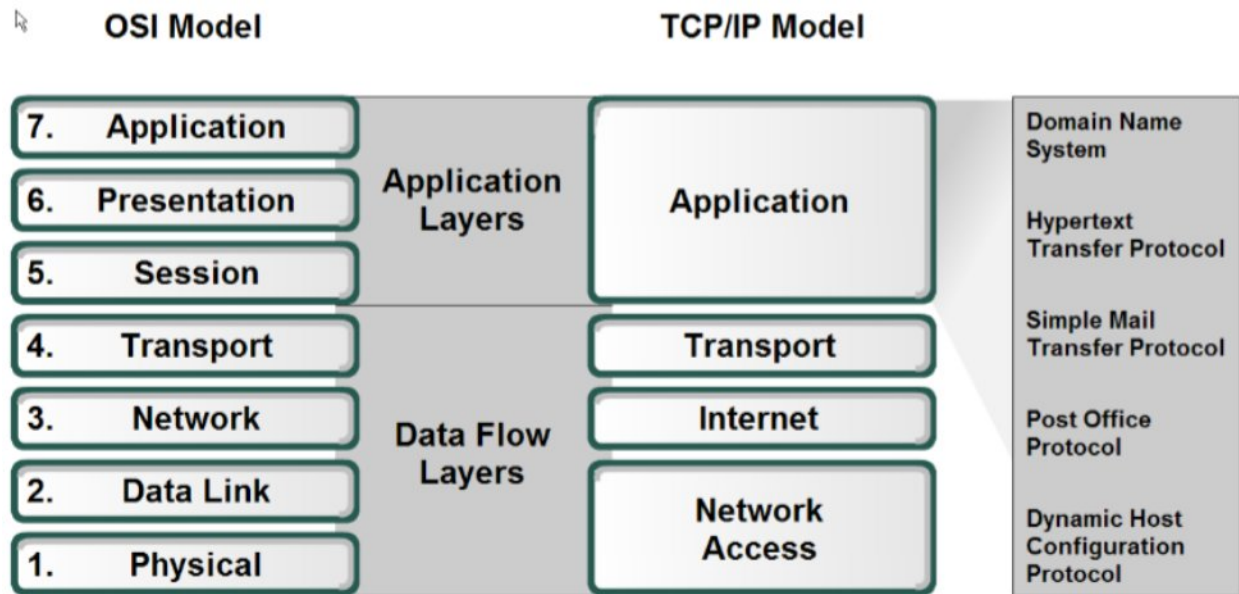


Aplikacioni sloj

Aplikacioni sloj je jedini sloj kojem krajnji korisnik pristupa.



Usluge prezentacionog I sesijskog sloja su integrisane unutar aplikacionog sloja.

Većina klijenata aplikacionog sloja (pretraživač, mail klijent, itd..), imaju već ugrađene funkcije prezentacionog I sesijskog sloja.

Proces je program u izvršavanju.

Sve procese možemo podijeliti u dvije kategorije:

- 1) **Aplikacije**
- 2) **Servisi**

Aplikacije otvara korisnik.

Servisi su procesi koje otvori operativni sistem da omogući korisniku određenu funkciju.

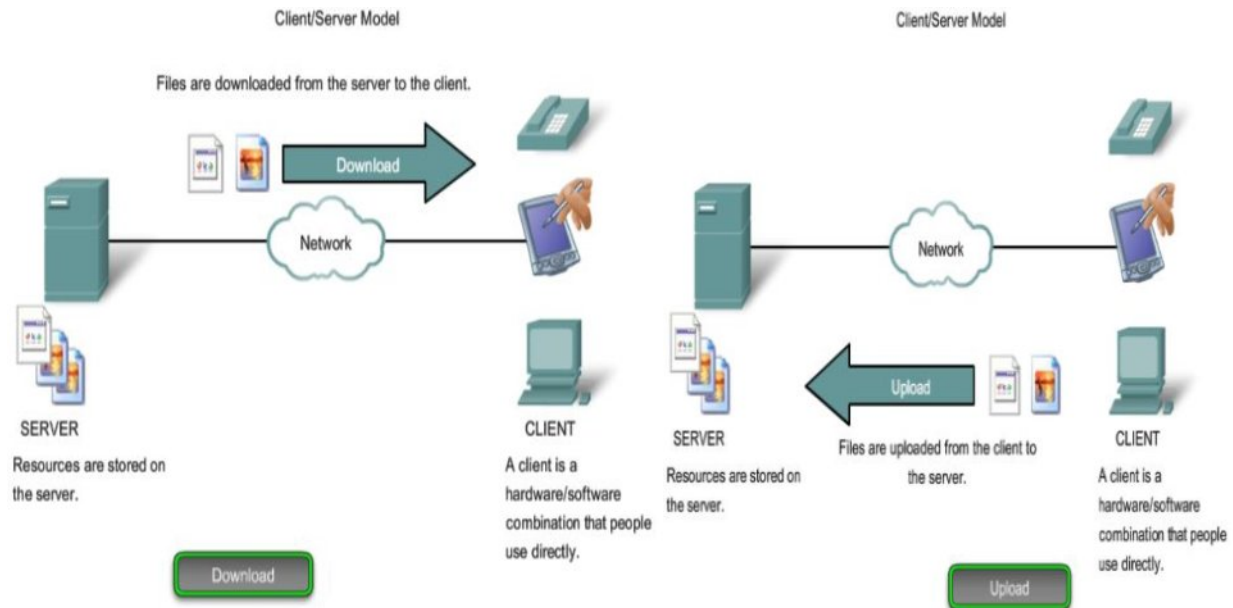
Dva načina za pristup udaljenim podacima:

- 1) **Klijent-server model**
- 2) **Peer-to-peer model**

Većina protokola se zasnivaju na **klijent-server modelu**.

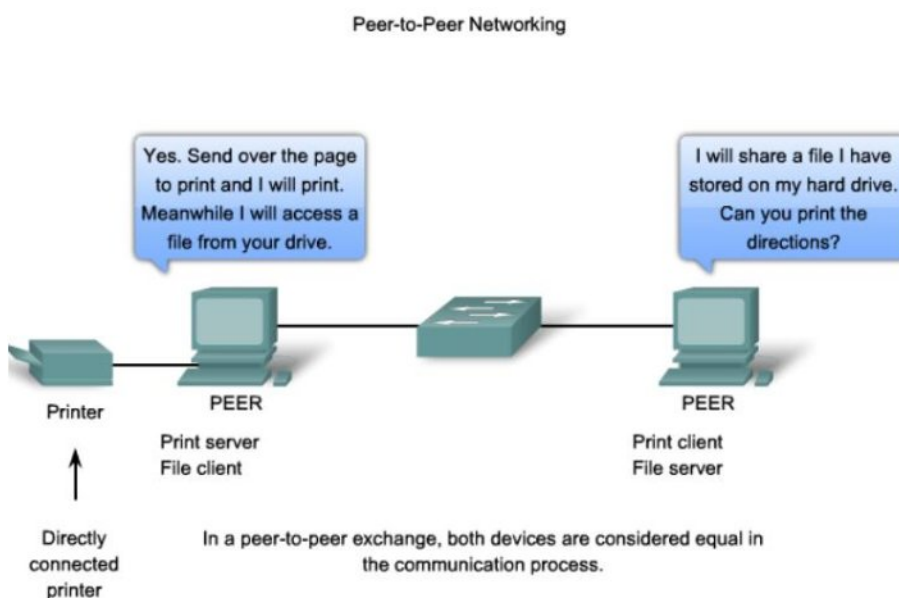
Kada klijent i server uspostave vezu prestaje biti važno ko je server, a ko klijent – komunikacija se odvija u oba smjera.

Razlika između klijenta i servera je u tome što server uvijek čeka klijenta na nekoj dobro poznatoj lokaciji, a ta lokacija je uglavnom predstavljena dobro poznatim portom – Klijent je taj koji inicira komunikaciju.



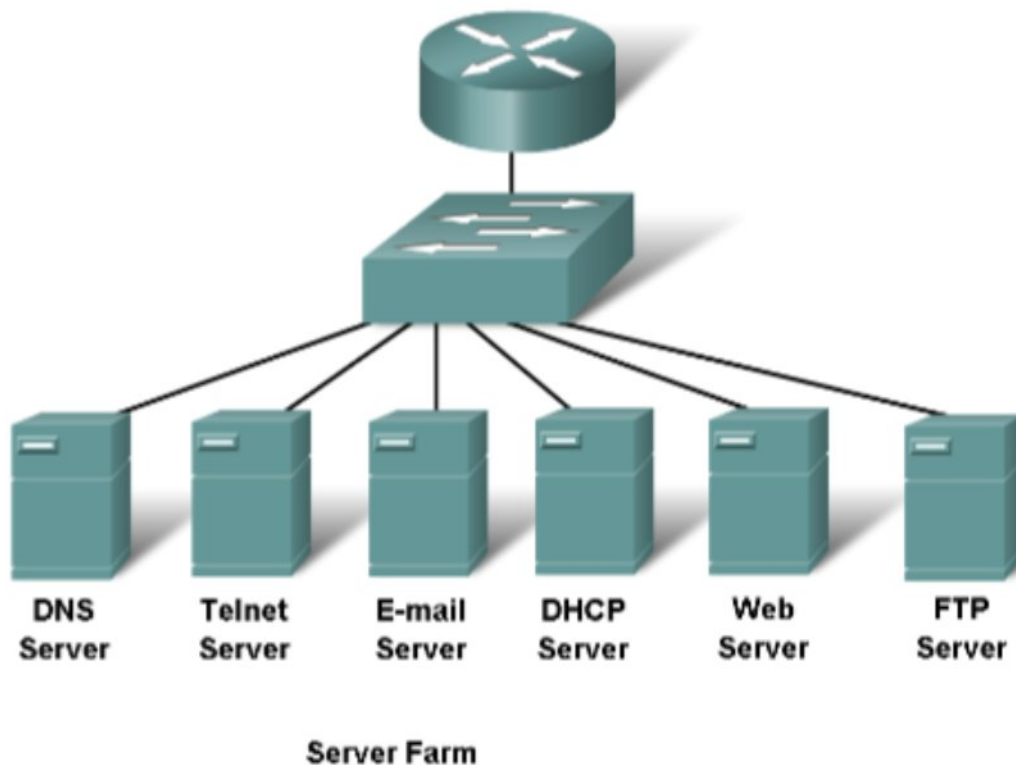
Suprotno od klijent-server modela je **peer-to-peer** model.

Peer-to-peer model je model kod kojeg su svi korisnici jednako zastupljeni.



PROTOKOLI APLIKACIONOG SLOJA:

- 1) **DNS** – Domain Name System **PORT: 53**
- 2) **HTTP** – HyperText Transfer Protocol **PORT:80**
HTTPS – Secure HTTP **PORT: 443**
- 3) Mail protokoli
SMTP – Simple Mail Transfer Protocol **PORT:25**
POP3 – Post Office Protocol **PORT:110**
IMAP – Internet Message Access Protocol **PORT:143**
- 4) **FTP** – File Transfer Protocol **PORT:20 & 21**
TFTP – Trivial FTP **PORT:69**
- 5) **DHCP** – Dynamic Host Configuration Protocol **PORT:67 & 68**
- 6) Protokoli za remote povezivanje uređaja
Telnet – Teletype Network **PORT:23**
SSH - Secure Shell **PORT:22**



DNS

DNS je protokol koji omogućava prevođenje simboličkih imena u IP adrese.

DNS je protokol koji radi na principu klijent-server modela, ali ne na potpuno klasičan način, zato što korisnik ne pristupa direktno DNS klijentu.

DNS klijent nije aplikacija, već servis. Operativni sistem ima ovaj proces otvoren i koristi ga u trenutku kada mu zatreba. Kada se otkuca simboličko ime, DNS klijent se aktivira i prevodi to simboličko ime u odgovarajuću IP adresu.

DNS klijent se još naziva i **DNS RESOLVER**.

Kada DNS klijent želi da sazna IP adresu simboličkog imena onda on kontaktira DNS server koji je jedan od četiri parametra svake adresne konfiguracije (uz IP adresu, subnet mask i defaultni gateway).

Na drugoj strani, na serveru, se vrti proces DNS DAEMON koji čeka zahtjeve DNS klijenata.

Zapisi na DNS serveru su organizovani tako da postoje preslikavanja između IP adresa i simboličkih imena.

Osim toga, tu postoji još jedna stavka, koja nam govori kakav je to tip zapisa u pitanju.

Stavka A: označava klasičan zapis na DNS serveru

Stavka NS: name server, odavde se vrši upućivanje na neki drugi server

Stavka MX: mail exchange, odnosi se na neki mejl server

CNAME: canonical name, ovo omogućava da imamo više simboličkih imena koji se pozivaju na istu IP adresu

Računar sadrži i **DNS cache**, radi bržeg rada. Tu se čuvaju zapisi koji su se u posljednje vrijeme tražili. Ako se pozove neko simboličko ime čije se prevođenje također tražilo i u određenom prethodnom vremenskom intervalu, onda DNS klijent ne stupa u komunikaciju sa DNS serverom, nego generiše IP adresu na osnovu toga što je sadržano u DNS cache, ako se to prevođenje tu nalazi.

Tok komunikacije između DNS klijenta i DNS servera:

DNS klijent se obraća **DNS serveru** u slučaju da nema to preslikavanje u DNS cacheu.

DNS server može da ima ili da nema to preslikavanje koje se traži.

Ako ima, DNS server pošalje tu traženu IP adresu DNS klijentu.

Ako DNS server nema u svojoj bazi to preslikavanje, onda se kreće u proceduru pretraživanja koja ide sa desna na lijevo.

Ako DNS server ne zna to preslikavanje, on se prvo obraća **ROOT DNS** serveru.

ROOT DNS servera postoji 13 u svijetu.

ROOT DNS vjerovatno neće znati da obradi to traženo preslikavanje. Njegov zadatak je da on uputi na neki drugi server koji je zadužen za taj TOP LEVEL domen.

TOP LEVEL domene možemo podijeliti na:

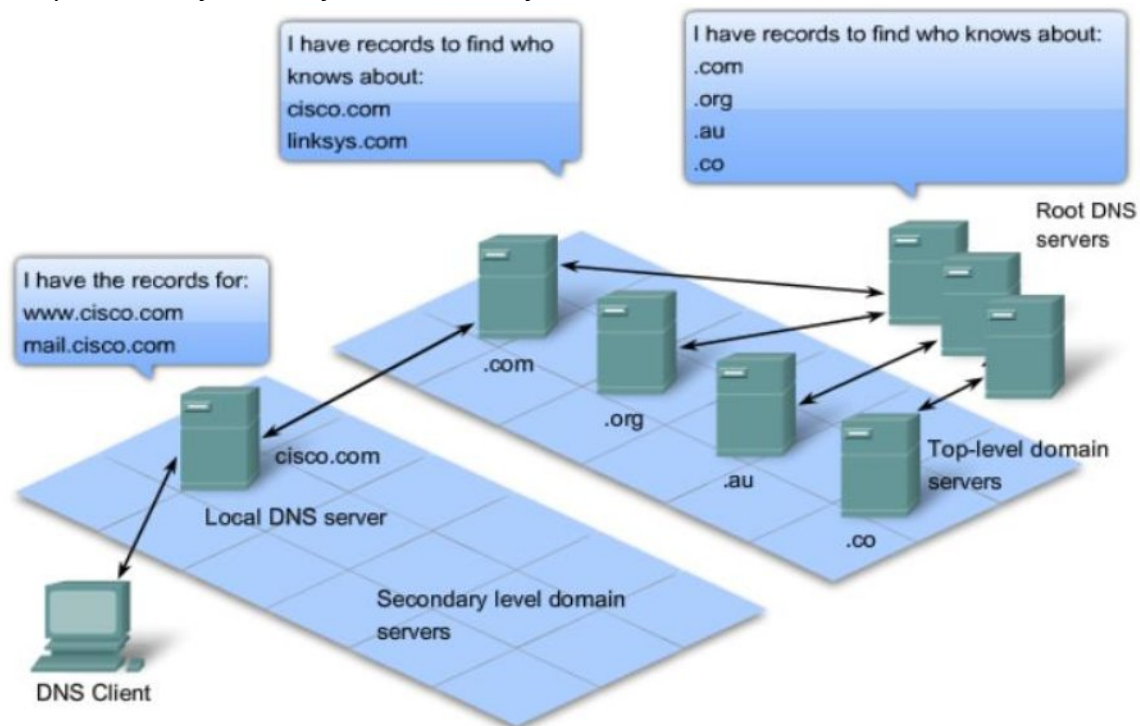
- 1) dobro-poznate domene: .com .gov .edu .org
- 2) državne domene: .ba .rs .uk .me

ROOT DNS server upućuje na TOP LEVEL DNS server koji je zadužen za .com domen. Ako I TOP LEVEL DNS server ne zna da preslika trazeno simboličko ime u IP adresu, on upućuje na drugi DNS server, itd., sve dok se ne pronađe traženi zapis.

Primjer: mail.yahoo.com

DNS Root upućuje na TOP LEVEL DNS server koji je zadužen za .com domene. On onda upućuje na server zadužen za .yahoo domene, itd.

Ovo pretraživanje se odvija sa desna na lijevo.



A hierarchy of DNS servers contains the resource records that match names with addresses.

HTTP

Ovo je tipičan request-response protokol.

On se inicira kad koristimo URL, a URL(Uniform Resource Located) je puno ime adrese koja se poziva.

U ovom slučaju se koristi klasičan klijent, koji je aplikacija I koji se zove web browser.

Web browser razumije HTML jezik (HyperText markup language).

Web browser poznaje samo HTML sadržaj, a da bi reprodukovao neki drugi sadržaj mora se instalirati plug-in za taj sadržaj.

URL se sastoji od 3 dijela:

- 1) Protokol
- 2) Ime servera
- 3) Datoteka na serveru koja se traži

Browser pomoću DNS protokola prevodi simboličko ime u neku numeričku adresu I onda je omogućeno povezivanje na server. Onda se prvo šalje neki get zahtjev da bi dobili odgovor od stranice koja se onda dekoduje u browser.

Postoje različite poruke kojima mogu komunicirati klijent I server, kao što su GET, POST, PUT.

U porukama POST I PUT se šalju neki podaci serveru od strane klijenta, kao što su npr. podaci za logovanje.

Sigurna verzija HTTP protokola je HTTPS, koji vrši kriptovanje sadržaja prije slanja.

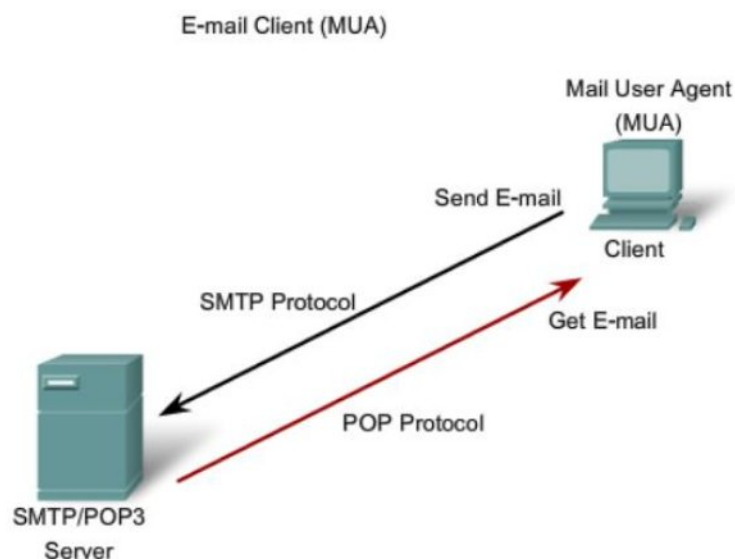
Mail protokoli:

Koriste se isključivo kad se koriste mail klijenti (kao što je Outlook Express), ako koristimo npr. gmail, on koristi https za slanje poruka.

SMTP je protokol koji se koristi za slanje mejlova.

Kada se mail sistem prvi put pojavio bilo je potrebno da primalac mejla bude na mreži da bi se izvršilo slanje mejla. Da bi se slanje mail-ova omogućilo I kada primalac nije na mreži, onda se mail prvo šalje na server, a primalac povlači sa tog servera svoj mail onda kada bude online.

POP3 I IMAP se koriste za primanje mail-ova (uzimanje mail-ova sa mail servera).



Clients send e-mails to a server using SMTP and receive e-mails using POP3.

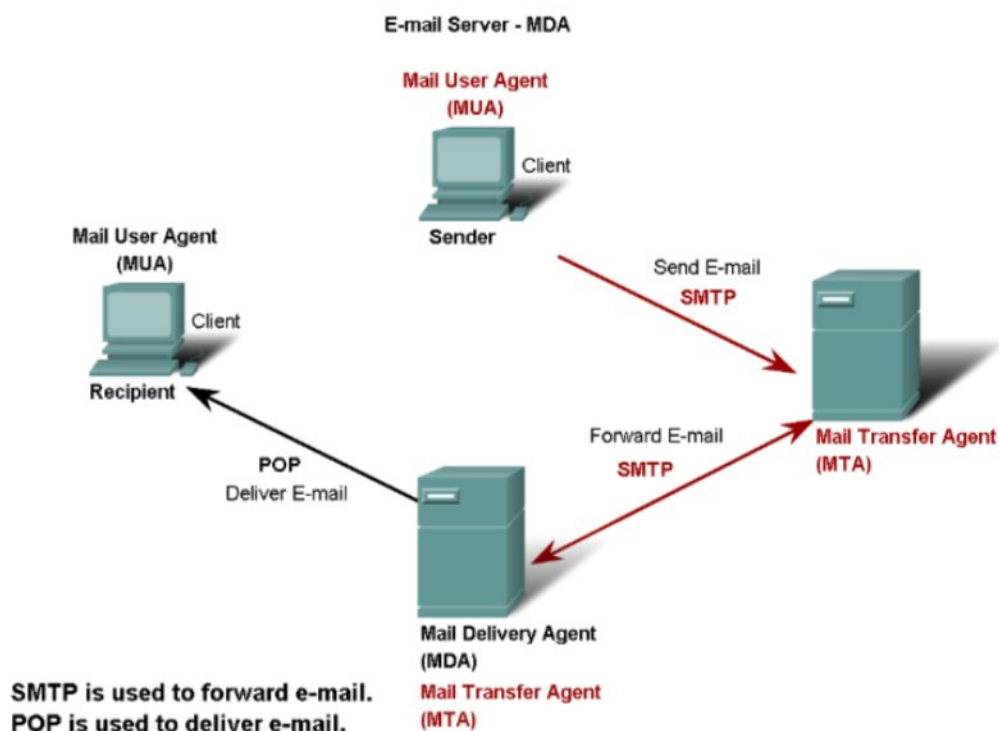
Kako teče tok slanja mail-a?

Sa mail klijenta se šalje mail na mail server. Za ovo slanje se koristi SMTP protokol. Ako korisnik koji prima mejl nema isti mejl server kao pošiljalac, mora se ostvariti komunikacija između različitih mail servera. Tu se onda vrši slanje mail-ova sa jednog servera na drugi. Tu se koristi SMTP protokol. Kada korisnik loguje na svoj mail, onda on povlači poruku sa svog mail servera pomoću protokola POP3 ili protokola IMAP.

Razlika izmedju POP3 I IMAP protokola:

POP3 dostavlja poruku na računar korisnika I neće je čuvati više na svom serveru. Ovo se najčešće koristi u praksi.

IMAP čuva mejlove na serveru.



Postoje I sigurne verzije ova 3 protokola:

Secure SMTP (port: 465), IMAP4 over SSL (IMAPS) (port: 993), Secure POP3 (SSL-POP) (port: 995)

MUA = Mail User Agent (generalni naziv za sve mail klijente)

Servisi koji se vrte na mail serverima:

- 1) Mail Transfer Agent (**MTA**)
- 2) Mail Deliveri Agent (**MDA**)

MTA će se aktivirati ako server treba da proslijedi mail nekom drugom serveru. Ovo se vrši pomoću SMTP protokola.

MDA će se aktivirati ako se poruka treba dostaviti krajnjem korisniku. Ovo se vrši pomoću POP3 ili IMAP protokola.

FTP i TFTP

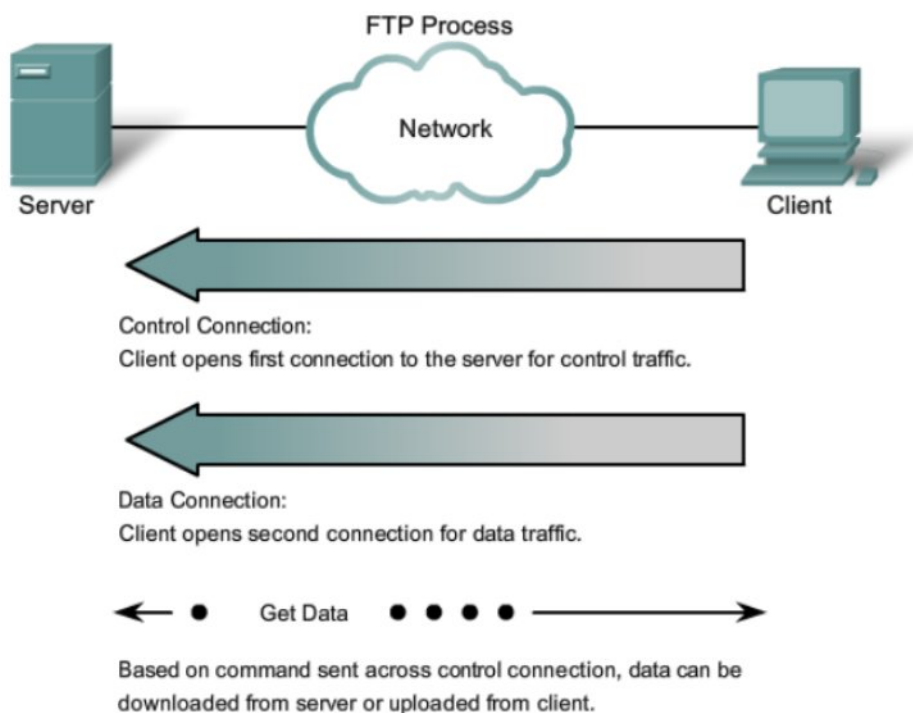
Port 21 se koristi za uspostavljanje veze između klijenta i servera.

Port 20 se koristi za slanje podataka (datoteka), nakon uspostavljanja veze.

FTP omogućava pouzdano slanje fajlova, pa koristi usluge protokola TCP.

TFTP ne osigurava pouzdanost prilikom slanja podataka, pa koristi usluge protokola UDP.

TFTP nema dva porta, nego samo jedan.



DHCP

Protokol koji omogućava krajnjem korisniku da posjeduje IP adresu.

4 osnovna podatka koje korisnik dobija pomoću DHCP protokola su:

- 1) IP adresa
- 2) Mrežna maska (subnet mask)
- 3) Defaultni gateway
- 4) DNS server

DHCP je klijent-server protokol.

Adresu računara se može podesiti na dva načina:

- 1) **Statički**: samostalno podešavanje konfiguracije
- 2) **Dinamički**: korištenjem usluga DHCP-a

Kako radi DHCP protokol?

Kada se klijent uključi u mrežu, on automatski šalje poruku u mrežu koja se zove **DHCP discover**.

Ovo je **broadcast poruka** (ta poruka stiže do svih uređaja u toj mreži).

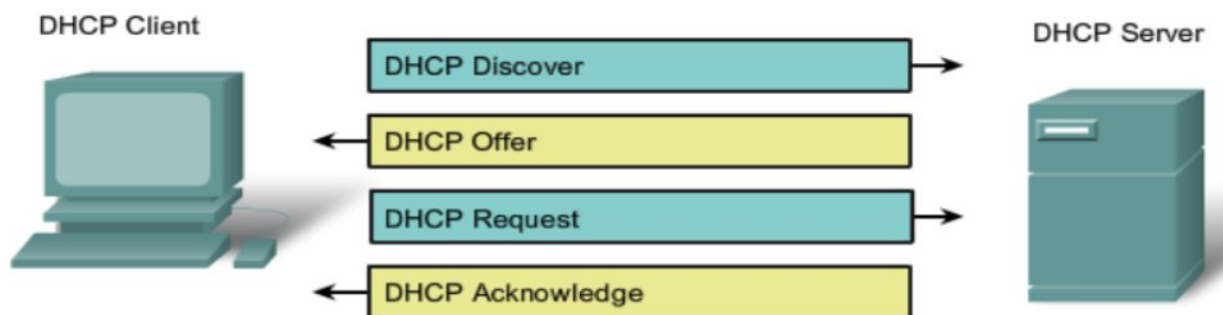
Tom porukom se traži DHCP server koji će ponuditi klijentu adresnu konfiguraciju.

Ako DHCP server postoji i primi poruku DHCP discover, on će kreirati svoju poruku, tj. ponuditi klijentu neku adresnu konfiguraciju.

Ovu adresnu konfiguraciju server šalje korisniku pomoću poruke **DHCP offer (unicast poruka)** = šalje se samo jednom uređaju, u ovom slučaju klijentu).

Klijent može da primi više DHCP offer poruka, ako postoji više DHCP servera u toj mreži. On prihvata jednu, uobičajno prvu koja dođe.

Onda on porukom **DHCP request (broadcast poruka)** javlja da je prihvatio određenu konfiguraciju.



Na taj način se obavještavaju svi DHCP serveri u mreži da je njihova konfiguracija koju su ponudili prihvaćena ili nije prihvaćena.

Server čija je konfiguracija prihvaćena odgovara sa porukom **DHCP acknowledge (unicast poruka)**, i tada potvrđuje da se može početi koristiti konfiguracija koju je on ponudio.

Ako neki korisnici odlaze i dolaze, njih je najbolje poslužiti dinamički pomoću DHCP.

Defaultnim gatewayima i serverima se uglavnom dodjeljuju statičke IP adrese koje se isključuju iz tog skupa adresa koji se koriste običnim korisnicima koji odlaze i dolaze.

DHCP uvijek iznajmljuje adresu na određeno vrijeme. Ako korisnik i poslije tog isteka vremena ostaje u mreži, onda se korištenje te adrese mora produžiti tako što će korisnik to zatražiti.

DHCP je naslijedio stari protokol BOOTP = boot protokol, koji je iznajmljivao adrese na neodređeno vrijeme, što se pokazalo kao loša praksa.

TELNET i SSH

Telnet omogućava povezivanje na neki uređaj sa udaljene lokacije.

Taj uređaj na koji se pristupa pomoću Telnet mora biti pripremljen za takvu vrstu komunikacije, mora da ima IP adresu i određene pristupne podatke.

Telnet je dobar za testiranje mreže, jer prolazi kroz sve slojeve mreže (kroz oba protokol steka, i primaoca i pošiljaoca).

Telnet je primitivan protokol, jer se podaci šalju bajt po bajt. U svakom paketu postoji samo jedan bajt korisnih podataka. Kad je rađen Telnet protokol, rađen je da radi i nije se vodilo toliko računa o sigurnosti.

Zbog toga je razvijen **SSH**, koji radi kao Telnet samo što kriptuje sve poruke u komunikaciji.