

TCP/IP Arhitektura

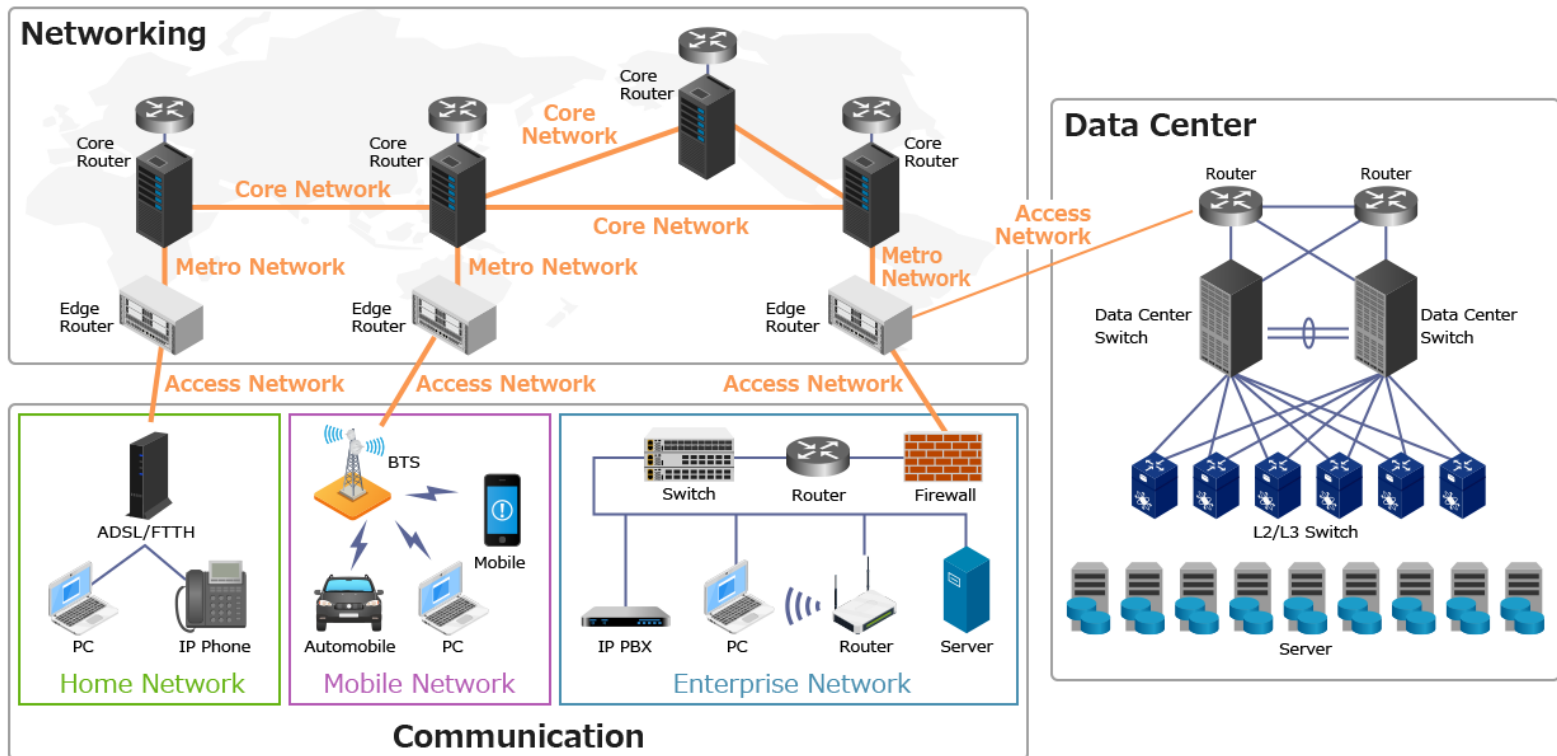
Predmet: Bezbednost Aplikacija

Predavač: dr Dušan Stefanović

Mrežna infrastruktura

Mrežnu infrastrukturu čine:

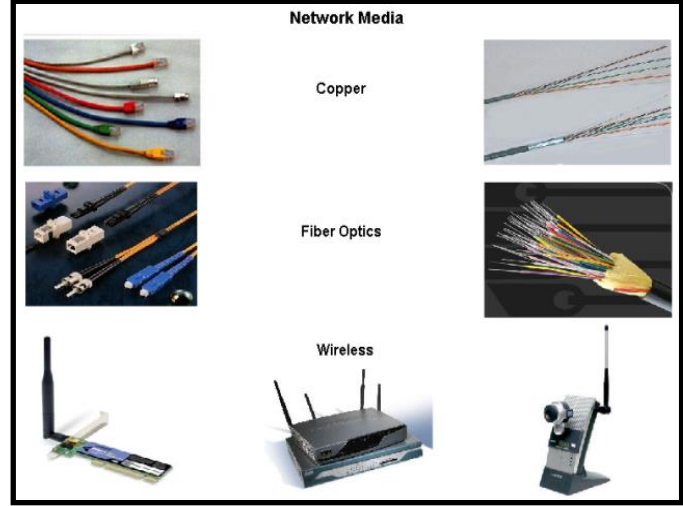
- Uređaji
- Medijum
- Servisi



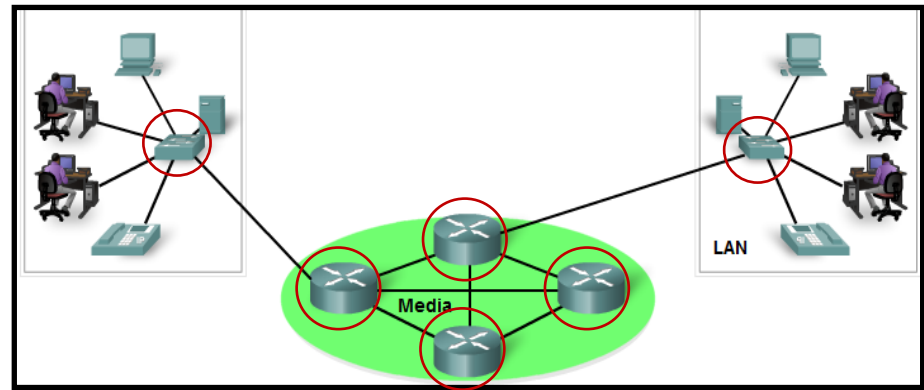
Komponente mrežne infrastrukture



Krajnji uređaji



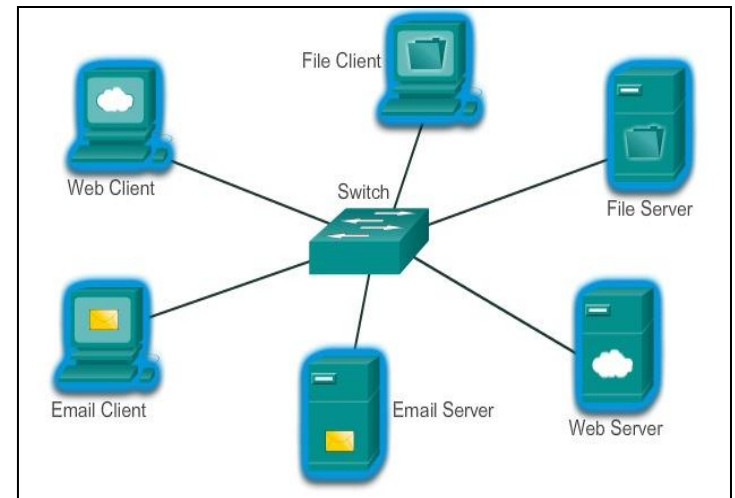
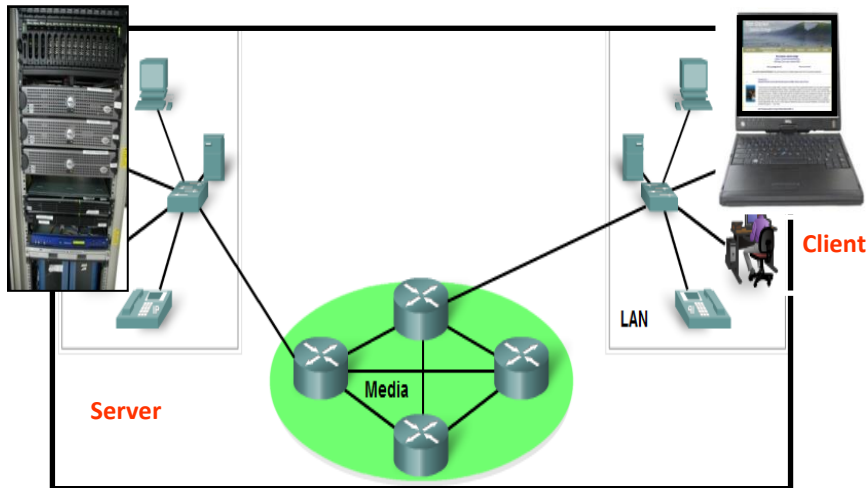
Prenosni medijumi



Aktivni mrežni uređaji

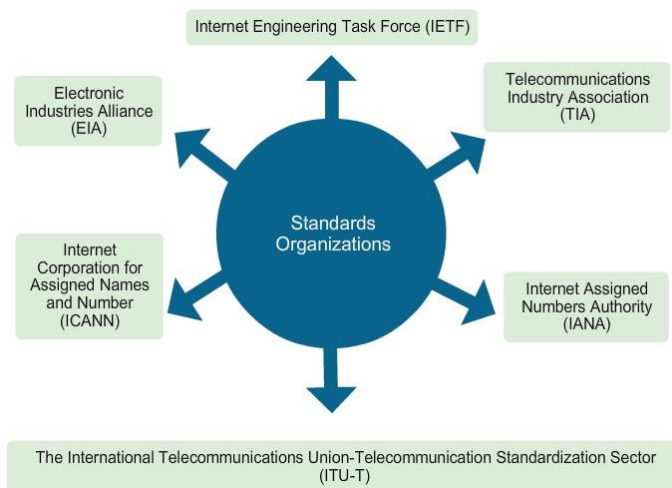
Server – Klijent Komunikacija

- 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

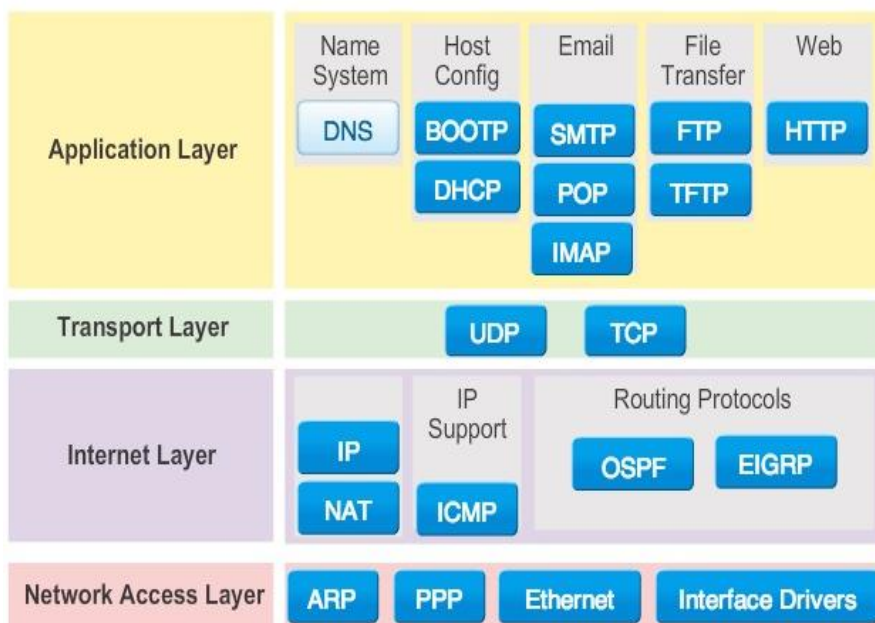


ORGANIZACIJE ZA STANDARDIZACIJU

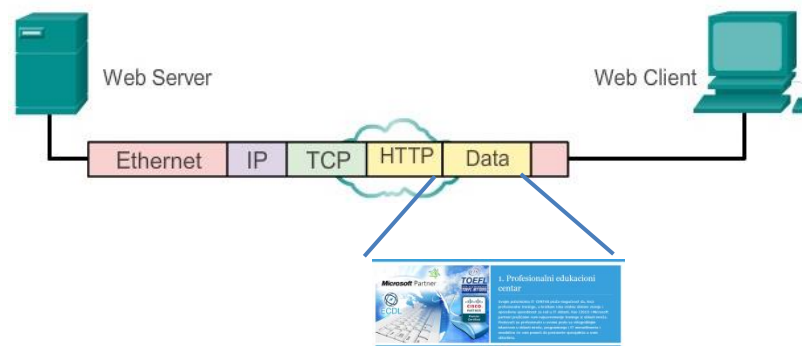
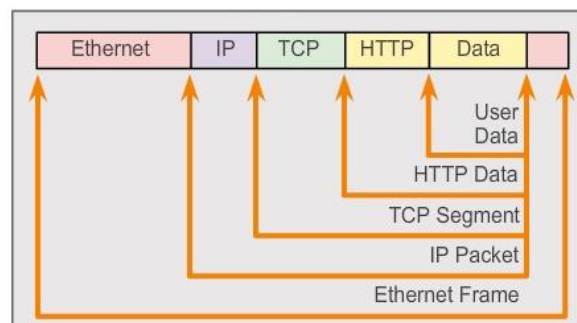
- Industrijski standard sprečava monopol jedne kompanije
- Ohrabruje i ubrzava razvoj tehnologije
- Organizacije za standardizaciju su:
 - The Internet Society (ISOC)
 - The Internet Architecture Board (IAB)
 - The Internet Engineering Task Force (IETF)
 - The Institute of Electrical and Electronics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



TCP/IP PROTOKOLSKI STEK

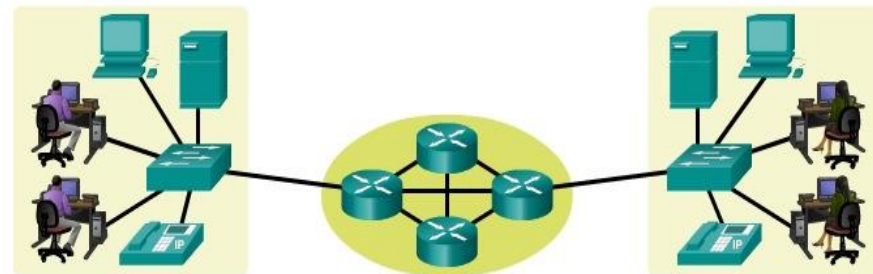


ENKAPSULACIJA PROTOKOLA



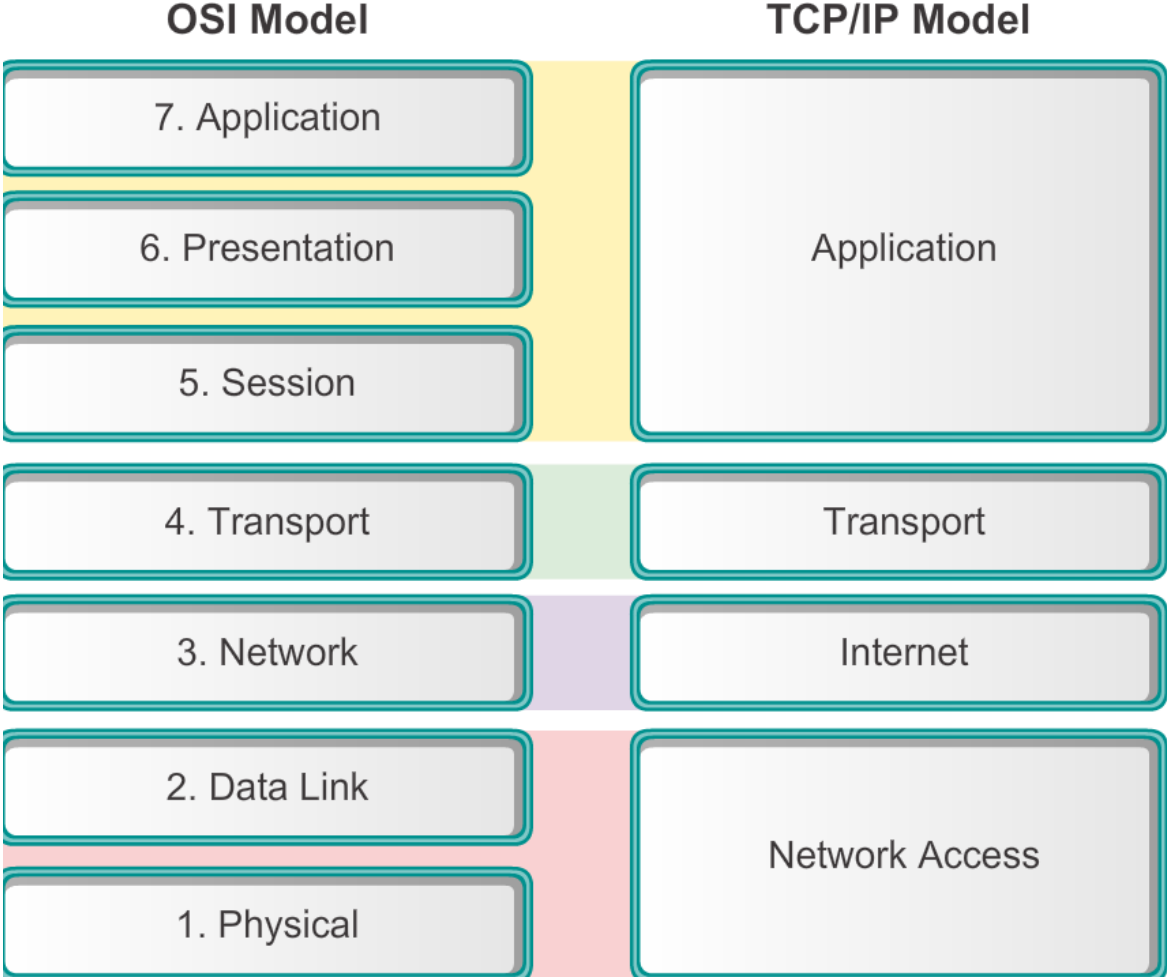
SLOJEVI U MREŽNOM MODELU

- 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

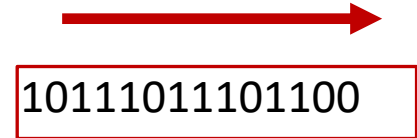
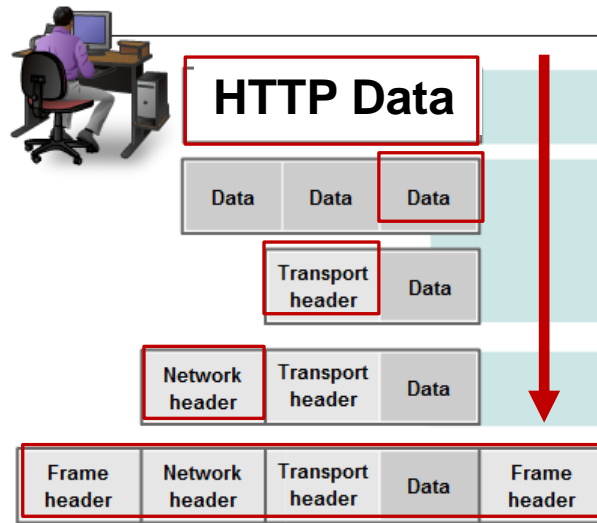


OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application	HTTP, DNS, DHCP, FTP	Application
Presentation		
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	PPP, Frame Relay, Ethernet	Network Access
Physical		

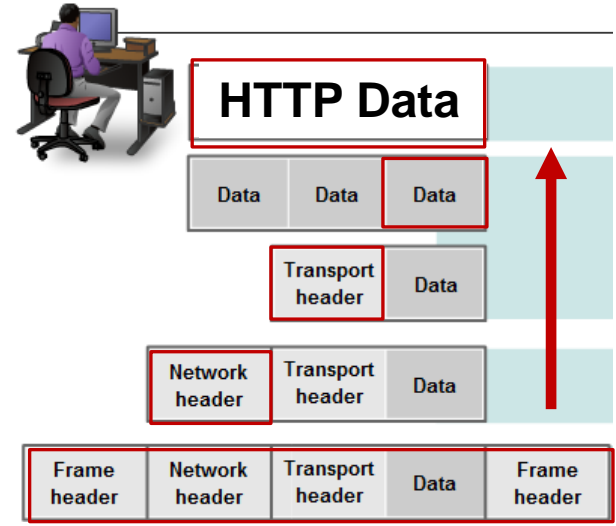
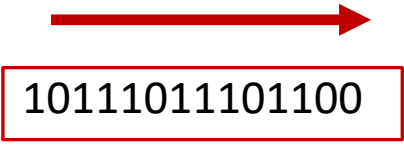
KOMPARACIJA OSI/TCP-IP MREŽNIH MODELA



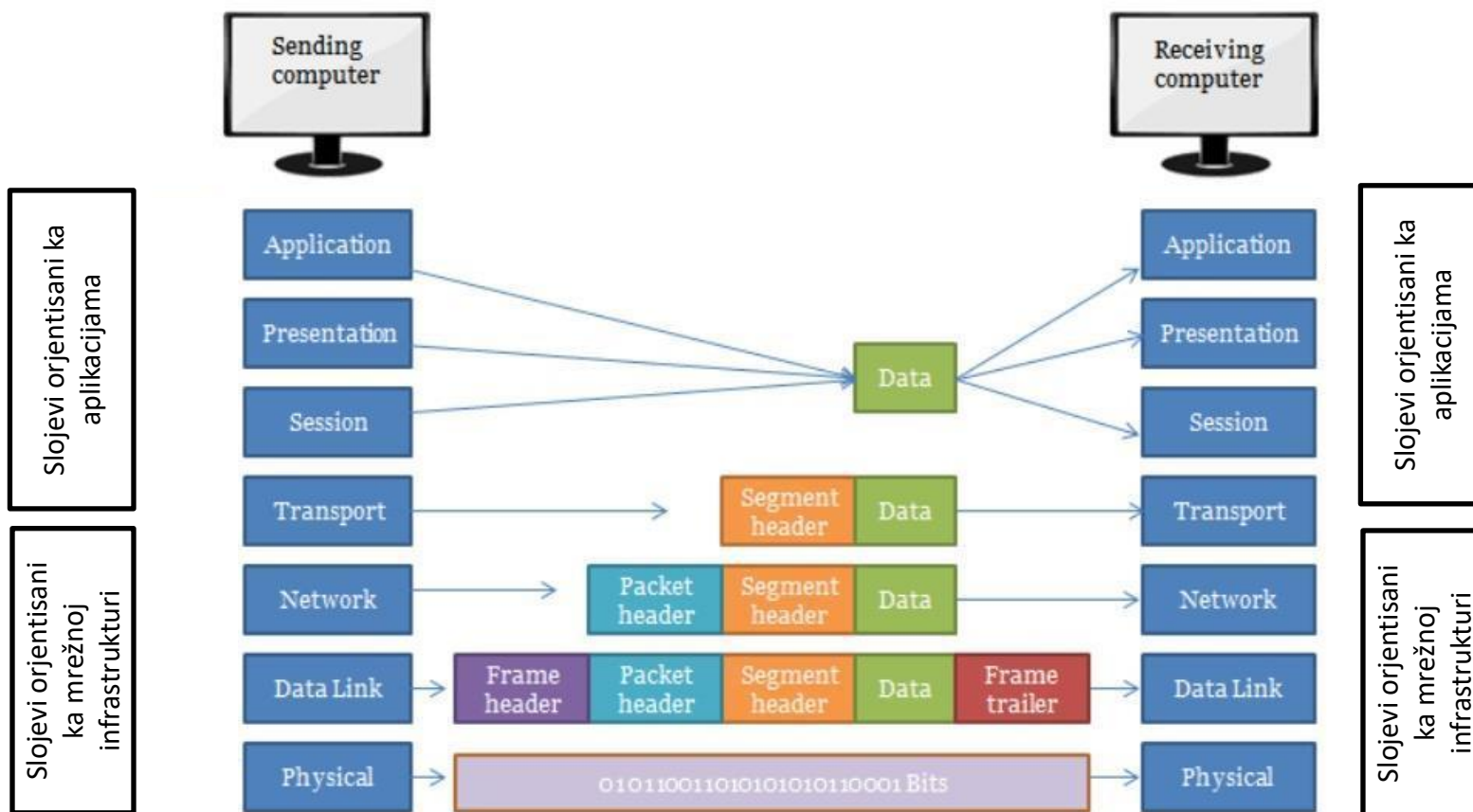
ENKAPSULACIJA PORUKE



DENKAPSULACIJA PORUKE



SLOJEVI TCP/IP MODELA ORJENTISANI KA APLIKACIJAMA

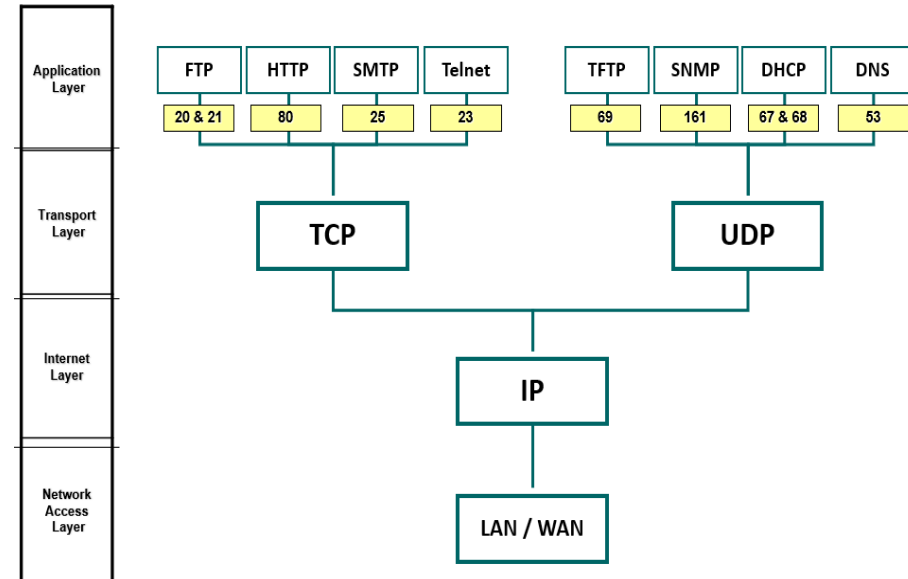
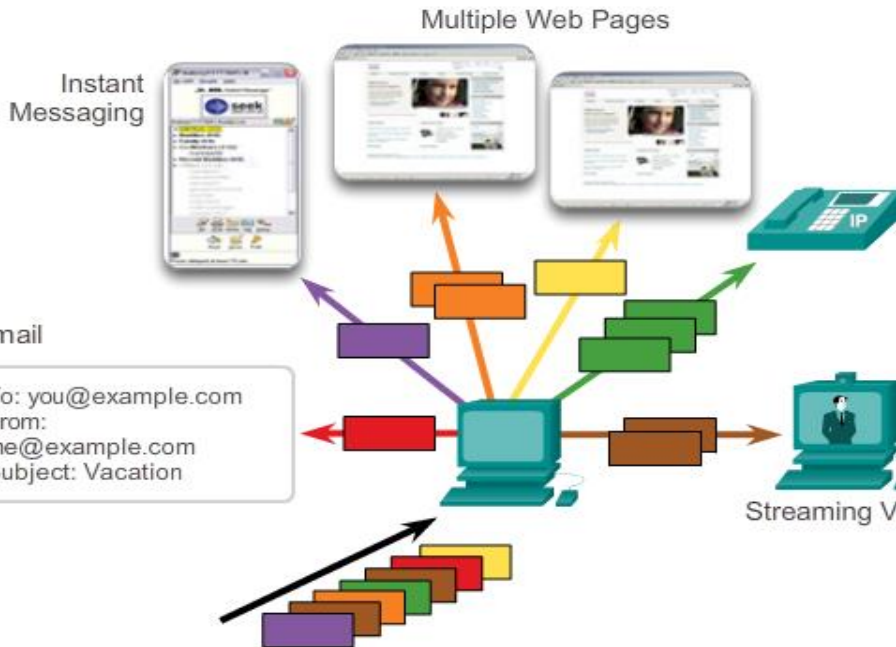


ULOGA PORTA - TRANSPORTNI SLOJ

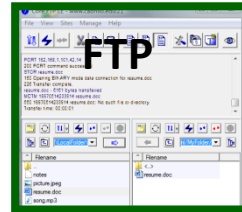
Svaki host u mreži može istovremeno da pokrene više aplikacija

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

Jedan klijent može da uspostavi više istovremenih konekcija sa različitim serverima



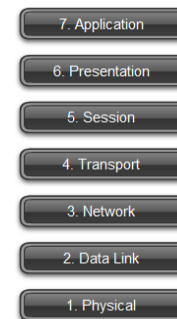
ULOGA PORTA - TRANSPORTNI SLOJ



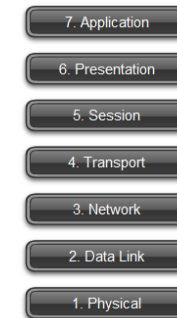
TCP
TCP
TCP
TCP

TCP
TCP

TCP
TCP



VTS Web Server



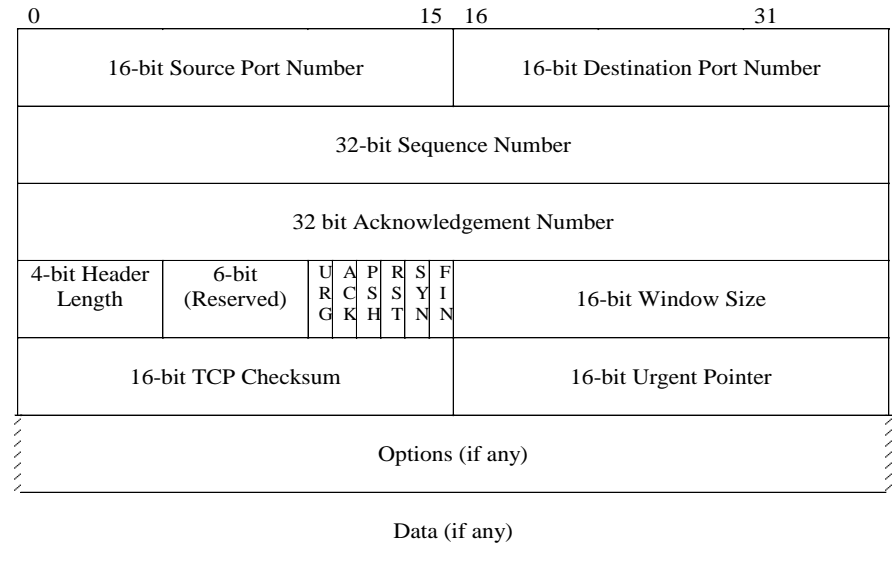
ISP Email i
FTP Server



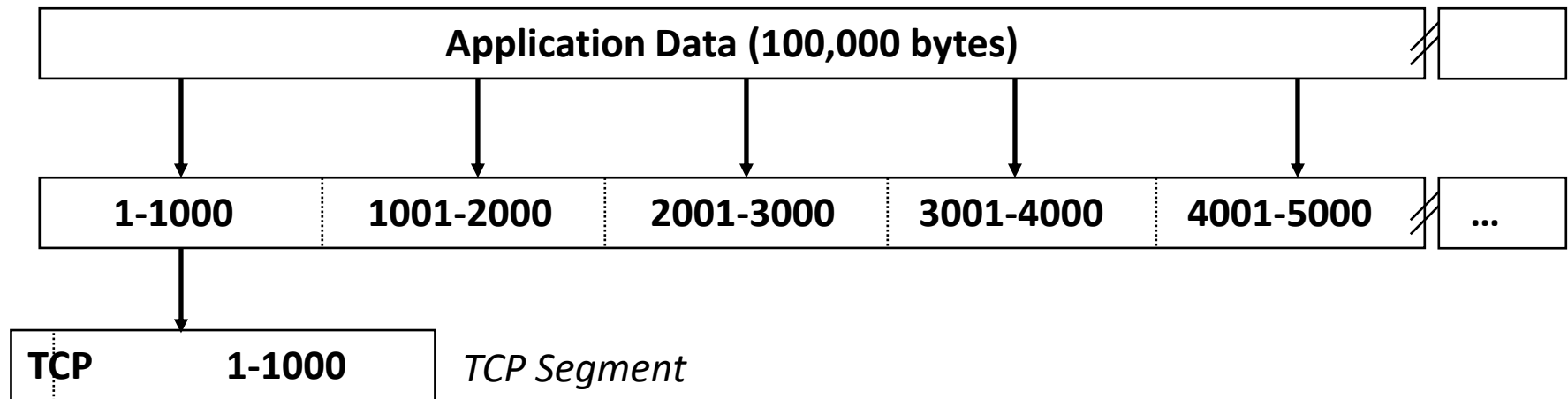
TCP SERVISI

TCP obezbeđuje sledeće servise:

- Pouzdana isporuka (**Reliable delivery**)
- Detekcija greške (**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)		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			

Source port: 49889 (49889)

Destination port: http (80)

[Stream index: 12]

Sequence number: 2457 (relative sequence number)

[Next sequence number: 3353 (relative sequence number)]

Acknowledgment number: 8167 (relative ack number)

Header length: 20 bytes

Flags: 0x018 (PSH, ACK)

window size value: 65520

[Calculated window size: 65520]

[window size scaling factor: -2 (no window scaling)]

Checksum: 0xfe88 [validation disabled]

[SEQ/ACK analysis]

Hypertext Transfer Protocol

Source Port (16 bita)

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

TCP SEGMENT U WIRESHARK-U

File Edit View Go Capture Analyze Statistics

Filter: http

No.	Time	Source
1010	9.73430700	173.37.145.8
1012	9.79521200	192.168.1.116
1016	9.84428000	66.117.23.100
1017	10.0038130	fe80::15ff:98d8

Frame 1012: 950 bytes on wire (7600 bytes captured) on interface eth0
Ethernet II, Src: IntelCor_45:53:00:14:00:00, Dst: IntelCor_45:53:00:14:00:00
Internet Protocol Version 4, Src: 192.168.1.116, Dst: 192.168.1.100
Transmission Control Protocol, Src port: 49889 (49889), Dst port: http (80)
[Stream index: 12]
Sequence number: 2457 (relative sequence number)
[Next sequence number: 3353 (relative sequence number)]
Acknowledgment number: 8167 (relative ack number)
Header length: 20 bytes
Flags: 0x018 (PSH, ACK)
window size value: 65520
[Calculated window size: 65520]
[window size scaling factor: 1]
Checksum: 0xfe88 [validation failed]
[SEQ/ACK analysis]
Hypertext Transfer Protocol

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			

Destination Port (16 bita)

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

TCP SEGMENT U WIRESHARK-U

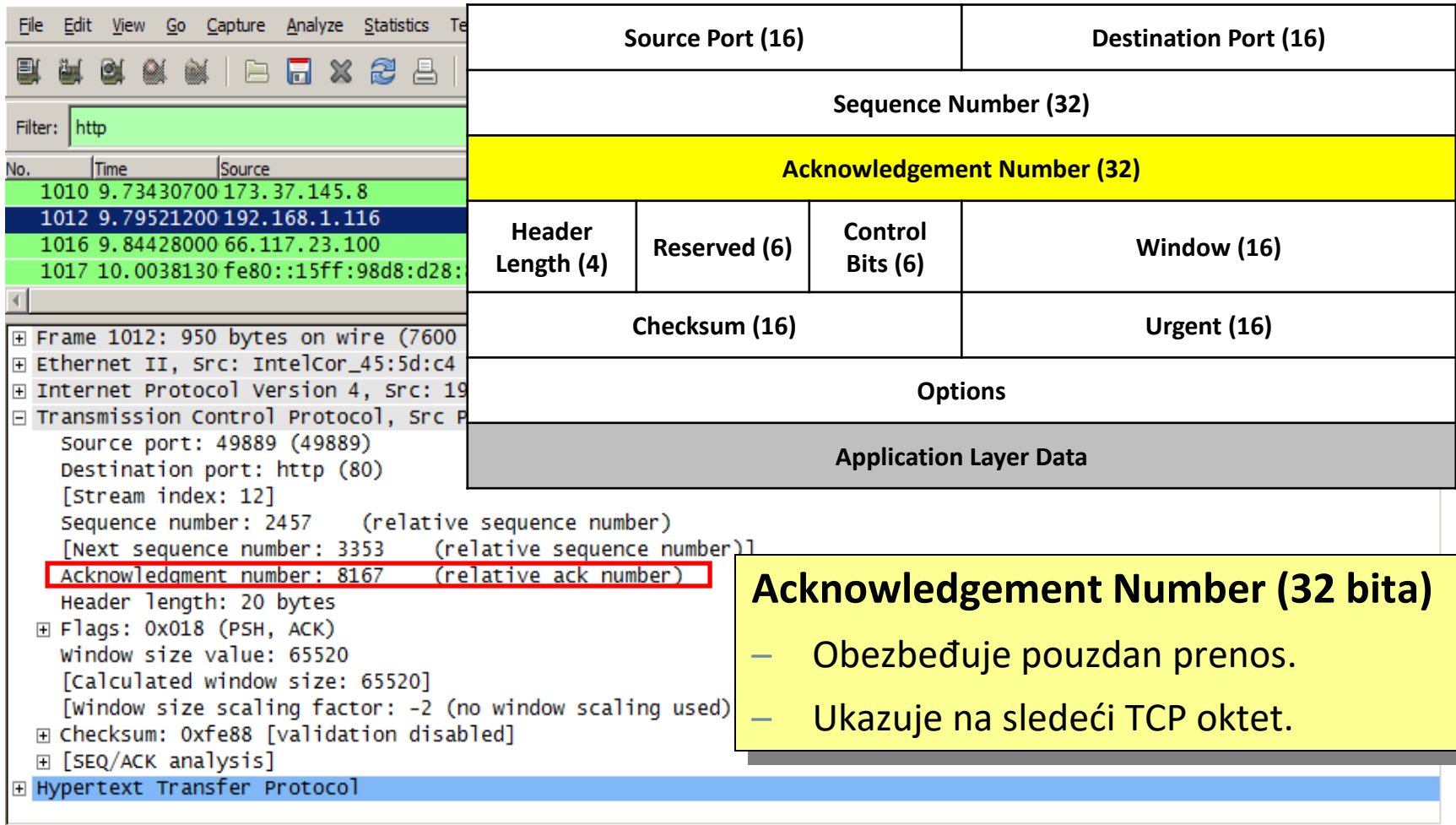
Source Port (16)		Destination Port (16)	
Sequence Number (32)			
Acknowledgement Number (32)			
Header Length (4)	Reserved (6)	Control Bits (6)	Window (16)
Checksum (16)		Urgent (16)	
Options			
Application Layer Data			

Sequence number: 2457 (relative sequence number)
[Next sequence number: 3353 (relative sequence number)]
Acknowledgment number: 8167 (relative ack number)
Header length: 20 bytes
Flags: 0x018 (PSH, ACK)
Window size value: 65520
[Calculated window size: 65520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0xfe88 [validation disabled]
[SEQ/ACK analysis]

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			

Filter: http

No.	Time	Source
1010	9.73430700	173.37.145.8
1012	9.79521200	192.168.1.116
1016	9.84428000	66.117.23.100
1017	10.0038130	fe80::15ff:98d8:d28:

Frame 1012: 950 bytes on wire (7600 bytes captured) on interface eth0

- Ethernet II, Src: IntelCor_45:5d:c4:00:00:00, Dst: 02:00:0c:00:00:00
- Internet Protocol Version 4, Src: 192.168.1.116, Dst: 173.37.145.8
- Transmission Control Protocol, Src Port: 49889, Dst Port: http (80)
 - Stream index: 12
 - Sequence number: 2457 (relative sequence number)
 - Next sequence number: 3353 (relative sequence number)
 - Acknowledgment number: 8167 (relative ack number)**
 - Header length: 20 bytes
 - Flags: 0x018 (PSH, ACK)
 - Window size value: 65520 [Calculated window size: 65520] [window size scaling factor: -2 (no window scaling used)]
 - Checksum: 0xfe88 [validation disabled]
 - [SEQ/ACK analysis]
- Hypertext Transfer Protocol

Acknowledgement Number (32 bita)

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

TCP SEGMENT U WIRESHARK-U

The image shows a Wireshark capture of a network packet. The packet list pane shows several packets, with packet 1012 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol version 4, and Transmission Control Protocol. The TCP header fields are expanded, showing source and destination ports, sequence and acknowledgment numbers, and flags. The 'Header length' field is highlighted in red in the details pane, indicating its value of 20 bytes. A yellow callout box with the text 'Header Length (4 bita)' and 'Ukazuje na dužinu TCP zaglavlja u segmentu' points to the 'Header Length (4)' field in the diagram above.

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			

Source port: 49889 (49889)
Destination port: http (80)
[Stream index: 12]
Sequence number: 2457 (relative sequence number)
[Next sequence number: 3353 (relative sequence number)]
Acknowledgment number: 8167 (relative ack number)
Header length: 20 bytes

Flags: 0x018 (PSH, ACK)
window size value: 65520
[Calculated window size: 65520]
[window size scaling factor: -2 ()]
checksum: 0xfe88 [validation disabled]
[SEQ/ACK analysis]

Hypertext Transfer Protocol

Header Length (4 bita)
— Ukazuje na dužinu TCP zaglavlja u segmentu

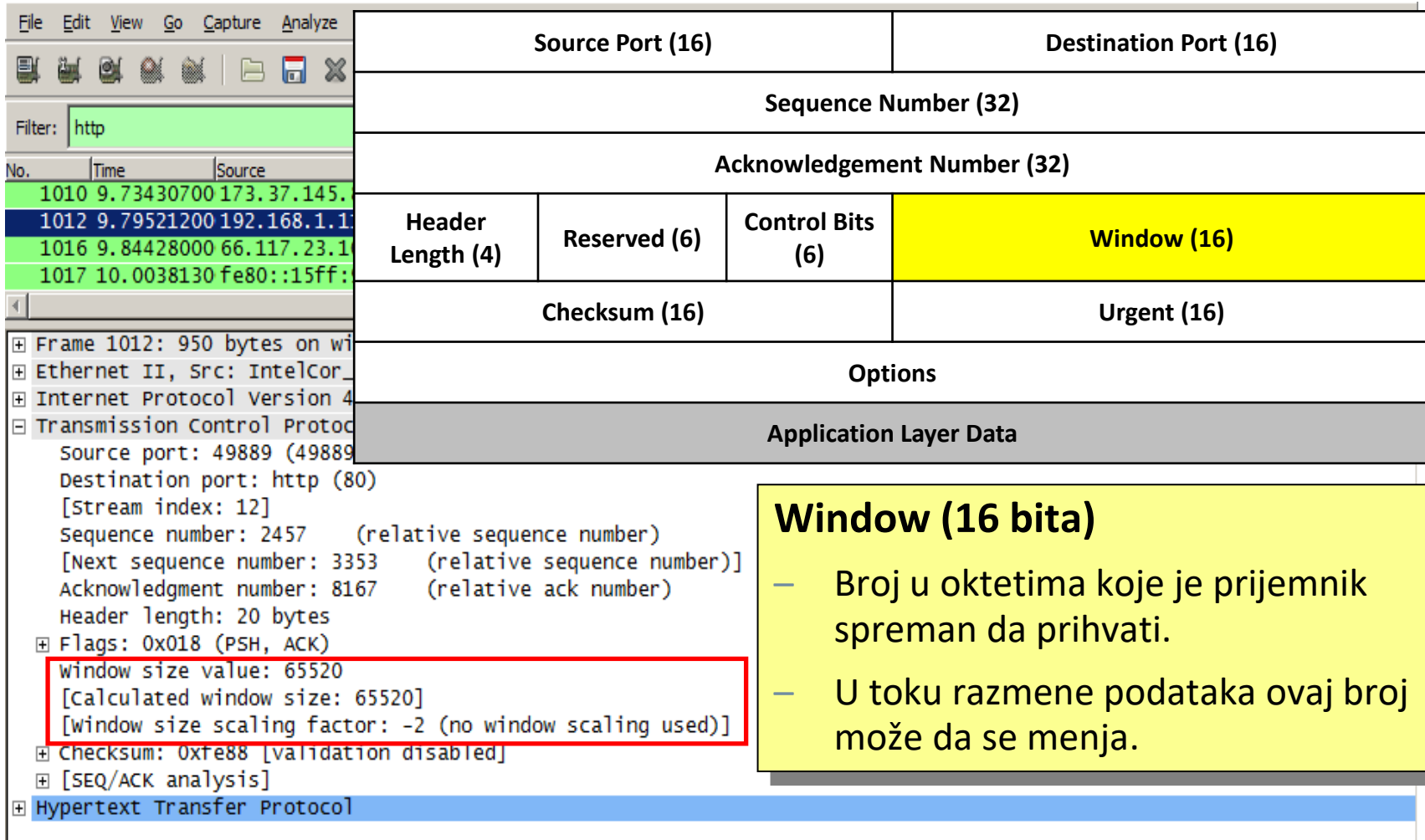
TCP SEGMENT U WIRESHARK-U

Wireshark interface showing a packet capture of an HTTP request. The packet list shows packet 1012 selected. The packet details pane shows the TCP segment structure with fields like Source Port, Destination Port, Sequence Number, Acknowledgement Number, Header Length, Reserved, Control Bits, Window, Checksum, Urgent, Options, and Application Layer Data. The Control Bits field is highlighted in yellow. A callout box explains that the Control Bits (Flags) indicate the type of TCP segment (Syn, Ack, Fin, etc.).

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			

Control Bits (Flags) (6 bita)
– Ukazuje na tip(Syn, Ack, Fin,...) TCP segmenta.

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			

Filter: http

No.	Time	Source
1010	9.73430700	173.37.145.
1012	9.79521200	192.168.1.1
1016	9.84428000	66.117.23.1
1017	10.0038130	fe80::15ff:

Frame 1012: 950 bytes on wire (7600 bytes captured) on interface eth0
Ethernet II, Src: IntelCor_08:00:00:08:00:08, Dst: 192.168.1.1
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.1
Transmission Control Protocol, Src Port: 49889, Dst Port: http (80)
Source port: 49889 (49889)
Destination port: http (80)
[Stream index: 12]
Sequence number: 2457 (relative sequence number)
[Next sequence number: 3353 (relative sequence number)]
Acknowledgment number: 8167 (relative ack number)
Header length: 20 bytes
Flags: 0x018 (PSH, ACK)
window size value: 65520
[Calculated window size: 65520]
[window size scaling factor: -2 (no window scaling used)]
Checksum: 0xfe88 [validation disabled]
[SEQ/ACK analysis]
Hypertext Transfer Protocol

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 ili Registered Port Number



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 Ports (Brojevi od 0 do 1023)

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



REGISTROVANI PORTOVI

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

Registered TCP Ports:

1863 MSN Messenger
8008 Alternate HTTP
8080 Alternate HTTP

Registered UDP Ports:

1812 RADIUS Authentication Protocol
2000 Cisco SCCP (VoIP)
5004 RTP (Voice and Video Transport Protocol)
5060 SIP (VoIP)

Registered TCP/UDP Common Ports:

1433 MS SQL
2948 WAP (MMS)

Well Known TCP Ports

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

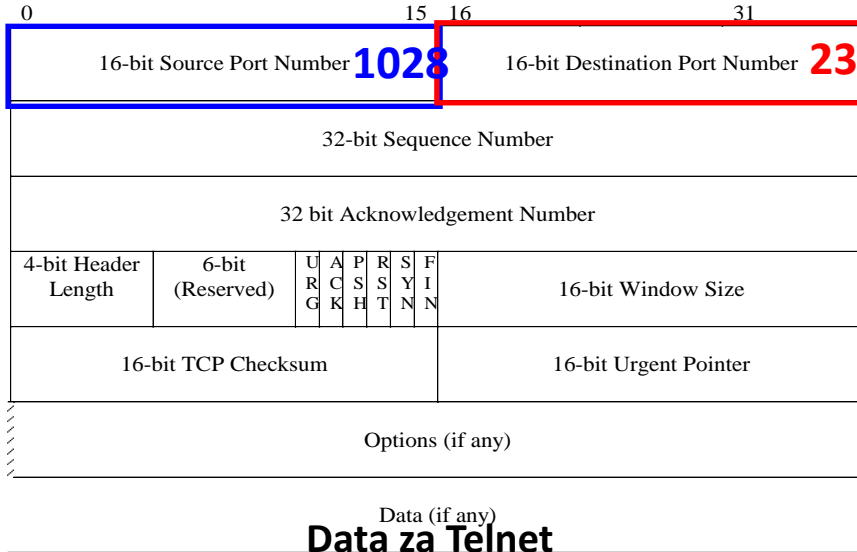
Well Known TCP/UDP Common Ports:

53 DNS
161 SNMP
531 AOL Instant Messenger, IRC

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

PRIMER DODELE PORTA APLIKACIJI

Client TCP Header



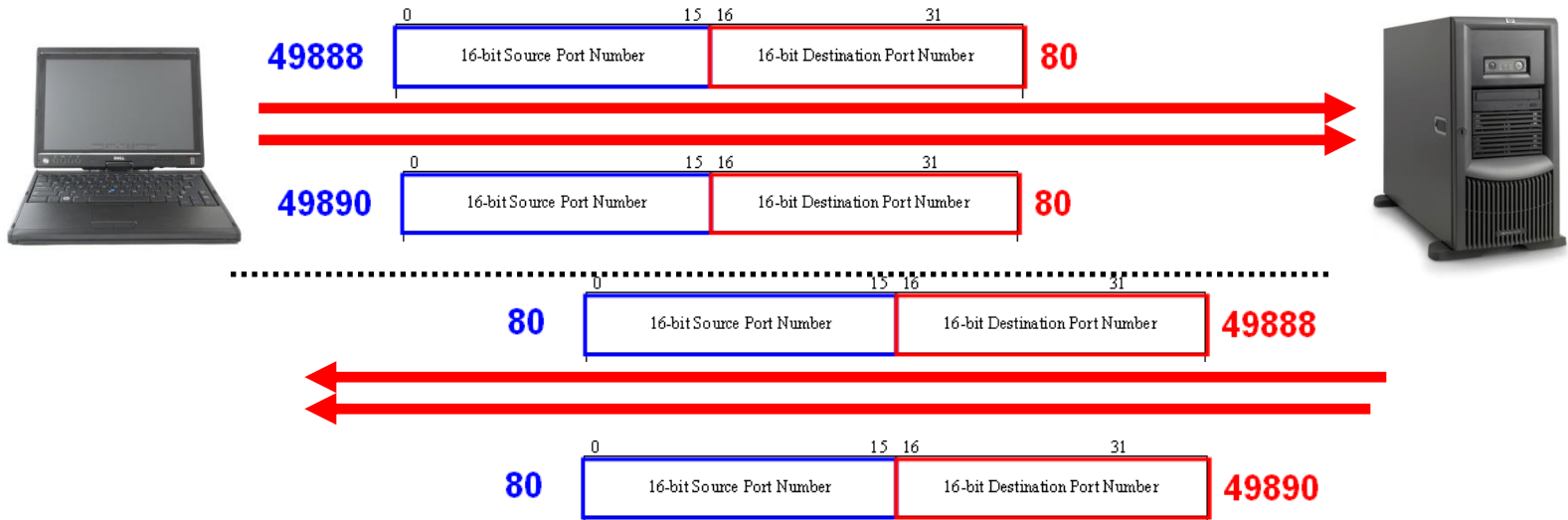
- Klijent šalje TCP segment:
 - Destination Port: 23 (Well known port)
 - Source Port: 1028 (Dynamic Port koji zadaje klijent)

Klijent

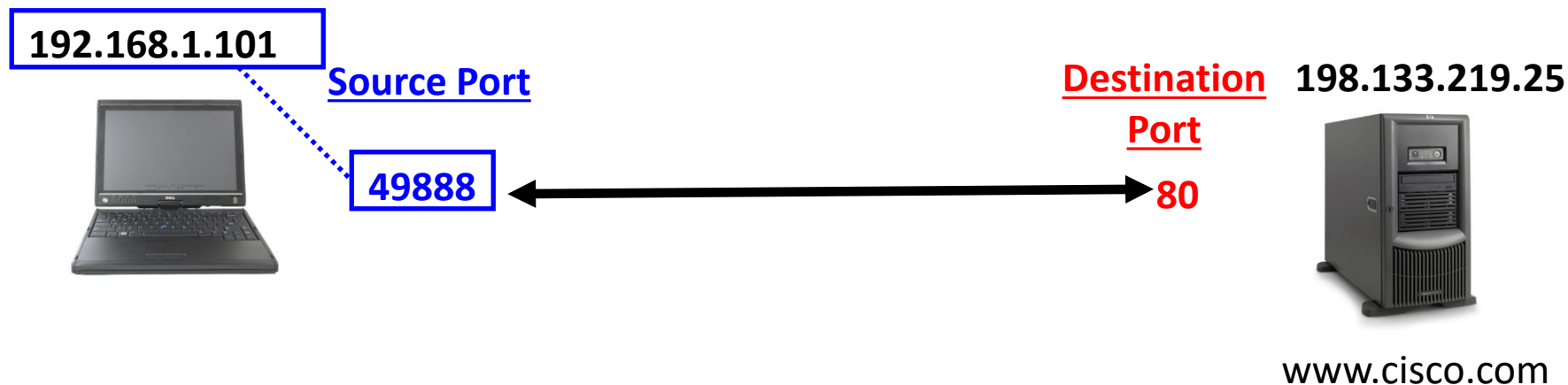


Server

USPOSTAVLJANJE VIŠE SESIJA

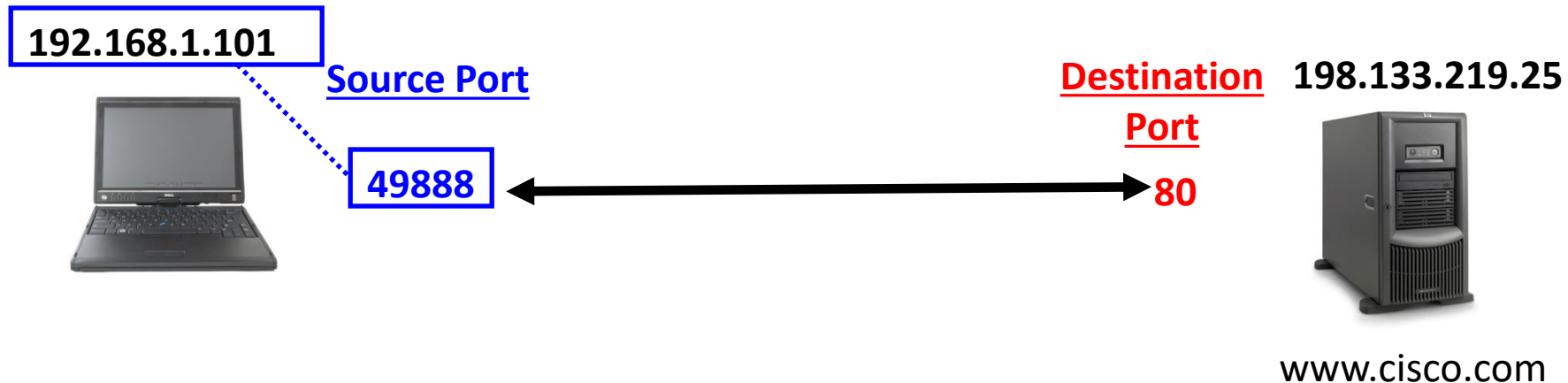


SOCKET



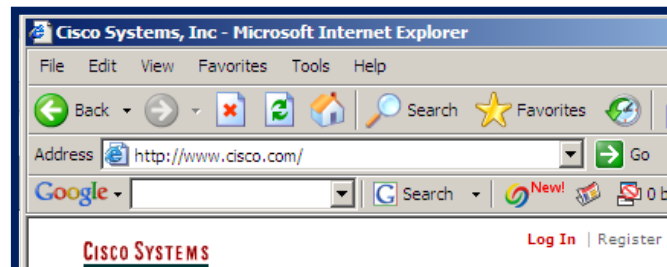
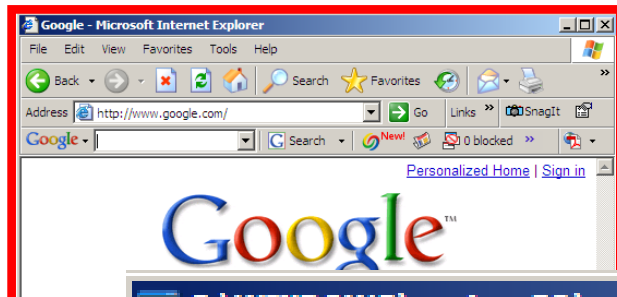
- Kombinovanjem broja porta na transportnom sloju i IP adrese na mrežnom sloju se na jedinstven način identifikuje konekcija (aplikacija) koja se izvršava
 - Kombinacija IP adrese i broja porta zove se **socket**.
- Komunikacija(flow) između dve aplikacije se na jedinstven način identifikuje koristeći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



TCP
ili
UDP

```
G:\WINDOWS\system32\cmd.exe
C:\>netstat -n
```

	Source IP	Source Port	Destination IP	Destination Port	Connection State
Active Connections					
Proto	Local Address		Foreign Address		State
TCP	172.17.150.112:1033		172.16.1.44:524		ESTABLISHED
TCP	172.17.150.112:1034		172.16.1.44:524		ESTABLISHED
TCP	172.17.150.112:1042		205.188.9.73:5190		ESTABLISHED
TCP	172.17.150.112:1050		64.12.165.95:5190		ESTABLISHED
TCP	172.17.150.112:1069		207.62.185.140:143		ESTABLISHED
TCP	172.17.150.112:1332		198.133.219.25:80		TIME_WAIT
TCP	172.17.150.112:1333		198.133.219.25:80		ESTABLISHED
TCP	172.17.150.112:1334		198.133.219.25:80		ESTABLISHED
TCP	172.17.150.112:1335		64.154.80.254:80		ESTABLISHED
TCP	172.17.150.112:1336		66.102.7.99:80		ESTABLISHED

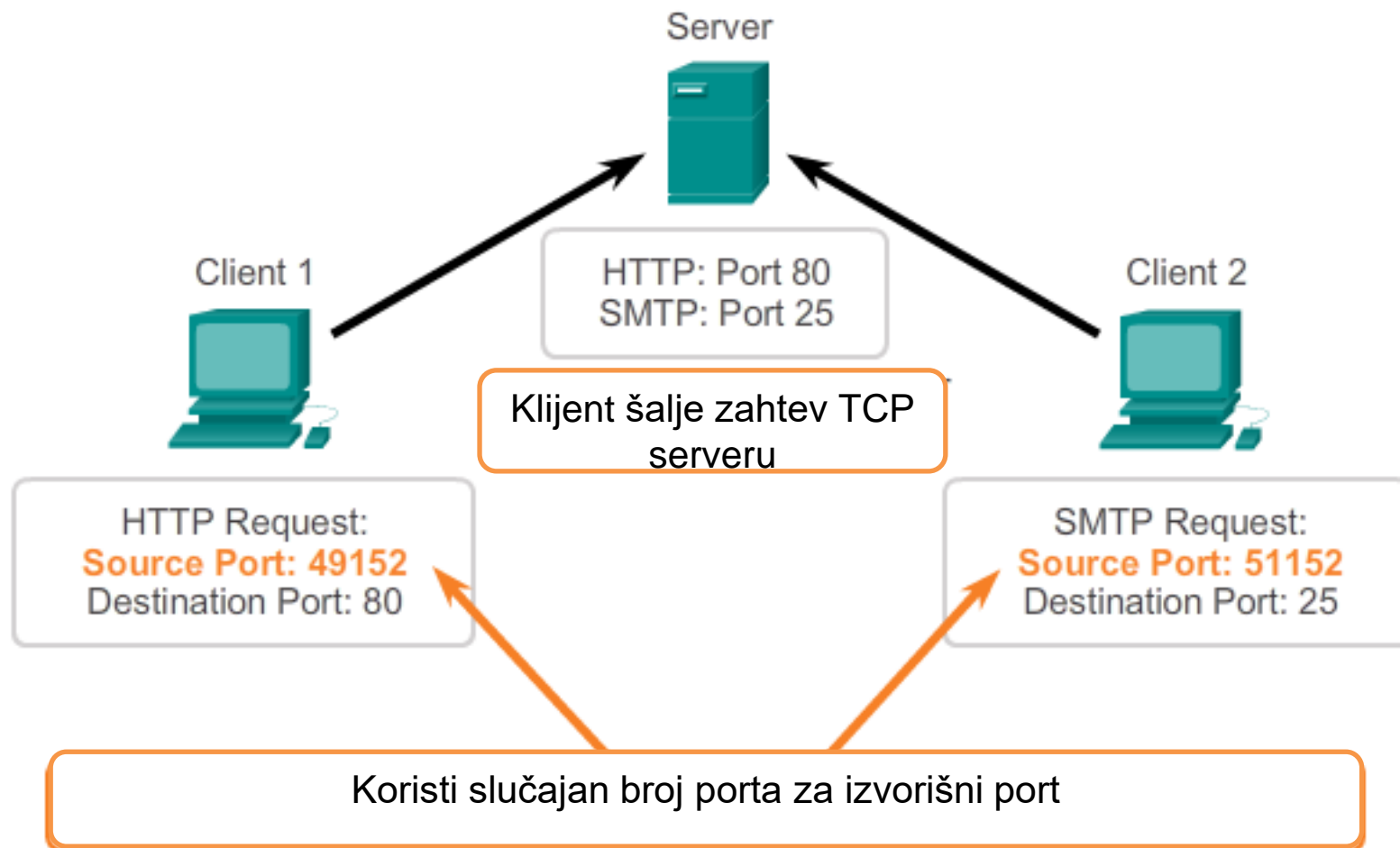
- **Napomena:** Kada učitavamo web stranu i njene objekte obično se uspostavljaju nekoliko TCP sesije.

USPOSTAVLJANJE SESIJE

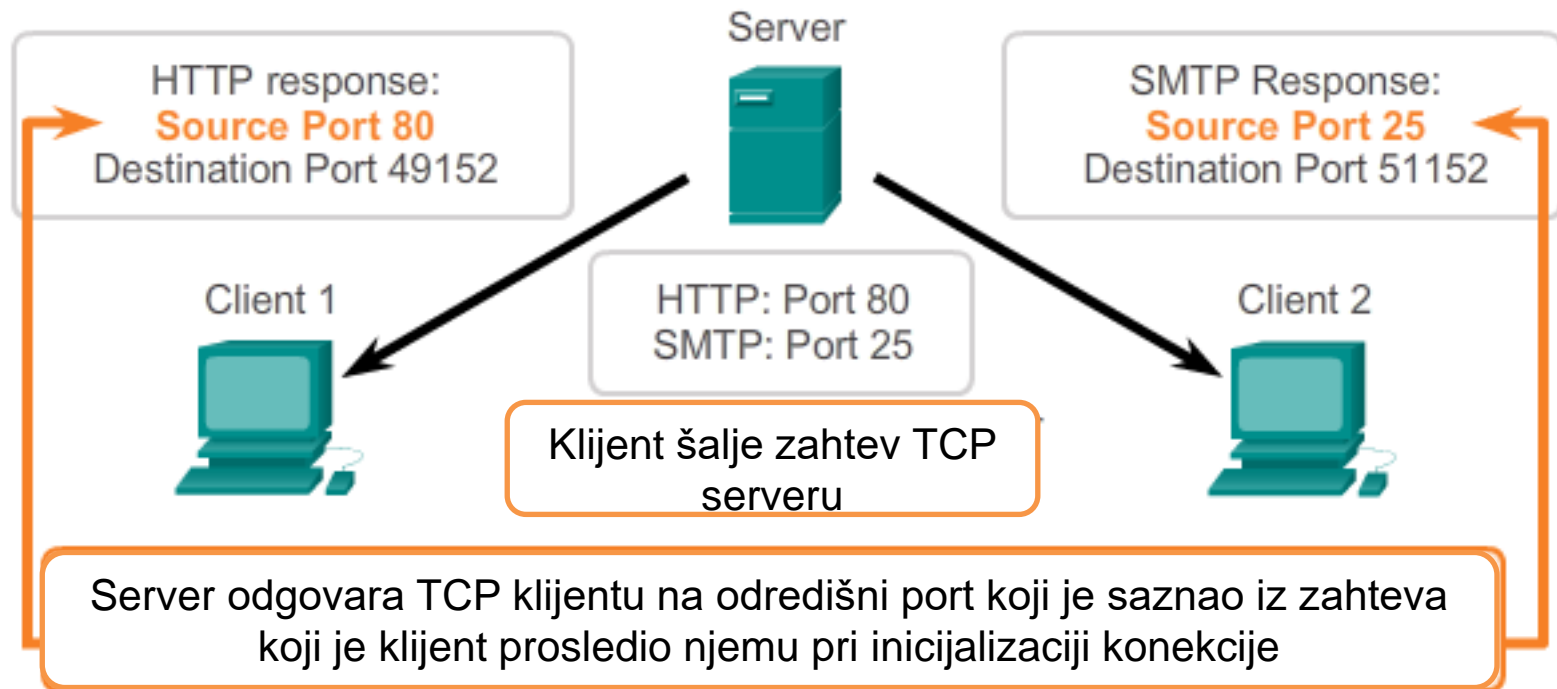
Uspostavljanje sesije (establishing session) obezbeđuje da je aplikacija spremna da šalje i prima podatke



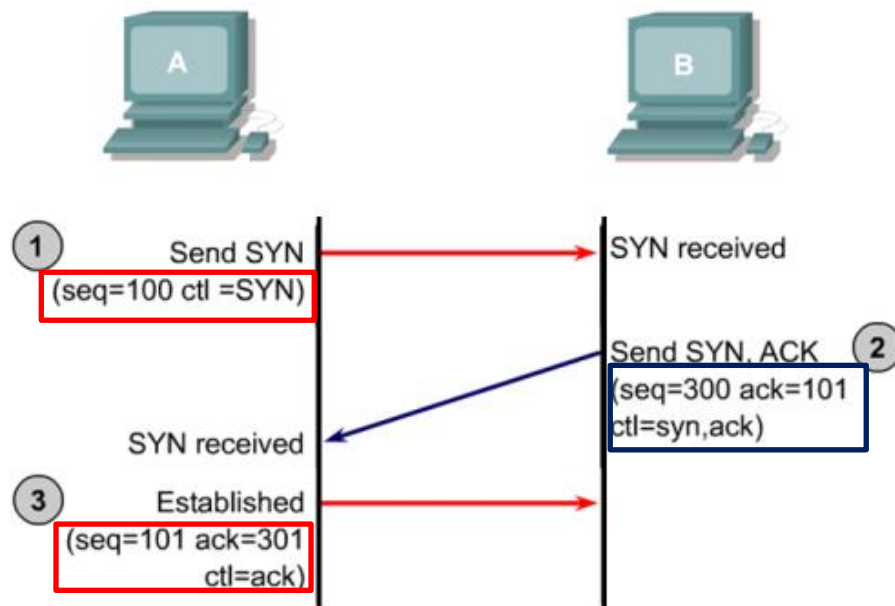
USPOSTAVLJENJE KONEKCIJE



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

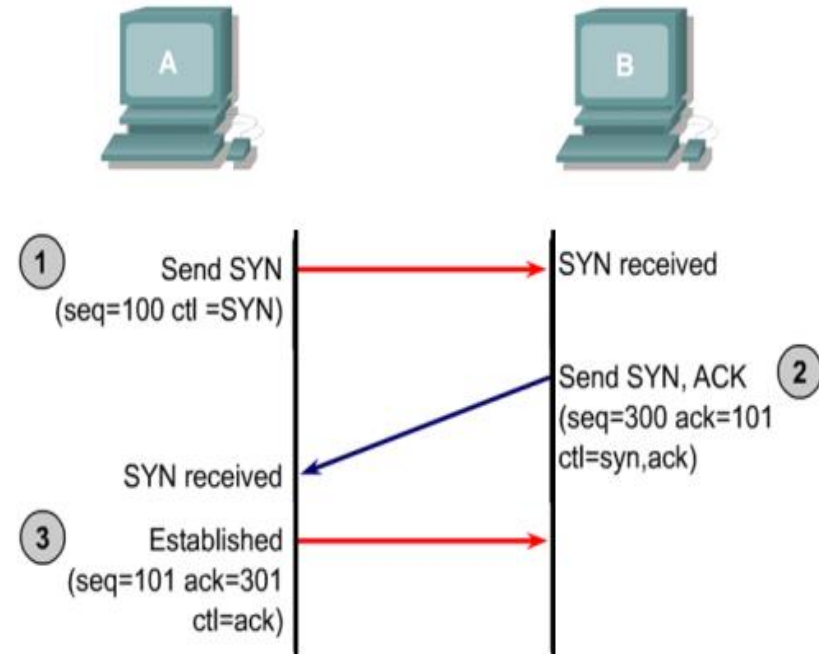
USPOSTAVLJENJE KONEKCIJE

Three-way handshake procedura:

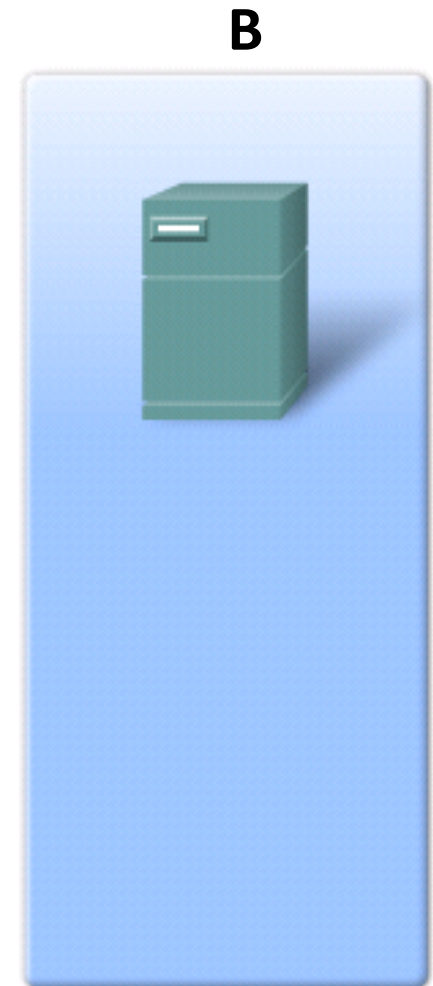
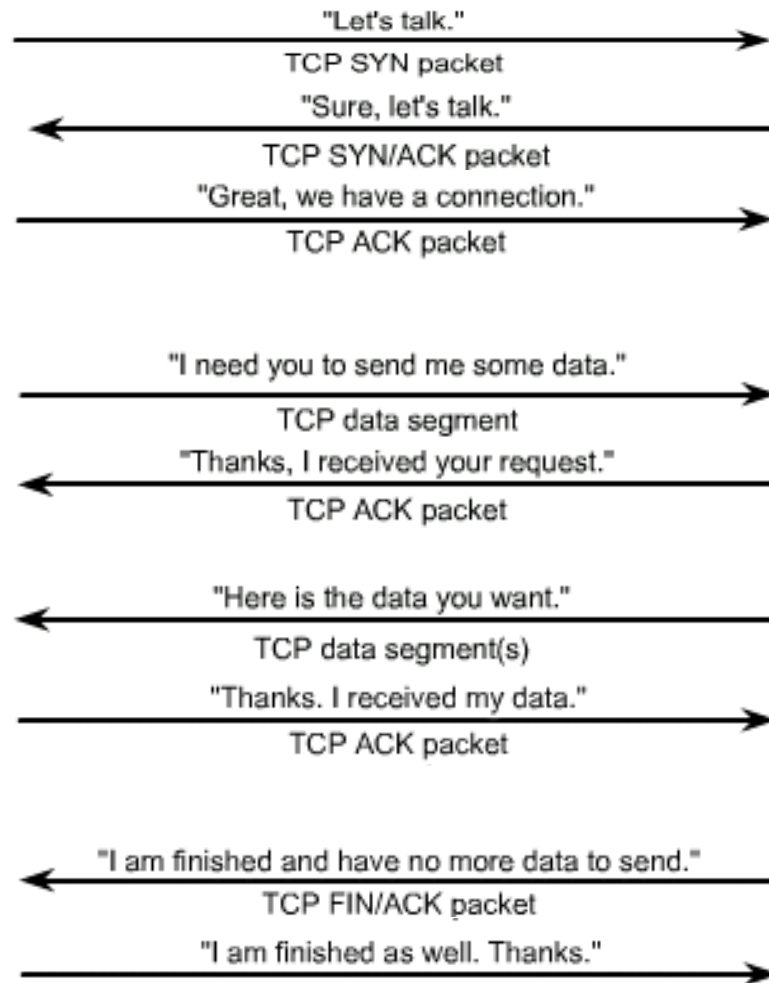
Utvrdjuje prisustvo odredišnog računara u mreži.

Utvrdjuje 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

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			

Control Bits (Flags) (6 bita)

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

Wireshark details for packet 1012:

- Source port: 49889 (49889)
- Destination port: http
- [Stream index: 12]
- Sequence number: 2457 (relative sequence number)
- [Next sequence number: 3353]
- Acknowledgment number: 8167
- Header length: 20 bytes
- Flags: 0x018 (PSH, ACK)
- window size value: 65520
- [Calculated window size: 65520]
- [window size scaling factor: -2]
- Checksum: 0xfe88 [validation disabled]
- [SEQ/ACK analysis]
- Hypertext Transfer Protocol

TCP FLAGS

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

```
Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
... 0... = Congestion window Reduced (CWR): Not set
... .0.. = ECN-Echo: Not set
... ..0. = Urgent: Not set
... ...0 = Acknowledgment: Not set
... .... 0... = Push: Not set
... ..0.. = Reset: Not set
+ ... ..1. = Syn: Set
... ..0 = Fin: Not set
```

- 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).

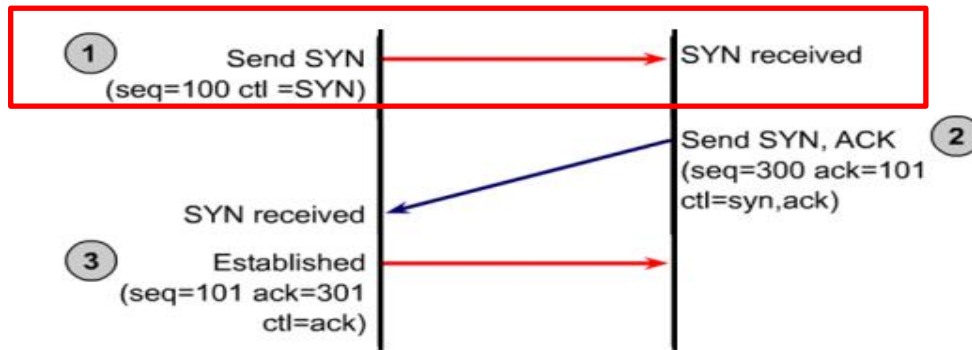
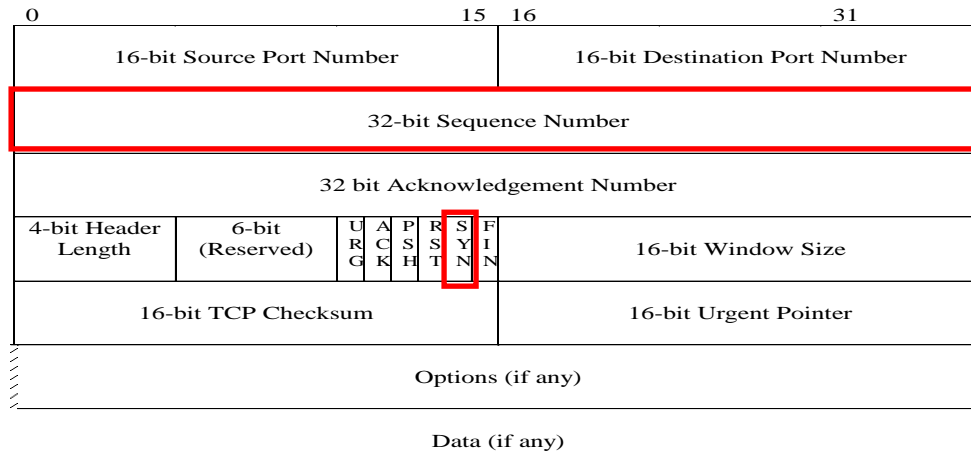
USPOSTAVLJENJE KONEKCIJE

- 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

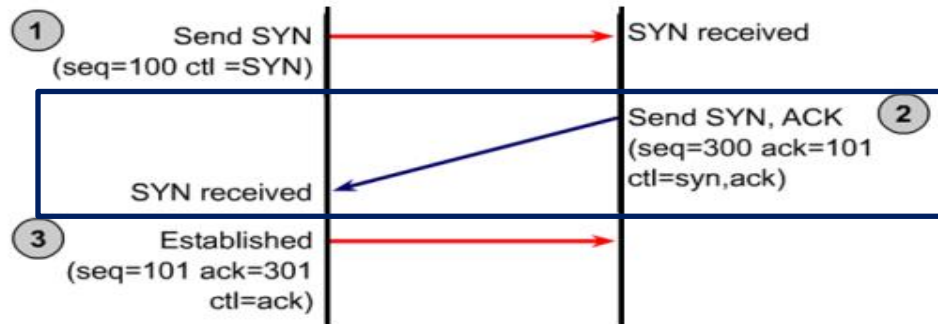
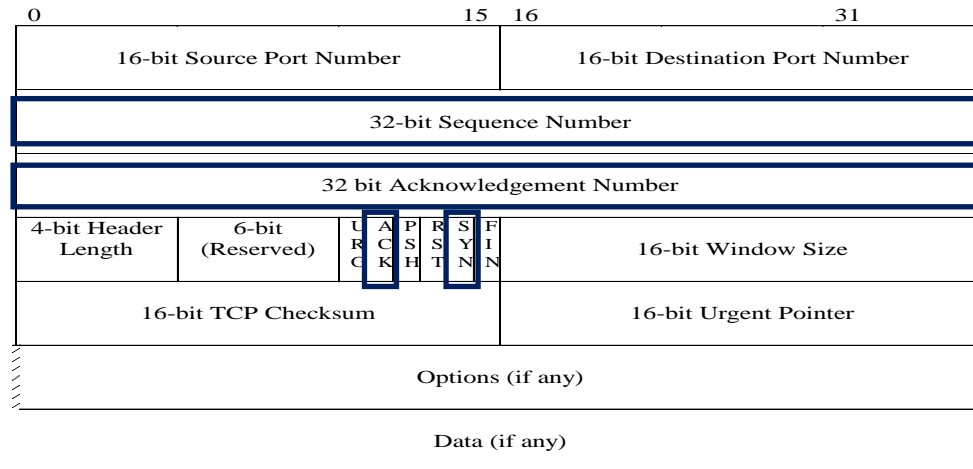
<http://packetlife.net/blog/2011/mar/2/tcp-flags-psh-and-urg/>

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

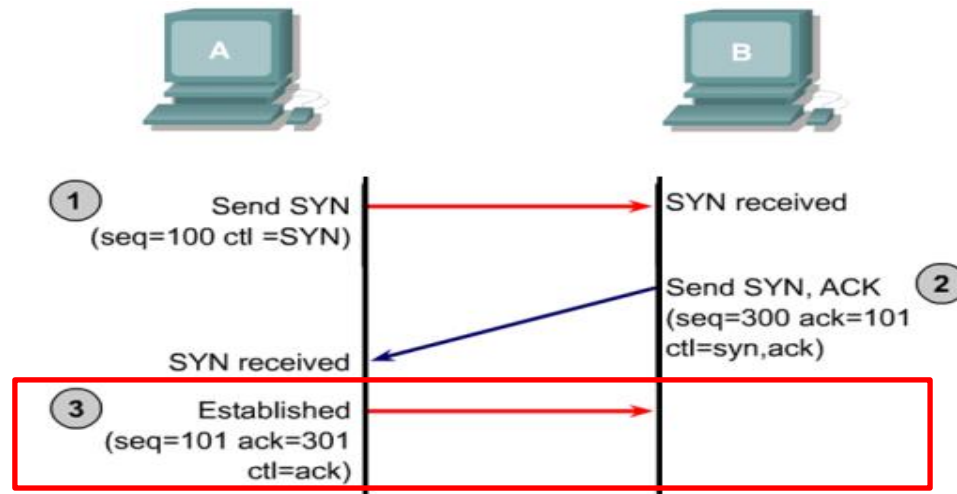
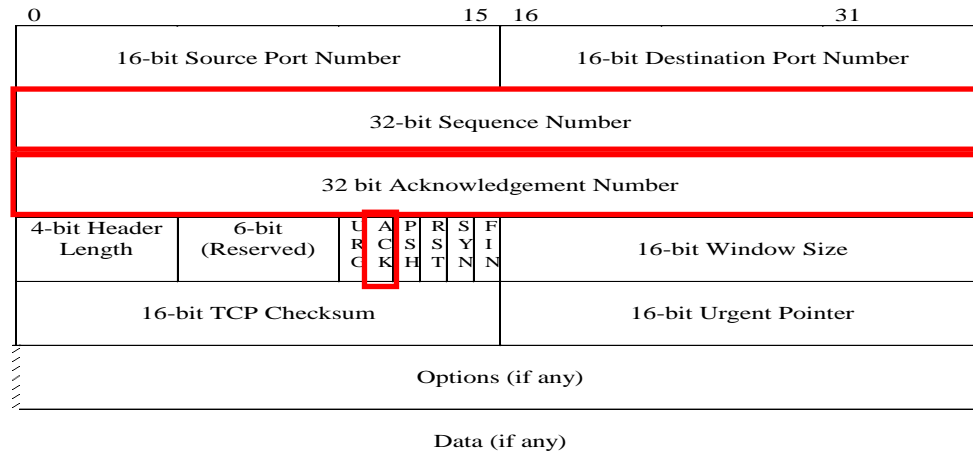
FAZE U USPOSTAVLJANJU KONEKCIJE



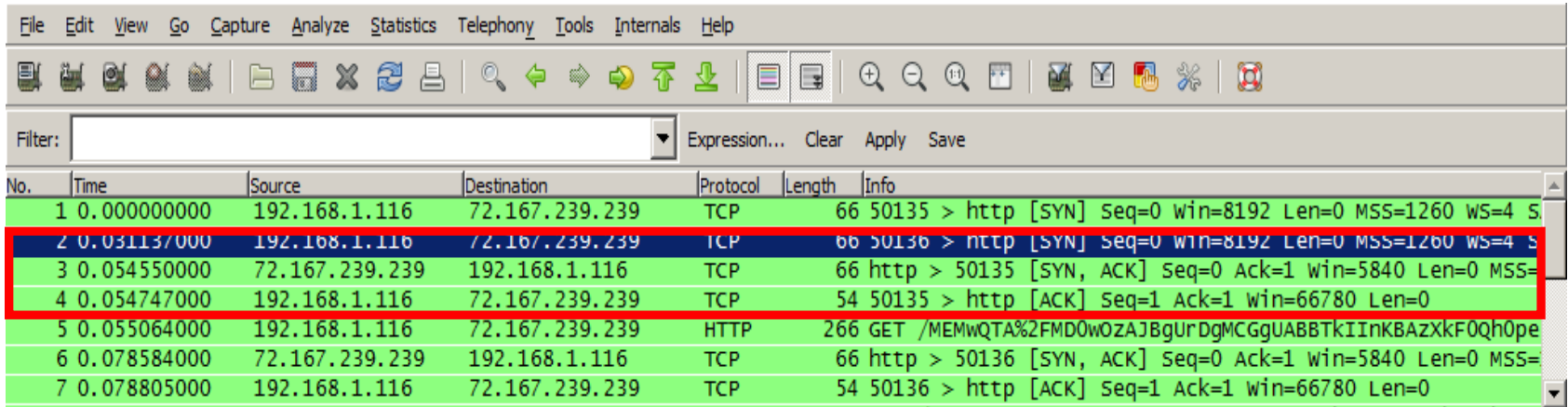
FAZE U USPOSTAVLJANJU KONEKCIJE



FAZE U USPOSTAVLJANJU KONEKCIJE



FAZE U USPOSTAVLJANJU KONEKCIJE (WIRE SHARK)



The screenshot displays the Wireshark interface with a list of captured network packets. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help), a toolbar with various icons, and a filter field. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.116	72.167.239.239	TCP	66	50135 > http [SYN] Seq=0 win=8192 Len=0 MSS=1260 WS=4 S
2	0.031137000	192.168.1.116	72.167.239.239	TCP	66	50136 > http [SYN] Seq=0 win=8192 Len=0 MSS=1260 WS=4 S
3	0.054550000	72.167.239.239	192.168.1.116	TCP	66	http > 50135 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=
4	0.054747000	192.168.1.116	72.167.239.239	TCP	54	50135 > http [ACK] Seq=1 Ack=1 win=66780 Len=0
5	0.055064000	192.168.1.116	72.167.239.239	HTTP	266	GET /MEMwQTA%2FMD0wOZAJBgUrDgMCGGUABBTkIInKBAZxkF0qh0pe
6	0.078584000	72.167.239.239	192.168.1.116	TCP	66	http > 50136 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=
7	0.078805000	192.168.1.116	72.167.239.239	TCP	54	50136 > http [ACK] Seq=1 Ack=1 win=66780 Len=0

FAZE U USPOSTAVLJANJU KONEKCIJE (WIRE SHARK)

The screenshot displays the Wireshark interface with a list of captured packets and a detailed view of the selected packet (Frame 2).

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.116	72.167.239.239	TCP	66	50135 > http [SYN] Seq=0 win=8192 Len=0 MSS=1260 WS=4 S
2	0.031137000	192.168.1.116	72.167.239.239	TCP	66	50136 > http [SYN] Seq=0 win=8192 Len=0 MSS=1260 WS=4 S
3	0.054550000	72.167.239.239	192.168.1.116	TCP	66	http > 50135 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=
4	0.054747000	192.168.1.116	72.167.239.239	TCP	54	50135 > http [ACK] Seq=1 Ack=1 win=66780 Len=0
5	0.055064000	192.168.1.116	72.167.239.239	HTTP	266	GET /MEMwQTA%2FMD0wOzAJBgUrDgMCGGUABBTkIInKBazXkF0qh0pe
6	0.078584000	72.167.239.239	192.168.1.116	TCP	66	http > 50136 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=
7	0.078805000	192.168.1.116	72.167.239.239	TCP	54	50136 > http [ACK] Seq=1 Ack=1 win=66780 Len=0

Frame 2 Details:

- Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Ethernet II, Src: IntelCor_45:5d:c4 (24:77:03:45:5d:c4), Dst: CiscoCon_cc:a0:85 (c8:d7:19:cc:a0:85)
- Internet Protocol Version 4, Src: 192.168.1.116 (192.168.1.116), Dst: 72.167.239.239 (72.167.239.239)
- Transmission Control Protocol, Src Port: 50136 (50136), Dst Port: http (80), Seq: 0, Len: 0
 - Source port: 50136 (50136)
 - Destination port: http (80)
 - [Stream index: 1]
 - Sequence number: 0 (relative sequence number)
 - Header length: 32 bytes
 - Flags: 0x002 (SYN)
 - 000. = Reserved: Not set
 - ...0 = Nonce: Not set
 - 0... = Congestion Window Reduced (CWR): Not set
 -0.. = ECN-Echo: Not set
 -0. = Urgent: Not set
 -0 = Acknowledgment: Not set
 - 0... = Push: Not set
 - 0 = Reset: Not set
 -1. = Syn: Set
 - 0 = Fin: Not set
 - window size value: 8192
 - [Calculated window size: 8192]
 - Checksum: 0x0284 [validation disabled]
 - Options: (12 bytes), Maximum segment size, No-Operation (NOP), window scale, No-Operation (NOP), No-Operation (NOP), SACK p

FAZE U USPOSTAVLJANJU KONEKCIJE (WIRE SHARK)

The screenshot displays the Wireshark network protocol analyzer interface. The main window shows a list of captured packets. Packet 3 is highlighted in blue and red, indicating it is the selected packet. The details pane for this packet shows the following information:

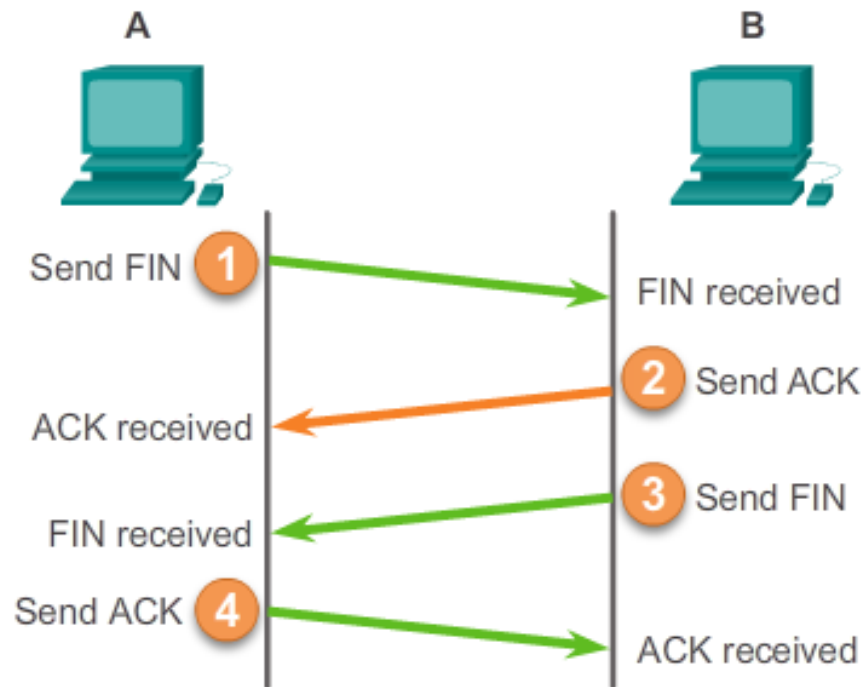
- Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Ethernet II, src: CiscoCon_cc:a0:85 (c8:d7:19:cc:a0:85), Dst: IntelCor_45:5d:c4 (24:77:03:45:5d:c4)
- Internet Protocol Version 4, src: 72.167.239.239 (72.167.239.239), Dst: 192.168.1.116 (192.168.1.116)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 50135 (50135), Seq: 0, Ack: 1, Len: 0
 - Source port: http (80)
 - Destination port: 50135 (50135)
 - [Stream index: 0]
 - Sequence number: 0 (relative sequence number)
 - Acknowledgment number: 1 (relative ack number)
 - Header length: 32 bytes
 - Flags: 0x012 (SYN, ACK)
 - 000. = Reserved: Not set
 - ...0 = Nonce: Not set
 - 0... = Congestion window Reduced (CWR): Not set
 -0.. = ECN-Echo: Not set
 -0. = Urgent: Not set
 -1. = Acknowledgment: Set
 -0... = Push: Not set
 -0. = Reset: Not set
 -1. = Syn: Set
 -0 = Fin: Not set
 - Window size value: 5840
 - [Calculated window size: 5840]
 - Checksum: 0x491d [validation disabled]

FAZE U USPOSTAVLJANJU KONEKCIJE (WIRE SHARK)

The screenshot displays the Wireshark interface with a list of network packets and a detailed view of the selected packet (No. 4). The packet list shows a sequence of SYN and ACK packets between 192.168.1.116 and 72.167.239.239. The selected packet (No. 4) is an ACK packet with the following details:

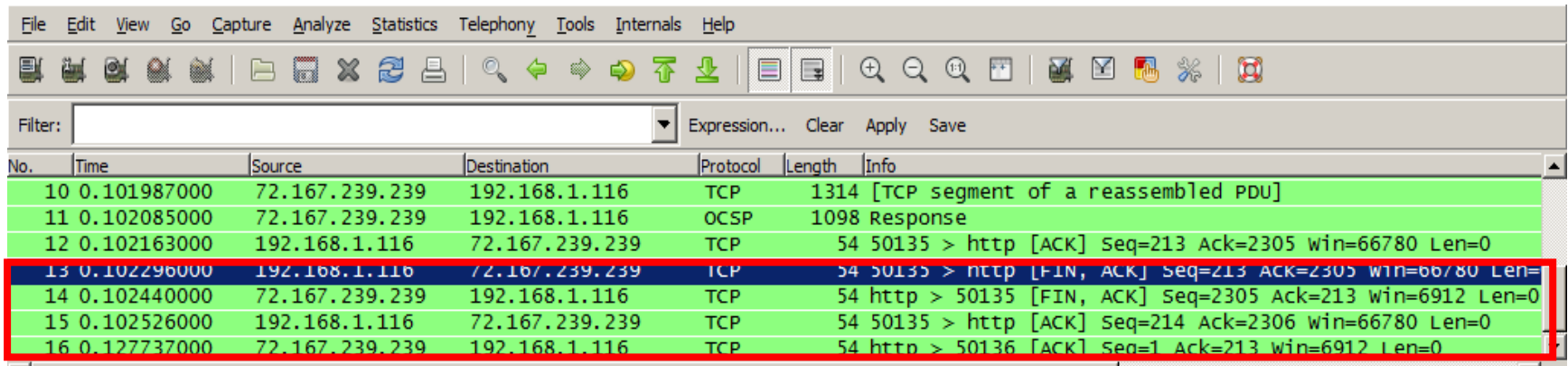
- Frame 4: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
- Ethernet II, Src: IntelCor_45:5d:c4 (24:77:03:45:5d:c4), Dst: CiscoCon_cc:a0:85 (c8:d7:19:cc:a0:85)
- Internet Protocol Version 4, Src: 192.168.1.116 (192.168.1.116), Dst: 72.167.239.239 (72.167.239.239)
- Transmission Control Protocol, Src Port: 50135 (50135), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
 - Source port: 50135 (50135)
 - Destination port: http (80)
 - [Stream index: 0]
 - Sequence number: 1 (relative sequence number)
 - Acknowledgment number: 1 (relative ack number)
 - Header length: 20 bytes
 - Flags: 0x010 (ACK)
 - 000. = Reserved: Not set
 - ...0 = Nonce: Not set
 - 0... = Congestion window Reduced (CWR): Not set
 -0.. = ECN-Echo: Not set
 -0. = Urgent: Not set
 -1 = Acknowledgment: Set
 - 0... = Push: Not set
 -0.. = Reset: Not set
 -0. = Syn: Not set
 -0 = Fin: Not set
 - window size value: 16695
 - [Calculated window size: 66780]
 - [window size scaling factor: 4]
 - Checksum: 0x5f88 [validation disabled]

RASKIDANJE KONEKCIJE

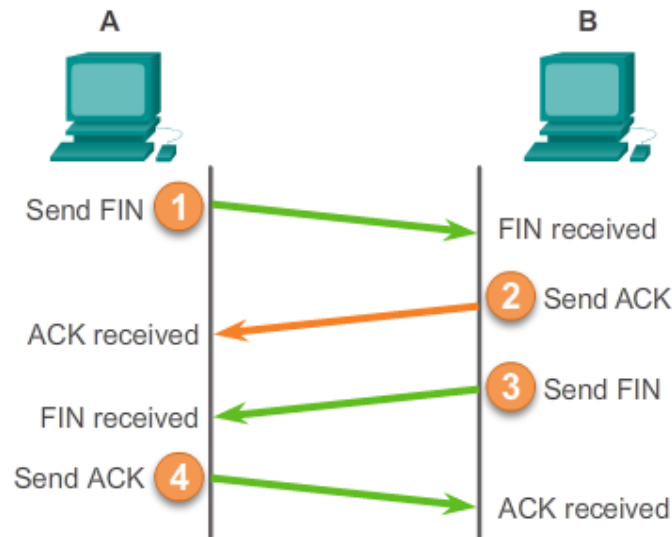


- Host A šalje segment sa setovanim FIN bitom.
- Host B odgovara sa setovanim ACK bitom.
- Host B odgovara sa segmentom kome je setovan FIN bit.
- Host A odgovara sa setovanim ACK bitom.

RASKIDANJE KONEKCIJE (WIRESHARK)



No.	Time	Source	Destination	Protocol	Length	Info
10	0.101987000	72.167.239.239	192.168.1.116	TCP	1314	[TCP segment of a reassembled PDU]
11	0.102085000	72.167.239.239	192.168.1.116	OCSP	1098	Response
12	0.102163000	192.168.1.116	72.167.239.239	TCP	54	50135 > http [ACK] Seq=213 Ack=2305 win=66780 Len=0
13	0.102296000	192.168.1.116	72.167.239.239	TCP	54	50135 > http [FIN, ACK] Seq=213 Ack=2305 win=66780 Len=0
14	0.102440000	72.167.239.239	192.168.1.116	TCP	54	http > 50135 [FIN, ACK] Seq=2305 Ack=213 win=6912 Len=0
15	0.102526000	192.168.1.116	72.167.239.239	TCP	54	50135 > http [ACK] Seq=214 Ack=2306 win=66780 Len=0
16	0.127737000	72.167.239.239	192.168.1.116	TCP	54	http > 50136 [ACK] Seq=1 Ack=213 win=6912 Len=0



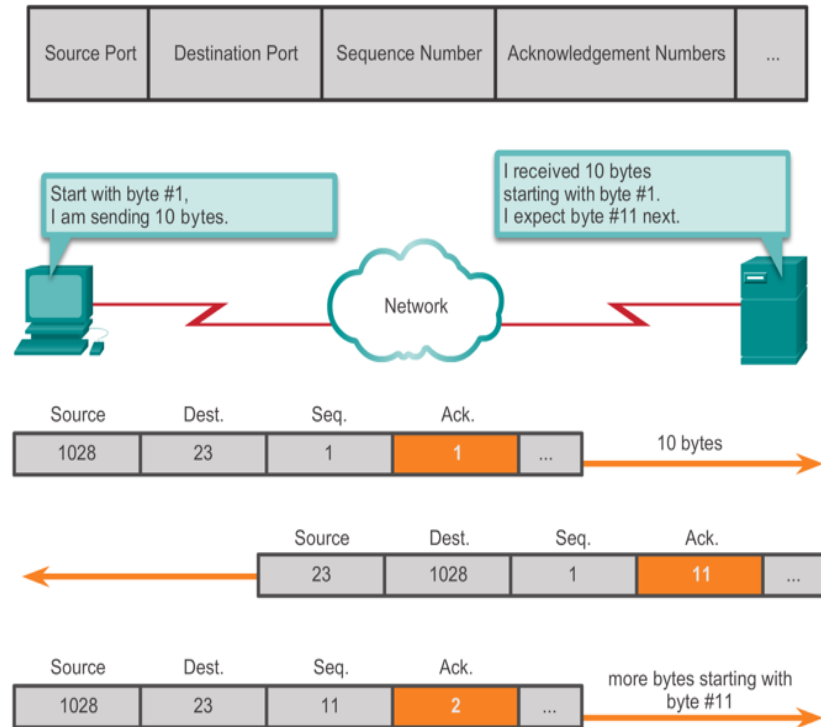
POLJA ZA POUZDAN PRENOS

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

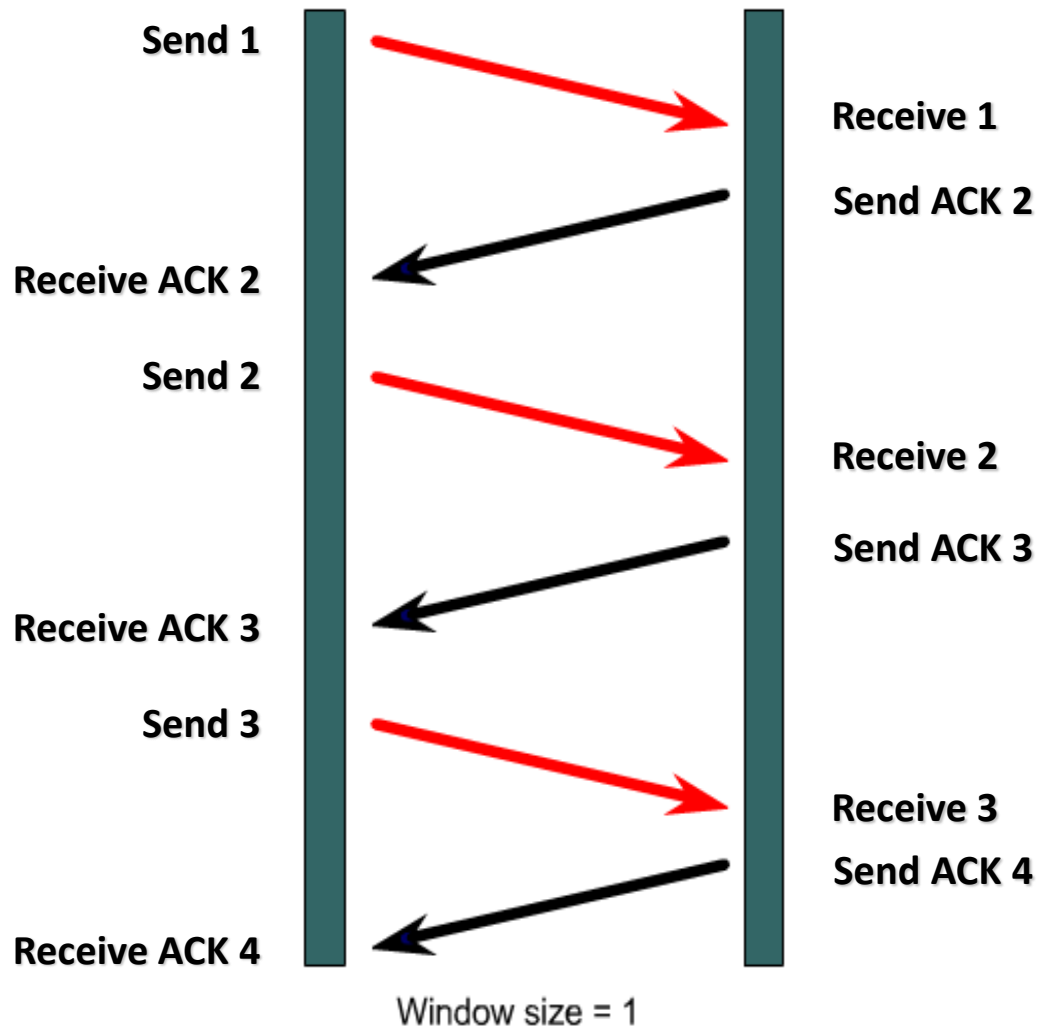
SN koisti odredište da bi saznalo koji je zadnji poslat segment, a Ack koristi izvor da bi saznao šta je odredište zadnje primilo.

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 (expectational acknowledgement).



UPROŠŤEN MODEL POUZDANOSTI



UPRAVLJANJE TCP SESIJOM

Source Port	Destination Port	Sequence Number	Acknowledgement Numbers	...
-------------	------------------	-----------------	-------------------------	-----

Start with byte #1,
I am sending 10 bytes.



Source	Dest.	SN	ACK #
1028	23	1	1

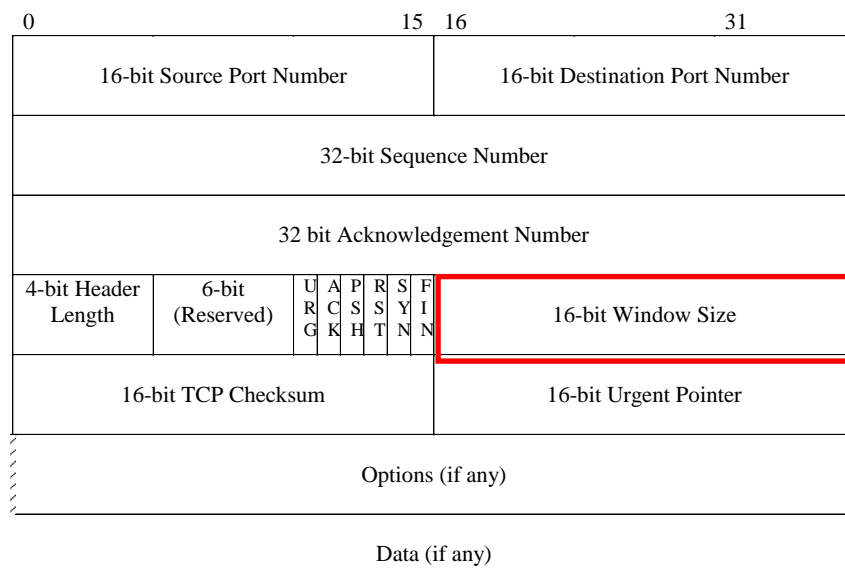
10 bytes

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)

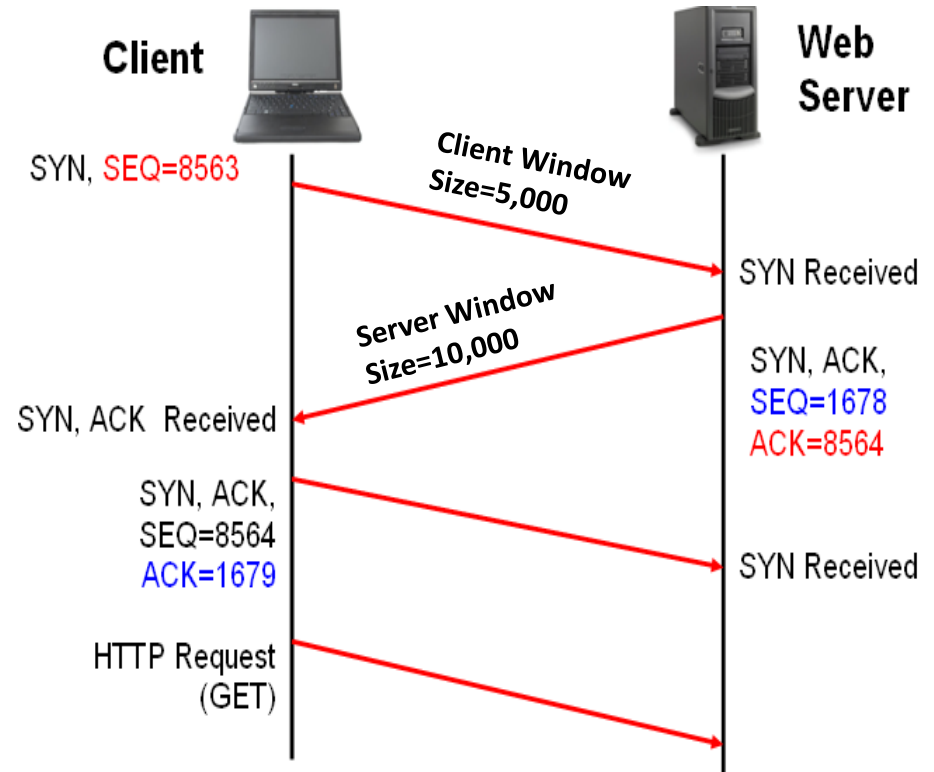


- Ukoliko čekamo Ack za svaki primljeni segment komunikacija bi bila ne efikasna.
- TCP ovaj problem rešava prosleđujući segmente na osnovu veličine polja “**window**” .
 - Polje window određuje broj segmenata koje pošiljaoc može da pošalje bez potvrde prijema (Ack)

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.

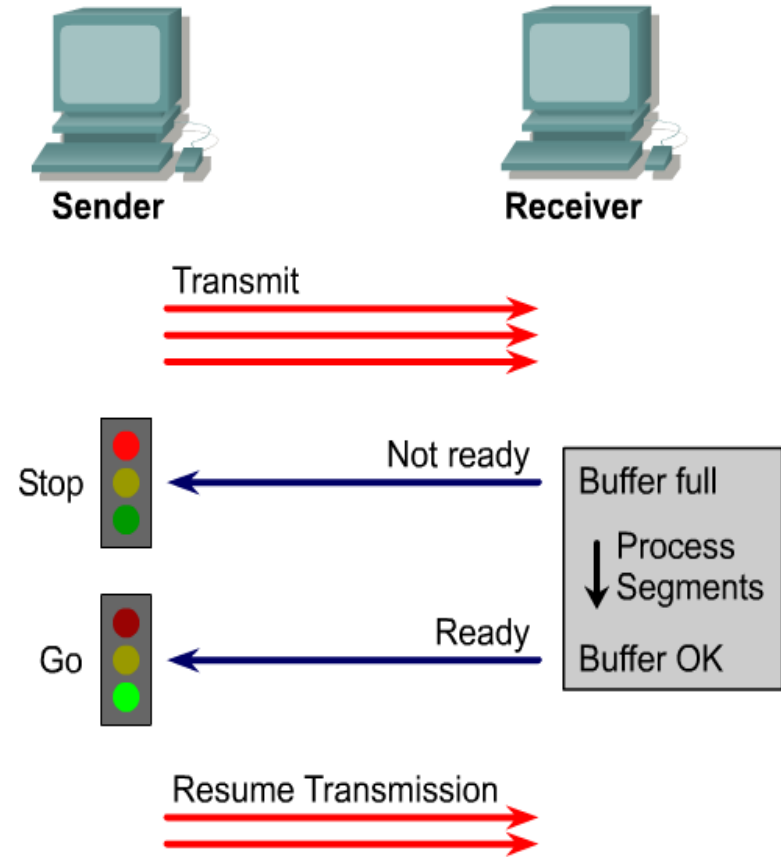


KLIZAJUĆI PROZORI (SLIDING WINDOWS)

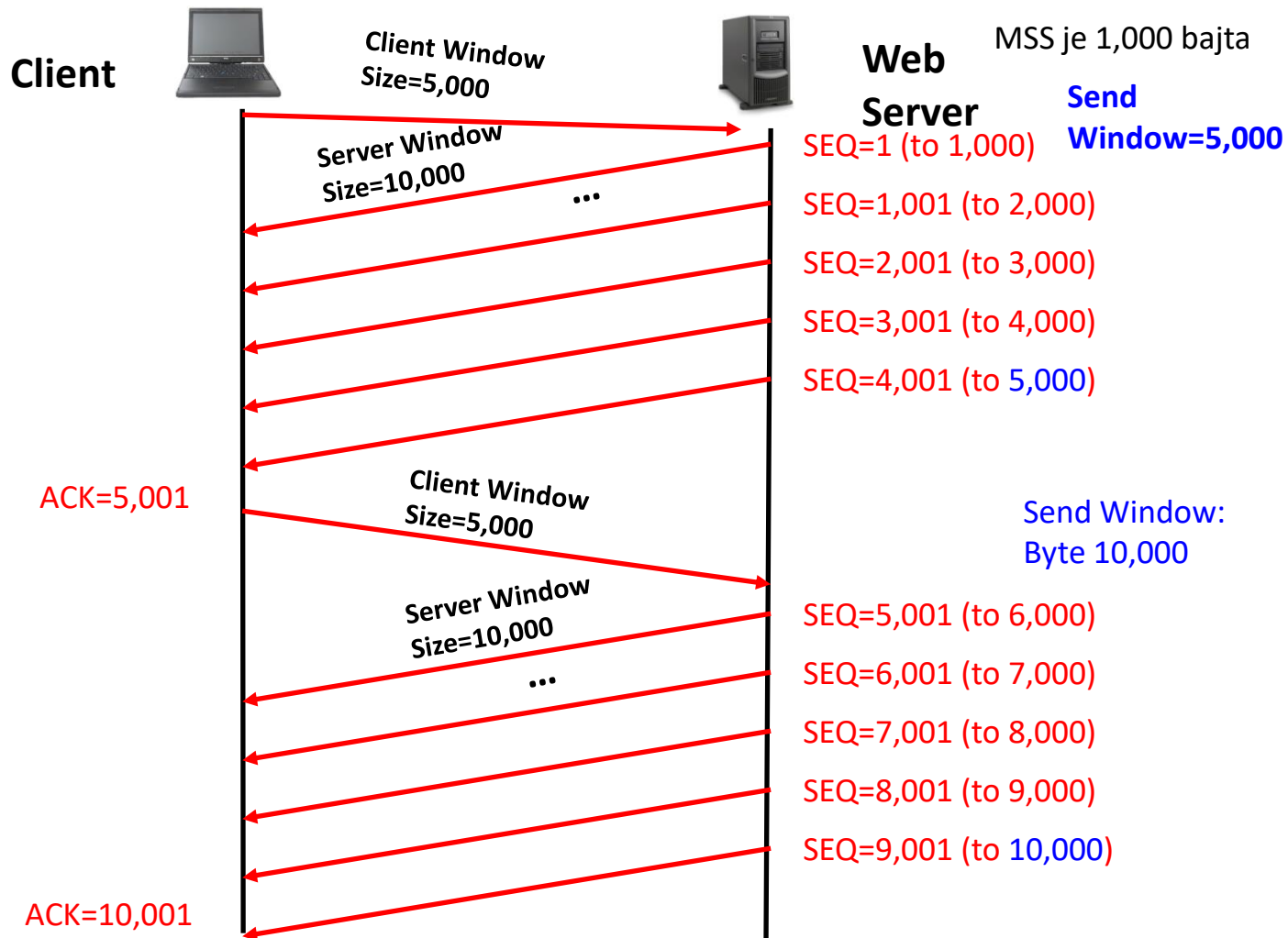
TCP implementira kontrolu toka povećavajući / smanjujući veličinu prozora.

- 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)



SEQ 1 | Bytes 1 - 1000

SEQ 1001 | Bytes 1001 - 2000

SEQ 2001 | Bytes 2001 - 3000

SEQ 3001 | Bytes 3001 - 4000

SEQ 4001 | Bytes 4001 - 5000

SEQ 5001 | Bytes 5001 - 6000



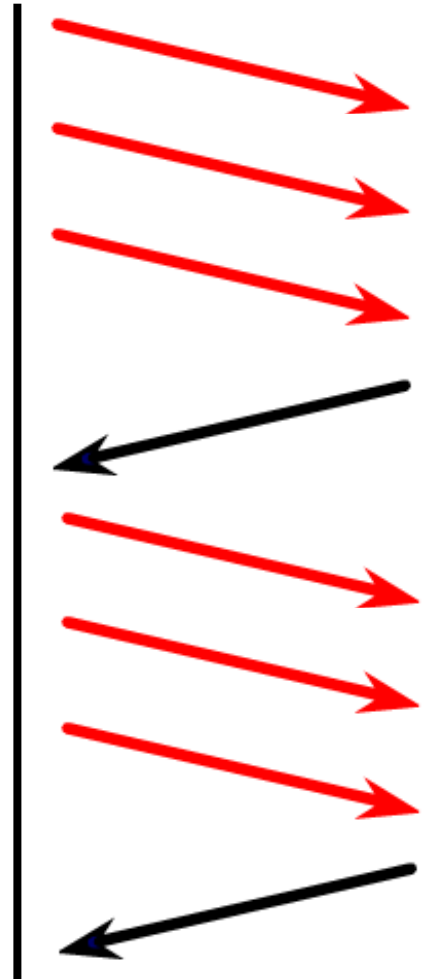
ACK = 3001

ACK = 6001

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

