

Uporedne karakteristike STP i PVST protokola

Saša Dulović, Dušan Stefanović, Prof. dr Dejan Blagojević

Savremene računarske tehnologije
Visoka tehnička škola strukovnih studija
Niš, Srbija

sasa.dulovic@gmail.com, dusan.stefanovic@vtsnis.edu.rs, dejan.blagojevic@vtsnis.edu.rs

Sadržaj—Upoređujući karakteristike STP i PVST protokola biće pokazane prednosti i nedostaci oba protokola i utvrdiće se koji od njih je pogodniji za korišćenje u LAN mrežama. Pošto PVST protokol formira zasebnu STP instancu za svaku VLAN mrežu, to će povećati opterećenje mreže slanjem BPDU poruka za svaku STP instancu. Klasičan STP formira zajedničku instancu za sve VLAN mreže. Uzimajući u obzir 1, 5, 10, 50 i 100 VLAN mreža, veličinu BPDU poruke i učestanost slanja, pokazuje se da je uticaj povećanja BPDU saobraćaja zanemarljiv. Na drugom primeru biće prikazano kako se konfiguriše PVST protokol da bi se koristili svi linkovi u mreži i omogućilo paralelno korišćenje redundantnih veza. Konfiguracija, STP logička stabla i raspodela saobraćaja biće prikazani na primeru redundantne mreže kroz simulaciju u programu Cisco Packet Tracer.

Ključne reči – STP; PVST; spanning tree; BPDU; VLAN;

I. UVOD

Kako bi mrežna infrastruktura bila što pouzdanija, u njen dizajn se uključuju dodatne veze i uređaji. Redundantnost mreže omogućava da mreža radi i u slučaju otkaza pojedinih veza u njoj. Redundantnost ima i lošu stranu, jer se u slučaju više konekcija između svičeva mogu pojaviti problemi u radu mreže. Može doći do dodatnog opterećenja mreže i usporenja saobraćaja zbog slanja više kopija istog frejma. Može se desiti da kada svič dobije isti frejm na različitim prenosnim portovima, dođe do zabune u tabeli sa MAC (eng. Media Access Control) adresama i do njenog neprestanog ažuriranja. Ova pojava je poznata kao nestabilnost (eng. Thrashing) MAC tabele [1]. Može doći i do pojave višestrukih petlji i emisionih oluja, kada dolazi do beskonačnog kruženja poruka kroz mrežu.

Razvijen je protokol koji rešava pomenute probleme, to je STP (eng. Spanning Tree Protocol). STP je standardizovan kao IEEE802.1D. Protokol funkcioniše na sloju dva. [2]

Postoji nekoliko varijanti STP protokola [3]:

a) PVST (eng. Per VLAN Spanning Tree) protokol koji je razvio Cisco.

b) RSTP (eng. Rapid Spanning Tree Protocol) standardizovan kao IEEE802.1w. Ovaj protokol omogućava znatno bržu konvergenciju posle promene topologije mreže. Za razliku od STP protokola kome je za konvergenciju potrebno od 30 do 50 sekundi RSTP je potrebno do 6 sekundi. Svaki svič generiše Hello BPDU (eng. Bridge Protocol Data Unit) poruke, a kada na nekom portu izostane ta poruka, smatra se da je veza prekinuta.

c) MSTP (eng. Multiple Spanning Tree Protocol) je standardizovan kao IEEE 802.1s. Primenom MSTP administrator grupiše VLAN mreže i za svaku grupu se definiše po jedna STP instanca, što omogućava ravnomerniju raspodelu saobraćaja.

Posle objašnjenja kako STP protokol rešava problem redundantnih veza i stvaranja petlji upoređićemo osnovni STP protokol i PVST protokol.

II. SPANNING TREE PROTOCOL

Da bi mreža sa redundantnim vezama funkcionisala, topologija prosljeđivanja frejmova mora biti u obliku stabla (eng. spanning tree). Osnovni cilj je upravo stvaranje logičke topologije stabla. Portovi stabla se stavljaju u stanje prosljeđivanja (eng. forwarding), dok se portovi koji zatvaraju petlje blokiraju (eng. blocking). STP nadgleda mrežu da bi pronašao sve veze i sprečava pojavu petlji blokiranjem redundantnih veza. STP koristi spening tri algoritam (eng. Spanning Tree Algorithm) koji gradi logičku strukturu stabla od korena (eng. root) do svih čvorova u mreži.

III. NAČIN RADA STP PROTOKOLA

Prvo što STA algoritam uradi je da odredi koji svič će biti na vrhu stabla (eng. Root Bridge). Kada se odredi, ovaj svič postaje centralna tačka i u odnosu na njega se donose sve dalje odluke. Rut bridž će biti onaj koji ima najmanju vrednost bridž ID (eng. Bridge ID). Bridž ID je deo BPDU poruke, dug je 8 bajtova i sadrži prioritet sviča i njegovu MAC adresu [2]. Kao osnovni svič se bira onaj sa najmanjim konfiguracionim prioritetom, a ukoliko postoji više svičeva koji imaju isti prioritet, onda se bira onaj sa najmanjom MAC adresom. Po standardnom podešavanju, na svim Cisco svičevima prioritet je postavljen na 32.768. Često je potrebno ručno konfigurisati rut svič u mreži, jer za rut svič treba postaviti onaj koji je ključni u mreži i time uticati na brzinu kojom će STP vršiti konvergenciju. Bridž ID se može promeniti tako što se izmeni prioritet. Snižavanjem prioriteta svič će postati rut bridž. Svi portovi na rut bridžu se stavljaju u stanje prosljeđivanja.

Svičevi međusobno razmenjuju BPDU poruke. Ove poruke sadrže informacije koje se koriste za izbor rut sviča i STP konfiguraciju mreže. Podrazumevano, BPDU poruke se razmenjuju svake dve sekunde [4] čime se omogućava da svičevi prate promene u mreži i reaguju na njih. BPDU poruka sadrži: jedinstveni bridž ID sviča koji je identifikovan kao rut svič; STP cenu linka do rut bridža; bridž ID sviča; message

age; identifikator interfejsa pošiljaoca; vrednosti tajmera – hello, forward-delay, max-age.

Sledeći korak je određivanje stanja portova. Portovi mogu biti u jednom od pet stanja [3]:

- **Blokiranje** – port ne učestvuje u prosleđivanju frejmova, osluškiju se BPDU poruke. Po standardnom podešavanju, svi portovi su u blokiranom stanju kada se svič uključi.
- **Osluškivanje** (eng. listening) – ovo je prvo tranziciono stanje nakon stanja blokiranja dok STP ne utvrdi da li port treba da učestvuje u prosleđivanju frejmova. Port osluškuje. Traje 15 sekundi.
- **Učenje** (eng. learning) – port se priprema za učešće u prosleđivanju frejmova. Port osluškuje BPDU i popunjava tabelu MAC adresa. Traje 15 sekundi.
- **Prosleđivanje** – port prosleđuje i prima frejmove podataka. Port ulazi u stanje prosleđivanja ako je na kraju stanja učenja: rut ili namenski.
- **Neaktivnost** (eng. disabled) – port ne učestvuje u STP jer je isključen.

Prvo se biraju rut portovi (RP). Svaki svič, koji nije rut, mora imati tačno jedan rut port i to će biti onaj koji ima najmanju cenu putanje (eng. path cost) do rut bridža. Cena putanje je zbir vrednosti cena svih linkova na putanji do rut bridža. Cena porta se računa prema propusnom opsegu (Tabela I) [4]. Svaki RP se stavlja u stanje prosleđivanja.

TABELA I. CENA LINKA PREMA PROPUSNOM OPSEGU

Propusni opseg	Cena linka	
	nova IEEE specifikacija	stara IEEE specifikacija
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

Dalje, određuju se namenski (eng. designated) portovi (DP) na svakom segmentu, to je port koji oglašava najmanju cenu do rut bridža. Ovim portovima je dopušteno prosleđivanje.

Svi preostali portovi će biti blokirani portovi (BP) i stavljaју se u stanje blokiranja. U Spanning-Tree mreži postoji jedan rut bridž, po jedan rut port za svaki svič koji nije rut i po jedan namenski port za svaki segment.

Portovi se kreću kroz sledeća stanja: inicijalizacija – blokiranje, blokiranje – osluškivanje (ili neaktivnost), osluškivanje – učenje (ili neaktivnost), učenje – prosleđivanje (ili neaktivnost), prosleđivanje – neaktivnost, neaktivnost – blokiranje.

Portovi su najčešće u stanju blokiranja ili u stanju prosleđivanja. Ukoliko u mreži dođe do promena zbog otkaza, ili iz nekog drugog razloga, portovi na svičevima će biti u stanju osluškivanja i učenja dok se ne odrede najbolje putanje do rut bridža. Za STP rekalkulaciju i konvergenciju iz stanja

blokiranja u stanje prosleđivanja obično je potrebno 50 sekundi. Vreme za detekciju gubitka BPDU i prelaska iz stanja blokiranja u stanje osluškivanja (maximum-aging time) – 20 sekundi, kašnjenje prosleđivanja (forward delay) pri prelasku iz stanja osluškivanja u stanje učenja – 15 sekundi i pri prelasku iz stanja učenja u stanje prosleđivanja – 15 sekundi.

A. Prednosti i nedostaci

Protokol STP je kreirao logičku topologiju stabla i na taj način sprečio pojavu petlji u mreži i omogućio da mreža funkcioniše. Topologija stabla se kreira blokiranjem određenih portova, što znači da postoje neaktivne veze. Te veze služe kao rezerva i mogu se aktivirati u slučaju da dođe do otkaza ili promene topologije mreže i to samo ukoliko se STP rekalkulacijom portovi koji su na tim vezama označe kao rut ili namenski. Znači, postoje pasivni elementi u mreži koji možda nikada neće biti aktivirani. Sa stanovišta iskorišćenosti mreže, bilo bi dobro da su svi resursi mreže aktivni. Aktiviranjem svih resursa mreže (linkova) izvršice se raspodela saobraćaja (eng. load balancing). Ukoliko dođe do otkaza, redundantne veze će nastaviti da vrše svoju funkciju i cela mreža će i dalje funkcionisati.

Standard definiše jednu STP instancu za celu mrežu. STP protokol ne uzima u obzir VLAN mreže, pa je logička topologija koju pravi STP jedinstvena za sve kreirane VLAN mreže. Pošto se koristi samo jedna STP instanca, to se samo za nju na svake 2 sekunde šalju BPDU poruke, bez obzira koliko ima VLAN mreža, što omogućava optimalno korišćenje procesora.

IV. PVST PROTOKOL

PVST protokol se zasniva na IEEE802.1D standardu i Cisco vlasničkim ekstenzijama [5]. Glavna odlika ovog protokola je da se za svaku VLAN mrežu kreira zasebna STP instanca. To omogućava da se kreiraju zasebne logičke topologije za različite VLAN mreže čime se omogućava korišćenje svake veze u mreži i obezbeđuje ravnomernija raspodela saobraćaja. Za svaku VLAN mrežu možemo imati poseban rut svič. Rut svič šalje STP informacije u vezi sa tom VLAN mrežom svakom sviču u mreži. Na taj način svaki svič u mreži ima iste informacije o mreži čime se osigurava održanje topologije.

VLAN (eng. Virtual Local Area Network) [2] je logička grupa uređaja ili njihovih korisnika kreirana prema zajedničkoj funkciji, odeljenju ili aplikaciji – nezavisno od njihove fizičke lokacije. Korišćenjem VLAN mreža pojednostavljuje se upravljanje mrežom, povećava se sigurnost u mreži, a smanjuje zauzimanje propusnog opsega u mreži. VLAN1 mreža je administrativna i svi portovi na sviču su članovi te mreže. Svaki VLAN mora imati sopstveni broj IP mreže. Komunikacija između čvorova koji se nalaze u različitim VLAN mrežama ide kroz uređaj sloja tri, odnosno ruter ili lejer 3 svič.

IEEE802.1Q [6] standard definiše kako se informacije o VLAN mrežama razmenjuju između mrežnih uređaja. Ovaj standard ubacuje dodatna četiri bajta u VLAN zaglavlje originalnog okvira ethernet hедера. Prvih 16 bita identifikuje okvir da je IEEE802.1Q označen okvir (Tag Protocol Identifier – TPID). Sledeća tri bita označavaju prioritet kojim se može

dati prednost određenoj klasi saobraćaja, npr. prenosu glasa. Sledeći bit se koristi za kompatibilnost Ethernet i Token Ring mreža. Na kraju je polje od 12 bita koje sadrži kojoj VLAN mreži okvir pripada. Može se označiti do 4094 VLAN mreža.

PVST protokol omogućava aktiviranje svih linkova u mreži, a time i maksimalno iskorišćenje resursa mreže. Pošto se formira posebna STP instanca za svaku VLAN mrežu, isti port može biti podešen da za jednu VLAN mrežu bude u stanju prosleđivanja, a za drugu VLAN mrežu bude u stanju blokiranja. Ovim se omogućuje paralelno korišćenje redundantnih linkova. Ukoliko dođe do otkaza ili promene topologije, vrši se STP rekalkulacija za svaku instancu posebno i uspostavlja nova logička topologija za svaku VLAN mrežu.

BPDU poruke se generišu za svaku VLAN mrežu posebno, što povećava saobraćaj u mreži i povećava opterećenje procesora. Obzirom da ethernet mreže omogućavaju veliki protok (100Mbps) očekuje se da neće doći do značajnog povećanja saobraćaja i opterećenja mreže bez obzira na generisanje velikog broja BPDU.

V. BPDU I OPTEREĆENJE MREŽE

Ispituje se na koji način povećanje broja VLAN mreža utiče na povećanje saobraćaja u mreži. Cilj je da se utvrdi koliko povećanje broja BPDU poruka povećava zauzetost propusnog opsega mreže i gde je gornja granica broja VLAN mreža za koje bi trebalo koristiti PVST protokol. Za primer, koristi se 1 VLAN, 5 VLAN, 10 VLAN, 50 VLAN i 100 VLAN mreža. Uzima se u obzir da se BPDU poruke po podrazumevanom podešavanju šalju na svake 2 sekunde. Format BPDU poruke prikazan je u tabeli (Tabela II). Iz tabele se vidi da je BPDU poruka veličine 35 bajtova [7].

TABELA II. STRUKTURA BPDU PORUKE

BPDU polje	broj bajtova	BPDU polje	broj bajtova
Protocol ID	2	Version ID	1
Type BPDU	1	Flags	1
Root Bridge ID	8	Root Path Cost	4
Sender Bridge ID	8	Port ID	2
Message Age	2	Max Age	2
Hello Time	2	Forward Delay	2

Sada se može izračunati koliko povećanje broja BPDU poruka povećava saobraćaj i opterećenje mreže. Uzimajući u obzir navedenu veličinu BPDU paketa i učestanost slanja, a obzirom na broj VLAN mreža, dobija se ostvareni BPDU saobraćaj što je i prikazano u tabeli (Tabela III).

TABELA III. OSTVARENI BPDU SAOBRAĆAJ

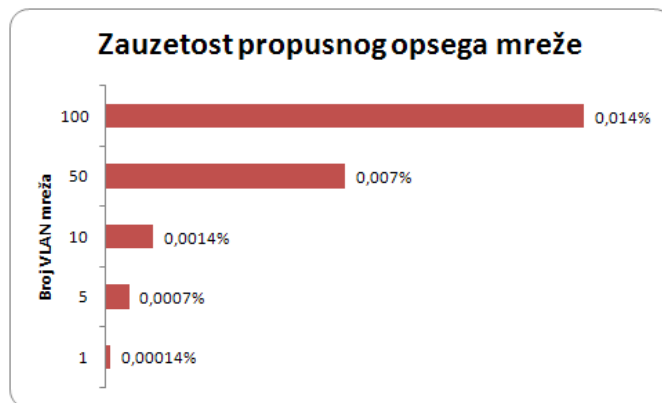
Broj VLAN mreža	Ostvareni BPDU saobraćaj		
	bps	Kbps	Mbps
1	140	0.14	0.00014
5	700	0.7	0.0007
10	1400	1.4	0.0014

Broj VLAN mreža	Ostvareni BPDU saobraćaj		
	bps	Kbps	Mbps
50	7000	7	0.007
100	14000	14	0.014

Pošto je izračunat BPDU saobraćaj u odnosu na broj VLAN mreža, moguće je prikazati koliko propusnog opsega 100Mbps mreže zauzima taj protok. Pregled vrednosti je dat u tabeli (Tabela IV), dok je grafički prikaz dobijenih vrednosti predstavljen na Sl. 1.

TABELA IV. ZAUZETOST PROPUSNOG OPSEGA MREŽE

Broj VLAN mreža	Brzina protoka u mreži (Mbps)	
	10	100
1	0.0014%	0.00014%
5	0.007%	0.0007%
10	0.014%	0.0014%
50	0.07%	0.007%
100	0.14%	0.014%



Slika 1. Percentualni prikaz zauzetosti propusnog opsega 100Mbps mreže u odnosu na broj VLAN mreža

Kao što se i očekivalo, dobijene vrednosti potvrđuju da PVST protokol ne utiče bitno na povećanje ukupnog saobraćaja u mreži, čak i kada ima 100 VLAN mreža i kada je propusni opseg mreže 10Mbps. Činjenica da savremene mreže imaju minimalni propusni opseg od 100Mbps dodatno smanjuje uticaj BPDU saobraćaja na zauzetost propusnog opsega.

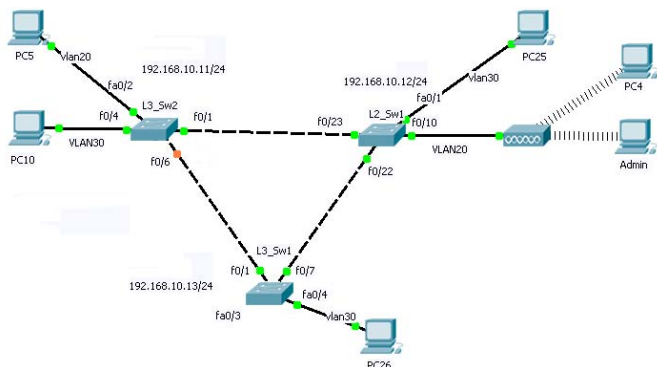
VI. PRAKTIČNI PRIMERI KONFIGURACIJE STP I PVST-A

Za prikazivanje konfiguracije PVST protokola korišćen je Packet Tracer i u njemu formirana mreža sa redundantnim linkovima. Topologija mreže prikazana je na Sl.2.

a) Simulator Cisco Packet Tracer

Simulator je razvijen od strane Cisco kompanije. U programu je na raspolaganju raznovrsna oprema koja se u simulatoru ponaša skoro identično kao u stvarnosti. Packet Tracer omogućuje kreiranje mrežne topologije i pristupanje aktivnim mrežnim uređajima preko grafičkog interfejsa (eng. Graphic User Interface). Svičevi i ruteri se konfiguriraju kroz

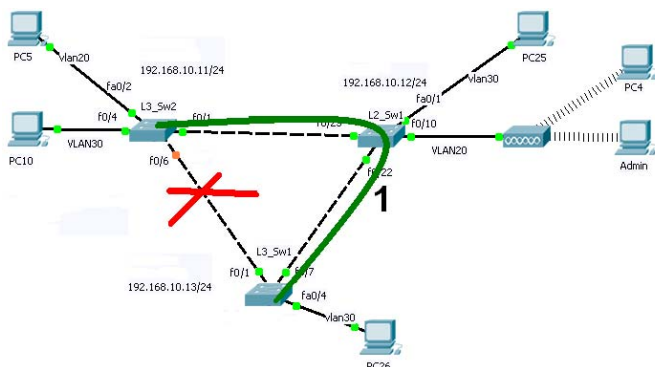
simuliranu verziju Cisco operativnog sistema (Cisco IOS). Simulator može raditi u realnom i simulacionom modu. U simulacionom modu se analizira funkcionalnost mreže praćenjem putanje paketa uz podešavanje različitih filtera. Kod simulacije u realnom vremenu se ne vidi putanja paketa, vidi se samo da li je paket stigao ili nije.



Slika 2. Osnovna topologija mreže

b) STP i Load Balancing

Već na slici sa osnovnom topologijom mreže vidi se da su neki portovi blokirani. To je zbog toga što je STP protokol po podrazumevanim podešavanjima uključen. Čim je mreža konfigurisana i postala funkcionalna, STP protokol je obavio svoj deo posla i formirao logičku topologiju stabla blokirajući port fa0/6 na sviču L3_Sw2. Logičko stablo i blokirani port su prikazani na Sli.3.



Slika 3. STP logička topologija stabla

Simulacioni mod Packet Tracer-a se koristi za praćenje putanje paketa između matičnih računara PC10 i PC26 koji se nalaze u VLAN30 mreži. U Event List tabeli (Sl.4.) je prikazan redosled svičeva kroz koje prolaze paketi. Kao što se vidi, putanja se poklapa sa logičkim stablom.

Slika oka u prvoj koloni prikazuje trenutnu poziciju paketa, dok druga kolona prikazuje proteklo vreme. Sledeće kolone prikazuju uređaje koji šalju i primaju paket u datom koraku i tip paketa. Klikom na obojeni kvadrat u koloni info otvara se prozor sa detaljnim prikazom sadržaja paketa.

Simulacija komunikacije bilo koja dva uređaja iz mreže pokazuje istu putanju. Raspodela saobraćaja u ovom slučaju nije omogućena. Blokirani je isti port za sve VLAN mreže, tako da saobraćaj iz svih VLAN mreža ide istim logičkim stablom.

Vis.	Time (sec)	Last Device	At Device	Type
0.000	--	--	PC 10	ICMP
0.001	0.001	PC 10	L3_Sw2	ICMP
0.002	0.002	L3_Sw2	L2_Sw1	ICMP
0.003	0.003	L2_Sw1	L3_Sw1	ICMP
0.004	0.004	L3_Sw1	PC26	ICMP
0.005	0.005	PC26	L3_Sw1	ICMP
0.006	0.006	L3_Sw1	L2_Sw1	ICMP
0.007	0.007	L2_Sw1	L3_Sw2	ICMP
0.008	0.008	L3_Sw2	PC 10	ICMP

Slika 4. Event lista simulacionog moda PT – komunikacija PC10 i PC26

c) PVST protokol i Load Balancing

Da bi se aktivirale sve veze u mreži, koristi se svojstvo PVST protokola da kreira posebnu instancu za svaku VLAN mrežu. Svičevi se konfigurisu tako da saobraćaj za mreže VLAN10 i VLAN20 ide preko sviča L3_Sw1, a za VLAN30 i VLAN40 preko sviča L3_Sw2. Za prikazanu topologiju mreže, željeni efekat se postiže tako što se svič L3_Sw1 definiše kao rut svič za mreže VLAN10 i VLAN20, a L3Sw2 kao rut svič za mreže VLAN30 i VLAN40.

Svičevi se konfigurisu komandama:

```
L3_Sw1(config)#spanning-tree vlan 10,20 root primary
```

```
L3_Sw2(config)#spanning-tree vlan 30,40 root primary
```

Ono što se primećuje u simulatoru je da su svi portovi postali aktivni. To ne znači da su svi portovi aktivni za sve VLAN mreže. Kao što je već rečeno, neki portovi su za određene mreže aktivni, dok su za druge blokirani.

Komandom: `L2_Sw1#show spanning-tree active`

prikazuje se status portova na sviču u odnosu na aktivne VLAN mreže. Konfigurisanjem rut svičeva postignuto je da se za VLAN10 i VLAN20 blokira port fa0/23 na sviču L2_Sw1, dok se za VLAN30 i VLAN40 blokira port fa0/22 na istom sviču. Simulacijom saobraćaja u mrežama VLAN20 (PC4 – PC5) i VLAN30 (PC25 – PC26), dobijaju se Event List tabelle iz kojih se vidi da saobraćaj u VLAN20 mreži ide preko sviča L3_Sw1 (Sl.5.), a u VLAN30 mreži ide preko sviča L3_Sw2 (Sl.6.).

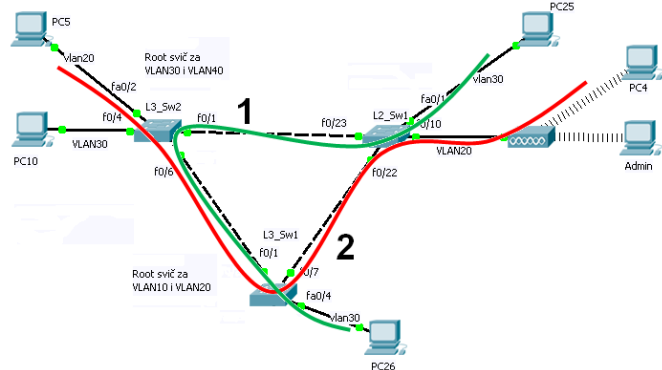
Vis.	Time (sec)	Last Device	At Device	Type	Info
0.000	--	--	PC 4	ICMP	
0.005	--	--	PC 4	ICMP	
0.006	0.006	PC 4	Wireless_AP VLAN20	ICMP	
0.007	0.007	Wireless_AP VLAN20	L2_Sw1	ICMP	
0.008	0.008	L2_Sw1	L3_Sw1	ICMP	
0.009	0.009	L3_Sw1	L3_Sw2	ICMP	
0.010	0.010	L3_Sw2	PC5	ICMP	
0.011	0.011	PC5	L3_Sw2	ICMP	
0.011	0.011	--	Wireless_AP VLAN20	ICMP	

Slika 5. Komunikacija računara PC4 i PC5 iz VLAN20 mreže

Vis.	Time (sec)	Last Device	At Device	Type	Info
0.000	--		PC25	ICMP	
0.001		PC25	L2_Sw1	ICMP	
0.002		L2_Sw1	L3_Sw2	ICMP	
0.003		L3_Sw2	L3_Sw1	ICMP	
0.004		L3_Sw1	PC26	ICMP	
0.005		PC26	L3_Sw1	ICMP	
0.006		L3_Sw1	L3_Sw2	ICMP	
0.007		L3_Sw2	L2_Sw1	ICMP	
0.008		L2_Sw1	PC25	ICMP	

Slika 6. Komunikacija računara PC25 i PC26 iz VLAN30 mreže

Upoređujući putanje paketa uočava se da paketi iz VLAN20 i VLAN30 mreže idu različitim logičkim stablima kao što je i očekivano. Ispitivanjem kretanja paketa u mrežama VLAN10 i VLAN40 utvrđuje se da VLAN10 ima isto logičko stablo kao VLAN20, a VLAN40 kao VLAN30 mreža. Na Sl.7 su prikazana logička stabla za sve mreže. Putanja paketa u VLAN 30 i 40 mrežama označena je brojem 1, dok je putanja paketa u VLAN 10 i 20 mrežama označena brojem 2.



Slika 7. Dve logičke topologije stabla za VLAN20 i VLAN30

VII. ZAKLJUČAK

Kada se sumiraju sva razmatranja i merenja, može se zaključiti da STP protokol rešava problem redundantnih mreža, tj. pojave beskonačnih petlji i emisionih oluja, ali ne rešava problem raspodele saobraćaja. STP protokol formira jedno logičko stablo bez obzira na broj VLAN mreža, što znači da sav saobraćaj ide samo aktivnim linkovima stabla, dok će blokirani portovi i linkovi biti pasivni i neiskorišćeni i imaju ulogu jedino u slučaju otkaza u mreži.

PVST protokol formira posebno logičko stablo za svaku VLAN mrežu. Takvo svojstvo PVST protokola omogućava paralelno korišćenje redundantnih linkova, što znači da će svi resursi biti aktivni i da će se postići raspodela saobraćaja. To što omogućava raspodelu saobraćaja daje prednost ovom protokolu u odnosu na standardni STP.

Kroz primer je pokazano da konfiguracija PVST nije komplikovana. Pokazano je i da povećan obim slanja BPDU poruka ne utiče bitno na povećanje ukupnog protoka kroz mrežu. Kada se koristi 100 VLAN mreža, zauzetost protoka 10Mbps mreže je 0,14% što je zanemarljivo. U ovom merenju nije uzet u obzir uticaj povećanog broja BPDU poruka na opterećenost procesora.

Ukoliko postoji veći broj VLAN mreža, dešava se da se logičke topologije poklapaju. To znači da saobraćaj za više VLAN mreža ima istu logičku topologiju. Bez obzira na to, BPDU poruke se i dalje šalju za svaku VLAN mrežu posebno.

Treba napomenuti da je Cisco kreirao PVST protokol i da ga ne podržavaju svi proizvođači opreme. Da bi uspešno implementirali ovaj protokol poželjno je da su svi uređaji proizvođača Cisco.

LITERATURA

- [1] Kevin Wallace, "CCNP TSHOOT 642-832 Official Certification Guide", Cisco Press 2010, Cisco Systems, INC.,
- [2] Todd Lammle, "CCNA: Cisco Certified Network Associate Study Guide, Third Edition", Cisco Press 2005, Cisco Systems, INC.,
- [3] Richard Froom, Balaji Sivasubramanian, Erum Frahim, "Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide", Cisco Press 2010, Cisco Systems, INC.,
- [4] W. Odom, "CCNA Official Exam Official Certification Guide, Second Edition", Cisco Press 2008, Cisco Systems, INC., pp.549-572
- [5] W. Odom, R. Healy, D. Donohue, "CCIE Routing and Switching Certification Guide, Fourth Edition", Cisco Press 2010, Cisco Systems, INC., pp.201-206
- [6] <http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf> (pristup: januar, 2012.)
- [7] http://www.cisco.com/en/US/tech/tk870/tk136/tk885/technologies_tech_note09186a0080093cc6.shtml (pristup: januar, 2012.)

ABSTRACT

Comparing the characteristics of STP and PVST protocols will be shown the advantages and disadvantages of both protocols and determine which of them is suitable for use in LAN networks. Since PVST protocol create a separate STP instance for each VLAN, sending BPDU for each STP instance of the network load increases. Standard STP creates only one common STP instance for all Vlans. Taking into account the 1, 5, 10, 50 and 100 VLANs, BPDU size and frequency of sending BPDU messages, will be shown that the impact of increasing BPDU traffic is negligible. In the second example, will be shown how to configure the PVST protocol to be used by all links in the network and allow parallel use of redundant links. Configuration, STP logical tree and load balancing will be shown in the example of redundant networks through simulation in Cisco Packet Tracer.

COMPARATIVE CHARACTERISTICS OF STP AND PVST PROTOCOLS

Saša Dulović, Dušan Stefanović, Dejan Blagojević