Praćenje navika studenata na Internetu analizom IP saobraćaja upotrebom NetFlow analajzera

Perica Federšpil, Dušan Stefanović, Slavimir Stošović
Savremene računarske tehnologije
Visoka tehnička škola strukovnih studija
Niš, Srbija
elektron@medianis.net
dusan.stefanovic@vtsnis.edu.rs slavimir.stosovic@vtsnis.edu.rs

***Sadržaj* - U ovom radu su prikazani rezultati analize navika studenata prilikom pristupanja Internetu. Praćenje mrežnog saobraćaja vršeno je upotrebom alata *NetFlow Analyzer*. Analizom je praćen protok saobraćaja kroz namenski postavljenu bežičnu mrežu u periodu od 28. januara do 30. juna na Visokoj tehničkoj školi u Nišu. Utvrđeno je koja vrsta mrežnog saobraćaja ima najveću zastupljenost, da li ima zloupotrebe protoka i koliko je opterećenje bežične mreže. Tokom analize Internet stranice Facebook i YouTube su zabranjivane na određeni period.**

Ključne reči - NetFlow; MikroTik; ManageEngine - NetFlow Analyzer;The Dude; Analiza saobraćaja.

I. UVOD

Uz stalni porast broja računara i uređaja koji se priključuju na sve veći broj mreža, rutera i svičeva koji učestvuju u upravljanju tim saobraćajem, postaje jasno da je administratorima mreža potrebna pomoć u praćenju saobraćaja. Protokoli i aplikacije predstavljaju alate koji su projektovani u nameri što bržeg i lakšeg uvida u mrežni saobraćaj. Ovi alati su potrebni ne samo radi otklanjanja problema na mreži u što kraćem roku već i u prevenciji da do problema ne dođe. Ovim alatima se takođe mogu detektovati unutrašnje i spoljašnje pretnje nad mrežom i kvalitetnije vršiti planiranje same mreže

Uglavnom svi uređaji koje želimo da nadgledamo poseduju već ugrađen protokol ili softver kojeg nazivamo agent. Agent prikuplja podatke i šalje aplikaciji za prikupljanje podataka, takozvanom kolektoru. Kada dođe do problema na mreži, agenti bi trebalo da detektuju grešku, izoluju i po mogućstvu otklone kvar. Uobičajeno je da agenti i kolektori u roku od par minuta upozore administratora da otkloni problem. Kada je mreža stabilna zadatak administratora je da nadgleda moguće napade kako sa spoljašnje tako i sa unutrašnje strane mreže. Takođe pomoću ovih alata administrator treba da vrši konstantno nadgledanje parametara mreže i uređaja na mreži kako ne bi došlo do preopterećenja u određenim delovima. Kada dođe do preopterećenja mreže prikupljeni podaci se mogu koristiti za planove proširenja mreže i nabavku uređaja sa većim protokom [1].

Primenom odgovarajućih alata utvrđuje se koja je vrsta saobraćaja najviše zastupljena, da li postoje zloupotrebe protoka i koliko je opterećenje bežične mreže. Cilj ove analize je praćenje ponašanja i navika studenata prilikom pristupanja Internetu. Praćene su lokacije koje se najviše posećuju i promene navika ukoliko neka od stranica nije dostupna. Radi preciznije analize podataka nije vršena analiza dolaznih podataka ka telefonima studenata, već samo zahtevi za podacima i informacije koje su studenti slali ka Internetu.

II. CILJ ANALIZE MREŽNOG SAOBRAĆAJA

Analizom saobraćaja dolazi se do sledećih podataka [2] :

- Zauzetost mreže.
- Razumevanje potreba korisnika.
- Merenje procenta ostvarenih potreba korisnika.
- Merenje promena u saobraćaju radi poboljšanja *QoS* (eng. Quality of Service) zasnovanog na iskustvu korisnika.
- Merenje efikasnosti promena na mreži.
- Efektivno merenje mrežnog protoka radi provere zahteva za protokom i stvarne iskorišćenosti mrežnog protoka.

Aplikacije za analizu saobraćaja nam pomažu u:

- Detekciji i otklanjanju zagušenja.
- Identifikaciji i prevazilaženju problema u performansama mreže.
- Identifikaciji bezbedonosnih propusta.
- Planiranju rasta potreba i pojave novih servisa.
- Naplaćivanju korišćenja protoka.

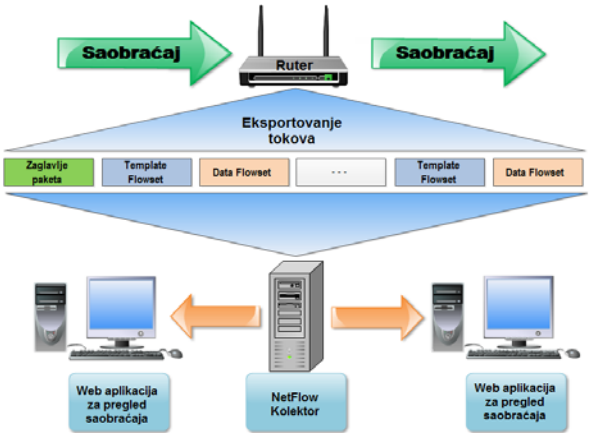
III. KORIŠĆENA OPREMA I PROTOKOLI

U ovom radu je za analizu korišćena *MikroTik Routerboard RB411* ploča. *MiktorTik RouterOS* ima u sebi implementiran *TraficFlow* protokol koji je kompatibilan u potpunosti sa *Cisco-NetFlow* protokolom.

NetFlow predstavlja mrežni protokol razvijen od strane *Cisco Systems*-a za potrebe prikupljanja informacija o *IP* (eng.

Internet Protocol) saobraćaju i nadgledanja mrežnog saobraćaja. Iako je naziv *NetFlow* postao svakako standard kada se misli na praćenje mrežnog saobraćaja, mnogi drugi proizvođači hardvera imaju implementiranu svoju verziju ovog protokola kao na primer: *Juniper (Jflow), 3Com/HP, Dell i Netgear (sflow), Huawei (NetStream), Alcatel-Lucent (Cflow), Ericson (Rflow) i MikroTik (TrafficFlow)*.

Ruteri i svičevi koji podržavaju *NetFlow* protokol, prikupljaju statistiku o *IP* saobraćaju na svim portovima na kojima je *NetFlow* protokol omogućen. Ovi podaci kreiraju tokove (eng. *flow*) koji se eksportuju ka najmanje jednom *NetFlow* kolektoru koji skladišti, vrši analizu i prikaz prikupljnih podataka (Sl. 1) [3].



Slika 1. Prikupljanje informacija o saobraćaju softverskim kolektorima.

IV. SOFTVER KORIŠĆEN ZA ANALIZU PODATAKA

Softverski alati koji su korišćeni za prikupljanje i anlizu podataka o mrežnom protoku su: *ManageEngine – NetFlow Analyzer, Mikrotik – The Dude* i *Zabbix* [4][5]. Akcenat je stavljen na program *NetFlow Analyzer* iz koga su vršene gotovo sve analize.

NetFlow Analyzer proizvod je kompanije *Zoho Corporation Pvt. Ltd* i predstavlja Web zasnovani alat za analizu propusnog opsega i analizu saobraćaja koji koristi *Cisco NetFlow, sFlow, cflowd, jFlow, IPFIX, NetStream i Cisco NBAR* protokol. *NetFlow Analyzer* daje odgovore *IT* administratorima na pitanje ko, šta, kada, gde i kako koristi propusni opseg mreže [6].

NetFlow Analyzer prikuplja i analizira sledeće informacije iz *NetFlow* paketa :

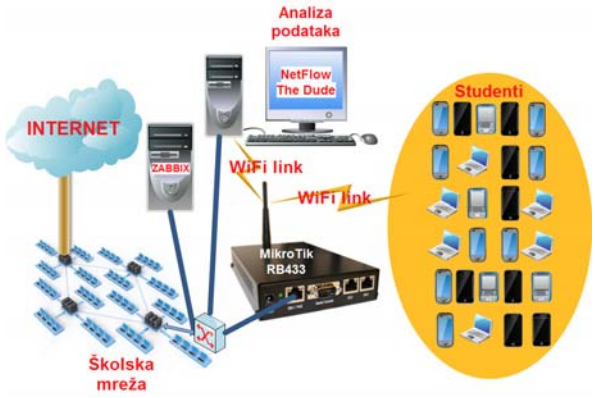
- Izvorišne i odredišne *IP* adrese
- Broj ulaznog i izlaznog interfejsa
- Broj izvorišnog i odredišnog porta
- Layer 4 protokol
- Broj paketa u toku
- Ukupan broj bajtova u toku
- Vremenski markeri u toku
- Izvorišni i odredišni *AS* (autonomni sistem)
- *TCP_Flag & TOS (eng. Type Of Service)*

V. ANALIZA PRIKUPLJENIH PODATAKA

Period praćenja saobraćaja i analize vršen je nad telefonima studenata koji su koristili namenski postavljenu bežičnu mrežu u periodu od 28. januara do 30. juna u visokoj tehničkoj školi u Nišu [7]. U ovom periodu vršene su promene i ograničenja na mreži čije datume je potrebno znati radi jednostavnijeg praćenja rezultata analize:

- 06. mart – DHCP = postavljen na 30 min
- 25. mart – Facebook = ukinut
- 16. april – YouTube = ukinut ; Facebook = omogućen
- 26. jun – YouTube = omogućen

Na Sl. 2 prikazan je šematski prikaz mrežne infrastrukture koja predstavlja školsku mrežu sa leve, i mobilne uređaje studenata sa desne strane, koji se putem bežične mreže povezuju na Internet. Između ove dve mreže nalazi se *MikroTik*-ov ruter RB433 koji razdvaja i onemogućava komunikaciju između školske i studentske bežične mreže. Bežična mreža je postavljena bez lozinke tako da je svako mogao da se poveže i koristi je. Uglavnom su se povezivanja vršila mobilnim telefonima i po neki slučaj prenosivog računara ali je njihov broj bio zanemarljiv. Takođe na Sl. 2 vide se i dva istaknuta računara, prvi (*Analiza podataka*) koji je korišćen za pokretanje *ManageEngine NetFlow Analyzer*-a, *MikroTik*-ovog *The Dude* programa kao i za pristup *Zabbix* interfejsu. Drugi računar je namenjen podizanju virtualne mašine sa *Zabbix* serverom.



Slika 2. Šematski prikaz mreže na kojoj je vršena analiza podataka.

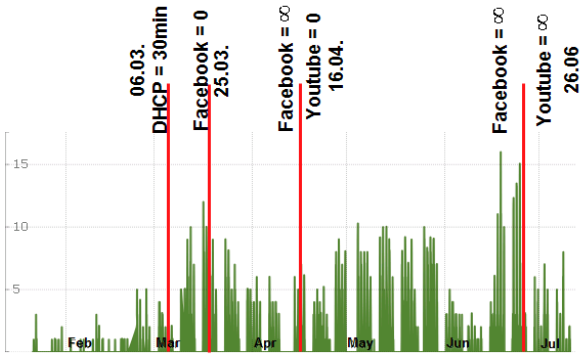
Studentskoj mreži je *MikroTik* dodeljivao adrese putem *DHCP-a* iz opsega od broja 100 do broja 200. Pri tom nikada nisu bile zauzete sve adrese istovremeno, maksimalno je na mreži bilo 73 uređaja.

Grafikon na Sl. 3 predstavlja poslatu količinu podataka prema Internetu prikazano po mesecima.

Na grafiku se vidi pad protoka od marta do aprila što se poklapa sa periodom ukidanja *Facebook-a*, ali se ne vidi dobro period pre i posle smanjenja vremena za izdavanje *IP* adresa na 30 min.

Na Sl. 4 detaljnije se vide promene protoka i ujedno su naznačeni dani kada su se dešavale promene u podešavanjima, grafik je preuzet iz programa *NetFlow Analyzer*.

Slika 3. Promena protoka podataka ka Internetu po mesecima.

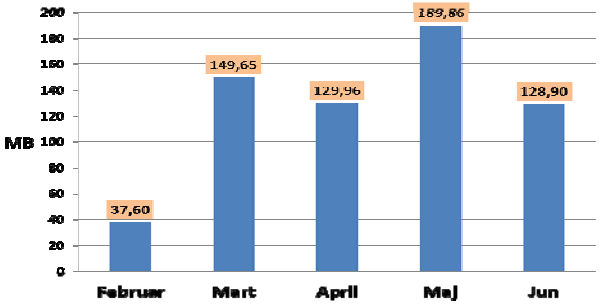


Slika 4. Protok podataka za ceo period analiziranja.

Na Sl. 4 se može videti da je protok od 06. marta uvećan gotovo dvostruko, kao i da je naglo opadao u periodu kada je *Facebook* bio ukinut 25. marta - 16. aprila. Sa ponovnim omogućavanjem pristupa *Facebook*-u 16. aprila protok se povećava i vraća na vrednosti pre 25. marta. Samo ukidanje *YouTube* stranice 16. aprila nije značajno uticalo na protok podataka kao ukidanje *Facebook*-a jer su u tom periodu studenti više koristili stranice na *Amazon AWS*-u i *Google*-ove stranice tako da nije zabeležen pad protoka u maju mesecu.

Grafik na Sl. 5 prikazuje prosečnu količinu podataka prenesenu u toku dana od strane korisnika ka Internetu, za ceo period analize podeljenu po mesecima.

Kada se prikaže tok promene količine podataka po danima u nedelji za kompletan period analize, dobija se grafik na Sl. 6. Za broj nedelje je uzeto svakih nedelju dana od početka analize i unošeni su podaci za svaki dan pojedinačno. Na ovaj način može se uočiti koji se dan u nedelji najviše ističe, kao i preciznu promenu za svaki dan tokom perioda analize. Postoje određene tačke kada je došlo do naglih oscilacija u protoku na koje će se više obratiti pažnja. Takođe su na grafiku obeleženi periodi kada su vršene promene u pristupu *Facebook* i *YouTube* stranicama kako bi se mogla videti promena u zavisnosti od tih parametara. Oko 6. nedelje počinje rast protoka što se poklapa sa periodom od 23. februara kada i počinju predavanja u letnjem semestru. Kao što je i ranije zaključeno od dana kada je vreme *DHCP* servera za izdavanje *IP* adresa smanjeno na 30 min vidi se osetno povećanje protoka.



Slika 5. Prosečna dnevna vrednost protoka podataka ka Internetu po mesecima.

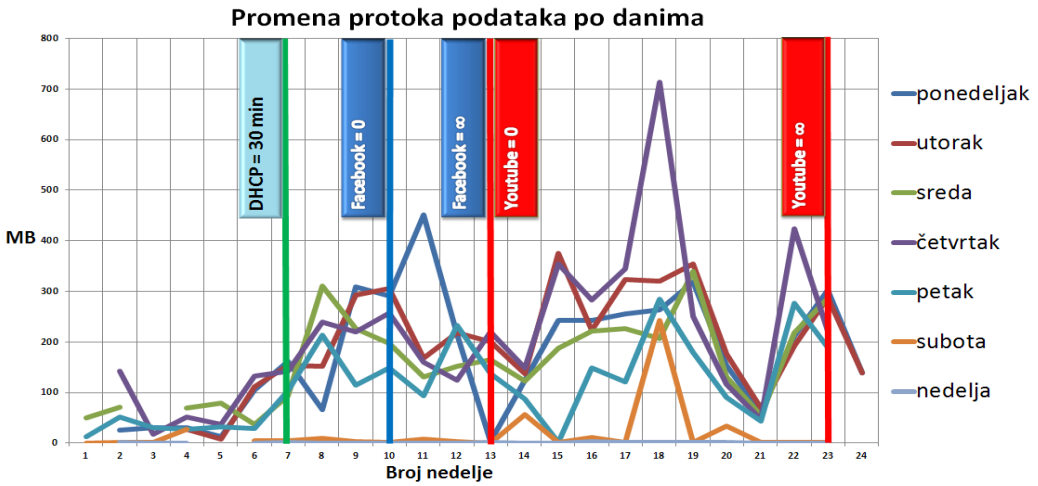
Rast protoka se nastavlja sve do 10. nedelje kada je ukinut pristup *Facebook* stranici, od tog datuma protok konstantno opada osim u ponedeljak 30. marta kada se javlja povećan protok. Kako je *YouTube* dostupan u ovom periodu, očekivalo se da će studenti u ovom periodu više koristiti ovaj sajt umesto *Facebook*-a. Međutim na prvom mestu po protoku ističe se *Amazon AWS Cloud* servis koji hostuje mnoge poznate Internet stranice. Razmena ove količine podataka sa *Amazon AWS Cloud* servisom ostaje i nakon omogućavanja pristupa *Facebook* stranici. Sledeća bitna tačka na grafiku je 13. nedelja u kojoj se 16. aprila omogućava pristup *Facebook*-u a zabranjuje *YouTube* stranica. Od ove linije počinje rast protoka i pored zabranjenog pristupa *YouTube-u* umesto koga studenti sada pristupaju *Amazon AWS-u*. Takođe u 13. nedelji beleži se nagli pad protoka u ponedeljak 13. aprila kada je bio Uskrs i neradan dan.

Interesantan momenat na grafiku je u 14. nedelji kada su skoro svi dani imali isti protok i nešto smanjen nego uobičajeno a subota nešto povećan protok. Ovo je period od 20-25. aprila kada se održavaju kolokvijumi u školi i tada studentima očigledno nije bio previše interesantan Internet, što je pohvalno, sa tim da je nešto povećan u Subotu kada je takođe bilo studenata u školi.

U 15. nedelji javlja se rast u svim danima osim u petak kada je protok pao na nulu što je i razumljivo obzirom da je to bio 1. maj, takođe neradan dan.

U 18. nedelji javlja se nagli skok protoka podataka u četvrtak 21. maja, kada je ostvaren najveći protok za posmatrani period analize. Samo jedan uređaj je ostvario najveći saobraćaj posećivanjem stranica *ber01s14-in-f10.1e100.net* i *Google*. O stranici *ber01s14-in-f10.1e100.net* (*IP* adresa 216.58.213.10) ne postoje informacije na Internetu osim da je u vlasništvu *Google*-a i da služi za praćenje, keširanje i zaštitu korisnika od malicioznih stranica. Usko je vezana za *Chrome* i za *Google*-ov pretraživač i ne može se izbeći ni blokirati, to su iskustva korisnika sa foruma. Takođe se došlo do zaključka da su sve stranice sa *1E100.net* na kraju adrese namenjene prikupljanu podataka o korisniku od strane *Google*-a. Drugi deo saobraćaja koji je u programu označen kao *Google*, predstavlja *IP* adresu 216.58.211.10 koja vodi do adrese *muc03s13-in-f10.1e100.net* što je još jedna od lokacija za keširanje navika i informacija o korisniku. Ove informacije samo potvrđuju da nema privatnosti na Internetu.

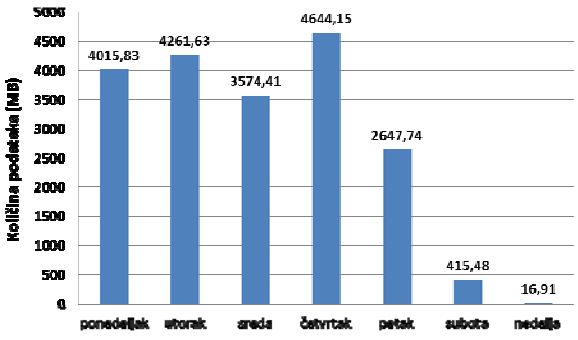
Sledi nagli pad protoka u toku 21. nedelje od 08-12. juna kada se po kalendaru škole završilo predavanje i sledi ispitni rok.



Slika 6. Tok promene količine poslatih podataka za svaki dan u nedelji tokom celokupnog perioda analize.

U 22. nedelji javlja se ponovni porast protoka ali u popodnevnim satima u četvrtak između 16h i 17h. U ovom periodu sa 75% ostvarenog protoka ističe se jedan korisnik. Posećivan je veliki broj stranica koje su gotovo ravnomerno raspoređene u prvih 100 naj posećenijih lokacija, što ukazuje na korišćenje torenta. U kratkom vremenskom periodu je ostvaren je saobraćaj sa 18 (osamnaest) država sveta i ka ovim lokacjama je ostvaren odlazni saobraćaj od 250MB podataka.

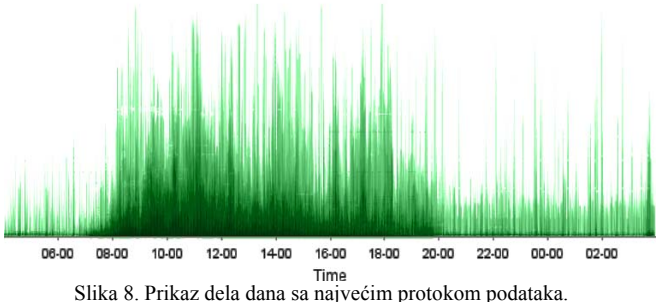
Kada se sabere protok po danima za ceo period dobija se grafik na Sl. 7. Grafik pokazuje da je dan sa ostvarenim najvećim protokom četvrtak, čak i kada se zanemari 21. maj kada je ostvaren veliki skok u protoku, i dalje je četvrtak jedan od dana sa najvećim protokom zajedno sa utorkom koji je odmah sledeći po protoku. Svi ostali podaci su očekivani, subota i nedelja su zanemarljivi obzirom da tada škola ne radi a petak je dan pred vikend kada kod svih dolazi do pada akivnosti pa i kod studenata.



Slika 7. Ukupan protok ostvaren po danima od 28. januara do 30. juna.

Sl. 8 je formirana preklapanjem svih grafikona dnevnog protoka podataka u periodu analize podataka. Za dobijanje perioda najvećeg protoka u toku dana uzete su 83 slike dnevnog izveštaja iz programa NetFlow *Analyzer*-a, obrađene su i postavljena je transparentnost slika na 10%. Zatim su slagane slike jedna na drugu kako bi se stalnim dodavanjem slojeva umanjila transparentnost i pojavile se tamne površine sa naj opterećenijim delovima dana. Iz dobijene slike vidi se da je zauzetost mreže najveća od 08h do 15h. Da je najveći protok od 09h do 12h i da se javlja dosta veliki protok oko 16,17 i 18h kada su i popodnevna predavanja na specijalističkim studijama.

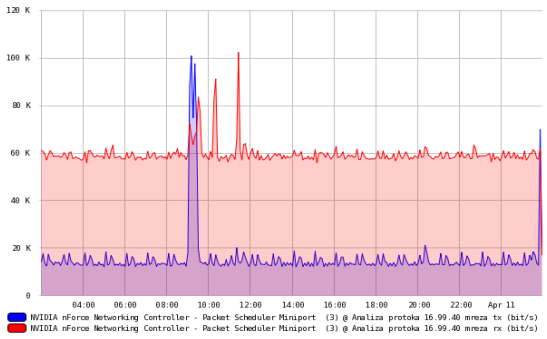
U periodu od 22h do 08h deluje kao da postoji značajan saobraćaj iako je on dobijen protokom informacija generisanih SNMP i Netflow protokolima u subotu i nedelju kada je samo ovaj saobraćaj prisutan pa je program aktivno menjao skalu i prikazivao ovaj saobraćaj kao značajan. Protok ostvaren ovim protokolima tokom radnih dana prikazan je kao tamna zelena linija pri dnu grafika.



Slika 8. Prikaz dela dana sa najvećim protokom podataka.

Analiziranjem 10. aprila, što je petak pred uskrs, neradan dan, mogu se dobiti interesantni grafici koji pokazuju protok saobraćaja prouzrokovanog *SNMP* i *NetFlow* protokolima prema računaru *Analiza podataka*. Na Sl. 9 prikazan je grafik protoka podataka od računara *Analiza podataka* prema *MikroTik*-u odakle se prikupljaju *SNMP* i *NetFlow* podaci za programe *NetFlow Analyzer* i *Dude*.

Osim u periodu oko 09:25 kada je pristupano radi prikupljanja podataka, protok koji se odvijao je konstantan u toku celog dana i kretao se oko 60Kbps za prijem podataka i oko 18Kbps za slanje podataka ka *MikroTik*-u. Protok uzrokovan protokolima bez prisustva saobraćaja uzrokovanog od strane korisnika, može se uporediti sa ostvarenim protokom protokola na dan 16. aprila kada je protok saobraćaja od strane korisnika bio 200 MB što je nešto više od najvećeg prosečnog protoka po mesecima.



Slika 9. Protok podataka *SNMP* i *NetFlow* protokola između *MikroTik*-a i računara za analizu podataka u danu bez saobraćaja

Iz ova dva primera može se zaključiti da se opterećenje mreže izazvano *SNMP* i *NetFlow* protokolima minimalno menja sa povećanjem protoka podataka kroz mrežu uzrokovanog od strane korisnika. Količina saobraćaja koju ostvaruju ovi protokoli zanemarljiva je u odnosu na saobraćaj korisnika, pogotovu ukoliko se ima u vidu da se na ovom računaru izvršavaju dva programa *Dude* i *NetFlow Analyzer*.

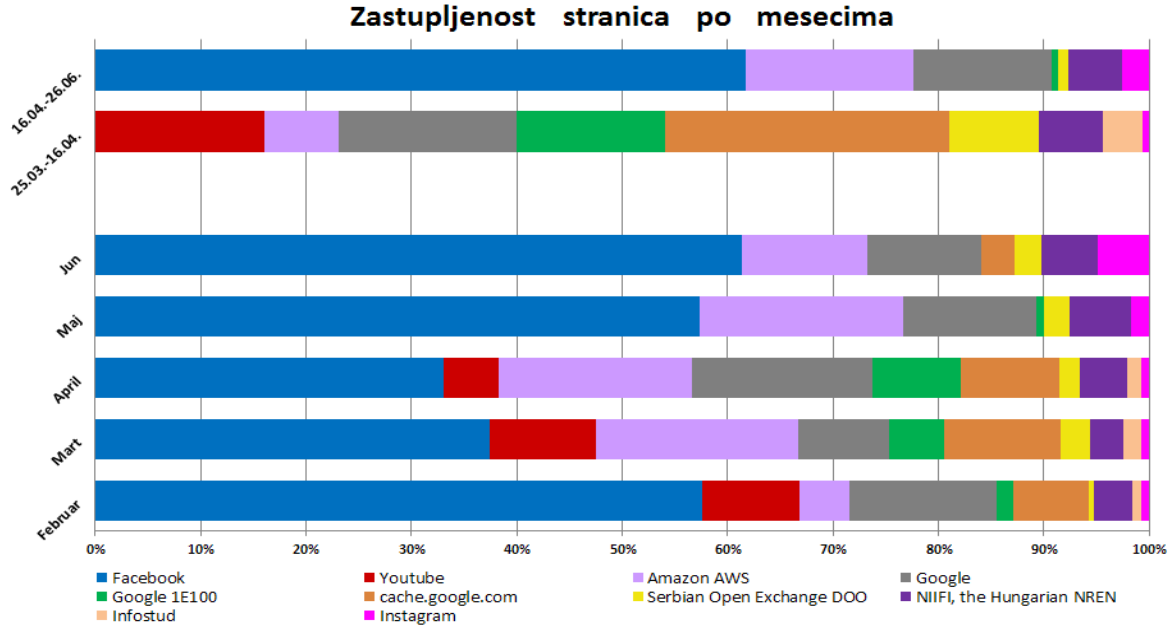
Nakon analize prenešene količine podataka, mogu se analizirati lokacije na Internetu koje su bile najposećenije u posmatranom periodu. Na Sl. 10 vidi se raspodela posećenosti stranica za svaki mesec pojedinačno kao i za period kada su bile zabranjene stranice *Facebook* i *YouTube*. Ovaj grafikon je formiran iz dnevnih izveštaja programa *NetFlow Analyzer* koji između ostalog sadrže protok podataka prvih 100 stranica koje su najviše zastupljene u ukupnom protoku tog dana. Sa grafikona je uočljivo da najveći procenat zauzima *Facebook* u svim mesecima od februara do juna meseca. Ovaj podatak deluje zbunjujuće kada se uzme u obzir da je *Facebook* bio isključivan u određenim periodima. Međutim, prikazan je period celih meseci tako da je u svakom mesecu *Facebook* bio omogućen određeni broj dana. Ako se pogledaju meseci mart i april vidi se da je smanjen udeo *Facebook* stranice i to su upravo meseci kada je ova stranica bila u određenim danima isključena. U maju i junu mesecu vidi se ponovni povratak *Facebook* stranice na procenat zastupljenosti iz februara meseca, dok stranice *YouTube* nema na grafiku pošto je ona u ovim mesecima zabranjena. Preciznija zastupljenost stranica u periodima zabranjivanja *Facebook* i *YouTube* stranica data je u vrhu grafika.

U periodu od 25. marta – 16. aprila kada je bio zabranjen *Facebook* najaktivnija stranica je *YouTube* ali ne toliko da bi zamenila *Facebook*, zastupljene su gotovo identično *Google* i *Amazon AWS* stranice. Takođe veliki procenat zauzima *cache.google.com* koji predstavlja keš stranice za preuzimanje *YouTube* video sadržaja. Protok ka stranici *Google 1E100*, koja predstavlja Google servere koji se aktiviraju kad god ima nekog *YouTube* sadržaja na stranici koja se posećuje, takođe je porastao u ovom periodu. Stranice sa delom *1E100* na kraju adrese pojavljuju se kada se koristi *Google Earth* i *Google Update* kao i kod mnogo drugih stranica u koje je uključen *Google* [8]. Dokazano je u praksi da se ove stranice ne mogu zaobići ukoliko se želi pristup Internetu. Važno je napomenuti da je opao ukupan protok podataka u ovom periodu što se može videti iz ranije prikazanih grafikona.

U periodu od 16. aprila – 26. juna. onemogućen je pristup stranici *YouTube*, stranica *Facebook* je omogućena i vraća se procentualno na period iz februara meseca. Ukupna količina podataka se povećava u ovom periodu i dostiže vrednost pre ukidanja *Facebook*-a. Uvećava se prisutnost stranica koje su hostovane na *Amazon AWS*-u. Treba primetiti da je u ovom periodu izostala prisutnost stranice *cache.google.com* koja je uvek vezana za *YouTube* stranicu odakle se i preuzima video sadržaj. Analiza pokazuje da je studentima najinteresantniji *Facebook* i pored mogućnosti korišćenja *YouTube*-a i svega ostalog na Internetu, da se vremenom sve više koristio *Instagram* kao i da se domaće stranice veoma malo koriste.

VI. ZAKLJUČAK

Analizom prikupljenih podatka došlo se do podatka da je mesec sa najvećim protokom za ovaj period analize, maj sa 5,73GB prenesenih podataka ka Internetu. Protok podataka od Interneta ka studentima je u proseku oko 10 puta veći od odlaznog saobraćaja. Prosečna dnevna vrednost prenesenih podataka tokom ovog perioda se kretala od 150 do 190 MB. Period dana sa najvećim obimom saobraćaja je od 08h do 15h što je i očekivan rezultat obzirom da je tada najveći broj studenata u školi. Uticaj saobraćaja koji prouzrokuju protokoli *SNMP* i *NetFlow* su zanemarljivi, kreću se od 18Kbps do 64Kbps kada nema studenata na mreži i od 25Kbps do 75Kbps prilikom svakodnevnog korišćenja mreže. Posmatranjem stranica koje su najviše posećivane, na prvom



Slika 10. Odnos zastupljenosti stranica u ukupnom protoku podataka.

mestu nalazi se *Facebook* pa zatim slede *Youtube, Amazon AWS, Google,...* što ukazuje na raznovrsno interesovanje samih studenata. Podaci takođe pokazuju da su korisnici privrženi pojedinim sajtovima što je u ovom slučaju *Facebook*. Ukidanjem pristupa došlo je do pada protoka, što govori da studenti nisu našli ništa interesantnije da nadomeste nemogućnost pristupa ovoj stranici.

Pored uvida u pojedine stranice koje je *NetFlow Analyzer* mogao da dešifruje u kombinaciji sa *MikroTik* ruterom, postoji veliki broj sajtova koji nisu otkriveni ili se skrivaju iza servisa kao što je *Amazon AWS*. Takođe veliki problem za kontrolu saobraćaja predstavlja i nemogućnost određivanja portova i protokola koji se koriste za komunikaciju. Nepostojanje ovih podataka otežava kontrolu protoka zabranom protoka po portovima i protokolima. Osobina javnih bežičnih mreža je nemogućnost postavljanja fiksnih *IP* adresa za svakog korisnika, to predstavlja prepreku za određivanje konkretnog korisnika koji koristi nedozvoljene sajtove ili protokom opterećuje mrežu. Kontrola je teško izvodljiva na javnim mestima gde se korisnici stalno smenjuju pa je zato veoma bitno imati što detaljniji prikaz stranica koje se posećuju kao i portova i protokola koji se koriste. Postoji mogućnost da se na *MikroTik*-u postavi ograničenje za pojedine stranice ali samo ukoliko se zna njihov *DNS* naziv i šta te stranice predstavljaju sobzirom da postoji veliki broj sajtova koji se skrivaju iza naziva jednog servisa u oblaku. Još jedan problem je korišćenje istog porta, na primer port 443 se koristi za mnoge stranice i namene, tako da se ne može jednostavno onemogućiti port. Da bi se uskratio pristup torentima na *MikroTik*-u potrebno je postaviti niz pravila koja nikada nisu 100% sigurna i retko mogu zabraniti kompletan saobraćaj, iz razloga što se pristup torentima stalno modifikuje i pronalazi način da se prevaziđu prepreke. Jedan od načina prevazilaženja ove situacije je da se dozvole torenti ali da se pravilno raspodeljuje protok na sve korisnike.

Ovom analizom je pokazano da *NetFlow Analyzer* u kombinaciji sa MikroTik-om i pored jednostavnosti korišćenja i davanja informacija o pojedinim aspektima rada mreže, ne pruža dovoljan nivo detalja saobraćaja koji je potreban za uspešnu kontrolu i nadgledanje jedne mreže.

Program *NetFlow Analyzer* ima mogućnost rada sa *Cisco AVC (eng. Application Visibility and Control)* tehnologijom koja vrši analizu samog paketa a ne samo zaglavlja paketa. Ovime se postiže značajno bolja analiza i prepoznavanje stranica koje se posećuju od strane korisnika, pa samim tim i njihova kontrola. Podaci koje Cisco generiše prenose se takođe putem *NetFlow* protokola, tako da svi programi za analizu saobraćaja mogu uvrstiti ovu tehnologiju u svoje proizvode.

LITERATURA

[1] Chakchai So-In – "A Survey of Network Traffic Monitoring and Analysis Tools", http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_traffic_monitors3.pdf (12.02.2015)

[2] Sonia Panchen – "Network traffic monitoring and management" - 11th November,2010 http://www.inf.ed.ac.uk/teaching/courses/cn/Traffic Monitoring.pdf (10.02.2015)

[3] Brad Hale – "Geek`s Guide to the NetFlow v9 Datagram", Whitepaper 2012 http://Web .swcdn.net/creative/pdf/Whitepapers/*NetFlow*_Datagram_-_Final.pdf (12.02.2015)

[4] https://www.Zabbix .com/documentation/2.4/manual (03.12.2015)

[5] http://wiki.MikroTik.com/wiki/Manual:The_Dude (05.12.2015)

[6] Charles M. Kozierok - *THE TCP/IP GUIDE*, No Starch Press, Inc. 2005 San Francisco, ISBN-13: 978-1-59327-047-6

[7] Perica Federšpil – "Softverski alati za nadgledanje saobraćaja i propusnog opsega na aktivnim mrežnim uređajima" – Specijalistički rad, Visoka tehnička škola strukovnih studija – Niš, Oktobar 2015

[8] https://en.wikipedia.org/wiki/MarkMonitor (07.12.2015)

ABSTRACT

This paper presents the results of students habits analysis when accessing the Internet. Monitoring network traffic was carried out using tools NetFlow Analyzer. The analysis is accompanied by the flow of traffic through a dedicated set the wireless network in the period from 28 January to 30 June at the College of Applied Technical Sciences in Niš. It is determined which type of network traffic has a major presence, whether there is abuse of flow and determine the load of wireless network. During the analysis, Internet sites Facebook and YouTube were banned for a certain period.

MONITORING HABITS OF STUDENTS ON THE INTERNET BY ANALYZING IP TRAFFIC USING NETFLOW ANALYZER

Perica Federšpil, Dušan Stefanović, Slavimir Stošović