TCP/IP Arhitektura

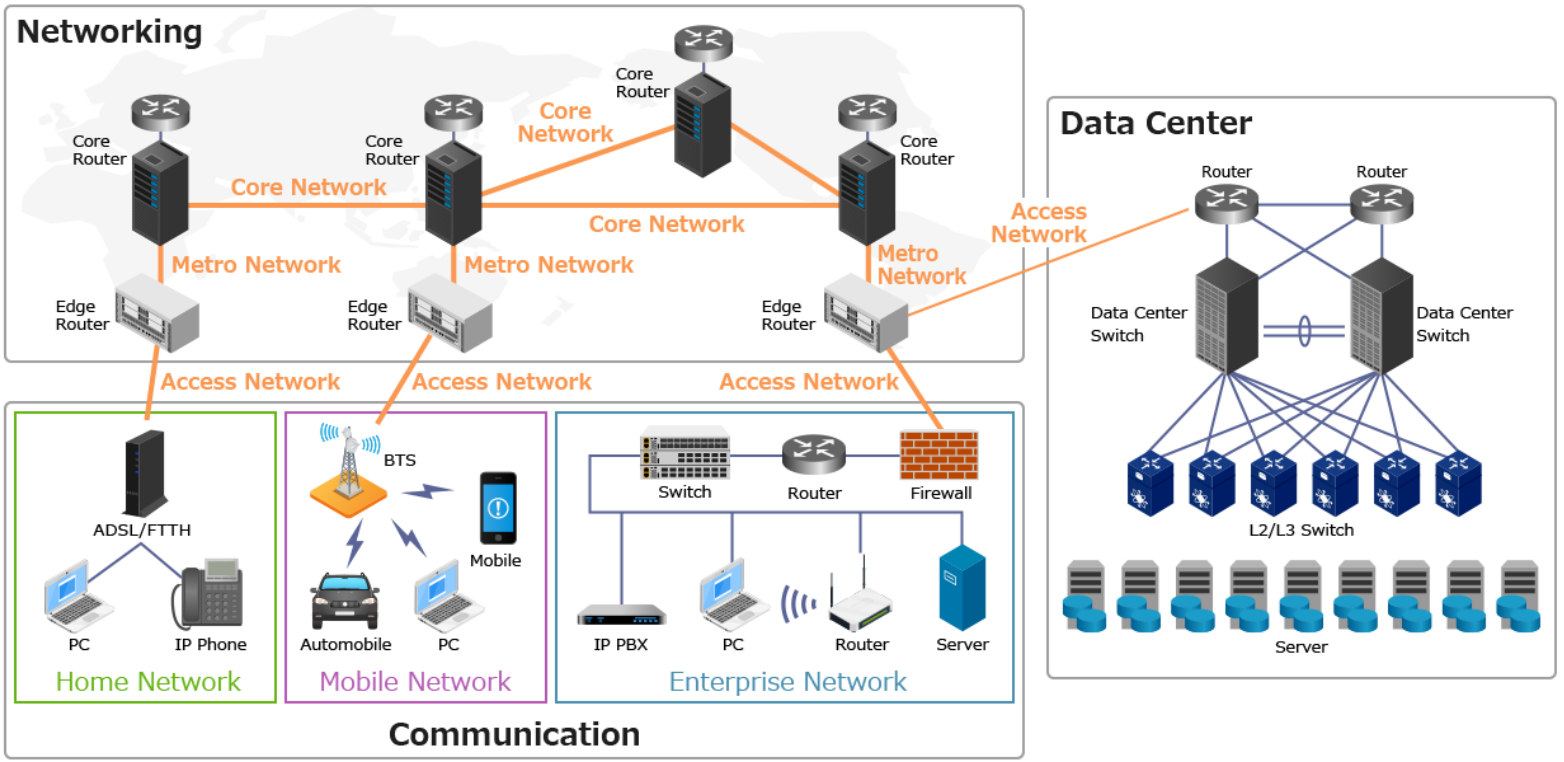
Predmet: Bezbednost Aplikacija

Predavač: dr Dušan Stefanović

Mrežna infrastruktura

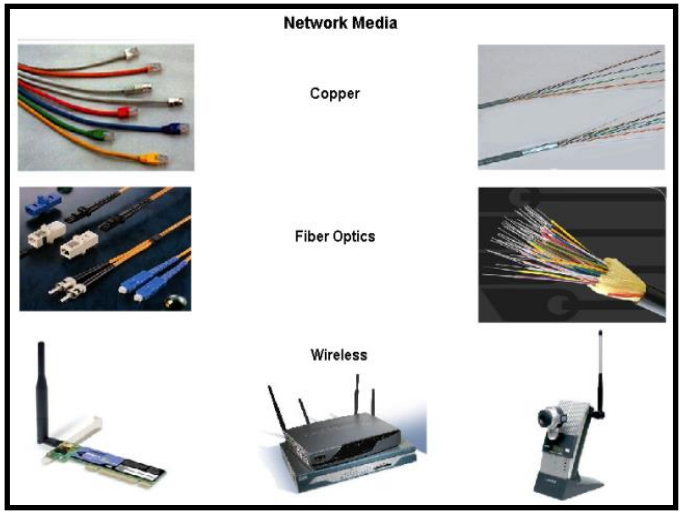
Mrežnu infrastrukturu čine:

- Uređaji
- Medijum
- Servisi

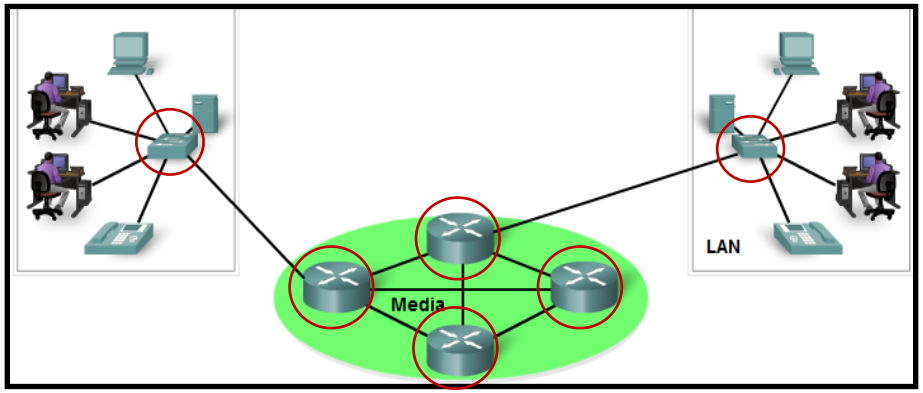


Komponente mrežne infrastrukture

Krajnji uređaji



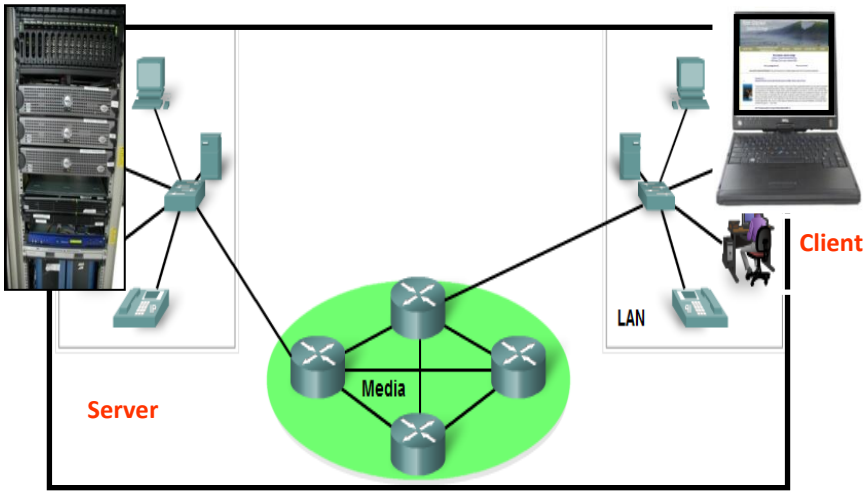
Prenosni medijumi

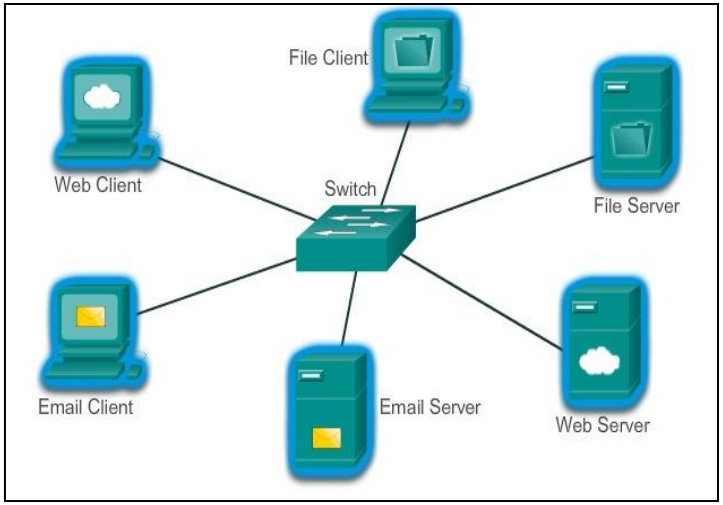


Aktivni mrežni uređaji

Server – Klijent Komunikacija

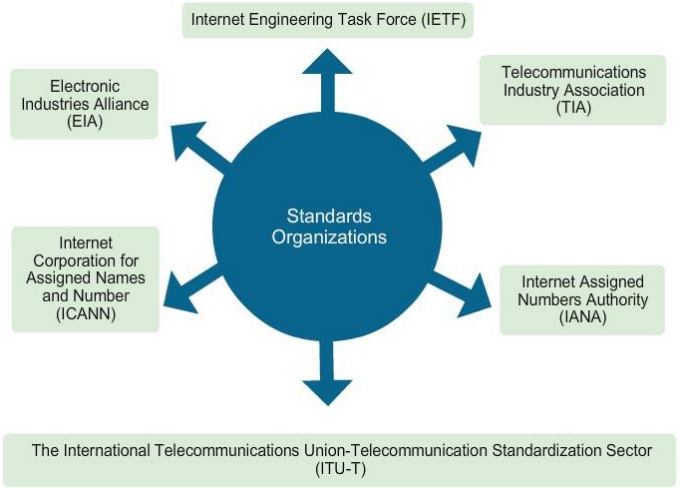
- Termin *HOST* odnosi se na: Klijent, Server ili oba.
- Softver određuje ulogu hosta.
- Server obezbeđuje uslugu klijentu: e-mail ili web stranicu
- Klijent zahteva informaciju od servera



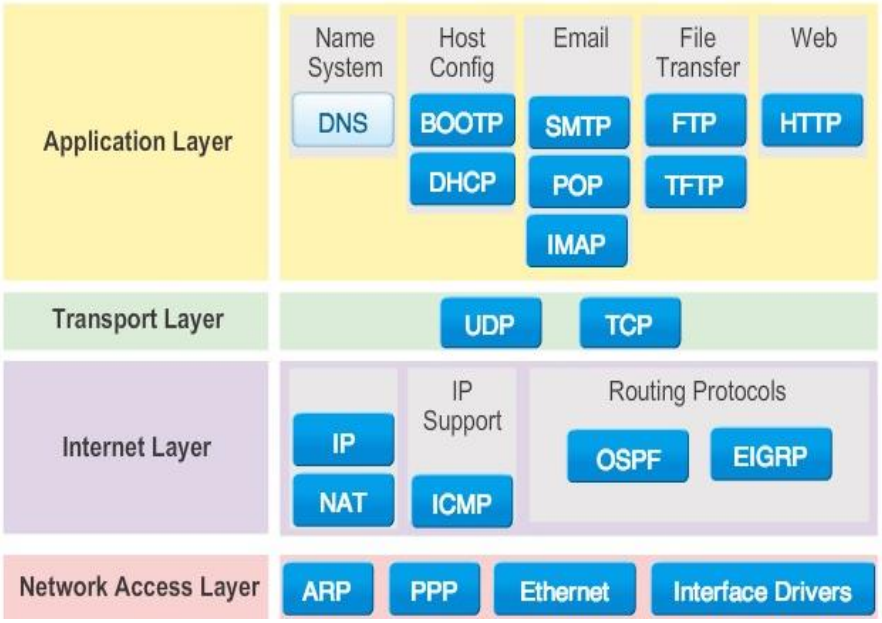


ORGANIZACIJE ZA STANDARDIZACIJU

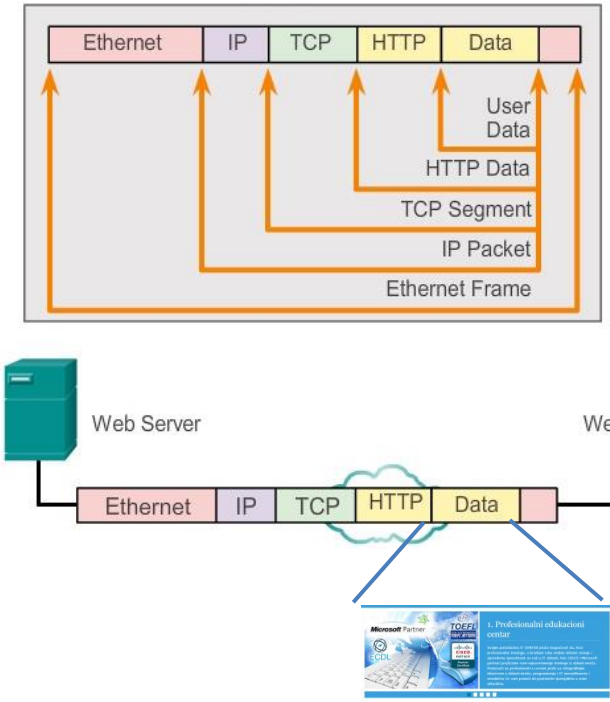
- Industrijski standard sprečava monopol jedne kompanije
- Ohrabruje i ubrzava razvoj tehnologije
- Organizacije za standardizaciju su:
  - The Internet Society (ISOC)
  - The Internet Architecture Board (IAB)
  - The Internet Engineering Task Force (IETF)
  - The Institute of Electrical and Electronics Engineers (IEEE)
  - The International Organization for Standardization (ISO)



TCP/IP PROTOKOLSKI STEK

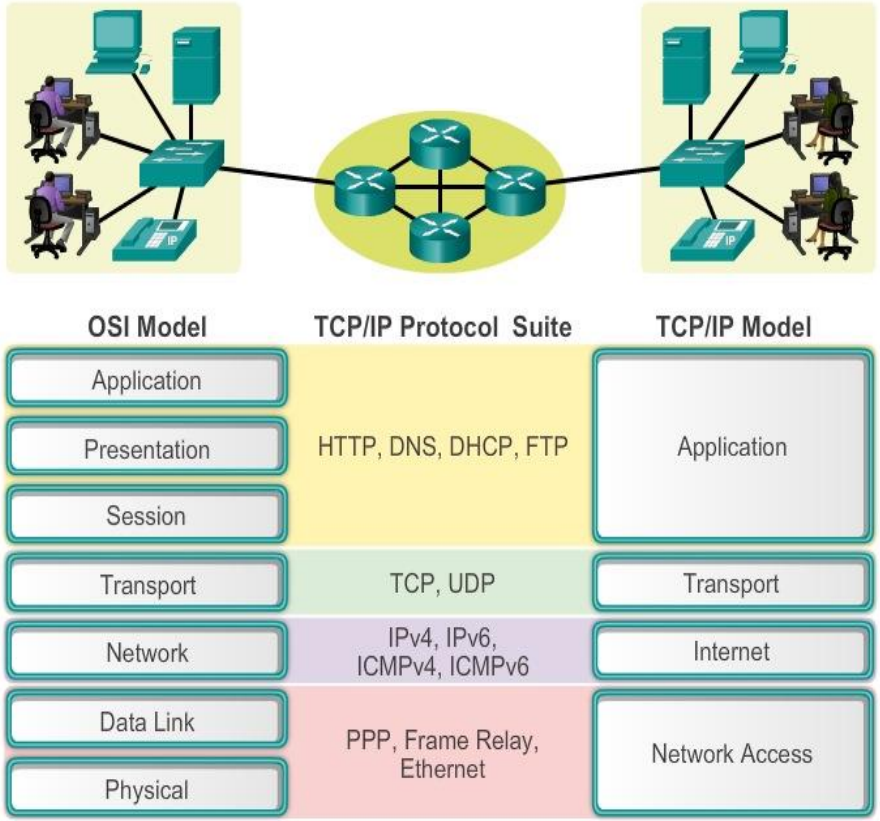


ENKAPSULACIJA PROTOKOLA

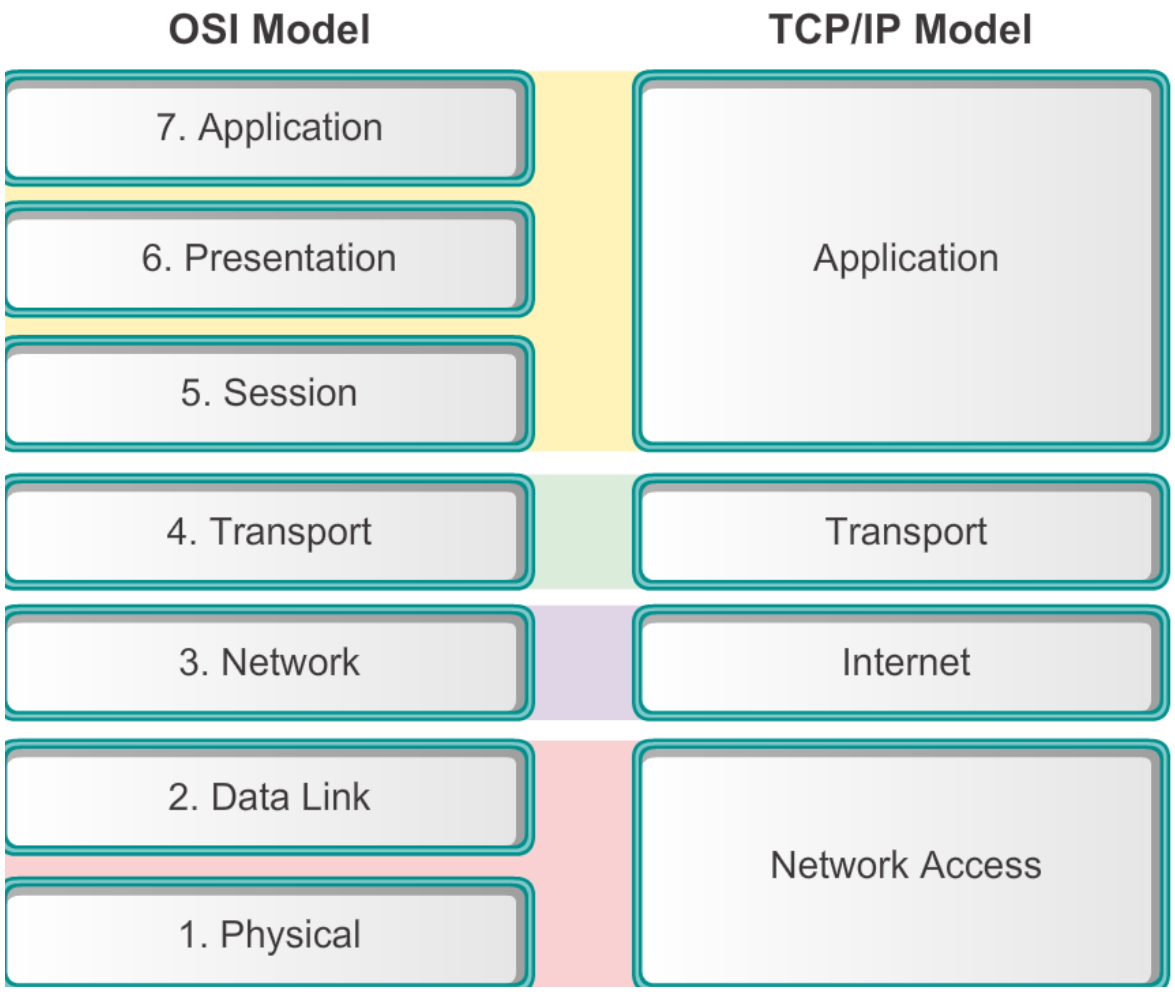


SLOJEVI U MREŽNOM MODELU

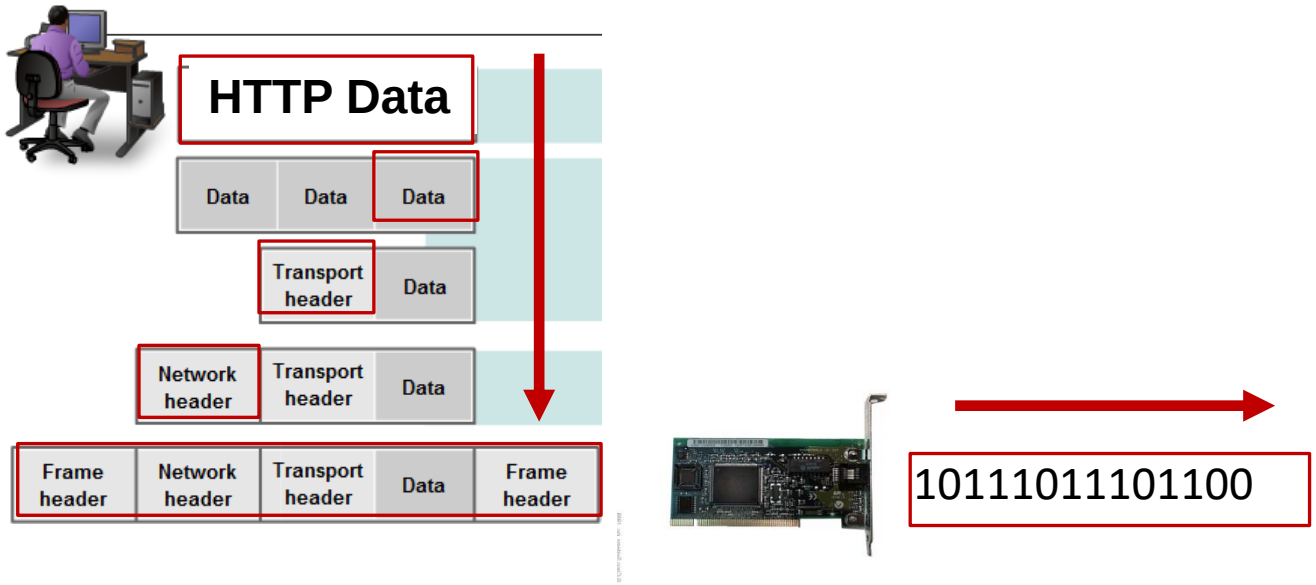
- Slojevita struktura mrežnog modela omogućava da se složen proces razloži na manje delove
- Na svakom sloju su definisani precizni zadaci
- Svaki sloj obezbeđuje uslugu nivou iznad njega
- Promena tehnologije na jednom sloju neće uticati na ostale slojeve
- Implementacija novih servisa i tehnologije je skalabilna tj. lako se može nadograditi
- Rešavanje problema je znatno olakšano kod ovakvih modela



KOMPARACIJA OSI/TCP-IP MREŽNIH MODELA



ENKAPSULACIJA PORUKE



DENKAPSULACIJA PORUKE

Data Link Header	IP Header	TCP Header	HTTP Header	Data 	Data Link Trailer

HTTP Data

Data	Data	Data

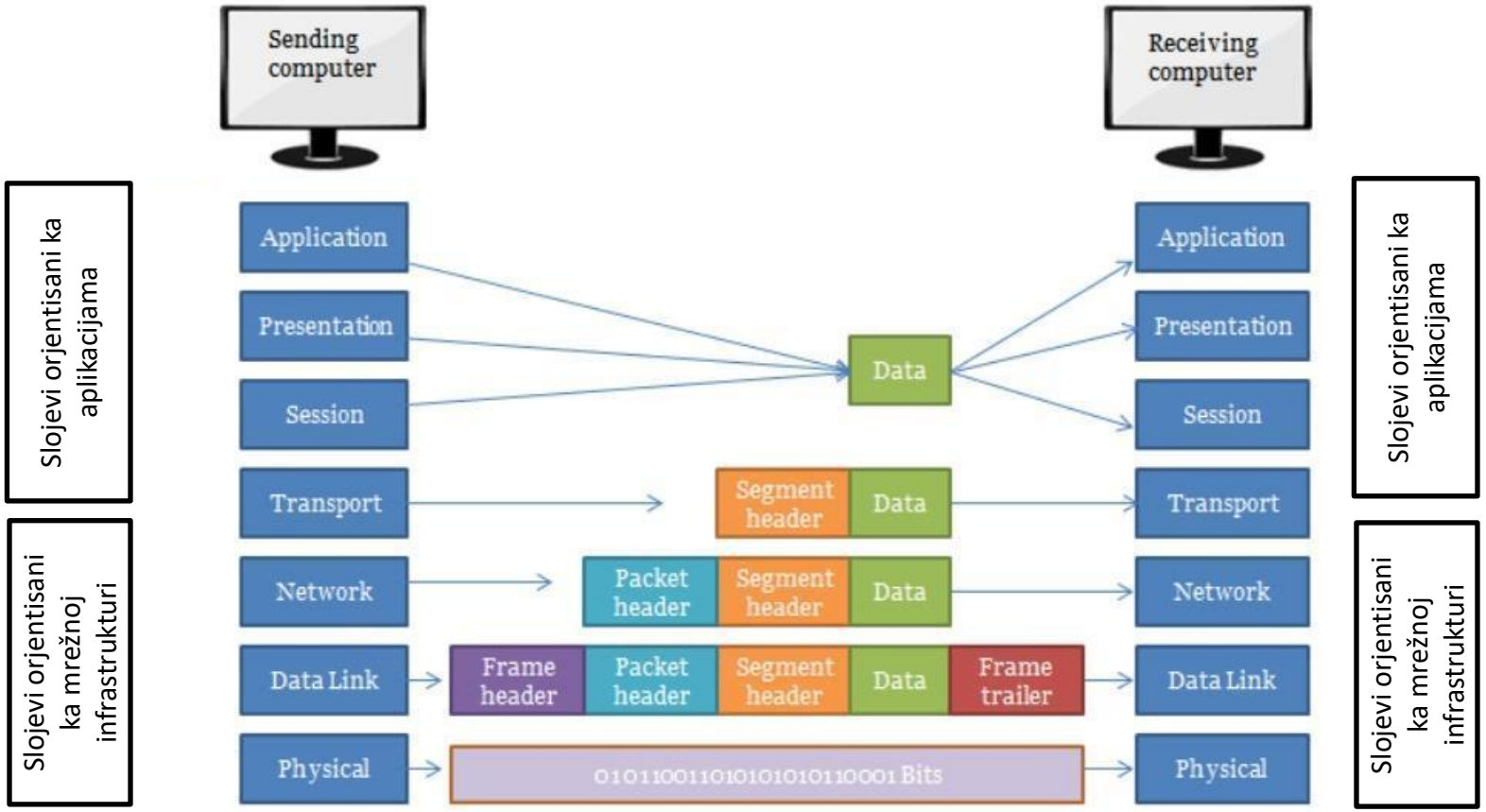
Transport header	Data

Network header	Transport header	Data

Frame header	Network header	Transport header	Data	Frame header

10111011101100

SLOJEVI TCP/IP MODELA ORJENTISANI KA APLIKACIJAMA

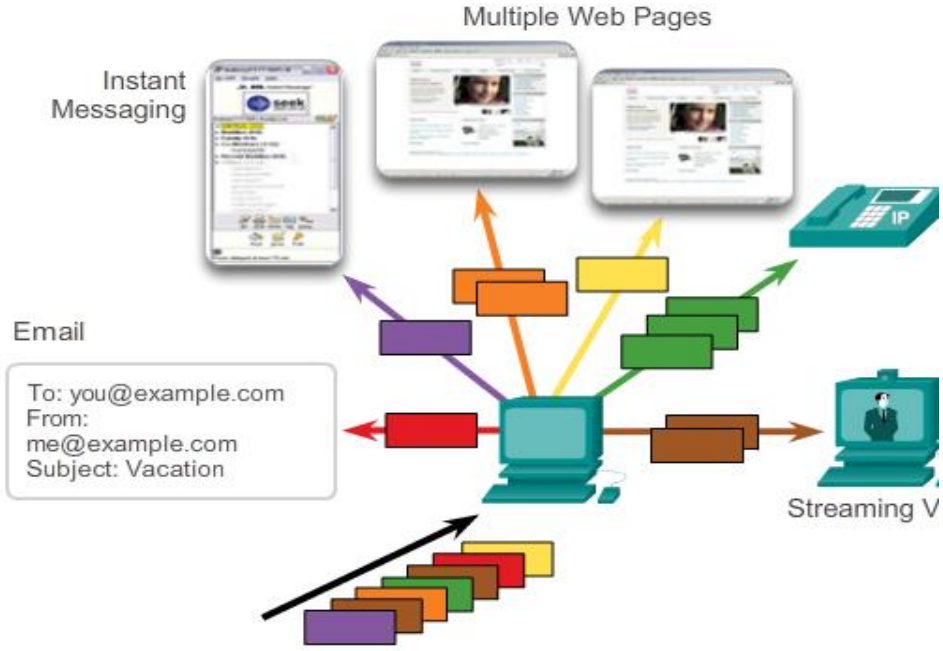


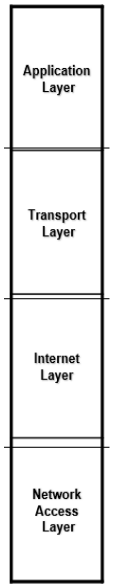
ULOGA PORTA - TRANSPORTNI SLOJ

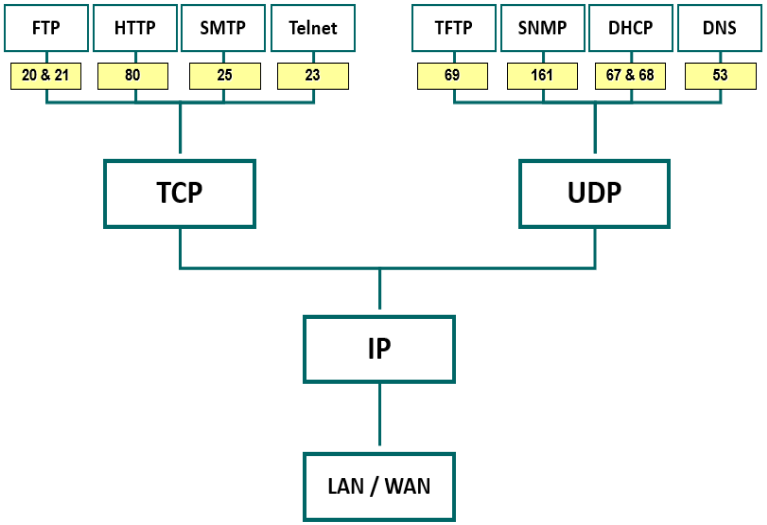
Svaki host u mreži može istovremeno da pokrene više aplikacija

Zadatak transportnog sloja je da upravlja ovim sesijama između izvorišnog i odredišnog računara

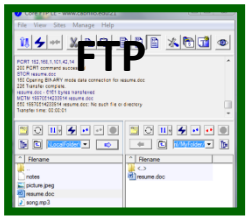
Jedan klijent može da uspostavi više istovremenih konekcija sa različitim serverima







ULOGA PORTA - 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

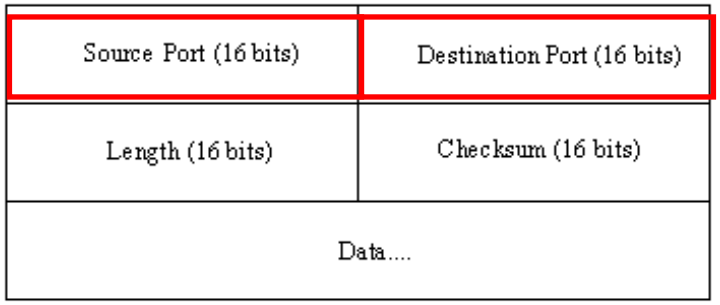
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical

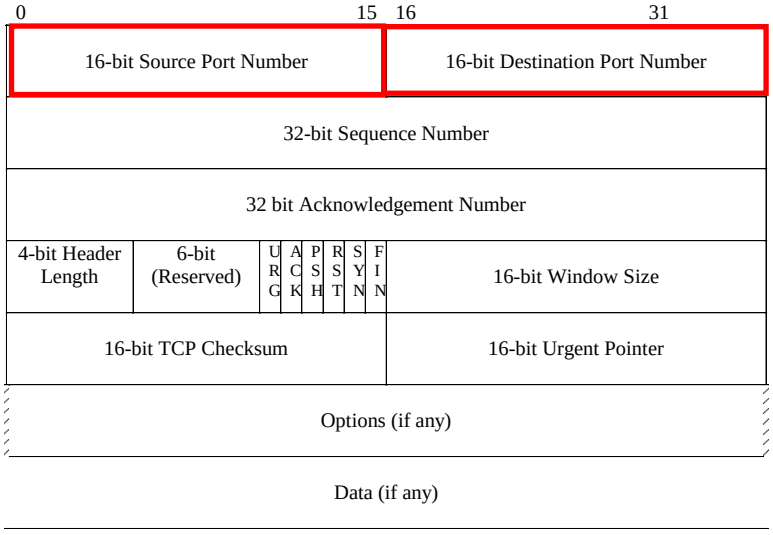
ISP Email i FTP Server

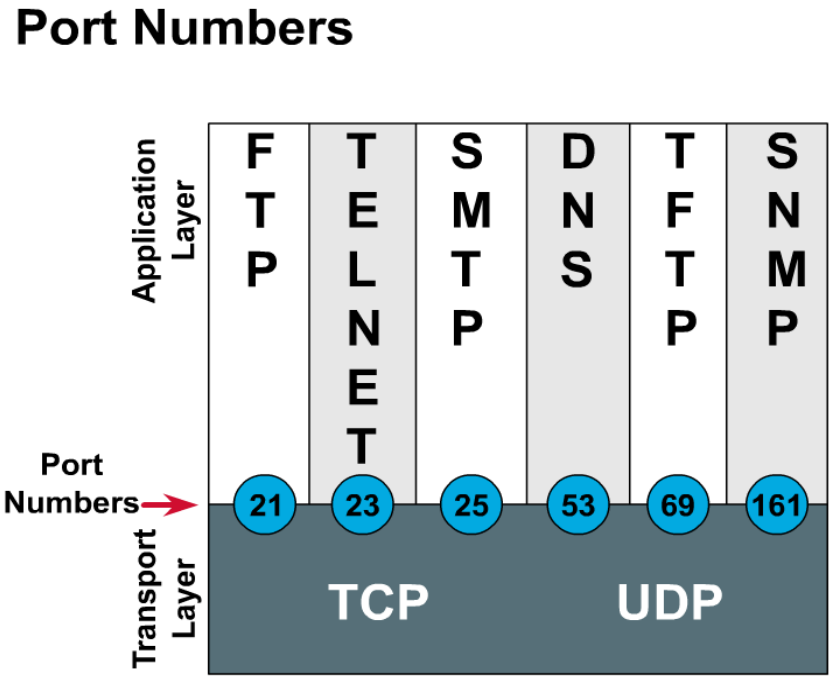
IDENTIFIKACIJA APLIKACIJE – TRANSPORTNI SLOJ

Transportni sloj zadaje svakoj aplikaciji identifikator koji se zove port.

Na osnovu broja porta transportni sloj identifikuje svaku aplikaciju.



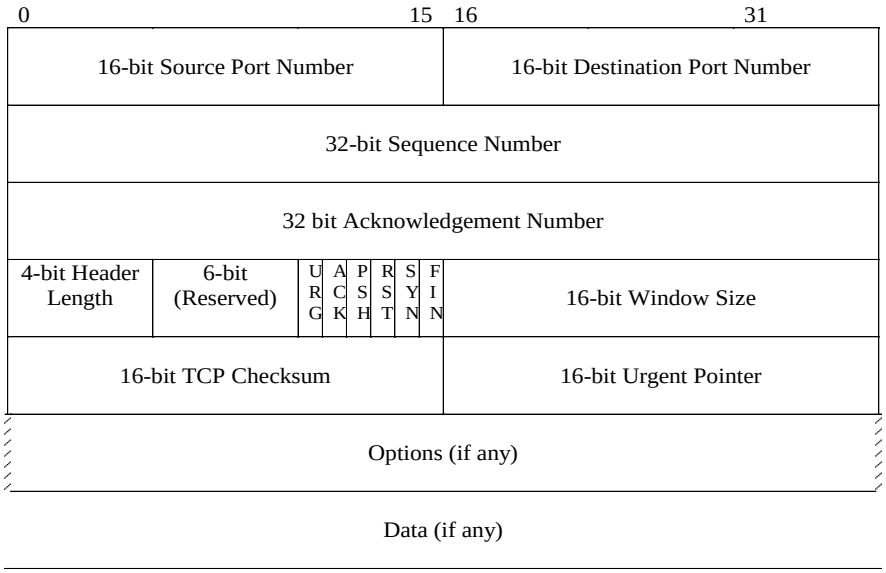




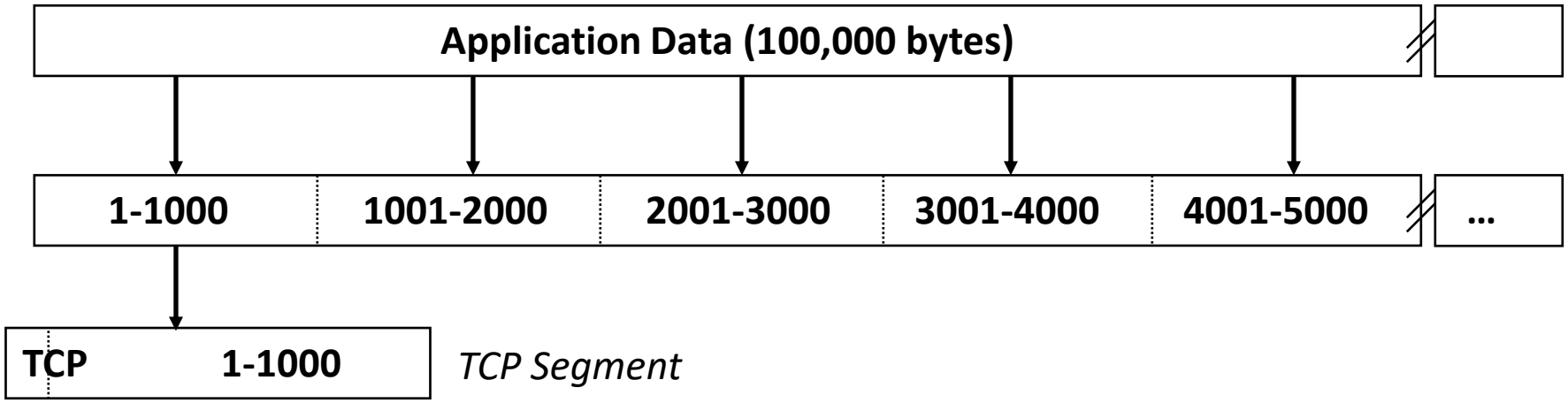
TCP SERVISI

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**)

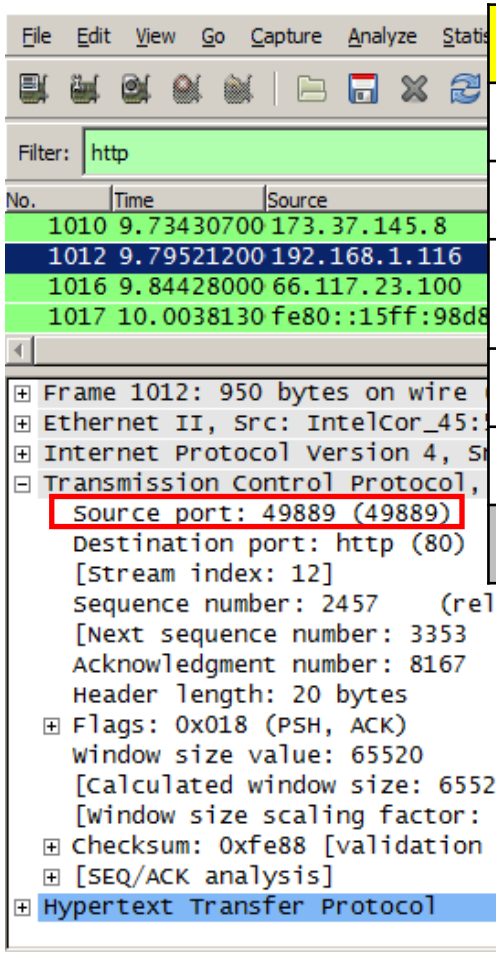


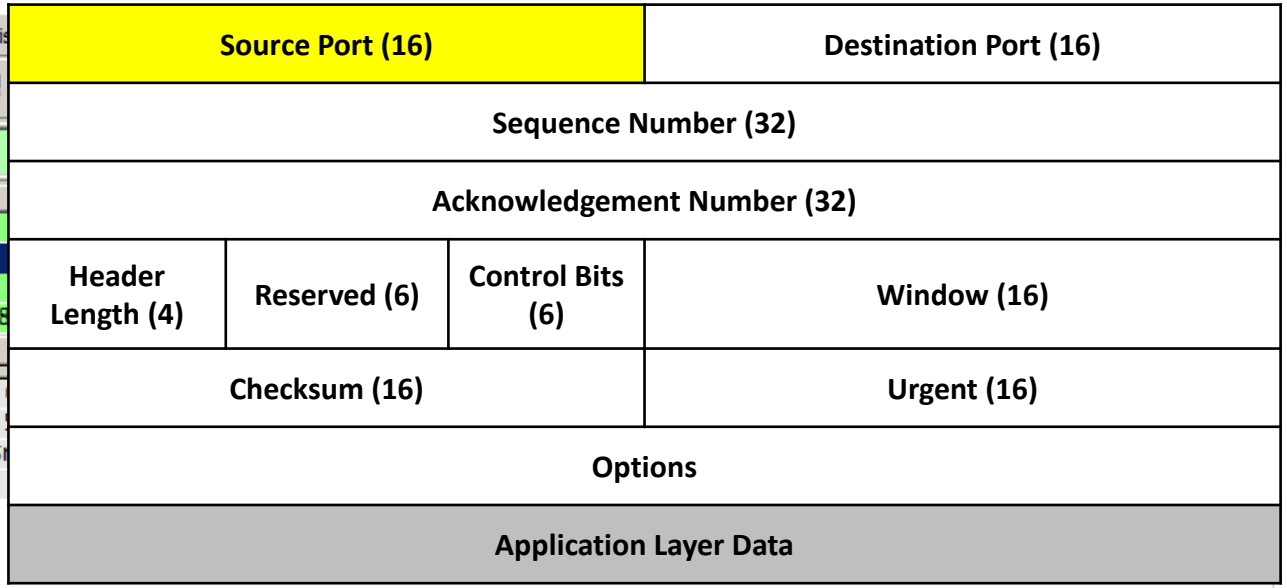
KARAKTERISTIKE TCP PROTOKOLA



- 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

TCP SEGMENT U WIRESHARK-U

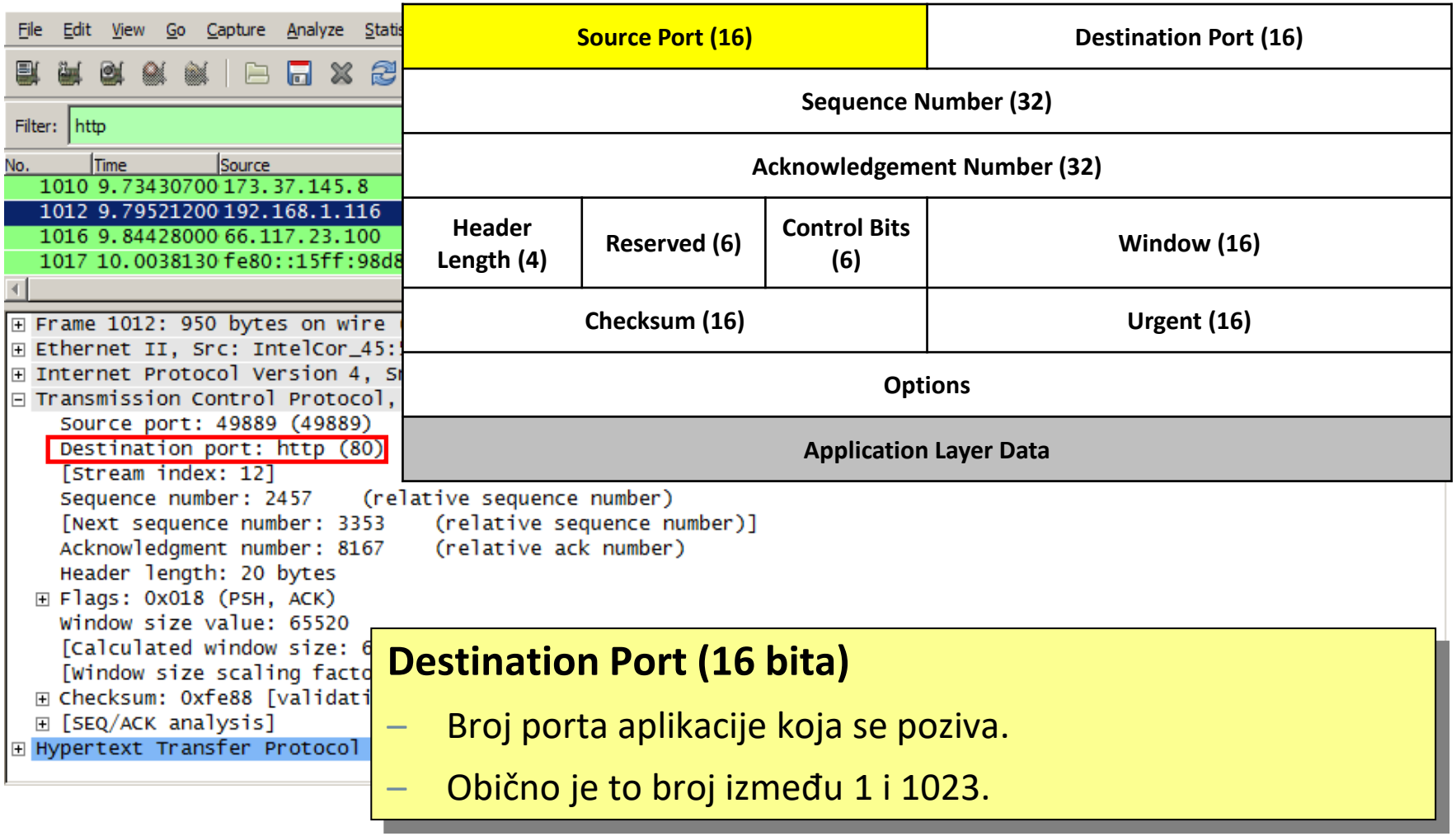




Source Port (16 bita)

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

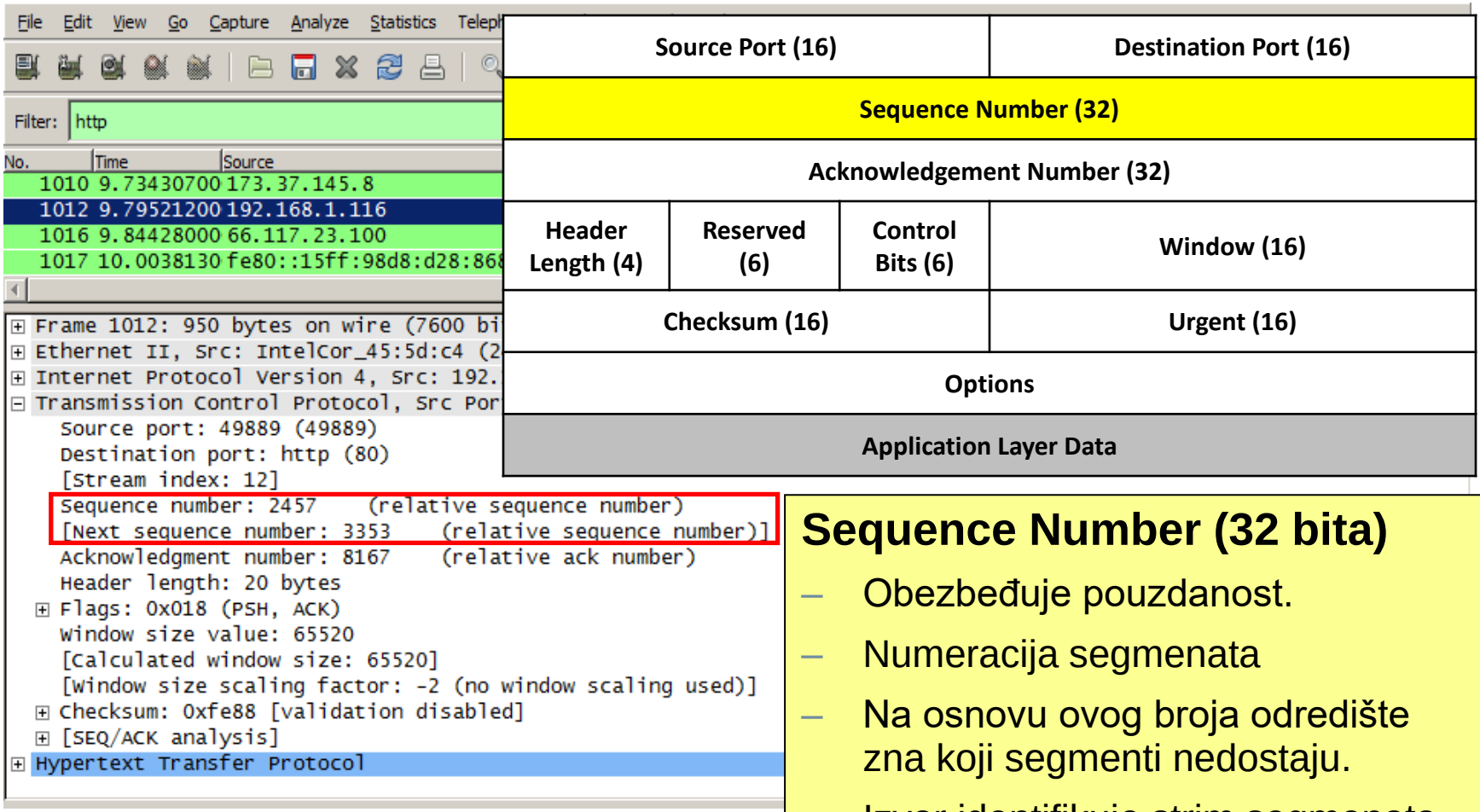
TCP SEGMENT U WIRESHARK-U



Destination Port (16 bita)

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

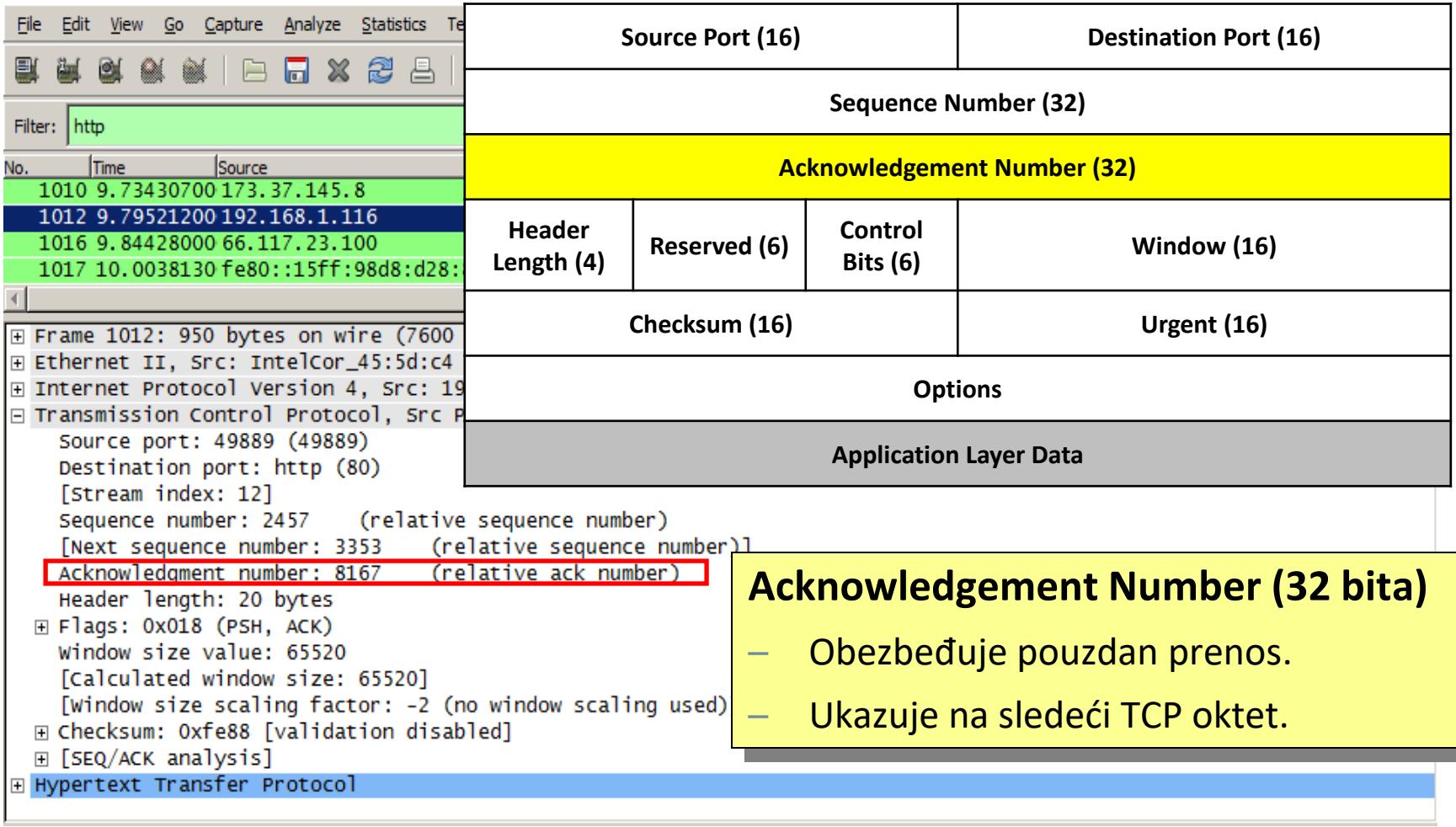
TCP SEGMENT U WIRESHARK-U



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

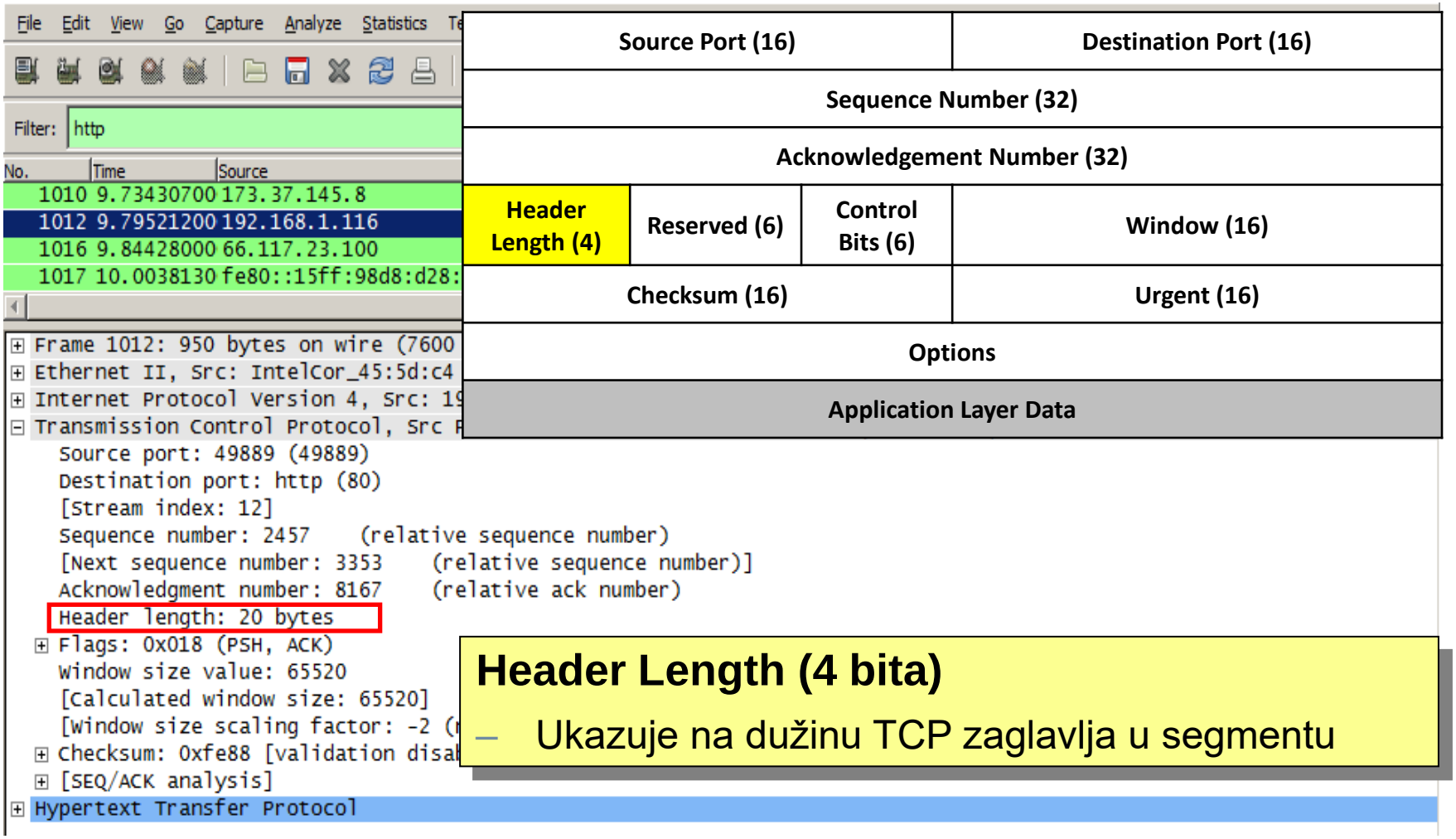


Source Port (16)			Destination Port (16)
Sequence Number (32)			
Acknowledgement Number (32)			
Header Length (4)	Reserved (6)	Control Bits (6)	Window (16)
Checksum (16)			Urgent (16)
Options			
Application Layer Data			

Acknowledgement Number (32 bita)

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

TCP SEGMENT U WIRESHARK-U

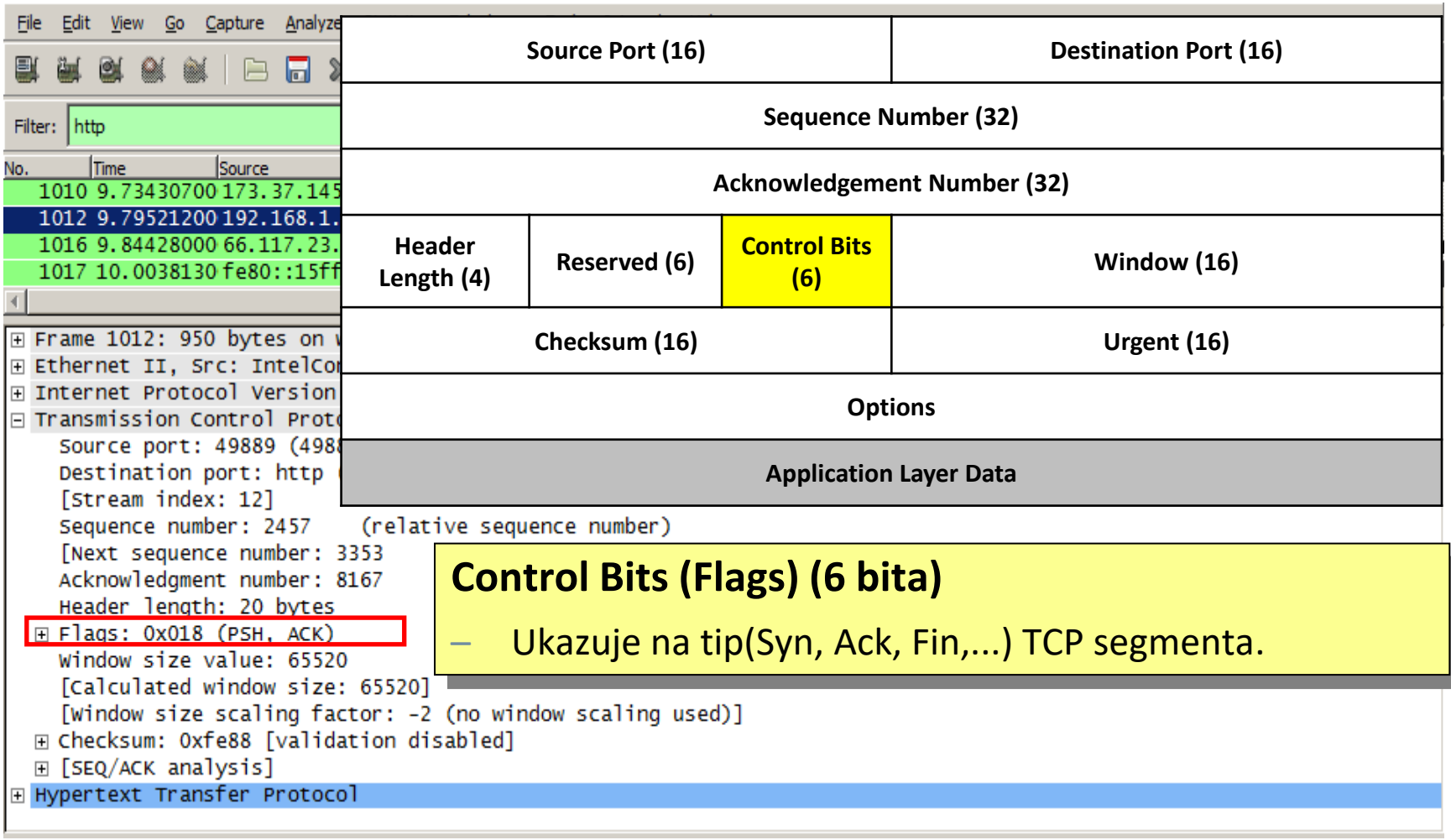


Source Port (16)			Destination Port (16)
Sequence Number (32)			
Acknowledgement Number (32)			
Header Length (4)	Reserved (6)	Control Bits (6)	Window (16)
Checksum (16)			Urgent (16)
Options			
Application Layer Data			

Header Length (4 bita)

- Ukazuje na dužinu TCP zaglavlja u segmentu

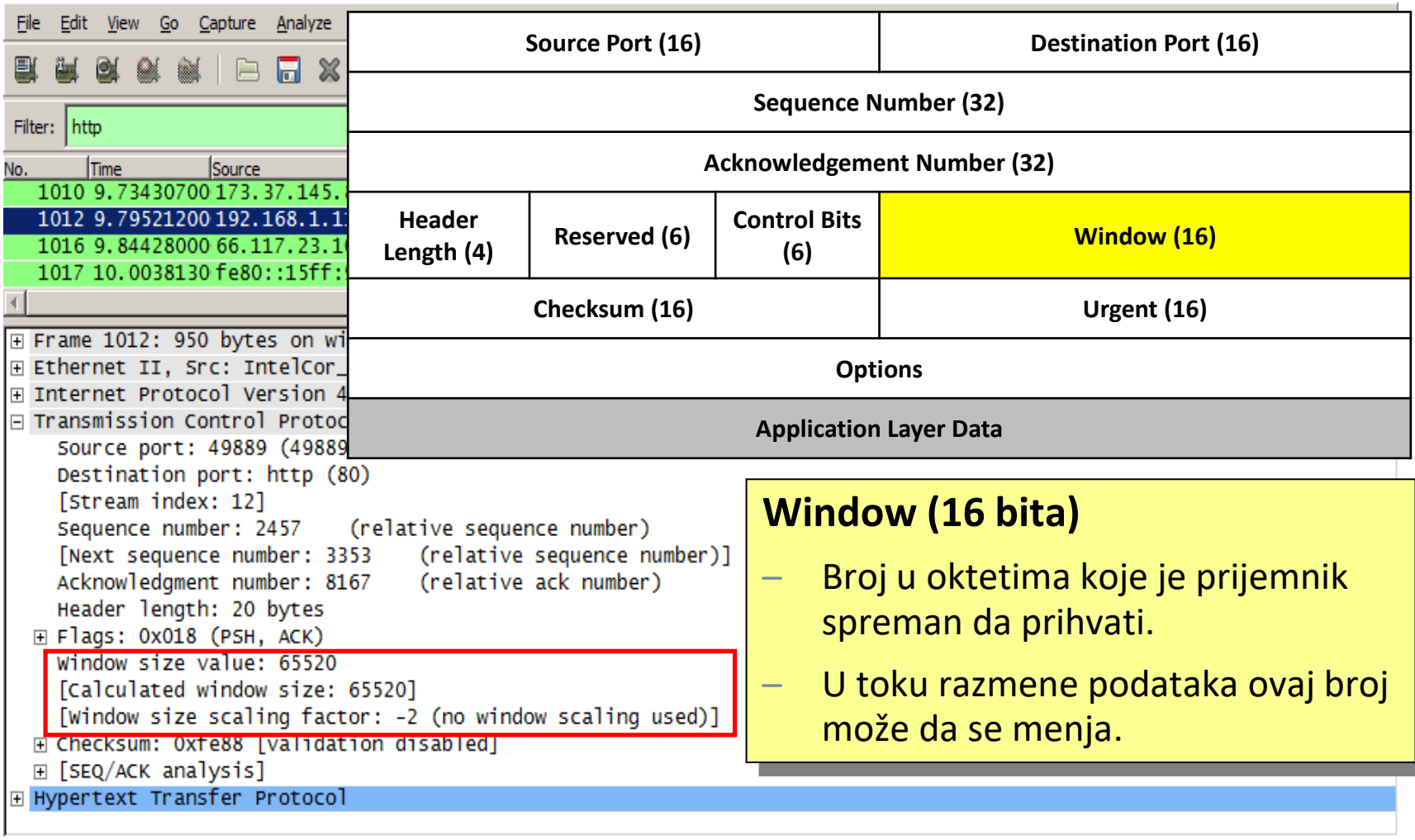
TCP SEGMENT U WIRESHARK-U



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.

DOBRO POZNATI PORTOVI (WELL KNOWN PORTS)

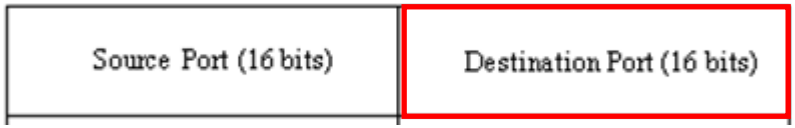
Port Number Range	Port Group
0 to 1023	Well Known (Contact) Ports
1024 to 49151	Registered Ports
49152 to 65535	Private and/or Dynamic Ports

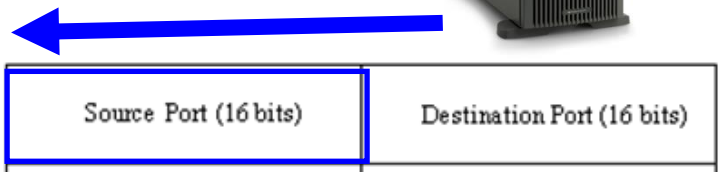
Well Known TCP Ports
21 FTP
23 Telnet
25 SMTP
80 HTTP
110 POP3
194 Internet Relay Chat (IRC)
443 Secure HTTP (HTTPS)

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

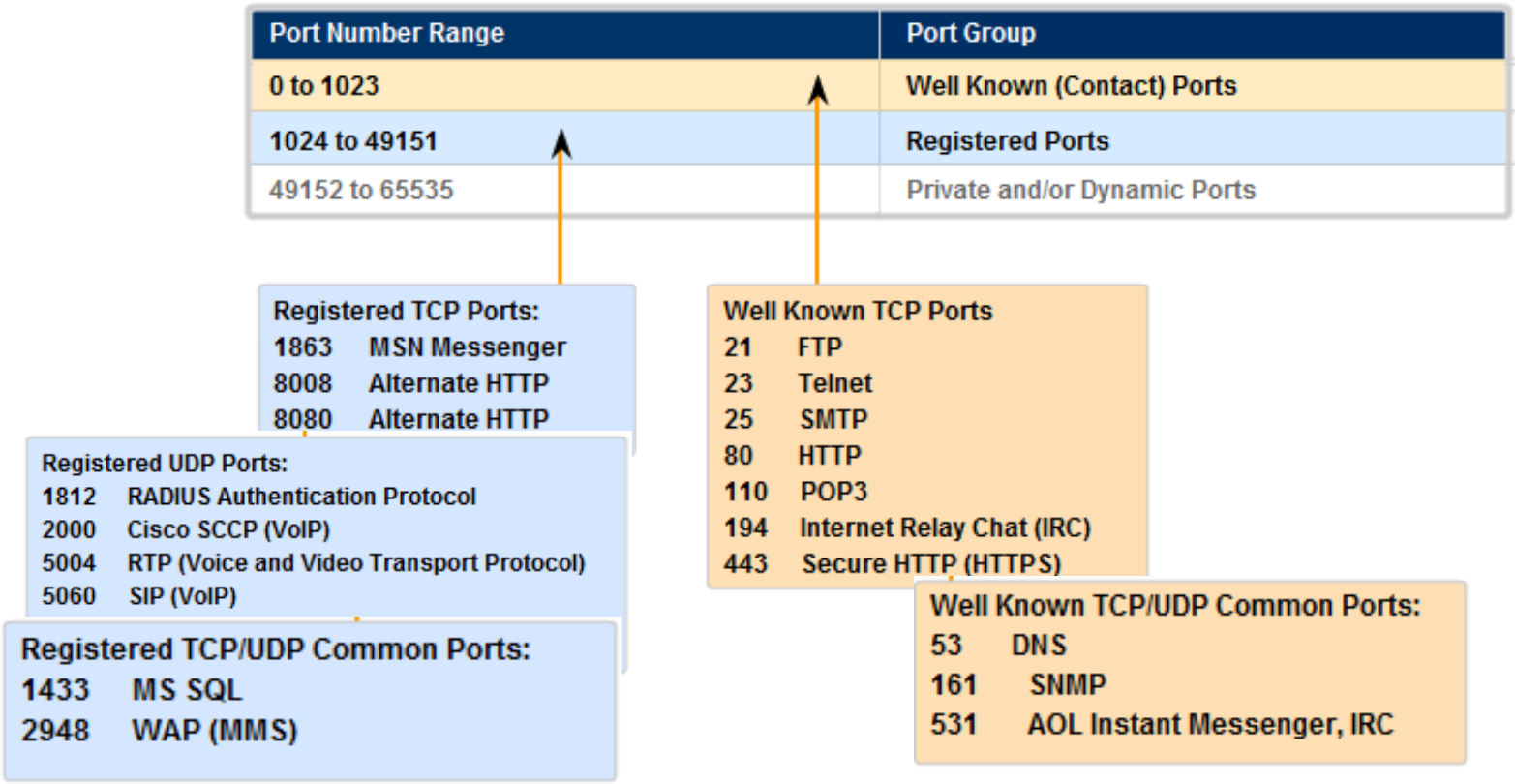




Well Known Ports (Brojevi od 0 do 1023)

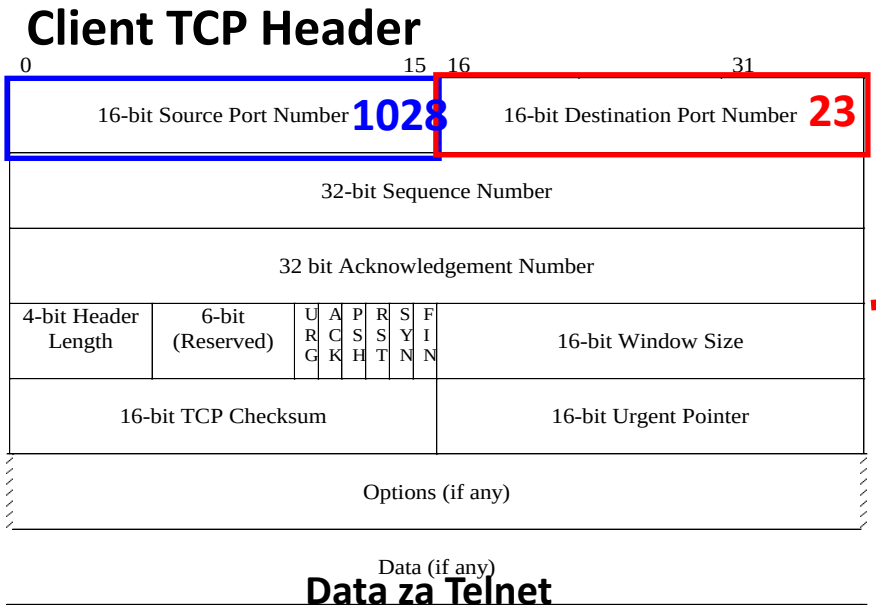
- Reservisani su za najpoznatije mrežne servise
- **Klient**: TCP destination port
- **Server**: TCP source port

REGISTROVANI PORTOVI



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

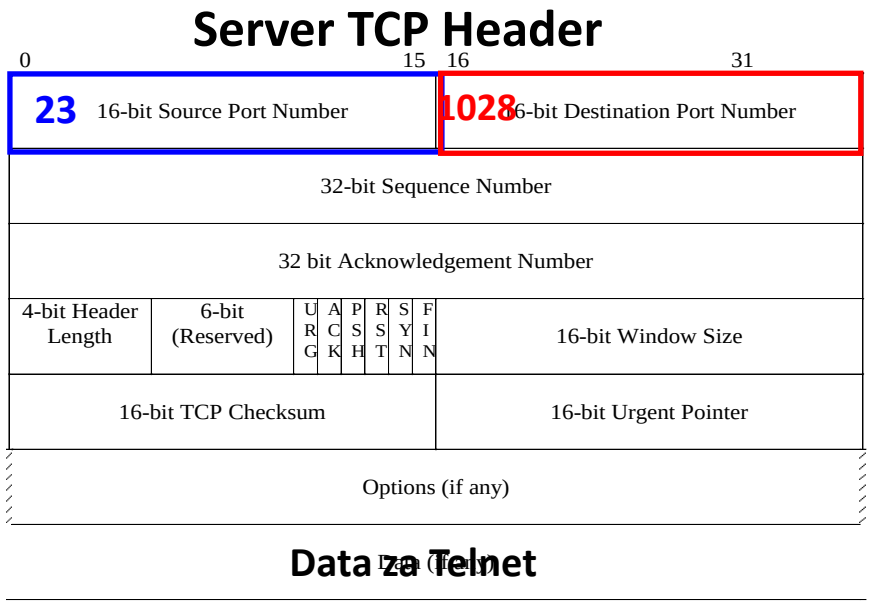
PRIMER DODELE PORTA APLIKACIJI



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

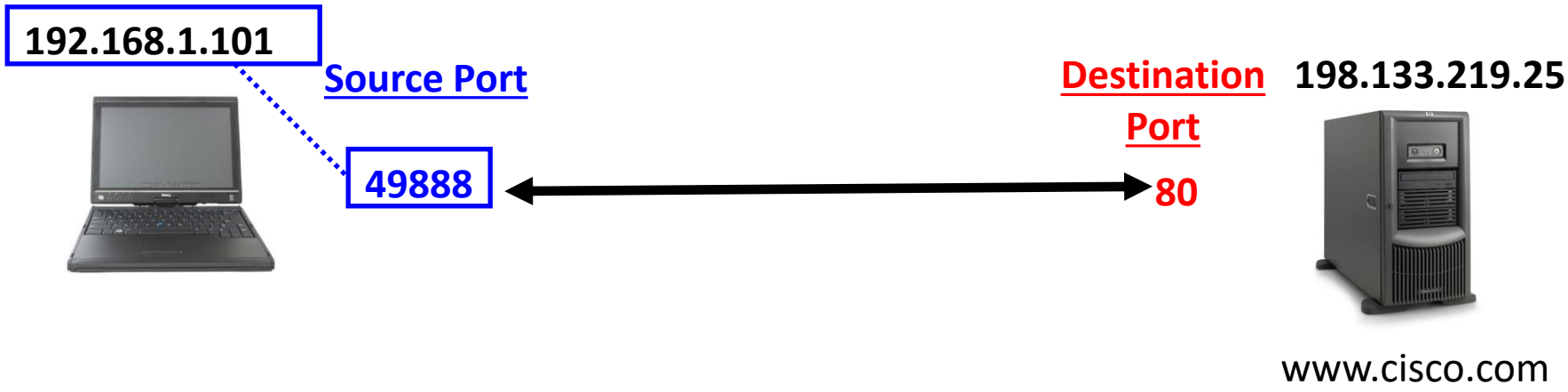
PRIMER DODELE PORTA APLIKACIJI

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



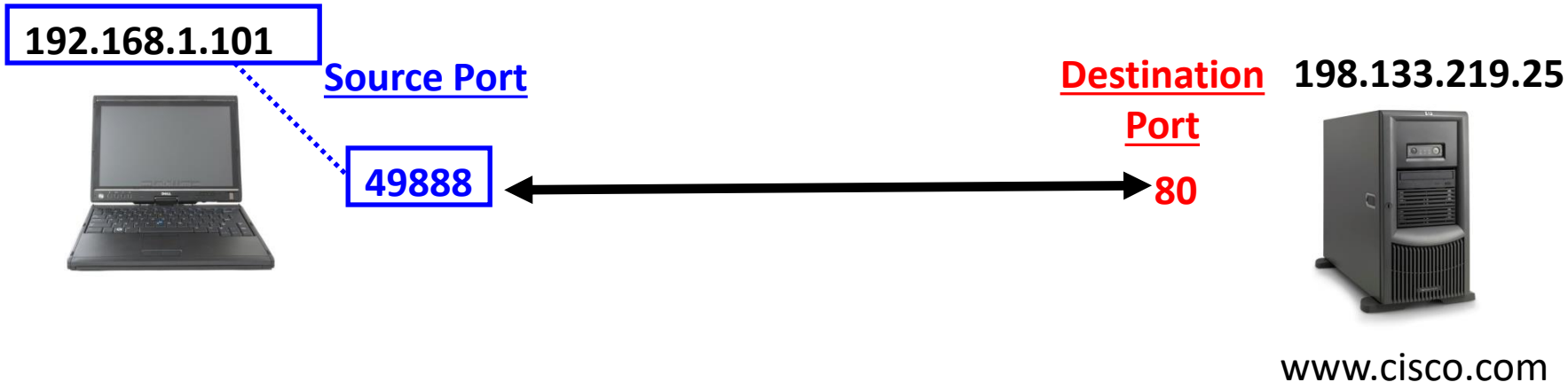
USPOSTAVLJANJE VIŠE SESIJA

SOCKET



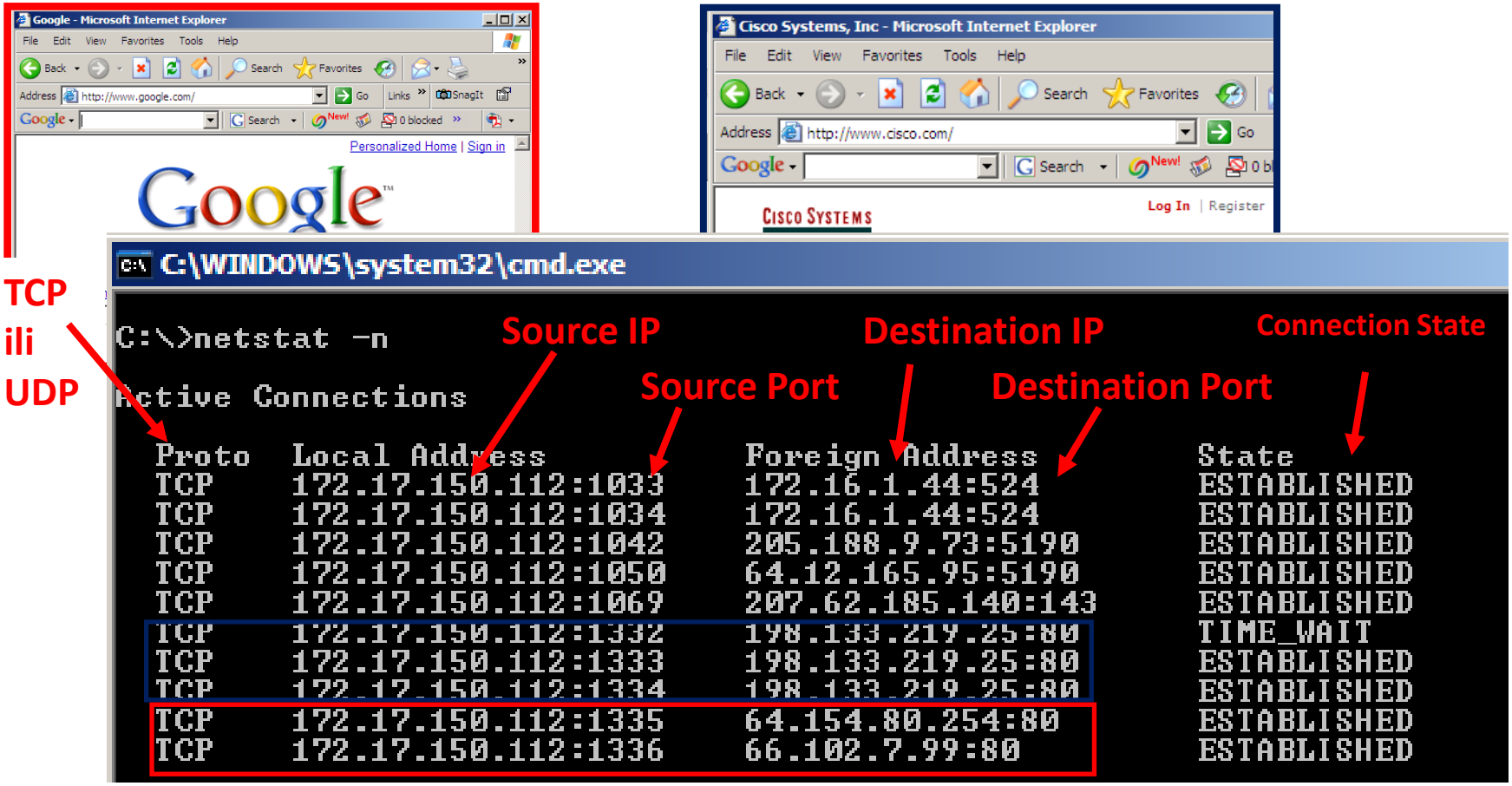
- Kombinovanjem broja porta na transportnom sloju i IP adrese na mrežnom sloju se na jedinstven način identifikuje konekcija (aplikacija) koja se izvršava
  - Kombinacija IP adrese i broja porta zove se **socket**.
- Komunikacija(flow) između dve aplikacije se na jedinstven način identifikuje koristeći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

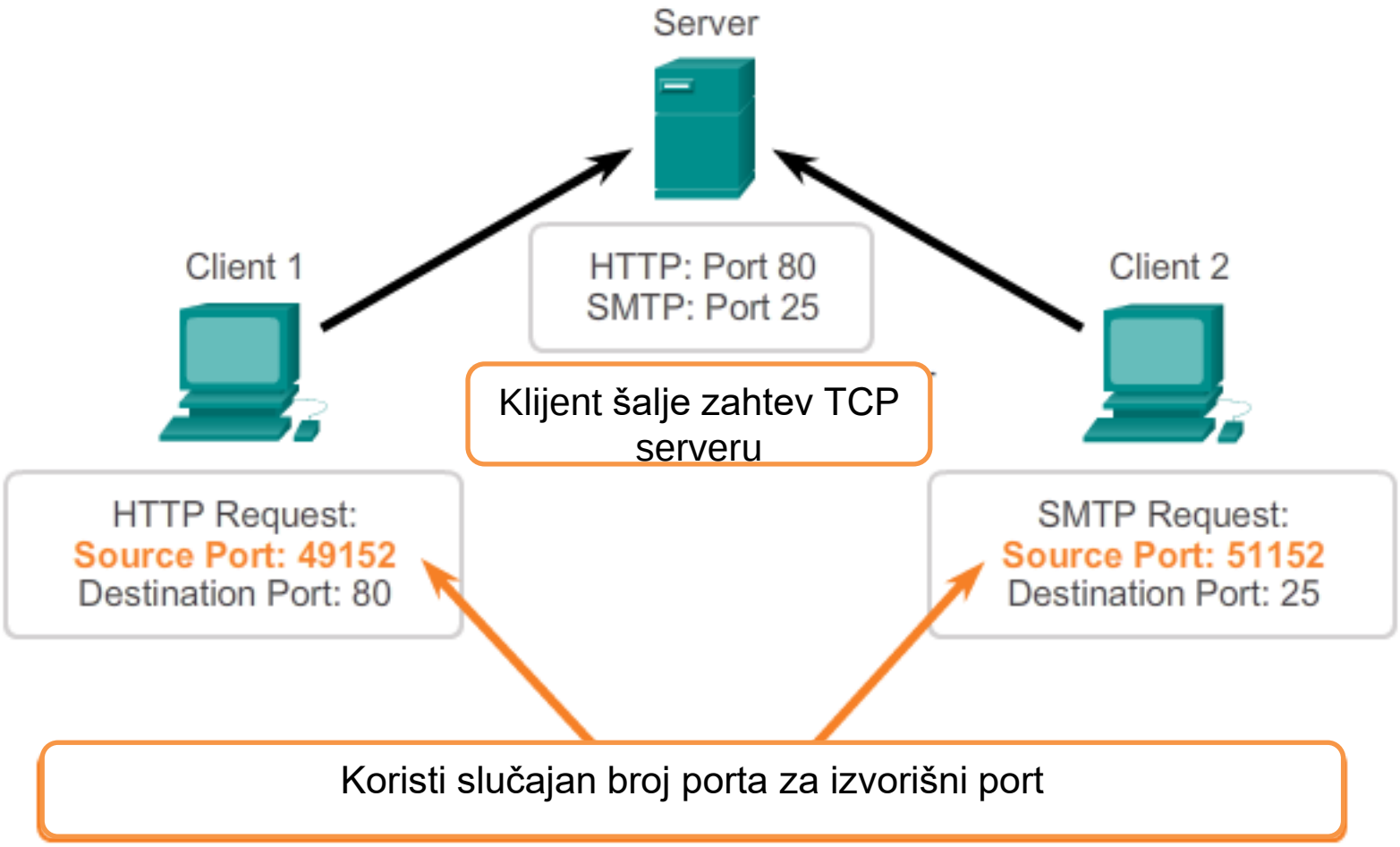


- **Napomena:** Kada učitavamo web stranu i njene objekte obično se uspostavljaju nekoliko TCP sesije.

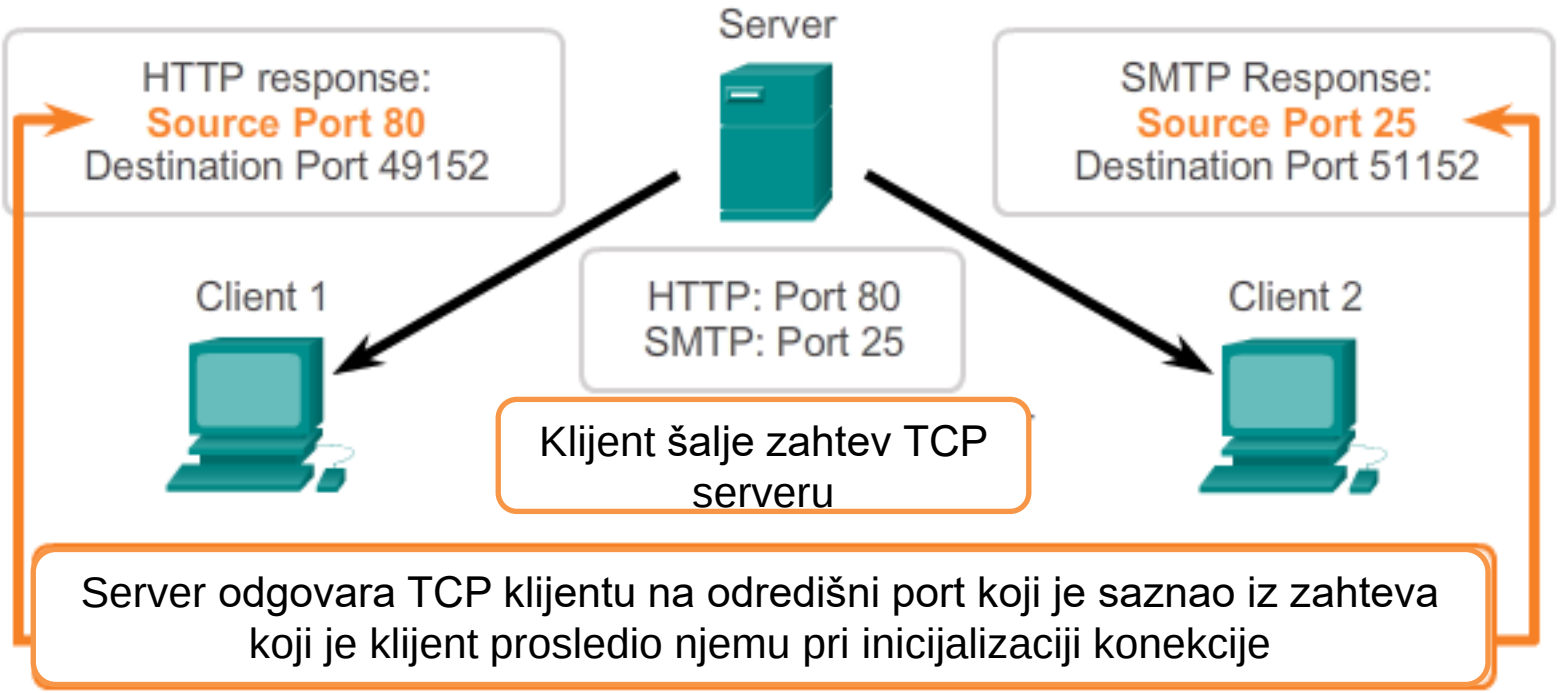
USPOSTAVLJANJE SESIJE

Uspostavljanje sesije (establishing session) obezbeđuje da je aplikacija spremna da šalje i prima podatke

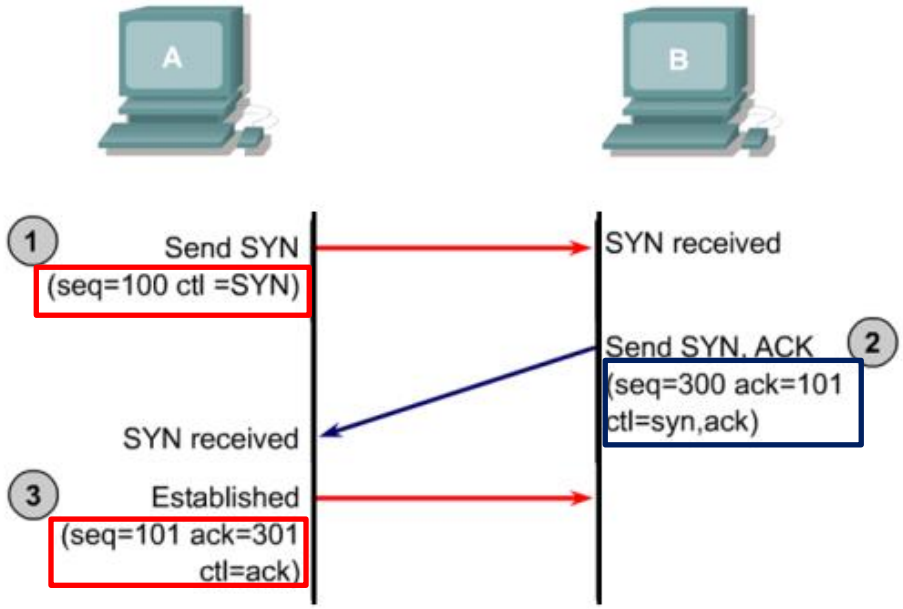
USPOSTAVLJENJE KONEKCIJE



USPOSTAVLJENJE KONEKCIJE



USPOSTAVLJENJE KONEKCIJE



TCP je pouzdan protokol jer ima mehanizam za uspostavljanje konekcije i praćenje sesije.

Konekcija između dva hosta mora prvo da se uspostavi pre nego što se krene sa razmenom podataka (**Three-way Handshake)**

Nakon završetka sa razmenom podataka sesija se zatvara i konekcija prekida

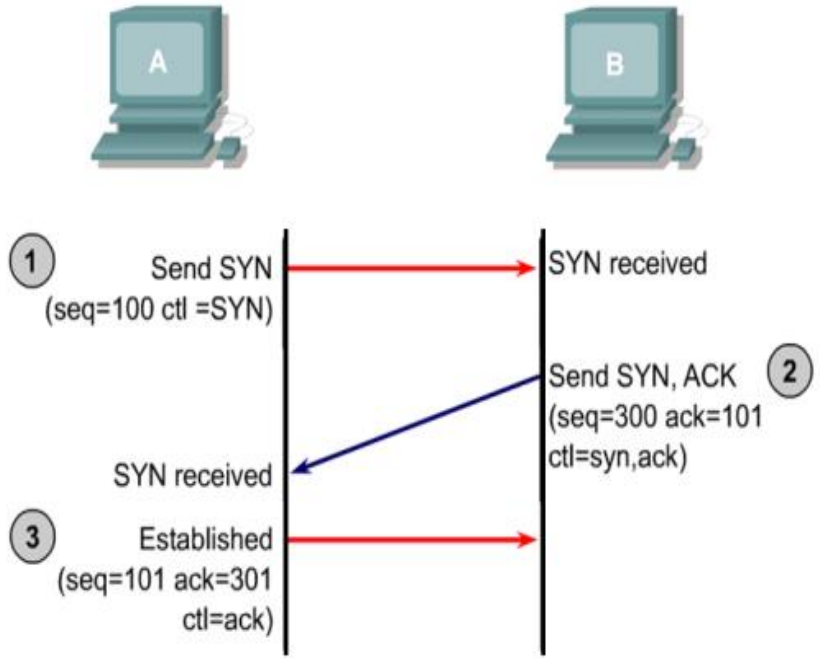
USPOSTAVLJENJE KONEKCIJE

Three-way handshake procedura:

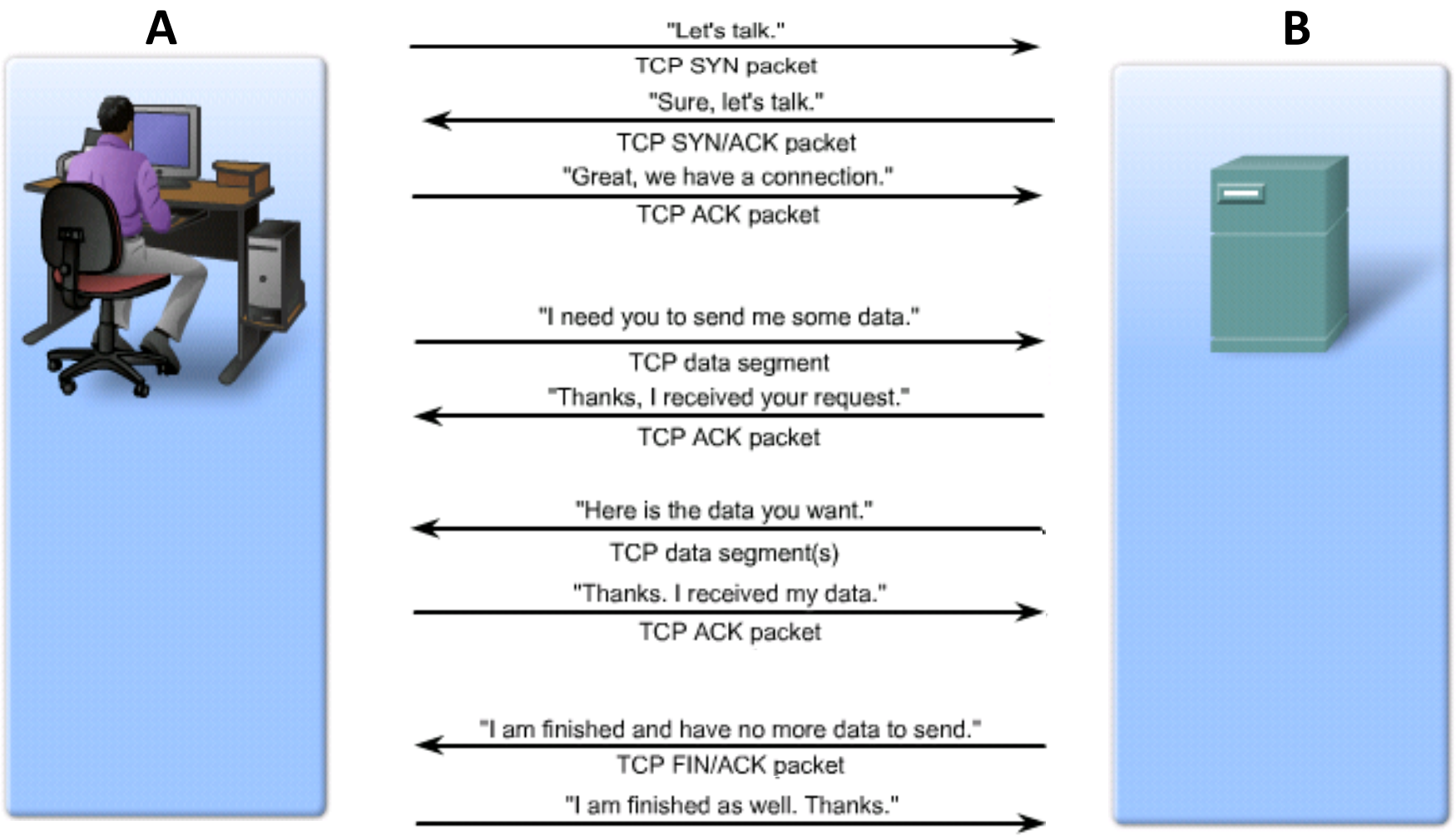
Utvrđuje prisustvo odredišnog računara u mreži.

Utvrđuje dostupnost servisa na odredištu i da li aplikacija sluša na definisanom odredišnom portu

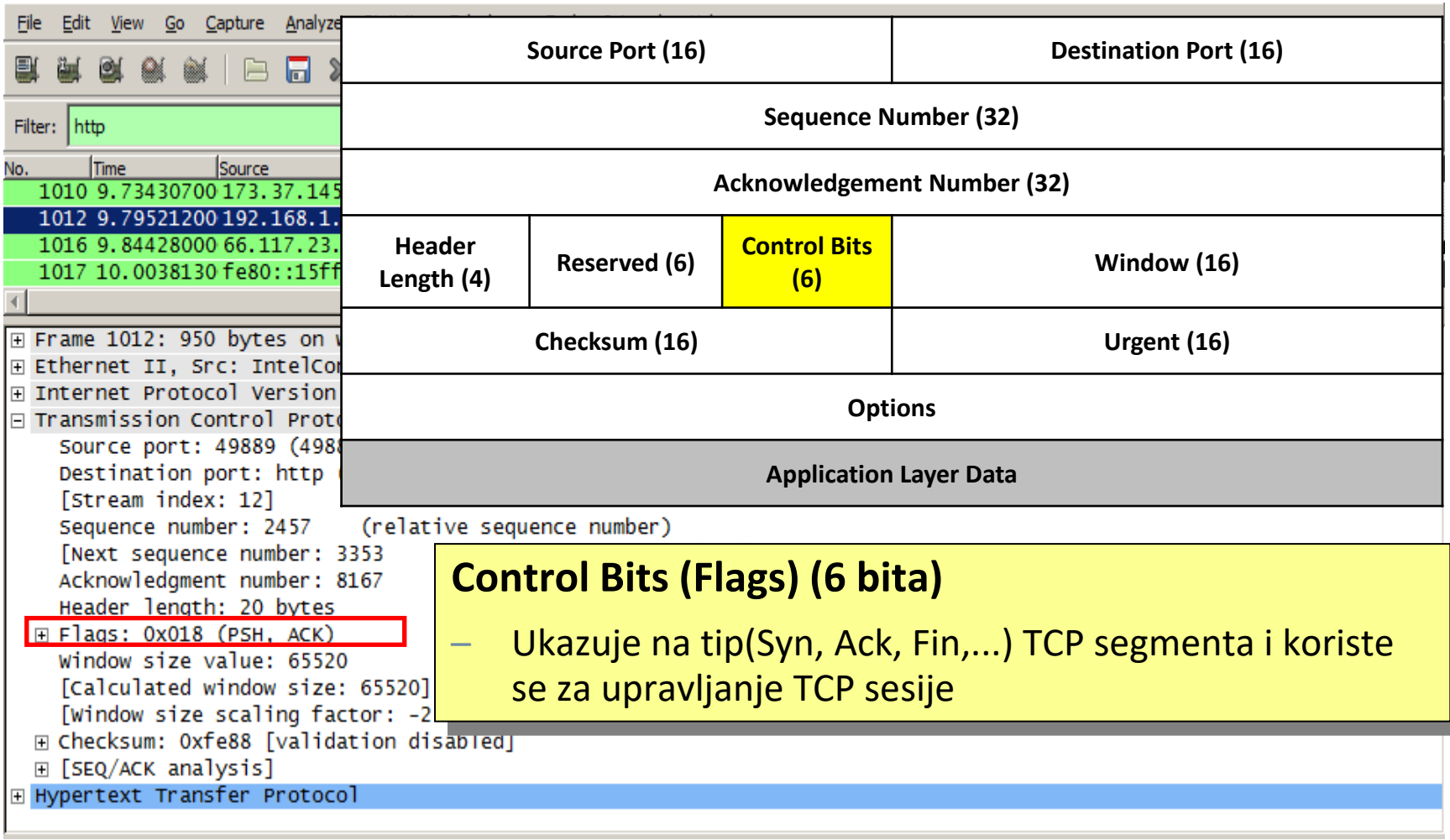
Informiše se odredište da klijent želi da uspostavi sesiju sa tim brojem porta



TCP KOMUNIKACIJA



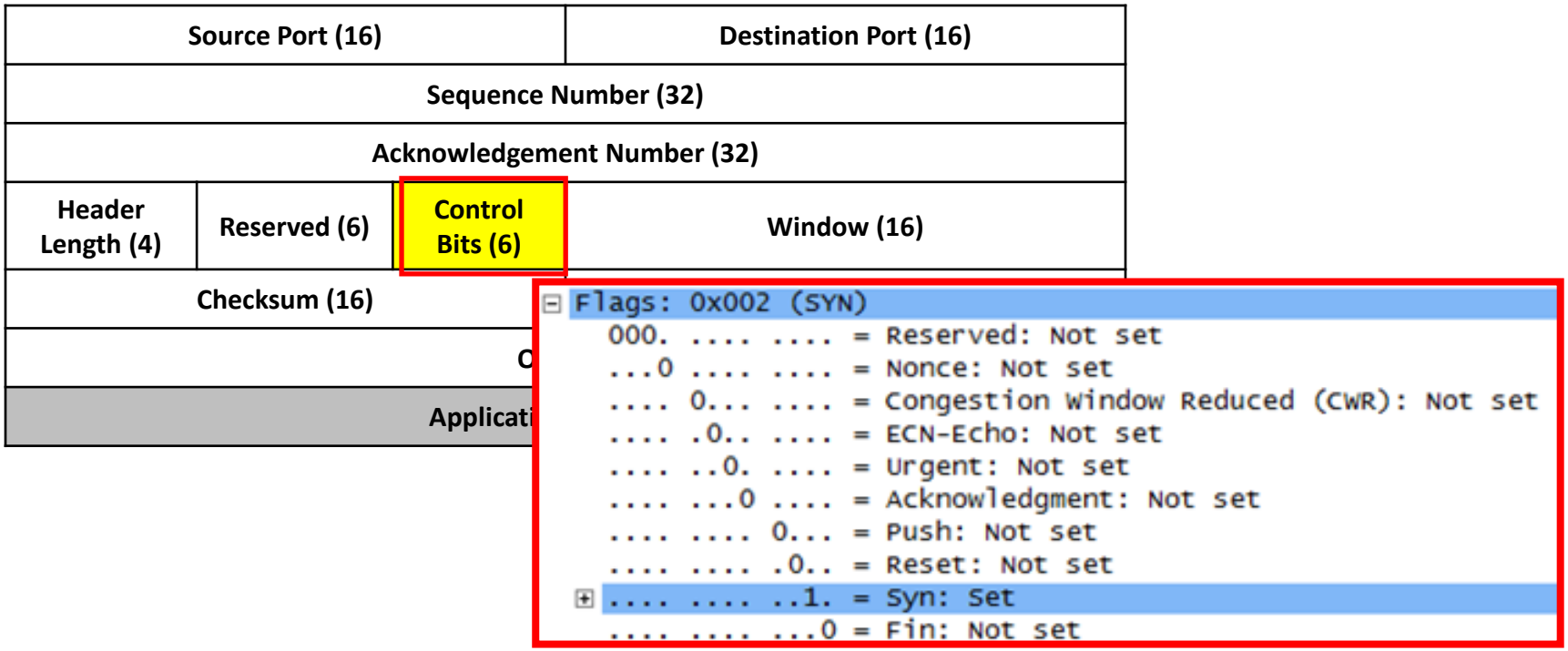
TCP KONTROLNI BITOVI



Control Bits (Flags) (6 bita)

- Ukazuje na tip(Syn, Ack, Fin,...) TCP segmenta i koriste se za upravljanje TCP sesije

TCP FLAGS



- U TCP kontrolnom polju mogu se setovati 6 bita koji upravljaju TCP sesijom
  - Svako polje je veličine 1 bita i zove se *flag*.
  - Flag može da sadrži 1(uključena opcija) ili 0 (isključena opcija).

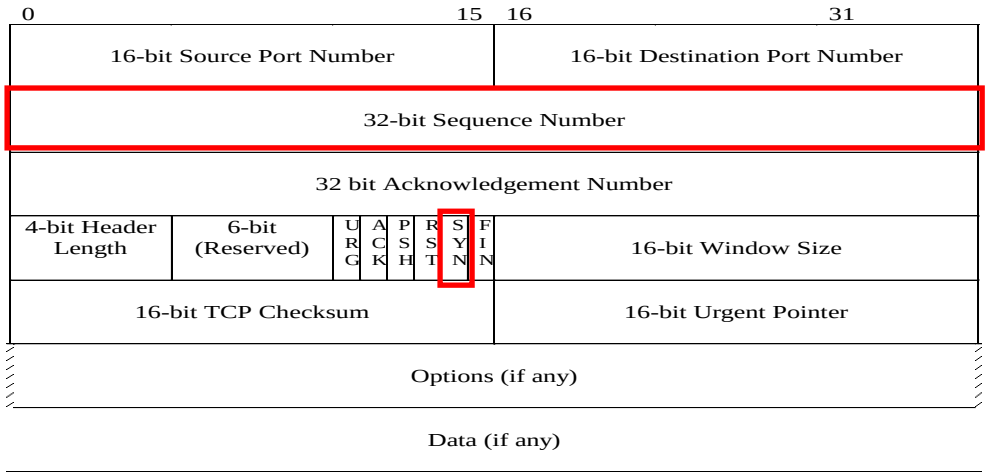
USPOSTAVLJENJE KONEKCIJE

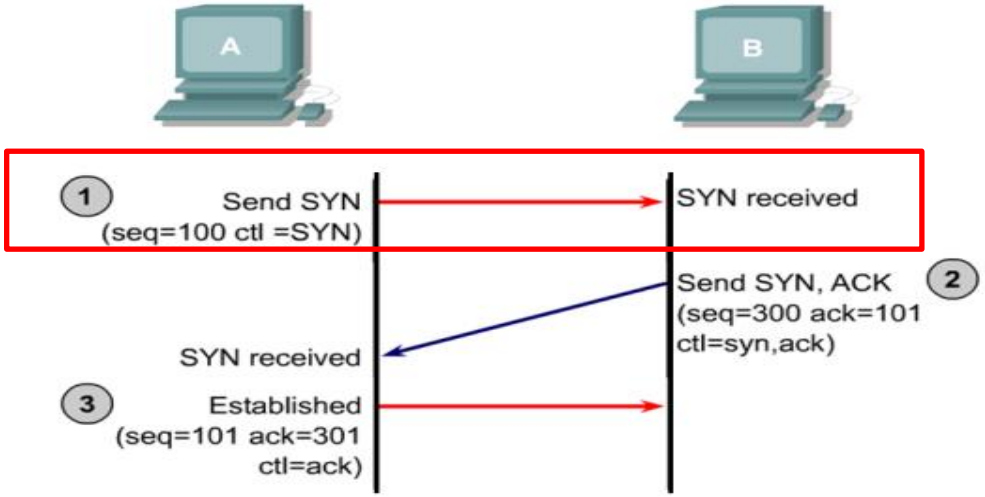
- U TCP koriste se 6 *flag*-a za upravljanje konekcijom:
  - URG - (0x020) Urgent pointer field significant
  - **ACK** - (0x010) Acknowledgement field significant
  - PSH - (0x004) Push function
  - RST - (0x003) Reset the connection
  - **SYN** - (0x002) Synchronize sequence numbers
  - **FIN** - (0x001) No more data from sender

http://packetlife.net/blog/2011/mar/2/tcp-flags-psh-and-urg/

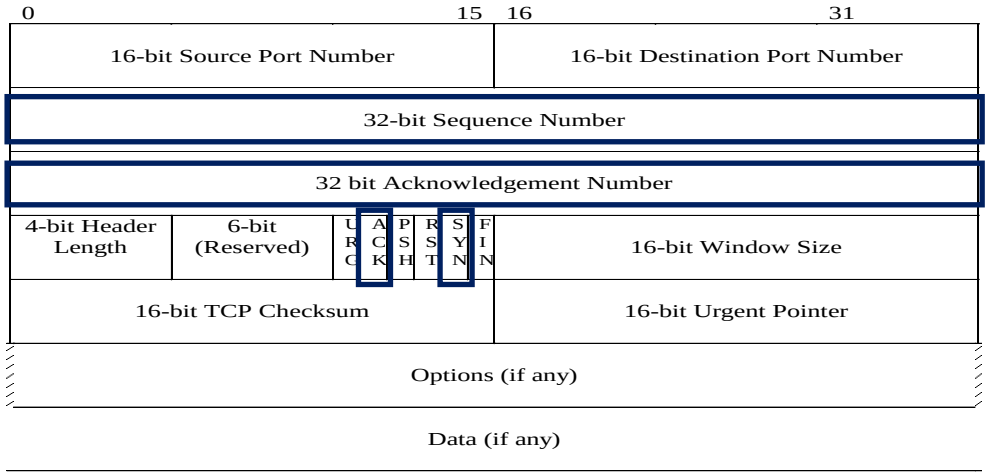
http://www.firewall.cx/networking-topics/protocols/tcp/136-tcp-flag-options.html

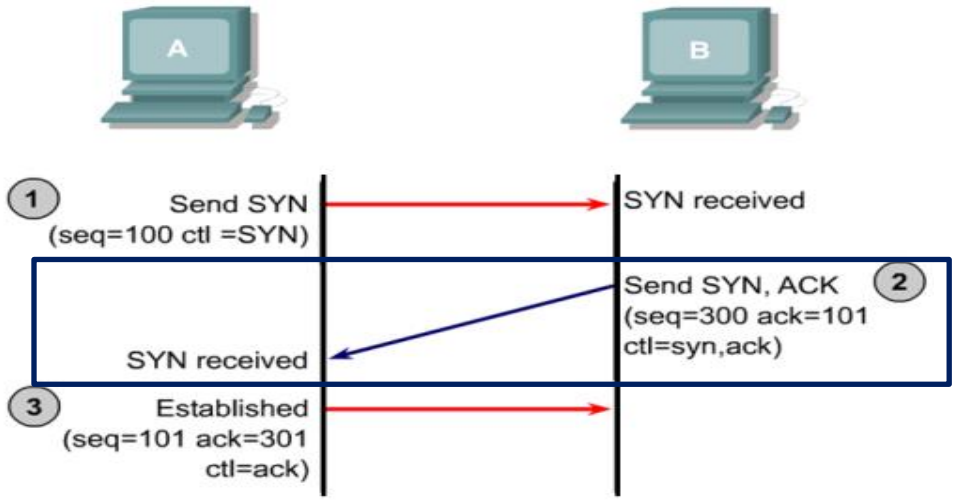
FAZE U USPOSTAVLJANJU KONEKCIJE



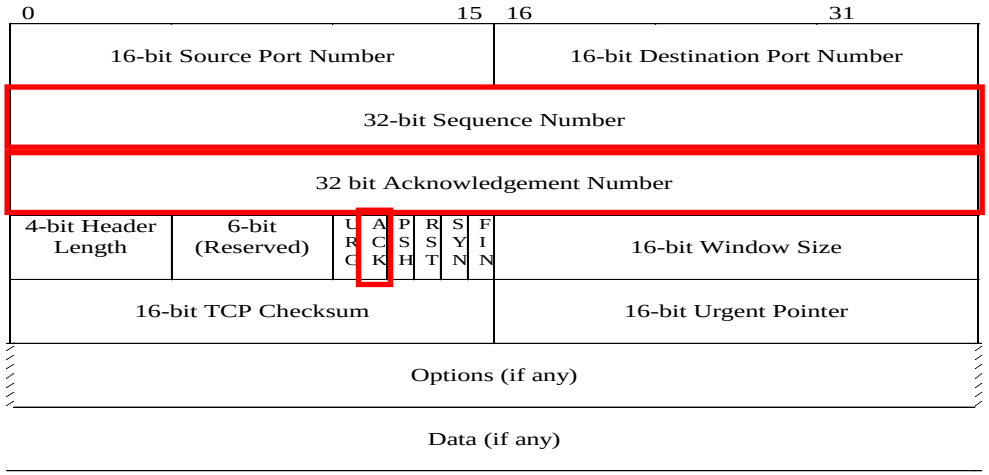


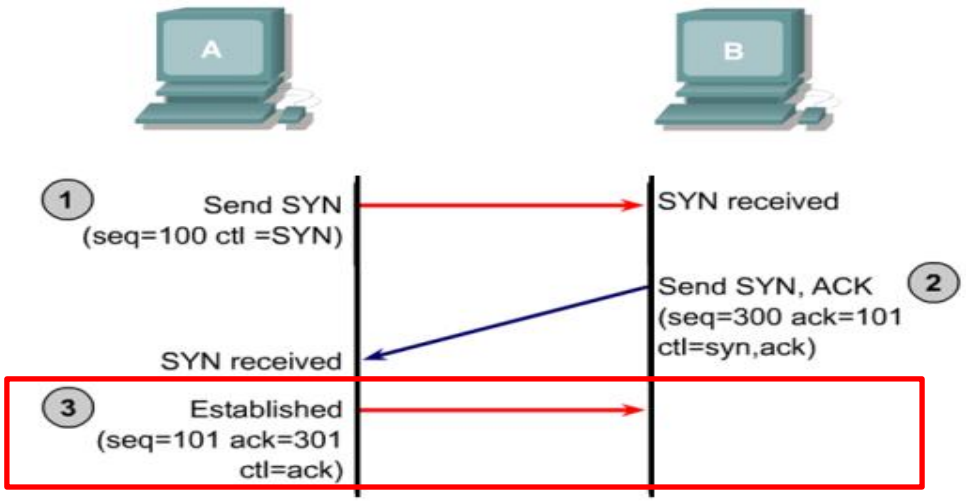
FAZE U USPOSTAVLJANJU KONEKCIJE



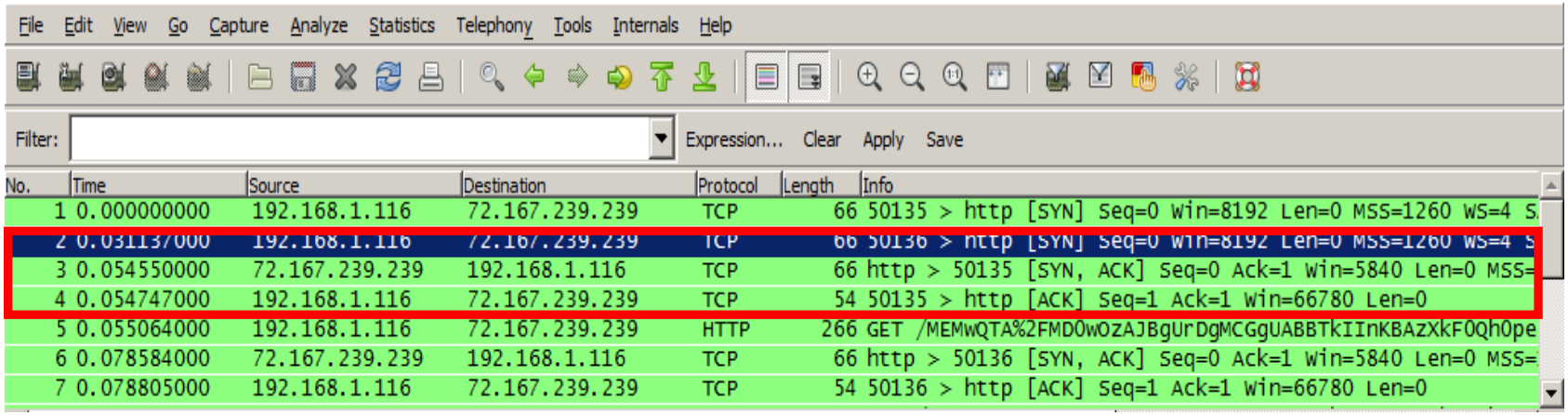


FAZE U USPOSTAVLJANJU KONEKCIJE

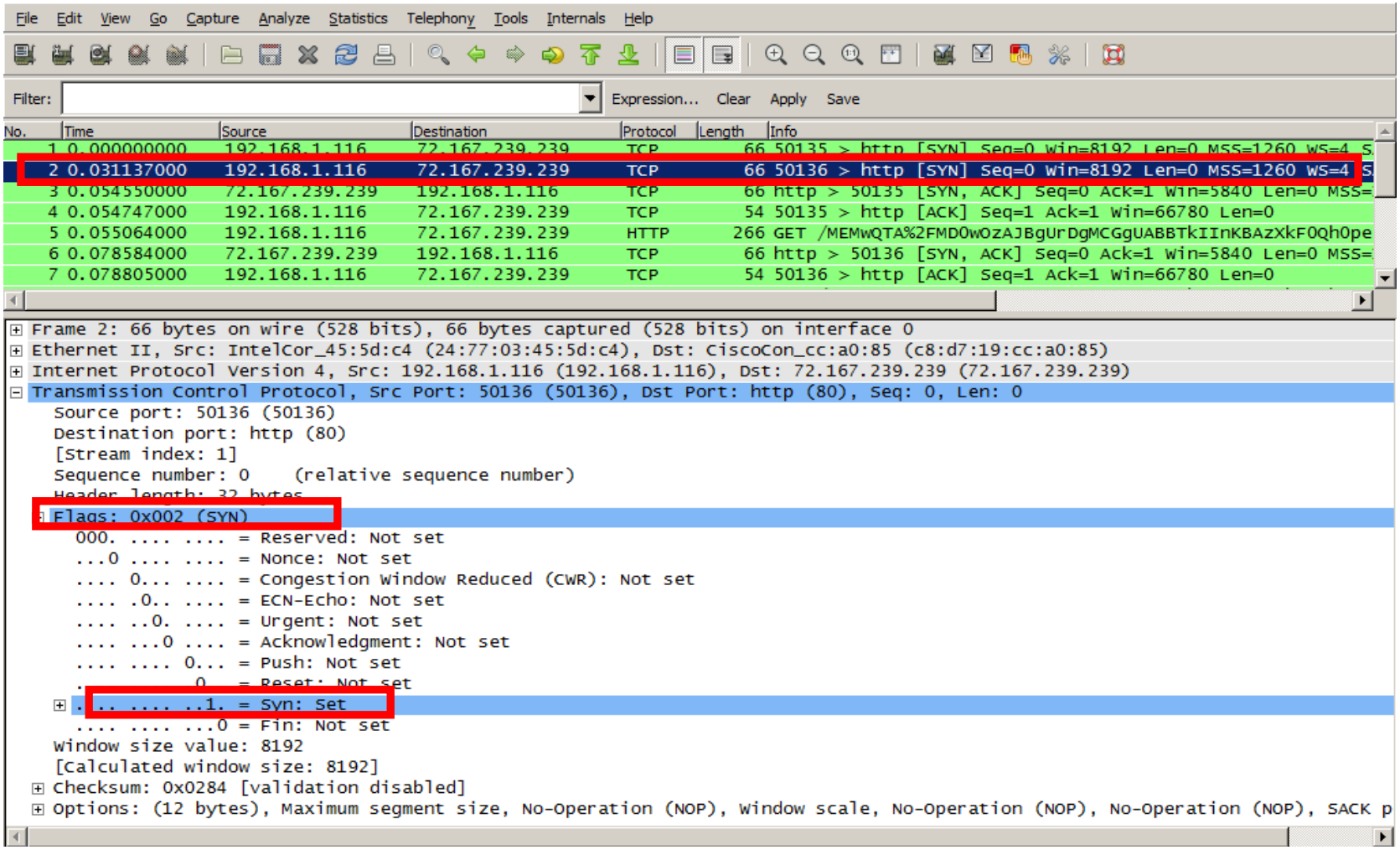




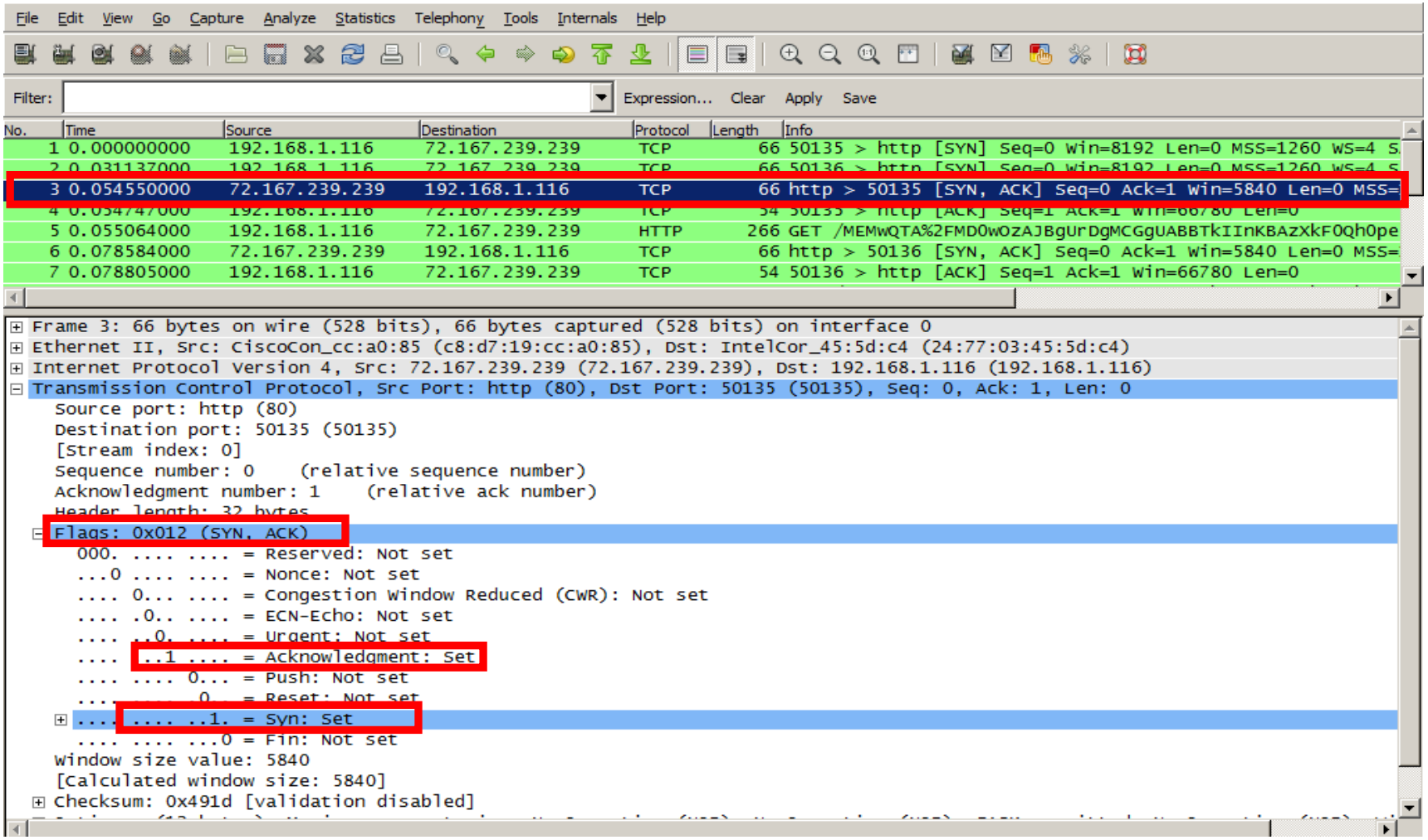
FAZE U USPOSTAVLJANJU KONEKCIJE (WIRE SHARK)



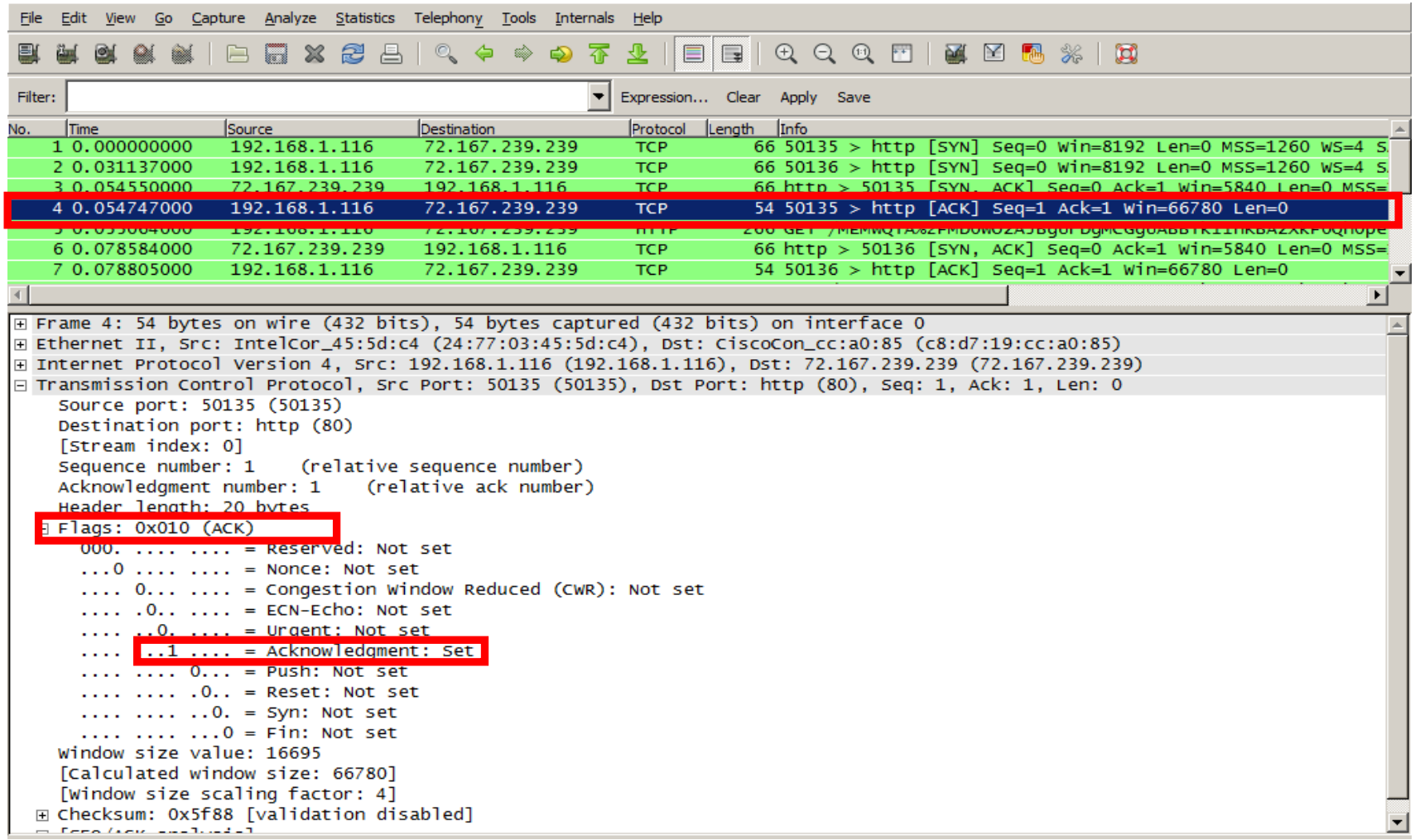
FAZE U USPOSTAVLJANJU KONEKCIJE (WIRE SHARK)



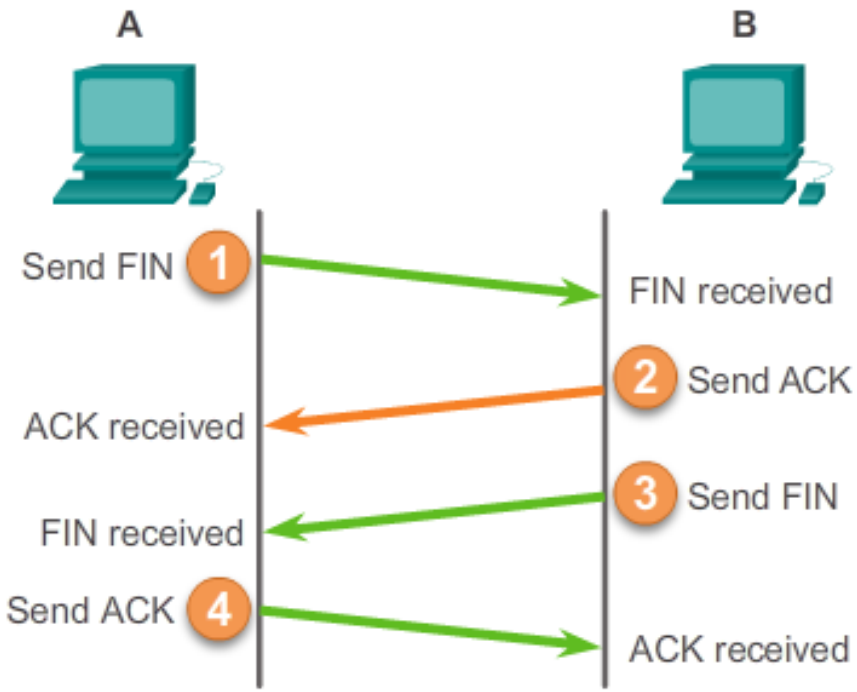
FAZE U USPOSTAVLJANJU KONEKCIJE (WIRE SHARK)



FAZE U USPOSTAVLJANJU KONEKCIJE (WIRE SHARK)

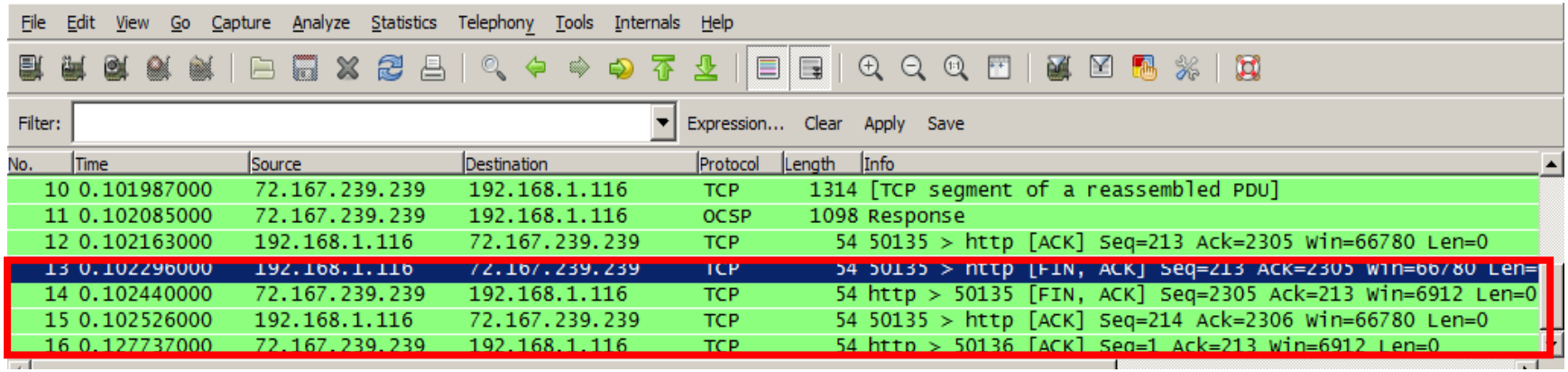


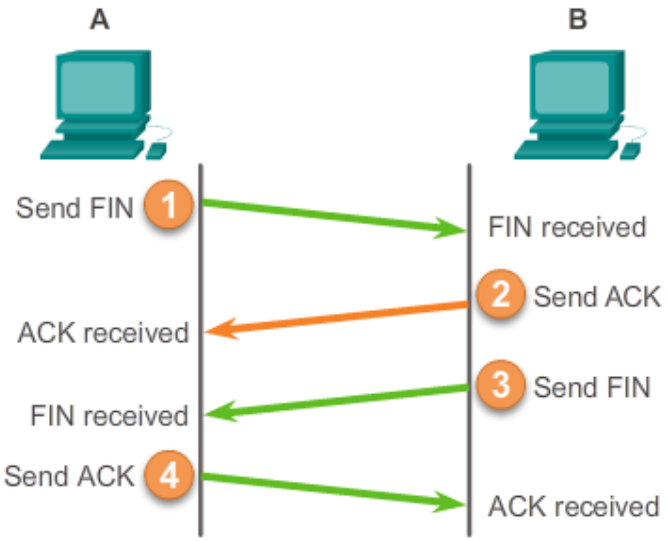
RASKIDANJE KONEKCIJE



- Host A šalje segment sa setovanim FIN bitom.
- Host B odgovara sa setovanim ACK bitom.
- Host B odgovara sa segmentom kome je setovan FIN bit.
- Host A odgovara sa setovanim ACK bitom.

RASKIDANJE KONEKCIJE (WIRESHARK)





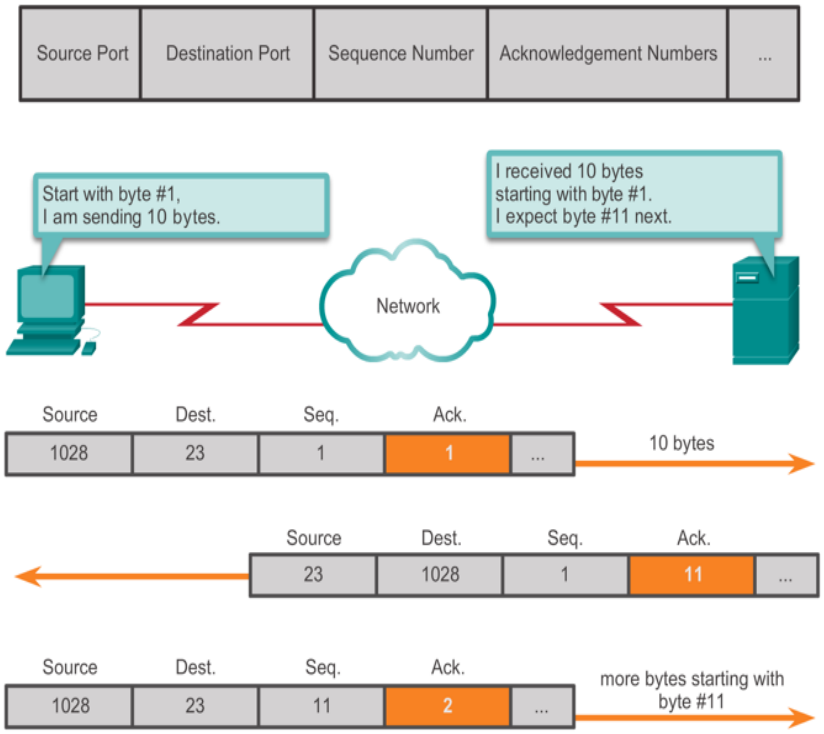
POLJA ZA POUZDAN PRENOS

SN (sequence number) i Ack polja obezbeđuju pouzdan prenos.

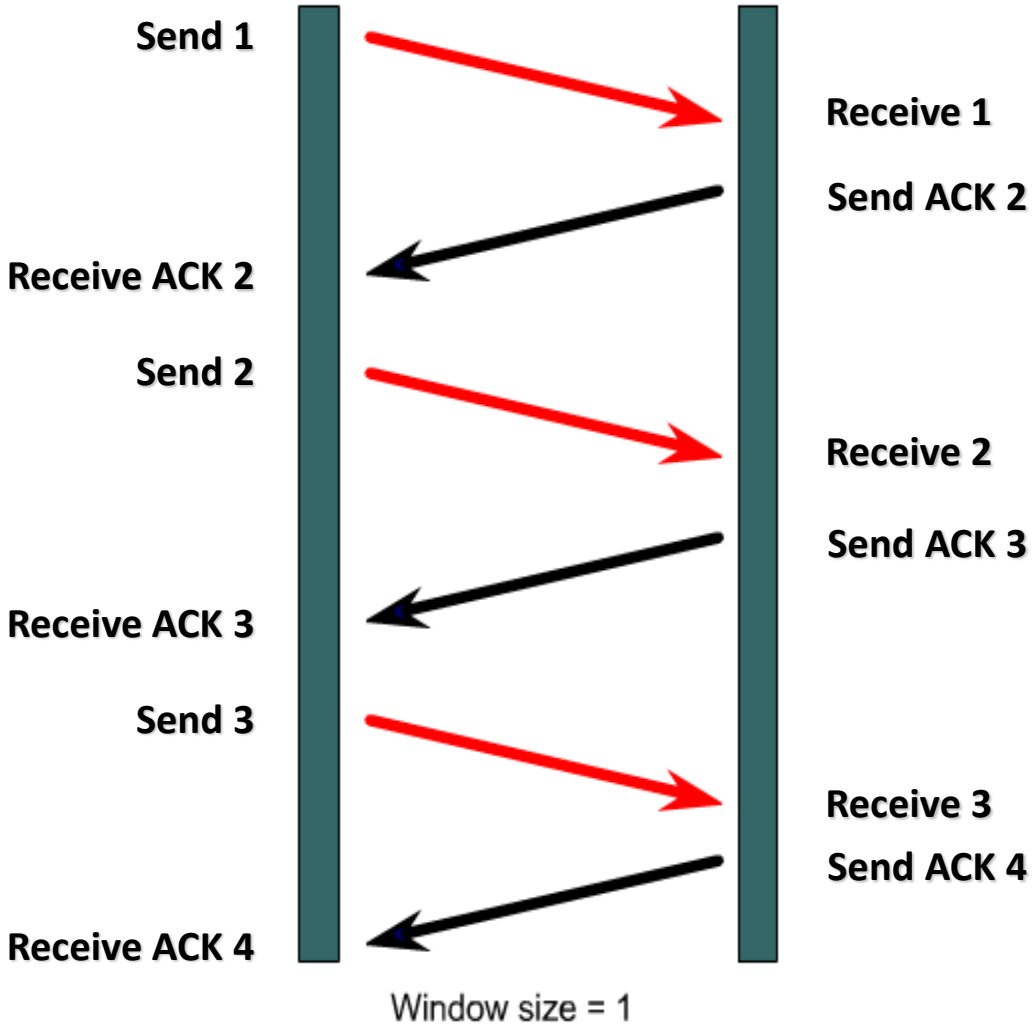
SN koisti odredište da bi saznalo koji je zadnji poslat segment, a Ack koristi izvor da bi saznao šta je odredište zadnje primilo.

SN broj ukazuje na prvi bajt u segmentu. Na osnovu ovog broja možemo da odredimo broj prenetih bajtova

TCP koristi ACK broj kojim prijemnik ukazuje koji je sledeći bajt koji očekuje da primi (**<u>expectational acknowledgement</u>**).

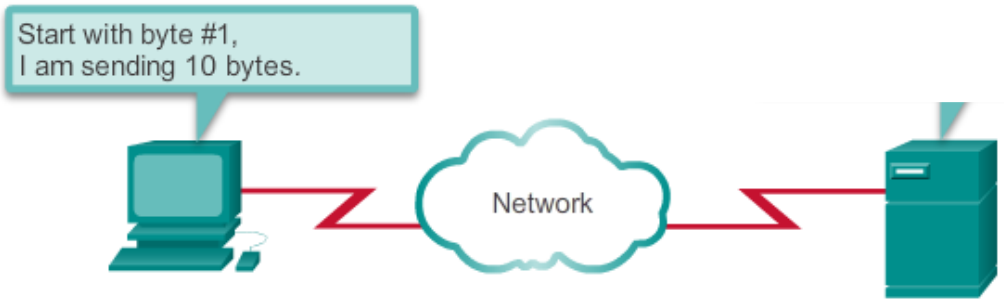


UPROŠĆEN MODEL POUZDANOSTI



UPRAVLJANJE TCP SESIJOM

Source Port	Destination Port	Sequence Number	Acknowledgement Numbers	...



Source	Dest.	SN	ACK #
1028	23	1	1

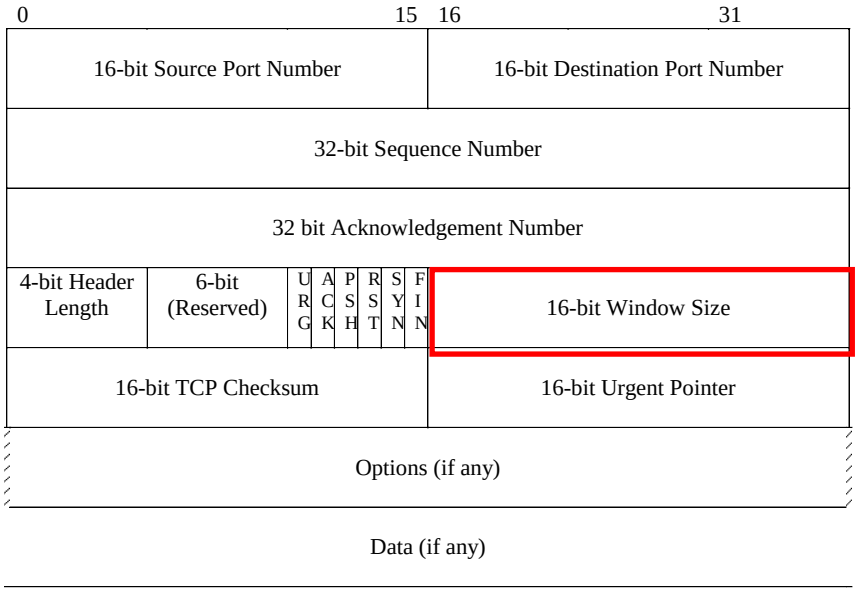
10 bytes

Source	Dest.	SN	ACK #
23	1028	1	11

Source	Dest.	SN	ACK #
1028	23	11	2

Next 10 bytes starting with byte 11

KONTROLA TOKA (FLOW CONTROL)

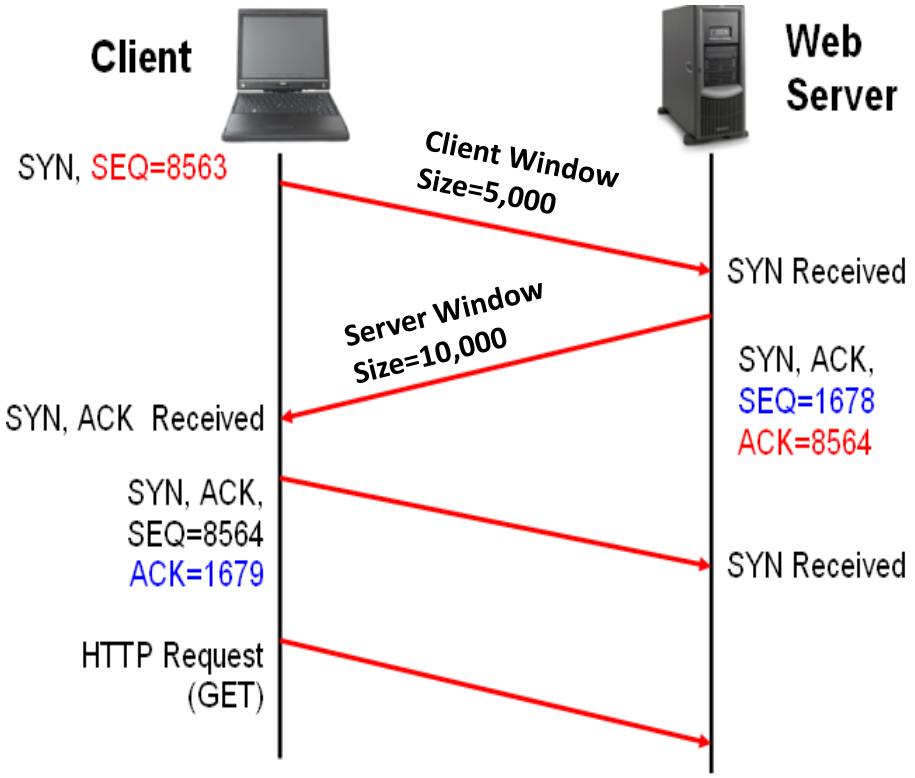


- Ukoliko čekamo Ack za svaki primljeni segment komunikacija bi bila ne efikasna.
- TCP ovaj problem rešava prosleđujući segmente na osnovu veličine polja "**window**".
  - Polje window određuje broj segmenata koje pošiljaoc može da pošalje bez potvrde prijema (Ack)

KONTROLA TOKA (FLOW CONTROL)

Kontrola toka i Pouzdanost

- Window size definiše broj bajta , unutar ACK poruke, signalizirajući drugoj strani koliko bajta sam spreman da primim
- Uključen je u svakom TCP segmentu počev od three-way handshake komunikacije
- TCP je full duplex servis
  - Klijent i server nezavisno određuju svoj window size.

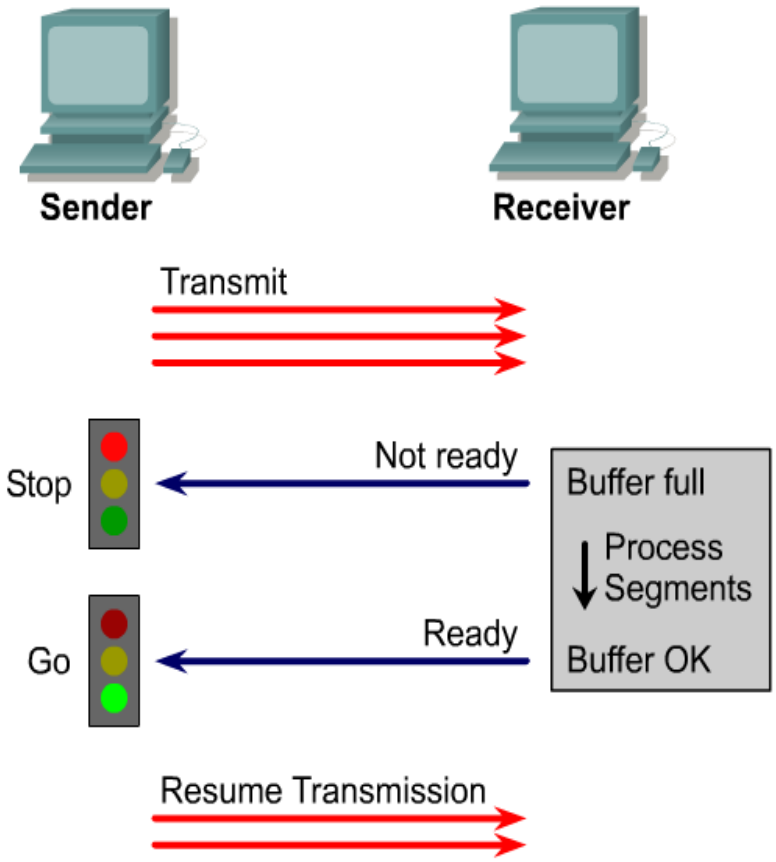


KLIZAJUĆI PROZORI (SLIDING WINDOWS)

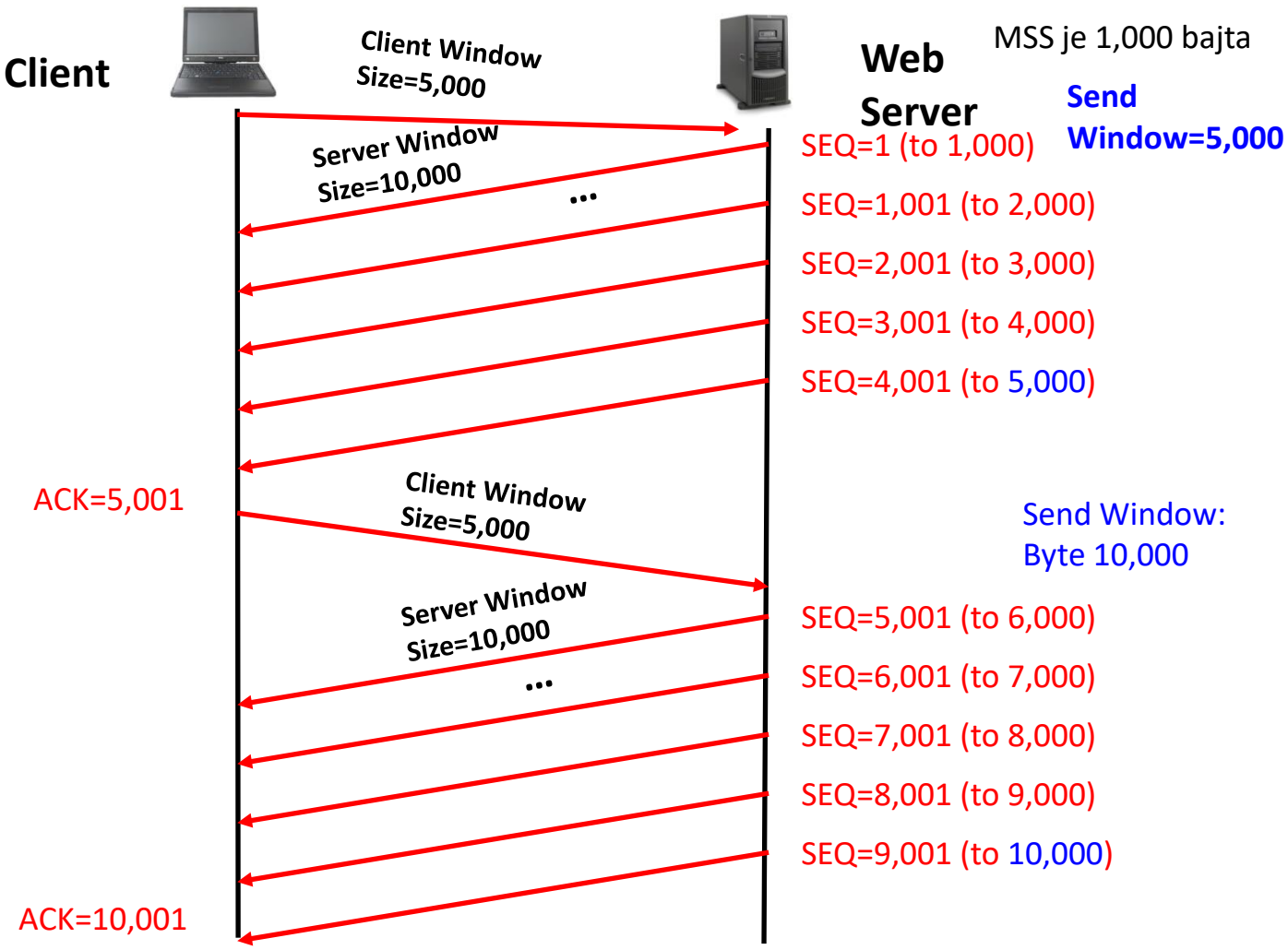
TCP implementira kontrolu toka povećavajući / smanjujući veličinu prozora.

- Window size se menja tokom trajanja konekcije.

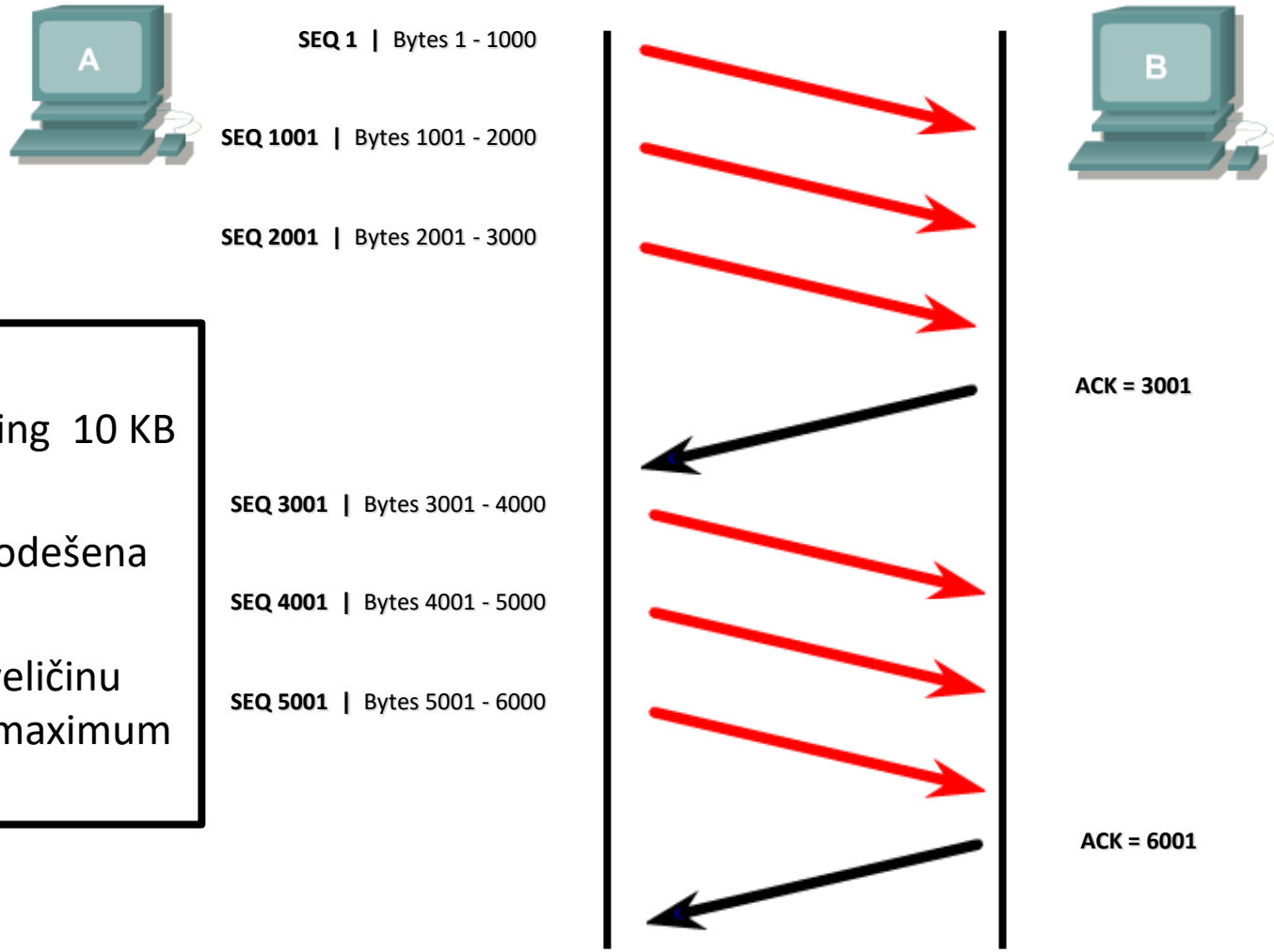
Da se segment ne bi odbacio na prijemnoj strani, indikator u vidu veličine prozora primlac šalje pošiljaocu da uspori (**Flow control)**.



KONTROLA TOKA (FLOW CONTROL)



KONTROLA TOKA (FLOW CONTROL)



Host B downloading 10 KB fajl sa Hosta A.

Window size je podešena na 3 KB.

Host B uzima za veličinu segmenta 1 KB (maximum segment size).

UPRAVLJANJE TCP KONEKCIJOM