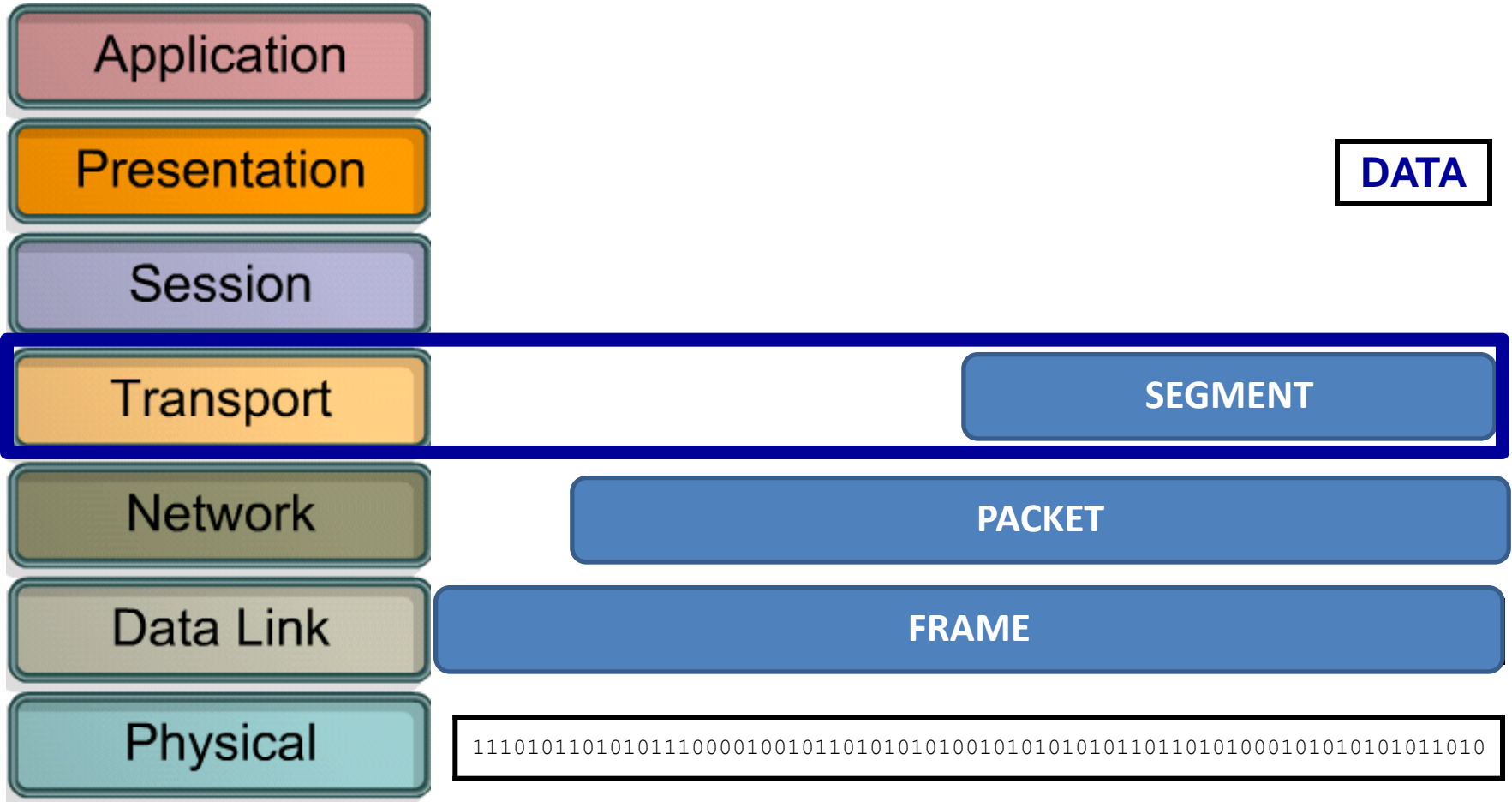


TRANSPORTNI SLOJ

Predmet: Aktivni mrežni uređaji

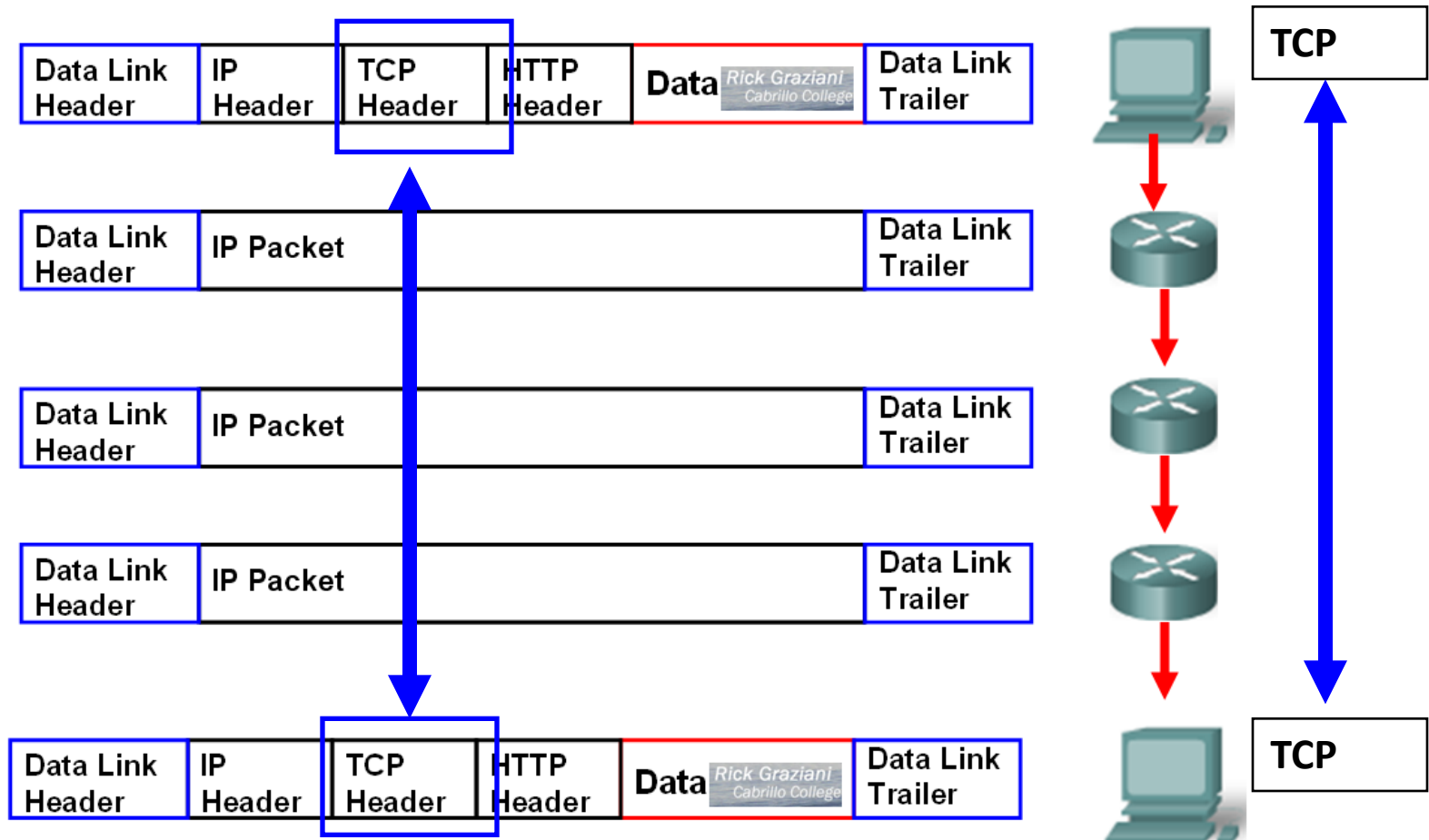
Predavač: dr Dušan Stefanović

ENKAPSULACIJA

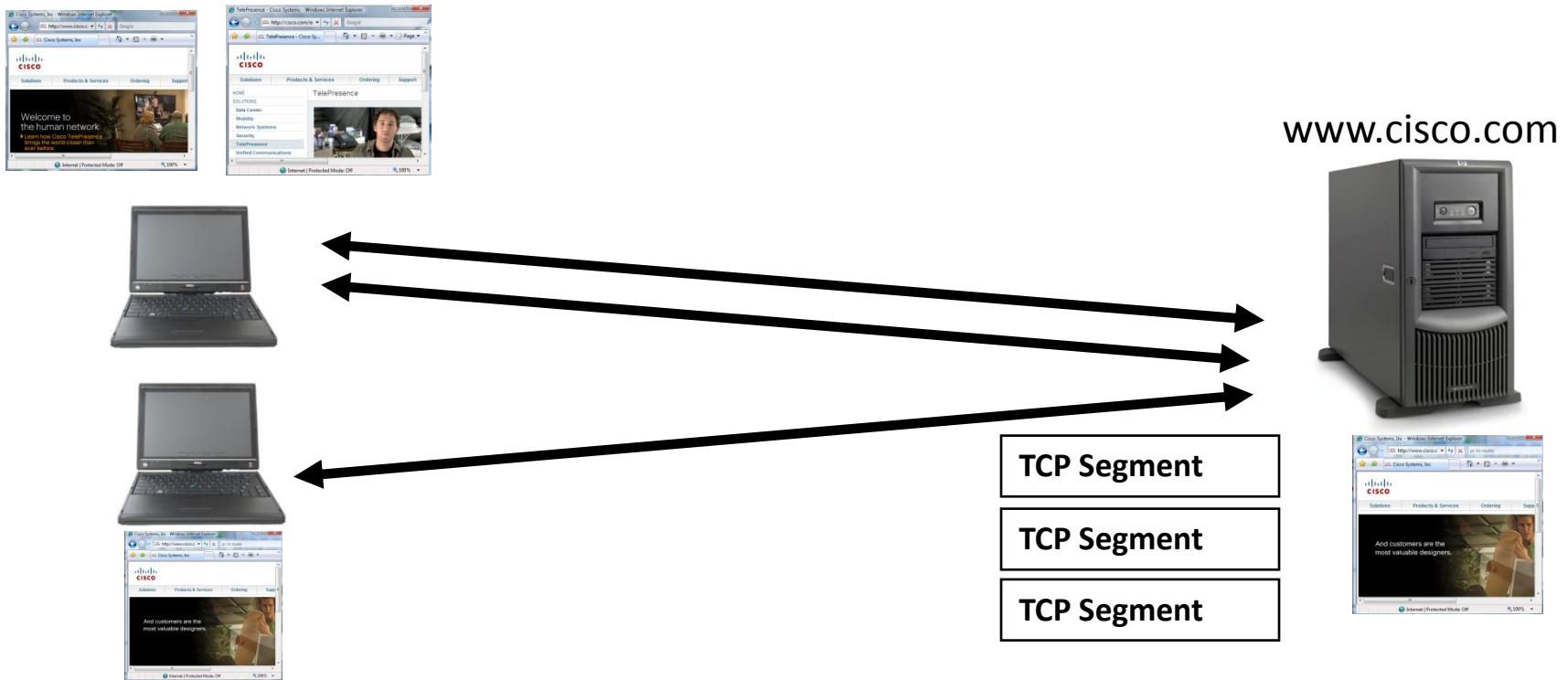


TRANSPORTNI SLOJ

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

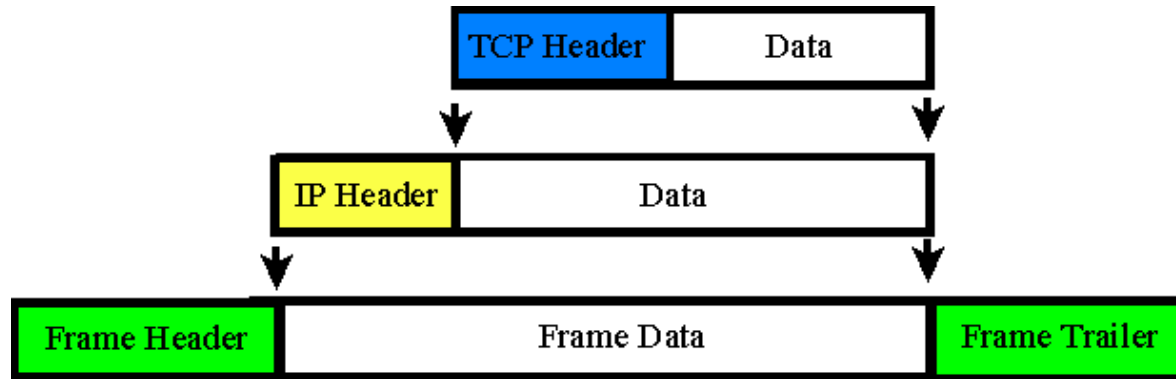


ULOGA TRANSPORTNOG SLOJA

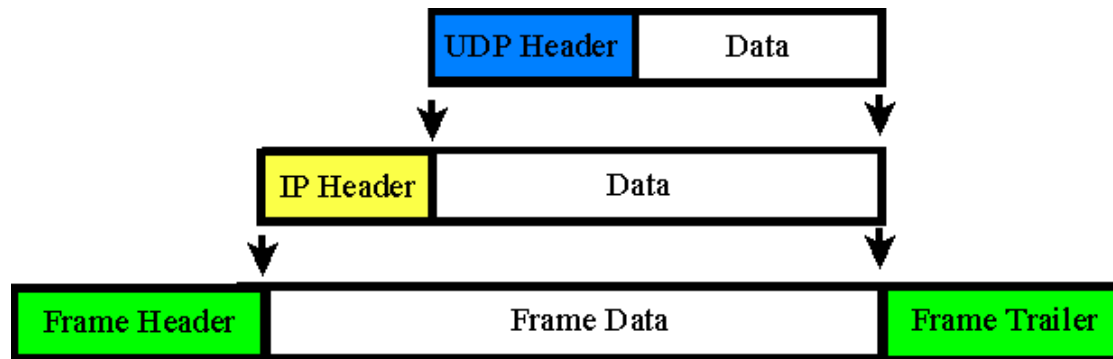


1. Prati individualnu komunikaciju između aplikacija na izvoru i odredištu
2. Od podatka kreira segmente koje na odredištu sastavlja ponovo u podatak
3. Na jedinstven način označava tj. identifikuje svaku sesiju

TCP (TRANSMISSION CONTROL PROTOCOL)

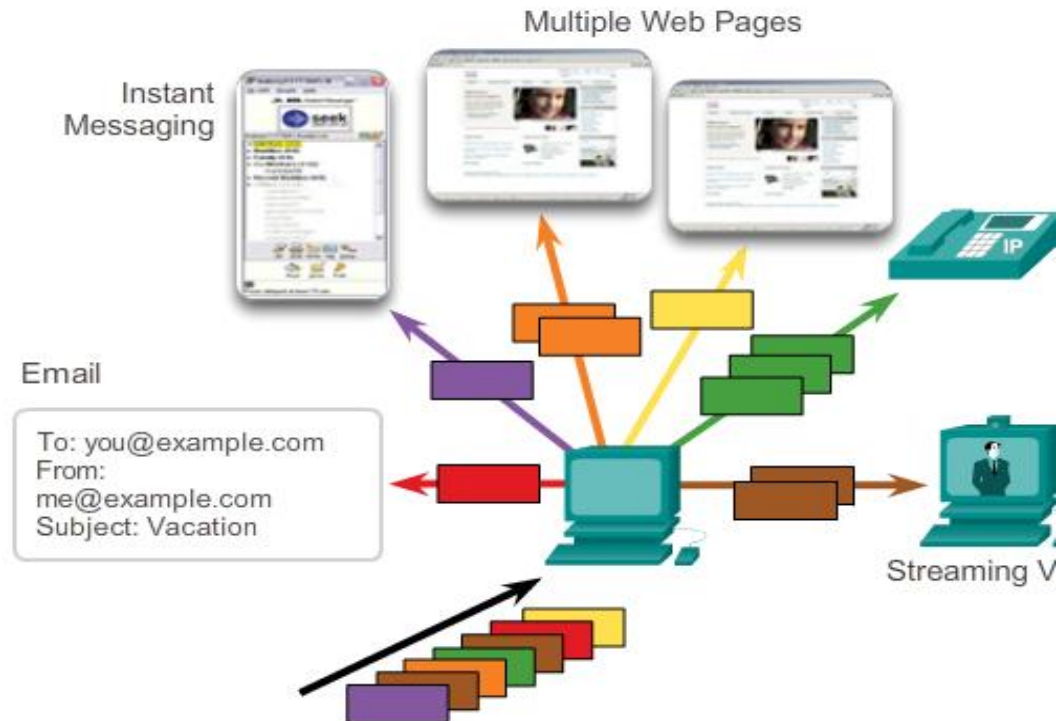


UDP (USER DATAGRAM PROTOCOL)

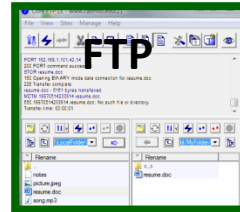


TRANSPORTNI SLOJ

- 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



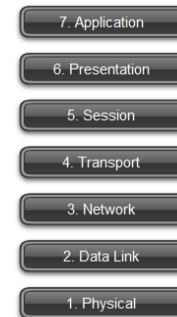
TRANSPORTNI SLOJ



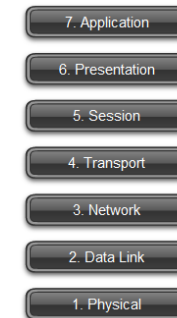
TCP
TCP
TCP
TCP

TCP
TCP

TCP
TCP



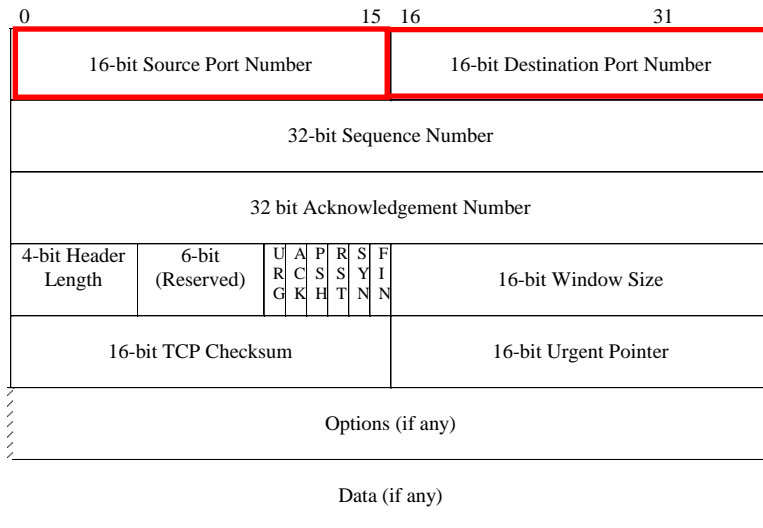
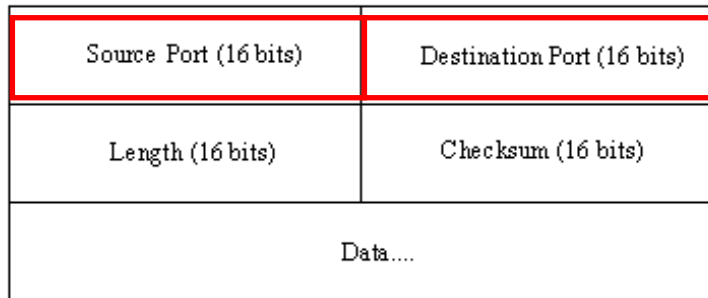
VTS Web Server



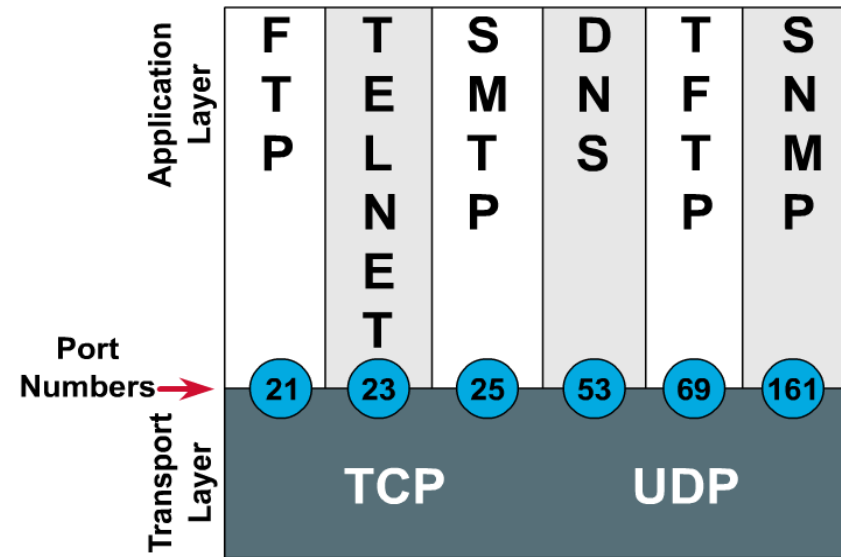
ISP Email i
FTP Server



IDENTIFIKACIJA APLIKACIJE



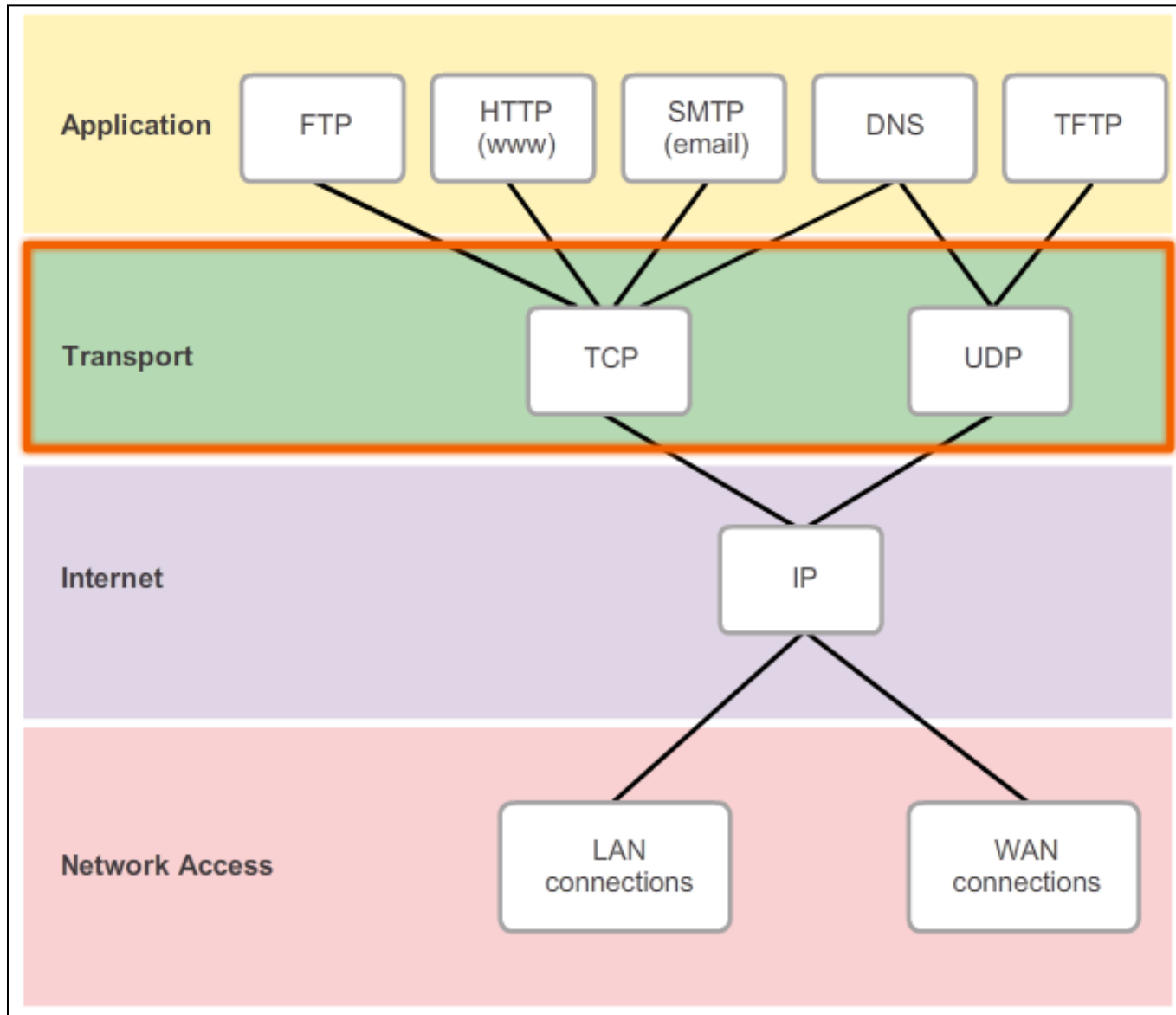
Port Numbers



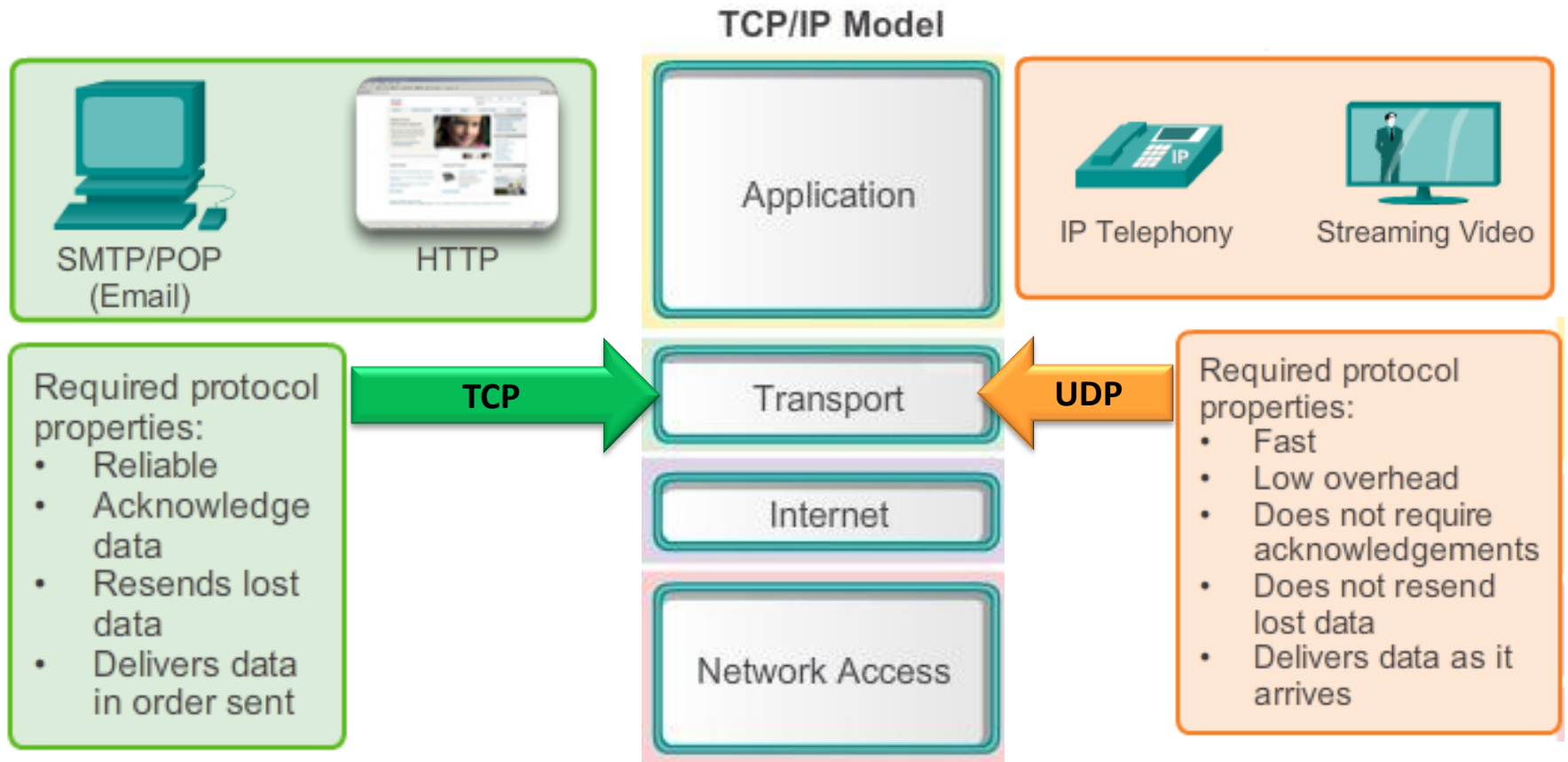
Transportni sloj zadaje svakoj aplikaciji identifikator koji se zove port.

Na osnovu broja porta transportni sloj identifikuje svaku aplikaciju.

TRANSPORTNI SLOJ

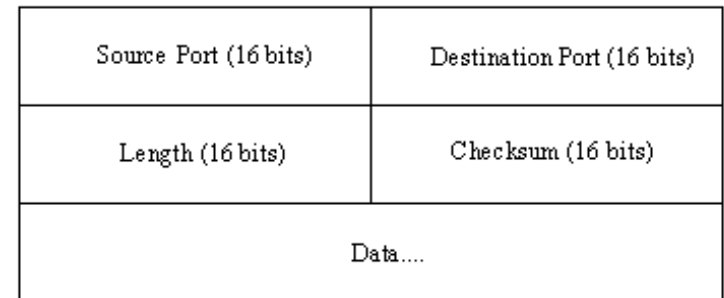
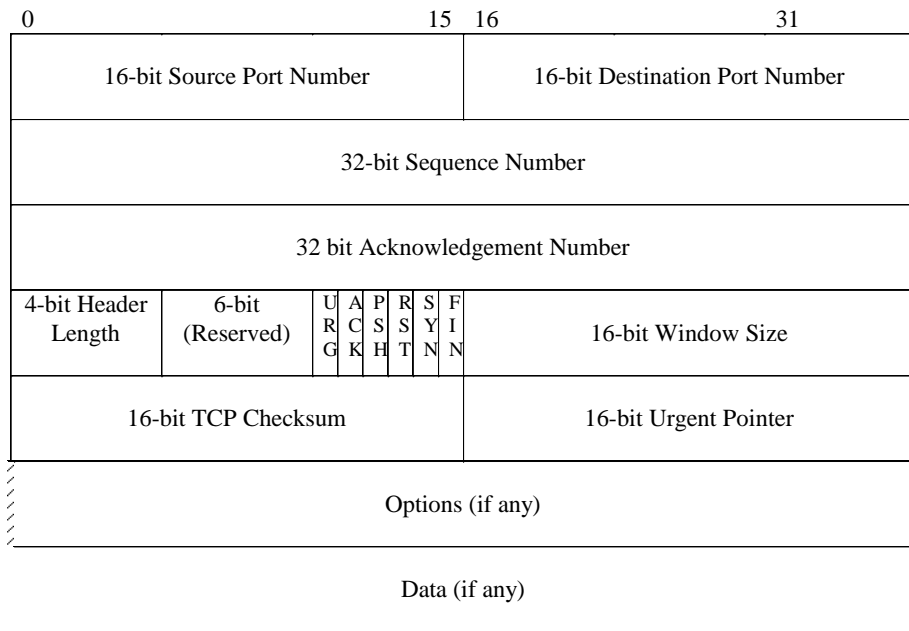


TCP / UDP



TCP i UDP koriste se za različitu vrstu saobraćaja

TCP / UDP



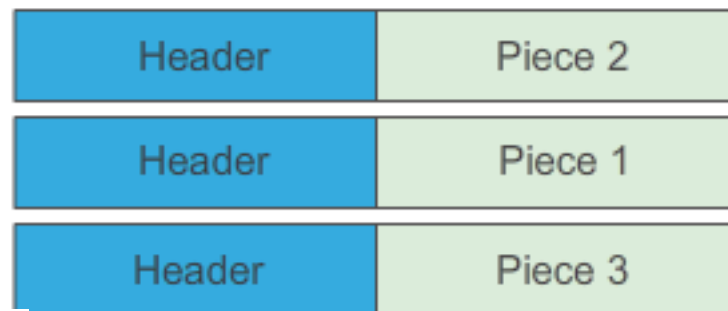
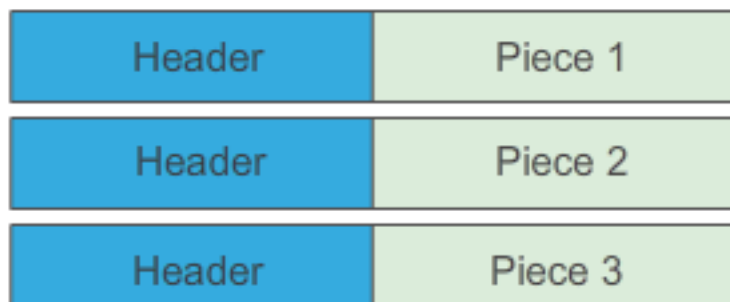
TCP je znatno kompleksniji od UDP-a

TCP / UDP



TCP Segment

UDP Datagram



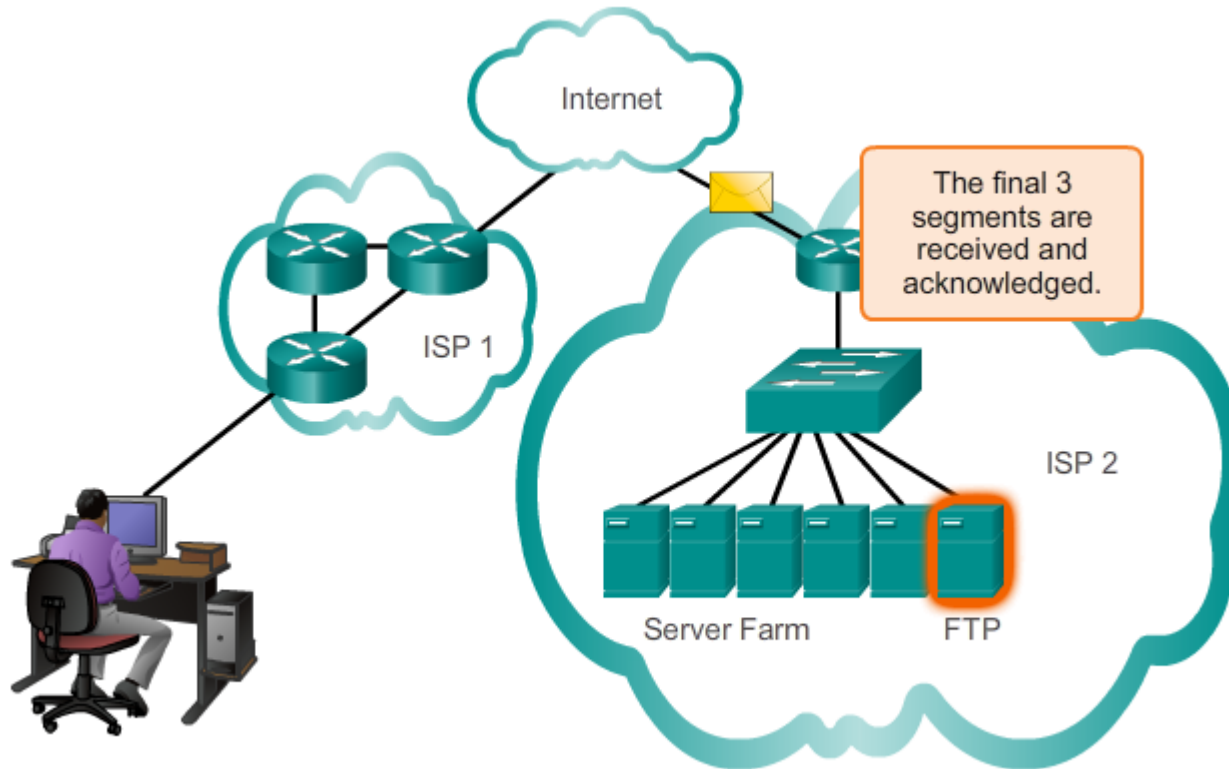
TCP HEADER obezbeđuje:

- Izvorišni i odredišni port
- Sekvenciranje segmenata
- Potvrda segmenata na prijemu
- Kontrola toka i upravljanje nagomilavanjem

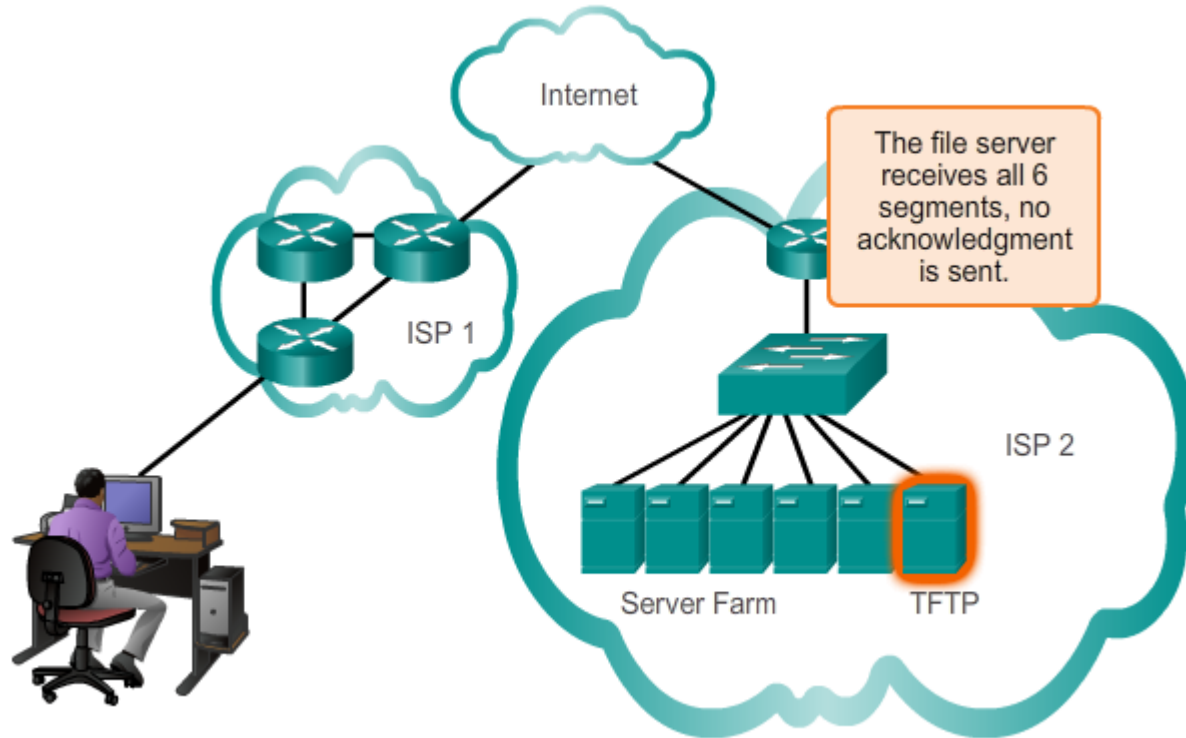
UDP HEADER obezbeđuje:

- Izvorišni i odredišni port

TCP



UDP

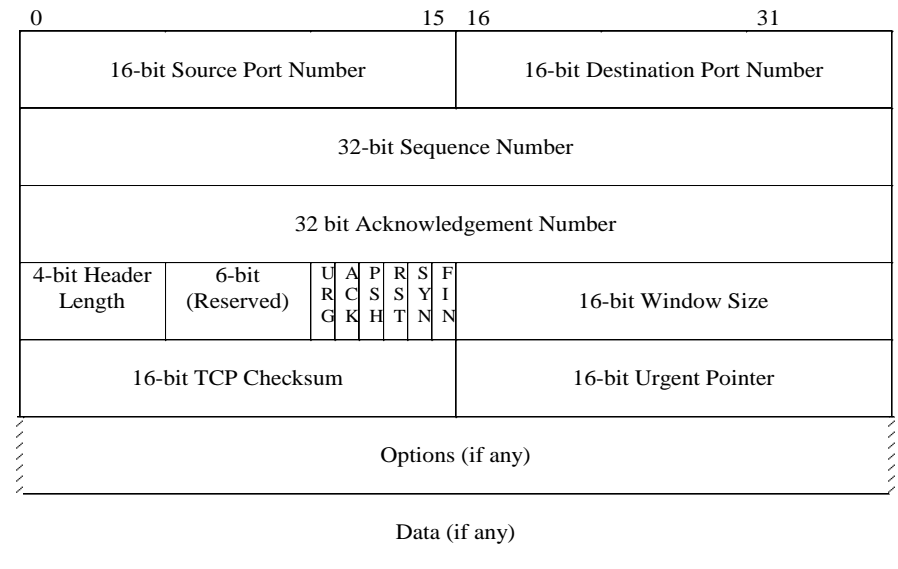


TCP SERVISI



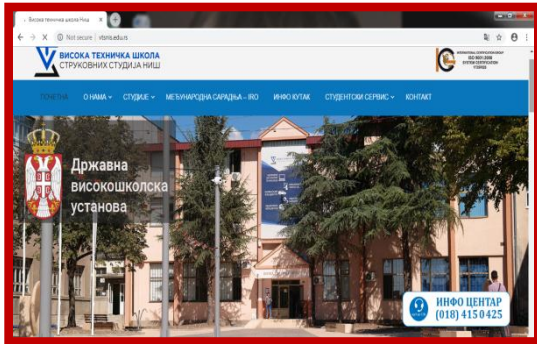
TCP obezbeđuje sledeće servise:

- 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**)

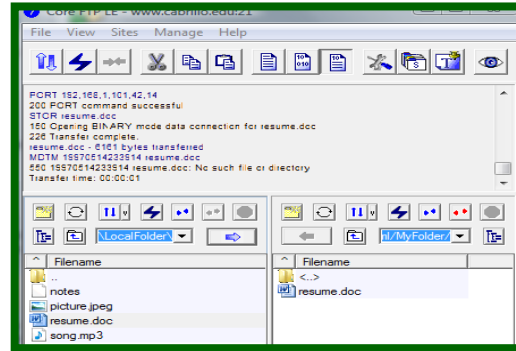


TCP - KARAKTERISTIKE

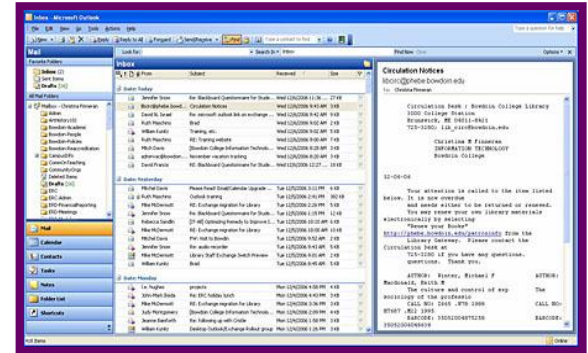
HTTP



FTP



SMTP

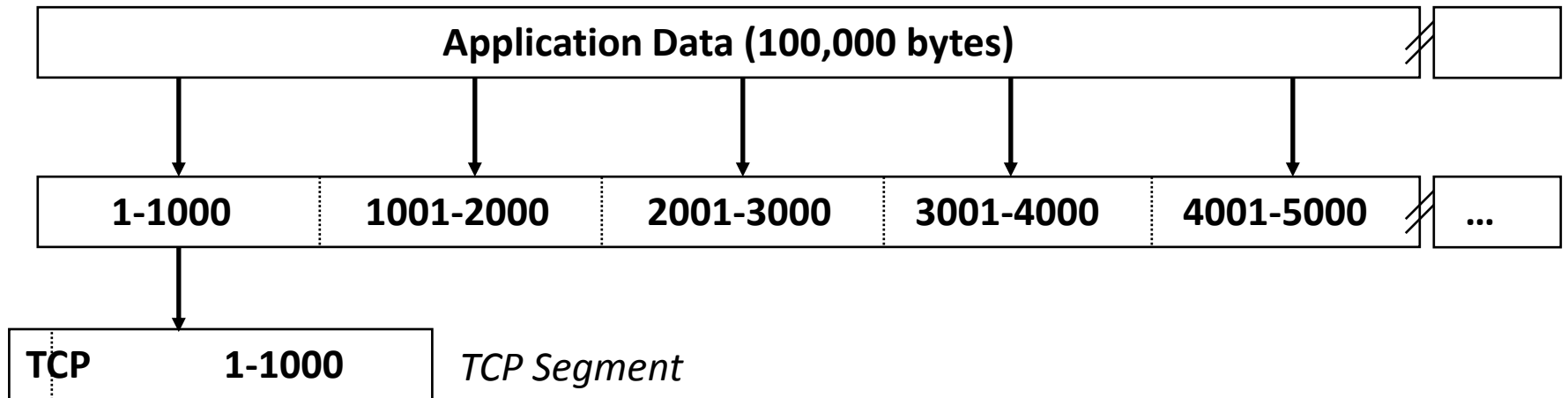


TCP je konekcioni protokol ([Connection-oriented](#))

TCP dodaje 20 Bajta kontrolnih informacija u zaglavlju za svaki segment

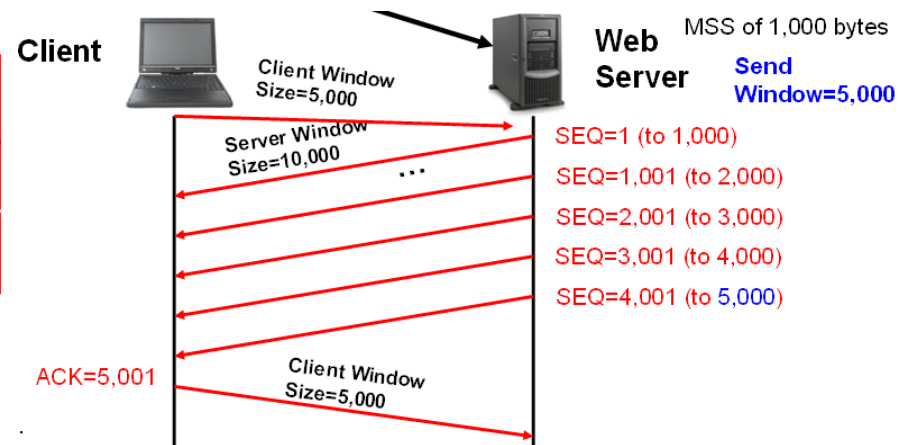
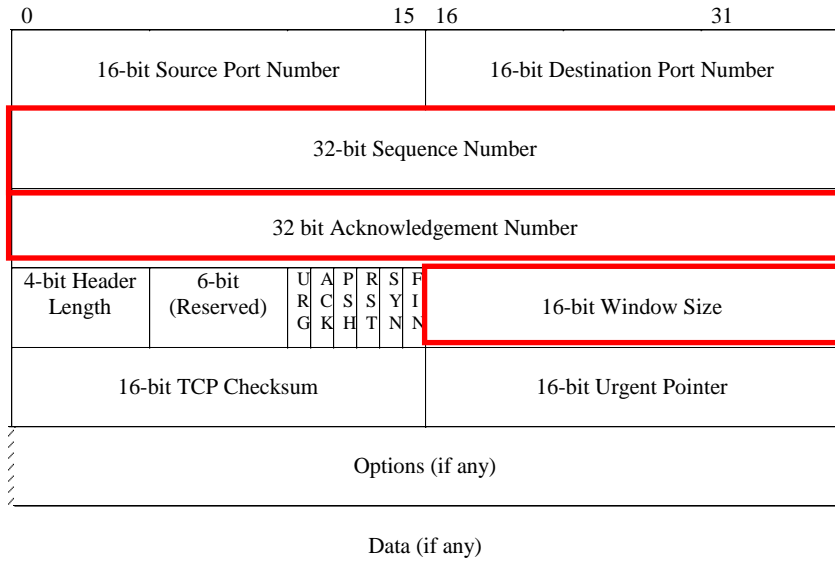
Podaci na transportnom sloju se zovu **segmenti**

TCP - KARAKTERISTIKE



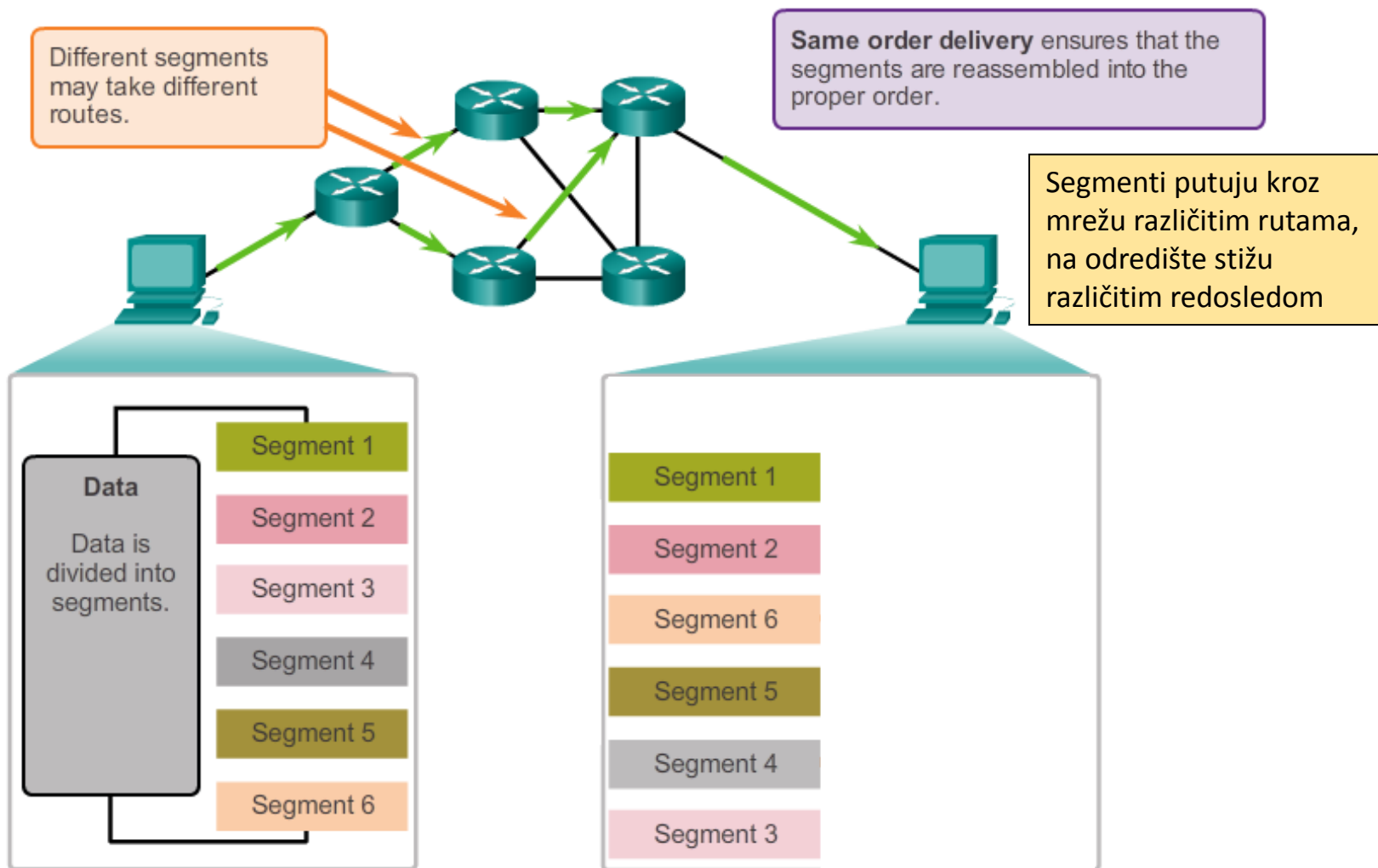
- TCP enkapsulira podatak u veliki broj segmenata.
 - Segmenti obezbeđuju da komunikacija kroz mrežu bude efikasna.
- TCP zaglavlje uključuje sledeće informacije:
 - [Source port number](#) i [Destination port number](#) prate svaku pojedinačnu komunikaciju
 - [Sequence numbers](#) numeracija svakog 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 SEGMENTATA



TCP SEGMENT U WIRESHARK-U

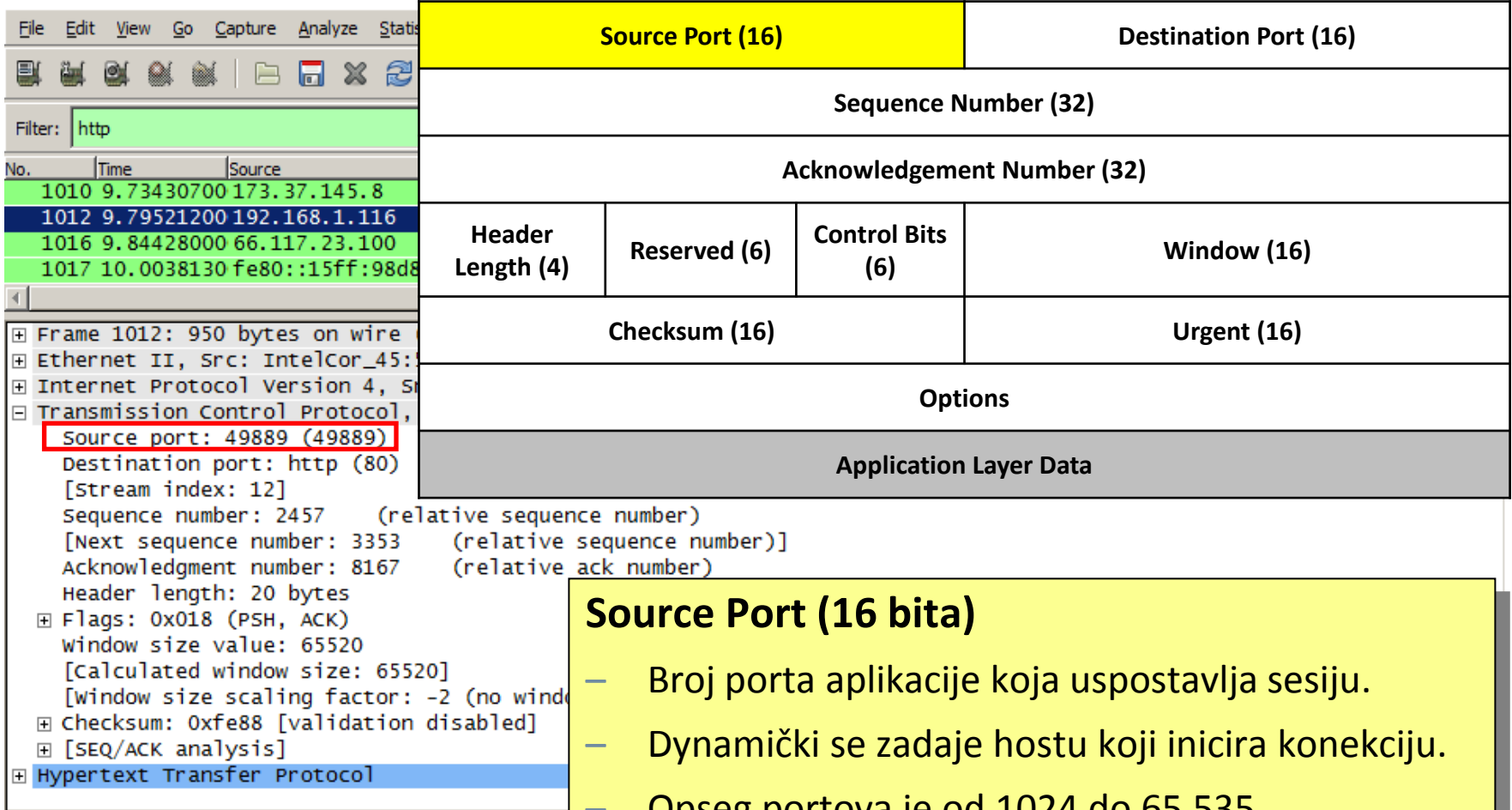
The image displays the Wireshark network protocol analyzer interface. The main focus is on a selected packet (No. 1012) which is a Hypertext Transfer Protocol (HTTP) request. The packet details pane shows the following structure:

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			

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 c8 d7 19 cc a0 85 24 77 03 45 5d c4 08 00 45 00 .....$w .E]...E.
0010 03 a8 0f c8 40 00 80 06 cb 92 c0 a8 01 74 42 75 ....@... ..tBu
0020 17 64 c2 e1 00 50 cc 6e 68 ce 2c d9 ba 56 50 18 .d...P.n h,...VP.
0030 ff f0 fe 88 00 00 47 45 54 20 2f 6d 32 2f 63 69 .....GE T /m2/ci
0040 73 63 6f 73 79 73 74 65 6d 73 69 6e 63 2f 6d 62 scosyste msinc/mb
0050 6f 78 2f 61 61 61 78 2f 6d 62 6f 78 48 6f 72 74 ox/ajax?mboxHost
```

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)

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

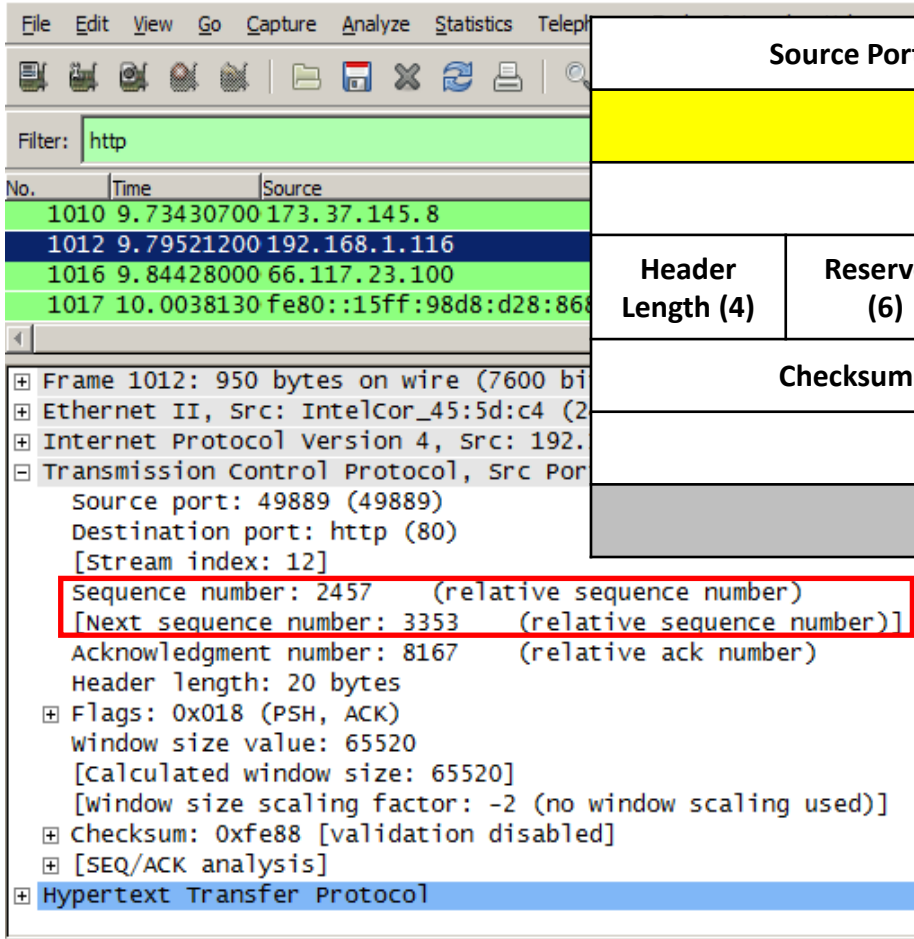
Frame 1012: 950 bytes on wire (7600 bytes captured) on interface eth0
Ethernet II, Src: IntelCor_45:53:00:14:00:00, Dst: IntelCor_45:53:00:14:00:00
Internet Protocol Version 4, Src: 192.168.1.116, Dst: 192.168.1.100
Transmission Control Protocol, Src port: 49889 (49889), Destination port: http (80)
[Stream 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: 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			

Frame 1012: 950 bytes on wire (7600 bytes captured) on interface eth0
Ethernet II, Src: IntelCor_45:5d:c4, Dst: 192.168.1.116
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.116
Transmission Control Protocol, Src Port: 49889, Dst Port: 80
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 displays the Wireshark network protocol analyzer interface. The packet list pane shows a list of captured packets, with packet 1012 selected. The packet details pane shows the structure of the selected packet, including the Ethernet II, Internet Protocol version 4, and Transmission Control Protocol (TCP) layers. The TCP layer details are expanded, showing fields such as Source port, Destination port, Sequence number, Acknowledgment number, and Header length. The 'Header length' field is highlighted with a red box, indicating its value of 20 bytes. A yellow callout box with a black border points to the 'Header Length (4)' field in the diagram above, with the text 'Header Length (4 bita)' and 'Ukazuje na dužinu TCP zaglavlja u segmentu'.

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

The image displays the Wireshark interface for analyzing 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 the TCP segment fields. The 'Control Bits (Flags)' field is highlighted in yellow in the diagram and red in the screenshot. A yellow callout box provides an explanation for this field.

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.

Filter: http

No. Time Source

1010 9.73430700 173.37.145

1012 9.79521200 192.168.1

1016 9.84428000 66.117.23.

1017 10.0038130 fe80::15ff

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

Ethernet II, Src: IntelCo

Internet Protocol Version 4

Transmission Control Protocol

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 (no window scaling used)]

Checksum: 0xfe88 [validation disabled]

[SEQ/ACK analysis]

Hypertext Transfer Protocol

TCP SEGMENT U WIRESHARK-U

The image shows a Wireshark interface with a packet list and a packet details pane. The packet list pane shows a list of packets, with packet 1012 selected. The packet details pane shows the structure of the selected packet, including the TCP segment fields. The window size value is highlighted in red in the details pane.

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_08:00:27:00:00:00, 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.

TCP SEGMENT U WIRESHARK-U

The image displays the Wireshark network protocol analyzer interface. The packet list pane shows a capture of several packets, with packet 1012 selected. The packet details pane shows the structure of the selected TCP segment. A yellow callout box highlights the Checksum field, indicating that it is calculated over the header and data.

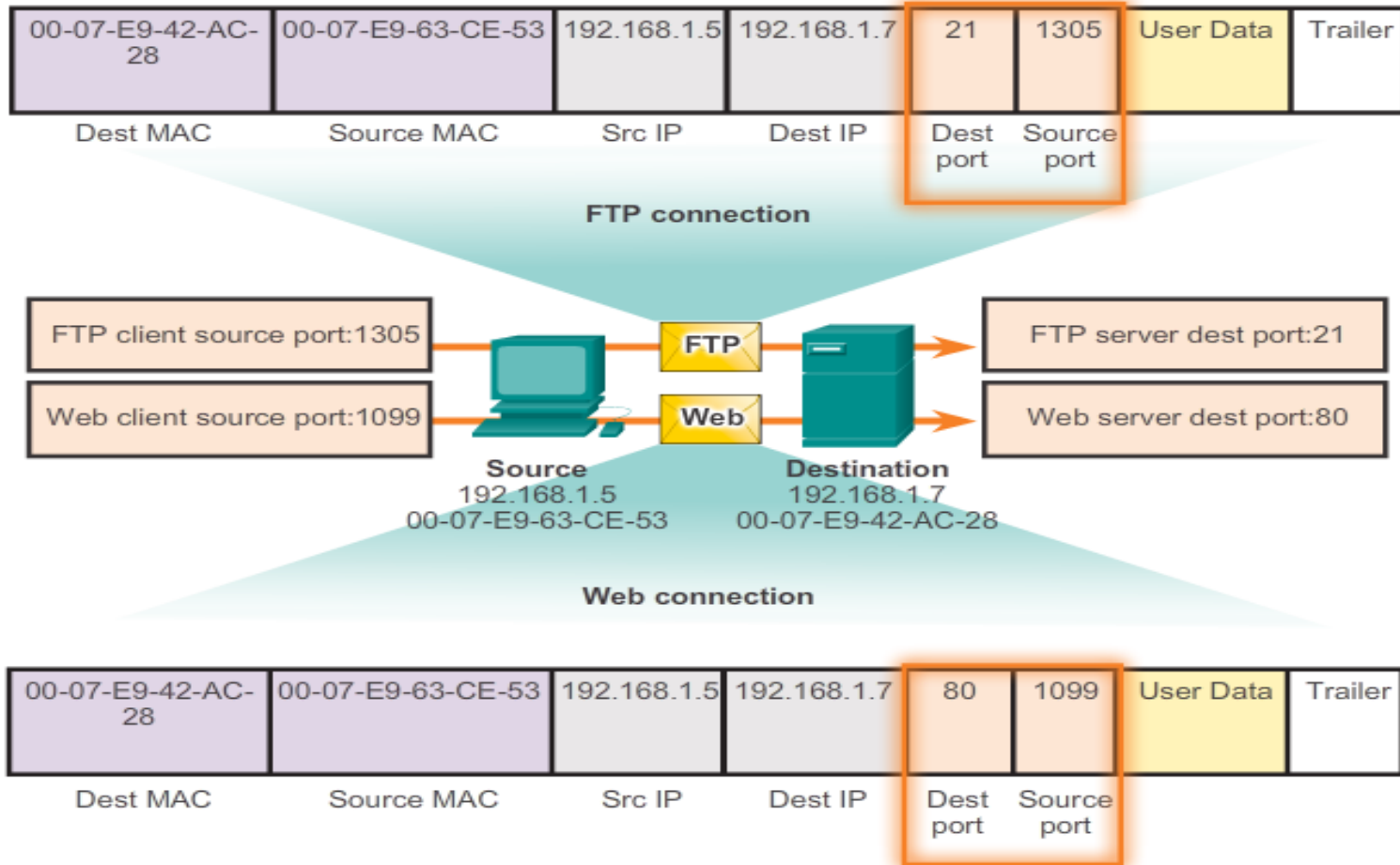
Source Port (16)		Destination Port (16)	
Sequence Number (32)			
Acknowledgement Number (32)			
Header Length (4)	Reserved (6)	Control Bits (6)	Window (16)
Checksum (16)		Urgent (16)	
Options			
Application Layer Data			

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

Checksum: 0xfe88 [validation disabled]

Checksum (16 bita)
– Računa checksum-u zaglavlju i data polju.

PORTOVI



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:

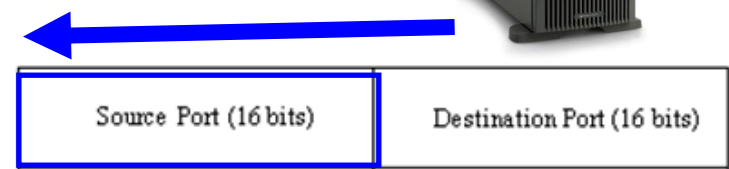
53	DNS
161	SNMP
531	AOL Instant Messenger, IRC

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

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

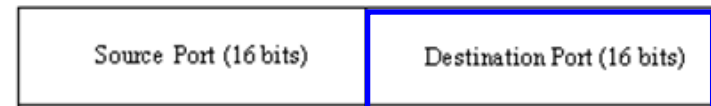
DODELA PORTA

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



Private/Dynamic Port
Number

Well Known ili
Registered Port

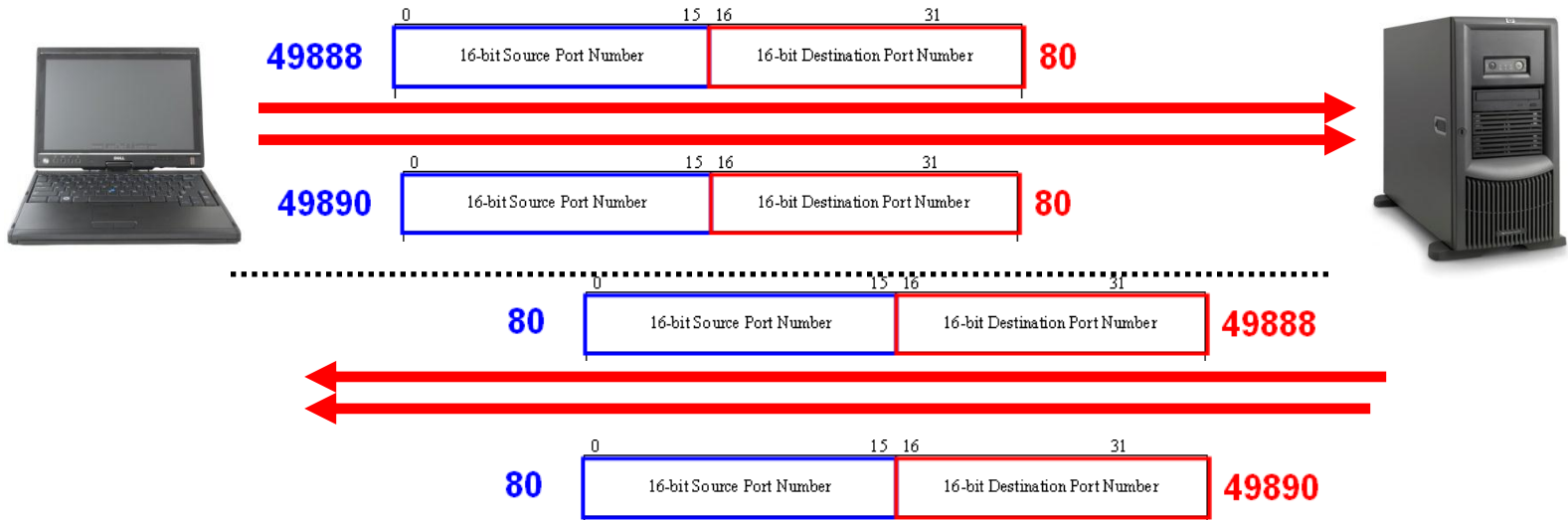
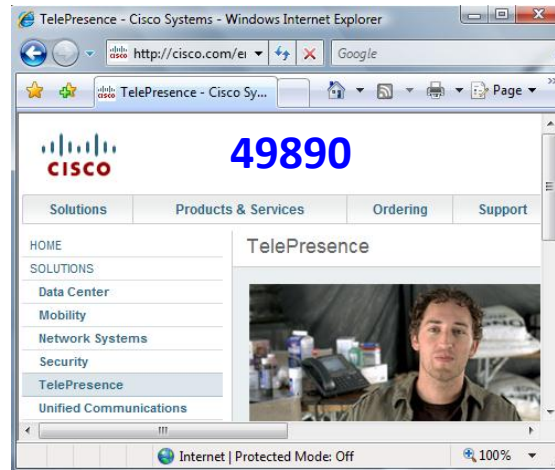


Well Known ili
Registered Port

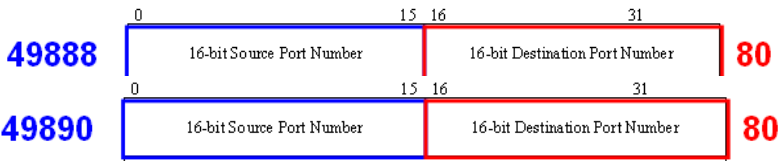
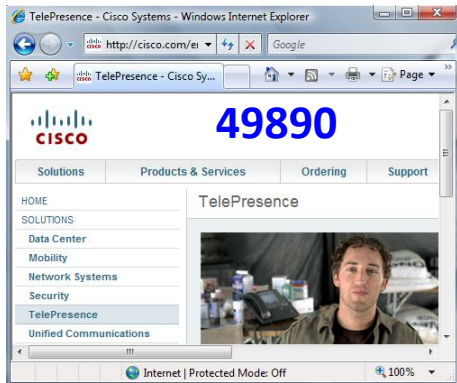
Private/Dynamic Port
Number

- **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)

USPOSTAVLJANJE VIŠE SESIJA



USPOSTAVLJANJE VIŠE SESIJA



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

Active Connections

TCP
ili
UDP

Proto	Local Address	Source Port	Foreign Address	Destination Port	Connection 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

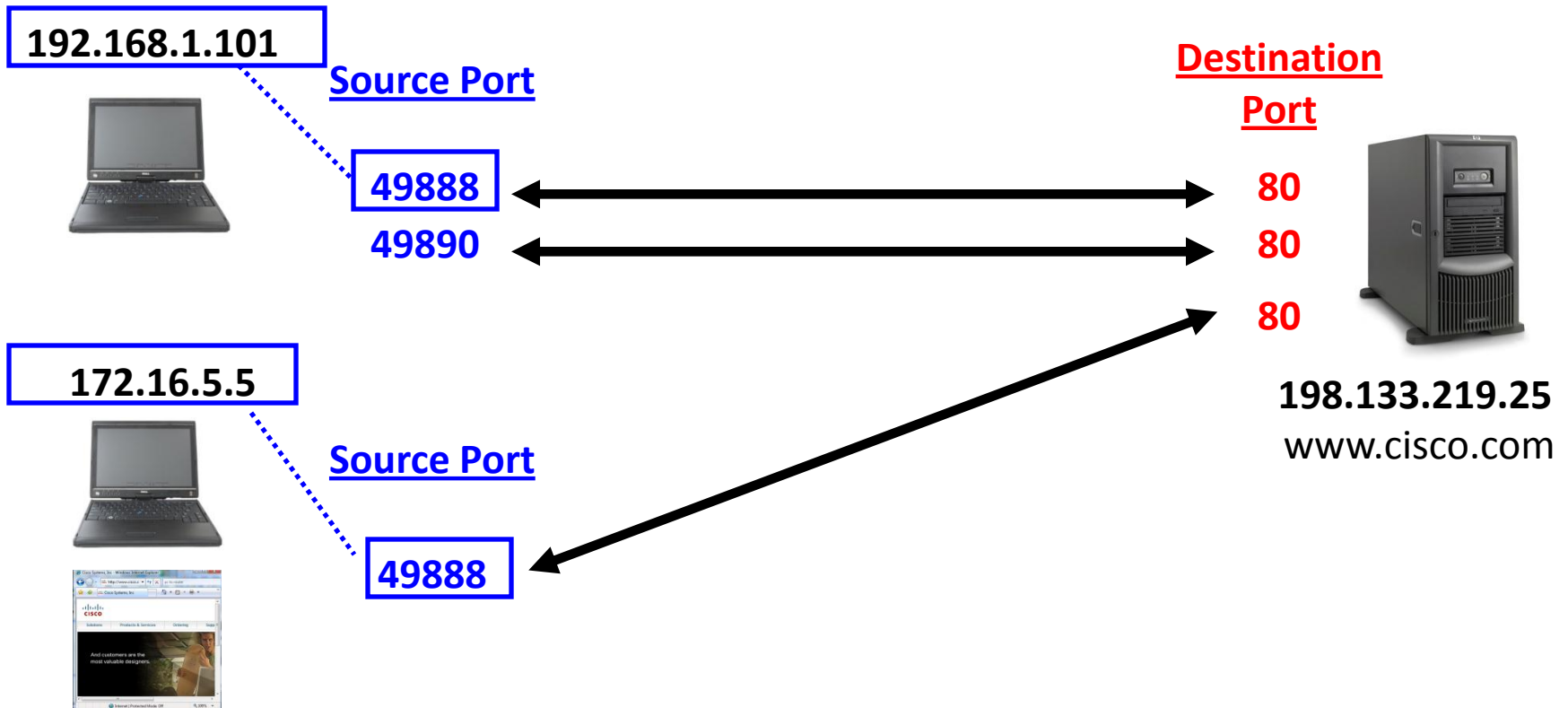
Source IP (points to 192.168.1.101)
Destination IP (points to 198.133.219.25)

SOCKET

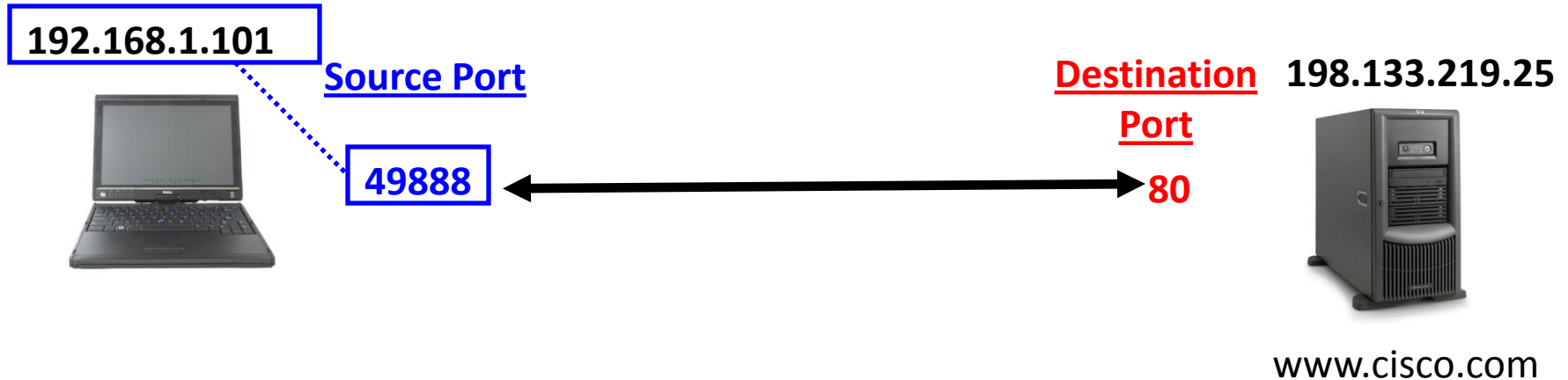


Šta obezbeđuje da svaka konekcija bude jedinstvena?

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

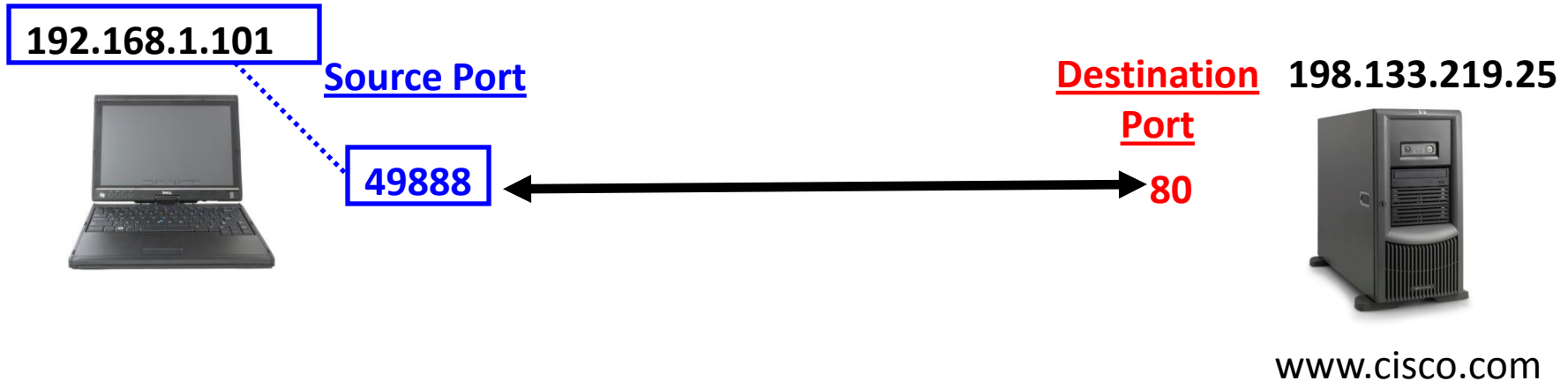


SOCKET



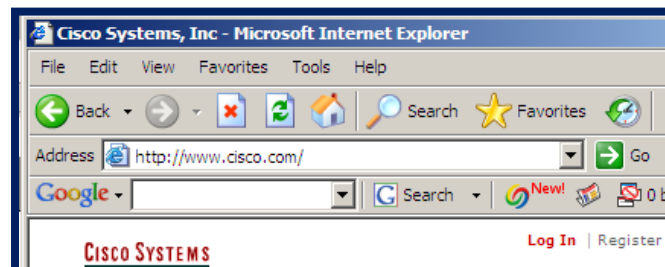
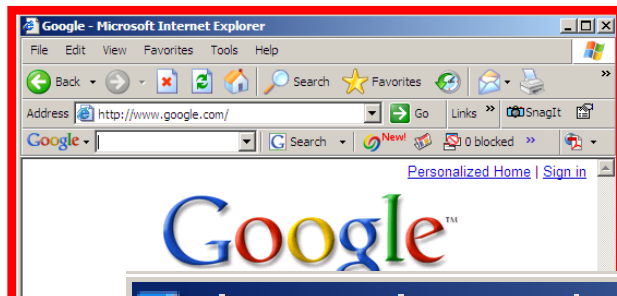
- Kombinovanjem broja porta na transportnom sloju i IP adrese na mrežnom sloju se na jedinstven način identifikuje aplikacija koja se izvršava
 - Kombinacija IP adrese i broja porta zove se **socket**.
- Komunikacija(flow) između dve aplikacije se na jedinstven način identifikuje koristeći izvornu i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



TCP
ili
UDP

```
C:\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

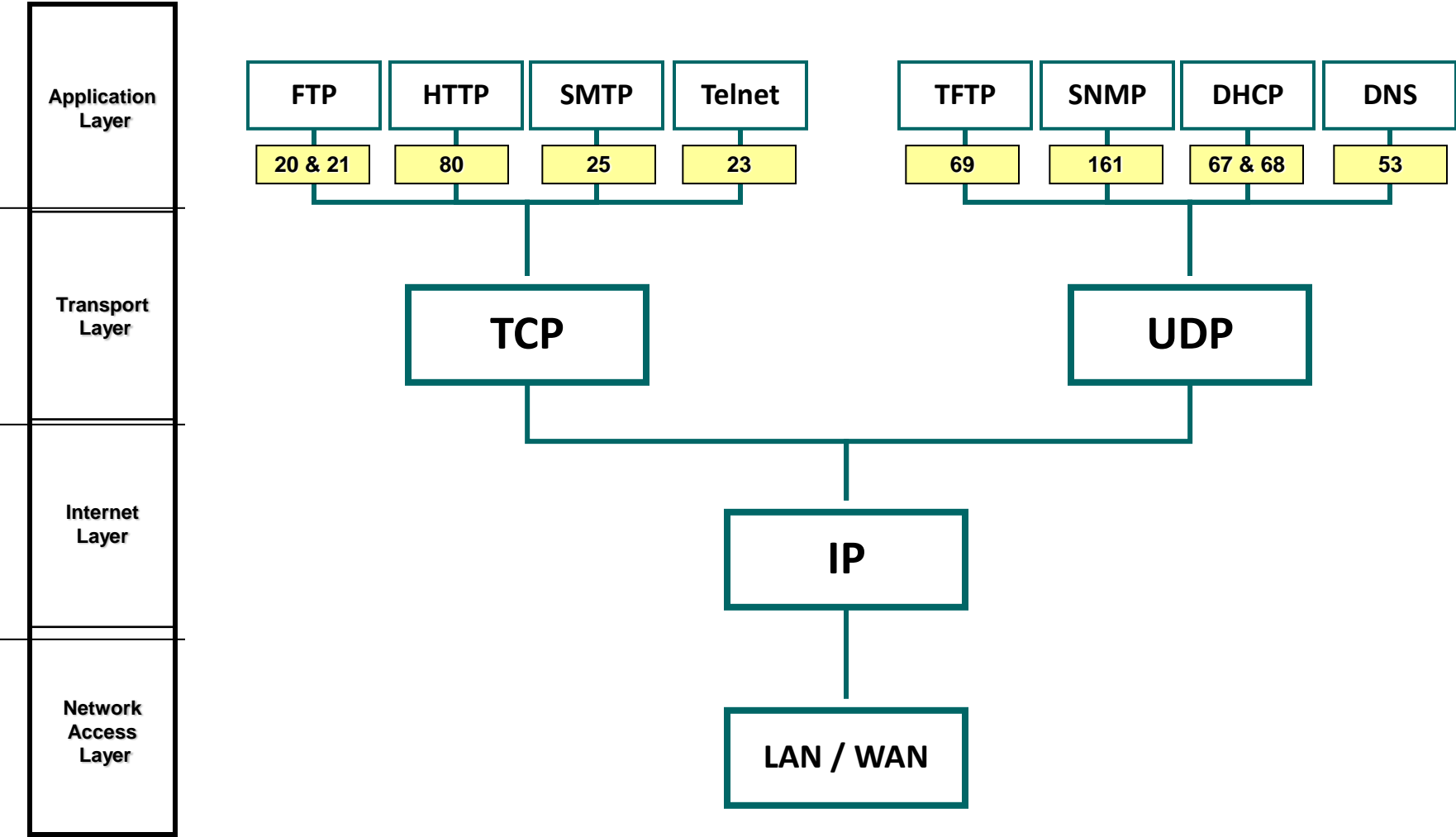
- **Napomena:** Kada učitavamo web stranu i njene objekte obično se uspostavljaju nekoliko TCP sesije.

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

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

```
C:\>
```

- 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](#)