SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Računalne mreže

LABORATORIJSKE VJEŽBE

Lada Sartori

Split, 2021.

Predgovor

Kolegij Računalne mreže obavezni je predmet na prvoj godini preddiplomskog stručnog studija Računarstva na Sveučilišnom odjelu za stručne studije Sveučilišta u Splitu i kao takav studentima daje osnovna znanja iz područja računalnih mreža.

Laboratorijske vježbe sadržajno prate predavanja, a cilj im je omogućiti studentima savladavanje praktičnih znanja o mrežama, te im olakšati povezivanje teoretskog gradiva.

Vježbe su podijeljene u šest cjelina i obrađuju sve razine TCP/IP modela. Poseban naglasak stavljen je na prve dvije razine (razina pristupa mreži i internet razina) koje spadaju pod mrežne razine. Studenti bi savladavanjem ovih vježbi usvojili potrebna znanja o protokolima korištenim u mreži internet (TCP, UDP, IP, ARP, Ethernet), savladali osnove usmjeravanja u mreži, IP adresiranja i podmrežavanja, te stekli osnovna znanja o bežičnim mrežama.

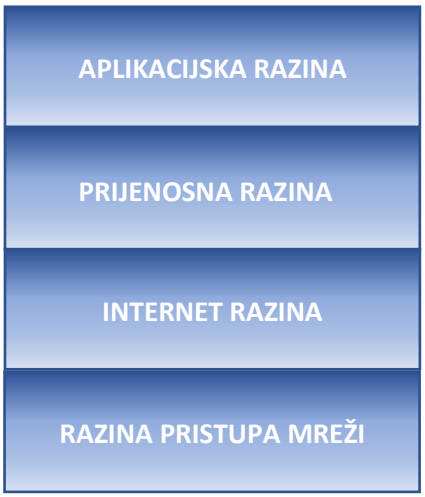
Akademska godina 2020/21. je godina u kojoj je svijetom vladala pandemija bolesti izazvana virusom COVID-19 i koja je sve prisilila na sasvim drugačiji način života. U edukacijskim sredinama to je značilo prelaženje dijelom ili u potpunosti na on-line način nastave. Koliko god smatrali da je nastava u izravnom kontaktu bitno kvalitetnija i rezultira većom razinom znanja i razumijevanja, povremeno smo bili prisiljeni nastavu održavati na udaljenosti. Ove vježbe su posebno prilagođene i pripremljene kako bi studenti, u trenutcima kad nismo imali izbora i kad smo morali održavati nastavu on-line, mogli uz ograničene resurse koji im stoje na raspolaganju kod kuće, odraditi sve ciljeve zadane nastavnim planovima i programima.

Sadržaj

1. TCP/IP model, adresiranje i nazivi uređaja

Računalna mreža omogućuje komunikaciju mrežnih korisnika, a slijed komunikacije se razdvaja na razine koje obavljaju pojedine procese.

Tip mreže koji se danas najčešće koristi je internet mreža. Komunikacijski proces se odvija kroz 4 razine izvornog TCP/IP modela komunikacije (danas se u literaturi koristi i model s 5 razina):



Slika 1.1: Razine izvornog TCP/IP modela

- **Aplikacijska razina** sadrži korisničke aplikacije koje su izvor ili odredište informacija (web preglednik, e-mail klijent, ssh klijent…).
- **Prijenosna razina** omogućuje komunikaciju aplikacija formiranjem logičkih kanala prilagođenih prijenosnim potrebama aplikacija (uspostava veze, održavanje, kontrola toka, kontrola pogreške, raskid veze).
- **Internet (mrežna) razina** omogućuje brzu, jednostavnu i nepouzdanu komunikacija krajnjih uređaja, kao i mrežnih uređaja koji omogućuju povezivanje krajnjih uređaja, omogućavajući povezivanje mreža realiziranih na različitim fizičkim prijenosnim medijima. Ova razina odgovorna je za globalno adresiranje uređaja, te za usmjeravanje paketa kroz mrežu.
- **Razina pristupa mreži** omogućuje prijenos binarnih podataka preko raspoloživog fizičkog medija (bakrene parice, optički kabeli, bežični prijenos…). Na ovoj razini obavlja se korekcija pogrešaka nastalih u prijenosu, kao i lokalno adresiranje zasnovano na fizičkim adresama mrežnih uređaja.

Na aplikacijskoj razini nalazi se korisnička aplikacija koja koristi usluge prijenosne razine za formiranje logičkog kanala prema aplikaciji na drugom uređaju s kojim se komunicira.

Prijenosna razina realizirana je unutar operativnog sustava uređaja i mrežna aplikacija koristi njene usluge za formiranje logičkih kanala i prijenos podataka. Postoje također dijagnostičke naredbe kojima operativni sustav omogućuje uvid u stanje svake pojedine mrežne veze.

Mrežna razina implementirana je također unutar operativnog sustava računala, ali je nije moguće izravno koristiti, već joj je moguće pristupiti isključivo uz pomoć dijagnostičkih programa.

Razina pristupa mreži nalazi se implementirana u mrežnom adapteru uređaja i njoj se također može pristupiti isključivo dijagnostičkih programima.

Tijekom laboratorijskih vježbi koristit ćemo program Wireshark koji omogućuje korisniku jasan pregled podataka koje računalo razmjenjuje s drugim uređajima na mreži.

IP adrese

Računalo spojeno na mrežu internet ima vlastitu numeričku adresu, koja se može saznati naredbom **`ipconfig`**:

```
C:>ipconfig
Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . :
fe80::3c1c:cf72:93cd:792e%12
IPv4 Address. . . . . . . . . . . : 192.168.0.106
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.0.1
```

U priloženom ispisu naredbe `ipconfig` istaknuta ja IPv4 adresa koja je definirana Internet protokolom verzije 4. Protokol IPv4 još uvijek je dominantni protokol mrežne razine. U ispisu u liniji iznad vidljiva je i IPv6 adresa uređaja. Glavni razlog uvođenja nove verzije protokola IP je nedostatak dovoljnog broja IPv4 adresa. Format IPv4 adrese su 32 bita podijeljena u 4 okteta, a prikazuju se dekadskim brojem (od 0 do 255). Ukupan broj IPv4 adresa je 2^{32}.

Format IPv6 adrese je 128 bitova koji se prikazuju kao 32 heksadecimalne znamenke (od 0 do f). IPv6 zapis može sadržavati manje znamenki ukoliko se koriste mogućnosti skraćivanja zapisa. Ukupan broj IPv6 adresa je 2^{128}. Primjer IPv6 adrese vidljiv je u gornjem ispisu, pod nazivom "Link-local IPv6 Address".

U ispisu naredbe `ipconfig` vidljiva je i adresa usmjernika (engl. *Default Gateway*) koji će preuzeti paket i poslati ga prema odredištu ukoliko paket nije namijenjen računalu unutar naše lokalne mreže.

DNS zapis

Budući da ljudi teže pamte numeričke adrese, odnosno nisu prikladne za ljudsku upotrebu, uveden je sustav zamjene numeričke adrese tekstualnim nazivom. Usluga koja omogućava saznavanje numeričke adrese uređaja na osnovu njegovog naziva i obrnuto je DNS (Domain Name System).

Ovoj usluzi može se pristupiti naredbom `nslookup`:

```
nslookup www.oss.unist.hr
Server:  195.29.150.3
Address:  192.168.0.1
Non-authoritative answer:
Name:    europa.oss.unist.hr
Address:  193.198.34.9
Aliases:  www.oss.unist.hr
```

ICMP (Internet Control Message Protocol)

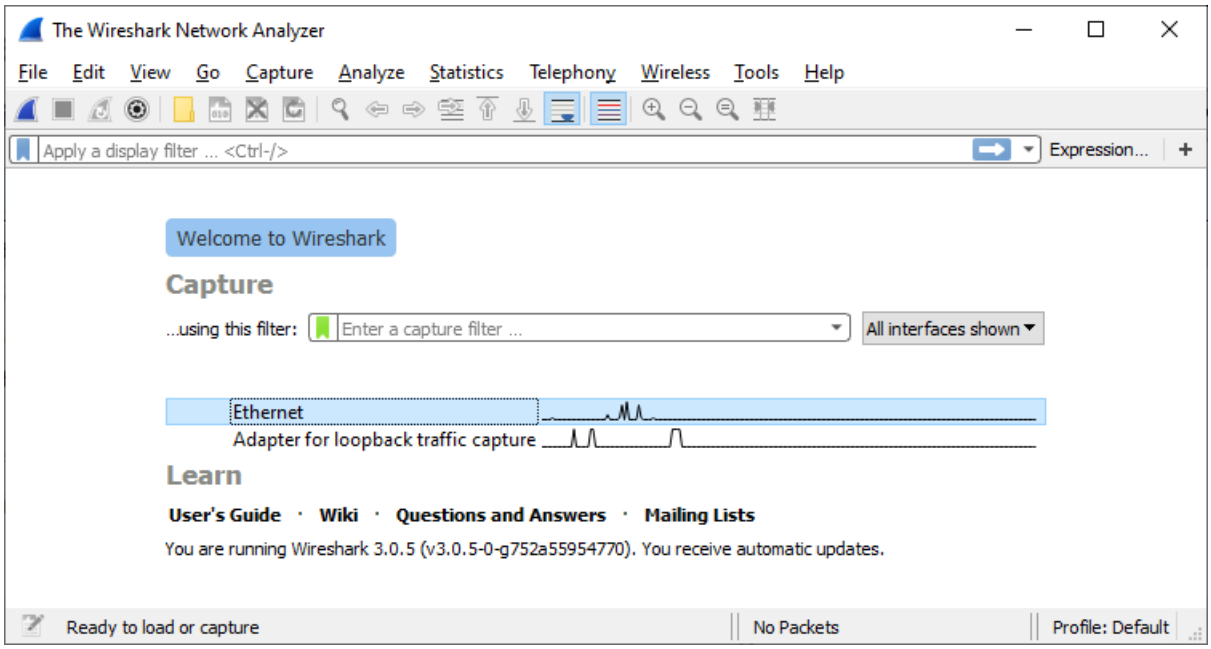
Protokol ICMP koristi se za dijagnostiku i komunikaciju mrežnih uređaja (primarno) i računala (sekundarno). Protokolom ICMP možemo generirati jednostavan mrežni promet koji ne potječe od aplikacije već ga generira operativni sustav na mrežnoj razini, kako bi se provjerila mogućnost komunikacije mrežnih uređaja. Time se najjednostavnije može provjeriti mogućnost prijenosa mrežnog prometa do odredišta.

Program `ping` ICMP poruku ECHO request šalje uređaju sa zadanom IP adresom, na koju taj uređaj treba odgovoriti ECHO Reply porukom.

```
ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Wireshark

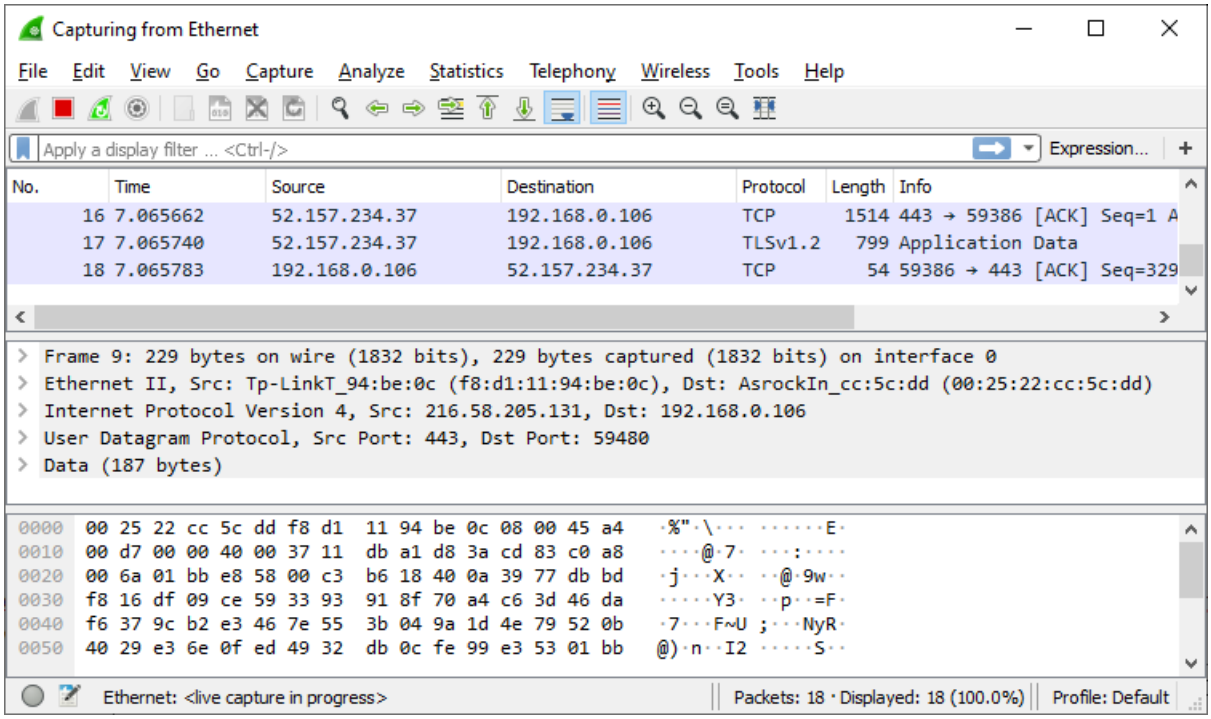
Program Wireshark omogućuje praćenje prometa koji prolazi preko mrežnog adaptera računala u realnom vremenu. Nakon pokretanja programa potrebno je odabrati mrežno sučelje za pregled (Ethernet kartica ili bežična kartica). Tipično računalo osim standardnih mrežnih sučelja (najčešće Ethernet) sadrži i različita virtualna sučelja za potrebe operativnog sustav i aplikacija. Potrebno je odabrati mrežno sučelje naziva Ethernet ili Ethernet Adapter Local Area Connection (Slika 1.2).



Slika 1.2: Prikaz aplikacije Wireshark

Nakon odabira mrežnog adaptera aplikacija prelazi u način snimanja (engl. *Capture*) u kojem u realnom vremenu prikazuje promet (Slika 1.3):

- gornji dio zaslona prikazuje snimljeni promet, zajedno s osnovnim dekodiranim informacijama o njemu (adrese, protokol, itd.)
- središnji dio zaslona prikazuje sadržaj poruke odabrane u gornjem dijelu zaslona, dekodirano po razinama internet modela
- posljednji blok prikazuje heksadecimalni zapis poruke odabrane u gornjem dijelu ekrana



Slika 1.3: Prikaz paketa uhvaćenog aplikacijom Wireshark

Program podržava različite kriterije filtriranja na temelju kojih se može izolirati samo promet koji nam je zanimljiv, jer je pregledavanje prometa bez filtara veoma nepraktično. Filtar se upisuje u polje u gornjem dijelu ekrana:

- `icmp` filtar izdvojit će samo poruke ICMP protokola
- `ip.addr==192.168.0.1` filtar izdvojit će samo promet kojem je odredišna ili izvorišna adresa 192.168.0.1.

Vježba 1: Izvještaj

Zadatak 1

Spojite računalo na mrežu koristeći UTP kabel. U operativno sustavu Windows pokrenite naredbeni redak (engl. *Command Prompt*) korištenjem naredbe `cmd`. Korištenjem naredbe `ipconfig` zabilježite sljedeće podatke:

IPv4 adresa: _____

IPv6 adresa (ukoliko je ispisana): _____

Default Gateway: _____

Zadatak 2

Naredbom `ping` provjerite dostupnost usmjernika (engl. *default gateway*) u mreži. Zabilježite podatke:

Broj poslanih paketa: _____

Broj bajtova podatka u paketu: _____

Vremena obilaska (engl. *round trip time, RTT*), najmanje, najveće, prosječno:

_____

Zadatak 3

Korištenjem naredbe `nslookup` doznajte IP adresu računala moodle.oss.unist.hr. Zabilježite sljedeće:

IP adresa računala moodle.oss.unist.hr: _____

IP adresa DNS poslužitelja koji je ponudio odgovor: _____

Ostali nazivi računala (aliasi), ukoliko postoje: _____

Zadatak 4

Pokrenite aplikaciju Wireshark i snimite promet generiran korištenjem naredbe `ping 8.8.8.8`. Koristite `icmp` filtar.

U uhvaćenim paketima pronađite koji se podaci šalju u podatkovnom dijelu ICMP paketa i zabilježite ih:

_____

2. Prijenosna razina, protokoli TCP i UDP

Prijenosna razina Internet modela zadužena je za uspostavu komunikacije između dva krajnja korisnika u mreži. Pod terminom "korisnik" u ovom slučaju smatramo dva procesa aplikacijske razine. Cilj nam je razlikovati dva komunikacijska toka koji se odvijaju između ista dva računala na mreži, ali jedan tok prenosi podatke npr. web stranice, a drugi npr. obavlja prijenos datoteke. Kako bi razdvojili različite tokove potrebne su nam različite adrese za svaki komunikacijski tok. Adrese na prijenosnoj razini definiraju se **priključnim točkama**, odnosno, portovima.

Priključna točka je 16-bitni broj koji se bilježi u zaglavlju protokola prijenosne razine u polju odredišne, odnosno izvorišne priključne točke. Ukupan broj priključnih točaka je $2^{16} = 65536$. Priključne točke 0 do 1023 smatraju se poznatim (engl. *well known*) priključnim točkama i definirane su od strane organizacije IANA (Internet Assigned Numbers Authority). Priključne točke od 1024 do 49151 organizacije koje razvijaju aplikacije mogu registrirati u IANA-i, te se smatraju djelomično rezerviranim, a priključne točke iznad 49152 koriste klijentske aplikacije (npr. web preglednik kao svoju izvorišnu adresu).

Popis nekih najpoznatijih usluga s odgovarajućim priključnim točkama prikazan je na Slici 2.1.

Usluga	Priključna točka
FTP (File Transfer Protocol) - podaci	20
FTP (File Transfer Protocol) – upravljačke naredbe	21
SSH (Secure Shell)	22
Telnet	23
SMTP (Simpe Mail Transport Protocol)	25
DNS (Domain Name System)	53
HTTP (HyperText Transfer Protocol)	80
POP3 (Post Office Protocol version 3)	110
NTP (Network Time Protocol)	123
IMAP4 (Internet Message Access Protocol 4)	143
IMAP4 over SSL	993
POP3 over SSL	995

Slika 2.1: Neke od poznatih priključnih točaka

Osim adresiranja od korisnika do korisnika, funkcije prijenosne razine su uspostava i raskid logičkog kanala, pouzdanost, te kontrola toka i izbjegavanje zagušenja na kanalu.

Dva glavna protokola prijenosne razine su **TCP** (Transmission Control Protocol) i **UDP** (User Datagram Protocol). Glavna razlika između ova dva protokola je u načinu odnošenja prema podacima koje prenose. TCP protokol je pouzdan i osigurava da svi podaci dođu na odredište, ispravno poredani, dok je UDP protokol nepouzdan, ali kako koristi minimalno mehanizama za uspostavu komunikacije, prijenos podataka veoma je brz i učinkovit.

TCP (Transmission Control Protocol)

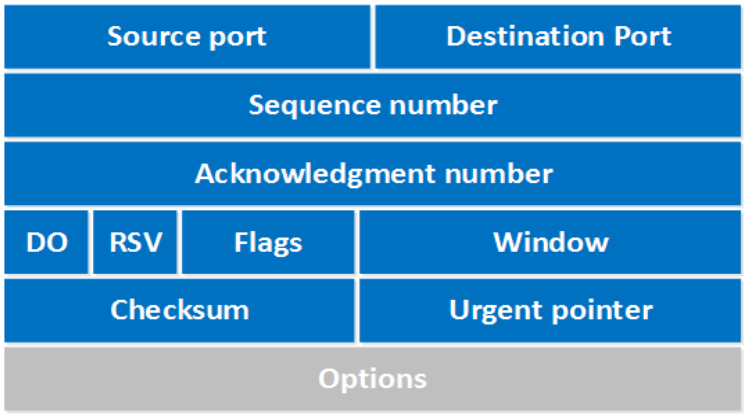
TCP protokol je protokol prijenosne razine koji osigurava pouzdani prijenos podataka preko mreže. Primjer koji pokazuje važnost pouzdanog prijenosa je npr. prijenos komprimirane (zip) datoteke. Možda ste se nekad susreli s porukom: "File is corrupted" kad ste pokušali raspakirati komprimiranu datoteku. Ukoliko je barem jedan bit u njoj neispravan ili nedostaje, datoteka se neće moći raspakirati.

Kako su datoteke koje prenosimo najčešće veće od maksimalne količine podataka koje u jednom odsječku možemo prenijeti, moramo ih rascjepkati na manje dijelove. Jedinice za prijenos podataka TCP protokolom nazivaju se **segmenti**.

Kad prenosimo komprimiranu datoteku moramo biti sigurni da će svaki poslani segment stići na odredište i da će se na odredištu svi segmenti moći složiti ispravnim redoslijedom. Takav način prijenosa nam osigurava TCP protokol svojim mehanizmom potvrde (engl. *acknowledgment*) koja provjerava je li svaki poslani segment zaista i stigao. Ukoliko izvorište nije dobilo potvrdu za neki od poslanih segmenata, nakon isteka unaprijed određenog vremena (timeout), segment se ponovo šalje (engl. *retransmission*). Mehanizmom numeriranja paketa (sequencing) osiguravamo da na osnovu rednog broja svaki segment na odredišnoj strani bude ispravno posložen.

Osim ova dva mehanizma, TCP osigurava i kontrolu brzine prijenosa podataka kako bi izbjegao nepotrebno gubljenje segmenata zbog potencijalnih zagušenja na mreži. Kontrola brzine prijenosa obavlja se mehanizmom prozora (engl. *window*) koji definira najveći broj segmenata koji se mogu poslati prije nego stigne potvrda. Ovaj broj se dinamički mijena, odnosno podiže se do prvog gubitka segmenta, nakon toga se smanjuje, da bi se nakon nekog vremena ponovo počeo povećavati i time optimalno iskoristio kanal koji nam stoji na raspolaganju.

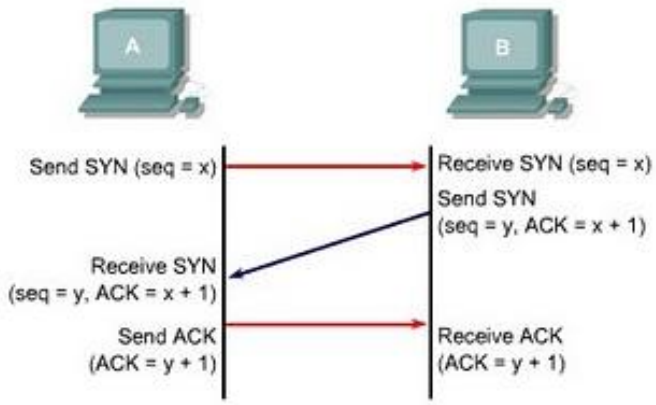
Svi ovi mehanizmi definirani su postavkama koje se zabilježene u poljima zaglavlja TCP protokola prikazanog na Slici 2.2.



Slika 2.2: Zaglavlje TCP protokola

Detaljnije o ostalim poljima u zaglavlju možete naći u materijalima s predavanja.

TCP protokol prije početka prijenosa uspostavlja logički kanal mehanizmom trostrukog rukovanja (engl. *three-way handshake*) koji je prikazan na Slici 2.3.



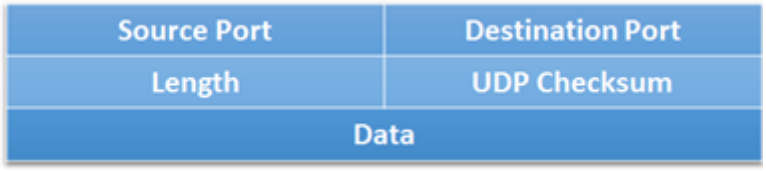
Slika 2.3: Mehanizam trostrukog rukovanja

UDP (User Datagram Protocol)

U nekim slučajevima pouzdanost koju osigurava TCP protokol nam uopće nije potrebna, ali bi nam veća brzina prijenosa mogla biti bitnija. Zamislimo da gledamo uživo prijenos nogometne utakmice između Hrvatske i Španjolske. Niz slika koji stiže do našeg zaslona već je podijeljen na manje odsječke koji se kod UDP protokola nazivaju datagrami. Ukoliko neki datagram ne stigne do nas mi ćemo to doživjeti kao mali crni kvadratić u cjelokupnoj slici i to samo na jedan tren, ali ćemo prijenos dalje nastaviti pratiti kao da se ništa nije dogodilo. Taj izgubljeni datagram naknadno nam zaista više ne treba, nemamo nikakve potrebe da nam ga izvorište ponovno šalje.

U ovom primjeru bitnije nam je da svi datagrami koji mogu stići do nas stignu što prije, a ne da čekaju u nekom redu dok ne dobiju dozvolu da se mogu poslati. Minimalna količina

mehanizama koju UDP koristi nam pridonosi kvaliteti prijenosa. Zbog te jednostavnosti UDP protokola i njegovo zaglavlje je bitno jednostavnije od zaglavlja TCP protokola i prikazano je na Slici 2.4.



Slika 2.4: Zaglavlje UDP protokola

Primjeri aplikacija koje koriste TCP i UDP protokole

Iz navedenih opisa TCP i UDP protokola možemo uočiti da će za neke aplikacije biti pogodnije koristiti jedan ili drugi protokol.

HTTP (Hypertext Transfer Protocol) protokol koji se koristi za komunikaciju između web poslužitelja i klijentskog preglednika koristi isključivo uslugu TCP protokola na prijenosnoj razini. Karakteristično za HTTP protokol je da za svaku sliku koja se prikazuje na stranici otvara zasebnu TCP vezu. Priključna točka za komunikaciju koja nije zaštićena enkripcijom je 80, a za stranice koje koriste certifikate i enkriptiraju sadržaj koristi se priključna točka 443.

Protokol za prijenos datoteka, FTP (File Transfer Protokol) također mora osigurati da odredište ispravno primi sve poslane podatke, te i on koristi usluge TCP protokola. Kod FTP-a se može uočiti da komunikacijski tok za prijenos datoteke i komunikacijski tok koji prenosi upravljačke naredbe (`get`, `put`, `cd`…) ne koriste istu priključnu točku, već da se za prijenos podataka koristi priključna točka 20, a za prijenos naredbi 21.

Neki protokoli mogu koristiti usluge oba protokola. Primjer jednog od takvih protokola je DNS (Domain Name System) koji omogućava dohvaćanje IP adrese računala na osnovu njegovog imena. U svrhu postizanja veće brzine komunikacija se odvija UDP protokolom, ali ukoliko odgovor ne stigne, komunikacija se prebacuje na TCP protokol. U oba slučaja koristi se priključna točka 53.

Vježba 2: Izvještaj

Zadatak 1

Pokrenite program Wireshark. Odaberite sučelje na kojem će te hvatati pakete. Ukoliko ste spojeni na Ethernet mrežu sučelje može imati naziv Ethernert # (neki broj) ili Local Area Connection # (neki broj), odnosno ukoliko ste spojeni na bežičnu mrežu naziv može biti WiFi. Započinje hvatanje svih paketa.

Otvorite web preglednik i u adresnu liniju unesite adresu https://www.oss.unist.hr/

Iz naredbene linije (engl. *Command Prompt, cmd*) naredbom `nslookup` pronađite IP adresu računala www.oss.unist.hr.

Korištenjem odgovarajućeg filtara izdvojite samo promet koji se odnosi na računalo www.oss.unist.hr.

U izvještaju navedite:

Naziv sučelja na kojem pratite promet: _____

Ime računala na kojem je podignut web site www.oss.unist.hr:

_____

IP adresa računala na kojem je podignut web site www.oss.unist.hr:

_____

Odaberite jedan od filtriranih paketa koji prenosi dio web stranice, recimo, u stupcu Info sadrži potvrdu [ACK] i neke je veće duljine. Pri tome možete koristiti složeniji filtar oblika: `ip.src == xxx.xxx.xxx.xxx and ip.len >= 1000 and tcp.flags.ack==1`.

U dijelu zaglavlja koji se odnosi na IP protokol pronađite sljedeće informacije:

Izvorišna IP adresa: _____

Odredišna IP adresa: _____

U dijelu zaglavlja koje se odnosi na TCP protokol pronađite sljedeće informacije:

Izvorišna priključna točka: _____

Odredišna priključna točka: _____

Možete li pročitati sadržaj bilo kojeg od dobivenih paketa? _____

Zašto? _____

Zadatak 2

Prekinite hvatanje paketa iz zadatka 1. Naredbom `nslookup` odredite IP adresu računala luna.fesb.hr i zabilježite je:

IP adresa računala luna.fesb.hr _____

Pokrenite novo hvatanje paketa i u web pregledniku otiđite na stranicu http://luna.fesb.hr/rm

U ispisu aplikacije Wireshark primijenite filtar koji će izdvojiti pakete kojima je izvorište IP adresa računala luna.fesb.hr, a samo su HTTP paketi. Filtar bi mogao izgledati: `ip.src ==xxx.xxx.xxx.xxx and http`

Pronađite paket koji u Info polju sadrži dio (text/html).

Možete li pročitati sadržaj podatkovnog dijela paketa (na samom kraju paketa)?

_____

Što je zabilježeno? _____

_____

Zašto smo sada mogli pročitati podatke?

_____

Zadatak 3

Pokrenite aplikaciju Wireshark (ili samo pokrenite novo hvatanje paketa).

Iz naredbene linije (cmd) korištenjem naredbe `ipconfig /flushdns` počistite prethodno zabilježene IP adrese računala.

Korištenjem naredbe `nslookup` doznajte IP adresu računala eduplan.oss.unist.hr. Zabilježite sljedeće:

IP adresa računala eduplan.oss.unist.hr: _____

IP adresa DNS poslužitelja koji je ponudio odgovor: _____

Ostali nazivi računala (aliasi), ukoliko postoje: _____

U aplikaciji Wireshark primijenite filtar koji će izdvojiti samo DNS pakete (filtar `dns`).

Kojim redom su zabilježeni paketi? Zabilježite:

prvi upit: _____

prvi odgovor: _____

drugi upit: _____

drugi odgovor:_____

Koji je protokol prijenosne razine izvršio komunikaciju? _____

Koja se priključna točka koristila na poslužitelju? _____

Koja se priključna točka koristila na vašem računalu? _____

3. Internet razina, IP adrese, podmrežavanje

Internet razina TCP/IP modela zadužena je za uspostavu komunikacije s kraja na kraj mreže. Ključne funkcije internet razine su **adresiranje** i **usmjeravanje**. Izvorište i odredište moraju imati jedinstvenu IP adresu na osnovu koje će uređaji koji usmjeravaju promet kroz mrežu moći odrediti optimalnu putanju. Određivanje puta paketa kroz mrežu naziva se usmjeravanje, a obavljaju ga usmjernici.

Dva tipa protokola povezana su s funkcijama internet razine: usmjeravani (engl. *routed*) i usmjerivački protokoli (engl. *routing*). Najčešće korišteni usmjeravani protokol internet razine je **IP protokol**. Usmjerivački protokoli, ovisno o njihovoj strukturi, mogu koristiti usluge IP protokola, ali i nekog od protokola prijenosne razine (UDP) čime se donekle narušava fiksni format komunikacije prema razinama, ali funkcija se zadržava na za to predviđenoj razini.

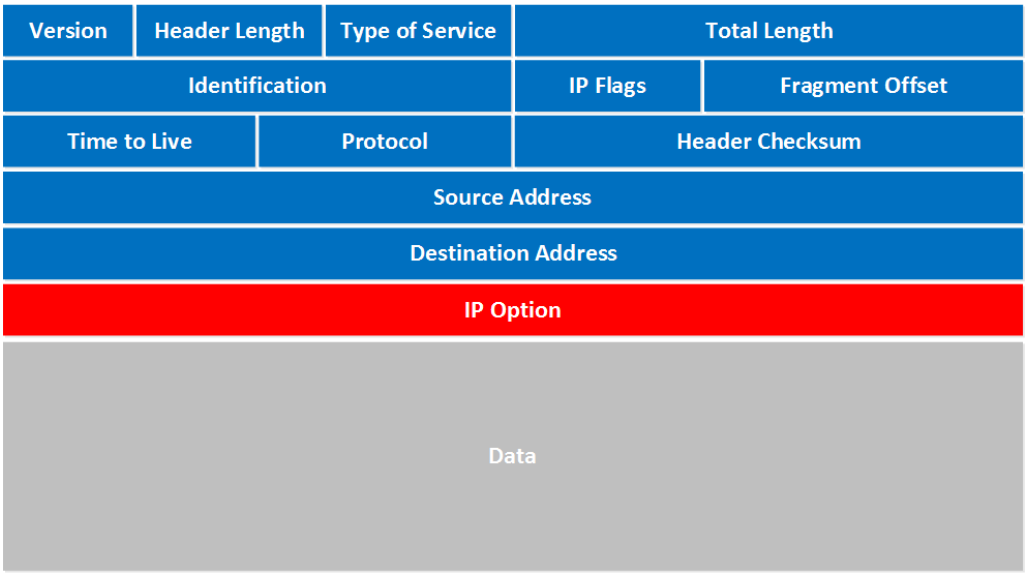
IPv4 protokol ima relativno ograničen broja adresa (2^{32}, odnosno približno 4×10^{9}) kojima može adresirati uređaje na mreži i taj broj je danas već potrošen. Mehanizmima podmrežavanja (engl. *subnetting*) i korištenjem rezerviranih blokova privatnih adresa, te uporabom NAT (Network Address Translation) protokola produžujemo vijek trajanja verzije 4. Još krajem 20. stoljeća definiran je standard nove verzije protokola, IPv6, za koju se već očekivalo da će postati dominantna na svjetskoj razini. Broj adresa koje se mogu upotrijebiti u IPv6 protokolu je 2^{128} (približno 3×10^{38}). Zbog relativno velikog broja uređaja spojenih na internet koji ne podržavaju IPv6 protokol on još nije preuzeo vodeću riječ.

IPv4 (Internet Protocol ver. 4)

IP protokol je tzv. best effort protokol, odnosno protokol koji ne garantira pouzdani prijenos podataka već se, ukoliko je to potrebno, za obavljanje te funkcije oslanja na pouzdani protokol prijenosne razine (TCP).

Osnovna jedinca prijenosa IP protokola naziva se paket.

Dva najbitnija polja u IP zaglavlju su izvorišna i odredišna IP adresa. IP adresa je 32-bitno polje. Zaglavlje IP protokola prikazano je na Slici 3.1. Detaljan opis ostalih polja možete pronaći u materijalima s predavanja.



Slika 3.1: Izgled zaglavlja IP paketa

IPv4 adrese

IPv4 adresa sastoji se od dijela koji identificira mrežu i dijela koji identificira računalo unutar mreže. U takvoj podjeli adresa se uvijek gleda kao niz binarnih znamenki odvojenih u 4 skupine po 8 znamenki. Tako je IP adresa računala moodle.oss.unist.hr u dekadskom zapisu:

`193.198.34.9`

a u binarnom:

`11000001.11000110.00100010.00001001`

Ukoliko vam je potrebno podsjetiti se kako se obavlja pretvorba iz dekadskog u binarni zapis, ili obrnuto, možete posjetiti stranicu:

https://www.learncisco.net/courses/icnd-1/lan-connections/binary-basics.html

Podjela na klase

IPv4 adrese podijeljene su u 5 klasa.

Kod adresa **klase A** prvih 8 bitova identificiraju mrežu, a ostalih 24 računala unutar mreže. Prva znamenka binarne adrese u klasi A je 0. Time klasa A koristi 50% ukupnog broja adresa u IPv4 adresnom prostoru. Ostale klase imaju prvu znamenku 1. Ostalih 7 binarnih znamenki (bitova) mrežnog dijela adrese omogućavaju razlikovanje 2^7 mreža u kojima se može adresirati 2^{24} adresa.

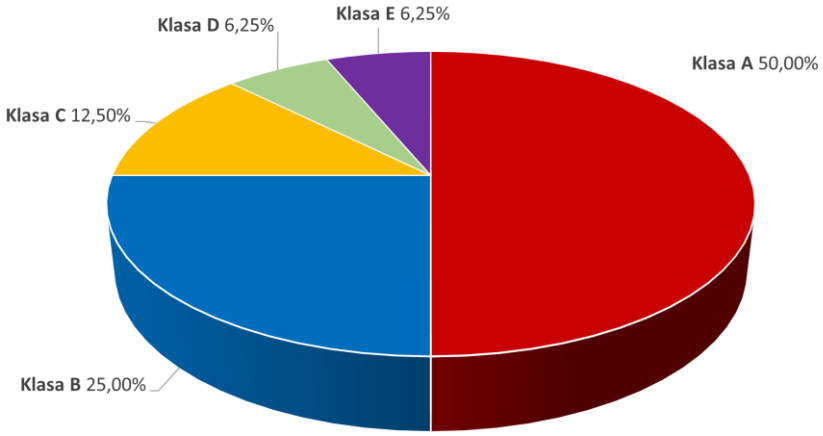
Kod adresa **klase B** prvih 16 bitova identificiraju mrežu, a ostalih 16 računala unutar pojedine mreže. Prva dva bita u klasi B su 10 čime ostaje 14 bitova za razlikovanje mreža, odnosno, u

klasi B možemo imati 2^{14} mreža s po 2^{16} adresa. Broj adresa koji pripada B klasama iznosi 25% ukupnog broja adresa.

Kod adresa **klase C** prva 24 bita identificiraju mrežu, a preostalih 8 računala. Prva 3 bita su 110, tako da za identifikaciju mreža ostaje 21 bit, odnosno, možemo imati 2^{21} mreža s po 2^{8} adresa.

Ostatak adresnog prostora podijeljen je podjednako na klase D i E. **Klasa D** koristi se za grupni (engl. *multicast*) prijenos, a prva četiri bita su 1110. **Klasa E** je ostavljena za eksperimentalne svrhe i prva 4 bita su 1111.

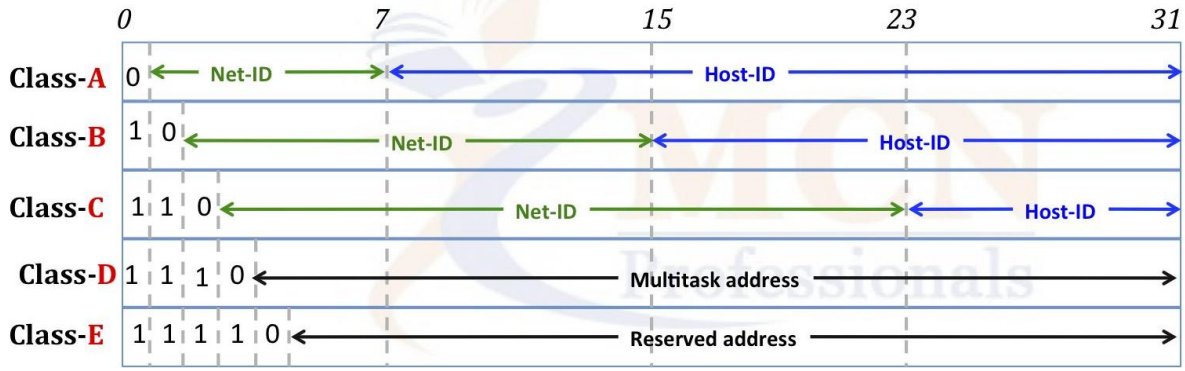
Na Slici 3.2 prikazan je omjer klasa u ukupnom broju adresa.



Slika 3.2: Omjer broja adresa po klasama

Iz Slike 2 vidljivo je da je 50% ukupnog broja adresa u IPv4 adresnom prostoru dodijeljen malom broju (128) mreža. Svaka od tih mreža sadrži 16,777,216 adresa. Mreže veličine 256 adresa (klasa C) koriste svega 12,5% ukupnog broja adresa.

Na Slici 3.3 prikazana je podjela adresa po klasama grafički.



Slika 3.3: Klase IPv4 adresa

Na Slici 3.4 prikazani su rasponi adresa u pojedinim klasama.

Klasa	Raspon adresa
A	1.0.0.0 – 126.255.255.25
B	128.0.0.0 – 191.255.255.255
C	192.0.0.0 – 223.255.255.255
D	224.0.0.0 – 239.255.255.255
E	240.0.0.0 – 254.255.255.255

Slika 3.4: Rasponi adresa u klasama

Iz Slike 3.4 mogu se uočiti dvije stvari:

1. na osnovu prvog okteta, odnosno prvog broja u IPv4 adresi može se znati kojoj klasi ta adresa pripada
2. pojedine adrese mreža nisu uključene u raspon adresa koje se mogu dodijeliti i rezervirane su za posebne namjene:
    - mreža 0.0.0.0 rezervirana je za standardnu oznaku za **unaprijed definiranu stazu** (engl. *default route*) za usmjeravanje paketa
    - mreža 127.0.0.0 rezervirana je za "vlastitu", odnosno "**povratnu" adresu** (engl. *loopback*) preko koje se može testirati ispravnost TCP/IP skupa protokola bez da je računalo zaista spojeno na mreži
    - mreža 255.0.0.0 rezervirana je za **generalnu univerzalnu adresu** (engl. *broadcast address*)

Osim navedenih rezerviranih mreža bitno je napomenuti da su i dvije adrese unutar svakog raspona rezervirane:

- adresa koja u dijelu namijenjenom za adresiranje računala ima sve **nule** (0) je **adresa mreže**, npr. 193.198.0.0
- adresa koja u dijelu namijenjenom za adresiranje računala ima sve **jedinice** (1) je **univerzalna adresa** (engl. *broadcast*) mreže, npr. 161.53.255.255

Iz ovog razloga stvarni broj adresa koji se može dodijeliti uređajima u pojedinoj mreži je $\mathbf{2^n-2}$, gdje je n broj binarnih znamenki koji se odnosi na računala, npr. raspoloživ broj adresa u mreži koja pripada C klasi je $2^8-2=254$.

Mrežne maske i IPv4 podmreže

Mrežna maska (engl. *subnet mask*) je 32-znamenkasti binarni broj koji jedinicama određuje koje znamenke IP adrese se odnose na mrežu. Znamenke koje se odnose na računala u mrežnoj maski imaju vrijednost 0. Mrežna maska se, kao i IPv4 adresa, radi preglednosti

prikazuje dekadskim znamenkama. Treći način prikaza je tzv. / (kroz) zapis (engl. *slash notation*) koji iza IPv4 adrese navodi broj bitova koji se odnose na dio adrese namijenjen mreži, npr. /24.

Kako je podjela na klase napravljena na način da je u svakoj klasi definirano koje se znamenke adrese odnose na mrežu, a koje na računalo, mrežne maske klasa su unaprijed definirane.

Mrežna maska za klasu A je:

11111111.00000000.00000000.00000000 ili 255.0.0.0 ili /8

Mrežna maska za klasu B je:

11111111.11111111.00000000.00000000 ili 255.255.0.0 ili /16

Mrežna maska za klasu C je:

11111111.11111111.11111111.00000000 ili 255.255.255.0 ili /24

Stoga nam Windows operacijski sustav pri ručnom unošenju IPv4 adrese automatski ponudi mrežnu masku prema klasi kojoj adresa pripada.

Dok se mreže unutar klasa nisu dalje dijelile ili spajale, mrežna maska nam nije bila potrebna, odnosno, podrazumijevala se.

Relativno brzo se uočio problem da će podjela adresa na klase izazvati nedostatak raspoloživih mreža što bi rezultiralo time da bi upotreba interneta, odnosno povezivanje dodatnih subjekata u mrežu, postalo nemoguće. Prvi korak prema rješavanju nastalog problema bio je omogućavanje podjele jedne velike mreže na veći broj manjih mreža. Kako bi se to ostvarilo, moralo se početi koristiti mrežne maske. One su tada definirale stvarnu veličinu pojedine podmreže.

Na primjer, jednu mrežu srednje veličine koja pripada B klasi može se podijeliti na 16 podmreža u kojoj bi svaka podmreža imala 4096 (2^{12}) adresa. Kako bi se osiguralo 16 mreža, od dijela adrese namijenjenog adresiranju računala potrebno je posuditi 4 bita, 2^4=16 čime za adresiranje računala ostaje 12 bitova.

MMMMMMMM.MMMMMMMM.mmmmrrrr.rrrrrrrr (M, m – mreža, r – računalo)

11111111.11111111.11110000.00000000

Zelenom bojom prikazani su bitovi koji standardno pripadaju adresi mreže klase B, a crvenom bitovi koji su posuđeni kako bi se napravio veći broj mreža.

Ostali zapisi ove mrežne maske su:

255.255.240.0 ili /20

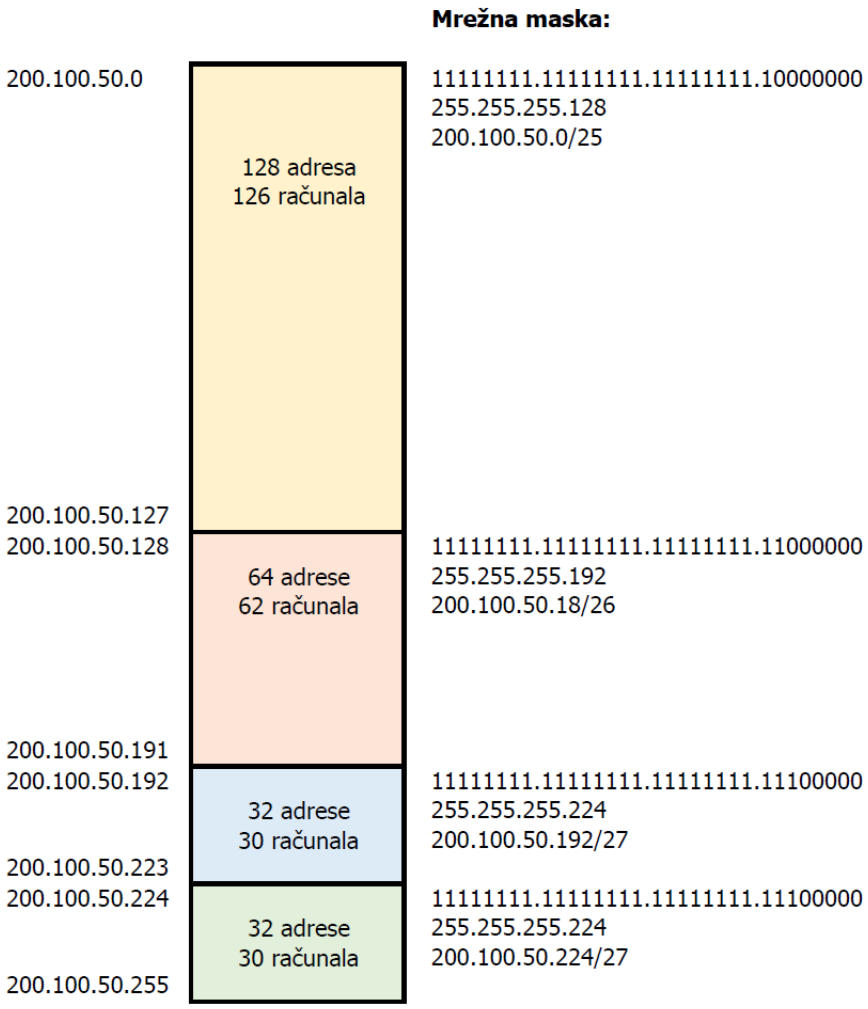
Tablica koja može pomoći pri početnom snalaženju u podjeli mreža klase B prikazana je na Slici 5. Slična tablica može se izvesti i za ostale mrežne klase.

Prefix Length	Subnet Mask	Subnet in Binary Network = N, Host = H, Borrowed = n Total IP addresses in /16 Network = 65536.	Available Network	Usable Host Per Network
/17	255.255.128.0	NNNNNNNN.NNNNNNNN.nHHHHHHH.HHHHHHHH 11111111.11111111.10000000.00000000	2^1=2	2^{15}-2 =32766
/18	255.255.192.0	NNNNNNNN.NNNNNNNN.nnHHHHHH.HHHHHHHH 11111111.11111111.11000000.00000000	2^2=4	2^{14}-2 =16382
/19	255.255.224.0	NNNNNNNN.NNNNNNNN.nnnHHHHH.HHHHHHHH 11111111.11111111.11100000.00000000	2^3=8	2^{13}-2 =8190
/20	255.255.240.0	NNNNNNNN.NNNNNNNN.nnnnHHHH.HHHHHHHH 11111111.11111111.11110000.00000000	2^4=16	2^{12}-2 =4094
/21	255.255.248.0	NNNNNNNN.NNNNNNNN.nnnnnHHH.HHHHHHHH 11111111.11111111.11111000.00000000	2^5=32	2^{11}-2 =2046
/22	255.255.252.0	NNNNNNNN.NNNNNNNN.nnnnnnHH.HHHHHHHH 11111111.11111111.11111100.00000000	2^6=64	2^{10}-2 =1022
/23	255.255.254.0	NNNNNNNN.NNNNNNNN.nnnnnnnH.HHHHHHHH 11111111.11111111.11111110.00000000	2^7=128	2^9-2 =510
/24	255.255.255.0	NNNNNNNN.NNNNNNNN.nnnnnnnn.HHHHHHHH 11111111.11111111.11111111.00000000	2^8=256	2^8-2 =254
/25	255.255.255.128	NNNNNNNN.NNNNNNNN.nnnnnnnn.nHHHHHHH 11111111.11111111.11111111.10000000	2^9=512	2^7-2 =126
/26	255.255.255.192	NNNNNNNN.NNNNNNNN.nnnnnnnn.nnHHHHHH 11111111.11111111.11111111.11000000	2^{10}=1024	2^6-2 =62
/27	255.255.255.224	NNNNNNNN.NNNNNNNN.nnnnnnnn.nnnHHHHH 11111111.11111111.11111111.11100000	2^{11}=2048	2^5-2 =30
/28	255.255.255.240	NNNNNNNN.NNNNNNNN.nnnnnnnn.nnnnHHHH 11111111.11111111.11111111.11110000	2^{12}=4096	2^4-2 =14
/29	255.255.255.248	NNNNNNNN.NNNNNNNN.nnnnnnnn.nnnnnHHH 11111111.11111111.11111111.11111000	2^{13}=8192	2^3-2 =6
/30	255.255.255.248	NNNNNNNN.NNNNNNNN.nnnnnnnn.nnnnnnHH 11111111.11111111.11111111.11111100	2^{14}=8192	2^2-2 =2

Slika 3.5: Podjele mreže klase B na podmreže

Na Slici 3.5 vide se mrežne maske za pojedinu podjelu, broj dobivenih podmreža, odnosno, broj računala koji se može adresirati u pojedinoj podmreži. Uočimo da nam je potrebno ostaviti barem 2 bita za adrese računala jer podmreža koja bi imala samo jedan bit ostavljen za adrese računala ne bi bila upotrebljiva. S jednim bitom možemo adresirati 2 adrese, a već znamo da bi u tom slučaju obje adrese već bile iskorištene: za adresu mreže i univerzalnu adresu.

Potrebno je još napomenuti da sve podmreže ne moraju imati istu veličinu. Na primjer, mrežu klase C možemo prvo podijeliti posudbom 1 bita čime dobijemo dvije podmreže od po 128 adresa, a zatim jednu od njih dijeliti dalje. Ni sljedeća podjela ne mora biti ujednačena. Na ovaj način dobivamo mrežne maske različitih veličina, VLSM (engl. *Variable Length Subnet Mask*). Primjer jedne od podjela prikazan je na Slici 3.6.



Slika 3.6: Primjer podjele na podmreže različitih veličina

Primjena mrežne maske

Mrežnu masku koristimo kako bi na osnovu nje i adrese računala dobili adresu podmreže u kojoj se računalo nalazi. Adresu mreže dobijemo kad binarno "pomnožimo" IP adresu i mrežnu masku koristeći operaciju logičko AND (logičko I):

```
IP adresa:        8.20.15.1 = 00001000.00010100.00001111.00000001    AND
Mrežna maska:  255.240.0.0 = 11111111.11110000.00000000.00000000
Adresa mreže:      8.16.0.0 = 00001000.00010000.00000000.00000000
```

Iz dobivenog rezultata vidimo da računalo pripada podmreži 8.16.0.0 (i to je adresa te podmreže, odnosno, adresa gdje su svi bitovi dijela za računalo u 0), a univerzalnu adresu dobijemo kad bitove dijela adrese namijenjene adresiranju računala postavimo u 1:

```
IP adresa:              8.20.15.1 = 00001000.00010100.00001111.00000001
Mrežna maska:        255.240.0.0 = 11111111.11110000.00000000.00000000
Univerzalna adresa: 8.31.255.255 = 00001000.00011111.11111111.11111111
```

Privatne adrese

Podjela klasa na podmreže samo je malo usporila brzo nestajanje dostupnih IPv4 adresa. Glavni koncept koji je omogućio da globalna mreža i danas funkcionira, iako su i zadnji blokovi slobodnih adresa podijeljeni pružateljima interneta još 2013. godine, je upotreba privatnih adresa. Već su u samom početku, prilikom donošenja standarda koji definira IP protokol i format adresa, rezervirani blokovi tzv. privatnih adresa. Tada je bilo zamišljeno da se te adrese koriste u mrežama koje uopće nisu trebale biti spajane na internet, ali su željele koristiti TCP/IP skup protokola.

Rezervirani blokovi privatnih adresa po klasama su:

- u dijelu klasa A: cijela **10.0.0.0/8** mreža
- u dijelu klasa B: raspon od 16 klasa B definiran adresama od 172.16.0.0 do 172.31.255.255, odnosno, **172.16.0.0/20**
- u dijelu klasa C: raspon do 256 klasa C definiran adresama od 192.168.0.0 do 192.168.255.255, odnosno, **192.168.0.0/16**

Ove adrese ne mogu se usmjeravati na internetu i usmjernici ih trebaju odbacivati, ali primjenom NAT protokola (engl. *Network Address Translation*) mogu se prevoditi u jednu ili više javnih adresa i na taj način omogućiti znatno povećanje ukupnog broja računala koja mogu koristiti mrežu internet.

Vježba 3: Izvještaj

Zadatak 1

Za zadane IP adrese i mrežne maske odrediti:

- adresu mreže
- broadcast adresu
- broj računala koji se može adresirati u toj mreži

a) 172.25.46.118/20
b) 10.10.100.200/10
c) 192.168.48.55/27

U rješenju raspisati postupak određivanja traženih podataka.

Zadatak 2

Organizacija se sastoji od 4 odjela: Prodaja, Servis, IT služba i Uprava. U Prodaji je 80 računala, u Servisu 40 računala, IT službi 18 i Upravi 7.

Odredite jednu od mogućih podjela mreže 192.186.5.0 na podmreže koje bi zadovoljavale navedene potrebe (ispisati adrese podmreža, mrežne maske, te veličinu svake podmreže, odnosno broj računala koji se može spojiti u tu podmrežu).

4. Usmjerivački protokoli i usmjeravanje

Druga ključna funkcija internet razine, uz adresiranje, je **usmjeravanje** paketa. Funkcija usmjeravanja paketa sastoji se od dva procesa. Jedan je određivanje optimalnog puta kroz mrežu do odredišta i bilježenje te staze u usmjerivačke tablice. Drugi proces je određivanje sučelja na koje će se paket poslati na osnovu informacija pohranjenih u usmjerivačkim tablicama.

Usmjernik je uređaj mrežne razine koji koristi jednu ili više usmjerivačkih metrika kako bi odredio optimalni put kojim bi usmjerio mrežni promet. **Usmjerivačka metrika** je vrijednost koja se koristi da bi se odredio stupanj prednosti jedne staze u odnosu na druge. Neki usmjerivački protokoli koriste samo jednu vrijednost za određivanje metrike, dok drugi koriste više vrijednosti u tzv. kompozitnoj metrici. Tipično se koriste sljedeće metrike:

- propusnost (engl. *bandwidth*) - kapacitet linka
- kašnjenje (engl. *delay*) - vrijeme potrebno da paket stigne kroz sve linkove do odredišta
- opterećenje (engl. *load*) - količina aktivnosti na pojedinom usmjerniku i/ili linku
- pouzdanost (engl. *reliability*) - vjerojatnost pogreške na linku
- broj skokova (engl. *hop count*) - broj usmjernika kroz koje paket mora proći na putu do odredišta
- cijena (engl. *cost*) - proizvoljna vrijednost, obično zasnovana na propusnosti, stvarnoj cijeni ili nekoj drugoj mjeri, dodjeljuje je administrator

Usmjerivačke tablice

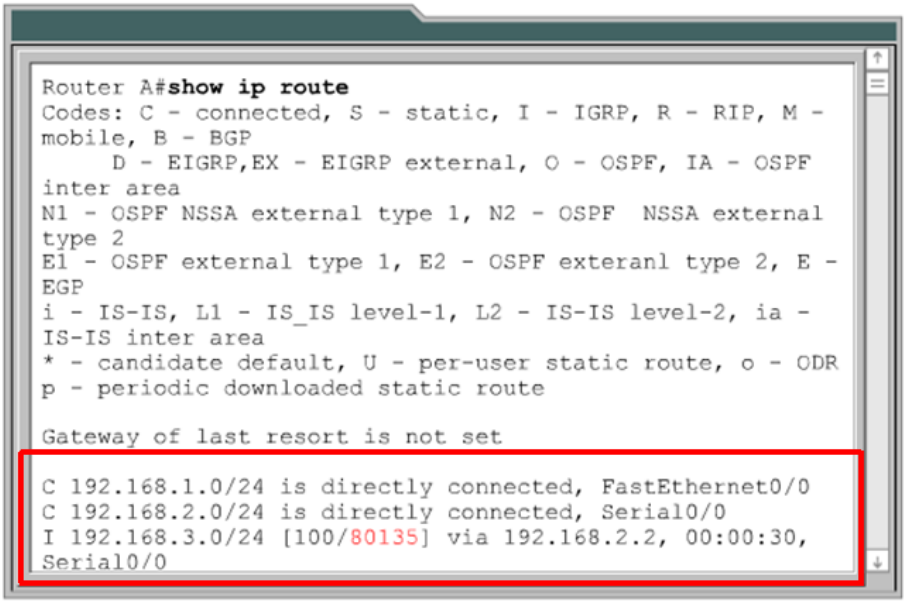
Usmjerivačke tablice se popunjavaju na dva načina: statički ili dinamički. **Statički** znači da administrator mreže ručno unosi zapise o pojedinim mrežama u tablicu i ti se zapisi samostalno ne mijenjaju, odnosno, ukoliko dođe do promjene topologije mreže, administrator mora, opet ručno, unositi te promjene u tablice. **Dinamički** unos u usmjerivačke tablice obavljaju usmjerivački protokoli.

Informacije sadržane u usmjerivačkim tablicama su:

- tip protokola – podatak koji identificira protokol koji je kreirao taj zapis
- povezivanje sljedećeg skoka - odredište je ili direktno spojeno na usmjernik ili se može doseći preko drugog usmjernika koji se naziva sljedeći skok (engl *next-hop*)
- usmjerivačka metrika - mjera poželjnosti staze (npr. broj skokova, brzina veze, propusnost, opterećenje, cijena…)
- izlazno sučelje - sučelje na koje se paket treba poslati da bi došao do odredišta

Neki usmjerivački protokoli šalju osvježavanja periodično, a drugi ukoliko dođe do promjene topologije mreže.

Primjer usmjerivačke tablice prikazan je na Slici 4.1.



Slika 4.1: Prikaz usmjerivačke tablice na Cisco usmjerniku

Određivanje puta kroz mrežu

Određivanje puta kroz mrežu je proces koji se koristi za određivanje staze za svaki pojedini paket kojeg treba usmjeriti. Proces se sastoji od sljedećih koraka:

- iz zaglavlja paketa pročita se odredišna IP adresa
- na odredišnu adresu primijeni se mrežna maska iz prvog zapisa u usmjerivačkoj tablici
- adresa maskirane mreže koja se dobije usporedi se sa zapisom u usmjerivačkoj tablici
- ukoliko se mreže poklapaju, paket se prosljeđuje na sučelje povezano sa zapisom u tablici
- ukoliko se mreže ne poklapaju, provjerava se sljedeći zapis u tablici (primijeni se njegova mrežna maska i usporedi adresa dobivene mreže)
- ukoliko paket ne odgovara niti jednom zapisu u tablici, provjerava se je li postavljena zadana staza (engl. *default route*)
- ukoliko je zadana staza postavljena, paket se prosljeđuje na odgovarajuće sučelje
- ukoliko nema zadane staze, paket se odbacuje

Zadana staza je zapis u usmjerivačkoj tablici koji određuje sučelje na koje će se proslijediti paket koji nije namijenjen niti jednoj mreži navedenoj u tablici. Najčešće se radi o sučelju koje je spojeno na mrežu preko koje se dalje spajamo na internet. Zadana staza se označava kao adresa mreže sa svim nulama: 0.0.0.0

Podjela usmjerivačkih protokola

Usmjerivački protokoli dijele se na vanjske i unutarnje usmjerivačke protokole.

Vanjski usmjerivački protokoli izmjenjuju informacije o stazama između autonomnih sustava. Autonomni sustav je mreža kojom upravlja jedan pružatelj usluge spajanja na internet, npr. kod nas je to CARNet, T-com, A1… Primjeri vanjskih usmjerivačkih protokola su Exterior Gateway Protocol (EGP) i Border Gateway Protocol (BGP).

Unutarnji usmjerivački protokoli razmjenjuju informacije o stazama unutar autonomnog sustava. Unutarnji usmjerivački protokoli prema načinu rada dijele se na protokole temeljene na **vektoru udaljenosti** (engl. *distant vector protocols*) i protokole temeljene na **stanju veze** (engl. *link-state protocols*).

Protokoli temeljeni na vektoru udaljenosti

Protokoli temeljeni na vektoru udaljenosti periodički prosljeđuju kopije usmjerivačkih tablica od usmjernika do usmjernika i kroz ta redovita osvježavanja usmjernicima dojavljuju promjenu topologije. Algoritam koji koriste ovi protokoli za izračun najbolje staze naziva se Bellman-Ford algoritam. Usmjernici koji imaju konfiguriran neki od protokola temeljenih na vektoru udaljenosti ne posjeduju sliku cijele topologije mreže, već vide samo susjedne usmjernike i od njih primaju usmjerivačke tablice, te u njih dodaju potrebne parametre (povećaju udaljenost, cijenu…) i zapisuju nove podatke u svoje tablice. Neki od ovih protokoli koriste jednostavnu, a neki složenu metriku. Primjeri protokola su **RIP** (Routing Information Protokol) koji je otvoreni standard i **IGRP** (Interior Gateway Routing Protokol) koji je u vlasništvu firme Cisco.

RIP (Routing Information Protokol)

RIP je najjednostavniji protokol temeljen na vektoru udaljenosti. Metrika mu je definirana samo brojem skokova. Ukoliko je broj skokova veći od 15 paket se odbacuje. Predefinirani vremenski interval u kojem šalje osvježenja svoje tablice iznosi 30 sekundi.

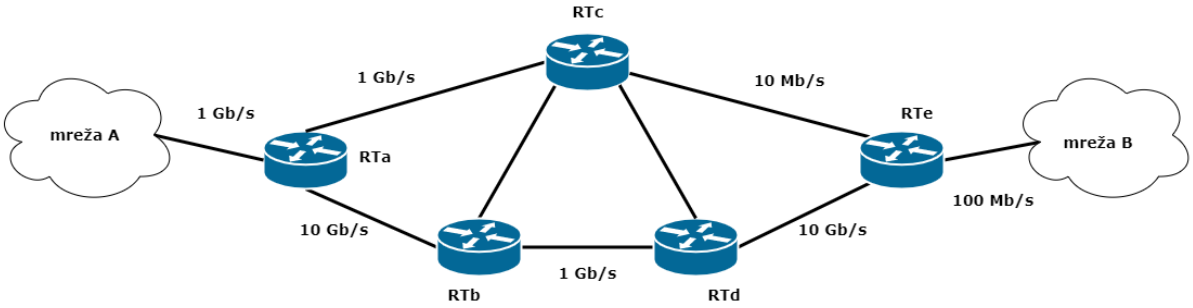
Protokoli temeljeni na stanju linka

Protokoli temeljeni na stanju linka za određivanje staza kroz mrežu algoritam najkraćeg puta (engl. *shortest path first – SPF*). Informacije koje dobivaju pohranjuju u kompleksnu bazu podataka topoloških informacija na osnovu koje imaju potpuno znanje o udaljenim usmjernicima i načinu kako su povezani. Ovi protokoli zahtijevaju veću procesorsku snagu i više memorija za rad, te više koriste mrežu jer je inicijalno preplavljuju paketima sa svim potrebnim informacijama (engl. *Link State Advertisements - LSA*). Primjeri protokola temeljenih na stanju linka su **OSPF** (Open Shortest Path First) i **IS-IS** (Intermediate System to Intermediate System).

Vježba 4: Izvještaj

Zadatak 1

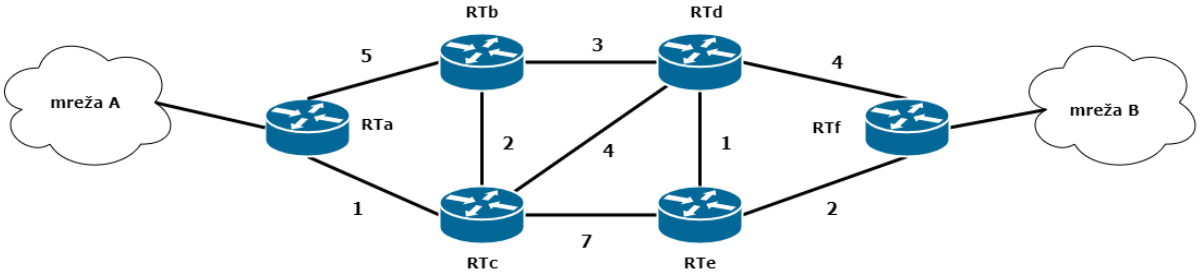
U mreži prikazanoj na slici za usmjeravanje se koristi RIP protokol. Odredite optimalni put od mreže A do mreže B



U rješenju raspisati postupak određivanja traženih podataka.

Zadatak 2

U mreži čija je topologija prikazana na slici koristi se kompozitna metrika. Težine pojedinih linkova prikazane su brojevima. Manja metrika znači poželjnija staza. Odredite optimalni put paketa od mreže A do mreže B.



U rješenju raspisati postupak određivanja traženih podataka.

Zadatak 3

Koristeći priloženi dio ispisa tablice usmjeravanja odrediti na koje sučelje usmjernika će biti proslijeđen paket s odredišnom adresom 172.21.10.7.

```
Fa0   172.23.255.254   255.254.0.0
Fa1   172.16.1.1       255.255.192.0
Se0   10.0.7.254       255.255.0.0
Se1   0.0.0.0          0.0.0.0
```

U rješenju raspisati postupak određivanja traženih podataka.

Zadatak 4

Pokrenuti naredbeni redak (engl. *Command Prompt*) korištenjem naredbe `cmd`. Korištenjem naredbe `tracert` ispratite kroz koje usmjernike prolazi paket do odredišta `www.google.com`.

U izvještaju navedite ispis naredbe.

5. Razina pristupa mreži, Ethernet, ARP

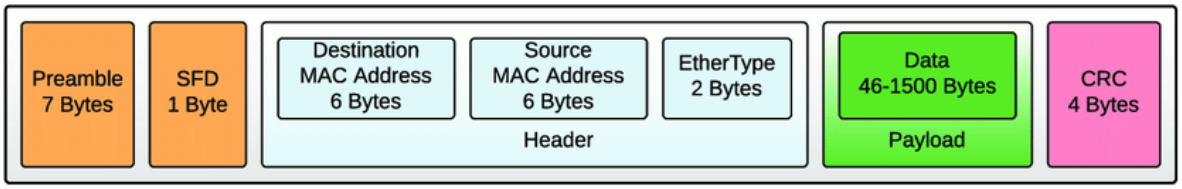
Razina pristupa mreži je prvi razina TCP/IP arhitekture. Integrira funkcije prve dvije razine ISO/OSI arhitekture: **fizičke** razine i **podatkovne** razine. Na ovoj razini određuju se fizičke, mehaničke i električne karakteristike kabela i mrežnih uređaja (funkcije fizičke razine ISO/OSI arhitekture), kao i funkcije kontrole pogreške i lokalnog adresiranja (funkcije podatkovne razine ISO/OSI arhitekture).

Ethernet protokol

Ethernet skupina protokola definira prijenos podatka preko različitih medija (tanki i debeli koaksijalni kabel, oklopljene i neoklopljene isprepletene parice, optički kabeli, bežični medij).

Brzine prijenosa su kroz godine rasle, tako da pokriva raspone od 10Mb/s do 10Gb/s, iako su već doneseni i standardi tzv. terabitnog Etherneta koji pokriva brzine preko 100Gb/s. Zadnji standard u nizu donesen je u siječnju 2020. godine pod nazivom IEEE 802.3cm i definira prijenos brzinama od 400 Gb/s preko 4-paričnog i 8-paričnog multimodnog optičkog kabela. Oprema koja se danas standardno prodaje za krajnje korisnike podržava brzine 10/100/1000Mb/s.

Podatke koje primi od protokola više razine (tipično IP protokola) Ethernet protokol enkapsulira u **okvir** (engl. *frame*) koji je osnovna podatkovna jedinica na razini pristupa mreži. Zaglavlje Ethernet protokola prikazano je na Slici 5.1. Zelenom bojom označeni su podaci koje Ethernet protokol prima od protokola više razine, a ostala polja se dodaju na ovoj razini.



Slika 5.1: Polja Ethernet okvira

Najbitnija polja u Ethernet zaglavlju su izvorišna i odredišna MAC adresa te CRC polje. MAC adrese definiraju lokalne adrese koje su vidljive unutar lokalne mreže, a CRC polje predstavlja zaštitnu sumu okvira na osnovu koje se određuje je li došlo do pogreške bitova u prijenosu, odnosno, treba li okvir radi toga odbaciti.

MAC adrese

MAC (Media Access Control) adresa je fizička adresa mrežnog uređaja i definirana je u procesu proizvodnje uređaja. Pohranjena je u ROM (engl. Read Only Memory) memoriji uređaja i nije promjenjiva. Sastoji se od 48 bitova podijeljenih u 6 bajtova. Primjer MAC adrese:

B8-8A-60-E7-1E-68

Prva tri bajta adrese definiraju proizvođača i nazivaju se OUI (engl. Organizational Unique Identifier). IEEE Registration Authority Committee dodjeljuje ovaj identifikator registriranim proizvođačima. Preostala tri bajta jedinstveno definiraju mrežno sučelje uređaja. Na internetu su mogu naći online baze koje sadrže popise dodijeljenih OUI-a, npr. https://dnschecker.org/mac-lookup.php.

Ovako formirana MAC adresa jedinstvena je na svijetu, ali nemamo praktičan način bilježenja i organizacije svakog pojedinog uređaja spojenog na mrežu u svakom trenutku, te se ipak ne može koristiti za globalno adresiranje.

Ukoliko neki uređaj ima više mrežnih sučelja (npr. usmjernik ili računalo više mrežnih kartica, Ethernet karticom i bežičnom karticom), svako sučelje ima svoju MAC adresu.

ARP protokol

Postupak formiranja podataka u zaglavlju Ethernet protokola ne može se obaviti ukoliko se ne zna odredišna MAC adresa. ARP protokol (engl. Address Resolution Protocol) doznaje MAC adresu odredišnog uređaja na osnovu njegove IP adrese.

Svako računalo spojeno na mrežu održava svoju ARP tablicu. Ukoliko računalo želi poslati podatke na mrežu, prije formiranja okvira potrebna je informacija o odredišnoj MAC adresi. Ukoliko se adresa već ne nalazi u ARP tablici, formira se ARP zahtjev (engl. ARP request) u kojem se nalazi pitanje: "Molim uređaj koji ima tu i tu IP adresu da mi se javi!". Ovaj zahtjev se šalje na univerzalnu (engl. broadcast) MAC adresu koja se sastoji od svih bitova postavljenih u vrijednost 1, odnosno FF:FF:FF:FF:FF:FF. Računalo koje prepozna svoju IP adresu vraća ARP odgovor (engl. ARP reply) u kojem se u polju izvorišne MAC adrese nalazi njegova adresa. Na osnovu tog podatka, popunjava se ARP tablica prvog uređaja i može se formirati okvir s ispravnom odredišnom MAC adresom.

Na računalima s Windows operacijskim sustavima ARP tablica se može dobiti iz naredbene linije pokretanjem naredbe `arp -a`.

Primjer pokretanja naredbe:

```
C:\Users>arp -a

Interface: 192.168.0.53 --- 0x6
  Internet Address      Physical Address      Type
  192.168.0.1           f0-b4-d2-10-99-23     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

```
  255.255.255.255          ff-ff-ff-ff-ff-ff       static
```

Vidimo da su u ARP tablici zapisi koji povezuju IP adresu i MAC adresu pojedinih uređaja, kao i zapis koji definira je li statički zabilježen ili se doznao dinamički (upotrebom ARP protokola).

ARP tablica se može pobrisati naredbom `arp -d`.

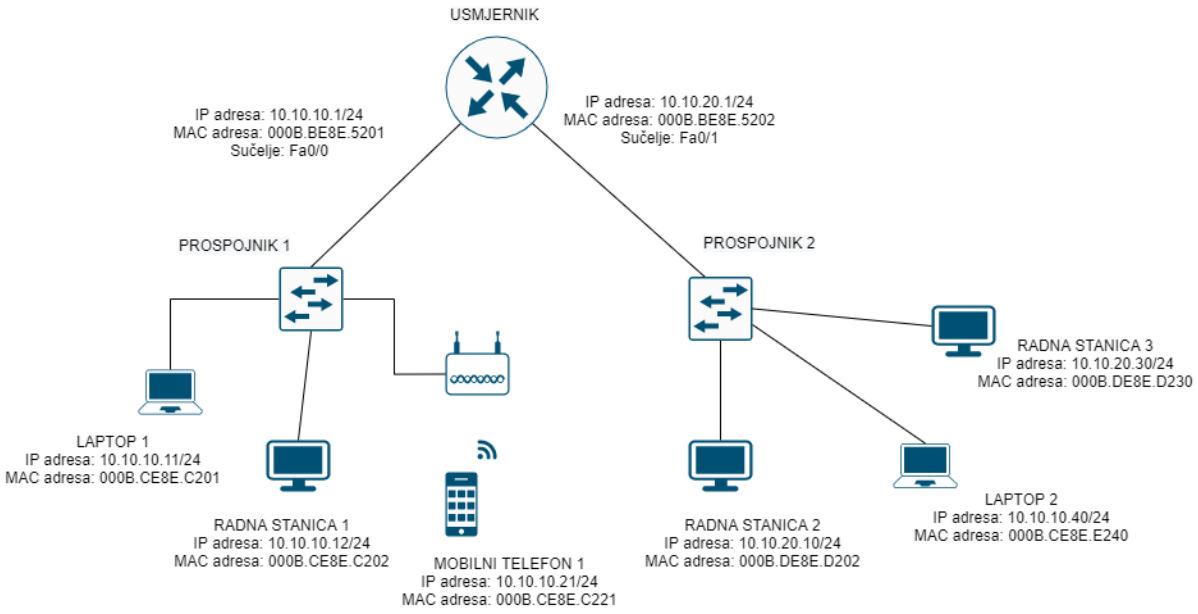
Tok podataka kroz mrežu (lokalno i globalno adresiranje)

Kako bi podaci stigli od izvorišta do odredišta sigurno su potrebni sljedeće informacije:

- IP adresa izvorišta
- IP adresa odredišta
- MAC adresa izvorišta
- MAC adresa odredišta

Ukoliko je odredište u istoj lokalnoj mreži, to su ujedno sve potrebne informacije. Izvorišno računalo prvo popunjava zaglavlje IP protokola s vlastitom izvorišnom IP adresom i IP adresom odredišta. Zatim se paket prosljeđuje nižoj razini koja popunjava polje MAC adrese izvorišta sa svojom MAC adresom, te odredišnu MAC adresu s MAC adresom odredišnog računala, ukoliko je već ima u ARP tablici. Ukoliko u tablici za odredišnu IP adresu nema zapis, pošalje ARP zahtjev na mrežu i na osnovu odgovora popuni tablicu, a nakon toga i polje odredišne MAC adrese.

Ukoliko se odredište nalazi na drugoj mreži, postupak je malo složeniji. Jedna jednostavna mrežna topologija prikazana je na Slici 5.2.



Slika 5.2: Primjer jednostavne mrežne topologije

Ukoliko LAPTOP 1 želi poslati paket RADNOJ STANICI 3, koja se nalazi na drugoj mreži, postupak počinje na isti način. Najprije se popunjavaju polja izvorišne i odredišne IP adrese u zaglavlju IP paketa:

Izvorišna IP adresa: 10.10.10.11
Odredišna IP adresa: 10.10.20.30

Nakon toga je potrebno popuniti polja Ethernet okvira. Izvorišnu MAC adresu LAPTOP 1 zna, jer je to njegova vlastita MAC adresa. Za određivanje MAC adrese odredišnog računala, LAPTOP 1 mora na osnovu odredišne IP adrese i vlastite mrežne maske (/24) odrediti je li odredište u istoj lokalnoj mreži. Nakon što ustanovi da odredište pripada drugoj mreži, LAPTOP 1 zna da taj paket mora poslati zadanom usmjerniku (engl. default gateway), koji je u ovom slučaju na adresi 10.10.10.1. Odredišna IP adresa u zaglavlju paketa se ne mijenja, ali se odredišna MAC adresa popunjava prema IP adresi zadanog usmjernika (ukoliko već postoji u ARP tablici, odnosno, ukoliko ne postoji šalje se ARP zahtjev s IP adresom usmjernika). To nam daje sljedeće podatke u Ethernet zaglavlju:

Izvorišna MAC adresa: 000B.CE8E.C201 (MAC adresa LAPTOPA 1)
Odredišna MAC adresa: 000B.BE8E.5201 (MAC adresa usmjernika na sučelju Fa0/0)

U sljedećem koraku usmjernik na osnovu odredišne IP adrese i vlastite tablice usmjeravanja zna na koje od svojih sučelja treba usmjeriti paket, u ovom slučaju na sučelje Fa0/1. Usmjernik formira novi okvir u kojem podaci u IP zaglavlju ostaju nepromijenjeni, a podaci u zaglavlju Ethernet protokola popunjavaju se na sljedeći način: izvorišna MAC adresa je sada adresa Fa0/1 sučelja usmjernika, a odredišna adresa je MAC adresa RADNE STANICE 3 koju popuni na osnovu svoje ARP tablice (odnosno, dozna ARP zahtjevom ukoliko je prethodno nije imao). Podaci u zaglavljima paketa na drugoj strani su sljedeći:

Izvorišna IP adresa: 10.10.10.11
Odredišna IP adresa: 10.10.20.30

Izvorišna MAC adresa: 000B.CE8E.C202 (MAC adresa usmjernika na sučelju Fa0/1)
Odredišna MAC adresa: 000B.DE8E.D230 (MAC adresa RADNE STANICE 3)

Iz ovog primjera možemo uočiti što znači GLOBALNO, a što LOKALNO adresiranje. Podaci o globalnim adresama (IP adresama) ne mijenjaju se s kraja na kraj mreže, ali MAC adrese se mijenjaju na svakom segmentu mreže kroz koje paket prolazi. LOKALNO adresiranje funkcionira samo unutar jedne lokalne mreže.

Napomena: ukoliko se izvorište i/ili odredište nalaze na mrežama u kojima se za adresiranje koriste privatne adrese, a komunikacija se odvija preko javne mreže, koncept globalnog adresiranja donekle je narušen. Naime, privatne adrese ne mogu se usmjeravati na javnim mrežama te ih je na izlasku iz privatne mreže potrebno prevesti u neku javnu adresu. Jedan od načina je korištenje NAT (Network Address Translation) protokola. U tom slučaju krajnja adresa koja se vidi na internetu je IP adresa uređaja koji obavlja prevođenje (NAT usmjernik), odnosno, tada se i IP adresa u zaglavlju IP protokola mijenja u trenutku prolaska kroz NAT uređaj.

Vježba 5: Izvještaj

Zadatak 1

Iz naredbene linije upotrebom naredbe `ipconfig` doznati vlastitu MAC adresu. Na osnovu te adrese na internetu pronađite proizvođača mrežne opreme čija je to mrežna kartica.

MAC adresa: _____

Proizvođač: _____

Zadatak 2

Korištenjem naredbe `arp` (i potrebne opcije) iz naredbene linije ispisati ARP tablicu na vašem računalu, te je priložiti kao rješenje zadatka.

Zadatak 3

Korištenjem odgovarajuće opcije pobrisati zapise iz ARP tablice, te priložiti ispis nakon brisanja.

Napomena: Prozor naredbene linije možda je potrebno pokrenuti kao administrator.

Zadatak 4

Korištenjem programa Wireshark uhvatiti ARP promet prilikom pinga adrese www.google.com. Nakon pokretanja snimanja paketa, najprije pobrisati ARP tablicu na računalu, a zatim pokrenuti `ping` naredbu (čime osiguravamo hvatanje ARP paketa).

U izvještaju ispišite dva ARP paketa koji su izmijenjeni u ovoj komunikaciji (možete koristiti filtar `arp`).

Za koju IP adresu se tražila MAC adresa? _____

Čija je to IP adresa? _____

Koja se MAC adresa dobila kao odgovor? _____

Možemo li na ovaj način doznati MAC adresu od www.google.com? _____

6. Bežične lokalne mreže

Prva računalna bežična mreža razvijena je 1969. godine na University of Hawai pod nazivom ALOHAnet i koristila je radio komunikaciju između računala.

Prva mreža razvijena za potrebe mobilnih komunikacija (1G mreža, mreža prve generacije) pokrenuta je u Tokiju u Japanu 1991. a temeljena je na analognom prijenosu. Druga generacija mobilnih mreža, 2G, razvijena je u Finskoj 1991. i predstavljala je pravu revoluciju u telekomunikacijama zamijenivši analognu komunikaciju digitalnom. Prva je omogućila slanje SMS i MMS poruka. Njihovi nasljednici, mreže druge, treće, četvrte i sad pete generacije (3G do 5G) povećavaju brzine prijenosa omogućavajući prijenos govora i videa između korisnika. I dok se u svijetu uvode 5G mreže u tijeku je razvoj 6G mreže.

IEEE razvija standarda tzv. WiFi bežičnih lokalnih mreža pod nazivom 802.11.

Mane i vrline bežičnih mreže prikazane su na Slici 6.1.

Vrline bežičnih mreža	Mane bežičnih mreža
dostupnost	SIGURNOST!
efikasnost	problemi s instalacijom
cijena	pokrivenost
fleksibilnost	brzina
skalabilnost	

Slika 6.1: Mane i vrline bežičnih mreža

Skupina bežičnih standarda 802.11

Prvi standard koji je IEEE objavio bio "čisti" 802.11 i to 1997. godine. Nakon njega su slijedili standardi prikazani na Slici 6.2.

Bežične mreže temeljene na ovim standardima rade na frekvencijama 2,4 GHz i 5 GHz koje su ujedno javno dostupne frekvencije za koje nije potrebno tražiti koncesiju za upotrebu. Pri tome treba paziti da takve frekvencije imaju ograničenja na najveću izlaznu snagu uređaja kako se ne bi ometalo sve ostale korisnike istih frekvencija.

Na Slici 6.2 uz nazive standarda prikazane su i brzine prijenosa kao i frekvencije na kojima mreže rade.

IEEE standard	Godina	Frekvencija	Brzina prijenosa	Novi naziv
802.11	1997.	2,4 GHz	1 – 2 Mb/s	(Wi-Fi 1)*
802.11b	1999.	2,4 GHz	1 – 11 Mb/s	(Wi-Fi 2)*
802.11a	1999.	5 GHz	6 – 54 Mb/s	(Wi-Fi 3)*
802.11g	2003.	2,4 GHz	6 – 54 Mb/s	(Wi-Fi 3)*
802.11n	2009.	2,4 GHz	72 – 600 Mb/s	Wi-Fi 4
802.11ac	2014.	5 GHz	433 – 6933 Mbps	Wi-Fi 5
802.11ax	2019.	2,4 GHz, 5 GHz	600 – 9600 Mb/s	Wi-Fi 6
802.11ax	2019.	6 GHz	600 – 9600 Mb/s	Wi-Fi 6E

* neslužbeno ime

Slika 6.2: Prikaz 802.11 standarda

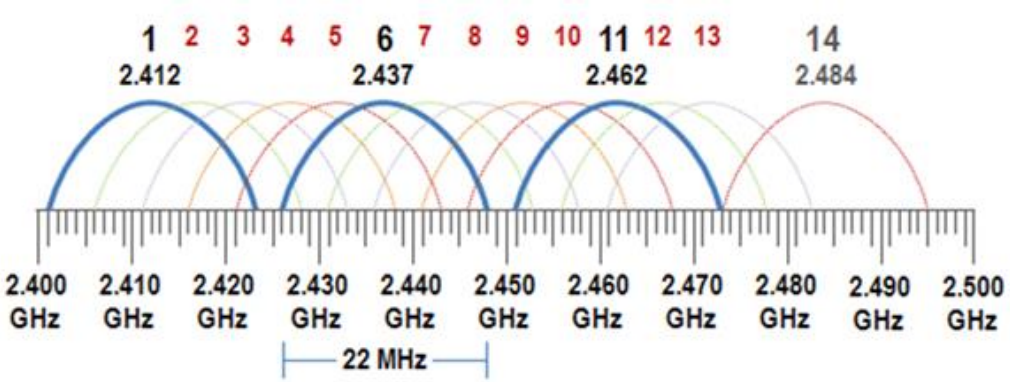
Wi-Fi 4 je uveo MIMO (Multiple Input, Multiple Output) 2 ili 3 antene čime se udvostručila, odnosno utrostručila, propusnost u odnosu na Wi-Fi 3.

Glavna prednost Wi-Fi 5 generacije je uvođenje prijenosnih kanala širine 80 MHz prelaskom na 5 GHz frekvencije (za razliku od kanala širine 20 MHz kod Wi-Fi 4 mreža) čime su se propusnost učetverostručila.

Wi-Fi 6 još dodatno povećava propusnost, 6E uvodi 6 GHz frekvenciju u bežične mreže.

Kanali u bežičnim mrežama na 2,4 GHz

Mreže koje rade na frekvenciji od 2,4 GHz koriste kanale širine 22 MHz i ukupan broj raspoloživih kanala je 14. U SAD-u legalno se može koristiti samo prvih 11, a u Europi 13. Na Slici 6.3 vidimo graf kanala na kojem se može uočiti preklapanje većeg broja kanala.



Slika 6.3: Raspodjela kanala u 2,4 GHz mrežama

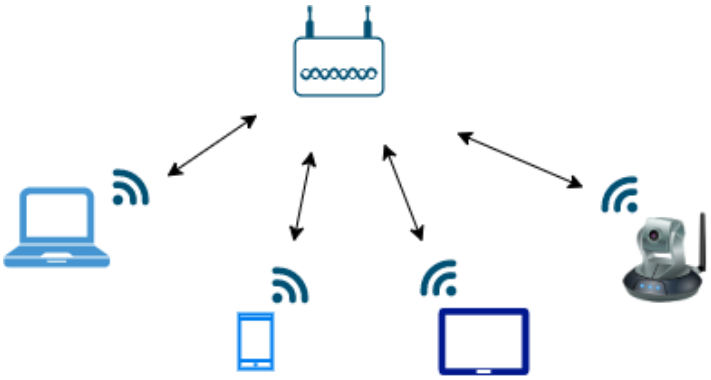
Postoje samo 3 kanala koji se ne preklapaju: 1, 6 i 11. Svi ostali kanali uzrokuje međusobne interferencije.

Načini spajanja bežičnih lokalnih mreža

Bežična lokalna mreža može se uspostaviti na dva načina: ad hoc i infrastrukturno. **Ad hoc** načinom direktno se spajaju dva uređaja koji imaju bežičnu mrežnu karticu kako je prikazano na Slici 6.4.

Slika 6.4: Ad hoc način spajanja

Infrastrukturno spajanje podrazumijeva upotrebu mrežnih bežičnih uređaja na koje se ostali uređaji spajaju, npr. bežične pristupne točke (engl. *access point*) na koje se spajaju laptopi, mobiteli, tableti… Primjer ovog načina spajanja prikazan je na Slici 6.5.



Slika 6.5: Infrastrukturni način spajanja

Način rada bežičnih lokalnih mreža

Bežična lokalna mreža konfigurira se na način da se odredi ime mreže, SSID (Service Set Identifier). SSID se može odašiljati na način da ga svi vide ili može biti skriven. Skrivanje SSID-a je jedan od načina podizanja sigurnosti bežične mreže, odnosno samo korisnici koji znaju ime mreže mogu se spajati. Pri tome treba biti svjestan činjenice da se alatima za skeniranje bežičnog prostora skriveni SSID-ovi mogu otkriti.

Pristup bežičnoj mreži može biti otvoren (na nju se svatko može spojiti) ili se može koristi neki od načina kontrole pristupa. Kako je bežični prostor dijeljeni medij i svi mogu pratiti sve što se prenosi, uvijek je preporuka šifrirati bežični promet. Danas je najčešće u upotrebi WPA2 (Wi-Fi Protected Access 2) koji svakom korisniku pruža jedinstveni ključ za šifriranje podataka. Za pristup mreži zaštićenoj WPA2 protokolom potrebno je poznavati lozinku.

U poslovnim okruženjima nije praktično koristiti metode šifriranja koje koriste jednu lozinku, te se autentikacija obavlja kontaktirajući bazu podataka u kojima se nalaze korisnička imena i lozinke. Primjer takve mreže je mreža eduroam koja koristi AAI sustav autentikacije temeljen na LDAP imeniku i RADIUS (Remote Authentication Dial-In User Service) protokolu.

Bežične mreže najčešće klijentima adrese dodjeljuju automatski, putem DHCP protokola.

Vježba 6: Izvještaj

Zadatak 1

Koristeći aplikaciju WiFi Analyzer () na mobilnom uređaju skenirati bežični prostor. U izvještaju zabilježiti koje ste mreže našli na 2,4 GHz području frekvencija, a koje na 5 GHz području (ukoliko vam uređaj podržava oba područja)

2,4 GHz: _____

_____

5 GHz: _____

_____

Zadatak 2

Na kojim se kanalima nalaze pojedine mreže?

_____

_____

Zadatak 3

Ima li slobodnih kanala na kojima bi se mogle postaviti nova mreža? Ukoliko ima, navedite ih.

_____

Zadatak 4

Unutar aplikacije pronađite podatke o mreži na koju ste spojeni i navedite sljedeće informacije:

Naziv mreže: _____

Frekvencija kanala: _____

Broj kanala: _____

Vrsta enkripcije: _____