

Redundantna povezljivost na ravni dostopa v omrežjih z internetnim protokolom (IP)

Elektrotehnika

Raziskovalna naloga

Rok Ilovar

3. letnik

Mentor: Sebastjan Zamuda, profesor fizike – Gimnazija
Bežigrad

Somentor: Boris Ilovar, dipl. inž. elektrotehnike, tehnični
direktor – Speed Connect Austria

2025

Gimnazija Bežigrad

KAZALO

POVZETEK IN KLJUČNE BESEDE	1
UVOD	2
RAČUNALNIŠKA OMREŽJA IN NJIHOVE KOMPONENTE	2
VRSTE OMREŽIJ	3
TEORETIČNI DEL	4
KARAKTERISTIKE OMREŽJA	4
NAČRTOVANJE RAČUNALNIŠKE MREŽE	6
STANDARDIZACIJA IN OSI REFERENČNI MODEL	7
PEER-TO-PEER KOMUNIKACIJA, ENKAPSULACIJA IN DEENKAPSULACIJA	9
TEŽAVE SLABO NAČRTOVANIH OMREŽIJ IN FIZIČNA REDUNDANCA V OMREŽJIH LAN	11
VIRTUALNO LOKALNO OMREŽJE (VLAN)	13
SPANNING TREE PROTOCOL (STP)	14
VRSTE IN STANDARDIZACIJA STP PROTOKOLA	14
KLJUČNI KONCEPTI STP PROTOKOLA	15
PREDNOSTI KONCEPTA ETHERCHANNEL ALI PORTGROUP	18
EKSPERIMENTALNI DEL	19
TOPOLOGIJA OMREŽJA	19
UPORABLJENA OPREMA	19
POSKUS 1:	21
1. del: STP protokol tipa PVST na stikalih	21
2. del: onemogočen STP protokol in posledice	24
3. del: klasičen tip STP protokola na stikalih	26
4. del: STP protokol tipa RPVST na stikalih	29
POSKUS 2:	30
ZAKLJUČEK IN RAZPRAVA	34
ZAHVALA	36
LITERATURA	37

Povzetek in ključne besede

Omrežja, ki temeljijo na internetnem protokolu (IP), omogočajo komunikacijo naprav s pomočjo standardiziranih protokolov in predstavljajo hrbtenico sodobnih komunikacijskih sistemov. Ključne lastnosti so redundanca, razširljivost in razpoložljivost, ki jih izboljšamo s pravilno konfiguracijo naprav in povezav.

V teoretičnem delu sem predstavil osnove računalniških omrežij, ki omogočajo razumevanje eksperimentalnega dela. Natančneje je opisana vloga stikal, osredotočena na zagotavljanje stabilnosti. Poudarek je bil na reševanju težav redundantnih povezav, ki lahko povzročijo zanke. Ključni rešitvi sta Spanning Tree Protocol (STP), ki preprečuje zanke in zagotavlja zanesljivost, ter EtherChannel, ki povečuje pasovno širino in redundanco.

Za eksperimentalen del sem konfiguriral dve Cisco stikali, in preizkusil STP ter EtherChannel v redundantnem omrežju. Testiral sem odzivnost in vpliv zanke, ter prikazal preprečevanje motenj v delovanju omrežja. Postavil sem manjše omrežje, sestavljenega iz dveh stikal in dveh računalnikov. V obeh poskusih, je en izmed računalnikov deloval kot strežnik za video in datoteke, drugi pa kot odjemalec. Rezultati so pokazali, da STP učinkovito preprečuje zanke in zagotavlja stabilnost redundantnih povezav. Meritve preklopnih časov so potrdile učinkovitost STP pri zagotavljanju razpoložljivosti omrežja. Sklep raziskovalne naloge poudarja, da sta pravilna konfiguracija STP in EtherChannela ključni za optimizacijo zmogljivosti in stabilnosti omrežja.

Ključne besede TCP/IP, STP, Etherchannel, stikalo, usmerjevalnik

Summary

Networks based on the Internet Protocol (IP) enable device communication through standardized protocols and form the backbone of modern communication systems. Key characteristics include redundancy, scalability, and availability, which can be improved through proper configuration of devices and connections.

In the theoretical part, I presented the fundamentals of computer networks, which provide the basis for understanding the experimental work. The role of switches is described in detail, with a focus on ensuring network stability. Emphasis was placed on solving issues related to redundant connections, which can cause network loops. The key solution is the Spanning Tree Protocol (STP), which prevents loops and ensures reliability, as well as EtherChannel, which increases bandwidth and redundancy.

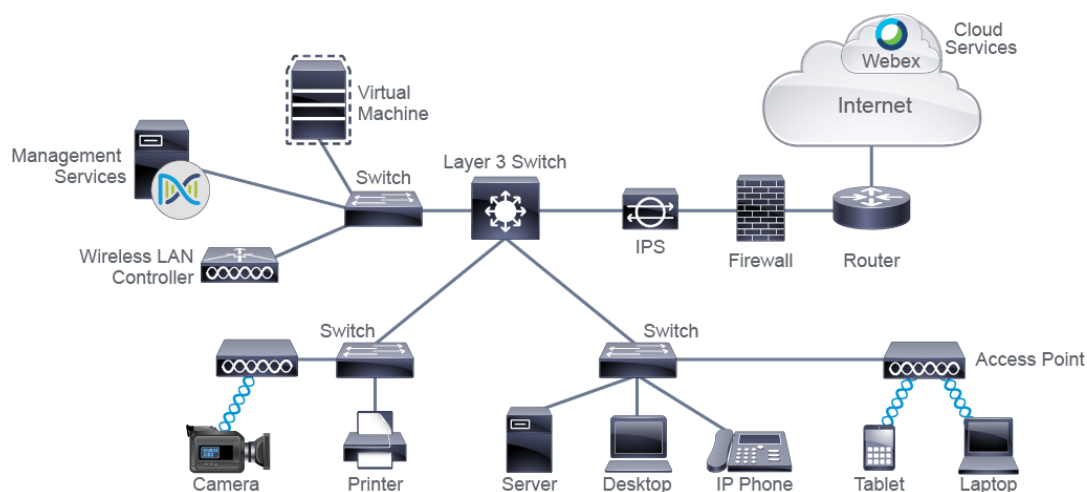
For the experimental part, I configured two Cisco switches and tested STP and EtherChannel in a redundant network. I analyzed convergence and the impact of loops, demonstrating how network disruptions can be prevented. I set up a small network consisting of two switches and two computers. In both experiments, one computer acted as a server for video streaming and file sharing, while the other functioned as a client. The results showed that STP effectively prevents loops and ensures the stability of redundant connections. Measurements of failover times confirmed STP's efficiency in maintaining network availability. The conclusion of this research highlights that proper configuration of STP and EtherChannel is essential for optimizing network performance and stability.

Uvod

Računalniška omrežja in njihove komponente

Omrežja so ključni del sodobne komunikacije in informacijske tehnologije, zato me je njihovo delovanje že od nekdaj zanimalo. Lansko leto sem se začel intenzivneje ukvarjati s to tematiko, saj sem si zadal cilj opraviti CCNA licenco, ki jo podeljuje podjetje Cisco Systems. Gre za osnovno, mednarodno priznano certifikacijo, ki potrjuje temeljno poznavanje računalniških omrežij. Priprava na pridobitev certifikata me je še bolj spodbudila k raziskovanju delovanja omrežij in odprla številna vprašanja, ki sem jih želel podrobneje preučiti. Prav ta radovednost in želja po poglobljenem razumevanju sta me vodili k pisanju te raziskovalne naloge.

Računalniška omrežja so v manjše ali večje mreže povezane različne naprave. Računalniško omrežje povezuje osebne računalnike, tiskalnike, strežnike, pametne telefone, kamere in druge vrste naprav tako, da lahko komunicirajo med seboj. Naprave v omrežju delimo na dve vrsti, končne in povezovalne naprave. S končnimi napravami se srečujemo vsak dan, to so pametni telefoni, računalniki, tiskalniki, strežniki in podobno. Te so na omrežje povezane neposredno s kablom ali brezžično. Povezovalne naprave so naprave z različnimi funkcionalnostmi, ki omogočajo komunikacijo med končnimi napravami. Najbolj tipične, ki so skoraj vedno prisotne, imenujemo stikala, usmerjevalniki in dostopovne točke.



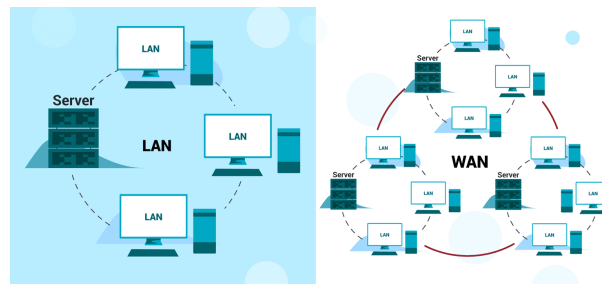
Slika 1: Prikaz računalniškega omrežja [5]

Vse končne naprave tipično priklapljamemo na stikala, ki so dostopovne naprave v omrežju. Te so nato naprej povezane na usmerjevalnike, ki služijo usmerjanju prometa med omrežji in povezavi v internet. Promet v omrežju in med omrežji predstavlja prenos podatkov med

končnimi napravami in to je na kratko vsakršna aktivnost končnih naprav, ki med seboj komunicirajo. V primeru manjših omrežij usmerjevalniki predstavljajo predvsem izhod iz omrežja. V primeru večjih omrežij pa usmerjevalniki poleg izhoda iz omrežja skrbijo tudi za povezovanje segmentov omrežij med seboj.

Vrste omrežij

V internetno omrežje so povezane končne naprave na vseh koncih sveta, ki so večinoma sprva del manjših omrežji, zatem pa so povezana na večja svetovna omrežja. Omrežja predstavljajo omrežja doma, v pisarnah manjših in večjih podjetij ter drugih ustanovah. Delimo jih na lokalna omrežja (LAN), ki pokrivajo manjše geografske površine in so tipično omrežja v manjših podjetjih in domovih, ter širokopasovna omrežja (WAN), ki povezujejo LAN omrežja preko večjega geografskega področja med seboj.



Slika 2: Shema lokalnega in širokopasovnega omrežja [6]

Primer bi lahko bilo podjetje za distribucijo goriva, ki ima glavno pisarno v glavnem mestu države in mnogo bencinskih črpalk po celi državi. Vsaka posamezna bencinska črpalka in omrežje v centralni lokaciji predstavljajo lokalna omrežja (LAN), med seboj pa so ta lokalna omrežja povezana preko večjih razdalj in jim rečemo WAN povezave. WAN povezave so lahko narejene preko najetih vodov, kjer uporabniki zakupimo svojo privatno povezavo in je ne delimo z nikomer, ali pa so narejene preko javnega Interneta in so del skupnih WAN povezav, ki si ji deli več uporabnikov oziroma podjetij. Za namen komunikacije ima vsaka naprava svojo edinstveno MAC (Media Access Control) številko in IP (Internet Protocol) številko, ki jima rečemo tudi MAC naslov in IP naslov.

Teoretični del

Karakteristike omrežja

Velikost in zmogljivost povezovalnih naprav vplivata na to, koliko končnih naprav sestavlja lokalna omrežja, ki so posledično različnih velikosti, zmogljivosti in topologij. Tako kot naprave imajo tudi omrežja posebne značilnosti in arhitekturo, ki nam omogočajo boljše razumevanje tega, kako je omrežje zasnovano in kakšno delovanje lahko od njega pričakujemo. Delovanje, ki ga pričakujemo od omrežja, se zelo navezuje na naše zahteve. Značilnosti in karakteristike omrežja, s katerimi lahko opišemo njihovo zmogljivost in strukturo, so topologija, hitrost, cena, varnost, razpoložljivost, razširljivost in zanesljivost.

V omrežjih obstajajo fizične in logične topologije. Fizična topologija opisuje, kako so omrežne in končne naprave povezane med seboj. Lahko so povezane s kabli ali brezžično. Z logično topologijo ponazarjamo, med katerimi točkami (napravami) se podatki prenašajo in nas ne zanima vedno točna fizična pot, po kateri podatki zares potujejo skozi omrežje.

Hitrost, temeljna značilnost katerega koli omrežja, se nanaša na hitrost prenosa in prejemanja podatkov, ki se običajno meri v bitih na sekundo (bps) ali večjih enotah, kot sta Mbps (megabiti na sekundo) in Gbps (gigabiti na sekundo). Različne vrste omrežnih povezav ponujajo različne hitrosti, ki so odvisne od tehnologije in zmogljivosti opreme. Optične povezave, ki za prenos uporabljajo laserske žarke, ki potujejo po steklenem jedru optičnega kabla, enostavneje dosegajo večje razdalje v primerjavi s prenosom električnega signala po žičnih povezavah, kot so UTP kabli. Povezave z optičnimi vlakni zagotavljajo izjemno visoke hitrosti brez znatnih izgub, ki so včasih segale do 10 Gbps oziroma do 100 Gbps, sedaj po razvoju pa so že hitrosti 400 Gbps in 800 Gbps povsem običajne. Zaradi tega so optične povezave idealne za podatkovno intenzivne naloge in za povezave na večje razdalje, kot sta pretakanje video posnetkov in računalništvo v oblaku. Poleg optičnih vlaken poznamo tudi zgoraj omenjene žične povezave po bakrenih kablích, tako imenovanih UTP kablích. Ti se dandanes bolj pogosto uporabljajo na krajših razdaljah pri povezavah strežnikov in redkeje pri ostalih napravah končnih uporabnikov na dostopna omrežja. Pri povezavah naprav končnih uporabnikov (prenosni računalniki, telefoni, tablice) prevladujejo predvsem brezžične povezave. Razvoj brezžičnih povezav preko omrežja WiFi je dosegel visoko stopnjo hitrosti, vendar je dejanska hitrost, ki jo občutijo uporabniki, odvisna od številnih dejavnikov. Ti vključujejo omrežno

prezasedenost, omejitve strojne opreme in motnje signala, zaradi česar je ponovno potrebno dovolj dobro poznavanje potreb omrežja in primerno načrtovanje.

UTP (Unshielded Twisted Pair) kabli so še vedno pogosto v uporabi in so razvrščeni v različne kategorije, ki določajo njihove zmogljivosti, kot so hitrost prenosa podatkov, pasovna širina in zaščita pred motnjami. UTP kabli so razdeljeni v več kategorij, ki poleg hitrosti določajo tudi maksimalne dolžine, do katere brez napak poteka prenos podatkov. Maksimalna dolžina UTP kabla za prenos podatkov je 100 metrov. S kvaliteto (kategorijo) UTP kabla povemo, kolikšno maksimalno hitrostjo lahko dosežemo pri 100 metrov dolgem kablu. Poznamo kategorije UTP Cat 1, Cat 2, Cat 3, Cat 4, Cat 5, Cat 5e, Cat 6, Cat 6a, Cat 7 in Cat 7a.

Dandanes je najslabša kvaliteta kabla, ki se uporablja, kategorije UTP Cat 5/5e. Pri ceni UTP Cat 5 kabla 1 EUR/meter in UTP Cat 7 kabla 2 EUR/meter je lahko razlika velika, če upoštevamo, da posloplje s petimi nadstropji in 100 uporabniki lahko zahteva uporabo tudi preko 2000 m kablov. Pri napredovanju tehnologije smo z veseljem izkoristili možnost brezžičnega povezovanja končnih naprav uporabnikov, kjer potreba po takšni količini kablov odpade. Tako, da sedaj v praksi srečujemo kombinacijo žičnih povezav z UTP kabli, brezžičnih povezav in povezav z optičnimi vlakni.

Omrežna oprema, ki jo uporabljamo pri postavitvi omrežij je odvisna glede na potrebe končnih uporabnikov. Izbira vodi do različnih cen in različnih načinov povezav. Cena različnih naprav v omrežju, ki jih uporabljamo, navadno ni nizka, zato štejemo ceno pod eno od karakteristik omrežja. Za večja podjetja in zahtevnejše naloge potrebujemo več denarja, saj oprema postaja vedno kompleksnejša.

Skozi čas se lahko naše omrežje širi, pri čemer je pomembna karakteristika razširljivosti. Namen pravilnega načrtovanja je povečati zmožnost omrežja, da kasneje pri njegovem širjenju s čim manjšo ceno in s čim manjšim trdom dodajamo nove naprave, povezujemo nove segmente omrežij in nove končne naprave.

V omrežjih je pomembna tudi varnost, ki se regulira z različnimi programi in napravami. Najbolj znane naprave za povečanje varnosti se imenujejo požarni zidovi. Poznamo pa tudi druge naprave in programsko opremo, ki se uporablja v ta namen.

Da lahko brez skrbi uporabljamo omrežje, mora biti razpoložljivo, kar pomeni, da mora biti narejeno zanesljivo, in kljub morebitnim okvaram nuditi rezervno povezavo, zaradi katere

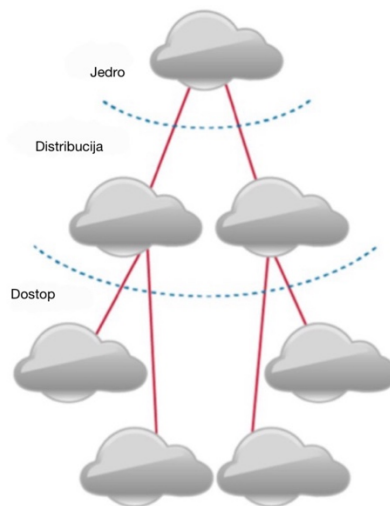
uporabniki ne izgubimo povezave. Pomembni karakteristiki sta torej tudi zanesljivost in razpoložljivost omrežja. Razpoložljivost se izračuna v časovnem obdobju enega leta:

$$\frac{[\text{Število minut v letu}] - [\text{Število minut nedelujočega omrežja v letu}]}{[\text{Število minut v letu}]} * 100 = 99.9971$$

Razpoložljivost (procenti)

Slika 3: Izračun razpoložljivosti v časovni enoti enega leta

Načrtovanje računalniške mreže



Slika 4: Prikaz nivojev postavitve omrežnih naprav pri načrtovanju omrežij [7]

Pri načrtovanju omrežja moramo upoštevati njegove funkcije in samo uporabo omrežja. Prav tako je pomembna arhitektura postavitve omrežja, saj vpliva na varnost, delovanje in razširljivost omrežja. Na vrsto povezav in število naprav vpliva velikost prostora in število uporabnikov, kateri bodo povezani na omrežje. Pri prostoru imamo v mislih velikost prostorov podjetja, kjer se bo omrežje postavilo. Pri načrtovanju poznamo tri nivoje postavitve, ki z različnimi nalogami pripomorejo temu, da vsi končni uporabniki dostopajo do storitev, strežnikov in zunanjega interneta.

Prvi nivo je dostopovni nivo. To je mesto, kjer se na omrežje povezujejo končne naprave uporabnika. To so končne naprave, ki jih nadzoruje uporabnik in končne naprave povezane z

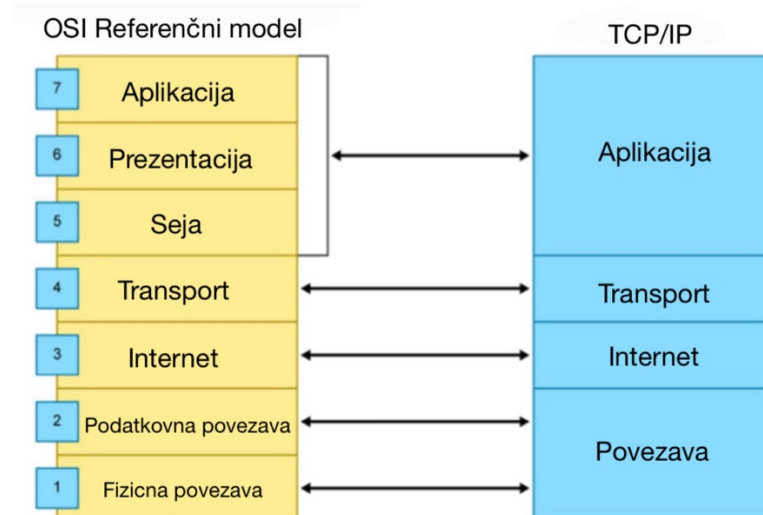
omrežjem, ki omogočajo uporabnikom določene storitve, na tiskalnik. Dostopovni nivo zagotavlja žično in brezžično povezljivost ter vsebuje funkcije in storitve, ki delno zagotavljajo varnost povezave na omrežje. Na dostopovnem nivoju so tipično dostopovna stikala z veliko vmesniki različnih hitrosti, preko katerih se priklaplajo končne naprave. Žične povezave so kabli, ki neposredno povezujejo končne naprave na omrežja. Brezžične povezave pa kablov ne uporabljajo, vendar se posredno preko dostopovnih točk končne naprave spet povezujejo na stikala. Dostopovne točke so tako vmesne naprave med končnimi uporabniki in stikali.

Naslednji nivo združuje vsa dostopovna stikala, na katera so povezane končne naprave, imenujemo ga distribucijski nivo. Ta nivo najpogosteje predstavljajo večja zmogljivejša in zanesljivejša stikala, ki združijo povezave končnih naprav do pomembnih storitev in jedra omrežja. Primeri storitev, ki so na voljo skupinam uporabnikov v omrežju, so podpora komunikaciji med različnimi segmenti omrežij, implementacija protokolov za večjo razpoložljivost in redundanco, razni varnostni mehanizmi (požarni zidovi in sistemi za zaznavanje/preprečevanje vdorov) in drugo.

Ko se omrežje širi, ima več distribucijskih stikal, kjer se združuje promet. Zato se mora za optimizacijo zasnove uvesti jedrni nivo, ki je tako imenovana centrala omrežja, predvsem skrbi za hitro povezavo med segmenti omrežij in povezavo na usmerjevalnike. Usmerjevalniki pa so naprave, ki prejmejo podatke oziroma ves promet med končnimi napravami in ga usmerijo na oddaljena omrežja oziroma v internet. Ves promet, ki je namenjen proti drugim bolj ali manj oddaljenim omrežjem ter proti internetu, se tako zbira preko stikal in se na usmerjevalnikih usmerja naprej s pomočjo IP naslovov.

Standardizacija in OSI referenčni model

Ob razvoju naprav so se v zgodovini pojavile težave zaradi različnih, nezdržljivih protokolov, saj je vsak izdelovalec implementiral po svoje. Da bi omogočili komunikacijo med napravami različnih vrst, so uvedli standardizirane protokole in obliko prenosa podatkov. Podatki, do katerih dostopamo ali jih pošljemo izven računalnika, morajo biti opremljeni še z veliko informacijami, ki zagotavljajo, da te prispejo na pravo končno destinacijo. V kontekstu standardizacije protokolov je bil ustvarjen OSI (Open Systems Interconnection) referenčni ali konceptualni model, ki opisuje ter s pravili določa, kako računalniški sistemi ali podsistemi komunicirajo v omrežju.



Slika 5: Prikaz plasti OSI in TCP/IP modela

OSI model je sestavljen iz sedmih nivojev, ki opravljajo specifične naloge:

- Fizična plast (nivo 1) prenaša signale na prenosnem mediju. Primer sta žica ali optično vlakno. Tukaj se predpisuje prenosni medij, preko katerega se prenašajo podatki. Definira se tudi nivo signala, hitrost prenosa in način zapisa podatkov.
- Povezovalna plast (nivo 2) zagotavlja zanesljiv prenos podatkov na lokalnem omrežju LAN prek uporabe MAC naslovov. Nivo določa enote sporočila, način ugotavljanja napak in kontrolo prenosa podatkov. Deli se na 2 podplasti, izmed katerih je ena MAC (Media Access Control). Na drugem nivoju se prenašajo podatki v obliki okvirjev (frame).
- Omrežna plast (nivo 3) skrbi za usmerjanje podatkov med omrežji. Vzpostavlja, prekinja in vzdržuje povezavo med uporabniki. Določa pravilno potovanje paketov različnih dolžin po različnih poteh. Upravlja fragmentacijo in defragmentacijo paketov ter pravilen vrstni red pošiljanja in prejemanja. Kot omenjeno se na tretjem nivoju prenašajo podatki v obliki paketov.
- Transportna plast (nivo 4) nadzira napake in prenos podatkov. Zagotavlja višje ležečim plastem povezavo med dvema končnima napravama (na primer računalnikoma). Na prenosni poti poskrbi za pravilen in zanesljiv prenos podatkov. Na četrtem nivoju se prenašajo podatki v obliki segmentov.
- Sejna plast (nivo 5) upravlja povezave. Določa vzpostavitev, vzdrževanje in prekinitve seje, kar določa komunikacije med končnimi napravami (na primer računalniki).
- Predstavitvena plast (nivo 6) skrbi za uskladitev različnih načinov predstavitve podatkov in pretvarja podatke v razumljive formate. Izvaja kompresijo in dekompresijo

podatkov, šifriranje podatkov za potrebe zaščite. Določa podatkovne formate, ki omogočajo uporabo standardnih predstavitvenih, zvočnih in video formatov za potrebe uporabe aplikacij na različnih računalniških sistemih.

- Aplikacijska plast (nivo 7) omogoča povezavo z uporabniškimi storitvami oziroma aplikacijami. Je vmesnik med uporabnikom in komunikacijskim omrežjem. Določa protokole, ki omogočajo elektronsko pošto, izdelavo predstavitvenih strani, prenašanje datotek in podobno. [2]

Standardizacija teh plasti zagotavlja združljivost med napravami različnih proizvajalcev in omogoča razvoj opreme, ki deluje samo na določenih plasteh, a vseeno komunicira z drugimi napravami prek ustreznih protokolov. Osebni računalnik vključuje vse plasti OSI modela. Na primer pri pošiljanju elektronske pošte podatki prehajajo skozi vse plasti – od aplikacijske plasti (pisanje elektronske pošte v programu za elektronsko pošto) do fizične plasti (žični ali brezžični prenos). Na drugi strani pa imamo omrežno opremo, ki deluje le na posameznih plasteh. Stikala delujejo večinoma na drugi plasti, kjer z uporabo MAC naslovov prenašajo podatke na lokalnem omrežju (LAN), ne morejo pa prebrati vsebine e-pošte, saj ne delujejo na višjih plasteh. Čeprav stikalo razume in obdeluje samo drugo OSI plast, lahko sodeluje z računalnikom, ker obe napravi komunicirata preko druge plasti, preko ustreznega protokola (na primer Ethernet).

OSI model je ključen za standardizacijo, saj omogoča enostavno integracijo različnih tehnologij, razvoj univerzalnih protokolov, odpravljanje napak na posameznih plasteh ter fleksibilnost pri uvajanju novih tehnologij. Na njegovi osnovi je bil razvit TCP/IP model, ki določa komunikacijo v IP omrežjih in v internetu.

Peer-to-Peer komunikacija, enkapsulacija in deenkapsulacija



Slika 6: Komunikacija med dvema enakovrednima končnima napravama

V procesu prenašanja podatkov med dvema končnima napravama (na primer dvema računalnikoma) naša vsebina, ki jo prenašamo, potuje skozi vse plasti OSI modela. Da je to mogoče, vsaka plast zapakira podatke v ustrezne podatkovne enote, imenovane PDU (Protocol

Data Unit). Vsaka plast vzame vsebino, ki jo dobi in ji doda glavo (header) ter vse skupaj pošlje na nižjo plast. Glava je dodatni del podatkovne enote, ki določa, kako so podatki zakodirani in kaj vsebujejo. Nižja plast vzame tako pridobljeno podatkovno enoto skupaj s podatki in glavo kot vsebino in ji spet doda svojo glavo ter pošlje naprej. Vsak sloj ima svoje ime za podatkovno enoto. Na aplikacijski plasti so to podatki, na transportni plasti segmenti, na omrežni plasti paketi, in na podatkovni plasti okvirji (frames). Na fizični plasti, na bakrenem kablu, se podatki prenesejo kot biti. Ko na primer v elektronsko sporočilo vključimo besedilo ali sliko, se ti podatki zapakirajo za namen prenosa preko plasti OSI modela. V tem procesu, ki mu včasih rečemo tudi enkapsulacija, naše elektronske naprave (na primer osebni računalniki ali tablice) vzamejo elektronsko sporočilo in ga zapakirajo v podatkovni paket, kateremu dodajo glavo (header). Pri prehodu med plastmi OSI modela vsaka plast vzame prejšnjo podatkovno enoto in ji doda svojo glavo kot dodatek k vsebini. Na ta način vsebina elektronskega sporočila preide iz plasti 7 preko vseh ostalih 5 plasti na plast 1, kjer se podatki (skupek vsebine zakodirane z več glavami – vsaka plast doda svojo) prenesejo kot biti po kablu ali brezžični povezavi. Ko vsebino na ta način pošljemo preko omrežja, je pomembno, da obe končni napravi podpirata enake protokole, ki na eni strani zapakirajo in na drugi strani odpakirajo podatke (oziroma vsebino) pri prehodu čez posamezne sloje OSI modela.

Če na prvi strani pri pošiljanju elektronskega sporočila govorimo o pakiranju podatkov ali o enkapsulaciji, se na ciljni strani zgodi obratni proces razpakiranja ali dekapsulacije. Vsaka plast na ciljni strani odstrani glavo, ki pripada tisti plasti in posreduje vsebino naslednji višji plasti, dokler uporabnik na koncu ne prejme prvotnega sporočila elektronske pošte. Ta zgradba v plasteh omogoča, da različne naprave različnih proizvajalcev sploh komunicirajo. Seveda pričakujemo tudi, da komunicirajo učinkovito in zanesljivo.

Med dvema računalnikoma, ki predstavljata končni napravi, je vmes več drugih vmesnih naprav (na primer: stikala in usmerjevalniki). Kot sem omenil zgoraj, vse te vmesne naprave ne delujejo na vseh plasteh. Te naprave ustrezno prejeto podatkovno enoto dekapsulirajo do plasti na kateri delujejo. Vsebino na tem sloju obravnavajo, na njeni podlagi sprejmejo odločitev, jo morebitno opremijo z novimi podatki, enkapsulirajo nazaj in kot bite na plasti 1 pošljejo naprej.

Omrežne naprave nivoja 2 in 3

Omrežja sestavljajo naprave, ki delujejo na različnih plasteh OSI modela. Na drugi plasti delujejo stikala, ki so temeljni del večine omrežij, saj omogočajo priklop končnih naprav preko

UTP ali optičnih kablov ter se odlikujejo po velikem številu vmesnikov, nizki ceni in zanesljivem delovanju. Njihova hitrost omogoča učinkovito prepošiljanje podatkovnih enot (okvirjev) med vmesniki, pri čemer uporabljajo MAC naslove, ki so unikatni za vsako napravo. Stikala lahko povežemo v različne topologije, v večjih lokalnih omrežjih pa so organizirana v več nivojev – prvi skrbi za priklop naprav, drugi za distribucijo podatkov, tretji pa za hiter prenos po omrežju, kot omenjeno. V podatkovnih centrih sta običajno le dva nivoja stikal. Večina podatkov iz lokalnega omrežja se nato prepošlje usmerjevalniku, ki deluje na tretji plasti in skrbi za povezavo več omrežij ter izhod na internet. Usmerjevalniki uporabljajo IP naslove, ki jih končne naprave pridobijo ob načrtovanju omrežja, in se odločajo, po kateri poti bodo poslali podatkovne enote (pakete). Čeprav nekatera naprednejša stikala lahko opravljajo naloge tretje plasti, je usmerjanje prometa tipično v domeni usmerjevalnikov. Ker se v tej raziskovalni nalogi osredotočam na stikala, so usmerjevalniki omenjeni zgolj za boljše razumevanje tematike.

Težave slabo načrtovanih omrežij in fizična redundanca v omrežjih LAN

V preprostih manjših lokalnih omrežjih so končne naprave običajno povezane na eno stikalo, ki deluje kot centralni element omrežja. Pri srednjih in večjih omrežjih je končnih naprav več in so povezane na več dostopovnih stikal (angleško: access switch). Ta stikala so po načelu tri nivojske topologije povezana na distribucijska stikala (angleško: distribution switch), ki so nadalje povezana na jedrna stikala (angleško: core switch). Jedrna stikala so naprej povezana na usmerjevalnik, ker tipično potrebujemo izhod iz lokalnega omrežja na internet ali povezavo do drugih omrežij. V raziskovalni nalogi sem se delno posvetil problematiki načrtovanja omrežja, zato bom podal le nekaj tipičnih primerov povezanih s tematiko, ki jo opisujem. Pri večjem številu končnih uporabnikov namreč lahko uporabimo več dostopovnih stikal, ki jih povežemo na vsaj dve distribucijski stikali, ki sta povezani na vsaj dve jedrni stikali. Pri uporabi več naprav je pomembno, da pri izpadu posamezne povezave ali posamezne naprave ne izgubimo dostopa do omrežja. Zato je pomembno, da stikala povežemo z več povezavami. Na ta način ne izgubimo povezljivosti, če se katerakoli od povezav prekine. Prav tako ne izgubimo povezljivosti, če imamo podvojena stikala na distribucijskem ali jedrnem nivoju. Kajti ob morebitni odpovedi stikala drugo prevzame nalogo povezovanja.

Distribucijska stikala se uporabljajo za združevanje (agregacijo) prometa končnih naprav (končnih uporabnikov) ter za povezavo na različne storitve v omrežju (opisano v prejšnjih poglavjih). Jedrna stikala skrbijo za hiter prenos podatkov proti izhodu iz omrežja ali med različnimi segmenti omrežja.

Če povečamo število jedrnih in distribucijskih stikal, torej lahko ustvarimo redundantne povezave, ki povečujejo zanesljivost omrežja in omogočajo, da se promet še vedno usmeri skozi drugo pot v primeru napak. Kljub temu pa redundanca lahko prinese tudi določene težave, med katerimi so najpogostejše naslednje:

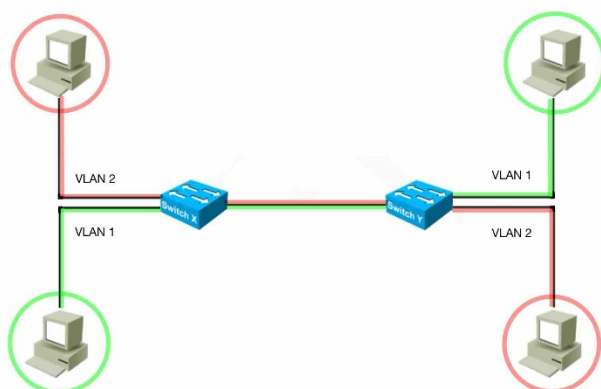
- Zaradi redundantnih povezav se lahko zgodijo zanke (loops) in lahko pride do napak pri zapisovanju MAC naslovov v MAC tabelo naslovov. Na vsakem stikalu se pojavijo podvojeni MAC naslovi v tabeli, kar lahko vpliva na pravilnost prenosa naših podatkov po omrežju.
- Redundantne povezave in posledično zanke lahko povzročijo broadcast nevihte (broadcast storm), kjer se paketi pošiljajo v krogu po zanki, kar povzroči nenehno dupliciranje prometa, dokler ne pride do preobremenitve stikal, kar upočasni in lahko tudi ustavi njihovo delovanje.
- V primeru redundantnih poti in zank lahko pride do podvajanja podatkov, ki se pošiljajo na plasti 2 kot okviri (frames), to se zgodi, ko isti okvir (frame) potuje po več različnih poteh. Ker je več kopij istega okvirja, lahko to povzroči napake v omrežju, kjer končne naprave kot prejemnik teh okvirjev ne zmorejo pravilno obdelati vse prejete podatke.

Za obvladovanje teh težav je nujno potrebno implementirati protokole in konfiguracije, ki omogočajo učinkovito posredovanje prometa in preprečujejo napake. Primer takšnega protokola je Spanning Tree Protocol (STP), ki pomaga pri obvladovanju redundantnih poti ter preprečevanju zgoraj omenjenih težav.

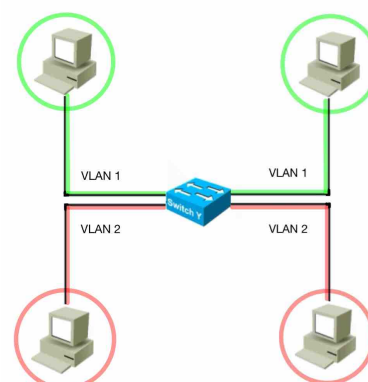
Poleg tega se slabo načrtovano omrežje pogosto sooča z težavami pri upravljanju in podpori. Če ni jasno določeno, kako potekajo tokovi prometa, in ni ustrezno organizirano, postane podpora in vzdrževanje zelo zahtevna. To lahko privede do dolgotrajnega reševanja težav in večjih stroškov.

Obvladovanje teh težav omogoča, da omrežje ostane stabilno, zanesljivo in bolj razpoložljivo, hkrati pa zmanjša možnosti za morebitne motnje v delovanju, ki bi jih opazili mi, uporabniki.

Virtualno lokalno omrežje (VLAN)



Slika 7: Dva VLAN-a na dveh LAN-ih



Slika 8: Razdelitev štirih vmesnikov na enem stikalu na dva VLAN-a

VLAN (Virtual Local Area Network) je tehnologija, ki omogoča segmentacijo omrežja in ločitev naprav v različne virtualne omrežne enote oziroma v različna virtualna lokalna omrežja. To se zgodi kljub temu, do so naprave fizično povezane na istem stikalu (ali na več stikalih povezanih skupaj). Kot vidimo na sliki 7, VLAN tako omogoča, da končne naprave na različnih fizičnih lokacijah v omrežju, ki pripadajo istemu VLAN-u, komunicirajo med seboj, kot da so na istem omrežju. Hkrati pa so lahko končne naprave povezane na ista stikala, vendar je na vmesniku nastavljen drugi VLAN, zato ločene od prvih. To je razvidno na sliki 8.

V primeru, ko so vsi vmesniki na stikalu v istem VLAN-u, naprave, povezane na te vmesnike, lahko brez težav komunicirajo in se med seboj "vidijo".

V nasprotju s tem, da so naprave na stikalu razdeljene na vmesnike, ki so nastavljeni na več različnih VLAN-ov, naprave v različnih VLAN-ih ne morejo med seboj neposredno komunicirati. Neposredna komunikacija je mogoča samo znotraj istega VLAN-a. Za komunikacijo med različnimi VLAN-i potrebujemo napravo plasti 3 (Layer 3 stikalo ali usmerjevalnik). Ta segmentacija omrežja omogoča boljše obvladovanje prometa, saj omeji obseg broadcast prometa in omogoči boljšo organizacijo omrežnega prometa ter zaščito med končnimi uporabniki. Broadcast promet je promet, ki poteka na vse naprave v VLAN-u.

Torej, VLAN-i omogočajo segmentacijo omrežja, kar povečuje varnost, zmanjša obremenitev in omogoča boljše optimizacijo omrežja. VLAN-i imajo lahko pomemben vpliv na reševanje redundance v omrežju, kar bomo raziskali v nadaljevanju, v povezavi s STP protokolom. [2]

Spanning Tree protocol (STP)

Kot je zgoraj omenjeno, pri večjih lokalnih omrežjih potrebujemo več stikal in če želimo večjo razpoložljivost ali večjo kapaciteto med stikali, moramo ta stikala povezati z več povezavami (z več kabli). V takih primerih, kot je omenjeno pri težavah načrtovanja omrežja, lahko med stikali nastanejo zanke, ki povzročijo nestabilnost omrežja in celo odpoved stikal. Take težave rešuje STP (spanning tree protocol) protokol. STP in protokoli, ki mu sledijo, zagotavljajo razrešitev zanke z upravljanjem fizičnih poti do danih segmentov omrežja. STP je protokol, ki preprečuje nastanek zanke v omrežjih, kjer z več povezavami povezujemo več različnih stikal. Omogoča redundanco fizične poti, hkrati pa preprečuje neželjene učinke aktivnih zank v omrežju. STP nekatere vmesnike prisili v stanje blokiranja. Ti blokirani vmesniki ne posredujejo okvirjev, oziroma omrežnega prometa, vendar so le v stanju pripravljenosti za primer, če se na že vzpostavljeni prioritetni povezavi kaj zgodi (na primer, da neha delovati ali se prekine). Skupni učinek je, da je v vsakem trenutku aktivna samo ena pot do posameznega segmenta omrežja. Če pride do težave s povezljivostjo s katerim koli segmentom v omrežju, STP ponovno vzpostavi povezljivost tako, da samodejno aktivira prej neaktivno pot, če ta obstaja. Aktivacija nove poti gre skozi proces protokola STP, ki je sestavljen iz več delov. Ta proces vzame določen čas. Temu času rečemo konvergenca in je odvisen od tipa STP protokola, ki je v uporabi. Poleg tega lahko STP protokol deluje samo na enem lokalnem omrežju in na enem VLANu ali pa uporabimo STP protokol, ki deluje na več VLAN-ih, kjer ima vsak VLAN svojo STP instanco protokola in vsak VLAN upravlja svojo topologijo za redundantne povezave preko posameznega VLANa.

Vrste in standardizacija STP protokola

Zaradi pomembnosti in kompleksnosti omrežij se je tako prvotni STP protokol razvijal v več vrst STP protokolov, ki se med seboj nekoliko razlikujejo. Med najpomembnejšimi različicami so osnovni STP (IEEE 802.1D) protokol, RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), PVST in RPVST (Cisco). Trije so priznani s strani IEEE (Institute of Electrical and Electronics Engineers) standardizacije, ki je mednarodna strokovna organizacija, ki se ukvarja s standardizacijo, raziskavami in razvojem na področju elektrotehnike, elektronike, telekomunikacij, računalništva in informacijskih tehnologij. Druga dva sta izvedenki, ki sta lastni samo podjetju Cisco Systems in jih drugi proizvajalci ne smejo uporabljati. Osnovni STP preprečuje omrežne zanke, vendar ima zelo počasno konvergenco, ki potrebuje od 30 do 50

sekund, da omrežje ponovno deluje po spremembi topologije. RSTP (Rapid STP) je njegova izboljšana različica, ki bistveno pospeši konvergenco na samo 3 sekunde in učinkoviteje prilagaja omrežne povezave. MSTP (Multiple STP) omogoča upravljanje več VLAN-ov z eno STP instanco, kar izboljša učinkovitost in skalabilnost v večjih omrežjih. Pri podjetju Cisco Systems pa je bil razvit PVST (Per VLAN STP), kjer ima vsak VLAN svojo STP instanco, kar omogoča večjo prilagodljivost, a deluje le na Cisco stikalih. Nadgrajena različica tega protokola je RPVST (Rapid Per VLAN STP), ki temelji na RSTP in omogoča zelo hitro konvergenco, saj vsak VLAN uporablja svojo RSTP instanco. Vsaka različica STP ima svoje prednosti in je primerna za različne vrste omrežij, odvisno od hitrosti konvergence, združljivosti in podpore za VLAN-e. Povzete glavne značilnosti različic STP protokola so prikazane v tabeli 1 spodaj:

Protokol	Standard	Hitrost konvergence	Podpora za več VLAN-ov	Združljivost
STP (IEEE 802.1D)	IEEE 802.1D	Počasna (do 50 sekund)	Ne	Starejši standard, združljiv s skoraj vsemi napravami
RSTP (IEEE 802.1w)	IEEE 802.1w	Hitrejša (okoli 3 sekunde)	Ne	Združljiv s STP, a potrebuje podporo v stikalu
MSTP (IEEE 802.1s)	IEEE 802.1s	Hitrejša (okoli 3 sekunde)	Da (več instanc STP za skupine VLAN-ov)	Združljiv z RSTP/STP, a zahteva dodatno konfiguracijo
PVST (Cisco)	Cisco	Počasna (do 50 sekund)	Da (ločena instanca STP za vsak VLAN)	Samo na Cisco stikalih
RPVST (Cisco)	Cisco	Hitrejša (okoli 3 sekunde)	Da	Samo na Cisco stikalih, temelji na RSTP

Tabela 1: Vrste STP protokola

Potrebno je dodati, da je implementacija različnih STP protokolov lahko različna med različnimi proizvajalci omrežne opreme. Prav tako je potrebno paziti, da v primeru različne opreme v istem omrežju uporabljamo protokole, ki jih podpirajo vsi proizvajalci uporabljene opreme.

Ključni koncepti STP protokola

STP potrebuje za svoje delovanje konfiguracijo STP na vseh stikalih, ki so vključena v STP, in na njih želimo kontrolirati redundanco in kapaciteto lokalnih omrežij. Ko je STP protokol omogočen na stikalih, začne svoje delovanje z vrsto korakov, s katerimi zagotovi topologijo omrežja brez zank. Stikala si med seboj izmenjujejo BPDU (Bridge Protocol Data Unit)

sporočila. BPDU sporočila se med stikali neprestano prepošiljajo z namenom posodabljanja informacije o topologiji in o konfiguraciji, ki jih stikala uporabljajo za določitev stanja svojih vmesnikov. Postopek se izvaja z naslednjimi koraki, ki so kasneje bolj podrobno razloženi:

- Stikala preko BPDU sporočil oglašujejo identifikacijsko število posameznega stikala, ki mu pravimo BID (Bridge ID).
- Stikala izvolijo korensko stikalo (Root Bridge).
- Stikala izračunavajo stroške poti (Cost).
- Stikala izberejo korenski vmesnik (Root Port).
- Stikala izberejo določen vmesnik (Designated Port).
- Vmesniki na stikalih gredo preko različnih stanj.

Stanja oziroma faze, preko katerih gredo vmesniki na stikalih, so naslednja:

Faza 1 - Blokiranje: Vmesniki ostanejo v stanju blokiranja in ne posredujejo prometa. Vmesniki samo poslušajo morebitno prisotnost BPDU-jev, ki jih prejmejo od sosednjih stikal. V tem stanju ostane stikalo 20 sekund. Primer, kako lahko vidimo v tem stanju LED prikazovalnike nad vmesniki, je prikazan na sliki 9.



Slika 9: Prikaz stanja vmesnikov v fazi blokiranja na zgornjem stikalu

Faza 2 – Poslušanje: Vmesniki se pripravljajo na posredovanje prometa, ampak ga še ne posredujejo. V tem času stikalo obdeluje informacije, ki jih je dobilo ob sprejemanju BPDU sporočil od sosednjih stikal. Z informacijami iz BPDU-jev si stikalo zgradi topologijo omrežja. Vmesniki so v tem stanju 15 sekund.

Faza 3 – Učenje: Vmesniki začnejo posodabljati tabelo MAC naslovov in se pripravljajo za posredovanje prometa, a še vedno ne posredujejo prometa. V primeru, da pridejo še kakšni BPDU-ji, jih dodatno obdelajo. Vmesniki so v tem stanju dodatnih 15 sekund.

Faza 4 – Posredovanje: Po pretečenih 50 sekundah, je stikalo prepričano, da ne bo tvorilo zanke s posredovanjem okvirjev (frames) in preide v stanje posredovanja prometa. Še vedno spremlja

spremembe topologije in obdeluje informacije od sprejetih BPDU sporočil, če le-ta pridejo. Sicer pa je sedaj to stanje stikala imenovano »normalno« stanje. To je stanje, ko se promet skozi stikalo posreduje.

Zgoraj omenjena izmenjava BPDU sporočil se zgodi vsaki 2 sekundi, zato so lahko napake predvidene in prepoznane že iz časovnih zamikov, ki se pojavijo in sprožijo odziv na spremembe v omrežju. Pred prepošiljanjem BPDU-jev se mora delovanje vmesnika najprej vzpostaviti. Del vzpostavitve so standardne STP faze omenjene zgoraj. Ta proces je pomemben za vmesnike, ki so povezani na druga stikala. Če vmesnik ni povezan na druga stikala, ampak predstavlja povezavo na končno napravo, to ni potrebno.

Zgoraj omenjeni koraki so osnova komunikacije med stikali, kjer je skonfiguriran STP protokol. Potrebno je namreč določiti vlogo stikal na enoličen način, da v vsakem trenutku stikala vedo, katero je glavno in da v vsakem trenutku pri spremembah topologije omrežje samodejno naredi novo odločitev in ohrani topologijo brez zank. Na začetku delovanja STP protokola je naprej določeno korensko stikalo (Root bridge), ki je vozlišče, preko katerega poteka funkcija protokola in glaven promet. Vse povezave in poti so določene glede na to stikalo. Korensko stikalo je izbrano na podlagi najnižjega identifikacijskega števila posameznega stikala, ki mu pravimo BID (Bridge ID). BID je določen kot kombinacija izračunane prioritete številke in MAC naslova stikala. Ko se BID izračuna med več stikali v omrežju, je kot korensko stikalo (Root Bridge) določeno tisto stikalo, ki ima najmanjšo število BID. Ko je korensko stikalo določeno, vsa stikala v omrežju izračunajo najkrajšo pot do njega.

Root Port je korenski vmesnik in je najbolj optimalna povezava vsakega stikala (razen samega korenskega stikala) proti korenskemu stikalu. To pomeni, da ima ta vmesnik najnižjo ceno poti do korenskega stikala. Cena vmesnika je določena s hitrostjo vmesnika. Večja kot je hitrost vmesnika, nižja je njegova cena v STP protokolu. Vmesnik z najnižjo ceno ima tako največjo hitrost proti korenskemu stikalu. Korenski vmesnik je tako vmesnik, ki je vedno v stanju pošiljanja prometa in omogoča pretok podatkov proti korenskemu stikalu.

Nato je za vsak segment izbran določen vmesnik, ki je odgovoren za posredovanje prometa naprej v omrežje. Je v stanju posredovanja in omogoča komunikacijo med segmenti. Izbran je na podlagi najnižje cene poti do korenskega stikala in če imata dva vmesnika enako ceno poti, se izbira nadaljuje glede na BID in MAC naslov. Vmesnik z manjšim BID številom oziroma manjšim MAC naslovom ima prednost.

Proces se začne z izbiro korenskega stikala, nato je določen korenski vmesnik na vsakem stikalu, za tem se za vsako povezavo določi določen vmesnik na segmentu. Vsi preostali vmesniki, ki bi lahko povzročili zanko, ostanejo v blokiranem stanju. Če pride do spremembe v topologiji (npr. odpove korenski vmesnik), STP ponovno izračuna najoptimalnejšo pot in ustrezno prilagodi stanje vmesnikov. Ob postavljeni konfiguraciji se to zlahka pogleda. To vidimo z le nekaj vnešenimi ukazi v CLI (Command Line Interface) komandnem vmesniku.

Prednosti koncepta Etherchannel ali Portgroup

STP protokol je primarno reševal redundantne povezave, zato je bila med napravama aktivna ena od dveh povezav, ki je bila na razpolago, druga pa je bila blokirana. S širjenjem aplikacij, ki zahtevajo veliko pasovno širino, kot so videoposnetki in interaktivna sporočila, se je pojavila potreba po večjih omrežnih kapacitetah in razširljivih pasovnih širinah. Kapaciteto omrežja lahko povečate z uporabo hitrejših povezav, vendar so hitrejša povezava dražje. Poleg tega se ta rešitev ne more spreminjati v nedogled in najde svojo omejitev, kjer najhitrejši možni vmesnik ni več dovolj hiter. Kapaciteta povezav med stikali se prav tako lahko poveča z uporabo več fizičnih povezav med stikali. Slaba stran te metode je, da morate biti pri konfiguraciji vsake fizične povezave strogo dosledni, saj se z uvedenim STP protokolom povezave lahko blokirajo in dodatne povezave služijo samo redundanci. S tem namenom je Cisco razvil protokol Etherchannel, ki ponuja rešitev v takih primerih. Tehnologija EtherChannel je bila razvita kot sredstvo za povečanje kapacitete med stikali z grupiranjem večih fizičnih vmesnikov (na primer FastEthernet ali GigabitEthernet) v eno logično povezavo EtherChannel. Protokol deluje tako, da dve ali več povezav združi v eno logično povezavo, ki ponuja na uporabo seštevek kapacitet vseh članov v grupi. Ker sta dve ali več fizičnih povezav združeni v en sam EtherChannel, STP ne vidi več posameznih fizičnih povezav, ampak namesto tega vidi eno samo EtherChannel povezavo. Posledično STP protokolu ni treba blokirati ene od fizičnih povezav, da prepreči zanko. Ker so vse fizične povezave v skupini EtherChannel aktivne, se pasovna širina in s tem kapaciteta poveča. EtherChannel zagotavlja dodatno pasovno širino brez nadgradnje povezav na hitrejšo in dražjo povezavo, ker se opira na obstoječe vmesnike na stikalih. Dodatno ponuja tudi zaščito, ker ob izgubi enega od vmesnikov v grupi sama grupa normalno deluje naprej. Zmanjša se le njena skupna kapaciteta. Ko vmesnik povrnemo v prvotno stanje se njegova kapaciteta prišteje v skupno kapaciteto grupe.

Eksperimentalni del

Namen raziskovalne naloge je bil povečati in omogočiti redundanco na ravni dostopa v omrežjih, ter povečati in omogočiti čim večjo kapaciteto prenosa podatkov med napravami. Pred eksperimentalnim delom sem si zadal tri hipoteze, ki so bile:

- STP lahko reši redundanco brez prekinitve prometa.
- Konvergenca STP protokola se lahko izboljša.
- Več povezav prinese večjo prepustnost omrežja.

Pri izvajanju eksperimentov sem uporabil različne metode in izvedel meritve, ki jih bom predstavil v nadaljevanju. Opazoval sem spremembe pri prenosu podatkov skozi omrežje in analiziral podatke.

Topologija omrežja

Za raziskovanje sem načrtoval manjše omrežje. Sestavljeno je bilo iz dveh stikal in dveh računalnikov. Ethernet povezave med njimi so UTP kabli kategorije 5e. Dve stikali sta bili povezani z več UTP kabli za zagotovitev redundance tega majhnega omrežja. Dva UTP kabla sta bila vključena v topologiji, kjer sem preizkušal Spanning Tree Protokol, trije pa so bili priključeni ko sem preizkušal Etherchannel protokol. Osnovna topologija brez redundančnih povezav in povezav za večanje zmogljivosti je prikazana na sliki 10 spodaj:



Slika 10: Prikaz osnovne topologije brez redundančnih povezav

Uporabljena oprema

V izvedbi raziskovalnega poskusa so bile uporabljene žične povezave z UTP kabli kategorije 5e, katerega hitrost prenosa podatkov je zadostovala potrebam mojih poskusov. Poleg dveh računalnikov, ki sta bila uporabljena za pretakanje filma (movie streaming) in za prenos datoteke, sta bila v omrežju uporabljeni še dve stikali. Uporabil sem računalnika znamke Apple in stikali podjetja Cisco Systems. Cisco Systems ponuja širok nabor stikal za različne potrebe,

od majhnih poslovnih omrežij do velikih podatkovnih centrov. Njihova ponudba vključuje serije, kot so Catalyst, Nexus in Meraki. Catalyst stikala so zasnovana za poslovna omrežja in podpirajo napredne funkcije, kot so VLAN, varnostne politike in mnogo drugih. Nexus stikala so optimizirana za podatkovne centre, medtem ko Meraki stikala omogočajo centralizirano upravljanje v oblaku. Predvsem Catalyst in Meraki seriji stikal imata modele tudi za manjša omrežja.

Uporabljeni sta bili dve stikali Cisco Catalyst 3560 Series PoE-24, ki ju lahko vidimo na slikah 11, 12 in 13. Cisco Catalyst 3560 Series PoE-24 je omrežno stikalo s štiriindvajsetimi FastEthernet vmesniki, ki podpirajo Power over Ethernet (PoE), kar omogoča napajanje naprav, kot so IP telefoni in dostopne točke, neposredno preko omrežnega kabla. Spada v kategorijo stikal plasti 3 (Layer 3), kar pomeni, da podpira usmerjanje med VLAN-i in se nekaj drugih funkcionalnosti, ki jih sicer uporabljamo pri usmerjevalnikih. Ima napredne varnostne funkcije in omogoča učinkovito upravljanje omrežja. Stikalo je primerno za mala in srednje velika podjetja, ki potrebujejo zanesljivo omrežno infrastrukturo z možnostjo napajanja priključenih naprav.



Slika 11: Cisco Catalyst 3560 Series PoE-24 stikali



Slika 12: Omrežne naprave



Slika 13: Cisco Catalyst 3560 Series PoE-24 stikali

Opravljen eksperimentalno delo sestavljata dva večja poskusa z unikatnimi scenariji. V vsakem poskusu so bile opažene spremembe, ter opravljene meritve sprememb. Osnovna topologija, ki je bila uporabljena pri obeh poskusih, je prikazana na sliki 14 spodaj. Med stikali ni narisanih povezav, saj se prav te v vsakem delu poskusov razlikujejo.



Slika 14: Prikaz osnovnih komponent LAN-a

Poskus 1:

Prvi poskus je sestavljen iz več delov, v katerih se je preizkušalo delovanje različnih tipov STP protokola, poleg tega pa tudi posledice zanke, ki se zgodi, če STP ni implementiran. Skozi celoten poskus, ki je bil izveden na omenjeni omrežni opremi, je potekalo pretakanje filma skozi omrežje. Film je bil deljen s strani strežnika, katerega je v tem primeru predstavljal prvi prenosni računalnik, video pa je sprejemal in predvajal drugi prenosnik na drugi strani omrežja. Da je to lahko potekalo, je bil na oba računalnika nameščen program VLC media player, ki je tovrstno povezavo omogočal in jo prikazal prijazno uporabniku. VLC media player je program, s katerim zlahka delimo video med dvema napravama.

1. del: STP protokol tipa PVST na stikalih.

Pred začetkom deljenja filma je morala biti narejena fizična postavitvev in povezava omrežnih naprav, poleg tega pa tudi konfiguracija na njih. Napravo se konfigurira s priklopom konzolnega kabla na omrežno napravo, v mojem primeru se je kabel priklopil na zadnjem delu naprave na konzolni vmesnik. Če se napravi določi IP število, je možno na že postavljenem omrežju brez konzolnega kabla dostopati do konfiguriranja naprave tudi s programom telnet, ki je namenjen dostopu na daljavo preko omrežja. Primer je prikazan na izpisu konfiguracije 1.

```
SW-DOWN#telnet 10.10.10.3
Trying 10.10.10.3 ... Open

SW-UP>enable
Password:
SW-UP#
```

Izpis konfiguracije 1: Primer uporabe programa telnet

Za namen testiranja konfiguracije in odpravljanja napak v omrežju se uporablja program ping, s katerim vidimo, ali so naprave med seboj povezane in je med njimi mogoča komunikacija. Če je rezultat testa ping programa klicaj (!), to pomeni, da je vse pravilno povezano, da je konfiguracija pravilna in se naprave vidijo med seboj. Če je rezultat pika (.), to vselej pomeni, da je nekaj narobe in da medsebojna komunikacija ni mogoča. Uspešen in neuspešen primer tega programa kažeta izpisa konfiguracij 2 in 3.

```
SW-UP#ping 10.10.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
```

Izpis konfiguracije 2: Primer uspešne konfiguracije z uporabo programa ping

```
SW-DOWN#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Izpis konfiguracije 3: Primer neuspešne komunikacije z uporabo programa ping

V prvem delu poskusa je bila topologija načrtovana tako, kot je prikazano na spodnji sliki 15:



Slika 15: Primer povezave za prvi del poskusa

Stikali sta bili povezani z dvema UTP kabloma in s hitrostjo povezave 100 Mbps. Ustvarjen je bil VLAN 10, ki je bil nameščen na vseh vmesnikih, ki so bili del poskusa. Tako so le naprave vključene v poskus lahko komunicirale med seboj. Globalno je bil implementiran STP protokol tipa PVST (Per VLAN STP), ki omogoča tudi lokalno delovanje na posamezna lokalna omrežja oziroma na posamezne VLAN-e. Globalno pomeni, da protokol poteka na vseh vmesnikih stikala in na vseh VLAN-ih. Vse to je bilo konfigurirano enako na vsakem stikalu posebej s spodnjo kodo, ki jo vidimo na izpisu konfiguracije 4:

```
SW-UP(config)#vlan 10
SW-UP(config-vlan)# exit
SW-UP(config)#spanning-tree mode pvst
SW-UP(config)#exit
SW-UP#
```

Izpis konfiguracije 4: Nastavitev VLAN-a 10 ter STP-ja tipa PVST

Po nastavitvah je bilo zagnano deljenje filma, ki je uspešno delovalo. Ker se je film pretakal brezhibno, vemo, da je bilo omrežje stabilno in pravilno skonfigurirano. Stanje vmesnikov je bilo pregledano z ukazom, ki je prikazan v izpisu konfiguracije 5 spodaj:

```
SW-DOWN#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
            Address    0014.6a27.4f00
            Cost      19
            Port      9 (FastEthernet0/7)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778 (priority 32768 sys-id-ext 10)
            Address    001b.54f6.eb00
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 15

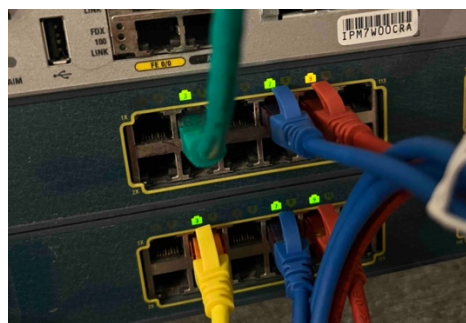
Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/3          Desg FWD 19        128.5   P2p
Fa0/7          Root FWD 19        128.9   P2p
Fa0/9          Altn BLK 19        128.11  P2p
```

Izpis konfiguracije 5: Pregled stanja vmesnikov med delovanjem STP protokola

Opazimo, da je promet potekal po vmesnikih Fa0/3 in Fa0/7, vmesnik Fa0/9 pa je bil blokiran zaradi implementiranega STP protokola. V procesu vzpostavitve STP je bilo določeno vodilno stikalo (RootBridge), glede na katerega se postavijo vmesniki v stanje, ki je odvisno od nastavitve protokola STP in od fizičnih parametrov vmesnikov na stikalu. Vmesnik Fa0/3 je vmesnik, ki je predstavljal povezavo stikala z računalnikom, Fa0/7 in Fa0/9 pa sta služila povezavi med stikaloma. Oba vmesnika Fa0/3 in Fa0/7 sta bila v stanju FWD (Forwarding) in sta omogočala prenos podatkov. Fa0/9 je predstavljal povezavo, kjer promet ne teče, saj je v stanju BLK (Blocking). Boljšo predstavo delovanja omogočata sliki 16 in 17:



Slika 16: Prikaz stanja vmesnikov med delovanjem STP protokola



Slika 17: Prikaz stanja vmesnikov z LED lučkami na stikalih

2. del: onemogočen STP protokol in posledice.

V drugem delu poskusa se je na vseh VLAN-ih onemogočil prej vzpostavljen STP protokol.

To sem naredil z ukazom, ki ga prikazuje izpis konfiguracije 6 spodaj:

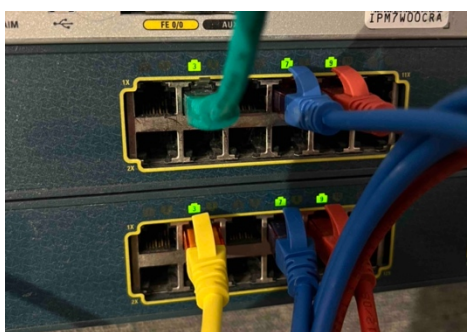
```
SW-UP(config)#no spanning-tree vlan 10
```

Izpis konfiguracije 6: Ukaz za onemogočanje STP protokola

Potem, ko se je STP protokol onemogočil, se je pretakanje videa ustavilo. Vsi vmesniki so bili v stanju FWD, kar pomeni, da tudi vmesnik Fa0/9 ni bil več blokiran. LED lučke na stikalih so bile zelene, kar nam potrjuje aktivnost uporabljenih vmesnikov. Prikaz stanja vmesnikov je razviden na slikah 18 in 19:



Slika 18: Prikaz stanja vmesnikov na stikalih brez STP protokola



Slika 19: Prikaz stanja vmesnikov z LED lučkami na stikalih

Promet na vmesnikih Fa 0/7 in Fa 0/9 se je iz minute v minuto povečeval in je bil na obeh vmesnikih enak, kar pomeni, da se je naredila zanka (loop). Promet se je na ta način povečeval do velikosti vmesnika (Fast Ethernet – 100 Mbps). Prav tako se na izpisu vidi, da se je povečevalo število paketov, ki so krožili med vmesniki in da sta bila v vseh primerih protokol (protocol) in linija (line) na obeh vmesnikih v stanju “up”. Razliko v prometu v različnih časovnih meritvah prikazujeta izpisa konfiguracije 7 in 8 na naslednji strani:

```

SW-DOWN#show interface FastEthernet0/9
FastEthernet0/9 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 001b.54f6.eb0b (bia
001b.54f6.eb0b)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 110/255, rxload 110/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:16, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
5 minute input rate 43365000 bits/sec, 75605 packets/sec
5 minute output rate 43378000 bits/sec, 75606 packets/sec

```

Izpis konfiguracije 7: Izpis prometa po prvi minuti vzpostavitve zanke

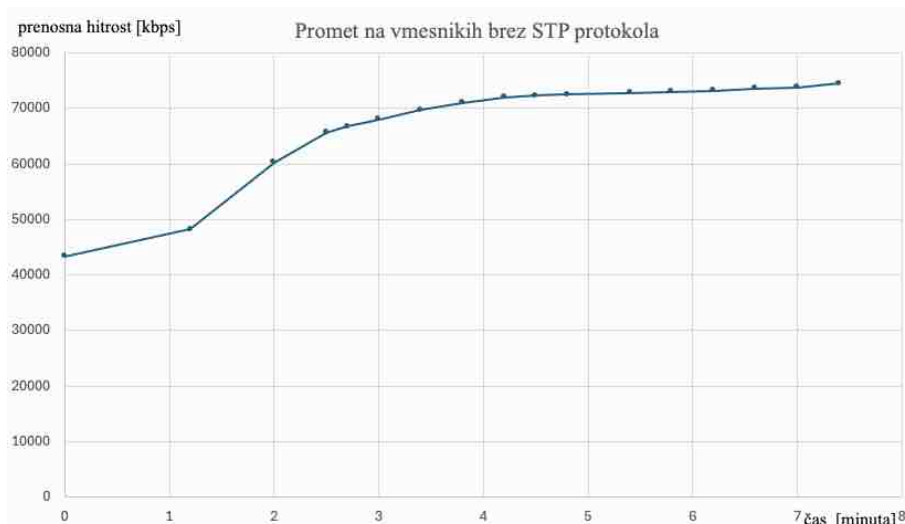
```

SW-DOWN#show interface FastEthernet0/9
FastEthernet0/9 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 001b.54f6.eb0b (bia
001b.54f6.eb0b)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 186/255, rxload 186/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:10, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
5 minute input rate 73089000 bits/sec, 103933 packets/sec
5 minute output rate 73091000 bits/sec, 103931 packets/sec

```

Izpis konfiguracije 8: Izpis prometa po sedmih minutah delovanja zanke

Promet, ki ga predstavljajo paketi na omrežju, se je ob izklopu STP protokola zelo hitro povečeval. Čas, v katerem količina prometa naraste do zgornje meje zmogljivosti vmesnika, je odvisen od količine prometa, ki teče skozi stikalo, od zmogljivosti stikala in od konfiguracije, ki je aktivna na stikalu. Ko se vmesniki do konca napolnijo s prometom, se pojavi več težav. Obremenitev procesorja se močno poveča, okvirji (frames) se začnejo izgubljati, močno se poveča zakasnitev prometa in stikalo postane izrazito nestabilno, kar vidimo kot slabo delovanje in na koncu prekinitve povezave. Kot je omenjeno v poglavju zgoraj, v žargonu rečemo, da se zgodi broadcast nevihta (broadcast storm). Pri mojem poskusu promet skozi stikalo ni bil pretirano velik, zato je zapolnitev stikala trajala dlje časa. Izkazalo se je, da se je promet v prvih šestih minutah povečeval hitreje, potem pa se je povečeval počasneje in enakomerneje. Na vmesnikih Fa0/7 in Fa0/9 je bil promet enak, saj sta obe povezavi sestavljali zanko, po kateri so se kopičili okvirji (frames). Film, ki se je prenašal skozi omrežje, je naprej imel zakasnitve, kasneje pa nehal delovati. Graf 1 na naslednji strani prikazuje večanje prometa v odvisnosti od časa pri mojem poskusu:



Graf 1: Prikaz večanja prometa na vmesnikih v odvisnosti od časa

3. del: klasičen tip STP protokola na stikalih.

V tretjem delu poskusa je bil po istem postopku kot v prvem delu nazaj implementiran STP protokol na obe stikali. Tokrat je bil implementiran klasičen tip STP protokola, ki je bil naprej omogočen na prvem stikalu. Tik ob zagonu ukaza so se vse tri LED lučke na povezanih vmesnikih Fa0/3, Fa0/7, Fa0/9 prižgale v oranžni barvi, kar pomeni, da so se začeli standardni koraki vzpostavitve vmesnikov za STP protokol. Kot omenjeno v predhodnem poglavju je prvi korak namreč stanje BLK (blokiranja). Prikaz stanja vmesnikov v času prve faze je prikazan na sliki 20:



Slika 20: Prikaz stanja vmesnikov v času prve faze

Pri vzpostavitvi vmesnikov v okviru STP le-ti preidejo skozi štiri ključne faze, ki so natančno opisane v prejšnjem poglavju. Ker je STP odgovoren za vzdrževanje topologije brez zanke, gre standardni proces vzpostavitve STP protokola vedno skozi vse faze preverjanja ali je zanka vzpostavljena ali ne. Dokler je STP vključen samo na enem stikalu, protokol vzpostavi stanje na enem stikalu. Če so vmesniki povezani z drugimi stikali, se BDPU-ji izmenjujejo med vsemi stikali, kjer je uporabljen oziroma skonfiguriran STP protokol. Izmenjava BDPU-jev v praksi pomeni, da se stikala med seboj dogovorijo kakšna je topologija omrežja in kateri vmesniki bodo v stanju FWD (posredovanja prometa) in bodo pošiljali promet naprej ter kateri vmesniki

bodo v stanju BLK (blokiranja prometa) in bo promet blokiran. Na ta način se ustvari topologija brez zank.

Standardni postopek vzpostavitve STP protokola tako potrebuje 50 sekund, da stikalo preide iz stanja blokiranja vmesnikov v stanje posredovanja vmesnikov. Pri pogostih spremembah nastavitvev STP protokola na Cisco Stikalih se lahko zgodi, da so vmesniki pri ponovni vzpostavitvi STP protokola že prešli preko stanja blokiranja in gredo pri ponovni vzpostavitvi STP protokola le preko stanja poslušanja in učenja. V tem primeru je čas trajanja med blokiranjem in posredovanjem lahko samo 30 sekund.

V mojem poskusu se je po tridesetih sekundah STP vzpostavil, topologija je bila določena in vmesnika Fa0/3 ter Fa0/7 sta stopila v stanje posredovanja. Vmesnik Fa0/9 je ostal v stanju blokiranja.

Po spremembi konfiguracije na prvem stikalu je bil isti postopek ponovljen še na drugem. Trideset sekund po zagonu je STP tudi na drugem stikalu postavil vmesnika Fa0/3 in Fa0/7 v stanje posredovanja (goreli sta zeleni LED lučki). Vmesnik Fa0/9 pa je bil v stanju blokiranja (gorela je oranžna LED lučka). Prav tako je bil med tem vmesnik Fa0/9 na prvem stikalu še vedno blokiran. V naslednjih 20 sekundah, skupno 50 sekundah, sta se stikali dokončno dogovorili za STP in je samo eno od stikal blokiral vmesnik Fa0/9. V mojem primeru so bili na prvem stikalu vsi vmesniki v stanju posredovanja, na drugem pa je bil Fa0/9 blokiran, da se je preprečil nastanek zanke. Stanje je bilo identično kot pri prvem delu poskusa. Pregled STP protokola na drugem stikalu nam prikazuje izpis konfiguracije 9 spodaj:

```
SW-DOWN#show spanning-tree

Spanning tree enabled protocol ieee
Root ID    Priority    32769
           Address    0014.6a27.4f00
           Cost      19
           Port      9 (FastEthernet0/7)
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    32778 (priority 32768 sys-id-ext 10)
           Address    001b.54f6.eb00
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time 15

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/3          Desg FWD 19        128.5    P2p
Fa0/7          Root FWD 19        128.9    P2p
Fa0/9          Altn BLK 19        128.11   P2p
```

Izpis konfiguracije 9: pregled STP protokola in stanja vmesnikov

Video je po ponovni vzpostavitvi spet tekkel naprej brezhibno.

Ob pretoku videa (v mojem primeru testnega filma) skozi vmesnike govorimo o UDP tipu prometa. Hitrost prenosa je odvisna od zahtev končne naprave, ki predvaja pretočni video. Dodatno je pomembno povedati, da je pretok videa samo v eni smeri (od strežnika proti končnemu uporabniku). Pretočnost prometa lahko preverimo na stikalih, kjer vidimo količino prometa kot 5-minutno povprečje hitrosti prenosa in količine okvirjev (frames oziroma kot piše v izpisu, packets). Promet, ki je potekal skozi vmesnike je bil pregledan z ukazom *show interface FastEthernet x/x*, kjer je x/x številka vmesnika. Vmesnik Fa0/9 je bil blokiran in skozi njega promet ni potoval, vmesnik Fa0/7 pa je bil v stanju posredovanja in je posredoval promet pretoka videa. Oba izpisa sta prikazana na izpisu konfiguracij 10 in 11 spodaj:

```
SW-DOWN#show interface FastEtherent 0/9
FastEthernet0/9 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 001b.54f6.eb0b (bia
001b.54f6.eb0b)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:04, output hang never
  Last clearing of "show interface" counters 00:25:32
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

Izpis konfiguracije 10: Pregled prometa, ki poteka skozi vmesnik Fa0/9

```
SW-DOWN#show interface FastEtherent 0/7
FastEthernet0/7 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 001b.54f6.eb09 (bia
001b.54f6.eb09)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:09, output hang never
  Last clearing of "show interface" counters 00:25:26
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 561000 bits/sec, 81 packets/sec
```

Izpis konfiguracije 11: Pregled prometa, ki poteka skozi vmesnik Fa0/7

Dodatno je potrebno omeniti, da je bil tudi promet na vmesniku Fa0/3. Promet je bil enako velik kot na vmesniku Fa0/7, ker je pretok videa potekal preko obeh vmesnikov v enaki hitrosti. Dodatno lahko vidimo, da je bil pretočni video na vmesniku Fa0/7 samo v eni smeri, ker je bil prenos videa samo od strežnika proti končnemu odjemalcu in ne v obratni smeri.

Po pregledu vseh nastavitev in stanja stikal sem izključil kabel iz vmesnika Fa0/7, po katerem je potekal ves promet. Video se je ustavil za čas, ki je potreben, da se promet prenese na

vmesnik Fa0/9, ki je bil prej blokiran in je čakal v pripravljenosti preko delovanja STP protokola. To je čas konvergence, ki je v primeru običajnega STP protokola znašal 30 sekund. Po 30 sekundni prekinitvi se je pretočni video spet vzpostavil in deloval naprej normalno. Pri pregledu STP-ja smo ugotovili, da sta bila vmesnika Fa0/9 na obeh stikalih tedaj aktivna, za vmesnika Fa0/7 pa se je izkazalo, da je bilo stanje vmesnikov "down". Stanje "down" pomeni, da je povezava onemogočena zaradi fizične napake na liniji. V mojem primeru je bil to iztaknjen kabel. Morda bi kdo mislil, da sta bila vmesnika Fa0/7 v stanju blokiranja (BLK), ampak če je fizična napaka na liniji, je stanje "down" prioritetno in nam hkrati več pove o sami napaki.

4. del: STP protokol tipa RPVST na stikalih

Četrty del poskusa je prikazoval implementacijo STP protokola tipa RPVST (Rapid Per VLAN STP). Tip RPVST še vedno uporablja BPDU sporočila med stikali. Razlika je v tem, da se BPDU sporočila izmenjujejo hitreje in vsebujejo dodatne informacije o topologiji, kar omogoča hitrejšo odločitev stikala. Poleg tega so dodana še nova stanja vmesnikov. Na ta način RPVST ne potrebuje prehoda skozi vsa stanja v času 50 sekund, kot je bilo to potrebno pri običajnem STP protokolu. Konvergenca se tako zgodi namesto v 50 sekundah samo v samo nekaj sekundah, tipično v treh sekundah. RPVST tip protokola je bolj prilagodljiv, a njegova implementacija poveča porabo procesorskih virov na stikalu. Cilj tega dela poskusa je bil prikaz hitrejše konvergence in nastavitve samega protokola, ki deluje isto kot v prvem in tretjem delu poskusa.

Konfiguracija RPVST-ja je prikazana v izpisu konfiguracije 12:

```
SW-UP(config)#spanning-tree mode rapid-pvst
```

Izpis konfiguracije 12: Implementacija STP tipa RPVST

Po konfiguraciji RPVST in konvergenci, ki je trajala nekaj sekund, se je pretočni video normalno prikazoval na zaslonu. Po izključitvi aktivnega kabla na stikalu se je video ustavil v eni sekundi. Pomembno je poudariti, da se je video v vseh poskusih ustavil po približno eni sekundi od napake. Razlog je ta, da program VLC pri pretočnem videu uporablja predpomnilnik (buffer) videoposnetka, ki v naprej shrani vsebino video posnetka za približno eno sekundo. S povečanjem predpomnilnika, bi lahko dosegli, da bi bilo več videa shranjenega vnaprej. Ko se je video po eni sekundi ustavil, je bilo potrebno počakati na konvergenco

RPVST protokola, ki je znašala tri sekunde. Ker je konvergenca bistveno krajša, se je namesto v 50 ali 30 sekundah promet prenesel na prej blokiran vmesnik že v treh sekundah in spet omogočil delovanje pretočnega videa. Kot sem omenil zgoraj, bi lahko s povečanjem predpomnilnika v VLC aplikaciji dosegli, da bi za čas konvergence RPVST protokola imeli vnaprej shranjen video v predpomnilniku, s tem med preklopom na drugi vmesnik stikala, med RPVST konvergenco, video ne bi zatal.

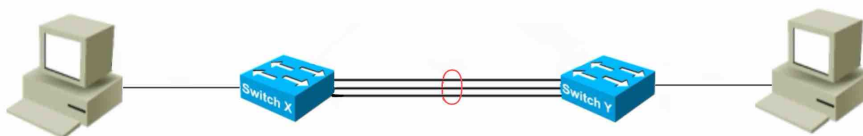
Poskus 2:

Drugi poskus se ne navezuje na STP protokol. Za namen povečanja kapacitete in hkrati redundantnih povezav so bili na obeh stikalih skonfigurirani trije vmesniki (Fa0/13, Fa0/14, in Fa0/15) v grupo Etherchannel, za katero je bila uporabljena koda, ki je prikazana v izpisu konfiguracije 13. Konfiguracija določa, katere vmesnike bomo uporabili v Etherchannel skupini in jo aktivira:

```
SW-UP>enable
SW-UP#configure terminal
SW-UP(config)#interface range FastEthernet0/13 - 15
SW-UP(config-if-range)#channel-group 1 mode active
```

Izpis konfiguracije 13: Dolocitev in združevanje vmesnikov v Etherchannel skupino

Topologija omrežja z Etherchannel in vsemi tremi delujočimi vmesniki in kabli je prikazana na slikah 21 in 22:



Slika 21: Prikaz implementiranega Etherchannelja



Slika 22: Prikaz stanja vmesnikov ob delovanju Etherchannelja

Po opravljeni konfiguraciji na vsakem stikalu je bilo pregledano stanje in pregledani so bili rezultati konfiguracije. V pregledu Etherchannel konfiguracije smo videli, da je bil le-ta uspešno konfiguriran na pravih vmesnikih, kot je prikazano v izpisu konfiguracije 14:

```

SW-UP#show etherchannel 1 summary
Flags: D - down          P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use        f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1 (SU)      LACP        Fa0/13(P)  Fa0/14(P)  Fa0/15(P)

```

Izpis konfiguracije 14: Izpis rezultata Etherchannel konfiguracije

V primeru pri drugem poskusu so bili vsi vmesniki, na katere so bili priključeni UTP kabli, uporabljeni v skupini Etherchannel, enake hitrosti oziroma pasovne širine (bandwidth). Znašala je 100 Mbps in zato povečanje števila povezav med obema stikaloma v mojem primeru ne prinese večje pretočnosti. Povezava končnih naprav (prva naprava z FTP (File Transfer Protocol) strežnikom za deljenje datotek in druga naprava z FTP odjemalcem za prevzem datotek) na stikalo je bila izvedena preko vmesnika s prenosno hitrostjo 100 Mbps. Kljub temu da so vse tri povezave v skupini Etherchannel (3x 100 Mbps) skupaj omogočale 300 Mbps prenosa, končna naprava s priklopom 100 Mbps ni mogla izkoristiti več kot 100 Mbps pasovne širine in tako v nobenem primeru ni presegla pretoka 100 Mbps.

Zaradi tega je bila za namen poskusa hitrost na vsakem vmesniku, Fa0/13, Fa0/14, in Fa0/15 nastavljena na 10 Mbps, kot je prikazano v izpisu konfiguracije 15. Skupaj je bila potem maksimalna hitrost 30 Mbps (3x 10 Mbps), kar vidimo na izpisu konfiguracije 16.

```

SW-UP#configure terminal
SW-UP(config)#interface FastEthernet0/13
SW-UP(config-if)#speed 10
SW-UP(config-if)#exit
SW-UP(config)#
SW-UP(config)#interface FastEthernet0/14
SW-UP(config-if)#speed 10
SW-UP(config-if)#exit
SW-UP(config)#
SW-UP(config)#interface FastEthernet0/15
SW-UP(config-if)#speed 10
SW-UP(config-if)#exit
SW-UP(config)#

```

Izpis konfiguracije 15: Nastavitev hitrosti vmesnikov na 10 Mbps

```

SW-UP#show interfaces Fa0/13 Fa0/14 Fa0/15
interface FastEthernet0/13
switchport access vlan 10
switchport mode access
speed 10
channel-group 1 mode active
!
interface FastEthernet0/14
switchport access vlan 10
switchport mode access
speed 10
channel-group 1 mode active
!
interface FastEthernet0/15
switchport access vlan 10
switchport mode access
speed 10
channel-group 1 mode active

```

Izpis konfiguracije 16: Pregled vmesnikov Fa0/13, Fa0/14, in Fa0/15

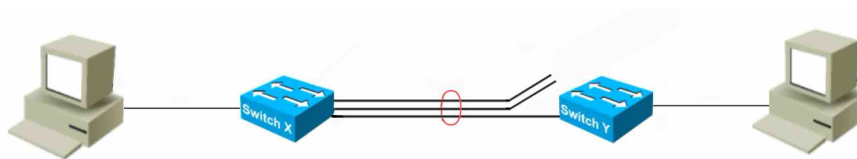
Kot sem omenil zgoraj, sem namesto pretočnega filma tokrat uporabil FTP strežnik za prenos datotek, ker je pretočni video potreboval precej manj pasovne širine in skupno ne bi dosegli niti 30 Mbps, kar je bila omejitev vseh treh vmesnikov v skupini Etherchannel. Pri uporabi FTP strežnika za prenos datotek pa je FTP odjemalec porabil toliko pasovne širine, kolikor je bilo na voljo. Po nastavitvi vmesnikov na nižjo hitrost (10 Mbps) je bil torej na prvi računalnik naložen FTP strežnik, na drugi računalnik pa FTP odjemalec, ki je sprejemal veliko datoteko, ki se je delila s strežnika.

Na začetku so bili vsi trije vmesniki v skupini Etherchannel vključeni in sem na FTP odjemalcu zagnal odjem datoteke. Port-channel 1 vmesnik, ki je prikazoval skupek vseh aktivnih vmesnikov v skupini Etherchannel je kazal pretok podatkov 30000 kbps (30 Mbps) pasovne širine.

V nadaljevanju poskusa je bil izklopljen kabel na vmesniku Fa 0/15 in je Port-channel 1 vmesnik kazal samo se 2 vmesnika v skupini kot "P" status ("P" status pomeni, da je vmesnik v skupini Etherchannel). Vmesnik Fa 0/15 je dobil status D ("D" status pomeni "down", kar prikazuje, da je vmesnik nekativen). Pasovna širina od Port-channel 1 se je zmanjšala s 30000 kbps na 20000 kbps, ker sta bila samo se dva delujoča vmesnika v skupini.

Ko sem v nadaljevanju izklopil kabel tudi na vmesniku Fa 0/14, je bil le še en vmesnik (Fa 0/13) s statusom P in pasovna širina se je zmanjšala na 10000 kbps. Stanje povezave med stikaloma po dveh izključenih UTP kabliah je dobro razvidno na sliki 12. Tudi pretok prometa preko Port-channel 1 (Etherchannel povezave, ki je imela tedaj samo en vmesnik v skupini) je padel s 30 Mbps na 20 Mbps in na koncu na 10 Mbps, kar lahko opazimo na izpisu konfiguracije 18. Dodatno je pomembno povedati, da se je čas prenosa datotek iz FTP strežnika

na FTP odjemalec z vsakim izklopom dodatnega vmesnika podaljševal. Slika 23 prikazuje končno verzijo s prometom 10 Mbps:



Slika 23: Prikaz povezave med stikaloma po dveh izključenih UTP kabliah

Prenos deljenja datoteke se ni nikoli ustavil, le hitrost se je zmanjševala pri manj aktivnih povezavah v Etherchannel skupini. Končno hitrost po dveh izključenih kabliah prikazuje izpis konfiguracije 18. Stanje aktivnih vmesnikov v Etherchannel skupini po dveh izklopljenih vmesnikih pregledamo z ukazom *show etherchannel 1 summary*, ki je prikazan v izpisu konfiguracije 17:

```
SW-DOWN#show etherchannel 1 summary
Flags: D - down          P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1 (SU)        LACP        Fa0/13(P) Fa0/14(D) Fa0/15(D)
```

Izpis konfiguracije 17: Izpis Ether channel obnove

```
SW-DOWN#show interface port-channel 1
Port-channel1 is up, line protocol is up (connected)
Hardware is EtherChannel, address is 001b.54f6.eb0f (bia
001b.54f6.eb0f)
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 236/255, rxload 3/255
Encapsulation ARPA, loopback not set
Full-duplex, 10Mb/s, link type is auto, media type is unknown
input flow-control is off, output flow-control is unsupported
Members in this channel: Fa0/13
ARP type: ARPA, ARP Timeout 04:00:00
```

Izpis konfiguracije 18: Kapaciteta Etherchannelja po dveh izključenih UTP kabliah

Ko sem začel vklapljati kable nazaj v vmesnike enega za drugim, se je pasovna širina povečevala s 10000 kbps na 20000 kbps in na koncu na 30000 kbps. Prav tako se je povečeval pretok podatkov preko Port-Chanel 1 vmesnika.

Zaključek in razprava

Raziskovalna naloga predstavi osnove računalniških omrežij, izzive, ki nastopijo ob zagotavljanju čim boljšega delovanja in načine, kako izzive uspešno rešujemo. Prvi del raziskovalne naloge predstavlja teoretični del, ki je zelo pomemben za razumevanje eksperimentalnega dela, ker je obravnavana vsebina zahtevna. Z večjim delom vsebine eksperimentalnega dela se navadno uporabniki neposredno ne srečujemo v vsakdanjem življenju, a moramo vedeti, da kadar vse deluje brezhibno, v ozadju tečejo procesi, ki k temu pripomorejo. Poznavanje delovanja omrežij lahko mnogim pomaga razumeti kompleksnost, zato lahko tudi začnemo ceniti trud, ki so ga v razvoj vložili inženirji vsepo svetu.

Prvi poskus prikazuje posledice napake zank v omrežju, do katerih pride, če je omrežje narobe načrtovano. Do izpada povezave ob napaki tako pride zelo hitro, kar je prikazano na priloženem grafu in dodatnih izpisih konfiguracij. Poskus opisuje razlike različnih STP protokolov, katerih različice so nastajale skozi čas, njihovo vzpostavitev in način konfiguracije. Predstavljene so tudi slike, preko katerih se naučimo, kako lahko to tudi kot laiki enostavno opazimo v primeru stika s temi napravami.

Glavni namen drugega poskusa je bil pokazati, da se prenos deljenja datoteke ob uporabi Etherchannelja ne prekine, temveč se samo zmanjša hitrost prenosa. Opazimo, da Etherchannel deluje neodvisno od STP protokola. Med povezavami v Etherchannel skupini ne nastaja zanka med vmesniki, ki so del skupine, saj ta protokol poveže vse povezave na vmesnikih v eno virtualno povezavo, ki ji pravimo Port-Channel in ji doda skupno kapaciteto vseh članov v Etherchannel skupini.

Po opravljenem eksperimentalnem delu sem dve hipotezi potrdil in eno ovrgel. Potrdil sem, da se konvergenca STP protokola lahko izboljša, saj lahko implementiramo boljše, naprednejše oblike STP protokola. Poleg te sem potrdil, da več povezav prinese večjo prepustnost. Za to pa ne zadošča protokol STP, temveč je potrebno implementirati protokol Etherchannel.

Ovrgel sem hipotezo, da STP lahko reši redundanco brez prekinitve prometa, saj, kot je razvidno v eksperimentalnem delu, ponovna vzpostavitev povezave potrebuje nekaj časa, ki je odvisen od tipa STP protokola.

V medijih pogosto zasledimo novice o razvoju tehnologij. Dandanes so najbolj aktualne novice o novih napravah, ter o umetni inteligenci. Moramo se zavedati, da novice potujejo po omrežju

in da umetna inteligenca prav tako izkorišča povezave naprav na omrežju. Vsa komunikacija poteka med vsaj dvema med seboj povezanima napravama. Povezave pa so implementirane na način z napravami, ki sem jih opisal v raziskovalni nalogi.

Sam sem se začel ukvarjati s to tematiko lansko leto, saj sem si zadal cilj, da opravi CCNA licenco v okviru podjetja Cisco Systems. Ta licenca je osnovna mednarodno priznana licenca, ki potrjuje poznavanje računalniških omrežij na osnovnem nivoju. To mi je dalo motivacijo in me spodbudilo k pisanju te raziskovalne naloge. Meritve in analiza rezultatov so potrdile, da STP učinkovito preprečuje omrežne zanke ter zagotavlja stabilnost redundantnih povezav. Preizkusi preklopa ob napakah so pokazali, da STP v določenih časovih dobro prispeva h razpoložljivosti omrežja. Ugotovitve raziskave poudarjajo, da sta pravilno konfigurirana STP in EtherChannel ključna za doseganje zmogljivosti in stabilnosti omrežja.

Raziskovalna naloga lepo predstavlja in odpira pogled v eno smer obsežne tehnologije, ki trenutno predstavlja velik del komunikacije človeštva in povezovanje vseh naprav na svetu v eno veliko omrežje, ki mu pravimo internet. Zato nameravam ta način dela in raziskovanja še nadgraditi, se lotiti nove raziskovalne naloge in se poglobiti v nove tematike, kot je na primer varnost internetnih omrežij, ki so prav tako zelo aktualne in zanimive.

V prihodnosti bi bilo za nadgradnjo raziskovalne naloge zanimivo poskusiti, kako bi kombiniral STP in Etherchannel protokol. V tem primeru bi bilo zanimivo preizkusiti delovanje dveh Etherchannel skupin, kjer bi bilo v vsaki od dveh skupin nekaj povezav med vmesniki na stikalih in bi STP protokol potekal med dvema takima Etherchannel skupinama. Šlo bi za naprednejšo in zmogljivejšo konfiguracijo, ki bi poleg redundance v omrežju omogočala tudi povečanje kapacitete in prepustnosti omrežja.

Zahvala

Za pomoč pri organizaciji oblike in časovnih rokov bi se rad zahvalil mentorju profesorju Sebastjanu Zamudi in profesorju Gregorju Križu. Za pomoč pri obdelavi podatkov ter za predstavitev tematike bi se rad zahvalil očetu Borisu Ilovarju.

Literatura

- [1] Cisco, "Cisco official website," spletni naslov: <https://www.cisco.com/>. (Pridobljeno: 11. 2. 2025).
- [2] Cisco Systems, "CCNA: Introduction to Networking," Cisco Networking Academy, 2024. Dostopno na: <https://www.netacad.com/courses/ccna>
- [3] Cisco, "Understanding Ethernet switching," spletni naslov: <https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/12006-chapter22.html>. (Pridobljeno: 17. 12. 2024).
- [4] Cisco, "EtherChannel configuration guide for Cisco 1900 routers," spletni naslov: https://www.cisco.com/c/en/us/td/docs/routers/access/1900/software/configuration/guide/Software_Configuration/etherchannel.html. (Pridobljeno: 19. 12. 2024).
- [5] Slika 1, M. Mitchell, "LANs, WANs, and other area networks," *Lifewire*, 6.3. , 2020. Spletni naslov: <https://www.lifewire.com/lans-wans-and-other-area-networks-817376>. (Pridobljeno: 28. 2. 2025).
- [6] Slika 2, Network Academy, "InterVLAN routing," *Network Academy*, 2025. Spletni naslov: <https://www.networkacademy.io/ccna/ethernet/intervlan-routing>. (Pridobljeno: 3. 3. 2025).
- [7] Slika 4, Wikipedia contributors, "VLAN," *Wikipedia, The Free Encyclopedia*, Dec. 27, 2024. Spletni naslov: <https://en.wikipedia.org/wiki/VLAN>. (Pridobljeno: 3. 3. 2025).