Otpornost konekcije na otkaz praćenjem objekata na Internetu u prisustvu redundantnog mrežnog prolaza

Dimitrije Kostić, dr Dušan Stefanović, dr Dejan Blagojević
Savremene računarske tehnologije
Visoka tehnička škola strukovnih studija
Niš, Srbija
mita4d@gmail.com, dusan.stefanovic@vtsnis.edu.rs, dejan.blagojevic@vtsnis.edu.rs

***Sadržaj*—U ovom radu pokazaćemo kako integracijom nekoliko Cisco rešenja možemo vezu sa Internetu učiniti otpornom na otkaz. Ukoliko imamo dve konekcije ka Internetu u slučaju otkaza, sav saobraćaj preusmeravamo na onu koja je u tom trenutku aktivna. Ovo se postiže praćenjem statusa tih konekcija. U slučaju kada su obe aktivne balansiramo saobraćaj na obe konekcije. Sprovešćemo merenja na osnovu kojih ćemo pokazati vreme tranzicije na aktivan link, vreme potrebno da saobraćaj nastavi da se odvija preko jednog linka i koje je vreme oporavka konekcije. Analiziraćemo kako se promenom učestalosti provere statusa objekta menja vreme oporavka.**

Ključne reči- Cisco IP SLA; praćenje objekata; merenje brzine konvergencije; redundantnost uređaja i veza

I. UVOD

Ostvarivanje permanentnog pristupa Internetu danas je imperativ koji se postavlja pred inženjera koji je zadužen za projektovanje ili održavanje jedne računarske mreže. Pristup Internetu ostvarujemo preko provajdera (eng. ISP- Internet Service Provider) koji nam pruža takvu vrstu usluge. Sklapanjem ugovora sa ISP-om ugovaramo i nivo usluge koja nam je potrebna, tj. propusnu moć linka kojim se povezujemo na Internet. Iako većina provajdera tvrdi da nam može omogućiti neprekidan pristup Internetu 365 dana u godini 24 časa dnevno, praksa je pokazala da to nije baš tako i da su prekidi veze sa Internetom i te kako mogući. Postoji mnogo uzroka zbog kojih dolazi do prekida veze sa Internetom, to mogu biti od softverskih problema preko hardverskih pa sve do vremeskih nepogoda, nestanka struje ...

Da bi predupredili ovakvu situaciju jedno od rešenja jeste zakup još jednog linka ka Internetu i to ako za to postoje tehničke mogućnosti od drugog provajdera koji omogućava istu uslugu. Rezervnom vezom (eng. backup link) smanjujemo mogućnost da ostanemo bez izlaska na Internet, jer je mnogo manja verovatnoća da oba linka u istom trenutku ne budu funkcionalna.

Međutim, ovakvo rešenje samo po sebi nije potpuno funkcionalno i bez dodatnih podešavanja na graničnom ruteru ne možemo tek tako prebaciti mrežni saobraćaj sa primarnog provajdera na rezervni. Potrebna je intervencija administratora mreže kako bi se saobraćaj preusmerio ka Internetu preko rezervnog linka. Uključivanjem ljudskog faktora u celu priču gubi se na pouzdanosti. Ukoliko administrator ne detektuje otkaz primarne konekcije ili ne bude prisutan na radnom mestu kada se desio otkaz, neće moći ni da blagovremeno preusmeri saobraćaj na rezervni link. Na ovaj način se mogu proizvesti gubici u poslovanju ukoliko se radi o preduzeću koje svoje poslovanje obavlja preko Interneta.

Jedan od načina da izbegnemo uticaj čoveka jeste da automatizujemo proces prelaska sa jednog linka na drugi. To možemo ostvariti programiranjem mrežnih uređaja, koristeći granični usmerivač (eng. Router) sa određenim hardverskim i softverskim specifikacijama.

U ovom radu biće predstavljena dva moguća načina povezivanja lokalne mreže sa Internetom preko dva različita Internet provajdera. I na koji način praćenjem objekata van lokalne mreže detektujemo prekid u komunikaciji sa Internetom, automatizijemo proces preusmeranja saobraćaja na aktivnu konekciju.

II. TOPOLOGIJA MREŽE SA JEDNIM GRANIČNIM RUTEROM

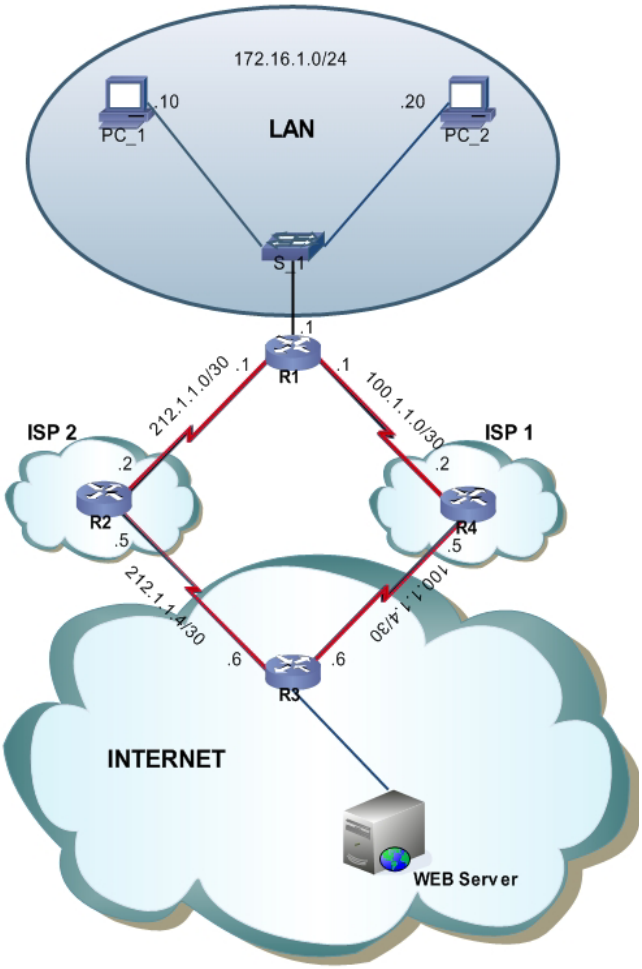
Konkretan problem koji je ovde postavljen pred administratora je taj da se obezbedi otpornost konekcije ka Internetu u slučaju otkaza jedne od dve konekcije i da se automatski obavi prelazak na onu aktivnu [1]. Topologija mreže prikazana je na Sl.1.

Ruter R1 je granični ruter, marke Cisco 2691 koji je preko serijskih veza povezan sa ISP 1 i ISP 2, a sa lokalnom mrežom je povezan preko *Fast Ethernet* interfejsa.

Za primarnu konekciju uzeta je konekcija preko ISP 1, a sekundarna je ona koja ide preko ISP 2. Takođe da se celokupan saobraćaj ne bi odvijao samo preko primarne konekcije raspodelićemo saobraćaj tako da se HTTP saobraćaj šalje preko sekundarne, a sav ostali mrežni saobraćaj šalje preko primarne veze. Računari PC_1 i PC_2 za potrebe provere ispravnosti konfiguracije slaće pakete preko različitih provajdera na Internet i to tako da PC_1 izlazi na Internet preko ISP 1, a računar PC_ 2 izlazi preko ISP 2 na Internet.

Da bi se ovo postiglo potrebno je integrisati nekoliko različitih servisa koje pruža Cisco IOS (Internetwork Operating System) operativni sistem rutera, a to su:

- Cisco IOS IP SLA (Service Level Ageement)
- Statičko rutiranje
- Policy Based Routing (PBR)
- Network Adress Translation (NAT)



Slika 1. Topologija mreže sa jednim graničnim ruterom [1]

Za praćenje statusa obe veze ka Internetu potrebno je na Cisco ruteru pokrenuti praćenje objekata koji mogu ukazati da li je veza aktivna. Za to se može iskoristiti mogućnost Cisco operativnog sitema IOS i upotrebiti servis IP SLA (Service Level Agreement) [2]. Za aktivno praćenje statusa izabranog objekta, iskoristićemo operaciju praćenja preko ICMP [5] protokola. Ova operacija meri vreme odziva mrežnog uređaja koje ima svoju IP adresu. Vreme odziva je vreme koje protekne od slanja ICMP (request) zahteva poslatog sa Cisco rutera i vreme dolaska ICMP (reply) odgovora od objekta kome je poslat zahtev. Ukoliko uređaj odgovori znači da je aktivan.

Pomoću statičkih ruta [6] određena je putanja paketa koji izlaze van lokalne mreže. Dodeljivanjem administrativne distance odeđrna je primarna i sekundarna konekcija sa Internetom. Ove statičke rute su direktno povezane i sa praćenim objektima koje pratimo pomoću IP SLA. Ukoliko praćeni objekat u nekom trenutku bude nedostupan granični ruter neće proslediti paket ka tom ISP čiji je otkaz detektovan.

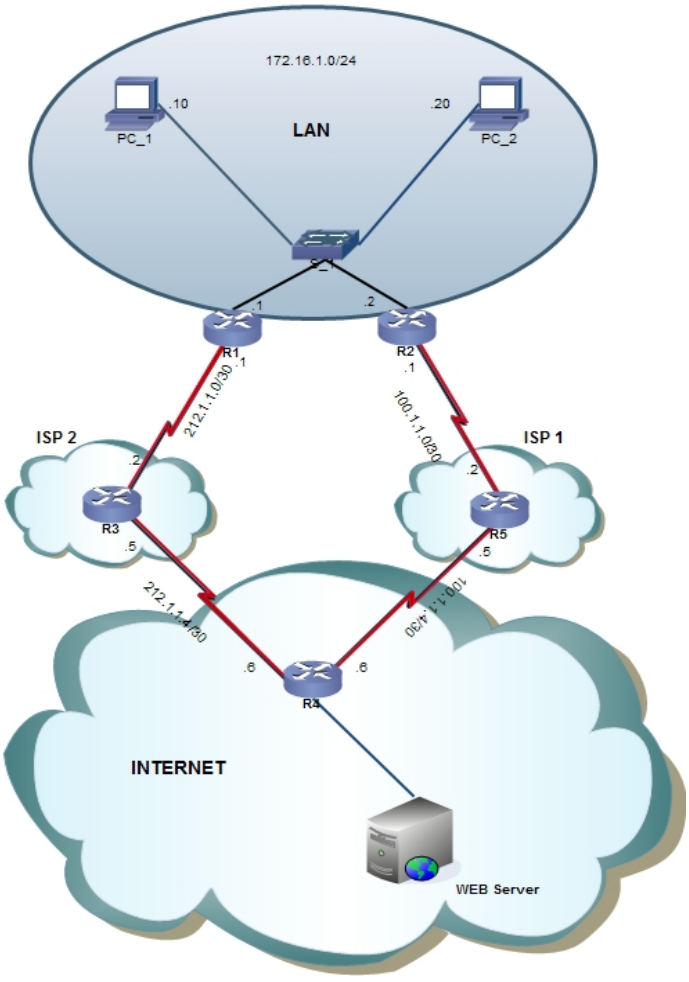
Upotrebom rutiranja na osnovu polisa (Policy Based Routing) [7] omogućena je raspodela saobraćaja na oba Internet provajdera u slučaju kada su obe veze aktivne. Saobraćaj se deli prema tipu. Pod predpostavkom da će najveći obim saobraćaja dolaziti sa Interneta baš u vidu HTTP saobraćaja, samo ovaj tip saobraćaja će prolaziti preko ISP_2, dok će se sav ostali saobraćaj sa Internetom odvijati preko ISP_1. Ovo važi samo u slučaju kada su obe konekcije aktivne.

Za prevođenje adresa iz LAN mreže koje su iz opsega privatnih adresa koristi se NAT (Network Address Translation) [8]. Prevođenje je potrebno jer postoji samo po jedna dodeljena javna IP adresa od stane oba provajdera preko kojih mreža izlazi na Internet.

III. TOPOLOGIJA MREŽE SA DVA GRANIČNA RUTERA

Mrežna infrastruktura implementirana u ovom radu je nadogradnja na infrastrukturu objašnjena u radu [1]. U osnovi problem koji treba rešiti je isti, a to je ostvarivanje permanentnog pristupa Internetu. Međutim u ovom slučaju biće pokazano kako da otpornost od otkaza podignemo na jedan viši nivo upotrebom dodatnog hardvera i servisa Cisco IOS operativnog sistema.

Prva i osnovna ideja jeste omogućiti praćenje objekata tj. provera veze između lokalne računarske mreže do neke udaljene lokacije na Internetu. Na Sl.2 je prikazana topologija mreže



Slika 2. Topologija mreže sa dva graničma rutera

Ruteri R1 i R2 predstavljaju granične rutere preko kojih računari iz lokalne mreže ostvaruju komunikaciju sa drugim računarima na Internetu. Za automatizaciju procesa detekcije otkaza i tranzicije saobraćaja na aktivan link na ovim ruterima moraju biti pokrenuti sledeći servisi Cisco IOS operativnog sistema:

- Cisco IOS IP SLA
- Statičko rutiranje
- Policy Based Routing (PBR)
- HSRP (Hot Standby Router Protocol)
- Network Adress Translation (NAT)

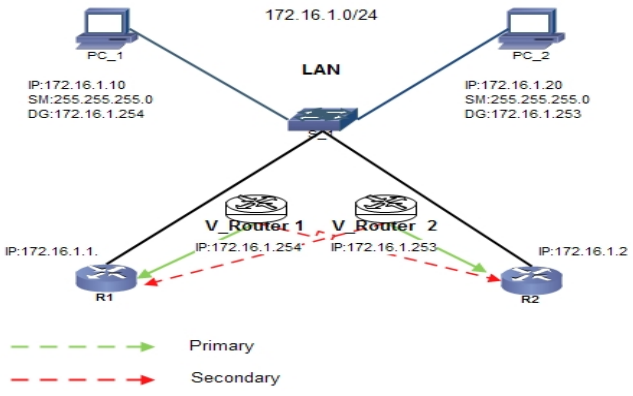
U topologiji sa dva granična rutera praćenje statusa konekcija vrši se na oba granična rutera pomoću Cisco IP SLA. Oba granična rutera prate status oba linka ka Internetu pomoću ICMP Etho operacije. Definisanjem vremenskog intervala učestalosti slanja ICMP poruka definisano je i vreme potrebno za otkrivanje promena nastalih u mrežnoj topologiji zbog otkaza konekcije sa Internetom ili nekog uređaja.

Pomoću statičkih ruta definisane su primarna i sekundarna ruta za granične rutere. Za ruter R1 je primarna ruta ona koja vodi ka ISP 2 i povezana je sa praćenjem statusa ISP 2, a sekundarna ruta vodi ka drugom graničnom ruteru preko koga se ostvaruje konekcija sa ISP 1 i povezana je sa praćenjem ISP 1. I na ruteru R2 su na sličan način definisane primarna i sekundarna ruta. Primarna je ona koja vodi ka ISP 1 povezana je sa praćenjem ISP 1 pomoću IP SLA, a sekundarna vodi ka ruteru R2 i povezana je se statusom ISP 2. Primarna ruta mora imati najmanju administrativnu distancu u odnosu na ostale. Ukoliko se pomoću IP SLA detektuje otkaz primarne konekcije ova ruta biće izbačena iz tabele rutiranja, a na njenom mestu će se naći sekundarna.

Rutiranje na osnovu polisa (PBR) primenjujemo na identičan način kao i u topologiji sa jednim graničnim ruterom[1]. HTTP saobraćaj će biti usmeren na ISP 2, dok sav ostali će ići preko ISP 1 u slučaju kada su obe veze sa Internetom aktivne. Prevođenje lokanih IP adresa u javne se vrši na oba granična rutera pokretanjem NAT servisa.

Pokretanjem ovih servisa iskorišćena je redundantnost veza sa Internetom i osigurana komunikacija i u slučaju otkaza jedne od veza. U slučaju fizičkog otkaza jednog od graničnih rutera deo mreže kome je taj ruter bio izlaz iz lokalne mreže ostaće bez komunikacije sa Internetom. Međutim, pomoću HSRP[10] protokola biće iskorišćena prisutna redudatnost mrežnog prolaza za računare unutar lokalne računarske mreže.

U postojećoj topologiji u kojoj postoje dva rutera preko kojih računari fizički ostvaruju vezu sa Internetom, pomoću HSRP biće kreirana još dva virtuelna rutera sa jedinstvenim IP adresama iz opsega lokalne mreže. Ip adrese viruelnih rutera biće predstavljene klijentskim računarima kao izlaz iz lokane mreže. Svaki virtuelni ruter ima mogućnost da saobraćaj preusmeri na oba fizička rutera. Virtuelnom ruteru V_Router 1 primaran ruter R1, u slučaju prestanka sa radom saobraćaj će se preusmeriti ka R2. Obrnuta je situacija kod V_Router 2, njemu je primaran fizički ruter R2, a sekundarni R1. Logička topologija lokalne mreže prikazana je na Sl.3.



Slika 3. Logička topologija LAN mreže

IV. MERENJE VREMENA TRANZICIJE

U ovom delu rada biće prikazani dobijeni rezultati merenjem vremenskog intervala koji je potreban graničnim ruterima da izvrše tranziciju saobraćaja sa jednog ISP na drugi u slučaju otkaza. U predhodnom delu (Sl.1 i Sl.2) prikazane su dve različite konfiguracije nad kojim će biti izvršeno merenje. Pokazaće se kako promenom parametra utičemo na brzinu konvergencije mreže od nastanka otkaza pa do detektovanja tog otkaza i do oporavka veze tj. automatskog prelaza na aktivnu konekciju koja povezuje lokalnu mrežu i Internet.

Isto tako možemo izmeriti i vreme oporavka konekcije koja neaktivna, to vreme je isto kao i vreme preusmerenja saobraćaja na drugog provajdera. Razlog je taj da IP SLA prati statuse obe konekcije ka Internetu bile one aktivne ili ne. Najvažnije je vreme za koje će IP SLA otkriti da li je neki od praćenih objekata aktivan ili ne. Promenom parametra učestalosti provere određujemo nakon kog vremenskog intervala će IP SLA proveravati status konekcija. U tabeli I dati su rezultati merenja koja smo izvršili kada je učestalost slanja ICMP poruka bila podešena na 2, 5, 10 i 15 sekundi.

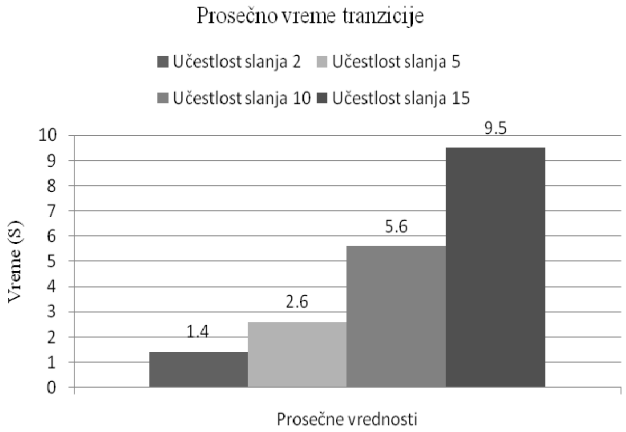
TABELA I. VREMENA TRANZICIJE U KONFIGURACIJI SA JEDNIM GRANIČNIM RUTEROM

	Učestalost slanja (s)			
Broj merenja	***2***	***5***	***10***	***15***
1.	1	3	3	12
2.	2	4	11	5
3.	1	2	6	11
4.	1	1	2	10
5.	1	5	6	3
6.	2	2	8	14
7.	1	1	4	16
8.	1	4	2	9
9.	2	2	9	5
10.	2	2	5	10

Kao što možemo uočiti u tabeli I, dobijeni rezultati su uglavnom manji od učestalosti slanja koja je bila podešena, iz razloga što se vremenski otkaz može dogoditi u bilo kom trenutku u intervalu između dve provere statusa praćenog objekta. U pojedinim slučajevima smo dobili i veće vrednosti od vremena koje smo podesili, ali to mozemo pripisati grešci,

koja ovim načinom merenja može iznositi do 1 sekunde, kao i ljudskom faktoru koji je ovde takođe prisutan.

Generalno prosečne vrednosti Sl.4 koje su dobijene nakon svakog merenja su manje od 36 do 48 procenata od maksimalnih. Tako da možemo očekivati i u realnom vremenu da vreme koje je potrebno graničnom ruteru da preusmeri saobraćaj ili izvrši oporavak konekcije bude manje od konfigurisanog vremenskog intervala nakon kog IP SLA proverava status praćenog objekta.



Slika 4. Prosečno vreme tranzicije

Merenja nad mrežnom topologijom u kojoj imamo dva granična rutera preko kojih računari iz lokalne mreže izlaze na Internet vršimo na identičan način kao i u topologiji sa jednim ruterom. Na računarima PC_1 i PC_2 je instalirana aplikacija *Ping Plotter* pomoću koje pratimo putanju kojom prolaze paketi do krajnje adrese, u našem slučaju je to IP adresa 60.1.1.1 koja pripada Web serveru koji se nalazi van lokalne mreže a predstvlja bilo koji server koji se nalazi na Internetu. Njemu se može pristupiti preko oba Internet provajdera. Prilikom konfiguracije graničnih rutera pomoću PBR-a definisali smo da PC_1 i PC_2 komunikaciju sa Internetom ostvaruju preko dva različita Internet provajdera, samim tim i putanja do Web servera je različita.

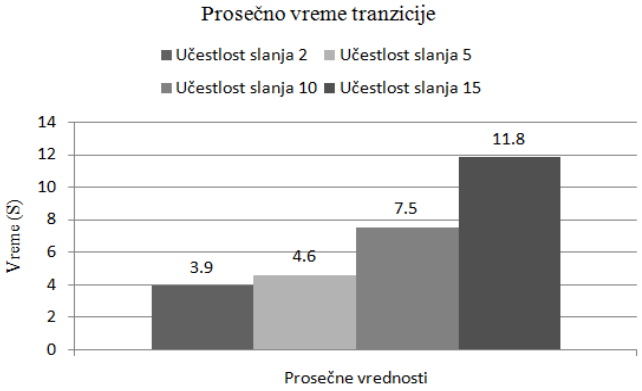
Simuliranje otkaza u nekom delu jedne od putanja do Web servera predstavlja nam početni trenutak merenja vremenskog intervala koji je potreban graničnim ruterima da detektuju da je došlo do prekida i da saobraćaj bude preusmeren na putanju koja je u funkciji. Kao krajnji trenutak završetka merenja je prosleđivanje saobraćaja preko konekcije koja ima vezu sa Internetom.

Promenom parametra učestalosti slanja ICMP zateva sa graničnih rutera ka IP adresama na Internetu pomoću kojih proveravamo status ISP1 i ISP2 menjamo i brzinu detekcije otkaza i brzinu tranzicije saobraćaja sa jedne na drugu konekciju. I ovde, kao i u predhodnom primeru uzećemo četiri vremenska intervala učestalosti slanja ICMP paketa kojima se proverava komunikacija sa Internetom. To su intervali od 2, 5, 10 i 15 sekundi. U tabeli II predstavljeni su dobijeni rezultati za svako od deset pojedinačnih merenja.

TABELA II. VREMENA TRANZICIJE U KONFIGURACIJI SA DVA GRANIČNA RUTERA

	Učestalost slanja (s)			
Broj merenja	**2**	**5**	**10**	**15**
1.	*4*	*4*	*7*	*5*
2.	*3*	*5*	*11*	*19*
3.	*6*	*4*	*5*	*13*
4.	*2*	*6*	*9*	*16*
5.	*5*	*4*	*3*	*6*
6.	*2*	*5*	*6*	*11*
7.	*4*	*3*	*10*	*9*
8.	*6*	*6*	*7*	*17*
9.	*3*	*2*	*12*	*14*
10.	*4*	*7*	*5*	*8*

Analizom dobijenih rezultata i izračunavanjem prosečnih vrednosti koje su prikazane na Sl.5, dolazimo do toga da se vrednosti dosta razlikuju od onih koje su teoretski očekivane. Zavisno od podešenja učestalosti slanja javljaju se i različita odstupanja koja se odražavaju na brzinu tranzicije saobraćaja sa jednog Internet servis provajdera na drugi. Ako uzmemo prosečnu vrednost dobijenih rezultata merenja kada je učestalost slanja ICMP paketa bila podešena na 2 sekunde videćemo da je vremenski interval nakon kog se izvršila tranzicija je za 95% veći u odnosu na učestalost slanja kojom detektujemo otkaz. Povećanjem vremenskog intervala učestalosti slanja Sl. 5 može se uočiti da se ovaj odnos menja pa tako se može zaključiti da su i dobijene prosečne vrednosti manje u odnosu na definisani interval učestalosti slanja ICMP paketa. U slučaju kada IP SLA vrši proveru na svakih 10 sekundi dobijen je najbolji rezultat, tada je prosečna vrednost bila manja za 25% u odnosu na vremenski interval učestalosti slanja. U slučaju kada je učestalost slanja podešena na 15 sekundi prosečna vrednost je bila manja za 22 % u odnosu na vrednost definisane učestalosti slanja. Najpribližniju prosečnu vrednost u odnosu na interval učestalosti slanja dobilo smo u slučaju kada je učestalost slanja bila 5 sekundi. U odnosu na nju dobijena prosečna vrednost je manja za 8 % u odnosu na vrednost definisane učestalosti slanja.



Slika 5. Prosečno vreme tranzicije u konfiguraciji sa dva rutera

V. ZAKLJUČAK

U predhodnim delovima rada analizirana su dva koncepta kojima rešavamo problem otkaza veze sa Internetom. U oba slučaja akcenat je stavljen na automatizaciju oporavka veze sa Internetom ukoliko dođe do otkaza jedne od konekcija.U oba slučaja zarad podizanja stepena otpornosti na otkaz pribegli smo dupliranju resursa, tj kreiranju rezervnog rešenja ukoliko kod primarnog dođe do zastoja. Osnovna ideja jeste da prikažemo na koji način povećavamo otpornost mreže u slučaju otkaza. Kako je akcenat stavljen na konektivnost lokalne mreže sa spoljnim mrežama, tačnije sa Internetom, osnovni resurs koji smo duplirali jeste redundantna veza sa Internet servis provajderima preko kojih ostvarujemo vezu sa Internetom. Zarad sigurnosti podižemo cenu celokupne mreže zakupom dve zasebne veze sa Internetom preko dva različita Internet provajdera. Iako je jednim linkom sa odgovarajućim propusnim opsegom moguće ostvariti komunikaciju lokalne mreže sa Internetom. Ovakvo rešenje može biti veoma nepouzdano, kada je permanentni pristup Internetu neophodan.

Zakupom dva linka ka Internetu mreža je zaštićena od neplaniranih zastoja u radu Internet provajdera, ali ukoliko imamo samo jedan granični ruter preko koga povezujemo lokalnu mrežu sa Internetom taj ruter predstavlja najkritičnije mesto gde se može desiti otkaz. U slučaju da dodje do otkaza na graničnom ruteru lokalna mreža ostaje bez komunikacije sa Internetom i ako su veze sa Internetom ispravne. Da bi ovakav scenario izbegli kreirali smo mrežnu topologiju sa dva granična rutera, koji u slučaju otkaza automatski preuzimaju ulogu onog koji je van funkcije i samim tim računari iz lokalne mreže imaju stalni pristup Internetu. Kreiranje redundantnih graničnih rutera sa jedne strane povećava cenu same implementacije ovakve računarske mreže, usložnjava konfiguraciju istih, sve u cilju podizanja otpornosti na otkaz celokupnog sistema. Pored cene u materjalnom smislu, za implementaciju složenije konfiguracije moramo uračunati i brzinu tranzicije saobraćaja sa jedne Internet konekcije na drugu.

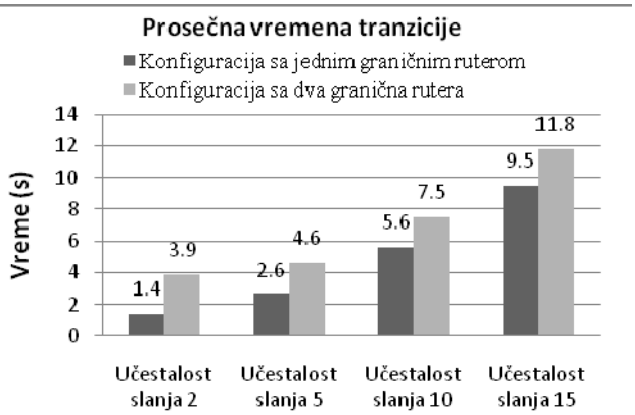
Analizom dobijenih rezultata merenja koja smo sproveli nad obe konfiguracije dolazimo do vremenskog intervala za koji je konfiguracija sa dva granična rutera sporija u odnosu na manje složenu konfiguraciju sa jednim graničnim ruterom. Uporedivši dobijene prosečne vrednosti kada učestalost slanja bila ista možemo zaključiti da se razlika u brzini tranzicije kreće u rasponu od 1,9 sekundi pa do 2,5 sekunde.

U tabeli III prikazane su prosečne vrednosti koje smo dobili nakon merenja u topologiji sa jednim graničnim ruterom i topologiji sa dva granična rutera za isti interval učestalosti slanja. Na osnovu rezultata merenja nameće se zaključak da povećanje otpornosti na otkaz ima svakako i svoju cenu, uvidom u prosečne brzine tranzicije saobraćaja za obe konfiguracije. Može se zaključiti da je kompleksnija konfiguracija sporija za oko 2 sekunde u odnosu na konfiguraciju sa jednim graničnim ruterom. Grafički uporedni prikaz prosečnih vrednosti prikazan je na Sl. 6. Pored cene u brzini koja se mora platiti tu je i veća cena u materjalnom smislu koja je potrebna za nabavku još jednog rutera. Ne sme se zanemariti i da je samo podešavanje dva granična rutera dosta složenije.

TABELA III. UPOREDNI PRIKAZ PROSEČNIH VREDNOSTI REZULTATA MERENJA

Učestalost slanja	Topologija sa jednim graničnim ruterom (s)	Topologija sa dva granična rutera (s)	Razlika prosečnih vrednosti
2	*1,4*	*3,9*	*2,5*
5	*2,6*	*4,6*	*2*
10	*5,6*	*7,5*	*1,9*
15	*9,5*	*11,8*	*2,3*
	Prosečna vrednost		**≈2,175**

Na osnovu analiza ne može se izvući konkretan zaljučak koja od ove dve topologije predstavlja univerzalno bolje rešenje jer oba rešenja nose svoje prednosti i nedostatke. Nedostatak konfiguracije sa jednim graničnim ruterom je taj što postoji jedna tačka u mreži preko koje se odvija sva komunikacija sa Internetom, a prednost je svakako veća brzina tranzicije saobraćaja sa jednog Internet provajdera na drugi i sama cena implementacije. Dok kod topologije sa dva granična rutera usled redundantnosti uređaja i linkova ka Internetu, otpornost na otkaz je na daleko višem nivou, ali je i cena same implementacije daleko veća.



Slika 6. Prikaz prosečnih vrednosti tranzicije

LITERATURA

[1] D. Kostić, D. Stefanović, D. Blagojević, "Otpornot konekcije na otkaz praćenjem objekata na Internetu", Zbornik radova konferencije "YU INFO 2012" Kopaonik, pp. 359-364

[2] W. Odom, "CCNP Route 642-902 Official Certification Guide", Cisco Press 2010, Cisco Systems, INC., pp.372-381

[3] "Cisco IOS IP SLAs Configuration Guide", Cisco Systems, Inc., 2008

[4] "Cisco IOS IP Service Level Agreements – White paper", Cisco Systems, Inc., 2005

[5] W. Odom, "CCNA Official Exam Official Certification Guide, Second Edition", Cisco Press 208, Cisco Systems, INC., pp.158-196

[6] W. Odom, "CCNP Route 642-902 Official Certification Guide", Cisco Press 2010, Cisco Systems, INC., pp.366-371

[7] W. Odom, "CCNA Official Exam Official Certification Guide, Second Edition", Cisco Press 208, Cisco Systems, INC., pp.231-266

[8] W. Odom, “CCNA Official Exam Official Certification Guide, Second Edition”, Cisco Press 208, Cisco Systems, INC., pp.549-572

[9] “PBR support for Multiple Tracking Option”, Cisco Systems, Inc., 2008

[10] W. Odom, R. Healy, D. Donohue, “*CCIE Routing and Switching Certication Guide, Fourth Edition”* Cisco Press 2010, Cisco Systems, INC., pp.201-206

ABSTRACT

In this paper we show how the integration of several Cisco solutions can make a connection to the Internet more resistant to failure. If you have two connections to the Internet in case of cancellation, all traffic is routed on one that was active at that moment. This is achieved by monitoring the status of these connections. In case when both are active we balance traffic on both connection. In addition, measurement shall effect, how long it takes to continue to the traffic goes through one link and that the recovery time connection. We will study how to change frequency that follow the object changes during recovery.

RESISTANCE CONNECTION TO FAILURE BY TRACKING OBJECTS ON INTERNET IN THE PRESENCE OF A REDUNDANT GATEWAY

Dimitrije Kostić, dr Dušan Stefanović, dr Dejan Blagojević