

6. USMJERAVANJE NA INTERNETU

Usmjeravanje kod paketskih mreža ima primarnu ulogu osigurati dostupnost od izvorišta do odredišta toka podataka, a sekundarnu pri tome utjecati na optimalno iskorištenje mreže i kvalitetu usluge. Usmjernici Interneta ostvaruju te funkcije.

6.1. Arhitektura usmjeravanja na Internetu

Prvobitno su usmjernici unutar Interneta bili organizirani hijerarhijski, što je bilo naslijeđe ranije ARPANET arhitekture. Postojao je centralni sustav (jezgra) mreže, kroz čije su usmjernike (core gateways) prolazile informacije o usmjeravanju među svim mrežama Interneta. Rastom Interneta, naglo je rasla i količina usmjerivačkih informacija koje je jezgra trebala obraditi, te je to postao i glavni nedostatak hijerarhijskog modela.

Novi model usmjeravanja zasniva se na ravnopravnim nezavisnim (autonomnim) sustavima. Svaki nezavisni sustav sastoji se od grupe mreža koje su pod istom administrativnom upravom. S obzirom na takvu podjelu razlikujemo slijedeće vrste usmjernika:

- **vanjske usmjernike** koji obavljaju usmjeravanje i razmjenjuju informacija o usmjeravanju između različitih nezavisnih sustava. Takvi sustavi koriste vanjske usmjerivačke protokole (npr. *BGP-Border Gateway Protocol*).
- **unutrašnje usmjernike** koji usmjeravaju pakete unutar nezavisnih sustava. Takvi sustavi koriste unutrašnje usmjerivačke protokole (npr. *RIP-Routing Information Protocol*).

Internet možemo promatrati kao sustav koji se sastoji od tri razine usmjeravanja:

- **osnovna mreža** (Backbone), povezuje vanjske usmjernike i predstavlja najvišu razinu. Paketi IP protokola isporučuju se optimalnim putem do usmjernika preko kojega je dostupna osnovna podmreža odredišta.
- **osnovna podmreža** (Autonomous system) predstavljena je s jednom ili više adresnih klasa, a karakterizirana je vlastitom administracijom adresa. Dijeli se na podmreže s fiksnom (klase) ili varijabilnom (adresna maska) mrežnom adresom. Najčešće je ostvarena jednostavnom do srednje složenom mrežom unutrašnjih usmjernika na koje su povezane podmreže. IP paketi se usmjeravaju optimalnim putem do usmjernika preko kojega je dostupna podmreža odredišta.
- **podmreža** (Subnetwork) je dio Interneta koji obuhvaća jednu zonu prostiranja lokalne mreže, a čija je mrežna IP adresa određena klasom ili mrežnom maskom. Podmreža je s osnovnom podmrežom povezana najčešće sa samo jednim usmjernikom, koji za računala podmreže predstavlja osnovni usmjernik (Default Gateway). Pakete koji dolaze na podmrežu osnovni usmjernik pakira u okvire s MAC adresom odredišta i prosljeđuje ih lokalnom mrežom. Pakete koji idu van iz podmreže, izvorište pakira u okvire s MAC adresom osnovnog usmjernika, koji će ih prosljediti dalje kroz osnovnu podmrežu. Paketi kojima je izvorište i odredište na istoj podmreži (unutar granica zone prostiranja), odredište pakira u okvir s MAC adresom odredišta i šalje ga direktno odredištu. U sva tri slučaja, pripadnost paketa podmreži određuje se na osnovu mrežnog dijela IP adrese, a pretvorba IP adrese odredišta ili usmjernika u MAC adresu obavlja se korištenjem ARP protokola i okvira s univerzalnim adresama (u granicama zone prostiranja).

6.2. Tablice usmjeravanja i RIP

Da bi olakšali traženje optimalnog puta usmjernici održavaju tablice usmjeravanja. One sadrže niz informacija potrebne za usmjeravanje i odabir najboljeg puta, primjerice:

- parovi adresa_odredišta-slijedeći_usmjernik kazuju usmjerniku da se odgovarajuće odredište može dosegnuti na optimalan način ako se pošalje na navedeni slijedeći usmjernik. Dakle usmjernici ne drže informacije o potpunom putu paketa već sadrže samo prvi slijedeći korak na tom putu. Odredište može biti mreža, radna stanica ili posebna oznaka koja označava osnovni usmjernik.
- mrežnu masku za određeno odredište

- metriku - koja definira mehanizam za uspoređivanje kakvoće pojedinih smjerova.
- ime mrežnog sučelja koje koristi navedeni smjer
- da li je smjer ispravan, koristi li usmjernike ili je vezan izravnom vezom i sl.
- vrijeme kada je pojedini smjer posljednji put ažuriran

Unutar tablice usmjeravanja postoji posebna adresa kojom se definira osnovni smjer (default route) i najčešće je to adresa koja sadrži sve nule (0.0.0.0). Na osnovni smjer šalju se svi paketi za koje se ne može pronaći odredište unutar tablice usmjeravanja (bilo bi nepraktično da svaki usmjernik ima u tablici usmjeravanja sva moguća odredišta). Osnovni smjer definiran je adresom osnovnog usmjernika (default gateway). Dakle, kada paket stigne na neki usmjernik, on provjerava tablicu usmjeravanja ne bi li našao odgovarajuću odredišnu adresu (radne stanice ili njenu mrežnu adresu) i ako je ne pronađe šalje je na vlastiti osnovni usmjernik.

RIP (Routing Information Protocol) se početkom 80-ih godina počeo isporučivati s BSD inačicom UNIX operativnog sustava (routed program). Danas je to vrlo popularan unutrašnji protokol za usmjeravanje, a formalno je definiran RFC 1058 (verzija 1).

RIP omogućuje usmjernicima i radnim stanicama razmjenu informacije o usmjerivačkim smjerovima unutar Internet mreže. Zasniva se na algoritmu "vektora udaljenosti" i to tako da odabire smjer s najmanjim "brojem koraka" (brojem usmjernika koje paket treba proći na putu do odredišta) kao najbolji. Najduži prihvatljivi smjer unutar RIP usmjerivačke tablice može imati najviše 15 koraka (za >15 RIP smatra da se odredište ne može doseći). RIP pamti samo najbolji put do odredišta, tj. ako nova informacija nudi bolji smjer (manji broj koraka), nova informacija zamjenjuje staru.

Kada neki RIP usmjernik detektira prekid jedne od svojih vlastitih veza on ažurira svoju tablicu (postavlja broj koraka za taj smjer na 16) i susjednim usmjernicima šalje vlastitu usmjerivačku tablicu. Svaki usmjernik koji primi ovu poruku ažurira vlastitu tablicu i šalje je dalje - promjena se propagira mrežom.

BITOVI							
0	7	8	15	16	23	24	31
command		version		NULE			
adress family identifier				NULE			
IP adresa							
NULE							
NULE							
metric							
adress family identifier				NULE			

...

Slika 6.1. Format RIP poruke

Oznake znače slijedeće:

- **COMMAND** (naredba)- može biti zahtjev (REQUEST) da usmjernik pošalje čitavu ili dio tablice usmjeravanja ili odgovor (REPLY). Odgovor se šalje ili na eksplicitni zahtjev ili kao redovita RIP poruka (routing update message) koja sadrži čitavu tablicu svakih 30 sek.
- **VERSION** - specificira korištenu verziju RIP-a.
- **ADDRESS FAMILY IDENTIFIER** (identifikator obitelji adresa)- definira protokol čije se adrese nalaze u tablici usmjeravanja (za IP to je 2).
- **ADDRESS** - definira adresu odredišta iz usmjerivačke tablice.

- METRIC -definira metriku koja služi za uspoređivanje pojedinih smjerova, tipično je to broj koraka (*hop count*).

Za prijenos dijelova vlastite usmjerivačke tablice RIP koristi UDP datagrame. Svaka radna stanica koja koristi RIP mora imati usmjerivački proces koji šalje i prima datagrame s UDP priključne točke 520. Svaki RIP IP paket može sadržavati do 25 vrijednosti iz tablice usmjeravanja, pa je maksimalna veličina paketa MTU=512. Ukoliko računalo nije usmjernik ono isto može motriti ove RIP poruke, ali ne šalje vlastitu tablicu. To je tzv. "tihi " RIP proces (silent RIP).

RIP proces svakih 30 sekundi šalje čitavu usmjerivačku tablicu svojim susjedima. Ukoliko nakon 180 sekundi usmjernik nije dobio potvrdu smjera u tablici on proglašava smjer neispravnim (broj koraka postavlja >15)., a ukoliko nakon daljnjih 120 sekundi (najčešće) ne dobije potvrdu smjera on ga briše iz tablice usmjeravanja. Ukoliko usmjernik detektira prekid neke veze on, po ažuriranju vlastite tablice, odmah šalje svoju tablicu susjednim usmjernicima ne čekajući istek 30 sekundi (triggered update).

RIP ne osigurava mehanizam za prijavu pogreški izvorišnom računalu kada dođe do pogreški pri usmjeravanju. Tu funkciju obavlja ICMP protokol.

RIP protokol, osim ograničavanja najvećeg broja koraka na 15, uključuje i niz dodatnih svojstava koja omogućuju stabilniji rad:

a) Podijeljena obzorja (Split Horizons)

Ovo svojstvo proizlazi iz činjenice da nije korisno slati informaciju o smjerovima u onom smjeru iz kojeg smo tu informaciju i primili. Ovim sprječavamo stvaranje usmjerivačkih petlji između 2 usmjernika.

b) Ažuriranje prekinutih smjerova (Poison Reverse Updates)

Ovo svojstvo namijenjeno je nalaženju i sprječavanju usmjerivačkih petlji između tri ili više računala, a temelji se na tome da povećavanje broja koraka za pojedini smjer obično ukazuju na pojavu usmjerivačke petlje. Stoga se pri uočavanju ovakvih smjerova šalju paketi (Poison reverse update poruke) koje brišu takve smjerove iz usmjerivačkih tablica.

c) Zadržavanje promjene izbrisanih smjerova (Hold-downs)

Budući da ažuriranje smjerova koji su prekinuti ne dolazi istovremeno na svaki usmjernik, može se dogoditi da usmjernik koji još nije obaviješten o prekidu veze šalje redovite poruke u kojima navodi da je takav smjer još ispravan. Usmjernik koji primi takvu poruku, a već je obaviješten o prekidu tog smjera, neće odmah takav smjer staviti u svoju tablicu već će određeno vrijeme zadržavati promjenu.

6.3. Privatne mreže (Intranet)

Privatne mreže (Intranet) su mreže organizirane na TCP/IP tehnologiji, a koje ne koriste javne, već privatne IP adrese. Za to postoje tri razloga: mreža nije povezana na Internet, mreža je povezana ali zbog sigurnosti koristi privatne adrese, te mreža je povezana, ali zbog nedostatka IP adresa koristi privatne adrese.

Za privatne mreže rezervirane su adrese 10.0.0.0/8, 172.16.0.0/16 i 192.168.0.0/16, dakle jedna A, jedna B i blok od 256 uzastopnih C klasa. Usmjernici Interneta pakete s ovim IP adresama odbacuju bez pokušaja daljeg usmjeravanja.

Nepovezane podmreže trebaju koristiti privatne adrese kako bi kod naknadnog povezivanja na Internet bili izbjegnuti poremećaji u usmjeravanju, mogući za slučaj dupliranja već iskorištenih adresa.

Sigurne podmreže (Intranet) koriste privatne adrese, a povezane su na Internet preko jednog usmjernika koji prema Internetu djeluje kao krajnje računalo. Na taj način vanjskom učesniku komunikacije nije poznat broj ni nazivi računala unutar sigurne podmreže. Veze na javnom dijelu mreže prenose se na unutarnju tehnikama maskarade i uslužnih veza.

Maskarada se obavlja na mrežnoj razini, kada usmjernik brojeve priključnice (priključne točke i IP adrese) mijenja vlastitim. Vezu je moguće inicirati samo iz zaštićenog dijela mreže.

Uslužne veze (proxy, najčešće SOCKS) usmjernik ostvaruje za potrebe i za račun korisnika na sigurnom dijelu mreže. Radi se o prenošenju segmenata na prijenosnoj razini sa vanjske veze na unutrašnju.

U oba slučaja, čitava podmreža predstavljena je prema Internetu jednom IP adresom računala, pa je sporedni efekt **ušteda čitave klase adresa**. To je korisno, zbog poznatog nedostatka IP adresa.

6.4. IPRoute

IPRoute je programski paket koji omogućuje usmjeravanje IP paketa koristeći računalo s 286 ili boljim procesorom, a pokreće se pod DOS operativnim sustavom. IPRoute podržava:

- Višestruka Ethernet sučelja
- Ethernet sučelja postavljaju se preko paketnog pogonskog programa kartice koje treba učitati prije pokretanja programa (**packet** naredba). IPRoute prepoznaje samo Ethernet II okvire, dok ostali nisu podržani.
- SLIP, CSLIP i PPP serijske veze, bilo izravno preko standardnih serijskih priključaka računala ili preko modema.
- Biranje na zahtjev (*demand dial*) i kodiranje odgovora preko *script* jezika (*answer scripting*)
- Filtriranje IP paketa koje omogućuje povećanje mrežne sigurnosti. Ono podrazumjeva propuštanje ili odbijanje paketa na temelju određenih parametara kao što su izvorišna i odredišna IP adresa, TCP/UDP priključna točka izvorišta ili odredišta, TCP zastavice (ACK, SYN...), ICMP tipovi poruka i sl. Sučelje na kojem se obavlja filtriranje sadrži dvije odvojene liste pravila:
 - za ulazne pakete (*inbound*)
 - za izlazne pakete (*outbound*).
- Translacije mrežnih adresa (NAT, eng. *Network Address Translation*) koja omogućuje mreži s privatnim (intranet) adresama pristup na Internet mrežu. NAT izvorišne IP adrese svih ili samo nekih paketa koji se šalju sa lokalnog sustava zamjenjuje vlastitom IP adresom usmjernika, a izvorišnu priključnu točku onom koja je navedena za pojedino pravilo translacije adresa (**nat** naredba).
- bilježenje paketa i događaja (*logging*) unutar lokalne datoteke ili preko *syslog* poslužnika.

IPRoute programu, pri pokretanju, treba dostaviti parametre potrebne za ispravan rad u obliku tekst datoteke u *script* jeziku (start.ipr). Ona definira naredbe koje će se izvršiti određenim redoslijedom ili pod određenim uvjetima. Sve naredbe trebaju biti pisane malim slovima. Unutar datoteke moguće je definirati različite događaje kao što su: pojava nekog modemskeg kontrolnog signala, istek vremena... Ova datoteka se poziva kao parametar pri pokretanju programa, primjerice:

```
ipr start.ipr .
```

Najčešće naredbe su:

async <sučelje> <U/I adresa> <IRQ> <brzina> [<labela>]

Definira COMx vezni sklop za rad s usmjernikom. Ukoliko je naveden parametar "labela", tada se pokreće novi *script* proces koji započinje s izvršavanjem od te labele. Slijedeći primjer definira standardni COM1 s imenom "sl0" i brzinom 9600b/s:

```
async sl0 0x3f8 4 9600
```

command <sučelje>

Pokreće interaktivni interpreter naredbi za navedeno sučelje. Ukoliko se navodi bez parametara na početku *script* datoteke tada pokreće IPRoute konzolu.

drop filter <sučelje> Isključuje filtriranje paketa na navedenom sučelju.

drop nat <sučelje> Isključuje NAT na navedenom sučelju.

filter <sučelje> [log] [nodial] {deny,drop,permit} {in,out} <protokol> <izvorište> <odredište>

Dodaje pravilo za filtriranje paketa u ulaznu ili izlaznu listu (*in,out*) za navedeno sučelje.

Ukoliko je prisutan "log" parametar onda će se svi paketi koji zadovoljavaju navedeno pravilo bilježiti u datoteku (ili drugdje, ovisno o **log** naredbi).

Ako je prisutan "nodial" parametar onda paketi koji zadovoljavaju pravilo će biti odbačeni ukoliko veza preko serijskog sučelja nije još uspostavljena.

"Protokol" parametar definira broj ili ime protokola, a može biti:

*	bilo koji IP paket
icmp	bilo koji ICMP paket
icmp-xx	neki specifični ICMP paket
tcp	bilo koji TCP paket
tcp-syn	TCP paket sa postavljenom SYN, ali ne i ACK zastavicom. Indicira zahtjev za uspostavu veze.
tcp-xsyn	TCP paket sa SYN zastavicom koja nije postavljena ili ACK koja jest. Indicira paket za već uspostavljenu vezu.
udp	bilo koji UDP paket
udp-zcs	UDP paket s zaštitnom sumom jednakoj nuli.

Parametri izvorišta i odredišta definirani su IP adresama u obliku:

IP_adresa/broj_bita_mrežne_maske:priključna_točka

nat <sučelje> <protokol> <unutarnja_adresa:priključna_točka> <vanjska_adresa:priključna_točka>

Dodaje pravilo za translaciju adresa u listu pravila za navedeno sučelje. Protokol parametar može biti "tcp", "udp", "icmp", ili "*" koji specificira bilo koji protokol. Pravilo određuje koju unutrašnju adresu i broj priključne točke treba pretvoriti u koju vanjsku adresu i broj priključne točke (vanjska mreža) pri translaciji adresa.

packet <sučelje> <int #> <IP_adresa/bitovi_maske> [broadcast <brdcst_adresa>] [mtu <mtu>]

Postavlja paketni pogonski program kao jedno od sučelja usmjernika. Parametar <int #> definira vektor na kojem je postavljen paketni pogonski program. Prema pretpostavljenoj vrijednosti univerzalana (*broadcast*) adresa je 255.255.255.255, a MTU je 1500.

Primjer konfiguracije za adresu 192.168.1.254 i masku 255.255.255.0, te vektora paketnog programa na 0x60:

```
packet en0 0x60 192.168.1.254/24
```

ping <IP_adresa> Provjera dostupnosti navedene adrese.

ppp <sučelje> <timeout> <IP_adresa/bitovi_maske> [broadcast <brdcst_adresa>] [mtu <mtu>] [dynamic-nat]

Pokreće PPP protokol za navedeno sučelje. Parametar timeout je vremenski interval u sekundama koliko će se čekati na uspostavu veze. Ukoliko ovo vrijeme istekne PPP protokol se isključuje. Parametar "dynamic-nat" koristi se kada je lokalna IP adresa dobivena PPP "pregovaranjem" i tada će sve linije NAT tabele biti promjenjene da odgovaraju toj adresi.

rip <sučelje> [default] [preference <pre>] [quiet] [{v1,v2,off}]

Uključuje/isključuje RIP poruke na navedenom sučelju. Prema pretpostavljenoj vrijednosti sve poruke se šalju po verziji 1 protokola. Parametar "v2" omogućuje slanje poruka RIP verzije 2. Parametar "default" naznačuje da će se slati samo osnovni smjer (*default route*), a ne i čitava tablica za usmjeravanje, dok "quiet" definira RIP proces koji ne šalje poruke već ih samo prima. "Preference" određuje koliki broj koraka će se dodati smjerovima koji idu preko navedenog sučelja.

route <IP_adresa/bitovi_maske> <sučelje> [*<adresa_usmjernika>*] [*metric <metric>*]
[*preference <pre>*] [*perm*]

Dodaje statički smjer u tablicu za usmjeravanje. Parametar "perm" je potreban ukoliko se radi o serijskoj vezi koja još nije uspostavila SLIP/PPP vezu.

set log file <ime_datoteke>

Definira datoteku u koju će se bilježiti događaji i paketi. "CON" kao ime datoteke označava bilježenje samo na zaslon usmjernika (*console*).

set log brief/data

Podaci koji se bilježe za svaki paket svode se na samo osnovne podatke o paketu, ili se pohranjuje čitav paket.

show arp/ filter <sučelje>/ **interface** [*<sučelje>*] / **nat** <sučelje> [*status*] / **route** / **down**

Prikazuje ARP tablicu / pravila IP filtriranja / parametre sučelja i statistiku / tablicu prevođenja / tablicu usmjeravanja / Isključuje programsku podršku usmjernika i vraća se u DOS

Da bismo omogućili pokretanje IProute programa odmah po uključanja računala koje će vršiti ulogu IP usmjernika treba učiniti slijedeće:

- 1) Na disk/disketu s kojeg ćemo pokretati računalo kopirati DOS systemske datoteke, primjerice, možemo korisiti DOS naredbu :

```
sys a:
```

koja će kopirati potrebne datoteke na A: disketu.

- 2) Na disk/disketu pohraniti IPR.EXE program i sve potrebne paketne pogonske programe za mrežne kartice.
- 3) Napisati start.ipr datoteku koja sadrži konfiguraciju usmjernika. Primjer:

```
command ;Start the console
packet en1 0x61 161.53.166.240/24 ;Set first interface
packet en0 0x60 161.53.169.241/28 ;Set second interface.
rip en1
set log file con
```

- 4) Napisati AUTOEXEC.BAT datoteku koja će pokrenuti sve pogonske programe i pokrenuti IPRoute program kao:

```
ipr start.ipr.
```

- 5) Zatim možemo s diska/diskete pokrenuti usmjernik resetiranjem računala.

6.5. Zadatak

Povezati lokalnu mrežu laboratorija na Internet korištenjem PC kompatibilnog računala i IPROUTE ili LINUX programske podrške.