	PCM (Pulse Code Modulation)	0.125	64.000
G.723.1	MP-MLQ (Multiple maximum-likelihood quantization)	30	6.3000
G.723.1	ACELP (Algebraic-code-excited linear prediction)	30	5.3000
G.729	CELP (Code-excited lineas prediction)	10	8.0000

Që të tre këto tipa koduesish bazohen në një rend kampionimi prej 8000-hertz (Hz) për sinjalin analog të zërit. Sidoqoftë, siç tregohet në tabelën më sipër ndryshimet në teknikat e kodimit krijojnë diferenca rrënjësore në gjatësinë e segmentit dhe sasinë e të dhënave të transmetuara. Këto karakteristika nga ana e tyre ndikojnë drejt për së drejti në karakteristikat e sinjaleve zanore të dëgjuesit në përdoruesi në një lidhje VoIP: vonesa dhe besnikëria ndaj sinjalit original.

4.4 Paketizimi

Një tjetër karakteristikë e sistemit që ndikon në mënyrën se si humbja e paketave në rrjet do ndikojë në shtrembërimet në komunikim të perceptuara nga përdoruesi është mënyra se si paketat ndërtohen për transmetim. VoIP përdor “packet-switching” për transmetimin e të dhënave zanore dhe për rrjedhojë bit-ëve të informacionit që do dërgohet ju shtohet informacioni i nevojshëm për rrugëzimin dhe manaxhimin e tyre nëpër rrjet. Informacioni i shtuar njihet si “koka e paketës” (*packet header*) dhe bit-et e informacionit njihen si *payload*. Kjo mënyrë transmetimi krijon një tepriçë informacioni që nga ana e saj rrit nivelin e rendit të transmetimit të të dhënave që duhet arritur për një nivel të caktuar cilësie në transmetim. Kjo bën që madhësia e kokës së paketës të ketë një ndikim të madh në QoS.

4.5 “Jitter buffer”

Në një komunikim VoIP kampionët e zërit duhet të paraqiten tek dekoderi në mënyrë të tillë që kampioni pauses në një rrjedhë informacioni të paraqitet për përpunim në

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

momentin kur dekoderi ka përfunduar me paraardhësin e tij të menjëhershëm. Kjo kërkesë kufizon rreptësisht sasinë e “*jitter*” që mund të tolerohet pa patur boshlliqenë kampionë. Kur *jitter* rezulton në një interval kohe më të madh ndërmjet paketave bartëse të kampjonëve të njëpasnjëshëm se sa koha e nevojshme për të rikrijuar sinjalin analog nga kampioni, dekoderi është i detyruar të vazhdojë funksionimin pa informacionin e kampionit pauses. Kështu efektet e *jitter* do të paqyrohen në një rritje të rendit të paketave të hedhura.

Për të evituar këtë efekt të papëlqyeshëm, dekoduesit janë të pajisur me një *jitter buffer* i cili vendos në rradhë një numër të caktuar segmentesh zëri shifror para dekodimit. Ky *buffer* krijon vonesa të nevojshme qërrjedha e të dhënave të jetë e qëndrueshme.

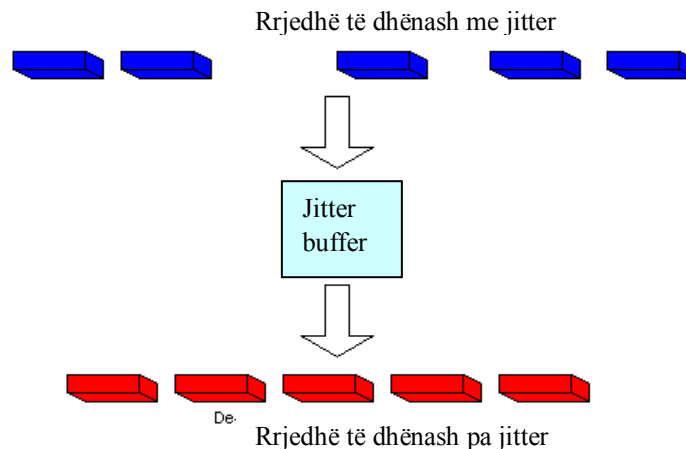


Figura 4.4: *Manaxhimi i jitter përmes jitter buffer*

Zgjedhja e duhur e tij përcakton marrëdhënien kompromisin ndërmjet rendit të paketave të hedhura dhe rritjes së vonesave në transmetim që përcaktohet nga madhësia se *jitter buffer* (vonesa duhet të jetë Brenda limiteve të toleruara).

4.6 Matja e Cilësisë së VoIP

Cilësia e një thirrjeje zakonisht matet përmes provave subjektive ose monitorimit instrumental. Në metodat e provave subjektive, njerëzve u kërkohet të vlerësojnë cilësinë e shërbimit sipas një procesi të standardizuar dhe të japin një vlerësim, zakonisht 1-5 (vlerësimi MOS), sipas një procesi të standardizuar.

Këto lloj provash kërkojnë shumë kohë si rrjedhojë e numrit të përdoruesve që duhen marë në konsideratë. Kjo është arsyeja pse vitet e fundit i është kushtuar më shumë vëmendje mjeteve të matjeve instrumentale, ku më i përdoruri është Modeli-E, i standardizuar nga ITU-T.

a) *Mean Opinion Score - MOS*

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Bazohet në provat subjektive, ku n jë numri përdoruesish i kërkohet të dëgjojnë një kampion zëri (që i koresponдон një *codec* të caktuar) dhe të japin një vlerësim për informacionin e marë ashtu siç ata e perceptojnë pas transmetimit. Vlerësimi MOS, i përlllogaritur nga mesatarja e vlerësimeve të të gjithë dëgjuesve, lëviz në kufinj të 1 deri në 5 (ku 1 është e papranueshme dhe 5 është shumë e mirë). Një rend tipik i MOS për një thirrje të ranueshme është 3.5 deri në 4.3.

Edhe pse mund të jetë një nga mjetet më të mira të vlerësimit të cilësisë për VoIP, MOS është i vështirë në implementim me që nevojitet ndërhyrja njerëzore. Për këtë arsye, po ITU-T propozoi Modelin-E..

b) Modeli-E

Modeli-E është një mjet planifikimi për vlerësimin e cilësisë së përgjithshme të një rrjeti telefonik. U prezantua nga rekomandimi i ITU G.107 [24] me objektivin për të përcaktuar një vlerësim të cilësisë që përfshin karakteristikat “nga goja-në vesh” të një shtegu fjalimi.

Dalja e një përlllogaritjeje Model-E është një scalar i vetëm, i njohur si faktori R, i derivuar nga vonesat dhe faktorët dobësues të pajisjeve. Pasi ky faktor llogaritet ai mund të lidhet më një vlerësim të përafërt të MOS.

Faktori R llogaritet përmes shprehjes së mëposhtme:

$$R = R_o - I_s - I_d - I_e + A$$

ku R_o përfaqëson raportin sinjali ndaj zhurmës (SNR), I_s përfaqëson kombinimin e gjithë dobësime që ndodhin njëkohësisht në sinjalin zanor, I_d përfaqëson dobësimet e shkaktuara nga vonesat, I_e përfaqëson dobësimet e shkaktuara nga codecs me rend të ulët bitesh, i njohu dhe si faktori i dobësimit të pajisjeve, dhe A është faktori i avantazhit që modelon pritshmëritë e përdoruesit për teknologjinë e përdorur. Për shembull, vlera e A është më e madhe në rrjetat satelitore se sa në ato kabllore me që pritshmëria e klientit për ato satelitore është më e ulët. Vlerat e A lëvizin në intervalin $[0,20]$ dhe vlerat shembull të propozuara nga ITU jepen në tableë si më poshtë, Tabela 3.6:

Tabela 6: Vlerat tipike të faktorit A

Sistemi i komunikimit	Faktori A
Telefonia kabllore	0
Celular në zona me ndërtesa (shumë hope satelitore)	5
Celulari në një makinë në lëvizje	10
Aksesi në zona gjeografike me vështirësi	20

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

arritjeje	
-----------	--

Pas llogaritjes së faktorit R, ekuivalenca midis R dhe MOS mund të përlogaritet si më poshtë:

Tabela 7: Ekuivalenca midis faktorit R dhe MOS

Opinionimi i përdoruesit	Faktori R	Vlerësimi MOS
Shumë i kënaqur	90 - 100	4.3 - 5.0
I kënaqur	80 - 90	4.0 - 4.3
Disa përdorues të kënaqur	70 - 80	3.6 - 4.0
Shumë përdorues të pakënaqur	60 - 70	3.2 - 3.6
Thuajse gjithë përdoruesit të pakënaqur	50 - 60	2.6 - 3.1
Jo e rekomandueshme	0 - 50	1.0 - 2.6

Faktori R do të përdoret për llogaritjen e vlerave të MOS në eksperimentet e simulimit të përshkruara më vonë në këtë tez bazuar në informacionin e mbledhur mbi humbjet dhe vonesat.

Kapitulli V

Ambjenti eksperimental, simulimet dhe rezultatet

5.1 Hyrje

Ky kapitull është kapitull metodologjik sepse këtu do të ngrihet ambienti eksperimental, do të realizohen simulimet dhe merren rezultate. Në këtë tezë, ambienti eksperimental do të realizohet përmes mjeteve dhe mundësive që ofron simulatori i rrjetit Ns-2 duke shfrytëzuar kështu të gjitha të mirat që vijnë nga eksperimentimi përmes simulimit. Për të ngritur këtë ambient nevojitet shkarkimi i kodit burim për Ns-2 dhe të moduleve përkatëse të tij për implementimin e BGP dhe VoIP, si dhe instalimi i tyre. Qëllimi i krijimit të këtij ambienti është që të improvizohet sjellja e këtij protokollit në rrjet për ta përshkallëzuar atë në përmasa më të mëdha reale. Këtu synohet që të krijohet perceptimi se si kryhen proceset e simulimit, si kryhet transferimi i të dhënave dhe se si ndikojnë rifreskimet e kryera të protokollit BGP në performancën e rrjetit. Kodi burim për Ns-2 i përshtatur sëbashku me modulet respektive për vlerësimin e rrjetit për protokollin BGP ku domeini modelohet me nyje që shkëmbejnë komunikimin BGP me njëra tjetrën. Këto nyje janë rutura kufitarë (edge). AS tranzit është e organizuar me një *cluster* dhe me reflektues rrugësh që janë nyjet përkatëse. Kjo topologji gjenerohet nga skedari në hyrje të GT-ITM. Për AS fundor është zgjedhur llogjika e paraqitjes së tyre me nga një nyje. Skema e adresimit është përzgjedhur në trajtën 10.0.\$i.1 për ruterat brenda AS tranzit, ku \$i është numrin nyjes dhe 10.\$j.\$i.1 për ruterat në AS stub, ku \$j përkon me numrin e AS dhe \$i me numrin e nyjes. Konfigurimi i rrjetit realizohet kur agjentët BGP konfigurohen në sejcilën prej nyjeve. Vlerat e intervaleve të *hold timer* dhe *keep-alive timer* janë ato default, agjentët UDP konfigurohen në nyjet dhe trafiku nëpër këto dy nyje kalon sipas tabelave të ndërtuara të rrugëzimit. Pasi bëhet konfigurimi i nyjeve, hapi pasues është përcaktimi i ngjarjeve të skeduluara. Në këtë simulim duam të shikojmë kohët e konvergencës të tre ruterave të përfshirë në komunikim që janë n15, n3 dhe n2. Ngjarjet skedulohen. Ngjarja e fundit është realizuar me synimin për të parë sjelljen e sistemit në një situatë kur një rrugë shfaqet dhe shkëputet vazhdimisht brenda një kohe të shkurtër (rute flapping).

Në këtë mënyrë do të vërehet në se ka humbje apo vonesa në paketa gjatë momentit të rifreskimit të tabelave të rrugëzimit BGP. Pas përfundimit të simulimeve elementi i parë që merret në konsideratë është numri i paketave të humbura para se të skedulohet ngjarja e paqëndrueshmërisë dhe pas skedulimit të kësaj ngjarjeje.

5.2 Simulimet

Modelimi i sistemit i referohet veprimit të paraqitjes të një sistemi aktual në mënyrë të thjeshtëzuar. Ekzistojnë dy mënyra kryesore për të realizuar një modelim sistemi: mënyra analitike dhe ajo me simulime.

Në modelimin analitik synohet të arrihet një përshkrim matematik i sistemit. Në se zbatohet saktë, ky modelim mund të jetë efektiv nga kostoja dhe të sigurojë një vështrim abstrakt të komponentëve që ndërveprojnë me njëritjetrin në sistem.

Në modelimin me simulator kërkohet më pak abstraksion në model (dhe më pak supozime thjeshtëzuese) me që pothuajse çdo detaj i sistemit mund të përfshihet në simulim. Ky lloj modelimi është i përshtatshëm për sistemet e mëdha ku një formulim i drejtpërdrejtë matematik nuk mjafton. Si dhe modelimi analitik, modelimi me simulatorë mund të lërë pa përfshirë disa detaje me që në të kundërt do kishim një simulim të pamanxhueshëm dhe do kërkohej aftësi e lartë përpunimi.

Një simulim mund të mendohet si një proces rrjedhes të entiteteve të rrjetit (psh. Nyjet, paketat etj.) Ndërsa entitetet lëvizin nëpër sistem, ato ndërveprojnë me entitete të tjera, i bashkohen disa aktiviteteve, trigerojnë ngjarje, i shkaktojnë disa ndryshime gjendjes së sistemit dhe dalin nga procesi. Herë pas here ato garojnë ose presin për një burim të caktuar. Kjo implikon që duhet të ketë një sekuencë llogjike ekzekutimi që të shkaktojë ekzekutimin e këtyre veprimeve në mënyrë të kuptueshme dhe të manaxhueshme. Një sekuencë ekzekutimi luan një rol të rëndësishëm në supervizimin e simulimit dhe ndonjëherë përdoret dhe për të karakterizuar tipin e simulimit.

5.2.1 Elementet e simulimit

Elementet kryesore të simulimit janë si më poshtë:

- *Entitetet* – Objektet që ndërveprojnë me njëritjetrin në një program simulimi për të shkaktuar ndryshime të gjendjes të sistemit. Entitetet dallojnë nga atributet që i vihen në përkatësi.
- *Burimet* – Këto janë zakonisht burimet që ndahen mes një grupi burimesh
- *Aktivitetet dhe ngjarjet* – Herë pas here entitetet përfshihen në disa aktivitete që krijojnë ngjarje dhe trigerojne ndryshime në gjendjen e sistemit (psh. Aktiviteti i pritjes në rradhë)
- *Skeduleri* – skeduleri mban listën e ngjarjeve dhe kohën e ekzekutimit të tyre
- *Variablat globalë* - Janë të kapshme nga çdo funksion ose entitet në sistem dhe mbajnë informacion mbi dia nga vlerat e përgjithshme të simulimit (psh. Numri total i paketave të transmetuara, gjatësia e rradhës së paketave etj.)

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

- *Gjeneratori* i numrave të rastësishëm (RNG – Random Number Generator) – Shërben poëpr të krijuar procese random përmes variablave random dhe marrjen kështu të të dhënave statistikore.
- *Mbledhësi i statistikave* – ka si qëllim kryesor mbledhjen e të dhënave nga simulimet.

5.2.2 Simulimet që varen nga koha

Janë simulime që vijnë në mënyrë kronologjike me ndihmën e një ore simulimi. Simulimi vazhdon deri sa ora arrin një vlerë të caktuar limit. Këto simulime mund të ndahen më tutje në: Simulime që drejtohen nga koha dhe Simulime që drejtohen nga ngjarjet.

Simulimet që drejtohen nga koha - Koha e simulimit avancon ekzaktësisht me një interval fiks njësisht kohe. Pas çdo avancimi të orës kontrollohet në se ka patur një ngjarje në këtë interval, në se po atëhere kjo ngjarje konsiderohet sikur ka ndodhur në fund të intervalit. Kjo përbën një problem në rastin kur ndodh më shumë se një ngjarje për interval me që duhet një procedurë për të përcaktuar se kush ngjarje duhet të ndodhi e para. Për lëtë arsye lëto simulime nuk këshillohen në rastet kur ngjarjet ndodhin në periudha të rastësishme kohore.

Simulimet që drejtohen nga ngjarjet - Ndryshe nga e para, avancimi I simulimeve bëhet nga një ngjarje në tjetrën dhe jo nga një interval në tjetrin. Ngjarjet zhvillohen sipas një rendi dhe koha midis dy ngjarjeve nuk është e njëjtë. Ndërkohë që simulimi avancon, një ngjarje mund të shkaktojë një ngjarje tjetër e cila do përfshihet në mënyrë kronologjike në zinxhirin e ngjarjeve ekzistuese. Simulimi vazhdon deri sa të përfundojë gjithë lista e ngjarjeve të përcaktuara ose deri sa të mbarojë koha e ekzekutimit.

5.3 Simulatori i Rrjetit 2 (Network Simulator 2 – ns2)

Ns-2 [25] është një simulator i drejtuar nga ngjarjet që mundëson studimin e natyrës dinamike të rrjetave kompjuterike. Falë fleksibilitetit dhe modularitetit ka fituar një popullaritet të madh në komunitetin kërkimor të rrjetave që nga lindja në 1989. Që nga atëhere janë bërë shumë rishikime të këtij mjete simulimi dhe ndër kontribuesit kryesorë mund të përmendim University of California dhe Cornell University të cilët zhvilluan bazat e këtij simulatori. Në këtë tezë është implementuar ns-BGP si një shtesë ndaj versionit të parafundit të simulatorit të rrjetit ns2-2.34. Duhet theksuar se mbi këtë shtesë është aplikuar një shtesë e dytë me emër ns-2.34-bgp 2.0 fild mrai. Kjo e fundit i shton funksionalitetin e Route Flap Damping si dhe Adaptive Minimal Route Advertisement Interval. Ns-2 është zhvilluar fillimisht në ISI (Universitetin e Kalifornisë së Jugut). Qëllimi kryesor i krijimit ishte si një shtesë ndaj simulatorit të rrjetit REAL. Ns-2 është

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

momentalisht pjesë e projektit VINT duke përfshirë USC/ISI, Xerox PARC, LBNL dhe UC Berkeley.

Si një nga simulatorët e eventeve diskretë më popullore, ns-2 suporton simulimin e TCP, rrugëzimeve dhe protokolleve *multicast* mbi rrjete me kabëll ose satelitorë. Ns-2 është shkruar si në C++ ashtu edhe në OTcl dhe suporton modelet e orientuara nga objekti. C++ përdoret për implementimin në nivel të ulët të procesimit të orientuar të paketave, ku performanca është më e rëndësishmja. OTcl është një gjuhë skriptimi për implementim të një niveli të lartë, ku fleksibiliteti është më i rëndësishëm. Një animator grafik i quajtur *nam* përdoret për të vizualizuar rezultatet e simulimit. Ai i kryen simulimet falë NAM dhe gjuhës së skriptimit AWK.

-NAM përfaqëson interpretuesin vizual të topogjisë së rrjetit duke kryer ekzekutime të drejtpërdrejta të skripteve Tcl.

-AWK nga ana tjetër është gjuhë programimi procesimi testesh.

5.3.1 Arkitektura e NS2

Arkitektura bazë për NS2 jepet në **Figura 5.1**. NS2 i ofron përdoruesve një komandë ekzekutimi ns e cila mer si argument një skript simulimi Tcl.

NS2 konsiston në dy gjuhë kryesore: C++ dhe *Object-oriented Tool Command Language* (OTcl). Ndërsa C++ përcakton mekanizmat e brendëshëm të objekteve të simulimit, Otcl ngre simulimin përmes assemblimit dhe konfigurimit të objekteve si dhe skedulimit të ngjarjeve diskrete. C++ dhe Otcl lidhen me njëra tjetrën përmes TclCl. Kur lidhen me një objekt C++, variablat në fushën OTcl njihen si 'doreza' (handle). Nga aspekti konceptual një 'dorezë' (psh n si doreza e Nyjes) është thjesht një stringë në fushën OTcl dhe nuk përmban asnjë funksionalitet. Funksionaliteti është i përcaktuar në objektin C++ të lidhur me të (psh. klasa Lidhës). E thënë në një gjuhë më të thjeshtë 'doreza' në fushën e OTcl mund të konsiderohet si pjesa e përparme (frontend) që ndërvepron me përdoruesit dhe objektet e tjera OTcl. Ajo mund të përcaktojë procedurat dhe variablat e veta për të lehtësuar ndërveprimin.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

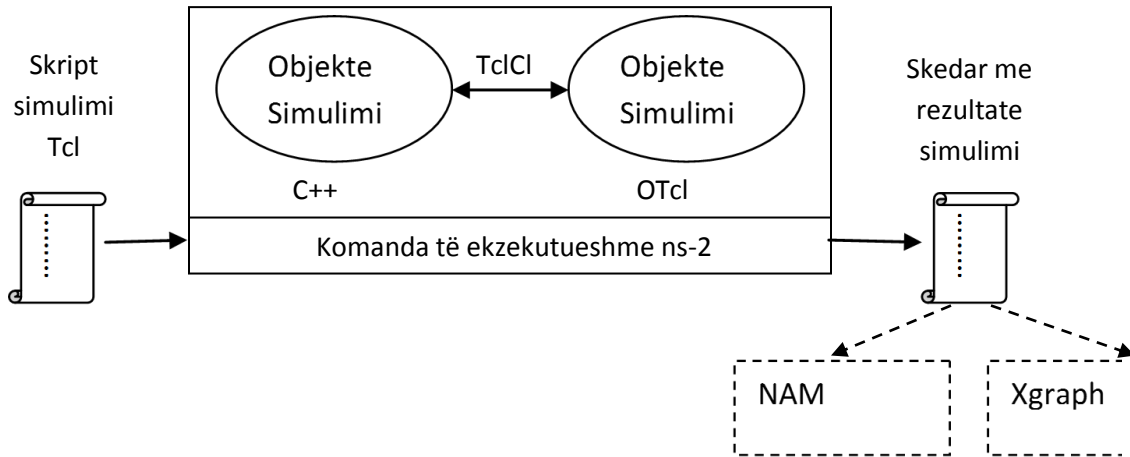


Figura 5.1: Arkitektura Bazë e ns-2

Pas simulimit NS2 nxjerr rezultatet në format teksti ose të animuar. Për ti interpretuar këto të dhëna grafikisht janë krijuar mjete si NAM (Network Animator) dhe *XGraph*. Për të analizuar një sjellje të caktuar të rrjetit, përdoruesit mund të nxjerrin një nënbashkësi të të dhënave në format teksti dhe ti transformojnë ato në një format më të kuptueshëm.

Klasat ns-BGP janë derivuar nga hierarkia ekzistuese e klasave ns-2. Si fillim do japim një përshkrim për strukturën e rrugëzimit *unicast* të simulatorit ns-2. Bazuar në këtë strukturë, do të përshkruajmë strukturën e ns-BGP së bashku me funksionalitet e tjera që ajo suporton. Për të rritur cilësinë e shërbimit (QoS), disa prej skedarëve janë modifikuar për të suportuar RFD. Kjo ndikon: 1) rrit stabilitetin dhe 2) rrit konvergencën e rrjetit.

5.3.2 Direktoritë e NS-2

Le të supozojmë se NS2 është instaluar në direktorinë *nsallinone-2.34*. **Figura 5.2** tregon strukturën e direktorive nën direktorinë *nsallinone-2.34*. Direktoria *nsallinone-2.34* është në nivelin e parë. Në nivelin e dytë, direktoria *tclcl-1.1.19* përmban klasat në TclCL (psh. Tcl, TclObject, TclClass).

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

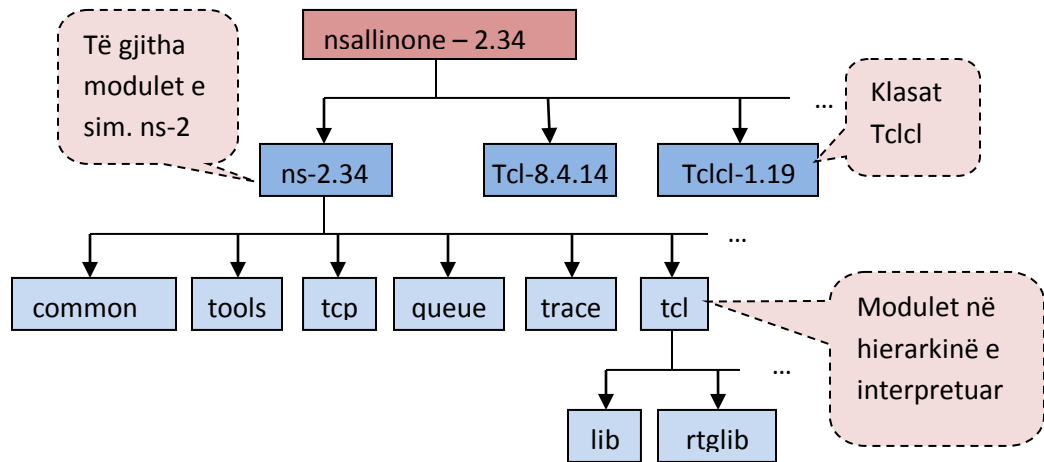


Figura 5.2: *Struktura e direktorive të ns2*

Në nivelin e tretë, modulet në hierarkinë e interpretuar janë nën direktorinë tcl. Më të përdorurit mes këtyre moduleve janë ns-lib.tcl, ns-node.tcl, ns-link.tcl etj. nën direktorinë lib të nivelit 4.

Modulet e simulimit në hierarkinë e kompiluar janë të klasifikuara në direktoritë e nivelit 2. Psh. Direktoria Tools mban klasa të ndryshme ndihmëse si gjeneratorët e variablave të rastësishëm. Direktoria Common, përmban modulet bazë që lidhen me avancimin e paketaave si simulatori, skeduleri, lidhësi dhe paketa.

5.3.3 Përdorimi i ns2

Përdorimi i ns2 kalon nëpër disa faza që përshkruhen dhe në figurën e mëposhtme:

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

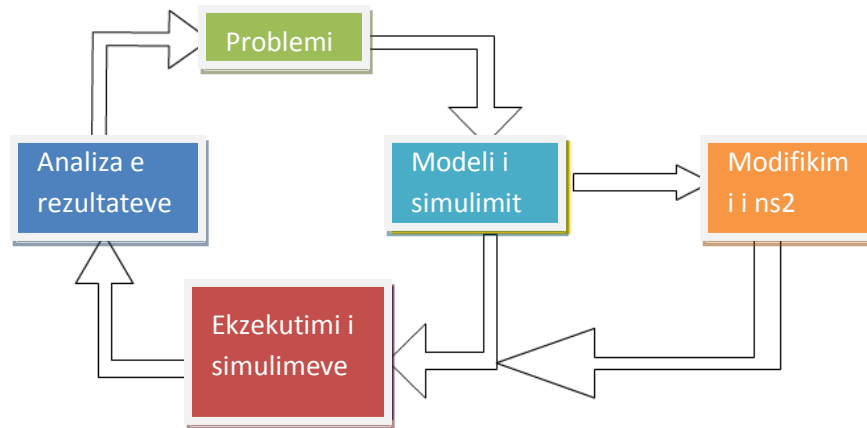


Figura 5.3: Hapat e përdorimit të ns2

Siç duket dhe nga figura hapi i parë është ai i përcaktimit në mënyrë të qartë të problemit që do trajtohet përmes simulimeve.

Në rastin konkret synohet të tregohet se momentet e rifreskimit të BGP vërtet mund të ndikojnë në cilësinë e shërbimit të thirrjeve VoIP. Për të zgjidhur këtë problem, hapi është evidentimi i modelit të simulimit. Ky model, si çdo ta trajtojmë dhe më vonë, përfshin modelimin e topologjisë, trafikut, të dhënave dhe skenarëve të simulimit. Secili nga këto modele mund të kërkojë implementimin e moduleve të reja në ns2. Paketa bazë e ns2 jo gjithmonë i përgjigjet kërkesave tona për simulim.

Pasi të jenë evidentuar modelet përkatëse dhe modifikimet e nevojshme për ns2 mund të kalohet në hapin pauses që ka të bëjë me realizimin e simulimeve. Siç kemi thënë dhe më sipër, kjo nënkupton krijimin e skedarëve përkatës tcl dhe ekzekutimin e tyre në ndprfaqen e ns2 përmes komandës `ns <skedar.tcl>`.

Për të parë rezultatet e simulimit gjenerohen skedarë me prapashtesën `.nam` që ekzekutohet përmes si një mjet grafik për vizualizimin e rezultateve të simulimit. Gjithashtu gjenerohen skedarët `.tr` (*trace file*) të cilët mundësojnë informacion më të plotë mbi simulimin, sipas figurës më poshtë:

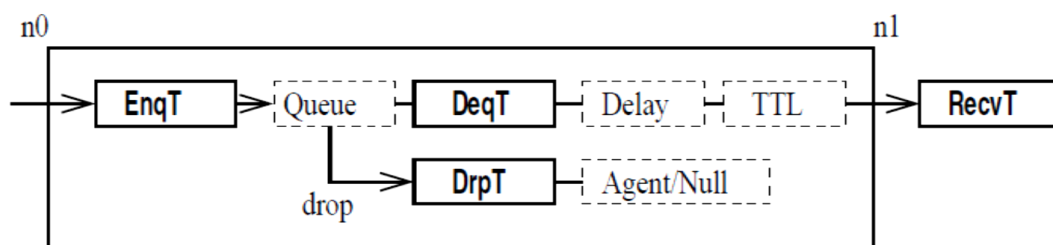


Figura 5.4: Objektet e regjistrimit në një link

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Tipi i fundit i skedarëve përbën një bazë shumë të mirë për nxjerrjen e rezultateve në kontekstin e vonesave dhe humbjes së paketave.

5.4 Modeli i simulimit

Kërkuesit që kërkojnë që përmirësojnë disa aspekte të funksionimit të Internetit shpesh i provojnë hipotezat e tyre duke përdorur disa forma simulimi por, të simulosh Internetin, nuk është aspak e thjeshtë. Diversiteti në administrimin teknik të tij, rritja e vazhdueshme dhe ndryshimet e vazhdueshme në kohë për sa i përket përdorimit të aplikacioneve, paraqesin vështirësi të pafundme për simulimin.

Analiza e aplikacioneve specifike është gjithashtu kuptimpolotë për ambjentet inter-domain, veçanërisht aty ku fokusi është në sjelljen e aplikacioneve që QoS ju varet nga ngarkesa inter-domain dhe vonesat. Kjo lloj analize në simulime nënkupton nevojën për modelim strukturor të aplikacionit dhe analiza në varësi të ngarseës e vonesave (modeli i të dhënave). E thënë ndryshe, kjo lloj analize kërkon përcaktimi i skenarëve për një simulim në kohë reale.

Të gjitha këto sa janë thënë më sipër mund të përmbliken në paragrafin e mëposhtëm:

Ambjenti i modelimit dhe simulimit bazohet në abstraksionin e përgjithshëm për trafikun inter-domain, QoS, topologjinë dhe rrugëzimin dhe teknika të ndryshme simulimi që përzgjidhen në përputhje me kërkesat.

Siç është përmendur në kapitullin e mëparshëm, studimet përmes simulimeve (në astin konkret në ambjentin e simulatorit të rrjetit ns2) kërkojnë ndjekjen e disa hapave themelorë, në funksion të një zhvillimi normal të studimit.

Pasi përcaktohet qartë problem që do trajtohet nevojitet të kalohet në fazën e modelimit dhe më pas të simulimit.

Në figurën më poshtë paraqiten në mënyrë të përmbledhur hapat që do të ndiqen për të realizuar procesin e modelimit dhe simulimit:

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

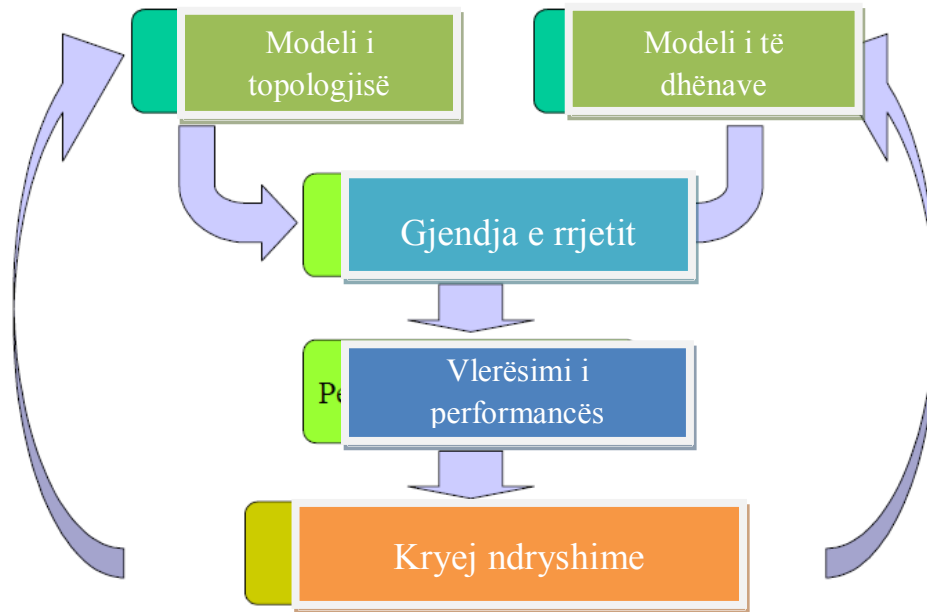


Figura 5.5: Diagrama rrjedhëse e metodologjisë së simulimeve

Sipas kësaj diagrame, hapi i parë është pikërisht modeli i cili përfshin:

- Modelimi i rrjetit – Ndërtimi i topologjisë së rrjetit dhe rrugëzimit
- Modelimi i të dhënave – Përcaktimi i karakteristikave të trafikut

Me të përcaktuar këto modele, marrëdhëniet ndërmjet elementeve të rrjetit dhe të dhënave përkatëse për çdo element, përftohet gjendja e rrjetit. Nga këtu, hapi pausës është vlerësimi i performancës, që përllorarit vlerat e QoS për rrjetin në studim.

Me të gjeneruar një pamje të performancës për një gjendje të caktuar rrjeti, realizohet një analizë e tipit “çfarë ndodh në se”, kjo analizë synon të evidentojë ndryshimet në vlerat e QoS kur ndryshohen komponentet e modelit të rrjetit ose të të dhënave.

5.5 Ndërtimi i modelit të rrjetit

Një rrjet karakterizohet nga dytribute kryesore: Topologjia dhe Rrugëzimi. Vetë rrjeti mund të paraqitet si një bashkësi nyjesh që ndërlidhen me njëra-tjetrën përmes linjave të komunikimit (link). Topologjia i referohet ndërlidhjes së nyjeve me njëra-tjetrën ndërsa rrugëzimi i referohet shtegjeve që ndiqen nga pëaketat për të kaluar nga një burim në atë destinacion. Përcaktimi i topologjisë dhe algoritmit të përshtatshëm të rrugëzimit kanë një ndikim të madh mbi performancën e shumë algoritmeve.

5.5.1 Topologjia e rrjetit

Simulimet e rrjetit ndikohen nga topologjitë e përdorura në simulim. Ky fakt qëndron he për simulimet e BGP ku forma dhe përmasat e topologjisë ndikojnë direkt në sjelljen e simulatorit. Përdorimi i topologjive të rrjetit BGP sa më reale është një element i rëndësishëm që ndikon në sjelljet e BGP në rast paqëndrueshmërisht.

Në pjesën më të madhe të simulatorëve të BGP topologjitë e përdorura janë ofrojnë abstraksion në nivel **Sistemi Autonom**. Nyjet e këtyre topologjive përfaqësojnë AS dhe topologjia komplekse e ruterave brenda AS-ve abstragohet në një ruter të vetëm që manaxhon komunikimin në këtë AS. Kjo lloj topologjie përftohet nga informacionet e nxjerra nga tabelat e rrugëzimit të BGP. Përpunime të mëtejshme mund ta ndajnë AS në AS të ndryshme llogjike të cilat do të përdoren për të paraqitur kompleksitetin e rrjetit brenda AS fillestare.

Modeli i topologjisë që do të përdoret në këtë punim synon që të riprodhojë sa më shumë të jetë e mundur paqëndrueshmëritë reale të internetit të sotëm. *Për këtë arsye është zgjedhur të përdoret një tip topologjie më afër realitetit, që mundëson paraqitje në nivel ruteri.*

Kjo lloj topologjie përdor ruterat (folësit BGP) si nyje elementare të të çdo AS-je. Këta folësa janë të lidhur me njëri tjetrin dhe sigurojnë lidhje ndërmjet AS-ve. Në këtë mënyrë nuk ka nevojë të krijojmë AS logjike. Topologjia është më reale. **Figura 5.2.1** më poshtë ilustron dallimin ndërmjet këtyre dy topologjive.

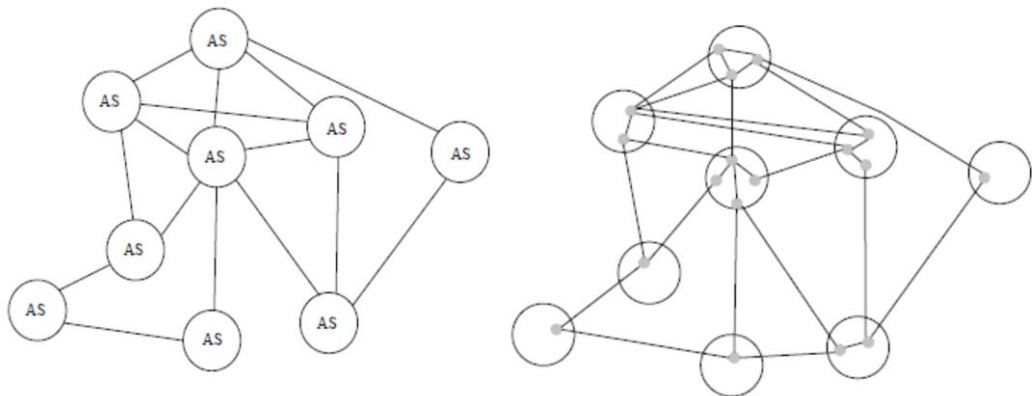


Figura 5.6: *Topologjia në nivel AS dhe topologjia në nivel ruteri*

Duke iu referuar kapitullit të dytë në këtë punim, Interneti përfaqësohet nga një hierarki që në dy nivelet kryesore të saj paraqitet përmes domain fundor dhe atyre tranzit. Topologjia e përzgjedur bazohet pikërisht në paraqitjen e këtyre dy niveleve kryesore të hierarkisë. Për të parë ndikimet që kanë rifreskimet e BGP në cilësinë e shërbimit të rifreskimeve VoIP fokusi kthehet tek folësit BGP që bëjnë të mundur komunikimin e

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

domaineve fundore me ato tranzit, të domaineve tranzit me njëri tjetrin apo domaineve fundore me njëri tjetrin.

Në vitet e fundit janë zhvilluar mjete të ndryshme që mundësojnë zhvillimin e modeleve për topologjinë e Internetit (gjeneratorë topologjie) dhe që përpiqen të paraqesin karakteristikat kryesore (nyjet dhe rrugëzimin) në mënyrë që të sigurojnë një ambient eksperimental sa më afër realitetit. Një gjenerator i mirë topologjie duhet të jetë i aftë të përfaqësojë këto karakteristika në mënyrë që topologjia e gjeneruar të jetë e ngjashme me atë të Internetit dhe rrugët të jenë të ngjashme në natyrë me ato të përshkuara në Internet.

Për të modeluar topologjinë në këtë punim do të përdoret gjeneratori i topologjive GT-ITM i cili i përbëhet nga specifikimeve të përmendura më sipër.

5.5.2 Struktura njëdrejtimore e rrugëzimit ns-2

Struktura e rrugëzimit *unicast* përbëhet nga dy plane: 1) atë të kontrollit dhe 2) atë të *forward*-imit. Në figurën 3.1 komponentët e planit të kontrollit janë të përfshira nga një trapezoid, ndërsa ata të planit të *forward*-imit janë qarkuar me një elips.

Plani i kontrollit ka për detyrë përlllogaritjen e rrugës, krijimin dhe mirëmbajtjen e tabelës së rrugëzimit. Gjithashtu, ajo implementon edhe algoritme specifike rrugëzimi. Komponentët kryesorë të planit të kontrollit janë: 1) llogjika e rrugës (*route logic*), 2) objekti i rrugës (*route object*), 3) entiteti i rrugës (*route peer*) dhe 4) protokollin e rrugës (*route protocol*).

1) Llogjika e rrugës është tabela qendrore e krijuar dhe që mirëmbahet për rrugëzim.

2) Objektet e rrugës përdoren vetëm në rastet e simulimit të rrugëzimeve dinamike. Objektet e rrugës që i shoqërohen një nyjeje sillen si koordinatorë për instancat e rrugëzimit të nyjes.

3) Një objekt i entitetit të rrugës vepron si një objekt mbajtës nga *protokolli i rrugëzimit*: ai ruan adresën e entitetit, metrikën si dhe preferencën për çdo rrugë të lajmëruar nga entiteti.

4) Protokollin e rrugëzimit implementon algoritme specifike rrugëzimi, si psh algoritmat vektor distance (*Distance Vector*) ose gjëndja e lidhjes (*Link State*).

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

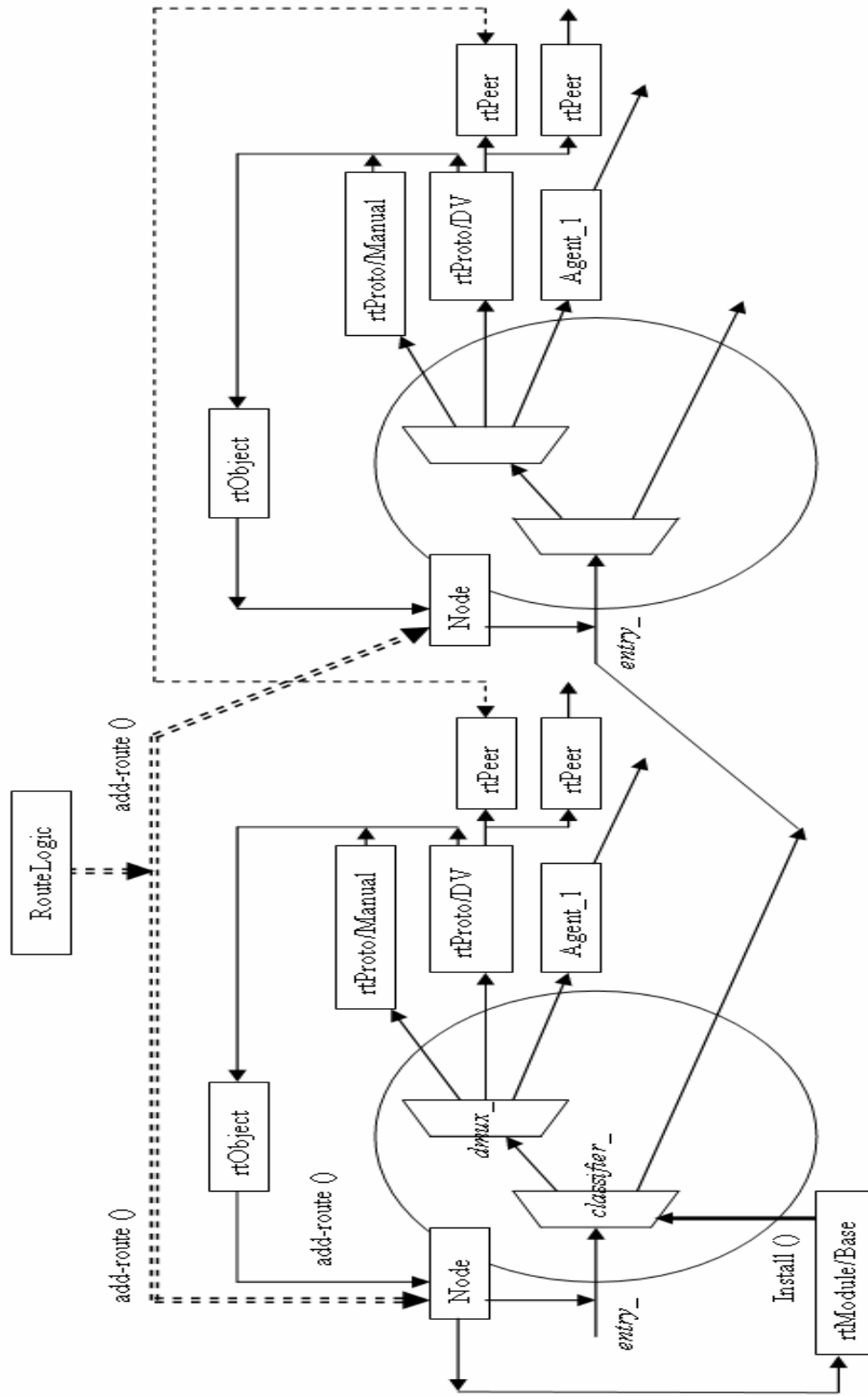


Figura 5.7 – Struktura njëdrejtimore e rrugëzimit në ns-2

Plani i *forward*-imit është përgjegjës për klasifikimin dhe *forward*-imin e paketave drejt nyjeve destinacion. Ai përfshin tipe të ndryshëm të klasifikuesve të lidhur si dhe të moduleve të rrugëzimit. Klasifikuesit (*classifier_*) dërgojnë paketat hyrëse ose në agjentin e duhur dalës ose drejt linjës dalëse. Moduli i rrugëzimit menaxhon klasifikuesin e nyjes dhe siguron një ndërfaqe për planin e kontrollit. Klasifikuesi i adresës (*classifier_*) dhe klasifikuesi i portës (*dmux_*) janë dy tipe të klasifikuesve në nyjen unicast të ns-2. Një *classifier_* ekzaminon adresën destinacion të paketës hyrëse dhe e çon përpara drejt *dmux_* nëse nyja është paketa destinacion. Në të kundërt, *classifier_* e dërgon paketën në një nyje më tutje. *dmux_* çon përpara paketën tek një agjent korrespondues me numrin e portës të paketës destinacion.

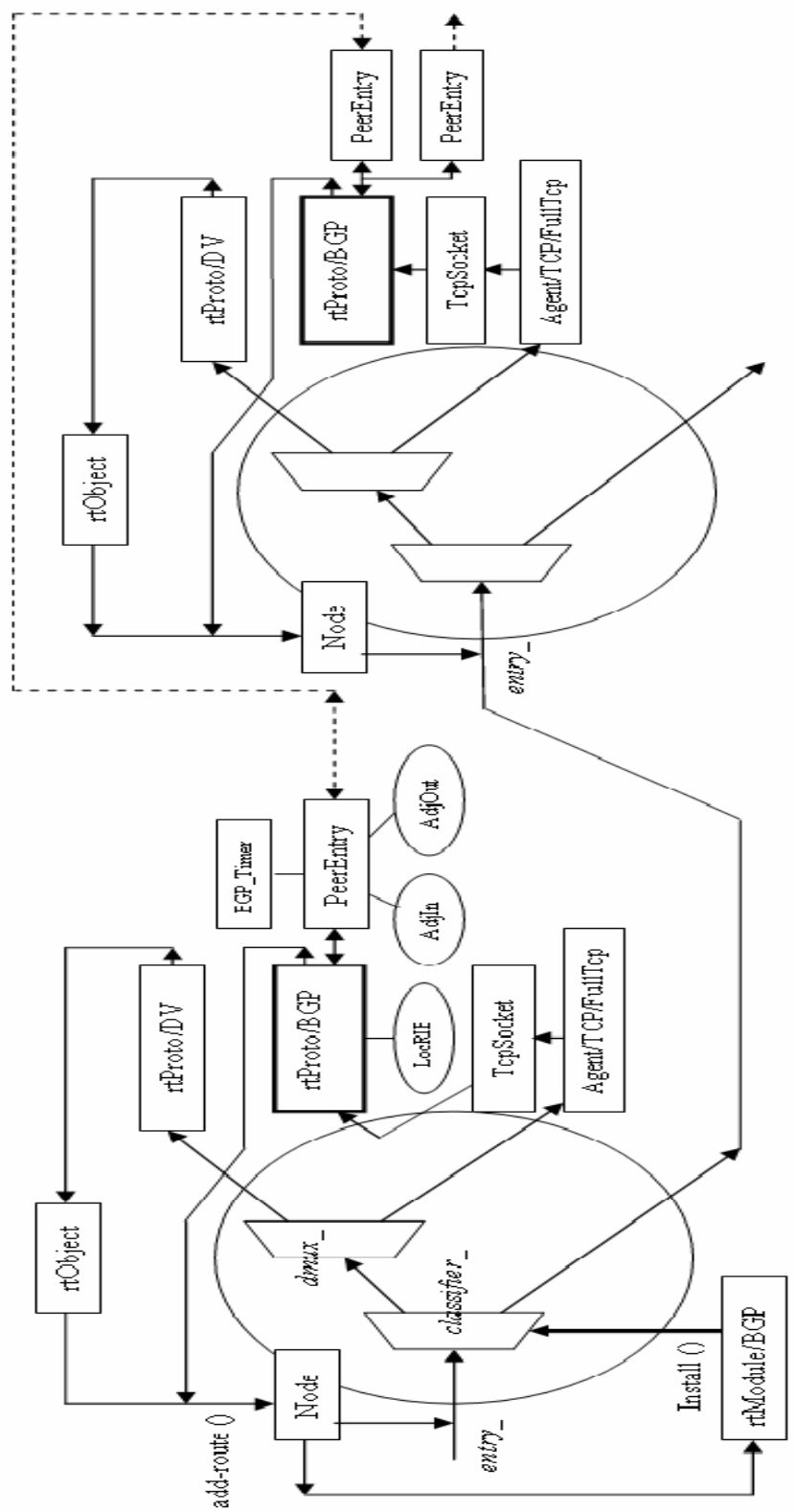
5.6 Struktura njëdrejtimore e rrugëzimit ns2-BGP

Nyja ns-BGP është bazuar në strukturën njëdrejtimore të rrugëzimit ns-2 si dhe në modelin SSF.OS.BGP4 të simulatorit SSFNet. Është importuar modeli SSF.OS.BGP4 në ns-2 dhe i janë shtuar funksionalitete si: shtresën *socket*, adresimin IPv4 dhe skemat e *forward*-imit të paketave.

Në mënyrë që të sigurojë mbështetje në nivel *socket* dhe në të njëjtën kohë të ruajë strukturën e SSF.OS.BGP4, gjithashtu u importua ns-2 *TcpSocket*, implementimi në nivel *socket* i SSFNet. Në mënyrë që të suportojë adresimin IPv4 dhe tejçimin përpara të paketave, klasifikuesi bazik i adresave është zëvendësuar me një të ri me emër *IPv4Classifier*. Për të suportuar transmetimin e të dhënave user, u modifikua *FullTcpAgent*, i cili është agjenti TCP për *TcpSocket*.

Në figurën 3.2 shfaqet struktura njëdrejtimore e rrugëzimit për ns-BGP. Klasifikuesi i adresave *classifier_* është *IPv4Classifier*. Një modul i ri rrugëzimi *rtModule/BGP* menaxhon *IPv4Classifier* dhe shërben si një zëvendësues për modulin bazë të rrugëzimit *rtModule/Base*. *TcpSocket* është shtuar tek *FullTcpAgent* i modifikuar, duke përfshirë shërbimet TCP në një ndërfaqe *socket*. Një protokoll i ri rrugëzimi *rtProtoBGP* bazohet në *TcpSocket* për transmetimin e paketave. *rtProto/BGP* ka nga një *PeerEntry* për çdo entitet. *PeerEntry* hap edhe mbyll një sesion komunikimi ndërmjet entiteteve si dhe shkëmben mesazhe BGP ndërmjet tyre.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Figura 5.8 – Struktura njëdrejtimore e rrugëzimit në ns2-BGP

Çdo instancë e *PeerEntry* përmban një *AdjIn*, një *AdjOut* dhe një variabël *BGP_Timer*. *LocRIB*, *AdjIn* dhe *AdjOut* korrespondojnë me tre pjesët e Rrugëzimit të Bazës së Informacionit (RIB) të BGP: *Loc-RIB*, *Adj-RIBs-In* dhe *Adj-RIBs-Out*. *BGP_Timer* siguron mbështetje për veçoritë e kohës BGP. Pesë klasat më të rëndësishme të ns-BGP janë: *TcpSocket*, *IPv4Classifier*, *rtModule/BGP*, *rtProtoBGP* dhe *BGP_Timer*.

5.6.1 Klasifikuesi IPv4

Ky klasifikues derivohet nga *Classifier*. Është implementuar si një nga klasat duale të ns-2, si në C++ ashtu edhe në OTcl. Klasifikuesi IPv4 përdor *map* nga libraria standarte e etaloneve të C++, për të ruajtur dhe kërkuar tabelën e rrugëzimit. Për të klasifikuar një paketë të pakompletuar, klasifikuesi IPv4, si fillim ekzaminon adresën destinacion të paketës dhe më pas përkon këtë adresë në tabelën e rrugëzimit të klasifikuesit në mënyrë që të gjejë rrugën me prefiksin më të gjatë të përputhjes.

5.6.2 rtModule/BGP

RtModule/BGP, një modul i ri rrugëzimi i implementuar në Tcl, siguron një ndërfaqe regjistrimi. Kur një nyjë është krijuar, modelet e rrugës aktive duhet të rregjistrohen së bashku me nyjen. Ky rregjistrim zëvendëson objektet klasifikuese ekzistuese në nyje.

5.6.3 rtProtoBGP

Klasa *rtProtoBGP* ose më saktë *Agent/rtProto/BGP* është implementuar si një klasë duale në ns-2. Një pjesë e kësaj klase implementon BGP-4 në një nyje. Ky protokoll i ri rrugëzimi kryen të gjitha operacionet e BGP, si psh: vendosjen e sesioneve ndërmjet entiteteve BGP, mësimi i rrugëve të ndryshme nëpërmjet folësve BGP të brendshëm dhe të jashtëm, zgjedhja e rrugës më të mirë dhe ruajtja e saj në tabelën e *forward*-imit të IP (*IPv4Classifier*) dhe menaxhimi i makinës me gjëndje të fundme BGP.

5.6.4 TcpSockets

Një *socket* është një Ndërfaqe e Programimit të Aplikacionit (API) e përdorur në komunikimin e rrjetave. Aplikacionet *socket* trajtojnë lidhjet e rrjeteve si përshkrues

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

skedarësh UNIX. Njëlloj me skedarët, nyjet fundore të komunikimit mund të shkruhet në to, të lexohen nga to dhe të fshihen.

Klasa *TcpSocket* është një implementim i API të *socket*, njëlloj me implementimet UNIX. Funkzionet kryesore të saj janë: *bind*, *listen*, *connect*, *close*, *read* dhe *write*. Ndërfaja e *TcpSocket* ka përfshirë implementime të thirrjeve bllokuese duke përdorur thirrjet Vazhduese (*Continuation*), një klasë që konsiston në dy funksione rithirrëse: *Success* dhe *Failure*. Struktura të dhënash dhe klasa të nevojshme, si klasat e rradhëve që ruajnë të dhëna dhe klasa *TcpData* që përmban të dhënat që transmetohen të përdoruesve, janë shtuar gjithashtu në ns-2. *FullTcpAgent* u modifikua duke marrë dhe dërguar paketa të dhënash që përmbajnë të dhënat e përdoruesve dhe për të informuar *Tcpsocket*-in korrespondues për ndryshimet në statusin e TCP.

U implementuan thirrjet bllokuese duke përdorur thirrjen *Continuation*, e cila është një mbajtëse e 2 thirrjeve prapavepruese: *Success* dhe *Failure*. Thirrjet e funksioneve bllokuese janë të përdorura gjërësisht në mjediset e programimit të rrjeteve. Për shembull, nëse një funksion përdoruesi është duke dërguar një paketë të dhënash duke përdorur shërbimet *socket*, thirrësi do të bllokohet derisa lidhja me *socket* të arrihet (kthen *Success* te funksioni thirrës) ose dështon (kthen *Failure* te funksioni thirrës). Performanca e rrjetit është shpesh e paparashikueshme, për shkak të bllokimit të trafikut. Në këto raste, thirrësi *Continuation* mund të sinkronizojë funksionin thirrës me atë që thirret.

Strukturat e mëposhtme të të dhënave dhe klasat janë shtuar për të suportuar *TcpSocket* të jetë i aftë me transmetimin e të dhënave të përdoruesve: klasa *SendQueue* që ruan të dhënat të cilat janë kërkuar për tu dërguar nga dërguesi agjenti TCP, klasa *ReceiveQueue* e cila ruan të dhënat e mara nga dërguesi si dhe klasën *TcpData* e cila përmban të dhënat e transmetuara nga përdoruesi.

5.6.5 BGP_Timer

Si klasë *BGP_Timer* është derivuar nga klasa tjetër në ns-2 e cila quhet *TimeHandler*. Kjo klasë ofron suport për veçoritë e kohës të BGP, siç janë kohësi *start-up*, kohësi *keep-alive*, kohësi *hold*, kohësi *Minimum Route Advertisement Intervali* (MRAI). Gjatë procesit të auto-konfigurimit, kohësi *start-up* është skeduluar për çdo agjent BGP. Kur kohësi *start-up* skadon, do të sjellë agjentin BGP (*rtProtoBGP*) që të përpiqet të krijojë lidhje me entitetet fqinjë të BGP. Kur një kohës *keep-alive* skadon, ai do të aktivizojë një agjent BGP që të dërgojë mesazhe të tilla tek entitetet e tjera. Skadencia e një kohësi *hold* tegon për dështimin e një agjenti BGP që të marrë një mesazh gjatë intervalit të kohës *hold* nga një entitet. Në këtë rast, agjenti BGP do të raportojë gabimin tek entiteti fqinj duke dërguar një mesazh të tipit *notification*. Kohësi MRAI përdoret për të zhvendosur me M sekonda (vlera standarte është 30 sekonda) përditësimet të njëpasnjëshme drejt të njëjtit destinacion.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

5.6.6 VecRoutes

Kjo klasë është pjesë përbërëse e shtesës që i ofrohet ns-BGP për ta shndërruar në ns-BGP-rfd. Qëllimi kryesor i saj përfshin krijimin e një vektori me rrugët që gjendet si dhe një grupi me metoda, të cilat do të veprojnë mbi të. Një pjesëtar i kësaj klase përmban një *route* si dhe një numër që i përkon rendit që ze në tabelën e rrugëzimeve *counts*. Funksionet kryesore të implementuara nga ky funksion janë:

1) *add (Route* r)* e cila shton një rrugë të re në tabelë si dhe inkrementon me 1 numrin e *counts*.

2) *clear()* e cila fshin të gjitha *route* nga tabela si dhe reseton *counts* në zero.

3) *find (Route* r)* kjo e fundit kërkon nëse *route-i* i kërkuar ndodhet në tabelën e rrugëzimit dhe nëse ky kusht përmbushet kthen rrugën së bashku me *counts*.

5.6.7 damp_reuse_timer

Qëllimi i kësaj klase është krijimi i një kohësi duke u bazuar në 3 elementë: *rtProtoBGP*, *DampInfo* dhe një kohe *t*, e cila quhet *suppressTime*. Kjo klasë përmban një funksion me të njëjtin emër, i icli thirret kur *suppressTime* skadon dhe përditëson statusin e rrugës që do të shënjohe si e papërdorshme. Në rast se *suppressTime* arrin maksimumin e lejuar atëherë ekzekutohet edhe njëherë procesi i vendimmarrjes për të përcaktuar nëse kjo rrugë do përdoret më apo jo. Dy funksionet e tjera që përmban kjo klasë janë *reset()* e cila e kthen vlerën e këtij kohësi në vlerën 0, si dhe *scheduled()* që tregon nëse kohësi është skeduluar që më parë dhe në këtë rast kthen *true* ose jo dhe kthen *false*.

5.6.8 dampInfo

Kjo klasë përmban një funksion me të njëjtin emër, i cili krijon informacion për heqjen e rruge. Nga parametrat kryesorë që nfikojnë në këtë vendim mund të përmend: *withdrawPenalty*, *changePenalty*, *suppressLimit*, *reuseLimit*, *half_Life* dhe *maxSuppressTime*. Për të parë sesi përdoren këto parametra mund të shohim një shembull si më poshtë:

1) \$bgp_agent0 dampening 0 0 3000 750 900 1000 500 3600

2) \$bgp_agent0 dampening

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Më sipër tregohen 2 komanda konfigurimi që mund të përdoren për të aktivizuar veçorinë *Route Flap Damping* (RFD), për një folës të veçantë BGP. Opsioni 1 do të aktivizojë RFD për një folës të veçantë BGP duke përdorur 8 parametrat e mëposhtëm:

- Parametri i parë shërben për të përcaktuar se cili algoritëm *Damping* përdoret (vetëm 5 vlera mund të përdoren: 0, 1, 2, 3 dhe 4 përkatësisht për *original RFD*, *selective RFD*, *RFD+*, *modified RFD* dhe *combined RFD*)
- Parametri i dytë shërben për të përcaktuar nëse rilajmërimi pas tërheqjes duhet të penalizohet (vetëm dy vlera mund të lejohen këtu: 0, e cila implikon që “rilajmërimi pas tërheqjes NUK penalizohet” dhe 1, e cila implikon që “rilajmërimi pas tërheqjes penalizohet”)
- Parametri i tretë është *suppressLimit* (3000 në rastin tonë)
- Parametri i katërt është *reuseLimit* (750 në rastin tonë)
- Parametri i pestë është *halfLife_dc* (900 sekonda në rastin tonë)
- Parametri i gjashtë është penaliteti për çdo tërheqje rruge (1000 në listën tonë të parametrave)
- Parametri i shtatë është penaliteti për çdo ndryshim në atributet e rrugës (500 në rastin tonë)
- Parametri i tetë është *maxSuppressTime* (3600 sekonda në listën tonë të parametrave)

Opsioni i dytë do të aktivizojë RFD tek një folës i veçantë BGP duke përdorur vlerat standarte. Vlerat standarte për të tetë parametrat janë si më poshtë: 0, 0, 2000, 750, 900, 1000, 500 dhe 3600. Këto më sipër janë vlerat standart të CISCO. Në këtë mënyrë komanda e konfigurimit: “\$bgp_agent0 dampening” është ekuivalente me “\$bgp_agent0 dampening 0 0 2000 750 900 1000 500 3600”.

5.7 Gjeneratori i topologjisë GT-ITM

GT-ITM (Georgia Tech Internet topology models) siç e përshkruan dhe emri, është një gjenerator topologjish për Internetin. Ai implementohet mbi SGB (Stanford Graph Base), një koleksion fleksibël strukturash të dhënash dhe algoritmesh për krijimin, ruajtjen dhe manipulimin e grafeve abstrakte. GT-ITM mbështet krijimin e grafeve rastësorë me disa lloje strukturash si dhe ruajtjen e këtyre grafeve në një format të transportueshëm. Modeli *transit-stub* i GT-ITM synon të krijojë topologji realiste me dy nivele hierarkie dhe pesha të përshtatëshme të ruterave kufitarë në mënyrë që të implementohet një politikë rrugëzimi standarde ndërmjet *domaine-ve*.

GT-ITM lejon që parametrat e grafit të specifikohen në një skedar konfigurimi. Përmes këtij skedari përcaktohen përmasat e grafit si dhe parametra të tjerë që përcaktojnë karakteristikat e grafit. Më poshtë paraqiten parametrat e konfigurueshëm:

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

- *Metoda e gjenerimit të tabelave të rrugëzimit:* Përdoruesi mund të specifikojë modelin e grafit rastësor që gjeneroet (psh. Në rastin konkret ky do të jetë modeli *transit-stub*).
- *Numri i grafeve:* Numri i grafeve që do të gjenerohen (me që grafet e ndërtuara janë rastësore dhe me që modeli i grafit ka një rëndësi të madhe në rezultatin përfundimtar, shpesh lind nevoja të gjenerohet më shumë se një model grafi) .
- *Burimi fillestar:* burimi për gjenerimin e numrave rastësorë për krijimin e grafit
- *Numri i stub domains për çdo transit domain:* Numri mesatar i domein-eve të tipit fundorë që do I lidhen një të tipit transit.
- *Lidhjet rastësore transit-stub:* Lidhje ekstra që shtohen ndërmjet domein-eve transit dhe atyre fundorë.
- *Lidhjet rastësore stub-stub:* Lidhje ekstra që vendosen ndërmjet domeineve fundorë.
- *Probabiliteti i lidhjeve të dyfishta ndërmjet domein-eve tranzit:* Nqs. ky parametër është 1, do të ketë lidhje të dyfishta ndërmjet AS-ve tranzit të lidhura. Çdo numër ndërmjet 0 dhe 1 do të tregojë probabilitetin që një lidhje e dyfishtë të ekzistojë.
- *Numri domein-eve tranzit:* Numri i domeineve që do të shërbejnë si tranzit.
- *Metoda e lidhjes:* Ky parametër specifikon mënyrën e vendosjes së lidhjeve ndërmjet domeine-ve transit (mund të jetë tërësiht rastësore, Waxman 1, Waxman 2, Doar Leslie, Eksponenciale dhe kolakiteti).
- *Dendësia e lidhjeve ndërmjet domein-eve tranzit:* Përcakton dendësinë e lidhjeve të domeineve tranzit. Nqs. Ky parametër merr vlerën një, atëherë çdo domein tranzit është e lidhur me gjithë të tjerët.
- *Numri mesatar i nyjeve në domein tranzit*
- *Metoda e lidhjes:* Ky parametër specifikon mënyrën e vendosjes së lidhjeve ndërmjet nyjeve të domeine-ve transit
- *Dendësia e lidhjeve ndërmjet nyjeve të domein-eve tranzit:*
- *Numri mesatar i nyjeve në domein fundorë*
- *Metoda e lidhjes:* Ky parametër specifikon mënyrën e vendosjes së lidhjeve ndërmjet domeine-ve fundorë
- *Dendësia e lidhjeve ndërmjet nyjeve të domein-eve fundorë*

Grafi i gjeneruar ruhet në formatin e skedarit Stanford Graph Base i cili më vonë mund të konvertohet në format të lexueshëm nga ns2 (kod tcl) përmes konvertuesit përkatës.

5.7.1 Modelimi i rrugëzimit

Përdorimi i gjeneratorit të topologjisë ofron mundësinë e përfimit të topologjive sa më afër me realitetin si dhe përbën një mjet praktik. Problemi qëndron në faktin se gjeneratorë si GT-ITM sigurojnë topologjinë e rrjetit por nuk mundësojnë modelimin e mënyrës se si paketat transmetohen në këtë rrjet. Për këtë arsye nevojitet që kjo pjesë të implementohet vetë nga përdoruesi.

Në rastin konkret, interesi bie mbi ruter-at që bëjnë të mundur komunikimin mes Sistemeve Autonome dheqë implementojnë protokollin e rrugëzimit BGP. Ajo që duhet modeluar është pikërisht mënyra se si këto rutera komunikojnë me njëri tjetrin përmes sesioneve eBGP, tabelat e rrugëzimit që ndërtojnë dhe mënyrën se si e shkëmbejnë informacionin.

Për fat të keq, BGP nuk ofron një modul të gatshëm për implementimin e BGP. Si rrjedhojë, duke ju referuar **Figura 4.3.3**, nevojitet të bëhen disa modifikime në kodin e ns2, në mënyrë që të instalohet moduli përkatës. Moduli i BGP për ns2, i njohur si ns-BGP, është përshtatur për ns2 në vitin 2004 [14] nisur nga modulet e BGP dhe TcpSocket nga SSFNet [26] dhe implementon versionin 4 të këtij protokollit (BGP-4). SSFNet është një simulator rrjeti i bazuar në Java që mundëson simulimet përmes një gjuhe konfigurimi të njohur si DML (*Domain Modeling Language*). Me që SSFNet është i bazuar në gjuhë Object Oriented, moduli i tij i BGP përbënte një pikë të mirë nisjeje për modulin e ns2.

Në ns2, rrugëzimi *unicast* arrihet duke përdorur planet e përcjelljes dhe të kontrollit. Plani i parë bën klasifikimin dhe përcjelljen e paketave në destinacion duke përdorur klasifikues dhe module rrugëzimi. Moduli i rrugëzimit manaxhon klasifikuesin e nyjes dhe ofron një ndërfaqe për planin e rrugëzimit. Klasifikuesit janë dy llojesh: klasifikues adrese dhe klasifikues porte. Klasifikuesi kontrollon adresën e paketës dhe e dërgon atë tek *dmux* nëse nyja është vetë destinacioni i paketës ose ja përcjell atë nyjes në vijim. *dmux* ja kalon paketën një egjenti në përputhje me portën destinacion të specifikuar. Ndërsa plani i dytë mundëson krijimin e rrugës, përpunimin, algoritmat e rrugëzimit dhe manaxhimin e tabelave të rrugëzimit. **Figura 5.2.3** ilustron strukturën unicast të ns-BGP bazuar në strukturën fillestare të unicast për ns2.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

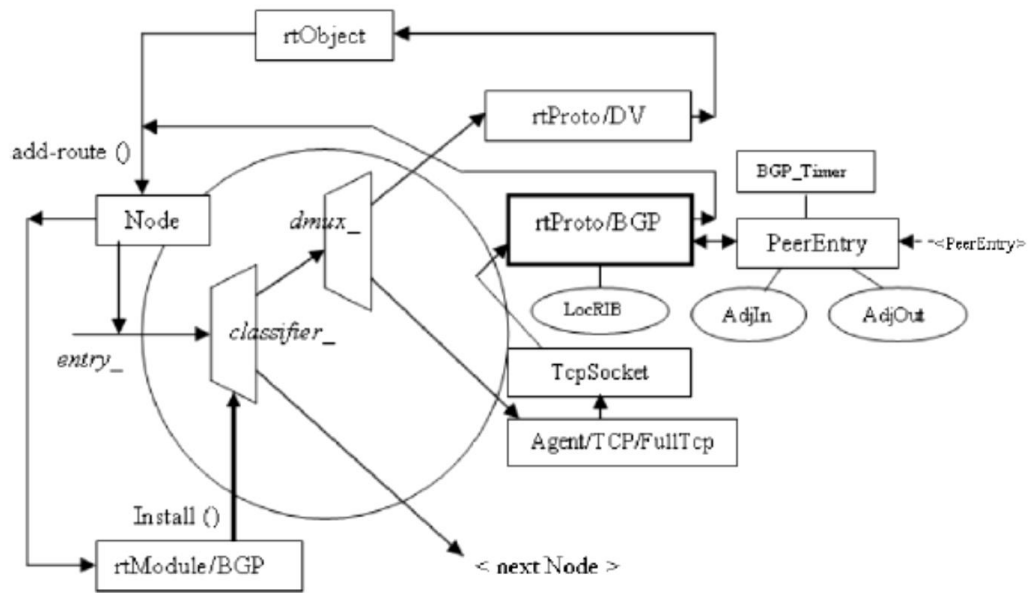


Figura 5.9: *Struktura unicast e ns-BGP*

Siç tregohet në figurë, modulet e klasifikimit si klasifikuesit e portës dhe të adresës, i dërgojnë paketat hyrëse në agjentin respektiv ose në një link dalës. Këto module në vetvete manaxhohen nga moduli i rrugëzimit.

Plani i kontrollit përbëhet nga componentët në vijim: llogjika e rrugës, objekti rrugëzimit, pala e rrugës dhe protokollin e rrugëzimit. Tabela qëndrore e rrugëzimit mirëbahet nga llogjika e rrugëzimit ndërsa objektet rrugëzimit përdoren në simulimet me rrugëzim dinamik. Objektet e palës së rrugëzimit enkapsulojnë protokollin e rrugëzimit duke kapur dhe mbajtur atributet e çdo rruge të lajmëruar. Së fundmi, nga componentët e protokollit të rrugëzimit janë implementuar dhe disa algoritma specifike rrugëzimi.

Për më tepër, me që nyja BGP derivon nga një nyje unicast ns, **Figura 5.2.3** parqet dhe përfshirjen e moduleve specifike të BGP dhe TcpSocket. Moduli rtModule/BGP manaxhon objektin IPv4Classifier ndërsa protokollin e ri rtProto/BGP, është vendosur në modulet e TcpSocket për transmetimin e paketave.

Për çdo pale komunikimi BGP alokohet një objekt i përdorur për të vendosur lidhjen, shkëmbyer mesazhe BGP dhe mbyllur sesionin.

Katër klasa kyçe të përdorura në implementimin e BGP janë:

TcpSockets

Një socket është një *Application Programming Interface* (API) e përdorur në komunikimet në rrjet. Aplikacionet socket i trajtojnë lidhjet në rrjet si përshkrues

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

skedarësh në UNIX. Në mënyrë të ngjashme me skedarët, skajet e komunikimit mund të shkruhen duke ofruar mundësi leximi ose fshirjeje.

Klasa *TcpSocket* është shtuar si një implementim i API të socket, e ngjashme me implementimet në UNIX. Funkzionet kryesore të saj janë *bind*, *dëgjo*, *lidhu*, *mbyll*, *lexo*, dhe *shkruaj*.

IPv4Classifier

IPv4Classifier derivohet nga klasa *Classifier*. çështë e implementuar sin një klasë e dyfishtë në ns2 (në C++ dhe OTcL). Kjo klasë përdor atë *map* nga libraritë standard të modeleve të C++ për të ruajtur dhe kërkuar në tableën e rrugëzimit. Për të klasifikuar një paketë në hyrje *IPv4Classifier* kontrollon adresen e destinacionit të paketës dhe përdor informacionin në tableën e rrugëzimit për të identifikuar rrugën.

rtModule/BGP

rtModule/BGP, është një modul i ri rrugëzimi i implementuar në Tcl që ofron një ndërfaqe regjistrimi. Kur një nyje krijohet informacioni duhet të regjistrohet dhe objektet ekzistuese *classifier* në nyje duhen zëvendësuar.

rtProtoBGP

Klasa *rtProtoBGP* (*Agent/rtProto/BGP*) implementohet si klasë e dyfishtë në ns2. Një instancë e kësaj klase implementon BGP-4 në një nyje. Ky protokoll i ri rrugëzimi realizon pjesën më të madhe të veprimeve të BGP: vendosja e sesionit të komunikimit BGP mes palëve, mësimi i shtegjeve të ndryshëm përmes folësive BGP, përzgjedhja e rrugës më të mirë dhe ruajtja e saj në tabelë (*IPv4Classifier*), dhe manaxhimi i makinës së gjendjeve të BGP.

Përfundimisht mund të thuhet se ns-BGP është në përputhje me RFC 1771.

Ky modul ofron mundësinë e përcaktimit të timer-ave (kohëzuesave) të BGP si dhe mundësinë për të zbatuar reflektuesit e rrugëve.

5.7.2 Ndërtimi i modelit të të dhënave.

Tipi i modelit të trafikut që përdoret për të kuptuar rrjedhën e trafikut në një rrjet, dhe niveli i përafrimit me realitetin, përbëjnë parametra jetësorë për rrjetin.

Analizimi i trafikut siguron informacione të tipit ngarkesa mesatare, kërkesat për gjerësinë e brezit në aplikacione të ndryshme etj. Modelet e trafikut i ndihmojnë projektuesit e rrjetit që të bëjnë supozime mbi rrjetin bazuar në një eksperiencë të kaluar dhe gjithashtu parashikime të performancës në përputhje me kërkesa të së ardhmes.

Në këtë punim është synuar që të evidentohet ndikimi që kanë momentet e rifreskimit të BGP në aplikacionet real-time dhe specifikuat në atë VoIP.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Për fat të keq ns-2 nuk disponon një modul të gatshëm të integruar për VoIP. Një modul i përdorur i VoIP për ns2 është Ns2Voip++, implementuar në Universitetin e Pizës [12]. Për fat të keq ekziston shumë pak informacion mbi përdorimin e këtij moduli. Gjithashtu, në përputhje me dokumentacionin ekzistues, ky modul ofron mundësinë e vlerësimit të performancës së thirrjeve VoIP në nivel përdoruesi, çka shkon përtej qëllimit të këtij punimi.

Në rastin konkret është përzgjedhur mënyra më e thjeshtë për modelimin e një trafiku në kohë reale, nisur dhe nga skema e mëposhtme për trafikun VoIP.

Struktura e një moduli VoIP jepet më poshtë, si në **Figura 5.3**.

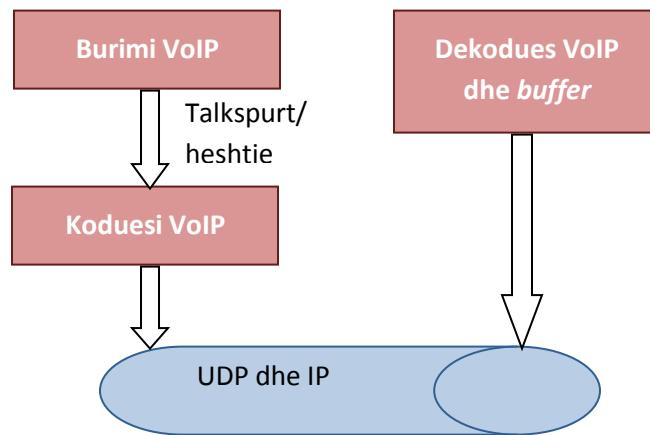


Figura 5.10: *Struktura e moduli të VoIP*

Në se do ta thjeshtonim këtë skemë, në nivel ns2, mund të themi semënyra më e thjeshtë për gjenerimin e trafikut VoIP është duke krijuar një agjent UDP të cilit i vihet në përkatësi trafik njëagjent në nivel aplikimi, CBR.

Për të përcaktuar parametrat e CBR përdoret **Tabela 5.3** e karakteristikave të koduesve të ndryshëm të VoIP.

Tabela 8: *Parametrat për koduesit e ndryshëm të VoIP*

Parameteat	G.711	G.723.1	G.729
Bit rate (Kbps)	64	6.3	8
Intervali mes frame (ms)	20	30	10
Sasia e të dhënave (Bytes)	160	24	10
Packeta/s, N_p	50	33	100

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Përfundimisht mund të dhemi së për qëllimet e këtij punimi trafiku VoIP modelohet sin jë rrjedhë të dhënash me një madhësi të caktuar pakëtë dhe rend transmetimi.

5.7.3 Gjendja e rrjetit dhe vlerësimi i performancës

Nisur nga diagram në **Figura 5.1**, pasi përcaktohet modeli i rrjetit dhe të dhënave, mund të përftojme gjendjen e rrjetit.

Ns2 është një simulator që varet nga koha dhe drejtohet nga ngjarjet. Për këtë arsye gjendja e rrjetit përftohet duke përcaktuar një moment fillimi dhe përfundimi të simulimeve, si dhe ngjarjet që do ndodhin në këtë kohë.

Në simulimet e këtij punimi është përzgjedhur që koha mesatare e ekzekutimit të një simulimi të jetë 80s. Simulimet fillojnë në çastin 0 dhe më pas zhvillohen me rradhë ngjarjet e ndryshme.

Grupi i parë i ngjarjeve është pikërisht shkëmbimi i informacionit të rrugëzimit mes nyjeve. Pasi nyjet shkëmbejnë informacionet me njëra-tjetrën, fillon transmetimi i trafikut CBR. Ky trafik do vazhdojë të dërgohet deri në përfundimin e kohës së simulimit.

Grupi i dytë i ngjarjeve është shfuqizimi dhe lajmërimi i vazhduesëm i një rruge tënjë ruteri. Kjo normalisht do të shoqërohet me një rifreskim të tabelave të rrugëzimit dhe do krijojë vonesa në rrjet si rrjedhojë e kohës së konvergencës të ruterave. Ky është dhe moment ku do të kontrollohen dy nga parametrat kryesorë të cilësisë: humbja e paketave dhe vonesat, pra realizohet vlerësimi i performancës.

5.7.4 Ndryshimet në model

Në mënyrë që të vlerësohet sa më saktë performanca, në përputhje me problemin e parashtruar, lind shpesh nevoja që disa nga parametrat e modeleve të ndryshohen.

Kjo nënkupton ndryshimin e numrit të nyjeve (simulimet fillestare kryhen gjithmonë me një numër shumë të kufizuar nyjesh në mënyrë që të testohen fillimisht skriptet e krijuara), skenarit të simulimit (psh. numrin e ngjarjeve dhe kohën e ekzekutimit të tyre), parametrat e koduesve etj.

5.8 Simulime dhe rezultate

Rezultatet e simulimit për arkitekturën e krijuar vlerësohen përmes skedarëve të ndryshëm që gjenerohen. Software i përdorur është Network Simulator version 2.34 (ns 3.34) mbi sistemin operativ Ubuntu 8.10.

5.8.1 Verifikimi i modelit të përzgjedhur të rrugëzimit

Për të verifikuar sjelljen e protokollit të implementuar të rrugëzimit kryhet një provë e thjeshtë me specifikimet në vijim.

Figura 5.11 tregon topologjinë e rrjetit të përdorur për simulim. Rrjeti përbëhet nga tre AS ku secila përfaqësohet nga një nyje: AS 0, AS 1, dhe AS 2 (nyjet 0,1 dhe 2 respektivisht). Adresa IP e çdo nyje tregohet në **Tabela 5.1**. Skema e adresimit është: 10.(AS nr).(numërnije).1.

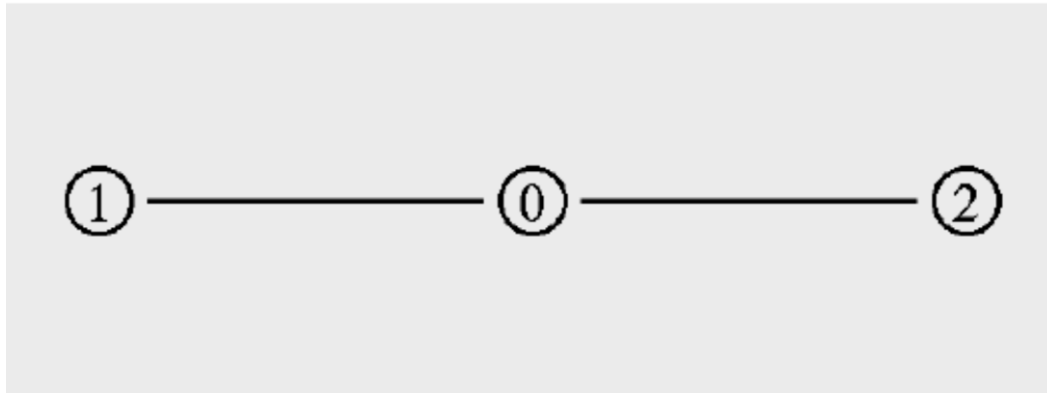


Figura 5.11: Topologjia e rrjetit

Tabela 9 : Adresat IP

node 0 10.0.0.1	10.0.0.1
node 1 10.1.1.1	1 10.1.1.1
node 2 10.2.2.1	2 10.2.2.1

Agjentët BGP konfigurohen në secilën prej tre nyjeve (0, 1, dhe 2). Për nyjet 0 dhe dy vlerat e intervaleve të *hold timer* dhe *keep-alive timer* janë ato default të specifikuara në RFC 1771 [15] (*hold time*: 90 s, *keep-alive* : 30 s). Për të parë sjelljen në situatë rilidhjeje, intervali i *keep-alive timer* për agjentin BGP në nyjen 1 mbahet në vlerën 200 s. Në këtë mënyrë, agjenti BGP në nyjen 0 nuk do të marrë mesazhin “mbaje lidhjen gjallë” brenda kohës dhe do kërkojë rivendosjen e lidhjes.

Në 0.25 s agjenti BGP në nyjen 0 lajmëron një rrugë të re për adresën IP 10.0.0.0/24. Në 0.35 s, agjenti BGP në nyjen 1 lajmëron një rrugë të re për adresën IP 10.1.1.0/24. Në 0.45 s, agjenti BGP në nyjen 2 lajmëron një rrugë për adresën IP 10.2.2.0/24. Në 28 s, 90.38 s, dhe 119.0 s, ns2 tregon tabelat e rrugëzimit për agjentët BGP. Simulimi përfundon më 120.0 s. Skedari *tcl* për këtë simulim është bashkangjitur në **Shtojca 1**.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

koha: 28

dump routing tables in all BGP agents:

BGP routing table of node0

BGP table version is 10, local router ID is 10.0.0.1

*Status codes: * valid, > best, i - internal.*

Network Next Hop Metric LocPrf Weight Path

**> 10.0.0.0/24 self - - -*

**> 10.1.1.0/24 10.1.1.1 - - - 1*

**> 10.2.2.0/24 10.2.2.1 - - - 2*

BGP routing table of node1

BGP table version is 16, local router ID is 10.1.1.1

*Status codes: * valid, > best, i - internal.*

Network Next Hop Metric LocPrf Weight Path

**> 10.0.0.0/24 10.0.0.1 - - - 0*

**> 10.1.1.0/24 self - - -*

**> 10.2.2.0/24 10.0.0.1 - - - 0 2*

BGP routing table of node2

BGP table version is 10, local router ID is 10.2.2.1

*Status codes: * valid, > best, i - internal.*

Network Next Hop Metric LocPrf Weight Path

**> 10.0.0.0/24 10.0.0.1 - - - 0*

**> 10.1.1.0/24 10.0.0.1 - - - 0 1*

**> 10.2.2.0/24 self - - -*

koha: 90.38

dump routing tables in all BGP agents:

BGP routing table of node0

BGP table version is 23, local router ID is 10.0.0.1

*Status codes: * valid, > best, i - internal.*

Network Next Hop Metric LocPrf Weight Path

**> 10.0.0.0/24 self - - -*

**> 10.2.2.0/24 10.2.2.1 - - - 2*

BGP routing table of node1

BGP table version is 42, local router ID is 10.1.1.1

*Status codes: * valid, > best, i - internal.*

Network Next Hop Metric LocPrf Weight Path

**> 10.1.1.0/24 self - - -*

BGP routing table of node2

BGP table version is 23, local router ID is 10.2.2.1

*Status codes: * valid, > best, i - internal.*

Network Next Hop Metric LocPrf Weight Path

**> 10.0.0.0/24 10.0.0.1 - - - 0*

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

```
*> 10.2.2.0/24 self - - -
```

Koha: 119

dump routing tables in all BGP agents:

BGP routing table of node0

BGP table version is 30, local router ID is 10.0.0.1

*Status codes: * valid, > best, i - internal.*

Network Next Hop Metric LocPrf Weight Path

```
*> 10.0.0.0/24 self - - -
```

```
*> 10.1.1.0/24 10.1.1.1 - - - 1
```

```
*> 10.2.2.0/24 10.2.2.1 - - - 2
```

BGP routing table of node1

BGP table version is 56, local router ID is 10.1.1.1

*Status codes: * valid, > best, i - internal.*

Network Next Hop Metric LocPrf Weight Path

```
*> 10.0.0.0/24 10.0.0.1 - - - 0
```

```
*> 10.1.1.0/24 self - - -
```

```
*> 10.2.2.0/24 10.0.0.1 - - - 0 2
```

BGP routing table of node2

BGP table version is 30, local router ID is 10.2.2.1

*Status codes: * valid, > best, i - internal.*

Network Next Hop Metric LocPrf Weight Path

```
*> 10.0.0.0/24 10.0.0.1 - - - 0
```

```
*> 10.1.1.0/24 10.0.0.1 - - - 0 1
```

```
*> 10.2.2.0/24 self - - -
```

Siç duket nga tabelat e rrugëzimit çdo agjent BGP mëson mbi agjentët e tjerë në sekondën e28-të. Në sekondën e 39.0 bie sesioni mes nyjes 0 dhe 1 dhe nyjet 0 dhe 2 e heqin rrugën për tek rrjeti 10.1.1.0/24 nga tabelat e tyre. Gjithashtu nyja 1 fshin rrugët që kishte për tek 0 dhe 2. Pasi rivendoset sesioni nyjet 0 dhe 1 shkëmbejnë gjithë informacionin që kishin në tabelat e rrugëzimit dhe konvergjojnë për herë të dytë. Ky testim verifikon korrektësinë e modelimit të protokollit të rrugëzimit.

5.8.2 Simulimi i topologjisë Stub-Domain me trafik CBR

Topologjia e përdorur në simulim jepet në figurën si më poshtë:

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

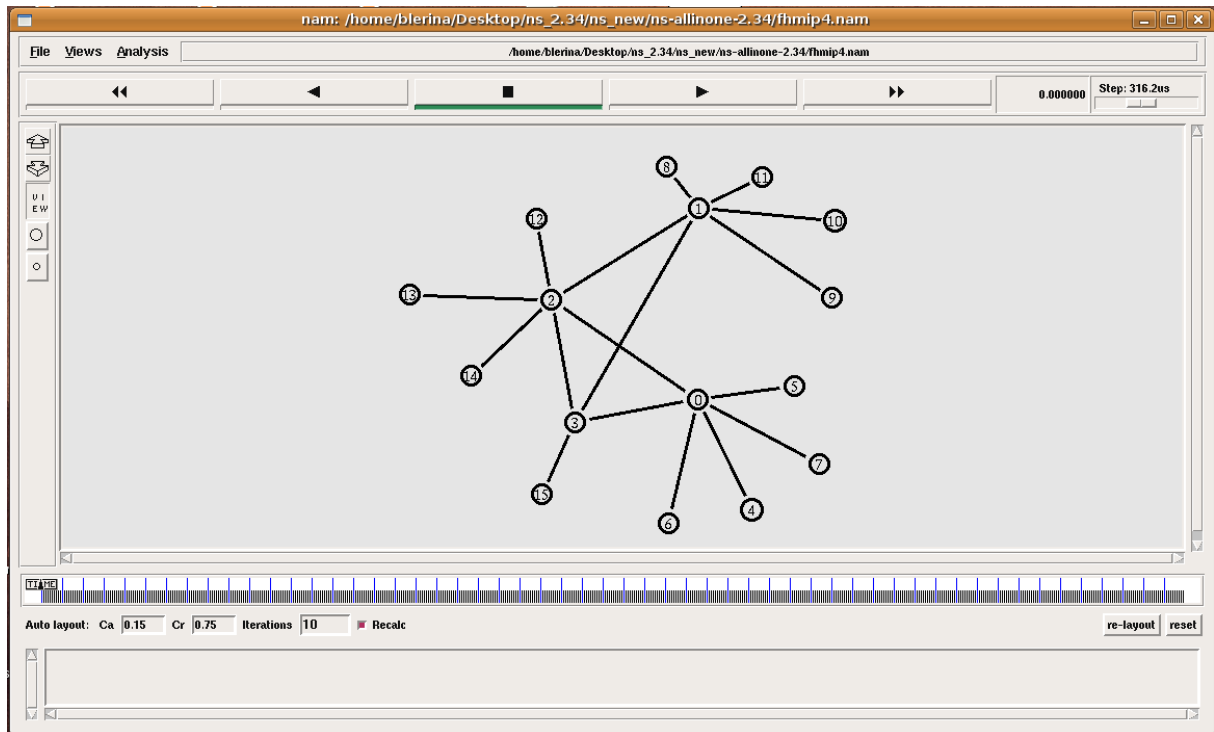


Figura 5.12: Topologjia e rrjetit sipas modelit stub-domain

Sic e kemi përmendur më sipër topologjia është gjeneruar përmes GT-ITM sipas modelit Transit-Stub të Internetit. Moduli i rrugëzimit nuk ofron shumë mundësi përshatjeje në rast numri të madh nyjesh dhe si rrjedhojë kemi zgjedhur opsionin e modelimit të një nëngrafi të Internetit.

Ky nëngraf përbëhet nga një *domein* tranzit që përbëhet nga katër nyje (rutera BGP) dhe nga 12 *domein* fundorë që modelohen me nga një ruter secili (përkufizimi për sistemin autonom përcakton se aim und të përbëhet nga 1 ose më shumë rutera).

Tabela 10 : Karakteristikat e grafit

Lloji i AS	Numri i AS	Numri i nyjeve	Nyjet
AS tranzit	1	4	0,1,2,3
AS fundorë	12	12	4,5,6,..15

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Kjo topologji gjenerohet nga skedari në hyrje të GT-ITM që është bashkëlidhur në **Shtojca 2**.

Në total kemi 16 nyje. Siç e tregon Tabela 6.2 domein tranzit është modeluar me 4 nyje që shkëmbejnë komunikimin BGP me njëra tjetrën. Të katërt këta janë ruterat kufitarë (edge). AS tranzit është e organizuar me një *cluster* dhe me dy reflektues rrugësh që janë nyjet 2 edhe 3. Kjo topologji gjenerohet nga skedari në hyrje të GT-ITM që është bashkëlidhur në **Shtojca 2**. Për AS fundor është zgjedhur llogjika e paraqitjes së tyre me nga një nyje. Kjo është në përputhje me përkufizimin që kemi thënë për AS i cili mund të përbëhet nga 1 ose më shumë nyje.

Skema e adresimit është përzgjedhur në trajtën 10.0.\$i.1 për ruterat brenda AS tranzit, ku \$i është numrin nyjes (0,1,2 apo 3) dhe 10.\$j.\$i.1 për ruterat në AS stub, ku \$j përkon me numrin e AS dhe \$i me numrin e nyjes (4,5..15).

Konfigurimi i rrjetit realizohet si më poshtë:

- Agjentët BGP konfigurohen në sejcilën prej nyjeve. Vlerat e intervaleve të *hold timer* dhe *keep-alive timer* janë ato default (*hold time*: 90 s, *keep-alive* : 30 s).
- Agjentët UDP konfigurohen në nyjet 0 (burimi) dhe 1 pusi. Trafiku nëpër këto dy nyje kalon përmes nyjes 2, sipas tabelave të ndërtuara të rrugëzimit.
- Trafiku CBR modelohet me këto karakteristika: *packetSize_ 160*, *interval_ 0.02* dhe *rate_ 64kb* sipas koduesit G.117 (referoju Tabela 4 dhe Shtojca 3).

Pasi bëhet konfigurimi i nyjeve, hapi pasues është përcaktimi i ngjarjeve të skeduluara. Në këtë simulim duam të shikojmë kohët e konvergencës të tre ruterave të përfshirë në komunikim që janë n15, n3 dhe n2. Ngjarjet skedulohen si më poshtë:

Në 5.0 fillon transmetohet trafiku CBR

Në 6.0 agjenti 15 tregon tabelën e rrugëzimit

Në 30.0 agjenti 3 tregon tabelën e rrugëzimit

Në 30.0 agjenti 2 tregon tabelën e rrugëzimit

Në 35.0 agjenti 15 lajmëron rënien e rrjetit 10.12.15.0/24"

Në 36.0 agjenti 15 tregon tabelën e rrugëzimit

Në 36.0 agjenti 3 tregon tabelën e rrugëzimit

Në 36.0 agjenti 2 tregon tabelën e rrugëzimit

Në 36.0 agjenti 15 network 10.12.15.0/24"

Në 55.0 agjenti 15 no-network 10.12.15.0/24"

Në 62.0 agjenti 3 tregon tabelën e rrugëzimit

Në 62.0 agjenti 2 tregon tabelën e rrugëzimit

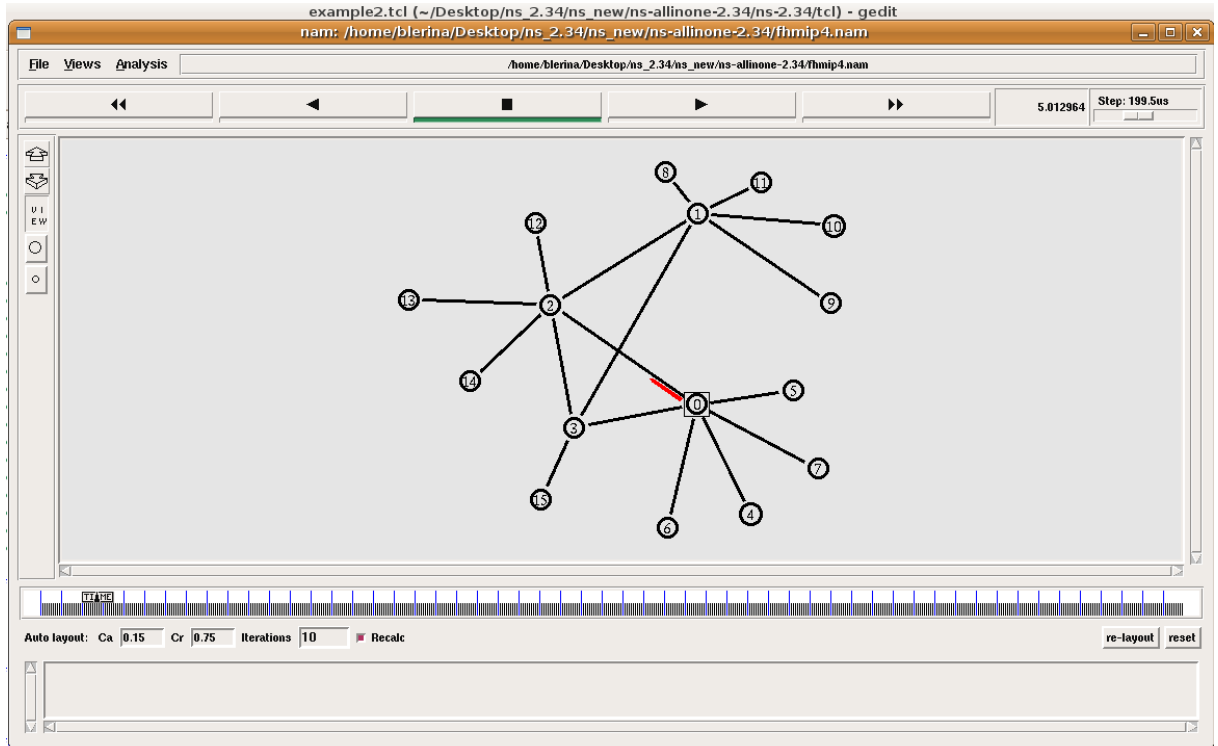
Ngjarja e fundit është realizuar me synimin për të parë sjelljen e sistemit në një situatë kur një rrugë shfaqet dhe shkëputet vazhdimisht brenda një kohe të shkurtër (rute flapping).

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Në këtë mënyrë do të vërehet në se ka humbje apo vonesa në paketa gjatë momentit të rifreskimit të tabelave të rrugëzimit BGP.

5.8.3 Rezultatet e simulimit

Përmes ambientit vizual Nam, shohim që paketa e parë CBR gjenerohet në



sekondën 5.0:

Figura 5.13-a: Dërgohet paketa e parë CBR

Në sekondën 35.0 shohim që dërgohet informacioni për rënien e një rruge nga nyja 15.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

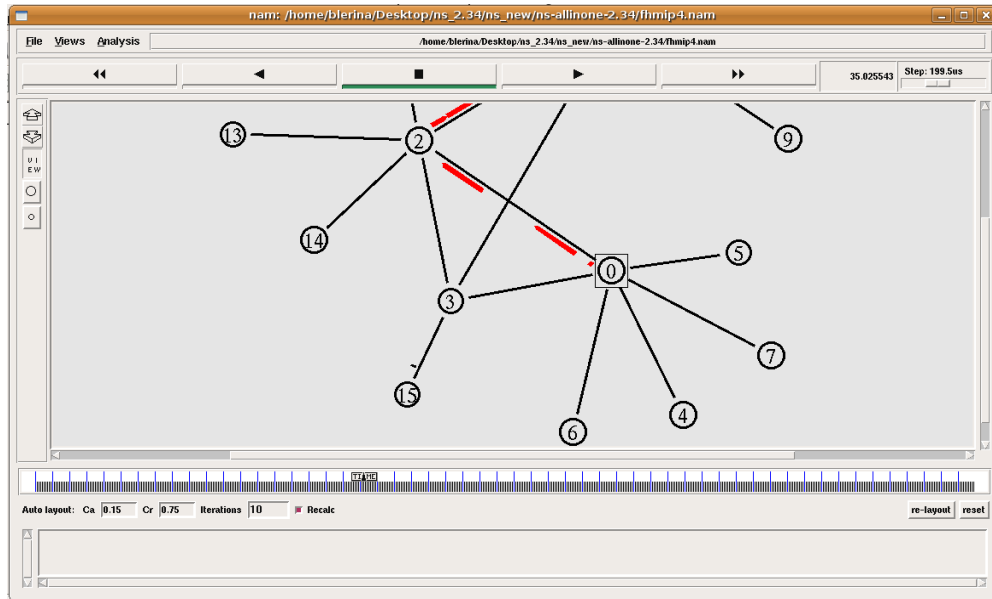


Figura 5.13-b: Dërgohet informacioni i rrugëzimit

Nyja 3 mëson për rënien e nyjes 15 dhe ia përcjell informacionin fqinjëve të saj:

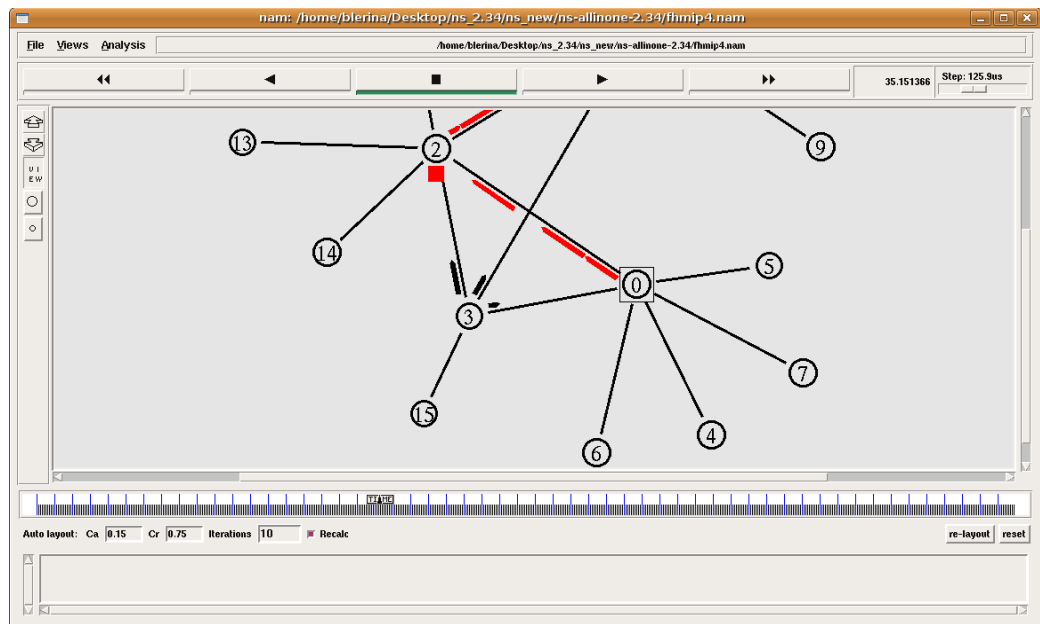


Figura 5.13-c: Shpërndahet informacioni rrugëzimit

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Gjatë ekzekutimit në ekran na shfaqen të dhënat e mëposhtme për tabelat e rrugëzimit:

Nyja 2 lajmëron nyjen 13 për ndryshimet në rrugëzimit si në figurën më poshtë:

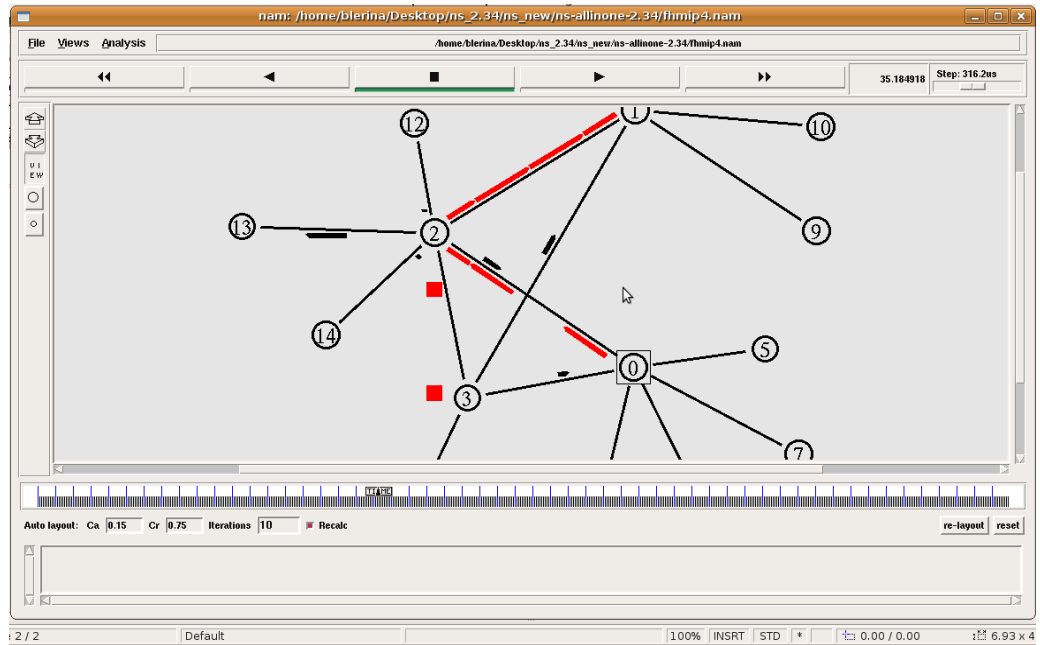


Figura 5.13-d: Shpërndahet informacioni rrugëzimit nga nyja 2

Ndërkohë tabelat e rrugëzimit në moment të ndryshme na paraqiten si më poshtë:

Koha: 30

BGP routing table of n3

BGP table version is 14, local router ID is 10.0.3.1

*Status codes: * valid, > best, i - internal.*

Network Next Hop Metric LocPrf Weight Path

```

10.0.0.0/24 self - - -
10.1.4.0/24 10.0.0.1/32 - - -1 i
10.2.5.0/24 10.0.0.1/32 - - -2 i
10.3.6.0/24 10.0.0.1/32 - - -3 i
10.4.7.0/24 10.0.0.1/32 - - -4 i

```

.....

```

10.10.13.0/24 10.0.2.1/32 - - -10 i
10.11.14.0/24 10.0.2.1/32 - - -11 i
10.12.15.0/24 10.12.15.1/32 - - -12

```

BGP routing table of n2

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

BGP table version is 12, local router ID is 10.0.2.1

*Status codes: * valid, > best, i - internal.*

<i>Network</i>	<i>Next Hop</i>	<i>Metric</i>	<i>LocPrf</i>	<i>Weight</i>	<i>Path</i>
<i>10.0.0.0/24</i>	<i>self</i>	-	-	-	
<i>10.1.4.0/24</i>	<i>10.0.0.1/32</i>	-	-	- 1	<i>i</i>
<i>10.2.5.0/24</i>	<i>10.0.0.1/32</i>	-	-	- 2	<i>i</i>
.....					
.....					
<i>10.10.13.0/24</i>	<i>10.10.13.1/32</i>	-	-	- 10	
<i>10.11.14.0/24</i>	<i>10.11.14.1/32</i>	-	-	- 11	
<i>10.12.15.0/24</i>	<i>10.0.3.1/32</i>	-	-	- 12	<i>i</i>

Nga këto të dhëna shohim se në sekondën e 30, agjentët 3 dhe 15 kanë konvergjuar dhe kanë një informacion të qartë për rrjetin.

Në sekondën 35 është lajmëruar rënia e rrjetit 10.12.15.0/24. Nyjet 2 dhe 3 e heqin rrugën për tek ky rrjet nga tabelat e rrugëzimit.

Në sekondën 36 rruga ngrihet prapë dhe nyjet 2 dhe 3 duhet të konvergjonin në sekondën 60 por në sekondën 55 rruga bie sërish. Nyja 15 e lajmëron përsëri rrjetin që rruga u ngrit. Të gjitha këto rënie dhe ngritje të shpeshta të rrugës shkaktojnë dërgim të shpeshtë paketash që nga ana e tyre konsumojnë gjerësinë e brezit dhe aftësitë përpunuese të nyjeve. Me që moduli i programuar nuk ka mekanizma për “route flap damping” rrjeti kalon në një gjendje divergjence që nuk arrin të zgjidhet brenda 80 sekondave të përzgjedhura për simulim.

Pas përfundimit të simulimeve elementi i parë që merret në konsideratë është numri i paketave të humbura para se të skedulohet ngjarja e paqëndrueshmërisë dhe pas skedulimit të kësaj ngjarjeje. Nga skedarët e regjistrimit del se në rastin kur simulimi kryhet pa praninë e ngjarjeve që shkaktojnë luhajtje të rrugës paketat e humbura janë në nivelin 776. Pasi ndodhin ngjarjet e përmendura më sipër ky numër shkon në 797. Kjo do të thotë se niveli i humbjeve në paketa është rritur me 21 brenda 100 sekondave të simulimit.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

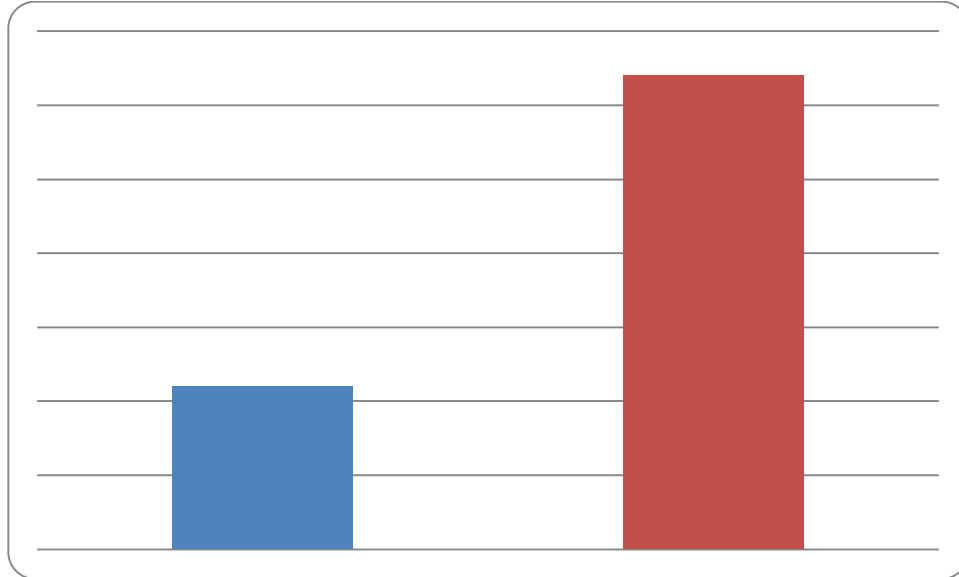


Figura 5.14: Humbjet në paketa

Përfundime

Një simulim mund të mendohet si një proces rrjedhes të entiteteve të rrjetit. Ns-2 [25] është një simulator i drejtuar nga ngjarjet që mundëson studimin e natyrës dinamike të rrjetave kompjuterike. Në këtë tezë është implementuar ns-BGP si një shtesë ndaj versionit të parafundit të simulatorit të rrjetit ns2-2.34. Duhet theksuar se mbi këtë shtesë është aplikuar një shtesë e dytë me emër *ns-2.34-bgp 2.0 fld mrai*. Kjo e fundit i shton funksionalitetin e *Route Flap Damping* si dhe *Adaptive Minimal Route Advertisement Interval*. Ns-2 është shkruar si në C++ ashtu edhe në OTcl dhe suporton modelet e orientuara nga objekti. C++ përdoret për implementimin në nivel të ulët të procesimit të orientuar të paketave, ku performanca është më e rëndësishmja. OTcl është një gjuhë skriptimi për implementim të një niveli të lartë, ku fleksibiliteti është më i rëndësishëm. Pas simulimit NS2 nxjerr rezultatet në format teksti ose të animuar. Për ti interpretuar këto të dhëna grafikisht janë krijuar mjete si NAM (Network Animator) dhe *XGraph*. Për të analizuar një sjellje të caktuar të rrjetit, përdoruesit mund të nxjerrin një nënbashkësi të të dhënave në format teksti dhe ti transformojnë ato në një format më të kuptueshëm. Për të rritur cilësinë e shërbimit (QoS), disa prej skedarëve janë modifikuar për të suportuar RFD. Kjo ndikon: 1) rrit stabilitetin dhe 2) rrit konvergjencën e rrjetit. Përdorimi i ns2 kalon nëpër disa hapa që nisnin fillimisht me identifikimin e problemit, vijon me ndërtimin e modelit të simulimit, kalon me modifikimin e ns2, pasohet nga ekzekutimi i simulimeve dhe përfundon me analizën e rezultateve. Në situatën tonë objektivi është të vihet në dukje se momentet e rifreskimit të BGP vërtet mund të ndikojnë në cilësinë e shërbimit të thirrjeve VoIP. Për të kapërcyer këtë problem, hallka vijuese është evidentimi i modelit të simulimit. Ky model, përfshin modelimin e topologjisë, trafikut, të dhënave dhe

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

skenarëve të simulimit. Secili nga këto modele mund të kërkojë implementimin e moduleve të reja në ns2. Pasi të jenë evidentuar modelet përkatëse dhe modifikimet e nevojshme për ns2 mund të kalohet në hallkën pausese që konsiston me realizimin e simulimeve që nënkupton krijimin e skedarëve përkatës tcl dhe ekzekutimin e tyre në ndërfaqen e ns2 përmes komandës ns <skedar.tcl>. Për të parë rezultatet e simulimit gjenerohen skedarë me prapashtesën .nam që ekzekutohen si një mjet grafik për vizualizimin e rezultateve të simulimit. Gjithashtu gjenerohen skedarët .tr (*trace file*) të cilët mundësojnë informacion më të plotë mbi simulimin.

Kapitulli VI

Realizimi dhe interpretimi i pyetësorit

6.1 Hyrje

Edhe kapitulli i gjashtë konsiderohet si një kapitull metodologjik. Pasi kemi shtjelluar në nivel teorik dhe në kuadrin eksperimental internetin, karakteristikat e tij, aplikacionet në kohë reale dhe protokollin BGP në vazhdimësi do të ndalemi në rastin konkret të një anketë të drejtuar përdoruesve të internetit nga të cilët janë marrë në shqyrtim studentët e UET dhe përjasjen që ata kanë ndaj cilësisë së shërbimit të internetit që ofrohet nga ISP-të në Shqipëri.

Nga të dhënat empirike të studimit të shtrirë në plotëaimin e anketave nga 524 studentë.

Analiza jep një studim të lidhjes mes variablave të varur e atyre të pavarur që janë respektivisht cilësia e shërbimit dhe teknologjia, shërbimi ndaj klientit e kompania shpërndarëse e internetit.

Dimë që anketat ndahen në dy kategori:

Në anketa përgjigjet e të cilave janë numra dhe në anketa përgjigjet e të cilave janë fjalë.

Në tipin e dytë ku përgjigjet janë fjalë bën pjesë dhe anketa jonë. Në këtë rast variablat konsiderohen variabla kategorikë dhe duke qenë se i përkasin këtij tipi mund të analizohen tre çështje sikurse janë:

1-numri i elementeve që përfshin frekuencën e përgjigjeve për një kategori të caktuar

2-përqindja që shpreh numrin e elementeve të pikës paraardhëse

3-grafikët përkatës që pasqyrojnë këto përgjigje

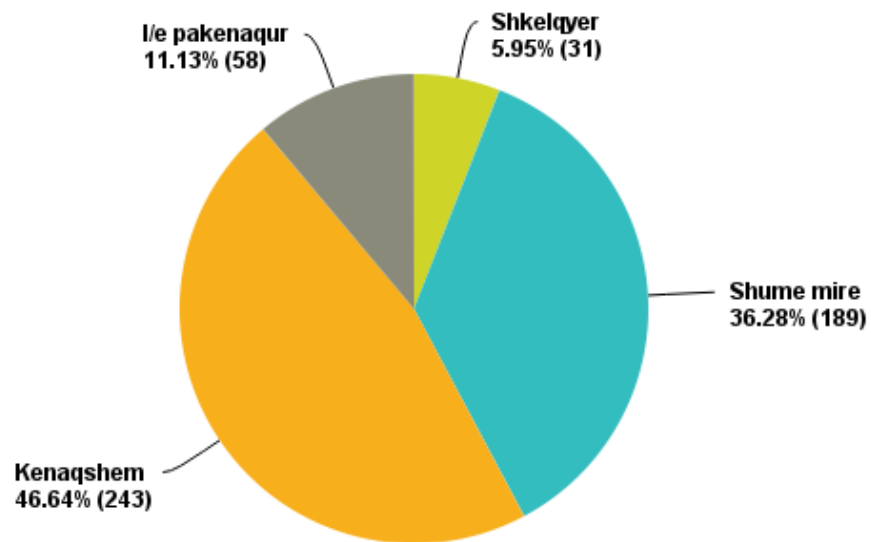
Nisur nga këto rezultate jemi në gjendje të përcaktojmë dhe variablat e kushtëzuar nëse janë apo jo të pranishëm si edhe të gjykojmë mbi prezencën e pavarësisë midis variablave, pra a ndikon një variabël në një tjetër apo jo.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Rezultatet e pyetësorit i kemi si më poshtë ku japim një tablo të përgjithshme të rezultateve të përfuara duke sjellë te tre pikat shtjelluese për këto variabla si dhe kalojmë më pas në nivelin e dytë ku bëjmë një përballje të të dhënave të marra nga dy ekstremitetet e qëndrimeve të përdoruesve kundrejt QoS së internetit në Shqipëri.

Në lidhje me pyetjet e parastruara kemi si në vijim përmbledhjet:

1-Si ndiheni me shërbimin e ISP tuaj si ofrues interneti?



Pra përgjigjet respektive në këtë rast do të qenë:

Tabela ,11

Kategoria	Përqindje	Niveli
Shkelqyer	5.95%	31
Shume mire	36.28%	189
Kenaqshem	46.64%	243
I/e pakenaqur	11.13%	58
Total		521

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

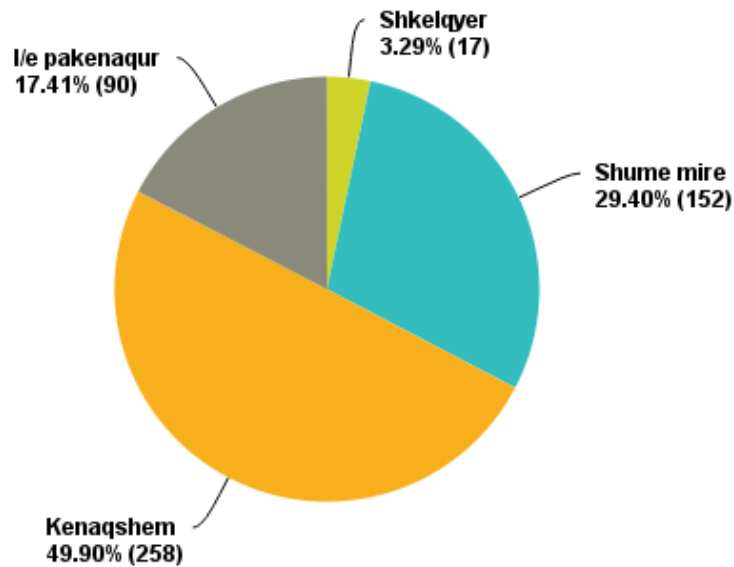
Këtu shohim që përdoruesit në pjesën më të madhe janë mesatarisht të kënaqur nga ofruesit e tyre të shërbimit të internetit. Pra nga 524 përdorues interneti 243 ishin mesatarisht të kënaqur duke përbërë kështu edhe 46.64% të përdoruesve.

Në vazhdim përdoruesat e internetit për nga përqindja e lartë e përgjigjeve janë shprehur shumë të kënaqur duke përbërë kështu edhe 36.28% të përdoruesve, pra në total 189 përdorues.

Të pakënaqur vërejmë që kemi 11.13% të përdoruesve pra e shprehur në numër total janë 58 përdorues interneti nga 524 në total.

Nga ana tjetër më të paktë kanë qenë ata që kanë qenë maksimalisht të kënaqur duke përbërë 5.95% të përdoruesve dhe e shprehur në numër janë 31 përdorues.

2-Si do ta kategorizonit ISP-në tuaj në bazë të (besueshmërisë, shpejtësisë, shkeputjeve të sinjalit)?



Pra përgjigjet respektive në këtë rast do të qenë:

Tabela.12

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Shkelqyer	3.29%	17
Shume mire	29.40%	152
Kenaqshem	49.90%	258
I/e pakenaqur	17.41%	90
Total		517

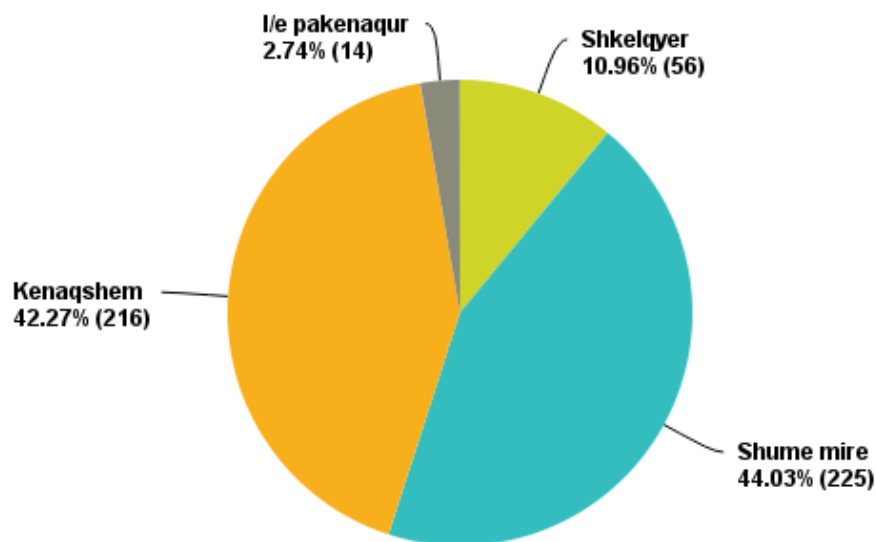
Këtu shohim që përdoruesit në pjesën më të madhe janë mesatarisht të kënaqur nga cilësia e tyre e internetit. Pra nga 524 përdorues interneti 258 ishin mesatarisht të kënaqur duke përbërë kështu edhe 49.90% të përdoruesve pra gati gjysma e përdoruesve.

Në vijim përdoruesat e internetit për nga përqindja e lartë e përgjigjeve janë shprehur shumë të kënaqur duke përbërë kështu edhe 29.40% të përdoruesve, pra 152 përdorues.

Të pakënaqur vërejmë që kemi 17.41% të përdoruesve pra e shprehur në total janë 90 përdorues interneti nga 524 të anketuar.

Nga ana tjetër më të paktë kanë qenë ata që kanë qenë maksimalisht të kënaqur duke përbërë 3.29% të përdoruesve dhe e shprehur në numër janë 17 përdorues.

3-Si do ta vlerësonit software-in e instalimit si lehtësi në montim dhe në përdorim?



Pra përgjigjet respektive në këtë rast do të qenë:

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Tabela .13

Shkelqyer	10.96%	56
Shume mire	44.03%	225
Kenaqshem	42.27%	216
I/e pakënaqur	2.74%	14
Total		511

Këtu shohim që përdoruesit në pjesën më të madhe janë mesatarisht të kënaqur nga teknologjia e internetit. Pra nga 524 përdorues interneti 225 ishin mesatarisht të kënaqur duke përbërë kështu edhe 44.03% të përdoruesve të anketuar.

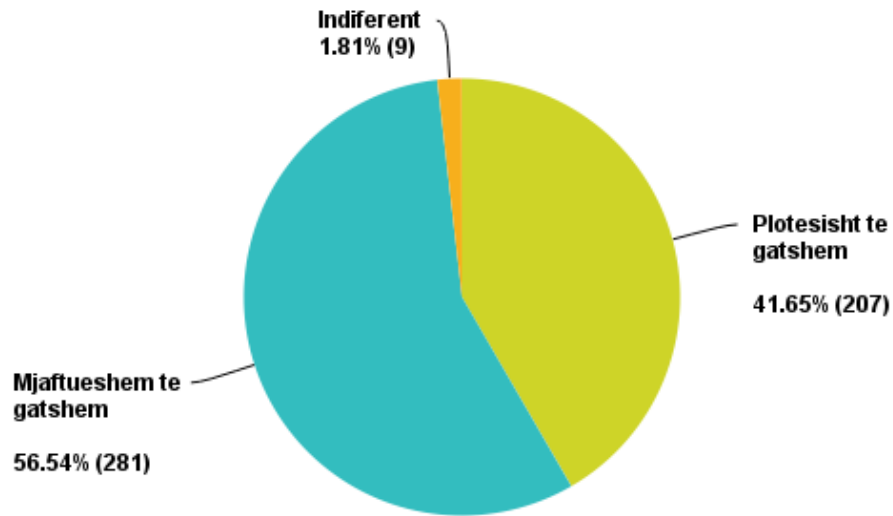
Në vijim përdoruesat e internetit për nga përqindja e lartë e përgjigjeve janë shprehur shumë të kënaqur duke përbërë kështu edhe 42.27% të përdoruesve, pra 216 përdorues.

Nga ana tjetër ata që kanë qenë maksimalisht të kënaqur duke përbërë 10.94% të përdoruesve dhe e shprehur në numër janë 56 përdorues.

Përgjigjet më të pakta janë për përdoruesit të pakënaqur e vërejmë që kemi 2.74% të përdoruesve pra e shprehur në total janë 14 përdorues interneti nga 524 të anketuar.

4-Në lidhje me operatorët e shërbimit të klientit, si do ti vlerësonit?

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



Pra përgjigjet respektive në këtë rast do të qenë:

Tabela .14

Kategoria	Përqindje	Numër
Plotesisht te gatshem	41.65%	207
Mjaftueshem te gatshem	56.54%	281
Indiferent	1.81%	9
Total		497

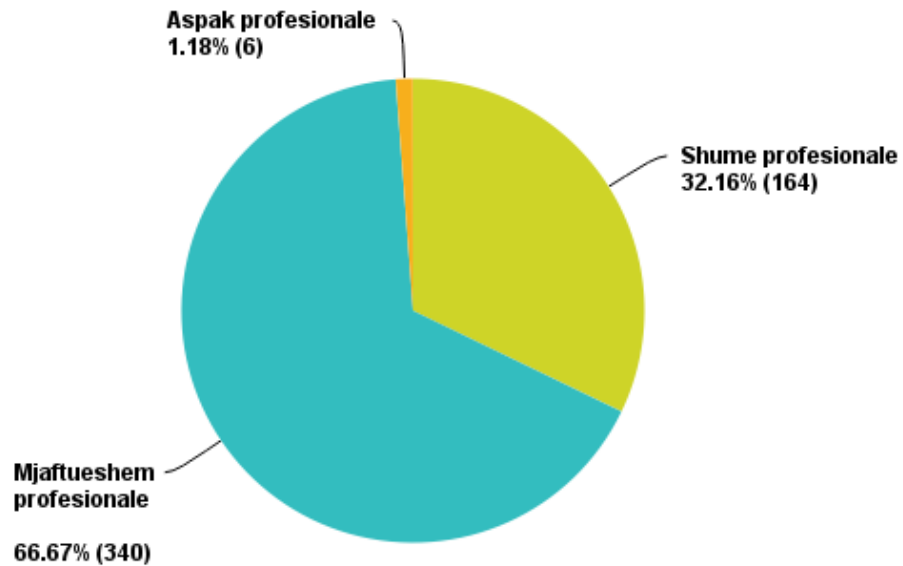
Përsa i përket shërbimit ndaj klientit dhe konkretisht gatishmërisë për të ardhur në ndihmë përdoruesve shohim që përdoruesit në pjesën më të madhe janë mjaftueshëm të kënaqur nga cilësia e tyre. Pra nga 524 përdorues interneti 281 ishin mesatarisht të kënaqur duke përbërë kështu edhe 56.54% të përdoruesve

Në vazhdim të analizës së përgjigjeve shohim se përdoruesat e internetit janë shprehur plotësisht të kënaqur duke përbërë kështu edhe 41.65% të përdoruesve, pra 207 përdorues.

Të pakënaqur vërejmë që kemi 1.81% të përdoruesve pra e shprehur në total janë 9 përdorues interneti nga 524 të anketuar pra një numër shumë i vogël.

5-Sa profesionalë do t'i vlerësonit operatorët e shërbimit ndaj klientit?

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



Pra përgjigjet respektive në këtë rast do të qenë:

Tabela.15

Shume profesionale	32.16%	164
Mjaftueshem profesionale	66.67%	340
Aspak profesionale	1.18%	6
Total		510

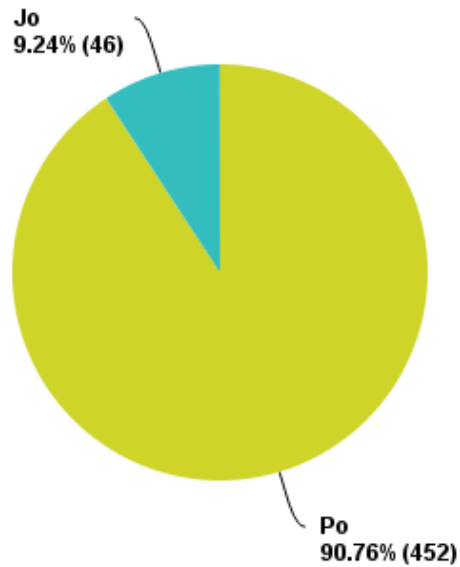
Në lidhje me profesionalizmin e operatorëve të shërbimit ndaj klientit shohim që përdoruesit në pjesën më të madhe janë mesatarisht të kënaqur nga cilësia e tyre e internetit. Pra nga 524 përdorues interneti 340 ishin mesatarisht të kënaqur duke përbërë kështu edhe 66.67% të përdoruesve..

Në vijim përdoruesat e internetit për nga përqindja e lartë e përgjigjeve janë shprehur shumë të kënaqur duke përbërë kështu edhe 32.16% të përdoruesve, pra 164 përdorues.

Të pakënaqur vërejmë që kemi 1.18% të përdoruesve pra e shprehur në total janë 6 përdorues interneti nga 524 të anketuar.

6- U zgjidh problemi juaj pas telefonatës me operatorin e shërbimit?

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



Pra përgjigjet respektive në këtë rast do të qenë:

Tabela.16

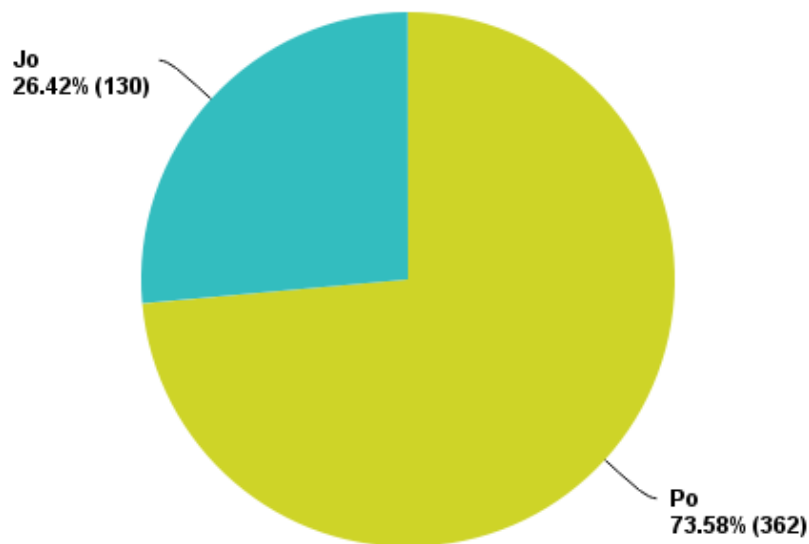
Po	90.76%	452
Jo	9.24%	46
Total		498

Në vazhdim pyetja pasuese konsiston në lidhje me gjendjen e problemit pas telefonatës me operatorin e shërbimit dhe gati pjesa më e madhe u përgjigj pozitivisht pra 90.76% treguan se problemi i tyre mori zgjidhje duke përbërë kështu rreth 452 të anketuar.

Nga ana tjetër shumë më të paktë në numër janë ata, përgjigjja e të cilëve ishte negative duke dëshmuar se nuk kishin gjetur zgjidhje të problemit të ndeshur dhe ishin pikërisht 9.24% e të anketuarve, pra 46 prej tyre.

7-Krahasuar me teknikët e ISP-ve të mëparshme që keni pasur kontratë shërbimi është më cilësor apo jo?

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



Pra përgjigjet respektive në këtë rast do të qenë:

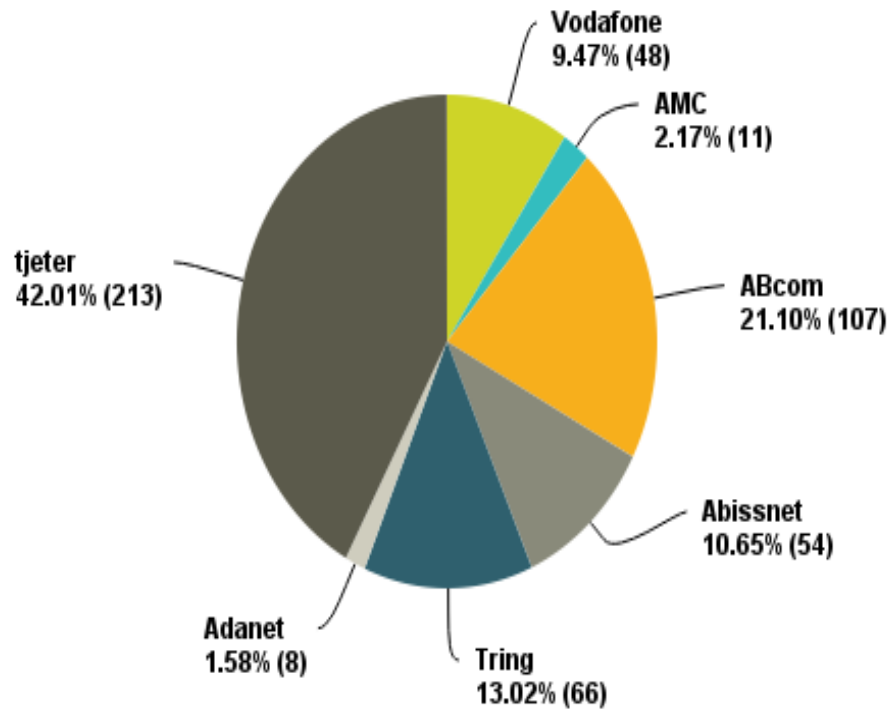
Tabela.17

Po	73.58%	362
Jo	26.42%	130
Total		492

Në vazhdim pyetja pasuese e pyetësorit lidhet me krahasimin midis teknikëve të ISP-ve të mëparshme dhe atyre aktualë nëse e kanë përmirësuar shërbimin apo jo dhe pozitivisht janë përgjigjur 73.58% pra 362 përdorues nga 524 të tillë. Negativisht, ndërkaq janë përgjigjur 26.42% e përdoruesve që do të thotë 130 prej tyre.

8-Cilën ISP keni zgjedhur për tu ofruar internet në ambientet tuaja?

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



Pra përgjigjet respektive në këtë rast do të qenë:

Tabela.18

Vodafone	9.47%	48
AMC	2.17%	11
ABcom	21.10%	107
Abissnet	10.65%	54
Tring	13.02%	66
Adanet	1.58%	8
tjeter	42.01%	213
Total		507

Së fundmi në lidhje me kategoritë e ISP-ve të përzgjedhura për ofrim të shërbimit të internetit përdoruesit janë përgjigjur kryesisht për ISP të tjera të papërfshira në listë

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

(sikurse Albtelecom etj) duke përbërë kështu rreth 42.01% të përgjigjeve të të anketuarve pra 213 përdorues në total nga 524.

Në vazhdim për nga renditja e përgjigjeve 21.10% e përdoruesve kishin zgjedhur si ISP operatorin ABCOM duke përfshirë 107 përdorues.

Në vijim përdoruesit më së shumti kanë zgjedhur shërbimin e internetit nga operatori Tring duke përbërë 13.02% të përdoruesve e shprehur në vlerë numerike 66 përdorues.

Operatori Abissnet mban një kuotë përgjigjesh të të anketuarve prej 10.65% ose 54 përdorues nga 524 në total.

Nga ana tjetër operatori Vodafone përfshin 9.47% të përgjigjeve të të anketuarve, pra 48 përdorues në total nga 524 të tillë duke u pasuar nga operatori Amc me 2.17% të përgjigjeve të të anketuarve që i korrespondojnë 11 përdorues.

Së fundmi me më pak të abonuar qëndron operatori Adanet me 1.58% pra 8 përdorues nga 524 në total.

6.2. Analiza e përgjigjeve për rastin e përdoruesve të cilët e konsiderojnë QoS maksimale në Shqipëri.

Tabela.19

Si ndiheni me shërbimin e ISP tuaj si ofruer interneti?	Si do ta kategorizonit ISP-ne tuaj në baze të (besueshmërisë, shpejtësisë, shkeputjeve të sinjalit)?	Si do ta vlerësonit software-in e instalimit si lehtësi në montim dhe në përdorim?	Ne lidhje me operatorët e shërbimit të klientit, si do ti vlerësonit ?	Sa profesional do ti vlerësonit operatorët e shërbimit ndaj klientit	U zgjidh problemi juaj pas telefonates me operatorin e shërbimit?	Krahasuar me teknikat e ISP-ve të mëparshme që keni pasur kontrate shërbimi është me cilësor apo jo?	Cilen ISP keni zgjedhur për tu ofruar internet në ambientet tuaja?
Shkëlqyer	Shumë mire	Shumë mire	Plotësisht të gatshëm	Shumë profesionalë	Po	Po	ABcom
Shkëlqyer	Shumë mire	Shkëlqyer	Plotësisht të gatshëm	Shumë profesionalë	Po	Po	ABcom
Shkëlqyer	Shumë mire	Shumë mire	Plotësisht të gatshëm	Shumë profesionalë	Po	Po	ABcom
Shkëlqyer	Shumë mire	Shkëlqyer	Plotësisht të gatshëm	Shumë profesionalë	Po	Po	Tring
Shkëlqyer	Shumë mire	Shkëlqyer	Plotësisht të gatshëm	Shumë profesionalë	Po	Po	Vodafone
Shkëlqyer	Shkëlqyer	Shkëlqyer	Plotësisht të gatshëm	Shumë profesionalë	Po	Po	Vodafone
Shkëlqyer	Shkëlqyer	Shkëlqyer	Plotësisht të gatshëm	Shumë profesionalë		Po	ABcom
Shkëlqyer	Shumë mire	Shkëlqyer	Plotësisht të gatshëm	Shumë profesionalë	Po	Po	Vodafone
Shkëlqyer	Shkëlqyer	Shkëlqyer	Plotësisht të gatshëm	Shumë profesionalë	Po	Po	tjetër

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Shkëlqyer	Shkëlqyer	Shkëlqyer	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	ABcom
Shkëlqyer	Shkëlqyer	Shkëlqyer	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	tjetër
Shkëlqyer	Shkëlqyer	Shkëlqyer	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	tjetër
Shkëlqyer	Shkëlqyer	Shkëlqyer	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	ABcom
Shkëlqyer	Shkëlqyer	Shkëlqyer	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	Vodafone
Shkëlqyer	Shkëlqyer	Shumë mire	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	ABcom
Shkëlqyer	Shkëlqyer	Shkëlqyer	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	Vodafone
Shkëlqyer	Shkëlqyer	Shkëlqyer	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	ABcom
Shkëlqyer	Shumë mire	Shumë mire	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Po	Vodafone
Shkëlqyer	Kënaqshëm	Shkëlqyer	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	Tring
Shkëlqyer	Shumë mire	Shumë mire	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	Vodafone
Shkëlqyer	Shkëlqyer	Shkëlqyer	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	AMC
Shkëlqyer	Shkëlqyer	Shkëlqyer	Mjaftueshëm te gatshëm	Shumë profesionalë	Po	Po	Vodafone
Shkëlqyer	Shumë mire	Shkëlqyer	Plotësisht te gatshëm	Mjaftueshëm profesionalë	Po	Po	Vodafone
Shkëlqyer	Shkëlqyer	Shkëlqyer	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	ABcom
Shkëlqyer	Shumë mire	Shkëlqyer	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	Vodafone
Shkëlqyer	Shkëlqyer	Shkëlqyer	Plotësisht te gatshëm	Mjaftueshëm profesionalë	Po	Po	tjetër
Shkëlqyer	Shumë mire	Shumë mire	Plotësisht te gatshëm	Mjaftueshëm profesionalë	Po	Po	AMC
Shkëlqyer	Shumë mire	Shumë mire	Plotësisht te gatshëm	Mjaftueshëm profesionalë	Po	Po	Vodafone
Shkëlqyer	Shkëlqyer	Shkëlqyer	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	Vodafone
Shkëlqyer							
Shkëlqyer	Shumë mire	Shumë mire	Plotësisht te gatshëm	Mjaftueshëm profesionalë	Po	Po	ABcom

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Ne lidhje me pyetjen e parë shtruar drejt përdoruesve të internetit në Shqipëri duke filtruar përgjigjet për kategorinë Shkëlqyer në lidhje me shërbimin e ISP-ve marrim këtë tabelë për:

1-Si ndiheni me shërbimin e ISP tuaj si ofrues interneti?

Tabela.20

Si ndiheni me shërbimin e ISP tuaj si ofrues interneti?	Si do ta kategorizonit ISP-ne tuaj në baze të (besueshmërisë, shpejtësisë, shkeputjeve të sinjalit)?
Shkëlqyer	Shumë mire
Shkëlqyer	Shumë mire
Shkëlqyer	Shumë mire
Shkëlqyer	Shumë mire
Shkëlqyer	Shumë mire
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shumë mire
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shumë mire
Shkëlqyer	Kënaqshëm
Shkëlqyer	Shumë mire
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shumë mire
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shumë mire

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

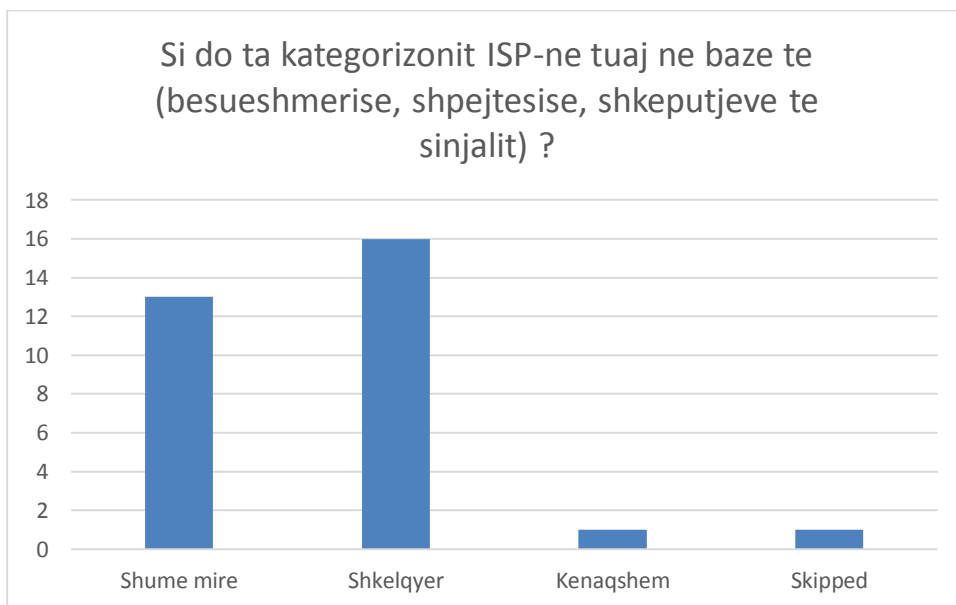
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shumë mire
Shkëlqyer	Shumë mire
Shkëlqyer	Shkëlqyer
Shkëlqyer	
Shkëlqyer	Shumë mire

Totali i përgjigjeve në këtë rast për pyetjen e parë përmbledhet në:

Tabela.21

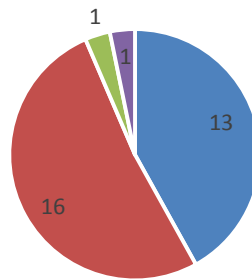
Shumë mire	13	42%
Shkëlqyer	16	52%
Kënaqshëm	1	3%
Skipped	1	3%

Atëherë përmes programeve të përdorura marrim këto grafikë respektive për përgjigjet e dhëna:

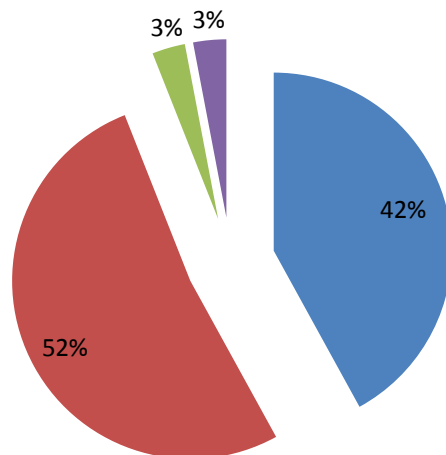


Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Si do ta kategorizonit ISP-ne tuaj ne baze te (besueshmerise, shpejtesise, shkeputjeve te sinjalit)?



■ Shume mire ■ Shkelqyer ■ Kenaqshem ■ Skipped



■ Shume mire
■ Shkelqyer
■ Kenaqshem
■ Skipped

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Përsa i përket përgjigjeve për pyetjen e dytë për kategorinë e përgjigjeve Shkëlqyer mbi shërbimin e internetit në Shqipëri kemi:

2-Si do ta vlerësonit software-in e instalimit si lehtësi në montim dhe në përdorim?

Tabela.22

Si ndiheni me shërbimin e ISP tuaj si ofrues interneti?	Si do ta vlerësonit software-in e instalimit si lehtësi në montim dhe në përdorim?
Shkëlqyer	Shumë mire
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shumë mire
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shumë mire
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shumë mire
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shumë mire
Shkëlqyer	Shkëlqyer

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

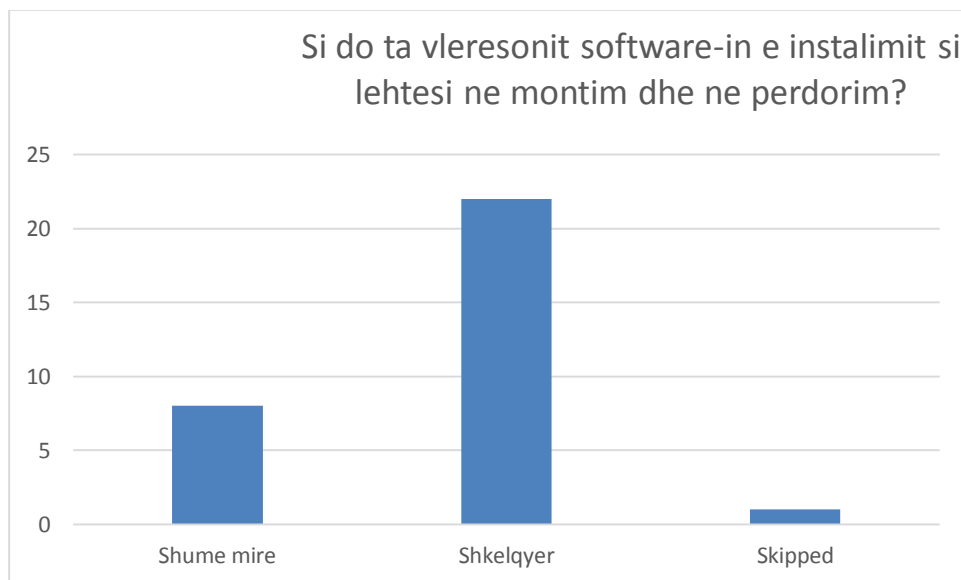
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shkëlqyer
Shkëlqyer	Shumë mire
Shkëlqyer	Shumë mire
Shkëlqyer	Shkëlqyer
Shkëlqyer	
Shkëlqyer	Shumë mire

Pra totali i përgjigjeve për pyetjen e dytë përmbledhet në:

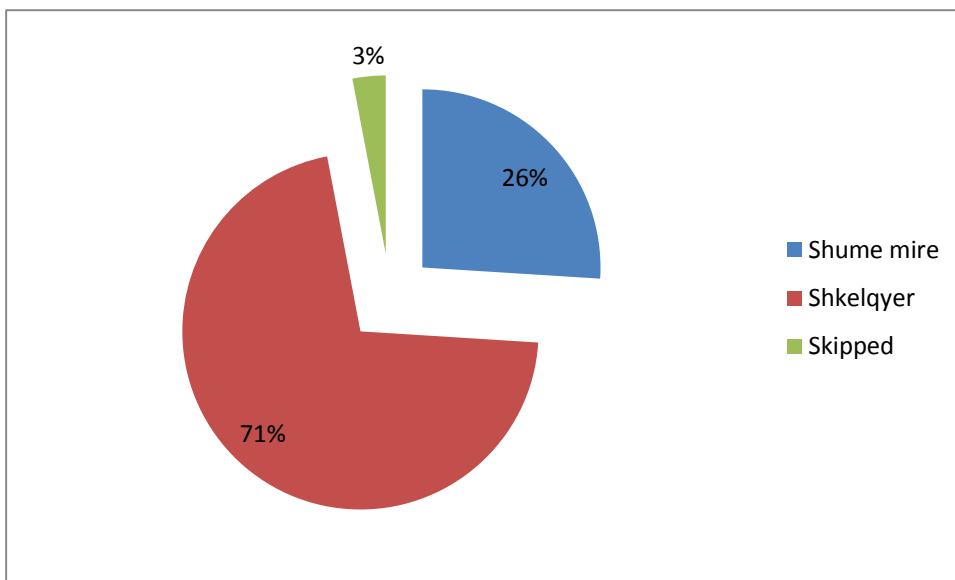
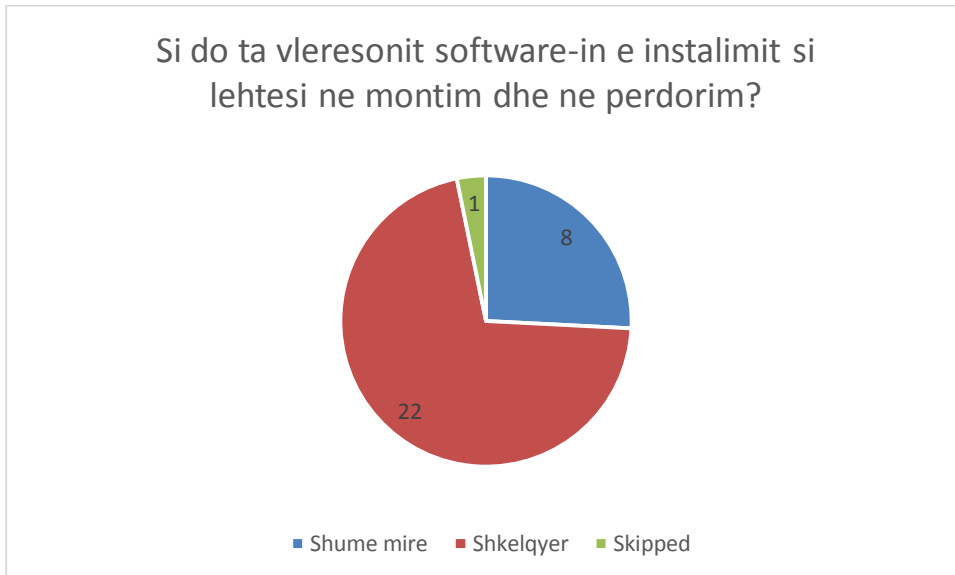
Tabela.23

Shumë mire	8	26%
Shkëlqyer	22	71%
Skipped	1	3%

Diagramat respektive të përfuara nga programet përkatëse do të qenë këto si në vijim për pyetjen e dytë:



Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



Në vazhdim kemi pyetjen e tretë që merret në shqyrtim sërish nga kategoria e përgjigjeve shkëlqyer për shërbimin e ISP-së.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

3-Në lidhje me operatorët e shërbimit të klientit, si do ti vlerësonit?

Tabela.24

Si ndiheni me shërbimin e ISP tuaj si ofrues interneti?	Ne lidhje me operatorët e shërbimit të klientit, si do ti vlerësonit ?
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Mjaftueshëm te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Mjaftueshëm te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	Plotësisht te gatshëm
Shkëlqyer	
Shkëlqyer	Plotësisht te gatshëm

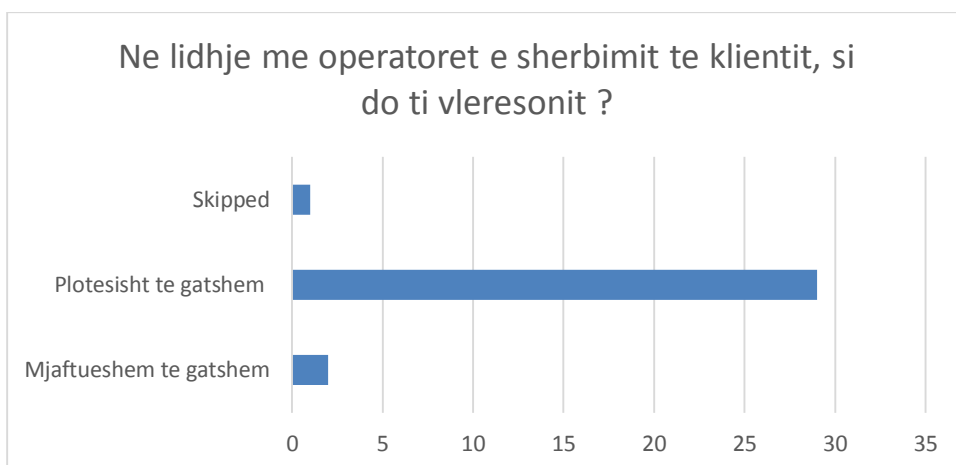
Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Pra totali i përgjigjeve për pyetjen e tretë përmbledhet në:

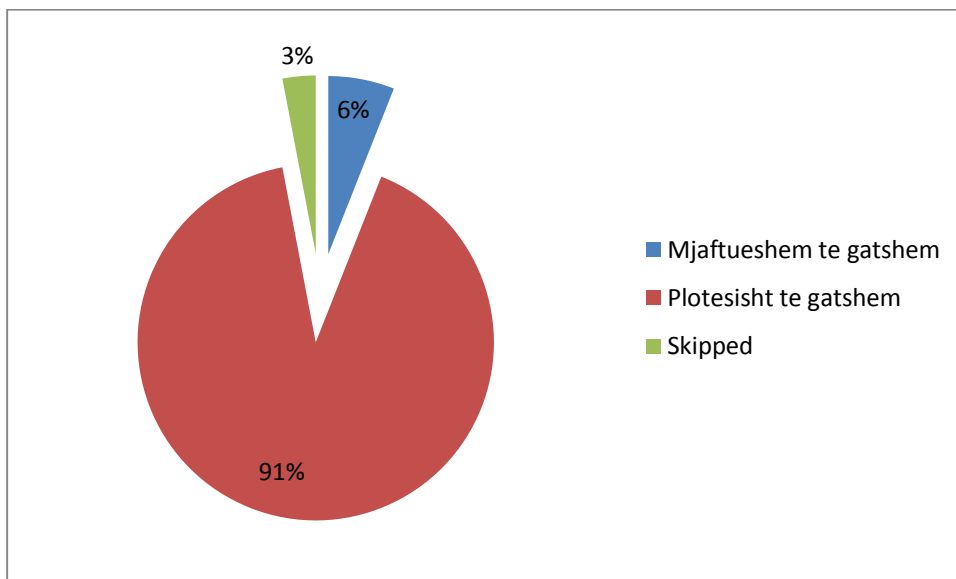
Tabela.25

Mjaftueshëm të gatshëm	2	6%
Plotësisht të gatshëm	29	91%
Skipped	1	3%

Grafiket e përftuar në këtë rast do të ishin:



Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



Pyetja tjetër pasuese sërish e kategorisë së përgjigjeve shkëlqyer për shërbimin e internetit përfshin:

3-Sa profesionalë do ti vlerësonit operatorët e shërbimit ndaj klientit?

Tabela.26

Si ndiheni me shërbimin e ISP tuaj si ofruer interneti?	Sa profesional do ti vlerësonit operatorët e shërbimit ndaj klientit?
Shkëlqyer	Shumë profesionalë
Shkëlqyer	Shumë profesionalë
Shkëlqyer	Shumë profesionalë
Shkëlqyer	Shumë profesionalë
Shkëlqyer	Shumë profesionalë
Shkëlqyer	Shumë profesionalë
Shkëlqyer	Shumë profesionalë
Shkëlqyer	Shumë profesionalë
Shkëlqyer	Shumë profesionalë
Shkëlqyer	Shumë profesionalë
Shkëlqyer	Shumë profesionalë
Shkëlqyer	Shumë profesionalë
Shkëlqyer	Shumë profesionalë

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Shkëlqyer	Shumë profesionale
Shkëlqyer	Shumë profesionale
Shkëlqyer	Shumë profesionale
Shkëlqyer	Shumë profesionale
Shkëlqyer	Mjaftueshëm profesionale
Shkëlqyer	Shumë profesionale
Shkëlqyer	Shumë profesionale
Shkëlqyer	Shumë profesionale
Shkëlqyer	Shumë profesionale
Shkëlqyer	Mjaftueshëm profesionale
Shkëlqyer	Shumë profesionale
Shkëlqyer	Shumë profesionale
Shkëlqyer	Mjaftueshëm profesionale
Shkëlqyer	Mjaftueshëm profesionale
Shkëlqyer	Mjaftueshëm profesionale
Shkëlqyer	Shumë profesionale
Shkëlqyer	
Shkëlqyer	Mjaftueshëm profesionale

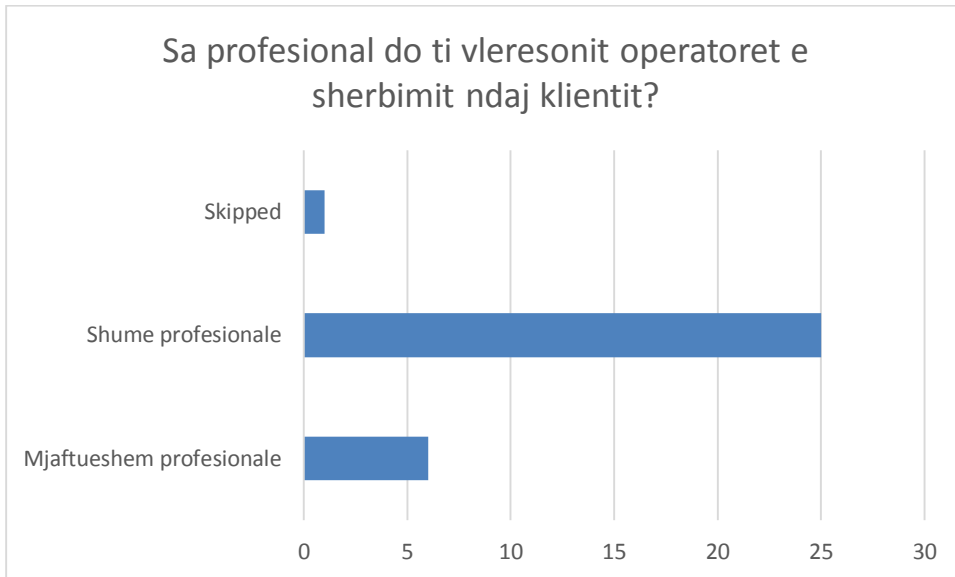
Pra totali i përgjigjeve për pyetjen e katërt përmblihet në:

Tabela.27

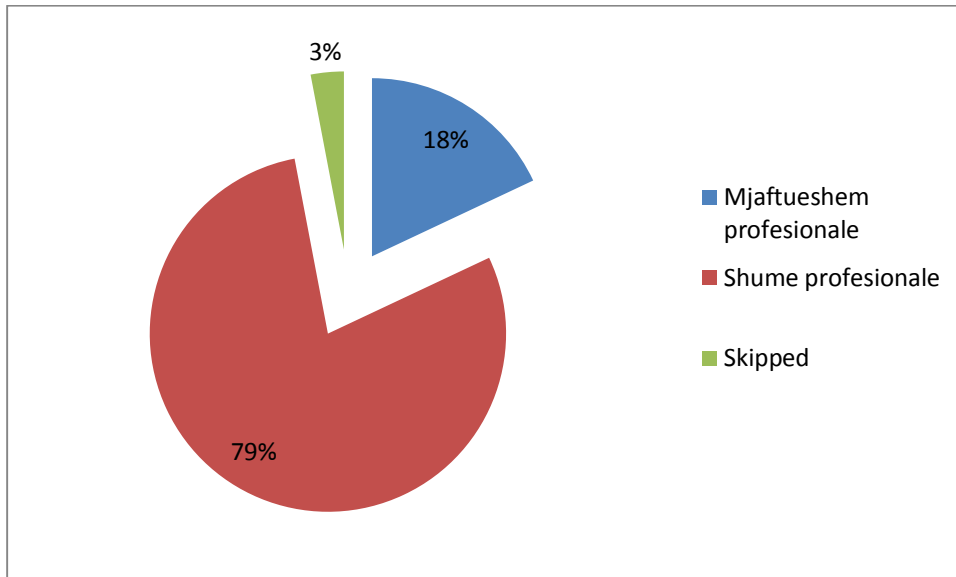
Mjaftueshëm profesionale	6	18%
Shumë profesionale	25	79%
Skipped	1	3%

Ne këtë rast do të merrnim pikërisht këto grafikë :

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



5-U zgjidh problemi juaj pas telefonatës me operatorin e shërbimit?

Tabela.28

Si ndiheni me shërbimin e ISP tuaj si ofrues interneti?	U zgjidh problemi juaj pas telefonatës me operatorin e shërbimit?
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

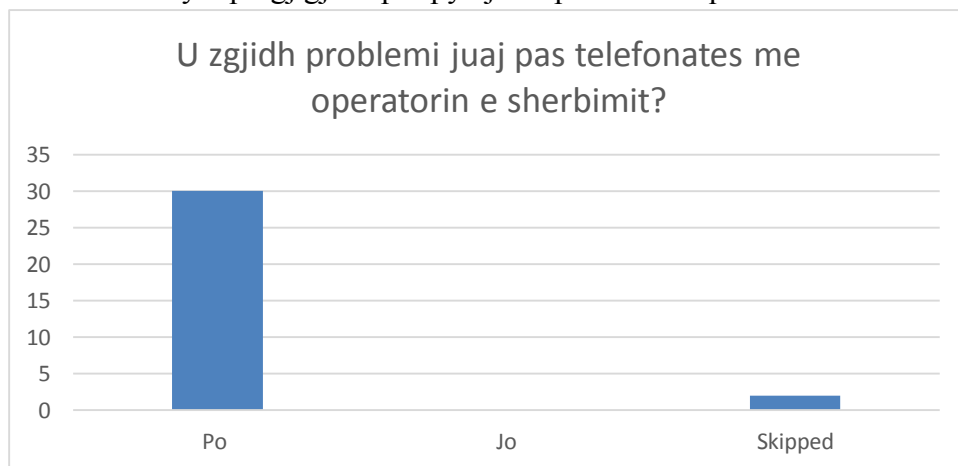
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	
Shkëlqyer	Po

Pra totali i përgjigjeve për pyetjen e pestë përmbledhet në:

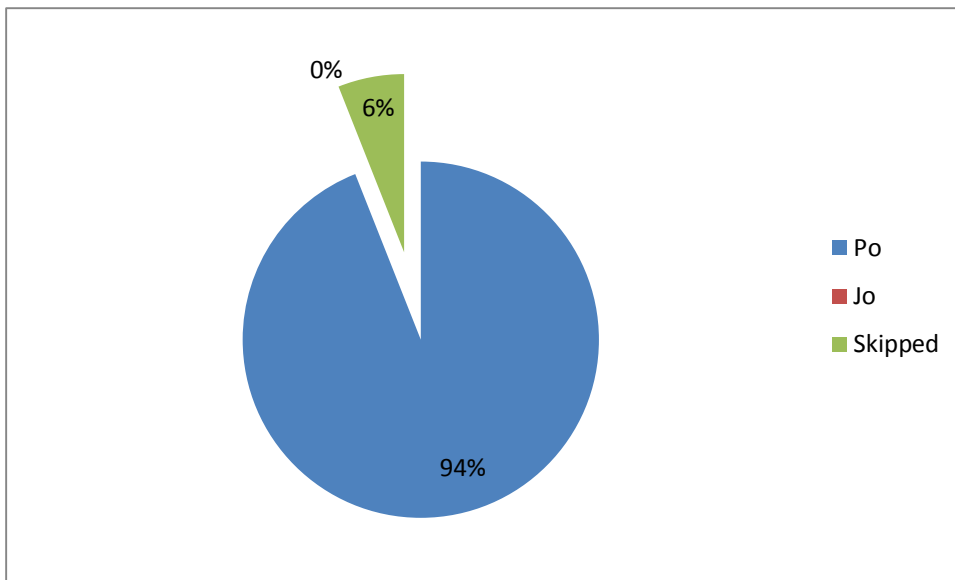
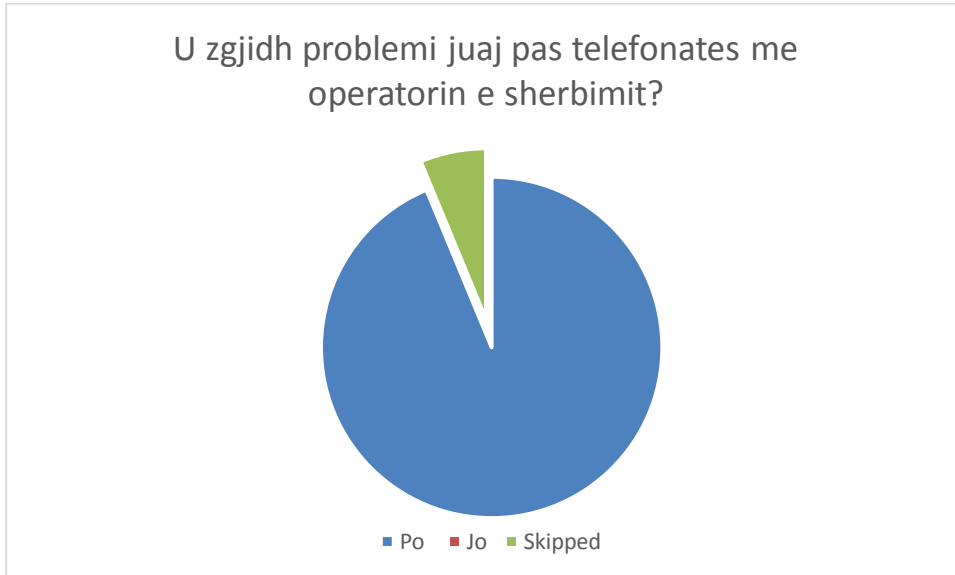
Tabela.29

Po	30	94%
Jo	0	0%
Skipped	2	6%

Grafikët e këtyre përgjigjeve për pyetjen e pestë do të qenë këta:



Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



Pyetja që pason përben pyetjen e gjashtë të kategorisë së përgjigjeve shkëlqyer dhe është:

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

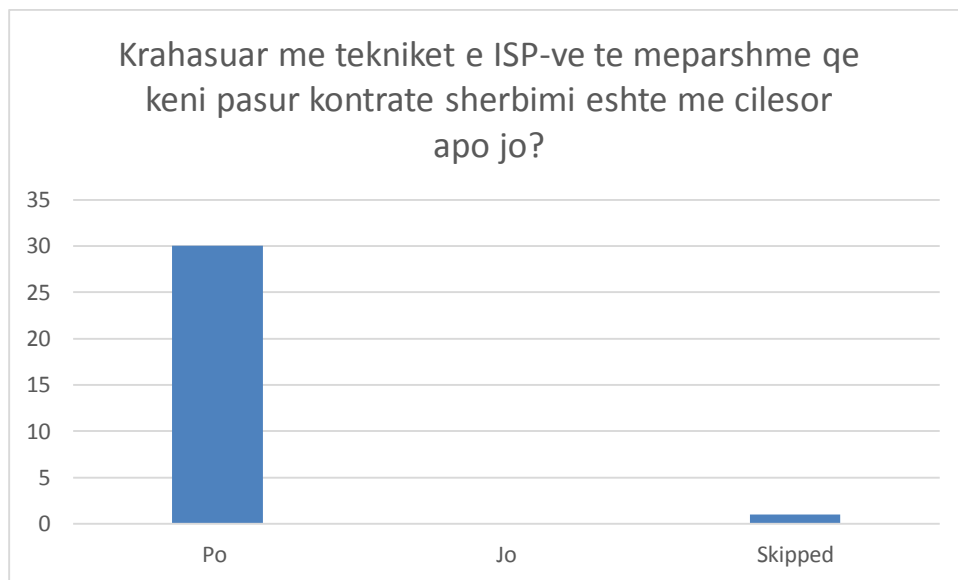
Shkëlqyer	Po
Shkëlqyer	Po
Shkëlqyer	
Shkëlqyer	Po

Pra totali i përgjigjeve per pyetjen e gjashtë përmbledhet në:

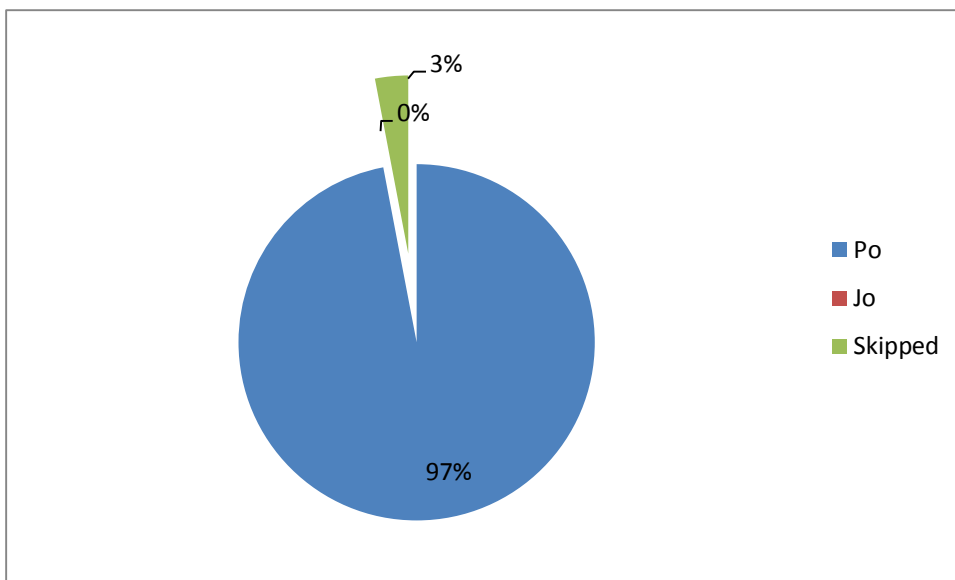
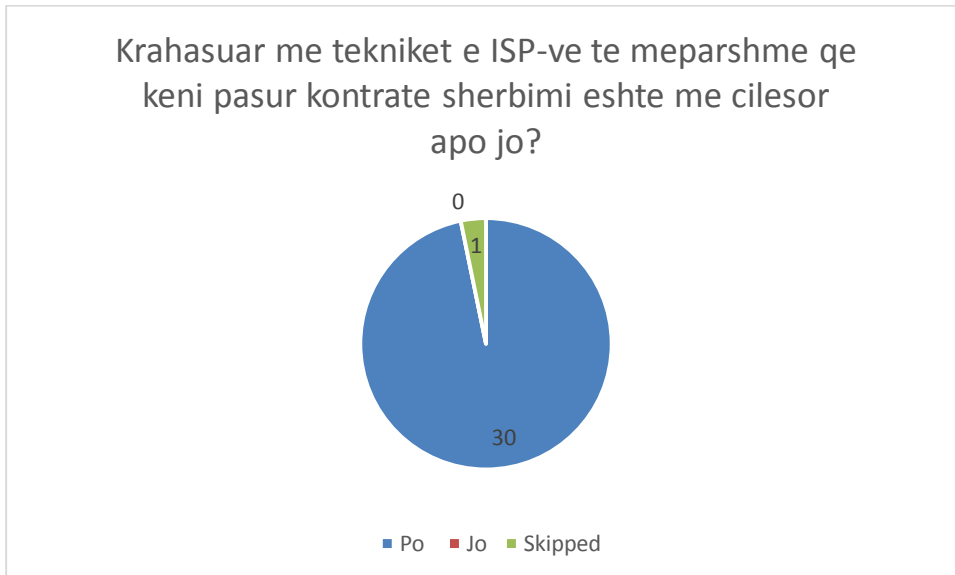
Tabela.31

Po	30	97%
Jo	0	0%
Skipped	1	3%

Grafikët në këtë rast do të ishin këta:



Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



Pyetja në vazhdim e kësaj kategorie është:

7-Cilën ISP keni zgjedhur për tu ofruar internet në ambientet tuaja?

Tabela.32

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Si ndiheni me shërbimin e ISP tuaj si ofrues interneti?	Cilen ISP keni zgjedhur për të ofruar internet në ambientet tuaja?
Shkëlqyer	ABcom
Shkëlqyer	ABcom
Shkëlqyer	ABcom
Shkëlqyer	Tring
Shkëlqyer	Vodafone
Shkëlqyer	Vodafone
Shkëlqyer	ABcom
Shkëlqyer	Vodafone
Shkëlqyer	tjetër
Shkëlqyer	ABcom
Shkëlqyer	tjetër
Shkëlqyer	tjetër
Shkëlqyer	ABcom
Shkëlqyer	Vodafone
Shkëlqyer	ABcom
Shkëlqyer	Vodafone
Shkëlqyer	ABcom
Shkëlqyer	Vodafone
Shkëlqyer	Tring
Shkëlqyer	Vodafone
Shkëlqyer	AMC
Shkëlqyer	Vodafone
Shkëlqyer	Vodafone
Shkëlqyer	ABcom
Shkëlqyer	Vodafone
Shkëlqyer	tjetër
Shkëlqyer	AMC
Shkëlqyer	Vodafone
Shkëlqyer	Vodafone
Shkëlqyer	
Shkëlqyer	ABcom

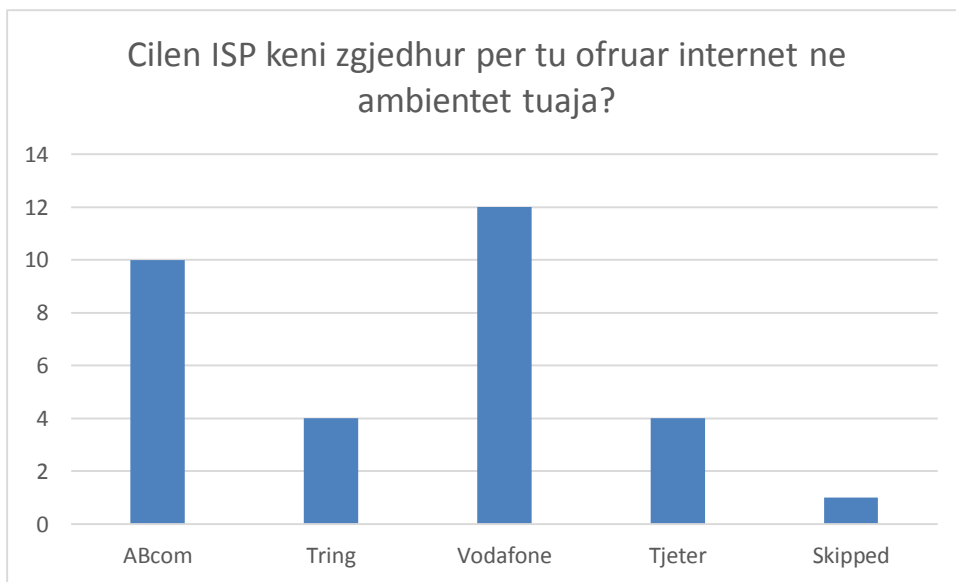
Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Pra totali i përgjigjeve për pyetjen e shtatë përmbledhet në:

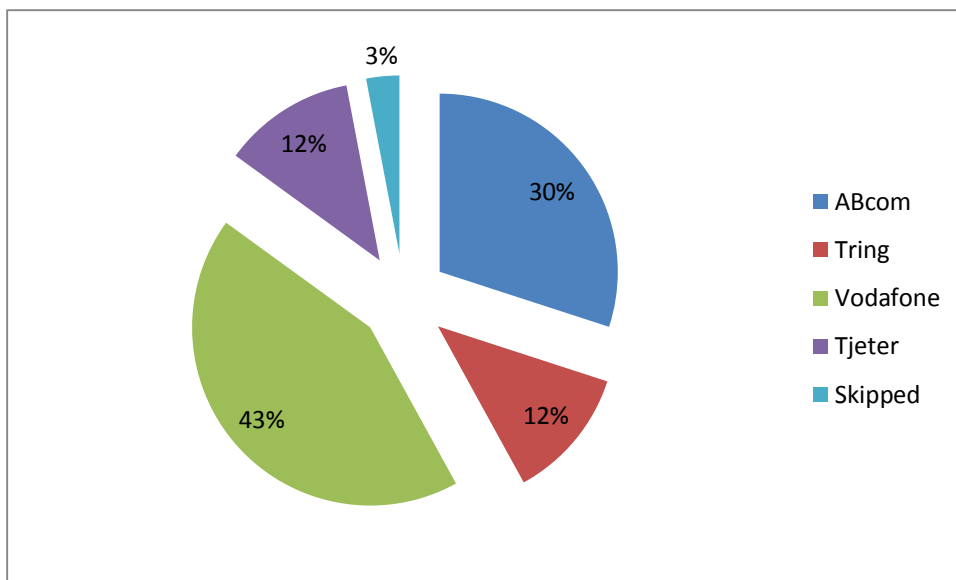
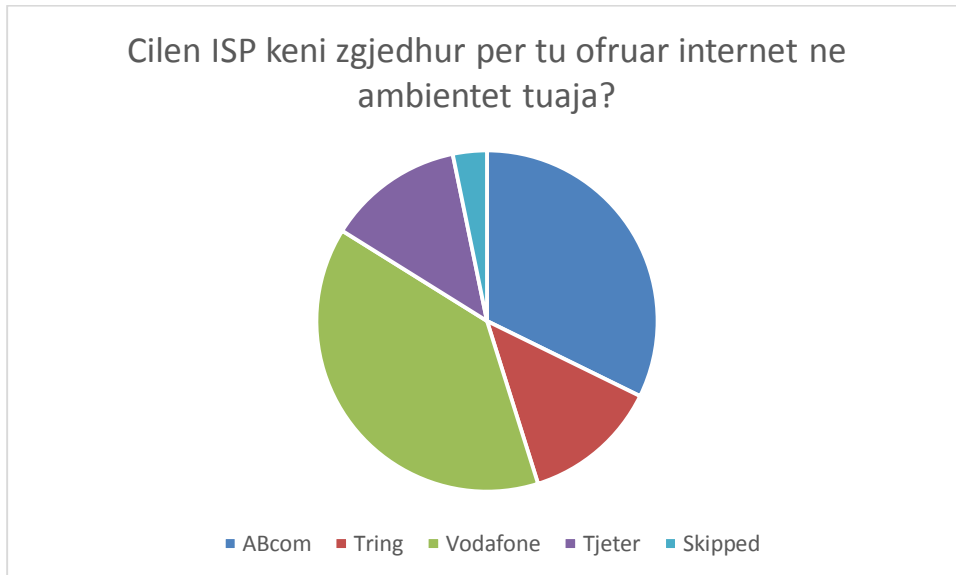
Tabela.33

ABcom	10	30%
Tring	4	12%
Vodafone	12	43%
Tjetër	4	12%
Skipped	1	3%

Grafikët në këtë rast do të ishin:



Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



6.3. Analiza e përgjigjeve për rastin e përdoruesve të cilët e konsiderojnë QoS minimale në Shqipëri.

Tabela.34

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Si ndiheni me shërbimin e ISP tuaj si ofrues interneti?	Si do ta kategorizonit ISP-ne tuaj ne baze te (besueshmërisë, shpejtesisë, shkeputjeve te sinjalit)?	Si do ta vlerësonit software-in e instalimit si lehtësi ne montim dhe ne perdorim?	Ne lidhje me operatorët e shërbimit te klientit, si do ti vlerësonit ?	Sa profesional do ti vlerësonit operatorët e shërbimit ndaj klientit	U zgjidh problemi juaj pas telefonates me operatorin e shërbimit?	Krahasuar me tekniket e ISP-ve te meparshme qe keni pasur kontrate shërbimi eshte me cilesor apo jo?	Cilen ISP keni zgjedhur per tu ofruar internet ne ambientet tuaja?
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Po	tjetër
I/e pakënaqur	Kënaqshëm	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Po	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Jo	Abissnet
I/e pakënaqur	I/e pakënaqur	I/e pakënaqur	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Po	tjetër
I/e pakënaqur	I/e pakënaqur	I/e pakënaqur	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Jo	Abissnet
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Jo	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	I/e pakënaqur	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Po	tjetër
I/e pakënaqur	I/e pakënaqur	I/e pakënaqur	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Po	tjetër
I/e pakënaqur	I/e pakënaqur	I/e pakënaqur					tjetër
I/e pakënaqur	I/e pakënaqur	Shumë mire	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Plotësisht te gatshëm	Shumë profesionalë	Po	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm					
I/e pakënaqur	I/e pakënaqur						
I/e pakënaqur	I/e pakënaqur			Mjaftueshëm profesionalë			
I/e pakënaqur	I/e pakënaqur	Kënaqshëm		Mjaftueshëm profesionalë			

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Po	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Po	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	tjetër
I/e pakënaqur	I/e pakënaqur	Shumë mire	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Jo	
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm		Mjaftueshëm profesionalë	Po	Jo	
I/e pakënaqur	I/e pakënaqur	Shumë mire	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Jo	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Shumë mire	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Po	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Plotësisht te gatshëm	Mjaftueshëm profesionalë	Po	Po	Abissnet
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Po	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Po	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Po	Abissnet
I/e pakënaqur	I/e pakënaqur	Shumë mire	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	tjetër
I/e pakënaqur	I/e pakënaqur	Shumë mire	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Po	Tring
I/e pakënaqur	I/e pakënaqur	Shumë mire	Plotësisht te gatshëm	Shumë profesionalë	Po	Po	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Plotësisht te gatshëm	Shumë profesionalë	Po		
I/e pakënaqur	I/e pakënaqur	Shumë mire	Plotësisht te gatshëm	Shumë profesionalë	Po	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Plotësisht te gatshëm	Mjaftueshëm profesionalë	Po	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Jo	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Jo	tjetër

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

pakënaqur	pakënaqur		gatshëm	profesionalë			
I/e pakënaqur	I/e pakënaqur	Shumë mire	Plotësisht te gatshëm	Mjaftueshëm profesionalë	Po	Po	Abissnet
I/e pakënaqur	I/e pakënaqur	Shumë mire	Plotësisht te gatshëm	Shumë profesionalë	Po	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Shumë mire	Plotësisht te gatshëm	Mjaftueshëm profesionalë	Po	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Shumë mire	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Jo	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Jo	Abissnet
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Jo	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Jo	Abissnet
I/e pakënaqur	I/e pakënaqur	I/e pakënaqur	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	I/e pakënaqur	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Jo	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	I/e pakënaqur	Indiferent	Aspak profesionalë	Jo	Jo	tjetër
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Plotësisht te gatshëm	Mjaftueshëm profesionalë		Po	tjetër
I/e pakënaqur	Kënaqshëm		Mjaftueshëm te gatshëm		Jo	Po	ABcom
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Indiferent	Mjaftueshëm profesionalë	Jo	Jo	Vodafone
I/e pakënaqur	I/e pakënaqur	I/e pakënaqur	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Po	Po	ABcom
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Indiferent	Aspak profesionalë	Jo	Jo	tjetër
I/e pakënaqur	Kënaqshëm	Kënaqshëm	Mjaftueshëm te gatshëm	Mjaftueshëm profesionalë	Jo	Jo	ABcom
I/e pakënaqur	I/e pakënaqur	Kënaqshëm	Indiferent	Mjaftueshëm profesionalë	Jo	Jo	ABcom

Po të bejmë tashmë një përballje me rastin e kundërt më ekstrem në përgjigje që është ai ku përdoruesi është i pakënaqur do të kemi këto përgjigje për secilën kategori respektive:

I-Si do ta kategorizonit ISP-në tuaj në bazë të (besueshmërisë, shpejtësisë, shkëputjeve të sinjalit)?

Tabela.35

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	I/e pakënaqur

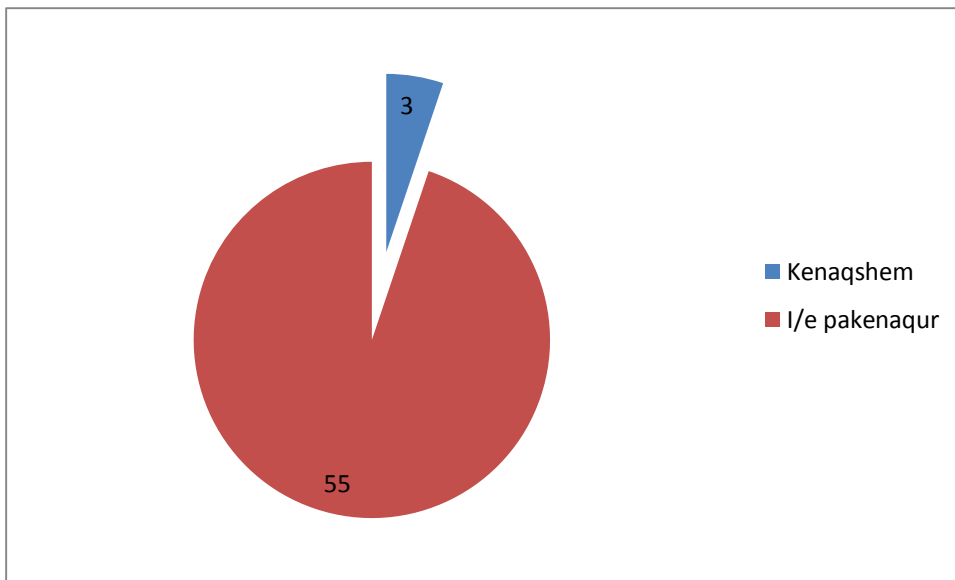
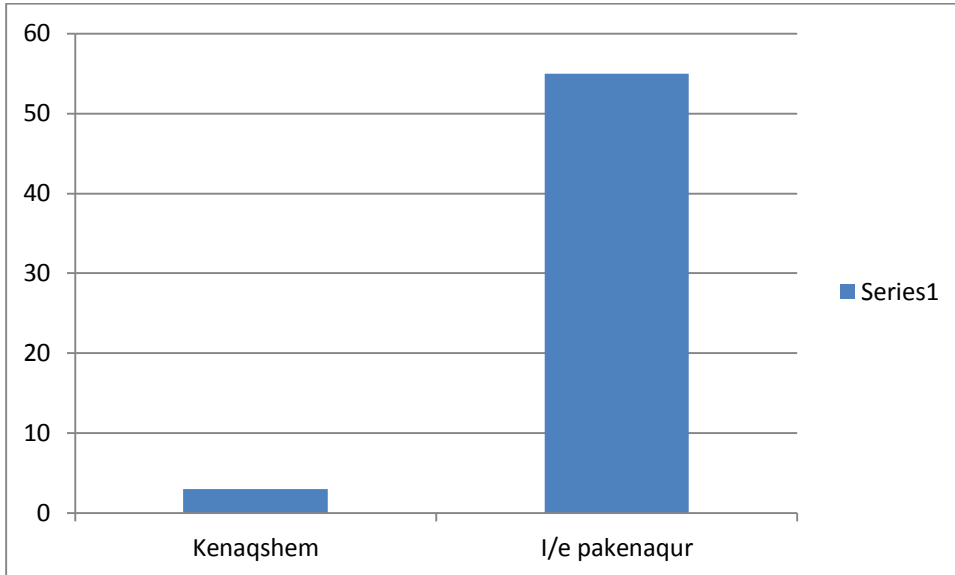
Pra totali i përgjigjeve për pyetjen e parë përmbledhet në:

Tabela.36

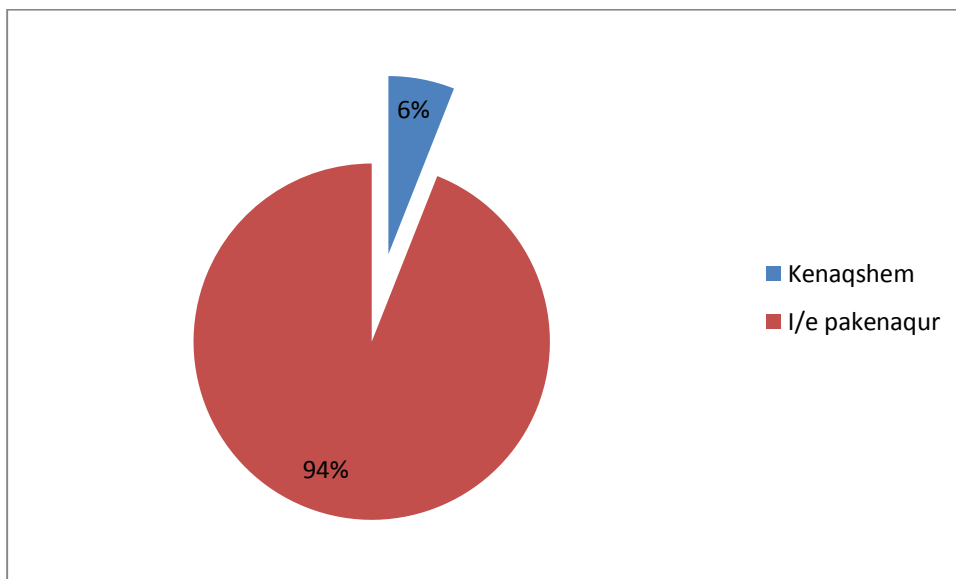
Kënaqshëm	3	6%
I/e pakënaqur	55	94%

Grafikët ndërkaq do të ishin këta për pyetjen e parë:

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



2-Si do ta vlerësonit software-in e instalimit si lehtësi në montim dhe në përdorim?

Tabela.37

Si ndiheni me shërbimin e ISP tuaj si ofrues interneti?	Si do ta vlerësonit software-in e instalimit si lehtësi ne montim dhe ne perdorim?
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	Shumë mire
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	
I/e pakënaqur	

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Shumë mire
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Shumë mire
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Shumë mire
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Shumë mire
I/e pakënaqur	Shumë mire
I/e pakënaqur	Shumë mire
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Shumë mire
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Shumë mire
I/e pakënaqur	Shumë mire
I/e pakënaqur	Shumë mire
I/e pakënaqur	Shumë mire
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

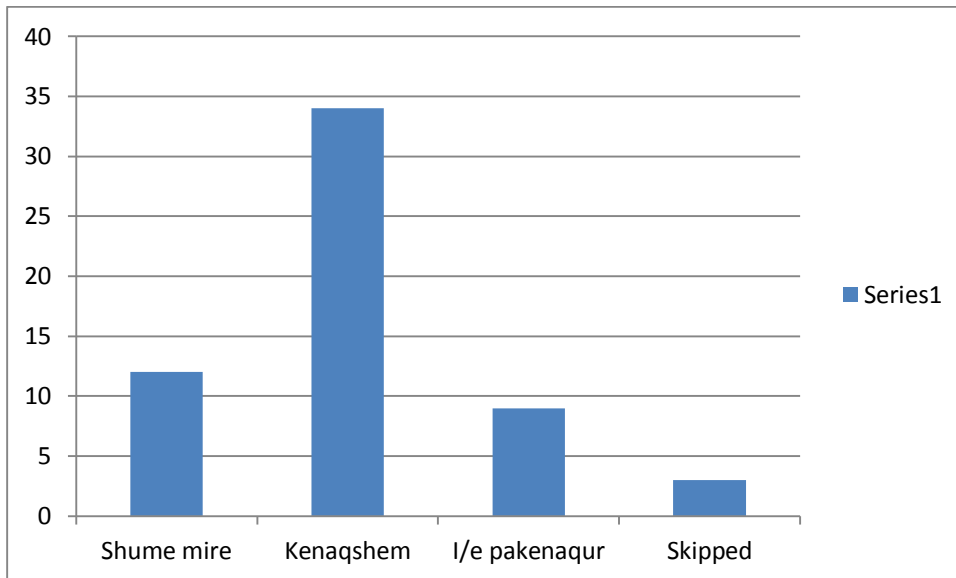
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	I/e pakënaqur
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm
I/e pakënaqur	Kënaqshëm

Pra totali i përgjigjeve për pyetjen e dytë përmbledhet në:

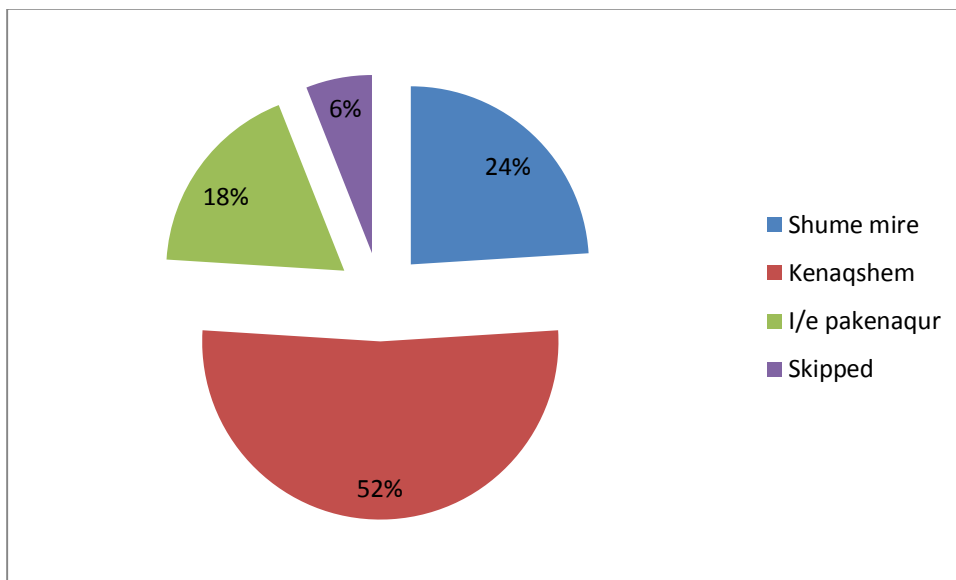
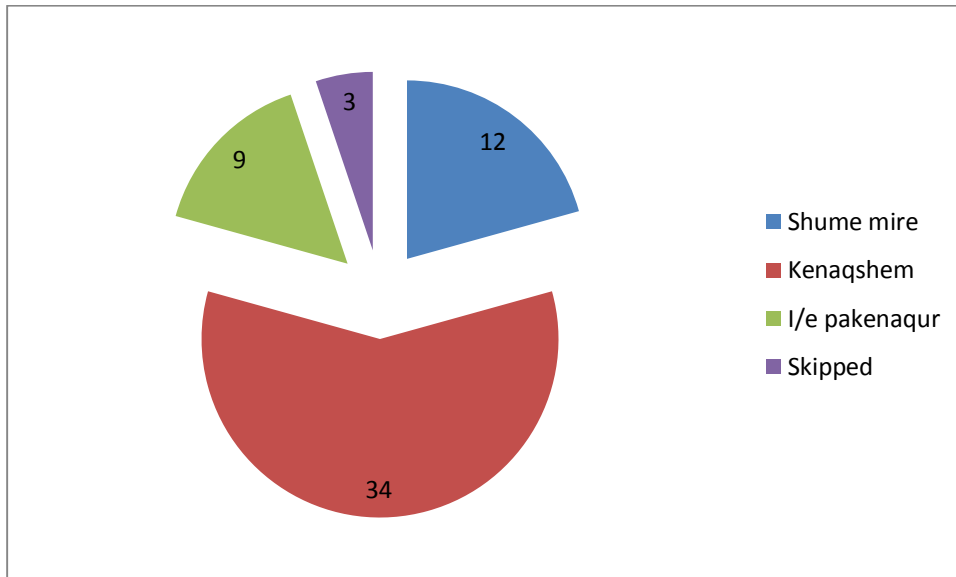
Tabela.38

Shumë mire	12	24%
Kënaqshëm	34	52%
I/e pakënaqur	9	18%
Skipped	3	6%

Respektivisht do të përftojmë këta grafikë në lidhje me këtë pyetje:



Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



3-Në lidhje me operatorët e shërbimit te klientit, si do ti vlerësonit?

Tabela.39

Si ndiheni me shërbimin e ISP tuaj si ofrues interneti?	Ne lidhje me operatorët e shërbimit te klientit, si do ti vlerësonit ?
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	
I/e pakënaqur	Plotësisht te gatshëm
I/e pakënaqur	Plotësisht te gatshëm
I/e pakënaqur	
I/e pakënaqur	
I/e pakënaqur	
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Plotësisht te gatshëm
I/e pakënaqur	Plotësisht te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Plotësisht te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Plotësisht te gatshëm
I/e pakënaqur	Plotësisht te gatshëm
I/e pakënaqur	Plotësisht te gatshëm
I/e pakënaqur	Plotësisht te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

I/e pakënaqur	Plotësisht te gatshëm
I/e pakënaqur	Plotësisht te gatshëm
I/e pakënaqur	Plotësisht te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Indiferent
I/e pakënaqur	Plotësisht te gatshëm
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Indiferent
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Indiferent
I/e pakënaqur	Mjaftueshëm te gatshëm
I/e pakënaqur	Indiferent

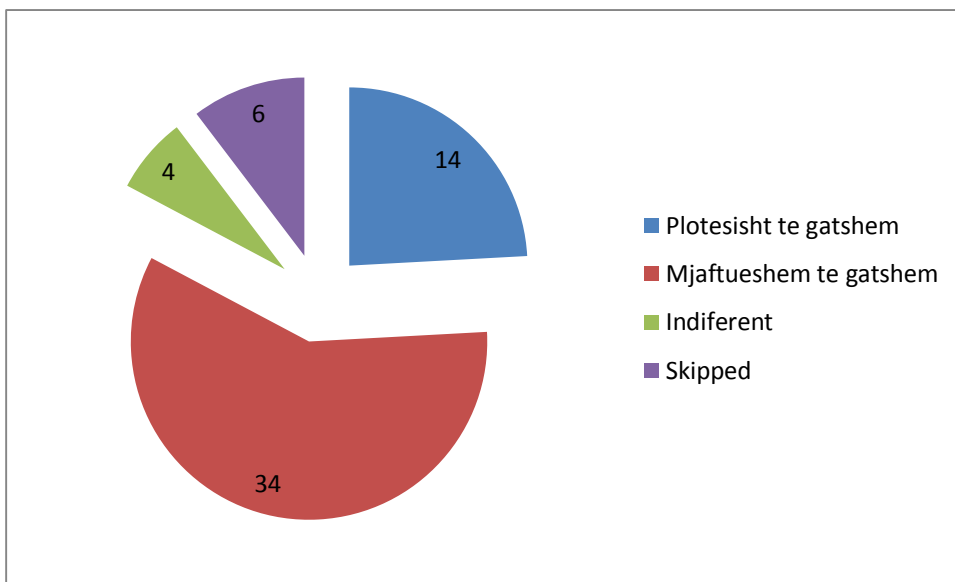
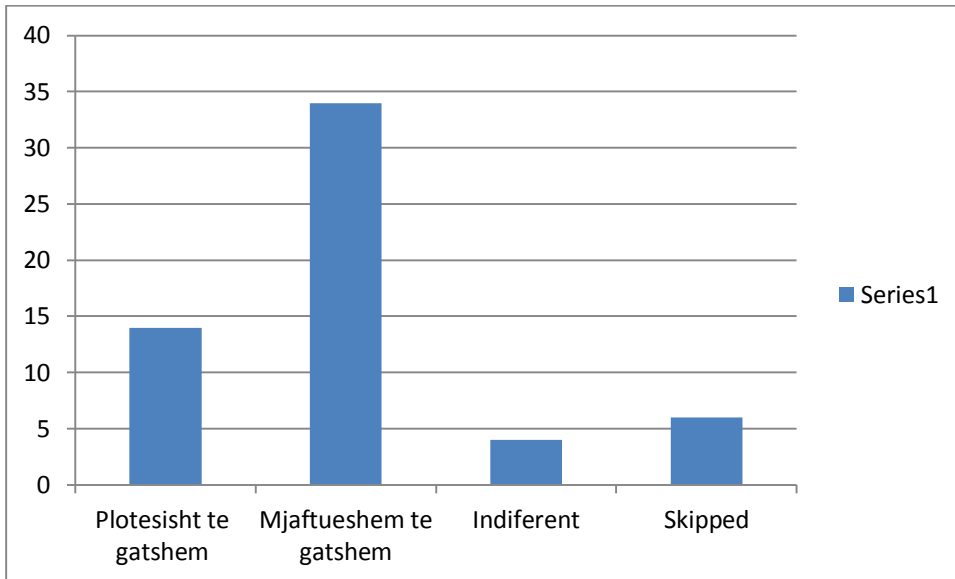
Pra totali i përgjigjeve për pyetjen e tretë përmbledhet në:

Tabela.40

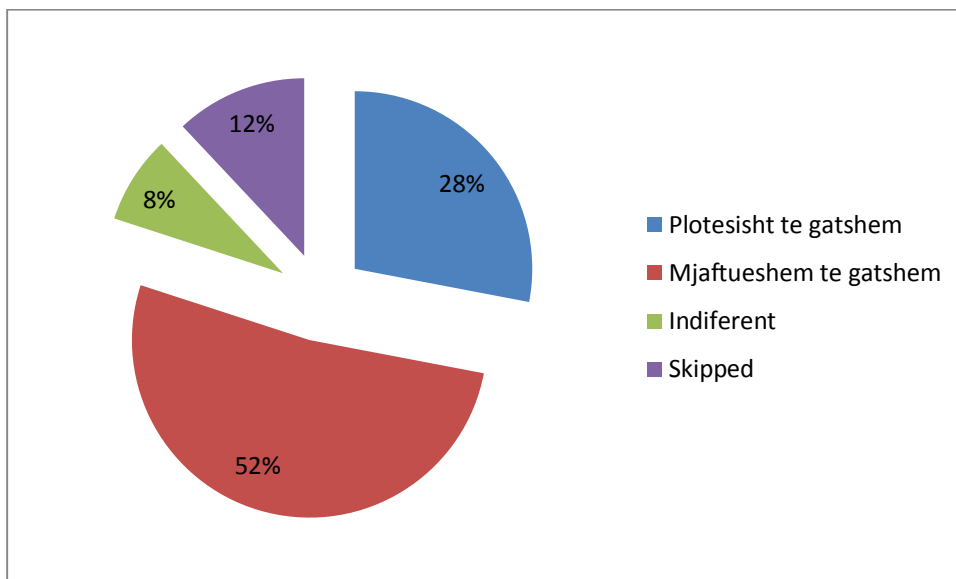
Plotësisht te gatshëm	14	28%
Mjaftueshëm te gatshëm	34	52%
Indiferent	4	8%
Skipped	6	12%

Grafikët e përftuar përmes programeve në këtë rast janë:

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



4-Sa profesionalë do ti vlerësonit operatorët e shërbimit ndaj klientit?

Tabela.41

Si ndiheni me shërbimin e ISP tuaj si ofrues interneti?	Sa profesional do ti vlerësonit operatorët e shërbimit ndaj klientit?
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	
I/e pakënaqur	Shumë profesionalë
I/e pakënaqur	Shumë profesionalë
I/e pakënaqur	
I/e pakënaqur	
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Shumë profesionalë
I/e pakënaqur	Shumë profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Shumë profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Shumë profesionalë
I/e pakënaqur	Shumë profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Aspak profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	
I/e pakënaqur	Mjaftueshëm profesionalë

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

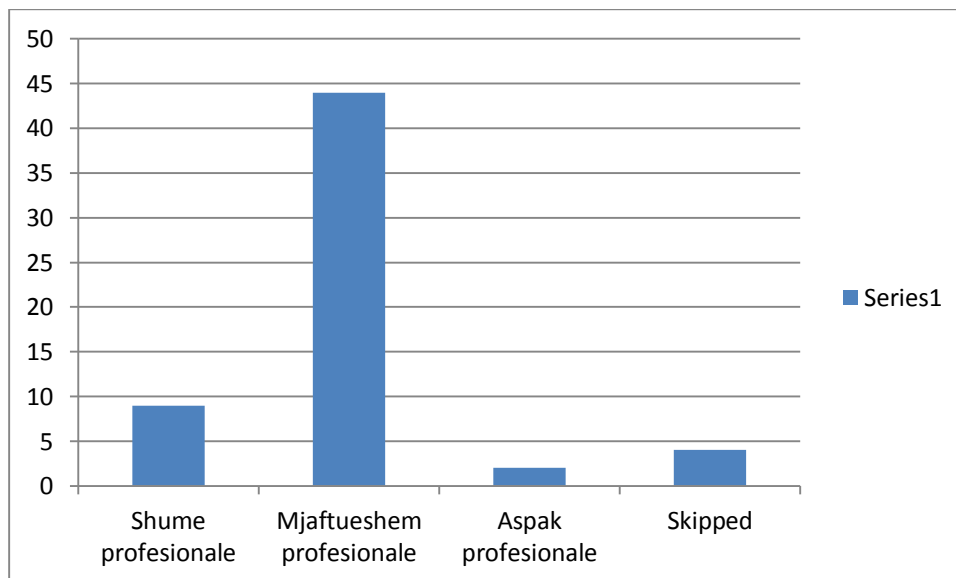
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Aspak profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë
I/e pakënaqur	Mjaftueshëm profesionalë

Pra totali i përgjigjeve për pyetjen e katërt përmblihet në:

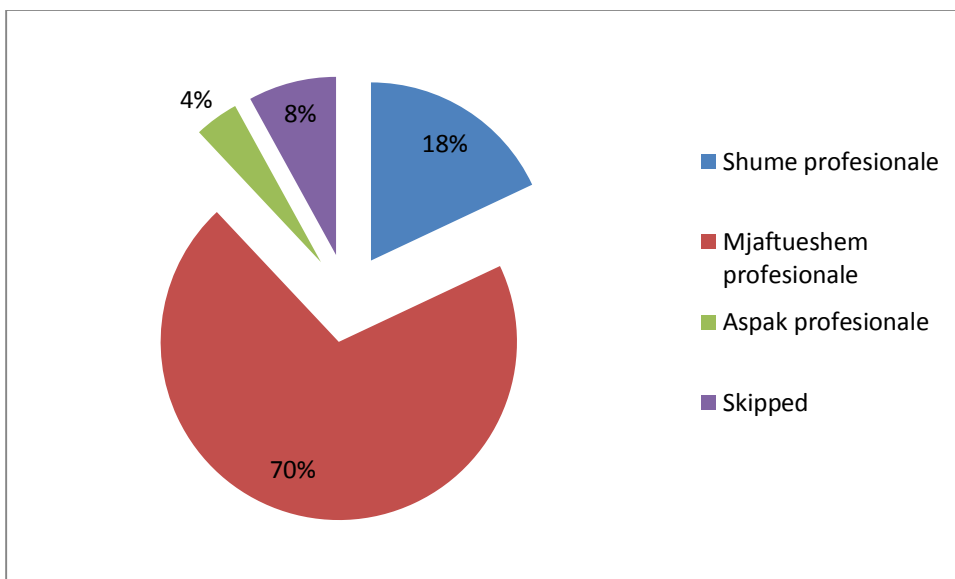
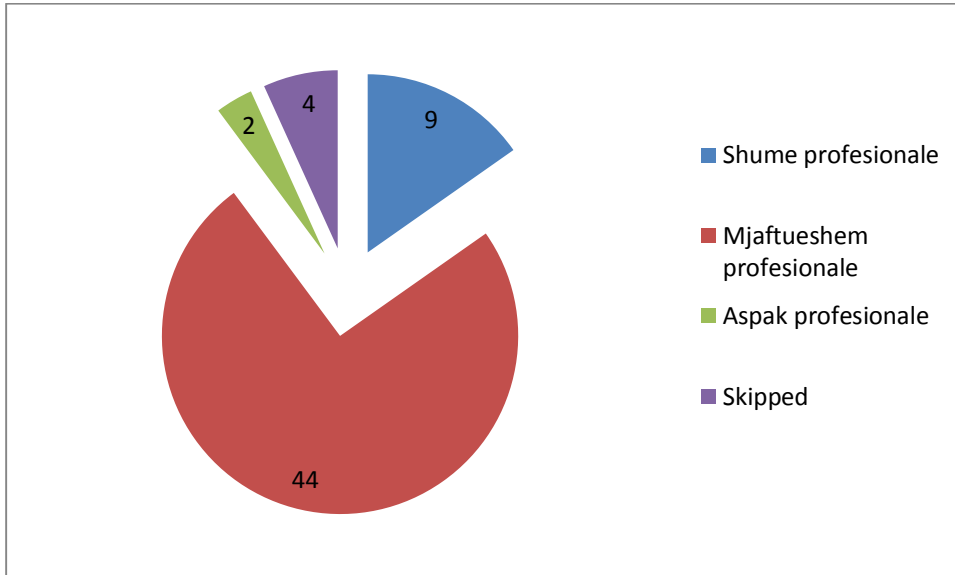
Tabela.42

Shumë profesionalë	9	18%
Mjaftueshëm profesionalë	44	70%
Aspak profesionalë	2	4%
Skipped	4	8%

Grafikët në këtë rast do të qenë:



Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



5-U zgjidh problemi juaj pas telefonatë me operatorin e shërbimit?

Tabela.43

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Si ndiheni me shërbimin e ISP tuaj si ofrues interneti?	U zgjidh problemi juaj pas telefonates me operatorin e shërbimit?
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Jo
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	
I/e pakënaqur	
I/e pakënaqur	
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Jo
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Jo
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Jo
I/e pakënaqur	Po
I/e pakënaqur	Jo
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Jo
I/e pakënaqur	Jo
I/e pakënaqur	
I/e pakënaqur	Jo
I/e pakënaqur	Jo
I/e pakënaqur	Po
I/e pakënaqur	Jo
I/e pakënaqur	Jo
I/e pakënaqur	Jo

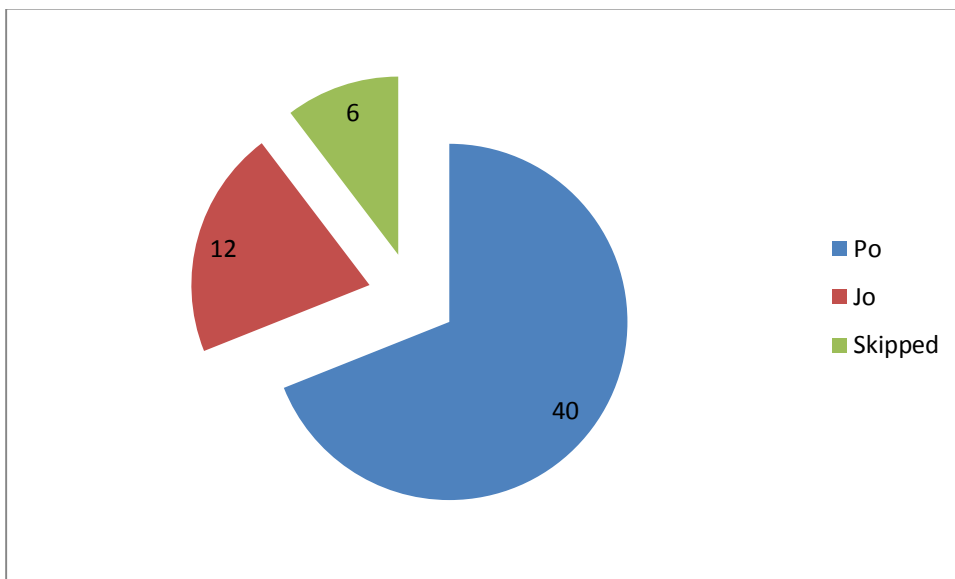
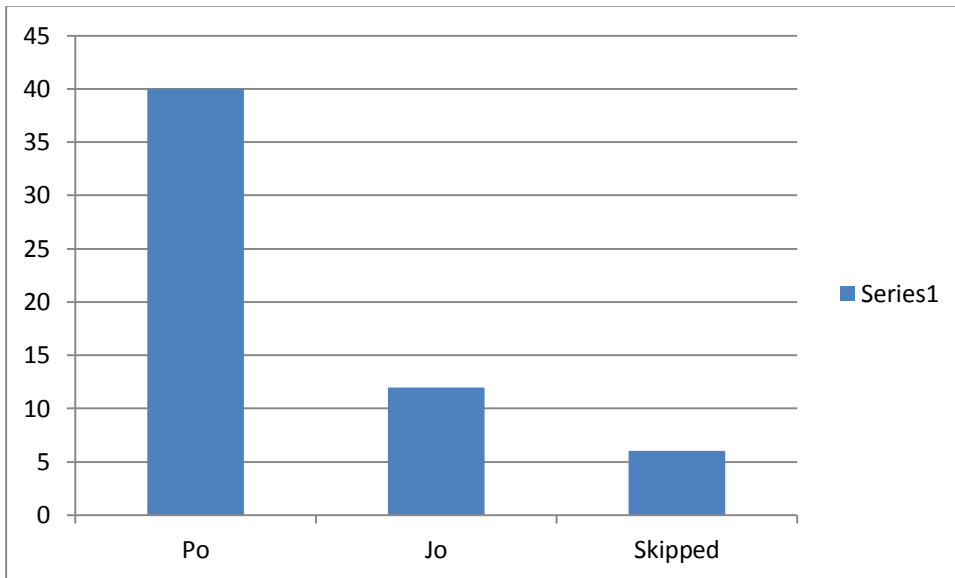
Pra totali i përgjigjeve për pyetjen e pestë përmbledhet në:

Tabela,44

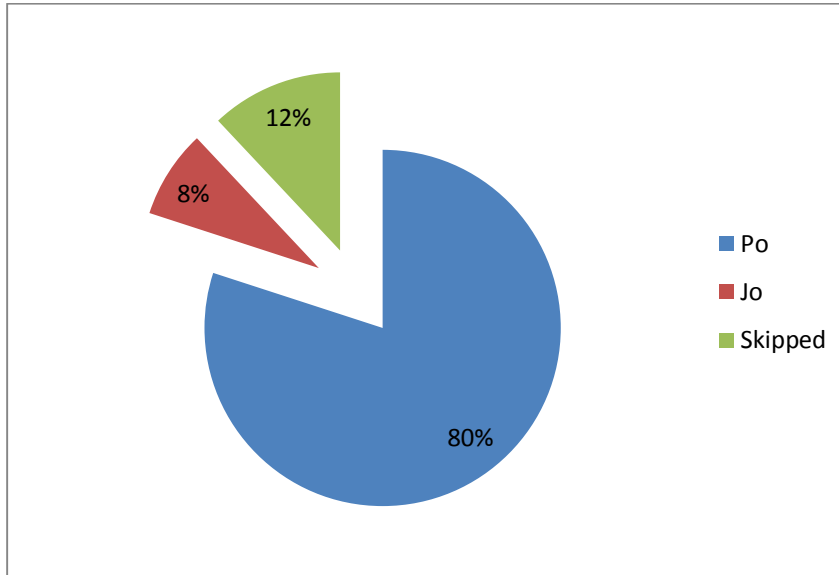
Po	40	80%
Jo	12	8%
Skipped	6	12%

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Grafikët në këtë rast do të ishin:



Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



6-Krahasuar me teknikët e ISP-ve të mëparshme që keni pasur kontratë shërbimi është me cilësor apo jo?

Tabela.45

Si ndiheni me shërbimin e ISP tuaj si ofrues interneti?	Krahasuar me tekniket e ISP-ve të mëparshme që keni pasur kontratë shërbimi është me cilësor apo jo?
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	Jo
I/e pakënaqur	Po
I/e pakënaqur	Jo
I/e pakënaqur	Jo
I/e pakënaqur	Po
I/e pakënaqur	Po
I/e pakënaqur	
I/e pakënaqur	Po
I/e pakënaqur	Jo
I/e pakënaqur	
I/e pakënaqur	

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

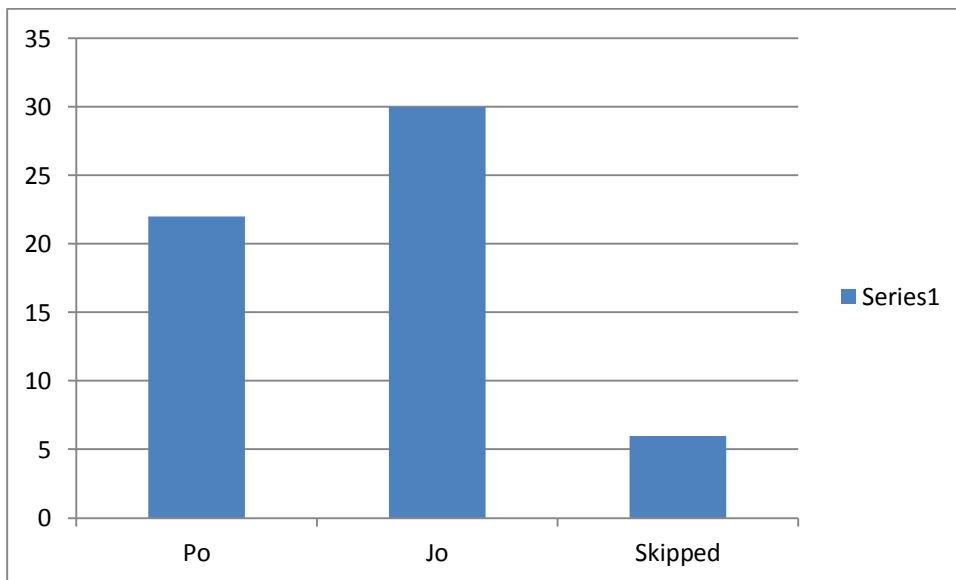
I/e pakënaqur	Po
I/e pakënaqur	Jo
I/e pakënaqur	Po
I/e pakënaqur	Jo
I/e pakënaqur	Jo
I/e pakënaqur	Jo

Pra totali i përgjigjeve për pyetjen e gjashtë përmbledhet në:

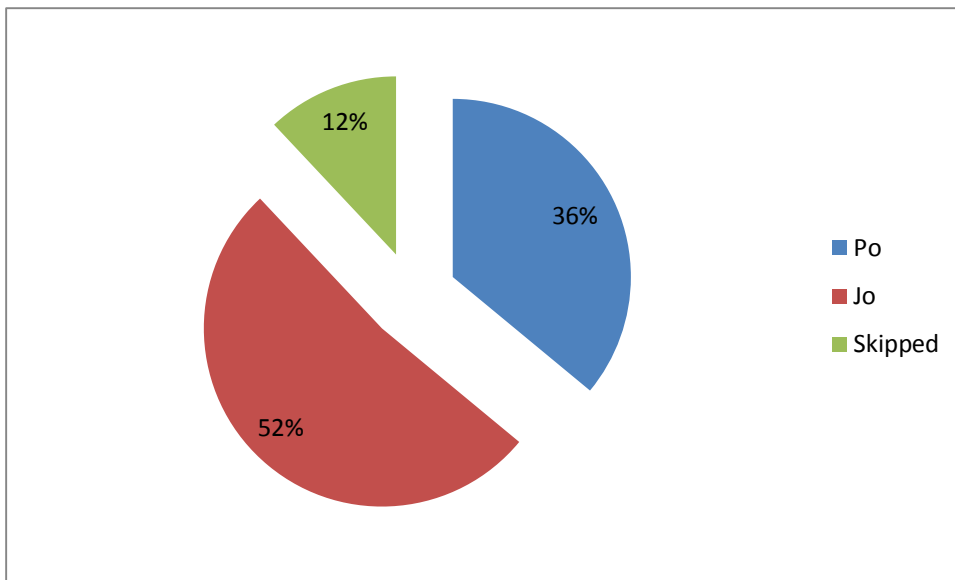
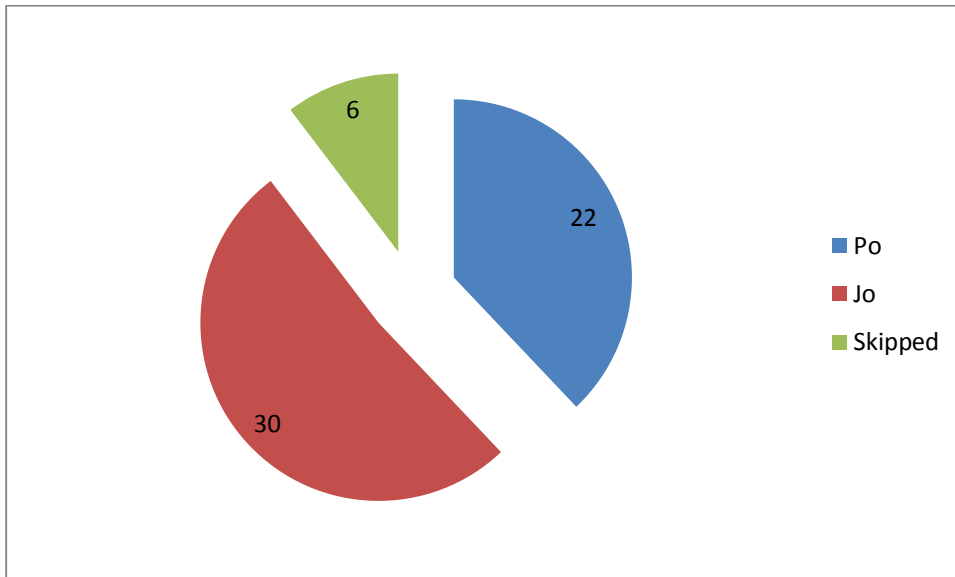
Tabela.46

Po	22	36%
Jo	30	52%
Skipped	6	12%

Grafikët e ndërtuar në këtë rast në lidhje me pyetjen janë:



Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



7-Cilën ISP keni zgjedhur për tu ofruar internet në ambientet tuaja?

Tabela.47

Si ndiheni me shërbimin e ISP tuaj si ofrues interneti?	Cilën ISP keni zgjedhur për tu ofruar internet në ambientet tuaja?
I/e pakënaqur	tjetër

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

I/e pakënaqur	tjetër
I/e pakënaqur	Abissnet
I/e pakënaqur	tjetër
I/e pakënaqur	Abissnet
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	
I/e pakënaqur	
I/e pakënaqur	
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	
I/e pakënaqur	tjetër
I/e pakënaqur	
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	Abissnet
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	Abissnet
I/e pakënaqur	tjetër
I/e pakënaqur	Tring
I/e pakënaqur	tjetër
I/e pakënaqur	
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

I/e pakënaqur	tjetër
I/e pakënaqur	Abissnet
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	Abissnet
I/e pakënaqur	tjetër
I/e pakënaqur	Abissnet
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	tjetër
I/e pakënaqur	ABcom
I/e pakënaqur	Vodafone
I/e pakënaqur	ABcom
I/e pakënaqur	tjetër
I/e pakënaqur	ABcom
I/e pakënaqur	ABcom

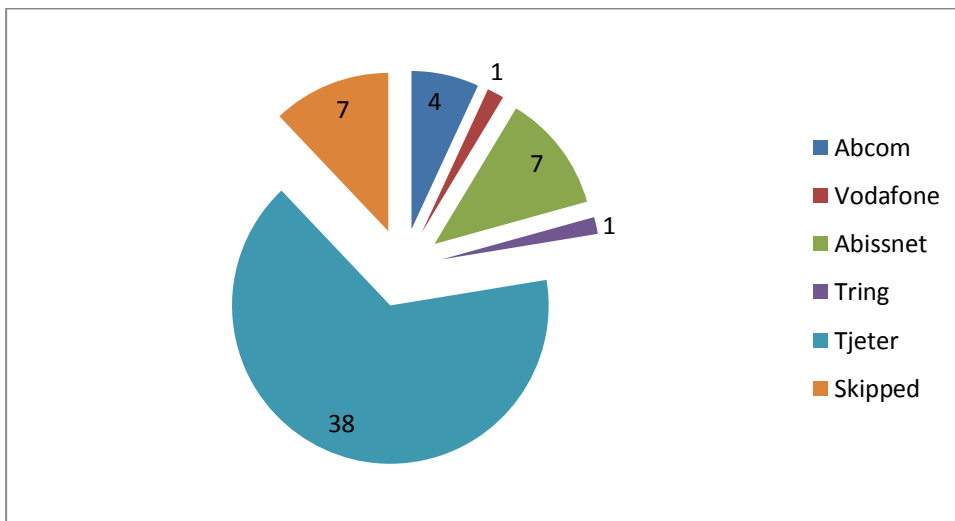
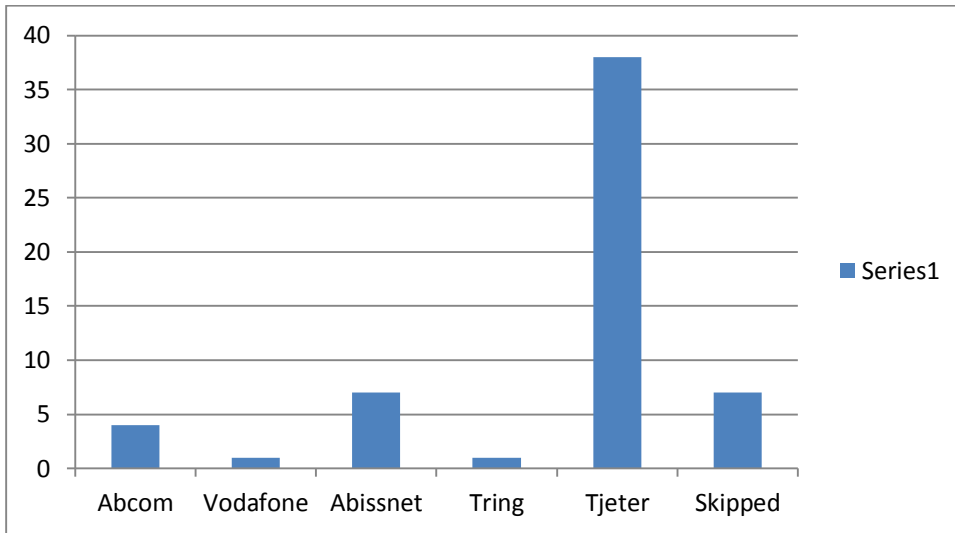
Pra totali i përgjigjeve për pyetjen e shtatë përmbledhet në:

Tabela.48

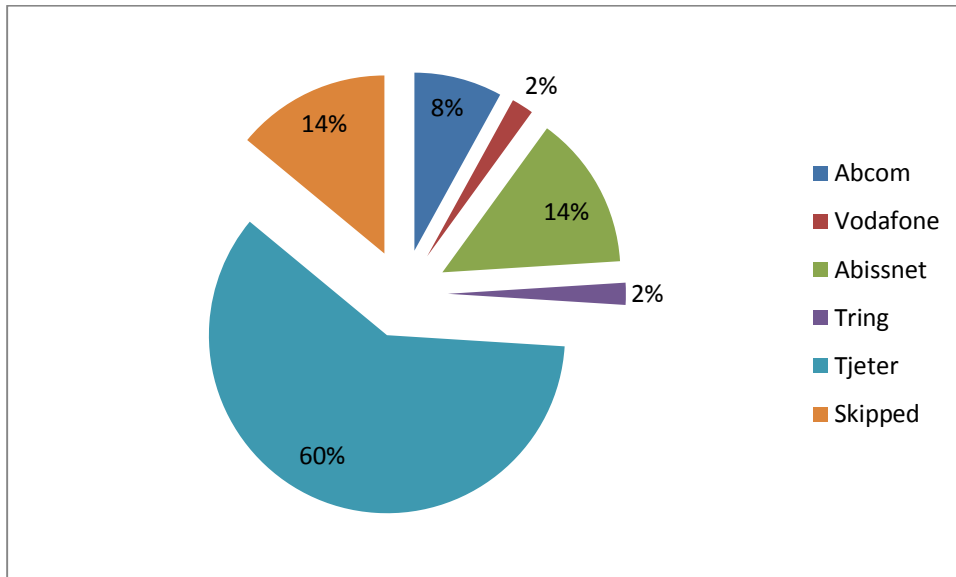
Abcom	4	8%
Vodafone	1	2%
Abissnet	7	14%
Tring	1	2%
Tjetër	38	60%
Skipped	7	14%

Diagrama përkatëse do të ishte për këtë rast:

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri



Konkluzione

Në këtë punim u ofrua një ambjent i integruar për realizimin e simulimeve që synojnë të studiojnë ndikimin e problemit të konvergencës së BGP mbi trafikun e aplikimeve në kohë reale në komunikimet *cross-domain*.

U evidentuan pikat e forta të protokollit BGP sikurse janë:

1) Fleksibiliteti

Ndryshe nga IGP, BGP është më tepër si një mjet për përcaktimin e politikave sesa thjesht një protokoll rrugëzimi. Për të zgjedhur rrugën më të mirë, BGP i vendos 11 attribute çdo rruge dhe një nga atributet më të rëndësishme të rrugëve është *Autonomous System Path* ose *AS_PATH*. *AS_PATH* lejon bllokim të menjëhershëm të cikleve në rrugëzimin e informacionit. *AS_PATH* shërben si një mekanizëm i fuqishëm dhe fluidpë rrugëzimet e bazuara mbi politika, për më tepër që çdo atribut i tij mund të aktivizohet veçmas për të lejuar një kontroll granular. Në kontrast protokollat IGP janë krijuar me qëllimin për të siguruar mbulim dhe konvergencë të shpejtë.

2) Besueshmëria

BGP përdor TCP për të siguruar komunikim të sigurt të trafikut midis entiteteve (T, Rekhter & Hares). Në vend që të krijojë gjithçka nga fillimi, BGP shfrytëzon të gjitha funksionet e TCP siç mund të përmendim: Fragmentarizimi, Ritransmetimi, Ack dhe Sekuencialiteti. Gjithashtu ajo mund të përdorë çdo skemë autentifikimi që përdor TCP, kjo e fundit rrit ndjeshëm kapacitetin e BGP në vendosjen e lidhjeve, ruajtjen e tyre si dhe saktësinë e informacionit të rrugëzuar.

3) Shkallëzueshmëria

Ndryshe nga protokollat IGP, BGP mund të suportojnë me mijëra rrugë në databazat e saj, pasi është krijuar me idenë e përshtatjes ndaj ndryshimeve në përmasa të internetit. Mekanizmi nga i cili është krijuar BGP lejon deri në 200 000 prefikse në ambjente rrjetesh prodhimi dhe më shumë se 500 000 në ambjente testesh laboratorike. Limitimi i vetëm praktik në numër prefiksesh të suportuar është në memorijen e router-it.

4) Qëndrueshmëria

Duke patur parasysh madhësinë e Internetit në ditët e sotme mund të themi se “ulje-ngritjet” e një numri të madh rrugësh mund të jetë fatal për rrjetin. Për të kaluar këto probleme BGP ka implementuar një sërë mekanizmash për të ulur nivelin e instabilitetit, si psh: *Route Flap Damping (RFD)*, *Adaptive Minimal Route Advertisement Interval (AMRAI)*, rikonfigurime si dhe rifreskim të rrugëve janë mjete në nevojshme për të ndryshuar politikat e BGP pa qënë nevoja e rivendosjes së sesionit BGP.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Pikat e dobëta të protokollit BGP që u vërtetuan përmes simulimeve laboratorike:

1) Konvergjenca e dobët (e ngadaltë)

Protokolli BGP është protokoll më i ngadaltë nga të gjithë. Mungesa e sinkronizimit shpesh shpie në probleme me konvergjencën. (Griffin and Premore) përdorën simulime për të treguar sesi konvergjenca ndikohet nga parametri i kohës MRAI dhe eksplorimi i impaktit të tij në topologji të ndryshme. Vlera e parametrut MRAI duket të jetë më i madh sesa nevojitet.

2) Rritja e madhësisë së tabelave

Interneti rritet me hap eksponencial çdo vit, nëse tabelat globale të rrugëzimit do të rriteshin në atë pikë ku router-at e vjetër dhe me më pak mundësi të mos përmbushnin dot kërkesat për Cpu/Memorje, këta router-a do të pushonin së qeni efektiv si gateway për pjesët të cilat ata lidhnin, duke lënë kështu shërbimet e rrjetit të pabesueshme ose më keq jashtë funksionit.

3) Balanca e ngarkesës

BGP *by-default* nuk e ndan ngarkesën e rrjetit midis rrugëve të ndryshme, gjë e cila shkakton probleme në QoS, pasi në një moment që është duke u përdorur një rrugë, një tjetër mund të jetë më efektive për të arritur në të njëjtin destinacion.

Në këtë punim u ofrua një ambjent i integruar për realizimin e simulimeve që synojnë të studiojnë ndikimin e problemit të konvergjencës së BGP mbi trafikun e aplikimeve në kohë reale në komunikimet *cross-domain* ku u ndoq një metodologji që fillon me përcaktimin e modelit të rrjetit (përmes përcaktimit të topologjisë, rrugëzimit dhe modelit të të dhënave), përcaktimin e moduleve të nevojshme të ns2, përcaktimit të skenarëve të simulimeve dhe analizës së vazhdueshme “What-If”.

Për të krijuar një model sa më afër realitetit u zgjodh gjeneratori i topologjisë të tipit random, por që modelon pjesërisht hierarkinë e Internetit. Mangësia e këtyre gjeneratorëve qëndron në faktin se zakonisht ata nuk mundësojnë modelim të rrugëzimit në Internet.

Për modelimin e rrugëzimit në Internet, u ndërtua një modul përkatës i cili duhet të integrohej në strukturën e simulatorit të rrjetit, e ndoqi të gjitha specifikimet për BGP-4 përmes disa simulimeve që evidentojnë parimet bazë të rrugëzimit në Internet.

Modelimi i trafikut përbën gjithashtu një hap të rëndësishëm në përcaktimin e parametrave të cilësisë të rrjetit të simuluar. Për modelimin e një trafiku në kohë reale, siç është ai i komunikimeve VoIP, në këtë punim u përzgjedh modeli që bazohet në UDP përmes një gjeneratori trafiku CBR. Karakteristikat e trafikut përcaktohen në përputhje me ato të një koduesi VoIP.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

Konkluzione të tjera nga simulimet e kryera dhe studimi i trafikut interdomain janë:

-Simulimet e realizuara dëshmojnë se modeli i përzgjedhur i rrugëzimit i cili është në përputhje me kërkesat bazë për BGP dëshmon se problemi i kohës së konvergencës së BGP ndikon drejt për së drejti në trafikun që përshkon rrjetin. Ky ndikim në simulimet në fjalë është i vogël si rrjedhojë e përmasave të rrjetave të përzgjedhura. Në një simulim në shkallë të gjërë ky ndikim do shumëfishohej në përputhje me përmasat e rrjetit duke marrë në konsideratë faktin se gjerësia e brezit të konsumuar nga paketat BGP është në varësi të drejtë me numrin e përmasave të rrjetit duke vërtetuar kështu hipotezën e parashtruar.

-Edhe pse modelimi i trafikut VoIP përmes CBR në UDP përshtatet me qëllimin e këtij punimi, do të ishte mirë që ky thjeshtëzim të konvertohej në diçka më të plotë në të ardhmen. Një modelim i mirë nënkupton dhe përfshirjen e kokave të paketave dhe sigurisht periudhave on - off.

-Pra nga simulimet e kryera u vu re se në cdo rast që gjeneratori gjeneronte trafik të paketave, kishim një vonesë në transmetimin e tyre sa herë që ndeshnim në një update-im të protokollit të internetit BGP. Kjo vërteton dhe hipotezën.

-Optimizimi i paketave në rrjetat me topologji të ndryshme dhe integrimi i tyre në një format të vetëm rrit performancën e komunikimit midis kostove të ndryshme fikse dhe mobile me dhe pa infrastrukturë.

-Protokolli i rrugëzimit interdomain Border Gateway Protocol shfaq konvergencë të ngadaltë në nivel performance dhe paraqet integritet të ulët duke vërtetuar dhe hipotezën tonë.

-Interneti ka heterogjenitet, përmasa shumë të mëdha, ndryshueshmëri të vazhdueshme, tre tipare këto thelbësore me peshë në transmetimin e paketave.

Inxhinierimi i trafikut është përcaktuar si procesi i vlerësimit dhe rritja e performancës së rrjeteve IP operacionale.

-Objektivat e Inxhinierisë së Trafikut mund të përmbliken në shmangien e bllokimit congestion, duke siguruar elasticitet dhe mbështetje të cilësisë së shërbimit (QoS). Shumica e kompleksitetit të Inxhinierisë së Trafikut vjen nga shpërndarja IP me bazë destinacionin hop-by-hop, dmth secili router në rrugë zgjedh routerin tjetër për të përcjellë pakëta të bazuar në vetëm destinacionin e paketave. Nuk ka asnjë mënyrë për të përcaktuar në mënyrë të qartë rrugën e ndjekur nga datagramet IP për të arritur destinacionin e tyre. Për më tepër, vendimet e rrugëzimit janë marrë në mënyrë të shpërndarë nga çdo hop përgjatë rrugës.

-Një nga vështirësitë kryesore të Inxhinierisë së Trafikut vjen kështu nga rrugëzimi. Brenda një domaini të vetëm, rrugëzimi është bërë në sajë të protokolleve Lidhje-gjëndje si IS-IS ose OSPF. Nga perspektiva e Inxhinierisë së Trafikut, këto protokolle kanë

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

avantazhin e dyfishtë të përhapjes së informacionit në të gjithë topologjinë dhe optimizimin e një objekti të vetëm global (rruga me kosto më të ulët).

-Në të kundërt, kur Inxhinieria e Trafikut duhet të kryhet mbi kufijtë e domaineve të shumtë, gjërat janë shumë më të vështira. Në qendër të problemit është vetë sistemi i rrugëzimit të Internet. Rrugëzimi i internetit është ndërtuar aktualisht rreth (BGP). BGP është një protokoll path-vektor, që është ai i cili propagandon vetëm një pamje të kufizuar të topologjisë. Një router BGP do të reklamojë për fqinjët e tij një rrugë të vetme për destinacionin e arritshëm. Duke pasur parasysh madhësinë e internetit, ky ka përparësi të mëdha në aspektin e shkallëzueshmërisë dhe stabilitetit.

-Një karakteristikë tjetër e BGP është se çdo domain administrohet në mënyrë të pavarur. Për këtë arsye, BGP në çdo fushë është konfiguruar për të optimizuar objektive lokale. Objektivat e një domain mund të jenë shumë të ndryshme nga ato të një tjetri. Për më tepër, çdo domain është i lejuar për të filtruar rrugët e reklamuar në domaine të tjera.

-Kjo paraqet sfidë serioze për Inxhinierinë e Trafikut interdomain. Së pari, pamja e kufizuar e topologjisë për shkak të natyrës path-vektoriale e BGP dhe për shkak të politikave të rrugëzimit lokal ulin diversitetin e rrugëve interdomain dhe më pas të lirisë së një AS për të drejtuar trafikun përgjatë rrugëve alternative. Së dyti, një AS nuk është i etur për të lënë AS-të e tjerë të kontrollojnë rrugëzimin në rrjetin e vet. BGP siguron kontroll shumë të kufizuar në vendimet e rrugëzimit të marra nga domaine të tjerë. Për shkak të ndërveprimit midis dy llojeve të protokolleve të rrugëzimit (link-state dhe path-vector) është një detyrë komplekse parashikimi i ndikimit në rrugëzim i një rrjeti ISP I ndryshimeve topologjike dhe konfigurimi.

-Është vlerësuar shfrytëzimi i peerings virtuale për të zgjidhur dy objektivat e trafikut inxhinierik: ngarkesës-balancimi dhe përmirësimi i vonësës fund-më-fund.

-BGP, protokollin aktual i rrugëzimit interdomain nuk është i bazuar në optimizimin e një metrike të vetme si në protokollet Lidhje-gjëndje, por në një proces kompleks vendimmarrjeje të përbërë nga disa rregulla. Procesi i Inxhinierisë së Trafikut është i vështirë, kur kryhet në të gjithë kufijtë e domaineve të shumëfishta.

– Modelimi i Rrugëzimit BGP është diskutuar për modelimin e rrugëzimit BGP dhe vlerësimin e teknikave inxhinierike të trafikut interdomain. Është treguar se ky vlerësim është i vështirë për dy arsye kryesore. Së pari, topologjia e internetit është e madhe gjë që i bën njehsimet e simulimeve shtrenjtë. Së dyti, zgjedhja e rrugëve e kryer nga BGP është komplekse dhe modelimi nuk mund të mbështetet në shkurtesat srrugëzime përdoret për protokollet lidhje-gjëndje(link-state).

-Janë studiuar mjetet që janë përdorur tradicionalisht për të studiuar rrugëzimin BGP dhe u konstatua se asnjë prej tyre aktualisht nuk është i përshtatshëm në mënyrë efektive për të studiuar zgjedhjen e rrugëve BGP në internetin global duke përcaktuar një qasje të re për problemin që është e quajmë një solver rrugëzimi BGP.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

- Në mënyrë tipike, një ISP do të përpiqet për të ulur vonesën e tranzitimit brenda rrjetit të saj për destinacione të jashtme dhe në të njëjtën kohë të balancojë ngarkesën e trafikut në lidhjet e saj peering. Kjo është e vështirë të optimizohet për shkak të bashkëveprimit të IGP dhe protokolleve të rrugëzimit BGP.

- Është treguar se duke përdorur një model të një ISP-je bëhet e mundur shqyrtimi i zgjidhjeve të ndryshme peering. Kjo nuk do të ketë qenë e mundur për të kryer këtë lloj të analizës, pa një model të ISP që merr parasysh informacionin e rrugëzimit interdomain të marrë nga jashtë ISP.

- Në një studim të dytë shqyrtuam ndikimin e dështimeve të lidhjeve dhe routerave në rrugëzim dhe në matricën e trafikut brenda një ISP-je. Ky është një problem i rëndësishëm meqë ngjarje të rrjetit të tilla si dështime të hardwareve të routerave, shkurtime të lidhjeve link dhe mirëmbajtjet janë të shpeshta. C-BGP ndihmon operatorin e rrjetit për të identifikuar lidhjet dhe routerat që mund të çojnë në ndërprerje të mëdha të shërbimit.

- Këto lidhje do të jenë kandidat i mirë për shtimin e lidhjeve paralele apo vendosjes së teknikave të mbrojtjes të tilla si SONET-SDH dhe tuneleve MPLS. Është treguar se një model i pastër intradomain e një ISP siç përdoret nga versionet e tanishme të projektimit të rrjetit komercial dhe mjetet e planifikimit do të humbasë shumicën e ndryshimeve të rrugëzimit që ndodhin nën dështimet e Lidhjeve dhe routerave të vetme. Ky është një motivim i dytë për të marrë në konsideratë rrugët interdomain në një model të një ISP-je. Është vërejtur se një pjesë e madhe e rrugëve interdomain zgjidhen nga rregullat tie-breaking të procesit të vendimmarrjes BGP. Ky është një lajm i keq për teknikat e tanishme të inxhinierisë së trafikut në hyrje që shumë vendime rrugëzimi varen në kushtet lokale në AS-ët e largët.

Është vërejtur se rezultati i AS-Path prepending është i vështirë të parashikohet. Në praktikë, dobia e AS-Path prepending është e kufizuar për të sinjalizuar linqet backup.

- Një teknikë e dytë që është vendosur gjithnjë e më shumë nga ISP-të mbështetet në komunitetet BGP. Edhe pse ajo ofron një granularitet më fin se AS-Path prepending, rezultati i saj nuk është i lehtë të parashikohet. Shkaku kryesor është pamja e kufizuar që një ISP ka në topologjinë e internetit për shkak të natyrës path-vektoriale e BGP dhe zbatimit të politikave të rrugëzimit. Përveç kësaj, komunitetet BGP janë më të vështira për përdorim në praktikë pasi numri i caktimit të komuniteteve të mundshme është kombinator.

- U arrit në përfundimin se teknikat aktuale të inxhinierisë së trafikut me bazë BGP nuk janë të përshtatshme për të kontrolluar trafikun në hyrje të një ISP-je në internetin e sotëm duke propozuar një zgjidhje alternative për inxhinierinë e trafikut interdomain problem i cili mbështetet në bashkëpunimin. U përshkrua Peerings Virtual, një zgjidhje e shkallëzuar deterministike që AS-ët bashkëpunues mund të përdorin për të kontrolluar më mirë shtigjet interdomain mes njëri-tjetrit. Avantazhi kryesor i kësaj qasjeje është të jenë

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

të dislokueshme në internetin aktual meqë Peerings Virtual janë transparente për bërthamën e internetit dhe ata kërkojnë vetëm modifikime të vogla për routerat BGP në AS-ët bashkëpunues. U vlerësua përdorimi i Peerings virtuale për të zgjidhur dy probleme të ndryshme inxhinierike të trafikut interdomain.

-Shumë ISP në këtë situatë kanë trafikun e tyre në hyrje të pabarabartë të ekuilibruar në lidhjet e tyre të aksesit. Ky çekuilibër mund të shkaktojë mbipopullim në lidhjet e aksesit dhe prishë shërbimin e lidhjes. Duke përdorur Virtual Peering, është e mundur për të kontaktuar disa AS bashkëpunues që janë përgjegjës për një tejkalim të trafikut në një lidhje të qasjes dhe i pyet ata për të shpërndarë paketat të destinuara për ISP stub në një tunel të drejtuar në një tjetër router hyrjeje.

-Përdorimi i Peerings Virtual dëshmon në këtë mënyrë të jetë një zgjidhje e shkallëzuar e problemit ngarkesë-balancimi. Të njëjtën teknikë mund të përdorim edhe për optimizimin e kostos-kursime apo për të zbatuar politikat e trafikut të tilla si një shërbim të diferencuar përmes një ofruesi premium dhe një ofruesi të best-effort.

-Aplikimi i dytë i Peerings Virtual që u hetua është reduktimi i fshehtë mes dy ISP-ve. Duke përdorur Peerings virtuale, është e mundur për të kontrolluar segmentet e para dhe të fundit të një rruge interdomain. Në mesin e këtyre rrugëve, BGP është i etur për të zgjedhur një më të keqe në terma vonese (latency) që procesi i vendimmarrjes BGP nuk përfshin një metrikë QoS dhe gjatësia AS-Path lidhet rrallë me vonesën.

-Bazuar në një topologji interneti sintetike, u hetua se sa herë vonesa midis një çifti domainesh stub mund të reduktohet duke përdorur Peerings Virtual. Është vërejtur se një pjesë e rëndësishme e çifteve stub (40% për topologji tonë sintetike) mund të përfitojnë nga një përmirësim i vonesës, ndërsa përmirësime të tilla mund të jenë në rendin e dhjetra milisekondave.

Konkluzionet në lidhje me cilësinë e shërbimit të internetit në Shqipëri nga statistika e zhvilluar mbi kampionin e përdoruesve të internetit sikurse janë studentet e UET përftuan 524 përgjigje të cilat na cuan në disa përfundime të rëndësishme:

-Kështu pjesa në minorancë, pra gati 5% u përgjigjën që ishin maksimalisht të kënaqur nga shërbimi i internetit të ofruar nga ISP-të operuese në Shqipëri.

-Pjesa më e madhe e përdoruesve ishin disi dhe mesatarisht të kënaqur me atë cka ofrojnë ISP-të në vendin tonë.

-Kjo tregon pra që QoS nuk është në nivelet e duhura në vendin tonë. Ka një pozicion mesatar në lidhje me cilësinë e shërbimit ku ndikojnë shumë faktore sëbashku.

-Nga anketa e zhvilluar pjesa më e madhe u përgjigjën se ishin kënaqshëm të shpërblyer nga QoS e ISP-ve operuese në vendin tonë. Pra në një shkallë nga 1-4 në lidhje me

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

cilësinë 46.73% e tyre rezultuan të ishin në shkallën 3 të kënaqur. Ndërkaq pjesa tjetër dërrmuese që përfshin jo pak, por plot 36.15% janë përgjigjur në shkallën 2 të vlerësimit si shumë mirë përsa i përket QoS së internetit në vendin tonë. Pjesa më e pakët ka rezultuar të jetë maksimalisht e kënaqur nga cilësia e shërbimit në vendin tonë pra vetëm gati 6% konkluduan shkëlqyer në shkallën 1 si vlerësim për internetin dhe QoS e tij në Shqipëri. Sakaq pjesa e mbetur pra rreth 11% rezultuan me vlerësimin më të ulët për QoS në vendin tonë, si të pakënaqur plotësisht me shërbimin e ISP-ve respektive si ofrues interneti.

Nëse vazhdojmë me konkluzionet e analizës së mëtejshme evidentojmë që disa nga aspektet e QoS në Shqipëri sikurse janë: besueshmëria, shpejtësia, shkëputjet e sinjalit do të renditeshin në këto shkallë vlerësimi prej përdoruesve si në vijim.

-Pra pjesa dërrmuese që përfshin dhe thuhet 50% të të anketuarve e konsiderojnë të kënaqur mjaftueshëm ISP-në e tyre në përputhje me këto karakteristika duke e vlerësuar në 1 shkallë nga 1 në 4 me 3 ISP-në e tyre. Nga ana tjetër pjesa më e lartë e mbetur nga të anketuarit do të vlerësonin me shkallën 2 ISP-në e tyre duke përbërë edhe 30% të të anketuarve. Këtu shohim që thuhet 17.5% japin vendimin e tyre si të pakënaqur plotësisht me ISP-në respektive pra duke i kategorizuar me shkallën e fundit të vlerësimit, 4 në lidhje me karakteristikat e shërbimit të internetit si: besueshmëria, shpejtësia, shkëputjet e sinjalit etj. Sakaq pjesa e mbetur rezulton të jetë në kuotën e 3.5% me vlerësim maksimal në shkallën 1 të këtyre parametrave të shërbimit të ISP-ve.

-Në vazhdim në lidhje me një variabël sikurse është software-i i instalimit si lehtësi në montim e përdorim kemi një diferencë në vlerësimin që i bëjnë përdoruesit krahasuar me 2 variablat paraardhëse. Këtu shohim që mbizotërojnë përgjigjet e të anketuarve në shkallën 2 të vlerësimit, pra 44.1% janë të mendimit që software i përzgjedhur nga ISP-të është në nivelin e duhur, pra shumë i mirë për lehtësi, facilitet instalimi e përdorimi. Krahas tyre kemi dhe një pjesë të anketuarish prej 42.3% të cilët e votojnë me kënaqshëm këtë variabël. Shkëlqyer do të përgjigjeshin rreth 10.8% të të anketuarve duke cuar në 2.7% përqindjen e atyre që e vlerësojnë me shkallën minimale këtë faktor.

-Pra shohim që variabli i software-it të hedhur në treg nga ISP-të shqiptare janë të duhur dhe ndikojnë pozitivisht në vlerësimin e përgjithshëm të QoS së internetit në Shqipëri.

-Një tjetër variabël i marrë në studim janë pikërisht operatorët e shërbimit ndaj klientit si nivel shërbimi ndaj abonentit. Lidhur me këtë pikë pjesa dërrmuese rreth 56.7% janë të kënaqur në shkallën 2 në një vlerësim nga 1 në 3 këtë herë duke i konsideruar operatorët e shërbimit 'mjaftueshëm të gatshëm' në shërbim ndaj klientit. Nga pjesa e mbetur e të anketuarve plot 41.5% i kanë dhënë vlerësimin maksimal operatorëve të shërbimit duke i cilësuar plotësisht të gatshëm operatorët shqiptarë kundrejt klientëve respektivë. Prej këtej shohim se vetëm një masë e vogël, gati e pakonsiderueshme prej 1.8% rezultojnë të

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

pakënaqur duke i renditur në shkallën 3 që i korrespondon vlerësimit 'indiferent', nga 1 në 3 operatorët e shërbimit.

-Po ashtu studiohet dhe profesionalizmi që kanë operatorët e shërbimit ndaj klientit duke pasqyruar zgjidhjen ose jo të problemeve të paraqitura nga klientët në kohë të ndryshme. Edhe në këtë situatë qëndrimi i mbajtur nga të anketuarit është pozitiv ku thuhet se 67% e tyre ndajnë mendimin e përbashkët që operatorët e shërbimit janë mjaftueshëm profesionalë, pra i vlerësojnë me 2 në 1 shkallë nga 1 në 3 dhe 2% e tyre i vlerësojnë maksimalisht me 1 duke i cilësuar si shumë profesionalë operatorët e shërbimit ndaj klientit dhe një pjesë shumë e vogël prej 1% do ta rendiste si aspak profesionalë pra me vlerësim në shkallë 3.

-Në vijim pyetja e radhës e cila sërish lidhet me shërbimin ndaj klientit dhe konsiston në dilemën nëse u zgjidh apo jo problemi i ndeshur me internetin i përdoruesit pas telefonatës së drejtuar operatorit të shërbimit. Në këtë rast pjesa dërrmuese prej 91% e konsideron të zgjidhur çdo lloj problemi drejtuar operatorëve të shërbimit ndaj klientit dhe vetëm 9% do ta vlerësonin si të pazgjidhur problemin e deleguar këtyre operatorëve pa marrë zgjidhjen e kërkuar.

-Në pyetjen pasardhëse bëhet një krahasim mes teknikëve të ISP-ve të mëparshme dhe atyre aktuale me ISP-të e të cilëve përdoruesit kanë pasur kontratë shërbimi rezultatet reflektojnë një përqindje prej 74% si të përmirësuar dhe 26% jo të përmirësuar.

-Kështu variabli operatorë shërbimi ndaj klientit evidentohet si faktor pozitiv në rritjen e QoS së internetit në Shqipëri.

-Së fundmi përdoruesit vendosen para pyetjes ku duhet të cilësojnë se kë prej ISP-ve kanë zgjedhur në ambientet e tyre për tu ofruar shërbimin e internetit dhe në këtë rast pjesa dërrmuese prej 42% ka përzgjedhur një tjetër ISP nga ato të listuarat në pyetësor, dhe me pas vjen Abcom që mbizotëron me 21.2%, e pasuar nga Tring që përfshin 13%, Abissnet që përbën 11% të të anketuarve, Vodafone që përbën 9.2% dhe së fundmi Adanet që përfshin 1.5% të përdoruesve.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

-Nëse përballim përgjigjet e filtruara mes dy kategorive minimale e maksimale në shkallë përgjigjeje në lidhje me qëndrimin e tyre ndaj shërbimit të ISP-ve si ofrues interneti shohim që për rastin e përdoruesve të pakënaqur ata janë 11% ku ajo që të bie në sy për perceptimin që ata kanë kundrejt karakteristikave të internetit është që 94% e tyre janë të pakënaqur dhe 6% të kënaqur.

-Nga ana tjetër kur krahasojmë po këto dy kategori në lidhje me perceptimin që kanë në lidhje me karakteristikat kyçe të ISP-ve respektive (besueshmëria, shpejtësia,shkëputjet e sinjalit etj) shohim që raporti i kategorisë shkëlqyer është përgjigjur në shkallën maksimale në 52 % kurse kategoria e pakënaqur është përgjigjur në shkallën minimale në 94%.

-Nëse shohim variablin tjetër që është software-i i instalimit mes dy kategorive vërejmë që për ata shkëlqyer u përgjigjën shkëlqyer në masën 71% ndërsa grupi i pakënaqur u përgjigj i pakënaqur në masën 18%.

-Po ashtu kur krahasojmë rezultatet për dy kategoritë prag minimale e maksimale evidentojmë se në lidhje me operatorët e shërbimit ndaj klientit kategoria shkëlqyer ishte përgjigjur në shkallën sipërore me një vlerë prej 91% kurse kategoria e pakënaqur ishte përgjigjur me aspak të gatshëm në kuotën 8%.

Kategoria e parë e vlerëson maksimalisht profesionalizmin e operatorëve në vlerën 79% kurse kategoria e dytë e vlerëson minimalisht profesionalizmin e tyre në kuotën 4%.

-Kur u pyetën të anketuarit se a u janë zgjidhur problemet teknike pas telefonatave të drejtuara operatorëve të shërbimit kategoria shkëlqyer u përgjigj në shkallën sipërore me një vlerë prej 94% ,sakaq kategoria e dytë u përgjigj negativisht vetëm në 8% .

-Nëse do tu duhej të bënin një krahasim mes teknikëve të mëparshëm nga ISP-te e kontraktuara më parë kategoria shkëlqyer përgjigjet pozitivisht për përmirësim shërbimi në masën 97% ndërsa kategoria e pakënaqur ka pasqyruar një rezultat të përgjigjeve negative prej 52%.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

-Së fundmi në pyetjen përfundimtare ku të anketuarit pyeten në lidhje me kompanitë që kanë përzgjedhur, kategoria e përgjigjur si shkëlqyer ka zgjedhur në vlerën 43% kompaninë Vodafone kurse kategoria e pakënaqur ka zgjedhur në kuotë të barabartë si më pak të votuar Vodafone e Tring me 2%.

-Pra nga ky krahasim nxjerrim që QoS në Shqipëri ka ardhur duke përmirësuar. Faktorët pozitivë që kanë influencuar në një performancë të përparuar kanë qenë padyshim teknologjia e përdorur, shërbimi teknik dhe profesionalizmi gjithnjë e në rritje i tyre, dhe padyshim kompania e përzgjedhur.

-Kurse faktorët që kanë nevojë për përmirësime të mëtejshme për rritjen e QoS së internetit në Shqipëri janë karakteristika sikurse shpejtësia e sinjalit të transmetuar, besueshmëria, shkëputjet e sinjalit etj. faktorë të përngjashëm.

Një investim në këtë pikë do të rriste ndjeshëm QoS e internetit në Shqipëri.

BIBLIOGRAFIA

Artikuj dhe libra

1. T. G. Griffin dhe G. Wilfong, *An analysis of BGP convergence properties*, në *Proc. ACM SIGCOMM*, Shtator 2009.
2. C. Labovitz, A. Ahuja, A. Bose, dhe F. Jahanian. *Delayed Internet routing convergence*. Në *Proc. ACM SIGCOMM*, Gusht/Shtator 2010.
3. C. Labovitz, R. Wattenhofer, S. Venkatachary, dhe A. Ahuja. *The impact of Internet policy and topology on delayed routing convergence*. Në *Proc. IEEE INFOCOM*, Prill 2011
4. F. Wang, Z. M. Mao, J. W. L. Gao, dhe R. Bush. *A Measurement Study on the Impact of Routing Events On End-to-End Internet Path Performance*. Në *SIGCOMM*, 2016.
5. F. Wang, N. Feamster, dhe L. Gao. *Quantifying the Effects of Routing Dynamics on end-to-end Internet Path Failures*. Raport Teknik TR-05-CSE-03, Universiteti i Massachusetts, 2006.
6. Fouad A. Tobagi, Athina P. Markopoulou dhe Mansour J. Karam. *Is the Internet ready for VoIP? In Proceedings of Distributed Computing, Mobile and Wire- less Computing 4th International Workshop (IWDC)*, faqet 49–57. Microsoft Press, 2002.
7. Y. Amir, C. Danilov, S. Goose, D. Hedqvist, dhe A. Terzis. *An Overlay Architecture for High Quality VoIP Streams*. Në *IEEE Transactions on Multimedia*, Djetor 2006.
8. R. K. Rajendran *et al.*, *Performance Optimization of VoIP using an Overlay Network*, Raport Teknik, NEC, 2005.
9. S. Tao *et al.* *Improving VoIP Quality Through Path Switching*. Në *INFOCOM*, 2005.
10. [W. Jiang dhe H. Schulzrinne. *Assessment of VoIP Service Availability in the Current Internet*. Në *PAM*, 2003.
11. I. Marsh dhe F. Li. *Wide Area Measurements of Voice over IP Quality*, Raport Teknik, Swedish Inst of Computer Science, 2003.
12. N. Kushman, S. Kandula, and D. Katabi. *Can you hear me now?! It must be bgp*. Në *SIGCOMM*, 2007.
13. A. Bacioccola, C. Cicconetti, dhe G. Stea, *User-level performance evaluation of VOIP using NS-2*, në *Proc. Int. Conf. Performance evaluation methodologies and tools*, Brukles, Belgjikë, 2007, ICST.
14. T. D. Feng, R. Ballantyne, dhe L. Trajkovi. *Implementation of BGP in a network simulator*. Në *Proc. of Advanced imulation Technologies Conference 2004 (ASTC'04)*, Prill 2004.
15. Y. Rekhter dhe T. Li., *A Border Gateway Protocol 4 (BGP-4)*, Mars 2015. RFC 1771.
16. C. Labovitz,, G. R. Malan, dhe Jahanian, *Internet routing instabilities*, *Proceedings of ACM/SIGCOM 1997*, *Computer communication review*, Vol 27, No 4, Tetor 1997.
17. C. Labovitz, A. Ahuja, A. Bose, dhe F. Jahanian, *Experimental study of Internet stability and Wide Area Backbone Failures*, *Proceedings of INFOCOM'99*, March 1999
18. C. Labovitz, A. Ahuja, R. Wattenhofer, dhe S. Venkatachary, *Resilience characteristics of the Internet backbone routing infrastructure*, në *Third Information Survivability Workshop*, Boston, MA, 2000.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

19. Sally Floyd dhe Van Jacobson., *The synchronization of periodic routing messages*, *IEEE/ACM Transactions on Networking*, 2(2):122-136, 1994.
20. C. Villamizar, R. Chandra, dhe R. Govindan., *BGP route flap damping*, 1998. RFC 2439.
21. John Moy. *OSPF: Anatomy of an Internet Routing Protocol*. Addison- Wesley, 1998.
22. H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson., RFC3550: *RTP: A Transport Protocol for Real-Time Applications*, Internet Engineering Task Force, 2003.
23. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. RFC3261., *SIP: Session Initiation Protocol*, Internet Engineering Task Force, 2002.
24. ITU-T Rec. G.107., *The E-model, a computational model for use in transmission planning*, 2000.
25. D. Katz and D. Ward. Internet Draft. Bidirectional Forwarding Detection. draft-ietf-bfd-base-05.txt.
26. N. Kushman, S. Kandula, and D. Katabi. Can you hear me now?! it must be bgp. In CCR, 2007.
27. N. Kushman, S. Kandula, D. Katabi, and B. Maggs. R-BGP: Staying Connected In a Connected World. Technical Report TR-, MIT, 2007
28. R. Brown. Calendar Queues: A Fast O(1) Priority Queue Implementation for the Simulation Event Set Problem. *Communications of the ACM*, 31(10), October 1988.
29. O. Bonaventure, P. Trimintzios, G. Pavlou, B. Quoitin (Eds.), A. Azcorra, M. Bagnulo, P. Flegkas, A. Garcia-Martinez, P. Georgatsos, L. Georgiadis, C. Jacquenet, L. Swinnen, S. Tandel, and S. Uhlig. *Internet Traffic Engineering*. Chapter of COST263 final report, LNCS 2856, Springer-Verlag, September 2003.
30. R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jarmin. Resource ReserVation Protocol (RSVP). Internet Engineering Task Force, RFC2205, September 1997. [Cah98] R. S. Cahn. *Wide Area Network Design: Concepts and Tools for Optimisation*. Morgan Kaufmann, 1998. [CB96] E. Chen and T. Bates. An Application of the BGP Community Attribute in Multi-home Routing. Internet Engineering Task Force, RFC1998, August 1996.
31. B. Y. Choi and S. Bhattacharyya. Observations on CISCO sampled NetFlow. In *Proceedings of ACM SIGMETRICS Workshop on LargeScale Network Inference (LSNI)*, June 2005.
32. K. Calvert, M. Doar, and E. Zegura. Modeling Internet Topology. *IEEE Transactions on Communications*, pages 160–163, December 1997.
33. H. Chang, R. Govindan, S. Jamin, S. Shenker, and W. Willinger. Towards capturing representative AS-level Internet topologies. *Computer Networks*, 44(6):737–755, April 2004.
34. R.K.C. Chang and M. Lo. Inbound Traffic Engineering for Multihomed ASs Using AS-Path Prepending. *IEEE Network Magazine*, pages 18–25, March/April 2005. 164 BIBLIOGRAPHY
35. J.H. Cowie, D.M. Nicol, and A.T. Ogielski. Modeling the global Internet. *IEEE Computational Science and Engineering*, 1(1):42–50, January/February 1999. Available from <http://www.ssfnet.org>.
36. S. Uhlig C. Pelsser and O. Bonaventure. On the difficulty of establishing interdomain LSPs. In *Proceedings of the IEEE International Workshop on IP Operations and Management (IPOM)*, October 2004.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

37. M. Caesar and J. Rexford. BGP routing policies in ISP networks. *IEEE Network Magazine*, 19(6), November 2005.
38. E. Chen and S. R. Sangli. Avoid BGP Best Path Transition from One External to Another. Internet draft, draft-chen-bgp-avoid-transition- 04.txt, work in progress, December 2005.
39. K. Deb. Multi-Objective Optimization Using Evolutionary Algorithms. John Wiley & Sons, June 2001. [Dik] J. Dike. User-mode linux. Available from [http:// user-mode-linux.sourceforge.net](http://user-mode-linux.sourceforge.net).
40. X. Dimitropoulos, D. Krioukov, and G. Riley. Revisiting Internet AS-level Topology Discovery. In *Proceedings of the 6th Passive and Active Measurement Workshop (PAM)*, 2005.
41. C. de Launois, O. Bonaventure, and M. Lobelle. The NAROS Approach for IPv6 Multi-homing with Traffic Engineering. In *Proceedings of QoFIS, LNCS 2811*, Springer-Verlag, pages 112–121, October 2003.
42. C. de Launois, B. Quoitin, and O. Bonaventure. Leveraging network performance with IPv6 and multiple provider-dependent aggregatable prefixes. *Computer Networks*, 50:1145–1157, June 2006.
43. G. Dommety. Key and Sequence Number Extensions to GRE. Internet Engineering Task Force, RFC2890, September 2000.
44. B. Davie and Y. Rekhter. *MPLS Technology and Applications*. Morgan Kauffmann, 2000.
45. X. A. Dimitropoulos and G. F. Riley. Large-Scale Simulation Models of BGP. In *Proceedings of 12th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS 2004)*, October 2004. BIBLIOGRAPHY 165 [DR06] X. A. Dimitropoulos and G. F. Riley. Large-Scale Simulation Models of BGP. *Computer Networks (Elsevier)*, 50:2013–2027, August 2006.
46. B. Donnet, P. Raoult, T. Friedman, and M. Crovella. Efficient Algorithms for Large-Scale Topology Discovery. In *Proceedings of ACM Sigmetrics*, June 2005.
47. A. E. Eiben and J. E. Smith. *Introduction to Evolutionary Computing*. Springer-Verlag, 2003.
48. N. Feamster and H. Balakrishnan. Detecting BGP Configuration Faults with Static Analysis. In *Proceedings of the 2nd Symposium on Networked Systems Design and Implementation (NSDI)*, May 2005.
49. N. Feamster, J. Borckenhagen, and J. Rexford. Guidelines for interdomain traffic engineering. *ACM SIGCOMM Computer Communications Review*, October 2003.
50. D. Fernandez, T. de Miguel, and F. Galan. Study and Emulation of IPv6 Internet-Exchange-Based Addressing Models. *IEEE Communications Magazine*, 42(1), January 2004.
51. C. Filsfils and J. Evans. Deploying Diffserv in Backbone Networks for Tight SLA Control. *IEEE Internet Computing*, January-February 2004.
52. M. Faloutsos, P. Faloutsos, and C. Faloutsos. On power-law relationships of the Internet topology. In *Proceedings of ACM SIGCOMM 1999*, August 1999.
53. F. Georgatos, F. Gruber, D. Karrenberg, M. Santcroos, A. Susanj, H. Uijterwaal, and R. Wilhelm. Providing Active Measurements as a Regular Service for ISP's. In *Proceedings of the Passive and Active Measurements Workshop (PAM2001)*, Amsterdam, April 2001.

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

54. A. Feldmann, A. Greenberg, C. Lund, N. Reingold, and J. Rexford. NetScope: Traffic Engineering for IP Networks. IEEE Network Magazine, March 2000.
55. D. Farinacci, T. Li, S. Hanks, D. Meyer, and P. Traina. Generic Routing Encapsulation (GRE). Internet Engineering Task Force, RFC2784, March 2000.
56. L. Forst, M. Mares, P. Machek, and O. Filip. BIRD Internet Routing Daemon. <http://bird.network.cz/>, 2005.
57. S. Floyd and V. Paxson. Difficulties in simulating the internet. IEEE/ACM Transactions on Networking, 9(4), November 2001.

58. Faqe interneti

59. [28] <http://www.cl.cam.ac.uk>
60. [29] <http://nslam.isi.edu/nslam/> Aksesuar: 27 Korrik, 2010
61. [26] SSFNet: <http://www.ssfnet.org/homePage.html>. Aksesuar: 27 Korrik, 2010

62. Shtojca 1

```
#
# reconnect.tcl
#

puts ""
puts "Testi i rivendosjes se lidhjes:"
puts ""

set nf [open reconnect.nam w]
set ns [new Simulator]
$ns namtrace-all $nf

$ns node-config -BGP ON
set n0 [$ns node 0:10.0.0.1]
set n1 [$ns node 1:10.0.1.1]
set n2 [$ns node 2:10.0.2.1]
$ns node-config -BGP OFF

$ns duplex-link $n0 $n1 1Mb 1ms DropTail
$ns duplex-link $n0 $n2 1Mb 1ms DropTail

set bgp_agent0 [$n0 get-bgp-agent]
$bgp_agent0 bgp-id 10.0.0.1
$bgp_agent0 neighbor 10.0.1.1 remote-as 1

set bgp_agent1 [$n1 get-bgp-agent]
$bgp_agent1 bgp-id 10.0.1.1
$bgp_agent1 neighbor 10.0.0.1 remote-as 0
$bgp_agent1 neighbor 10.0.0.1 keep-alive-time 200
$bgp_agent0 neighbor 10.0.2.1 remote-as 2

set bgp_agent2 [[$n2 get-module BGP] get-bgp-agent]
$bgp_agent2 bgp-id 10.0.2.1
$bgp_agent2 neighbor 10.0.0.1 remote-as 0

$ns at 0.25 "puts \"\n time: 0.25 \n n0 (ip_addr 10.0.0.1) \
defines a network 10.0.0.0/24.\"\"
$ns at 0.25 "$bgp_agent0 network 10.0.0.0/24"

$ns at 0.35 "puts \"\n time: 0.35 \n n1 (ip_addr 10.0.1.1) \
defines a network 10.0.1.0/24.\"\"
$ns at 0.35 "$bgp_agent1 network 10.0.1.0/24"

$ns at 0.45 "puts \"\n time: 0.45 \n n2 (ip_addr 10.0.2.1) \
defines a network 10.0.2.0/24.\"\"
$ns at 0.45 "$bgp_agent2 network 10.0.2.0/24"

## Network converges at 27.25*.
```

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

```
$ns at 31.0 "puts \"\n time: 31 \  
    \n Shfaq tabelat e rruzimit per cdo agjent BGP: \n\""  
$ns at 31.0 "$bgp_agent0 show-routes"  
$ns at 31.0 "$bgp_agent1 show-routes"  
$ns at 31.0 "$bgp_agent2 show-routes"  
  
## At 90.01, HoldTimer i bgp_agent0 ka skaduar, bgp_agent0 do te  
## 1. shkepuse lidhjen me bgp_agnet1  
## 2. shfuqizojte rruzgen e mesuar nga bgp_agent1  
  
## Connection closing finished at 90.36*.  
$ns at 90.37 "puts \"\n time: 90.37 \  
    \n dump shfaq tabelat e rruzimit per cdo agjent BGP: \n\""  
$ns at 90.37 "$bgp_agent0 show-routes"  
$ns at 90.37 "$bgp_agent1 show-routes"  
$ns at 90.37 "$bgp_agent2 show-routes"  
  
## Network converges at 121.0* again after reconnection.  
$ns at 121.0 "puts \"\n time: 121 \  
    \n shfaq tabelat e rruzimit per cdo agjent BGP: \n\""  
  
$ns at 121.0 "$bgp_agent0 show-routes"  
$ns at 121.0 "$bgp_agent1 show-routes"  
$ns at 121.0 "$bgp_agent2 show-routes"  
  
$ns at 130.0 "finish"  
  
proc finish {} {  
    global ns nf  
    $ns flush-trace  
    close $nf  
    puts "Simulimi mbaroi. Duke ekzekutuar nam..."  
    exec nam reconnect.nam  
    exit 0  
}  
  
puts "Simulimi filloi..."  
$ns run
```

Shtojca 2

```
# <method keyword> <number of graphs> [<initial seed>]
# <# stubs/trans node> <#rand. t-s edges> <#rand. s-s edges>
# <n> <scale> <edgemethod> <alpha> [<beta>] [<gamma>]
# number of nodes =  $1 \times 4 \times (1 + 3 \times 8) = 100$ 
ts 1 47
3 0 0
1 10 3 1.0
4 20 3 0.6
1 10 3 0.4
```

Shtojca 3

```
#
# cbr.tcl
#

#Krijo objektin simulator
set ns_ [new Simulator]

#Hap skedarin nam per ruajtje te dhenash
set nf [open out.nam w]
$ns_ namtrace-all $nf

#Percakto proceduren 'finish'
proc finish {} {
    global ns_ nf
    $ns_ flush-trace
    #Close the trace file
    close $nf
    #Execute nam on the trace file
    exec nam out.nam &
    exit 0
}
set n0 [$ns_ node]
set n1 [$ns_ node]

$ns_ duplex-link $n0 $n1 2000Mb 100ms DropTail

set udp0 [new Agent/UDP]
$ns_ attach-agent $n0 $udp0

set sink [new Agent/LossMonitor]
    $ns_ attach-agent $n1 $sink
$ns_ connect $udp0 $sink

set cbr0 [new Application/Traffic/CBR]
$cbr0 set packetSize_ 160
$cbr0 set interval_ 0.5
$cbr0 set rate_ 64kb
$cbr0 set random_ 1
$cbr0 attach-agent $udp0

set fthrput [open throughput_prove.txt w]
set fpcklost [open packet_loss_prove.txt w]
set fpktrcv [open packet_receive_prove.txt w]
set flstpktt [open last_pkt_time_prove.txt w]
set fexpt [open expected_seq_pkt_prove.txt w]
```

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

```
proc record {} {  
  
    global fthrput fpcklost sink fpktrcv flstpckt fexpt  
    #Krijo nje instance te simulatorit  
    set ns_ [ Simulator instance ]  
    #Percakto hapin  
    set time 0.5  
    #Sa byte janë marre ne pusin e trafikut  
    set bw1 [ $sink set bytes_ ]  
    set lpkts [ $sink set nlost_ ]  
    set pkrvc [ $sink set npkts_ ]  
    set lstpckt [ $sink set lastPktTime_ ]  
    set expt [ $sink set expected_ ]  
    set now [ $ns_ now ]  
    puts $fthrput " $now [ expr $bw1 / $time * 8 ]"  
    puts $fpcklost " $now $lpkts"  
    puts $fpktrcv " $now $pkrvc"  
    puts $flstpckt " $now $lstpckt"  
    puts $fexpt " $now $now $expt"  
  
    $sink set bytes_ 0  
    $sink set nlost_ 0  
    $sink set npkts_ 0  
    $sink set lastPktTime_ 0  
    $sink set expected_ 0  
  
    $ns_ at [ expr $now + $time ] "record"  
}  
  
$ns_ at 0.0 "record"  
$ns_ at 0.5 "$cbr0 start"  
$ns_ at 5.0 "finish"  
$ns_ run
```

Shtojca 4

```
#
# bgp_cbr.tcl
#
#Krijo objektin simulator
    set ns_ [new Simulator]
    global node_

#hapskedarin nam per ruajtje te dhenash
    set nf [open out.nam w]
    $ns_ namtrace-all $nf

    set rng [new RNG]
    $rng seed 0
    set tmp [new RandomVariable/Uniform]
    $tmp set min_ 65250
    $tmp set max_ 65750
    $tmp use-rng $rng
    $rng seed [expr int([$tmp value])]
    set opt(seed) [$rng seed]
    if {$opt(seed) > 0} {
        puts stderr "Duke ushqyer gjeneratorin e numrave rastesore $opt(seed)\n"
        ns-random $opt(seed)
    }

set tracefd [open fhmp4.tr w]
$ns_ use-newtrace
$ns_ trace-all $tracefd
set namtracefd [open fhmp4.nam w]
$ns_ namtrace-all $namtracefd

#Define a 'finish' procedure
proc finish {} {
    global ns_ nf
    $ns_ flush-trace
    #Close the trace file
    close $nf
    #Execute nam on the trace file
    exec nam out.nam &
    exit 0
}

set j 1
    set verbose 1

    if {$verbose} {
        puts "creating nodes..."
    }

    $ns_ node-config -BGP ON
```

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

```
        for {set i 0} {$i < 4} {incr i} {
            set n$i [$ns_ node 0:10.0.$i.1]
        }
    for {set i 4} {$i < 16} {incr i} {

        set n$i [$ns_ node $j:10.$j.$i.1]
            incr j
    }
$ns_ node-config -BGP OFF

# linqet (nga nyja a ne nyjen b):
if {$verbose} {
    puts -nonewline "Creating links 0..."
    flush stdout
}
$ns_ duplex-link $n0 $n7 500Mb 180ms DropTail
$ns_ duplex-link $n0 $n6 500Mb 170ms DropTail
$ns_ duplex-link $n0 $n5 500Mb 160ms DropTail
$ns_ duplex-link $n0 $n4 500Mb 160ms DropTail
$ns_ duplex-link $n0 $n2 500Mb 50ms DropTail
$ns_ duplex-link $n0 $n3 500Mb 60ms DropTail
$ns_ duplex-link $n1 $n11 500Mb 120ms DropTail
$ns_ duplex-link $n1 $n10 500Mb 250ms DropTail
$ns_ duplex-link $n1 $n9 500Mb 190ms DropTail
$ns_ duplex-link $n1 $n8 500Mb 200ms DropTail
if {$verbose} { puts -nonewline "10..."; flush stdout }
$ns_ duplex-link $n1 $n2 500Mb 80ms DropTail
$ns_ duplex-link $n1 $n3 500Mb 70ms DropTail
$ns_ duplex-link $n2 $n14 500Mb 140ms DropTail
$ns_ duplex-link $n2 $n13 500Mb 20ms DropTail
$ns_ duplex-link $n2 $n12 500Mb 160ms DropTail
$ns_ duplex-link $n2 $n3 500Mb 20ms DropTail
$ns_ duplex-link $n3 $n15 500Mb 140ms DropTail

set bgp_agent0 [$n0 get-bgp-agent]
$bgp_agent0 bgp-id 10.0.0.1
$bgp_agent0 neighbor 10.0.2.1 remote-as 0
$bgp_agent0 neighbor 10.0.3.1 remote-as 0
$bgp_agent0 neighbor 10.1.4.1 remote-as 1
$bgp_agent0 neighbor 10.2.5.1 remote-as 2
$bgp_agent0 neighbor 10.3.6.1 remote-as 3
$bgp_agent0 neighbor 10.4.7.1 remote-as 4

#agenti bgp1
set bgp_agent1 [$n1 get-bgp-agent]
$bgp_agent1 bgp-id 10.0.1.1
$bgp_agent1 neighbor 10.0.2.1 remote-as 0
$bgp_agent1 neighbor 10.0.3.1 remote-as 0
$bgp_agent1 neighbor 10.5.8.1 remote-as 5
$bgp_agent1 neighbor 10.6.9.1 remote-as 6
```

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

```
$bgp_agent1 neighbor 10.7.10.1 remote-as 7
$bgp_agent1 neighbor 10.8.11.1 remote-as 8

#agjenti bgp2
set bgp_agent2 [$n2 get-bgp-agent]
$bgp_agent2 bgp-id 10.0.2.1
$bgp_agent2 cluster-id 1000
$bgp_agent2 neighbor 10.0.0.1 route-reflector-client

$bgp_agent2 neighbor 10.0.1.1 route-reflector-client
$bgp_agent2 neighbor 10.0.3.1 remote-as 0
$bgp_agent2 neighbor 10.9.12.1 remote-as 9
$bgp_agent2 neighbor 10.10.13.1 remote-as 10
$bgp_agent2 neighbor 10.11.14.1 remote-as 11

#agjenti bgp3
set bgp_agent3 [$n3 get-bgp-agent]
$bgp_agent3 bgp-id 10.0.3.1
$bgp_agent2 cluster-id 1000
$bgp_agent3 neighbor 10.0.0.1 route-reflector-client
$bgp_agent3 neighbor 10.0.1.1 route-reflector-client
$bgp_agent3 neighbor 10.0.2.1 remote-as 0
$bgp_agent3 neighbor 10.12.15.1 remote-as 12

#agjenti bgp4
set bgp_agent4 [$n4 get-bgp-agent]
$bgp_agent4 bgp-id 10.1.4.1
$bgp_agent4 neighbor 10.0.0.1 remote-as 0

#agjenti bgp5
set bgp_agent5 [$n5 get-bgp-agent]
$bgp_agent5 bgp-id 10.2.5.1
$bgp_agent5 neighbor 10.0.0.1 remote-as 0

#agjenti bgp6
set bgp_agent6 [$n6 get-bgp-agent]
$bgp_agent6 bgp-id 10.3.6.1
$bgp_agent6 neighbor 10.0.0.1 remote-as 0

#agjenti bgp7
set bgp_agent7 [$n7 get-bgp-agent]
$bgp_agent7 bgp-id 10.4.7.1
$bgp_agent7 neighbor 10.0.0.1 remote-as 0

#agjenti bgp8
set bgp_agent8 [$n8 get-bgp-agent]
$bgp_agent8 bgp-id 10.5.8.1
$bgp_agent8 neighbor 10.0.1.1 remote-as 0

#agjenti bgp9
set bgp_agent9 [$n9 get-bgp-agent]
```


Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

```
$bgp_agent9 bgp-id 10.6.9.1
$bgp_agent9 neighbor 10.0.1.1 remote-as 0

#agjenti bgp10
set bgp_agent10 [$n10 get-bgp-agent]
$bgp_agent10 bgp-id 10.7.10.1
$bgp_agent10 neighbor 10.0.1.1 remote-as 0

#agjenti bgp11
set bgp_agent11 [$n11 get-bgp-agent]
$bgp_agent11 bgp-id 10.8.11.1
$bgp_agent11 neighbor 10.0.1.1 remote-as 0

#agjenti bgp12
set bgp_agent12 [$n12 get-bgp-agent]
$bgp_agent12 bgp-id 10.9.12.1
$bgp_agent12 neighbor 10.0.2.1 remote-as 0

#agjenti bgp13
set bgp_agent13 [$n13 get-bgp-agent]
$bgp_agent13 bgp-id 10.10.13.1
$bgp_agent13 neighbor 10.0.2.1 remote-as 0

#agjenti bgp14
set bgp_agent14 [$n14 get-bgp-agent]
$bgp_agent14 bgp-id 10.11.14.1
$bgp_agent14 neighbor 10.0.2.1 remote-as 0

#agjenti bgp15
set bgp_agent15 [$n15 get-bgp-agent]
$bgp_agent15 bgp-id 10.12.15.1
$bgp_agent15 neighbor 10.0.3.1 remote-as 0

$ns_ at 0.4 "$bgp_agent0 network 10.0.0.0/24"
$ns_ at 0.4 "$bgp_agent2 network 10.0.0.0/24"
$ns_ at 0.4 "$bgp_agent3 network 10.0.0.0/24"
$ns_ at 0.4 "$bgp_agent1 network 10.0.0.0/24"
$ns_ at 0.7 "$bgp_agent5 network 10.2.5.0/24"
$ns_ at 0.7 "$bgp_agent4 network 10.1.4.0/24"
$ns_ at 0.7 "$bgp_agent6 network 10.3.6.0/24"
$ns_ at 0.9 "$bgp_agent7 network 10.4.7.0/24"
$ns_ at 0.9 "$bgp_agent8 network 10.5.8.0/24"
$ns_ at 1.2 "$bgp_agent9 network 10.6.9.0/24"
$ns_ at 1.2 "$bgp_agent10 network 10.7.10.0/24"
$ns_ at 1.2 "$bgp_agent11 network 10.8.11.0/24"
$ns_ at 1.5 "$bgp_agent12 network 10.9.12.0/24"
$ns_ at 1.5 "$bgp_agent13 network 10.10.13.0/24"
$ns_ at 1.5 "$bgp_agent14 network 10.11.14.0/24"
$ns_ at 1.5 "$bgp_agent15 network 10.12.15.0/24"

#Krijo agjentin udp dhe lidhe me nyjen n0
```

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

```
set udp0 [new Agent/UDP]
$udp0 set fid_ 2
$ns_ attach-agent $n0 $udp0
$ns_ color 2 Red
#Krijo agjentin LossMonitor (pus trafiku) dhe lidhe me nyjen n1
set sink [new Agent/LossMonitor]
$ns_ attach-agent $n1 $sink

#Lidh burimin me pusin e trafikut
$ns_ connect $udp0 $sink

# Krijo nje burim trafiku CBR dhe ngjitja udp0
set cbr0 [new Application/Traffic/CBR]
$scr0 set packetSize_ 160
$scr0 set interval_ 0.02
$scr0 set rate_ 64kb
$scr0 set random_ 1
$scr0 attach-agent $udp0

$scr0 attach-agent $udp0

set fthrput [open throughput4.txt w]
set fpcklost [open packet_loss4.txt w]
set fpktrcv [open packet_receive4.txt w]
set flstpkt [open last_pkt_time4.txt w]
set fexpt [open expected_seq_pkt4.txt w]

proc record {} {

    global fthrput fpcklost sink fpktrcv flstpkt fexpt
    #Mer nje instance simulatori
    set ns_ [Simulator instance]
    #Vendos hapin
    set time 0.1
    #Sa byte janë marre ne pusin e trafikut
    set bw1 [$sink set bytes_]
    set lpkts [$sink set nlost_]
    set pktrcv [$sink set npkts_]
    set lstpkt [$sink set lastPktTime_]
    set expt [$sink set expected_]
    set now [$ns_ now]
    puts $fthrput "$now [expr $bw1/$time*8]"
    puts $fpcklost "$now $lpkts"
    puts $fpktrcv "$now $pktrcv"
    puts $flstpkt "$now $lstpkt"
    puts $fexpt "$now $now $expt"
    $sink set bytes_ 0
    $sink set nlost_ 0
    $sink set npkts_ 0
    $sink set lastPktTime_ 0
    $sink set expected_ 0
```

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

```
#Re-schedule the record function
$ns_ at [expr $now+$stime] "record"
}

$ns_ at 0.0 "record"
$ns_ at 5.0 "$cbr0 start"
$ns_ at 6.0 "$bgp_agent15 show-routes"
$ns_ at 30.0 "$bgp_agent3 show-routes"
$ns_ at 30.0 "$bgp_agent2 show-routes"
$ns_ at 35.0 "$bgp_agent15 no-network 10.12.15.0/24"
$ns_ at 36.0 "$bgp_agent15 show-routes"
$ns_ at 36.0 "$bgp_agent3 show-routes"
$ns_ at 36.0 "$bgp_agent2 show-routes"
$ns_ at 36.0 "$bgp_agent15 network 10.12.15.0/24"
$ns_ at 55.0 "$bgp_agent15 no-network 10.12.15.0/24"
$ns_ at 62.0 "$bgp_agent3 show-routes"
$ns_ at 62.0 "$bgp_agent2 show-routes"
$ns_ at 70.0 "$bgp_agent15 network 10.12.15.0/24"
$ns_ at 100.0 "$cbr0 stop"

    for {set t 10} {$t < 80} {incr t 10} {
        $ns_ at $t "puts stderr \"kompletohet $t/80 secs...\""
    }
$ns_ at 0.0 "puts stderr \"Fillon Simulimi...\""
set opt(stop) 80
$ns_ at [expr $opt(stop) + 0.0001] "puts stderr \"Simulimi ndalon\""
$ns_ at [expr $opt(stop) + 0.0002] "close $tracefd"
$ns_ at [expr $opt(stop) + 0.0002] "close $namtracefd"
$ns_ at [expr $opt(stop) + 0.0003] "$ns_ halt"

$ns_ run
```

Perspektiva

Një hipotezë e rëndësishme që kemi bërë është topologjia sintetike e nivelit router që është projektuar për të vlerësuar përdorimin e Peerings virtuale për përmirësimin e vonesës. Edhe pse përfundimi se një numër i madh çiftesh AS mund të përfitojnë nga ulje të konsiderueshme të vonesës, rezultatet sasiore e marra nga ky vlerësim mund të ndryshojnë nga ato të marra në internetin e botës reale. Ka pasur dy motive të rëndësishme për hartimin e një topologji ad-hoc. Së pari, na nevojitet një topologji interdomain me vonesa realiste. Në modelin tonë, ne caktojmë vonesën e çdo lidhjeje të bazuar në lidhje kilometrazhi [ZCBD05]. Së dyti, është nevojë për AS-ë të përbërë nga routera të shumta. Struktura e brendshme e një domaini është e rëndësishme pasi ajo kufizon rrugët që protokollet e rrugëzimit intradomain dhe interdomain do të zgjidhnin. Politikat e rrugëzimit Hot-potato dhe interdomain mund të çojnë në shtigjet me një rritje vonese [SPK02]. Sot, ne nuk kemi matjet topologjike mjaft të detajuara të vërtetë të internetit në mënyrë që të ndërtojmë një model të vlefshëm. Asnjë gjenerator topologjike nuk është në gjendje të prodhojë topologji të nivelit router të internetit global në mënyrë të kënaqshme.

Problemi i marrjes së një pamjeje të saktë të topologjisë së internetit nuk është e re si botimet e kohëve të fundit dëshmojnë [MP01, SARK02, SMW02, GR02, MRWK03, CGJ + 04, MH05, SS05, DRFC05, DKR05]. Ne nuk e dimë formën e saktë të Internetit, sidomos në nivelin routeri dhe ka arsye të shumta për këtë. Së pari, ne nuk e dimë në lidhje me strukturën e brendshme të fushave që prej operatorëve të tyre shpesh hezitojnë të publikojnë topologji të rrjetit të tyre. Së dyti, ne nuk e dimë se si domain-et janë të lidhura së bashku. Nuk ka asnjë hartë interneti në dispozicion sot. Duke parë tabelat e rrugëzimit BGP nga një grup i vogël i pikave të monitorimit [SARK02, DKR05] ofrohet një foto bruto e grafikut interdomain.

Megjithatë, nga kjo qasje mungon një numër i madh i lidhjeve peering, kryesisht të tipit të përbashkët me kosto siç tregohet në [CGJ + 04]. Këto lidhje janë të vlefshme për protokollin e rrugëzimit interdomain. Përveç kësaj, grafiku interdomain që kemi sot, tregon se dy domaine janë të lidhura së bashku, por kjo nuk do të japë informacion mbi ku interkoneksioni zhvillohet ose tepicën e linkut. Së fundi, një karakteristikë e rëndësishme e grafikut interdomain janë politikat e rrugëzimit. Në të kundërtën e grafikut intradomain, jo të gjitha shtigjet përmes grafikut interdomain janë të lejuara. Këto rrugë janë të kufizuara nga politikat që zbatohen nga fusha në mënyrë të pavarur [Gao00, SARK02, BPP03]. Ne avokojmë për zhvillimin e një modeli të vërtetuar të strukturës së nivelit router të internetit. Ky model duhet të marrë parasysh aspektet e mëposhtme. Së pari, vendndodhja gjeografike e routerave [Mal02, SPK02, LBCM03] është e rëndësishme meqenëse ajo kufizon dizajnin e topologjisë së rrjetit në çdo domain. Së dyti, mbulimi gjeografik i domainave është një tjetër faktor i rëndësishëm. Në mënyrë tipike, ka fusha rajonale, domaine kombëtare dhe domain që mund të kapërcejnë kontinente të shumta. Së treti, struktura e rrjetit të domaineve, duke përfshirë kapacitetet e lidhjeve, vonesat dhe peshat IGP, kufizon shtigjet që mund të përdoren për të kaluar një domain dhe drejton zgjedhjen e rrugëve të preferuara. Për më tepër, lidhja, vonesat dhe

Studimi i trafikut interdomain bazuar në protokollin BGP, rast studimor në Shqipëri

kapacitetet brenda një domaini janë komponentët e karakteristikave fund-me-fund të rrugëve interdomain [ZCBD05]. Konfigurimi iBGP brenda secilit domain është gjithashtu një aspekt i rëndësishëm. Një rrjetë e plotë e seancave iBGP do të ofrojë një shumëllojshmëri më të mirë të rrugëve se një iBGP hierarkike [CPB04]. Në mënyrë tipike, domaine të mëdha do të mbështeten në një konfiguracion iBGP hierarkik ndërsa domainet e vogjël apo në përmasa të moderuara do të përdorin një rrjetë të plotë. Së katërti, ka rëndësi vendndodhja gjeografikë e lidhjeve peering. Dy domaine zakonisht do të vendosin lidhje peering në vendet ku ata të dy kanë pajisje [SPK02, RS02]. Së pesti, tepricat e lidhjeve interdomain (lidhjet paralele) duhet të modelohen. Në internetin e botës reale, domainet krijojnë lidhje paralele për arsye elasticiteti dhe performance. Së fundi, duhet gjithashtu të modelohen llojet e ndryshme të biznesit të kryera nga domainet, si dhe marrëdhëniet e biznesit midis domaineve. Në të vërtetë, ka lloje të ndryshme të domaineve të tilla si domain tranzit, ofruesit e përmbajtjes, rrjeteve hulumtuese dhe kështu me radhë dhe sjelljet e tyre ndryshojnë.

Përveç kësaj, përdorimi i Peerings Virtual paraqet sfida serioze nga një këndvështrim operacional dhe meriton më shumë vëmendje. Për herë të parë do të ishte një punë më tej për të studiuar se si të bëjmë Peerings Virtual më të sigurt. Virtual Peerings paraqet dy çështje kryesore në lidhje me sigurinë. Në anën e trafikut, shfrytëzimi e një protokollit të tillë si IPSec mund të shërbejë për të kontrolluar identitetin e pjesëmarrësve si dhe për të siguruar privatësinë e të dhënave. Në anën e rrugëzimit, mund të përdoren versionet e siguruara të BGP aktualisht të diskutuara në IETF. Pengesa kryesore për shfrytëzimin e gjerë të të dy IPSec dhe S-BGP / soBGP është nevoja për një infrastrukturë globale çelsash publike (PKI). Për fat të keq, duket të jetë e vështirë për tu vendosur dhe dobët për tu shkallëzuar. Në kontekstin e Peerings virtuale, një alternativë do të ishte që të mbështetet në një vendosje lokale më të besuar nëpërmjet përdorimit të një web të besimit për shembull. Një punë e dytë më tej do të ishte për të studiuar përdorimin e Peerings Virtual në domaine tranzit. Në tezë, ne kufizuam përdorimin e tyre në domainet stub. Në këtë rast ndikimi në rrugëzim është i kufizuar në iBGP e stubeve bashkëpunuese. Së fundi, një punë e cila mund të jetë e mundur më tej do të jetë për të vazhduar përmirësimin e shkallëzueshmërisë së një solver rrugëzimi të propozuar në Kapitullin 2. C-BGP është projektuar për të kryer eksperimentet e paraqitura në këtë tezë në një kohë të arsyeshme dhe me një sasia të burimeve njehsuese të kufizuara. Një zbatim dhe vlerësim i teknikës së propozuar nga Hao dhe Kopol [HK03] në C-BGP do të jetë e vlefshme jo vetëm për përdoruesit C-BGP, por edhe për gjithë komunitetin e modelimit të rrugëzimit BGP. Modeli që pason mesazhin i përdorur në CBGP gjithashtu meriton më shumë vëmendje. Kjo mund të çojë në eksplorimin e rrugëve të shtrenjta që përkeqësojnë kohën e ekzekutimit. Një model caktimi mesazhesh më i zgjuar siguri do të të provojë dobishmëri..