DOI: 10.19279/TVZ.PD.2014-2-2-16

UREĐAJI ZA ANALIZU I KONTROLU MREŽNOG PROMETA

Mladen Maksimović[1], Valter Perinović[2], Dubravko Žigman[2]

[1]Student TVZ-a diplomirao 2014.
[2]Tehničko Veleučilište u Zagrebu

Sažetak

Eksponencijalni rast korisnika Interneta zajedno s rastućim brojem ***web-based*** aplikacija rezultira velikom potražnjom za što većom propusnošću. Međutim, konstantno povećavanje propusnosti nije moguće, a da bi riješili moguća ''uska grla'' potrebno je kontrolirati mrežni promet te odrediti skup pravila prioriteta prometa za dostupni kapacitet.

U radu se opisujuproblemi s kojima se svakodnevno susreću mrežni administratori, kako uređaj prepoznaje mrežni promet, zašto su bolji od implementiranih QoS mehanizama u usmjernicima i preklopnicima te kako uređaj za kontrolu mrežnog prometa nakon ugradnje u sustav pomaže mrežnim administratorima u prioritizaciji određenog mrežnog prometa i raspodjeli kapaciteta linka.

Ključne riječi: *uređaji za kontrolu mrežnog prometa, zagušenje kapaciteta linka, prioritizacija mrežnog prometa*

Abstract

The exponential growth of Internet users along with a growing number of ***web-based*** applications results in high demand for maximum throughput. However, the constant increase of bandwidth is not possible, and to resolve possible bottlenecks it is necessary to control network traffic and determine a set of priority rules for the available transport capacity.

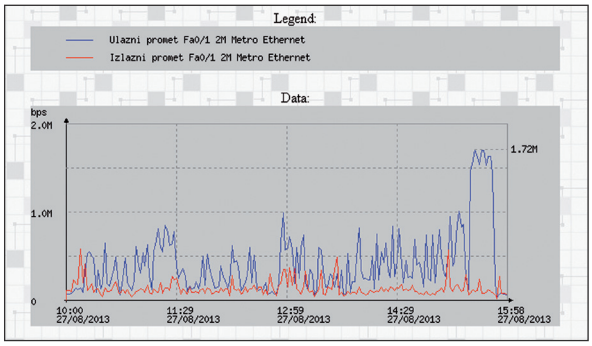
The paper describes the problems network administrators face every day,how device identifies network traffic, why they are better than the implemented QoS mechanisms in routers and switches, and how device after installing into system helps network administrators in prioritizing certain network traffic and distribution capacity of the link.

Key words: *network traffic devices, congestion link capacity, prioritization of network traffic*

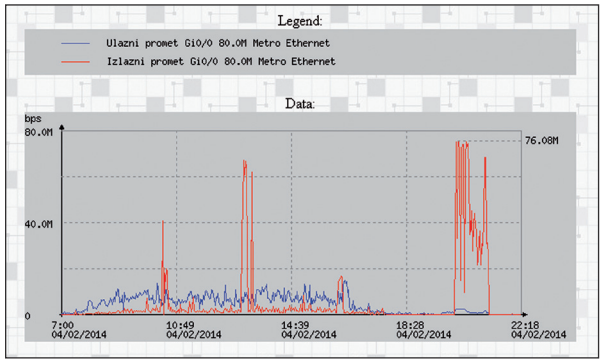
1. Uvod

U tvrtki čija komunikacijska i mrežna infrastruktura je kompleksna, postoje lokacije gdje je potrebno analizirati i prioritizirati mrežni promet. Na svakoj lokaciji nalazio bi se uređaj za kontrolu mrežnog prometa s pripadajućim pravilima samo za taj segment. Problemi s kojima se susreću mrežni administratori su razni. Kod Internet dijela mreže, korisnici aplikacije za video poziv žale se na trzanje slike i kašnjenje zvuka prilikom video poziva. Distribucija antivirusne aplikacije ili distribucija sigurnosnih zakrpa za operacijski sustav na računala, zauzela je veze prema podružnicama i poslovnicama te su se zaposlenici žalili na sporost sustava.

Slika 1. prikazuje graf prometa prema udaljenoj poslovnici kroz jedan dan. Kapacitet linka je 2 Mbit/s što je dovoljno za rad poslovnice.



Slika 1. *Zagušenje veze prema udaljenoj poslovnici*



Slika 2. *Zagušenjeveze prema lokalnoj poslovnici*

U jednom trenutku dolazi do povećanog prometa u dolaznom smjeru koji zauzima cijeli link, te zaposlenici primjećuju iznenadnu sporost sustava i aplikacija, a IP telefoniranje više nije moguće. U ovom slučaju problem je uzrokovala distribucija antivirusne aplikacije prema jednoj radnoj stanici unutar poslovnice.

Slika 2. prikazuje sličan problem, kapacitet linka prema lokalnoj poslovnici je 80 Mbit/s. U jednom trenutku dolazi do povećanog prometa u izlaznom smjeru koji zauzima cijeli link, te zaposlenici primjećuju iznenadnu sporost sustava i aplikacija, a IP telefoniranje više nije moguće. U ovom slučaju je radnica u poslovnici počela kopirati sve podatke pohranjene na svom lokalnom računalu na mrežni disk koji se nalazi na centralnoj lokaciji tvrtke. Radilo se o par desetaka gigabajta podataka. [1]

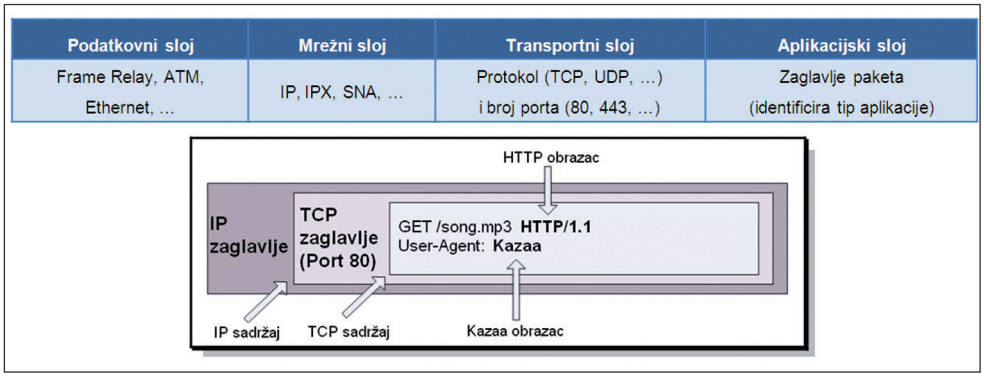
2. Uređaji za analizu i kontrolu mrežnog prometa

U današnje vrijeme mnogi proizvođači komunikacijske opreme implementirali su u svoje uređaje mogućnost kontrole prometa. Prioritizacija prometa može se konfigurirati na usmjernicima i preklopnicima, ali identifikacija prometa, kojeg je potrebno prioritizirati, nije tako detaljna i precizna kao na specijaliziranim uređajima, npr. identifikacija aplikacija ili servisa koji koriste port 80. U velikim mrežnim sustavima potrebno je konfigurirati veliki broj pravila koji zahtijevaju veliku procesorsku snagu usmjernika ili preklopnika, što je vrlo skupo a zbog velikog broja pravila na odlaznim sučeljima usmjernika mogućnost pogreške se povećava kao i vrijeme otklona pogreške u pravilima. [1], [2]

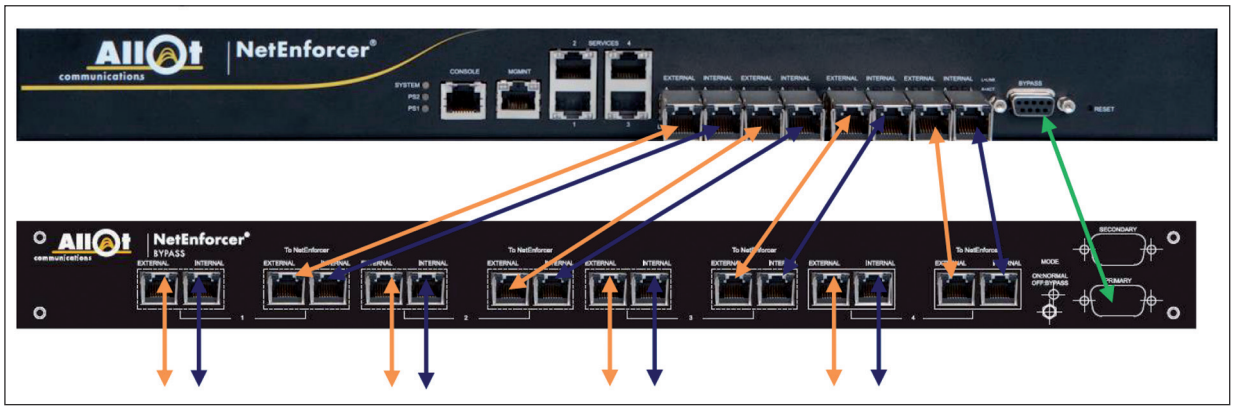
Razne informatičke tvrtke predstavile su IP *"traffic manager"*, odnosno uređaj čija je osnovna namjena analiziranje i prioritiziranje prometa na TCP/IP mrežama kako bi se što bolje iskoristio dostupan kapacitet. Uređaji mogu određivati na koji način se dostupan kapacitet raspoređuje ovisno o korisnicima, ciljanim računalima, protokolima i aplikacijama koje se koriste. Za analizu mrežnog prometa koristi se DPI (*engl. Deep Packet Inspection*) tehnologija za dubinsku analizu paketa na mreži, ne ulazeći detaljno u sadržaj svakog mrežnog paketa. Obzirom da moderne informatičke komunikacije koriste uglavnom jedan protokol (HTTP) i često puta jedan port (80 ili 443) kroz kojeg se tuneliraju različite aplikacije, posebna pozornost je posvećena identifikaciji i klasifikaciji mrežnih aplikacija te mogućnostima ostvarivanja boljeg QoS-a, npr. ako broj porta nije dovoljan za identifikaciju aplikacije, DPI će dodatno provjeriti zaglavlje paketa [1].

Kada se odredi mjesto u informatičkoj infrastrukturi gdje je potrebno nadzirati mrežni promet, unutrašnja strana mreže spoji se na unutrašnje sučelje npr. preklopnik, a vanjska strana se spoji u vanjsko sučelje npr. usmjernik. Svaki uređaj sadrži pasivnu komponentu za premoštenje, integriran u postojeći uređaj ili kao zaseban uređaj (slika 4.) Ako se uređaj pokvari, nestane struje ili se dogodi greška u programu, komponenta za premoštenje osigurava nesmetan prolazak prometa kroz uređaj.

Sav promet koji prolazi kroz uređaje spada u nepoznati (*engl.fallback*) promet. Analizirajući taj promet saznajemo koja računala ili serveri razmjenjuju podatke na unutarnjoj i vanjskoj strani uređaja. Mrežni sistem inženjeri znaju koji servisi i serveri trebaju imati prioritet, pa se sukladno tome kreiraju pravila u centraliziranom sustavu upravljanja uređajima. U aplikaciji se grafički prikazuje IP promet koji prolazi kroz



Slika 3. *DPI – identifikacija aplikacije* [2]



Slika 4. *Izgled uređaja zajedno sa uređajem za premoštenje prometa* [2]

Identification	Conditions								Actions		
Name	Alarms Assignment	In Use	Internal	Direction	External	Service	Time	Interface	Access	Quality of Service	DoS
Fallback		☑	Any	⇔	Any	All Service	Anytime	Any	Accept	Normal Line QoS	Ignore dos

Slika 5. *Izgled pravila u aplikaciji*

uređaj u realnom vremenu ili kroz neki duži vremenski period ograničen ili prioritiziran pripadajućim pravilom. [1], [2]

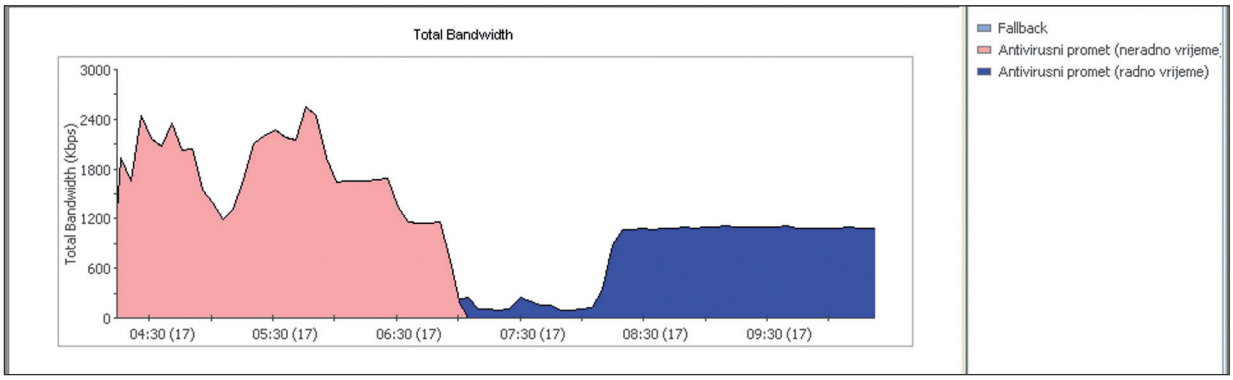
Pravilo u aplikaciji sastoji se od tri dijela (slika 5.), identifikacije (*engl. Identification*), uvjeta (*engl. Conditions*) i akcije (*engl. Action*). [2]

Pod poljem identifikacija nalazi se ime pravila. Pod poljem uvjeti nalaze se kartice:

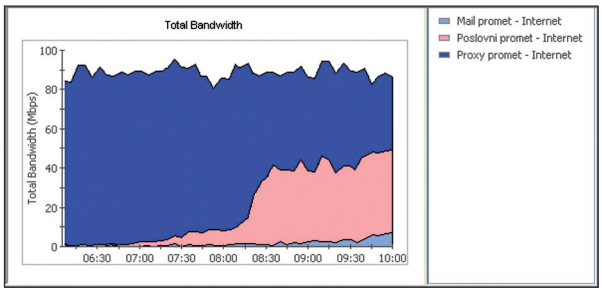
- *Alarm Assignment* – definiranje slanja elektroničke pošte, SMS-a mrežnom administratoru ukoliko nastanu određeni problemi, recimo kapacitet za određeni promet približi se maksimumu,
- *In Use* – definira da li je pravilo aktivno,
- *Internal* - definiranje prometa koji ulazi u uređaj prema unutarnjim korisnicima ili serverima. Opcije su prema bilo kojoj IP adresi (*engl.Any*), određenom skupu i pojedinačnoj IP adresi (IPv4 ili IPv6),
- *Direction* – definiranje u kojem smjeru se primjenjuje pravilo, opcije su u oba smjera, samo za promet iz unutrašnje mreže prema vanjskoj mreži, te samo za promet iz vanjske mreže prema unutrašnjoj mreži,
- *External* – definiranje prometa koji izlazi iz uređaja prema vanjskim korisnicima ili serverima. Opcije su prema bilo kojoj IP adresi, određenom skupu i pojedinačnoj IP adresi (IPv4 ili IPv6),
- *Service* – definiranje protokola kojeg je potrebno prioritizirati. Protokol može biti TCP i UDP tipa IP, te protokoli tipa IPX, Appletalk i NetBIOS. TCP i UDP protokoli IP tipa definirani su ovisno o tipu porta. HTTP protokol ima definicije po sadržaju, npr. specifične Internet stranice ili URL obrazac. Postoje i predefinirani protokoli koji su specifični samo za određene aplikacije, uključujući mrežne protokole i transportne protokole,
- *Time* – definira u koje vrijeme će određeno pravilo biti primijenjeno, npr. nadogradnja operacijskog sustava može u radno vrijeme biti blokirano, a dozvoljeno poslije radnog vremena,
- *Interface* – definira sučelja kroz koje prolazi promet. Npr. ako postoji više prolaznih sučelja, određena pravila mogu se definirati tako da se primjenjuju samo na određeno sučelje (unutrašnje i vanjsko). [2]

Pod poljem akcije nalaze se kartice:

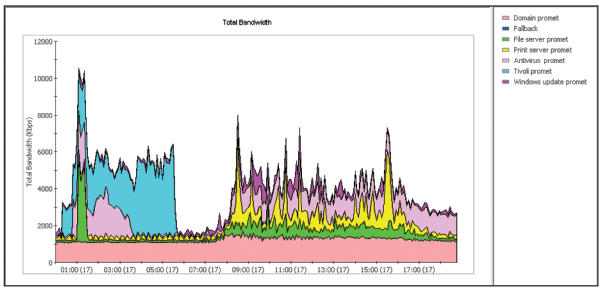
- *Access* – definira da promet prolazi kroz uređaj. Ostale opcije su odbijanje (*engl.Reject)* i odbacivanje (*engl.Drop*) prometa,
- *Quality of Service* – definira propusnost i prioritet. Opcije propusnosti su definiranje maksimalne ili minimalne (garantirane) propusnosti u dolaznom i/ili odlaznom smjeru prometa, dok kod prioriteta opcije su "*Best Effort*", te prioritet od 1 do 4, gdje je 4 maksimalni prioritet,



Slika 6. *Distribucija antivirusnog programa prema poslovnicama*



Slika 7. *Prioritizacija prometa prema Internetu*



Slika 8. *Grupiranje različitih distribucija aplikacija*

- *DoS* - kontrolira i ograničava broj uspostavljenih konekcija u sekundi te maksimalan broj konekcija, ako se jedan od navedenih uvjeta ostvare promet se odbacuje ili odbija. [2]

3. Rezultati nakon ugradnje

Nakon ugradnje uređaja i kreiranja pravila prema potrebama za svaki dio mreže, mogu se vidjeti poboljšanja u radu osjetljivih aplikacija kojima je dan prioritet, zagušenja prema poslovnicama više nema zbog ograničenosti linka za distribucije antivirusnog programa i za kopiranje podataka.

Slika 6. prikazuje kako se pravilo primjenjuje u radno i neradno vrijeme. U neradno vrijeme od 21:00 do 07:00 ograničenje linka je 3 Mbit/s dok u radno vrijeme od 07:00 do 21:00 ograničenje linka je 1 Mbit/s. Graf prikazuje kako distribucija antivirusnog programa koristi oko 2 Mbit/s linka u neradnom vremenu, sve do 07:00 sati gdje se aktivira pravilo od 1 Mbit/s. Zbog ovog pravila distribucija antivirusnog programa više ne može zagušiti cijeli link prema poslovnici.

Na Internet dijelu mreže postoje definirana tri pravila, sa različitim prioritetima (slika 7). *"Proxy"* promet generiraju zaposlenici tvrtke koji pretražuju i pregledavaju sadržaj Interneta imaju prioritet 1, mail promet ima prioritet 2, a poslovni promet ima maksimalni prioritet 4. Veličina linka je 100 Mbit/s i većinu linka zauzima *Proxy* promet. Ako je poslovnom prometu potrebno više linka, zbog većeg prioriteta, poslovni promet bude potiskao *Proxy* promet i mail promet. [1], [2]

Zbog postojanja više različitih distribucija aplikacija, moguće je grupirati sve distribucije u jedan graf, što mrežnom administratoru olakšava nadzor (slika 8.).

4. Zaključak

Tehnologija i komunikacije postižu eksponencijalan rast svake godine te se očekuje tijekom sljedećih godina (a već i danas) da će svi uređaji u kućanstvu biti umreženi, plaćanje računa putem Interneta, IP telefoniranje, gledanje HDTV programa putem Interneta, *"online"* igre, itd. Takav rast Internet aplikacija rezultira velikom potražnjom za što većom propusnošću i mrežnim resursima.

U radu su opisani uređaji za analizu i kontrolu mrežnog prometa koji na jednostavan način mrežnim administratorima omogućavaju kontroliranje tj. prioritiziranje, nadzor i ograničavanje mrežnog prometa. Nadzor se vrši

prema grafovima koji se mogu kreirati prema vlastitim potrebama. Grafovi koji se osvježavaju u realnom vremenu pružaju trenutačno stanje opterećenosti pojedinih mreža. Bez uređaja, kada nastupi zagušenje veze, potrebno je snimati promet te utvrditi koji promet je zagušio vezu. To zna biti dosta dugotrajan proces, što je nedopustivo za današnje poslovno kritične aplikacije i sustave.

Konstantno povećavanje propusnosti nije moguće, stoga će u budućnosti više doći do izražaja kontrola mrežnog prometa, pogotovo kod Internet pružatelja usluga. Proizvođači uređaja za kontrolu mrežnog prometa konstantno unapređuju vlastite uređaje, da mogu kvalitetno i brzo reagirati na potrebe tržišta. U budućnosti jedan takav uređaj biti će sposoban obavljati više različitih specijaliziranih radnji, npr. inteligentna obrana od DDoS napada, tarifiranje po korisniku koji koristi mobilne Internet usluge, te ciljani marketing prema korisničkim posjetama Internet stranica.

5. Reference

[1] Vedran Markić:“Deep Packet Inspection – (DPI)“, IT Pro Rijeka, lipanj 2011.

[2] Allot Communications:“NetEnforcer AC1400/AC3000 Hardware Guide”,July2013.

AUTORI

Valter Perinović - biografija se nalazi u ovom broju časopisa Polytechnic & Design Vol. 2, No. 2, 2014. na stranici 268.

Mr. sc. Dubravko Žigman - nepromjenjena biografija nalazi se u časopisu Polytechnic & Design Vol. 2, No. 1, 2014.