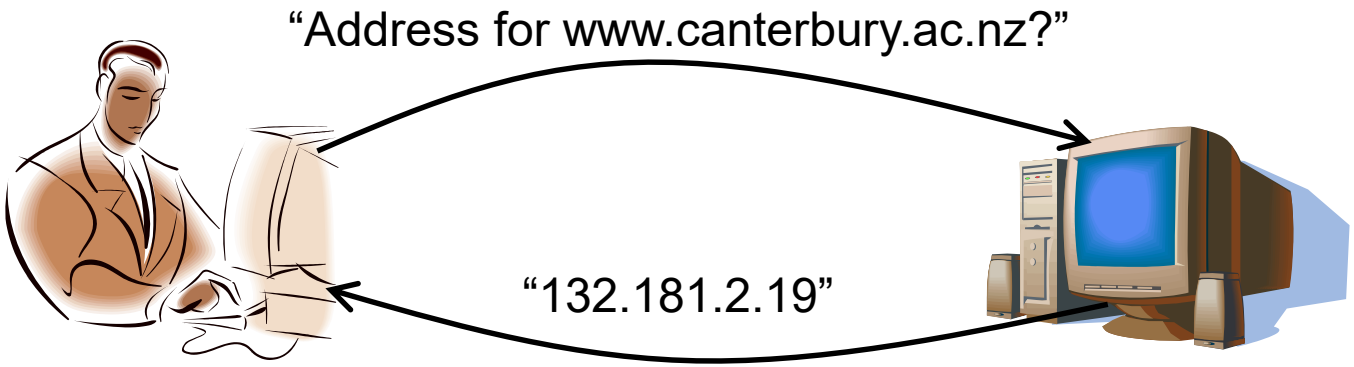
UDP/TCP dump analysis

Popular Applications That Use UDP

- Multimedia streaming
  - Retransmitting lost/corrupted packets is not worthwhile
  - By the time the packet is retransmitted, it's too late
  - e.g., telephone calls, video conferencing, gaming
  - ***Modern streaming protocols using TCP (and HTTP)***
- Simple query protocols like Domain Name System (DNS)
  - Overhead of connection establishment is overkill
  - Easier to have application retransmit if needed



Question

- The following is a dump (contents) of a UDP header in hexadecimal format.

e587003500305b6d

a. What is the source port number?
b. What is the destination port number?
c. What is the total length of the user datagram?
d. What is the length of the data?
e. Is this packet directed from a client to a server or vice versa?
f. What is the application-layer protocol?
g. Has the sender calculated a checksum for this packet?

Question - Answer

- The following is a dump (contents) of a UDP header in hexadecimal format.

e587 0035 0030 5b6d

a. What is the source port number? $(e587)_{16}$ = 58759
b. What is the destination port number? $(0035)_{16}$ = 53
c. What is the total length of the user datagram? $(0030)_{16}$ = 48 bytes
d. What is the length of the data? 48 – 8 = 40 bytes
e. Is this packet directed from a client to a server or vice versa? A client to a server
f. What is the application-layer protocol? DNS
g. Has the sender calculated a checksum for this packet? Yes, the checksum is 5b6d

DNS UDP packet example

- An Example DNS Packet

Link level (layer 2): Ethernet II
Network level (layer 3): IP
Transplort level (layer 4): UDP
Application Level: DNS

```
0000  00 18 8b 75 1d e0 00 1f f3 d8 47 ab 08 00 45 00   ...u......G...E.
0010  00 44 ad 0b 00 00 40 11 72 72 ac 14 02 fd ac 14   .D....@.rr......
0020  00 06 e5 87 00 35 00 30 5b 6d ab c9 01 00 00 01   .....5.0[m......
0030  00 00 00 00 00 00 09 6d 63 63 6c 65 6c 6c 61 6e   .......mcclellan
0040  02 63 73 05 6d 69 61 6d 69 03 65 64 75 00 00 01   .cs.miami.edu...
0050  00 01                                             ..
```

http://www.cs.miami.edu/home/burt/learning/Csc524.092/notes/ip_example.html

Segment – A Packet in TCP

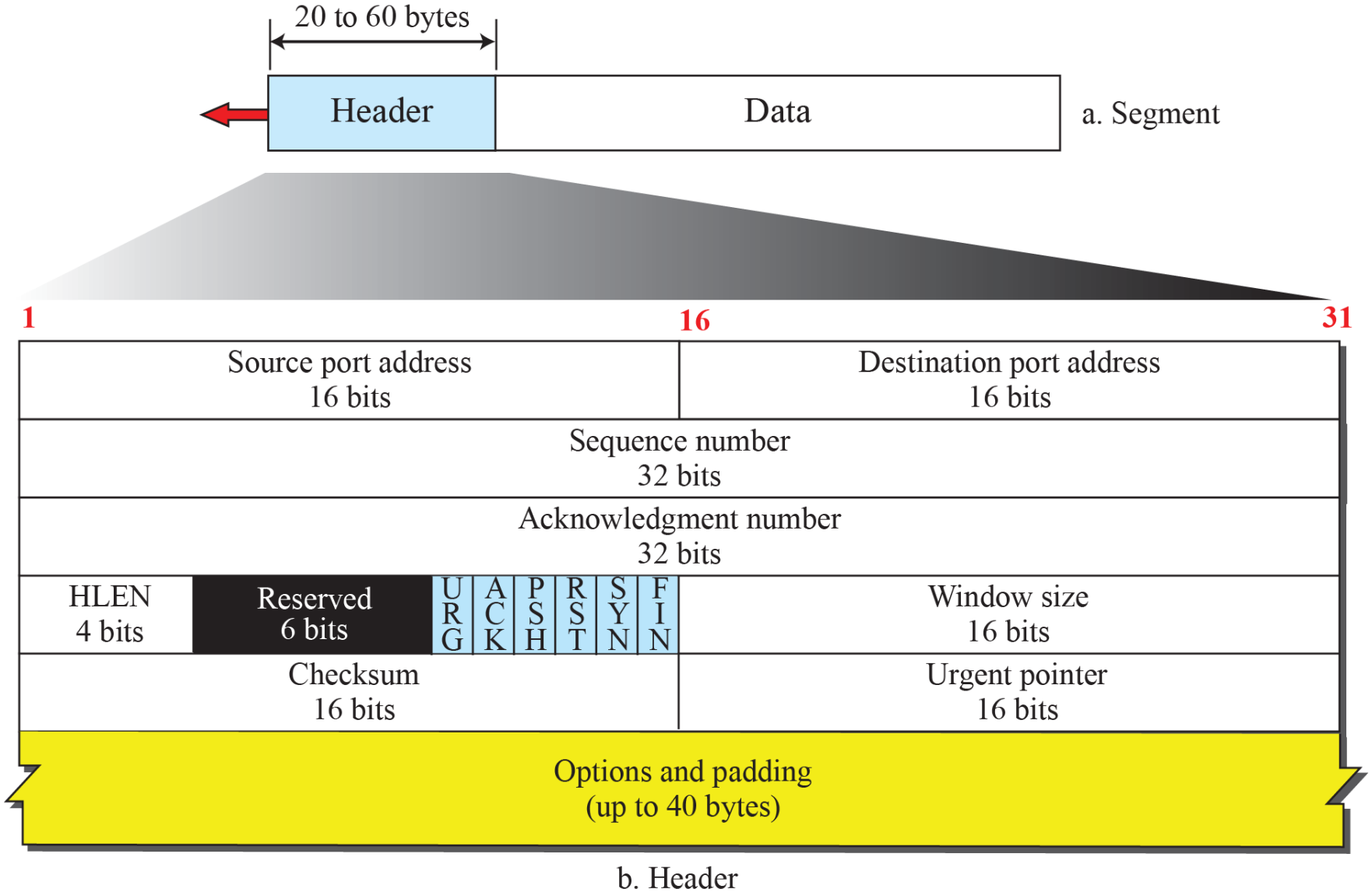


*Figure 24.7: **TCP segment format***

Question – TCP header

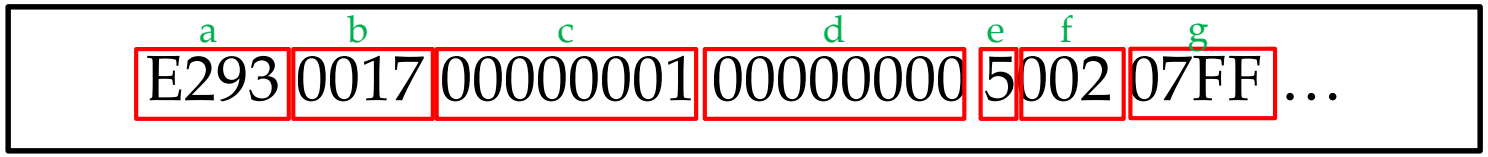
- The following is a dump (contents) of a TCP header in hexadecimal format.

E293 0017 00000001 00000000 5002 07FF …

a. What is the source port number?
b. What is the destination port number?
c. What is the sequence number?
d. What is the acknowledgment number?
e. What is the length of the header?
f. What is the type of the segment?
g. What is the window size?

Question - Answer

- The following is a dump (contents) of a TCP header in hexadecimal format.



a. What is the source port number? $(E293)_{16}$ = 58,003
b. What is the destination port number? $(0017)_{16}$ = 23
c. What is the sequence number? $(00000001)_{16}$ = 1
d. What is the acknowledgment number? $(00000000)_{16}$ = 0
e. What is the length of the header? The HLEN =5. The header is 5 x 4 = 20 bytes long
f. What is the type of the segment?
   - $(002)_{16}$
   - $(000000000010)_2$, the right most 6 bits are 000010, which means only the SYN bit is set. This is the SYN segment used for connection establishment.
g. What is the window size? $(07FF)_{16}$ or 2047 in decimal. The window size is 2047 bytes.