pd.tvz.hr
POLYTECHNIC & DESIGN Vol. 7, No. 1, 2019.
DOI: 10.19279/TVZ.PD.2019-7-1-09

SPANNING TREE PROTOKOL

SPANNING TREE PROTOCOL

Jelečki Nikola[1], Turkalj Vedran[2]

[1]Tehničko veleučilište u Zagrebu, Vrbik 8, Zagreb, Hrvatska, Student
[2]Tehničko veleučilište u Zagrebu, Vrbik 8, Zagreb, Hrvatska

Sažetak

Interna računalna mreža je velika računalna mreža koja se sastoji od više međusobno povezanih LAN mreža i obično se nalaze na istom geografskom području. Prema hijerarhijskom mrežnom modelu dijeli se u tri jasno odvojena sloja, pristupa, distribucije i jezgre.
Spanning Tree protokol (STP) ima zadatak utvrditi postoje li preklopne petlje te onemogućiti ili u potpunosti blokirati sve portove (sučelja) potrebne da se izbjegnu petlje u navedenoj topologiji. Također omogućava redundantnost veza računalne mreže tako da se računalne mreže na sloju 2 mogu pravovremeno oporaviti od grešaka bez intervencije administratora. Upravo to objašnjava važnost drugog sloja odnosno sloja distribucije kod funkcioniranja Spanning Tree protokola. Izgradnja STP protokola je višestupanjski proces odabira osnovnog mosta (Root Bridge), osnovnih portova (Root Ports), namjenskih portova te stavljanje portova u stanje blokiranja kako bi se spriječio nastanak petlja. Alternative STP-u kao što su SPB i MLAG još uvijek nisu stekle šire usvajanje jer su ili vezane uz pojedinog proizvođača ili su standardi implementirani na međusobno nekompatibilne načine te stoga svoje mjesto uglavnom nalaze u velikim mrežama podatkovnih centara. Zbog ograničenja većine drugih opcija, STP je još uvijek jedina opcija u heterogenim okruženjima.

Ključne riječi: *spanning tree protokol (STP), lokalna računalna mreža (LAN), redundandnost veza, preklopne petlje*

Abstract

A campus network is an enterprise network that consist of many connected LANs that are all usually in the same geographic area.
According to the Network Hierarchy, a campus network has three separated layers - Access Layer, Distribution Layer and Core Layer.
Spanning Tree Protocol was designed to identify and prevent switching loops with disabling or blocking ports. It also provides network link redundancy so that a Layer 2 switched network can recover from failures without intervention in a timely manner. That explains importance of distribution layer or Layer 2 in the successful operation of Spanning Tree Protocol.
The process of building STP Protocol is multistage process of electing Root Bridges, Root Ports, Designated Ports and putting ports in blocked state in order to prevent formation of switching loops. STPs alternatives such as SPB and MLAG have not yet received broader adoption because they are either tied to specific manufacturers or standards are still implemented in a non-compatible ways and are therefore mostly used in a large data center networks. Due to limited support for most other options, STP is still the only option in heterogeneous environments.

Keywords: *spanning tree protocol (STP), local area network (LAN), network link redundancy, switching loops*

1. Uvod

1. *Introduction*

Sloj distribucije odnosno drugi sloj hijerarhijskog modela računalne mreže najvažniji je sloj kod funkcioniranja Spanning Tree protokola te ima više funkcija. Tri su osnovne funkcije drugog sloja učenje adresa, što podrazumijeva pamćenje izvora hardverske adrese svakog okvira primljenog na sučelje i unos tih informacija u MAC bazu podataka, zatim prosljeđivanje/

filtriranje odluka što podrazumijeva prosljeđivanje okvira na određeni odredišni port, te izbjegavanje petlja što podrazumijeva sprječavanje nastanka mrežnih petlji.

Spanning Tree Protokol (STP) razvijen je kako bi spriječio tzv. „broadcast storms“ (oluje) uzrokovane preklopnom petljom te je izvorno definiran u IEEE 802.1D. STP protokol ima zadatak utvrditi postoje li uopće petlje te onemogućiti ili u potpunosti blokirati sve portove potrebne da se izbjegnu petlje u navedenoj topologiji, no blokirani portovi također mogu biti reaktivirani u slučaju da dođe do pada ostalih portova. Zahvaljujući tome STP protokol je u mogućnosti održavati redundantnost i sačuvati otpornost na pogreške. Međutim, budući da su portovi blokirani kako bi spriječili petlje, STP protokol ne podržava mogućnost balansiranja opterećenja. Protokol STP omogućava redundantnost veza računalne mreže tako da se računalne mreže na sloju 2 mogu pravovremeno i samostalno oporaviti od grešaka, bez intervencije administratora. Upravo to objašnjava važnost drugog sloja odnosno sloja distribucije kod funkcioniranja Spanning Tree protokola.

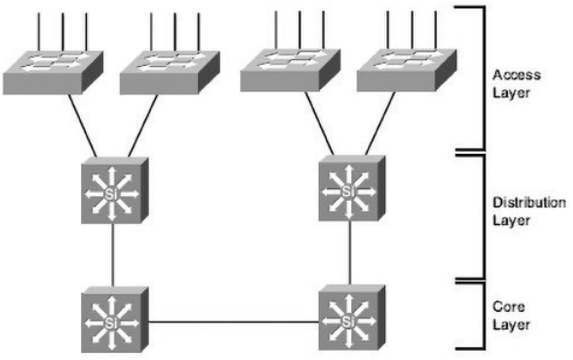
Izgradnja Spanning Tree protokola je višestupanjski proces konvergencije koji uključuje odabir osnovnog mosta (Root Bridge), odabir osnovnih portova (Root Ports), odabir namjenskih portova te, po potrebi, stavljanje portova u stanje blokiranja kako bi se spriječio nastanak petlji.

2. Struktura hijerarhijske računalne mreže

2. *Hierarchical network design model*

Hijerarhijski model internu računalnu mrežu dijeli u tri jasno odvojena sloja (slika 1), od kojih svaki sloj ima osobine koje omogućuju da se na odgovarajućem mjestu u internoj računalnoj mreži mogu koristiti fizičke i logičke mreže. Ti slojevi su:

1. Sloj pristupa,
2. Sloj distribucije i
3. Sloj jezgre.



Slika 1 *Struktura hijerarhijske računalne mreže[1]*

Figure 1 *Hierarchical Network Design Model[1]*

2.1. Sloj pristupa

2.1. *Access layer*

Sloj pristupa postoji tamo gdje su krajnji korisnici povezani u računalnu mrežu. Uređaji na ovom sloju, poznati i kao pristupni preklopnici u zgradi („*building access switch*“), trebali bi imati sljedeće osobine:

- niske troškove na portu preklopnika,
- veliku gustoću porta,
- skalabilne izlazne veze k višim slojevima,
- funkcije pristupa korisnika, te
- elastičnost izlaznih veza.[1]

2.2. Sloj distribucije

2.2. *Distribution layer*

Sloj distribucije predstavlja vezu između sloja pristupa i sloja jezgra interne računalne mreže. Uređaji na ovom sloju, poznati i kao distribucijski preklopnici u zgradi (*„building distribution switch“*), trebali bi imati sljedeće osobine:

- agregaciju više uređaja na sloju pristupa,
- veliki protok na sloju 3 (Layer 3) za obradu paketa,
- mogućnost uspostavljanja osigurane veze i veze koja kontrolira pravilima pristupa ili filterima poruka
- QoS,
- skalabilne i elastične veze velike brzine k slojevima jezgre i pristupa.[1]

U sloju distribucije, izlazne veze sa svih uređaja na sloju pristupa se agregiraju.

Preklopnici na sloju distribucije moraju biti takvi da mogu obrađivati cjelokupni mrežni promet svih uređaja koji su povezani u računalnu mrežu, ti preklopnici moraju imati nekoliko portova velike brzine kako bi se mogli skupljati svi preklopnici na sloju pristupa.

2.3. Sloj jezgre
2.3. *Core layer*

Sloj jezgre u internoj računalnoj mreži osigurava povezanost svih uređaja na sloju distribucije. Jezgra, koja se ponekad naziva glavna mreža (*„backbone“*), treba efikasno preklapati promet. Uređaji na sloju jezgre, poznati i kao preklopnici glavne računalne mreže (*„campus backbone switch“*), trebali bi imati sljedeće osobine:

- veliki protok na sloju 2 i sloju 3,
- manipulacija paketima mora biti efikasna i bez nepotrebne obrade,
- trebali bi biti redundantni i elastični kako bi im se povećala dostupnost.[1]

3. Modeli internih mreža
3. *Interior network models*

Interna računalna mreža je velika računalna mreža koja se sastoji od mnogo LAN mreža u jednoj ili više zgrada, koje su povezane i obično se nalaze na jednom užem geografskom području. Interne mreže obično se sastoje od *Etherneta*, 802.1 bežičnih LAN mreža, brzih *Fast Ethernet-a*, *Fast EtherChannela i Gigabit Ethernet* te *10 Gigabit Ethernet* LAN mreža.[1]
Postoje razni modeli računalnih mreža koji se mogu upotrijebiti za klasificiranje i strukturiranje internih mreža.

3.1. Model dijeljene računalne mreže
3.1. *Shared Network Model*

Ranih devedesetih interne mreže tradicionalno su se sastojale od jedne LAN mreže na koju su se svi korisnici prijavljivali i koristili. Svi uređaji u LAN mreži morali su dijeliti propusni opseg. Raspoloživost računalne mreže i performanse padale su razmjerno povećanju broja uređaja u računalnoj mreži.

Ukoliko su dva ili više uređaja pokušala poslati svoje podatke istovremeno, dolazilo je do sudara u računalnoj mreži pa su svi uređaji morali prestati sa slanjem podataka i čekati novu priliku da ih pošalju. Ovakav tip LAN mreže naziva se kolizijska domena jer su svi uređaji osjetljivi na koliziju.

3.2. Model segmentacije LAN mreže
3.2. *LAN segmentation Model*

Lokaliziranje mrežnog prometa i efikasno smanjenje broja radnih stanica u segmentu računalne mreže naziva se segmentacija računalne mreže („network segmentation“). Segmentacija računalne mreže neophodna je za sprječavanje sudara i zbog smanjenja performansi segmenta računalne mreže.[1]

Smanjivanjem broja radnih stanica smanjuje se vjerojatnost nastanka sudara budući da manji broj radnih stanica može u nekom trenutku slati podatke. Segmentacija računalne mreže može se ostvariti korištenjem usmjerivača ili preklopnika.

3.3. Modeli mrežnog prometa
3.3. *Network Traffic Models*

Da bi se uspješno napravila interna računalna mreža, potrebno je razumijeti kakav mrežni promet generiraju aplikacije koje se koriste, kao i mrežni promet koji se odvija od i prema pojedinim dijelovima računalne mreže. Svi uređaji u računalnoj mreži će kroz nju slati podatke te se na svakom uređaju može izvršavati više aplikacija koje generiraju podatke različitog oblika i količine.[1]

3.4. Model predvidive računalne mreže
3.4. *Predictive Computer Network Model*

Kako bi se smanjili troškovi održavanja i povećala dostupnost računalne mreže, potrebno je voditi brigu o njenom predvidljivom ponašanju. U slučaju da se interna računalna mreža treba brzo oporaviti od padova i prometa topologije, to bi trebala učiniti na predvidljiv način. Računalnu mrežu stoga je potrebno kreirati na način da se lako može proširiti i nadograditi.

Zbog velike raznolikosti protokola i višesmjernog mrežnog prometa, računalna mreža trebala bi biti takva da sa stajališta mrežnog prometa može podržati primjenu pravila 80/20, što znači da računalnu mrežu treba kreirati prema mrežnom prometu, a ne prema tipu mrežnog prometa.[1]

4. Standard IEEE 802.1D
4. *IEEE 802.1D standard*

Struktura kvalitetne računalne mreže ne uključuje samo učinkovit transfer paketa ili okvira, već uzima u obzir i način za brzo oporavljanje od grešaka koje mogu nastati u računalnoj mreži.

Preklopni blok (*„switch block“*) sadrži balansiranu mješavinu funkcionalnosti slojeva 2 i 3, koja postoji u slojevima pristupa i distribucije. Preklopnici sloja 2 koji se nalaze na sloju pristupa povezuju krajnje korisnike interne računalne mreže.[1] Sloj 2 prenosi podatke između svih povezanih preklopnika u centralnoj točki povezivanja. Funkcionalnost sloja 3 se također može osigurati u obliku usmjeravanja i drugih mrežnih usluga. Prema tome, uređaj sloja distribucije treba biti višeslojni preklopnik.[1]

Dok se u okruženju sloja 3 protokoli usmjeravanja koriste za praćenje nepotrebnih putanja do odredišne računalne mreže, u okruženju sloja 2 (komutiranje ili premošćivanje) ne koristi se niti jedan protokol za usmjeravanje, a aktivne nepotrebne putanje nisu dozvoljene niti poželjne. Umjesto toga, za transport podataka između računalnih mreža ili portova preklopnika koristi se neki drugi oblik premošćivanja.
Protokol STP omogućava redundantnost veza računalne mreže tako da se računalne mreže na sloju 2 mogu pravovremeno oporaviti od grešaka bez intervencije administratora te je definiran standardom IEEE 802.1D.[4] Također, STP protokol koristi i koncept troškova. Kada se bira osnovni port izračunava se trošak osnovne putanje. Vrijednost troška predstavlja ukupni trošak svih veza koje vode prema osnovnom mostu. Svakoj vezi preklopnika pridružuje se trošak koji se naziva trošak putanje (*„Path Cost“*). Originalni standard IEEE 802.1D trošak putanje definira kao količnik 1000Mbps i propusnog opsega veze izraženo u megabitima u sekundi.[3]

Poznavanje standarda IEEE 802.1D STP je vrlo važno jer se protokol općenito koristi za održavanje kontinuiranih računalnih mreža i računalne mreže s mostovima. Međutim, sada se taj protokol smatra vlasničkim protokolom čija vremena za promjenu topologije i konvergencije više nisu prihvatljiva.

5. Spanning tree protokol
5. *Spanning Tree Protocol*

Spanning tree protokol (STP) razvijen je kako bi spriječio *„broadcast storms“* (oluje) uzrokovane preklopnom petljom te je izvorno definiran u IEEE 802.1D.

Spanning tree protokoli pokrenuti od strane preklopnika izgraditi će kartu ili topologiju cijele preklapajuće mreže. U tom slučaju, STP protokol će utvrditi postoje li uopće petlje te onemogućiti ili u potpunosti blokirati sve portove potrebne da se izbjegnu petlje u navedenoj topologiji. Blokirani portovi također mogu biti reaktivirani u slučaju da dođe do pada ostalih portova. Zahvaljujući tome STP protokol je u mogućnosti održavati redundantnost i sačuvati otpornost na pogreške. Međutim, budući su portovi blokirani kako bi spriječili petlje, STP protokol ne podržava mogućnost balansiranja opterećenja.[2]

Tri su podvrste izvorne 802.1D verzije STP protokola:

- *Common Spanning Tree (CST)* – koristi jednu instancu STP-a za sve VLAN-ove,
- *Per–VLAN Spanning Tree (PVST)* – zapošljava zasebnu instancu STP-a za svaki VLAN te poboljšava fleksibilnost i performanse, a nije kompatibilan s CST-om,
- *Per – VLAN Spanning Tree Plus (PVST+)* – kompatibilan je s CST-om i PVST-om, te podržava i ISL i 802.1Q enkapsulaciju.[2]

Međutim, u okruženju sloja 2 (komutiranje ili premošćivanje) ne koristi se ni jedan protokol za usmjeravanje, a aktivne nepotrebne putanje nisu dozvoljene niti poželjne. No umjesto toga, za transport podataka između računalnih mreža ili portova preklopnika koristi se neki drugi oblik premošćivanja.

Protokol STP omogućava redundantnost veza računalne mreže tako da se računalne mreže na sloju 2 mogu pravovremeno oporaviti od grešaka bez intervencije administratora.

6. Konfiguracija razgranatog stabla
6. *Spanning tree configuration*
6.1. Osnovni most STP protokola
6.1. *STP Protocol Root Bridge*

STP i njegova izračunavanja su predvidiva. Međutim, razni faktori mogu neprimjetno utjecati na STP odluke, tako da se može dobiti neočekivana struktura stabla koja nije idealna. Poziciju osnovnog mosta (*„Root Bridge"*) treba odrediti tijekom projektiranja računalne mreže. Kada je pravilno konfiguriran onda se za ravnomjerno distribuiranje mrežnog prometa može upotrijebiti redundantna veza. Također, STP protokol se može konfigurirati na način da brže konvergira i da se ponaša predvidljivo kada se promijeni topologija računalne mreže.[1]

6.2. Konfiguracija osnovnog mosta
6.2. *Root bridge configuration*

Osnovni most (i sekundarni most), kao zajednička referentna točka, trebaju se nalaziti blizu centra računalne mreže sloja 2. Na primjer, preklopnik na sloju distribucije bio bi bolji izbor za osnovni most nego preklopnik na sloju pristupa jer se očekuje da veći mrežni promet prolazi kroz sloj distribucije. U ravnoj komutiranoj računalnoj mreži bez usmjerivača, preklopnik blizu servera bio bi efikasniji osnovni most od svih drugih preklopnika u računalnoj mreži. Veći dio mrežnog prometa bi dolazio i odlazio sa servera i imao bi koristi od unaprijed definiranih direktnih putanja. Preklopnik se može konfigurirati tako da bude osnovni most koristeći jednu od dvije metode koje su konfigurirane na slijedeći način:

- Zadaje se prioritet mosta tako da preklopnik ima niži prioritet identifikatora mosta od podrazumijevanog prioriteta identifikatora mosta kako bi bio odabran za osnovni most. Moraju se znati prioriteti mostova svih ostalih preklopnika u VLAN mreži tako da možete zadati vrijednost koja je manja od svih ostalih vrijednosti.

Switch(config)# *spanning-tree* ***vlan ID priority 0-65535***

Podrazumijevana vrijednost za prioritet mosta je 32768, ali se može zadati vrijednost iz opsega od 0-65535. Ako se koristi prošireni sistemski identifikator, podrazumijevana vrijednost za prioritet mosta je 32768 plus broj VLAN mreže. U tom slučaju može se zadati vrijednost iz opsega od 0 do 64440, ali samo kao višekratnik broja 4096. Poželjno je zadati niži prioritet mosta. Preklopnici izvršavaju jednu instancu STP protokola za svaku VLAN mrežu (PVST+) pa VLAN ID uvijek mora biti zadan.

Switch(config)# *spanning-tree* ***vlan ID*** *priority 4096*

Switch(config)# *spanning-tree vlan vlan-id root* ***{primary | secondary} [diameter*** *diameter**]***

Prethodna naredba zapravo je makro na preklopnicima koji izvršava nekoliko drugih naredbi. Rezultat je direktniji i automatiziran način da se preklopnik postavi za osnovni most. Svojstva mosta nisu zadana prethodnom komandom. Preklopnik umjesto toga mijenja svoje STP vrijednosti u skladu s tekućim vrijednostima koje se koriste u aktivnoj računalnoj mreži. Te se vrijednosti mijenjaju samo jednom, onda kada se zada makro naredba. Rezerviranu riječ *Primary* zadaje se kako bi se preklopnik pokušao postaviti za osnovni most. Tom naredbom se mijenja prioritet mosta preklopnika tako da postane manji od prioriteta mosta tekućeg osnovnog mosta.[1]

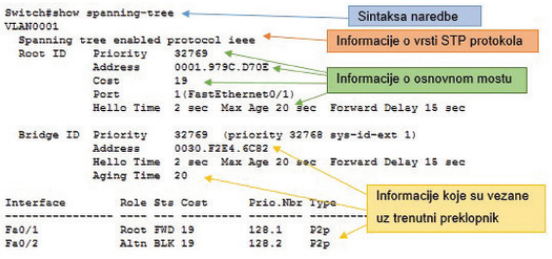
Kada je prioritet tekućeg osnovnog mosta veći od 24576, lokalni preklopnik za prioritet svog mosta zadaje vrijednost 24576. Kada je pak prioritet tekućeg osnovnog mosta manji od te vrijednosti, lokalni preklopnik za prioritet svog mosta zadaje vrijednost koja je manja za 4096 od prioriteta tekućeg osnovnog mosta. Za prioritet osnovnog mosta za sekundarni osnovni most zadaje se vrijednost 28672. Ne postoji način da se ispita računalna mreža kako bi se pronašao drugi potencijalni sekundarni osnovni most jer ne postoje objave ili izbor sekundarnih osnovnih mostova. Umjesto toga, koristit će se zadani prioritet sekundarnog mosta pod pretpostavkom da je manji od unaprijed definiranih prioriteta (32768) koji postoje na ostalim preklopnicima.

Također, može se promijeniti promjer računalne mreže tako da se rezervirana riječ *Diameter* upotrebljava prilikom zadavanja prethodne naredbe.[1]

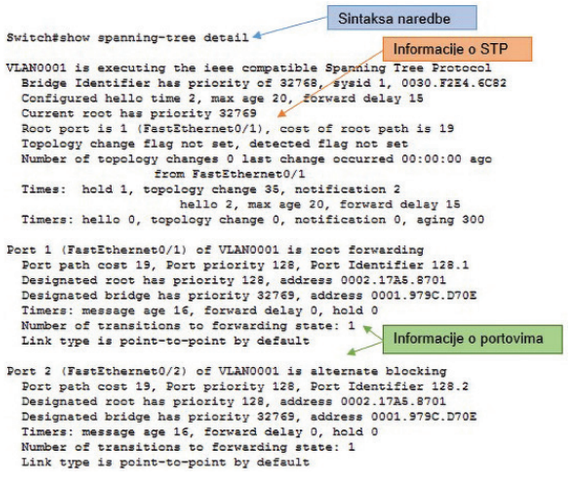
7. SPANNING TREE PROTOKOL kroz osnovne naredbe

7. *SPANNING TREE PROTOCOL through basic commands*

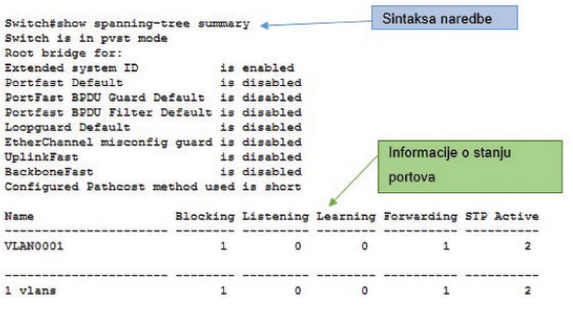
Koristeći naredbu *Switch#* ***show spanning-tree*** dolazimo do informacija vezanih za svaku VLAN mrežu koja se nalazi na preklopniku:



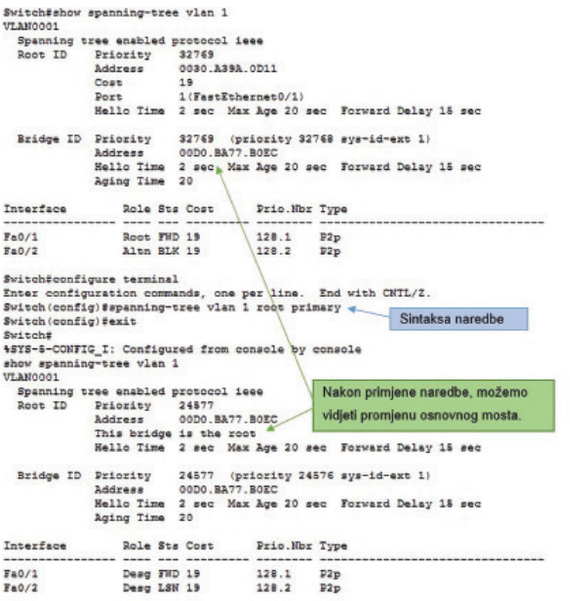
Koristeći naredbu *Switch#* ***show spanning-tree detail*** dobivamo detaljne informacije o STP-u i o svim portovima preklopnika:



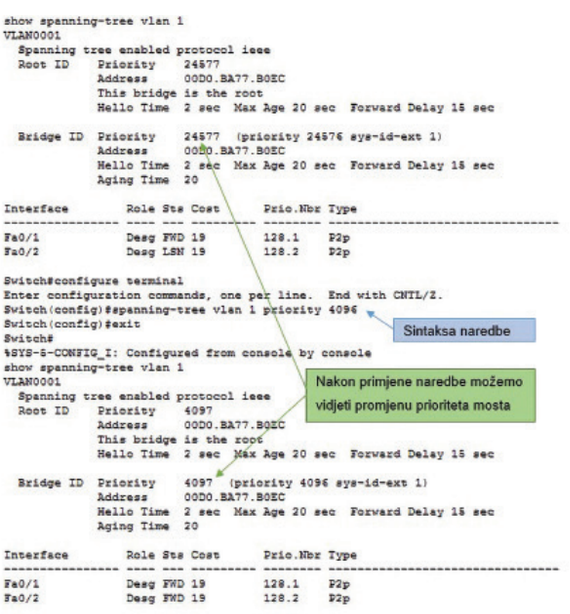
Koristeći naredbu ***Switch# show spanning-tree summary*** dobivamo informaciju o stanju portova u VLAN mreži:



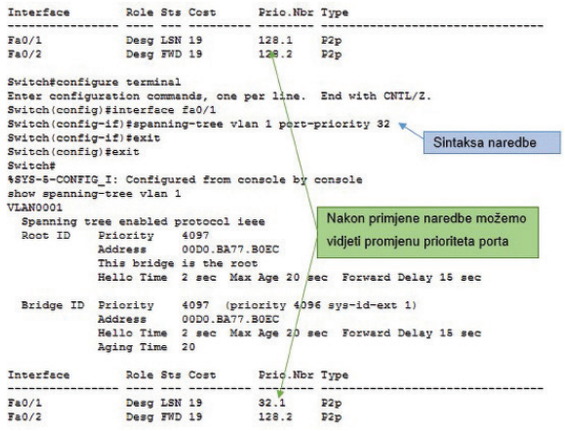
Naredbom ***Switch(config)#*** *spanning-tree vlan* ***vlan-ID*** *root* ***primary*** promijenjen je osnovni most. Može se vidjeti razlika u Bridge ID Priortiy, no nije ništa ručno mijenjano nego se automatski promijeni:



Koristeći naredbu ***Switch(config)#*** *spanning-tree* ***vlan ID priority 0-65535*** promijenjen je Bridge ID Priority.



Koristeći naredbu ***Switch(config)#*** *interface fastEthernet 0/1* te zatim naredbu ***Switch(config-if)#*** *spanning-tree vlan ID* ***port-priority 0-255*** promijenjen je prioritet porta:



8. Usporedba STP-a s SPB-om i drugim alternativnim rješenjima

8. *Comparison of STP with SPB and other alternative solutions*

Koja je najbolja alternativa Spanning Tree protokolu?

Dvije najčešće raspravljane alternative STP-u su Shortest Path Bridging (SPB) i TRansparent Interconnect of Lots of Links (TRILL). STP ima svojih ograničenja poput nepotrebnih protoka paketa, slabijih vremena konvergencije i održavanja CAM tablica. Kako Spanning Tree domena u mreži raste s širenjem mreže, ona postaje sve sporija, složenija i manje učinkovita.

Među proizvođačima mrežne opreme postoji suglasje da bi IT tvrtke trebale gledati dalje od STP-a, što je nažalost i jedina točka oko koje se slažu. Zaključili su i da je Multi-Chassis Link Aggregation (MLAG) dobra zamjena za STP, ali i da svaki proizvođač ima drugačiju implementaciju i nisu se uspjeli dogovoriti oko toga kako bi se to trebalo provesti. Osim toga, neki gledaju na MLAG kao potencijalno dugoročno rješenje, dok ga drugi smatraju više srednjoročnim rješenjem dok se ne postigne konsenzus oko jednog od nekoliko rješenja zasnovanih na standardima.

Osim SPB-a i TRILL-a postoje još i LACP (802.3ad Link Aggregation Control Protocol), LAG, MC-LAG (Multi-Chassis Link Aggregation Group, drugo ime za MLAG) i mLACP, QFabric, SDN i druga rješenja od kojih je većina specifična za određenog proizvođača i trebalo bi ih izbjegavati ako se želi izbjeći tzv. „vendor lock-in“ (vezivanje uz određenog dobavljača):

- Extreme - Multi System Link Aggregation (MLAG)
- HP – IRF (Intelligent Resilient Framework), SPB, TRILL
- Avaya – Switch Clustering (SC), SPB
- Cisco – FabricPath (baziran na TRILL-u, ali nije s njime kompatibilan), STP, VSS, vPC
- Brocade – Virtual Cluster Switching, TRILL, Data Center Bridging (DCB)
- Juniper – QFabric

(IRF je bila prva tehnologija virtualizacije mreže u industriji i omogućila je korisnicima uklanjanje STP-a i VRRP-a na svakom sloju mreže.)

LACP (Link Aggregation Control Protocol)
Unutar IEEE specifikacije, Link Aggregation Control Protocol (LACP) pruža metodu za kontrolu povezivanja nekoliko fizičkih sučelja kako bi se formirao jedan logički kanal. LACP omogućuje mrežnom uređaju da pregovara automatsko povezivanje linkova slanjem LACP paketa na „peer“ (izravno povezan uređaj koji također ima implementiran LACP).

MLAG (MC-LAG)
MC-LAG-a je tip umrežavanja koji se postiže MC-LAG tehnologijom. MLAG (MC-LAG), skraćenica za Multi-Chassis Link Aggregation Group, tehnologija je za agregaciju linkova između više Ethernet preklopnika u podatkovnim centrima. MLAG konfiguracija centralizira sastavna sučelja na odvojenim šasijama i služi primarno za dijeljenje opterećenja linkova zbog povećanja propusnosti i osiguravanje redundancije u slučaju kvara jednog od uređaja. LAG je definiran IEEE 802.1AX-2014 standardom, gdje MC-LAG nije uključen, pa su nažalost implementacije MLAG-a različite kod različitih proizvođača; međutim, kombinirane šasije su i dalje usklađene s IEEE 802.1AX-2014 standardom.

Koja je najznačajnija razlika između MLAG-a i STP-a?

Općenito, konfiguracija MC-LAG HA („High Availability“) je superiornija STP-u jer sve veze mogu dijeliti promet tijekom normalnog rada, dočim Spanning Tree mora onemogućiti neke veze kako bi se postigla prevencija petlji.

MC-LAG je također nadmoćan i nad LAG tehnologijom zbog redundancije na razini čvora dodanu na redundantnost na razini veza. HA MLAG konfiguracija također nadilazi spanning tree, jer nije potrebno onemogućivanje nekih veza za prevenciju petlji.

SPB (Shortest Path Bridging) i TRILL (TRansparent Interconnect of Lots of Links)
U prvom dijelu članka smo objasnili kako STP blokira redundantne puteve da bi spriječio nastanak petlji. Time se ograničava ukupno dostupna propusnost mreže koja je sve potrebnija kako se povećava promet u visoko virtualiziranim podatkovnim centrima.
Potaknuti tim nedostacima, Internet Engineering Task Force (IETF) i Institute of Electrical and Electronics Engineers (IEEE) vratili su priču na početak i stvorili dva konkurentna standarda mrežnog povezivanja - TRILL i SPB - usmjerenih zadovoljavanju rastućih potreba suvremenih podatkovnih centara. Nažalost, ova su dva pristupa i standarda općenito nekompatibilna, a još je gore što i mnoge implementacije istih protokola nisu interoperabilne.

Shortest Path Bridging (SPB), naveden u IEEE 802.1aq standardu, je tehnologija umrežavanja računala namijenjena pojednostavljenom dizajniranju i konfiguriranju mreža, uz omogućavanje „multipath“ usmjeravanja. SPB pruža visoko pouzdanu, visoko skalabilnu višesmjernu mrežu u kojoj se usluge pružaju samo na mjestima pristupa mreži. SPB omogućuje da sve veze budu aktivne s jednakom vrijednošću (isti „cost-paths“), omogućava mnogo veće mrežne topologije na sloju 2, podržava bržu konvergenciju mreže (dolazak u stabilno stanje) i poboljšava učinkovitost omogućavajući prometu da koristi sve mrežne veze. Sama priroda dizajna praktički otklanja svaku mogućnost ljudske pogreške tijekom konfiguracije te također zadržava mogućnost jednostavnog širenja koja je i utvrdila Ethernet kao praktički isključivi mrežni protokol na 2. sloju.

Podržani su unicast, multicast i broadcast, a svo usmjeravanje je bazirano na simetričnim najkraćim putevima. Upravljačka razina se temelji na Intermediate System to Intermediate System (IS-IS) protokolu, korištenjem malog broja proširenja definiranih u RFC 6329.

Shortest Path Bridging stoga nasljeđuje sve ključne prednosti link state usmjeravanja:

- mogućnost korištenja svih dostupnih fizičkih veza, jer se za izbjegavanje petlji koristi upravljačka razina s cjelovitim znanjem o topologiji mreže
- brza obnova povezanosti nakon stanja greške, također zbog cjelovitog „link state“ znanja topologije mreže
- za vrijeme trajanja greške i tijekom oporavka jedini je utjecaj na promet koji je bio izravno zahvaćen; sav mrežni promet van tog područja utjecaja se normalno nastavlja
- brza obnova broadcast i multicast povezanosti jer IS-IS šalje sve potrebne informacije u SPB ekstenzijama IS-IS-a, čime se paralelno instalira unicast i multicast povezivost

Shortest path bridging je konceptualno sličan IETF-ovom TRILL-u, no razlikuje se od njega drugačijim korištenjem strukture grananja. Također, SPB rute su simetrične, što znači da je ruta od jedne do druge točke identična povratnoj ruti, što znači da SPB može koristiti neke od postojećih tehnologija upravljanja i nadzora koje su već u upotrebi, kao što su npr. traceroute i loopback.

Shortest path bridging, IEEE 802.1aq standard, namijenjen je zamjeni spanning tree protokola (STP) IEEE 802.1D, IEEE 802.1w, IEEE 802.1s. STP je stvoren kako bi se spriječilo stvaranje petlji dopuštajući samo jedan put između mrežnih preklopnika ili sučelja. Kada neki dio mreže postane nedostupan odabire se alternativni put, a taj proces odabira može prouzročiti neprihvatljiva kašnjenja za mrežu jednog podatkovnog centra. Baš poput TRILL-a i SPB je dizajniran za rješavanje ovog problema primjenom protokola usmjeravanja sloja 3 na uređaje sloja 2. Ovo u biti dopušta uređajima sloja 2 da usmjeravaju Ethernet okvire. Uklanjanjem STP-a i oslobađanjem više puteva na sloju 2, olakšava se migriranje virtualnih strojeva (VM-ova) kroz mreže podatkovnih centara. Za intenzivne aplikacije kao što su komunikacija u stvarnom vremenu (RTC) i za transport prometa za pohranu preko Ethernet mreže s Fibre Channel over Ethernet (FCoE) i iSCSI, biti će dostupna veća propusnost.

Glavna razlika između SPB-a i TRILL-a je u načinu na koji obrađuju promet. 802.1aq koristi jednostavnu i elegantnu metodu za korištenje višestrukih putova kroz mrežu. Nakon što IS-IS izgradi topologiju mreže, SPB izračunava i određuje najkraće puteve na temelju metrika veza, a zatim prosljeđuje promet (i unicast i multicast) na taj put, stoga je vrlo lako predvidjeti prometne tokove kroz tzv. mesh mreže jer se one izračunavaju jednom za cijeli put.

TRILL ("TRansparent Interconnection of Lots of Links") je IETF standard implementiran putem uređaja nazvanih RBridges (routing bridges) ili TRILL preklopnika. TRILL kombinira tehnike s premošćivanjem i usmjeravanjem te je primjena link state usmjeravanja na VLAN-ove.

TRILL koristi dva različita mehanizma za slanje paketa na temelju vrste prometa. Za unicast promet gdje je izlazni Rbridge poznat, TRILL koristi IS-IS bazu podataka kako bi se promet dodijelio najoptimalnijem putu (slično SPB-u). Međutim za multicast i broadcast TRILL koristi distribucijska stabla i Rbridge kao root za prosljeđivanje. U mnogim slučajevima ti putovi neće biti podudarni i čine TRILL osjetljivim na pakete koji ne dolaze po redu, a također to otežava poznavanje točnog puta kroz mrežu kad se gleda iz pozicije bilo kojeg sučelja na preklopniku na temelju vrste prometa.
TRILL je danas slabije prihvaćen od SPB-a koji se nastavlja razvijati. Oba se protokola danas najčešće primjenjuju u mrežama podatkovnih centara. Najbolja tehnologija koja bi mogla zamijeniti spanning tree u podatkovnim centrima je vjerojatno MLAG. On proširuje opseg redundancije na razini veza i mehanizma dijeljenja opterećenja (load-sharing) koje već koristi LAG (Link Aggregation) kako bi podržao redundantnost na razini mreže i uređaja, aktivno-aktivno dijeljenje opterećenja za potpuno iskorištenje propusnog pojasa mreže i brzu konvergenciju. MLAG je jednostavna, ekonomična i skalabilna tehnologija koja zamjenjuje spanning tree u podatkovnim centrima.

Protokoli poput VXLAN i NV-GRE su se pojavili da bi tunelirali pakete sloja 2 preko mreža sloja 3 i time riješili neposrednu potrebu i uklonili ograničenja u hardveru.

U tom je trenutku softverski definirano umrežavanje („software-defined networking“), odnosno SDN, počeo zauzimati tržište. SDN je postao ozbiljna stvar onog trenutka kad je korisnicima omogućio rješavanje problema bez kupnje dodatnih fizičkih uređaja. Smatra se i da je problem sprečavanja nastanka petlji u modernoj mreži bolje rješavati SDN-om koji može rekonfigurirati cijelu mrežu s centralnog kontrolera.

SDN (Software-defined networking)
Softverski definirana mrežna tehnologija (SDN) je pristup cloud računalstvu koji olakšava upravljanje mrežom i omogućava programski učinkovitu konfiguraciju mreže kako bi se poboljšale mrežne performanse i nadzor. SDN se obično povezuje s OpenFlow protokolom, no pojedini proizvođači razvijaju i vlastite podvarijante koje nisu uvijek međusobno interoperabilne. SDN mreže pružaju fleksibilnost, programabilnost i jednostavnost radu mreža. Promet se može usmjeravati, prilagođavati ili personalizirati bez potrebe za fizičkim promjenama ožičenja.

Najvažnije karakteristike SDN-a su:

- može se izravno programirati
- prilagodljivost (agilnost)
- centralno upravljanje
- testiranje nije skupo
- brze nadogradnje

SDN arhitektura relativno je nova mrežna tehnologija namijenjen rješavanju problema statične arhitekture tradicionalnih decentraliziranih kompleksnih mreža, dok mreže danas zahtijevaju veću fleksibilnost i lako rješavanje problema. SDN centralizira inteligenciju mreže u jednoj mrežnoj komponenti tako što razdvaja proces prosljeđivanja mrežnih paketa (podatkovna razina, eng. „data plane“) od procesa usmjeravanja (upravljačka razina, eng. „control plane“). Upravljačka razina je odgovorna za izradu i provedbu pravila i sastoji se od jednog ili više kontrolera koji se smatraju mozgom SDN mreže, što pojednostavljuje usluge umrežavanja jer to znači da više svaki mrežni uređaj ne šalje pakete na sljedeći mrežni uređaj neovisno o drugima.

Svi paketi koji ulaze u mrežu se ispituju na upravljačkoj razini i donosi se odluka o tome da li se paket odbacuje ili se prosljeđuje sljedećem hostu, a također može ažurirati i unos IP tablice. Ovakva centralizacija i naglašeno fizičko razdvajanje mrežne (podatkovne) i upravljačke razine ima i svojih nedostataka, pogotovo kada su u pitanju sigurnost i skalabilnost, tako da su to glavna pitanja koja još treba riješiti prije nego SDN postane prevladavajući način izgradnje mreža.

9. Zaključak
9. *Conclusion*

Jasno je da su računalne mreže važne komponente malih, srednjih i velikih tvrtki. Zbog toga IT administratori trebaju provesti redundanciju u svojim hijerarhijski izgrađenim mrežama. Dodatne veze prema preklopnicima u mreži mogu dovesti do petlji u mrežnom prometu. Kad se izgubi povezanost s preklopnikom, druga veza treba uskočiti, ali bez stvaranja petlji. U tom slučaju koristi se STP protokol koji sprječava nastajanje takvih petlji.
Redundantnost u mreži povećava dostupnost mrežne topologije štiteći mrežu od zasebne točke kvara (poput kvara mrežnog kabela ili preklopnika), no istovremeno uvodi i fizičke petlje koje mogu rezultirati smetnjama u 2. sloju, a te petlje utjecati na dostupnost mreže. Kako bi se spriječili problemi koji time mogu nastati, razvijen je STP (Spanning Tree Protokol).
STP sprječava formiranje petlji u hijerarhijskoj mreži koja sadrži redundantne veze te koristi različita stanja portova i tajmera kako bi spriječio nastajanje tih petlji. Jedan je preklopnik u mreži određen kao osnovni most, a određuje se kroz izborni proces između susjednih preklopnika u domeni prijenosa. Svi ostali preklopnici u mreži koriste STP protokol kako bi odredili uloge svojih portova.
STP osigurava postojanje samo jednog logičkog puta među svim odredištima u mreži tako da blokira sve suvišne putove koji bi mogli prouzrokovati petlju. Port (mrežno sučelje) se smatra blokiranim kad se mrežnom prometu ne dopušta da uđe u taj port ili da izađe iz njega. Blokiranje suvišnih putova važno je za sprječavanje petlji u mreži.

Fizički putevi postoje kako bi osigurali redundanciju, ali su onesposobljeni dok ne budu potrebni, da bi se spriječilo nastajanje petlji. Ako i kada nastane potreba za tim određenim putem kako bi se nadomjestio mrežni kabel ili preklopnik, STP ponovno „izračunava“ putove i deblokira potrebne portove, kako bi se dopustilo do tada suvišnim putevima da postanu aktivni. Kako se u svakom procesu može dogoditi pogreška isto tako i STP može naići na probleme u radu, a najveći je problem što tada postoji mogućnost pada cjelokupne mreže.
Zašto alternative STP-u već nisu stekle šire usvajanje? Najbolje alternative su ili vezane uz pojedinog proizvođača ili su još uvijek zbunjujuće korisnicima. Nalaze svoje mjesto u velikim mrežama koje zahtijevaju neblokirajuću arhitekturu (najviše potrebne za „big data“ i hiperkonvergirane mreže podatkovnih centara). STP vjerojatno u skorije vrijeme neće biti zamijenjen u lokalnim mrežama sve dok se svi igrači na tržištu ne usuglase o jednom standardu. Velike kampusne mreže su pak uglavnom već zamijenile STP s usmjerenom mrežom sve do sloja distribucije.
Zbog ograničene podrške za većinu drugih opcija, STP je još uvijek sam sebi jedina alternativa u heterogenim okruženjima.
Uzevši u obzir sve čimbenike smatramo da je STP vrlo kvalitetan protokol koji će i dalje omogućavati internim mrežama redundantnost bez mogućnosti petlje.

10. REFERENCE
10. *REFERENCES*

[1] Hucaby, D. (2007.) CCNP Building Cisco Multilayer Switched Networks (BCMSN), Cisco Press; ISBN-10: 1-58705-273-3; ISBN-13: 978-1-58705-273-6

[2] Balchunas, A. (2014.) Spanning Tree Protocol, www.routeralley.com

[3] Hucaby, D. (2015.) CCNP Routing and Switching SWITCH 300-115 Official Cert Guide; ISBN-10: 1-58720-560-2; ISBN-13: 978-1-58720-560-6

[4] WENDELL ODOM, (2013.) Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide; ISBN-13: 978-1587144851; ISBN-10: 1587144859

AUTORI · *AUTHORS*

Nikola Jelečki
Rođen je 1989. godine u Varaždinu, završio osnovnu školu u Konjščini, a srednju pohađao u općoj gimnaziji A.G.M Zabok. Studij informatike upisao je 2008. godine na Tehničkom veleučilištu u Zagrebu. Nastavio školovanje na istom fakultetu upisom na specijalistički diplomski stručni studij informatike. Trenutno zaposlen kao SharePoint administrator u HEP-Proizvodnji d.o.o u Zagrebu.

Korespodencija
nikola@jelecki.com

Vedran Turkalj
Rođen je 1972. godine u Zagrebu, završio osnovnu i srednju školu u Zagrebu te studij elektrotehnike na VTŠ Zagreb, a zatim nastavio školovanje na Cisco mrežnoj akademiji za CCNA i CCNP. Završio specijalistički politehnički diplomski stručni studij informatike na Tehničkom veleučilištu u Zagrebu. Trenutno zaposlen kao stručnjak za sigurnost i za računalne mreže te Data Protection Officer u Sveučilišnom računskom centru - Srce u Zagrebu te radi kao asistent na TVZ-u i certificirani instruktor na NetAkademiji.

Korespodencija
vturkalj@tvz.hr