

Analiza i rješavanje problema broadcast storm u lokalnoj mreži

Puceković, Kristijan

Undergraduate thesis / Završni rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: <https://urn.nsk.hr/urn:nbn:hr:119:482747>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-11-04**



Repository / Repozitorij:

[Faculty of Transport and Traffic Sciences - Institutional Repository](#)



Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, Zagreb

ZAVRŠNI RAD

ANALIZA I RJEŠAVANJE PROBLEMA BROADCAST STORM U LOKALNOJ MREŽI

ANALYSIS AND RESOLUTION OF PROBLEM WITH BROADCAST STORM IN LOCAL NETWORK

Mentor: doc. dr. sc. Ivan Grgurević

Student: Kristijan Puceković
JMBAG: 0135245475

Zagreb, srpanj 2020.

SAŽETAK

U modernom svijetu, zbog obavljanja poslovnih ili privatnih obaveza, ključno je ostati stalno povezan na Internet. U tu svrhu se osiguravaju redundantne (rezervne) veze kako bi korisnici i u slučaju pada primarne veze ili uređaja ostali povezani. U radu je analizirana problematika koja se javlja prilikom pogrešne implementacije redundantnih veza, a to je nastanak petlji drugog sloja koje dovode do stanja mreže pod nazivom *broadcast storm*. Simulacijom je prikazano zašto je važno poznavanje te problematike i do čega ona dovodi te u konačnici kako je spriječiti. Kako bi se mogao spriječiti *broadcast storm*, važno je razumjeti njezin nastanak. Sukladno tome, opisano je broadcast odašiljanje, na koji način radi preklopnik te proces nastajanja petlji drugog sloja koje dovode do *broadcast storm-a*. Na kraju, razrađeni su algoritmi i protokoli u svrhu njezinog sprječavanja.

Ključne riječi: lokalna mreža, *broadcast storm*, redundancija, broadcast odašiljanje

SUMMARY

In the modern world, due to performing business or private obligations it is very important to constantly stay connected to the internet. For that purpose, redundant (backup) links are provided so that users remain connected even in a case of failure of primary link or device. This paper analyzes the problem that occurs in the event of wrong implementation of redundant links, and that is formation of layer two loops that lead to broadcast storm. The simulation shows why it is important to understand this problem, what it leads to and ultimately how to prevent it. In order to prevent a broadcast storm, it is important to understand its occurrence. Accordingly, broadcasting is described, how the switch works and the process of forming layer two loops. Finally, algorithms and protocols that are developed for this purpose are elaborated in this paper.

Keyword: local network, broadcast storm, redundancy, broadcasting

Sadržaj:

1. Uvod.....	1
2. Značajke broadcast prometa	3
2.1. Kolizijska domena.....	5
2.2. Broadcast domena	6
2.3. Aplikacije i servisi koji koriste broadcast odašiljanje	8
3. Definiranje problematike <i>broadcast storm</i>	11
3.1. Prikaz rada preklopnika.....	11
3.2. Nastanak <i>broadcast storm</i> -a.....	13
4. Simulacijsko modeliranje <i>broadcast storm</i> -a korištenjem programskog alata Cisco Packet Tracer	17
5. Pregled i korištenje protokola i algoritama u funkciji rješavanja problema <i>broadcast storm</i> ..	23
5.1. STA (engl. <i>Spanning Tree Algorithm</i>)	23
5.2. Kruskalov algoritam.....	24
5.3. STP (engl. <i>Spanning Tree Protocol</i>).....	26
5.3.1. Odabir <i>root bridge</i> -a.....	28
5.3.2. Odabir <i>root port</i> -a	29
5.3.3. Odabir <i>designated port</i> -a.....	30
5.3.4. Odabir alternativnih (blokirajućih) sučelja.....	31
5.3.5. Statusi sučelja na preklopticima	33
5.3.6. STP brojači	33
5.3.7. PortFast.....	34
6. Objašnjenje i razrada tipova STP-a (RSTP, PVST+, MSTP).....	34
6.1. RSTP	35
6.2. PVST	36

6.3. MSTP	37
7. Zaključak.....	39

1. Uvod

U današnjem svijetu, potreba za obavljanjem poslova internetskim putem je neizbježna realnost te isto rezultira napretkom računalnih mreža. Sve veći broj računala i ostalih terminalnih uređaja zahtjeva internetsku povezanost te samim time i raste veličina lokalnih mreža. U lokalnu mrežu se implementira veći broj preklopnika kako bi se svi uređaji povezali. Zbog potrebe za stalnom povezanošću javlja se problematika oko pouzdanosti lokalnih mreža, odnosno u slučaju da pojedina veza ili preklopnik padnu, da ne padne i cijela mreža. S tim ciljem se osiguravaju redundantne (rezervne) veze između preklopnika tako da ako padne glavna veza, promet se može preusmjeriti na rezervnu vezu. Implementacija rezervnih veza je puno kompleksnija od samog fizičkog povezivanja, potrebno je poznavati te implementirati odgovarajuće algoritme i protokole sa svrhom da se ne dogodi upravo suprotna stvar od željene, a to je kolaps cijele lokalne mreže.

Cilj završnog rada je provedba analize i rješavanje problema *broadcast storm* u lokalnoj mreži.. Dok je svrha rada cjelokupni pregled nastanka, stanja i sprječavanja *broadcast storm-a* u lokalnoj mreži.

Rad je sastavljen od sljedećih cjelina:

1. Uvod
2. Značajke broadcast prometa
3. Definiranje problematike *broadcast storm*
4. Simulacijsko modeliranje *broadcast storm-a* korištenjem programskog alata Cisco Packet Tracer
5. Pregled i korištenje protokola i algoritama u funkciji rješavanja problema *broadcast storm*
6. Objašnjenje i razrada tipova STP-a (RSTP, PVST+, MSTP)
7. Zaključak

Prvo poglavlje (Uvod) predstavlja kratki uvod u temu, cilj i svrhu završnog rada.

U drugom poglavlju su opisane značajke broadcast prometa, zašto je važan te su opisane najznačajnije aplikacije koje koriste broadcast odašiljanje.

U trećem poglavlju je prikazano kako se kreiraju petlje drugog sloja koje dovode do stanja *broadcast storm* te kako bi se lakše shvatilo kreiranje petlji, opisan je način rada preklopnika.

Korištenjem Cisco Packet Tracer-a, u četvrtom poglavlju je napravljena simulacija *broadcast storm-a* te ponašanje mreže u takvom stanju.

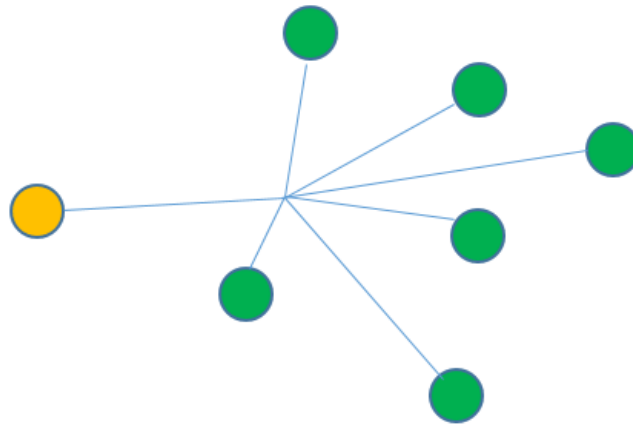
Kako bi se spriječio takav scenarij, u petom poglavlju su razrađeni algoritmi i protokoli koji se implementiraju u svrhu sprječavanja *broadcast storm-a*.

S obzirom na prednosti i nedostatke određenih protokola, ne postoji jedinstveni protokol za sprječavanje *broadcast storm-a*, stoga su u šestom poglavlju razrađeni tipovi protokola koji se mogu koristiti u istu svrhu.

Posljednje poglavlje je Zaključak do kojeg se dolazi na temelju obrade prethodnih poglavlja odnosno postavljenih teza završnog rada.

2. Značajke broadcast prometa

Broadcast odašiljanje u računalnim mrežama je istovremeno slanje iste poruke na više klijenata, odnosno na sve klijente unutar određene mreže. Značajka broadcast poruke je što ne zahtijeva odgovor svih klijenata u mreži već samo od klijenata za koje je ta poruka namijenjena jer prilikom slanja poruke, pošiljalatelj ne stavlja određenu adresu primatelja, kao što je slučaj kod unicast prijenosa¹, nego za odredišnu adresu stavlja *broadcast* adresu. Primjer broadcast odašiljanja je prikazan na slici 1. na kojoj je žutom bojom prikazan pošiljalatelj, a zelenom bojom svi klijenti u mreži. [1]



Slika 1. Broadcast odašiljanje

Izvor: [1]

Razlikujemo broadcast odašiljanje na 2. sloju OSI referentnog modela, sloju podatkovne veze te broadcast odašiljanje na 3. sloju, mrežnom sloju OSI referentnog modela.²

Kod 2. sloja, broadcast promet ostaje u granicama lokalne mreže (engl. *Local Area Network* - LAN), ta granica se još zove *broadcast* domena koja će biti pojašnjena u nastavku.

¹ *Unicast* predstavlja prijenos podataka iz jedne točke u mreži u drugu, odnosno jedan pošiljalatelj i jedan primatelj.

² OSI model (engl. *Open Systems Interconnection*) je slojeviti model koji služi kao preporuka koja olakšava razvoj protokola i komunikacija fokusirajući se na pojedini sloj, neovisno o ostalim slojevima. [34]

Broadcast promet se šalje koristeći najvišu fizičku, MAC (engl. *Media Access Control*) adresu kao određujuću adresu koja iznosi FF:FF:FF:FF:FF:FF. Svi uređaji prepoznaju tu adresu kao *broadcast* adresu te mrežni uređaji 2. sloja poput preklopnika (engl. *switch*) prosljeđuju *broadcast* promet svim ostalim uređajima u broadcast domeni. [2]

Kod broadcast odašiljanja na 3. sloju, broadcast promet se šalje koristeći broadcast adresu mrežnog sloja, IP (engl. *Internet Protocol*) adresu.

Razlikujemo dvije vrste broadcast odašiljanja 3. Sloja:

- Limitirani broadcast (engl. *Limited Broadcast*)
- Usmjereni broadcast (engl. *Directed Broadcast*) [1]

Za limitirano broadcast odašiljanje se koristi određujuća IP adresa 255.255.255.255. Teoretski bi ovaj broadcast bio poslan svim IP adresama koje postoje, međutim, ta adresa služi za broadcast unutar pojedine mreže tako da je određuje unutar mreže u kojoj se broadcast šalje. Usmjernik (engl. router) ne prosljeđuje takve pakete. [1]

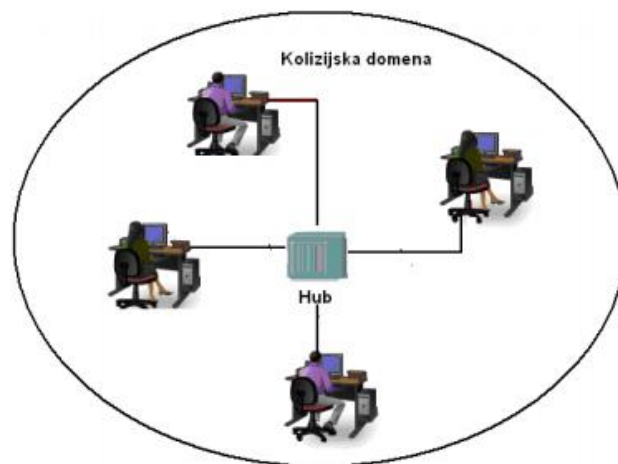
Kod usmjerenog broadcast odašiljanja, svaka mreža ima svoju broadcast adresu te se svi primatelji nalaze unutar te ciljane mreže. Broadcast adresa pojedine mreže je zadnja adresa u adresnom rasponu. Primjerice, mreža 192.168.30.0 s mrežnom maskom 255.255.255.0 odnosno /24 koristi adresu 192.168.30.255 kao broadcast adresu za svoju mrežu. Svi klijenti koji se nalaze unutar 192.168.30.0/24 mreže će zaprimiti broadcast promet 3. sloja, ostali će taj promet odbaciti. Ako određuje nije unutar pošiljačeve (pod)mreže, usmjernik će proslijediti taj promet. [1]

2.1. Kolizijska domena

Kolizijska domena predstavlja Ethernet³ segment unutar kojeg može doći do kolizije. *Ethernet* je koristio CSMA/CD (engl. *Carrier Sense Multiple Access / Collision Detection*) tehniku pristupa dijeljenom mediju koja omogućuje pristup mediju za slanje podataka samo ako je medij dostupan, odnosno nema slanja podataka od drugog klijenta koji se nalazi na tome dijeljenom mediju jer ako dva klijenta šalju podatke istovremeno, dogodi se kolizija te se podaci šalju tek nakon nekog vremena čekanja. [3]

Koristeći CSMA/CD bila je moguća samo poludupleksna (engl. *half-duplex*) komunikacija kod koje je samo jedan klijent u određenoj jedinici vremena mogao slati podatke. [3]

Prvobitne mrežne topologije koje su koristile CSMA/CD su bile topologija zvijezde (engl. *star topology*) i topologija oko centralnog vodiča (engl. *bus topology*). Kod topologije zvijezde je centralni uređaj bio konzentator (engl. *hub*). Hub je mrežni uređaj koji povećava domet pojačavajući signal, ali ujedno i prosljeđuje kolizije. Spajajući više uređaja na konzentator, on povećava kolizijsku domenu. [3] Takva topologija s konzentatorom kao centralnim uređajem je prikazana na slici 2.

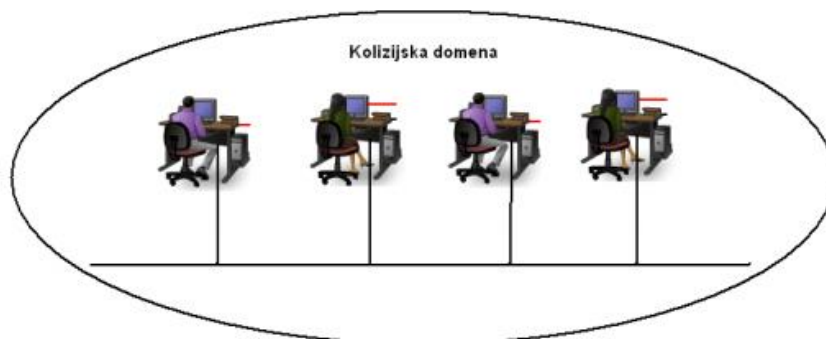


Slika 2. Kolizijska domena koristeći hub

Izvor: [4]

³ *Ethernet* (IEEE 802.3 standard) predstavlja skup mrežno-računalnih tehnologija primjenjenih unutar lokalnih mreža (LAN) [33]

Kod topologije centralnog vodiča klijenti se spajaju na dijeljeni centralni vodič oko kojeg se tvori kolizijska domena, prikaz te topologije je dan na slici 3.



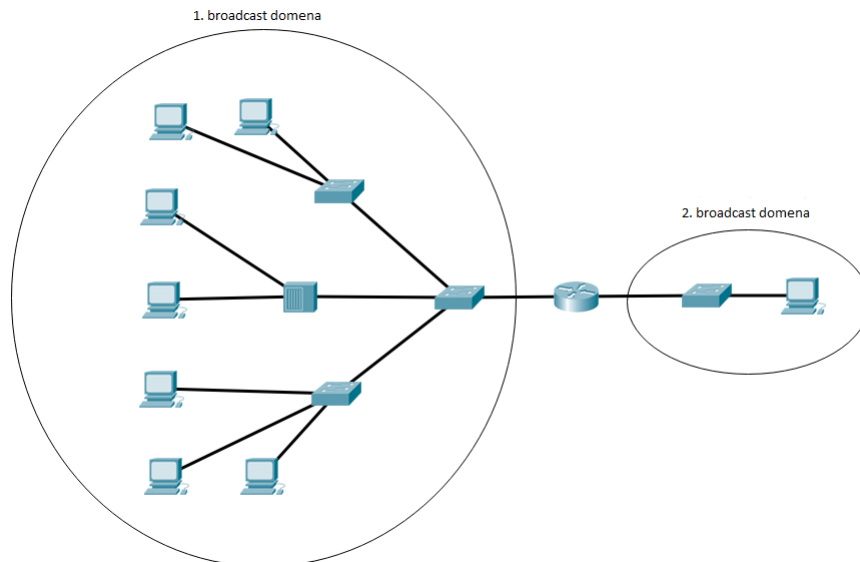
Slika 3. Kolizijska domena topologije centralnog vodiča

Izvor: [4]

Problematika kolizijskih domena je riješena pojavom preklopnika koji izolira kolizijske domene, odnosno svako sučelje na preklopniku predstavlja svoju vlastitu kolizijsku domenu. Također, omogućava puni dupleks (engl. *full-duplex*) komunikaciju. Kod *full-duplexa* oba uređaja mogu istovremeno slati i primiti podatke, a da se ne dogodi kolizija. [3]

2.2. Broadcast domena

Broadcast domena opisuje grupu uređaja na određenom mrežnom segmentu koji mogu doći jedni do drugih putem broadcast odašiljanja, najčešće se radi o lokalnoj mreži. Broadcastovi koji se pošalju u jednoj broadcast domeni se ne prosljeđuju na drugu broadcast domenu. Preklopnici, koncentratori, mostovi (engl. *bridge*) kao uređaji 2. sloja prosljeđuju broadcast promet na sva sučelja osim ulaznog s kojega je promet pristigao. Odnosno, koliko god mrežnih uređaja 2. sloja se spojilo u mreži, broadcast domena se neće razdijeliti već će samo rasti, i dalje će se raditi o jednoj broadcast domeni. Broadcast domene mogu razdijeliti uređaji 3. sloja poput usmjernika. Svako sučelje na usmjerniku predstavlja zasebnu broadcast domenu. [5]



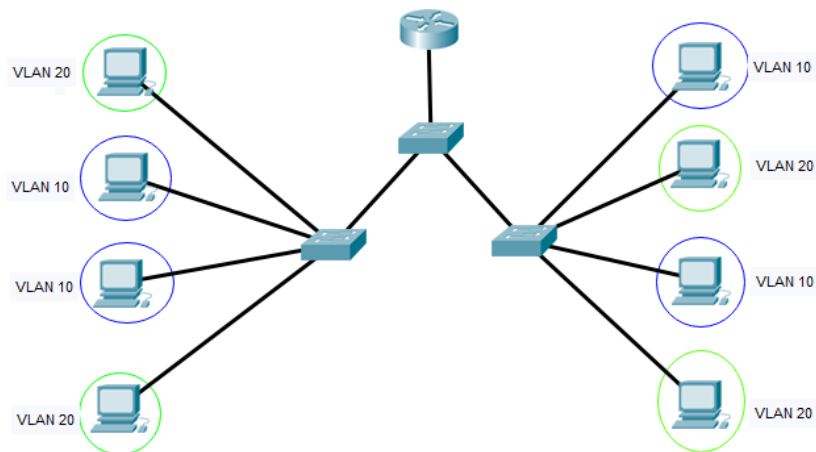
Slika 4. Prikaz broadcast domena

Prema [5]

Na slici 4. je prikaz broadcast domena. Prva broadcast domena se sastoji od više mrežnih uređaja 2. sloja s mnoštvo spojenih klijenta putem osobnih računala, a druga broadcast domena se sastoji samo od jednog preklopnika i jednog klijenta što dokazuje da neovisno o veličini mreže, radit će se o jednoj broadcast domeni sve dok ju mrežni uređaj 3. sloja ne razdvoji, u ovom slučaju usmjerivač.

Drugi način podjele broadcast domena je upotreba virtualnih lokalnih mreža (engl. *Virtual Local Area Network* - VLAN). VLAN predstavlja logičku broadcast domenu koja može obuhvatiti više fizičkih LAN segmenata. Može biti izvedena da tvori neovisne broadcast domene za određene skupine klijenata. [6] Primjerice, unutar lokalne mreže fakulteta, studentska referada može biti na jednom VLAN-u, knjižnica na drugome VLAN-u, nastavno osoblje na trećem VLAN-u i tako dalje. Svi oni će biti unutar svoje vlastite broadcast domene, neovisno što se svi zajedno nalaze na istoj fizičkoj lokalnoj mreži. Komunikacije između VLAN-ova će i dalje vršiti mrežni uređaj 3. sloja, u praksi usmjerivač ili preklopnik 3. sloja.⁴

⁴ Preklopnik 3. sloja (engl. Layer 3 Switch) je preklopnik koji uz svoje funkcionalnosti ima i mogućnost usmjeravanja prometa odnosno rutiranja. [32]



Slika 5. Podjela broadcast domena putem VLAN-ova

Na slici 5. je prikazan primjer lokalne mreže koja fizički tvori jednu broadcast domenu, ali preko VLAN-ova je napravljena podjela na dvije logičke broadcast domene. Ako klijent koji se nalazi u VLAN-u 20 (zelena boja) pokrene broadcast odašiljanje, samo će klijenti koji se nalaze u tom VLAN-u zaprimiti broadcast promet, prema ostalim klijenima koji su u VLAN-u 10 (plava boja) taj promet neće biti usmjeren, isto vrijedi i u suprotnoj situaciji.

2.3. Aplikacije i servisi koji koriste broadcast odašiljanje

Najznačajnije aplikacije i servisi koji koriste broadcast odašiljanje:

1. DHCP (engl. *Dynamic Host Configuration Protocol*)
2. ARP (engl. *Address Resolution Protocol*) [2]

DHCP

DHCP je protocol koji koriste DHCP serveri kako bi dinamički dodijelili mrežne parametre klijentima kao što su IP adresa, mrežna maska, adresa mrežnog pristupnika (engl. *Default Gateway*), IP adresu/adrese DNS servera (engl. *Domain Name System - DNS*) te vrijeme na koliko se parametri dodjeljuju. Dodjela mrežnih parametara putem DHCP-a se koristi kroz 4 koraka (poruke) [7]:

1.) DHCP otkrivanje (engl. *DHCP Discover*)

Klijent koji traži mrežne parametre šalje broadcast *DHCP Discover* poruku kako bi pronašao DHCP server u mreži (unutar broadcast domene) jer klijent nema informaciju na kojoj adresi se server nalazi. [7]

2.) DHCP ponuda (engl. *DHCP Offer*)

Kada DHCP server zaprimi *DHCP Discover* poruku od klijenta, rezervira dostupne mrežne parametre i pošalje klijentu, ova poruka je unicast prema klijentu. [7]

3.) DHCP zahtjev (engl. *DHCP Request*)

Kada klijent zaprimi *DHCP Offer* poruku od servera, šalje broadcast *DHCP Request* poruku koja služi za prihvatanje dodijeljenih parametara i implicitno odbijanje drugih ponuda od drugih DHCP servera koji su ponudili mrežne parametre klijentu. Iz tog razloga se ova poruka šalje kao broadcast. [7]

4.) DHCP potvrda (engl. *DHCP Acknowledgment*)

DHCP server šalje *DHCP Acknowledgment* poruku klijentu da je zaprimio prihvatanje mrežnih parametara. Ova poruke se šalje kao unicast. [7]

ARP

ARP protokol se koristi kako bi se preko IP adrese klijenta/mrežnog uređaja došlo do njegove MAC adrese. Uređajima 3. sloja je ARP nužan kako bi povezali IP adresu s MAC adresom da se paketi mogu poslati putem mreže. Također se koristi kada uređaj 3. sloja treba saznati MAC adresu odredišnog klijenta ili kada klijent treba saznati MAC adresu svog mrežnog pristupnika i slično. [8]

ARP zahtjev se šalje putem broadcasta jer pošiljalac nema MAC adresu odredišta, u ARP zahtjevu se traži MAC adresa koja odgovara IP adresi u zahtjevu. Kako bi se limitirali broadcast zahtjevi, uređaji privremeno spremaju ARP ulaze koje su zaprimili preko ARP zahtjeva u svoju ARP memoriju (engl *ARP cache*)⁵. Nadalje, uređaji će prvi pogledati u svoju ARP memoriju da vidi da li imaju spremljenu MAC adresu za određenu IP adresu, ako nemaju tek onda šalju broadcast ARP zahtjev. [8]

⁵ *ARP cache* je privremena memorija stoga se ulazi (zapisi) u njoj brišu nakon određenog vremena koje je definirano ARP brojačem (engl. *ARP cache timeout*). [31]

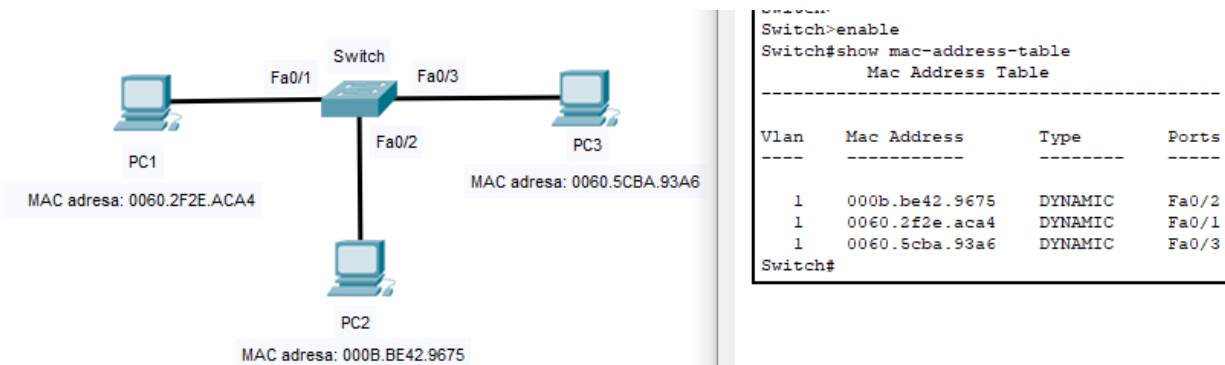
3. Definiranje problematike *broadcast storm*

Oluja razašiljanja (engl. *broadcast storm*) je stanje mreže s abnormalno velikim brojem broadcast prometa u vrlo kratkom vremenu. Iniciraju ju okviri koji završe u beskonačnoj petlji. *Broadcast storm* može onesposobiti mrežu unutar samo nekoliko sekundi na način da zasipa preklopnike i krajnje uređaje broadcast prometom. [9]

3.1. Prikaz rada preklopnika

Kako bi se lakše shvatio nastanak *broadcast storm-a* potrebno se osvrnuti na način rada preklopnika, odnosno na koji način prosljeđuje okvire (engl. *frame*).

Kada preklopnik zaprimi okvir na svoje sučelje, on pogleda odredišnu MAC adresu okvira te istu uspoređuje sa zapisima u svojoj MAC adresnoj tablici. Ako u MAC adresnoj tablici postoji odredišna MAC adresa, preklopnik će taj okvir proslijediti na sučelje koje je povezano s tom MAC adresom te će samo uređaj s tom odredišnom MAC adresom zaprimiti okvir. U slučaju da u MAC adresnoj tablici ne postoji MAC adresa pošiljatelja, preklopnik će istu dodati u svoju tablicu i povezati sa sučeljem na koji je okvir stigao, a ako postoji zapis MAC adrese, isti će osvježiti. Na taj način preklopnik gradi svoju MAC adresnu tablicu. [10]

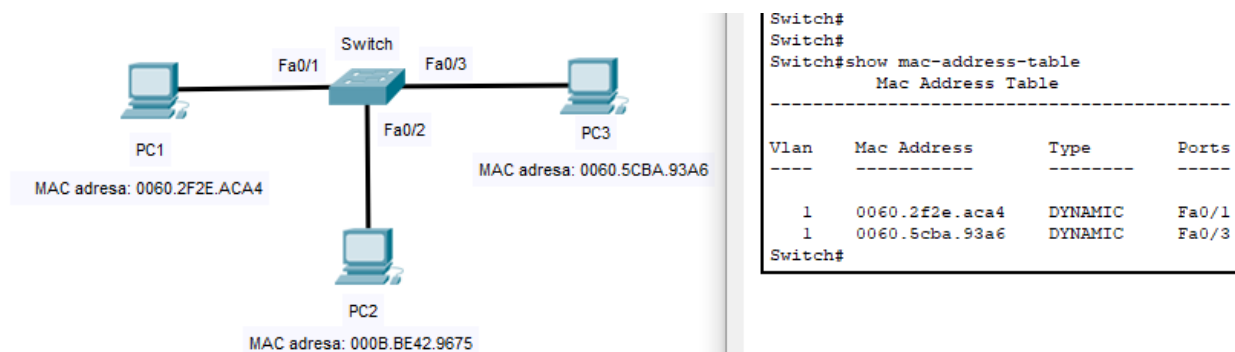


Slika 6.. Prikaz rada preklopnika kada je odredišna MAC adresa poznata

Prema [10]

Na slici 6. je prikazan primjer rada preklopnika (engl. *switch-a*). Ako klijent PC1 želi kontaktirati klijenta PC2, PC1 pošalje okvir s odredišnom MAC adresom 000B.BE42.9675, preklopnik će tu MAC adresu provjeriti u svojoj MAC adresnoj tablici, vidjet će da ima zapis o njoj i proslijediti okvir na sučelje Fa0/2. Radit će se o *unicast* prijenosu. [10]

U slučaju da preklopnik zaprimi okvir s određišnom MAC adresom o kojoj nema zapis u svojoj MAC adresnoj tablici, preklopnik će takav okvir proslijediti na sva svoja aktivna sučelja osim sučelja na koji je okvir pristigao. Međutim, samo klijent za koga je taj okvir namijenjen će ga preuzeti, ostali klijenti će vidjeti da određišna MAC adresa nije njihova i isti će odbaciti. [10]



Slika 7. Prikaz rada preklopnika kada je određišna MAC adresa nije poznata

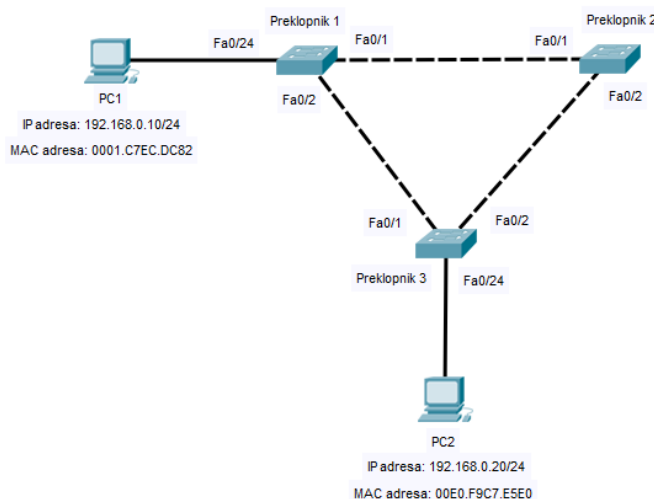
Prema [10]

Na slici 7. je napravljena ista situacija kao i na slici 6., samo što ovoga puta MAC adresa klijenta PC2 nije poznata u MAC adresnoj tablici na preklopniku. Kada klijent PC1 pošalje okvir s određišnom MAC adresom klijenta PC2, 000B.BE42.9675, preklopnik će vidjeti da u svojoj MAC adresnoj tablici nema zapisa za tu MAC adresu te će taj okvir poslati na sva aktivna sučelja osim ulaznoga, odnosno okvir će biti poslan na Fa0/2 i na Fa0/3 neovisno što za sučelje Fa0/3 ima zapis o MAC adresi koja nije određišna. Klijent spojen na Fa0/3 će vidjeti da u okviru nije njegova određišna MAC adresa i isti odbaciti. Klijent PC2 će vidjeti da je određišna MAC adresa njegova i isti okvir preuzeti.

Posljednje, kada preklopnik zaprimi okvir s broadcast određišnom adresom FF:FF:FF:FF:FF:FF, on će taj okvir proslijediti na sva aktivna sučelja osim na sučelje s kojega je okvir pristigao, odnosno na isti način kao što je slučaj kada ne zna određišnu MAC adresu.

3.2. Nastanak *broadcast storm-a*

U dobro organiziranoj lokalnoj mreži, česta je praksa da se rade dodatne veze (engl. *link*) između preklopnika kako bi se dobila redundancija. Redundancija je važna ako se prekiine primarna veza ili put između preklopnika da se promet može preusmjeriti na rezervnu vezu (engl. *backup link*). Naime, takvo spajanje bez primjene odgovarajućih protokola dovodi do velikog problema u mreži, a to se petlje 2. sloja (okviri) koji naposljetku dovode do nastanka *broadcast storm-a*. [11] Na slici 8 su prikazana tri međusobno spojena preklopnika u svrhu redundancije. Ako primjerice direktna veza između Preklopnika 1 i Preklopnika 3 padne, komunikacija između njih se može odviti preko Preklopnika 2.

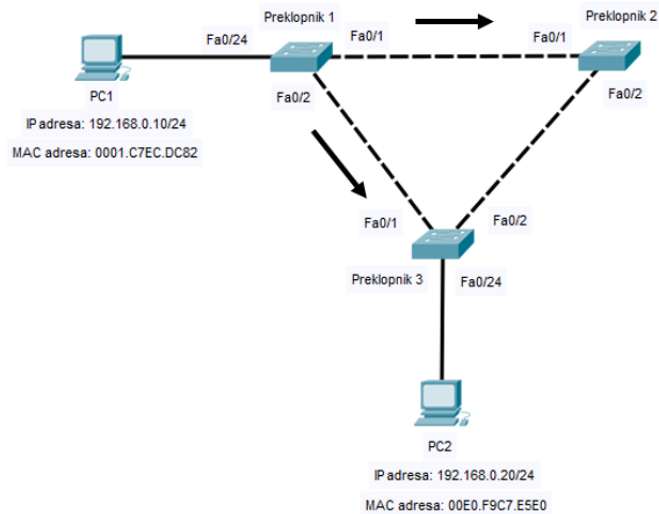


Slika 8.. Prikaz redundancije preklopnika

Prema slici 8, klijent PC1 želi komunicirati s klijentom PC2. PC1 ne zna MAC adresu PC2, samo IP adresu, stoga šalje ARP zahtjev s podacima prikazanim u tablici 1.

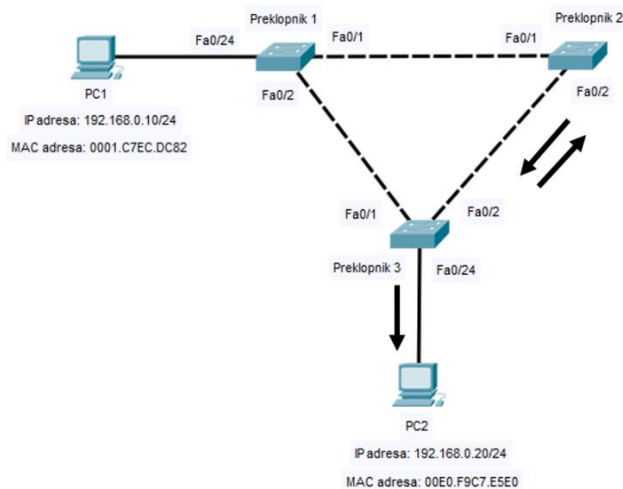
Tablica 1. Prikaz podataka u ARP zahtjevu

Odredišna MAC adresa	Izvorišna MAC adresa	Odredišna IP adresa	Izvorišna IP adresa
FF:FF:FF:FF:FF:FF	00:01:C7EC:DC:82	192.168.0.20	192.168.0.10



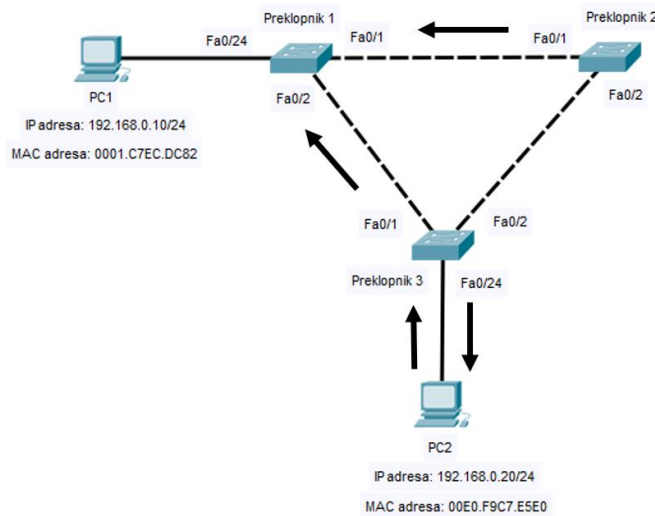
Slika 9. Prikaz nastajanja petlji I.

S obzirom na to da je odredišna MAC adresa broadcast adresa, Preklopnik 1 prosljeđuje taj okvir na sva svoja aktivna sučelja, u ovom slučaju Fa0/1 i Fa0/2, osim na Fa0/24 s kojega je okvir pristigao. Isto je prikazano na slici 9.



Slika 10. Prikaz nastajanja petlji II.

Nadalje, Preklopnik 3 je zaprimio okvir na Fa0/1 sučelje te isti prosljeđuje na sva svoja aktivna sučelja. Preko sučelja Fa0/24 okvir pristiže do klijenta PC2 za koja je bio namijenjen, ali je okvir također poslan i na Fa0/2 prema Preklopniku 2. Paralelno je Preklopnik 2 odradio isti proces te na Preklopnik 3 preko njegovog Fa0/2 istovremeno pristiže isti okvir. Proces je prikazan na slici 10.



Slika 11. Prikaz nastajanja petlje III.

Nastavno na sliku 10, na slici 11 je prikazan daljnji tijek radnje. Klijent PC2 je zaprimio ARP zahtjev i šalje ARP odgovor prema PC1, za određenu MAC i IP adresu stavlja te iste izvorišne adrese iz ARP zahtjeva. Preklopnik 2 i 3 šalju ARP zahtjev iniciran od strane PC1 natrag prema Preklopniku 1. Preklopnik 1 će ARP zahtjev koji je pristigao od Preklopnika 2 proslijediti prema PC1, ali i prema Preklopniku 3, a zahtjev koji je pristigao od Preklopnika 3 će proslijediti prema Preklopniku 2 te ponovno do PC1 te je vidljivo kako se dogodila petlja.

U međuvremenu, PC2 je poslao ARP odgovor kao unicast prema PC1. S obzirom na to da je ARP zahtjev od PC1 stigao prije na Preklopnik 1, on je u svoju MAC tablicu naveo MAC adresu PC1 da se nalazi na sučelju Fa0/2. Na to isto sučelje će primiti ARP odgovor za PC1, iz razloga jer se radi o istom sučelju, preklopnik neće znati što da radi i taj će ARP odgovor odbaciti.

ARP zahtjev koji je pokrenuo PC1 će se vrtjeti u petlji između preklopnika te će on konstantno primati svoj zahtjev, svaki put će isti odbaciti jer prilikom enkapsulacije će vidjeti da određena IP adresa nije njegova. Taj isti zahtjev će također stalno pristizati prema PC2, on će ga svaki put obraditi jer je zahtjev za njega te poslati ARP odgovor jer nije svjestan petlje.

ARP odgovor od strane PC2 će pristizati na PC1 ovisno o trenutnom stanju MAC tablice Preklopnika 1, ako će MAC adresa PC1 zbog petlje biti navedena na Fa0/2 sučelju u tom trenutku, paket će biti odbačen, ako će biti na nekom drugo sučelju, PC1 će zaprimiti taj ARP odgovor. Klijent PC1 će ga obraditi samo prvi put kada pristigne te će dodati MAC adresu zajedno s IP

adresom klijenta PC2 u svoju ARP memoriju, svaki sljedeći odgovor koji pristigne će odbaciti. Klijent PC2 će taj ARP odgovor svaki put odbaciti jer prilikom enkapsulacije će vidjeti da određena MAC adresa nije njegova.

Kao što je navedeno, *broadcast storm* se događa na drugom sloju OSI referentnoj modela. Za razliku od protokola trećeg sloja, IPv4 i IPv6, na drugom sloju Ethernet protokola ne postoji mehanizam koji će ograničiti koliko puta će preklopnik ili neki drugo uređaj drugog sloja poslati isti Ethernet okvir. IPv4 u zaglavlje paketa stavlja mehanizam vrijeme življenja (engl. *Time to Live* - TTL) koji nakon određenog broja skokova između usmjerivača ne dođe do odredišta, odbacuje paket iz mreže. Kod IPv6 je slična situacija, samo se kod tog protokola koristi limitiranje skokova (engl. *Hop Limit*) u zaglavlju paketa. Ethernet okviri će završiti u beskonačnoj petlji koju je moguće zaustaviti samo fizičkim isključivanjem veze, odnosno kabela. Velik broj ovakvih petlji drugog sloja dovodi do *broadcast storm-a*. [9]

4. Simulacijsko modeliranje *broadcast storm-a* korištenjem programskog alata Cisco Packet Tracer

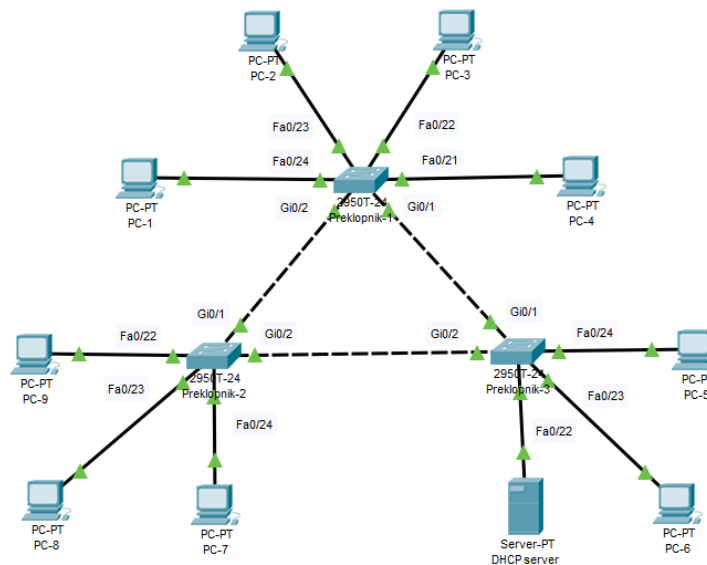
Cisco Packet Tracer je softver koji omogućava simulaciju i vizualizaciju mreža. Razvila ga je kompanija Cisco Systems, Inc. iz SAD-a u svrhu da studenti koji pohađaju njihove akademije razviju praktične vještine u mrežama. Cisco Packet Tracer pruža dva operacijska moda, prvi je mod stvarnog vremena mreže (engl. *real-time mode*) gdje se mreža i uređaji ponašaju kao u stvarnog vremenu te pružaju stvarno vremenske odgovore za sve mrežne aktivnosti. Simulacijski mod omogućava detaljan uvid u sami prijenos podataka te kako se isti propagiraju kroz mrežu. [12]

U navedenom softveru je napravljena simulacija nastajanja *broadcast storm-a* u lokalnoj mreži.

Simulacija je napravljena koristeći:

- 3 Cisco WS-C2950T-24 preklopnika
- 9 osobnih računala (PC – *personal computer*) koji predstavljaju klijente
- DHCP server

Topologiju simulacijske mreže te korištene uređaje možemo vidjeti na slici 12.



Slika 12.. Topologija simulacijske mreže

Cisco WS-C2950T-24 preklopnik je dio Catalyst 2950 Cisco serije inteligentnih *Ethernet* preklopnika. Ova inačica pruža 24 brzih Ethernet sučelja (engl. *Fast Ethernet*) koji podržavaju brzine do 100 Mbps te 2 Gigabitna Ethernet (engl. *Gigabit Ethernet*) sučelja koji podržavaju brzine do 1 Gbps. Predviđeno je da se koristi u mrežama srednjih veličina. [13]

DHCP server je konfiguriran da dodjeljuje parametre navedene u tablici 2. Raspon IP adresa (engl. *IP address pool*) predstavlja raspon IP adresa koji će DHCP server dodjeljivati s odgovarajućom mrežnom maskom. Praksa je da se ne stavi cijeli raspon na dodjelu kako bi se sačuvao određeni broj IP adresa za statičku dodjelu te se ne stavlja zadnja IP adresa raspona (u ovom slučaju 192.168.0.255) jer se ona koristi za broadcast promet na trećem sloju.

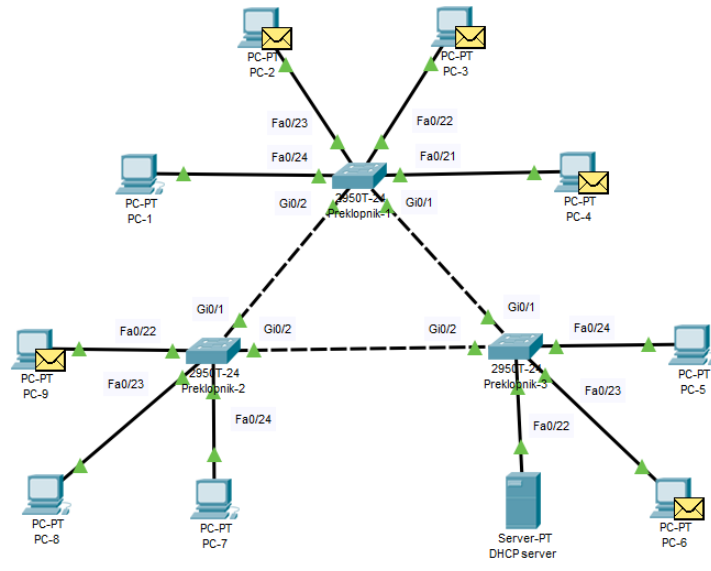
Također, dodjeljuje adresu mrežnog pristupnika (IP adresa sučelja usmjerivača na koji su klijenti spojeni) kako bi klijenti znali gdje usmjeriti promet prema vanjskoj mreži te IP adresu DNS servera kako bi klijenti znali koga kontaktirati za prijevod domenskih imena (alfanumeričkih zapisa) u IP adrese. Usmjerivač i DNS server nisu prikazani u simulaciji.

Tablica 2. Mrežni parametri

IP raspon adresa	Mrežna maska	Adresa mrežnog pristupnika	DNS server
192.168.0.21-192.168.0.254	255.255.255.0	192.168.0.1	192.168.3.10

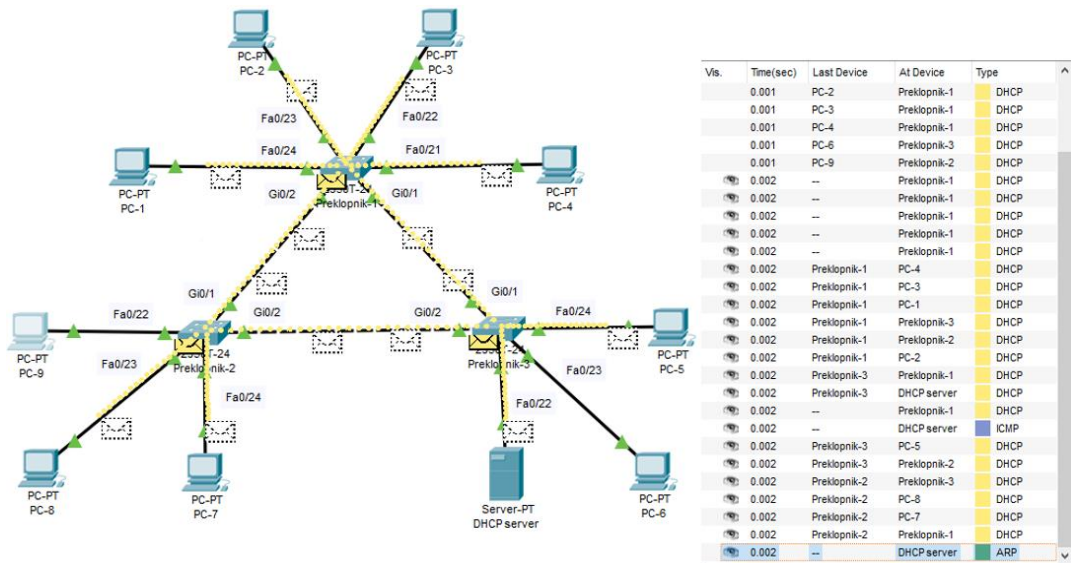
Cisco WS-C2950T-24 preklopnici imaju u početnoj konfiguraciji omogućen *spanning tree* protokol STP (engl. *Spanning Tree Protocol*) koji se koristi za sprječavanje petlji u mreži koje naposljetku dovode do *broadcast storm-a*. [14] Protokol će biti objašnjen u narednom poglavlju. Kako bi simulacija bila uspješna, isti se isključio pomoću komande `#no spanning-tree vlan 1`. S obzirom na to da se u komandi mora definirati VLAN na kojemu se isključuje STP, u simulaciji se nisu kreirati dodatni VLAN-u te samim time cijela prikazana mreža pripada u VLAN 1.

Na slici 13. je prikazano kako klijenti PC-2, PC-3, PC-4, PC-6 i PC-9 šalju DHCP *Discover* poruku kako bi pronašli DHCP server. Kako je navedeno u poglavlju 2.3, klijenti nisu svjesni gdje se nalazi DHCP server te ovu poruku šalju kao broadcast.



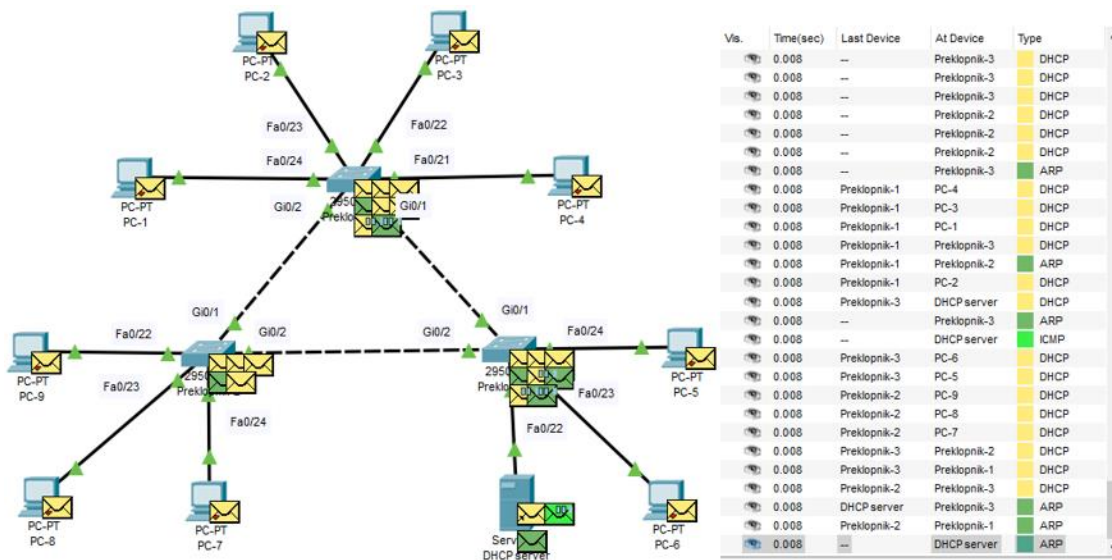
Slika 13. Kreiranje broadcast storm-a I.

Svaku DHCP Discover poruku zaprimljenu od klijenta, preklopnici će proslijediti na sva svoja aktivna sučelja osim ulaznog, isto je prikazano na slici 14. Na slici također možemo vidjeti popis događaja (engl. *event list*), odnosno što se događa sa svakim okvirom. Vidimo tip okvira (engl. *type*), na kojem je uređaju trenutno okvir (engl. *at device*), kod kojeg je uređaja zadnje bio okvir (engl. *last device*) te u kojem vremenu se događaj dogodio (engl. *time*) koje se mjeri od početka simulacije.



Slika 14. Kreiranje broadcast storm-a II.

Na slici 14. može se vidjeti da je DHCP *Request* iniciran od strane klijenta PC-6 stigao do DHCP servera te je započela njihova međusobna komunikacija (4 koraka objašnjena su u poglavlju 2.3.). Na slici 15. možemo vidjeti da nakon već 8 ms se pojavilo niz okvira koji se završili u petlji, uz DHCP okvire i ARP zahtjevi su završili u petlji. Vidljivo je na preklopticima niz zahtjeva koji čekaju na obradu što iskorištava velik dio njihove procesorske snage (CPU). Zbog konstantnog rasta broja okvira koji završavaju u petlji, pojavljuje se *broadcast storm* u simulacijskoj mreži.



Slika 15. Kreiranje broadcast storm-a III.

Klijenti	MAC adrese
PC-1	0040.0B2C.874D
PC-2	0001.C9CE.7362
PC-3	00D0.BA6D.D646
PC-4	0060.3E16.232E
PC-5	000B.BED2.92D0
PC-6	0002.4A8E.8135
PC-7	0001.429A.BE52
PC-8	0000.0CB3.8C11
PC-9	00E0.B021.0B34
DHCP server	00D0.BC3C.D413


```

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

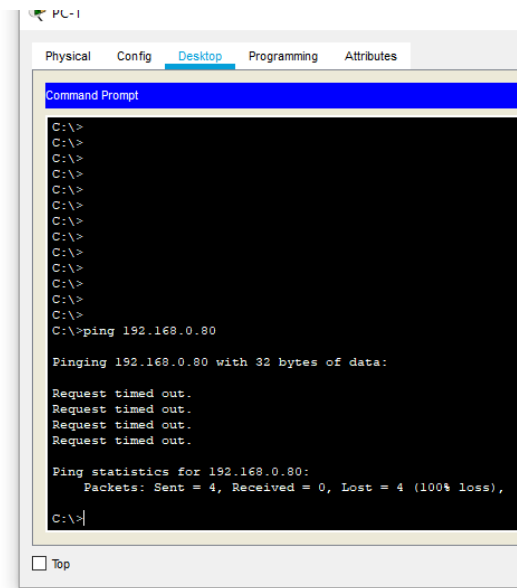
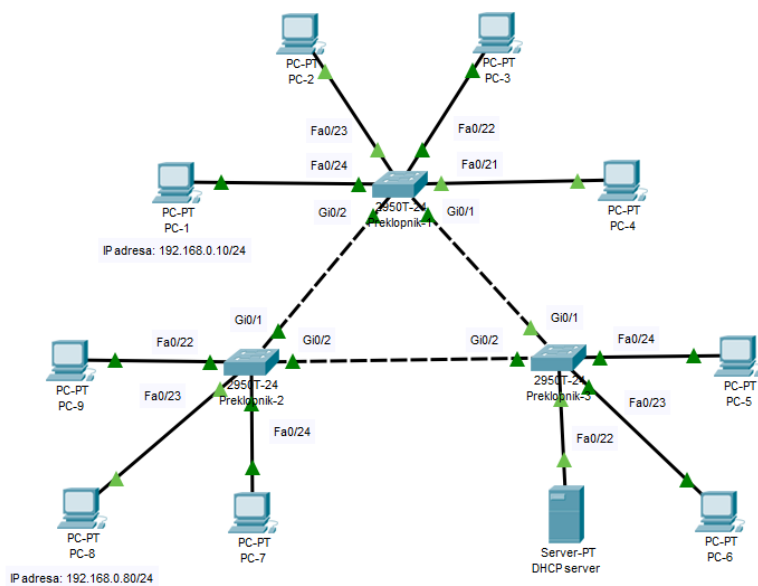
Preklopnik1>
Preklopnik1>
Preklopnik1>en
Preklopnik1#show mac ad
Preklopnik1#show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0001.c9ce.7362   DYNAMIC Gig0/1
1       0002.4a8e.8135   DYNAMIC Gig0/1
1       00d0.bdc4.5315   DYNAMIC Gig0/1
1       0040.0b2c.874d   DYNAMIC Fa0/24
1       0060.3e16.232e   DYNAMIC Gig0/1
1       00d0.ba6d.d646   DYNAMIC Gig0/1
1       00d0.bc3c.d413   DYNAMIC Gig0/2
1       00e0.8f37.6719   DYNAMIC Gig0/2
1       00e0.b021.0b34   DYNAMIC Gig0/2
Preklopnik1#

```

Slika 16. MAC adresna tablica Preklopnika 1

Vrlo kratko nakon pokretanja simulacije je na slici 16. prikazana MAC adresna tablica Preklopnika 1 te MAC adrese klijenata. Kao rezultat petlji, MAC tablica prikazanog preklopnika pokazuje krive zapise, odnosno MAC adrese klijenata povezana s krivim sučeljima. Gledajući po topologiji simulacijske mreže, za klijenta PC-1 zapis u MAC tablici u tom trenutku odgovara, on stvarno i je spojen na sučelje Fa0/24. Međutim, ostali klijenti koji su spojeni na Preklopnik 1, PC-2, PC-3, PC-4 su u MAC adresnoj tablici asocirani s Gig0/1 sučeljem. Svaki unicast okvir koji preklopnik zaprimi za te klijente će poslati prema Preklopniku 3, osim ako okvir za te klijente zaprimi upravo na to Gig0/1 sučelje, tada će te okvire odbaciti.

Kao rezultat konstantne promjene MAC adresne tablice te velikog broja petlji, onemogućena je komunikacija u mreži. Prema slici 17. klijenti PC-1 i PC-2 su imali unaprijed dodijeljene IP adrese. PC-1 pomoću *ping* alata koji služi za provjeru dostupnosti pokušava doći do PC-2, kao što je pretpostavljeno, komunikacija nije uspjela. Svaki od 4 zahtjeva poslanih prema PC-2 nije uspio. Za potrebe provjere, mod u softveru je prebačen sa simulacijskog u mod stvarnog vremena mreže.



Slika 17. Pokušaj komunikacije između klijenata

U ovoj simulaciji smo dokazali kako *broadcast storm* djeluje na komunikaciju u mreži. U vrlo kratkom vremenu od pokretanja broadcast zahtjeva u mreži bez odgovarajućih protokola koji kontroliraju njihovo razasiłjanje, odnosno sprječavaju da završe u petlji, komunikacija u mreži je onemogućena.

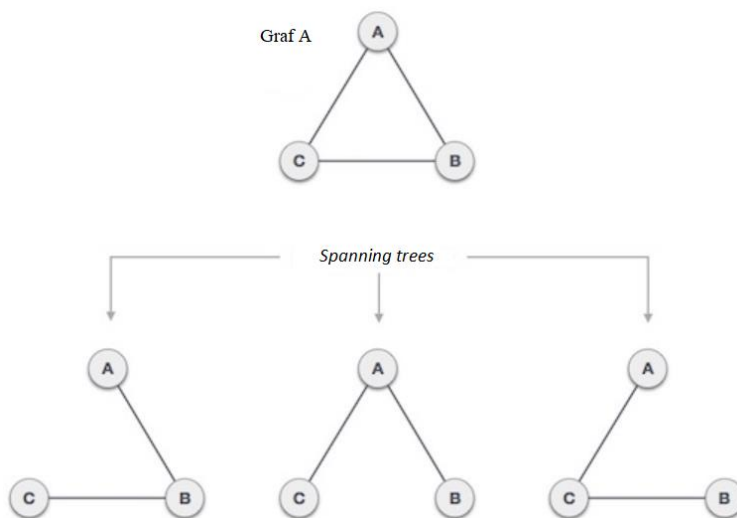
5. Pregled i korištenje protokola i algoritama u funkciji rješavanja problema *broadcast storm*

Da bi se izbjeglo stanje mreže koje uzrokuje *broadcast storm*, odnosno okviri koji završe u beskonačnoj petlji, potrebno je osigurati jedinstveni put prometa kroz mrežu. Odabir jedinstvenog (najboljeg) puta kroz mrežu bazira se na matematičkom algoritmu *spanning tree* (engl. *Spanning Tree Algorithm* - STA). U nastavku je opisano kako navedeni algoritam općenito odabire jedinstveni put te protokol kroz koji se očituje njegova primjena u računalnim mrežama. [9]

5.1. STA (engl. *Spanning Tree Algorithm*)

Kako bi se razumio *spanning tree* protokol (STP), potrebno je analizirati algoritam na kojem se temelji, a to je *spanning tree* algoritam (STA – *Spanning Tree Algorithm*).

Spanning tree je dio podskupa grafa A koji je prikazan na slici 18. Graf A ima sve vrhove pokrivene s najmanjim mogućim brojem veza (engl. *edges*). U *spanning tree*-u nema kružnog ciklusa gdje se može stvoriti petlja i stablo se ne može odspojiti. Prema tome, svaki spojeni i neusmjereni graf poput grafa A ima najmanje jedan *spanning tree*. Nespojeni grafovi nemaju nijedan *spanning tree* jer se ne može raširiti prema svim njegovim vrhovima. [15]



Slika 18. Pronalazak *spanning tree*-a

Izvor: [15]

Iz grafa A možemo dobiti tri *spanning tree-a* prema matematičkom izrazu da svaki potpuno neusmjereni graf može imati maksimalno n^{n-2} *spanning tree-a* gdje n predstavlja broj čvorova. U grafu A imamo tri čvora stoga je vrijednost $n=3$, ubacivši to u formulu dobimo tri *spanning tree-a*. [15]

Svojstva *spanning tree-a* prema primjeru grafa A:

- Spojeni graf A može imati više od jednog *spanning tree-a*
- Sva moguća *spanning tree-a* grafa A imaju isti broj veza i vrhova
- U *spanning tree-u* nema kužnih ciklusa (petlji)
- Maknuvši jednu vezu iz *spanning tree-a* graf će biti odspojen, odnosno stablo (engl. *tree*) je već spojeno s minimalnim brojem veza
- Dodajući jedan vezu *spanning tree-u* će kreirati kružni ciklus (petlju), odnosno stablo je već maksimalno acikličko [15]

Spanning tree se koristi u svrhu da se nađe put s minimalnim troškom za spajanje svih čvorova u grafu. Najčešću primjenu ima u općenitom planiranju mreža, u analiti klastera (grupiranja) te u usmjerivačkim protokolima u računalnim mrežama. [15]

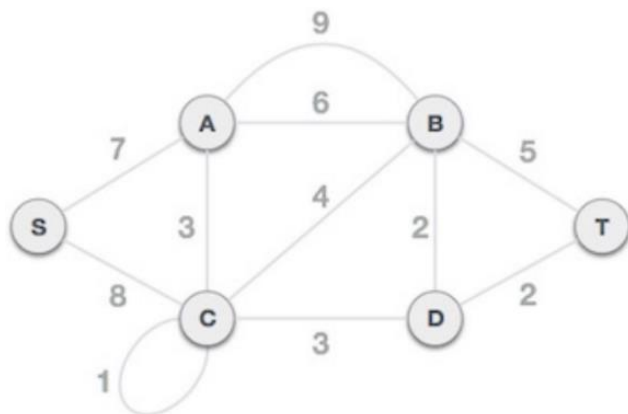
Minimalni *spanning tree* (engl. *Minimum Spanning Tree* - MST) je *spanning tree* koje ima minimalnu težinu (engl. *weight*) od svih ostalih stabala na istom grafu. Ta težina se može mjeriti kao udaljenost, zagušenje, prometno opterećenje ili bilo koja druga proizvoljna vrijednost koja ovisi o rubovima. Težina se još označava kao trošak (engl. *cost*). Dva najznačajnija algoritma za pronalaženje minimalnog *spanning tree-a* su Kruskalov i Primov algoritam. U sljedećem poglavlju će biti analiziran Kruskalov algoritam. [15]

5.2. Kruskalov algoritam

Kruskalov algoritam se koristi za pronalazak minimalnog *spanning tree-a* koje ima najmanji sveukupni trošak (engl. *cost*) koje se označava kao MST. Kruskalov algoritam tretira graf kao šumu i svaki čvor kao zasebno stablo. Svako stablo, odnosno čvor se spaja s drugim samo ako imaju najmanji međusobni trošak od svih ponuđenih opcija povezivanja ta dva čvora. [16]

Kruskalov algoritam za određivanje MST-a koristi 3 koraka:

- 1.) Uklanjanje svih petlji i paralelnih veza
- 2.) Slaganje svih veza po vrijednosti troška
- 3.) Dodavanje veza koji imaju najmanji trošak [16]



Slika 19. Graf prije primjene Kruskalovog algoritma

Izvor: [16]

Koraci Kruskalovog algoritma su opisani prema grafu iz slike 19. Brojevi na vezama između čvorova označavaju trošak veze. [16]

U prvom koraku se uklanjaju sve petlje te paralelne veze. Prema grafu se uklanja petlja oko čvora C koja ima trošak 1. Također, na grafu imamo paralelne veze između čvorova A i B, uklanja se veza koja ima veći trošak, a to je veza s troškom 9. [16]

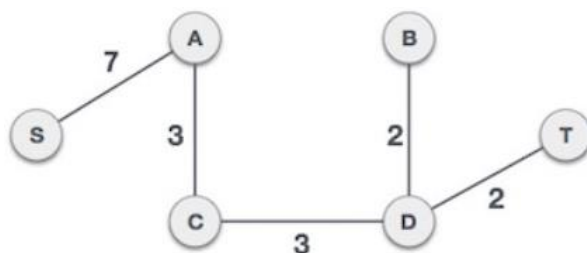
Drugi korak se odnosi na slaganje svih veza po vrijednosti troška kako bi napravili pripremu za treći korak. Vrijednosti troška svake veze između čvorova za zadani graf su prikazani u tablici 3. [16]

Tablica 3. Vrijednosti troškova svake veze prema grafu

B-D	D-T	A-C	C-D	C-B	B-T	A-B	S-A	S-C
2	2	3	3	4	5	6	7	8

Izvor: [16]

U trećem koraku se primjenjuju veze između čvorova na način da se kod više izbora veza dodaju one koje imaju najmanju vrijednost troška. Pri primjenjivanju veza je potrebno paziti da se poštvaju svojstva *spanning tree-a* navedena u prethodnom poglavlju. [20]



Slika 20. Graf poslije primjene Kruskalovog algoritma

Izvor: [16]

Nakon primjene svih koraka, gotovi *spanning tree* je prikazan na slici 20. [16]

5.3. STP (engl. *Spanning Tree Protocol*)

Kao što je prethodno navedeno u radu, redundancija je važan segment u dizajniranju mreža. Pruža rezervne veze (engl. *backup link*) u slučaju da primarna veza postane neaktivna. Kako su primarna i rezervne veze istovremeno spojene dolazi do petlje. U 4.) poglavlju je bila prikazana simulacija koja dokazuje koliko je važno da u slučaju kada imamo više veza koje formiraju petlju potrebno osigurati da okviri koji završeni u toj mreži ne završe u petlji koja dovodi do *broadcast storm-a*. To se osigurava pomoću *spanning tree* protokola (engl. *Spanning Tree Protocol – STP*)).

STP⁶ je protokol drugog sloja koji aktivno nadzire sve veze u mreži. Oznaka protokola je IEEE 802.1D. [17] Kako bi pronašao redundantne (rezervne) veze koristi STA algoritam. STA prvo kreira topologijsku bazu podataka te nakon toga pronalazi i onesposobi redundantne veze. Nakon što se redundantne veze onesposobe, samo veze odabrane od strane STP-a ostaju aktivne. U slučaju da se u mrežu doda nova veza ili makne neka postojeća veza, STP ponovno pokreće STA pomoću kojega prilagođava sve veze u skladu s promjenama u mreži. [18]

⁶ STP se još naziva CST (engl. *Common spanning tree*) [9]

BPDU (engl. *Bridge Protocol Data Units*) su multicast okviri koji preklopnici koriste kako bi razmijenili informacije o sebi i svojim konekcijama (vezama). Osim same razmjene informacija, preklopnici koriste BDPU okvire kako bi naučili topologiju mreže, koji preklopnik je spojen s kojim preklopnicima te kako bi vidjeli da li postoji kakva petlja na drugom sloju u topologiji koju su naučili. [18]

Svaki BDPU okvir sadrži BID (engl. *bridge ID*) koji identificira koji je preklopnik poslao BDPU. BID se koristi za razne odluke kod STA algoritma poput definiranja glavnog (korijenskog) preklopnika (engl. *root bridge*) u mreži te dodjele uloga sučeljima na tim preklopnicima. [9]

BID se sastoji od sljedećeg:

- Prioriteta preklopnika (engl. *bridge priority*)
- Proširenog sistemskog identifikatora (engl. *extended system ID*)
- MAC adrese [9]

Bridge priority je numerička vrijednost definirana od strane IEEE 802.1D koja u početnoj konfiguraciji iznosi 32768, isti se po potrebi može promijeniti. [19]

Extended system ID je vrijednost koja se dodaje *bridge priority-u* (zbrajaju se), označava VLAN za taj BDPU okvir. [19]

MAC adresa preklopnika u BID-u se koristi u slučaju da su prve dvije vrijednosti (*bridge priority* i *extended system ID*) izjednačene, tada će preklopnik koji ima najmanju vrijednost MAC adrese (izražene u heksadecimalnom zapisu) imati najmanji BID. [9]

Svaki BDPU okvir se sastoji od nekoliko polja. Polja su prikazana u tablici 4.

Tablica 4. Polja u BDPU okviru

Polje	Opis
<i>Root Bridge ID</i> ili <i>Root BID</i>	BID preklopnika za koji pošiljatelj misli da je <i>root bridge</i>
Pošiljateljev BID (engl. <i>senders BID</i>)	BID preklopnika koji šalje BDPU
Trošak to <i>root bridge-a</i>	STP trošak (engl. <i>STP cost</i>) između tog preklopnika i trenutnog <i>root bridge-a</i>
Vrijednosti brojača (engl. <i>timer values</i>) na <i>root bridge-u</i>	<i>Hello timer</i> , <i>Max age timer</i> , <i>Forward delay timer</i>

Izvor: [20]

Koristeći STA, STP gradi topologiju bez petlji kroz 4 koraka (odabir uloga):

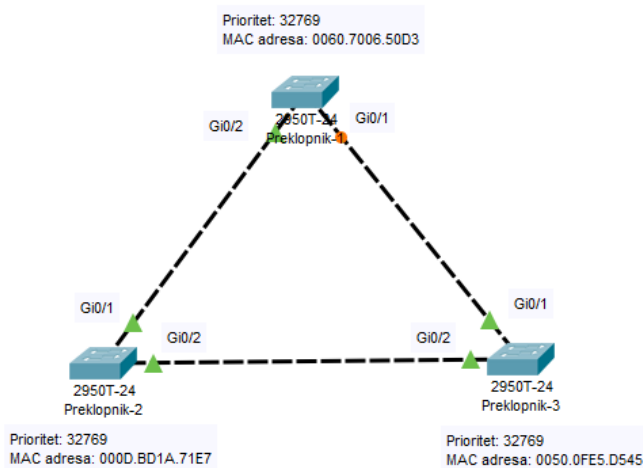
- 1.) Odabir glavnog (korigenskog) preklopnika (engl. *root bridge*)
- 2.) Odabir glavnih (korigenskih) sučelja (engl. *root ports*)
- 3.) Odabir označenih (prihvatnih) sučelja (engl. *designated ports*)
- 4.) Odabir alternativnih odnosno blokirajućih sučelja (engl. *alternate/blocked ports*) [9]

5.3.1. Odabir *root bridge-a*

Root bridge je specijalni preklopnik na “vrhu” *spanning tree-a*. Svi ostali preklopnici, odnosno njihove konekcije se usmjeravaju prema njemu. *Root bridge* je ujedno i početna točka kreiranja STP mrežne topologije. [19]

Sami proces odabira *root bridge-a* je vrlo jednostavan. Preklopnik koji ima najmanji BID će postati *root bridge*. Prvo se gleda *bridge priority s extended system ID*, ako je to izjednačeno, onda se gleda MAC adresa te će preklopnik s najmanjom MAC adresom postati *root bridge*. [20]

Kada se preklopnik pokrene, počinje slati BDPU okvire svake dvije sekunde, radi se o pozdravnom BDPU (engl. *hello BDPU*). Na početku procesa svi preklopnici proglašavaju sebe kao *root bridge-om* te u polje Root BID stavljaju vlastiti BID, u pošiljatelj BID je stavljaju također njihov vlastiti te trošak do *root bridge-a* je 0 jer nemaju troška do samoga sebe. Nakon razmjene BDPU-a između preklopnika se utvrdi da samo jedan u mreži ima najmanji BID i taj preklopnik je proglašen *root bridge-om*. [20]



Slika 21. Odabir *root bridge-a*

Na slici 21. je prikazana topologija iz simulacijske mreže korištena u 4. poglavlju rada, ali bez klijenta jer nisu potrebni za ovaj dio rada. S obzirom na to da se prioriteta preklopnika nisu mijenjali i svi rade u istom VLAN-u, o odabiru *root bridge-a* će odlučivati najmanja MAC adresa. U ovom slučaju će Preklopnik 2 biti odabran kao *root bridge* jer ima najmanju MAC adresu (u heksadecimalnom zapisu).

5.3.2. Odabir *root port-a*

Nakon odabira *root bridge-a*, svaki preklopnik u mreži mora odabrati jedinstveno sučelje preko kojega se dolazi do *root bridge-a* koje se naziva *root port*, skraćena oznaka RP. *Root port* se odabire na preklopniku na temelju najmanjeg cjelokupnog troška puta (engl. path cost) do *root bridge-a*. [21] Cjelokupni trošak puta se još zove interni trošak puta (engl. *internal root path cost*). [9]

Cjelokupni trošak puta se računa kao suma svih individualnih troškova sučelja (engl. port cost) od preklopnika do *root bridge-a*. [9] Troškovi sučelja ovise o brzini na kojem sučelja rade. Troškovi sučelja su prikazani u tablici 5. [18] Neovisno o tome što sučelja imaju baznu vrijednost za troškove sučelja, ista se mogu konfigurirati. [9]

Tablica 5. Troškovi sučelja [18]

Brzina veze	STP trošak (IEEE 802.1D)
10 Gbps	2
1 Gbps	4
100 Mbps	19
10 Mbps	100

Izvor: [18]

Na topologiji mreže sa slike 21. vidimo da su tri preklopnika spojena međusobno preko gigabitnih (engl. *gigabit*) sučelja koji rade na brzini od 1 Gbps te je njihov trošak sučelja za svaki iznosi 4 prema tablici 5. Prethodno je Preklopnik 2 odabran kao *root bridge*, druga dva preklopnika će koristeći STA odabrati *root port* do *root bridge-a*.

Preklopnik 1 će računati trošak puta preko sučelja Gi0/1 i Gi0/2. Preko sučelja Gi0/1 veza ide do Preklopnika 3 te iz Preklopnika 3 do Preklopnika 2 (*root bridge*) također preko gigabitnog sučelja. S obzirom na to da se svaka veza gleda zasebno, cjelokupni trošak će se računati kao zbroj tih dviju veza, odnosno 4+4 te će cjelokupni trošak puta iznositi 8. Preko sučelja Gi0/2 je Preklopnik 1 direktno spojen na *root bridge* te cjelokupni trošak puta iznosi 4. S obzirom na to da je cjelokupni trošak puta manji preko sučelja Gi0/2, isti će biti odabran kao *root port*. Isto vrijedi i za Preklopnik 3 koji će izabrati svoje Gi0/2 sučelje kao *root port*.

5.3.3. Odabir *designated port-a*

Svaki segment između dva preklopnika će imati jedan *designated port* skraćena oznaka DP. *Designated port* je sučelje koje ima najmanji cjelokupni trošak puta do *root bridge-a* (najbolji put). Drugim riječima, *designated port* ima najbolji put za primanje prometa koji ide prema *root bridge-u*. [9] Za razliku od *root port-a* koji mora biti jedinstven na svakom preklopniku, preklopnik može imati više *designated port-ova*. [22]

Načini na koje STA odabire *designated port-ove*:

1. *Designated port-ovi* na *root bridge-u*
2. *Designated port-ovi* gdje postoji *root port*
3. *Designated port-ovi* gdje nema *root port-a*
4. *Designated port-ovi* prema krajnjim uređajima (klijentima) [9]

1.) Kako je prethodno navedeno, *designated port* ima najbolji put (najbolji cjelokupni trošak) za primanje prometa prema *root bridge-u*. Na *root bridge-u* su sva sučelja *designated port-ovi* jer *root bridge* ima najbolji put do samoga sebe. [9]

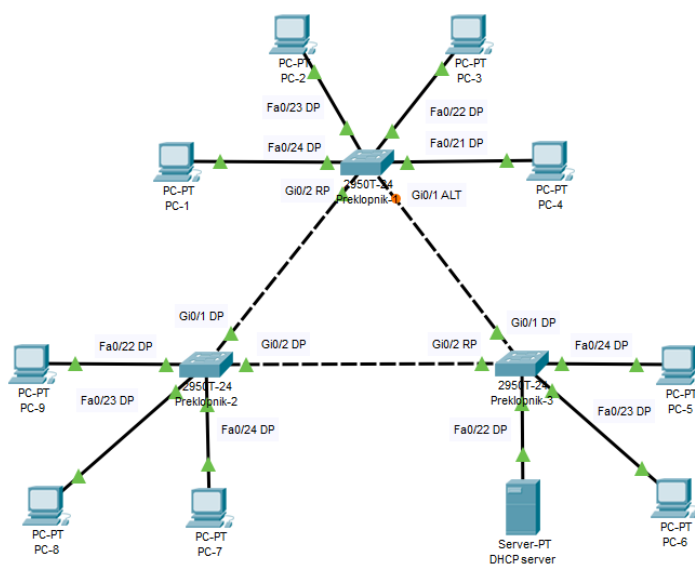
2.) Gledajući segment između dva preklopnika, ako je na jednom preklopniku *root port*, na drugom preklopniku na tom segmentu je onda *designated port*. Primjerice, jedan preklopnik ima *root port* prema drugom preklopniku, sučelje na drugom preklopniku gdje je spojen prvi preklopnik je *designated port* jer ima najbolji put za primanje prometa od strane prvog preklopnika koji vodi prema *root bridge-u*. [9]

3.) U segmentu između dva preklopnika gdje ne postoji *root port*. Odluka čije će sučelje biti *designated port* će se odlučiti na temelju koji sučelje ima najbolji put do *root bridge-a*, ako oba sučelja imaju istu vrijednost cjelokupnog troška do *root bridge-a*, *designated port* će biti na onom preklopniku koji ima manji BID. Na drugom preklopniku koji ima veći BID, sučelje će biti u blokirajućem stanju. [9]

4.) Sva sučelja na preklopticima na koja su spojeni krajnji uređaji (klijenti) će biti *designated port-ovi* jer imaju najbolji put za njihov promet do *root bridge-a*, odnosno jedina su sučelja. [9]

5.3.4. Odabir alternativnih (blokirajućih) sučelja

Svako sučelje koje nije *root port* ili *designated port* će postati alternativno (blokirajuće) sučelje, oznaka ALT. Ona blokiraju sav promet koji se pošalje prema njima kako bi spriječili pojavu petlji. Alternativno sučelje se gleda još kao rezervno (engl. *backup*) sučelje, u slučaju pada nekih od veza u mreži ili bilo kakvom promjenom topologije, ona mogu postati *root* ili *designated port* ako za istim ima potrebe. [9]



Slika 22. Odabir uloga sučelja

Na slici 22. je prikazana topologija korištena u simulaciji (sa spojenim klijentima), a na slici 23. su prikazana svojstva (karakteristike) STP-a na Preklopniku 2 (*root bridge*) i Preklopniku 1. Svojstva STP-a na svakom preklopniku se mogu vidjeti preko komande #show spanning-tree.

```

Preklopnik1#
Preklopnik1#
Preklopnik1#
Preklopnik1#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 000D.BD1A.71E7
Cost 4
Port 26(GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0060.7006.50D3
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/23 Desg FWD 19 128.23 P2p
Fa0/22 Desg FWD 19 128.22 P2p
Gi0/1 Altn BLK 4 128.25 P2p
Fa0/21 Desg FWD 19 128.21 P2p
Fa0/24 Desg FWD 19 128.24 P2p
Gi0/2 Root FWD 4 128.26 P2p
Preklopnik1#

Preklopnik2#
Preklopnik2#
Preklopnik2#
Preklopnik2#
Preklopnik2#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 000D.BD1A.71E7
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 000D.BD1A.71E7
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/23 Desg FWD 19 128.23 P2p
Fa0/24 Desg FWD 19 128.24 P2p
Fa0/22 Desg FWD 19 128.22 P2p
Gi0/1 Desg FWD 4 128.25 P2p
Gi0/2 Desg FWD 4 128.26 P2p
Preklopnik2#

```

Slika 23. Karakteristike STP-a na Preklopniku 1 i 2

Na slikama je vidljivo da su sva sučelja na preklopnicima na koja su spojeni klijenti *designated port-ovi*, osim na *root bridge-u* (Preklopnik 2) gdje su sva sučelja *designated*, uključujući Gi0/1 i Gi0/2 sučelja koja predstavljaju vezu s ostalim preklopnicima u mreži. Na segmentu (vezi) između Preklopnika 1 i Preklopnika 3 je odluka o *designated port-u* donesena na temelju BID-a preklopnika.

Oba sučelja imaju isti trošak puta do *root bridge-a*, ali Preklopnik 3 ima manji BID jer ima manju MAC adresu što je vidljivo na slici 21. Sukladno tome, Gi0/1 sučelje na Preklopniku 3 će biti *designated port*, a Gi0/1 sučelje na Preklopniku 1 će biti alternativno sučelje koje neće propuštati promet kako se ne bi stvorila petlja. Odabir *root port-a* na Preklopniku 1 i 3 je prethodno objašnjen. Na slici 23. uz uloge sučelja vidimo BID (*bridge ID*) preklopnika te *root ID* koji označava *root bridge*. Na Preklopniku 2 je *Root ID* njegov BID s obzirom da je on *root bridge* u ovoj mreži. Također, vidljivi su troškovi sučelja, za gigabitna (Gigabit Ethernet - Gi) sučelja trošak iznosi 4 kako je prethodno navedeno, a za brza Ethernet (Fast Ethernet - Fa) sučelja na koja su spojeni klijenti, trošak iznosi 19 jer sučelje radi na brzini od 100 Mbps (Tablica 5). Vidljivi brojači i statusi sučelja će biti objašnjeni u nastavku.

5.3.5. Statusi sučelja na preklopticima

Sva sučelja na preklopticima na kojima je omogućen STP se nalaze na jednom od 5 stanja (statusa):

- 1.) Stanje blokiranja (engl. *blocking state*)
- 2.) Stanje slušanja (engl. *listening state*)
- 3.) Stanje učenja (engl. *learning state*)
- 4.) Stanje prosljeđivanja/slanja (engl. *forwarding state*)
- 5.) Onemogućeno stanje (engl. *disabled state*) [23]

- 1.) Sučelje u blokirajućem stanju ne sudjeluje u prosljeđivanju okvira te odbacuje okvire koje je zaprimio od segmenta mreže na koji je spojen. Sučelje samo sluša i obrađuje BPDU okvire kako bi utvrdio lokaciju i *root ID* of *root bridge-a*. Sva sučelja na preklopticima su za vrijeme selekcije, odnosno uspostave STP-a u stanju blokiranja. Nakon 20 sekundi, ako preklopnik zaprimi BPDU koji inicira da bi to sučelje trebalo postati *designated* ili *root port*, će promijeniti svoje stanje. [23]
- 2.) Nakon stanja blokiranja, *root* ili *designated port* ulazi u stanje slušanja. Razlika u odnosu na blokirajuće stanje je ta da sučelje osim obrade BPDU okvira, iste i šalje kako bi informirao ostale preklopnike da se sučelje priprema pristupiti aktivnoj topologiji. Nakon 15 sekundi sučelje mijenja svoje stanje u stanje učenja. [23][9]
- 3.) U stanju učenja sučelje uz obradu i slanje BPDU okvira počinje ažurirati MAC tablicu preklopnika, ali se okviri i dalje ne prosljeđuju. Nakon 15 sekundi, sučelje mijenja svoje stanje u stanje prosljeđivanja. [23]
- 4.) Stanje prosljeđivanja je normalno stanje sučelja. Sučelje obrađuje i šalje BPDU okvire, ažurira MAC tablicu preklopnika te prosljeđuje promet klijenata. [23]
- 5.) Sučelje koje je nalazi u onemogućenom stanju ne sudjeluje u prosljeđivanju okvira ni nije dio STP-a jer se smatra da nije funkcionalan. [23]

5.3.6. STP brojači

STP konvergencija zahtjeva tri brojača, a to su:

- 1.) *Hello timer* – predstavlja interval između BDPU okvira te iznosi 2 sekunde
- 2.) *Forward delay timer* – vrijeme koje sučelje provede u stanju slušanja i stanju učenja te iznosi 15 sekundi.
- 3.) *Max age timer* – maksimalno vrijeme koje preklopnik čeka prije nego što pokuša promijeniti topologiju te iznosi 20 sekundi. [9]

5.3.7. PortFast

Portfast omogućava da sučelje odmah pređe u stanje prosljeđivanja nakon spajanja, bez da mora proći kroz stanja slušanja i učenja. Konfigurira se na razini sučelja (fizičkog ili logičkog) i to tipično na rubnim sučeljima⁷ jer se na njima ne očekuje spajanje mrežne opreme zbog koje može doći do kreiranja petlji u mreži. Kao što je prethodno navedeno, zbog brzog (automatskog) prelaska u stanje prosljeđivanja ignorirajući STP proces, dolazi do opasnosti pojave petlji. Osim standardne prakse da se PortFast konfigurira samo na rubnim sučeljima, uz PortFast se konfigurira i BDPU Guard koji štiti sučelje da zaprimi STP BDPU na način da ako BDPU stigne na sučelje na kojemu je konfiguriran BDPU Guard, on automatski stavlja to sučelje u *ErrDis*⁸ stanje u kojemu ostaje sve dok se ručno ne unesu konfiguracijske komande *shut* te *no shut*. Portfast i BDPU guard se konfiguriraju odvojeno i nije nužno da se stave oba na sučelje, ali zbog svojih funkcionalnosti je praksa da se konfiguriraju zajedno. [29]

6. Objašnjenje i razrada tipova STP-a (RSTP, PVST+, MSTP)

⁷ Rubna sučelja se odnose na pristupna (engl. *access*) sučelja na koja se spajaju krajnji uređaji [29]

⁸ *ErrDis* je drugim riječima onemogućeno stanje [29]

Kada je STP razvijen, udovoljavao je kriterijima tadašnjih računalnih mreža, međutim, razvitkom mreža očitavaju se njegovi nedostaci. Jedan od njih je to što je imao samo jedan *root bridge*, odnosno samo jednu instancu *spanning tree-a* za cijelu mrežu dok današnje mreže zahtijevaju različite referentne točke za pojedine VLAN-ove. Drugi nedostatak je spora konvergencija do stanja prosljeđivanja za svaku promjenu u topologiji. U nastavku su opisani protokoli koji su razvijeni u svrhu rješavanja tih nedostataka. [35]

6.1. RSTP

RSTP (engl. *Rapid Spanning Tree Protocol*) nosi oznaku 802.1W predstavlja evoluciju na 802.1D standard (STP). Terminologija i većina parametra je ostala nepromijenjena tako da ukoliko se pozna STP, nema poteškoća s implementacijom RSTP-a. [24] Kako je prethodno navedeno, na STP-u postoje 5 stanja sučelja. Gledajući s operativne strane, ne postoji razlika između stanja blokiranja, slušanja i onemogućenog stanja, svi odbacuju okvire i ne uče MAC adrese, iz tog razloga ih RSTP objedinjuje u jedno stanje koje se naziva odbacujuće stanje (engl. *discarding state*). [24]

Tablica 6. Usporedba statusa sučelja STP-a i RSTP-a

STP (802.1D)	RSTP (802.1W)	Da li je sučelje uključene u aktivnu topologiju.	Da li sučelje uči MAC adrese.
Onemogućeno stanje	Odbacujuće stanje	Ne	Ne
Stanje blokiranja	Odbacujuće stanje	Ne	Ne
Stanje slušanja	Odbacujuće stanje	Da	Ne
Stanje učenja	Stanje učenja	Da	Da
Stanje prosljeđivanja/slanja	Stanje prosljeđivanja/slanja	Da	Da

Izvor: [24]

Što se tiče uloga sučelja, *root* i *designated* sučelja ostaju ista dok se blokirajuće sučelje dijeli na rezervno sučelje (engl. *backup port*) i alternativno sučelje (engl. *alternative port*). Blokirajuće sučelje kod STP-a prima korisniji BDPU od onoga kojeg šalje na segmentu na kojemu

se nalazi te blokirajuće sučelje mora primati BDPU-e kako bi ostalo u blokirajućem stanju, isto se događa i kod RSTP-a. [24]

I kod rezervnog sučelja i alternativnog sučelja, sučelje mora biti u blokirajućem stanju. Sučelje postaje alternativno ukoliko zaprimi korisniji BDPU od drugog preklopnika, a postaje rezervno sučelje ukoliko zaprimi korisniji BDPU od istog preklopnika na kojem se nalazi. [24]

Najznačajnije svojstvo RSTP-a je brzi prijelaz (konvergenciju) sučelja do stanja prosljeđivanja. Ima mogućnost potvrde da sučelje može sigurno prijeći u stanje prosljeđivanja bez da se mora oslanjati na bilo kakvu konfiguraciju brojača (*forward delay* i *max age timer*). Kako bi se omogućila brza konvergencija sučelja koriste se dvije nove varijable, a to su rubna sučelja (engl. *edge ports*) i tip veze (engl. *link type*). [24]

Koncept rubnih sučelja u osnovi odgovara konceptu PortFast-a. Sva sučelja na koja su spojeni krajnji klijenti ne mogu kreirati petlje te se stoga direktno stavljaju u stanje prosljeđivanja, bez da moraju proći kroz prijašnja stanja. Ni rubna sučelja ni PortFast nemaju mogućnost generiranja promjene topologije kada se veza promjena. Sukladno tome, ako na rubno sučelje pristigne BDPU, ono automatski gubi status rubnog sučelja i postaje standardno *spanning tree* sučelje. Kod konfiguracije rubnih sučelja i dalje se upotrebljava ključna riječ PortFast kako bi se olakšala tranzicija sa STP-a na RSTP. [24]

Tip veze je automatski izveden iz dupleks moda sučelja. Za sučelje koja radi na *full-duplex* modu se pretpostavlja da je *point-to-point*, dok se *half-duplex* smatra kao dijeljeno sučelje. Većina linkova danas radi na *full-duplex* modu te ih samim time RSTP tretira kao *point-to-point* linkove. Takvi linkovi postaju kandidati za brzi prijelaz u stanje prosljeđivanja. RSTP taj brzi prijelaz može ostvariti samo na rubnim sučeljima i na *point-to-point* linkovima. [24]

6.2. PVST

PVST (engl. *Per-VLAN Spanning Tree*) je protokol tvrtke Cisco koji radi na način da ima odvojenu instancu STP-a za svaki VLAN posebno. Ta instanca omogućava da se STP za svaki VLAN neovisno konfigurira. [25] Cisco uređaji mogu raditi sa *spanning tree-ovima* na drugim PVST uređajima, ali ne mogu funkcionirati s uređajima koji rade na IEEE 802.1Q protokolu⁹ jer sučelja na tim uređajima rade na jedinstvenom *spanning tree-u*. [26] Kako bi isto funkcioniralo, PVST zahtjeva ISL (engl. *Inter-Switch Link*)¹⁰. [25]

PVST+ je ekstenzija PVST standarda. Glavna značajka protokola je što omogućava interoperabilnost između PVST-a i CST-a na Cisco uređajima te podržava 802.1Q standard. [25]

Glavni nedostatak PVST i PVST+ protokola je to što imaju broj instanca *spanning tree-a* koliko i VLAN-ova, odnosno za svaki VLAN je jedna instanca *spanning tree-a*. Uzeći u obzir da svaka instanca zauzima dio procesorske snage, PVST+ zahtjeva značajne resurse kada radi u mreži s puno VLAN-ova. [27]

6.3. MSTP

MSTP (engl. *Multiple Spanning Tree Protocol*) nosi oznaku IEEE 802.1s te omogućava da uređaji koriste više *spanning tree-a* što kao i kod PVST-a omogućava da promet koji pripada drugačijim VLAN-ovima može koristiti druge rute unutar istog LAN-a. [28]

Bitna razlika u odnosu na PVST je to što nije nužno da svaki VLAN ima svoju instancu *spanning tree-a* nego se VLAN-ovi mogu grupirati po želji te dodati pojedinom *spanning tree-u*. Primjerice, unutar lokalne mreže se nalazi 30 VLAN-ova, PVST bi za to imao 30 instanci *spanning tree-a* dok kod MSTP-a se VLAN-ovi mogu grupirati primjerice da 15 VLAN-ova pripada jednom *spanning tree-u*, 10 drugom te 5 trećem *spanning tree-u* što za rezultat daje 10 puta manje *spanning tree-a* u mreži što rezultira velikom uštedom procesorske snage.

⁹ IEEE 802.1Q standard koji podržava VLAN-ove na *Ethernet* mreži [9]

¹⁰ ISL je ekvivalent IEEE 802.1Q standardu napravljen od strane Cisco-a te je podržan samo na Cisco uređajima [30]

U praksi nije nužno da svaki VLAN se vrta u svom *spanning tree-u* tako da MSTP omogućava da svaki administrator koji konfigurira MSTP samostalno održi određeni balans između operabilnosti i utrošenih resursa. [27]

Također, MSTP je protokol otvorenog standarda tako da se može implementirati u mrežne uređaje bilo kojih proizvođača dok je PVST vezan za Cisco uređaje. S druge strane, mana MSTP je kompleksnost konfiguracije. [27]

7. Zaključak

Redundancija je iznimno važna kod dizajniranja bilo kakvih mreža pa tako i kod lokalnih mreža. Uvijek je potrebno imati rezervnu vezu u slučaju pada primarne kako ne bi afektiralo krajnje korisnike. U radu je prikazana “opasnost” koja se dogodi u mreži kod pogrešne implementacije redundancije uz prisustvo broadcast prometa. Broadcast promet je neizbježan te ga koriste brojne aplikacije bez kojih računalna povezanost ne bi bila moguća, stoga je potrebno pravilno rukovati s istim, pod time se misli na zatvaranje svih mogućih petlji u mreži. U simulaciji je prikazano kako broadcast promet nije jedini koji ima mogućnost napraviti petlje u mreži, odnosno prikazano je negativno mijenjanje MAC adresne tablice preklopnika tako da i unicast promet može završiti u petlji.

Broadcast storm ima mogućnost srušiti cijelu mrežu u samo nekoliko sekundi, u simulaciji provedenoj u završnom radu vidljivo je veliko opterećenje mreže u samo djeliću sekunde od pojave nekoliko okvira koji su završili u petlji. Također, pomoću alata *ping* je utvrđeno kako je komunikacija u takvom stanju mreže onemogućena. Uz povećanje lokalnih mreža, kompleksnost raste, ali princip ostaje isti. Postoji više protokola za sprječavanje *broadcast storm-a*, ali svi imaju istu zadaću te koriste isti algoritam za pronalazak jedinstvenog puta kroz lokalnu mrežu, odnosno *spanning tree-a*, kako za isti okvir ne bi postojalo više aktivnih ruta. S obzirom na njihovu jedinstvenu zadaću, ostaje na administratoru mreže da odabere protokol koji najviše odgovara za određenu lokalnu računalnu mrežu, ovisno o potrebama, broju VLAN-ova te omogućenim resursima. Kao što je vidljivo u simulaciji pri kojoj se prije početka provođenja morao isključiti STP na preklopticima, proizvođači mrežne opreme, u početnu konfiguraciju implementiraju STP kako bi odmah u početku smanjili mogućnost nastanka *broadcast storm-a*. *Broadcast storm* nije problem koji će s vremenom i razvitkom tehnologije nestati, uvijek je taj scenarij moguć te će kompleksnost njegova rješavanja povećanjem lokalnih mreža proporcionalno rasti. Kao što je do sada vidljiv razvitak protokola za rješavanje *broadcast storm-a* zbog određenih nedostataka istih, u budućnosti očekuje se daljnji napredak.

Popis literature:

- [1] <https://www.ionos.co.uk/digitalguide/server/know-how/broadcast-address/>
[Pristupljeno: 06.04.2020]
- [2] https://www.juniper.net/documentation/en_US/junos/topics/concept/broadcast-qfx-series-understanding.html [Pristupljeno: 06.04.2020]
- [3] <https://sysportal.carnet.hr/node/356> [Pristupljeno: 06.04.2020]
- [4] Milan Korac, Dario Car: Uvod u racunalne mreže, Algebra, Zagreb, 2014- godine
(http://www.umag.hr/sadrzaj/dokumenti/NATJECAJ_informaticki_referent_Uvod_u_racunalne_mreze_Visoko_uciliste_Algebra.pdf)
- [5] <https://geek-university.com/ccna/broadcast-domain-explained/>
[Pristupljeno: 07.04.2020]
- [6] <https://www.ciscopress.com/articles/article.asp?p=102157> [Pristupljeno: 10.04.2020]
- [7] <https://www.netmanias.com/en/post/techdocs/5998/dhcp-network-protocol/understanding-the-basic-operations-of-dhcp> [Pristupljeno: 10.04.2020]
- [8] https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_arp/configuration/15-mt/arp-15-mt-book/arp-config-arp.html [Pristupljeno: 10.04.2020]
- [9] CISCO CCNAv7 akademija: Switching, Routing, and Wireless Essentials
- [10] <https://geek-university.com/ccna/how-switches-forward-frames/>
[Pristupljeno: 22.04.2020]
- [11] <https://www.omniseu.com/cisco-certified-network-associate-ccna/what-is-broadcast-storm.php> [Pristupljeno: 22.04.2020]
- [12] https://www.cisco.com/c/dam/en_us/training-events/netacad/course_catalog/docs/Cisco_PacketTracer_DS.pdf
[Pristupljeno: 22.04.2020]
- [13] https://www.it-market.com/en/cisco-systems/cisco-switch-series/cisco-catalyst-2950-series/cisco-systems-ws-c2950t-24?gclid=CjwKCAjw-YT1BRAFEiwAd2WRtmqqfYldTp6_bxHBveDRMmMLXG_xbqaodVyIRuswYpdQg6n8n92PEh0Cv5wQAvD_BwE [Pristupljeno: 23.04.2020]

- [14] <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html> [Pristupljeno: 02.05.2020]
- [15] https://www.tutorialspoint.com/data_structures_algorithms/spanning_tree.htm
[Pristupljeno: 02.05.2020]
- [16] https://www.tutorialspoint.com/data_structures_algorithms/kruskals_spanning_tree_algorithm.htm [Pristupljeno: 02.05.2020]
- [17] <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html> [Pristupljeno: 03.05.2020]
- [18] <https://www.computernetworkingnotes.com/ccna-study-guide/stp-spanning-tree-protocol-explained-with-examples.html> [Pristupljeno: 03.05.2020]
- [19] <https://www.omniseccu.com/cisco-certified-network-associate-ccna/what-is-a-root-bridge-switch.php> [Pristupljeno: 04.05.2020]
- [20] <http://www.firewall.cx/networking-topics/protocols/spanning-tree-protocol/1054-spanning-tree-protocol-root-bridge-election.html> [Pristupljeno: 10.05.2020]
- [21] <https://www.omniseccu.com/cisco-certified-network-associate-ccna/what-is-a-root-port.php> [Pristupljeno: 10.05.2020]
- [22] <https://www.omniseccu.com/cisco-certified-network-associate-ccna/what-is-a-designated-port.php> [Pristupljeno: 10.05.2020]
- [23] <https://www.omniseccu.com/cisco-certified-network-associate-ccna/spanning-tree-port-states.php> [Pristupljeno: 10.05.2020]
- [24] <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html> [Pristupljeno: 10.05.2020]
- [25] <https://www.omniseccu.com/cisco-certified-network-associate-ccna/per-vlan-spanning-tree-pvst-and-per-vlan-spanning-tree-plus-pvst+.php> [Pristupljeno 01.06.2020]
- [26] <http://docs.ruckuswireless.com/fastiron/08.0.70/fastiron-08070-l2guide/GUID-F9905D20-F2BB-4286-B606-49BC36596CF1.html>[Pristupljeno 01.06.2020]
- [27] A Dell Technical White Paper: Comparison between PVST+ and MSTP, studeni 2014 (https://downloads.dell.com/solutions/networking-solution-resources/STP-MSTP_v5.pdf) [Pristupljeno 02.06.2020]
- [28] https://gtacknowledge.extremenetworks.com/articles/How_To/Understanding-MSTP
[Pristupljeno 03.06.2020]

- [29] https://www.arubanetworks.com/techdocs/ArubaOS_64x_WebHelp/Content/ArubaFrameStyles/Branch [Pristupljeno 16.06.2020]
- [30] <https://www.omniseu.com/cisco-certified-network-associate-ccna/inter-switch-link-isl-vlan-tagging.php> [Pristupljeno 16.06.2020]
- [31] <https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works/> [Pristupljeno 16.06.2020]
- [32] https://documentation.meraki.com/MS/Layer_3_Switching/Layer_3_vs_Layer_2_Switching [Pristupljeno 16.06.2020]
- [33] <https://sysportal.carnet.hr/node/356> [Pristupljeno 16.06.2020]
- [34] <https://sysportal.carnet.hr/node/352> [Pristupljeno 16.06.2020]
- [35] <https://www.learnisco.net/courses/icnd-2/vlans-and-spanning-tree/stp-protocol-types.html> [Pristupljeno 30.06.2020]

Popis ilustracija

Popis slika:

Slika 1. Broadcast odašiljanje	3
Slika 2. Kolizijska domena koristeći hub	5
Slika 3. Kolizijska domena topologije centralnog vodiča	6
Slika 4. Prikaz broadcast domena	7
Slika 5. Podjela broadcast domena putem VLAN-ova	8
Slika 6.. Prikaz rada preklopnika kada je određena MAC adresa poznata	11
Slika 7. Prikaz rada preklopnika kada je određena MAC adresa nije poznata	12
Slika 8. Prikaz redundancije preklopnika	13
Slika 9. Prikaz nastajanja petlji I.....	14
Slika 10. Prikaz nastajanja petlji II.	14
Slika 11. Prikaz nastajanja petlji III.....	15
Slika 12. Topologija simulacijske mreže	17
Slika 13. Kreiranje broadcast storm-a I.	19
Slika 14. Kreiranje broadcast storm-a II.	19
Slika 15. Kreiranje broadcast storm-a III.....	20
Slika 16. MAC adresna tablica Preklopnika 1	21
Slika 17. Pokušaj komunikacije između klijenata	22
Slika 18. Pronalazak spanning tree-a	23
Slika 19. Graf prije primjene Kruskalovog algoritma	25
Slika 20. Graf poslije primjene Kruskalovog algoritma	26
Slika 21. Odabir root bridge-a	28
Slika 22. Odabir uloga sučelja	31
Slika 23. Karakteristike STP-a na Preklopniku 1 i 2	32

Popis tablica:

Tablica 1. Prikaz podataka u ARP zahtjevu.....	13
Tablica 2. Mrežni parametri.....	18
Tablica 3. Vrijednosti troškova svake veze prema grafu.....	25
Tablica 4. Polja u BDPU okviru	27
Tablica 5. Troškovi sučelja.....	29
Tablica 6. Usporedba statusa sučelja STP-a i RSTP-a	35