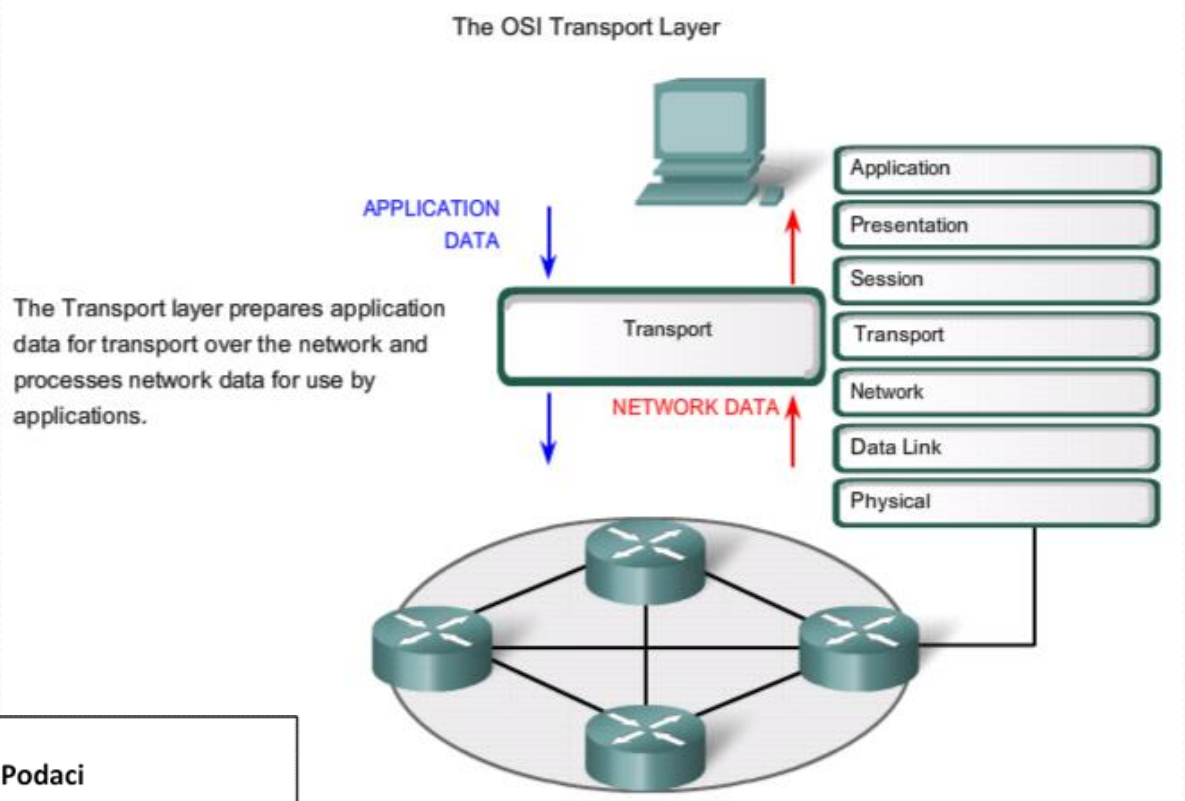
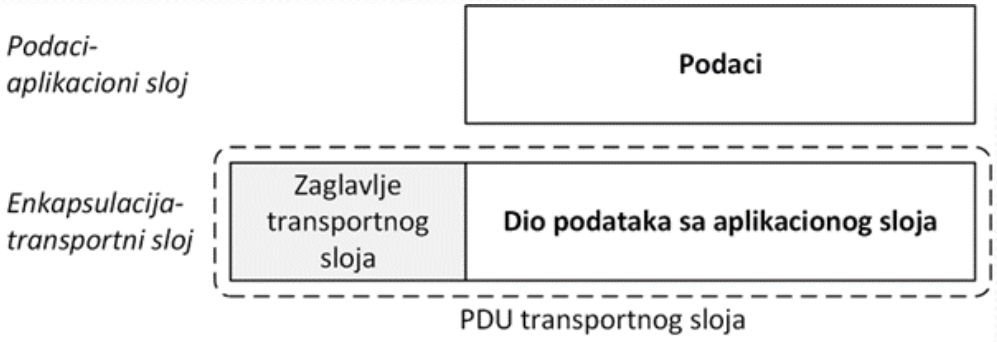
RAČUNARSKE MREŽE

08 – Transportni sloj

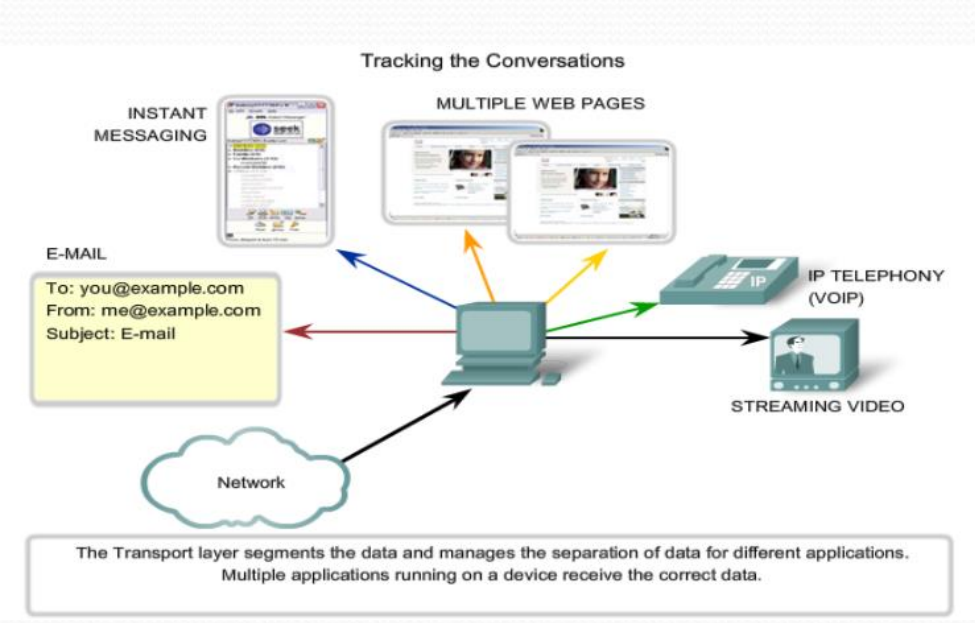
Uvod

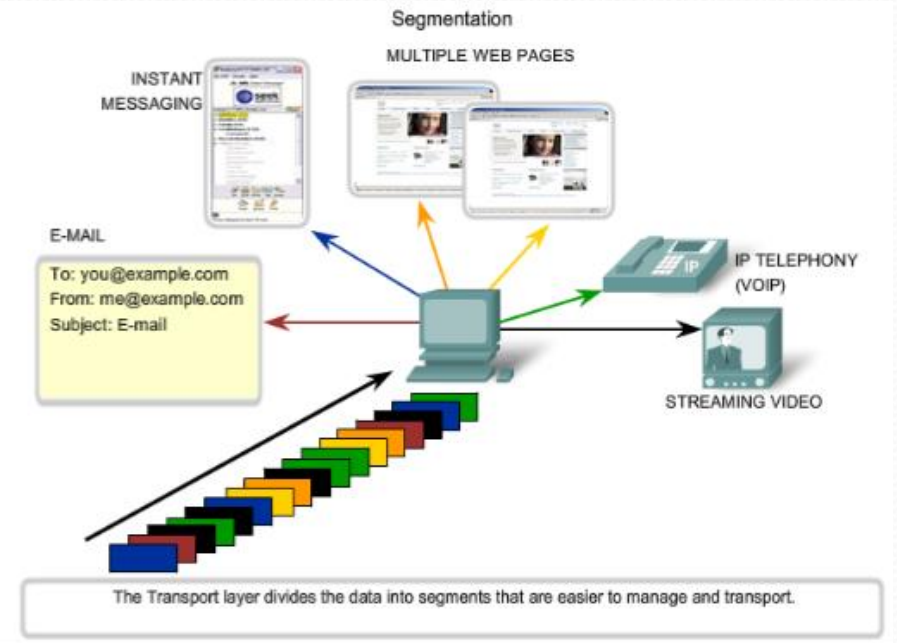

The OSI Transport Layer
The Transport layer prepares application data for transport over the network and processes network data for use by applications.
APPLICATION DATA
Transport
NETWORK DATA
Application
Presentation
Session
Transport
Network
Data Link
Physical


Podaci-
aplikacioni sloj
Podaci
Enkapsulacija-
transportni sloj
Zaglavlje transportnog sloja
Dio podataka sa aplikacionog sloja
PDU transportnog sloja

Funkcije transportnog sloja

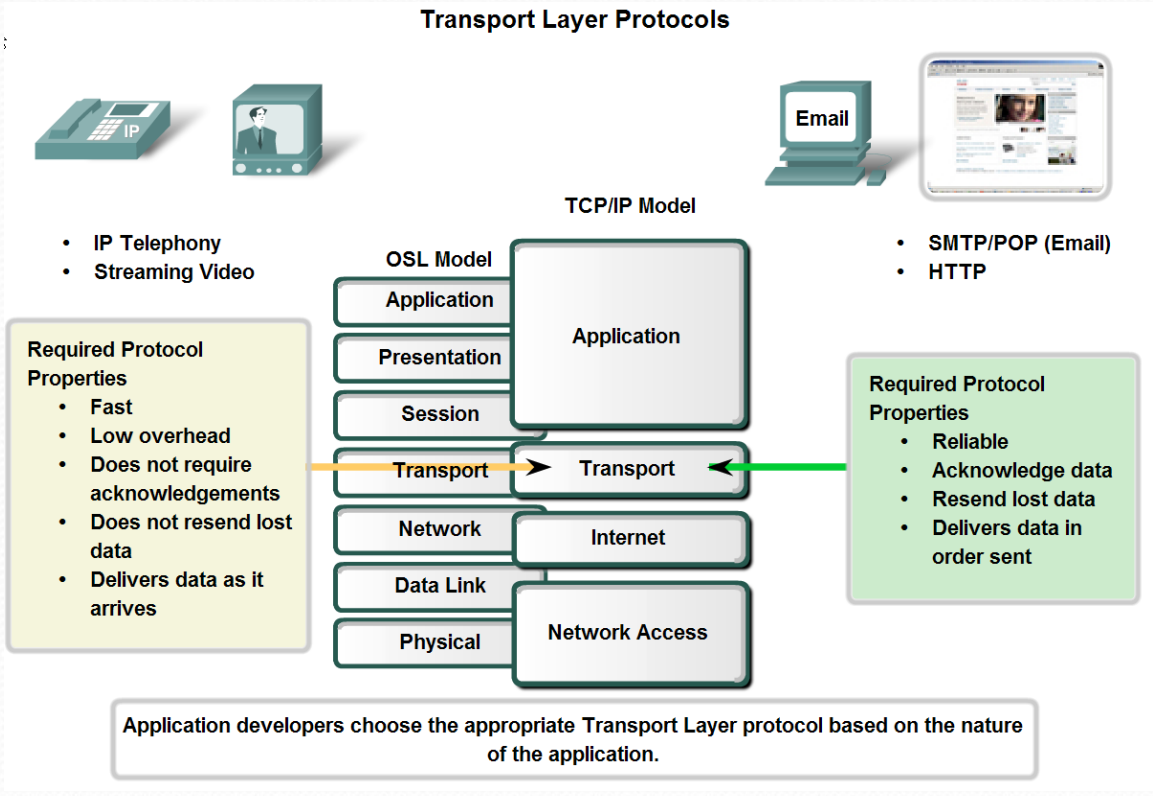
- odluka o (ne)pouzdanom prenosu na osnovu prirode aplikacije – izbor između TCP-a i UDP-a
- identifikovanje različitih aplikacija (portovi)
- Segmentacija podataka aplikacionog sloja



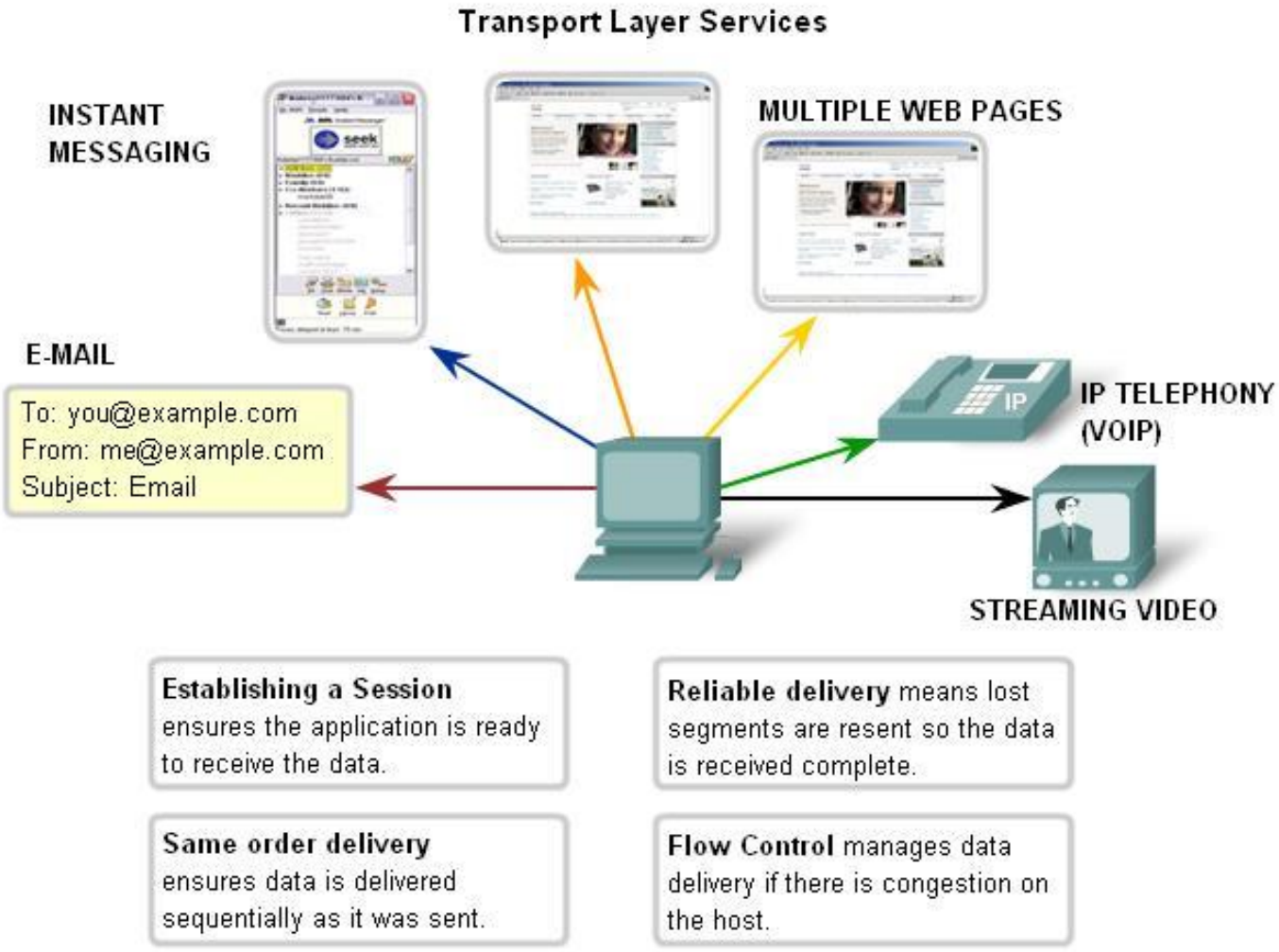


(Ne)pouzdan prenos

- Različite aplikacije imaju različite zahtjeve za svoje podatke
- Na osnovu prirode aplikacije bira se odgovarajući protokol transportnog sloja



Četiri glavne usluge pouzdanog prenosa



1. Uspostavljanje sesije
2. Pouzdana isporuka
3. Isporuka segmenata u istom redoslijedu u kojem su poslani
4. Kontrola toka

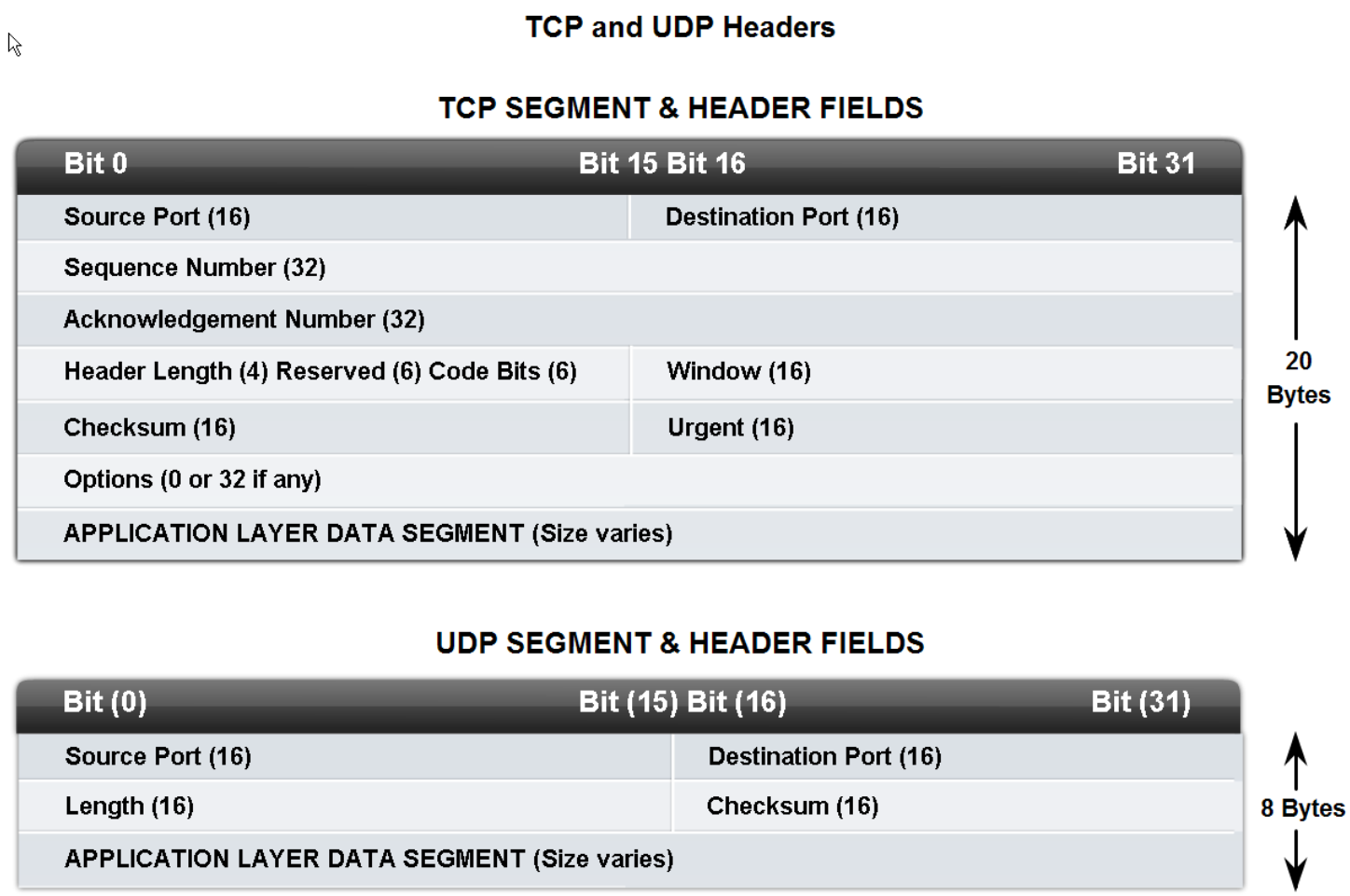
Protokoli transportnog sloja – TCP i UDP

- Oba upravljaju komunikacijom između različitih aplikacija

- TCP (*Transmission Control Protocol*)
- *Osobine:*
  - *connection-oriented* protokol
  - dostavljanje segmenata u originalnom redoslijedu (vrši reasembliranje)
  - pouzdana isporuka
  - kontrola toka
- *header* se sastoji od 20 bajtova
- Aplikacije: *Web browser*, *E-mail*, Prenos fajlova

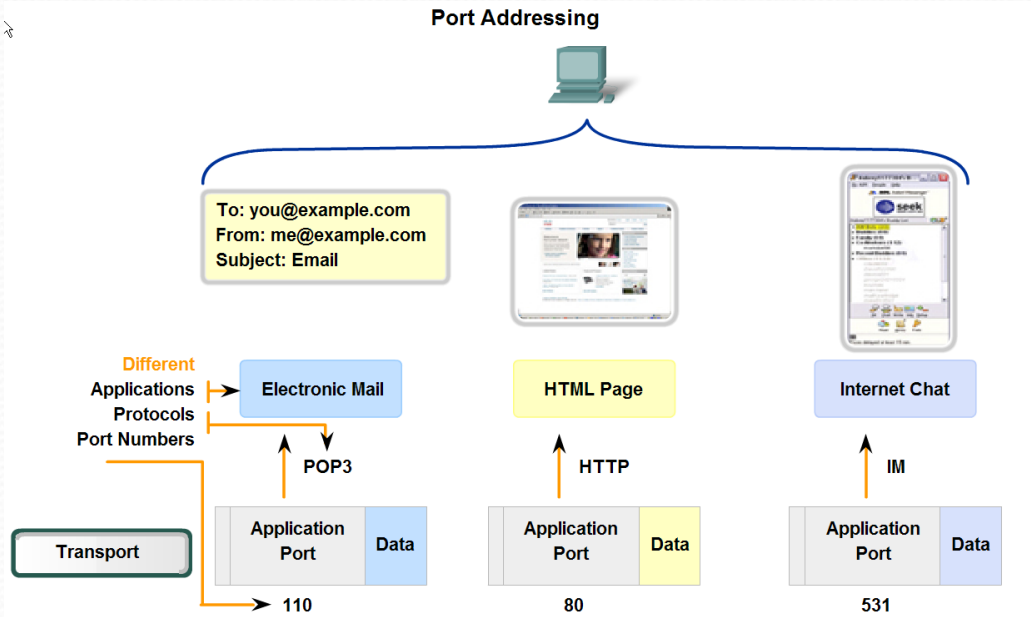
- UDP (*User Datagram Protocol*)
- *Osobine:*
  - *connectionless* protokol
  - *best effort*
- malo opterećenje (*header* samo 8 bajtova)
- Aplikacije: DNS, VoIP, Video *streaming*

TCP i UDP zaglavlja



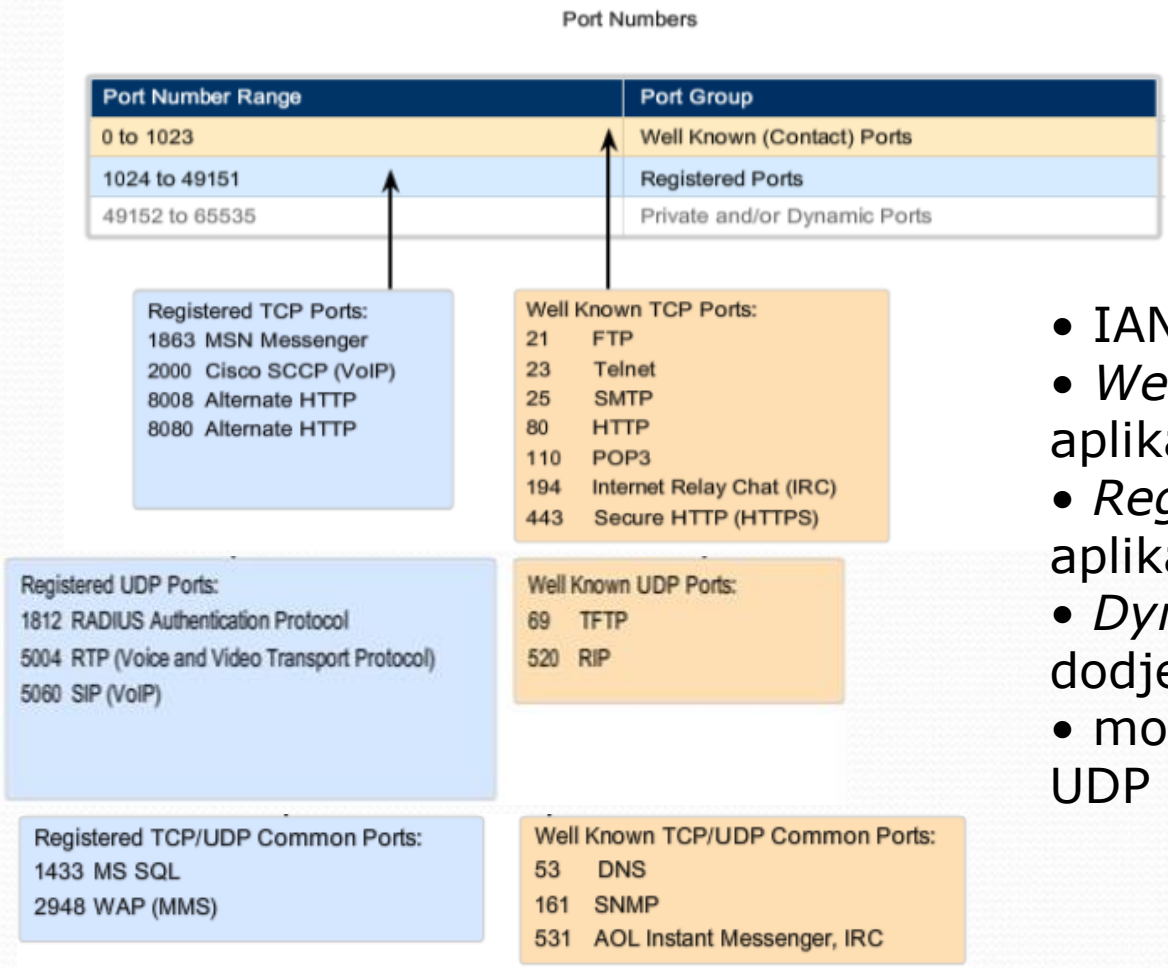
Portovi

- Jedinstveno identifikuju aplikacije koje komuniciraju
- *Source* i *destination*
- Serverski procesi imaju statičke portove, dok klijenti dinamički dobijaju port za svaku konverzaciju
- IP adresa + port = *socket* (npr. 192.168.1.20:80)



Data for different applications is directed to the correct application because each application has a unique port number.

Portovi (2)



- IANA
- *Well known* ports – servisi i aplikacije
- *Registred* – individualne aplikacije
- *Dynamic* – dinamičko dodjeljivanje klijentima
- moguće korištenje i TCP i UDP (npr. DNS)

Portovi (3)

- **netstat**

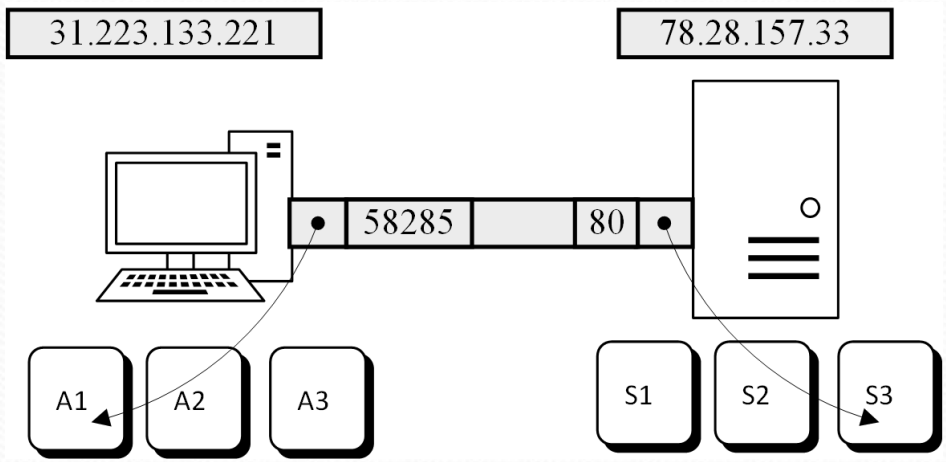
Portovi (3)

- **Komandne opcije komande netstat**

Opcija	Opis
-a	Prikazuje sve konekcije i portove na kojima se osluškuje
-b	Prikazuje program/proces koji je povezan sa kreiranjem konekcije
-e	Prikazuje Ethernet statistiku
-f	Prikazuje imena odredišnih hostova u FQDN (Fully Qualified Domain Name) formi
-n	Prikazuje imena odredišnih hostova u numeričkoj formi
-o	Prikazuje u dodatnoj koloni ID procesa koji je vlasnik konekcije
-p proto	Prikazuje konekcije samo za protokol specificiran parametrom proto, validne vrijednosti su TCP, UDP, TCPv6, UDPv6. Ako se ova opcija koristi u kombinaciji sa -s, onda se mogu navesti i dodatni protokoli IP, IPv6, ICMP, ICMPv6
-q	Prikazuje sve konekcije, portove na kojima se osluškuje, kao i povezane TCP portove na kojima se ne osluškuje konekcija
-r	Prikazuje tabelu rutiranja hosta
-s	Prikazuje statistiku po protokolima IP, IPv6, ICMP, ICMPv6, TCP, UDP, TCPv6, UDPv6. U kombinaciji sa opcijom -p može se suziti prikaz na samo jedan od mogućih protokola.
interval	Periodično prikazuje podatke u intervalima zadatim ovim parametrom, vrijednost se zadaje u sekundama

Soketi

- jednoznačan identifikator aplikacije na nekom hostu predstavljen je kombinacijom IP adrese hosta i broja porta koji aplikacija koristi. Primjer -78.28.157.33:80
- Za komunikaciju od veb čitača prema veb serveru, izvorišna aplikacija (A1, veb čitač) je predstavljena soketom 31.223.133.221:58285, nalazi se na hostu sa IP adresom 31.223.133.221 i koristi dinamički port 58285. Odredišna aplikacija (S3, veb server) je predstavljena soketom 78.28.157.33:80, nalazi se na hostu sa IP adresom 78.28.157.33 i koristi dobro poznati port 80.



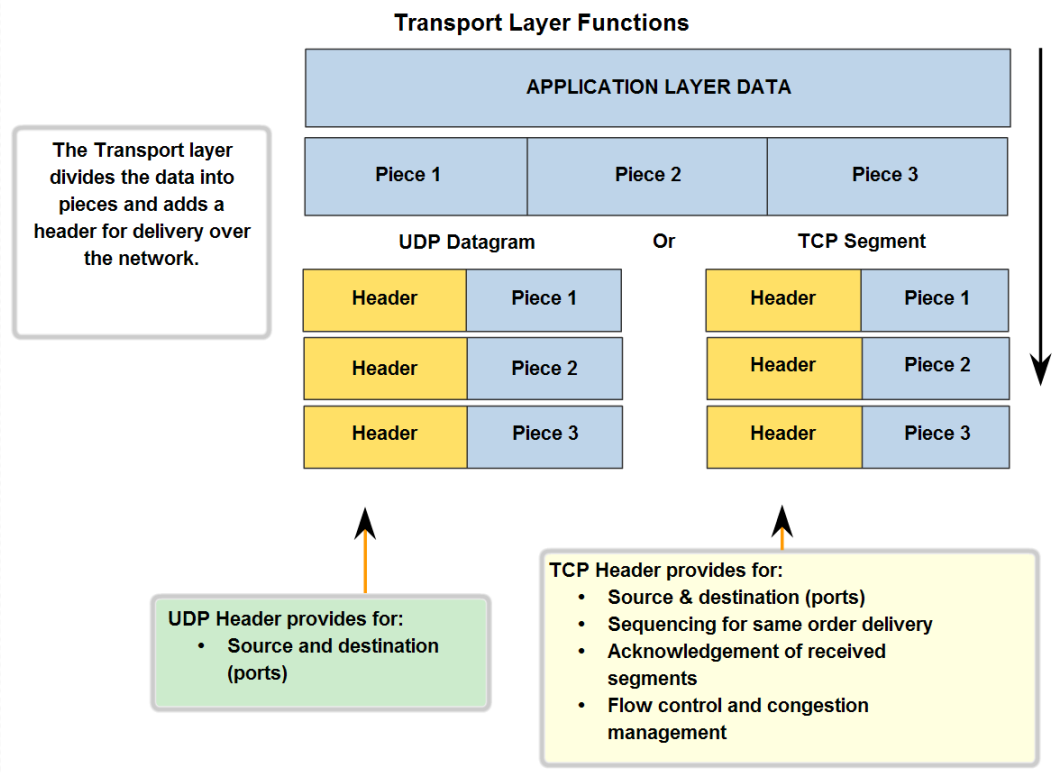
Transportni protokoli

- Aplikacije na internetu koriste jedan, a u nekim slučajevima mogu da koriste i oba pomenuta transportna protokola.

Port	Protokol	Internet servis/aplikacija
20, 21	TCP	File Transfer Protocol (FTP)
22	TCP, UDP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	TCP, UDP	Domain Name System (DNS)
67, 68	UDP	Dynamic Host Configuration Protocol (DHCP)
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	HyperText Transfer Protocol (HTTP)
110	TCP	Post Office Protocol (POP3)
123	UDP	Network Time Protocol (NTP)
143	TCP, UDP	Internet Message Access Protocol (IMAP)
161, 162	UDP	Simple Network Management Protocol (SNMP)
443	TCP	HTTP Secure (HTTPS)

Segmentacija & reasembliranje

- TCP – *sequence numbers*
- UDP – ne postoji reasembliranje



TCP zaglavlje

H Length

Header Length - Specifies the length of the segment header in bytes

Flags

Used in session management and in the treatment of segments.

Window Size

Is the value of the dynamic window - how many octets can be sent before waiting for acknowledgement.

TCP Checksum

Used for error-checking the header and data.

Urgent Pointer

Only used with an URG (Urgent) flag.

Sequence Number

Specifies the number of the last octet (byte) in a segment.

Acknowledgment Number

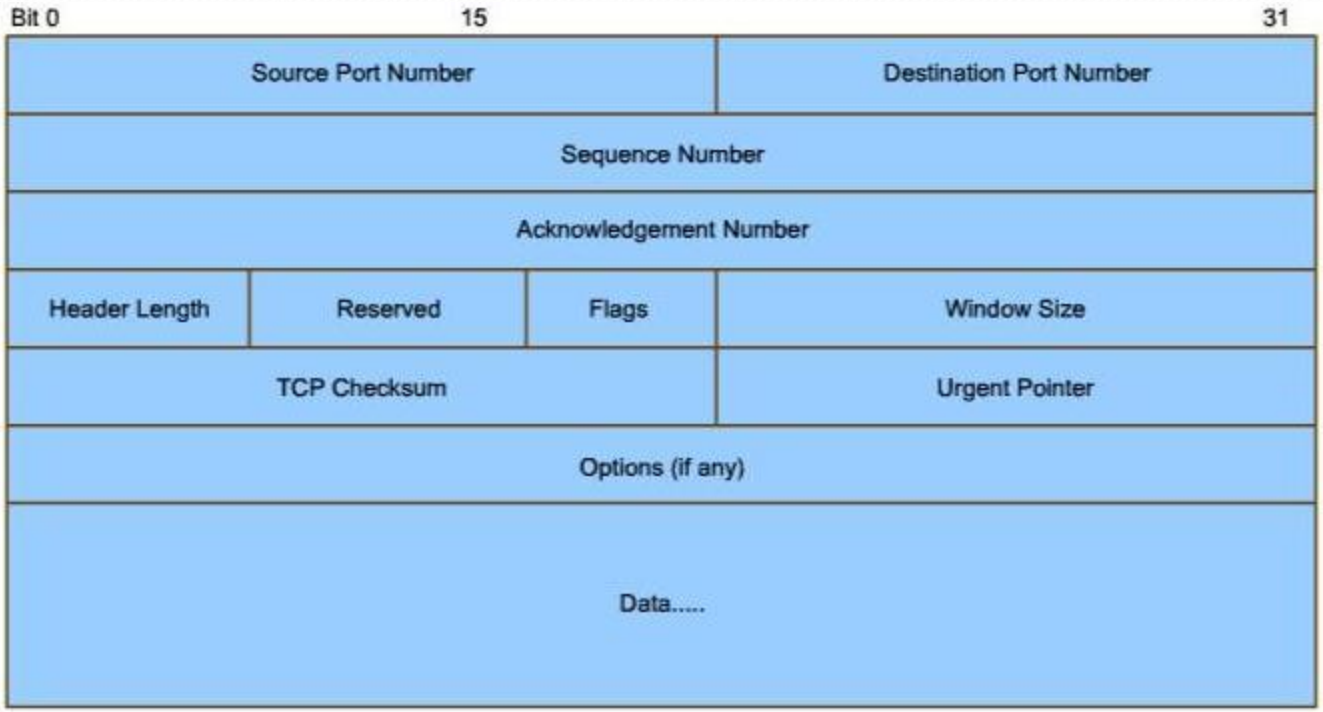
Specifies the next octet expected by the receiver.

Source Port Number

TCP session on the device that opened a connection - normally a random value above 1023.

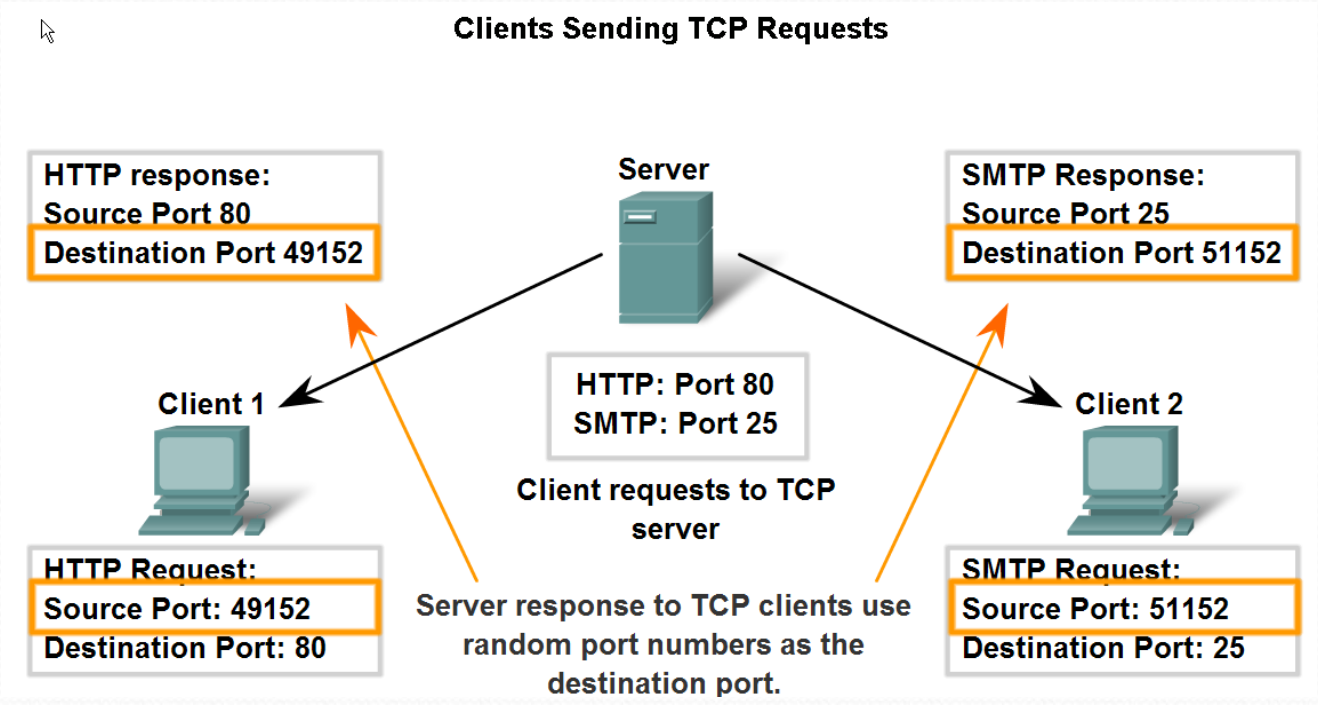
Destination Port Number

Identifies the upper layer protocol or application on remote site.



TCP serveri

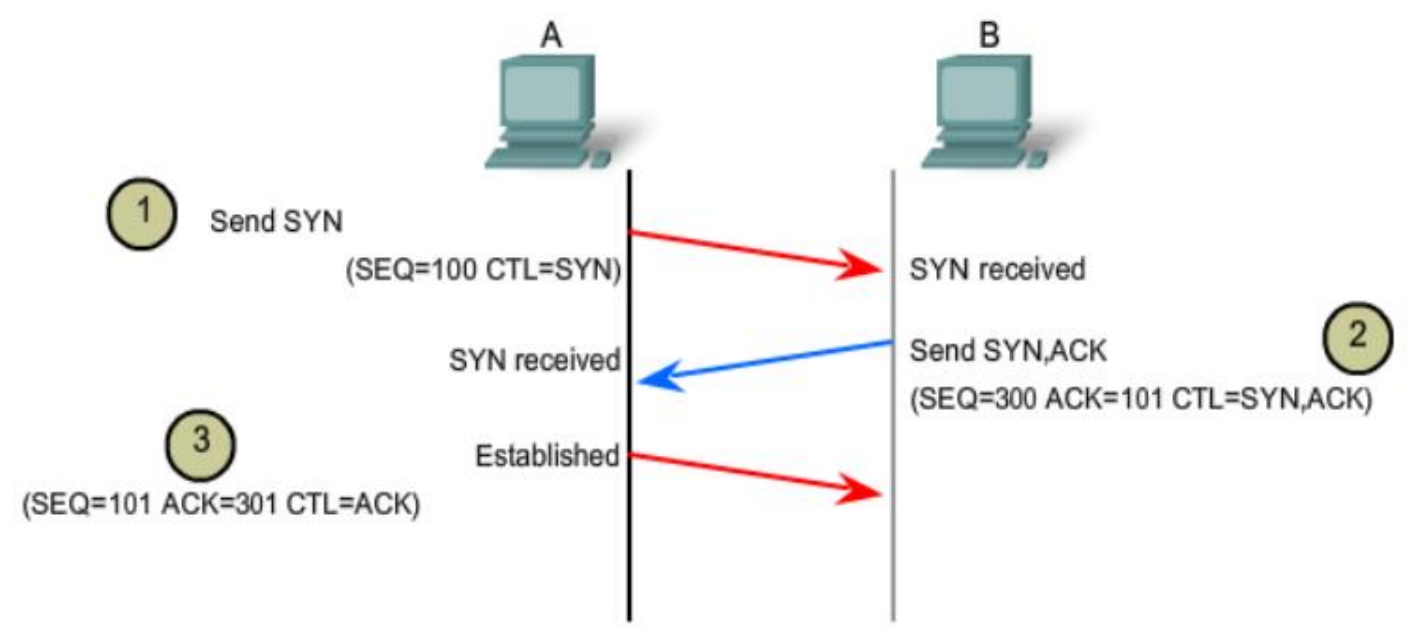
- Jedan server ne može imati isti broj porta za dvije svoje različite usluge!
- Sigurnost servera se povećava ako se odobri pristup samo autorizovanim korisnicima tih usluga



Uspostavljanje konekcije

- *three-way handshake*:

1. utvrđivanje da je odredišni uređaj na mreži
2. potvrđivanje da taj uređaj nudi aktivnu uslugu i da prima zahtjeve na traženom portu
3. obavještavanje uređaja da želimo da uspostavimo komunikaciju



Flags

- Unutar TCP zaglavlja postoji osam jednobitnih polja koja sadrže kontrolne informacije koje se koriste za upravljanje TCP procesima. Šest nama bitnih polja su:
  - URG – označava segmente koji se odmah procesiraju (urgent)
  - ACK – potvrda uspješnog primanja segmenta
  - PSH – "guranje" podataka aplikacionom sloju
  - RST – resetovanje konekcije
  - SYN – sinhronizacija, pri uspostavljanju veze
  - FIN – označava da nema više podataka za slanje, pri zatvaranju veze

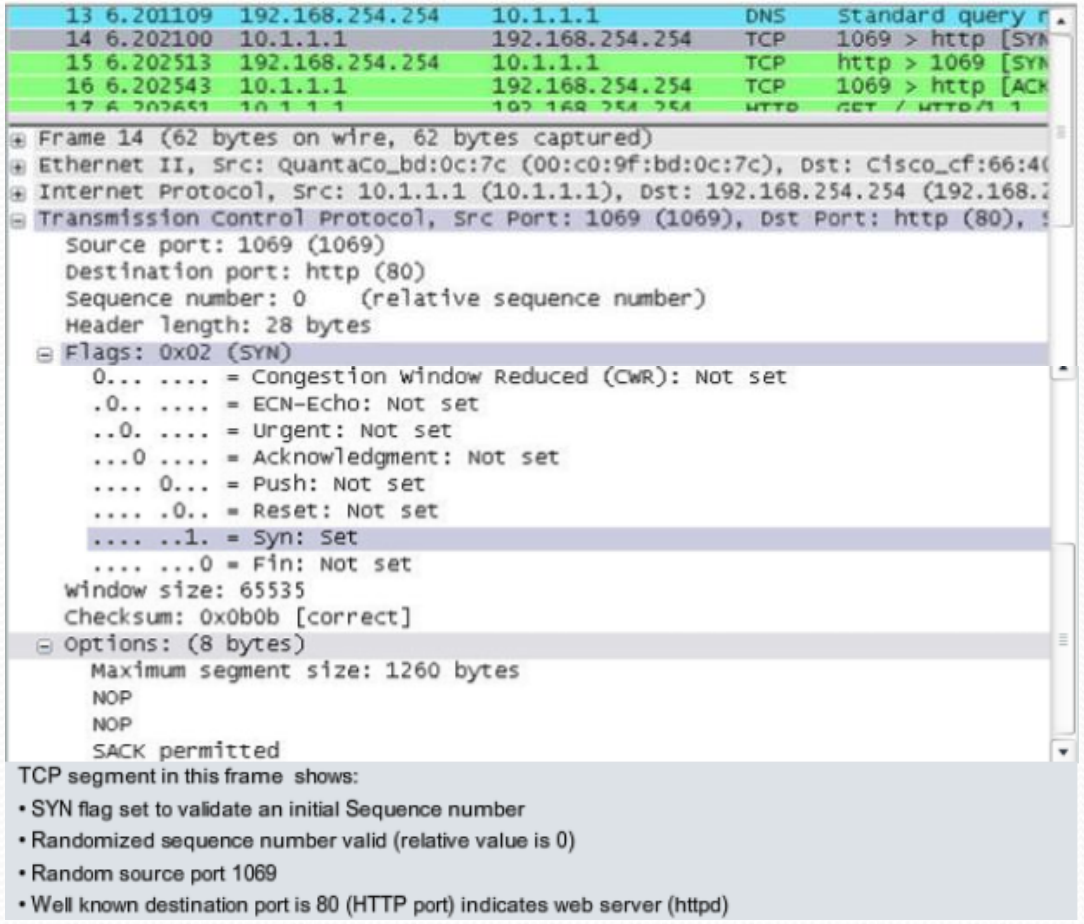
Moguća stanja TCP konekcije

Stanje	Opis
CLOSED	Zatvorena konekcija
LISTEN	Osluškivanje konekcije od strane servera
SYN RCVD	Zahtjev za otvaranje konekcije je stigao serveru, čeka se potvrda
SYN SENT	Zahtjev za otvaranje konekcije je poslan serveru
ESTABLISHED	Uspostavljena konekcija, omogućena je razmjena podataka
FIN WAIT 1	Lokalna aplikacija je završila sa slanjem podataka
FIN WAIT 2	Druga strana je prihvatila prekid konekcije
TIMED WAIT	Čekanje da isteknu tajmeri nakon zatvaranja konekcije
CLOSING	Obje strane su istovremeno pokušale prekid konekcije
CLOSE WAIT	Druga strana je inicirala prekid konekcije
LAST ACK	Čekanje na potvrdu prekida konekcije od druge strane

TCP three-way handshake (1)

- Primjer : SYN

TCP 3-way Handshake (SYN)



TCP segment in this frame shows:

- SYN flag set to validate an initial Sequence number
- Randomized sequence number valid (relative value is 0)
- Random source port 1069
- Well known destination port is 80 (HTTP port) indicates web server (httpd)

TCP three-way handshake (2)

- Primjer :
  SYN + ACK

TCP 3-way Handshake (SYN, ACK)

```
13 6.201109  192.168.254.254  10.1.1.1          DNS   Standard query
14 6.202100  10.1.1.1         192.168.254.254   TCP   1069 > http [S
15 6.202513  192.168.254.254  10.1.1.1          TCP   http > 1069 [S
16 6.202543  10.1.1.1         192.168.254.254   TCP   1069 > http [A
17 6.202651  10.1.1.1         192.168.254.254   HTTP  GET / HTTP/1.1

⊞ Frame 15 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: Cisco_cf:66:40 (00:0c:85:cf:66:40), Dst: QuantaCo_bd:0c:
⊞ Internet Protocol, Src: 192.168.254.254 (192.168.254.254), Dst: 10.1.1.1 (
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: 1069 (1069),
    Source port: http (80)
    Destination port: 1069 (1069)
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 28 bytes
  ⊟ Flags: 0x12 (SYN, ACK)
      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: 5840
    Checksum: 0x91a4 [correct]
  ⊟ Options: (8 bytes)
      Maximum segment size: 1460 bytes
      NOP
      NOP
```

- ACK flag set to indicate a valid Acknowledgement number
- Acknowledgement number response to initial sequence number as relative value of 1
- SYN flag set to indicate the Initial sequence number for the server to client session
- Destination port number of 1069 to corresponding to the clients source port
- Source port number of 80 (HTTP) indicating the web server service (httpd)

TCP three-way handshake (3)

- Primjer : ACK

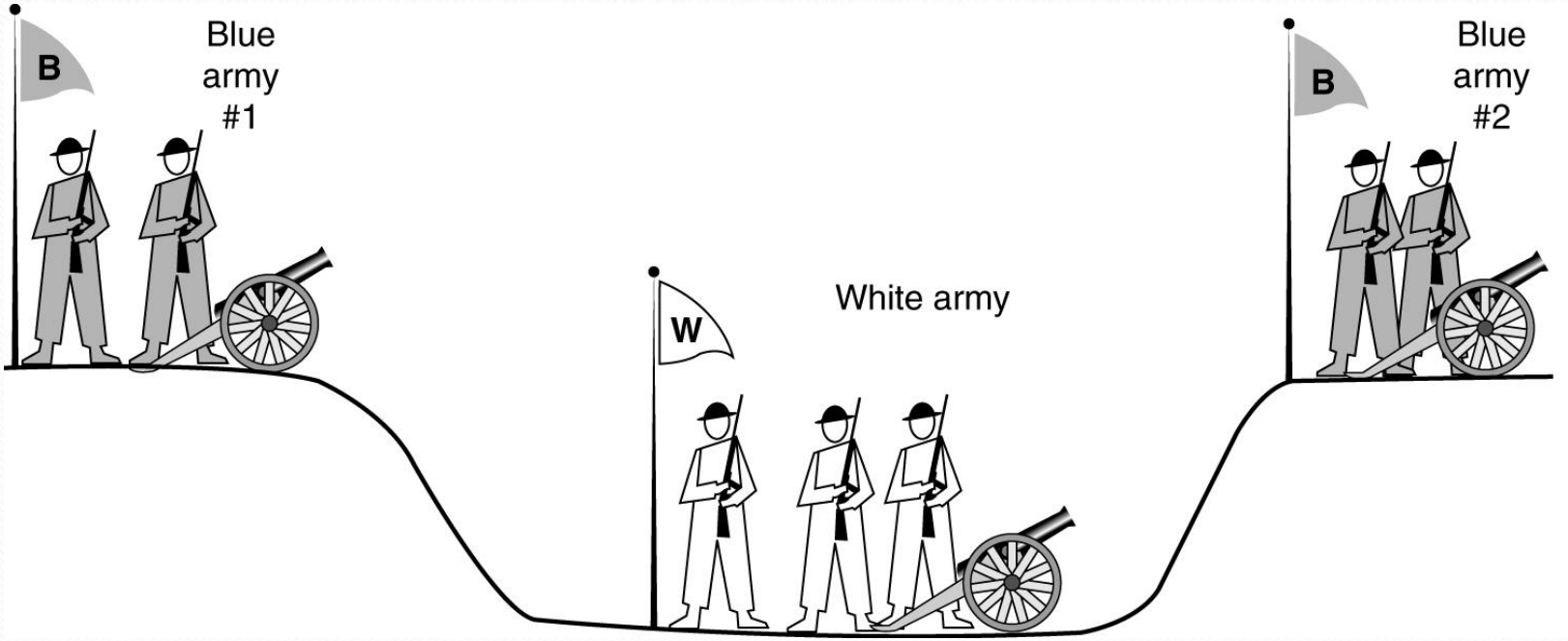
TCP 3-way Handshake (ACK)

```
    13 6.201109  192.168.254.254   10.1.1.1          DNS    Standard query re
    14 6.202100  10.1.1.1          192.168.254.254   TCP    1069 > http [SYN]
    15 6.202513  192.168.254.254   10.1.1.1          TCP    http > 1069 [SYN,
    16 6.202543  10.1.1.1          192.168.254.254   TCP    1069 > http [ACK]
    17 6.202651  10.1.1.1          192.168.254.254   HTTP   GET / HTTP/1.1
⊞ Frame 16 (54 bytes on wire, 54 bytes captured)
⊞ Ethernet II, Src: QuantaCo_bd:0c:7c (00:c0:9f:bd:0c:7c), Dst: Cisco_cf:66:40
⊞ Internet Protocol, Src: 10.1.1.1 (10.1.1.1), Dst: 192.168.254.254 (192.168.25
⊟ Transmission Control Protocol, Src Port: 1069 (1069), Dst Port: http (80), Se
    Source port: 1069 (1069)
    Destination port: http (80)
    Sequence number: 1    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊟ Flags: 0x10 (ACK)
      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: 65535
    Checksum: 0xd538 [correct]
  ⊟ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 15]
      [The RTT to ACK the segment was: 0.000030000 seconds]
```

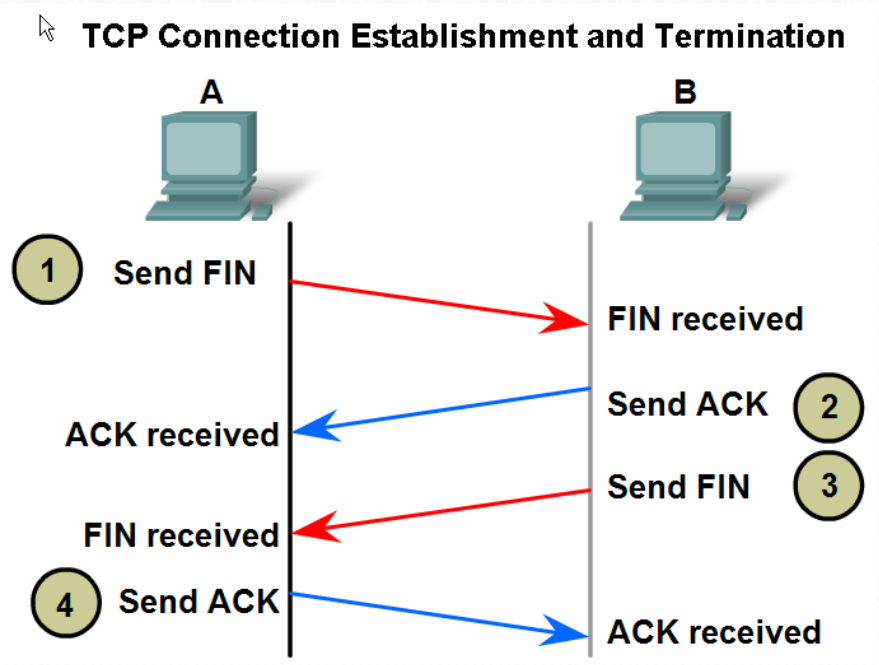
- ACK flag set to indicate a valid Acknowledgement number
- Acknowledgement number response to initial sequence number as relative value of 1
- Source port number of 1069 to corresponding
- Destination port number of 80 (HTTP) indicating the web server service (httpd)

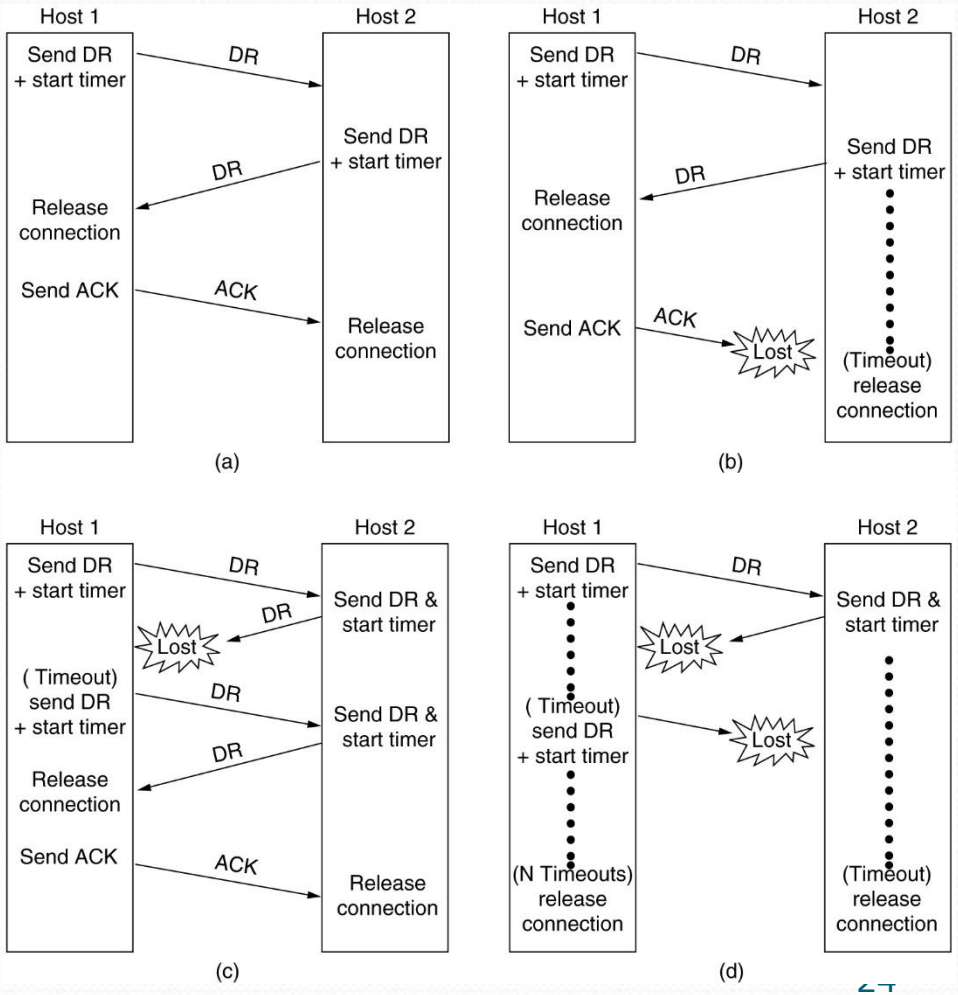
Zatvaranje konekcije

- Problem dvije armije

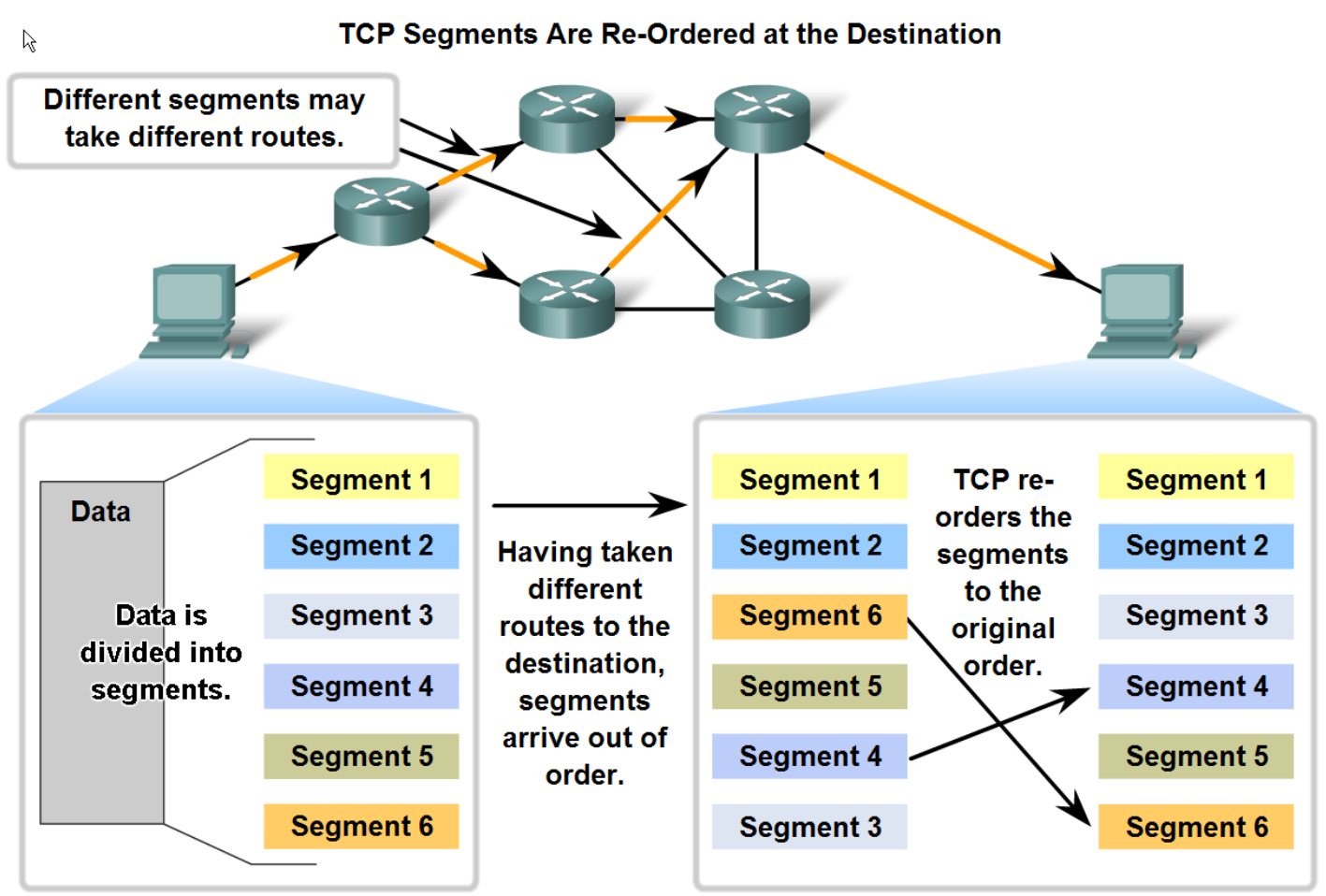


Zatvaranje konekcije (2)





TCP – reasembliranje segmenata



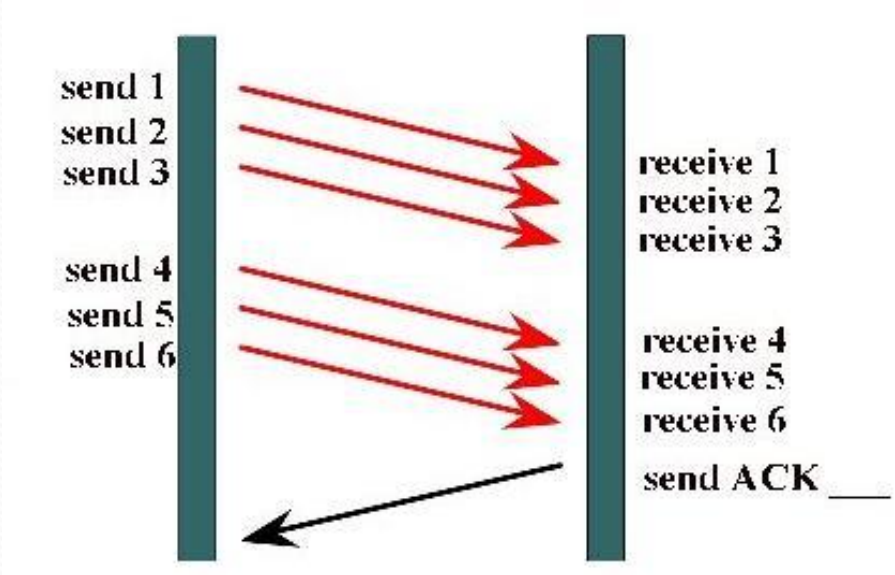
TCP – retransmisija

- U originalnoj TCP implementaciji host šalje bajt, stavlja njegovu kopiju u red za ponovno slanje i starta tajmer. Ako se primi potvrda, bajt se briše iz reda. U suprotnom, ponovo se šalje.
- Potvrđivanje svakog bajta vremenski zahtjevno => ideja da se primi sekvenca bajtova pa potvrdi samo zadnji (windowing)
- Odredišni host koji koristi TCP potvrđuje samo podatke u neprekidnom nizu bajtova (potvrđuju se samo bajtovi koji kompletiraju niz)
- Na primjer, ako se prime bajtovi sa sequence brojevima od 1500 do 3000 i od 3400 do 3500, ACK broj bi bio 3001.

TCP – Windowing (primjer)

window size – broj bajtova nakon kojih se očekuje potvrda

ACK *number* – redni broj sljedećeg očekivanog bajta



Ne potvrđuje se svaki bajt već samo šesti (window size = 6)!

=> ACK = 7

Pošiljalac odgovara sa rednim brojem bajta kojeg sljedećeg očekuje!

Ne miješati flag ACK (0-1) sa poljem ACKnowledgment Number (0 – 2^{32}-1)!

UDP protokol

- Kod primjene UDP protokola, PDU transportnog sloja se zove datagram.
- Vidi se da je UDP datagram dosta jednostavniji od TCP segmenta jer je izostavljena većina kontrolnih podataka.

Source port	Destination port
UDP length	UDP checksum
Data	

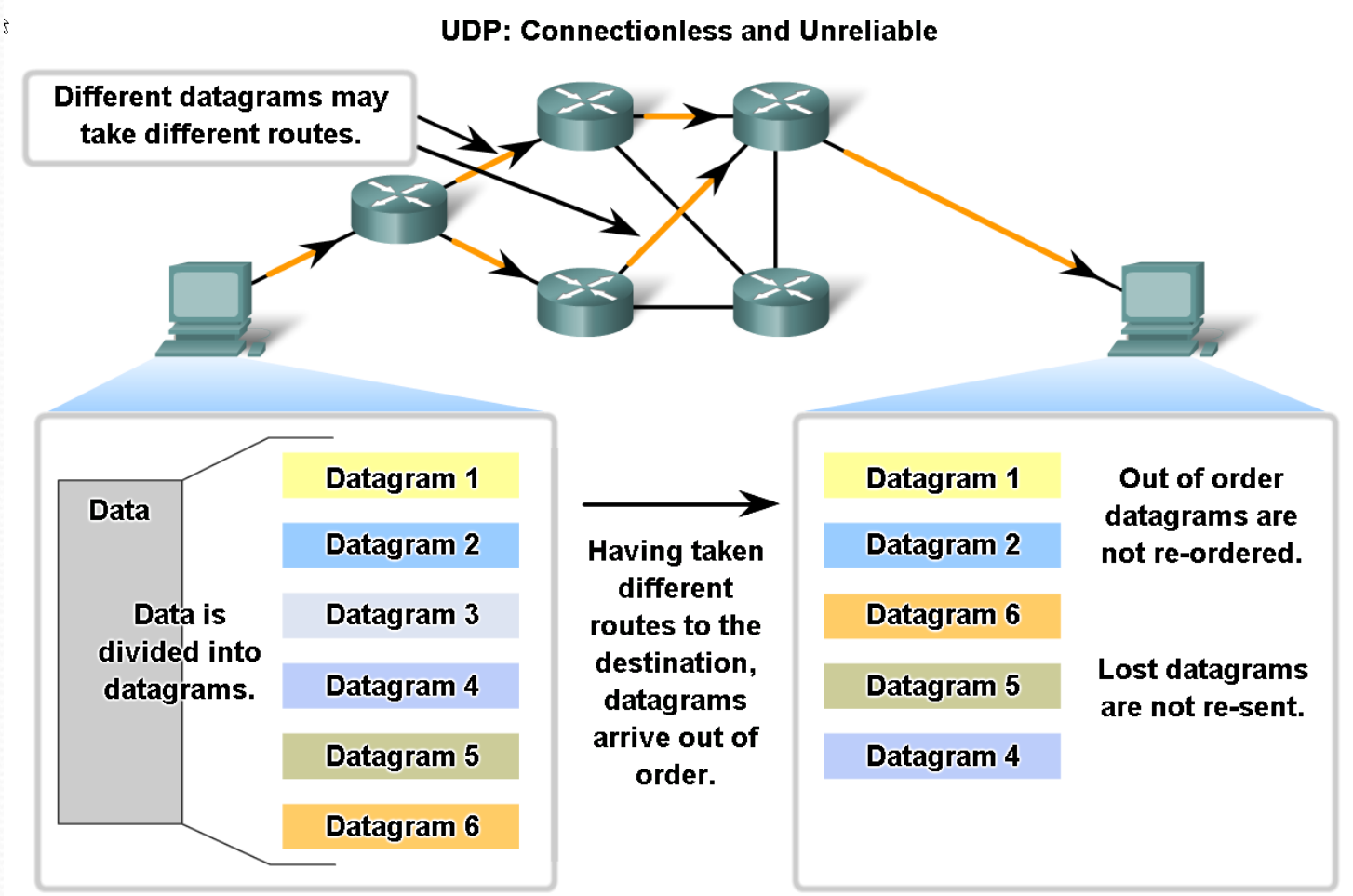
- Zahvaljujući jednostavnosti UDP datagrama, omogućena je brža obrada datagrama, a samim tim i brži rad aplikacija koje koriste UDP.
- Osim toga, povećana je efikasnost prenosa i smanjeno je opterećenje mreže dodatnim kontrolnim saobraćajem
- UDP se ne bavi detekcijom izgubljenih datagrama, kontrolom toka i kontrolom zagušenja, kao ni sortiranjem podataka na prijemnoj strani.
- Sve ove funkcionalnosti su odgovornost aplikacija koje koriste UDP.

UDP protokol

- manje opterećenje vs. pouzdanost
- Ne nudi retransmisiju, sekvenciranje i kontrolu toka
- Ne mora značiti da će komunikacija biti nepouzdana, samo znači da to nije obezbjeđeno na transportnom sloju

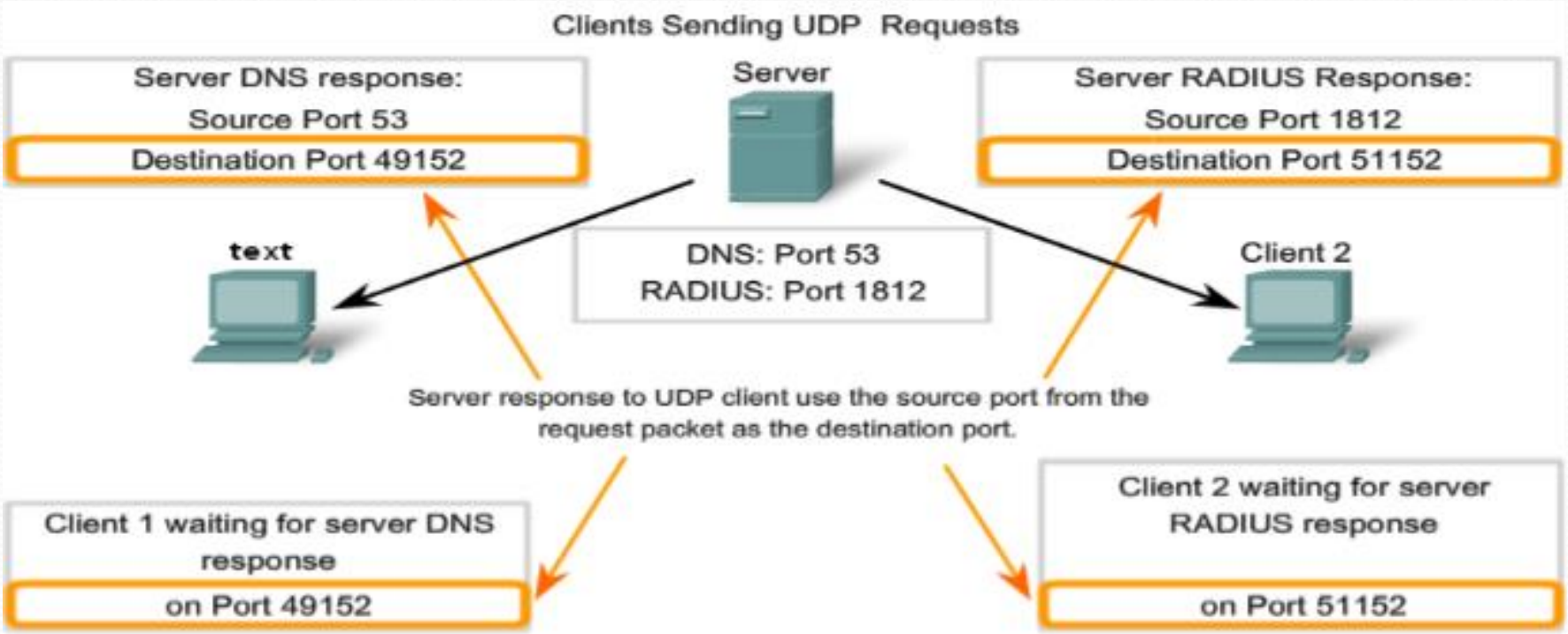
- Protokoli:
- *Domain Name System* (DNS)
- *Simple Network Management Protocol* (SNMP)
- *Dynamic Host Configuration Protocol* (DHCP)
- *Routing Information Protocol* (RIP)
- *Trivial File Transfer Protocol* (TFTP)
- *Online games*

UDP reasembliranje datagrama?



UDP serverski i klijentski portovi

- Identičan princip kao kod TCP-a



Primjer 2 – analiza mrežnog saobraćaja i identifikacija učesnika

C:\> **netstat -n**

Active Connections

Proto	Local Address	Foreign Address	State
TCP	192.168.1.101:1031	64.100.173.42:443	ESTABLISHED
TCP	192.168.1.101:1037	192.135.250.10:110	TIME_WAIT
TCP	192.168.1.101:1042	128.107.229.50:80	ESTABLISHED

- Kokalni računar, sa IP adresom 192.168.1.101, ima tri aktivne TCP konekcije, tj. komunicira sa tri različita hosta, i to:
  - host sa IP adresom 64.100.173.42, HTTPS saobraćaj (port 443), gdje je lokalni računar klijent, a odredišni je server, konekcija je uspostavljena i moguća je razmjena podataka (stanje konekcije je ESTABLISHED);
  - host sa IP adresom 192.135.250.10, POP3 saobraćaj (port 110), gdje je lokalni računar klijent, a odredišni je server, konekcija je pred zatvaranjem, čeka se potvrda zatvaranja od druge strane (stanje konekcije TIME_WAIT);
  - host sa IP adresom 128.107.229.50, HTTP saobraćaj (port 80), gdje je lokalni računar klijent, a odredišni je server, konekcija je uspostavljena i moguća je razmjena podataka;