



FAKULTET ZA POSLOVNU INFORMATIKU

TEHNIKE RUTIRANJA

- Diplomski rad -

Mentor:
Prof dr Mladen Veinović

Student:
Jasmina Marković

Br. indeksa:
III-43/2004



FAKULTET ZA POSLOVNU INFORMATIKU

UNIVERZITET SINGIDUNUM
FAKULTET ZA POSLOVNU INFORMATIKU
Beograd, Danijelova 32

Broj: _____/2006

Kandidat: Jasmina Marković

Broj indeksa: III-43/2004

Smer: Projektovanje i programiranje

Tema: TEHNIKE RUTIRANJA

Zadatak: Prikaz OSI modela kao osnove svakog umrežavanja i na koji način su osnove OSI referentnog modela integrisane u aplikacije koje se koriste u komunikaciji od uređaja do uređaja. TCP/IP adresiranje sa posebnim osvrtom na IP adresiranje. WAN mreže, tehnologije, standardi i uloga rutera u WAN mrežama. Rutiranje, rutiranje protokoli i algoritmi za rutiranje. Komandno linijski interfejs rutera, radni modovi i komponente rutera, konfiguracioni fajl i konfiguracioni modovi.

MENTOR

Prof. dr Mladen Veinović

Datum odobrenja teme:
20.06.2006.
Beograd

DEKAN

Prof. dr Milan Milosavljević

Sažetak

Raznolikost i brojnost Internet aplikacija uslovljavaju da njegove naredne generacije budu prilagođene spajanju velikog broj domena uz garantovan kvalitet prenosa podataka, i tačno određenim propusnim opsegom. Ruteri su sastavni deo Interneta i bili su tema razmatranja mnogih studija i istraživanja. Ruteri koji podržavaju *multicasting* omogućavaju uštedu propusnog opsega izbegavanjem transmisije dupliranih paketa. Na ruterima su istovremeno konfigurisani različiti protokoli i bezbednosne polise. Performanse nekih popularnih ruting algoritama koji se koriste za multicast komunikaciju i jedna od kritičnih komponenti za rad rutera, ruting tabela, su ovde analizirani.

Abstract

As the Internet has grown in size and diversity of applications, the next generation is designed to accommodate flows that span over multiple domains with quality of service guarantees, and in particular bandwidth. Routers are integral parts of the Internet, and they have been the focus of much study and research in the networking community. Routers that support multicasting help their networks save bandwidth by avoiding transmission of duplicated packets over the same links. Routers in an operational network are simultaneously configured with multiple protocols and security policies while forwarding traffic and being managed. The performances of some popular routing algorithms used for multicast communications and one of the most performance critical components of a router, the routing table and its access and search mechanisms, are analyzed.

SADRŽAJ

1. UVOD	- 1 -
2. INTERNETWORK.....	- 2 -
3. OPEN SYSTEM INTERCONNECTION REFERENCE MODEL – OSI REFERENTNI MODEL	- 4 -
3.1 Arhitektura slojeva	- 4 -
3.2 Relacije između slojeva OSI modela	- 5 -
3.3 Protokoli	- 5 -
3.4 Kako rade protokoli.....	- 5 -
3.5 Protokoli u slojevitoj arhitekturi	- 6 -
3.6 Stekovi protokola.....	- 6 -
3.7 TCP/IP [5]	- 7 -
3.8 Definisanje osnovnih protokola skupa TCP/IP protokola	- 8 -
3.8.1 Protokoli Internet sloja	- 8 -
3.8.2 Address Resolution Protocol (ARP).....	- 8 -
3.8.3 Internet Control Message Protocol (ICMP)	- 9 -
3.8.4 Internet Protocol (IP).....	- 9 -
3.8.5 Internet Group Management Protocol (IGMP)	- 10 -
3.10 Internet protokol (IP) adrese	- 11 -
3.10.1 Klase IP adresa.....	- 11 -
A klasa adresa	- 11 -
B klasa adresa	- 11 -
C klasa adresa	- 11 -
D klasa adresa	- 11 -
E klasa adresa	- 11 -
3.11 Transport Control Protocol (TCP)	- 11 -
3.11.1 Uspostavljanje TCP sesije (TCP Three-Way-Handshake).....	- 12 -
3.12 Budućnost TCP/IP protokola	- 12 -
3.13 Formati adresa kod IPv6 protokola	- 12 -
3.13.1 Format IPv6 zaglavlja.....	- 13 -
4. WAN tehnologije i standardi.....	- 14 -
4.1 Uloga rutera u WAN mrežama.....	- 14 -
4.2 Komponente rutiranja	- 14 -
4.2.1 Switching (komutacija).....	- 15 -
4.2.2 Određivanje ruting putanje (Path Determination)	- 16 -
4.2.3 Uključivanje statičkih putanja.....	- 17 -
4.2.4 Dinamičko određivanje putanja	- 18 -
5. Protokoli za rutiranje.....	- 20 -
5.1 Exterior Gateway Protocol (EGP).....	- 20 -
5.2 Border Gateway Protocol (BGP)	- 21 -
5.3 Unutrašnji gateway protokoli [3]	- 21 -
5.4 Routing Information Protocol (RIP)	- 23 -
5.5 IGRP [3]	- 24 -
5.6 EIGRP [3].....	- 24 -
5.7 Open Shortest Path First (OSPF).....	- 25 -

5.8 IS-IS [3]	- 25 -
5.9 MPLS.....	- 26 -
6. PRIMER IZBORA RUTE NA CISCO RUTERIMA [4]	- 28 -
6.1 Pravljenje ruting tabele	- 28 -
6.2 Backup Rute	- 29 -
6.3 Menjanje Administrative Distance	- 29 -
6.4 Dužina prefiksa.....	- 30 -
6.5 Forwarding Decisions	- 30 -
6.6 Forvardovanje paketa (Packet Forwarding) korišćenjem ARP (Address Resolution Protocol).....	- 31 -
6.7 Primer tabele rutiranja kod Windows operativnog sistema.....	- 33 -
6.8 Problemi zaštite tabele rutiranja [1].....	- 34 -
7. ALGORITMI ZA RUTIRANJE	- 38 -
7.1 LS algoritmi.....	- 39 -
7.2 DV algoritmi	- 42 -
7.3 Hijerarhijsko rutiranje (Hierarchical Routing).....	- 48 -
7.4 Rutiranje emisijom (Broadcast Routing) [6].....	- 50 -
7.5 Rutiranje višestrukim usmeravanjem (Multicast Routing) [6].....	- 52 -
8. KOMPONENTE I RADNI MODOVI RUTERA (CISCO®) [2].....	- 55 -
8.1 Interne komponente rutera.....	- 55 -
8.2 Eksterne komponente.....	- 55 -
8.3 Startup procedura	- 55 -
8.4 Konfigurisanje registra.....	- 56 -
8.5 Cisco CLI Komandni modovi (Cisco® CLI Command Modes)	- 56 -
9. ZAKLJUČAK.....	- 59 -
10. LITERATURA	- 60 -
PRILOG 1.....	- 61 -
POJMOVI	- 63 -
SADRŽAJ POGLAVLJA	- 66 -

1. UVOD

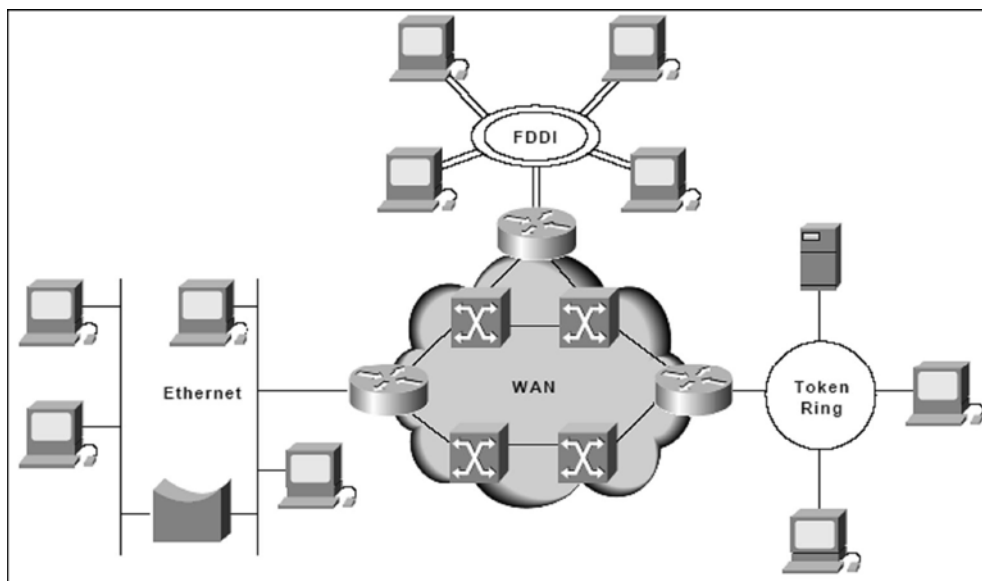
Glavna uloga rutera u mreži je da rutiraju pakete da bi oni došli do svog odredišta. Informacija koja se koristi za ovu funkciju je odredišna adresa smeštena u paketu. Ruter obavlja ovu funkciju tako što po prispeću paketa izvuče odredišnu adresu, zatim nađe odgovarajući zapis u tabeli rutiranja gde su smešteni podaci na koji port treba paket da se prosledi i adresa sledećeg rutera na putu tj. ka kojem se paket usmerava. Ovaj proces se naziva „*address lookup*“. Kada se dobije ova informacija onda se vrši proces komutacije (*switching*) i paket se komutira sa ulaza na odgovarajući izlazni port odakle se šalje dalje. Naravno pored ovih osnovnih funkcija postoje i druge elementarne funkcije kao npr. provera ispravnosti paketa, obrada kontrolnih paketa itd. Međutim, najnoviji trend je da ruteri treba da obavljaju i dodatne funkcije kao npr. „*security*“ protokoli, kvalitet servisa i sl. koji nameću dodatne zahteve ruterima. Takođe, broj korisnika na Internetu je u stalnom porastu tako da saobraćaj koji generišu korisnici je sve veći. Saobraćaj se takođe uvećava usled sve zahtevnijih aplikacija koje zahtevaju veoma velike propusne opsege (npr. prenos videa u realnom vremenu). Da bi se izborilo sa povećanim saobraćajnim zahtevima implementiraju se linkovi sve većeg kapaciteta do nekoliko desetina gigabajta po sekundi sa tendencijom da se ti protoci podignu na terabitske brzine. To znači da obrada paketa mora biti veoma brza i efikasna jer ruter sada pri takvim kapacitetima linkova mora da procesira milione paketa u sekundi i prosleđuje ih na odgovarajuće izlazne portove. Jedan od glavnih problema je upravo proces „*address lookup*“ i iz tog razloga su razvijeni razni algoritmi koji treba ovaj proces da načine što efikasnijim da bi samim tim ruter bio što efikasniji.

2. INTERNETWORK

Tehnologija koja omogućava povezivanje različitih LAN i WAN mreža u jednu univerzalnu mrežu. Internetwork je skup fizičkih mreža povezanih ruterima, koja funkcioniše kao velika jedinstvena mreža. Elementi Internetwork-a:

- Fizičke mreže (*Physical network*)
- Ruteri (*Router, Intermediate System, IS*)
- Stanice (*Host, End System, ES*)

Slika 2.1 ilustruje različite oblike mrežnih tehnologija koje mogu biti povezane ruterima i drugim mrežnim uređajima kako bi se kreirao Internetwork.



Sl. 2.1. Različite mrežne tehnologije povezane radi kreiranja Internetwork-a

Prva mreža je bila *time-sharing* mreža koju su koristili mainframe računari i terminali.

Local-area networks (LAN) se razvila tokom PC revolucije. LAN omogućava velikom broju korisnika na relativno malom prostoru da razmenjuju fajlove i poruke, kao i pristup različitim deljenim resursima kao što su fajl serveri i štampači.

Wide Area Network -WAN (Mreža širokog područja) povezuje LAN-ove geografski rasutih korisnika radi omogućavanja njihovog komuniciranja. Neke od tehnologija za povezivanje

LAN-ova su: T1(E1), T3 (E3), ATM, ISDN, ADSL, prespajanje okvira (*Frame Relay*), radio veze i slično. Ove mreže se nazivaju i okosnice ili kičma-mreže (*backbone*).

Internetwork se koristi u rešavanju tri ključna problema: kod izolovanih LAN-ova, dupliranja resursa, nemogućnosti primene centralizovane metode za upravljanje i rešavanje problema na mreži.

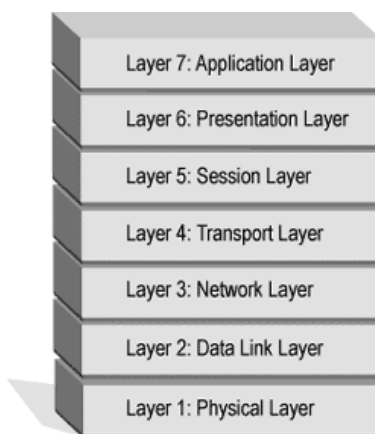
3. OPEN SYSTEM INTERCONNECTION REFERENCE MODEL – OSI REFERENTNI MODEL

Međunarodna organizacija za standarde – International Standards Organization (ISO) izdala je 1987. godine skup specifikacija koje opisuju arhitekturu mreže koja služi za povezivanje raznorodnih računarskih uređaja. Originalni dokument se odnosio na sisteme koji su bili otvoreni za povezivanje jedni prema drugima, jer su za razmenu informacija svi mogli da koriste iste protokole i standarde.

ISO je 1984. godine štampao reviziju ovog modela i nazvao ga **Referentni model za otvoreno povezivanje sistema – Open Systems Interconnection (OSI) reference model**. Ova revizija postala je međunarodni standard i služi kao vodič za umrežavanje. OSI model je najpoznatiji i najčešće korišćen model za slikovitu predstavu umreženih okruženja. Proizvođači ga se pridržavaju kada projektuju proizvode za mrežu. Model opisuje način na koji mrežni hardver i softver zajednički deluju kako bi se omogućila komunikacija. Model takođe pomaže pri rešavanju problema tako što nudi referentni okvir koji opisuje kako se pretpostavlja da komponente rade.

3.1 Arhitektura slojeva

Arhitektura OSI referentnog modela razvrstava mrežne komunikacije u sedam slojeva. Svaki sloj pokriva različite mrežne aktivnosti, opremu ili protokole. Slojevitost označava različite funkcije i usluge pri prenosu podataka sa jednog na drugi računar preko mrežne instalacije. OSI model definiše kako svaki sloj komunicira i sarađuje sa slojevima koji su neposredno iznad i ispod njega. Na primer, sloj sesije komunicira i sarađuje sa slojevima prezentacije i transporta.



Sl. 3.1 Sedmoslojni OSI model.

Svaki sloj obezbeđuje neke usluge ili postupke koji pripremaju podatke za dostavu putem mreže do drugog računara. Slojevi najnižeg nivoa, 1 i 2, definišu fizički medijum mreže i srodne poslove, kao što je način prosleđivanja bitova podataka u mrežne kartice (NIC) i kablove. Najviši slojevi definišu kako aplikacije pristupaju komunikacionim uslugama. Što je nivo sloja viši, složeniji su i njegovi poslovi.

Slojevi su međusobno razdvojeni granicama koje se nazivaju interfejsi. Svi zahtevi jednog sloja od susednog sloja prosleđuju se preko interfejsa. Svaki sloj se oslanja na standarde i aktivnosti sloja koji je ispod njega[7].

3.2 Relacije između slojeva OSI modela

Svaki sloj obezbeđuje usluge za sloj koji je neposredno iznad njega i rešava ga detalja o tome kako su one stvarno primenjene. Istovremeno, izgleda kao da je svaki sloj u direktnoj komunikaciji sa odgovarajućim slojem na drugom računaru. Ovo nudi logičnu ili virtualnu komunikaciju između ravnopravnih slojeva. Međutim, stvarna komunikacija između susednih slojeva odvija se samo na jednom računaru. Na svakom sloju softver primenjuje mrežne funkcije prema određenim protokolima.

3.3 Protokoli

Protokoli su pravila i procedure koje služe za komuniciranje. Izraz „protokol” se koristi u različitim kontekstima. Kada je više računara umreženo, pravila i tehničke procedure, koje upravljaju njihovom komunikacijom i saradnjom, nazivaju se protokoli.

Kod protokola u mrežnom okruženju, treba imati u vidu tri stvari: - Postoji mnogo protokola; - Mada svaki protokol omogućava osnovnu komunikaciju, svaki ima različitu namenu i izvršava različite poslove; - Svaki protokol ima svoje prednosti i ograničenja.

Neki od ovih protokola uključuju *LAN protokole*, *WAN protokole*, *mrežne protokole*, i *rutabilne protokole*. *LAN protokoli* funkcionišu na fizičkom sloju i data link sloju (sloju veze) OSI modela i obezbeđuje komunikaciju različitih LAN medija. *WAN protokoli* funkcionišu na tri najniža sloja OSI modela i obezbeđuju komunikaciju između različitih *wide-area* medija. *Rutabilni protokoli* su protokoli mrežnog sloja i odgovorni su za razmenu informacija između rutera u smislu izbora adekvatne putanje za mrežni saobraćaj. *Mrežni protokoli* su različiti protokoli višeg sloja koji postoje u nekom steku protokola.

Neki protokoli rade samo na određenom OSI sloju. Sloj na kome protokol radi opisuje njegove funkcije. Na primer, protokol koji radi na fizičkom sloju obezbeđuje da paket podataka prođe kroz mrežnu karticu (NIC) do mrežnog kabla.

Protokoli, takođe, mogu zajednički da rade u steku ili nizu protokola. Kao što mreža na svakom sloju OSI modela ima nove funkcije, tako i različiti protokoli zajednički rade na različitim nivoima jednog steka protokola. Nivoi u steku protokola „preslikavaju” izgled slojeva OSI modela. Na primer, sloj aplikacije TCP/IP protokola preslikava se na sloj prezentacije OSI modela. Protokoli obezbeđuju sve funkcije i mogućnosti steka.

3.4 Kako rade protokoli

Ukupne tehničke operacije, pomoću kojih se podaci prenose preko mreže, biće podeljeni u posebne, sistematične korake. Na svakom od tih koraka događaju se izvesne akcije kojih

nema na nekom drugom koraku. Svaki korak sadrži sopstvena pravila i procedure ili **protokol**.

Koraci protokola moraju da se sprovedu u skladu sa redosledom koji je isti za svaki računar u mreži. U predajnom računaru ovi koraci se izvršavaju od vrha ka dnu. U prijemnom računaru ovi koraci moraju da se sprovedu u obrnutom redosledu.

Na predajnom računaru protokol:

1. Deli podatke u manje celine, nazvane paketi, koje može da obrađuje.
2. Paketima dodaje adresne informacije tako da određeni računar na mreži može da odluči da li oni pripadaju njemu.
3. Pripremi podatke za prenos kroz mrežnu karticu (NIC) i dalje kroz mrežni kabl.

Na prijemnom računaru, protokoli sprovode isti niz koraka, ali obrnutim redosledom:

1. Preuzimaju pakete podataka sa kabla.
2. Kroz mrežnu karticu unose pakete podataka u računar.
3. Iz paketa podataka uklanjaju sve informacije o prenosu koje je dodao predajni računar.
4. Kopiraju podatke iz paketa u prihvatnu memoriju (bafer) koja služi za ponovno sklapanje.
5. Ponovno sklopljene podatke prosleđuju aplikaciji u obliku koji ona može da koristi.

Potrebno je da oba računara, predajni i prijemni, svaki korak izvedu na isti način kako bi primljeni podaci imali istu strukturu kakvu su imali pre slanja.

3.5 Protokoli u slojevitoj arhitekturi

U mreži, više protokola mora da radi zajedno. Njihov zajednički rad obezbeđuje ispravnu pripremu podataka, prenos do željenog odredišta, prijem i izvršavanje. Rad više protokola mora da bude usaglašen kako se ne bi događali konflikti ili nekompletne operacije, odnosno nekompletan prenos informacija. Rezultat tog usaglašavanja naziva se slojevitost (*layering*).

3.6 Stekovi protokola

Stek protokola je kombinacija, odnosno tačno definisan skup protokola. Svaki sloj steka određuje različiti protokol za obradu funkcija ili podsistema komunikacionog procesa. Svaki sloj ima sopstveni skup pravila. Slika 3.2 prikazuje OSI model i pravila koja važe za svaki sloj. Protokoli određuju pravila za svaki sloj OSI modela.

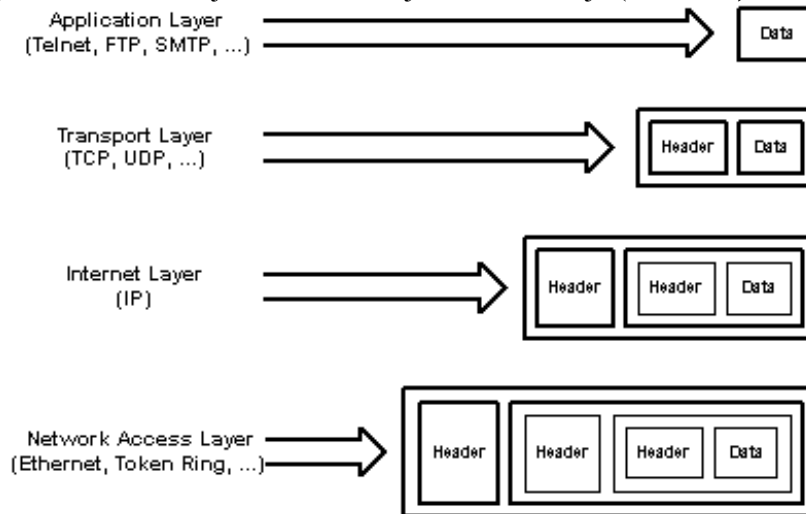
Sloj aplikacije	Započinje ili prihvata zahtev.
Sloj prezentacije	Paketu dodaje informacije koje služe za formatiranje, prikazivanje ili šifrovanje.
Sloj sesije	Dodaje informacije o toku saobraćaja kako bi se odredio trenutak slanja paketa.
Transportni sloj	Dodaje informacije koje služe za detektovanje i prevazilaženje greške u prenosu.
Sloj mreže	Dodaje informacije koje služe za sekvenciranje i adresiranje paketa.
Sloj veze	Dodaje informacije koje služe za proveru postojanja greške i priprema podatke za fizičko povezivanje.
Fizički sloj	Šalje paket kao niz bitova.

Sl. 3.2. Referentni model prikazuje slojeve protokola.

Niži slojevi OSI modela određuju proizvođačima kako da naprave opremu koja može međusobno da se povezuje; na primer, korišćenje mrežnih kartica (NIC) različitih proizvođača u istoj lokalnoj mreži (LAN). Sve dok koriste iste protokole, u mogućnosti su da jedne drugima šalju podatke i primaju ih. Viši slojevi određuju pravila po kojima se odvija komunikaciona sesija (period u kome dva računara održavaju vezu) i interpretacija aplikacija. Što su poslovi na višem nivou u steku, oni i njima odgovarajući protokoli su sve složeniji.

3.7 TCP/IP [5]

TCP/IP slojni model baziran je na modelu koji ima četiri sloja (slika 3.3.):



Sl. 3.3. Četvoroslojni TCP/IP model.

U **sloju mrežnog interfejsa**, samo se fizičke MAC adrese koriste za adresiranje. Ovaj sloj predaje pakete na mrežni kabl i preuzima pakete sa mreže. Mrežni sloj dodaje preambulu na početak paketa i dodaje CRC proveru, radi provere integriteta paketa, u slučaju da se paket ošteti u prenosu. Kada paket stigne na odredište, CRC se ponovo izračunava i proverava se da li je paket oštećen, ako nije predaje se mrežnom sloju, ako jeste on se za sada odbacuje.

Internet sloj pruža tri osnovne funkcije: adresiranje, pakovanje i rutiranje. Internet protokol (IP) je deo ovog sloja. IP protokol omogućuje isporuku informacije bezkonekcionog tipa i ne garantuje se sigurna isporuka informacije. IP protokol ne izvršava provere bilo kakvog tipa i ne poseduje mehanizme sigurnog prenosa informacije na odredišni računar. Paketi mogu biti izgubljeni, ili stići u nepredviđenom redosledu.

Kada podatak stigne od transportnog sloja, IP mu dodaje zaglavlje. Zaglavlje sadrži sledeće podatke:

- *Izvornu IP adresu;*
- *Odredišnu IP adresu;*
- *Transportni protokol.* Protokol koji koristi transportni sloj je smešten u ovo zaglavlje. Ovim se daje informacija Internet sloju da li je potrebno koristiti TCP ili UDP za transfer.
- *Kontrolni zbir (Checksum).* Ovim se vrši provera integriteta paketa.

- *Vreme egzistiranja (Time to live – TTL)*. Pri svakom prolasku paketa kroz ruter, vrednost TTL parametra se umanjuje najmanje za jedan. Kada vrednost TTL postane nula, paket se uklanja sa mreže.

Internet sloj određuje i način rutiranja paketa do odredišnog računara. U internet sloju odvija se i proces fragmentacije i defragmentacije.

Transportni sloj obezbeđuje krajnju komunikaciju između računara, upotrebom portova. TCP/IP poseduje dva protokola kojima se ostvaruje transport podataka:

- Transmission Control Protocol (TCP)
- Universal Datagram Protocol (UDP)

TCP obezbeđuje komunikaciju konekcionog tipa na TCP/IP mreži. TCP veza pruža visok nivo pouzdanosti. U prenosu se koriste brojevi sekvence i poruke potvrde, da bi se utvrdilo da je podatak uspešno primljen. Ukoliko odredišni računar ne primi specifičan segment, on može zatražiti ponovno slanje tog paketa.

UDP protokol obezbeđuje vezu bezkonekcionog tipa. U ovom slučaju ne garantuje se da će odredišni računar primiti informaciju. Aplikacije koje koriste UDP moraju same obezbediti mehanizam koji će omogućiti uspešnost prijema. Jedan vid kontrole koji poseduje UDP je kontrolna suma koja postoji u zaglavlju paketa. Kontrolna suma se koristi za proveru integriteta prispelog paketa.

U **aplikacioni sloj** su smeštene mrežne aplikacije. Mrežne aplikacije su aplikacije koje putem mreže komuniciraju sa drugim umreženim računarima. Mrežne aplikacije na TCP/IP mreži se mogu svrstati u:

- Winsock aplikacije (koriste Windows Sockets skup programskih interfejsa (API) i to su npr. FTP, Telnet, SNMP i IRC)
- NetBIOS aplikacije koriste NetBIOS imena i servise preko TCP/IP mreže.

3.8 Definisanje osnovnih protokola skupa TCP/IP protokola

3.8.1 Protokoli Internet sloja

Protokoli ovog sloja su u interakciji sa fizičkim delom mrežnog sloja, ili obezbeđuju logičko adresiranje transportnom sloju. Svi protokoli Internet sloja su:

- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP)
- Internet Protocol (IP)
- Internet Group Messaging Protocol (IGMP)

3.8.2 Address Resolution Protocol (ARP)

Da bi dva računara uspešno ostvarila komunikaciju na mreži, oni moraju da znaju fizičke adrese mrežnih adaptera. Ovo se obezbeđuje upotrebom ARP protokola. ARP vrši razlučivanje IP adrese odredišnog računara u MAC adresu. Takođe, proverava se da li odredišni računar može da izvede istu operaciju. ARP protokol koristi keš. ARP keš poseduje listu IP adresa koje su već prevedene u MAC adrese.

ARP proces:

1. Računar koji inicira vezu proverava ARP keš.

2. Ako zapis postoji, računar koji zahteva vezu kreira ARP paket koji sadrži upit namenjen određenoj računaru za njegovom MAC adresom. U tom ARP paketu nalazi se i IP i MAC adresa računara koji inicira vezu. Ovaj ARP paket se šalje na Ethernet broadcast adresu i svi računari na tom mrežnom segmentu analiziraju taj paket.
3. Svaki računar analizira ARP paket da bi proverio da li određena IP adresa paketa odgovara njegovoj IP adresi. Ukoliko se ne poklapaju adrese, paket se ignoriše. Ukoliko se poklapaju, određeni računar dodaje IP i MAC adresu računara koji je poslao paket, kao zapis u svoj ARP keš.
4. Određeni računar kreira ARP odgovor koji sadrži IP i MAC adresu. Ovaj odgovor vraća se računaru koji inicira vezu.
5. Računar koji inicira vezu dodaje IP i MAC adresu svom ARP kešu. Tada se može ostvariti komunikacija između dva računara.

3.8.3 Internet Control Message Protocol (ICMP)

Internet protokol kontrolnih poruka obezbeđuje mehanizam prijave greški i kontrolnih poruka TCP/IP protokolu. Protokol je izvorno kreiran radi prijavljivanja greški u toku rutiranja paketa kroz mrežu. Funkcije koje obavlja ICMP protokol:

- Posедуje eho poruke i poruke prijema potvrde kojima se testira pouzdanost veze između dva računara. Ovo se postiže primenom PING komande.
- Redirekcija saobraćaja, radi poboljšanja rutiranja u slučaju zagušenja rutera.
- Šalje poruke o isteku vremena predviđenog za egzistiranje paketa.
- Obezbeđuje slanje poruka računaru sa direktivom za usporavanje saobraćaja, u slučaju da je ruter opterećen.
- Utvrđuje masku podmreže mrežnog segmenta.

3.8.4 Internet Protocol (IP)

Internet protokol obezbeđuje sve logičke adrese računarima u mreži. Svakom računaru se dodeljuje jedinstvena IP adresa, shodno mreži na koju je povezan. IP protokol ostvaruje veze bezkonekcijskog tipa. Da bi dva računara komunicirali pomoću IP protokola, oni ne moraju da uspostave sesiju. Upoređivanjem IP adrese određenoj računaru sa izvorišnom IP adresom, IP može utvrditi da li se paket može direktno poslati računaru, ili se mora naći ruta.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
version				hlen				type of service								total lenght															
identification																flags				fragment offset											
time-to-live								protocol								header checksum															
source IP address																															
destination IP address																															
options																															
data (<= 65536 octets)																															

Verzija ukazuje na verziju IP protokola koja se koristi za kreiranje IP paketa. Trenutna verzija IP protokola koja se koristi je verzija 4.

Dužina Ukazuje na dužinu IP zaglavlja. Sva polja u IP paketu su fiksne dužine, osim Opcije i umetka. Ovo polje određuje granicu između zaglavlja i samih podataka u okviru paketa.

Tip servisa Ukazuje IP protokolu kako da rukuje sa IP paketom. Ovo polje poseduje pet polja: Prvenstvo, Korišćenje, Propusnost, Pouzdanost, Nije u upotrebi.

Dužina paketa Vrednost totalne dužine IP paketa, zaglavlje i podaci.

Offset fragmenta Sledeća tri polja imaju veliku važnost u procesu fragmentacije i procesu ponovnog sastavljanja fragmentiranih paketa. Polje za identifikaciju sadrži jedinstveni identifikator koji markira originalni paket. Polje Indikator (Flag), dužine 3 bita, kontroliše fragmentaciju. Prvi bit se trenutno ne koristi. Drugi bit predstavlja Don't Fragment (DF) bit, a treći je More Fragments (fragmentiran).

Time-to-live TTL polje ukazuje na period egzistencije paketa na mreži. Pri svakom prolasku paketa kroz ruter, vrednost ovog polja se smanjuje barem za jednu sekundu. Kada vrednost TTL parametra postane nula, ovaj paket se odbacuje na ruteru.

Protokol polje Protokol polje ukazuje na protokol više ravni koji je korišćen za kreiranje podataka smeštenih u delu paketa. Ova informacija je od značaja pri prolasku paketa kroz slojeve TCP/IP slojnog modela.

Kontrolna suma zaglavlja obezbeđuje informaciju o integritetu zaglavlja paketa, odnosno o tome da li je zaglavlje oštećeno u transferu. Ova suma se odnosi samo na zaglavlje, ne na ceo paket, smanjuje se vreme potrebno za analizu svakog pojedinačnog paketa, kada se nađe na ruteru.

Polja za izvorišnu i odredišnu IP adresu Ova polja sadrže 32-bitne IP adrese odredišnog i izvorišnog računara. Ove vrednosti se ne menjaju u toku saobraćaja.

Polja za opcije Ovo polje može biti sastavljeno od nekoliko kodova promenljive dužine. U IP paketu se može koristiti više opcija. Ukoliko postoji više opcija, polja se sukcesivno nalaze u zaglavlju. Svaka opcija je dužine 8 bitova i sadrži 3 podpolja. Prvi bit označava *copy flag*. Opcija *option class* predstavljena je sa 2 bita, a broj opcije (*option number*) smešten je u poslednjih pet bitova.

3.8.5 Internet Group Management Protocol (IGMP)

Polja IGMP paketa su:

Verzija	Tip	Neiskorišćen	Kontrolna suma
Adresa grupe			

Verzija Ovo polje ukazuje na verziju protokola koji je u upotrebi. Za IGMP pakete ovo polje ima vrednost 1.

Tip Polje ukazuje da li je IGMP poruka zahtev poslat od *multicast* rutera (vrednost 1) ili odgovor od IP računara (vrednost 2)

Kontrolna suma Ovo polje nosi vrednost sume cele IGMP poruke. Obezbeđuje informaciju za proveru integriteta paketa, odnosno da li je paket oštećen ili ne, u toku prenosa.

Adresa grupe Polje poseduje IP adresu za *multicast* grupe u kojoj se nalazi računar.

3.10 Internet protokol (IP) adrese

IP adresa jedinstveno identifikuje svaki host u TCP/IP mreži. Host može biti računar, terminal, ruter, pa čak i hab. Svaki host na mreži mora da poseduje jedinstvenu IP adresu. Ova adresa mora biti jedinstvena na celoj mreži. U velikim mrežama, kao što je Internet, postoji posebna institucija koja dodeljuje IP adrese. Za Internet ovo obavlja Internet Assigned Number Agency (IANA), koja postavlja politiku dodeljivanja IP adresa. Svaka IP adresa je niz od 32 nule i jedinice. Ovaj vid reprezentacije adrese bi bio veoma komplikovan za stalnu upotrebu, stoga je u upotrebi vid decimalne reprezentacije uz upotrebu tačaka. IP adresa se sastoji od četiri okteta koji čine 32-bitnu adresu. Svaki oktet se konvertuje u decimalni ekvivalent. Okteti se međusobno odvajaju tačkom.

3.10.1 Klase IP adresa

A klasa adresa

Klasa A koristi 8 bitova za mrežni deo adrese i 24 bita za host deo adrese. Prvi oktet adrese klase A uzimaju vrednost od 1 do 126. Ovim se može obezbediti 126 različitih mreža sa 16, 774, 214 hostova po mreži.

B klasa adresa

B klasa koristi 16 bitova za mrežni deo i 16 bitova za host deo adrese. Klasa B za prvi oktet uzima vrednosti od 128 do 191. Ovo dozvoljava 16 384 jedinstvene mreže sa 65 534 hosta na svakoj mreži.

C klasa adresa

Klasa C koristi 24 bita za oznaku mreža i 8 bita za oznake hostova. Klasa C uzima za vrednost prvog okteta raspon cifara od 192 do 223. Ovim se mogu obezbediti 2 097 152 jedinstvene mreže sa 254 hosta na svakoj mreži.

D klasa adresa

Adrese klase D rezervisane su za *multicast* upotrebu i ne mogu se dodeliti pojedinačnom hostu na mreži. Vrednost prvog okteta adresa iz klase D uzimaju vrednosti između 224 i 239.

E klasa adresa

Adrese ove klase su eksperimentalne i nisu dostupne za javnu upotrebu. Rezervisane su za buduću primenu. Vrednost prvog okteta adresa u klasi E uzimaju se iz opsega između 240 i 255.

3.11 Transport Control Protocol (TCP)

TCP protokol pruža sledeće funkcije:

- mehanizam pouzdane komunikacije između hostova koji inače koriste nepouzdanu IP protokol
- sekvencu za uspostavljanje krajnje komunikacije
- mehanizam za rekonstrukciju originalnih paketa podataka, ukoliko paketi ne dolaze po redosledu koji je određen njihovim brojem sekvenci
- mogućnost da izvorišni host može razlikovati aplikacije na drugom računaru
- vremensku kontrolu prenosa koja obezbeđuje ponovnu transmisiju paketa
- jednostavniji razvoj aplikacija

Aplikacije koje koriste TCP kao transportni protokol su npr: FTP, Telnet, SMTP mail serveri, Web serveri

3.11.1 Uspostavljanje TCP sesije (TCP Three-Way-Handshake)

Kada host treba da komunicira sa drugim hostom pomoću TCP protokola, odredišni host mora da odobri komunikaciju. Ukoliko odredišni host ne odobri komunikaciju TCP sesija se neće kreirati. Ova sesija se uspostavlja mehanizmom koji se naziva TCP three-way handshake.

1. U prvom koraku, računar koji inicira uspostavljanje veze, šalje TCP paket sa SYN flagom postavljenim na vrednost 1. Ovo znači da host koji šalje zahtev želi da sinhronizuje brojeve sekvenci sa odredišnim hostom.
2. Ukoliko odredišni host želi da uspostavi vezu, on šalje poruku sa potvrdom, odnosno postavlja flag ACK na 1, kao signal potvrde. Ova poruka potvrde šalje i sledeći broj sekvenci koji se očekuje. Ovim se TCP veza ostvaruje u jednom smeru. Za uspostavljanje veze i u drugom smeru, odredišni host takođe postavlja SYN flag na 1 i šalje broj sledeće sekvence koju očekuje.
3. Host koji je inicirao uspostavljanje veze odgovara na dobijeni TCP paket od odredišnog hosta slanjem poruke o potvrdi sa očekivanim brojem sekvence. Ovim se ostvaruje dupleks veza.

3.12 Budućnost TCP/IP protokola

Razvojem Interneta, trenutnom IP adresnom prostoru ponestaje adresa. Organizacija IETF je kreirala novu verziju IP protokola pod nazivom IPv6.

Bitne izmene koje donosi IPv6:

- **Proširene adresne mogućnosti.** Adresni prostor IPv6 će biti 128 bitni. Ovim se obezbeđuje veći skup IP adresa dostupnih na Internetu.
- **Uprošćavanje zaglavlja IP paketa.**
- **Poboljšavanje IP zaglavlja.** IP zaglavlje će biti formatirano tako da obezbedi efikasnije prosleđivanje, veću fleksibilnost kod dužine opcionih polja i lakše umetanje novih opcija.
- **Poboljšanje kontrola protoka.** IP paketi će moći da zahtevaju bolji kvalitet servisa.
- **Povećana sigurnost.** IP zaglavlje će posedovati dodatke kojima će se obezbediti autentifikacija hostova koji zahtevaju komunikaciju i poboljšana provera integriteta podataka.

3.13 Formati adresa kod IPv6 protokola

Hostovima koji koriste IPv6 dodeljuju se 128-bitne adrese. Ove adrese će spadati u jednu od sledećih klasa adresa:

- unicast
- anycast
- multicast

Klasa *unicast* je jedinstven identifikator dodeljen jednom interfejsu.

Klasa *anycast* je identifikator koji se dodeljuje za više interfejsa, generalno na različitim hostovima. *Anycast* adrese koriste istu sintaksu kao i *unicast* adrese. One postaju *anycast* adrese kada se dodele za više interfejsa. Hostovi, kojima su dodeljene *anycast* adrese, moraju biti eksplicitno konfigurisani, tako da znaju da se radi o *anycast* adresi.

Multicast adresa je identifikator za više interfejsa na različitim hostovima. Paket isporučen na multicast adresu, se isporučuje na sve interfejse kojima je dodeljena ta multicast adresa.

3.13.1 Format IPv6 zaglavlja

IPv6 zaglavlje poseduje sledeće osobine:

Verzija	Prioritet	Labela razvoja		
Payload dužina		Next Header		Hop Limit
Izvorna adresa				
Odredišna adresa				

- **Version.** Ovo polje, dužine 4-bita, ukazuje na broj verzije IP protokola.
- **Priority.** Ovo polje, dužine 4 bita, omogućuje izvoru da postavi prioritet za svoje pakete. Niži prioritet imaju paketi označeni sa 0 do 7.
- **Flow label.** Ovo polje, dužine 24 bita vrši označavanje paketa od izvornog hosta od strane IPv6 rutera.
- **Payload Length.** Ovo polje, dužine 16 bita, ukazuje na dužinu ostatka IP paketa.
- **Next Header.** Ovo polje, dužine 4 bita, je IPv6 ekvivalent Time-To-Live (TTL) polju u IPv4 protokolu. Pri svakom prosleđivanju paketa preko mrežnih segmenata, ova vrednost se umanjuje za jedan. Kada vrednost postane nula, paket se odbacuje.
- **Source Address.** Ovo polje, dužine 128 bita, sadrži IPv6 adresu odredišnog hosta.
- **Destination Address.** Ovo 128 bitno polje sadrži IPv6 adresu odredišnog hosta.

4. WAN tehnologije i standardi

WAN računarske mreže obuhvataju neograničen geografski prostor, sa propusnim opsegom reda 10 kbps do 40 Gbps. WAN standardi uobičajeno definišu protokole i fizičkog i sloja veze. Organizacije vezane za WAN standarde:

- International Telecommunication Union-Telecommunication Standardization Sector (ITU-T), bivši Consultative Committee for International Telegraph and Telephone (CCITT)
- International Organization for Standardization (ISO)
- Internet Engineering Task Force (IETF)
- Electronic Industries Association (EIA)

WAN tehnologije:

- Layer 1 - RS-232, RS-449, X.21, V.35, G.703 itd.
- Layer 2 - HDLC, PPP, Frame Relay, X.25
- Multilayer - ISDN, ATM, SDH/SONET

4.1 Uloga rutera u WAN mrežama

Kao što i samo ime ukazuje ruter se, kao uređaj, koristi za usmeravanje paketa kroz mrežu. Svaki ruter u računarskoj mreži poseduje znanje koje se odnosi na moguće puteve koje paketi podataka treba da pređu na putu od izvorišta do odredišta. "Znanje" o usmeravanju paketa (rutiranju) ugrađuje se u ruting tabelu koja se periodično ažurira i memoriše u bazi podataka rutera. Da bi odredio portove kojima se pridružuju odredišne adrese ruter koristi *broadcast* šemu koja se bazira na ARP-u (*Address Resolution Protocol*). Ono što je takođe važno i treba istaći je to da ruter može čitati sadržaje paketa podataka koji pristižu na dati port na osnovu čega može da odredi izvorišnu i odredišnu adresu, zatim tip podataka, kao i vreme prijema paketa. Nakon toga, koristeći ruting tabelu, ruter usmerava paket podataka ka jednom ili većem broju izlaznih portova, tj. prema odredišnoj adresi. Naime, paket podataka se usmerava ka portu ako se poruka prenosi od izvorišta ka odredištu, ili ka većem broju portova ako je paket tipa *broadcast* ili *multicast*.

4.2 Komponente rutiranja

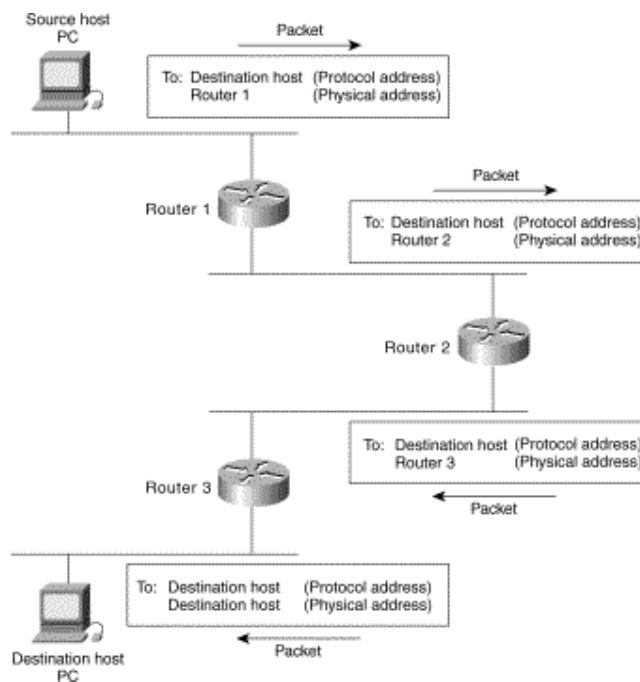
Rutiranje obuhvata dve osnovne aktivnosti: određivanje optimalne ruting putanje i transport paketa kroz *internetwork*. U kontekstu procesa rutiranja, ova druga komponenta se naziva *packet switching* (*komutacija paketa*). Iako je *packet switching* relativno jednostavan postupak, utvrđivanje putanje može biti veoma složeno.

4.2.1 Switching (komutacija)

Algoritam za komutaciju je relativno jednostavan i isti je za većinu rutirajućih protokola. U većini slučajeva, host pokušava da pošalje paket drugom hostu, zatim traži adresu rutera, šalje adresiran paket tačno na ruterovu MAC adresu zajedno sa protokolom (*network sloj*) adresom destinacionog hosta.

Nakon što proveriti destinacionu protokol adresu paketa, ruter utvrđuje da li zna ili ne kako da forvarduje paket do sledećeg odredišta. Ako ruter ne zna kako da forvarduje paket, paket se odbacuje. Ako ruter zna kako da forvarduje paket, menja destinacionu fizičku adresu u adresu narednog *hop*-a i šalje paket.

Naredni *hop* može biti destinacioni host. Ako to nije slučaj, naredni *hop* je obično naredni ruter. Dok paket putuje kroz *internetwork*, menja mu se fizička adresa, ali protokol adresa ostaje ista, kao što je prikazano na slici.



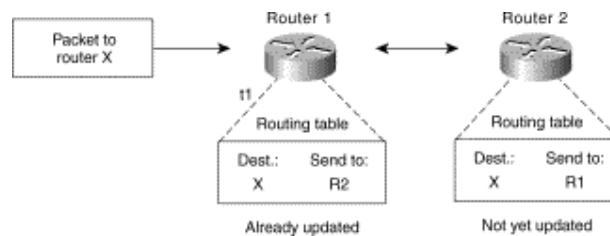
SI. 4.1. Switching Proces

International Organization for Standardization (ISO) je ustanovila terminologiju koja opisuje proces komutacije između izvornog (*source*) i odredišnog (*destination end*) sistema. Po toj terminologiji, mrežni uređaji koji nemaju mogućnost da forvarduju pakete između podmreža se nazivaju *end systems (ESs)*, dok mrežni uređaji koji imaju tu mogućnost se nazivaju *intermediate systems (ISs)*. ISs sistemi se dalje dele na one koji imaju mogućnost komunikacije u okviru nekog rutirajućeg domena (*intradomain ISs*) i na one koji mogu da komuniciraju i u i između rutirajućih domena (*interdomain ISs*). Pod rutirajućim domenom (*routing domain*) se obično podrazumeva deo mreže pod zajedničkim administrativnim autoritetom. Rutirajući domeni se takođe nazivaju i autonomnim sistemima (*autonomous systems*) [8].

4.2.2 Određivanje rutin putanje (Path Determination)

Ruting protokoli koriste metriku radi utvrđivanja koja putanja je najbolja za transport paketa. Metrika je standard mera, koju koriste ruting algoritmi da bi utvrdili optimalnu putanju do destinacije. Kao pomoć procesu utvrđivanja putanje, ruting algoritmi inicijalizuju i održavaju ruting tabele, koje sadrže informacije o rutama. Informacije o rutama variraju u zavisnosti od toga koji se ruting algoritam koristi.

Ruting algoritam upisuje u ruting tabelu različite informacije. *Destination/next hop* govori ruteru da je optimalan put do određene destinacije ruter koji je predstavljen kao „next hop“ na tom putu. Kada ruter dobije paket, on proverava adresu destinacije i pokušava da je poveže sa adresom sledećeg skoka. Slika 4.2. pokazuje primer *destination/next hop*



Sl. 4.2. Primer Destination/next hop

Da bi mogao da rutira pakete sa informacijama, ruter ili bilo koji drugi uređaj koji je za to zadužen treba da poseduje sledeće ključne informacije:

- **Adresu odredišta** - Adresa do koje informacija treba da se rutira. Ovaj podatak obezbeđuje matični računar.
- **Izvor informacija** - Od kojih izvora (drugih rutera) ruter može da sazna putanje do željenih odredišta.
- **Moguće putanje** - Koje su inicijalne moguće putanje ili putanje do željenog odredišta.
- **Najbolje putanje** - Najbolja putanja do željenog odredišta.
- **Informacije o održavanju rutiranja i njihovo proveravanje** - Način provere da li su poznate putanje i dalje važeće i aktuelne.

Informacije o rutiranju koje ruter dobija od svojih izvora smeštaju se u njegovu tabelu rutiranja. Na ovu tabelu ruter se oslanja prilikom određivanja izlaznog porta koji će se koristiti za prosleđivanje paketa do odredišta. U tabeli rutiranja nalaze se podaci o mrežama koje su značajne za ruter. Ukoliko nije direktno povezan sa odredišnim mrežama, ruter mora da sazna i izračuna najbolju moguću putanju za prosleđivanje paketa do njih.

Tabela rutiranja popunjava se na jedan od sledeća dva načina:

- Ručno je popunjava administrator mreže - Mrežni administrator kreira ruting tabele sa ciljem da optimizira mrežne performanse u odnosu na nekoliko parametara, kakve su cena ruta, kašnjenje, propusni opseg, i dr.
- Popunjava se dinamičkim procesima koji funkcionišu u okviru mreže

Prosleđivanje paketa do mreža sa kojima ruter nije u direktnoj vezi može da se vrši na dva načina:

- **Statičke putanje** - Reč je o putanjama koje je ruter upoznao nakon što ih je administrator ručno ustanovio. Kada god topologija mreže iziskuje ažuriranje (na primer, prilikom kvara na vezi), administrator mreže ovakvu putanju mora da ažurira.
- **Dinamičke putanje** - Ove putanje ruter automatski saznaje nakon što administrator konfiguriše protokol rutiranja koji pomaže u procesu njihovog određivanja. Za razliku od statičkih putanja, čim mrežni administrator uključi dinamičko rutiranje, informacije o rutiranju se samim procesom rutiranja automatski ažuriraju svaki put kada se od nekog rutera u okviru mreže primi informacija o novoj topologiji.

4.2.3 Uključivanje statičkih putanja

Da bi mogao da izvrši rutiranje paketa, ruter samo treba da poznaje putanju do određene mreže. Statičke putanje su putanje koje određuju administratori mreže, i njima se izričito određuje put paketa od računara izvora do odredišnog računara. Ova vrsta putanja omogućava vrlo preciznu kontrolu nad celokupnim procesom rutiranja u okviru mreže. Statičke putanje su značajne kada mrežni operativni sistem ne može da odredi putanju do nekog odredišta. Pored toga, ove putanje koriste se i za naznačavanje "mrežnog prolaza poslednjeg utočišta". Mrežni prolaz poslednjeg utočišta ("*gateway of last resort*") predstavlja adresu na koju će ruter da pošalje paket koji je adresiran na mrežu koja se ne nalazi u njegovoj tabeli rutiranja. Statičke putanje se najčešće koriste prilikom rutiranja između glavne i izdvojene mreže. Izdvojene mreže ("*stub network*"), za koje se ponekad koristi i termin "čvor bez potomaka" ("*leaf node*") jesu mreže kojima može da se pristupi samo jednom putanjom. U ovakvim situacijama često se koriste statičke putanje zato što je to onda jedina putanja koja vodi u ovakvu mrežu ili iz nje. Pošto do ovakvih mreža (i iz njih) vodi samo jedan put, na ruterima mogu da se konfigurišu statičke putanje i time izbegne postojanje onog dela mrežnog saobraćaja koji potiče od protokola rutiranja. Ovde treba spomenuti da se konfigurišanjem statičkih putanja obezbeđuje mogućnost povezivanja sa slojem povezivanja podataka koji nije u direktnoj vezi sa ruterom. Da bi se dobila mogućnost povezivanja od jedne do druge krajnje tačke, putanja mora biti konfigurisana za oba smera. Statičke putanje se konfigurišu u režimu globalne konfiguracije rutera unošenjem komande IP ROUTE. Uz ovu komandu koriste se i parametri kojima se statičke putanje dodatno definišu. Kod statičkih putanja moguće je ručno konfigurišanje tabele rutiranja. Ovako unet upis ostaje u tabeli dokle god je putanja aktuelna. Jedini izuzetak od ovog pravila je opcija *permanent* koja je prikazana u sledećem primeru. Aktiviranjem opcije *permanent*, putanja ostaje u tabeli čak i ako više nije aktivna.

Sintaksa komande IP ROUTE (za CISCO rutere):

```
ip route network [mask] {address | interface} [distance] [permanent]
```

Značenje argumenata komande IP ROUTE:

network - odredišna mreža ili podmreža

mask - maska podmreže

address - IP adresa rutera sledećeg skoka

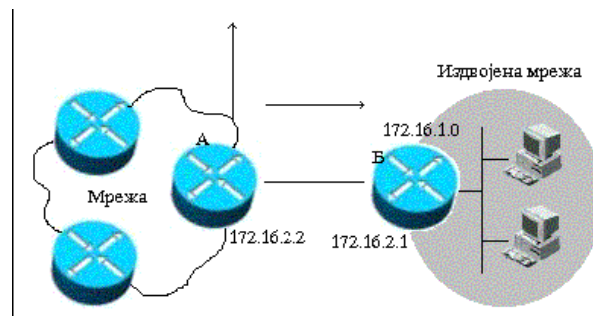
interface - ime interfejsa kojim se paket šalje do odredišne mreže

distance - ovo je opciona parametar kojim se definiše administrativna udaljenost

permanent - takođe opciona parametar kojim se naznačava da putanja neće biti uklonjena čak ni u slučaju da se interfejs isključi

Primer statičkog određivanja putanja:

Router (config) #ip route 172.16.1.0 255.255.255.0 172.16.2.1



Sl. 4.3. Primer određivanja statičke putanje

U ovom slučaju statička putanja od rutera A do izdvojene mreže konfigurisana je na sledeći način:

Router (config) #ip route 172.16.1.0 255.255.255.0 172.16.2.1

Značenje parametara ove komande:

- **ip route** - komanda za statičko rutiranje
- **172.16.1.0** - definiše statičku putanju do odredišne podmreže
- **255.255.255.0** - odnosi se na masku podmreže (8 bitova je na snazi)
- **172.16.2.1** - IP adresa rutera sledećeg skoka na putu do odredišta

U slučaju rutera A, dodeljivanje statičke putanje do izdvojene mreže 172.16.1.0 je ispravno, zato što do ove mreže može da se dospe samo jednim putem. Da bi mogla da postoji dvosmerna komunikacija, mora da se konfiguriše i putanja u suprotnom smeru. Podrazumevana putanja je posebna vrsta statičke putanje koja se koristi kada putanja od izvora do odredišta nije poznata, ili kada u tabeli rutiranja nije moguće skladištenje svih potrebnih informacija o potrebnim putanjama. Podrazumevana putanja naziva se takođe i mrežni prolaz poslednjeg utočišta.

4.2.4 Dinamičko određivanje putanja

Drugi način za konfigurisanje rutiranja, dinamičko rutiranje, baziran je na automatskom kreiranju ruting tabela koje opisuju mrežu. Ukoliko se desi izmena u topologiji mreže, dinamički ruting protokol prenosi informacije o promenama na mreži svim ruterima. Nakon toga ruteri ponovo pronalaze najbolju moguću rutu do odredišnog mrežnog segmenta. Dva najčešća tipa protokola koja se danas koriste su *distance vector protokol* i *link state protocol*.

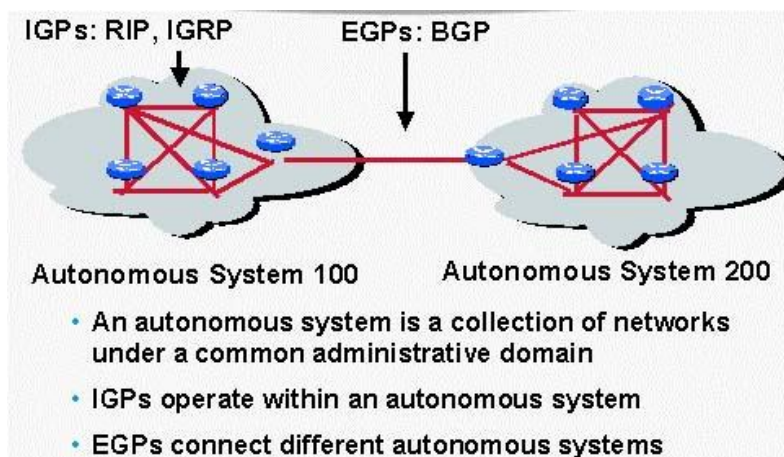
Distance vector protokol je baziran na broadcast-u koji kao kriterijum uzima broj hop-ova. Njegovo konfigurisanje je jednostavno. Kada se doda nov ruter on sam kreira svoje ruting tabele. Ovaj protokol ima i svojih mana. U većim mrežama se pokazao kao neskalabilan, jer svaki paket u mreži nosi informaciju o svim putanjama na toj mreži. Ovim se povećava mrežni saobraćaj, koji je posvećen samom rutiranju. Informacija o rutiranju se šalje samo susedima tog rutera tj. onima koji su povezani na isti fizički segment. Karakteristika ovih

protokola je i da veoma sporo konvergiraju. Vreme konvergencije je vreme koje je potrebno da se mreža prilagodi promena topologije i da ponovo izračuna sve ruting tabele.

Link state protokoli šalju informacije o rutiranju svim čvorovima u mreži. Ova informacija sadrži rutu samo do direktno spojenih mreža. Svaki ruter pothranjuje najbolje putanje u mrežni ID. Ovim se dobija u vremenu konvergencije. Jedina mana ovog protokola je što njegova implementacija zahteva više planiranja, konfigurisanja i CPU vremena za konfigurisanje rutiranja.

5. Protokoli za rutiranje

Autonomni sistemi imaju ključnu ulogu u definisanju da li je gateway protokol spoljni (*exterior*) gateway protokol (EGP) ili unutrašnji (*interior*) gateway protokol (IGP). Spoljašnji gateway protokoli razmenjuju informacije o rutiranju između autonomnih sistema. Dva najčešće implementirana protokola ovog tipa su *Exterior Gateway Protocol* i *Border Gateway Protocol*.



Sl. 5.1 Autonomni sistemi

Primeri IGP su [3]:

- *Routing Information Protocol (RIP)*
- *Interior Gateway Routing Protocol (IGRP)*
- *Enhanced Interior Gateway Routing Protocol (EIGRP)*
- *Open Shortest Path First (OSPF)*

5.1 Exterior Gateway Protocol (EGP)

Ovaj protokol je razvijen kao protokol za interdomensko povezivanje. EGP je dinamički protokol za rutiranje, ali ne izračunava bilo kakvu metriku. Kao rezultat toga, on nije u mogućnosti da načini inteligentne odluke pri rutiranju. Jedino kada informacija o rutiranju može da se koristi za EGP je kada se rute koje se porede potiču od istog autonomnog sistema. EGP je u stanju da informiše samo drugi ruter o dostupnosti druge mreže.

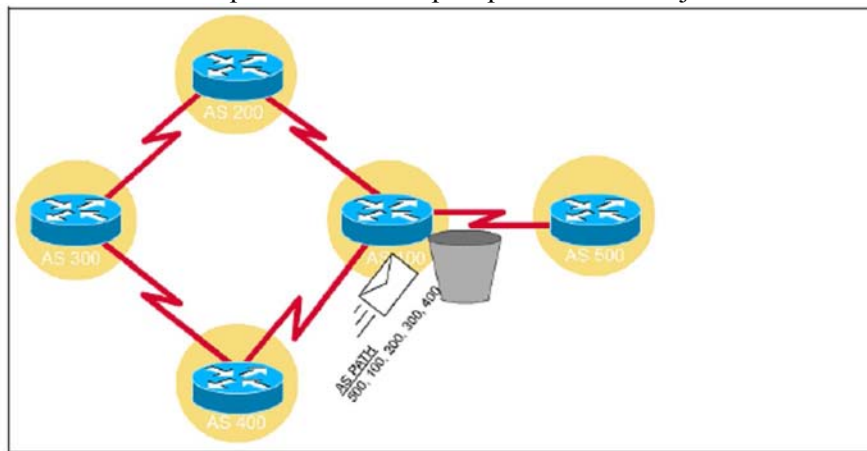
Osnovne tri funkcije EGP-a su:

- ustanovljavanje suseda
- pozivanje suseda; susedni ruteri se pozivaju da bi se proverilo da li funkcionišu

- slanje poruka o ažuriranju; EGP ruteri šalju poruke o ažuriranju koje sadrže informacije o dostupnosti mreže u okviru svojih autonomnih sistema.

5.2 Border Gateway Protocol (BGP)

Primarna funkcija BGP protokola je razmena informacija o dostupnosti mreža sa ostalim autonomnim sistemima. U odnosu na EGP ovaj protokol poseduje punu putanju autonomnog sistema (*autonomous-system path*), kroz koju saobraćaj mora proći na putu ka odredištu. BGP koristi TCP protokol za transport poruka o rutiranju između BG rutera.

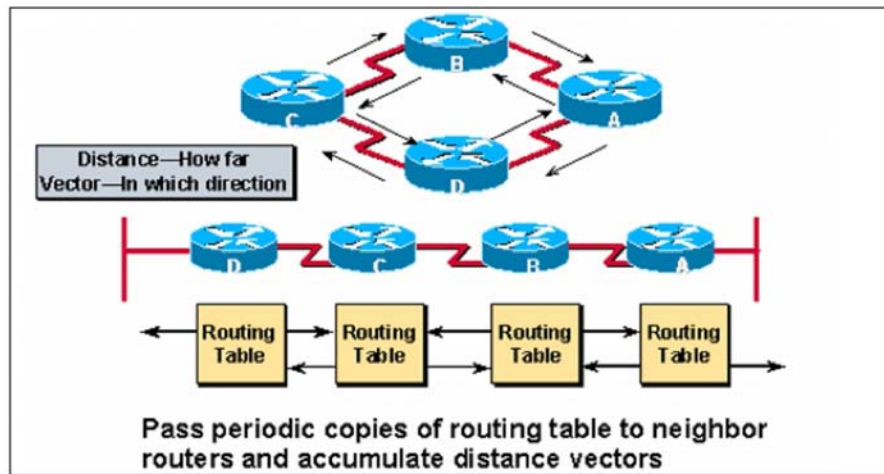


Sl. 5.2. BGP sprečava Routing Loop

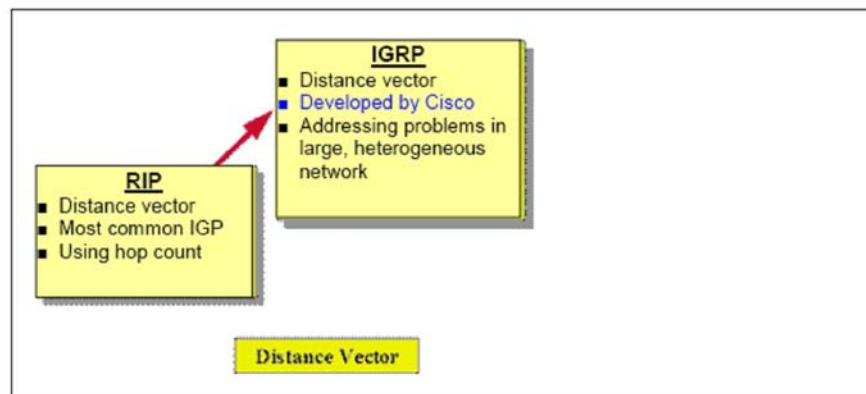
BGP koristi TCP protokol za transport poruka o rutiranju između BGP rutera. BGP koristi port 179 za uspostavljanje konekcije. Kada komuniciraju dva BGP sistema oni inicijalno razmene kompletne BGP ruting tabele. Nakon toga, između sistema se razmenjuju samo inkrementalne izmene.

5.3 Unutrašnji gateway protokoli [3]

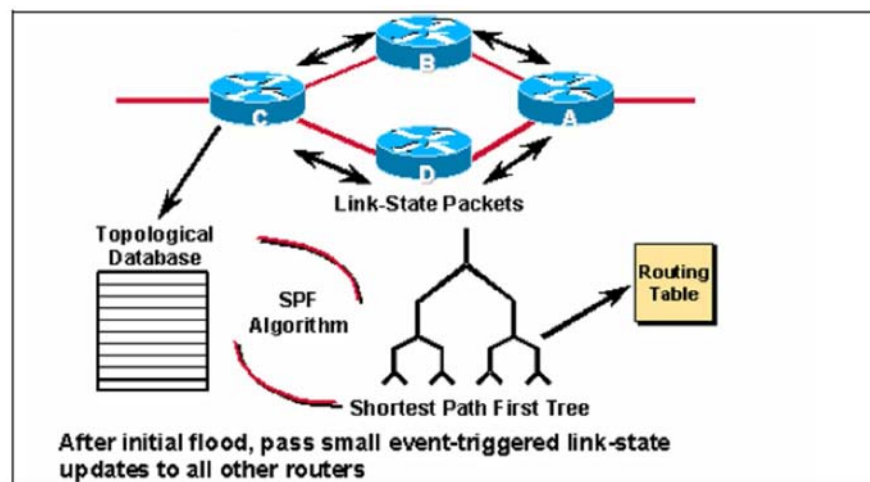
Ovi protokoli razmenjuju informacije o rutiranju između rutera koji pripada istom autonomnom sistemu. Pošto se sve informacije skupljaju u okviru istog autonomnog sistema, ovaj protokol više zavisi od metrike rutiranja, da bi se što preciznije mogla doneti odluka pri kreiranju ruting tabela. Dva najrasprostranjenija tipa protokola ovog tipa su *distance vector protokol* i *link state protokol*.



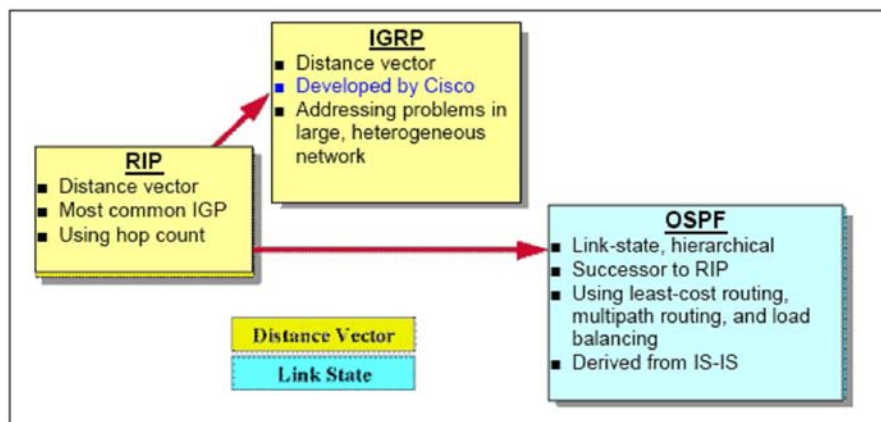
SI. 5.3. Distance Vector Routing Protocols



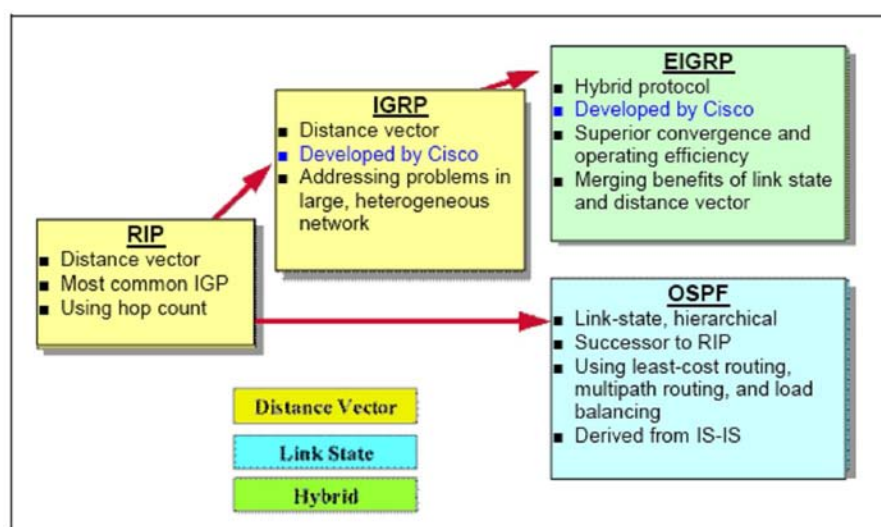
SI 5.4. Distance-Vector Routing Protocols



SI. 5.5. Link-State Routing Protocols



Sl. 5.6. Link-State Routing Protocols



Sl. 5.7. Hybrid Routing Protocols

5.4 Routing Information Protocol (RIP)

RIP je protokol za rutiranje baziran na *distance vector* tipu rutiranja, koji je razvijen za upotrebu na *Xerox Network Systems*. RIP koristi broj hop-ova kao metriku za rutiranje.

RIP održava samo najbolje rute ka odredišnoj mreži. RIP ruteri razmenjuju ruting informacije slanjem RIP broadcast poruke preko UDP porta broj 520. Ukoliko RIP ruter primi broadcast poruku koja savetuje bolju rutu ka drugoj mreži, ova bolja ruta zamenjuje staru već postojeću u ruting tabeli.

Po defaultu, RIP ruteri razmenjuju ruting informacije svakih 30 sekundi. *RIP broadcast* se šalje na sve interfejsе rutera i on sadrži kompletnu listu svih mrežnih ID oznaka do kojih su izrutirani. Maksimalni broj mreža koje se mogu prijaviti u jednoj RIP poruci je 25. Ovo dovodi do problema u skalabilnosti, ukoliko je mreža velika.

5.5 IGRP [3]

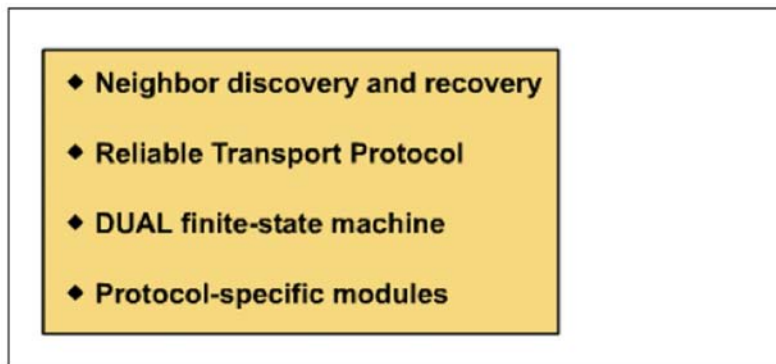
	Metric	Maximum No. of Routers	Origins
RIP	Hop count	15	Xerox
IGRP	Bandwidth load delay reliability	255, successfully run in largest internetworks in world	Cisco

Sl. 5.8. IGRP vs. RIP

IGRP je *distance-vector* rutinški protokol razvijen od strane Cisco-a. Razvijen je prvenstveno zbog problema vezanih za rutiranje u velikim mrežama čiji broj premašuje mogućnosti RIP protokola. U slučaju kada RIP bira putanju sa najmanje hopova, IGRP može da odabere najbržu putanju, zasnovano na *delay*, *bandwidth*, *load* i *reliability*. Administratori mogu da odrede važnost metrike, ili da dozvole da IGRP automatski izračuna optimalnu putanju. Po *default*-u IGRP koristi metriku samo za *bandwidth* i *delay*. IGRP ima mnogo viši limit maksimalnih hopova nego RIP. Po *default*-u, IGRP ruteri razmenjuju rutinške informacije svakih 90 sekundi. Ključne karakteristike IGRP bi bile:

- Prilagodljivost koja omogućava upravljanje neodređenim, kompleksnim topologijama
- Fleksibilnost za segmente koji imaju različite *bandwidth* i *delay* karakteristike
- Skalabilnost u funkcionisanju u velikim mrežama

5.6 EIGRP [3]



Sl. 5.9. EIGRP

Kao IGRP, EIGRP je takođe Cisco protokol. EIGRP je naprednija verzija IGRP protokola. EIGRP ima mnogo veću operativnu efikasnost kao što je brža konvergencija. On kombinuje prednosti *link-state* protokola i *distance-vector* protokola. Četiri osnovne prednosti u odnosu na IGRP su:

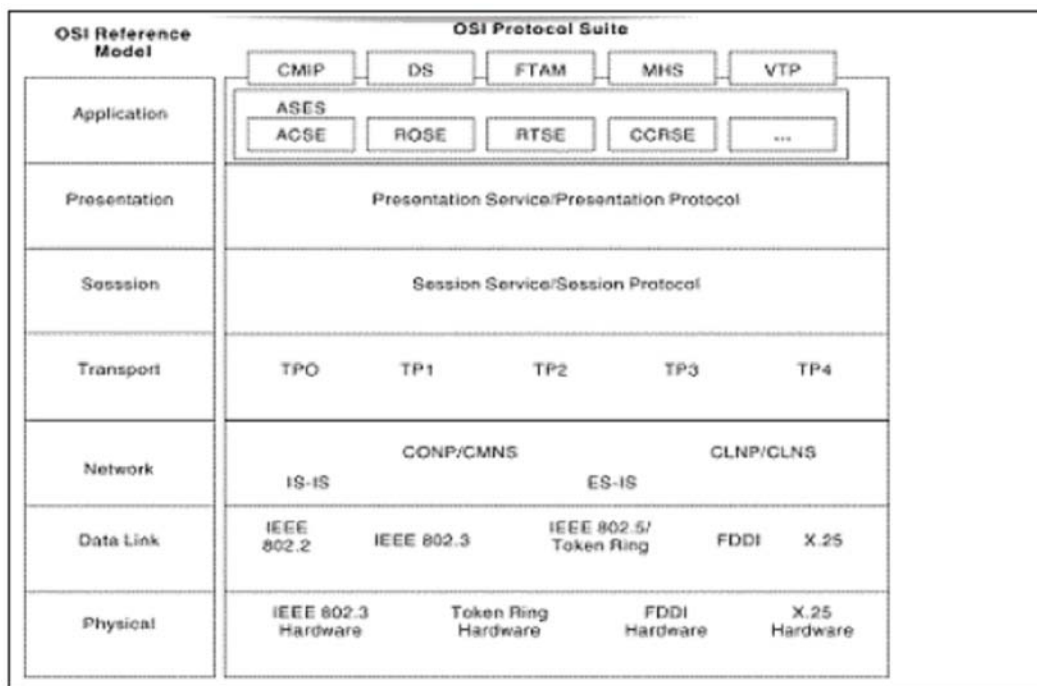
- *Neighbor discovery/recovery* - Omogućava ruterima da dinamično nauče 1870 susednih rutera.
- Pouzdan transportni protokol - Ova tehnologija garantuje isporuku paketa.
- *DUAL finite-state machine (Diffusing Update Algorithm (DUAL))* - prati sve rutere objavljene od strane suseda tako da je moguće izabrati *loop-free* putanju.
- *Protocol-dependent modules* - ovi moduli su odgovorni za mrežni sloj, za specifične zahteve protokola da bi se donela ruting odluka. EIGRP podržava rutabilne protokole kao što je IP, IPX i Appletalk.

5.7 Open Shortest Path First (OSPF)

OSPF protokol je *link state* tip protokola za rutiranje, koji je razvijen da bi otklonio neke nedostatke RIP protokola. OSPF je skalabilniji od RIP protokola i omogućuje konfigurisanje dinamičkog rutiranja u velikim, razuđenim mrežama.

Mreža može biti podeljena na autonomne sisteme, da bi se lakše održavala. OSPF je ruting protokol, koji se može implementirati u autonomnim sistemima. OSPF omogućuje implementiranje dodatne hijerarhije koja se ne može ostvariti u RIP okruženjima. OSPF može napraviti podpodelu autonomnog sistema u grupe mreža koje se nazivaju oblasti. Mrežni broj identifikuje svaku oblast.

5.8 IS-IS [3]



Sl. 5.10. IS-IS

OSI protocol suite podržava brojne standardne protokole na svakom od sedam OSI slojeva. Prethodna slika prikazuje OSI protocol suite i njegov odnos sa slojevima OSI referentnog modela. *Intermediate System-to-Intermediate System (IS-IS)* je dinamički *link-state* ruting protokol za OSI protokol stek. Kao takav on distribuira ruting informacije za rutiranje

Connectionless Network Protocol (CLNP) podataka u *ISO Connectionless Network Service (CLNS)* okruženju.

Integrisan IS-IS je implementacija IS-IS protokola za rutiranje više mrežnih protokola. Integrisan IS-IS šalje CLNP rute sa informacijama koje se tiču IP mreže i *subnet*-a. On je alternativa za OSPF u IP okruženju, tj. mešavina ISO CLNS i IP rutiranja u jednom protokolu. Može biti korišćen isključivo za IP rutiranje, isključivo za ISO rutiranje ili za njihovu kombinaciju. OSPF s druge strane, podržava samo IP.

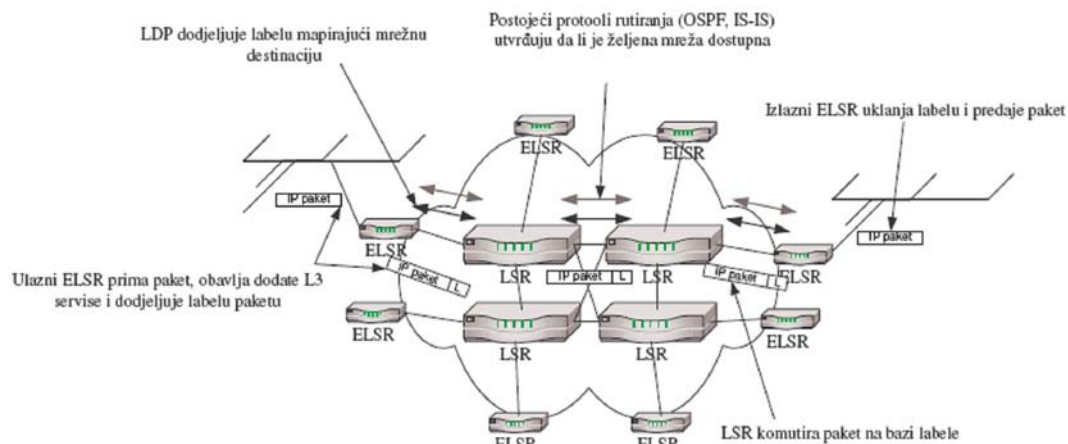
5.9 MPLS

Multiprotocol Label Switching (MPLS) kombinuje inteligentno rutiranje sa performansama svičinga. Ovaj protokol obezbeđuje značajne prednosti na mrežama sa čistom IP arhitekturom, kao i onima sa IP i ATM, ili kod mešavine drugih Layer 2 tehnologija. MPLS tehnologija je ključna za skalabilne *virtual private networks* (VPNs), *end-to-end* QoS. Ovo omogućava efikasno korišćenje postojeće mreže i budući rast kao i brzu korekciju prilikom otkazivanja nekog linka i čvora.

MPLS je standardizovan u sklopu aktivnosti IETF-a, i predstavlja pristup koji za prenos IP paketa koristi princip prosleđivanja na bazi labela. To znači da se umesto IP adrese za atribut usmeravanja i usluga koriste labele. Ulazni paketi se obrađuju na pristupnom delu MPLS mreže i tu im se dodeljuju odabrane labele. Ruteri jezgra mreže procesiraju samo labele, primenjuju odgovarajuće usluge i prosleđuju pakete na osnovu labela. Prema tome, analiza, filtriranje i utvrđivanje redosleda se vrše samo na ulaznom pristupnom delu. Na izlazu iz MPLS mreže labele se uklanjaju, a paketi se prosleđuju do odredišta na bazi nekog drugog protokola.

MPLS tehnologija podrazumeva upotrebu sledeće terminologije:

- **Ruter sa komutiranjem labela (Label Switch Router - LSR)** je uređaj u jezgru koji komutira pakete sa labelama u skladu sa unapred izračunatim tabelama komutiranja. U principu ovaj uređaj može biti ATM komutator (ATM - LSR) ili ruter (LSR).
- **Labela** je zaglavlje koje LSR koristi za prosleđivanje paketa, pri čemu format zaglavlja zavisi od osobina mreže. U mrežama sa ruterima koji koriste serijski pristup, LAN veze ili FR (Frame Relay) labela je 32-bitno odvojeno zaglavlje. U ATM mrežama labela je smeštena u VPI/VCI zaglavlju ćelije. U jezgru LSR čita samo labelu, ne zaglavlje paketa mrežnog sloja. Ključ prilagodljivosti MPLS-a je činjenica da labele imaju samo lokalno značenje između dva uređaja koja komuniciraju.
- **Ivični ruter sa komutiranjem labela (Edge label switch router – Edge LSR)** je uređaj koji obavlja početnu obradu i razvrstavanje paketa, te dodeljuje prvu labelu. Ovaj uređaj može biti ruter ili komutator sa ugrađenim sposobnostima usmeravanja.
- **Protokol distribucije labela (Label distribution protocol - LDP)** je protokol koji obezbeđuje dodjeljivanje labela u ivičnim i jezgrenim uređajima radi usklađivanja LSR-a sa protokolima rutiranja.



Sl. 5.11. Način rada MPLS-a

Najznačajnija prednost MPLS-a je sposobnost dodeljivanja labela koje imaju posebno značenje, tako da grupe labela razlikuju informacije potrebne za rutiranje, vrstu aplikacije i klasu usluge. MPLS labela se upoređuje sa unapred izračunatim tabelama komutiranja u uređajima jezgra koji sadrže L3 informaciju, dozvoljavajući svakom komutatoru da automatski primeni odgovarajuće IP servise na svaki paket. Tabele su unapred izračunate, tako da nema potrebe za obradu podataka pri svakom hopu. To ne samo da omogućava odvajanje raznih vrsta saobraćaja, npr saobraćaja “*best effort*” od vremenski kritičnog saobraćaja, već ujedno čini MPLS rješenje izuzetno prilagodljivim i nadogradivim. MPLS ne obavlja prosleđivanje po zaglavlju IP paketa jer koristi druge mehanizme dodele labela, koje imaju lokalno značenje. Na taj način je gotovo nemoguće ostati bez slobodnih labela. Ova osobina je osnovna u primeni naprednih IP servisa QoS, VPN i projektovanje saobraćaja.

6. PRIMER IZBORA RUTE NA CISCO RUTERIMA [4]

Tri procesa su uključena u pravljenje i održavanje ruting tabele na Cisco ruteru:

- različiti mrežni ili ruting protokoli kao što su EIGRP, BGP, IS-IS, i OSPF
- ruting tabela, koja prihvata informacije od ruting procesa i takođe odgovara na zahteve za informacijama od *forwarding* procesa
- *forwarding* procesi koji zahtevaju informacije iz ruting tabele da bi doneli odluku gde da forvarduju paket

6.1 Pravljenje ruting tabele

Kada svaki ruting proces dobije potrebne informacije, on bira najbolju putanju do neke date destinacije i pokušava da upiše tu putanju u ruting tabelu. Npr, ako EIGRP nauči putanju do 10.1.1.0/24, i odluči da je ova putanju najbolja EIGRP putanja do te destinacije, on pokušava da upiše naučenu putanju u ruting tabelu.

Ruter donosi odluku da li ili ne da upiše rutu koju mu je dostavio ruting proces na osnovu *administrative distance* koju ima data ruta. Ako ova putanja ima najnižu *administrative distance* do te destinacije (u poređenju sa ostalim rutama u tabeli), ruter je upisuje u ruting tabelu. Ako ova ruta nema najbolju *administrative distance*, onda se ona odbacuje.

Primer:

Pretpostavimo da ruter ima četiri aktivna ruting procesa: EIGRP, OSPF, RIP, i IGRP. Svaki od ovih procesa je naučio različite rute do 192.168.24.0/24 mreže, i svaki je odabrao najbolju putanju do te mreže preko svoje interne metrike i procesa.

Svaki od ova četiri procesa pokušava da upiše svoju rutu do 192.168.24.0/24 mreže u ruting tabelu. Svakom ruting procesu je dodeljena *administrative distance* koja se koristi za donošenje odluke koja će se ruta upisati.

Tabela 6.1. Default Administrative Distances

Default Administrative Distances	
Connected	0
Static	1
eBGP	20
EIGRP (internal)	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP (external)	170
iBGP	200
EIGRP summary route	5

Pošto internal EIGRP ruta ima najbolju *administrative distance*, ona se upisuje u ruting tabelu.

6.2 Backup Route

Pitanje je šta rade drugi protokoli RIP, IGRP i OSPF, sa rutama koje nisu upisane u tabelu? U slučaju kada prioriteta ruta, naučena od EIGRP otkáže, *Cisco IOS Software* ima dva pristupa za rešavanje ovog problema:

- Periodično, svaki ruting proces pokušava da upiše najbolju rutu. Ako prioriteta ruta otkáže, sledeća najbolja (na osnovu *administrative distance*) biva upisana u narednom pokušaju
- Druga opcija je da ruting protokol koji nije uspeo da upiše rutu u tabelu ostane pri toj ruti, ali prijavi da pokušaj upisa najbolje putanje u tabelu nije uspeo.

Kod protokola koji nemaju svoje informacije o ruting tabeli, kao što je IGRP, koristi se prva metoda i svaki put kada IGRP dobije *update* neke rute, on pokušava da je upiše u ruting tabelu. Ako već postoji ruta do te destinacije u ruting tabeli, pokušaj upisa ne uspeva.

Kod protokola koji imaju svoju bazu o ruting informacijama, kao što je EIGRP, IS-IS, OSPF, BGP i RIP, *backup* ruta se registruje kada inicijalni pokušaj upisa rute ne uspe. Ako neka ruta više nije u funkciji, iz nekog razloga, proces koji održava ruting tabelu poziva svaki proces ruting protokola koji ima backup rutu, i traži ponovno upisivanje rute u tabelu. Ako postoji više protokola sa registrovanim backup rutama, bira se ona sa najnižom *administrative distance*.

6.3 Menjanje Administrative Distance

Pošto *default administrative distance* nije uvek adekvatna moguće ju je izmeniti, ako npr. ako želimo da RIP rute imaju prednost nad IGRP rutama. Za sve protokole, promena distance je relativno jednostavna, koristi se ***distance*** komanda. Takođe je moguće promeniti distance za rute naučene od samo jednog izvora u nekim protokolima, ili promeniti distance samo nekih ruta. Kod statičkih ruta, menja se distance svake rute unošenjem distance nakon ***ip route*** komande:

ip route <network> <subnet mask> <next hop> <distance>

Moguće je promeniti administrative distance za sve statičke rute odjednom.

6.4 Dužina prefiksa

Još jedna uobičajena situacija kojom ruteri upravljaju odnosi se na menjanje dužine prefiksa. Pretpostavimo da ruter ima četiri aktivna ruting procesa i da je svaki proces dobio sledeće rute:

- EIGRP (internal): 192.168.32.0/26
- RIP: 192.168.32.0/24
- OSPF: 192.168.32.0/19

Pitanje je koja će od ovih ruta biti upisana u ruting tabelu? Pošto *EIGRP internal* ruta ima najbolju *administrative distance*, za pretpostaviti je da će ona biti upisana u tabelu. Ipak, pošto svaka od ruta ima različitu dužinu prefiksa (*subnet mask*), one uzimaju u obzir različite destinacije, pa će zato sve biti upisane u ruting tabelu.

6.5 Forwarding Decisions

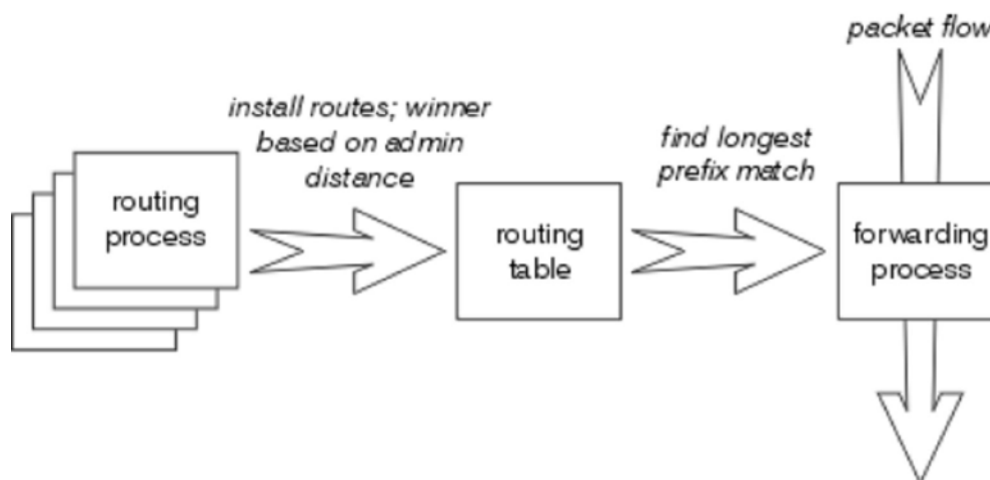
Primer upisanih ruta u ruting tabeli:

```
router#show ip route
....
D 192.168.32.0/26 [90/25789217] via 10.1.1.1
R 192.168.32.0/24 [120/4] via 10.1.1.2
O 192.168.32.0/19 [110/229840] via 10.1.1.3
....
```

Ako paket namenjen za 192.168.32.1 stigne na interfejs rutera, koju će rutu ruter izabrati? To zavisi od dužine prefiksa, ili broja bitova u *subnet mask*. Duži prefiksi uvek imaju prednost u odnosu na kraće kada je forvardovanje paketa u pitanju. U ovom slučaju, paket upućen za 192.168.32.1 se usmerava preko 10.1.1.1, zato što 192.168.32.1 prolazi do 192.168.32.0/26 mreži (192.168.32.0 do 192.168.32.63). Takođe, paket može da prođe koristeći i preostale dve rute, ali pošto 192.168.32.0/26 ima najveći prefiks u ruting tabeli, on se koristi.

Takođe, ako paket upućen za 192.168.32.100 dođe do nekog od interfejsa na ruteru, biće forvardovan do 10.1.1.2, pošto 192.168.32.100 nije u opsegu 192.168.32.0/26 (192.168.32.0 *through* 192.168.32.63), ali može da prođe koristeći 192.168.32.0/24 destinaciju (192.168.32.0 *through* 192.168.32.255). Paket je u opsegu i 192.168.32.0/19 mreže, ali 192.168.32.0/24 mreža ima duži prefiks.

Donošenje odluke o forvardovanju se sastoji od tri seta procesa: ruting protokola, ruting tabele, i samog procesa koji donosi odluku o forvardovanju i prebacivanju paketa.



Sl. 6.1. Forwarding Decisions

Ruta sa najdužim prefiksom uvek ima prednost u odnosu na ostale rute upisane u ruting tabeli, dok ruting protokol sa najnižom *administrative distance* uvek ima prednost kod upisa rute u ruting tabelu.

6.6 Forvardovanje paketa (Packet Forwarding) korišćenjem ARP (Address Resolution Protocol)

Primer: Korak po korak komunikacija između dva hosta na različitim mrežama.



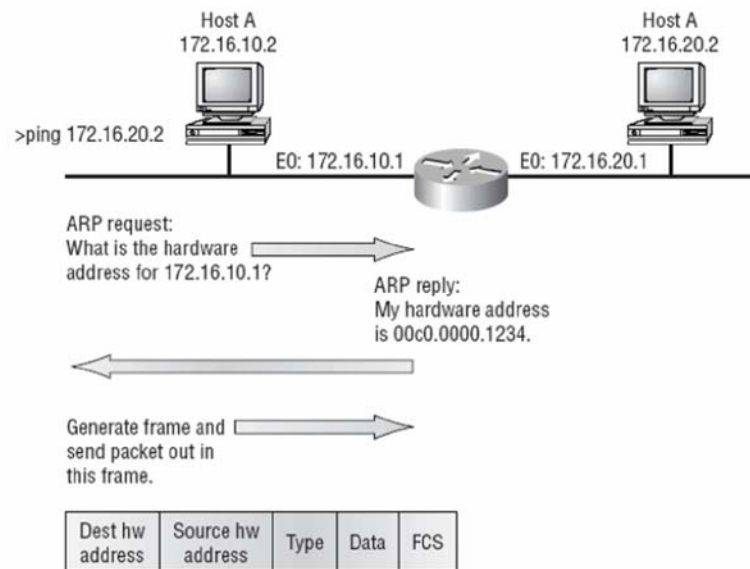
Slika 6.2. IP ruting primer (dva hosta i jedan ruter)

U primeru, korisnik kompjutera Host A pinguje IP adresu kompjutera Host B.

Koraci:

1. Iz command prompt-a, korisnik kuca ping 172.16.20.2. Paket se generiše na kompjuteru Host A korišćenjem IP i ICMP *Network layer* protokola.
2. IP sarađuje sa ARP protokolom da odrediti mrežu destinacije paketa tako što prvo utvrdi IP adresu i *subnet mask* računara Host A. Pošto je u pitanju paket za *remote host-a*, a ne za host-a na lokalnoj mreži, paket se šalje ruteru.
3. Da bi Host A poslao paket ruteru, mora da zna hardversku adresu interfejsa rutera koja je na lokalnoj mreži. *Network layer* (mrežni sloj) prosleđuje paket i hardversku adresu destinacije do Data Link sloja koji ih dalje prosleđuje ka *local host-u*. Da bi saznao hardversku adresu (MAC address), host pregleda memorijsku lokaciju zvanu *ARP cache*.

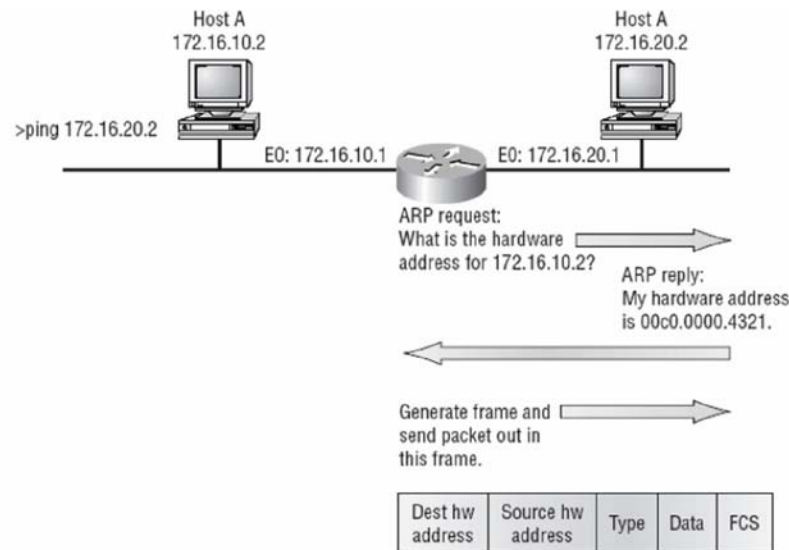
4. Ako IP adresa nije razrešena u hardversku adresu (MAC address) i ako je nema u ARP cache, host šalje ARP broadcast tražeći MAC adresu IP adrese 172.16.10.1.
5. Ruter odgovara i dostavlja MAC adresu mrežnog interfejsa koji je konektovan na lokalnu mrežu. Host sada ima sve neophodne podatke za slanje paketa do rutera. *Network layer* upućuje paket sa **Ping** zahtevom do Data Link sloja, zajedno sa MAC adresom odredišta. Paket uključuje početnu i krajnju IP adresu, kao i ICMP navedenim u *Network layer*-u.
6. *Data Link layer* kreira frejm, koji enkapsulira paket sa kontrolnom informacijom potrebnom za prenos na lokalnoj mreži. Ovo uključuje početnu i krajnju MAC adresu i tip polja specificiran *Network layer* protokolom. Na slici se vide sve informacije potrebne za komunikaciju sa ruterom: početna i krajnja MAC adresa, početna i krajnja IP adresa, podaci i CRC frejm u okviru *Frame Check Sequence (FCS)* polja.



Sl. 6.3. Frejm generisan od strane Host A

7. *Data Link layer* računara Host A, prosleđuje frejm do fizičkog sloja, koji kodira 1 i 0 u digitalni signal i šalje ih dalje.
8. Signal prima interfejs rutera Ethernet 0 i kada ugradi frejm, pokreće CRC i na kraju frejm, proverava FCS polje da se uveri da se CRC poklapaju i da nije došlo do kolizije ili fragmentacije.
9. Destinacija MAC adrese se proverava. Pošto se ona poklapa, polje tip u frejmu se proverava da bi se videlo šta će ruter uraditi sa paketom. IP je naravno u polju tip, i ruter prosleđuje paket do IP protokola. Frejm se odbacuje, i originalan paket koji je generisao Host A se sada nalazi u baferu rutera.
10. IP utvrđuje destinacionu IP adresu paketa da bi utvrdio da li je taj paket za taj ruter. Pošto je krajnja IP adresa 172.16.20.2, ruter u ruting tabeli pronalazi da je 172.16.20.0 direktno povezana mreža na interfejsu Ethernet 1.
11. Ruter smešta paket u bafer interfejsa Ethernet 1, zatim kreira frejm da bi poslao paket do krajnjeg hosta. Prvo, ruter proverava u ARP cache da li je MAC adresa razrešena. Ako nije, ruter šalje ARP broadcast do Ethernet 1 da bi otkrio MAC adresu za 172.16.20.2.
12. Host B šalje ARP *reply* sa svojom MAC adresom. Ethernet 1 interfejs na ruteru ima sve neophodne podatke krajnje destinacije paketa. Bez obzira da li se destinacija

MAC adrese menja na bilo kom interfejsu rutera, početna i krajnja IP adresa se ne menjaju. Paket se takođe ne menja, samo se frejm menja.



13. Host B dobija frejm i pokreće CRC. Nakon toga odbacuje frejm i predaje paket do IP. IP onda proverava krajnju IP adresu. Pošto krajnja IP adresa odgovara IP adresi Host B, proverava polje protokol da bi ustanovio svrhu paketa.
14. Pošto je paket ICMP *echo-request*, Host B generiše nov ICMP *echo-reply* paket sa početnom IP adresom Host B i krajnjom IP adresom Host A. Ceo proces počinje ponovo, samo u suprotnom smeru.

6.7 Primer tabele rutiranja kod Windows operativnog sistema

Tabela rutiranja se sastoji iz sledećih polja:

Network Destination: mrežni ID koji odgovara ruti. U ovom polju je moguće da budu: klasna adresa, podmreža, ili IP adresa hosta

Netmask: to je maska koja se koristi da odgovara određenoj adresi mrežne destinacije

Gateway: ovo polje se takođe naziva i polje prosleđivanja (forwarding) ili sledeći skok IP adrese za mrežno odredište. Skok (hop) je segment između rutera. Ako paket mora da prođe kroz dva rutera, to su dva skoka. To je adresa sledećeg rutera, koji sprovodi pakete izvan lokalne (pod)mreže.

Interface: IP adresa mrežne kartice koja se koristi za prosleđivanje IP podataka. Svaki ruter mora da ima najmanje dva interfejsa.

Metric: ovaj broj predstavlja relativnu cenu određene rute. Koristi se za određivanje najbolje rute, kada ima više mogućnosti. Uobičajeno, ruta sa najmanjim brojem skokova (broj rutera koji moraju da se prođu) ima najnižu metriku. Međutim, mrežni administrator može da podesi ovo polje da bi sprečio neki tip saobraćaja da koristi određene rute. Ako dve rute imaju isti *network destination* i *netmask*, ruta sa manjom metrikom će se koristiti.

Dodatno, pored ovih neophodnih elemenata, tabela rutiranja može da sadrži dodatne informacije. Naredna četiri polja obezbeđuju sledeće informacije:

Direktno vezane mrežne ID rute: koristi se za pakete čije je odredište lokalna ili povezana mreža. Ako su pošiljalac i primalac na istoj podmreži, paket se šalje ovom metodom.

Udaljene mrežne ID rute: koristi se za rute koje su dostupne indirektno, kroz druge rutere. IP adresa *gateway*-a je IP adresa lokalnog rutera koji se nalazi između čvora koji šalje pakete i udaljene mreže.

Host rute: to je ruta za određenu IP adresu. Ovo polje omogućava da se unese ruta za određeni računar i na taj način se paketi šalju na određenu IP adresu. Network destination je IP adresa željenog hosta i subnet maska je 255.255.255.255.

Default ruta: koristi se kada određena ruta ne može biti pronađena, kada nije moguće pronaći mrežni ID ili host rutu. Ona je definisana kao mrežni ID 0.0.0.0 i sa subnet maskom 0.0.0.0.

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>route print

IPv4 Route Table
=====
Interface List
=====
0x1 ..... MS TCP Loopback interface
0x10003 ...00 0c 29 72 a7 14 ..... AMD PCNET Family PCI Ethernet Adapter
=====

Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
-----
0.0.0.0                    0.0.0.0          192.168.1.5      192.168.1.1       30
127.0.0.0                  255.0.0.0        127.0.0.1        127.0.0.1         1
192.168.1.0                255.255.255.0    192.168.1.1      192.168.1.1       30
192.168.1.1                255.255.255.255  127.0.0.1        127.0.0.1        30
192.168.1.255             255.255.255.255  192.168.1.1      192.168.1.1       30
192.168.2.0                255.255.255.0    192.168.2.1      192.168.1.1       30
192.168.2.1                255.255.255.255  127.0.0.1        127.0.0.1        30
192.168.2.255             255.255.255.255  192.168.2.1      192.168.1.1       30
224.0.0.0                  240.0.0.0        192.168.1.1      192.168.1.1       30
255.255.255.255           255.255.255.255  192.168.1.1      192.168.1.1         1
Default Gateway:          192.168.1.5

Persistent Routes:
None

```

Sl. 6.4. Prikaz tabele rutiranja iz command prompt-a

6.8 Problemi zaštite tabele rutiranja [1]

Napadi bi se mogli svrstati u četiri kategorije napada:

- zlonamerna modifikacija tabele rutiranja
- modifikacija, falsifikovanje i replikacija paketa u čvorovima,
- napadi na QoS signalizacione protokole i
- odbijanje servisa – DoS (*Denial of Service*)

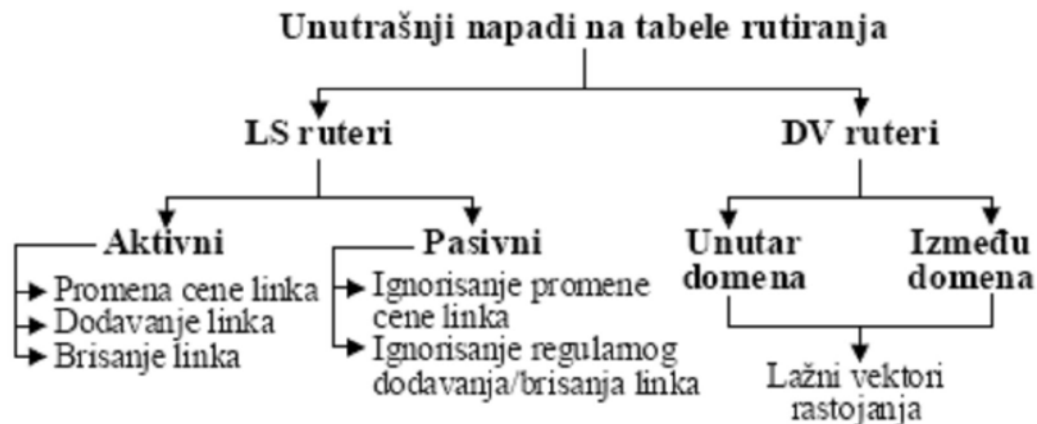
Zlonamerna modifikacija tabele rutiranja

Zlonamerna modifikacija tabele rutiranja vrši se unošenjem lažnih informacija u kontrolne pakete koje razmenjuju ruteri, na osnovu kojih se obavlja ažuriranje tabele rutiranja. Posledice takvih napada mogu biti: rutiranje po putanjama koje nisu optimalne, što prouzrokuje degradaciju QoS i/ili "krađu resursa" (propusnog opsega, memorijskog prostora rutera) za pojedine klase saobraćaja, kreiranje veštačkih particija koje su izolovane od ostatka mreže, formiranje petlji, DoS za pojedine klase saobraćaja, otkrivanje sadržaja informacija ("prisluškiivanje") usled prolaza kroz deo mreže koji nije predviđen za prenos te klase saobraćaja i dr. Napadi na tabele rutiranja i moguće tehnike zaštite u IP QoS mrežama mogu se generalno klasifikovati slično kao u tradicionalnim IP mrežama.

Za većinu LS i DV protokola rutiranja definisane su tehnike zaštite od spoljnih napada, kojima se zapravo sprečava neovlašćen pristup mrežnim linkovima. Mehanizmi zaštite od spoljnih napada su:

- Primena tehnika digitalnog potpisa za zaštitu integriteta i utvrđivanje verodostojnosti kontrolnih poruka, među kojima su najpoznatija rešenja zasnovana na javnim kriptografskim ključevima (*Public Key Infrastructure*). U tom slučaju svaki ruter poseduje par kriptografskih ključeva – privatni i javni. Ruter koji generiše kontrolni paket potpisuje taj paket svojim privatnim ključem, a ostali ruteri mogu da verifikuju potpis pomoću javnog ključa. Definišu se metodi distribuiranja sertifikovanih informacija o svakom ruteru i javnim ključevima.
- Obeležavanje kontrolnih poruka rednim brojevima ili vremenskim pečatima, radi zaštite od promene redosleda ili replikacije kontrolnih poruka. Validnost poruke proverava se pomoću brojača kontrolnih poruka ili mehanizama vremenske kontrole.

Drugu vrstu napada na tabele rutiranja predstavljaju unutrašnji napadi, koje vrše ruteri koji su i sami napadnuti (tzv. kompromitovani ruteri). U zavisnosti od tipa protokola, takvi ruteri mogu generisati različite vrste napada. Napadi na LS rutere mogu biti aktivni, kada kompromitovani ruter menja cenu linka, dodaje nepostojeći link ili briše regularan link, ili pasivni, kada kompromitovani ruter ignoriše regularne promene stanja linkova. U napadima na DV rutere, kompromitovani ruter formira lažne vektore rastojanja i šalje ih susednim ruterima, koji prihvataju ove podatke, pošto nema načina da utvrde verodostojnost porekla vektora rastojanja.



Sl. 6.5. Unutrašnji napadi na tabele rutiranja

Zaštita od unutrašnjih napada na LS rutere može se vršiti pomoću dve klase rešenja:

1. Centralizovani sistem za otkrivanje napadača, u kome modul za analizu detektuje napade na osnovu određenog kriterijuma, kao što su sekvence alarma.
2. Implementacija mehanizama za detekciju napada u samom LS protokolu, koja se zasniva na potvrđivanju kontrolnih poruka za ažuriranje stanja linkova.

Zaštita od napada na DV rutere može se vršiti pomoću procedure za proveru doslednosti, u svakom ruteru, pri čemu se tabele rutiranja proširuju podacima o čvoru koji prethodi svakom odredištu i broju hop-ova do svakog odredišta.

Modifikacija, falsifikovanje i replikacija paketa u čvorovima

Ova vrsta napada vrši se modifikacijom paketa, generisanjem lažnih paketa ili replikacijom paketa sa korisničkim informacijama. Iako ima ograničene efekte zbog toga što obično pogađa samo određeni segment mreže, glavni problem je što je ove napade teško detektovati. U multiservisnim IP mrežama ovaj tip napada najčešće prouzrokuje degradaciju QoS, a u nekim slučajevima i DoS.

Modifikacija paketa markiranjem za niži prioritet prouzrokuje opsluživanje paketa u čvorovima mreže sa većim kašnjenjem ili manjim težinskim faktorom, zavisno od primenjene discipline, usled čega se povećava kašnjenje i džiter. U uslovima opasnosti od zagušenja, povećava se verovatnoća odbacivanja paketa, usled primene neadekvatno konfigurisanih mehanizama za upravljanje redovima. Usled krađe resursa moguća je degradacija QoS i za pakete koji su regularno markirani za niži prioritet.

Modifikacija paketa markiranjem za viši prioritet prouzrokuje krađu resursa paketima koji su regularno markirani za viši prioritet, što je posebno nepovoljno ako se propusni opseg za dati prioritet rezerviše unapred.

Generisanje lažnih paketa i replikacija paketa mogu da ugroze i servise viših i nižih prioriteta. Pošto se potpuno zaobilaze mehanizmi kontrole ulaznog saobraćaja, postoji opasnost od zagušenja pojedinih linkova i, indirektno, odbijanja servisa ako se nekontrolisano velike količine saobraćaja usmeravaju prema odredištu koje je žrtva napada.

Standardizovano rešenje zaštite od modifikacije, falsifikovanja i replikacije paketa u tradicionalnim IP mrežama su IPSec protokoli – skup otvorenih IETF standarda koji obezbeđuju kriptografske zaštitne mehanizme za IP pakete. Standardizovana su dva protokola:

1. *ESP (Encapsulating Security Protocol)* koji obezbeđuje poverljivost, integritet, utvrđivanje verodostojnosti porekla paketa i zaštitu od replikacije.
2. *AH (Authentication Header)* koji obezbeđuje integritet, utvrđivanje verodostojnosti i zaštitu od replikacije paketa.

I ESP i AH mogu da funkcionišu u dva režima rada: transportnom i tunelskom. U transportnom režimu rada se servisi zaštite primenjuju samo na protokole viših slojeva od IP-a. U tunelskom režimu rada obavlja se enkapsulacija originalnog IP paketa u novi IP datagram, a IPSec zaglavlje se smešta između spoljnog i unutrašnjeg IP zaglavlja. Funkcije zaštite primenjuju se, prema tome, na celokupan originalni IP paket.

Servisi poverljivosti i integriteta podataka zahtevaju tajne kriptografske ključeve zajedničke za par rutera, koji se mogu distribuirati manuelno ili dinamički. *IPSec* specificira protokol za dinamičko uspostavljanje ključeva – *IKE (Internet Key Exchange)*. Tokom ugovaranja *IKE*, obe strane usaglašavaju metod utvrđivanja verodostojnosti, algoritme šifriranja i hash algoritam koji će biti korišćen za generisanje zajedničkih kriptografskih ključeva. Ako se *IKE* uspešno ugovori, omogućeno je kreiranje jednosmerne zaštitne asocijacije (*SA – Security Association*), po kojoj se realizuju servisi zaštite posredstvom *IPSec* protokola.

Napadi na QoS signalizacione protokole

QoS signalizacioni protokoli su zaduženi za dinamičko ugovaranje QoS između provajdera servisa i korisnika, razmenu informacija u procesu kontrole pristupa (*admission control*) novih tokova saobraćaja u mrežu i razmenu QoS upravljačkih informacija između upravljačke stanice i elemenata mreže.

Napadi na QoS signalizacione protokole mogu obuhvatati: lažno predstavljanje napadača, koje omogućava nelegitiman pristup određenom profilu saobraćaja, modifikaciju signalizacionih poruka promenom zahtevanog/odobrenog prioriteta za dati tok IP saobraćaja ili ugovorenih karakteristika date klase QoS i DoS napade, sa tehnikama sličnim kao i za druge protokole (videti poglavlje II.D).

Obavezne mere zaštite od napada na QoS signalizacione protokole obuhvataju utvrđivanje verodostojnosti porekla signalizacionih poruka i zaštitu integriteta poruka.

Odbijanje servisa – DoS

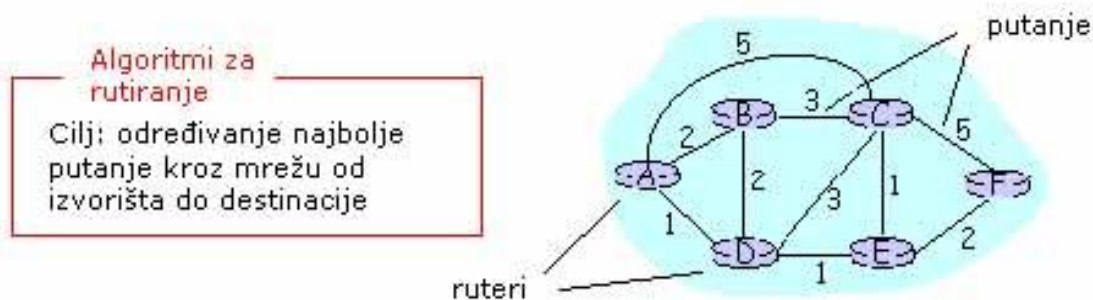
U tipičnom DoS napadu, napadač falsifikuje IP adresu izvora saobraćaja i koristi infrastrukturu mreže da uputi velike količine saobraćaja odredištu koje predstavlja metu. Efekat napada se uvećava ako se koriste distribuirani napadači (tzv. "agenti"), koji istovremeno napadaju ciljni server, što može potpuno da spreči pristup jednog broja korisnika mreži. U multiservisnim mrežama, cilj DoS napada može da bude potpuno blokiranje servisa za određene klase saobraćaja. DoS se događa i kao posledica drugih tipova napada. Moguća rešenja zaštite mogu se klasifikovati na preventivna i reaktivna.

Preventivne tehnike se zasnivaju na nekoj prethodnoj informaciji pomoću koje se sprečava napad. Vrlo su značajna rešenja koja sprečavaju da napadač identifikuje operative sisteme mrežnih uređaja (tzv. "uzimanje otiska prsta" – fingerprinting), što predstavlja uvod u napade na infrastrukturu mreže. Noviji pristup zaštite su tzv. "čistači" (scrubbers) protokola – aktivni mehanizmi koji se mogu implementirati u okviru *firewall* sistema, a u realnom vremenu uklanjanju ključeve na osnovu kojih se može identifikovati operativni sistem nekog mrežnog uređaja.

Cilj reaktivnih tehnika zaštite je da identifikuju napadača kada je napad već izvršen. Ovo je, takođe, jedno od aktivnih područja istraživanja, jer su postojeće tehnike zaštite najčešće manuelne i mogu da traju veoma dugo.

7. ALGORITMI ZA RUTIRANJE

Pošto je ruterima neophodna informacija o mreži i mrežama, kako bi mogli da donesu odluku o daljem prosleđivanju, ove odluke se donose upoređivanjem destinacionih adresa sa adresama u tabelama rutiranja. Sistem za rutiranje selektuje zapis iz tabele rutiranja i određuje masku mreže za taj zapis. Zatim se vrši logičko I (AND) na ovoj vrednosti i destinacionoj adresi. Rezultujuća vrednost se upoređuje sa adresama mreža u tabeli rutiranja. Ako su dve vrednosti iste znači da je destinacija dostupna kroz prolaze koji su definisani u tom zapisu. Ako se te dve vrednosti razlikuju sistem za rutiranje ispituje sledeći zapis u tabeli. Ako je cela tabela pregledana i ako nema zapisa koji se poklapaju, obično je rezultat takav da se paket odbacuje i generiše se poruka koja obaveštava da je destinaciona mreža nedostupna. Već je pomenuto da se u tu svrhu koriste algoritmi za rutiranje. **Namena rutera nije da samo proslede pakete na datu adresu, već i da odrede najbolju, najefikasniju i najbržu putanju.** Kada se kaže najbolja putanja, tu se misli na skokove (sledeći skok= IP adresa drugog hosta ili rutera koji su direktno dostupni ili preko Eterneta, serijske veze ili neka druga fizička konekcija), zatim na vreme za koje će paket putovati i troškove tog prosleđivanja. Takođe, za putanju se koristi takozvani IP adresni prefiks. IP adresni prefiks je skup destinacija za koje je ruter validan. Adresni prefiks se sastoji od 0 do 32 značajna bita.



SI. 7.1. Ilustracija rutiranja

Da bi se izbeglo unošenje svih mogućih putanja na svetu na jednom mestu, većina rutera i hostova koristi takozvanu default putanju (na primer, neke tabele rutiranja sadrže samo tu putanju).

Posmatrano na koji način ruter određuje najbolju putanju, imamo dve vrste algoritama za rutiranje. To su:

- Globalni algoritam za rutiranje
- Lokalni algoritam za rutiranje

U lokalnom modelu svaki ruter ima informaciju o ruterima koji su direktno vezani za njega, dakle nema informacije o svim ruterima na mreži. Ovi algoritmi su takođe poznati kao DV-Distance vector algoritmi.

U globalnim algoritmima za rutiranje, svaki ruter ima kompletne informacije o svakom ruteru u mreži. Ovi algoritmi su takođe poznati kao LS-Link state algoritmi.

7.1 LS algoritmi

U LS algoritmima svaki ruter mora da obavlja sledeće radnje:

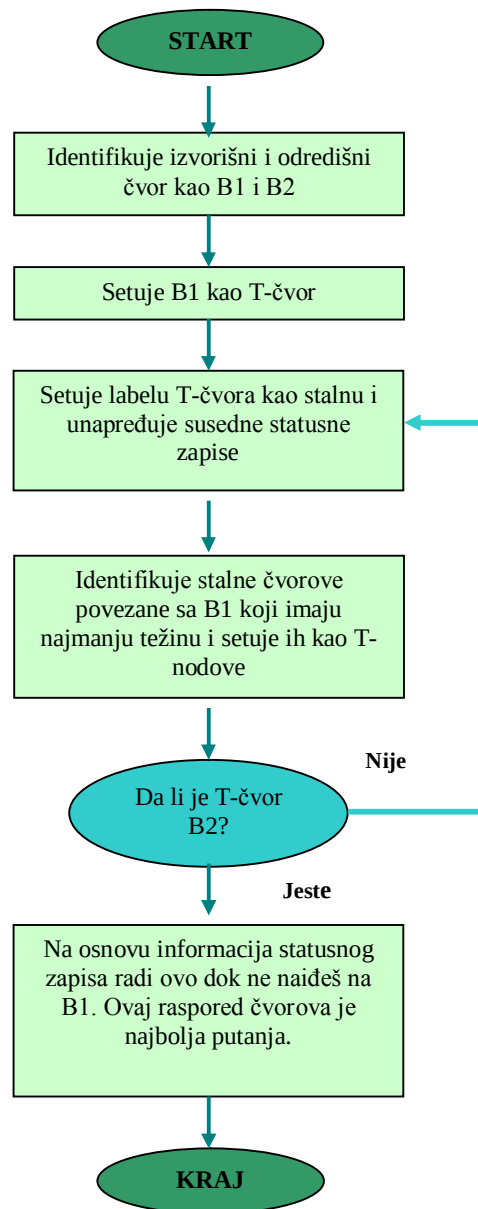
1. Identifikuje rutere koji su fizički povezani sa njim i pronalazi njihove IP adrese. Kada se ruter pokrene, on prvo šalje tzv. pozdravni paket ("hello packet") kroz mrežu. Svaki ruter koji primi taj paket uzvraća sa eho paketom. Na ovaj način ruter takođe meri vreme koje je potrebno paketu da stigne do destinacije i vrati se nazad.
2. Šalje svoje informacije preko mreže ostalim ruterima i prihvata informacije o ostalim ruterima na mreži. U ovom koraku, svi ruteri dele informacije međusobno, tako da svaki ruter poznaje strukturu i status mreže.
3. Koristeći odgovarajući algoritam, identifikuje najbolji put između dva čvora u mrežama. U ovom koraku, ruteri pronalaze najbolju putanju za svaki čvor u mreži.

Primer za ovo je Dijkstra algoritam. U ovom algoritmu, ruter na osnovu informacija o stanju na mreži sastavlja graf mreže. Ovaj graf pokazuje lokacije rutera i njihovu međusobnu povezanost. Svaka veza je označena sa brojem koji se zove težina (*weight*) ili cena (*cost*). Ovaj broj predstavlja funkciju vremena putanje, prosečne zauzetosti mreže i ponekad jednostavno broj skokova (*hops*) između čvorova. Na primer, ako imamo dve veze između izvorišta i destinacije, ruter će izabrati putanju sa manjom težinom.

Dijkstra algoritam [6] prolazi kroz sledeće korake:

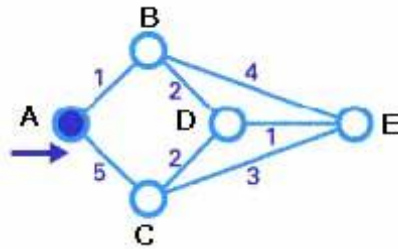
1. Ruter pravi graf mreže i identifikuje odredišne i izvorišne čvorove, na primer B1 i B2. Zatim gradi tzv "matricu susedstva" ("*adjacency matrix*"). U toj matrici koordinate predstavljaju težinu. Na primer, matrica [i,j] predstavlja težinu između čvorova B1 i B2. Ako ne postoji direktna veza između ova dva čvora, ova težina je označena kao beskonačna.
2. Zatim ruter pravi statusni zapis za svaki čvor u mreži. Zapis sadrži tri polja:
 - o Prethodno polje- Ovo prvo polje prikazuje prethodni čvor
 - o Polje za dužinu- Drugo polje pokazuje sumu težina od odredišta do tog čvora.
 - o Polje za labelu- Poslednje polje sadrži status čvora.Svaki čvor može imati dva stanja: trajno ili probno.
3. Ruter inicijalizuje parametre statusnog zapisa (za sve čvorove) i njihove dužine određuje na beskonačne a labele na probne.
4. Ruter setuje tzv. T-čvor. Na primer, ako je B1 izvorišni T-čvor, ruter labelu datog čvora definiše kao trajnu. Kada labela dobije oznaku "trajna", nikad se više ne menja. T-čvor se ponaša kao agent.
5. Ruter unapređuje probne zapise za sve probne čvorove koji su direktno povezani sa izvornim T-čvorom.
6. Ruter gleda u sve probne čvorove i bira one kojima je težina sa B1 čvorom najmanja. Taj čvor sada postaje destinacioni T-čvor.
7. Ako taj čvor nije B2 (nameravana destinacija), ruter se vraća na 5. korak.

8. Ako taj čvor jeste B2, ruter navodi prethodni čvor iz statusnog zapisa sve dok ne naiđe na B1. Ova lista čvorova prikazuje najbolju putanju od čvora B1 do čvora B2. Ovi koraci su dati u sledećem prikazu:

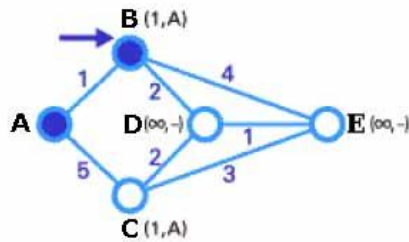


Primer: U ovom slučaju želimo da nađemo najbolju putanju između tačaka A i E. Može se videti da postoje šest mogućih ruta između A i E tačaka (ABE, ACE, ABDE, ACDE, ABDCE i ACDBE), i da je očigledno da je ABDE najbolja putanja zato što je njena težina najmanja. Ali koristimo algoritam da bi pronašli najbolju putanju.

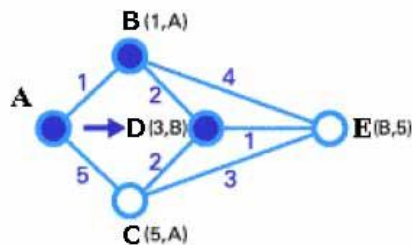
1. Kao što se vidi na donjoj slici, izvorišni čvor (A) je izabran za T-čvor, tako da je njegova labela obeležena kao stalna (stalni čvorovi su prikazani punim krugovima a T-čvorovi simbolom -->).



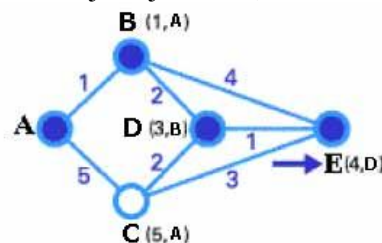
2. U sledećem koraku, vidi se da je statusni zapis stalnog čvora direktno vezanog za T-čvor (B,C) promenjen. Takođe, pošto B ima manju težinu on je odabran kao T-čvor i njegova labela je izabrana kao stalna.



3. U ovom koraku, kao i u koraku 2., statusni zapis privremenog čvora koji ima direktnu vezu sa T-čvorom (D,E) se menja. Takođe, budući da D ima manju težinu on je izabran za T-čvor i njegova labela se menja u "stalni čvor".



4. U ovom koraku nema više privremenih čvorova, tako da se samo identifikuje sledeći T-čvor. Pošto E ima najmanju težinu, on se identifikuje kao T-čvor.



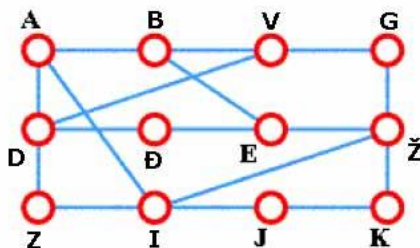
5. Pošto je E destinacija, ovde se zaustavljamo.

Kada smo došli do kraja, treba da se identifikuje putanja. Prethodni čvor čvora E je D, a njegov prethodnik je B, dok je prethodnik čvora B je A. Dakle, najbolja putanja je ABDE. U ovom slučaju, celokupna dužina je 4 (1+2+1).

Bez obzira što ovaj algoritam radi dobro, on je isuviše komplikovan tako da ruteru treba mnogo vremena da procesuiraju datu putanju i samim tim efikasnost mreže opada. Takođe, ako ruter ostalim ruterima pošalje pogrešne informacije, njihove naredne odluke neće biti validne. Međutim, ovaj algoritam je dobar kao primer koji pokazuje princip određivanja putanje.

7.2 DV algoritmi

Kao što smo ranije naveli, Distance Vector algoritmi spadaju u lokalne algoritme. DV algoritmi su takođe poznati kao Belman-Ford rutirajući algoritmi i Ford-Fulkerson algoritmi. U ovim algoritmima svaki ruter ima tabelu rutiranja koja pokazuje najbolju putanju za svaku destinaciju. Tipični graf i tabela rutiranja za ruter I:



Sl. 7.2 Tipičan graf rutiranja

Tabela 7.1. Tabela rutiranja za ruter I

Destinacija	Težina	Linija
A	8	A
B	20	A
V	28	I
G	2	Ž
D	17	I
Đ	30	I
E	18	Ž
Ž	12	Ž
Z	10	I
I	0	---
J	6	K
K	15	K

Kao što je u tabeli prikazano, ako ruter I želi da pošalje paket ruteru G, treba da ga pošalje prvo do rutera Ž. Kada paket stigne do rutera Ž, on proverava svoju tabelu rutiranja i odlučuje kako da šalje paket do rutera D.

Kod DV algoritama, svaki ruter mora da odradi sledeće korake:

1. Broji težine za sve veze sa kojima je direktno spojen i te informacije čuva u svojoj tabeli.
2. U specifičnim periodima vremena, ruter šalje svoju tabelu ka susednim ruterima (ne svim ruterima) i prima tabele rutiranja ostalih rutera.
3. Na osnovu informacija dobijenih od susednih rutera, on unapređuje i konfigurira svoju tabelu.

Pre nego što se formira tabela rutiranja, formira se tzv. tabela razdaljina, gde svaki red sadrži svaku moguću destinaciju a kolona svaku direktno-spojeni susedni čvor. Primer za dobijanje tabele razdaljina:

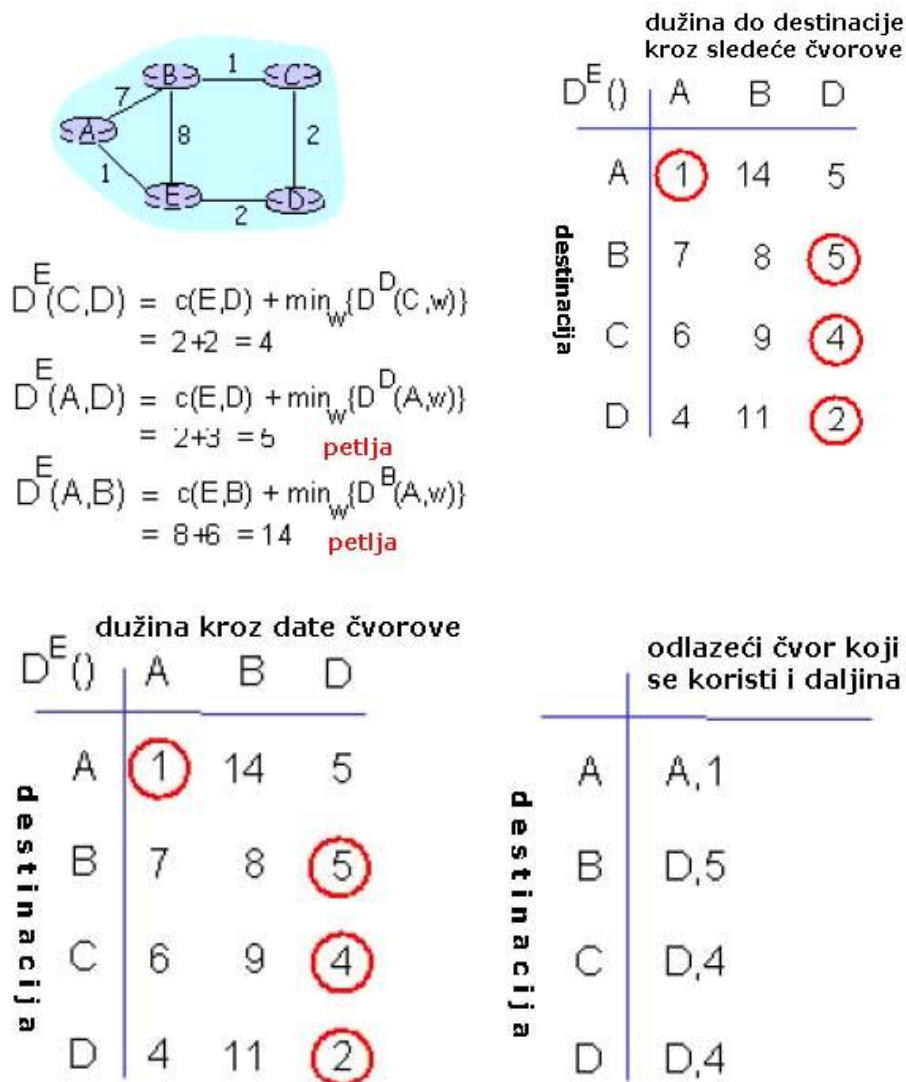


Tabela razdaljina → **Tabela rutiranja**

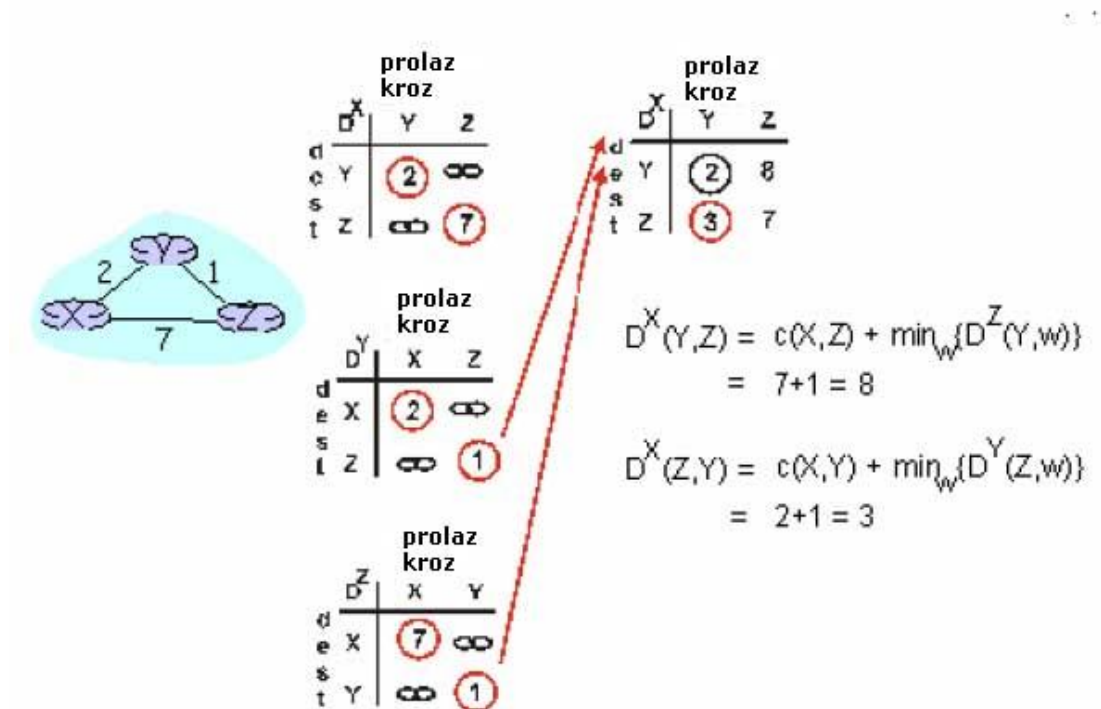
Sl. 7.3. Primer tabele razdaljina

Prethodni primer prikazuje putanje od izvorišta E do C i od E do A preko čvora D, kao i od E do A preko B. Vidimo tabelu razdaljina, koja prikazuje razdaljine od rutera (čvora) E do čvorova A, B, C i D preko čvorova A, B i D. Na osnovu tabele razdaljine, formira se tabela rutiranja jer tabela rutiranja mora da nastane na osnovu nekog prethodnog analiziranja mreže.

Lokalna poruka od susednog rutera se dobija u slučaju samo ako je nešto promenjeno. U tom slučaju, svaki čvor obaveštava susedni čvor. To može da se pojasni pomoću dijagrama toka:



Primer formiranja tabela razdaljina:



Sl. 7.4. Formiranje tabele razdaljina

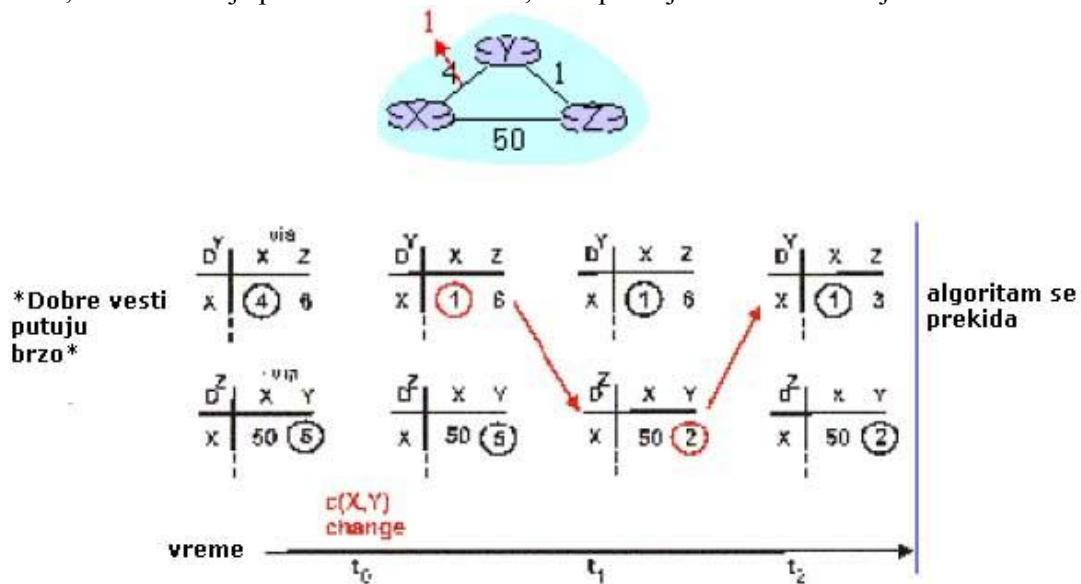
U ovom primeru se mogu uočiti tri čvora, X, Y, Z. Između njih se nalaze različite dužine (2, 1, 7). Na osnovu njih, i pomoću DV algoritma određuje se tabela razdaljina.

Sam vektorski algoritam (Distance vector algorithm) bi izgledao na sledeći način:

1. Inicijalizacija:

2. za sve susedne čvorove v:
3. $DX(*,v) = \text{infinity}$ /operator * znači "za sve redove"/
4. $DX(v,v) = c(X,v)$
5. za sve destinacije, y
6. pošalji $\min WDX(y,w)$ svakom susedu / W preko svih suseda od X /
7. petlja
8. **wait** (until ne vidim promenu dužine za suseda V
9. **or until** (ne dobijem promenu od suseda V)
- 10.
11. **if** ($c(X,V)$ se promeni od strane d)
12. / promeni dužinu svim destinacijama kroz susedni V od strane d/
13. / napomena: d može biti pozitivno ili negativno /
14. za sve destinacije y: $DX(y,V) = DX(y,V) + d$
- 15.
16. **else if** (promeni primljene od strane čvora V i destinacije Y)
17. / kraći put od V do čvora Y je promenjen /
18. / V je poslao novu vrednost za njegov $\min WDV(Y,w)$ /
19. / zovi ovu novoprimljenu vrednost kao "newval"
20. za pojedinačnu destinaciju y: $DX(Y,V) = c(X,V) + \text{newval}$
- 21.
22. **if** imamo novu $\min WDX(Y,w)$ za bilo koju destinaciju Y
23. pošalji novu vrednost $\min WDX(Y,w)$ svim susedima
- 24.
25. **forever**

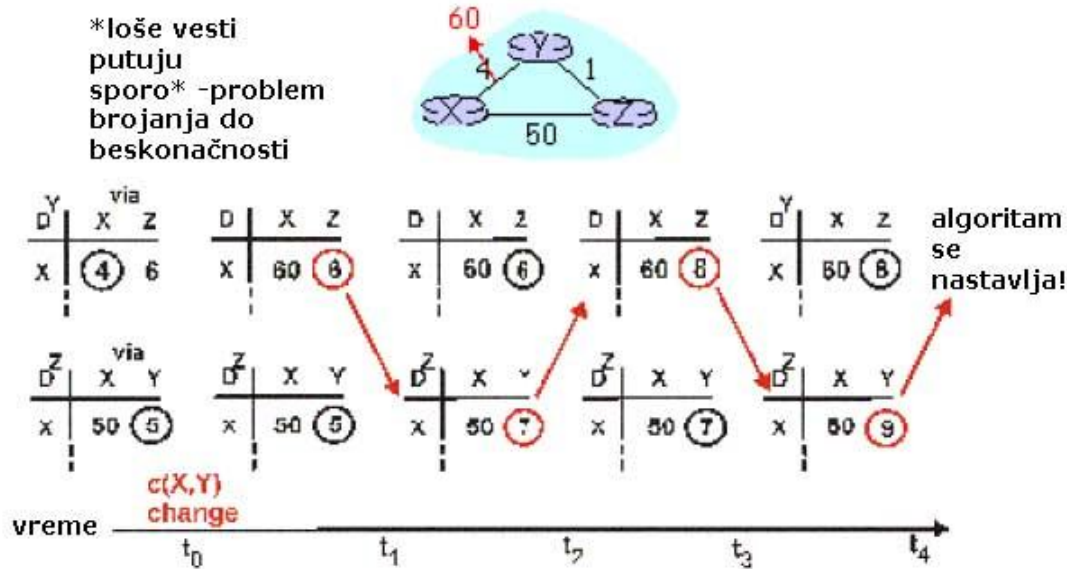
Dakle, čvor detektuje promenu lokalne veze, i unapređuje se tabela razdaljina.



Sl. 7.5. "Dobre vesti putuju brzo"

U ovom primeru je opisana mreža sa tri čvora (rutera) X, Y i Z. Tabela razdaljina se menja, jer se razdaljina tj. težina između čvorova X i Y promenila sa 4 na 1. Zato se to i naziva "dobre vesti putuju brzo", jer se dužina promenila na bolje.

Sledeći primer nam prikazuje šta se dešava kada se dužina pogorša:



Sl. 7.6. "Loše vesti putuju sporo"

Dakle, u ovom slučaju dužina između X i Y se promenila sa 1 na 60. Ovo pogoršanje utiče na celokupnu efikasnost algoritma, i može se nazvati "loše vesti putuju sporo". U krajnjoj distanci, to dovodi do problema koji se zove "brojanje do beskonačnosti", što će biti objašnjeno u sledećem primeru.

Jedan od najvećih problema sa DV algoritmima se zove "brojanje do beskonačnosti". Problem ćemo najbolje uočiti u sledećem primeru:

	A	B	V	G
A	0,-	1,A	2,B	3,C
B	1,B	0,-	2,C	3,D
V	2,B	1,C	0,-	1,C
G	3,B	2,C	1,D	0,-

Pretpostavimo da je veza između A i B presečena. U tom momentu, ruter B ispravlja svoju tabelu. Posle specifičnog vremena, ruteri međusobno razmenjuju njihove tabele, tako da ruter B prima tabelu rutera V. Pošto ruter V nema informacije o raskidu između A i B, on saopštava da je povezan sa A težinom 2 (1 od V do B, i 1 od B do A). Dakle, on nema informaciju o raskidu između A i B. B prima ovu tabelu i zaključuje da postoji veza između V i A, tako da ispravlja svoju tabelu i menja vrednost "beskonačno" u 3 (1 za B do V, i 2 za V do A, kao što mu je V saopštio). Ponovo, ruteri razmenjuju svoje tabele.

Kada V primi tabelu od B, uočava da je B promenio težinu za vezu do A sa 1 na 3, tako da V unapređuje svoju tabelu i menja težinu za vezu do A na 4 (1 za V do B, i 3 za B do A, kako je B saopštio). Ovaj proces se nastavlja sve dok svi čvorovi spoznaju da je težina veze do A beskonačna. U ovom slučaju, kaže se da DV algoritmi imaju sporo pritanje (*slow convergence rate*).

Jedan od načina da se ovaj problem reši jeste da ruteri šalju informacije samo do susednih rutera čije veze nisu ekskluzivne do destinacija. Na primer, u ovom slučaju, V ne bi trebao da šalje do rutera B nikakve informacije o ruteru A, zato što je put preko B jedini put do A.

Takođe, razvijeni su i algoritmi koji rešavaju ovaj problem. Nazivi tih algoritama (korišćenih od strane RIP protokola) su *split horizon* (razdvojeni horizonti) i *triggered updates*.

Algoritam "razdvojeni horizonti" se koristi za izbegavanje problema izazvanih uključivanjem putanja u nove informacije poslate ruterima od kojih je putanja i dobijena. To se postiže izbegavanjem putanja dobijenih od susednih uređaja u obnavljanju informacija koje su poslate istom tom susednom uređaju. U prethodnom primeru, gde je presečena veza između A i B, i ako A želi da stigne do npr. G, onda A treba da obavesti B da on ne može da stigne do G, tako da će B znati da ne postoji putanja od A do G. Ovo je slučaj za tačka-tačka veze. Ali ako zamislimo da su A i G povezani preko neke brodkast mreže, na primer *Eterneta*, i postoje drugi prolazi između te dve lokacije. U tom slučaju, A treba da objavi nepovezanost sa G svim gateway uređajima na toj mreži. Ti ostali gateway uređaji sami mogu dopreti do destinacije G, ali nikad preko A, jer je veza prekinuta. Ovaj način je dobar jer se šalje brodkast informacija svim ruterima, što umnogome pojednostavljuje ceo proces. Na primer, ako imamo neki kampus čija kičma (*backbone*) je povezana sa različitim zgradama, u svakoj zgradi se nalazi gateway koji povezuje kičmu sa lokalnim mrežama. Ako nastane neki problem sa kičmom, ruteri međusobno razmenjuju informacije, i lokalne mreže moraju znati jedino da li su priključeni na nju.

Algoritam "razdvojenog horizonta" je dobar u slučaju ako imamo samo 2 gateway uređaja. **Problem:** stanica A veruje da ima sigurnu putanju kroz B, B kroz V, a V kroz G. Algoritam "razdvojeni horizont" ne može sprečiti pojavu petlje u ovom primeru. Tu se primenjuje tzv. trigerovanje (*triggered updates*). Ovaj algoritam za otklanjanje problema kod rutiranja se zasniva na pravilu da svaki put kad ruter menja metriku za rutiranje, potrebno je da pošalje poruku o tome istog momenta, iako možda nije vreme za slanje regularnih poruka. Na primer, ako putanja do tačke P ide kroz ruter M. Ako neko novo obaveštenje dođe od rutera M, onda ruter P mora da veruje novoj informaciji. Ako nova informacija donosi neke novine u algoritmu, ruter P šalje svim svojim stanicama nove informacije. Dalje ove stanice (ili ruteri) šalju nove informacije svojim susednim stanicama, i tako dalje. Rezultat je kaskada trigerovanih dobavljanja novih informacija. Lako je prikazati koji ruteri i koje stanice su obuhvaćene ovim algoritmom. Pretpostavimo da se prekinula putanja između rutera A i B. A ruter će poslati nove informacije svim susednim ruterima. Naime, susedni ruteri koji će jedini verovati novim informacijama su oni na putanji između A i B. Ostali ruteri (koji nisu na ovoj putanji) neće prihvatiti ovu novu informaciju jer će je smatrati lošijom od njihovih trenutnih, tako da će je ignorisati. Susedni ruteri koji su na putanji od A do B će prihvatiti nove informacije i poslati njihovim susednim stanicama. Ponovo, samo stanice koje se nalaze na datoj putanji će uzimati u obzir nove informacije. S toga, nove informacije o putanjama će biti prosleđivane kroz sve puteve koji vode do rutera 2, unapređujući metriku do beskonačnosti. Ova propagacija će se završiti dok ne dođe do dela mreže čija destinacija do rutera B vodi nekim drugim putem.

Ako bi sistem (tj. mreža) bio u mogućnosti da ništa ne radi dok se vrši ažuriranje novih informacija, problem brojanja do beskonačnosti ne bi postojao. Istovremeno, loše putanje

bi bile eliminisane i nikakve petlje koje usporavaju ili zaustavljaju rutiranje ne bi bile formirane.

Međutim, dok se triggerovane informacije momentalno šalju, i regularni *update* se dešava u isto vreme. Ruteri koji su primili regularne informacije, a nisu primili nove (*triggerovane*) informacije, će ostalim ruterima i stanicama slati podatke o putanjama koje ne postoje. Moguće je i da ruter koji je primio *triggerovane* informacije ponovo dobije neki normalni update od rutera koji nije primio *triggerovane* informacije. Ovo može ponovo uspostaviti pogrešnu i netačnu putanju. Ako se *trigerski update* obavi dovoljno brzo, ovo se neće desiti. Ipak, brojanje do beskonačnosti je još uvek moguće.

7.3 Hijerarhijsko rutiranje (Hierarchical Routing)

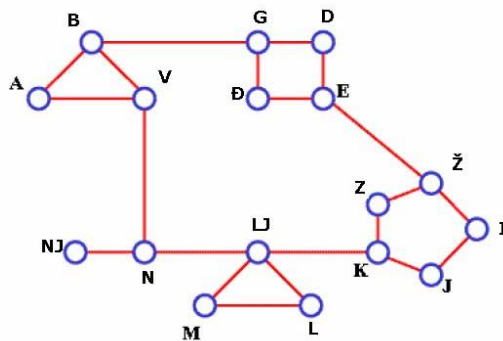
Kako rastu mreže, proporcionalno rastu i tabele rutiranja. Ne samo da se troši memorija rutera na tabele koje se neprestano povećavaju, već je potrebno i više procesorskog vremena da ih pregleda i više propusnog opsega za slanje izveštaja o njihovom stanju. Kada mreže narastu do određene tačke, više neće biti izvodljivo da svaki ruter ima zapis o svakom drugom ruteru, pa rutiranje treba sprovesti na hijerarhijski način.

U hijerarhijskom rutiranju ruteri su raspodeljeni u regije i svaki ruter zna sve detalje o rutiranju paketa u okviru svoje regije, ali ne zna ništa o unutrašnjoj strukturi drugih regija. Kada se različite mreže međusobno spoje, prirodno je proglasiti svaku posebnom regijom, kako bi se ruteri jedne mreže oslobodili potrebe poznavanja topologije drugih mreža. Kod velikih mreža dvonivovska hijerarhija može biti nedovoljna. Tad je potrebno regije podeliti u grozdove, grozdove u zone, zone u grupe, itd. dok postoji potreba da daljim deljenjem.

Primer: Koristićemo **DV** (*distance vector*) algoritam za pronalaženje najbolje putanje između dva čvora. U ovom primeru svaki čvor u mreži mora da zapamti tabelu rutiranja sa 17 zapisa. Dat je tipičan graf mreže i tabela rutiranja za ruter A:

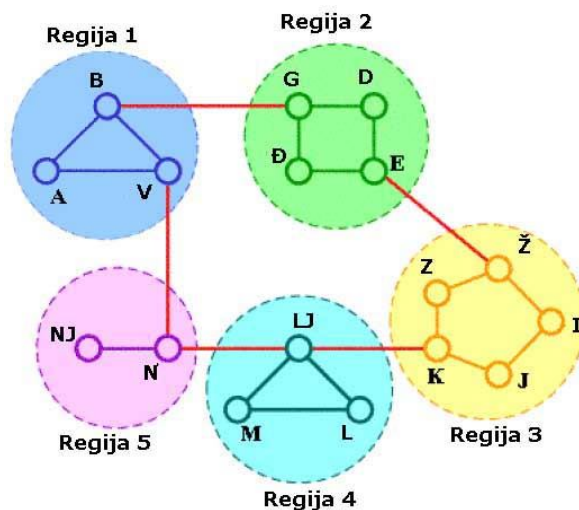
Tabela 7.2. Tabela rutiranja za ruter A

Destinacija	Linija	Težina
A	---	---
B	B	1
V	V	1
G	B	2
D	B	3
Đ	B	3
E	B	4
Ž	B	5
Z	V	5
I	V	6
J	V	5
K	V	4
L	V	4
LJ	V	3
M	V	4
N	V	2
NJ	V	3



Sl. 7.7. Tipičan graf mreže

U hijerarhijskom rutiranju, ruteri su klasifikovani u grupe poznate kao regioni. Svaki ruter ima samo informacije o svom regionu i nema informacija o ostalim regionima. Ruteri čuvaju samo jedan zapis u njihovim tabelama o ostalim regionima. Na primer, mrežu smo podelili u 5 regiona:



Sl. 7.8. Regije kod hijerarhijskog rutiranja

Tabela 7.8. Regije kod hijerarhijskog rutiranja

Destinacija	Linija	Težina
A	---	---
B	B	1
V	V	1
Region 2	G	2
Region 3	D	2
Region 4	D	3
Region 5	D	4

Ako ruter A želi da pošalje pakete prema bilo kom ruteru u regiji 2 (G, D, \ ili E) on ih šalje prema B, i tako dalje. Kao što se može videti, u ovoj vrsti rutiranja tabele mogu biti ukratko prikazane što dodatno povećava efikasnost mreže. Prethodni primer prikazuje dvo-nivovsko hijerarhijsko rutiranje.

7.4 Rutiranje emisijom (Broadcast Routing) [6]

U nekim aplikacijama, hostovi treba da pošalju poruke velikom broju hostova ili čak svima. Slanje paketa svim odredištima istovremeno zove se difuzna emisija (*broadcasting*). Postoje razne metode kojima se to može učiniti. Zbog jednostavnosti, u daljem toku rada koristiće se termin emisija (*broadcast*).

Jedan metod koji ne zahteva specijalne karakteristike pod mreže je jednostavno slanje različitog paketa svakom odredištu. Ovo ne samo da troši mnogo propusnog opsega, već zahteva i da izvor ima kompletnu listu odredišta. U praksi može biti jedina mogućnost, ali je svakako najmanje poželjna.

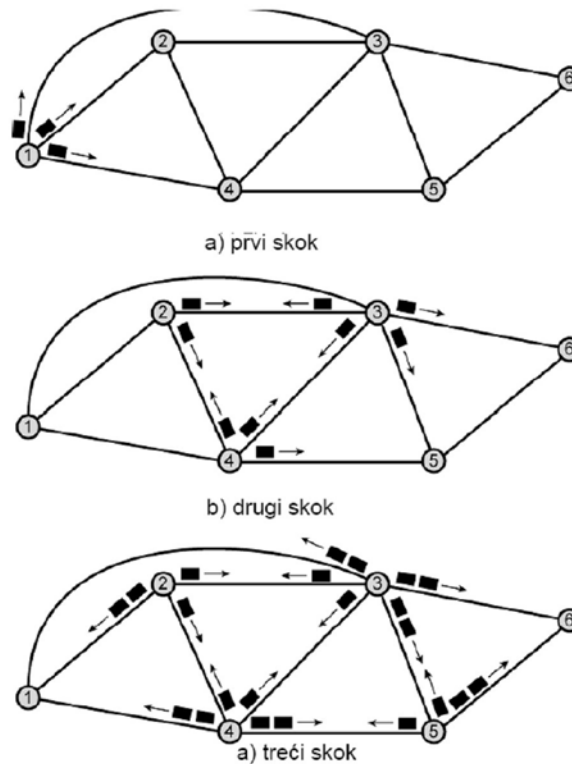
Flooding (plavljenje) je još jedan metod koji se može koristiti. Kod plavljanja se ne zahteva informacija o mreži, a šema radi na sledeći način. Od strane izvorišnog čvora paket se šalje svakom od susednih čvorova. Kod svakog čvora, dolazeći paket se retransmituje na sve izlazne linkove (veze) sa izuzetkom linka po kojem je primljen. Na primer, ako čvor 1 na slici 7.9a) treba da pošalje paket ka čvoru 6 on predaje kopiju tog paketa (sa odredišnom adresom 6), ka čvorovima 2, 3 i 4. Čvor 2 slaće kopiju čvorovima 3 i 4. Čvor 4 slaće kopiju čvorovima 2, 3 i 5. Proces predaje se dalje nastavlja na istom principu. Eventualno veći broj kopija paketa će stići u čvor 6. Svaki paket mora da ima jedinstveni identifikator (tj. izvorišni čvor i redosledni broj, ili broj virtuelnog kola i redosledni broj) tako da čvor 6 zna da eliminiše sve pristigle pakete, istog tipa, sa izuzetkom prve kopije.

Sa ciljem da se spreči neprekidna retransmisija paketa, tj. da se broj paketa koji cirkuliše (onih paketa čija je predaja inicirana od strane jedinstvenog izvorišnog čvora) povećava bez ograničenja, svaki čvor treba da pamti identitet onih paketa koje je već retransmitovao. Za slučaj da pristignu duplikati paketa isti se izbacuju. Jednostavnija tehnika je da se u svakom paketu uvede polje tipa brojač-preskoka. Brojač se početno postavlja na neku maksimalnu vrednost, kakav je dijametar (najveći broj preskoka u mreži) mreže. Svaki put kada paket predje kroz čvor brojač se dekrementira za jedan. Kada brojač dostigne vrednost 0, paket se eliminiše. Primer zadnje taktike prikazan je na slici 7.9. Paket se šalje od čvora 1 ka čvoru 6, a polje brojača preskoka se postavlja na vrednost 3. Kod prvog preskoka, kreiraju se tri kopije paketa. Kod drugog preskoka kreiraju se ukupno 9 kopija. Jedna od ovih kopija stigne do čvora 6, koji prepoznaje da je to za njega i on ne vrši njenu dalju retransmisiju. Ipak ostali čvorovi generišu ukupno 22 nove kopije za treći konačni preskok. U slučaju da čvor ne čuva trag o identifikatoru paketa, on može da generiše veći broj kopija u trećem koraku (stepenu). Svi paketi primljeni u trećem preskoku se eliminišu. Sve u svemu, čvor 6 je primio još 4 dodatne kopije paketa.

Tehniku plavljenja karakterišu sledeće osobine:

- Pokrivene su sve moguće rute između izvorišta i odredišta. Nezavisno od toga koji je link ili čvor u kvaru, paket će uvek pristići do njega pod uslovom da postoji najmanje jedan put između izvorišta i odredišta
- S obzirom da su sve rute pokrivene, najmanje jedna kopija paketa će pristići na odredište, a prva će biti ona koja je koristila rutu sa najmanjim brojem preskoka (pod uslovom da je prenos idealan (bez greške u prenosu) i da je brzina prenosa podataka po svim rutama isti).
- Do svih čvorova, koji su direktno ili indirektno povezan na izvorišni čvor, je stigla poruka.

Zbog svoje prve osobine, tehnika plavljenja je veoma robusna i najčešće se koristi za prenos hitnih poruka. Glavni nedostatak plavljenja je veliki saobraćaj koji ova tehnika generiše i što je taj saobraćaj direktno proporcionalan povezljivosti mreže.



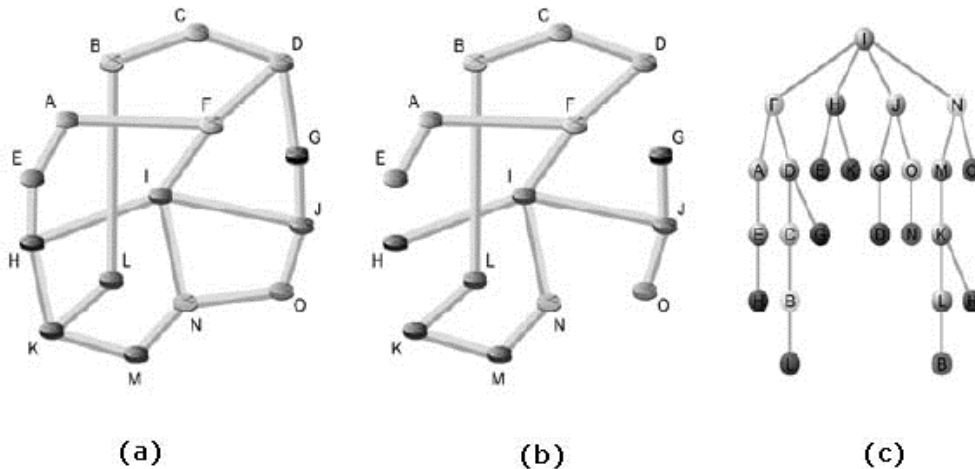
Sl. 7.9. Primer tehnike plavljenja

Treći algoritam je višedređišno rutiranje (*multidestination routing*). Svaki paket sadrži listu odredišta ili bitmapu sa označenim odredištima. Kada paket stigne u ruter, ruter proverava sva odredišta kako bi odredio skup izlaznih linija koje će koristiti (izlazna linija se koristi ako je to najbolja putanja do bar jednog odredišta). Ruter generiše novu kopiju paketa za svaku izlaznu liniju koju koristi i uključuje u svaki paket samo ona odredišta za koja koristi tu liniju. Dakle, skup odredišta je podeljen među izlaznim linijama. Nakon dovoljnog broja skokova, svaki paket će nositi samo jedno odredište i tretiraće se kao običan paket. Višedređišno rutiranje je slično odvojeno adresiranim paketima, osim što kad nekoliko paketa slijedi istu putanju, samo jedan zauzima propusni opseg.

Četvrti algoritam koristi *sink* stablo rutera koji inicira emisiju, ili neko drugo pogodno *spanning* stablo. *Spanning* stablo je podskup podmreže koji uključuje sve rutere, ali ne sadrži petlje. Ako svaki ruter zna koje njegove linije pripadaju *spanning* stablu, on može da kopira pristigli emisioni paket na sve linije *spanning* stabla osim na onu sa koje je stigao paket. Ovaj metod odlično koristi propusni opseg, generišući minimalan broj paketa potrebnih za obavljanje posla. Jedini problem je što svaki ruter mora poznavati strukturu *spanning* stabla da bi metod bio primenljiv. Ponekad je ova informacija pristupačna (npr. link state routing), a nekad ne (npr. distance vector routing).

Poslednji algoritam je pokušaj da se proceni ponašanje prethodnog algoritma, čak i ako ruteri ne znaju baš ništa o *spanning* stablu. Ideja, nazvana prosleđivanje reverznom

putanjom (*reverse path forwarding*) je veoma jednostavna. Kada emisioni paket dospe u ruter, on proverava da li je paket stigao linijom koja se obično koristi za slanje paketa izvoru emisije. Ako je tako, velike su šanse da je emisioni paket takođe pratio najbolju putanju i da je, prema tome, prva kopija pristigla u ruter. U ovom slučaju ruter prosleđuje njegove kopije na sve linije sem na onu sa koje je stigao paket. Ako je, međutim, emisioni paket stigao drugom linijom, paket se odbacuje kao verovatni duplikat.



Sl. 7.10. Prosleđivanje reverznom putanjom (a) Podmreža. (b) Sink stablo (c) Prikaz rada algoritma

Primer ovog algoritma prikazan je na slici 7.10. Deo (a) pokazuje podmrežu, deo (b) sink stablo, a deo (c) prikazuje funkcionisanje algoritma. Na prvom skoku, ruter I šalje pakete ka F, H, J i N. Svaki od ovih paketa stiže najboljom putanjom do I i to je označeno krugom oko slova. Na drugom skoku, osam paketa se generiše, dva od svakog rutera koji je primio paket u prvom skoku. Kako se ispostavlja, svih 8 stižu na dosad neposećene rutere, a 5 od njih stiže najboljom putanjom. Od 6 paketa generisanih u trećem skoku, samo 3 stižu najboljom putanjom; ostali su duplikati. Posle 5 skokova i 24 paketa, emisija se prekida. Četiri skoka i 14 paketa su pratili sink stablo.

Osnovna prednost algoritma *reverse path forwarding* je u tome da je istovremeno veoma efikasan i lak za implementaciju. Ne zahteva se znanje rutera o *spanning* stablima. Nema pretrpanu listu odredišta, a ni bitmapu u svakom odredišnom paketu, kao što to zahteva višedrežno adresiranje. Takođe nije potreban nikakav specijalni mehanizam za zaustavljanje procesa, kao kod poplave.

7.5 Rutiranje višestrukim usmeravanjem (Multicast Routing) [6]

Neke aplikacije zahtevaju da prilično razdvojeni procesi rade zajedno u grupi, npr. grupa procesa koja implementira sistem distribuiranih baza podataka. U ovakvim situacijama, često je neophodno da jedan proces pošalje poruku ostalim članovima grupe. Ako je grupa mala, svakom članu može se poslati tačka-tačka poruka. Međutim, ako je grupa velika, ova strategija je skupa. Ponekad se može koristiti emisija, ali koristiti emisiju za obaveštenje 1000 računara na mreži sa milion čvorova je neefikasno, jer većina čvorova nije zainteresovana za poruku (ili možda još gore; veoma su zainteresovani, ali ne treba da je vide). Prema tome, potreban je način za slanje poruka precizno definisanim grupama, koje imaju mnoštvo članova, ali su male u poređenju sa mrežom kao celinom.

Slanje poruke takvoj grupi zove se višestruko usmeravanje (*multicasting*). Pri tom se koristi algoritam za rutiranje višestrukim usmeravanjem (*multicast routing*). Za ovu tehniku neophodno je upravljanje grupama. Potreban je neki način stvaranja i brisanja grupa, kao i način da se omogući procesima da se priključuju grupama, i da ih napuštaju.

Kad se neki proces priključi određenoj grupi, veoma je bitno da obavesti svog hosta o tome. Od velike je važnosti da ruteri znaju koji od njihovih hostova pripada kojoj grupi. Ili hostovi obaveštavaju rutere o promenama svojih grupa ili ruteri periodično ispituju svoje hostove. Ruteri obaveštavaju svoje susede o tome, pa se informacije šire mrežom. Da bi se obavilo ovakvo rutiranje, svaki ruter izračunava svoje *spanning* stablo. Npr. na slici 7.11 (a) imamo dve grupe, 1 i 2. Neki ruteri su priključeni na hostove koji pripadaju jednoj ili obe grupe. *Spanning* stablo za krajnji levi ruter možete videti na slici 7.11 (b).

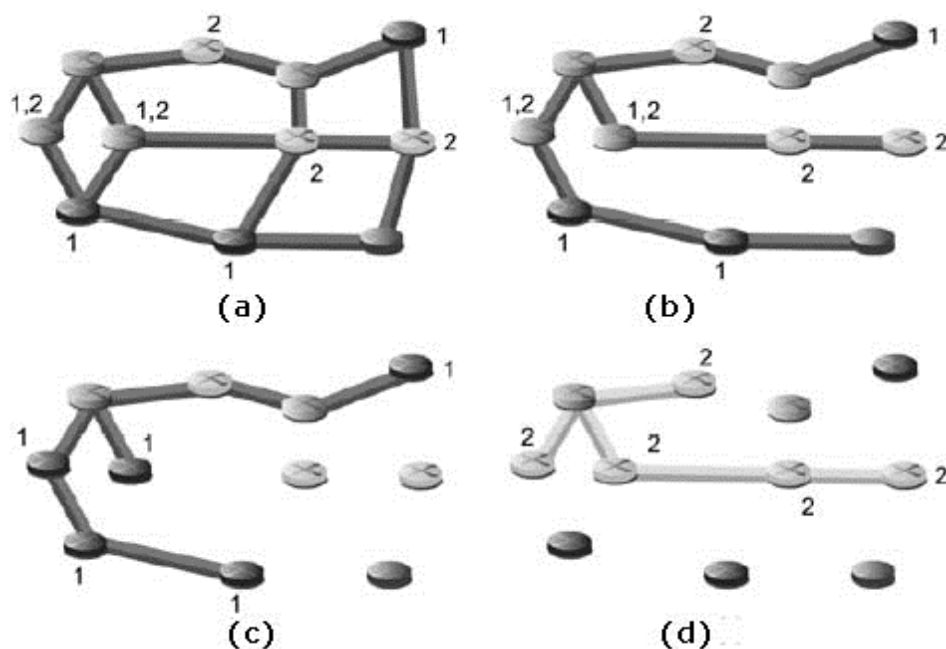
Kad proces pošalje grupi paket za *multicast*, prvi ruter pregleda svoje *spanning* stablo i skraćuje ga, odstranjujući one linije koje ne vode do hostova koji su članovi grupe. Slika 7.11 (c) prikazuje skraćeno *spanning* stablo za grupu 1. Slično, slika 7.11 (d) prikazuje isto za grupu 2. *Multicast* paketi se prosleđuju samo duž odgovarajućeg *spanning* stabla.

Razni načini skraćivanja *spanning* stabla su mogući. Najjednostavniji način koristi se kod rutiranja pomoću stanja veza. Tu je svaki ruter svestan kompletne topologije mreže, uključujući i to koji hostovi pripadaju kojim grupama. *Spanning* stablo se skraćuje, krećući od kraja svake putanje prema korenu, uklanjajući sve rutere koji ne pripadaju traženoj grupi.

Kod *distance vector routing* primenjuje se drugačija strategija. Osnovni algoritam je *reverse path forwarding*. Kad god ruter bez hostova zainteresovanih za određenu grupu i bez veza sa drugim ruterima, primi *multicast* poruku za tu grupu, on odgovara sa **PRUNE** porukom, kojom daje do znanja pošiljaocu da mu više ne šalje poruke za tu grupu. Na ovaj način, podmreža se rekurzivno skraćuje.

Jedan potencijalni nedostatak ovog algoritma je da se slabo prilagođava velikim mrežama. Pretpostavimo da mreža ima n grupa, od kojih svaka ima u proseku m članova. Za svaku grupu, u memoriji treba čuvati m skraćenih *spanning* stabala, što je ukupno mn stabala. Ako postoji mnogo velikih grupa, potreban je ogroman prostor za čuvanje svih informacija.

Alternativno, može se računati jedno stablo po grupi, sa korenom (jezgrom) blizu središta grupe (*core-based* stabla). Da bi poslao *multicast* poruku, host je šalje jezgru, koje to čini umesto njega. Iako nije optimalno za sve čvorove, smanjenje memorijskih troškova sa m stabala na jedno stablo po grupi je značajna ušteda.



Sl. 7.11. (a) Mreža. (b) Razgranato stablo 1 za krajnji levi ruter, (c) Stablo za grupu 1
(d) stablo za grupu 2

8. KOMPONENTE I RADNI MODOVI RUTERA (CISCO®) [2]

8.1 Interne komponente rutera

ROM

ROM se koristi za čuvanje ruterovog *bootstrap* (početno punjenje) startup programa, OS softvera, i *power-on* test.

Flash Memory

Ona čuva imidž operativnog sistema. Flash memorija se može brisati. Flash sadržaj ostaje kada se ruter isključi ili restartuje.

RAM

RAM se koristi za čuvanje operativnih informacija kao što su ruting tabele, ruterov konfiguracioni fajl. RAM takođe ima mogućnost keširanja i *packet buffering*. Njegov sadržaj se gubi prilikom restarta ili isključivanja rutera.

NVRAM

NVRAM (postojan RAM), se koristi za čuvanje ruterovog startup konfiguracionog fajla. Podaci se ne gube prilikom isključivanja.

Mrežni interfejsi

Mrežni interfejsi su locirani na matičnoj ploči ili na odvojenim modulima. Ethernet ili Token Ring interfejsi se konfigurišu da bi se omogućila LAN konekcija. Sinhroni serijski interfejs se konfiguriše da bi se omogućila WAN konekcija. Takođe se može konfigurisati ISDN BRI interfejs da bi se omogućila konekcija putem ISDN WAN.

8.2 Eksterne komponente

Ruter se može konfigurisati preko bilo kog mrežnog interfejsa. Konfiguracione informacije mogu se poslati ruteru preko:

- TFTP servera: Trivial File Transfer Protocol, pojednostavljene verzije FTP koja omogućava da fajlovi budu prebačeni sa jednog kompjutera na drugi preko mreže,
- virtuelnog terminala
- računara za network menadžment

8.3 Startup procedura

Svaki put kada se uključi, ruter prolazi kroz power-on self-test dijagnostički proces proveravajući osnovne operacije CPU, memorije i mrežnih interfejsa. Sistem vrši inicijalno

punjenje softvera u ROM (*boot image*) izvršava i traži važeći ruterov operativni sistem (*Cisco® IOS* imidž). IOS je akronim za *Internetwork Operating System*.

Postoje tri mesta sa kojih se može učitati *Cisco® IOS* imidž:

- fleš memorija
- TFTP server na mreži
- ROM

Lokacija *Cisco® IOS* imidža se utvrđuje iz boot polja u konfiguracionom registru rutera.

8.4 Konfigurisanje registra

16-bit registar određuje kako će se ruter butovati, gde je IOS imidž, kako postupati sa NVRAM konfiguracijom, podešavanje *console baud rate* (*brzina u bodima*) i da li je *break* funkcija omogućena ili onemogućena. *Default* podešavanja za konfiguraciju registra ukazuju da ruter treba da pokuša da učitava *Cisco® IOS* sa fleš memorije. Ako ruter pronađe validan IOS imidž, on traži validan konfiguracioni fajl. Ukoliko ne postoji validan sistemski imidž ili je konfiguracioni fajl oštećen, sistem će običi NVRAM podešavanja i ući u *ROM monitor mode*. Ovakav pristup ruteru je moguć i kada je izgubljen pasvord.

Konfiguracioni fajl, koji se čuva u NVRAM, se učitava u memoriju i izvršava se linija po linija. Konfiguracione komande pokreću proces rutiranja, dodeljuju adrese interfejsima, i setuju medija karakteristike. Ako konfiguracioni fajl ne postoji u NVRAM, OS izvršava inicijalnu konfiguracionu rutinu koja se zove *system configuration dialog*. Ovaj specijalni mod se naziva *Setup mode*.

Skripta za podešavanje predstavlja seriju pitanja koja služe za dobijanje inicijalne konfiguracije rutera. Svako pitanje ima i odgovarajući podrazumevani odgovor koji se nalazi u zagradi. Primer listinga nekih pitanja pri prvom startovanju rutera dat je u prilogu.

8.5 Cisco CLI Komandni modovi (*Cisco® CLI Command Modes*)

Cisco® IOS softver omogućava nekoliko različitih komandnih modova. Svaki od njih ima određenu grupu komandi.

Cisco® Command Line Interface (CLI) se naziva **EXEC**. **EXEC** ima dva moda:

- *user mode*
- *privileged mode*

Iz razloga bezbednosti svrha ova dva moda se odnosi na nivo pristupa *Cisco® IOS* komandama. *EXEC user* naredbe omogućavaju:

- konektovanje na udaljeni uređaj
- vršenje privremenih izmena u *terminal settings*
- pregled sistemskih informacija

Ukoliko se želi pristup privilegovanom modu mora se uneti lozinka. Komande dostupne u *Privileged mode* takođe uključuju i one iz *User mode*. *Privileged EXEC* komande se koriste za:

- podešavanje osnovnih parametara
- detaljan pregled statusa rutera

- testiranje i *debug* operacija koje izvodi ruter
- pristup globalnom i ostalim konfiguracionim modovima

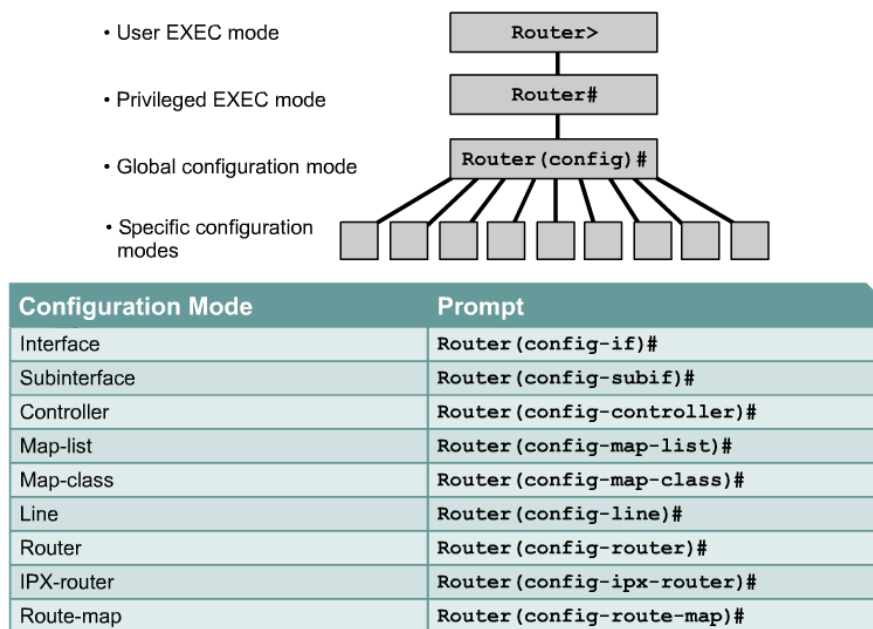
Iz *Privileged mode* može se pristupiti konfiguracionom modu. Ovaj mod omogućava pristup konfiguracionim komandama koje se odnose na ceo sistem, i ostalim konfiguracionim modovima. Kao lokacija konfiguracionih komandi može se navesti:

- terminal
- memorija
- mreža

Iz *Global Configuration mode* može se pristupiti drugim modovima i vršiti razna dodatna podešavanja.

Setup Mode: Ako ruter nema konfiguracioni fajl kada se uključi, onda automatski ulazi u Setup mode. Setup mode pokreće dijalog, pod nazivom *system configuration dialog*, preko koga se vrši inicijalna konfiguracija.

Rom Monitor Mode: Ako ruter ne pronađe validan imidž operativnog sistema, ili ako se prekine *boot* sekvenca, sistem može ući u ROM monitor mod. Iz ovog moda može se butovati uređaj ili izvoditi dijagnostički testovi.



Sl. 8.1. Cisco® CLI Command Modes

Pregled show komandi:

- **show interfaces** – Prikazuje statistiku svih interfejsa na ruteru. Da bi se videla statistika određenog interfejsa, unosi se **show interfaces** komanda praćena imenom interfejsa i brojem porta
- **show controllers serial** – Prikazuje hardverske informacije interfejsa
- **show clock** – Pokazuje podešeno vreme na ruteru

- **show hosts** – Prikazuje *cache* listu imena i adresa hostova
- **show users** – Prikazuje sve user-e konektovane na ruter
- **show history** – Prikazuje istoriju prethodno unetih komandi
- **show flash** – Prikazuje informacije u vezi sa flash memorijom i IOS fajl koji se tu čuva
- **show version** – Prikazuje informacije u vezi sa ruterom i IOS koji se nalazi u RAM
- **show ARP** – Prikazuje ARP tabelu rutera
- **show protocol** – Prikazuje globalan i status interfejsa sa konfigurisanim Layer 3 protokolima
- **show startup-configuration** – Prikazuje konfiguraciju koja se nalazi u NVRAM
- **show running-configuration** – Prikazuje konfiguraciju koja se trenutno nalazi u RAM

```

Router>show interface ethernet 0
Ethernet0 is administratively down, line protocol is down, using hub 0
Hardware is Lance, address is 0010.7b3a.cf84 (bia 0010.7b3a.cf84)
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 01:05:35, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 input packets with dribble condition detected
 63 packets output, 11676 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
Router>

```

Data link encapsulation (Ethernet-II) points to Encapsulation ARPA.

Status points to administratively down, line protocol is down.

MAC Address points to 0010.7b3a.cf84.

Routing metric information points to rely 255/255, load 1/255.

ARP cache entries timer points to ARP Timeout 04:00:00.

Sl. 8.2. Show interfaces <interface> command.

9. ZAKLJUČAK

Značaj rutiranja informacija je izuzetan u društvima koja funkcionišu i opstaju na osnovu pouzdane isporuke elektronskih informacija. Rutiranje predstavlja glavni proces kojim se izvodi prenos informacija sa jedne na drugu lokaciju. Čak i globalna ekonomija je zavisna od mogućnosti rutiranja informacija iz jednog sistema u drugi.

Sa ulaskom u 21 vek, Internet je nastavio sa ogromnim porastom. Bez ikakvog merenja, porast je primetan na svim frontovima: broj hostova, broj korisnika, količina saobraćaja, broj linkova, kapacitet pojedinačnih linkova, ili porast mreža nudilaca internet servisa. Taj kontinualni brzi porast, povezan sa raznolikim servisima za koje se očekuje da će Internet da obezbedi, stvorio je dva glavna izazova u projektovanju i implementaciji komutacije paketa (IP ruteri), upravljanje redovima čekanja i prosleđivanje.

Ruteri preuzimaju podatke u formi elektronske pošte, zahteva za pretraživanje interneta, prenosa datoteka i njihovog isporučivanja na odgovarajuća odredišta. Elektronska pošta se šalje na tačan server, zahtevi za pretraživanje interneta se prosleđuje na internet, a prenete datoteke se isporučuju željenom primaocu. Sve ove funkcije se zasnivaju na ispravno postavljenim i održavanim ruterima.

10. LITERATURA

- [1] Mirjana Stojanović, Vladanka Aćimović-Raspopović, *Problemi zaštite infrastrukture multiservisnih IP mreža*
- [2] Mark Tripod, *Cisco ruteri Konfigurisanje i rešavanje problema*, prevod, CET, 2000.
- [3] *IP Addressing and Routing*, Cisco Systems, Inc., 2001.
- [4] *Route Selection in Cisco Routers*, Cisco Systems, Inc., 2001.
- [5] Richard Stevens, *Tcp-ip Illustrated*
- [6] Mr Verica Vasiljević, Algoritmi za rutiranje, VETŠ, Beograd
- [7] Dragan Marković, *Osnovi umrežavanja*, CET, Beograd
- [8] http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm

PRILOG 1

Listing 1. Primer skripta za podešavanje

```
--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Refer to the 'Getting Started' Guide for additional help.
Default settings are in square brackets '[]'.
Would you like to enter the initial configuration dialog? [yes]:
Configuring global parameters:
  Enter host name [Router]: test-r1
  Enter enable password: cisco
  Enter virtual terminal password: termpwd
  Configure SNMP Network Management? [yes]: no
  Configure IP? [yes]:
  Configure IGRP routing? [yes]: no
Configure DECnet? [no]:
  Configure XNS? [no]:
  Configure Novell? [no]:
  Configure AppleTalk? [no]:
  Configure Vines? [no]:
  Configure bridging? [no]:
  Configure MOP? [no]:
Configuring interface parameters:
Configuring interface Ethernet0:
  Is this interface in use? [yes]:
    Configure IP on this interface? [yes]: yes
      IP address for this interface: 192.168.17.2
      Number of bits in subnet field [8]:
      Class B network is 192.168.0.0, 8 subnet bits; mask is 255.255.255.0
Configuring interface Serial0:
  Is this interface in use? [yes]: no
Configuring interface Ethernet1:
  Is this interface in use? [yes]:
    Configure IP on this interface? [yes]: yes
      IP address for this interface: 192.168.80.2
      Number of bits in subnet field [8]:
      Class B network is 192.168.0.0, 8 subnet bits; mask is 255.255.255.0
```

Configuring interface Serial1:

Is this interface in use? [yes]: **no**

Listing 1. predstavlja primer nekih od pitanja pri prvom startovanju rutera. Nakon odgovora na sva pitanja program za podešavanje generiše konfiguracionu datoteku. Ova nova konfiguracija se prikazuje na ekranu i treba odgovoriti na pitanje da li je prihvatamo ili ne.

Listing 2. Jednostavna konfiguracija generisana iz Setupa

```
--- System Configuration Dialog ---
hostname test-r1
enable password cisco
line vty 0 4
  password termpwd
!
ip routing
!
interface Ethernet0
  ip address 192.168.17.2 255.255.255.0
!
interface Serial0:
  shutdown
  no ip address
!
interface Ethernet1
  ip address 192.168.80.2 255.255.255.0
!
interface Serial1:
  shutdown
  no ip address
!
end
```

Na listingu 2. prikazan je primer konfiguracije koju je, na osnovu pitanja iz listinga 1. generisao program za podešavanje.

Program za podešavanje nije pružio mogućnost da se podese protokoli OSPF ili BGP, kao i mnoge druge funkcije koje postoje u IOS-u. Ove preostale funkcije se posebno podešavaju, ili kroz privilegovani EXEC režim interfejsa komandne linije, ili korišćenjem već postojeće konfiguracione datoteke sa TFTP servera ili sa fleš kartice.

POJMOVI

Admission control

Označava procedure za kontrolu pristupa novih tokova IP saobraćaja u mrežu saglasno zahtevima za QoS i raspoloživost resursa mreže

Access control

Označava mehanizam zaštite kojim se pristup elementima mreže ili informacijama dozvoljava samo ovlašćenim osobama, entitetima ili procesim

Bandwith - širina prenosnog opsega; propusni opseg

1. Razlika između najviše i najniže učestanosti koje mogu da prenesu analogni komunikacioni sistemi. Na primer, za telefonski prenos koristi se prenosni opseg od 3000 Hz. To je razlika između najniže (300 Hz) i najviše (3300 Hz) učestanosti koja se prenosi.
2. Kapacitet prenosa podataka digitalnog komunikacionog sistema.

Baud rate - brzina u bodima

Brzina u bodima je broj događaja ili promena signala koji se dešava u jednoj sekundi, a ne broj prenesenih bitova u sekundi (bps). U visokobrzinskim digitalnim komunikacijama, jedan događaj može stvarno da bude kodiran pomoću više od jednog bita i modemi se tačnije opisuju brojem bitova u sekundi nego brzinom u bodima. Na primer, tzv. 9600-bodni modem stvarno radi na 2400 boda, ali prenosi 9600 bitova u sekundi korišćenjem 4 bita za kodiranje po događaju ($2400 \times 4 = 9600$) i, prema tome, predstavlja 9600-bps modem.

Broadcast - difuzno emitovan

Poslan velikom broju primalaca. U komunikacijama i mrežama, emitovana poruka je ona koja se šalje svim stanicama.

Debug - otkloniti greške

Detektovati, locirati i ispraviti logičke ili sintaksičke greške u programu ili kvarove hardvera. Kad se radi o hardveru, češće se koristi izraz *troubleshoot* (otkrivanje i rešavanje problema)

Default - podrazumevana vrednost

Izbor koji pravi sâm program, ako se korisnik ne opredeli za neku drugu vrednost. Podrazumevane vrednosti ugrađuju se u program onda kada neka vrednost ili opcija moraju postojati kako bi program funkcionisao.

Frame relay - protokol prenosa okvira

Protokol za komutaciju paketa koji se koristi na regionalnim računarskim mrežama. Frame relay prenosi pakete različite dužine brzinom do 1 544 Mbps. To je varijanta protokola

X.25 kod koje su izostavljene neke mogućnosti za detekciju grešaka u cilju postizanja veće brzine.

Gateway - mrežni prolaz

Uređaj koji povezuje mreže i omogućava prenos informacija iz jedne mreže u drugu koristeći različite komunikacione protokole. Mrežni prolaz transformiše informacije i konvertuje ih u oblik kompatibilan sa protokolom koji koristi prijemna mreža.

Internetwork – međumrežni

Odnosi se na uzajamnu komunikaciju međusobno povezanih mreža. Često označava komunikaciju preko Interneta između dve lokalne računarske mreže ili između lokalne i regionalne računarske mreže.

Load - Opterećenje

1. Ukupno opterećenje sistema istovremenim računskim operacijama. 2. Količina struje u elektronici koju provodi uređaj. 3. Ukupan saobraćaj na telekomunikacionoj liniji.

Path - putanja

1. Komunikaciona veza između dva čvora na mreži. 2. Put kroz strukturirani skup informacija, kao što su baza podataka, program ili datoteke smeštene na disku. 3. Niz instrukcija u programiranju koje računar obavlja tokom izvršavanja rutine. 4. U obradi informacija, logički tok kroz grane stabla zaključivanja koji vodi do zaključka kao što je teorija na kojoj se zasnivaju ekspertske (deduktivne) sistemi. 5. Put koji operativni sistem sledi kroz kataloge u pronalaženju, sortiranju i uzimanju datoteka sa diska

Protocol suite - stek protokola, skup protokola

Skup protokola koji rade zajedno na različitim nivoima omogućavajući komunikaciju na mreži. Na primer, TCP/IP stek protokola na Internetu obuhvata više od 100 standarda uključujući FTP, IP, SMTP, TCP i Telnet.

Reliability - pouzdanost

Verovatnoća da će računarski sistem ili uređaj uspešno raditi tokom datog vremenskog perioda pod zadatim uslovima. Pouzdanost se meri različitim pokazateljima performansi.

Router - usmerivač, ruter

Uređaj za posredovanje u komunikacionoj mreži koji ubrzava prosleđivanje poruka. Na mreži sa velikim brojem računara, povezanih preko više mogućih puteva, usmerivač prima poruke i prosleđuje ih na njihova odredišta najefikasnijim raspoloživim putem. U skupu međusobno povezanih lokalnih računarskih mreža (LAN-ova) usmerivač ima nešto drugačiju funkciju: koristeći iste komunikacione protokole služi kao veza između LAN-ova, omogućavajući slanje poruka sa jednog LAN-a na drugi.

Routable protocol - protokol usmeravanja, usmerivi protokol

Komunikacioni protokol za usmeravanje podataka iz jedne mreže u drugu pomoću mrežne adrese i adrese uređaja. TCP/IP je primer protokola usmeravanja.

Scalable - koji je podesive veličine, koji je promenljive veličine

Karakteristika dela hardvera ili softvera koja omogućava proširivanje radi zadovoljavanja budućih potreba. Na primer, mreža promenljive veličine dopušta mrežnom administratoru dodavanje velikog broja čvorova bez ponovnog projektovanja osnovnog sistema.

Switching - komutacija

Komunikacioni metod koji za uspostavljanje veze ili usmeravanje informacija između dve strane koristi privremene, a ne trajne veze. Komutacija poruka i komutacija paketa u računarskim mrežama omogućavaju razmenu informacija između dve strane. U oba slučaja poruke se prosleđuju (komutiraju) preko međustanica koje služe za povezivanje i pošiljaoca i primaoca.

QoS - Quality Of Service

Skup standarda i mehanizama koji obezbeđuju kvalitet prenosa podataka

Vreme konvergencije

Vreme koje je potrebno da se mreža prilagodi promena topologije i da ponovo izračuna sve rutirane tabele

SADRŽAJ POGLAVLJA

DEO I: UVOD

Uvodne informacije o ulozi rutera u mreži.

DEO II: INTERNETWORK

Pojam, ilustracija i elementi internetwork. Kratak opis LAN i WAN mreža.

DEO III: OPEN SYSTEM INTERCONNECTION REFERENCE MODEL – OSI

U ovom delu opisan je OSI referentni model i relacije između slojeva OSI modela, data je definicija pojma protokola i kako rade protokoli. U nastavku opisuje se TCP/IP model, definišu se osnovni protokoli skupa TCP/IP protokola i Internet protokol (IP) adrese. Budućnost TCP/IP protokola (IPv6) i formati adresa kod IPv6 protokola.

DEO IV: WAN TEHNOLOGIJE I STANDARDI

Četvrti deo govori o WAN računarskim mrežama i ulozi rutera u WAN mrežama. Opisane su komponente rutiranja, statičko i dinamičko određivanje putanja.

DEO V: PROTOKOLI ZA RUTIRANJE

Peti deo opisuje protokole za rutiranje: *Routing Information Protocol* (RIP), *Interior Gateway Routing Protocol* (IGRP), *Enhanced Interior Gateway Routing Protocol* (EIGRP), *Open Shortest Path First* (OSPF), *Border Gateway Protocol* (BGP), IS-IS, MPLS

DEO VI: PRIMER IZBORA RUTE NA CISCO RUTERIMA

U šestom delu dat je primer izbora rute na CISCO ruterima, pravljenje rutingske tabele, čemu služe backup rute, menjanje administrativne distance, forvardovanje paketa korišćenjem ARP. Dat je i primer tabele rutiranja kod Windows operativnog sistema. Deo ovog poglavlja odnosi se na probleme zaštite tabele rutiranja (zlonamerna modifikacija tabele rutiranja; modifikacija, falsifikovanje i replikacija paketa u čvorovima; napadi na QoS signalizacione protokole i odbijanje servisa – DoS (*Denial of Service*))

DEO VII: ALGORITMI ZA RUTIRANJE

Ovo poglavlje posvećeno je algoritmima za rutiranje: DV-Distance vector algoritmi i LS-Link state algoritmi. Opisano je Hijerarhijsko rutiranje (*Hierarchical Routing*), Rutiranje emisijom (*Broadcast Routing*) i Rutiranje višestrukim usmeravanjem (*Multicast Routing*).

DEO VIII: KOMPONENTE I RADNI MODOVI RUTERA (CISCO®)

Osmo poglavlje se bavi komponentama i radnim modovima CISCO rutera. Opisane su interne i eksterne komponente rutera, startup procedura, konfigurisanje registra, Cisco CLI komandni modovi, dat je pregled i opis *show* komandi.

DEO IX: ZAKLJUČAK