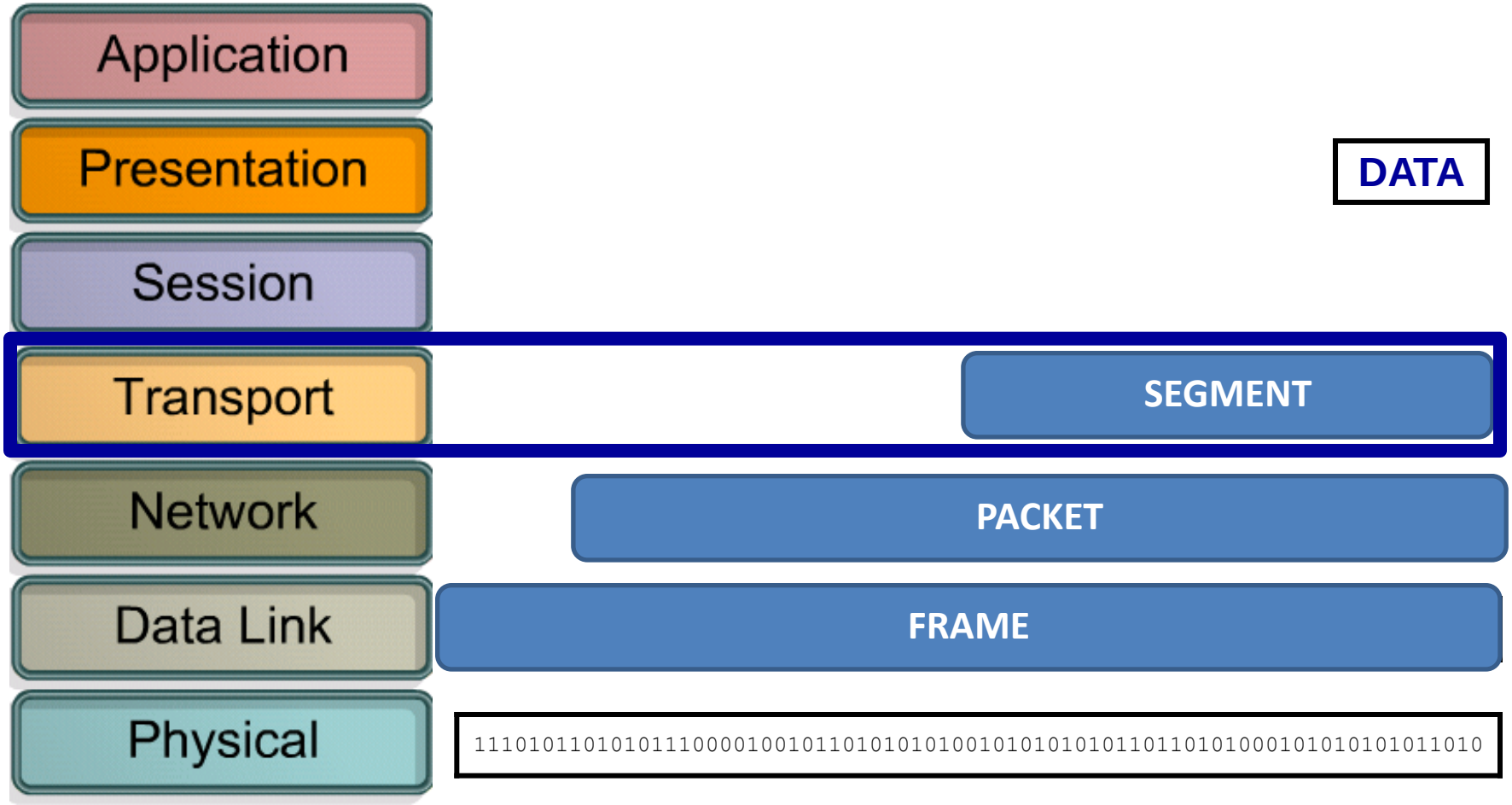
TRANSPORTNI SLOJ

Predmet: Aktivni mrežni uređaji

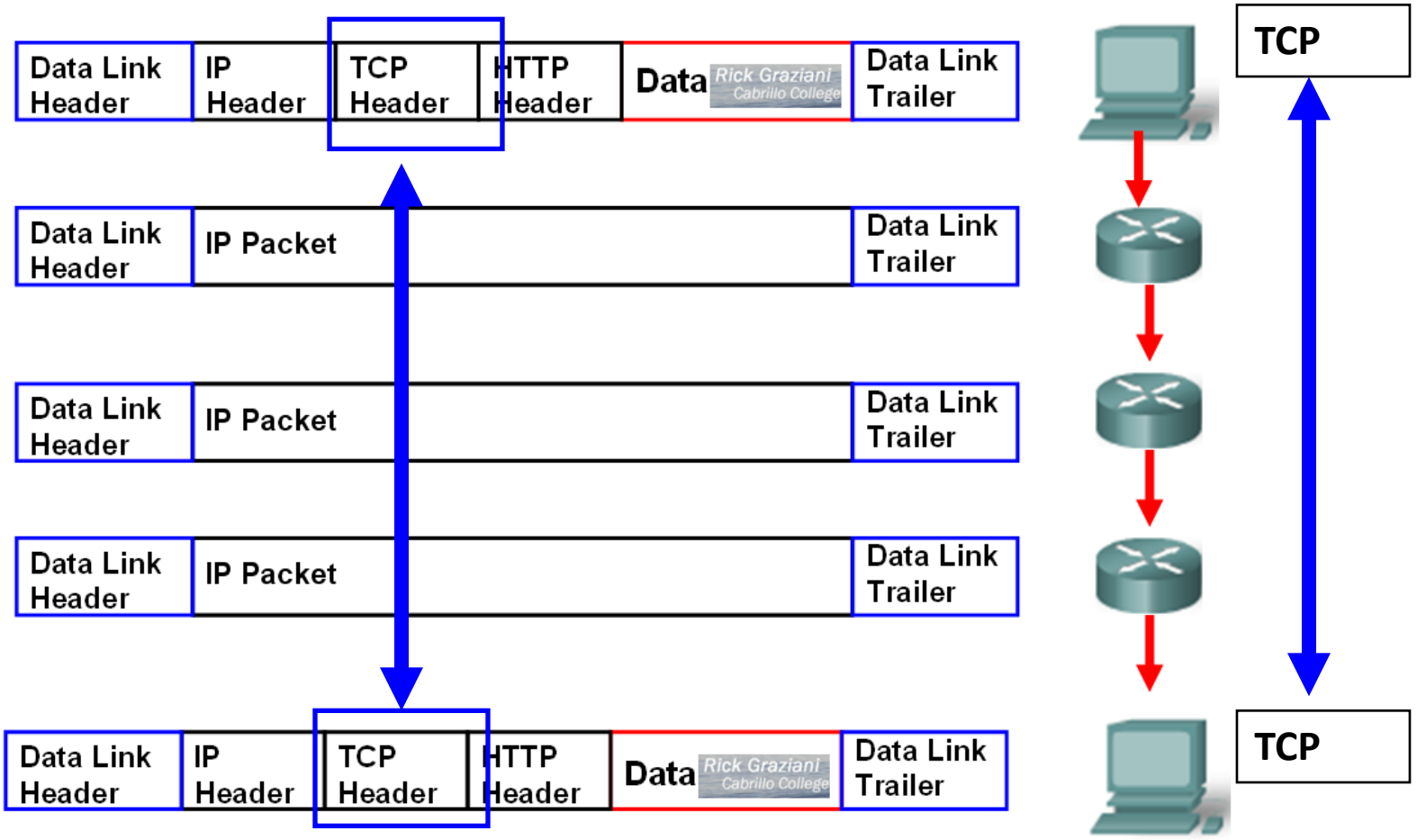
Predavač: dr Dušan Stefanović

ENKAPSULACIJA

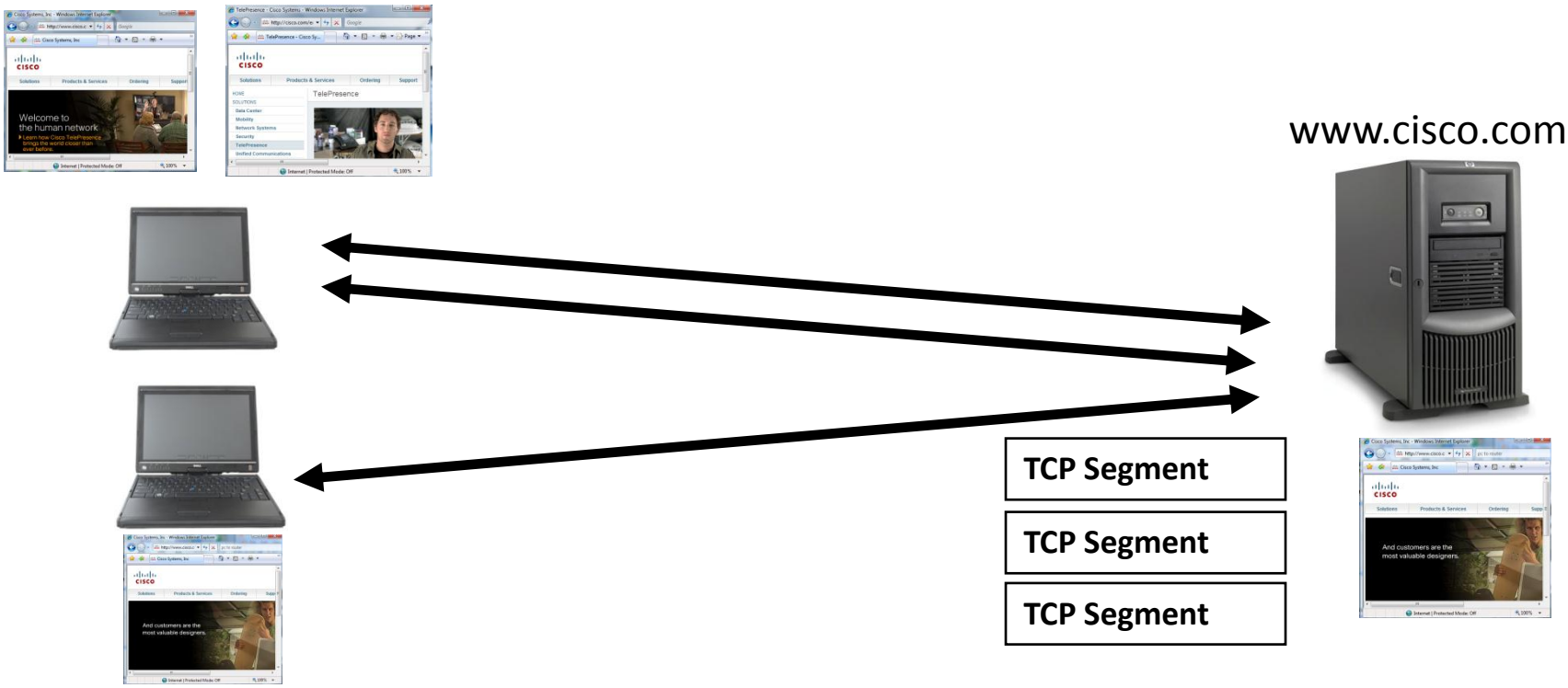


TRANSPORTNI SLOJ

- Komunikacija na transportnom sloju se ostvaruje između krajnjih hostova u komunikaciji.
- Obezbeđuje pouzdanost i kontrolu toka

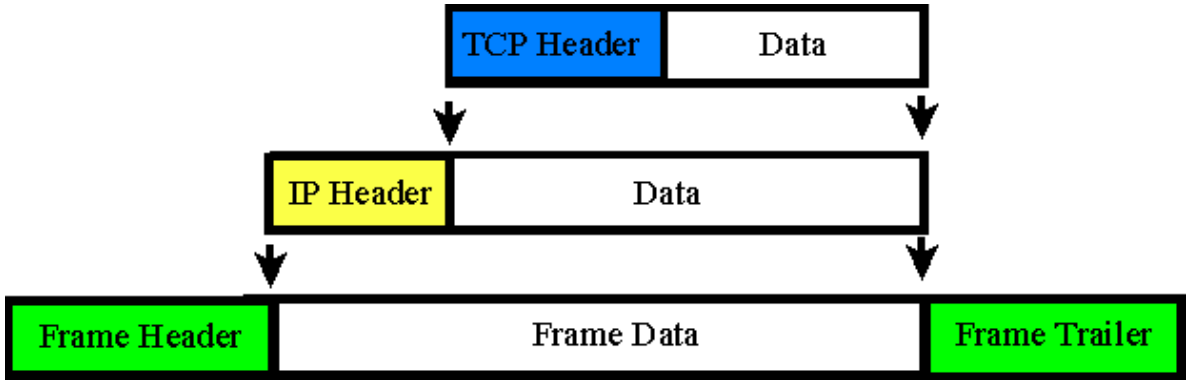


ULOGA TRANSPORTNOG SLOJA

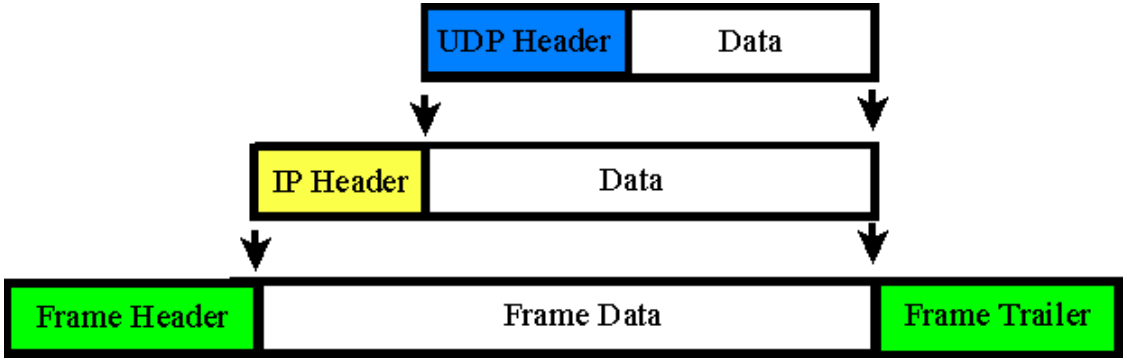


1. Prati individualnu komunikaciju između aplikacija na izvoru i odredištu
2. Od podatka kreira segmente koje na odredištu sastavlja ponovo u podatak
3. Na jedinstven način označava tj. identifikuje svaku sesiju

TCP (TRANSMISSION CONTROL PROTOCOL)

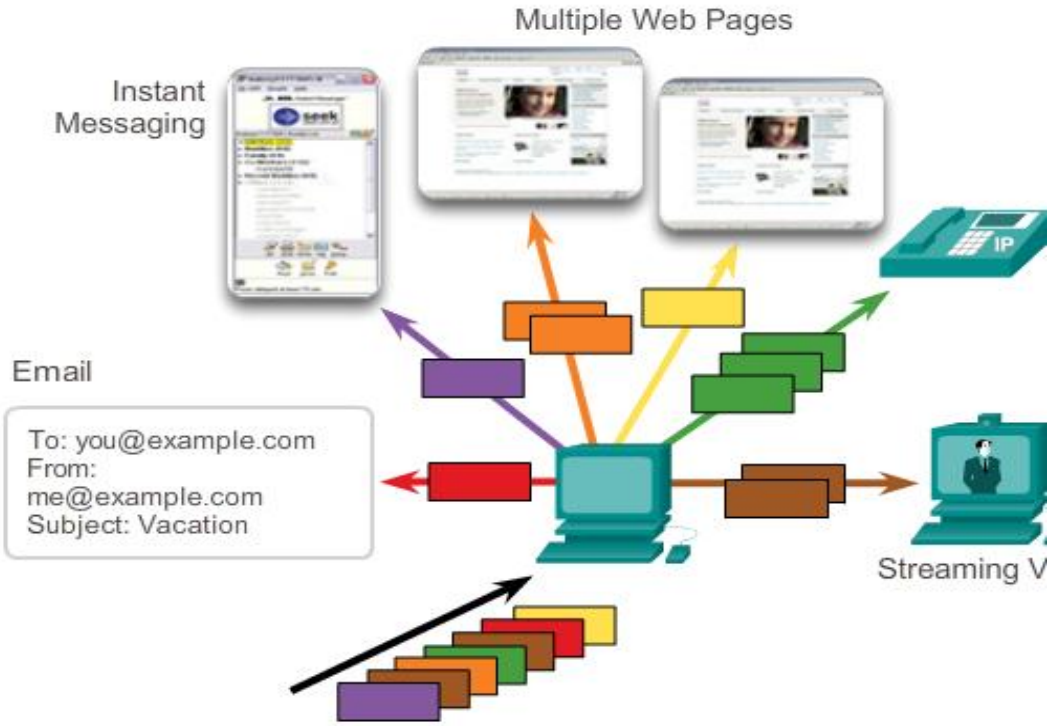


UDP (USER DATAGRAM PROTOCOL)

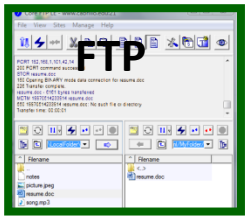


TRANSPORTNI SLOJ

- Svaki host u mreži može istovremeno da pokrene više aplikacija
- Zadatak transportnog sloja je da upravlja ovim sesijama između izvorišnog i odredišnog računara
- Jedan klijent može da uspostavi više istovremenih konekcija sa različitim serverima



TRANSPORTNI SLOJ



7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical

TCP
TCP
TCP
TCP
TCP
TCP

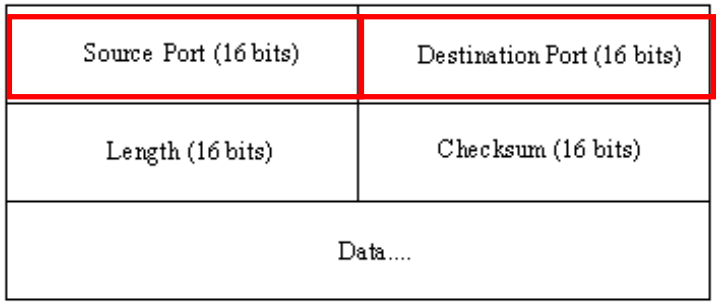
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical

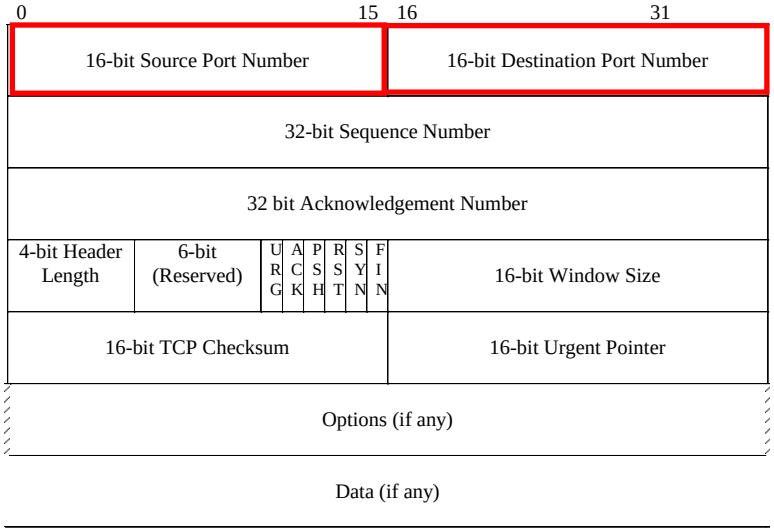
VTS Web Server

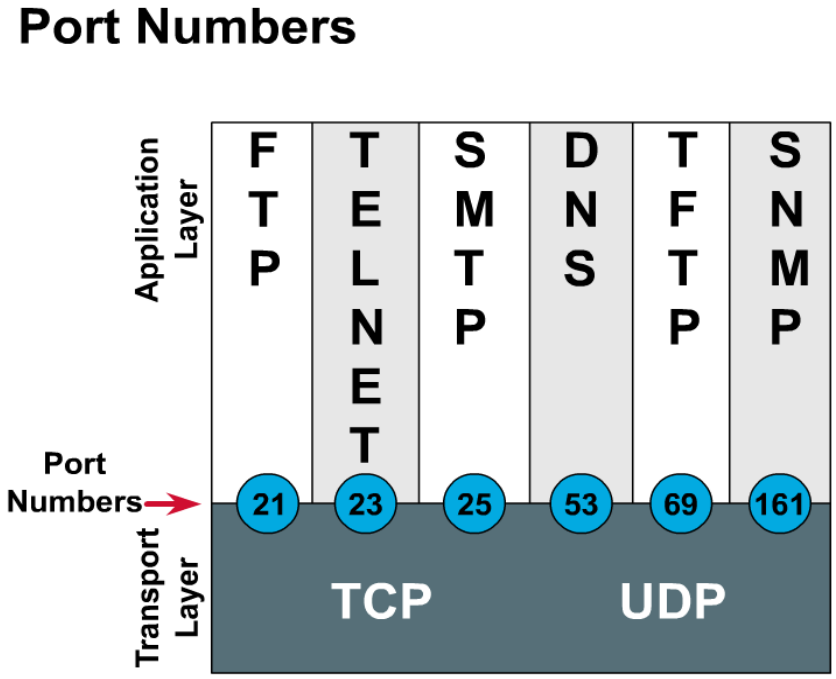
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical

ISP Email i FTP Server

IDENTIFIKACIJA APLIKACIJE



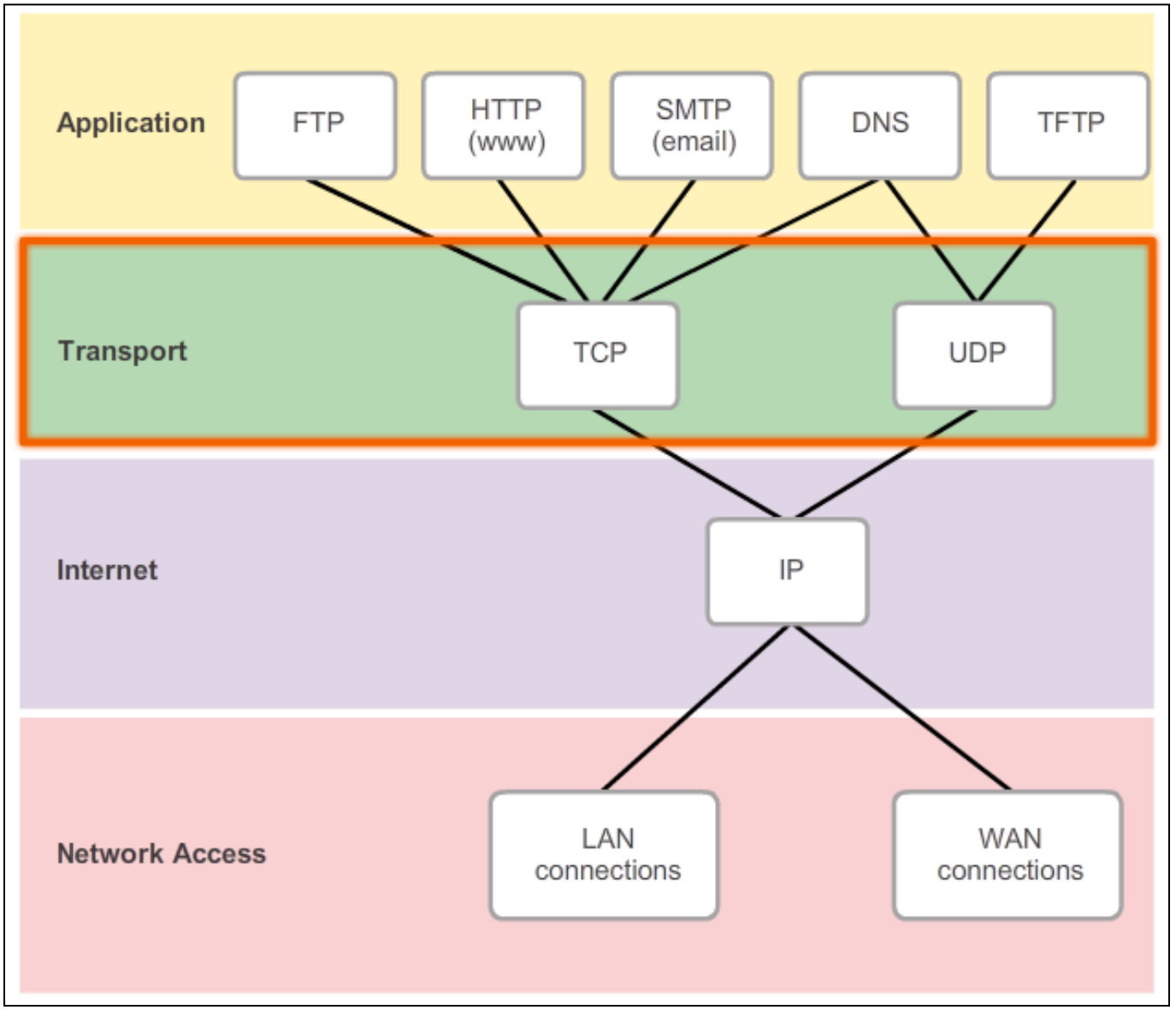




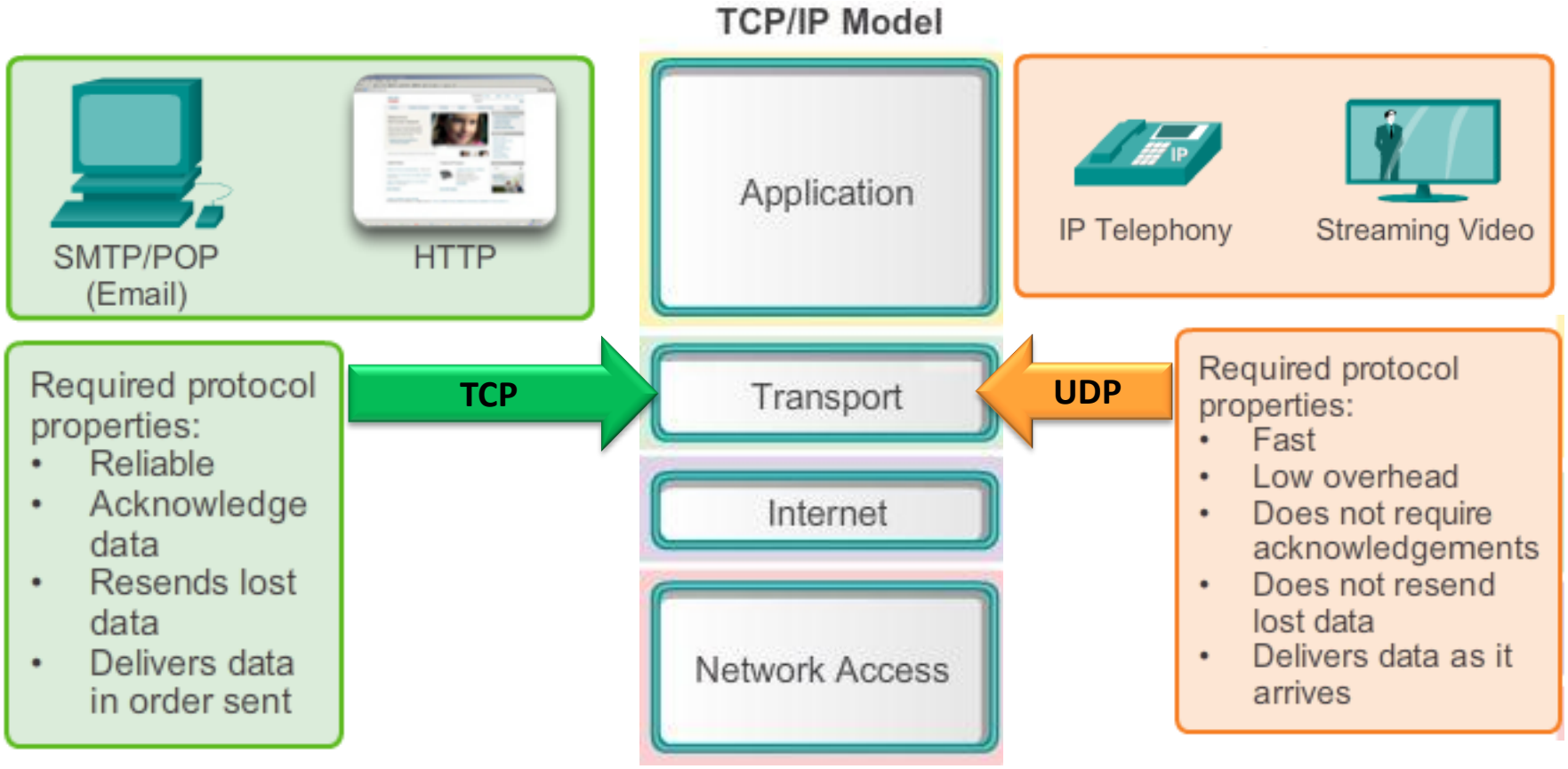
Transportni sloj zadaje svakoj aplikaciji identifikator koji se zove port.

Na osnovu broja porta transportni sloj identifikuje svaku aplikaciju.

TRANSPORTNI SLOJ

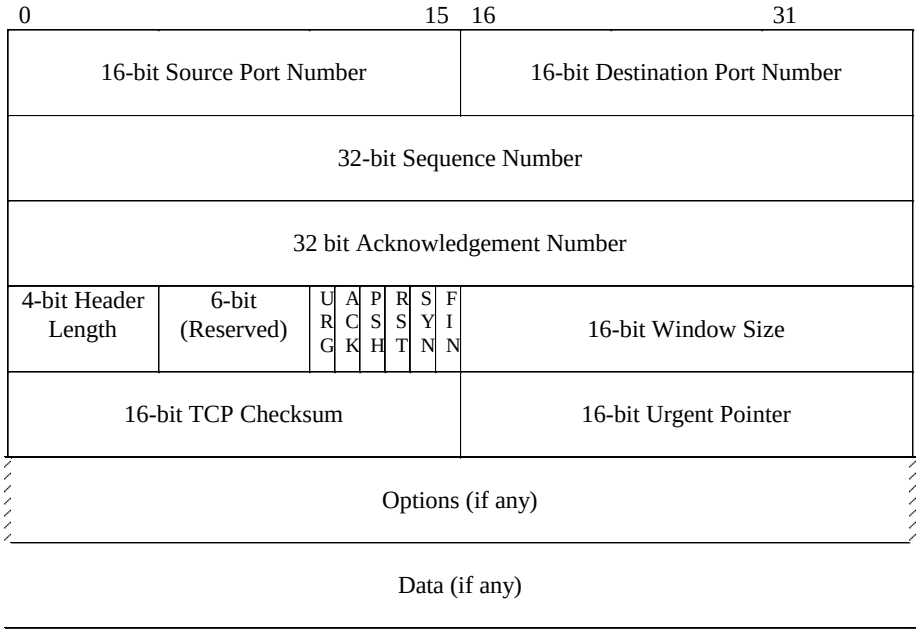


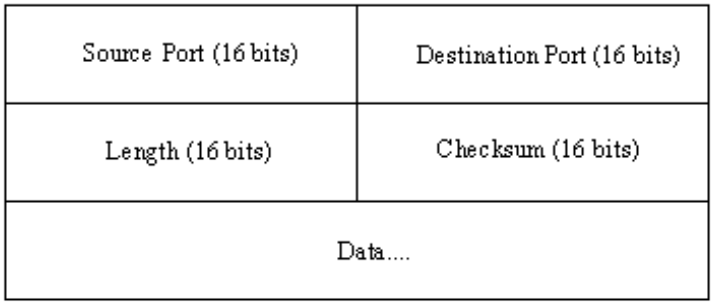
TCP / UDP



TCP i UDP koriste se za različitu vrstu saobračaja

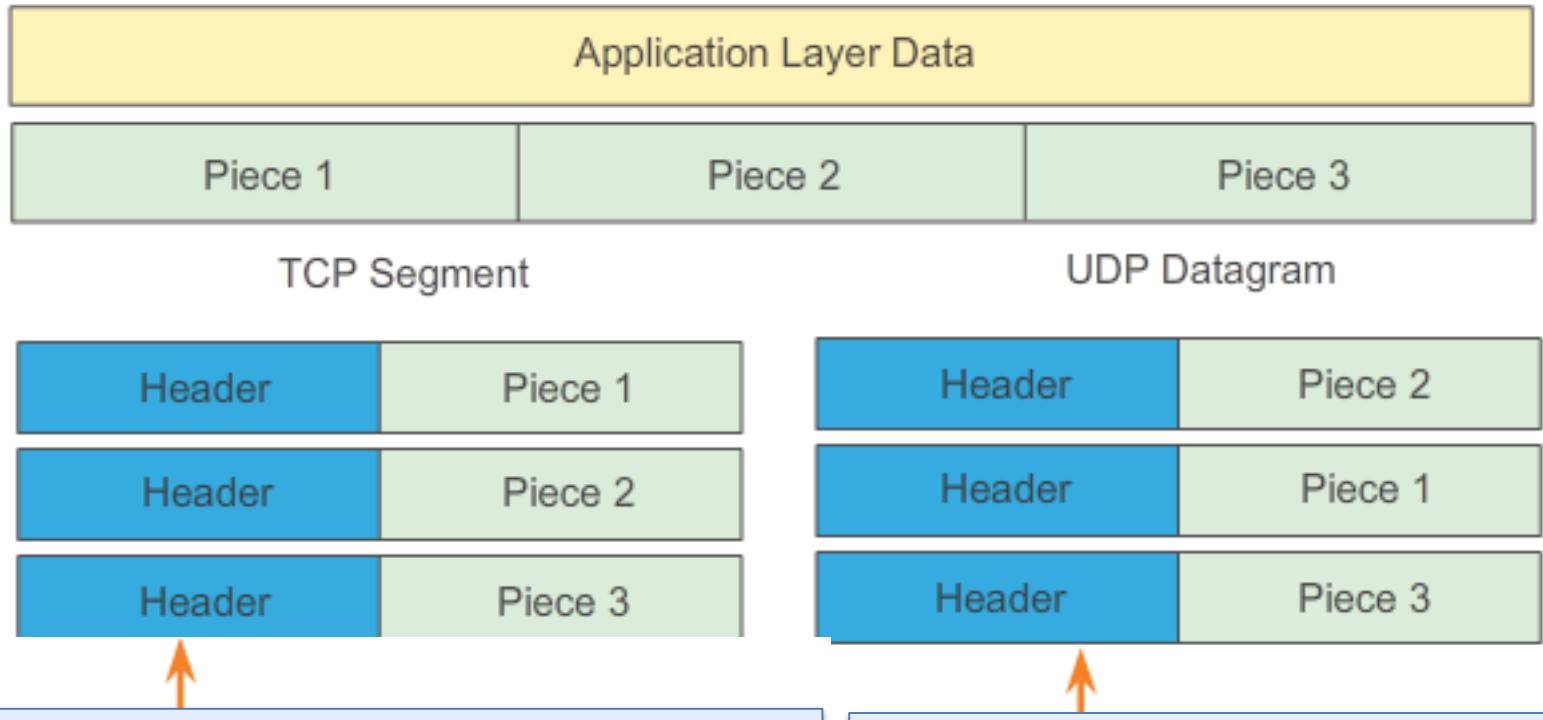
TCP / UDP





TCP je znatno kompleksniji od UDP-a

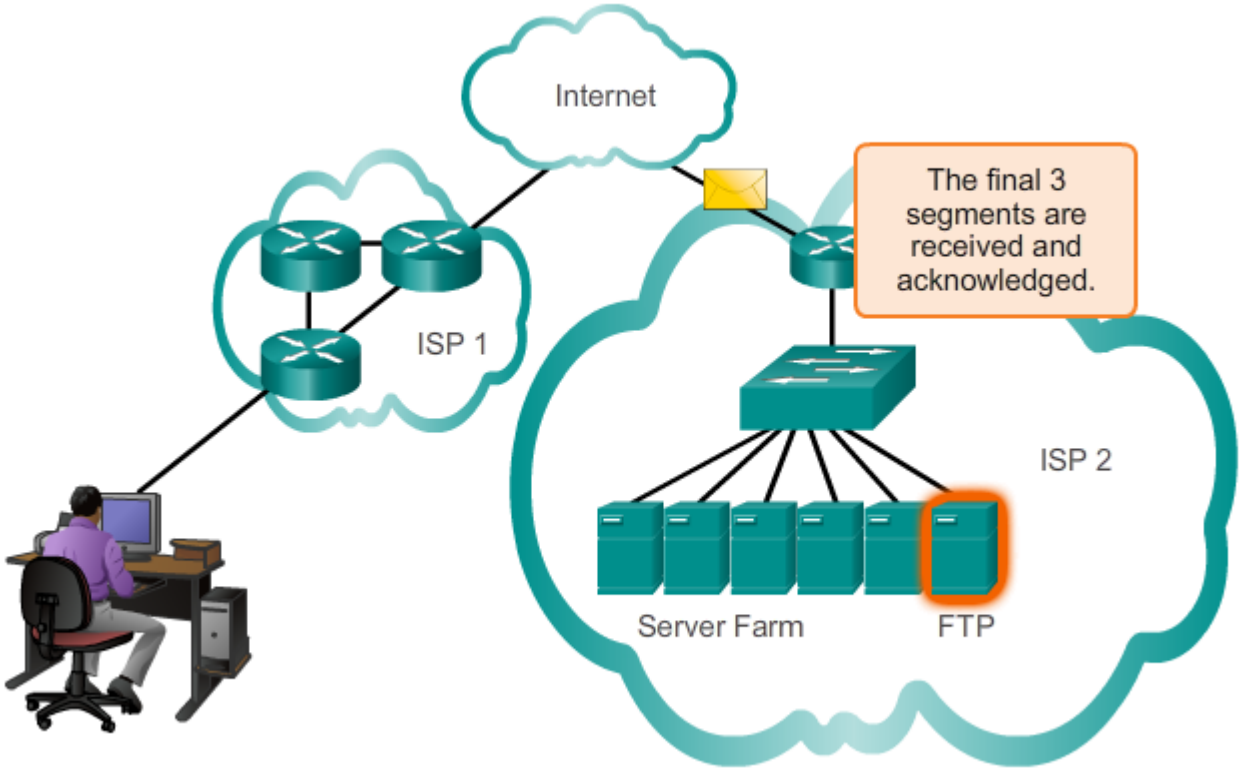
TCP / UDP



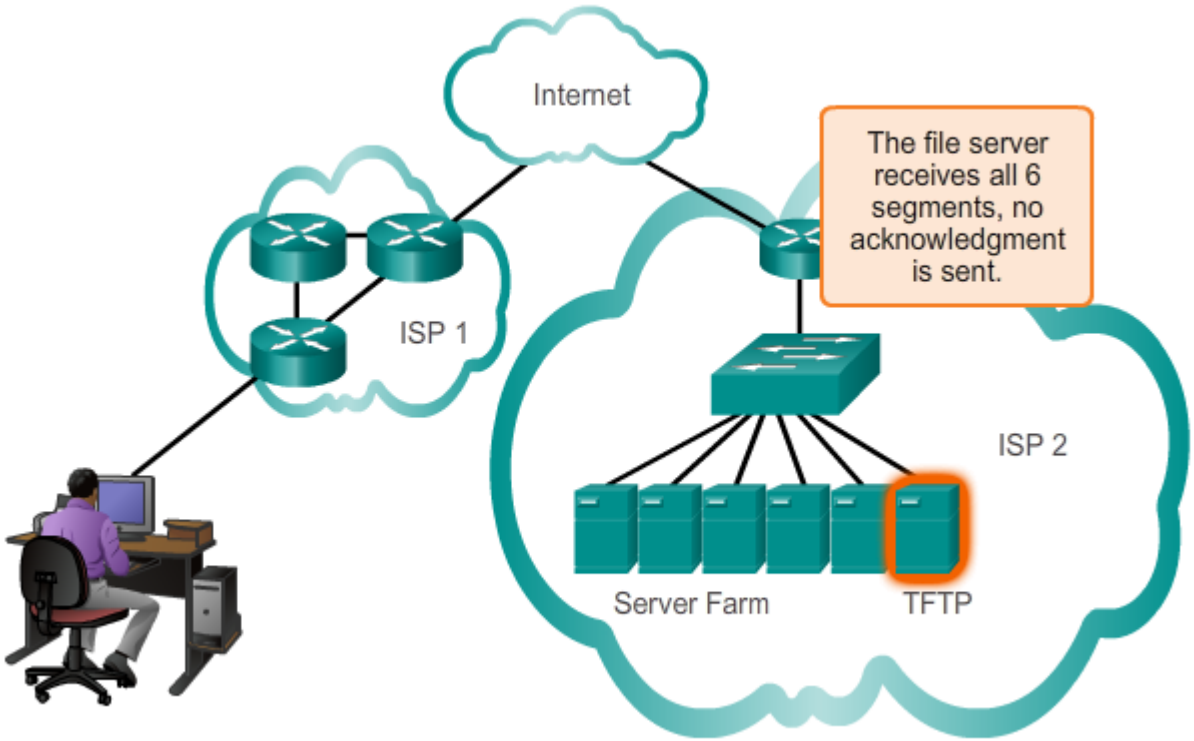
TCP HEADER obezbeđuje:
- Izvorišni i odredišni port
- Sekvenciranje segmenata
- Potvrda segmenata na prijemu
- Kontrola toka i upravljanje nagomilavanjem

UDP HEADER obezbeđuje:
- Izvorišni i odredišni port

TCP


Internet
The final 3 segments are received and acknowledged.
ISP 1
ISP 2
Server Farm
FTP

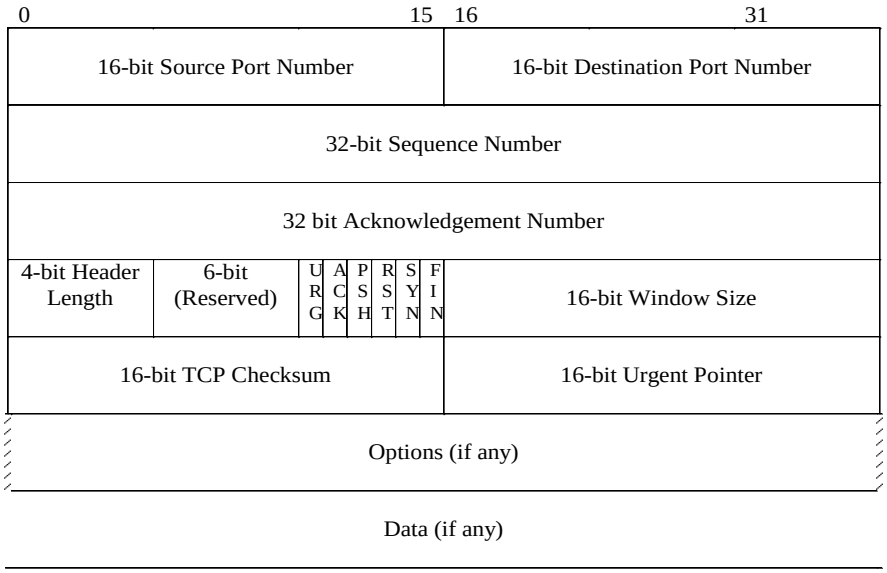
UDP


Internet
The file server receives all 6 segments, no acknowledgment is sent.
ISP 1
ISP 2
Server Farm
TFTP

TCP SERVISI

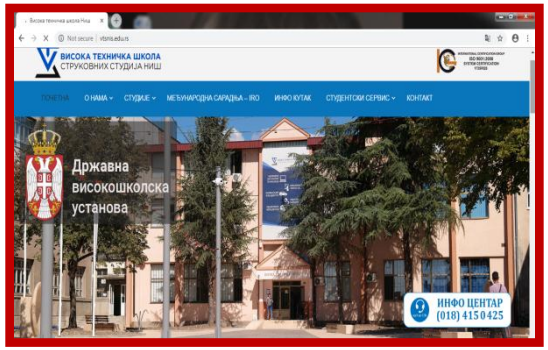
TCP obezbeđuje sledeće servise:

- Pouzdana isporuka (**Reliable delivery**)
- Detekcija grešake (**Error checking**)
- Kontrola toka (**Flow control**)
- Kontrola nagomilavanja (**Congestion control**)
- Isporuka u tačnom redosledu (**Ordered delivery**)
- Uspostavljanje konekcije (**Connection establishment**)

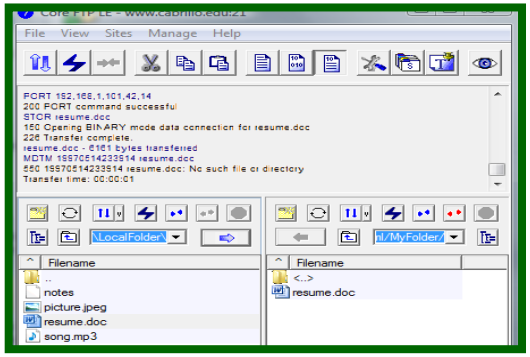


TCP - KARAKTERISTIKE

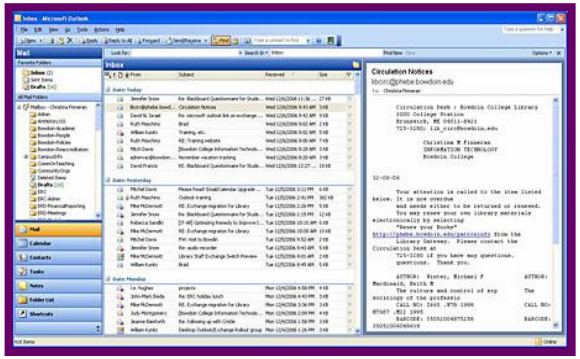
HTTP



FTP



SMTP

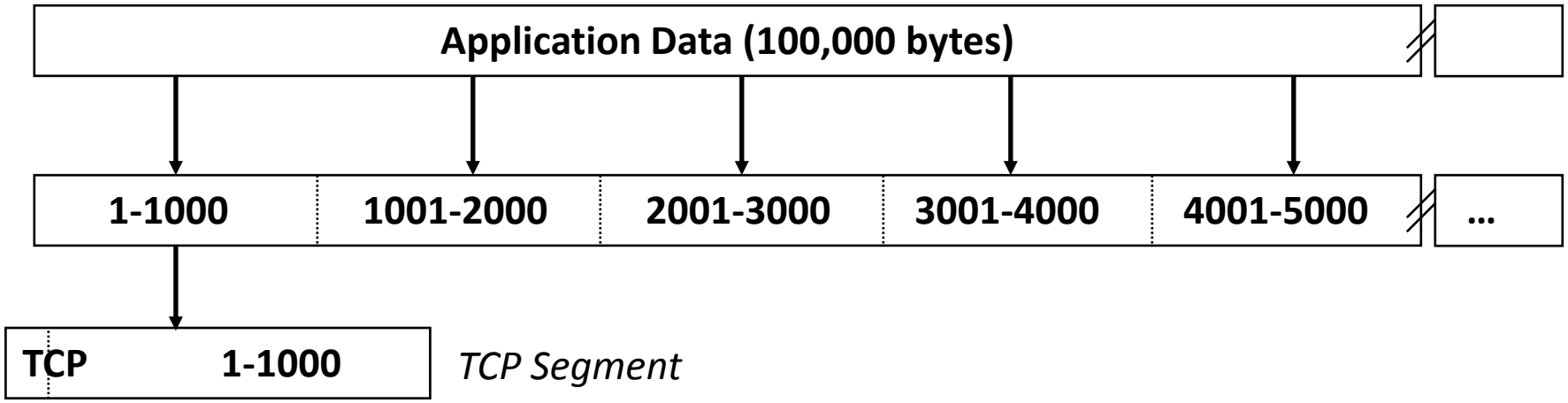


TCP je konekcioni protokol (Connection-oriented)

TCP dodaje 20 Bajta kontrolnih informacija u zaglavlju za svaki segment

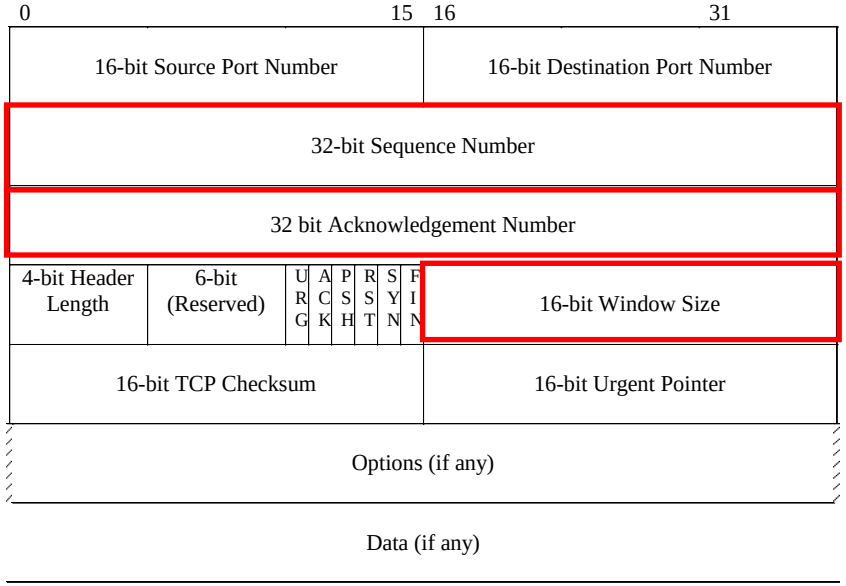
Podaci na transportnom sloju se zovu **segmenti**

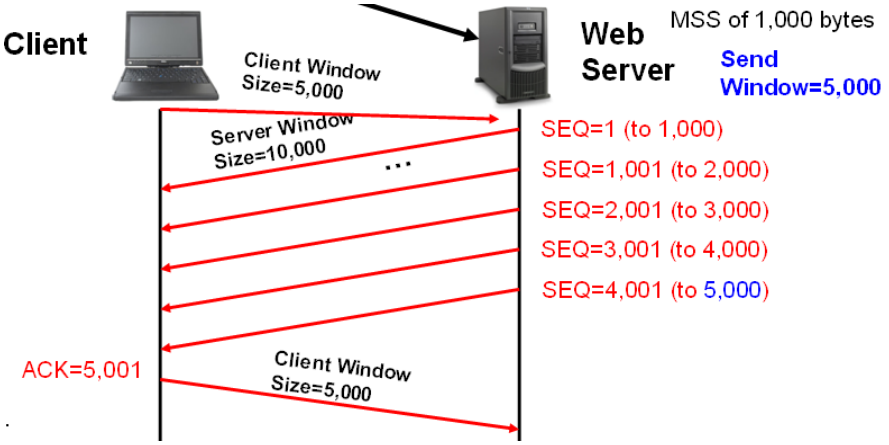
TCP - KARAKTERISTIKE



- TCP enkapsulira podatak u veliki broj segmenata.
  - Segmenti obezbeđuju da komunikacija kroz mrežu bude efikasna.
- TCP zaglavlje uključuje sledeće informacije:
  - Source port number i Destination port number prate svaku pojedinačnu komunikaciju
  - Sequence numbers numeracija svakog segmenta.
  - Window size definiše kontrolu toka za sesiju.
  - Error checking mehanizam za proveru grešaka

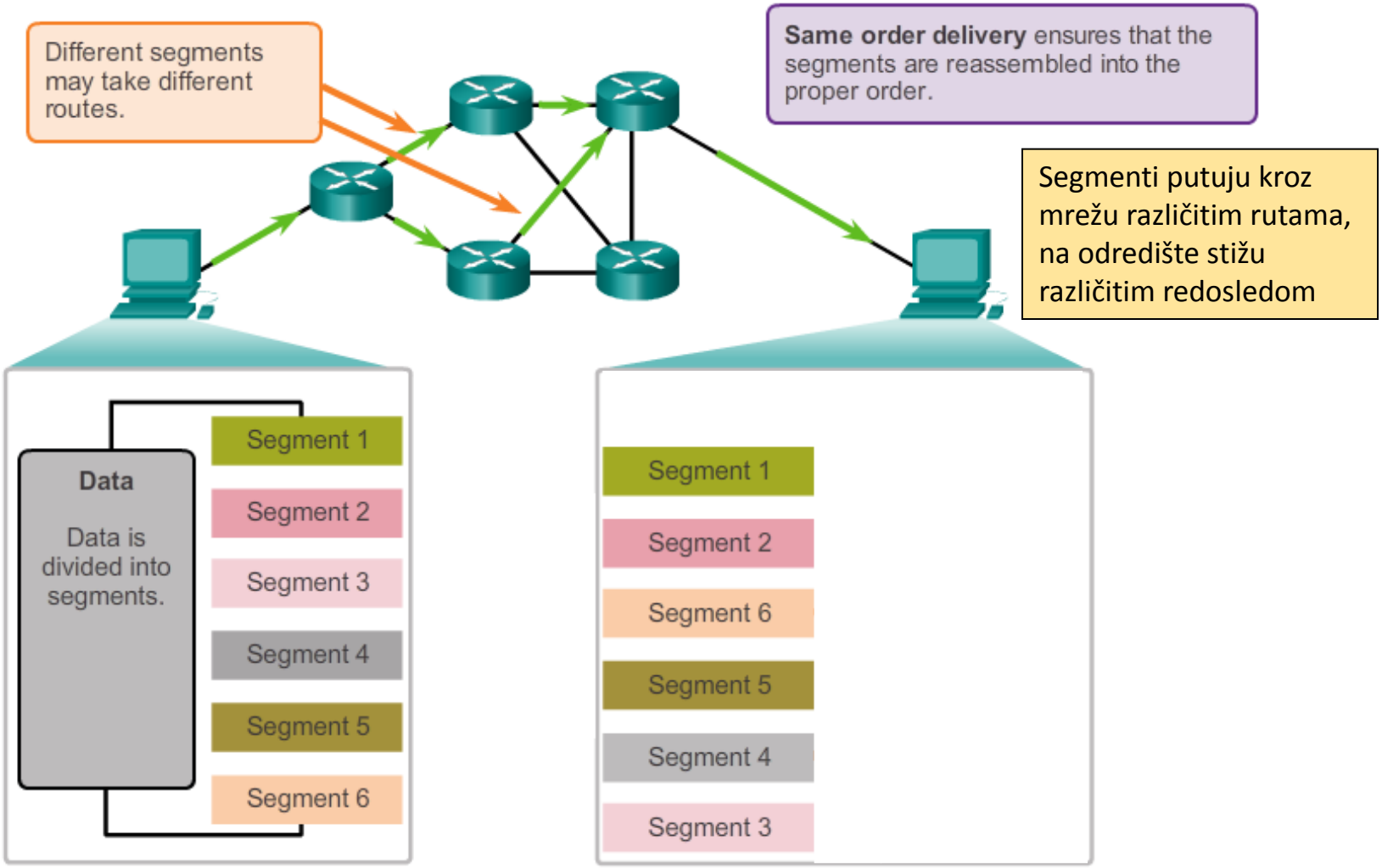
POUZDAN PRENOS I KONTROLA TOKA



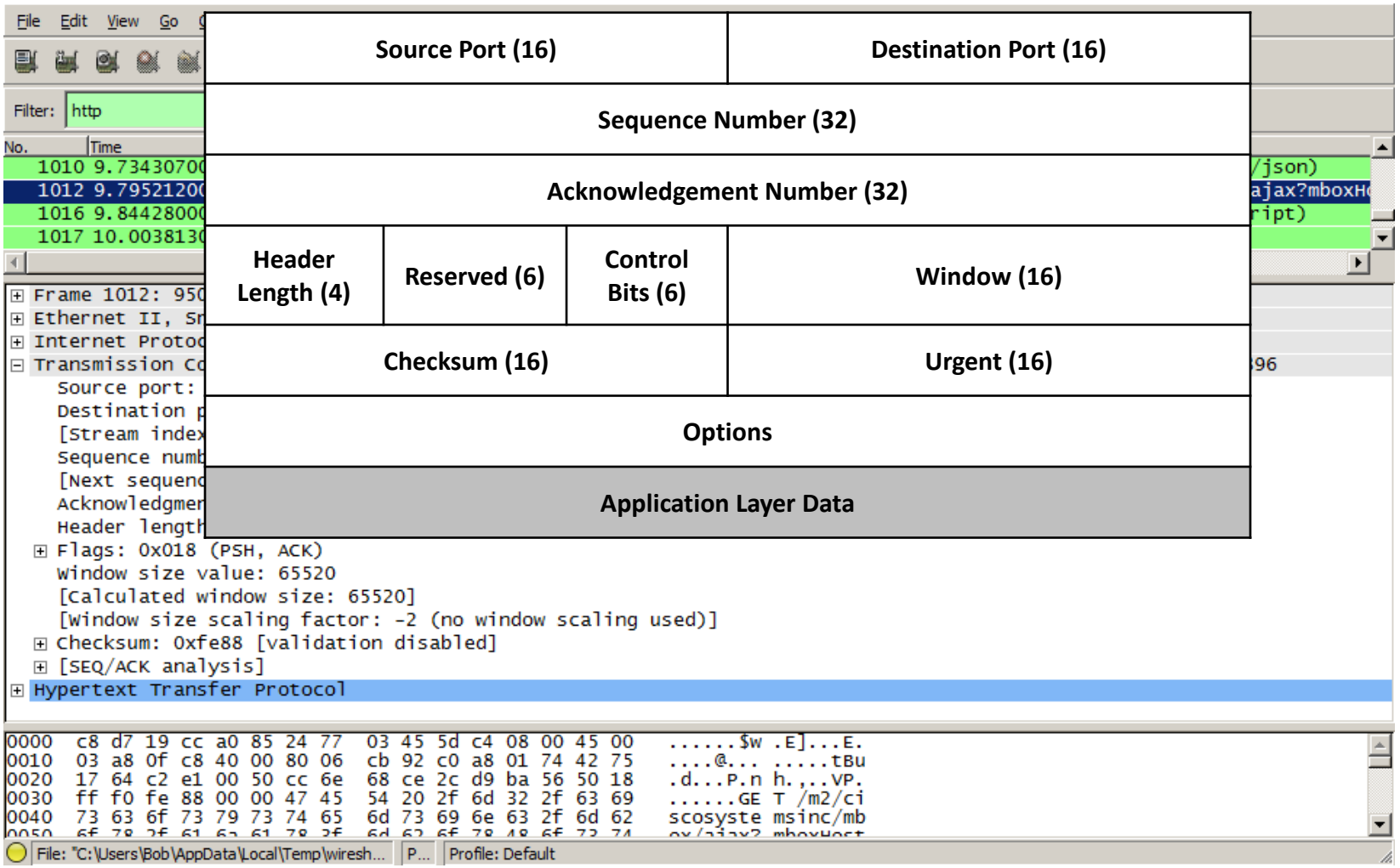


- Na prijemu, svaki segment se pregleda i rekonstruiše u data stream na osnovu sequence brojeva
  - Segment koji nedostaje traži se od izvora.
- Nakon toga se segment prosleđuje odgovarajućoj aplikaciji

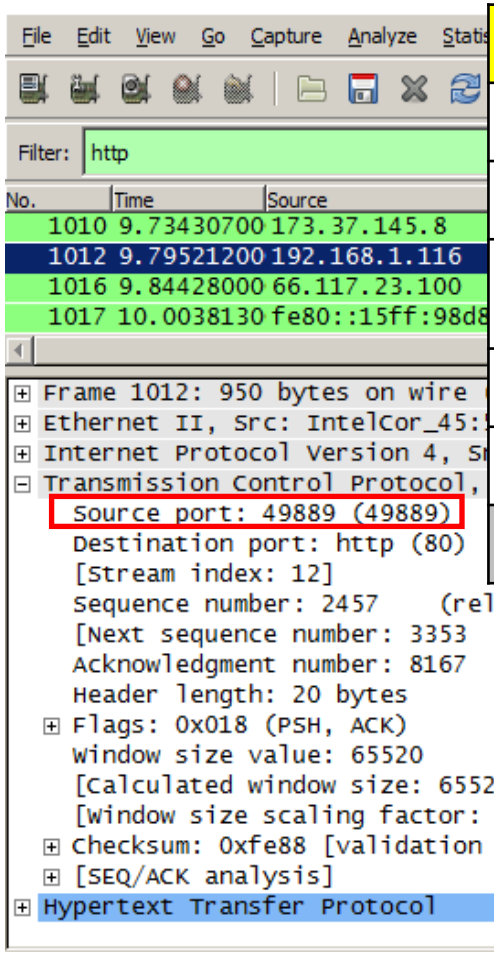
REDOSLED ISPORUKE SEGMENATA

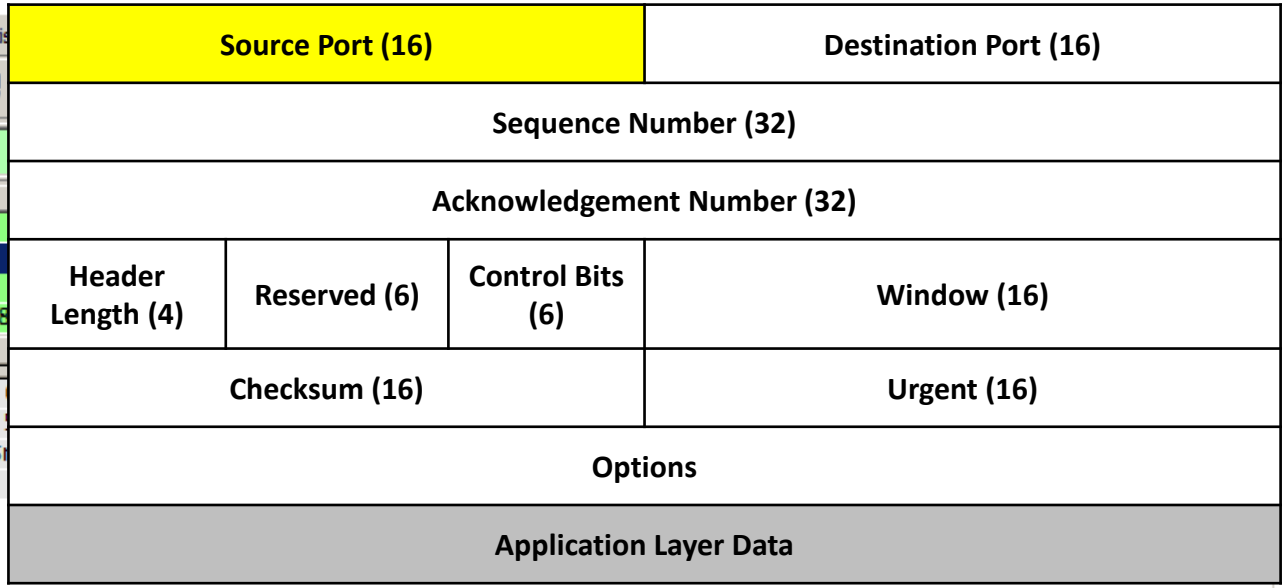


TCP SEGMENT U WIRESHARK-U



TCP SEGMENT U WIRESHARK-U

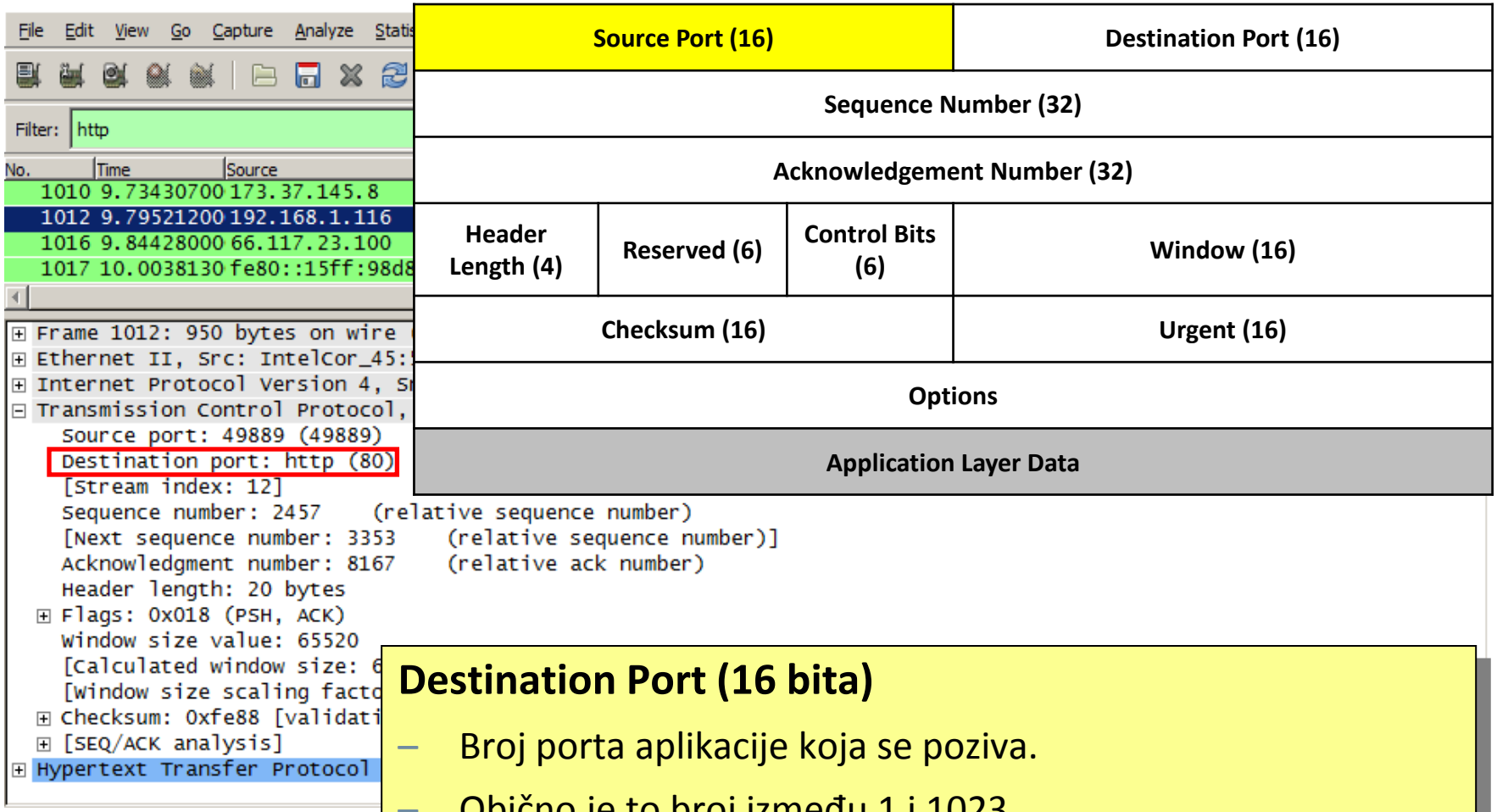




Source Port (16 bita)

- Broj porta aplikacije koja uspostavlja sesiju.
- Dynamički se zadaje hostu koji inicira konekciju.
- Opseg portova je od 1024 do 65,535.

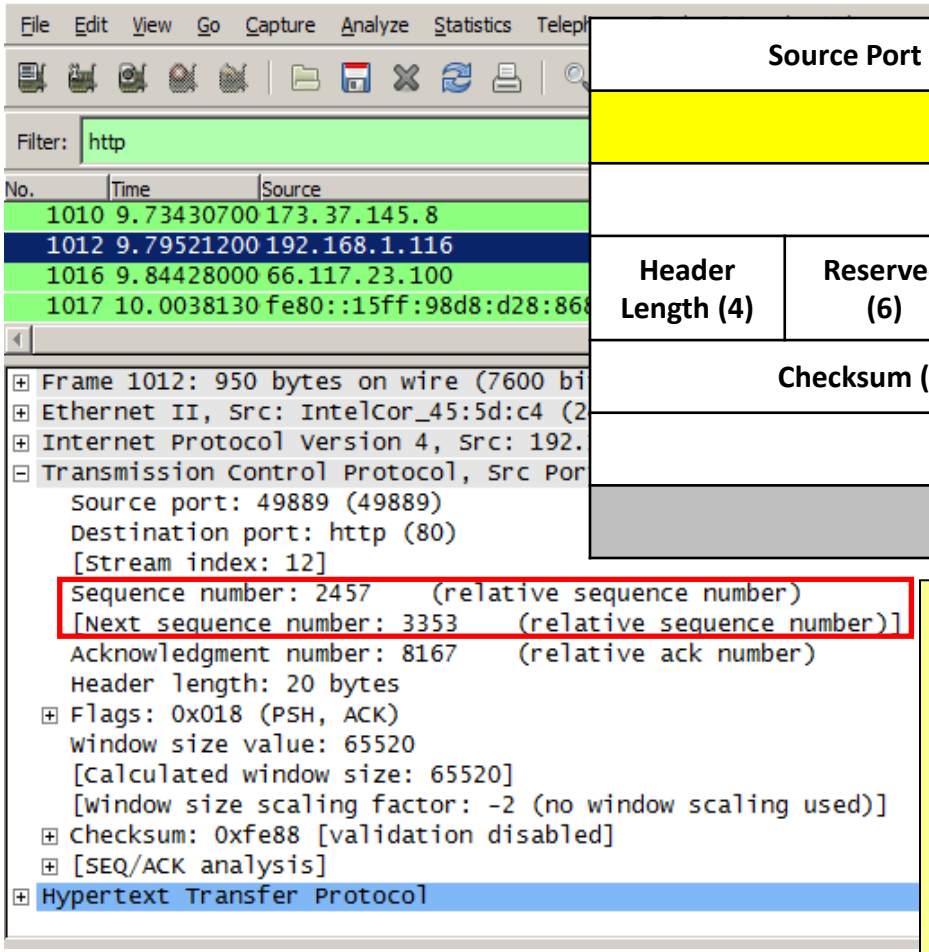
TCP SEGMENT U WIRESHARK-U

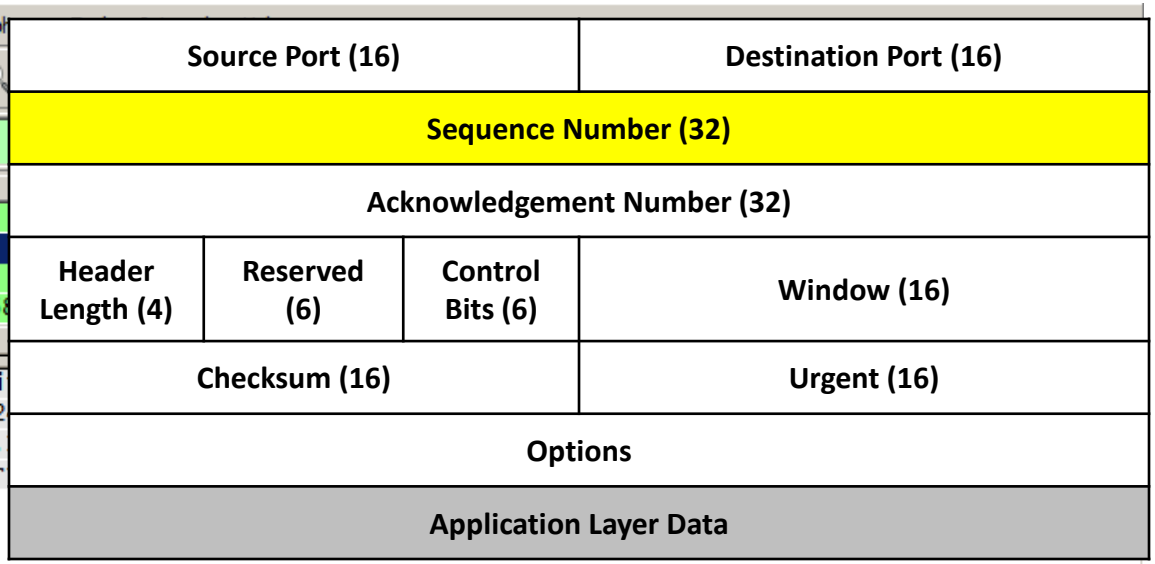


Destination Port (16 bita)

- Broj porta aplikacije koja se poziva.
- Obično je to broj između 1 i 1023.

TCP SEGMENT U WIRESHARK-U

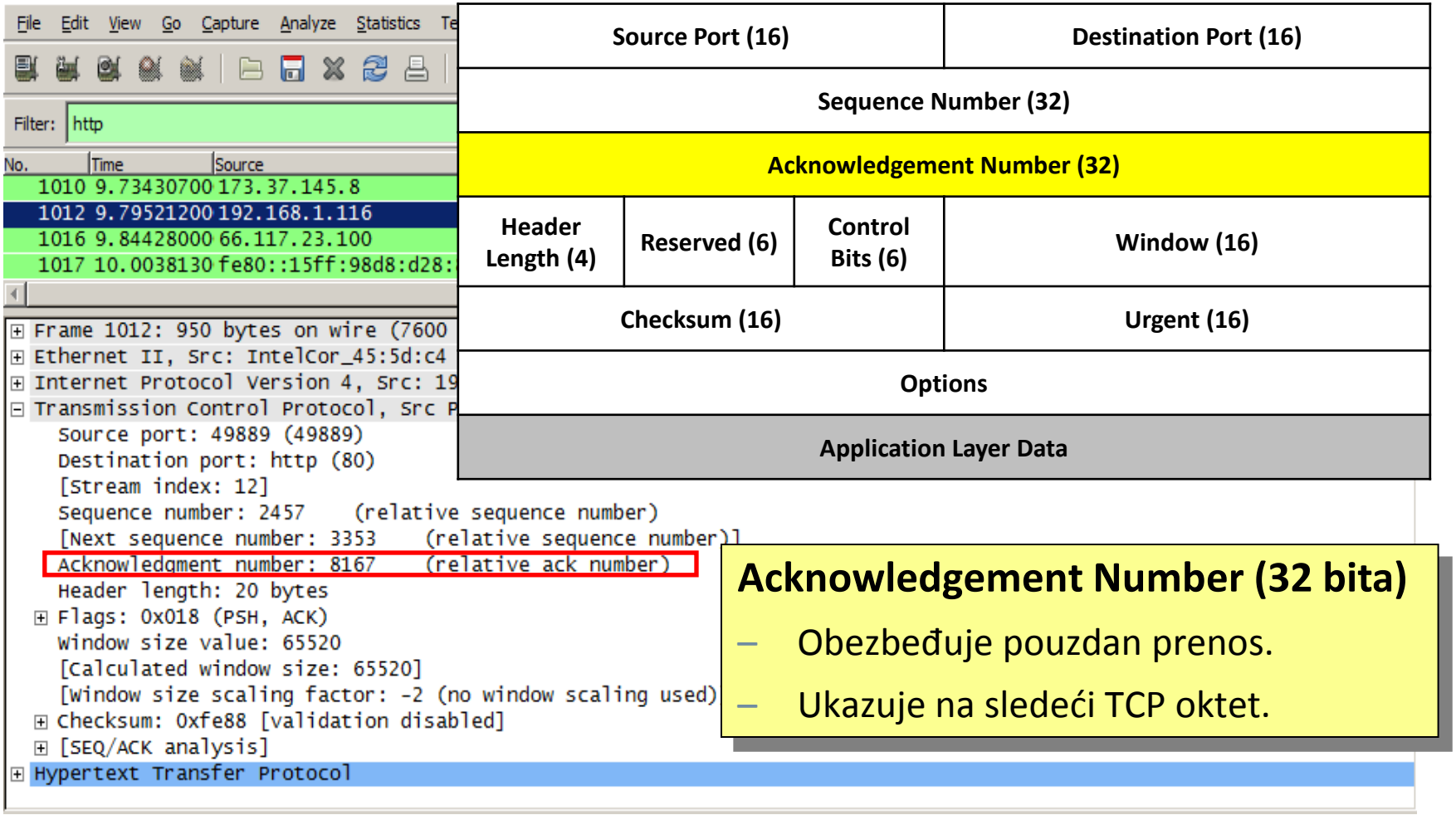




Sequence Number (32 bita)

- Obezbeđuje pouzdanost.
- Numeracija segmenata
- Na osnovu ovog broja odredište zna koji segmenti nedostaju.
- Izvor identifikuje strim segmenata.

TCP SEGMENT U WIRESHARK-U

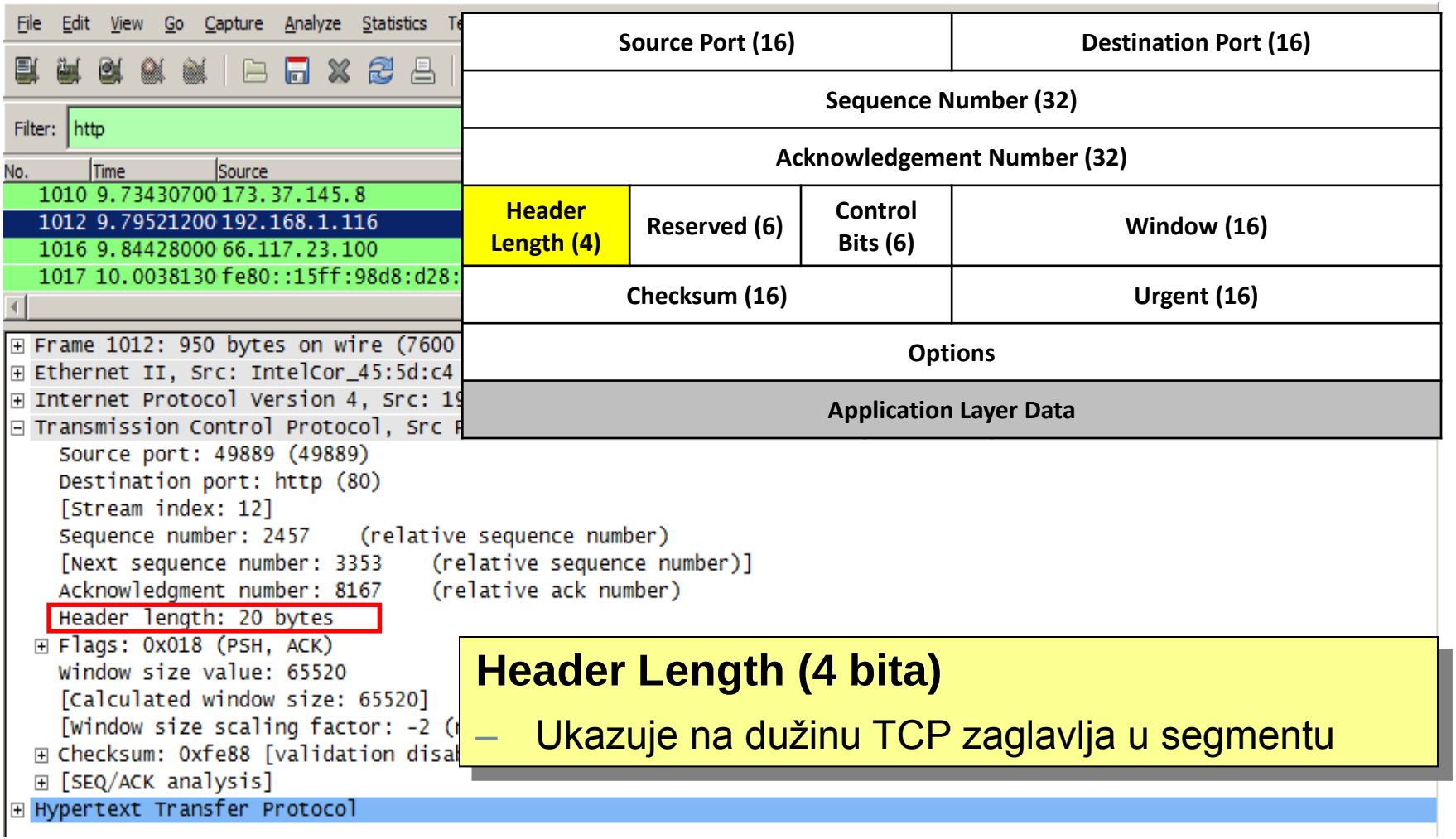


Source Port (16)			Destination Port (16)
Sequence Number (32)			
Acknowledgement Number (32)			
Header Length (4)	Reserved (6)	Control Bits (6)	Window (16)
Checksum (16)			Urgent (16)
Options			
Application Layer Data			

Acknowledgement Number (32 bita)

- Obezbeđuje pouzdan prenos.
- Ukazuje na sledeći TCP oktet.

TCP SEGMENT U WIRESHARK-U

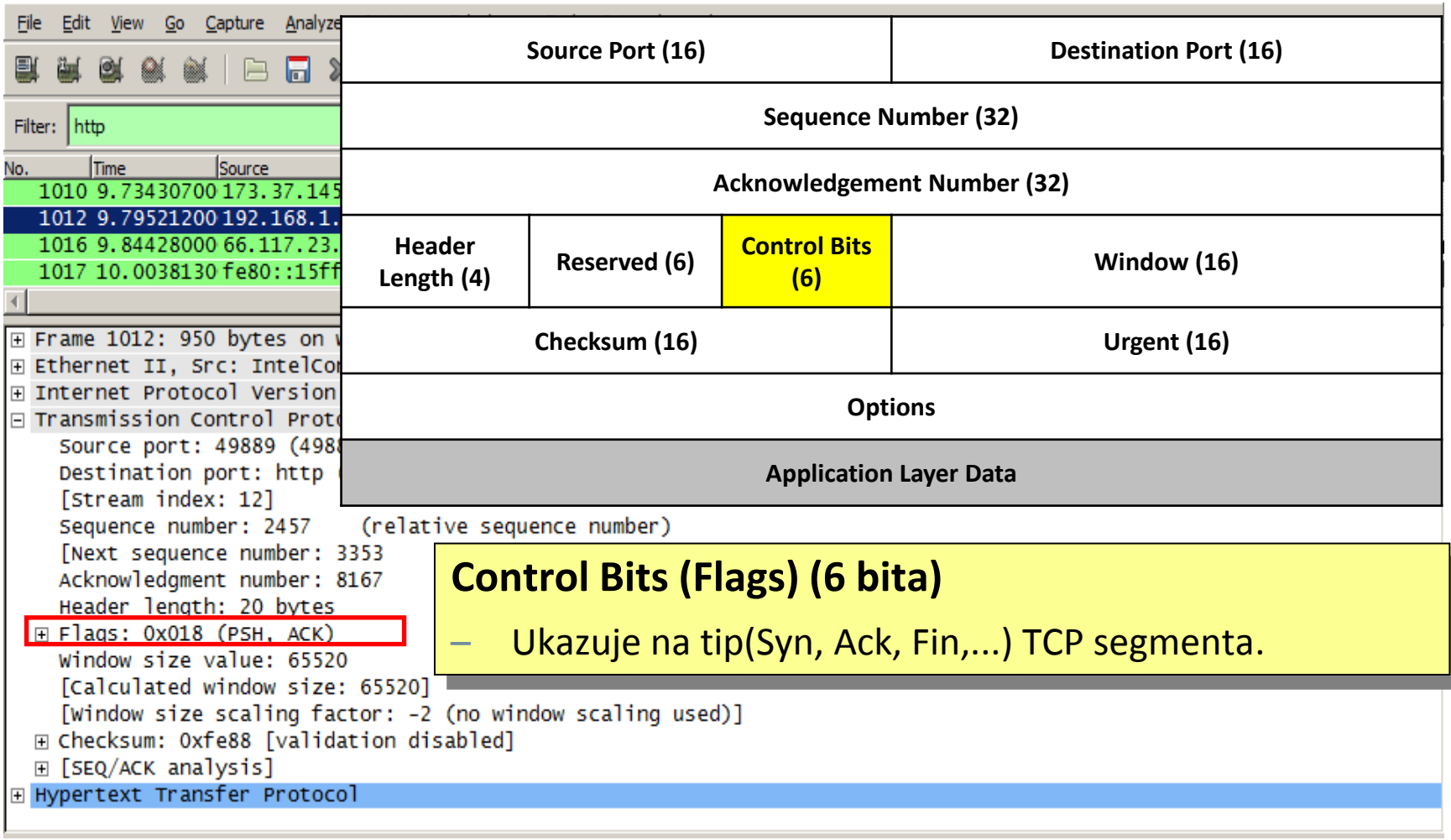


Source Port (16)			Destination Port (16)
Sequence Number (32)			
Acknowledgement Number (32)			
Header Length (4)	Reserved (6)	Control Bits (6)	Window (16)
Checksum (16)			Urgent (16)
Options			
Application Layer Data			

Header Length (4 bita)

- Ukazuje na dužinu TCP zaglavlja u segmentu

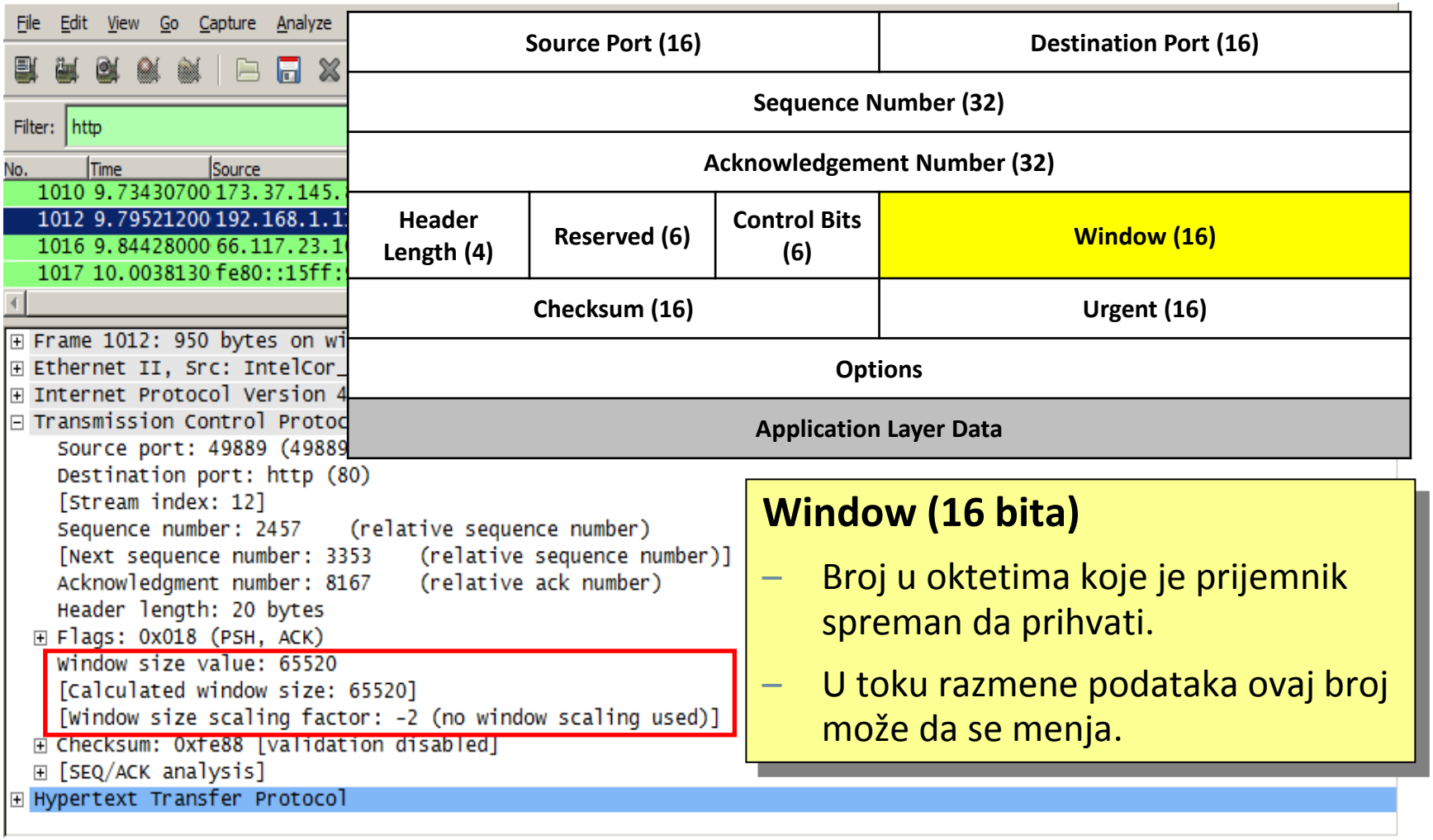
TCP SEGMENT U WIRESHARK-U



Control Bits (Flags) (6 bita)

- Ukazuje na tip(Syn, Ack, Fin,...) TCP segmenta.

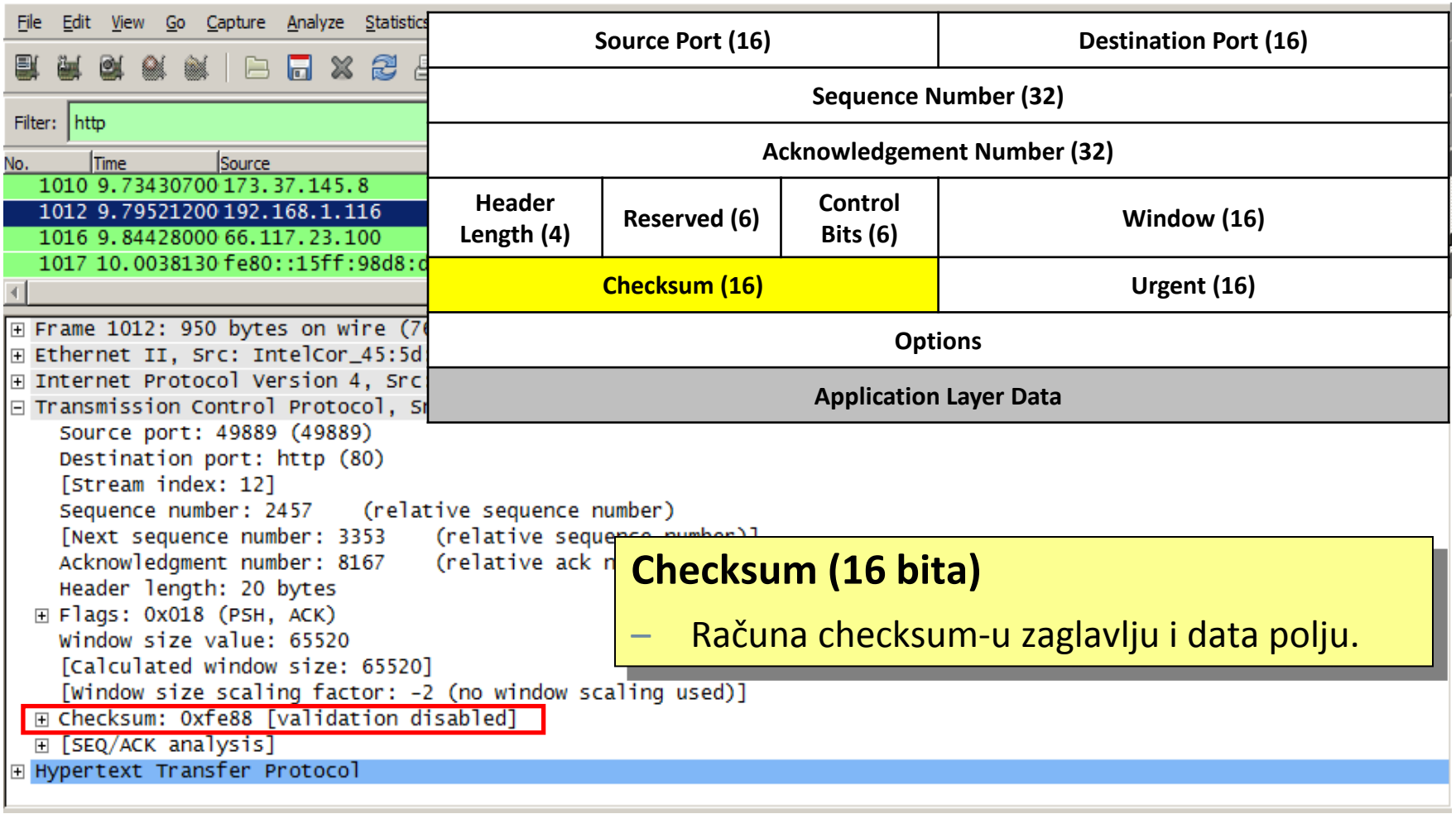
TCP SEGMENT U WIRESHARK-U



Window (16 bita)

- Broj u oktetima koje je prijemnik spreman da prihvati.
- U toku razmene podataka ovaj broj može da se menja.

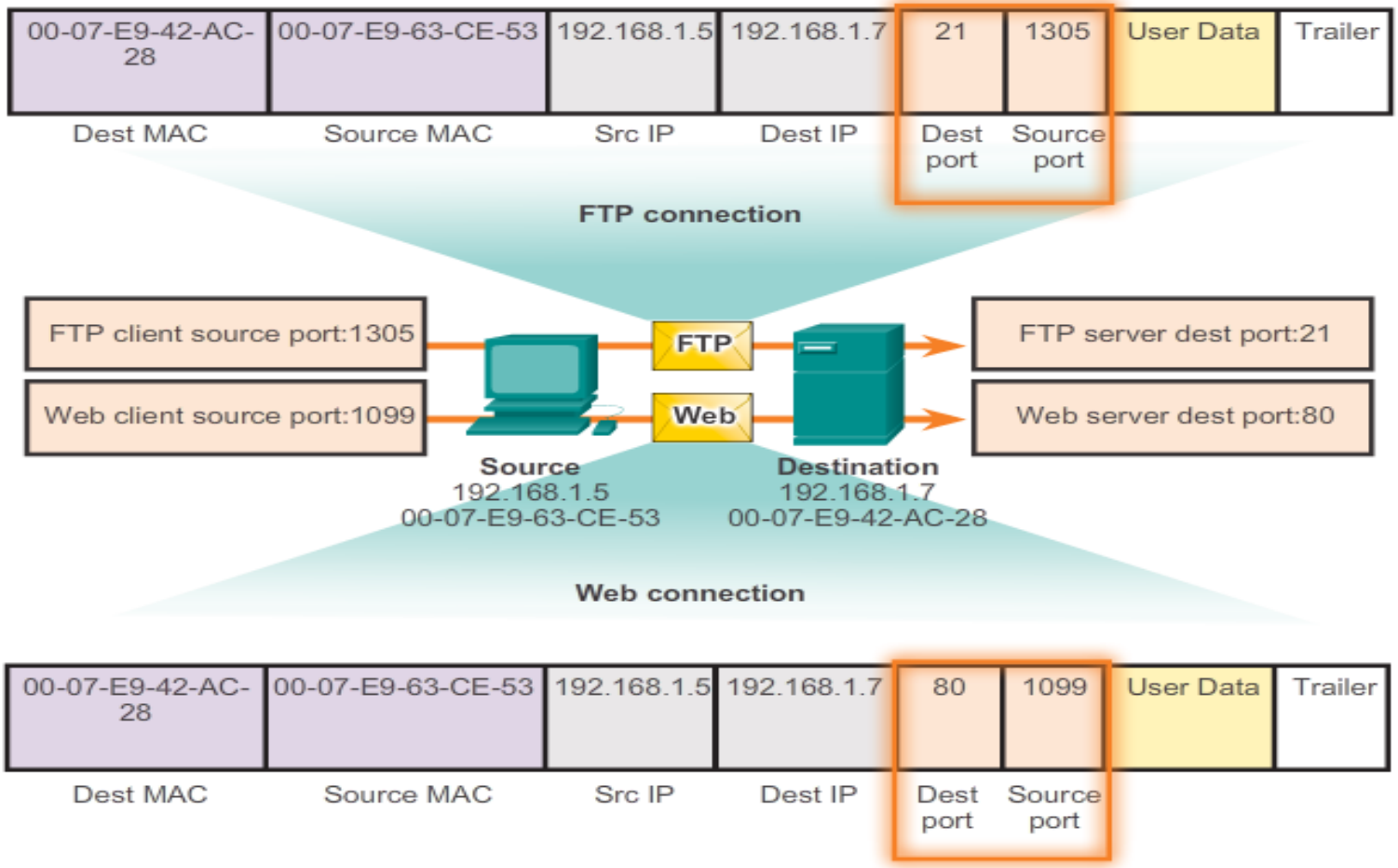
TCP SEGMENT U WIRESHARK-U



Checksum (16 bita)

- Računa checksum-u zaglavlju i data polju.

PORTOVI


00-07-E9-42-AC-28
00-07-E9-63-CE-53
192.168.1.5
192.168.1.7
21
1305
User Data
Trailer
Dest MAC
Source MAC
Src IP
Dest IP
Dest port
Source port
FTP connection
FTP client source port:1305
Web client source port:1099
FTP
Web
FTP server dest port:21
Web server dest port:80
Source
192.168.1.5
00-07-E9-63-CE-53
Destination
192.168.1.7
00-07-E9-42-AC-28
Web connection
00-07-E9-42-AC-28
00-07-E9-63-CE-53
192.168.1.5
192.168.1.7
80
1099
User Data
Trailer
Dest MAC
Source MAC
Src IP
Dest IP
Dest port
Source port

DOBRO POZNATI PORTOVI (WELL KNOWN PORTS)

Port Number Range	Port Group
0 to 1023	Well Known (Contact) Ports
1024 to 49151	Registered Ports
49152 to 65535	Private and/or Dynamic Ports

Well Known TCP Ports

21	FTP
23	Telnet
25	SMTP
80	HTTP
110	POP3
194	Internet Relay Chat (IRC)
443	Secure HTTP (HTTPS)

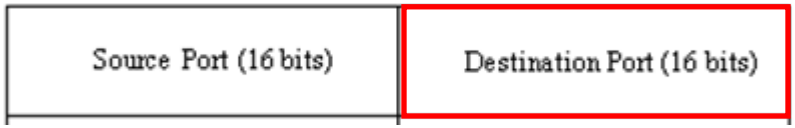
Well Known UDP Ports:

69	TFTP
520	RIP

Well Known TCP/UDP Common Ports:

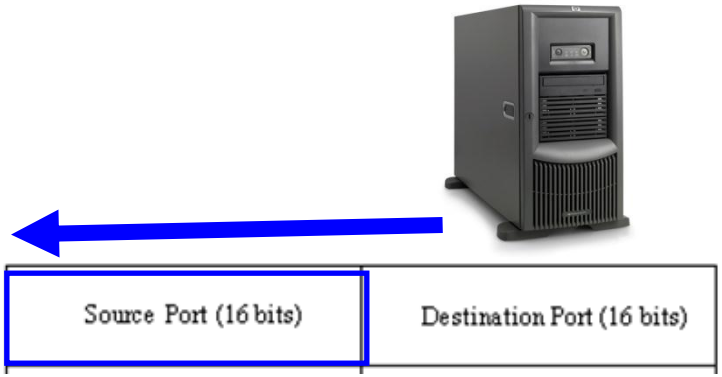
53	DNS
161	SNMP
531	AOL Instant Messenger, IRC

Well Known ili Registered Port Number

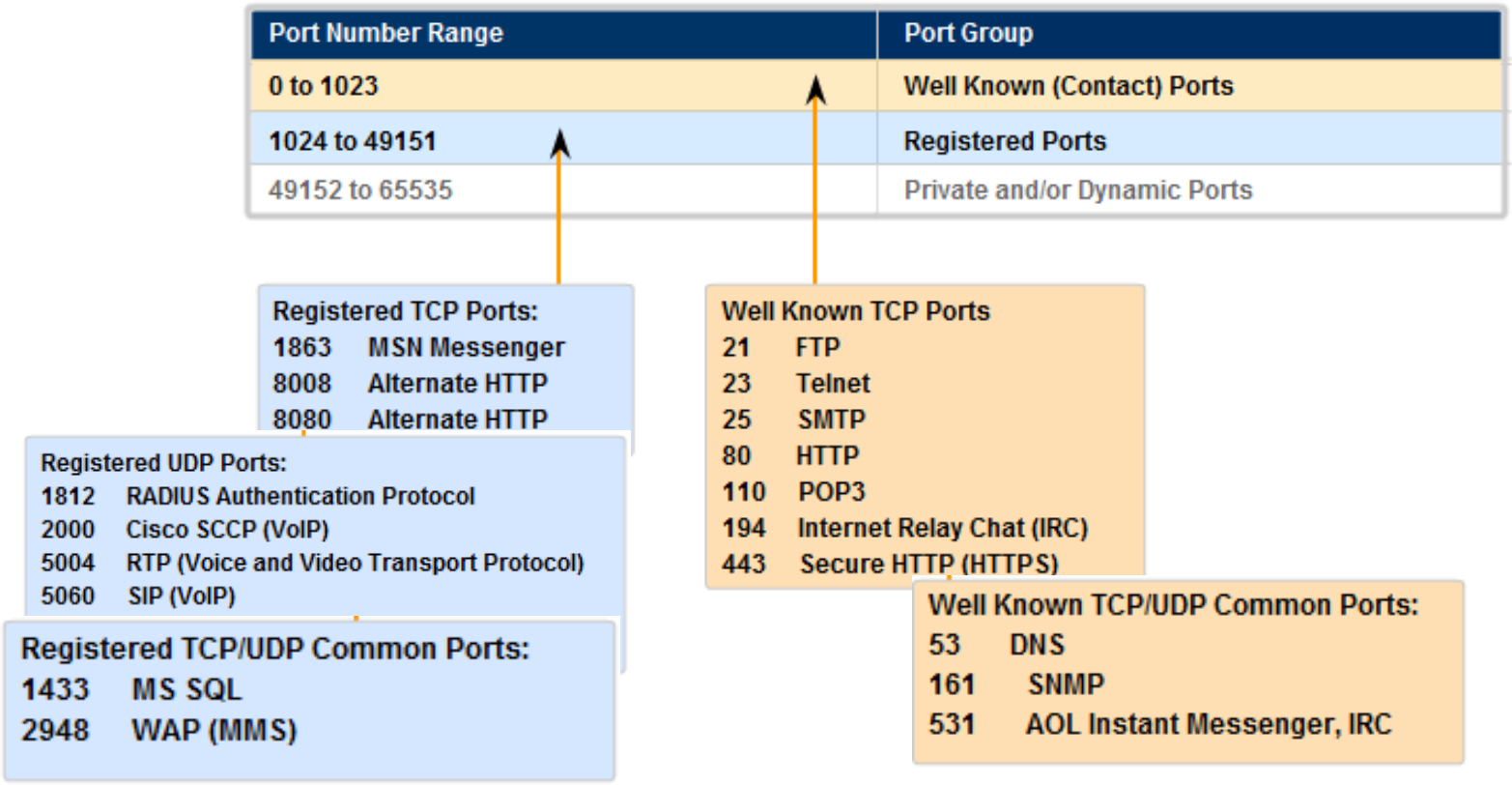


Well Known Ports (Brojevi od 0 do 1023)

- Reservisani su za najpoznatije mrežne servise
- **Klient**: TCP destination port
- **Server**: TCP source port



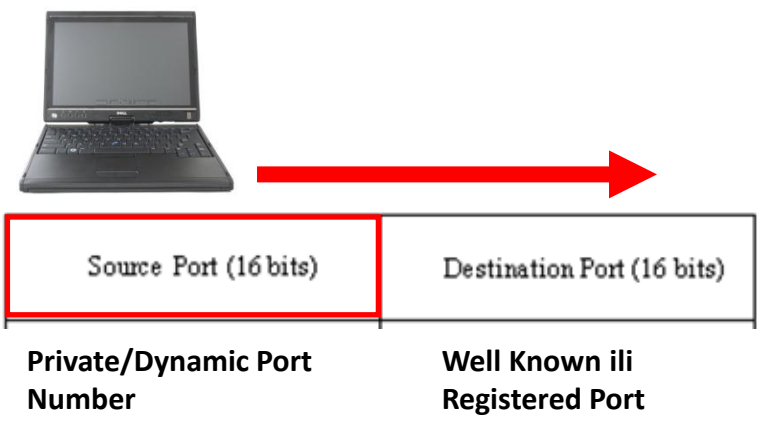
REGISTROVANI PORTOVI

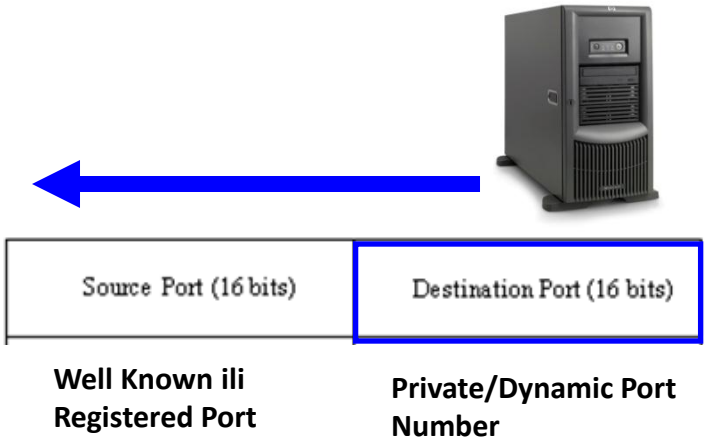


- **Registrovani Portovi (Brojevi od 1024 do 49151)**
  - Zadaju se aplikacijama ili korisničkim procesima.
  - Reč je o aplikacijama privatnih kompanija

DODELA PORTA

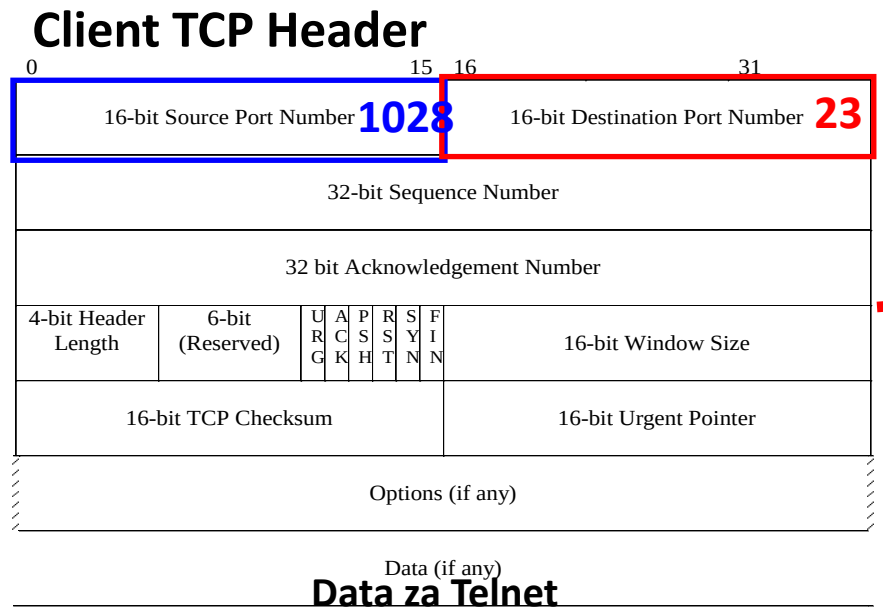
Port Number Range	Port Group
0 to 1023	Well Known (Contact) Ports
1024 to 49151	Registered Ports
49152 to 65535	Private and/or Dynamic Ports





- **Dynamic ili Private Ports (Brojevi od 49152 do 65535)**
  - Obično se dinamički zadaju klijentskim aplikacijama
    - **Client**: TCP source port **Server**: TCP destination port
  - Može da uključi opseg Registered Ports (Brojevi od 1024 do 49151)

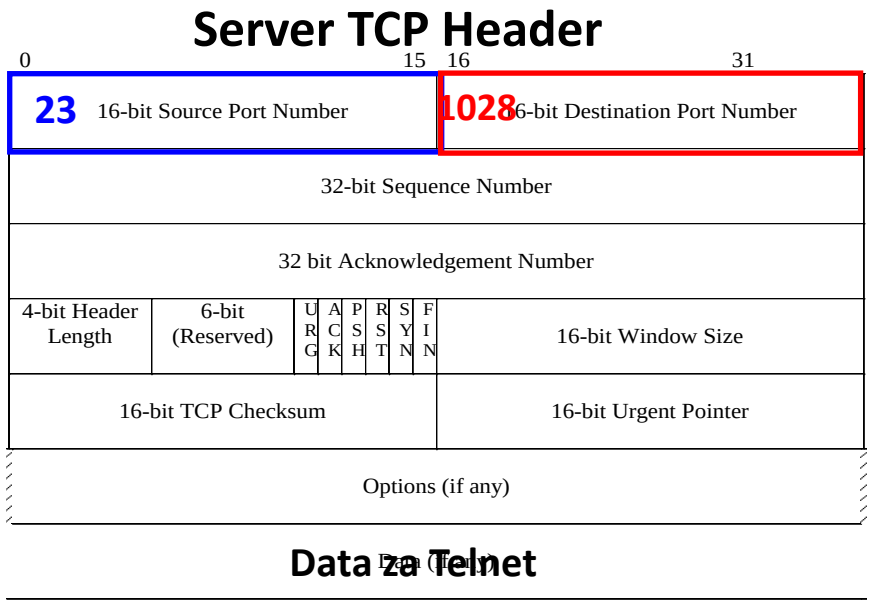
PRIMER DODELE PORTA APLIKACIJI



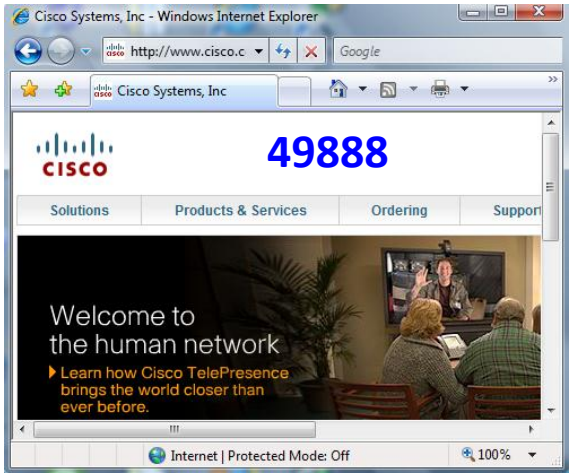
- Klijent šalje TCP segment:
  - Destination Port: 23 (Well known port)
  - Source Port: 1028 (Dynamic Port koji zadaje klijent)

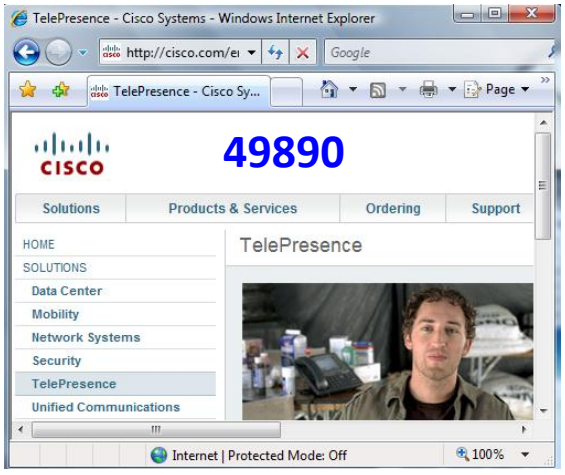
PRIMER DODELE PORTA APLIKACIJI

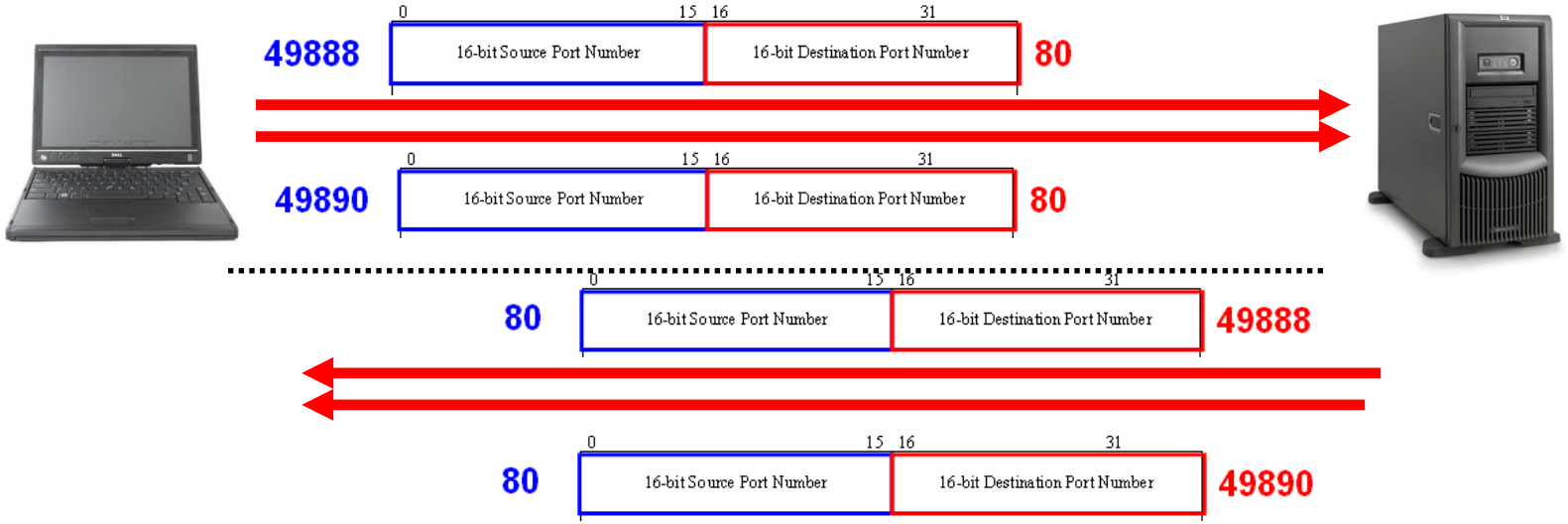
- Server šalje TCP segment:
  - Destination Port: 1028 (Well known port)
  - Source Port: 23 (Dynamic Port koji zadaje klijent)



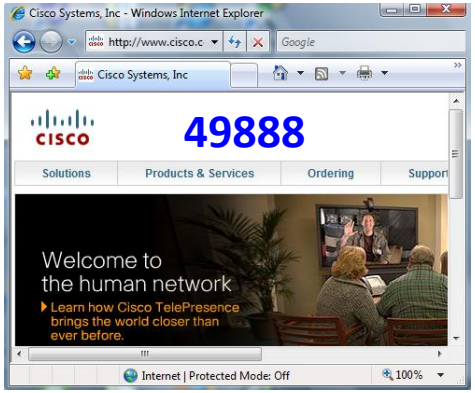
USPOSTAVLJANJE VIŠE SESIJA

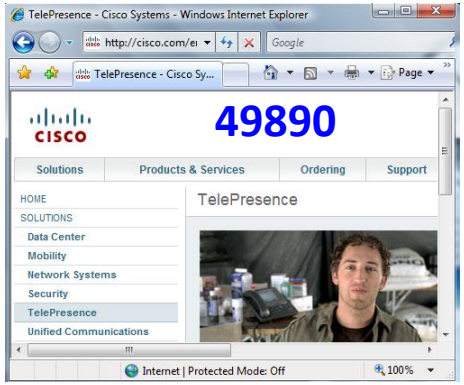


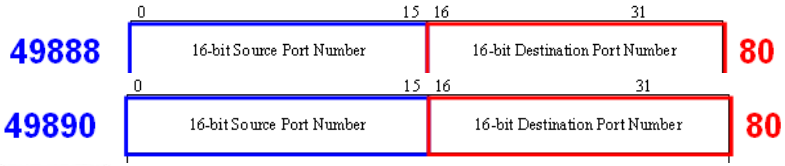




USPOSTAVLJANJE VIŠE SESIJA







```
C:\Users\Dusan>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.101:49888    198.133.219.25:80      TIME_WAIT
  TCP    192.168.1.101:49890    198.133.219.25:80      TIME_WAIT
```

Source Port

Destination Port

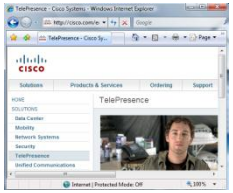
Connection State

Source IP

Destination IP

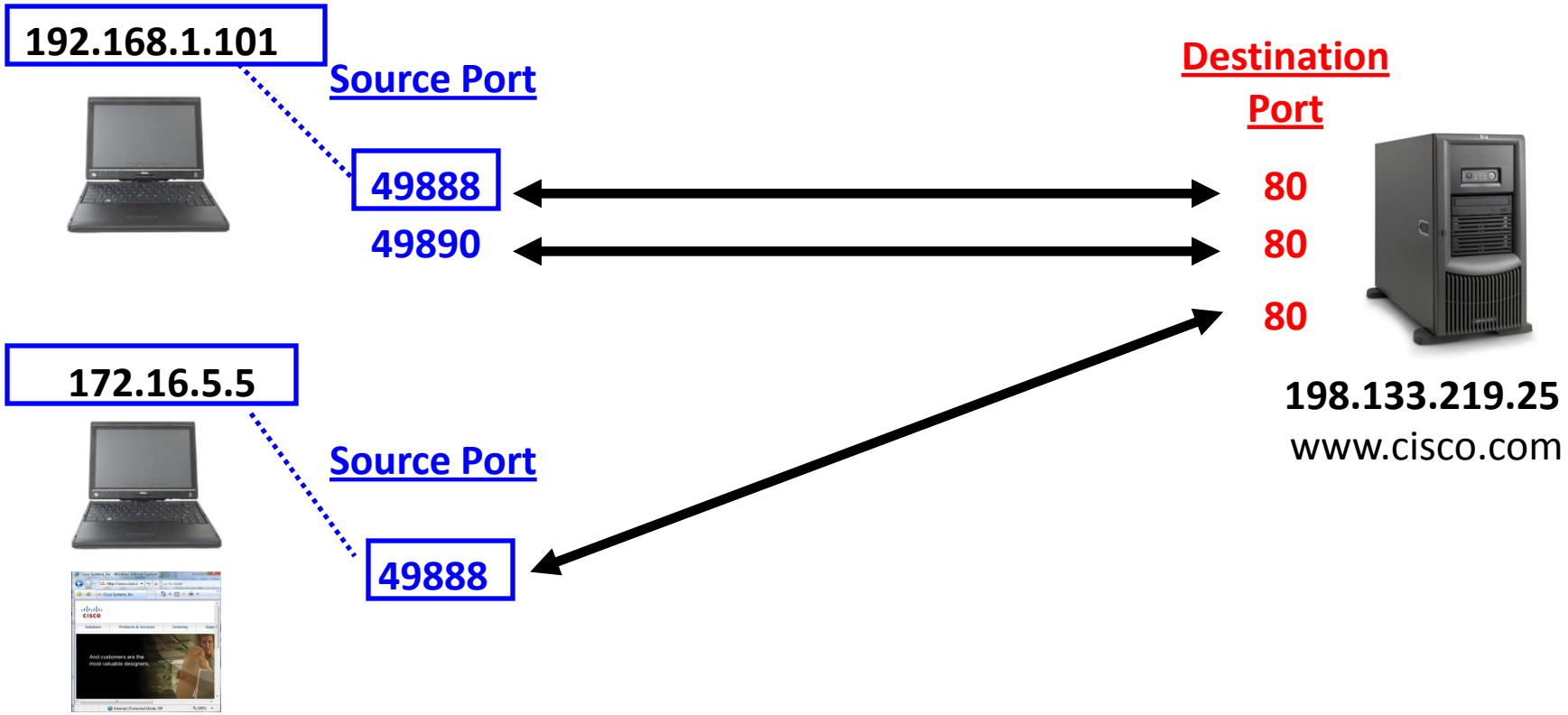
TCP
ili
UDP

SOCKET

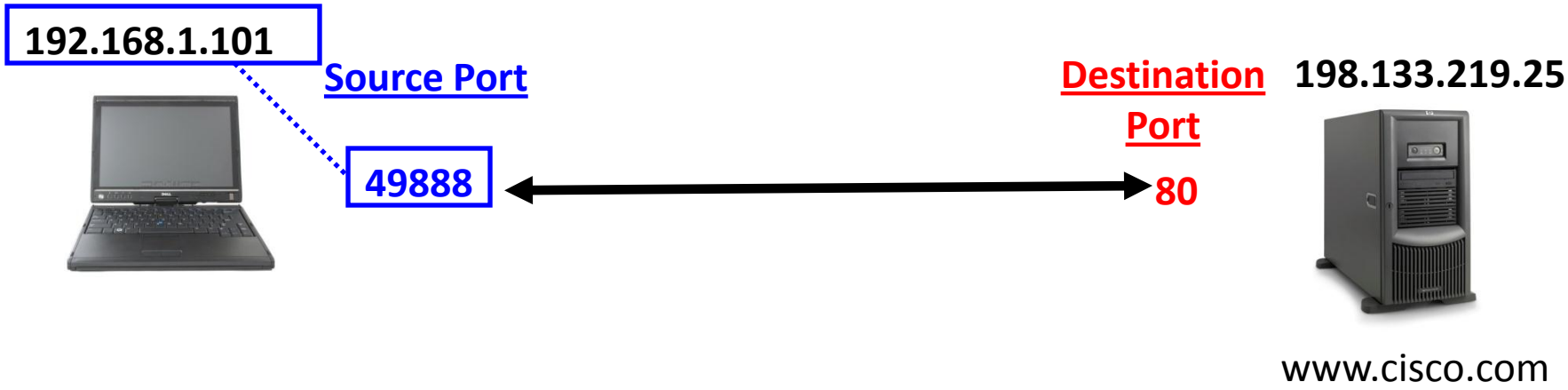


Šta obezbeđuje da svaka konekcija bude jedinstvena?

- Konekciju definišu sledeći parovi:
  - **Source IP address**, **Source port** (Klijent - Server)
  - **Destination IP address**, **Destination port** (Server – Klijent)

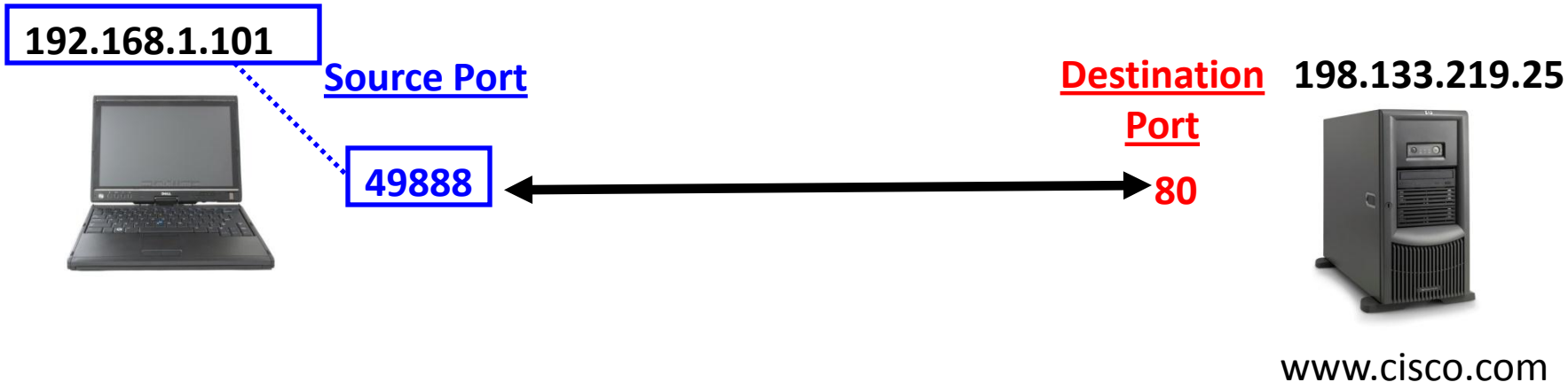


SOCKET



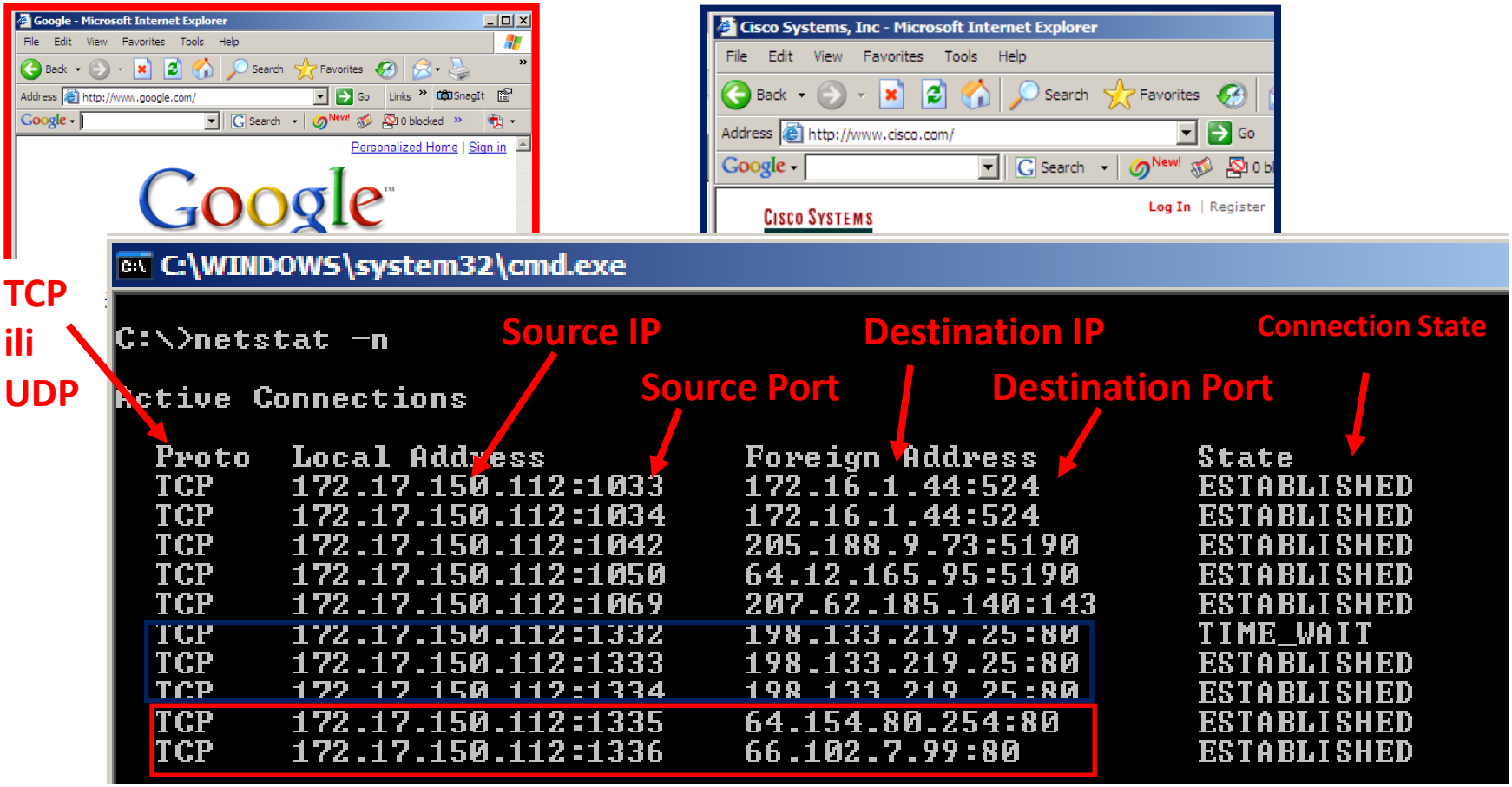
- Kombinovanjem broja porta na transportnom sloju i IP adrese na mrežnom sloju se na jedinstven način identifikuje aplikacija koja se izvršava
  - Kombinacija IP adrese i broja porta zove se **socket**.
- Komunikacija(flow) između dve aplikacije se na jedinstven način identifikuje koristeći izvornu i odredišnu IP adresu i brojeve porta zove se **socket pair**.

SOCKET



- Socket na klijentskoj strani uključuje izvorišnu IP adresu i izvorišni broj porta
  - 192.168.1.101:49888
- Socket na Web serveru uključuje odredišnu IP adresu i odredišni broj port:
  - 192.133.219.25:80
- Kombinacija ova dva socket-a zove se socket pair:
  - 192.168.1.101:49888, 192.133.219.25:80

PRIKAZ KONEKCIJA NA RAČUNARU



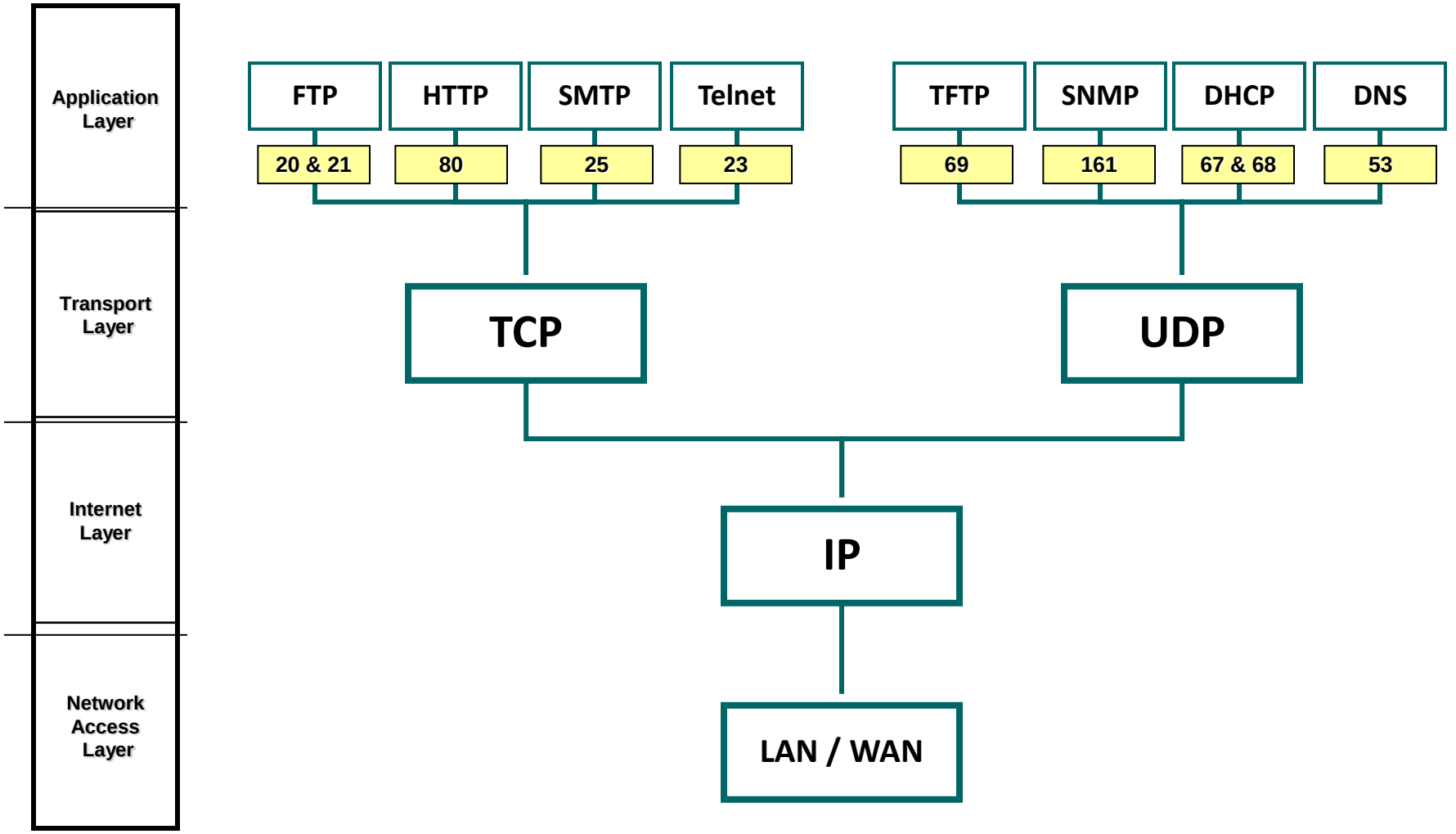
- **Napomena:** Kada učitavamo web stranu i njene objekte obično se uspostavljaju nekoliko TCP sesije.

DOBRO POZNATI PORTOVI

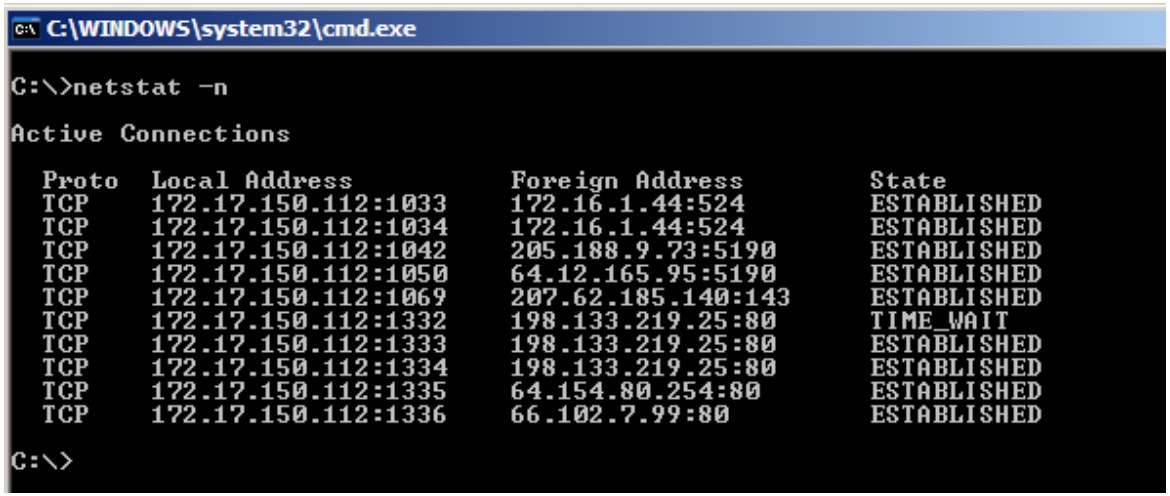
- Hypertext Transfer Protocol (HTTP) - TCP Port **80**
- HTTP Secure (HTTPs) - TCP Port **443**
- Simple Mail Transfer Protocol (SMTP) - TCP Port **25**
- Post Office Protocol (POP) - TCP Port **110**
- Telnet - TCP Port **23**
- File Transfer Protocol (FTP) - TCP Ports **20** & **21**
- Trivial FTP (TFTP) - UDP **69**
- Domain Name System (DNS) - TCP/UDP Port **53**
- Dynamic Host Configuration Protocol (DHCP) - UDP Port **67 & 68**

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

TRANSPORTNI SLOJ



NADGLEDANJE KONEKCIJA



- Ne identifikovane TCP konekcije mogu da izazovu bezbedonosni problem jer mogu da označe da je neko konektovan na vaš računar.
- Nepotrebne TCP konekcije mogu da izazovu prilično korišćenje sistemskih resursa što dovodi do pada performansi hosta.
- **`Netstat`** se koristi da proverimo koje su otvorene sesije kada primetimo da su nam performanse narušene.
  - Netstat Security Podcast
  - TCPView