

Servisi u mreži

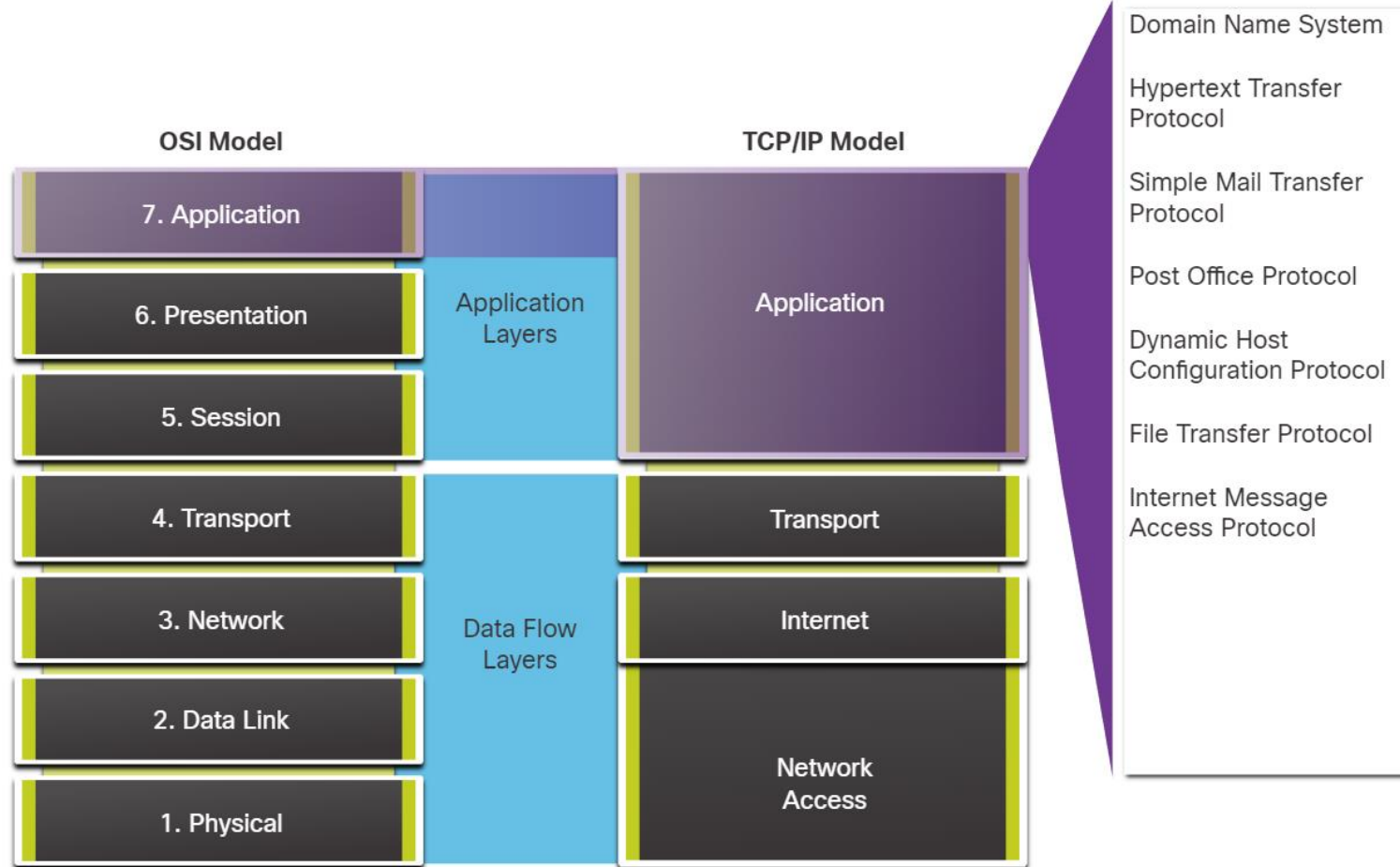
- Komunikacija između računala u mreži
- Peer-to-Peer
- Web i Email Protokoli
- DHCP
- DNS
- NAT
- File Sharing Services

Netacademy:

15 Application Layer



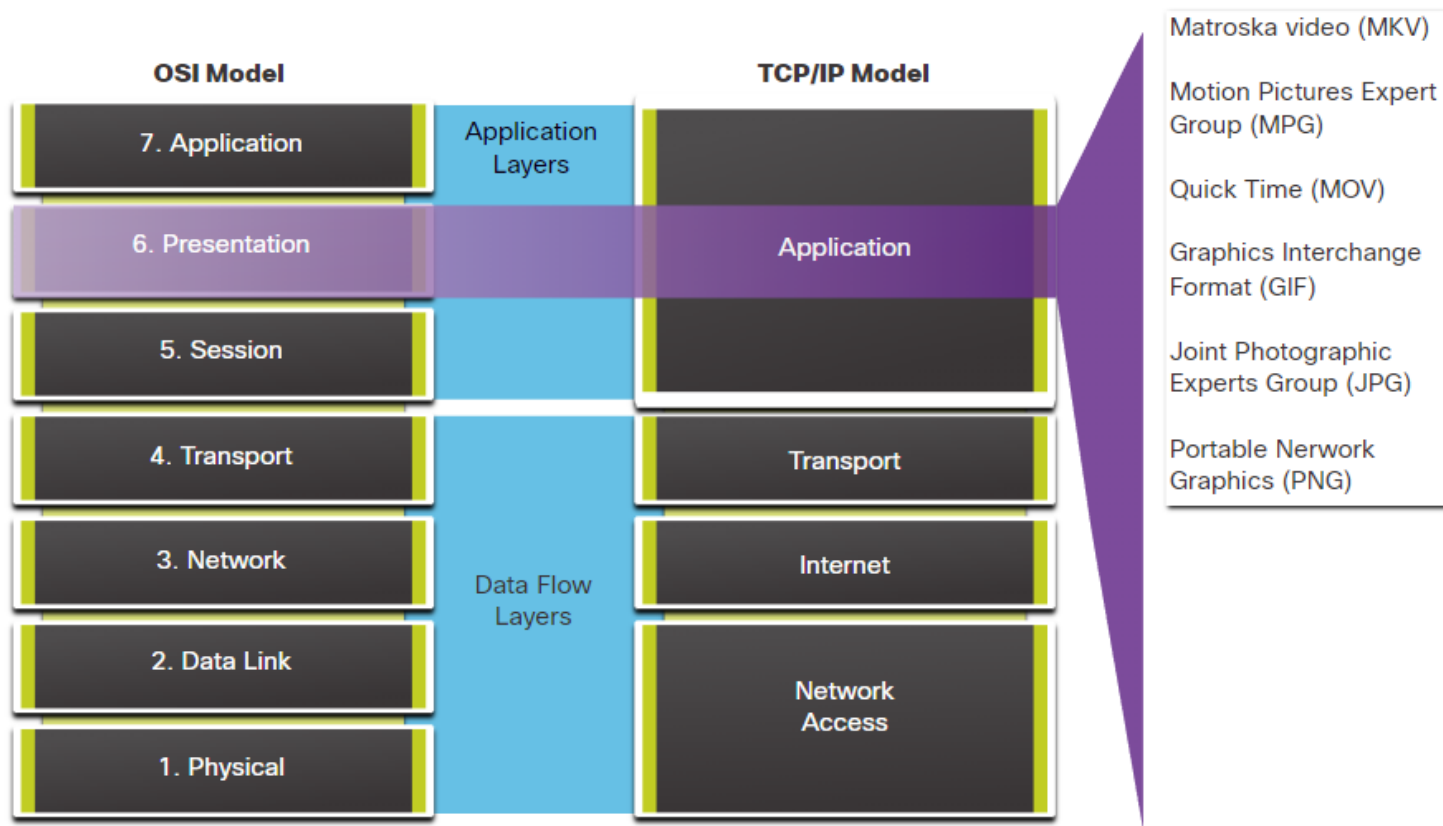
Aplikacijski, prezentacijski sloj i sloj sesije



Aplikacijski sloj

U OSI i TCP/IP modelima, sloj aplikacije je **najbliži sloj krajnjem korisniku**. To je sloj koji osigurava vezu između aplikacija koje se koriste za komunikaciju i mreže preko koje se poruke prenose. Protokoli aplikacijskog sloja koriste se za razmjenu podataka između programa koji se izvode na izvornom i odredišnom računaru.

Aplikacijski, prezentacijski sloj i sloj sesije



Prezentacijski sloj

Ima tri primarne funkcije:

- **Formatiranje** podataka na izvorišnom uređaju u kompatibilan format za primanje i korištenje od strane odredišnog uređaja.
- **Komprimiranje** podataka na način da ih odredišni uređaj može dekomprimirati.
- **Kriptiranje** podataka za prijenos i dekriptiranje podataka po primitku.

Sloj sesije (Sjednički sloj)

Kao što naziv implicira, funkcije na sloju sesije stvaraju i održavaju „dijaloge” (sesije) između izvorišnih i odredišnih aplikacija. Sloj sesije upravlja razmjenu informacija za pokretanje sesija, njihovo održavanje aktivnim i ponovno pokretanje sesija koje su poremećene ili neaktivne dulje vrijeme.

TCP/IP Protokoli aplikacijskog sloja

- TCP/IP protokoli aplikacijskog sloja određuju format i kontrolne informacije potrebne za mnoge uobičajene funkcije internetske komunikacije. Protokole aplikacijskog sloja koriste i izvorni i odredišni uređaji tijekom komunikacijske sesije. Da bi komunikacija bila uspješna, protokoli aplikacijskog sloja koji su implementirani na izvornom i odredišnom hostu moraju biti kompatibilni.

DNS - Domain Name System (ili Service)

- TCP, UDP 53
- Pretvara (mapira) domenska imena npr. U IP adrese

DHCP - Dynamic Host Configuration Protocol

UDP client 68, server 67

Dinamička dodjeljivanje IP postavki računalima u mreži

Web

HTTP - Hypertext Transfer Protocol

- TCP 80, 8080
- Skup pravila za razmjenu teksta, grafičkih slika, zvuka, videa i drugih multimedijских datoteka na World Wide Webu

•HTTPS - HTTP Secure

- TCP, UDP 443
- Preglednik koristi enkripciju za zaštitu HTTP komunikacije
- Autentificira web mjesto na koje se povezujete s preglednikom

TCP/IP Protokoli aplikacijskog sloja

Email

SMTP - Simple Mail Transfer Protocol

- TCP 25
- Omogućava slanje email poruka s računala prema mail serveru
- Omogućava slanje email poruka između mail servera

POP3 - Post Office Protocol

- TCP 110
- Omogućava klijentima povlačenje email poruka sa servera u aplikaciju za čitanje email poruka na računalo

IMAP - Internet Message Access Protocol

- TCP 143
- Omogućava klijentima pristup porukama koje se nalaze na mail serveru

File Transfer

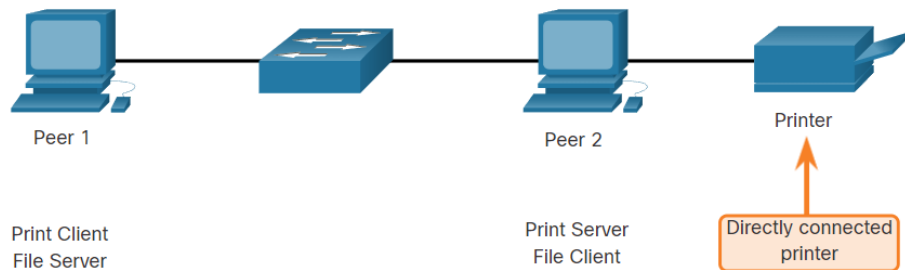
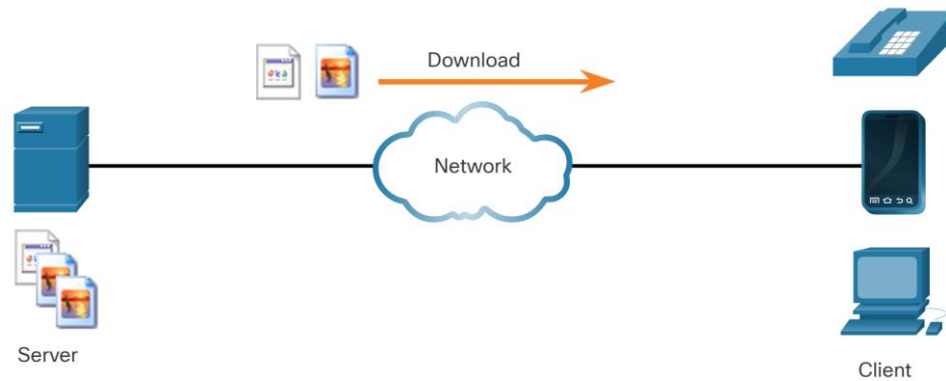
FTP - File Transfer Protocol

- TCP 20 to 21
- Sadrži set pravila koja korisniku na jednom računalu omogućuju pristup i prijenos datoteka na i s drugog računala preko mreže
- FTP je pouzdan, na vezu usmjeren (connection oriented) i često korišten protokol za „kopiranje” datoteka

TFTP - Trivial File Transfer Protocol

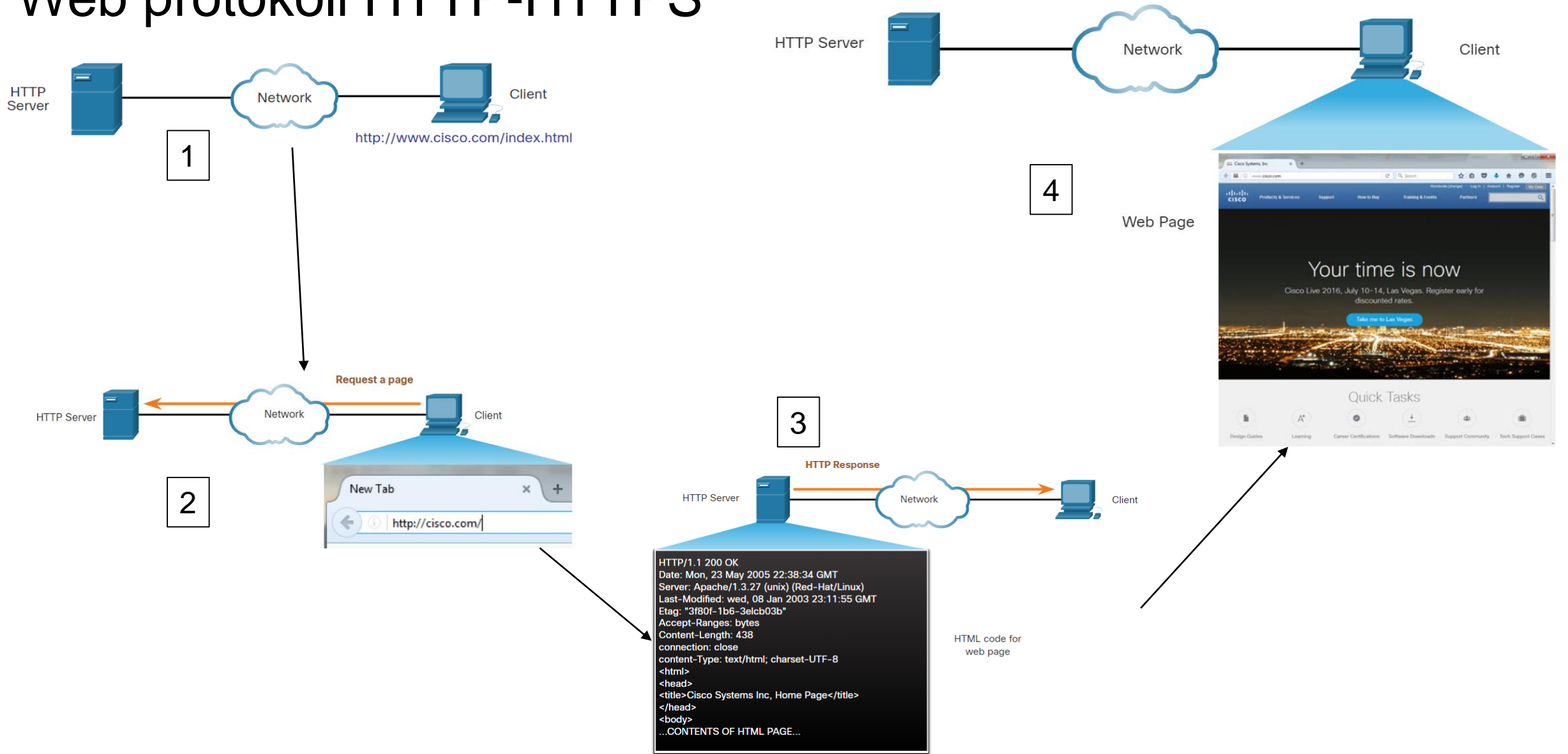
- UDP client 69
- Jednostavan protokol za prijenos datoteka bez uspostavljanja veze s maksimalnom isporukom datoteka bez potvrđivanja
- Koristi manje opisnih podataka nego FTP

Peer-to-Peer



- Procesi klijenta i poslužitelja nalaze se na aplikacijskom sloju. **Klijent započinje** razmjenu traženjem podataka od poslužitelja, koji odgovara slanjem jednog ili više tokova podataka klijentu.
- **Protokoli aplikacijskog sloja opisuju format zahtjeva i odgovora** između klijenata i poslužitelja.
- Uz stvarni prijenos podataka, ova razmjena također može zahtijevati **autentifikaciju** korisnika i **identifikaciju** podatkovne datoteke koja se prenosi.
- Model **P2P mreže** uključuje dva dijela: **P2P mreže** i **P2P aplikacije**. Oba dijela imaju slične značajke, ali u praksi rade sasvim drugačije.
- U P2P mreži, dva ili više računala su povezana putem mreže i mogu dijeliti resurse (kao što su pisači i datoteke) bez namjenskog poslužitelja. **Svaki povezani krajnji uređaj (poznat kao peer) može funkcionirati i kao poslužitelj i kao klijent.** Jedno računalo može preuzeti ulogu poslužitelja za jednu transakciju dok istovremeno služi kao klijent za drugu. Uloge klijenta i poslužitelja postavljaju se prema zahtjevu.
- U peer-to-peer razmjeni, oba uređaja se smatraju jednakima u komunikacijskom procesu. **Podacima se pristupa s ravnopravnog uređaja bez upotrebe namjenskog poslužitelja**

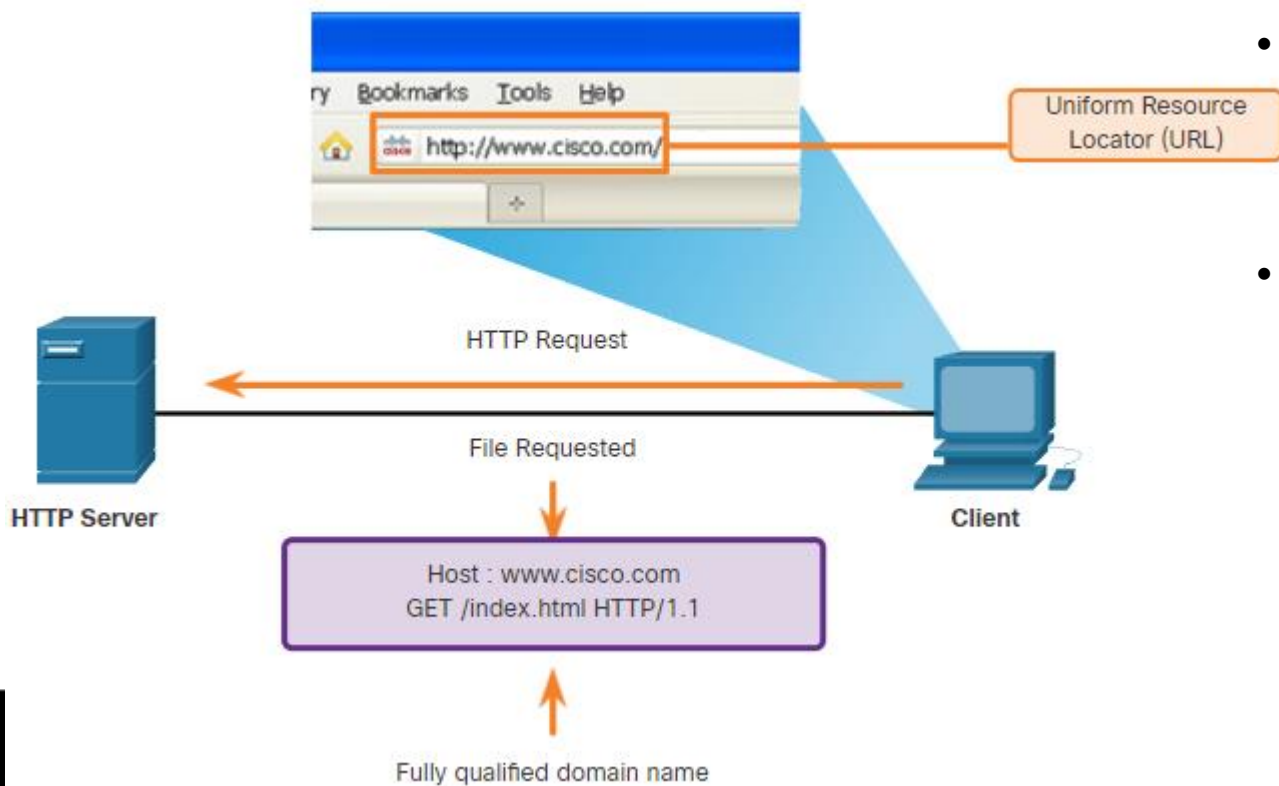
Web protokoli HTTP-HTTPS



Webprotokoli HTTP-HTTPS

- **HTTP** je protokol koji radi po principu zahtjeva/odgovora (request and reply). Kada klijent, obično web-preglednik, pošalje zahtjev web-poslužitelju, HTTP specificira vrste poruka koje se koriste za tu komunikaciju. Tri uobičajene vrste poruka su GET (vidi sliku), POST i PUT:

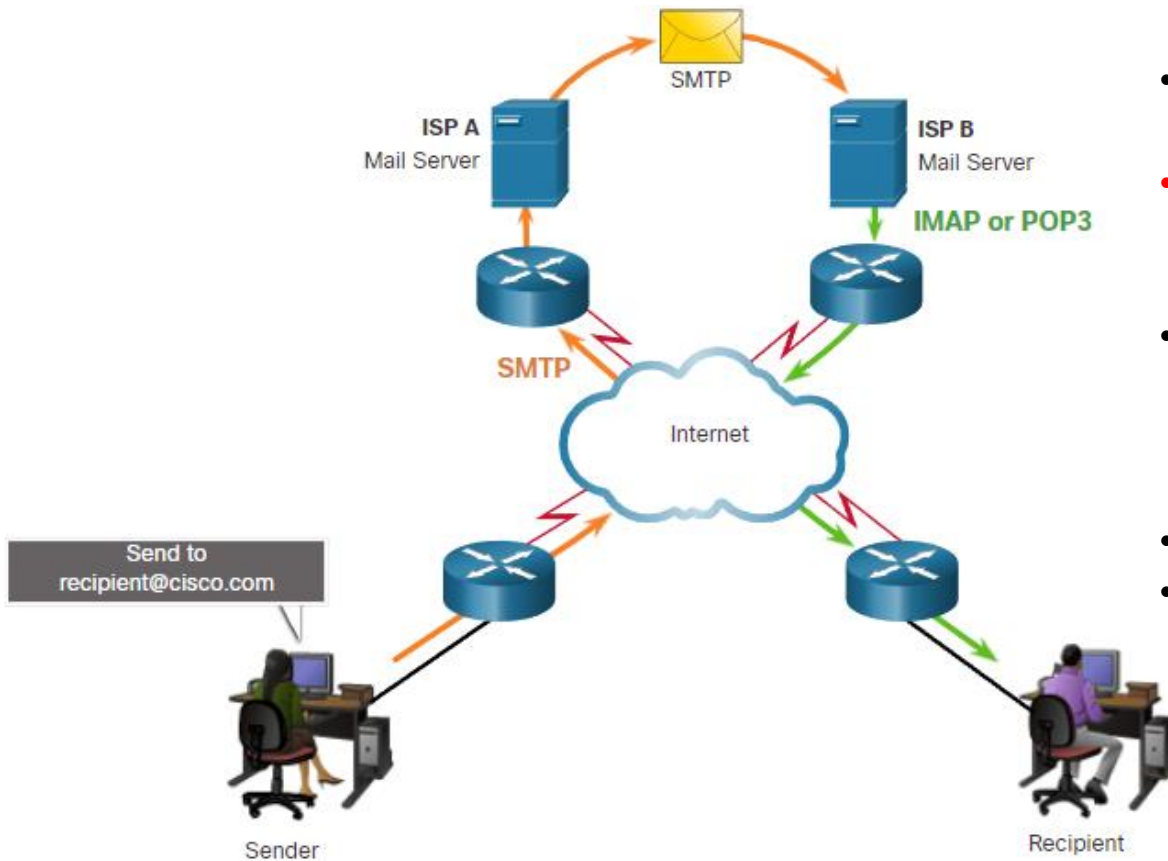
- GET - Ovo je zahtjev klijenta za podacima. Klijent (web preglednik) šalje GET poruku web poslužitelju da zatraži HTML stranice.
- POST – Ovime se učitavaju (uplodaju) podatkovne datoteke na web poslužitelj, poput podataka obrazaca.
- PUT - Ovo prenosi resurse ili sadržaj na web poslužitelj, poput slike, videa itd..



- Iako je **HTTP** izuzetno fleksibilan, on **nije siguran protokol**. Poruke zahtjeva šalju informacije poslužitelju u otvorenom tekstu koji se može presresti i pročitati. Odgovori poslužitelja, obično HTML stranice, također **nisu kriptirani**.
- Za sigurnu komunikaciju preko interneta koristi se **HTTP Secure (HTTPS)** protokol. HTTPS koristi **autentifikaciju** i **enkripciju** za zaštitu podataka dok putuju između klijenta i poslužitelja. **HTTPS koristi isti proces odgovora klijenta i poslužitelja kao i HTTP, ali je tok podataka šifriran** s **Transport Layer Security (TLS)** ili njegovim prethodnikom **Secure Socket Layer (SSL)** prije prijenosa preko mreže.

Email Protokoli

- Tda bi imali email poruke na računalu potrebno je nekoliko protokola i aplikacija (mail protokoli, ali i DNS i email klijentska aplikacija)
- Email koristi princip „**Store and forward**” za slanje email poruka prema mail serveru, prosljeđivanje email poruka između email servera i za povlačenje email poruka sa servera na računalo



- Klijenti e-pošte komuniciraju s poslužiteljima e-pošte za slanje i primanje e-pošte.
- Poslužitelji e-pošte komuniciraju s drugim poslužiteljima e-pošte za prijenos poruka s jedne domene na drugu.
- **Klijent e-pošte ne komunicira izravno s drugim klijentom e-pošte prilikom slanja e-pošte.** Umjesto toga, oba se klijenta oslanjaju na poslužitelj pošte za prijenos poruka.
- E-pošta podržava tri odvojena protokola za rad:
 - Jednostavni protokol za prijenos pošte (**SMTP**), TCP port 25
 - Protokol pošte (**POP**), port TCP 110
 - i **IMAP**. Port TCP 143
- Proces aplikacijskog sloja koji šalje poštu koristi SMTP.
- Klijent dohvaća e-poštu pomoću jednog od dva protokola aplikacijskog sloja: POP ili IMAP.



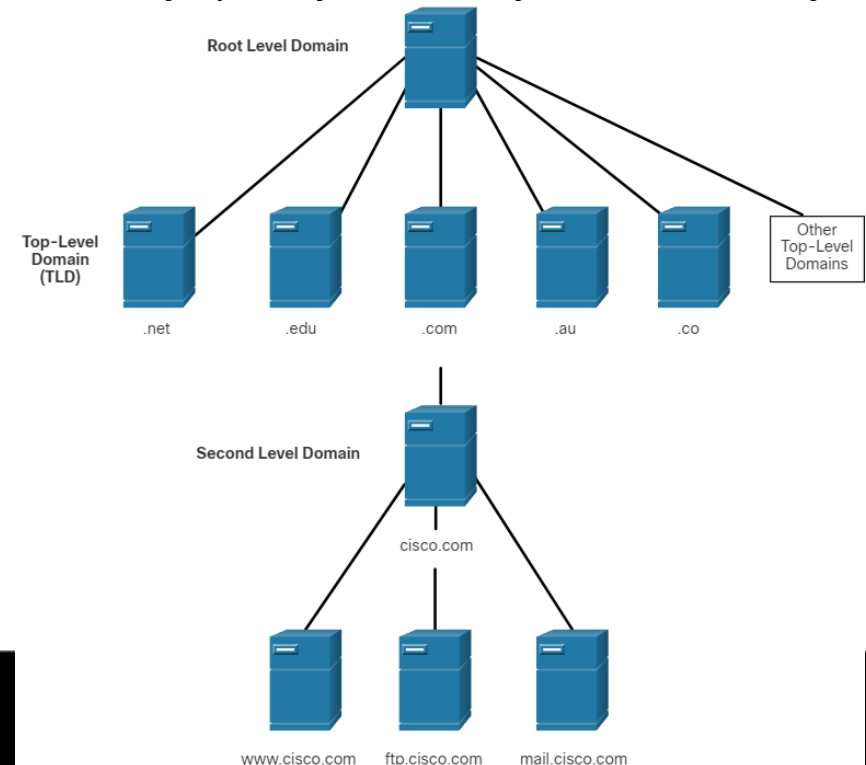
Domain Name System- *pokazati u PacketTracer*

- U podatkovnim mrežama uređaji su označeni numeričkim IP adresama za slanje i primanje podataka preko mreža. **Nazivi domena stvoreni su kako bi se brojčana adresa pretvorila u jednostavno, prepoznatljivo ime.**
- Naredba **ipconfig /displaydns** prikazuje sve predmemorirane DNS unose, a naredba **nslookup** omogućuje dijalog s DNS poslužiteljem
- Na internetu, ljudi puno lakše pamte potpuno kvalificirane nazive domena (FQDN), kao što je `http://www.cisco.com` nego `198.133.219.25`, što je stvarna numerička adresa ovog poslužitelja.
- **Ako Cisco odluči promijeniti numeričku adresu `www.cisco.com`, to je transparentno za korisnika jer naziv domene ostaje isti.** Nova adresa se jednostavno povezuje s postojećim nazivom domene i povezanost se održava.
- DNS poslužitelj pohranjuje različite vrste zapisa resursa koji se koriste za rješavanje imena. Ti zapisi sadrže ime, adresu i vrstu zapisa. Neke od ovih vrsta zapisa su sljedeće:
 - **A** - IPv4 adresa krajnjeg uređaja
 - NS - Autoritativni poslužitelj imena
 - AAAA - IPv6 adresa krajnjeg uređaja (izgovara se quad-A)
 - **MX** - zapis o razmjeni pošte

`ipconfig/flushdns` –clears DNS cache on the computer

Domain Name System- *pokazati u PacketTracer*

- DNS je **hijerarhijski sustav u kojem postoji mnogo baza** u kojima su povezana domenska imena s IP adresama. DNS koristi nazive domena za formiranje hijerarhije (različite domene imaju različite DNS servere).
- **Struktura imenovanja podijeljena je na male zone kojima se može upravljati.** Svaki DNS poslužitelj održava određenu bazu podataka i **odgovoran je** samo za upravljanje mapiranjem imena i IP-a **za taj mali dio cijele DNS strukture.**
- **Kada DNS poslužitelj primi zahtjev za prijevod imena koji nije unutar njegove DNS zone, DNS poslužitelj prosljeđuje zahtjev drugom DNS poslužitelju unutar odgovarajuće zone za prijevod.**
- DNS je **skalabilan** jer je rezolucija naziva *hosta* raspoređena na više poslužitelja.
- Različite domene najviše razine predstavljaju ili vrstu organizacije ili zemlju podrijetla. Primjeri domena najviše razine (Top Level Domain) su sljedeći:
 - .com – tvrtka ili industrija
 - .org - neprofitna organizacija
 - .au - Australija
 - .co - Kolumbija

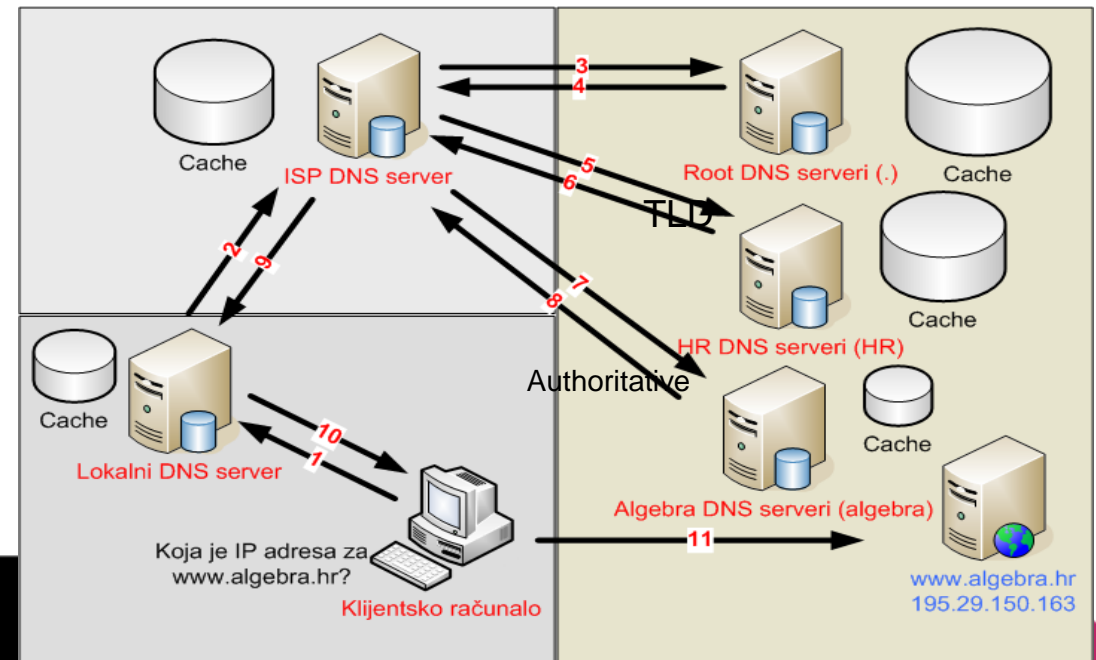


Hijerarhija DNS

- Nazivi domena obično su podijeljeni u dva ili tri dijela, svaki **odvojen točkom**. Kada se čitaju **od desne strane prema lijevoj**, identifikatori u nazivima domena idu od **najopćenitijih do najspecifičnijih**. Odjeljak s desne strane zadnje točke u nazivu domene je domena najviše razine (TLD). To uključuje 'generičke' TLD-ove kao što su '.com', '.net' i '.org', kao i TLD-ove specifične za državu kao što su '.uk' i '.jp'.
- Lijevo od TLD-a nalazi se domena druge razine (2LD), a ako postoji nešto lijevo od 2LD-a, to se naziva domena treće razine (3LD).
- Za Googleov naziv američke domene, "google.com":
 - '.com' je TLD (najopćenitiji)
 - 'google' je 2LD (najspecifičniji)
- Ali za naziv domene Google UK, "google.co.uk":
 - '.uk' je TLD (najopćenitiji)
 - '.co'* je 2LD
 - 'google' je 3LD (najspecifičniji)

Primjer rada DNS-a-klijent želi otvoriti www.algebra.hr

1. Klijent pita svoj lokalni DNS (koji mu je konfiguriran u IP postavkama)
2. Lokalni DNS gleda da li je zadužen za tu domenu, ako nije pita DNS ISP-a (tako je konfiguriran)
3. ISP-ov DNS ne zna domenu, pa traži korijenski DNS (Root DNS)-koji mu je konfiguriran
4. Root DNS ga usmjerava na DNS zadužen za domenu najviše razine **.hr**
5. ISP-ov DNS pita DNS nadležan za domenu **.hr**
6. DNS za tld **.hr** zna i vraća DNS-u ISP-a koji je DNS poslužitelj zadužen za traženu domenu **.algebra**
7. ISP-ov DNS traži od DNS-a za algebra domenu IP adresu specifičnog servera
8. DNS za algebra.hr poslužitelja vraća podatke DNS-u ISP-a
9. ISP-ov DNS vraća odgovor lokalnom DNS-u klijenta
10. Lokalni DNS vraća adresu danu klijentu
11. Na kraju klijent može izravno kontaktirati poslužitelj na 195.29.150.163 i otvara web stranicu

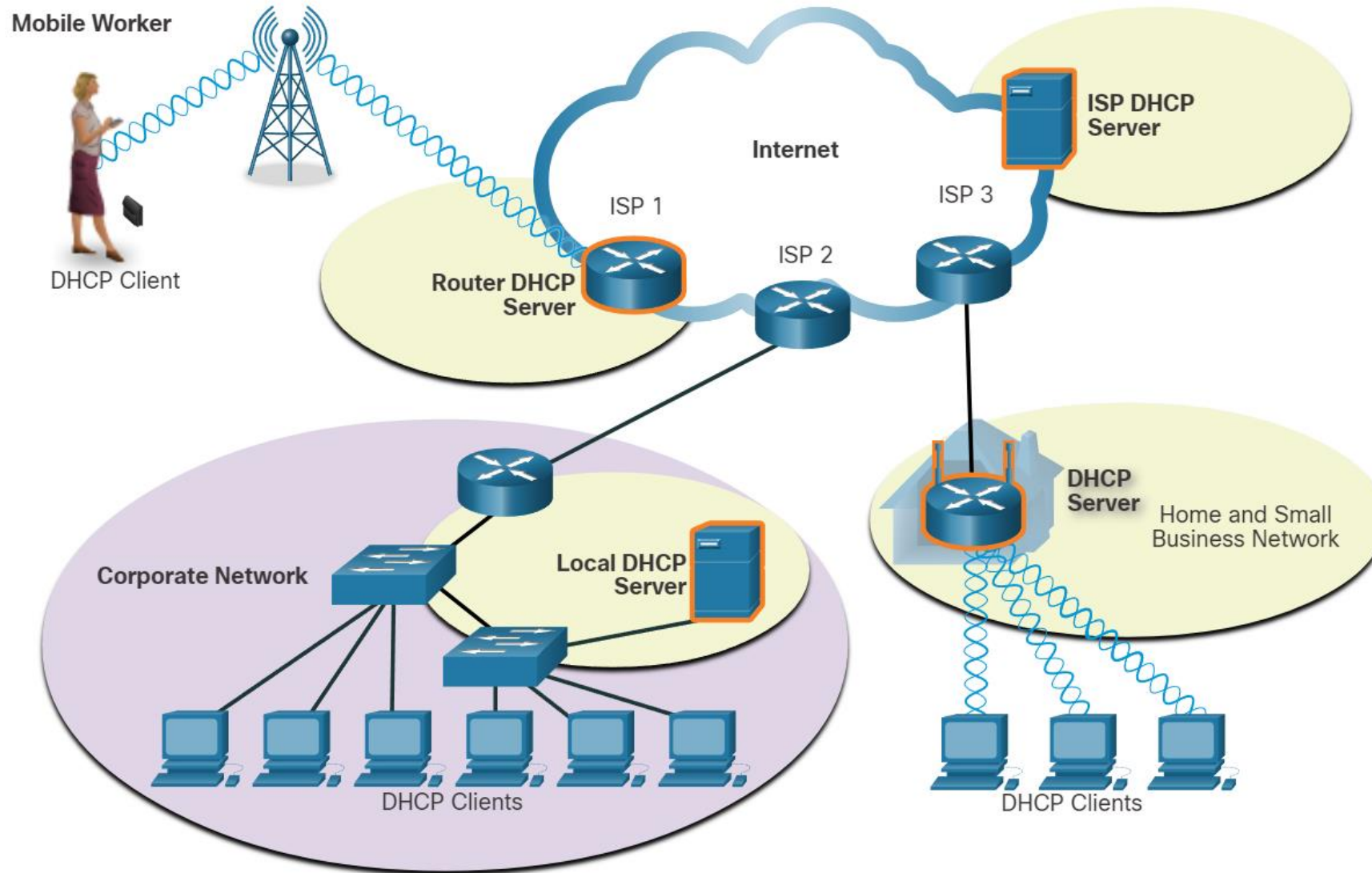




DHCP (Dynamic Host Configuration Protocol)-*pokazati u PTraceru*

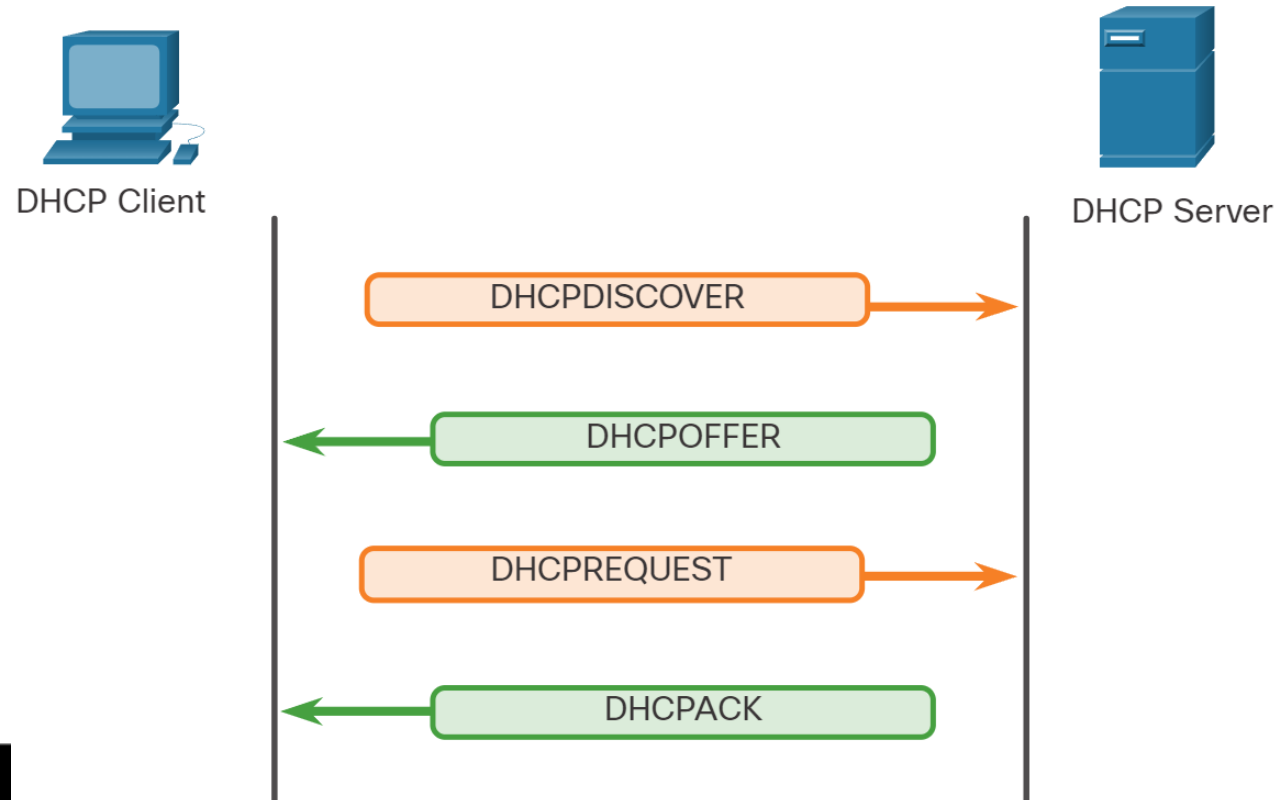
- Dynamic Host Configuration Protocol (DHCP) za IPv4 uslugu automatizira dodjelu **IPv4 adresa, podmrežnih maski, pristupnika i drugih IPv4 mrežnih parametara**. Ovo se naziva **dinamičko adresiranje**. Alternativa dinamičkom adresiranju je **statičko adresiranje**. Kada koristite statičko adresiranje, mrežni administrator ručno unosi podatke o IP adresi na hostove.
- Kada se host spoji na mrežu, kontaktira se DHCP poslužitelj i traži se adresa. DHCP poslužitelj odabire adresu iz konfiguriranog raspona adresa koji se naziva skup i dodjeljuje (iznajmljuje) je glavnom računalu.
- Na većim mrežama ili tamo gdje se broj korisnika često mijenja, DHCP je poželjan za dodjelu adresa. Umjesto korištenja statičkog adresiranja za svako računalo, učinkovitije je imati IPv4 adrese dodijeljene automatski pomoću DHCP-a.
- DHCP može dodijeliti IP adrese na određeni vremenski period (lease period). Lease period je važna DHCP postavka. Kada lease period istekne ili DHCP poslužitelj dobije DHCPRELEASE poruku, adresa se vraća u DHCP raspon (pool) za ponovnu upotrebu. Korisnici se mogu slobodno kretati s mjesta na mjesto i jednostavno ponovno uspostaviti mrežne veze putem DHCP-a.
- DHCP poslužitelj u većini srednjih do velikih mreža obično je lokalni namjenski poslužitelj temeljen na računalu. Kod kućnih mreža, DHCP poslužitelj se obično nalazi na lokalnom usmjerivaču koji povezuje kućnu mrežu s ISP-om.
- Mnoge mreže koriste i DHCP i statičko adresiranje. DHCP se koristi za hostove opće namjene, kao što su uređaji krajnjih korisnika. Statičko adresiranje koristi se za mrežne uređaje, kao što su gateway usmjerivači, preklopnici, poslužitelji i pisači.

DHCP (Dynamic Host Configuration Protocol)-*pokazati u PTraceru*



DHCP (Dynamic Host Configuration Protocol)-*pokazati u PTraceru*

- Kada se računalo postavljeno da dobije IP postavke putem DHCP-a poveže na mrežu i uključi prvo šalje **broadcast DHCP discover** (DHCPDISCOVER) poruke kako bi otkrilo ima li dostupnih DHCP servera u lokalnoj mreži
- DHCP server odgovara porukom **DHCP OFFER**, u kojoj nudi određene IP postavke računalu DHCP OFFER poruka sadržava **IPv4 adresu, subnet masku, IPv4 adresu DNS servera i IPv4 adresu default gateway uređaja, također uključuje i lease period**



DHCP (Dynamic Host Configuration Protocol)-*pokazati u PTraceru*

- Klijent može primiti više poruka DHCPOFFER ako postoji više od jednog DHCP poslužitelja na lokalnoj mreži. Stoga mora birati između njih. Da bi to moglo računalo šalje poruku **DHCPREQUEST** koja **identificira eksplicitni poslužitelj i ponudu koju klijent prihvaća**. Klijent također može odlučiti zatražiti adresu koju je već koristilo, a koju mu je prethodno dodijelio DHCP poslužitelj.
- Pod pretpostavkom da **je IPv4 adresa** koju zahtijeva klijent ili koju nudi poslužitelj još uvijek **dostupna**, poslužitelj vraća poruku **DHCPACK** koja klijentu potvrđuje da je najam finaliziran. Ako **ponuda više ne vrijedi**, tada odabrani poslužitelj odgovara porukom **DHCPNAK**. Ako se vrati DHCPNAK poruka, **tada proces odabira mora započeti ponovno s novom DHCPDISCOVER porukom**.
- Nakon što klijent dobije zakup, **mora se obnoviti prije isteka najma** putem druge DHCPREQUEST poruke.
- DHCP poslužitelj osigurava da su **sve IP adrese jedinstvene** (ista IP adresa ne može se dodijeliti dvama različitim mrežnim uređajima istovremeno). Većina ISP-ova koristi DHCP za dodjelu adresa svojim korisnicima.
- Možemo na računalo inicirati obnovu IP postavki:
 - **ipconfig / release** – otpušta trenutne IP postavke
 - **ipconfig / renew** – Ponovno traži IP postavke od DHCP servera



File Transfer Protocol (FTP)

- U **client/server modelu**, klijent može uplodati podatke na server i downloadati podatke sa servera ako obje strane koriste FTP protokol
- FTP omogućava razmjenu podataka (kopiranje datoteka) između klijenta i servera
- **FTP klijent je aplikacija koja se koristi** which runs on na računalu i koristi princip „**push and pull**” princip za upload i download datoteka na i sa servera
- **Klijent može downloadati (pull) podatke sa servera i može uplodati (push) podatke na server.**



1. Control Connection:

Client opens first connection to the server for control traffic.



2. Data Connection:

Client opens second connection for data traffic.



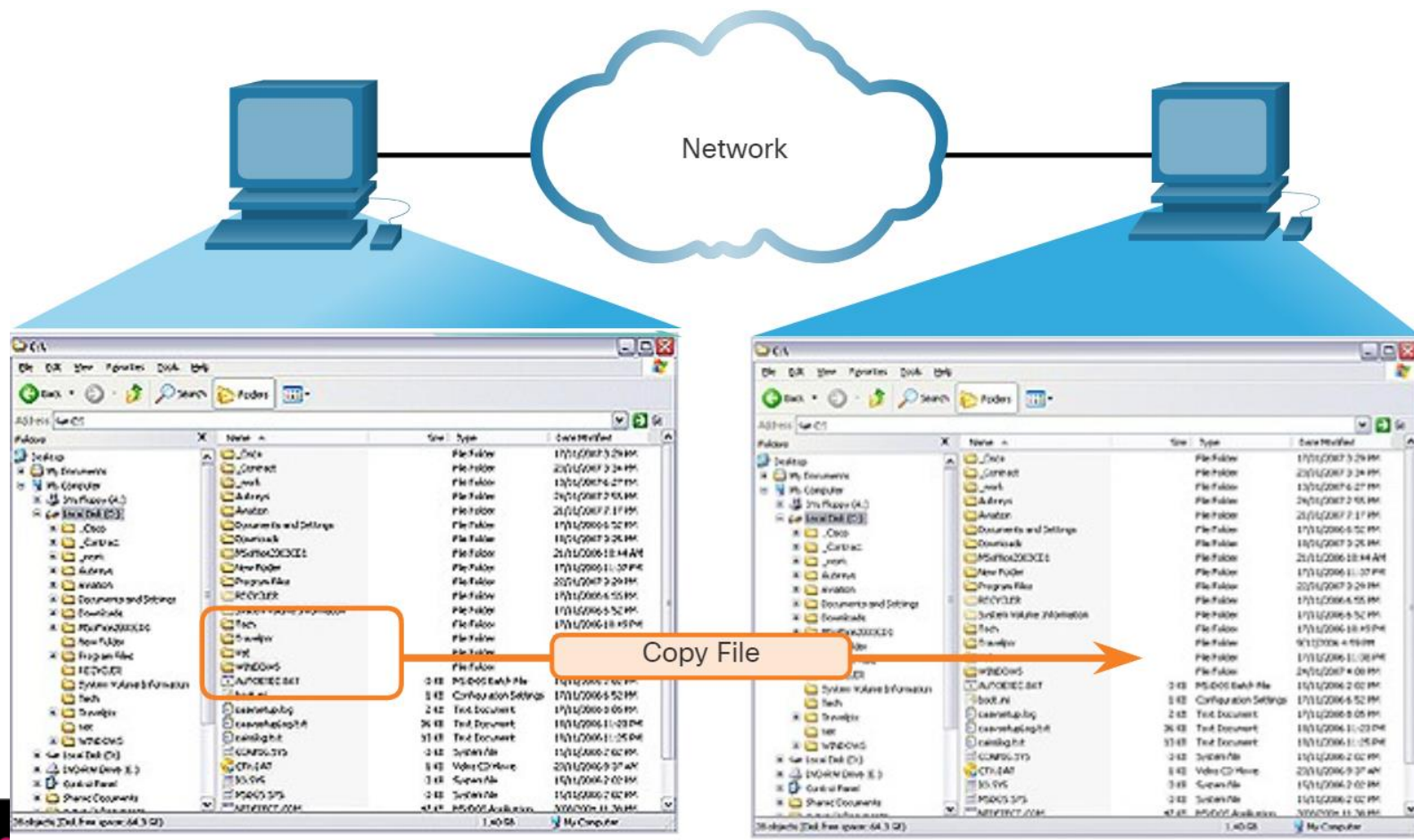
3. Data Transfer:

Server transfers data to the client.

- Klijent uspostavlja vezu sa serverom koristeći **TCP port 21**. Ovaj dio komunikacije se sastoji od raznih upita i odgovora koji služe za uspostavljanje veze između klijentske i serverske aplikacije.
- Za kopiranje datoteka između klijenta i servera koristi se **TCP port 20** i ova se veza uspostavlja svaki puta kada se podatci kopiraju.

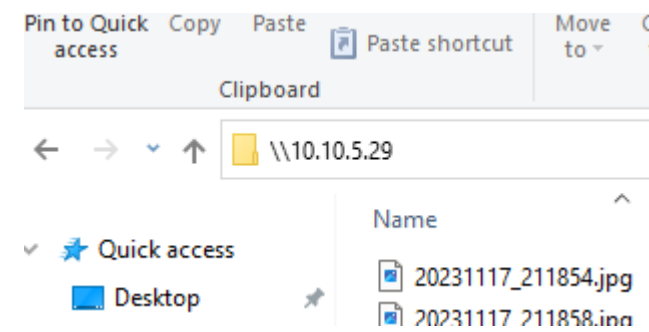
Server Message Block-SMB

- Server Message Block (SMB) je **client/server file sharing protocol (protokol za dijeljenje datoteka/resursa)** koji opisuje strukturu dijeljenih resursa kao što su **mape, datoteke, printeri i serijska sučelja (serial port)**.
- Radi po principu request-response sve poruke koriste isti format sa zaglavljima fiksne veličine iza kojeg su varijabilni podatci- koristi **TCP port 445**



Pristupanje dijeljenoj mapi na udaljenom računalu

1. Izraditi mapu na PC1
2. Promijeniti postavke za dijeljenje na samoj mapi na PC1
3. Pristupiti dijeljenoj mapi s udaljenog računala PC2





NAT (Network Address Translation)

- Za zatvorene sustave možemo koristiti 3 raspona IP adresa bez da trebamo ikome to javiti ili tražiti dopuštenje. Privatni rasponi IP adresa su opisani u dokumentu RFC1918
 - 10.0.0.0/8 -> A klasa privatnih IP adresa (16M adresa)
 - 172.16.0.0/12 -> B klasa privatnih IP adresa (1M adresa)
 - 192.168.0.0/16 -> C klasa privatnih IP adresa (64k adresa)
- Mreže 192.168.0.0/16 su najčešće korištene u malim privatnim mrežama (rezidencijalni korisnici)
- Ako računalo iz privatne mreže želi komunicirati s računalima na javnom adresnom prostoru (Internet) mora proći kroz uređaj koji radi NAT ili PAT (Port Address Translation)
- U javnoj mreži svaka pojava privatnih IP adresa na internetu smatra se greškom i takvi paketi se odbacuju

NAT (Network Address Translation)

Javna IP adresa je ista za sva računala u privatnoj meži

| | |
|----------------------------|----------------|
| Your IP Address Is: | |
| 94.253.193.23 | |
| City: | Zagreb |
| State: | Grad Zagreb |
| Country: | HR |
| ISP: | B.net Hrvatska |

```
Command Prompt
(c) 2015 Microsoft Corporation. All rights reserved.
C:\Users\Sharkon>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet 3:

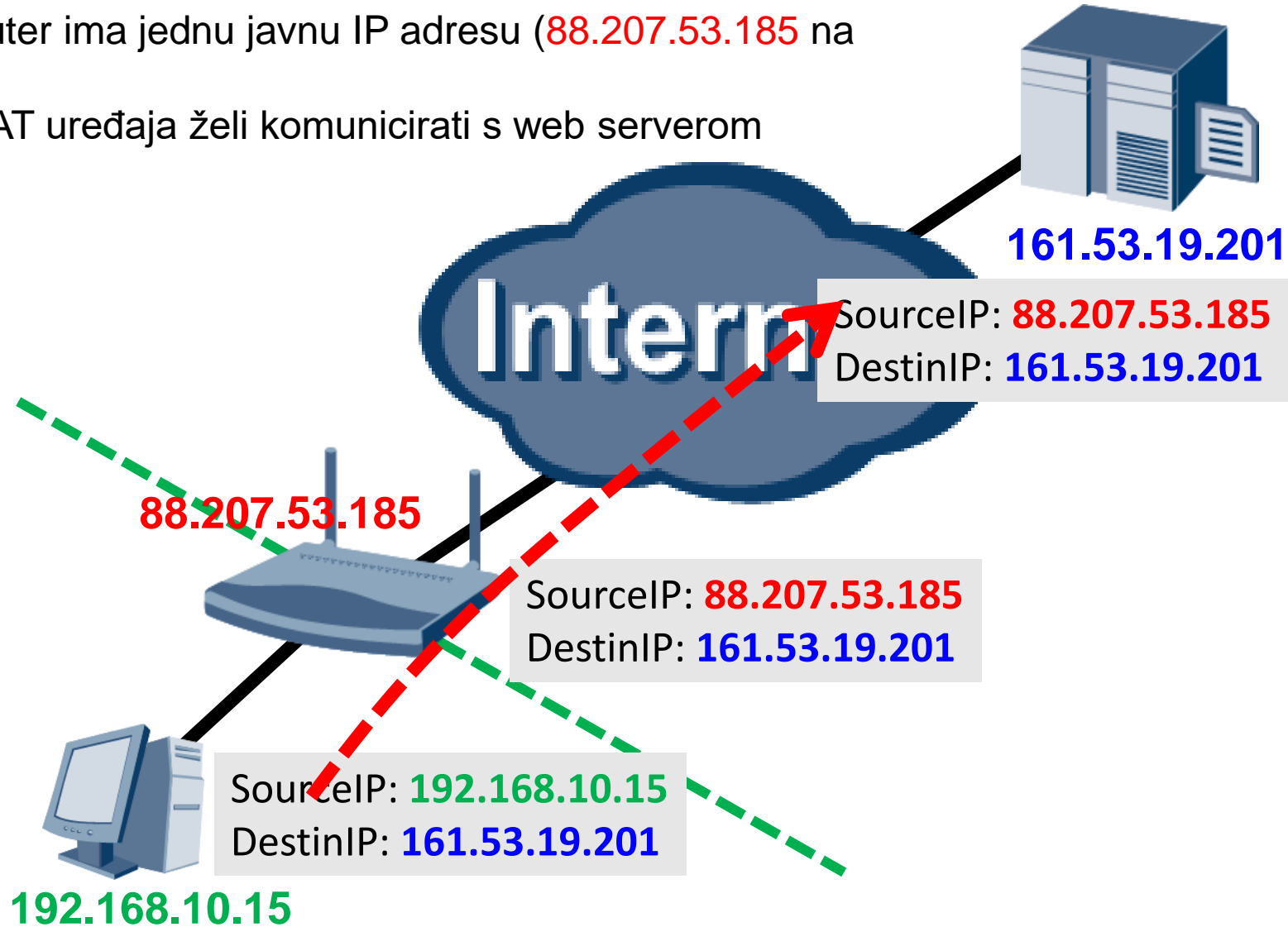
    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.0.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1
```

Privatna IP adresa je jedinstvena za svako računalo u privatnoj mreži

- NA mrežnom sloju uređaji koji su konfigurirani da rade NAT mijenjaju privatnu IP adresu računala i stavljaju svoju javnu IP adresu kao source i takav paket šalju na javnu mrežu prema odredištu
- **Nije moguće** (bez eksplicitnog mapiranja na vatrozidu-”port forwarding”) **otvoriti konekcije prema računalima unutar privatne mreže**

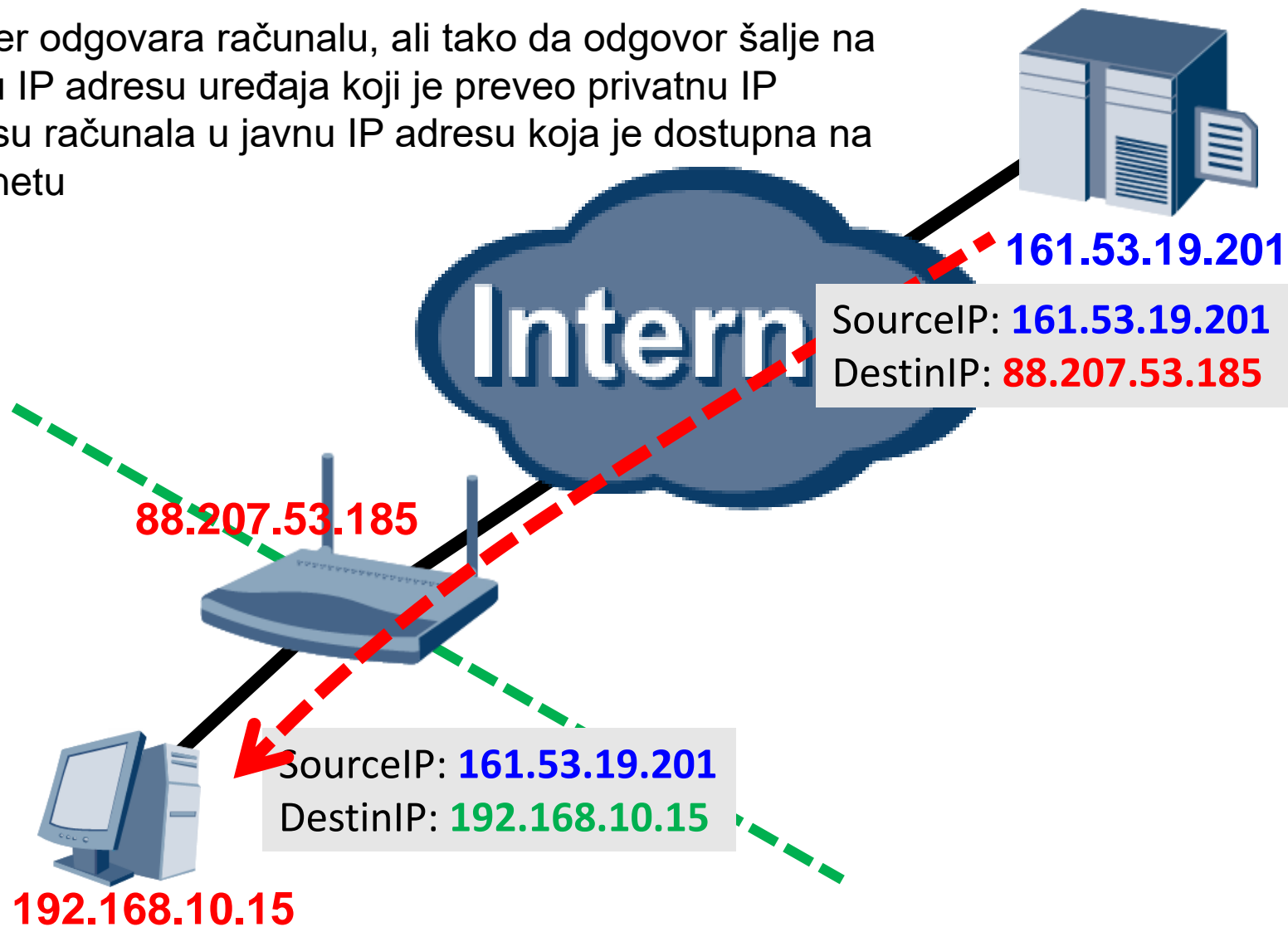
NAT-outgoing traffic

- DSL modem/router ima jednu javnu IP adresu (**88.207.53.185** na slici)
- Računalo iza NAT uređaja želi komunicirati s web serverom **161.53.19.201**



NAT- povratni promet

- Server odgovara računalu, ali tako da odgovor šalje na javnu IP adresu uređaja koji je preveo privatnu IP adresu računala u javnu IP adresu koja je dostupna na internetu



Što neće raditi kroz NAT

1. **Console gaming** – Neke igre neće raditi dobro ili uopće neće raditi ako je više računala iza uređaja koji radi NAT
2. **Video streaming** – performanse su narušene kada imamo više video streamova prema računalima iza jednog uređaja koji radi NAT
3. **Peer-to-peer** – Neke peer-to-peer aplikacije neće raditi jer ne mogu prihvatiti dolazne konekcije, ako nisu eksplicitno propuštene kroz NAT
4. **Geo-location** – Ako je krajnje računalo iza NAT-a geolokacija nije pouzdana
5. **Višestruka logiranja (prijava)** – Neke mrežne stranice ograničavaju broj istovremenih prijava s jedne javne IP adrese

