Analiza tokova mrežnog saobraćaja na mreži Elektrotehničkog fakulteta u Beogradu

Petar Vasić, mentor: Mr Nenad Krajnović

***Sadržaj* — U ovom radu objašnjeni su sistemi za analiziranje tokova mrežnog saobraćaja. Prikazana je dosadašnja implementacija sistema, zasnovanog na *pmacct* programu, koja se koristi na mreži Elektrotehničkog fakulteta i prezentovani su rezultati merenja.**

***Ključne reči* — analiza saobraćaja, nadzor mreže, netflow, pmacct, optimizacija mreže.**

I. Uvod

Merenje i analiza saobraćaja su od ključnog značaja u današnjim kompleksnim IP mrežama. Tradicionalno, mrežni administratori se oslanjaju na *Simple Network Management Protocol* (SNMP) za merenje protoka. Međutim, iako SNMP omogućava planiranje kapaciteta, on nema mnogo mogućnosti za dublju analizu mrežnog saobraćaja. Protok paketa i bitova na interfejsima je koristan podatak, ali granularnije statistike poput poznavanja IP adresa i aplikacija koje generišu saobraćaj može da pruži bolji uvid u način korišćenja i eventualne zloupotrebe mreže, kao i da doprinese finansijskim uštedama (biranjem boljih interkonekcija) i efikasnijem rutiranju saobraćaja. [1]

Cilj ovog rada je da, uz korišćenje već postojećih i proverenih tehnika i rešenja za prikupljanje i filtriranje statistika o mrežnom protoku, i pisanjem novog interfejsa za pregled i vizuelizaciju prikupljenih podataka, pruži administratorima akademske mreže na Elektrotehničkom fakultetu bolji uvid u funkcionisanje mreže.

II. Tehnologije, standardi i alati

Velike savremene mreže u kratkom periodu generišu ogromnu količinu saobraćaja koju treba analizirati. Da bi se to pojednostavilo pakete grupišemo u tokove.

Tok ili „*flow*“ čini određeni skup IP paketa koji za vreme nekog intervala prođe kroz tačku posmatranja u mreži. Svi paketi jednog toka imaju set zajedničkih osobina po kojima su grupisani. Te osobine mogu biti: izvorišna i odredišna IP adresa, izvorišni i odredišni port, protokol, klasa servisa, ... [2]

Trenutno najpoznatije i najrasprostranjenije rešenje za analiziranje IP tokova je Cisco-v NetFlow.

A. Netflow

Netflow je tehnologija koju je razvio Cisco za potrebe svog QoS (*Quality of Service*) programa.

Netflow protokol definiše format paketa za prenošenje statistika o saobraćaju. Trenutno je aktuelna verzija 9, definisana u RFC 3954 [2]. Kako je Netflow Cisco proprietary rešenje, nastali su i drugi slični protokoli koji se bave istim problemom: sflow, IPFIX (IEEE rešenje koje se bazira na Netflow V9 formatu paketa) i dr.

Rešenja za analiziranje IP tokova mrežnog saobraćaja obično funkcionišu u tri sloja: 1) analiza; 2) prikupljanje i skladištenje; 3) prezentovanje podataka.

B. Analiza

Analiza saobraćaja može se raditi na ruteru, pomoću ugrađenih programa koji sa kolektorima komuniciraju preko netflow, sflow ili sličnog protokola; ili na računaru opšte namene uz pomoć interfejsa za prikupljanje paketa (pcap – *packet capture interface*) i specijalizovanih programa za analiziranje paketa. Ovi programi, bilo da se izvršavaju na ruteru ili računaru, u opštem slučaju nazivaju se sonde (probes).

Cisco-vo rešenje za Netflow podrazumeva da se analiza saobraćaja obavlja na ruteru. Ovaj pristup zahteva rutere koji podržavaju Netflow, a specifične potrebe ovog rada (sortiranje po ASN atributima i klasifikacija po servisima) dalje sužavaju izbor na one rutere koji u sebi imaju aktivan BGP (*Border Gateway Protocol*) proces i koji imaju mogućnost tzv. „duboke“ klasifikacije paketa i tokova (*Deep Packet Inspection*).

Drugi način prikupljanja statistika, koji je znatno ekonomičniji od nabavke novih rutera u mreži, koristi softverske pakete *tcpdump* i *libpcap* na računarima opšte namene za prisluškivanje (*sniffing*) saobraćaja i specijalizovane programe za obradu tog saobraćaja i prikupljanje statistika.

C. Softverske sonde

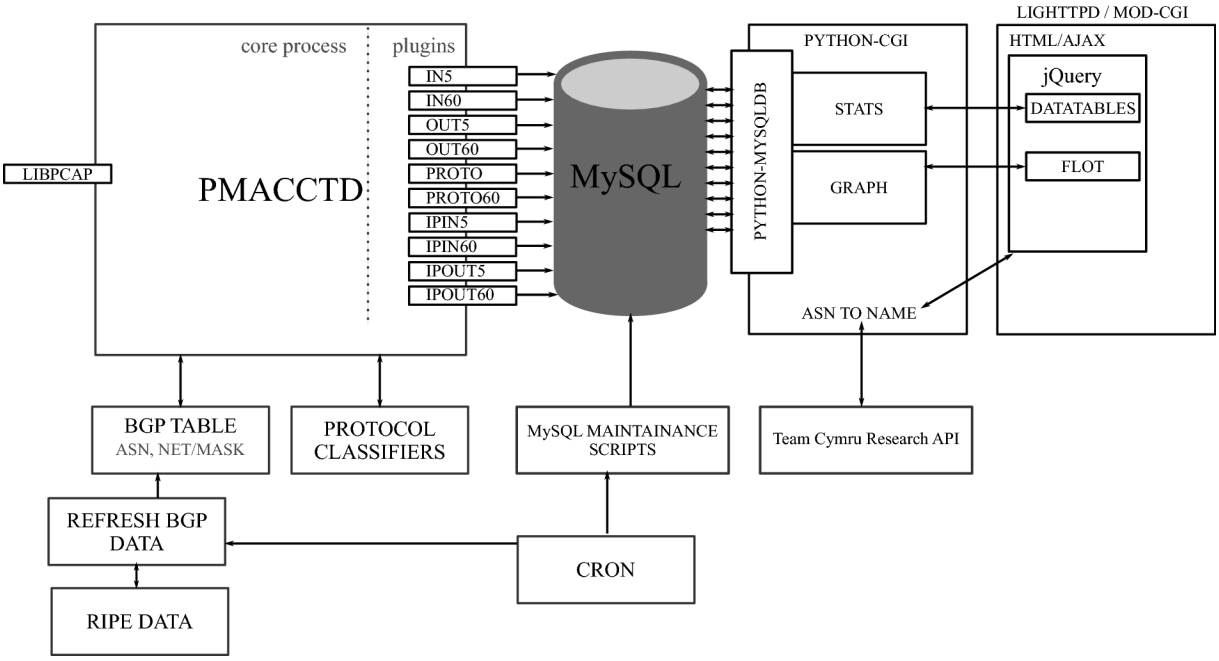
Prilikom analiziranja saobraćaja na računarima opšte namene, sav odlazni i dolazni saobraćaj mreže se šalje i na port mrežne kartice računara, koja funkcioniše u *promiscuous* modu. Taj mod joj omogućava da skuplja sve *Ethernet* pakete, a ne samo one koji su njoj namenjeni i da ih dalje obrađuje.

Libpcap je biblioteka za sakupljanje paketa koja se koristi u programima poput tcpdump-a i pmacct-a na Unix-olikim sistemima. Ona pruža interfejs visokog nivoa sistemima za analiziranje paketa, dobro je testirana i dokumentovana. Pomoću nje paketi se mogu skupljati i skladištiti na disku ili se mogu direktno prosleđivati programima za analizu (tj. sondama). [3]

Programi kao što su *nProbe*, *sflowd*, *IPCAD* ili *pmacct* mogu se koristiti kao softverske sonde za analiziranje mrežnog saobraćaja i prosleđivanje statistika o tokovima

Petar Vasić, Elektrotehnički fakultet u Beogradu, Bulevar kralja Aleksandra 73, 11120 Beograd, Srbija (telefon: 381-64-9905742, e-mail: p.vasic@gmail.com).

Nenad Krajnović, Elektrotehnički fakultet u Beogradu,(e-mail: krajko@etf.rs).



Sl. 1: Dijagram sistema

ka kolektorima koji te podatke dalje procesiraju i skladište. Komunikacija sa kolektorima može se obavljati preko netflow ili sličnog protokola, ili direktno (neki kolektori imaju ugrađene sonde).

Rad ovih programa uglavnom se zasniva na korišćenju libpcap biblioteke, ali, po potrebi, neki od njih mogu koristiti i druge metode.

D. Prikupljanje i skladištenje podataka

Kolektori sakupljaju statistike koje im šalju sonde, obrađuju ih i filtriraju i potom smeštaju u sisteme za skladištenje podataka, ili ih direktno prosleđuju programima za prezentaciju.

Oni mogu imati ugrađene sonde, ili koristiti zasebne (bilo hardverske ili softverske). U potonjem slučaju, komunikacija između sonde i kolektora odvija se preko netflow ili sličnog protokola.

Zbog velike količine saobraćaja koji generišu savremene mreže, čak i informacije o tokovima mogu da zauzimaju velike količine memorije, pa se ne mogu dovoljno brzo procesirati i prikazati u aplikacijama za prezentaciju. Iz tog razloga, vrlo je bitno kontrolisati veličinu i kvalitet skupa podataka koji skladištimo.

Agregacija saobraćaja umnogome ublažava ovaj problem tako što smanjuje broj atributa koji definišu jedan tok i grupiše atribute u opštije vrednosti (npr. IP adrese u mreže ili autonomne sisteme). Ovim postupkom grupišemo mikrotokove u makrotokve (ili agregate), pritom čuvajući zahtevanu detaljnost podataka.

Za potrebe ovog projekta korišćen je program pmacct, koji služi i kao softverska sonda i kao kolektor koji ima ugrađene napredne mogućnosti filtriranja i agregacije saobraćaja.[4]

E. Načini skladištenja podataka

Alati za prikupljanje i skladištenje podataka mogu koristiti više različitih metoda skladištenja: RRD, relacione baze podataka ili *proprietary* rešenja.

Proprietary rešenja su specifična za svakog proizvođača, često slabo dokumentovana; predstavljaju lošije rešenje od standardizovanih tehnologija, pa ovde nisu ni razmatrana.

RRD je tip cirkularnih baza namenjenih skladištenju podataka koji se menjaju u vremenu, poput mrežnog protoka, temperature, opterećenja procesora i sl. Međutim, zbog prirode našeg problema (praćenje statistika za odlaznog i dolaznog saobraćaja za svaki AS posebno u vremenu), ovo rešenje nije optimalno.

Relacione baze poput MySQL-a predstavljaju provereno, već isprobano rešenje, koje ima dokazanu fleksibilnost i skalabilnost. Čuvanje podataka u njima omogućava i veliku slobodu proširenja sistema, ili pravljenja posebnih izveštaja iz drugih aplikacija.

F. Prezentacija dobijenih podataka

Kada sonde i kolektori počnu da upisuju statistike u bazu, potrebno je te podatke prezentovati na što efikasniji način.

Gotova rešenja se mogu naći, ali nijedno od njih ne pokriva tačno onaj slučaj koji je nama potreban, pa smo ovde pristupili pravljenju novog rešenja, specifičnog za ovaj problem.

III. Implementacija

Detaljan dijagram sistema dat je na Sl. 1.

Sav saobraćaj sa ivičnih tačaka mreže šaljemo na port mrežne kartice servera. Kao sondu i kolektor koristimo *pmacctd*, koji prisluškuje saobraćaj preko libpcap biblioteke. Pomoću njega vršimo agregaciju po 5 zasebnih atributa: 1) izvorišni ASN za dolazni saobraćaj, 2) odredišni ASN za odlazni saobraćaj, 3) tip servisa saobraćaja, 4) izvorišna IP adresa za odlazni saobraćaj i 5) odredišna IP adresa za dolazni saobraćaj.

Za svaki od atributa čuvamo broj prenetih paketa i bajtova.

Prevođenje IP adresa u brojeve autonomnih sistema radi se pomoću posredne tabele u formatu „ASN, mreža/prefiks“ koji se posebnom skriptom periodično

skida sa RIPE-ovog sajta.

Klasifikacija saobraćaja prema servisu radi se pomoću klasifikatora iz *l7-filter* projekta koji su u formi regularnih izraza.

Navedeni podaci se upisuju u tabele u MySQL bazi na svakih 5 i 60min, pa ukupno imamo 10 tabela. Tabele su u formatu „ID, atribut, broj prenetih paketa, broj prenetih bajtova, vreme ubacivanja, vreme osvežavanja“.

Za održavanje baze koristimo posebne Python skripte koje brišu zastarele i nepotrebne podatke, a koje se periodično pokreću preko *cron* servisa.

Prezentaciju podataka vrši *lighttpd* web server, sa omogućenim *mod-cgi* dodatkom. On opslužuje statičke HTML strane, koje sadrže tabele i grafike. Za njihovo popunjavanje koristimo JSON podatke koje nam prosleđuju Python CGI skripte. Zarad lakšeg pisanja koda i bolje kompatibilnosti sa popularnim pregledačima, koristimo *jQuery* biblioteku i dodatke *Datatables* i *Flot*. Prvi nam omogućava da popunjavamo interaktivne tabele koje se mogu proizvoljno sortirati, a Flot koristimo za iscrtavanje grafika.

Dobijanje imena vlasnika ASN-a takođe se radi AJAX zahtevom i Python skriptom koja koristi *Team Cymru Research API* za tu uslugu.

Podaci se iz baze čitaju Python skriptama preko python-mysqldb modula i potom služe u JSON formatu pogodnom za učitavanje u tabele i grafike. Korišćena su dva seta skripti: prvi za popunjavanje tabela (kome u zahtevu prosleđujemo period za koji nam trebaju podaci) i drugi za crtanje grafika (kome pored perioda prosleđujemo i parametar po kome radimo iscrtavanje: broj AS-a, servis, ili IP adresu).

IV. Rezultati

Sistem je implementiran na računaru sa procesorom Pentium 4 (3.2GHz, 1GB RAM) i 100 Mb/s mrežnom karticom. Kako je ukupni saobraćaj prosleđivan kartici ponekad prelazio kapacitet fizičkog interfejsa, deo paketa bio je odbačen. Upoređivanjem sa sistemima za merenje protoka na ruterima, dobili smo da je analizirano oko 90% saobraćaja. Sem toga, sistem je lako podneo obrađivanje podataka: opterećenje procesora ne prelazi 50%, a veličina MySQL baze posle 15 dana praćenja je ispod 500MB.

Tabela 1: Prvih 10 AS-ova po količini dolaznog saobraćaja

Institucija kojoj pripada AS	***Preneto GB***	***% Saobraćaja***
Lemuria Communications Inc	148.02	6.36
Youtube Europe	86.94	3.73
Leaseweb AS	76.64	3.29
Choopa, LLC	70.84	3.04
Level 3 Communications	63.24	2.72
Canonical LTD	61.72	2.65
NASA	56.37	2.42
Hungarnet	51.06	2.19
Microsoft Corp	47.56	2.04
GONET	47.26	2.03

U periodu od 21.9.2010. do 3.10.2010. zabeležena je komunikacija sa 30666 AS-ova od ukupno aktivnih 35532 u tabeli rutiranja[5]. U tabelama 1 i 2 prikazani su prvih 10 AS-ova za dolazni i odlazni saobraćaj, količina prenetih podataka u tom periodu, kao i njihov udeo u ukupnom dolaznom (tj. odlaznom) saobraćaju.

Tabela 2: Prvih 10 AS-ova po količini odlaznog saobraćaja

Institucija kojoj pripada AS	***Preneto GB***	***% Saobraćaja***
Serbia BroadBand – Srpske kablovske mreže	356.25	8.24
NTL group limited	111.90	2.59
Verizon Online LLC	93.18	2.15
UPC Broadband	71.69	1.66
YUnet International	69.33	1.60
BeotelNet	64.40	1.49
AT&T Internet Service	63.80	1.47
Avatar Broadband Ltd	62.86	1.45
BTnet UK Regional Network	60.28	1.39
RSC&RPS S.A	54.77	1.27

U oba slučaja, prvih 10 AS-ova generišu skoro četvrtinu saobraćaja. Daljom analizom podataka u bazi, utvrđeno je da prvih 100 AS-ova generišu oko 75% saobraćaja.

Raspored saobraćaja po servisima dat je u tabeli 3.

Tabela 3: Raspored saobraćaja po servisima

Servis	***% Saobraćaja***
bittorent	41.79
http	30.88
unknown	19.86
ssl	1.40
nbns	1.39
edonkey	0.96
ntp	0.82
sypetoskype	0.80
http-itunes	0.58
ssh	0.35

Kao što se vidi, skoro 20% saobraćaja ostaje neidentifikovano. To se može pripisati nedovoljno dobrim klasifikatorima koji su korišćeni, kao i šifrovanom saobraćaju koji se ne može pouzdano detektovati i klasifikovati.

A. Domaći saobraćaj

U Srbiji trenutno ima 94 registrovana AS-a[6] Prema izmerenim podacima za period od 28.9.2010. do 03.10.2010, njihov udeo u ukupnom saobraćaju iznosi 3.03% za dolazni saobraćaj i 6.2% za odlazni saobraćaj. Pet najprometnijih AS-ova iz Srbije za odlazni i dolazni saobraćaj, za taj period, dati su u tabelama 4 i 5.

Tabela 4: Top pet srpskih AS-ova za dolazni saobraćaj

Institucija na koju glasi AS	***% Saobraćaja***
Telekom Srbija A.D	0.938
Univerzitet u Beogradu	0.657
Serbia BroadBand – Srpske kablovske mreže d.o.o.	0.430
Internet komunikacioni sistemi – INT CS d.o.o	0.275
YUnet International d.o.o.	0.212

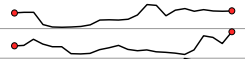
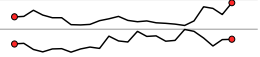
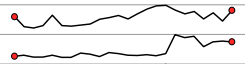
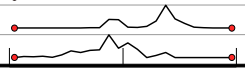
Tabela 5: Top pet srpskih AS-ova za odlazni saobraćaj

Institucija na koju glasi AS	*% Saobraćaja*
Serbia BroadBand – Srpske kablovske mreže d.o.o.	3.772
YUnet International d.o.o.	0.528
Univerzitet u Beogradu	0.514
Verat d.o.o.	0.361
Društvo za telekomunikacije Orion Telekom d.o.o.	0.279

U tabeli 5 nedostaje BeotelNet, koji se javlja u tabeli 2, ali RIPE-ovi podaci[6] njemu dodeljuju kod za Litvaniju.

B. Dan i noć

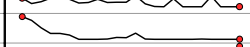
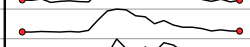
Tabela 6: Intenzitet saobraćaja po servisima

Servis	*Prosečan saobraćaj u toku dana* 0h 12h 23h
bittorent	
http	
unknown	
ssl	
nbns	
edonkey	
ntp	
sypetoskype	
http-itunes	
ssh	
	0h 12h 23h

Kao što se iz tabele 6 vidi, neki servisi poput HTTP-a i SSL-a imaju veliki pad saobraćaja u toku noći, dok je kod drugih (bittorrent, edonkey) taj pad mnogo manje izražen. Neki servisi poput popularnog VOIP servisa Skype i iTunes-a aktivni su samo u poslepodnevnim i večernjim satima.

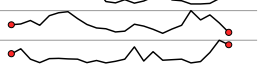
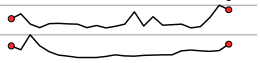
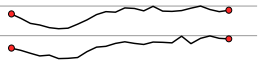
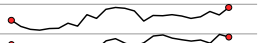
Isto tako, možemo da primetimo da su neki AS-ovi aktivniji noću, a neki danju. Tabela 7 daje pregled dolaznog saobraćaja u toku dana, sa primerima četiri AS-a koji imaju izražen noćni saobraćaj i 4 AS-a koji imaju izražen dnevni saobraćaj.

Tabela 7: Intenzitet dolaznog saobraćaja u toku dana i noći za AS-ove koji imaju izražene oscilacije

Institucija kojoj pripada AS	*Prosečan saobraćaj u toku dana* 0h 12h 23h
AS-ovi aktivni noću	
Canonical LTD	
IP Exchange GmbH	
Verizon Online LLC	
T.net	
AS-ovi aktivni preko dana	
Lemuria Communications Inc	
Leaseweb AS	
Choopa, LLC	
Hungarnet	
	0h 12h 23h

Ova pojava se još jasnije može uočiti za odlazni saobraćaj, za koji su podaci prikazani u tabeli 8. Možemo primetiti da su AS-ovi koji imaju najizraženiju aktivnost preko dana isključivo domaći.

Tabela 8: Intenzitet odlaznog saobraćaja u toku dana i noći za AS-ove koji imaju izražene oscilacije

Institucija kojoj pripada AS	*Prosečan saobraćaj u toku dana* 0h 12h 23h
AS-ovi aktivni noću	
T.net	
Avatar BroadBand	
Ziggo – tv, internet, telefon	
Telenet Operatics	
AS-ovi aktivni preko dana	
Telekom Srbija AD	
Serbia BroadBand	
YUnet	
BeotelNet	
	0h 12h 23h

V. Zaključak

Sistem se uspešno primenjuje na mreži Elektrotehničkog fakulteta, a u praksi se pokazao kao vrlo stabilan i pouzdan.

Merenjima je ustanovljeno da, iako se komunicira sa najvećim delom aktivnog interneta, manje od jednog procenta AS-ova odgovorno je za 90% saobraćaja. Što se servisa tiče, aplikacije za razmenu podataka (posebno Bittorrent) odgovorne su za najveći deo saobraćaja.

U budućim istraživanjima pažnju bi trebalo posvetiti usavršavanju postojećih klasifikatora i dodavanju novih, pošto trenutno skoro petina saobraćaja ostaje neklasifikovana. Takođe, praćenje novih atributa i izvođenje složenijih korelacija (npr. koje IP adrese koriste p2p protokole, detekcija DDoS napada i sl.) omogućilo bi još bolji uvid u funkcionisanje mreže.

Literatura

[1] *"Introduction to Cisco IOS NetFlow"*, Cisco Systems Inc., 2007. http://bit.ly/99IVKr

[2] RFC 3954, B. Claise, Ed. Cisco Systems, October 2004. "*Cisco Systems NetFlow Services Export Version 9"*

[3] V. Jacobson, et al, "*Pcap man page"*, November 2003. http://bit.ly/bjoV6L

[4] P. Lucente, *"pmacct: steps forward interface counters"*, March 2005, http://bit.ly/csfWLX

[5] www.cidr-report.org

[6] ftp://ftp.ripe.net/ripe/stats/2010/delegated-ripencc-20101003.bz2

Abstract

This paper describes the systems for network flow analisys. Solution, based on pmacct, currently in use on the network of the School of Electrical Engineering is presented, as well as the results of trafiic measurements and analisys.

ANALISYS OF THE NETWORK TRAFFIC FLOWS ON THE NETWORK OF BELGRADE'S SCHOOL OF ELECTRICAL ENGINEERING

Petar Vasić, mentor: Nenad Krajnović