Analiza rada protokola OSPF

Ilinović, Kristian

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

ZAVRŠNI RAD

Analiza rada protokola OSPF

Analysis of the OSPF Routing Protocol

Mentor: izv. prof. dr. sc. Marko Matulin

Student: Kristian Ilinović (0135256299)

Zagreb, 2023.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 8. svibnja 2023.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Tehnologija telekomunikacijskog prometa I**

ZAVRŠNI ZADATAK br. 7141

Pristupnik: **Kristian Ilinović (0135256299)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Analiza rada protokola OSPF**

Opis zadatka:

U radu je potrebno opisati ustroj LAN mreže te pružiti uvid u osnovne protokole usmjeravanja u takvom okruženju. Analizirati značajke protokola OSPF, hijerarhijskog ustroja OSPF mreže. Opisati osnovne značajke vrsta OSPF mreža.

Mentor:

izv. prof. dr. sc. Marko Matulin

Predsjednik povjerenstva za završni ispit:

Sažetak

Završni rad prikazuje LAN (*Local Area Network*) mrežu, fokusirajući se na usmjeravanje podataka i protokole usmjeravanja koji su bitni za njihovo funkcioniranje. Glavna tema rada je analiza *Open Shortest Path First* (OSPF) protokola, istražujući njegove značajke, ulogu i važnost u organizaciji LAN mreža. Osim toga, rad razmatra koncepte OSPF područja te vrste mreža koja se koriste u kontekstu OSPF-a. Rad istražuje kako OSPF protokol omogućuje efikasno usmjeravanje podataka unutar LAN mreža te kako područja i vrste mreža unutar OSPF-a doprinose skalabilnosti, sigurnosti i efikasnosti mrežnih infrastruktura.

Ključne riječi: LAN; usmjeravanje; protokoli usmjeravanja; OSPF; OSPF područja

Summary

The final paper presents a LAN (Local Area Network) network, focusing on data routing and routing protocols essential for their operation. The main theme of paper is the analysis of the Open Shortest Path First (OSPF) protocol, exploring its characteristics, role and importance in organizing LAN networks. Additionally, the paper examines OSPF are concepts and network types used in the context of OSPF. The paper explores how the OSPF protocol enables efficient data routing within LAN networks and how OSPF areas and network types contribute to scalability, security and efficiency of newtork infrastructures.

Keywords: LAN, routing, routing protocols, OSPF, OSPF areas

SADRŽAJ

1. UVOD....1
2. USTROJ LAN MREŽE....2
   2.1 OPĆENITO O LAN MREŽI....2
   2.2 TOPOLOGIJA LAN MREŽE....2
      2.2.1 FIZIČKA TOPOLOGIJA MREŽE....3
      2.2.2 LOGIČKA TOPOLOGIJA MREŽE....6
3. USMJERAVANJE I PROTOKOLI USMJERAVANJA....8
   3.1 USMJERAVANJE....8
   3.2 TABLICE USMJERAVANJA....9
   3.3 PROTOKOLI USMJERAVANJA....9
      3.3.1 PROTOKOL VEKTORA UDALJENOSTI....11
      3.3.2 PROTOKOL STANJA VEZE....12
      3.3.3 PROTOKOL VEKOTRA PUTANJE....13
4. ZNAČAJKE OSPF PROTOKOLA....14
   4.1 SPF ALGORITAM....15
   4.2 OSPF PAKETI....16
      4.2.1 OSPF ZAGLAVLJE PAKETA....16
      4.2.2 HELLO PAKET....17
      4.2.3 DATABASE DESCRIPTION PAKETI....18
      4.2.4 LINK STATE REQUEST PAKETI....18
      4.2.5 LINK STATE UPDATE PAKETI....19
      4.2.6 LINK STATE ACKNOWLEDGMENT PAKETI....19
   4.3 POUZDANOST OSPF PROTOKOLA....20
   4.4 OSPF METRIKA....20
   4.5 OSPF AUTENTIFIKACIJA....21
5. OSPF PODRUČJA....22
   5.1 BACKBONE PODRUČJE....23
   5.2 STUBY PODRUČJE....24
   5.3 POTPUNO STUBBY PODRUČJE....24
   5.4 NOT SO STUBBY PODRUČJE (NSSA)....25
6. OSPF VRSTE MREŽA....26
   6.1 POINT TO POINT MREŽA....26

6.2 BRODACAST MREŽA 26
6.3 NON-BROADCAST MREŽA 27
6.4 NON BROADCAST MULTI ACCESS (NBMA) 27
6.5 POINT TO MULTIPOINT 28
7. ZAKLJUČAK 29
LITERATURA 30
POPIS KRATICA 33
POPIS SLIKA 34

1. UVOD

U modernom društvu pojavljuje se eksponencijalni rast količine podataka prenesenih telekomunikacijskim mrežama. Rastom broja uređaja koji se spajaju na mrežu dolazi do sve veće potrebe za učestalom nadogradnjom mrežne infrastrukture. Kako bi se osigurala sigurna isporuka informacija od izvora do odredišta, koristi se dinamička metoda usmjeravanja koja je otporna na promjene topologije mreže, njenu nadogradnju i prekide u mreži.

Svrha ovog rada je analizirati rad OSPF *(Open Shortest Path First)* protokola. Objasnit će se umjeravanje i protokoli usmjeravanja. Prikazat će se izrada tablica usmjeravanja. Prikazat i opisat će se izgled OSPF paketa. Objasnit će se OSPF područja i vrste OSPF mreža.

Završni rad se sastoji od sedam poglavlja:

1. Uvod.
2. Ustroj LAN mreže.
3. Usmjeravanje i protokoli usmjeravanja.
4. Značajke OSPF protokola.
5. OSPF područja.
6. OSPF vrste mreže.
7. Zaključak.

U drugom poglavlju bit će opisana LAN *(Local Area Network)* mreža. Prikazat će se razlika između fizičke i logičke topologije. Napravit će se podjela fizičke topologije. Treće poglavlje opisuje usmjeravanje u mreži. Prikazan je način izrade tablica usmjeravanja te su detaljno objašnjeni protokoli usmjeravanja.

U četvrtom poglavlju opisane su značajke OSPF protokola. Prikazani i objašnjeni su OSPF paketi, OSPF metrika, pouzdanost i autentifikacija OSPF protokola. Peto poglavlje bavi se OSPF područjima, svako pojedino područje je dodatno opisano.

U šestom poglavlju prikazane i opisane u vrste mreža u kojima OSPF protokol radi.

2. USTROJ LAN MREŽE

Local area network (LAN) je mreža namijenjena povezivanju računala i drugih mrežnih uređaja na manjim udaljenostima, primjerice unutar jedne zgrade, ureda ili kuće. Mnogi LAN-ovi mogu biti samostalni (odvojeni od bilo koje druge mreže) ili biti povezani s drugim LAN-ovima ili WAN-om *(Wide Area Network)* (poput Interneta)[1].

2.1 OPĆENITO O LAN MREŽI

Rast elektroničkih i računalnih tehnologija 1970-ih omogućio je dostupnost malih osobnih računala korisnicima. Prije toga, računalni su zadaci obavljani u velikoj mjeri računalima na centraliziranim lokacijama [2]. Raširena uporaba osobnih računala potaknula je potrebu za komunikacijskom opremom koja bi to mogla povezati. To je dovelo do stvaranja lokalnih mreža (LAN). One su olakšale decentralizaciju računalnih zadataka dopuštajući da računala povezana na mrežu razmjenjuju informacije između sebe, bez prolaska kroz središnje mjesto.

Lokalna mreža omogućuje komunikaciju na srednjim udaljenostima velikim brzinama. Za većinu LAN-ova, najveća udaljenost između dva usmjerivača u mreži je oko 100 metara, a brzina prijenosa je do 100 Mb/s. Također većina lokalnih mreža podržava do nekoliko stotina čvorova, tj. umreženih uređaja. Posebna vrsta lokalne mreže, industrijska mreža, je ona koja ispunjava sljedeće kriterije:

- Sposobnost za podršku kontrole u stvarnom vremenu.
- Visok integritet podataka (otkrivanje pogrešaka).
- Visoka pouzdanost u teškim uvjetima.

Druge dvije uobičajene vrste lokalnih mreža su mreže poslovnih sustava (npr. *Ethernet*) i mreže paralelne sabirnice (npr. *Cluster/One*). Poslovne mreže ne zahtijevaju toliku otpornost na smetnje kao industrijske mreže, budući da se koriste u uredskim okruženjima. Također imaju manje stroge zahtjeve glede vremena pristupa. Korisnik poslovne radne stanice može pričekati nekoliko sekundi za informacije, ali stroj kojim upravlja PLC (*Programmable Logic Controller*) može zahtijevati informacije unutar milisekundi za ispravan rad. Paralelne mreže imaju zahtjeve slične poslovnim mrežama i namijenjene su mikroračunalima i miniračunalima koja se koriste u uredskim okruženjima na malim udaljenostima.

2.2 TOPOLOGIJA LAN MREŽE

Mrežna topologija definira različite kategorije po kojima se mogu identificirati sastavni dijelovi i način funkcioniranja računalne mreže. Na osnovu tih kategorija mreže se mogu podijeliti na manje sastavne dijelove i organizirati raspored tih elemenata. Također, može se opisati način pristupa tih manjih dijelova cijeloj mreži.

Izgled topologije mreže izravnao utječe na njezinu funkcionalnost. Pravilnim odabirom topologije mogu se poboljšati performanse i učinkovitost prijenosa podataka, optimizirati raspodjela resursa i smanjiti operativni troškovi. Dijagrami mrežne topologije, koji su izrađeni softverom, važne su reference za pronalaženje problema s mrežnim povezivanjem, istraživanje usporavanje mreže i općenito rješavanje problema [3].

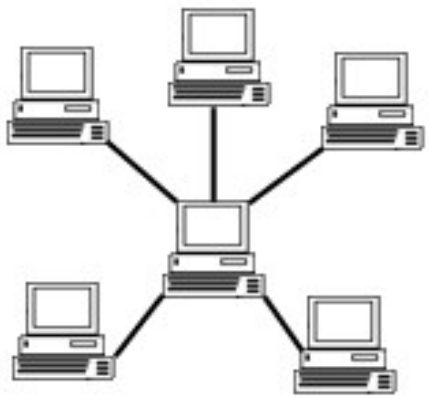
Jedna od primarnih upotreba mrežne topologije je definiranje konfiguracije raznih telekomunikacijskih mreža uključujući računalne mreže, zapovjedne i upravljačke radijske mreže. Najčešća podjela mrežne topologije se odnosi na fizičku i logičku topologiju.

2.2.1 FIZIČKA TOPOLOGIJA MREŽE

Fizička topologija objašnjava kako su mrežni uređaji fizički povezani ili kako su uređaji zapravo povezani jedni s drugima, poput kabela i bežičnih veza. To je dijagram koji prikazuje strukturu kako su uređaji fizički povezani unutar mreže, odnosi se na to kako mreža izgleda i funkcionira [4].

2.2.1.1 ZVJEZDASTA TOPOLIGIJA

Zvjezdasta topologija (slika 1), najčešća mrežna topologija, postavljena je tako da je svaki čvor u mreži izravno povezan s jednim središnjim čvorištem preko koaksijalnog ili optičkog kabela. Djelujući kao poslužitelj, ovaj središnji čvor upravlja prijenosom podataka budući da informacije poslane s bilo kojeg čvora na mreži moraju proći kroz središnji čvor da bi došle do odredišta. Također funkcionira kao repetitor kako bi pomogao u sprječavanju gubitka podataka [5].

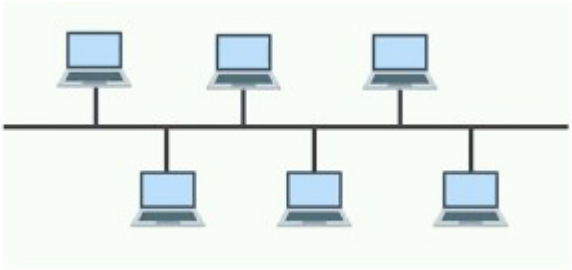


Slika 1. Zvjezdasta topologija [5]

Prednost zvjezdaste topologije je jednostavno dodavanje drugog uređaja na mrežu. Koristi se vrlo malo kabela za potpuno povezivanja uređaja na mrežu. Jednostavni mrežni dizajn omogućuje lakše prepoznavanje gdje se pojavljuju greške u mreži. Najveći problem kod ove topologije je mogućnost prestanka rada središnjeg preklopnika jer u tom slučaju cijela mreža pada i svi uređaji se isključuju iz mreže.

2.2.1.2 TOPOLOGIJA SABIRNICE

Topologija sabirnice je vrsta mrežne topologije gdje je svaki čvor, tj. svaki uređaj na mreži, spojen na glavnu kabelsku liniju što je prikazano slikom 2. Podaci se prenose jednom rutom, od jedne točke do druge. Nije moguće prenositi podatke u oba smjera. Kada ova topologija ima točno dvije krajnje točke, poznata je kao topologija linearne sabirnice. Uglavnom se koristi za male mreže [6].

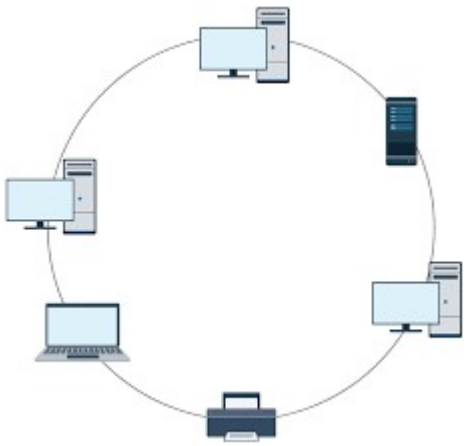


Slika 2. Sabirnička topologija [7]

Glavni problem sabirničke topologije nalazi se u mogućem kvaru glavnog kabela. U tom slučaju cijela mreža ne radi. Ova topologija uglavnom se koristi za male mreže. Prednosti sabirničke topologije su isplativost i jednostavnost. Proširenje se može izvesti jednostavnim povezivanjem kabela.

2.2.1.3 PRSTENASTA TOPOLIGIJA

Prstenasta topologija može biti mrežna konfiguracija u kojoj veze uređaja stvaraju kružni podatkovni put. Pri tome je svaki uređaj povezan s točno dva susjedna uređaja što je prikazano slikom 3. U ovom slučaju paketi putuju od jednog uređaja do drugog dok ne stignu do željenog odredišta. Podaci putuju samo u jednom smjeru, ali može biti i dvosmjerni način prijenosa podataka ako postoje dvije veze između svakog mrežnog čvora, to se naziva topologija dvostrukog prstena [8].



Slika 3. Prstenasta topologija [9]

Prednosti:

- Podaci putuju u jednom smjeru što smanjuje mogućnost kolizije paketa
- Mogu se dodati dodatni uređaji bez utjecaja na performanse mreže
- Nema potrebe za poslužiteljem za kontrolu povezanosti između čvorova
- Jeftino za ugradnju i proširenje
- Lako identificirati i izolirati pojedinačne točke kvara
- Prikladan za okruženje s velikim prometom u odnosu na topologiju sabirnice.

Nedostatci:

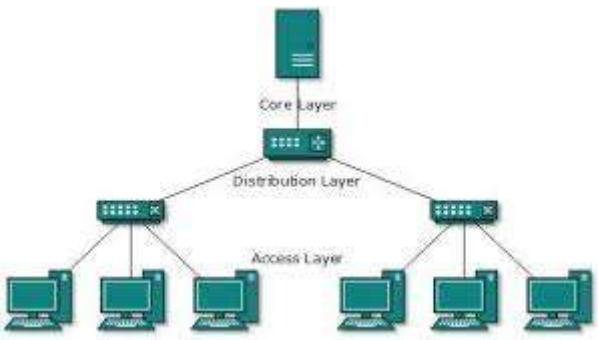
- Zbog jednosmjernog prstena svi podaci koji putuju moraju proći kroz svaki uređaj na svom putu do odredišta, što može smanjiti performanse
- Ako se jedan uređaj isključi to utječe na cijelu mrežu
- Ima sporiju izvedbu u usporedbi s topologijom sabirnice
- Skupo
- Teško je otkloniti kvar
- Kako bi svi uređaji komunicirali svi uređaji moraju biti uključeni
- Potpuna ovisnost o jednom kabelu.

2.2.1.4 TOPOLIGIJA STABLA

Također poznata kao hijerarhijska topologija, ovo je najčešći oblik mrežne topologije koja se trenutno koristi. Ova topologija oponaša proširenu zvijezdastu topologiju i nasljeđuje svojstva topologije sabirnice. Slika 4 prikazuje topologiju stabla.

Topologija stabla dijeli mrežu na više razina/slojeva. Uglavnom mreža je podijeljena na tri vrste mrežnih uređaja. Najniži je pristupni sloj na koji su priključena računala. Srednji sloj je poznat kao distribucijski sloj, koji djeluje kao posrednik između gornjeg i donjeg sloja. Najviši sloj poznat je kao sloj jezgre i središnja je točka mreže. Mreže koje su na višoj razini mogu upravljati mrežama na nižoj razini, [10].

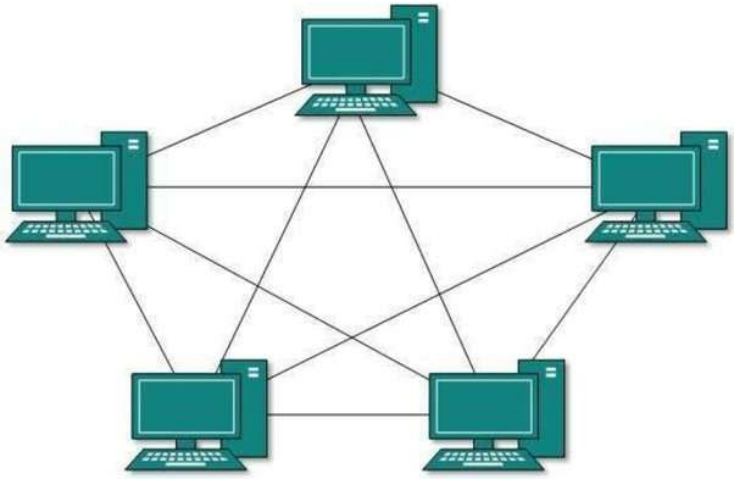
Glavna prednost ove toplogije leži u tome da je jednostavna za održavanje i upravljanje, te je lako otkriti grešku u mreži. Nedostatak topologije stabla je visoka cijena u odnosu na ostale topologije.



Slika 4. Topologija stabla [11]

2.2.1.5 POTPUNO POVEZANA TOPOLIGIJA (MESH)

Mesh topologija je kombinirana topologija prstena i zvijezde. Mesh topologija je oblik u kojem je svaki uređaj izravno povezan s drugim uređajima na mreži. Kao rezultat, u mrežnoj topologiji svaki uređaj može izravno komunicirati s predviđenim uređajem (namjenske veze). Svi uređaji u mreži su međusobno povezano što je prikazano slikom 5. Ako je broj priključene opreme vrlo veliki to će biti vrlo teško kontorlirati u odnosu na samo nekoliko povezanih uređaja.



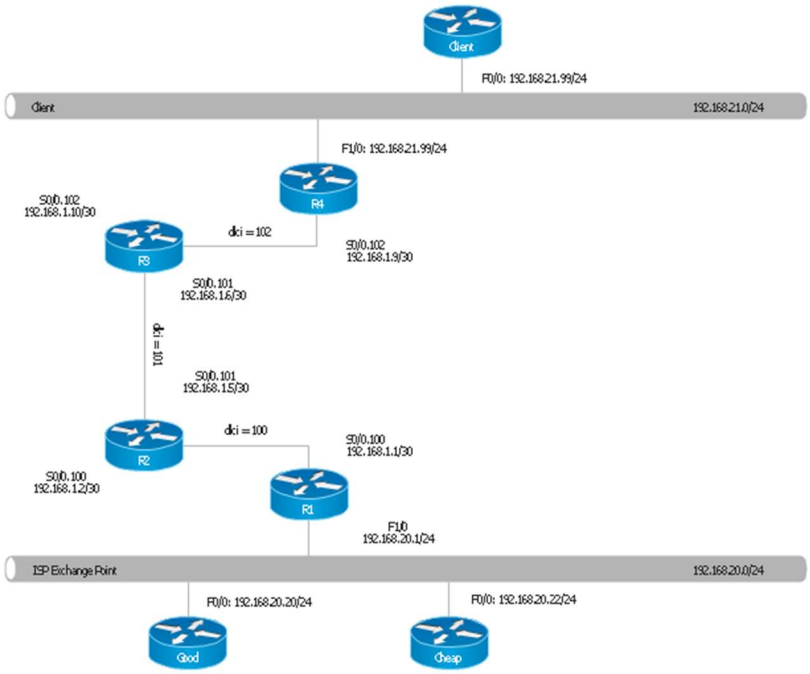
Slika 5. Mesh topologija [12]

2.2.2 LOGIČKA TOPOLOGIJA MREŽE

Logička topologija je način na koji se signali prenose putem mrežnog medija ili kako podaci putuju kroz mrežu s jednog uređaja na drugi, bez obzira na fizičko povezivanje uređaja. Logička topologija mreže nije nužno ista kao i fizička topologija. Na primjer, izvorna Ethernet mreža s upotrebom upletene parice koristi logičku topologiju sabirnice, iako je fizička topologija zvjezdasta, središnje orijentirana. Slično tome, *Token Ring* mreža koristi logičku topologiju prstena, iako je fizički organizirana kao zvjezdasta topologija s MAU (*Medium Access Unit*) kao središnjim čvorom [13].

Logička klasifikacija mrežnih topologija često slijedi slične kategorije kao i fizičke klasifikacije, ali opisuje put kojim podaci putuju između čvorova koji se koriste, za razliku od stvarnih fizičkih veza između tih čvorova. Logičke topologije obično su određene mrežnim protokolima, a ne fizičkim rasporedom kabela, žica i mrežnih uređaja ili protokom električnih ili optičkih signala. Ipak, u mnogim slučajevima, putanje signala između čvorova mogu usko odgovarati logičkom tijeku podataka. Stoga termini 'logička topologija' i 'topologija signala' često se koriste kao sinonimi.

Logičke topologije mogu se dinamički rekonfigurirati pomoću posebne opreme poput usmjerivača i preklopnika. Na slici 6 prikazana je logička topologija mreže.



Slika 6. Logička topologija [14]

3. USMJERAVANJE I PROTOKOLI USMJERAVANJA

3.1 USMJERAVANJE

Usmjeravanje (eng. *Routing*) je postupak odabira puta za slanje podataka računalnom mrežom. Ruta između dva mrežna uređaja može se odrediti na nekoliko načina: mrežni administrator ju može ručno unijeti, može se utvrditi slanjem probnih poruka ili objavljivanjem poznatih ruta. Bez obzira na način na koji je ruta postavljena, otkrivena ili primljena od drugog uređaja, pohranjuje se u tablicu usmjeravanja za kasniju upotrebu.

Da bi se omogućilo umrežavanje različitih računalnih sustava, razvijen je OSI (*Open Systems Interconnection*) model koji ne definira standarde i protokole, već pruža smjernice za njihov razvoj. Unutar ovog modela detaljno su definirani problemi usmjeravanja podataka na različitim razinama hijerarhije, te su predložene preporuke za izgradnju protokola usmjeravanja. Međunarodna standardizacijska organizacija ISO (*International Organization for Standardization*) potvrđuje usklađenost pojedinih protokola s OSI modelom [15].

Dinamičko usmjeravanje koristi protokole usmjeravanja za automatsku razmjenu informacija o usmjeravanju između mrežnih uređaja i dinamičko ažuriranje tablice usmjeravanja. Ovo omogućava efikasnije i prilagodljivije usmjeravanje u većim mrežama s promjenjivim uvjetima mreže. Protokoli dinamičkog usmjeravanja također mogu rukovati neuspjesima mreže preusmjeravanjem prometa duž alternativnih putanja.

Jedan od često korištenih protokola dinamičkog usmjeravanja je OSPF protokol. OSPF je protokol za unutarnje usmjeravanje dizajniran za uporabu unutar jednog autonomnog sustava, poput LAN mreže. Koristi SPF algoritam za izračunavanje najbolje putanje za podatke na temelju troška povezanom s svakom mrežnom vezom.

OSPF dijeli mrežu na područja, pri čemu svako područje ima vlastitu bazu podataka o stanju veze i tablicu usmjeravanja. Ova hijerarhijska struktura omogućava efikasno i skalabilno usmjeravanje u velikim mrežama. Usmjerivači OSPF-a razmjenjuju *Link State Advertisements* (LSA) poruke kako bi ažurirali svoje baze podataka i izračunali najkraći put do svake mreže [16].

OSPF protokol također podržava različite metrike za određivanje troška mrežnih veza, poput propusnosti, kašnjenja i pouzdanosti. Ove metrike se koriste u SPF algoritmu kako bi se odabrao najbolji put na temelju željenih metrika usmjeravanja. OSPF također podržava koncept OSPF područja, što može dodatno poboljšati skalabilnost i smanjiti zagušenje mreže stvaranjem manjih domena usmjeravanja unutar mreže.

Usmjeravanje je temeljni aspekt mrežne komunikacije, a OSPF protokol igra ključnu ulogu u osiguravanju efikasnog i pouzdanog usmjeravanja u LAN mrežama. Razumijevanje strukture i značajki OSPF-a ključno je za mrežne administratore i inženjere kako bi učinkovito dizajnirali i upravljali modernom mrežnom infrastrukturom.

3.2 TABLICE USMJERAVANJA

Tablice usmjeravanja predstavljaju baze podataka smještene na usmjerivačima unutar kojih su pohranjeni podaci o topologiji mreže. Koriste se prilikom prosljeđivanja podatkovnih paketa tako što se adresa odredišta povezuje s mrežnim rutama koje do njega vode. Izgradnja i održavanje ovih tablica osnovni je zadatak protokola usmjeravanja.

Osnovni problem u izgradnji tablica usmjeravanja leži u potrebi za pohranjivanjem ruta prema velikom broju mrežnih odredišta unutar ograničenog memorijskog prostora. Pretpostavka na kojoj se temelji usmjeravanje jest da slične adrese odnose se na uređaje blisko smještene unutar mreže; što su adrese sličnije, to su uređaji bliže međusobno smješteni. Ovo omogućava pohranjivanje rute prema većem broju odredišta jednim zapisom u tablici usmjeravanja. Postoje dva osnovna tipa usmjeravanja: statičko i dinamičko usmjeravanje [17]. Kada usmjerivač ima postavljenu IP adresu i masku podmreže (*Subnet mask*) od strane mrežnog administratora, tada se radi o statičkom usmjeravanju, i tablica usmjeravanja se ne mijenja. Kod dinamičkog usmjeravanja, usmjerivači u mreži izrađuju i održavaju tablicu usmjeravanja.

Zapisi u tablici usmjeravanja moraju sadržavati (slika 7):

- Tip rute (eng. *Interface*).
- Odredišnu mrežu.
- Masku podmreže (eng. *Subnet mask*).
- Slijedeći skok (eng. *Gateway*).
- Metriku.

Network Destination	Netmask	Gateway	Interface	Metric
101.25.67.0	255.255.255.0	10.0.0.2	eth3	1
default	0.0.0.0	10.0.0.1	eth0	0
192.25.67.0	255.255.255.0	10.0.0.3	eth5	10

Slika 7. Tablica usmjeravanja [18]

Osiguravanje dosljednosti tablica i ograničavanje njihove veličine glavni su zadaci protokola usmjeravanja.

3.3 PROTOKOLI USMJERAVANJA

Protokol je skup pravila koji određuje način komunikacije između dva uređaja i definira format podatkovnih paketa poslanih putem komunikacijskih linija. Protokoli usmjeravanja omogućuju usmjerivačima dinamično oglašavanje i učenje dostupnih ruta među pojedinim mrežnim uređajima te odabir najboljih ruta.

Protokol usmjeravanja regulira komunikaciju među usmjerivačima, omogućujući razmjenu informacija koje imaju utjecaj na izbor ruta između bilo koja dva čvora unutar računalne mreže. Algoritmi usmjeravanja determiniraju konkretni izbor rute. Svaki usmjerivač ima znanje samo o mrežama koje su izravno povezane s njim. Protokol usmjeravanja distribuira ove informacije prvo među neposrednim susjedima, a potom kroz cijelu mrežu, omogućujući usmjerivačima stjecanje saznanja o topologiji mreže.

Usmjerivač stječe informacije o udaljenim mrežama od susjednih usmjerivača ili od administratorskih intervencija. Zatim usmjerivač stvara tablicu usmjeravanja. U slučaju izravno povezanih mreža, usmjerivač već zna kako doći do mreže. No, ako mreže nisu povezane, usmjerivač mora naučiti kako pristupiti udaljenoj mreži putem statičkog usmjeravanja (administratorski ručni unos ruta u tablicu usmjeravanja) ili dinamičkog usmjeravanja (automatski proces putem protokola usmjeravanja poput EIGRP, OSPF, itd.).

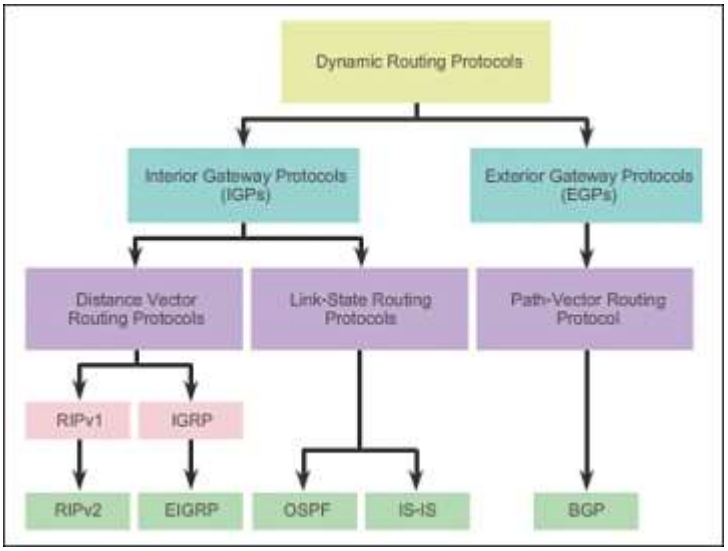
Usmjerivači međusobno ažuriraju podatke o svim mrežama koje poznaju. U slučaju promjene, dinamički usmjerivački protokoli automatski obavještavaju sve usmjerivače o promjenama. U slučaju statičkog usmjeravanja, administrator mora ručno ažurirati sve promjene na svim usmjerivačima, ne koristeći pritom protokole usmjeravanja.

Samo dinamičko usmjeravanje koristi protokole usmjeravanja kako bi usmjerivačima omogućilo izračunavanje ruta, distribuiranje ažuriranja usmjeravanja drugim usmjerivačima te postizanje sporazuma s drugim usmjerivačima o topologiji mreže [19].

Postoje tri vrste protokola za dinamičko usmjeravanje, a razlikuju se po tome kako otkrivaju i izračunavaju rute [19]:

- Vektor udaljenosti (eng. *Distance vector*).
- Stanje veze (eng. *Link state*).
- Vektor putanje (eng. *Path vector*).

Također moguće je klasificirati protokole usmjeravanja u smislu njihove lokacije na mreži. Na primjer, protokoli usmjeravanja mogu postojati unutar ili između autonomnih sustava. Protokoli usmjeravanja mogu se svrstati u različite skupine prema svojim karakteristikama. Konkretno, protokoli za usmjeravanje mogu se klasificirati prema svrsi (*Interior gateway protocol* (IGP) ili *Exterior gateway protocol* (EGP)) i radu (protokol vektora udaljenosti, protokol stanja veze ili protokol vektora putanje). Na slici 8 prikazan je hijerarhijski prikaz protokola usmjeravanja.



Slika 8. Hijerarhijski prikaz protokola usmjeravanja [20]

3.3.1 PROTOKOL VEKTORA UDALJENOSTI

Usporedno usmjeravanje vektora udaljenosti je jedan od najjednostavnijih algoritama za usmjeravanje paketnih mreža te je bio implementiran u čvoru koji provodi protokol usmjeravanja. Ovaj protokol usmjeravanja korišten je u ARPANET-u (*Advanced Research Project Agency Network*) još u ranim 1970-ima te se smatra prvim generacijskim algoritmom za usmjeravanje. Načelo rada ovog protokola temelji se na čestim razmjenama topoloških informacija između susjednih usmjerivača. Dva usmjerivača se smatraju susjedima ako su izravno povezani vezom i mogu se dosegnuti jednim skokom. Skok predstavlja put kojim podatkovni paket prođe između dva susjedna usmjerivača povezana fizičkom vezom [21].

Informacije se redovito razmjenjuju, ažurirajući se prema potrebi. Udaljenost i vektor su ključne informacije pohranjene u tablici usmjeravanja unutar ovog protokola. Udaljenost označava trošak pristizanja do usmjerivača. 'Cijena' može biti broj skokova, efektivna propusnost, zagušenje veze, stvarni trošak korištenja veze ili kombinacija tih ili drugih faktora. Kompanija Cisco Inc. uvela je pojam 'administrativne udaljenosti' temeljene na pouzdanosti korištenog međuprotokola. Administrativna udaljenost pomaže u odabiru između alternativnih ruta na temelju protokola usmjeravanja koji se koristi za put do odredišta. Vektor odnosi se na smjer kojim bi usmjerivač trebao proslijediti paket. Budući da usmjerivač ima niz sučelja, pruža smjernice o sučelju kroz koje paket treba biti proslijeđen.

Svaki usmjerivač započinje stvaranjem tablice usmjeravanja koja sadrži informacije o trošku veze njegovog neposrednog susjeda i sučelju preko kojeg je povezan. Nakon toga, ažurira tablicu informacijama o dostupnosti drugih usmjerivača na temelju informacija dobivenih od susjeda. Usmjerivači ne posjeduju topološke informacije o mreži putem vlastitog otkrivanja cijele mreže, već se moraju oslanjati na informacije koje dobiju iz druge ruke, odnosno od svojih susjeda. Usmjerivač vjeruje informacijama koje mu šalje susjed te manipulira vlastitom tablicom usmjeravanja na temelju toga. Zbog toga se ovaj protokol naziva "usmjeravanje putem glasina".

Budući da usmjeravanje vektora udaljenosti redovito razmjenjuje podatke sa svojim susjedima, prenosi značajnu količinu podataka za usmjeravanje kroz mrežu. No, zbog toga što se informacije razmjenjuju samo između susjeda, protokol zahtijeva značajno vrijeme za širenje informacija kroz mrežu u slučajevima kao što su kvar veze ili uvođenje jeftinijeg puta. Neke od često korištenih protokola usmjeravanja zasnovanih na usmjeravanju vektora udaljenosti su *Routing Information Protocol* (RIP), *Interior Gateway Routing Protocol* (IGRP) i *Enhanced Interior Gateway Routing Protocol* (EIGRP).

Prednosti protokola vektora udaljenosti:

- Lako je implementirati protokol u manjim mrežama.
- Vrlo jednostavno otklanjanje pogrešaka.
- Ograničena redundancija u maloj mreži.

Nedostatci protokola vektora udaljenosti:

- Prekinutu vezu između usmjerivača treba odmah ažurirati za svaki drugi usmjerivač u mreži. Ažuriranje zahtjeva dosta vremena.
- Vrijeme konvergencije u velikoj i složenoj mreži je preveliko.
- Svaka promjena u tablici usmjeravanja povremeno se prenosi na druge susjedne usmjerivače koji stvaraju promet na mreži.

3.3.2 PROTOKOL STANJA VEZE

Protokol usmjeravanja stanja veze, također poznat kao prvi protokol najkraćeg puta ili protokol distribuirane baze podataka. Radi na način da svaki usmjernik zna topologiju mreže i ne šalje se cijela tablica usmjeravanja, nego se svim usmjerivačima u mreži šalje samo informacija o stanju veze u obliku malih LSA (*Link State Advertisment*) paketa. Protokol stanja veze je složeniji. Međutim je pouzdaniji, lakši za upravljanje, troši manje propusnosti, više je skalabilan i može se koristiti za veće mreže. Nekoliko primjera protokola usmjeravanja stanja veze su OSPF i *Intermediate System to Intermediate System* (IS-IS), EIGRP i *Novel NetWare Link State Protocol* (NLSP) [22].

Prednosti protokola stanje veze su:

- Protokoli stanja veze koriste metriku troškova za odabir putanja kroz mrežu. Mjerilo troškova odražava kapacitet veza na tim putanjama.
- Protokoli stanja veze koriste pokrenuta ažuriranja kako bi odmah prijavili promjene u topologiji mreže svim usmjerivačima u mreži. To dovodi do brzih vremena konvergencije.
- Svaki usmjerivač ima potpunu i sinkroniziranu sliku mreže. Stoga je vrlo teško doći do petlji u usmjeravanju.
- Usmjerivači koriste najnovije informacije za donošenje najboljih odluka o usmjeravanju.
- Veličine baze podataka o stanju veze mogu se minimizirati pažljivim projektiranjem mreže. To dovodi do manjih izračuna i brže konvergencije.

Nedostatci:

- Zahtijevanje više memorije i snage procesora u odnosu na protokol vektora udaljenosti. Zbog toga je korištenje skupo.
- Strogi hijerarhijski dizajn mreže, tako da se mreža može podijeliti na manje područja kako bi se smanjila veličina topoloških tablica.
- Potreban administrator koji vrlo dobro razumije protokole

3.3.3 PROTOKOL VEKOTRA PUTANJE

Protokol vektora putanje noviji je koncept u usporedbi s protokolom vektora udaljenosti i protokola stanja veze. Cijela ideja o protokolu vektora putanje često je spojena sa *Border Gateway Protocol* (BGP) [23].

Protokol vektora putanje održava ažurirane informacije o putanji. Ažuriranja koja kruže mrežom i vraćaju se na isti usmjerivač lako se otkrivaju i odbacuju. Kako bi se izbjegao problem brojanja do beskonačnosti ponekad se koristi *Bellman-Ford* algoritam. Svaki unos u tablicu usmjeravanja sadrži odredišnu mrežu, slijedeći usmjerivač i put do odredišta.

Protokol vektora putanje ne prima samo vektor udaljenosti za određeno odredište, umjesto toga usmjerivač zaprima podatke o udaljenosti koji uključuju cijeli put do pojedinog odredišta. Informacije o putanji su tada korisne u otkrivanju petlji. Prednosti protokola vektora putanje su mali troškovi i sprečavanje petlje [24].

4. ZNAČAJKE OSPF PROTOKOLA

Protokol OSPF je široko korišten proaktivni protokol usmjeravanja prema stanju veze koji se koristi za distribuciju informacija o usmjeravanju unutar jednog autonomnog sustava. Budući da je protokol temeljen na stanju veze, usmjerivači razmjenjuju topološke informacije o vezama s susjedima u jednom skoku. Te informacije se šire kroz mrežu kako bi svaki usmjerivač imao potpuni prikaz topologije mreže. Usmjerivači koriste tu kompletnu sliku topologije za izračunavanje najkraćih/najboljih ruta između bilo koja dva usmjerivača, često koristeći Dijkstrin algoritam.

OSPF usmjerivači koriste HELLO poruke za otkrivanje susjednih usmjerivača. Ove poruke se emitiraju u redovitim intervalima prema svakom usmjerivaču i sadrže identifikaciju pošiljatelja te popis svih usmjerivača od kojih je pošiljatelj primio HELLO poruke. Iako ove poruke nisu preplavljene mrežom, šalju se samo jednim skokom od svog izvora. Usmjerivač distribuira informacije o stanju svojih veza slanjem paketa LSA (*Link State Advertisements*) [24].

Podaci koje usmjerivač prima za određivanje topologije mreže pohranjuju se u *Link-State Database* (LSDB). Ova baza podataka predstavlja trenutni pogled usmjerivača na topologiju mreže, sadrži posljednje primljene LSA od svakog jedinstvenog izvora. Uz LSDB, svaki usmjerivač održava popis otkrivenih susjeda s kojima se mogu razmjenjivati informacije o usmjeravanju. Kada usmjerivač primi prvu HELLO poruku od susjeda, saznaje o postojanju tog susjeda. Ukoliko usmjerivač prepozna vlastitu IP adresu unutar te HELLO poruke, provjerava treba li uspostaviti susjedstvo s tim susjedom [25].

Izraz *susjedstvo* opisuje odnos između dva susjedna usmjerivača koji moraju razmjenjivati sve topološke informacije (sadržaj njihovih LSDB-ova). Na kraju, ovi usmjerivači imaju identično razumijevanje mreže. Međutim, neće svi susjedi u jednom skoku formirati susjedstvo. To je zbog smanjenja mrežnog prometa formiranjem što je manjeg broja susjedstava, ali i osiguravanja da svi susjedi završe sa sinkroniziranim LSDB-ovima putem "lančanog povezivanja" susjedstava. Kada dva usmjerivača prepoznaju potrebu za postavljanjem susjedstva, jedan od njih bit će nominiran kao "glavni", a drugi kao "rob". "Glavni" inicira razmjenu podataka slanjem potrebnih informacija putem poruka o opisu baze podataka (DBD). "Rob" šalje DBD poruke kao odgovor na DBD poruke od "glavnog".

Nakon što usmjerivač primi potpuni opis LSDB-a od drugog usmjerivača, uspoređuje taj opis s vlastitim LSDB-om. Za rješavanje neslaganja između dva LSDB-a, kao što su nedostajući unosi, usmjerivač šalje *Link State Request* (LSR) poruke tražeći LSA-ove koji sadrže najnovije dostupne informacije. LSR poruke se potom odgovaraju s *Link State Update* (LSU) porukama koje sadrže tražene LSA. Svaka primljena LSU poruka se potvrđuje s *Link State Acknowledgement* (LSACK) porukom.

4.1 SPF ALGORITAM

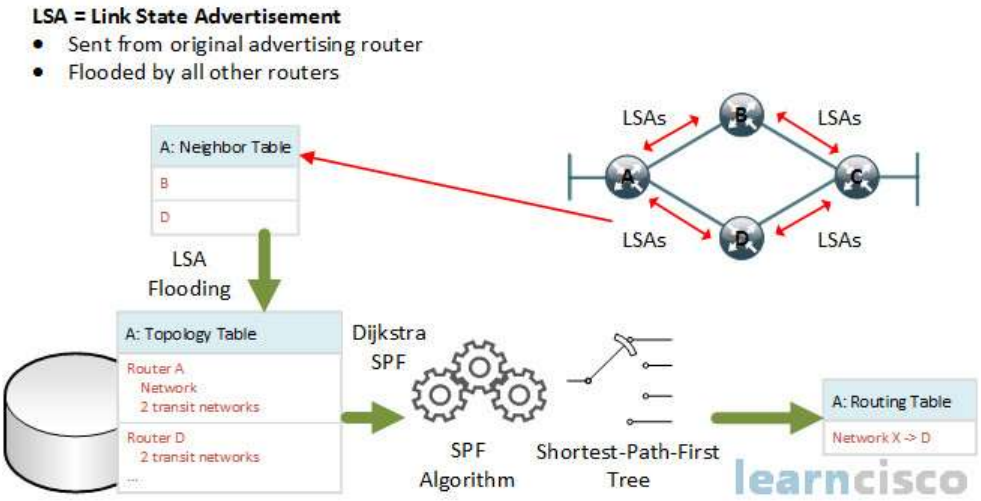
OSPF koristi algoritam najkraćeg puta (SPF), koji se koristi za izračunavanje najkraćeg puta između dva čvora u mreži. Svi usmjerivači u nekom području pokreću ovaj algoritam paralelno, pohranjujući rezultate u svoje pojedinačne topološke baze podataka. Usmjerivači sa sučeljima na više područja pokreću više kopija algoritma. Ovaj odjeljak daje kratak sažetak o tome kako SPF algoritam radi (slika 9).

Kada se usmjerivač pokrene, inicijalizira OSPF i čeka naznake od protokola niže razine da su sučelja usmjerivača funkcionalna. Usmjerivač zatim koristi OSPF pozdravni protokol za pronalaženje susjeda, slanjem *hello* paketa svojim susjedima i primanjem njihovih *hello* paketa [26].

Na *broadcast* ili *non-broadcast* (fizičke mreže koje podržavaju priključivanje više od dva uređaja za usmjeravanje) mrežama, OSPF pozdravni protokol bira određeni usmjerivač za mrežu. Ovaj usmjerivač odgovoran je za slanje oglasa stanja veze (LSA) koji opisuju mrežu, što smanjuje količinu mrežnog prometa i veličinu topoloških baza podataka uređaja za usmjeravanje.

Usmjerivač zatim pokušava formirati susjedstvo s nekim od svojih novostečenih susjeda. Na *broadcast* mrežama samo određeni usmjerivač i rezervni određeni usmjerivač tvore susjedstva s drugim uređajima za usmjeravanje. Susjedstva određuju distribuciju paketa protokola usmjeravanja. Paketi protokola usmjeravanja šalju se i primaju samo u susjedstvima, a ažuriranja topološke baze podataka šalju se samo uz susjedstva. Kada se uspostave susjedstva, parovi susjednih usmjerivača sinkroniziraju svoje topološke baze podataka.

Usmjerivač šalje LSA pakete kako bi oglasio svoje stanje povremeno i kada se stanje promijeni. Ovi paketi uključuju informacije o susjedstvu uređaja za usmjeravanje, što omogućuje otkrivanje neoperativnih uređaja za usmjeravanje.



Slika 9. Način rada SPF algoritma [27]

Koristeći pouzdani algoritam, usmjerivač preplavljuje LSA-ove u cijelom području, što osigurava da svi uređaji za usmjeravanje u području imaju točno istu topološku bazu podataka. Svaki usmjerivač koristi informacije u svojoj topološkoj bazi podataka za izračunavanje najkraćeg puta, sa samim sobom kao korijenom.

Kako bi interni usmjerivači mogli usmjeravati do odredišta izvan područja (usmjeravanje među područjem), granični usmjerivači područja moraju ubaciti dodatne informacije o usmjeravanju u područje. Budući da su granični usmjerivači područja povezani s okosnicom, oni imaju pristup potpunim topološkim podacima o okosnici. Područni granični usmjerivači koriste ove informacije za izračunavanje staza do svih odredišta izvan svog područja i zatim reklamiraju te putove unutarnjim usmjerivačima područja.

Granični usmjerivači autonomnog sustava (AS) preplavljuju informacije o vanjskim autonomnim sustavima u cijelom AS-u, osim u nedostupnim područjima. Granični usmjerivači područja odgovorni su za oglašavanje staza do svih graničnih usmjerivača AS-a.

4.2 OSPF PAKETI

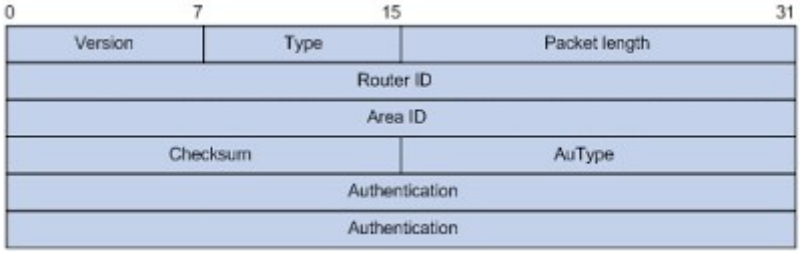
Postoji pet različitih vrsta OSPF paketa. A to su: HELLO paket, *Database Description* paket, *Link state request* paket, *Link state update* paket i *Link state acknowledgment* paket. Sve vrste OSPF paketa započinju standardnim zaglavljem od 24 bajta.

4.2.1 OSPF ZAGLAVLJE PAKETA

Svi OSPFv2 paketi imaju zajedničko zaglavlje od 24 bajta, a OSPFv3 paketi imaju zajedničko zaglavlje od 16 bajta koje sadrži sve informacije potrebne za određivanje treba li OSPF prihvatiti paket.

Zaglavlje se sastoji od sljedećih polja (slika 10):

- Broj verzije—trenutni broj verzije OSPF-a. Ovo može biti 2 ili 3.
- Tip – tip OSPF paketa.
- Duljina paketa—duljina paketa, u bajtovima, uključujući zaglavlje.
- ID usmjerivača—IP adresa usmjerivača s kojeg je paket potekao.
- Area ID—Identifikator područja u kojem paket putuje. Svaki OSPF paket povezan je s jednim područjem. Paketi koji putuju preko virtualne veze označeni su ID-om područja okosnice, 0.0.0.0.
- Kontrolni zbroj—Fletcher kontrolni zbroj.
- Autentikacija — (samo OSPFv2) Shema provjere autentičnosti i informacije o provjeri autentičnosti.
- ID instance — (samo OSPFv3) Identifikator koji se koristi kada postoji više područja OSPFv3 konfiguriranih na vezi.



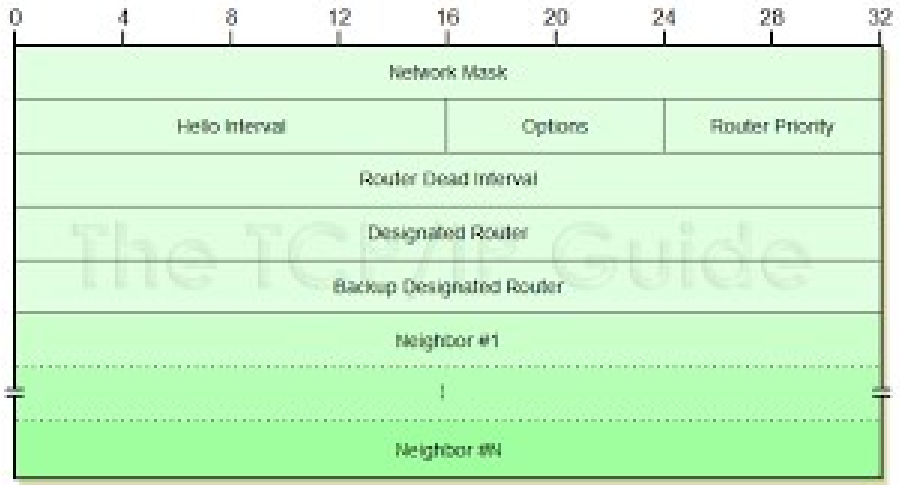
Slika 10. Zaglavlje OSPF paketa [28]

4.2.2 HELLO PAKET

Usmjerivači povremeno šalju Hello pakete na svim sučeljima, uključujući virtualne veze, kako bi uspostavili i održavali odnose susjeda. Hello paketi su multicast na fizičkim mrežama koje imaju mogućnost multicasta ili broadcasta, što omogućuje dinamičko otkrivanje susjednih usmjerivača [29].

Hello paketi se sastoje od OSPF zaglavlja i sljedećih polja (slika 11):

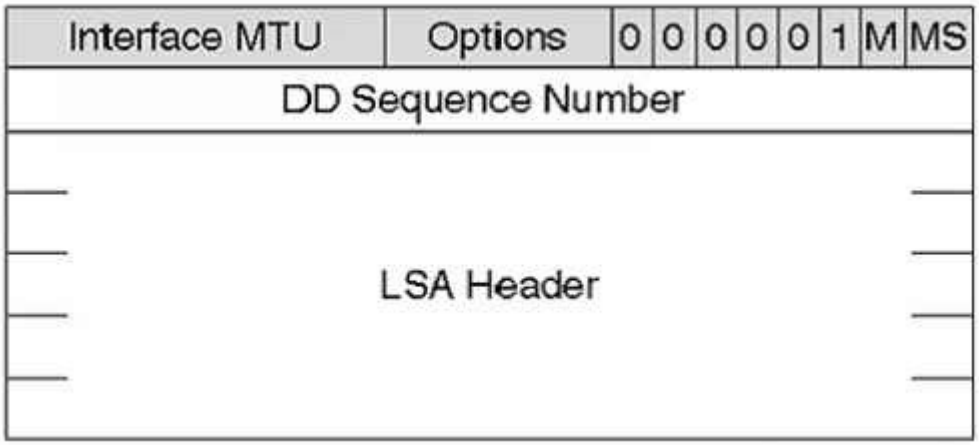
- Mrežne maske—(samo OSPFv2).
- Hello intervala—vrijeme između slanja uzastopnih Hello poruka.
- Opcija—neobavezne mogućnosti usmjerivača.
- Prioriteta usmjerivača—Prioritet usmjerivača da postane *designated router* (DR).
- Dead intervala—vremenski interval nakon kojeg usmjerivač smarta da je susjedni usmjerivač nedostupak ako nije primio Hello poruku od njega.
- Designated usmjerivača—IP adresa DR-a.
- Backup designated usmjerivača – IP adresa DBR-a.



Slika 11. Hello paket [30]

4.2.3 DATABASE DESCRIPTION PAKETI

Prilikom inicijalizacije susjedstva, OSPF razmjenjuje *database description* pakete podataka, koji opisuju sadržaj topološke baze podataka. Ovi se paketi sastoje od OSPF zaglavlja, sekvencijskog broja paketa i LSA zaglavlja što je prikazano slikom 12.

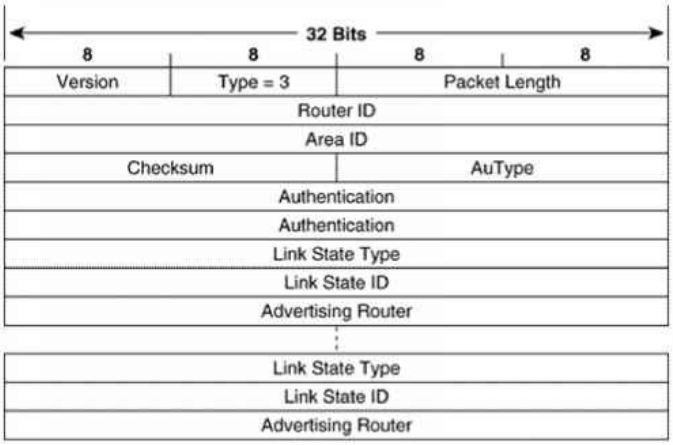


Slika 12. Database description paketi [31]

4.2.4 LINK STATE REQUEST PAKETI

Koristi se za izvlačenje informacija. Kada usmjerivač otkrije da su dijelovi njegove topološke baze podataka zastarjeli on susjedu šalje *link state request* paket tražeći preciznu instancu baze podataka. *Link state request* paket sadrži sljedeća polja koja se ponavljaju za svaki jedinstveni unos (slika 13):

- Link state tipa – identificira vrstu stanja kao što je usmjerivač ili mreža.
- Link state ID – diktira tip stanja.
- Advertising router – adresa usmjerivača koji je generirao LSA.



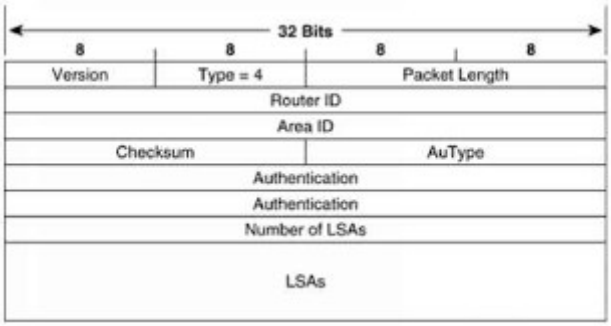
Slika 13. Link state request paketi [32]

4.2.5 LINK STATE UPDATE PAKETI

Kada usmjerivač primi LSA paket id susjednog usmjerivača, ažurira svoju lokalnu LSDB s informacijama koju su navedene u tom paketu. Onda na temelju tih promjena u LSDB-u, usmjerivač generira *link state update* paket

Paketi ažuriranja stanja veze sastoje se od OSPF zaglavlja i sljedećih polja (slika 14):

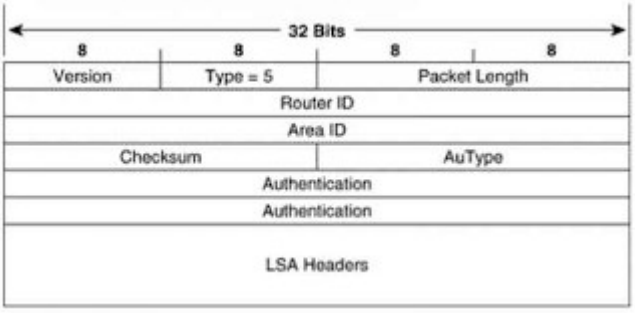
- LSA zaglavlje – sadrži informacije o samom LSA koji se šalje, uključujući tip, duljinu i verziju LSA.
- LSA – glavni dio LSU paketa je sam LSA, koji sadrži informacije o stanju veza ili topološke informacije o mreži.



Slika 14. Link state update paketi [32]

4.2.6 LINK STATE ACKNOWLEDGMENT PAKETI

Usmjerivač šalje *Link state acknowledgment* kao odgovor na *link state update* pakete kako bi potvrdio da su *link state update* paketi uspješno primljeni. Jedan paket potvrde može uključivati odgovore na više paketa ažuriranja. LSA paketi sastoje se od OSPF zaglavlja i LSA zaglavlja što je prikazano slikom 15.



Slika 15. Link state acknowledgment paketi [33]

4.3 POUZDANOST OSPF PROTOKOLA

OSPF protokol poznat je po svojoj pouzdanosti u komunikaciji u mreži. Osigurava učinkovito i tolerantan na greške u usmjeravanju, što ga čini popularnim izborom za LAN mreže. Jedna od ključnih značajki koja doprinosi pouzdanosti OSPF-a je korištenje SPF algoritma.

Još jedan faktor koji poboljšava pouzdanost OSPF-a je njegova hijerarhijska struktura. OSPF mreže su podijeljene na područja, pri čemu svako područje ima svoju tablicu usmjeravanja. Ovaj hijerarhijski dizajn omogućuje učinkovito usmjeravanje i smanjuje utjecaj kvarova mreže. Ako usmjerivač unutar područja zakaže, OSPF brzo može preusmjeriti promet kroz alternativni put unutar istog područja, minimizirajući vrijeme nedostupnosti i osiguravajući pouzdanu povezanost. Osim toga, OSPF podržava koncept redundantnih veza i usmjerivača. Redundancija pruža rezervne putanje u slučaju kvarova veza ili usmjerivača, povećavajući ukupnu pouzdanost mreže. OSPF može brzo otkriti i prilagoditi se promjenama u topologiji mreže, automatski preusmjeravajući promet kroz dostupne putanje [34].

OSPF koristi pouzdan mehanizam poplave (engl. *flood*) za distribuciju informacija. Kada dođe do promjene u mreži, poput dodavanja ili uklanjanja novog usmjerivača OSPF usmjerivači poplavljuju ažurirane informacije kako bi osigurali da svi usmjerivači imaju najsvježije tablice usmjeravanja. Taj mehanizam poplave garantira da usmjerivači imaju točne informacije o topologiji mreže, dodatno poboljšavajući pouzdanost.

Pouzdanost OSPF-a proizlazi iz korištenja SPF algoritma, hijerarhijske strukture, podrške za redundanciju i pouzdanog mehanizma poplave. Ove značajke omogućuju OSPF-u da pruži toleranciju na greške u usmjeravanju u LAN mrežama, osiguravajući pouzdanu komunikaciju između uređaja.

4.4 OSPF METRIKA

OSPF metrika se naziva trošak. To je vrijednost dodijeljena svakoj vezi u mreži na temelju propusnosti veze. Što je niži trošak, to je ruta poželjnija. Trošak je obrnuto proporcionalan propusnosti, što znači da veze s većom propusnošću imaju niže troškove.

Formula koja se koristi za izračun troška je [35]:

$$Trošak = \frac{Referentna\ propusnost}{Propusnost\ sučelja} \quad (1)$$

Referentna propusnost je unaprijed definirana vrijednost koja je obično postavljena na 100 Mb/s [35]. Propusnost sučelja je stvarna propusnost veze. Primjerice, ako je propusnost sučelja 10 Mb/s, trošak bi bio $\frac{100\ Mb/s}{10\ Mb/s}$ = 10.

OSPF metrika također može uzeti u obzir druge čimbenike poput kašnjenja, pouzdanosti i opterećenja. Ovi faktori mogu biti konfigurirani od strane mrežnog

administratora kako bi utjecali na OSPF usmjeravanje. OSPF metrika je ključna u određivanju odabira putanje u OSPF mrežama. Pomaže osigurati da se promet usmjerava učinkovito i pouzdano kroz mrežu. Koristeći SPF algoritam, OSPF izračunava najbolju rutu na temelju metrike i gradi tablice usmjeravanja u skladu s time. OSPF metrika igra značajnu ulogu u OSPF protokolu omogućavajući inteligentne i dinamične odluke o usmjeravanju u LAN mrežama.

4.5 OSPF AUTENTIFIKACIJA

Osim različitih značajki, OSPF također pruža mehanizme autentifikacije radi osiguranja sigurnosti i integriteta informacija o usmjeravanju. OSPF autentifikacija omogućava usmjerivačima provjeru identiteta OSPF paketa te sprječava neovlaštene usmjerivače da sudjeluju u OSPF procesu usmjeravanja. OSPF podržava dva tipa autentifikacije: autentifikacija u običnom tekstu i *digest* autentifikaciju.

Autentifikacija u običnom tekstu uključuje korištenje lozinke ili ključa konfiguriranog na svakom usmjerivaču. Prilikom razmjene OSPF paketa između usmjerivača, lozinka ili ključ uključuju se u zaglavlje paketa. Usmjerivač koji prima paket uspoređuje primljenu lozinku/ključ s konfiguriranom lozinkom/ključem kako bi autentificirao paket. Autentifikacija u običnom tekstu relativno je jednostavna za konfiguriranje, ali pruža slabu sigurnost jer se lozinke/ključevi prenose kao običan tekst [36].

Digest autentifikacija s druge strane pruža veću sigurnost koristeći kriptografsku funkciju sažetka. Svaki OSPF paket uključuje kriptografsku kontrolnu sumu, također poznatu kao *digest* poruka, koja se izračunava na temelju sadržaja paketa i tajnog ključa. Usmjerivač koji prima paket tada može provjeriti integritet paketa ponovnim izračunavanjem *digest* poruke koristeći isti ključ i usporedbom s primljenim *digest* porukama. Autentifikacija putem digesta sigurnija je od autentifikacije u običnom tekstu jer ne prenosi tajni ključ kao običan tekst [35].

Da bi se omogućila autentifikacija u OSPF-u, usmjerivači moraju biti konfigurirani s istim tipom autentifikacije, lozinkom/ključem i područjem u kojem je autentifikacija omogućena. Autentifikacija se može omogućiti na razini sučelja ili na razini područja. Kada je autentifikacija omogućena na razini sučelja, svi OSPF paketi razmijenjeni kroz to sučelje bit će autentificirani. Kada je autentifikacija omogućena na razini područja, svi OSPF paketi razmijenjeni unutar određenog područja bit će autentificirani.

Implementiranjem autentifikacije u OSPF-u, mrežni administratori mogu spriječiti neovlaštene usmjerivače da sudjeluju u procesu usmjeravanja OSPF-a i osigurati da su informacije o usmjeravanju sigurne i pouzdane.

5. OSPF PODRUČJA

OSPF koristi hijerarhijsku strukturu za učinkovito usmjeravanje unutar mreže. Ova hijerarhija se sastoji od OSPF područja. OSPF područje je skup usmjerivača koji imaju iste topološke informacije i dijele informacije o usmjeravanju međusobno. Svako područje ima vlastitu internu tablicu usmjeravanja i pokreće vlastitu instancu OSPF protokola. To omogućuje učinkovito usmjeravanja unutar područja bez opterećenja cijele mreže.

Kada je AS podijeljen na više područja, područja su međusobno povezana usmjerivačem koji je označen kao *area border router* (ABR). ABR ima različita OSPF sučelja koja su povezana s različitim OSPF područjima tako da može raditi u više od jednog područja. ABR čuva kopiju baze podataka o stanju veze za svako povezano područje.

Svi usmjerivači u području imaju identične kopije baze podataka topologije autonomnog sustava. Svaki usmjerivač izračunava vlastitu tablicu usmjeravanja koristeći Dijkstra algoritam, koji prvo izračunava najkraći put [37].

OSPF podržava *multipath*, što znači da podržava više ruta do istog odredišta. Kada se primi novi paket ažuriranja stanja veze, ponovno se računa cijelo „stablo“. Ostala razmatranja za *multipath* izračun uključuju sljedeće:

- *Tree routing* zadržava sve *multipath* rute jednake cijene.
- *Tree routing* odabire samo najkraći put za zadržavanje kada postoji više ruta do istog odredišta.
- Oba troška se zbrajaju kada dvije rute, koje imaju iste troškove, idu na isto odredište.
- OSPF uvijek dodaje rutu s najnižom cijenom u TCP/IP.
- *Multipath* rute do istog odredišta dodaju se u TCP/IP tablicu usmjeravanja kada te putanje imaju istu cijenu.

Svaki usmjerivač u OSPF području pokreće *link-state advertisement* (LSA), što je osnovno sredstvo OSPF komunikacije, kako bi prenio topologiju jednog usmjerivača svim ostalim usmjerivačima u istom OSPF području. Svaki oglas o stanju veze koji se stvori, u svakom usmjerivaču, pohranjen je u njegovoj bazi o stanju veza. Baza podataka je usklađena među usmjerivačima tako da svaki usmjerivač u OSPF području ima identičnu kopiju baze podataka o stanju veza.

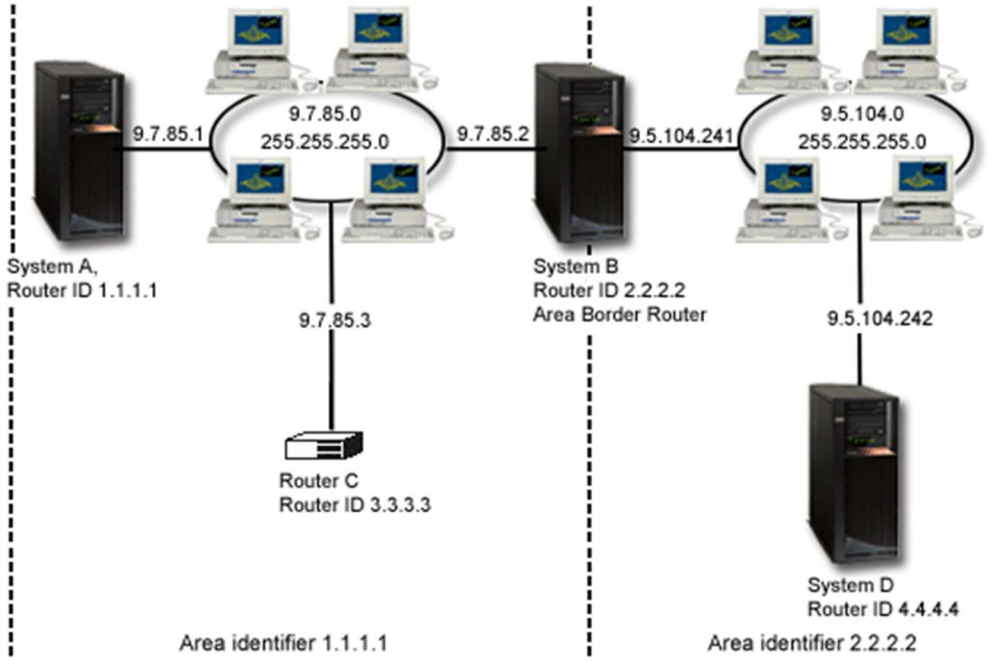
ABR koristi poseban sažeti LSA za oglašavanje svim drugim odredištima koja su poznata ABR-u, ali se nalaze izvan područja.

Područje određeno kao *backbone* područje je preduvjet u OSPF AS-u. Sva područja moraju biti povezana s *backbone* područjem jer je odgovorno za pružanje informacija o usmjeravanju između svih područja u AS-u.

Područja se identificiraju ID-om duljine četiri okteta. *Backbone* područje uvijek je dodijeljeno rezerviranom ID-u 0.0.0.0. Sva ostala područja u AS-u moraju imati jedinstveni

identifikator. Po definiciji OSPF područje je skup mreža, a ne skup usmjerivača. Segment okosnice mreže je IP podmreža koja pripada području identificiranom s 0.0.0.0. Područja koja nisu fizički povezana s *backbone* područjem logički su povezana pomoću OSPF virtualne veze.

OSPF je računalno intenzivan pa je uobičajeno popunjavati samo područja koja nisu *backbone* područja aplikacijskim poslužiteljima. Topologija jednog područja je skrivena od ostalih područja AS-a kako bi se smanjilo opterećenje usmjeravanja.



Slika 16. OSPF područja [38]

Na slici 16 *backbone* se nalazi na IP adresi 9.7.85.0. Tri *non-backbone* područja su područje 1.1.1.1, područje 2.2.2.2 i područje 3.3.3.3, pri čemu je područje 3.3.3.3 povezano s *backbone* područjem putem virtualne veze.

5.1 BACKBONE PODRUČJE

Backbone područje je centralno područje u OSPF domeni usmjeravanja koje povezuje sva druga područja. Označava se kao područje 0 i djeluje kao srce OSPF mreže. Sva ostala područja u mreži moraju biti povezana s *backbone* područjem. *Backbone* područje odgovorno je za razmjenu rutinskih informacija s drugim područjima i širenje tih informacija kroz cijelu mrežu. Osigurava da svi usmjerivači u različitim područjima imaju isti pogled na topologiju mreže [39].

Backbone područje ima ključnu ulogu u dizajnu OSPF mreže i pruža skalabilnost i fleksibilnost. Omogućuje stvaranje više područja, svako s vlastitim setom usmjerivača i mreža, dok se i dalje održava povezanost s ostatkom OSPF mreže. Korištenjem hijerarhijskog dizajna, OSPF može smanjiti veličinu tablica usmjerivanja i poboljšati učinkovitost mreže. *Backbone*

područje djeluje kao centralni čvor koji povezuje sva područja i olakšava učinkovito usmjeravanje unutar mreže.

Sveukupno, *backbone* područje u OSPF-u je ključna komponenta koja omogućuje učinkovito usmjerivanje i povezivanje u mrežama velikih razmjera. Pravilan dizajn i konfiguracija su ključni za ukupnu učinkovitost i stabilnost OSPF rutirajućeg protokola.

Usmjerivači koji čine *backbone* područje moraju biti fizički povezani. Ako nisu, potrebno je konfigurirati virtualne veze kako bi stvorili dojam povezivanja *backbone*-a. Moramo stvoriti virtualne veze između bilo koja dva ABR-a koji imaju sučelje sa *non-backbone* područjem. OSPF tretira dva uređaja za usmjeravanje spojena virtualnom vezom kao da su povezani na nenumeriranu *point-to-point* mrežu.

5.2 STUBY PODRUČJE

U OSPF-u, područje je logičko grupiranje usmjerivača koji dijele iste informacije o usmjeravanju. *Stuby* područje je posebna vrsta OSPF područja koja se koristi kada usmjerivač unutar područja ima samo jedno povezivanje s ostatkom OSPF mreže.

U *stuby* području, usmjerivač koji je povezan s ostatkom OSPF mreže poznat je kao ABR (*Area Border Router*). ABR je odgovoran za sažimanje ruta iz *stuby* područja i oglašavanje istih ostatku OSPF mreže. Također, ABR djeluje kao tranzitna točka za promet koji treba putovati između *stuby* područja i drugih OSPF područja [40].

Jedna važna karakteristika *stuby* područja je ta da ne prima vanjske rute iz drugih OSPF područja. To znači da usmjerivači unutar *stuby* područja imaju samo saznanje o rutama unutar vlastitog područja i zadanom rutom koju oglašava ABR. Ovo može biti korisno u scenarijima gdje usmjerivaču u *stuby* području nije potrebno poznavati punu tablicu usmjeravanja OSPF mreže [40].

Korištenje *stuby* područja može pomoći u smanjenju količine rutinskih informacija koje moraju biti obrađene i pohranjene od strane usmjerivača u OSPF mreži. To može dovesti do poboljšane skalabilnosti i efikasnosti u velikim mrežama.

Stuby područje je specijalizirana vrsta OSPF područja koja se koristi kada usmjerivač unutar područja ima samo jednu vezu s ostatkom OSPF mreže. Omogućuje učinkovito usmjeravanje i smanjuje količinu informacija koje moraju biti obrađene od strane usmjerivača u mreži.

5.3 POTPUNO STUBBY PODRUČJE

Potpuno *stubby* područje je vrsta OSPF područja koja ograničava oglašavanje vanjskih ruta. U potpunom *stubby* području, samo zadane rute se oglašavaju iz područja ostatku OSPF mreže. To znači da su sve vanjske rute, uključujući one naučene iz drugih autonomnih sustava, sažete u jednu zadanu rutu prije nego što se oglašavaju. Svrha stvaranja potpuno *stubby*

područja je smanjiti veličinu tablice usmjeravanja i kontrolirati tok prometa unutar OSPF mreže [41].

Potpuno *stubby* područja se obično koriste u većim OSPF mrežama gdje postoji potreba za smanjenjem količine informacija koje se razmjenjuju i obrađuju. Ova područja se često implementiraju na rubu ili granici OSPF mreže, gdje se vanjske rute primaju iz drugih autonomnih sustava ili s interneta.

Važno je napomenuti da u potpuno *stubby* području, samo se zadane rute oglašavaju iz područja, ali samo područje i dalje može primati i širiti unutarnje OSPF rute unutar OSPF mreže.

5.4 NOT SO STUBBY PODRUČJE (NSSA)

NSSA je OSPF područje koje omogućuje uvoz vanjskih ruta (rute iz drugih područja usmjerivanja ili autonomnih sustava) u OSPF područje koje nije *backbone* područje ili standardno područje.

Svrha NSSA-e je pružiti mehanizam za povezivanje područja s vanjskim rutama bez potrebe da se cijela OSPF mreža pretvori u autonomni sustav. NSSA područja omogućuju širenje vanjskih ruta unutar OSPF mreže dok se istovremeno održava stabilnost i skalabilnost OSPF protokola.

Unutar NSSA-e nalazi se ABR koji djeluje kao granica između NSSA-e i ostatka OSPF mreže. ABR oglašava zadanu rutu za NSSA-u, što omogućuje NSSA-i pristup vanjskim mrežama. Zatim NSSA generira tip 7 LSA za vanjsku rutu, koju zatim ABR pretvara u tip 5 LSA i distribuira ostatku OSPF mreže [42].

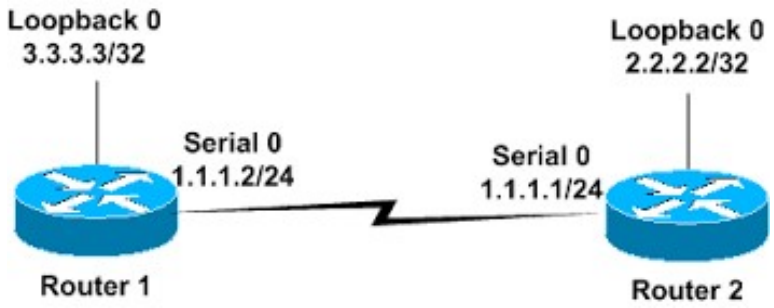
Korištenjem NSSA-e, administratori mreže mogu kontrolirati uvoz vanjskih ruta u OSPF mrežu, što omogućuje veću fleksibilnost i učinkovitost usmjeravanja.

6. OSPF VRSTE MREŽA

OSPF se koristi u *point-to-point, broadcast*, i *non-broadcast* mrežama.

6.1 POINT TO POINT MREŽA

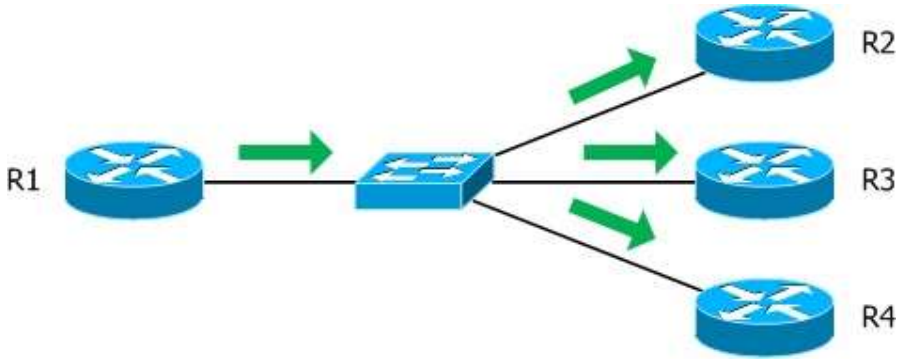
Ovo je daleko najjednostavnija vrsta mreže. *Point to point* mreža je veza između točno dvije točke (ili usmjerivača). Slika 17 prikazuje *point to point* mrežu. Paket poslan s jednog od usmjerivača uvijek će imati točno jednog primatelja na lokalnoj vezi.



Slika 17. Point to point mreža [43]

6.2 BRODACAST MREŽA

Puno učinkovitiji način povezivanja velikog broja uređaja je implementacija *broadcast* mreže koja može povezivati više krajnjih uređaja. Ethernet je primjer takve mreže.



Slika 18. Broadcast mreža [44]

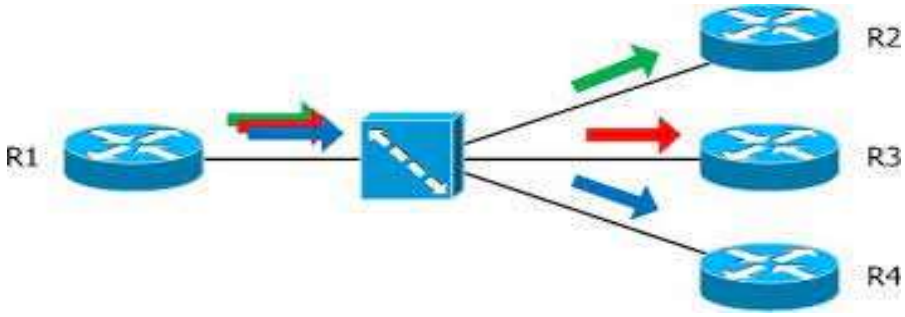
Ethernet mreže podržavaju *broadcast*, jedan paket koji prosljeđuje uređaj može se umnožiti tako da svaka druga krajnja točka dobije kopiju. Ovo je korisno u uštedi propusnosti i u olakšavanju automatskog otkrivanja susjeda.

U primjeru prikazanom na slici 18 usmjerivač R1 može emitirati samo određenim primateljima OSPF Hello poruke, znajući da će je svi drugi OSPF usmjerivači primiti i odgovoriti

svojom multicast porukom. Posljedično, susjedi se mogu brzo identificirati i formirati susjedstva bez prethodnog poznavanja adresa.

6.3 NON-BROADCAST MREŽA

Nažalost, ne podržavaju sve tehnologije *broadcast* prijenose. Frame relay i ATM (*Asynchronous tranfser mode*) su vjerojatno najčešći primjeri prijenosa bez emitiranja koji zahtijevaju individualne PVC-ove (*Permanent Virtual Circuits*) koji se konfiguriraju između krajnjih točaka.



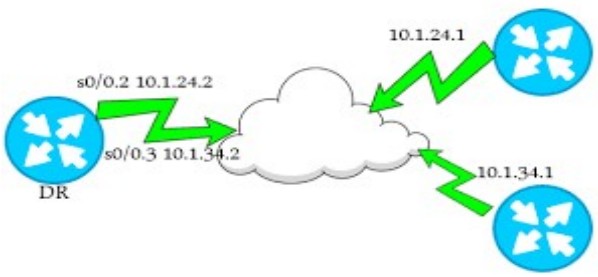
Slika 19. Non broadcast mreža [44]

U topologiji prikazanoj na slici 19 usmjerivač R1 mora izraditi i poslati pojedinačni paket za svako odredište do kojeg želi doći. Osim što je neučinkovito u pogledu širine pojasa, ovo ograničenje zahtijeva od usmjerivača da zna adrese svojih susjeda prije komunikacije s njima.

OSPF može raditi u jednom od dva načina preko *non-broadcast* mreže: *non-broadcast multiple acces* (NBMA) ili *point to multipoint*. Svaka od ovih topologija rješava nedostatak mogućnosti emitiranja iz drugog smjera.

6.4 NON BROADCAST MULTI ACCESS (NBMA)

NBMA segment oponaša funkciju mreže emitiranja. Svaki usmjerivač u segmentu mora biti konfiguriran s IP adresom svakog od svojih susjeda. OSPF hello paketi se zatim pojedinačno prenose kao unicast paketi svakom susjedu. Slika 20 prikazuje NBMA mrežu.

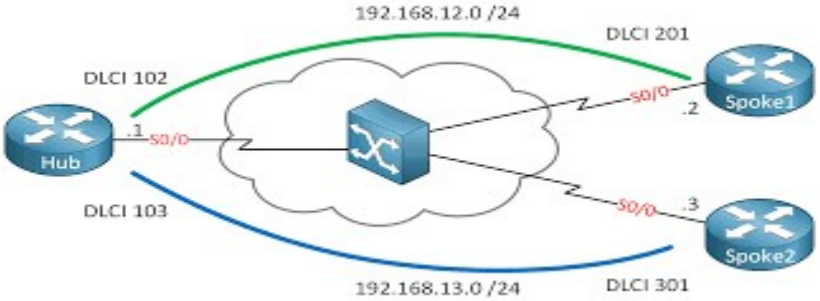


Slika 20. NBMA mreža [45]

6.5 POINT TO MULTIPOINT

Konfiguracija *point to multipoint* pristupa ograničenju *non-broadcast* mreže na drugačiji način. Umjesto da pokušava oponašati mogućnost emitiranja, nastoji organizirati PVC-ove u *point to point* mreži. Hello paketi se i dalje moraju replicirati i slati pojedinačno svakom susjedu, ali pristup s više točaka nudi dvije različite prednosti: nije potreban DR (*designated router*) / BDR (*backup designated router*), a emulirane *point to point* veze mogu zauzeti zajedničku podmrežu.

Svi usmjerivači priključeni na *non-broadcast* mrežu moraju biti ručno konfigurirani kako bi bili prepoznati kao *point to multipoint*. Na slici 21 prikazana je *point to multipoint* mreža.



Slika 21. Point to multipoint mreža [46]

7. ZAKLJUČAK

Protokoli usmjeravanja se prvenstveno dijele na područje rada, odnosno djeluju li unutar jednog autonomnog sustava ili služe za povezivanje više autonomnih sustava. Protokoli koji rade unutar jednog autonomnog sustava dijele se na protokole temeljene na algoritmu vektora udaljenosti, protokole na temelju algoritma stanja veze i protokole vektora putanje ovisno o načinu određivanja najboljeg puta.

OSPF je usmjerivački protokol koji koristi otvoreni standard, što znači da su njegove specifikacije javne. Definiran je RFC-om 2328 (OSPFv2) te koristi Dijkstra SPF algoritam za pronalaženje najkraćeg puta. OSPF je protokol stanja veze koji zahtjeva slanje obavijesti o stanju veze ostalim usmjerivačima unutar istog hijerarhijskog prostora.

U odnosu na ostale protokole, OSPF je otvoreni protokol i može se implementirati na opremu bilo kojeg proizvođača. OSPF ima veliku pouzdanost isporuke paketa, ali i sporu konvergenciju prilikom unosa novog najboljeg puta u tablicu usmjeravanja. Koristi se u velikim mrežama s puno različite opreme bez česte promjene topologije, primjer toga su jezgrene mreže pružatelja Internet usluge.

Pouzdanost OSPF-a proizlazi iz korištenja SPF algoritma, hijerarhijske strukture, podrške za redundanciju i pouzdanog mehanizma poplave. Ove značajke omogućuju OSPF-u da pruži toleranciju na greške u usmjeravanju u LAN mrežama, osiguravajući pouzdanu komunikaciju između uređaja. Implementacijom autentifikacije u OSPF-u možemo osigurati da su informacije o usmjeravanju sigurne i pouzdane.

LITERATURA

[1] Eyewated. Preuzeto sa: https://hr.eyewated.com/sto-je-lan/ (pristupljeno: srpanj 2022)

[2] Basu. Preuzeto sa: https://www.basu.org.in/wp-content/uploads/2020/03/LAN-WAN.pdf (pristupljeno: srpanj 2022)

[3] Techtarget. Preuzeto sa: https://www.techtarget.com/searchnetworking/definition/network-topology (pristupljeno: srpanj 2022)

[4] Techopedia. Preuzeto sa: https://www.techopedia.com/definition/4794/physical-topology (pristupljeno: srpanj 2022)

[5] Computerhope. Preuzeto sa: https://www.computerhope.com/jargon/s/startopo.htm (pristupljeno: kolovoz 2022)

[6] Javatpoint. Preuzeto sa: https://www.javatpoint.com/computer-network-topologies (pristupljeno: kolovoz 2022)

[7] Utechworld. Preuzeto sa: https://utechnoworld.com/what-is-bus-topology-in-network-topology/ (pristupljeno: kolovoz 2022)

[8] Sunbirddcim. Preuzeto sa: https://www.sunbirddcim.com/glossary/ring-topology (pristupljeno: kolovoz 2022)

[9] Creately. Preuzeto sa: https://creately.com/diagram/example/Noe2M9jJsLM/ring-topology (pristupljeno: kolovoz 2022)

[10] Geeksforgeeks. Preuzeto sa: https://www.geeksforgeeks.org/advantages-and-disadvantages-of-tree-topology/ (pristupljeno: kolovoz 2022)

[11] Free time learning. Preuzeto sa: https://www.freetimelearning.com/software-interview-questions-and-answers.php?What-is-Tree-Topology?&id=5749 (pristupljeno: kolovoz 2022)

[12] Quora. Preuzeto sa: https://www.quora.com/What-is-a-mesh-topology (pristupljeno: kolovoz 2022)

[13] Techopedia. Preuzeto sa: https://www.techopedia.com/definition/25890/logical-topology (pristupljeno: kolovoz 2022)

[14] Concept draw. Preuzeto sa: https://www.conceptdraw.com/examples/give-example-of-logical-topology (pristupljeno: kolovoz 2022)

[15] Imperva. Preuzeto sa: https://www.imperva.com/learn/application-security/osi-model/ (pristupljeno: rujan 2023)

[16] Science direct. Preuzeto sa: https://www.sciencedirect.com/topics/computer-science/interior-gateway-protocol (pristupljeno: studeni 2023)

[17] Cisco Networking Academy: „Routing Protocols and Concepts“ (pristupljeno: kolovoz 2022)

[18] Baeldung. Preuzeto sa: https://www.baeldung.com/cs/routing-table-entry (pristupljeno: kolovoz 2022)

[19] Cnna blog. Preuzeto sa: https://www.ccnablog.com/dynamic-routing-protocols/ (pristupljeno: kolovoz 2022)

[20] Cisco press. Preuzeto sa: https://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=7 (pristupljeno: kolovoz 2022)

[21] PC mag. Preuzeto sa: https://www.pcmag.com/encyclopedia/term/distance-vector-protocol (pristupljeno: kolovoz 2022)

[22] Medhi D., Ramasamy K. : Network Routing Algorithms, Protocols, and Architectures Second Edition (pristupljeno: kolovoz 2022)

[23] Packet coders. Preuzeto sa: https://www.packetcoders.io/routing-protocols-compared-distance-vector-path-vector-link-state-and-hybrid/ (pristupljeno: kolovoz 2022)

[24] Misra S., Goswami S. : Network Routing Fundamentals, Applications, and Emerging Technologies (pristupljeno: kolovoz 2022)

[25] Firewall.cx. Preuzeto sa: https://www.firewall.cx/networking/routing-protocols/ospf-adjacency-neighbor-forming-process-hello-packets-lsr-lsu.html (pristupljeno: rujan 2023)

[26] Network encylopedia. Preuzeto sa: https://networkencyclopedia.com/shortest-path-first-spf/ (pristupljeno: kolovoz 2022)

[27] Learn cisco. Preuzeto sa: https://www.learncisco.net/courses/icnd-2/an-overview-of-ospf/ospf-data-overview.html (pristupljeno: kolovoz 2022)

[28] Tech hub. Preuzeto sa: https://techhub.hpe.com/eginfolib/networking/docs/switches/3600v2/5998-7619r_l3-ip-rtng_cg/content/442284154.html (pristupljeno: kolovoz 2022)

[29] Techtarget. Preuzeto sa: https://www.techtarget.com/searchnetworking/definition/HELLO-packet (pristupljeno: kolovoz 2022)

[30] Tcp ip guide. Preuzeto sa: http://www.tcpipguide.com/free/t_OSPFMessageFormats-2.htm (pristupljeno: kolovoz 2022)

[31] Cc expert. Preuzeto sa: https://www.ccexpert.us/large-scale-ip/ospf-packet-types.html (pristupljeno: kolovoz 2022)

[32] Cc expert. Preuzeto sa: https://www.ccexpert.us/routing-tcp-ip/the-link-state-request-packet.html (pristupljeno: kolovoz 2022)

[33] Cc expert. Preuzeto sa: https://www.ccexpert.us/routing-tcp-ip/the-link-state-acknowledgment-packet.html (pristupljeno: kolovoz 2022)

[34] Mohanty, R., Sahoo, S., Kabat, M., R. (2023) A Network Reliability based Secure Routing Protocol (NRSRP) for Secure Transmission in Wireless Body Area Network 2023 8th International Conference on Communication and Electronics Systems (ICCES), 663-668 (pristupljeno: rujan 2023)

[35] Sysportal Carnet. Preuzeto sa: https://sysportal.carnet.hr/node/652 (pristupljeno: rujan 2023)

[36] Cisco CCNA 200-301 Official Cert Guide, Volume 1 (pristupljeno: srpanj 2022)

[37] Hartman, S., Zhang, D. (2013) Analysis of OSPF Security According to the Keying and Authentication for Routing Protocols (KARP) Design Guide RFC 6863, 1-11 (pristupljeno: rujan 2023)

[38] IBM. Preuzeto sa: https://www.ibm.com/docs/en/ssw_ibm_i_73/pdf/rzal6ospfpdf.pdf (pristupljeno: kolovoz 2022)

[39] Cisco. Preuzeto sa: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html#anc10 (pristupljeno: rujan 2023)

[40] Network Lessons. Preuzeto sa: https://networklessons.com/ospf/introduction-to-ospf-stub-areas (pristupljeno: rujan 2023)

[41] Routeralley. Preuzeto sa: https://www.routeralley.com/guides/ospf.pdf (pristupljeno: rujan 2023)

[42] Networks training. Preuzeto sa: https://www.networkstraining.com/not-so-stubby-area-ospf-nssa/ (pristupljeno: rujan 2023)

[43] Cisco. Preuzeto sa: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13687-15.html (pristupljeno: kolovoz 2022)

[44] Packet life. Preuzeto sa: https://packetlife.net/blog/2008/jun/19/ospf-network-types/ (pristupljeno: kolovoz 2022)

[45] Networkel. Preuzeto sa: https://networkel.com/ospf-over-nbma-network/ (pristupljeno: kolovoz 2022)

[46] Network lessons. Preuzeto sa: https://networklessons.com/ospf/ospf-point-to-point-network-type-over-frame-relaye (pristupljeno: kolovoz 2022)

POPIS KRATICA

OSPF – Open shortest path first

LAN – Local area network

WAN – Wide area network

PLC – Programmable logoic controller

ISO – International organization of standardization

IGP – Interior gateway protocol

EGP – Exterior gateway protocol

EIGRP – Enhanced interior gateway routing protocol

LSA – Link-state advertisement

IS-IS – Intermediate system - Intermediate system

NLSP – Netware link state protocol

LSDB – Link state database

LSU – Link state update

LSR – Link state request

LSAck – Link state acknowledgement

SPF – Shortest path first

AS – Autonomous system

TCP/IP – Transmission control protocol/Internet protocol

ABR – Area border router

NSSA – Not-so-stubby area

PVC – Permamnet virtual circuit

NBMA – Non-broadcast multiple access

ATM – Asynchronous transfer mode

DR – Designated router

BDR – Backup designated router

POPIS SLIKA

Slika 1. Zvjezdasta topologija 3
Slika 2. Sabirnička topologija 4
Slika 3. Prstenasta topologija 4
Slika 4. Topologija stabla 5
Slika 5. Mesh topologija 6
Slika 6. Logička topologija 7
Slika 7. Tablica usmjeravanja 9
Slika 8. Hijerarhijski prikaz protokola usmjeravanja 11
Slika 9. Način rada SPF algoritma 15
Slika 10. Zaglavlje OSPF paketa 17
Slika 11. Hello paket 17
Slika 12. Database description paketi 18
Slika 13. Link state request paketi 18
Slika 14. Link state update paketi 19
Slika 15. Link state acknowledgment paketi 19
Slika 16. OSPF područja 23
Slika 17. Point to point mreža 26
Slika 18. Broadcast mreža 26
Slika 19. Non broadcast mreža 27
Slika 20. NBMA mreža 27
Slika 21. Point to multipoint mreža 28

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je _____završni rad_____ isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.
Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom ___Analiza rada protokola OSPF___ , u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, __17.11.2023__

(ime i prezime, *potpis*)