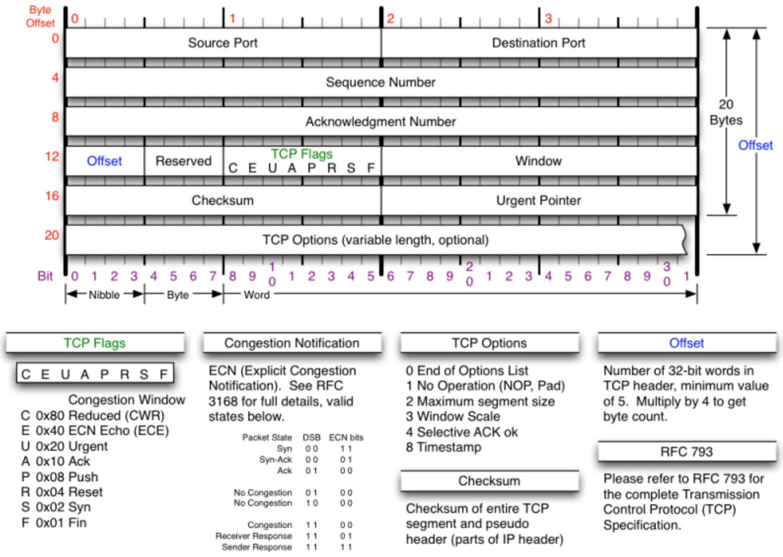
CS241 #37 Protocols

1> Protocol at the TCP level - Handshaking

TCP Packets: What is "SYN. SYN-ACK. ACK" ?

What is the sequence number and what is it used for? What is its initial value & why?

(I see the port number but where is the machine's IP address?)



Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum of entire TCP segment and pseudo header (parts of IP header)

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

2> What is a Denial of service?

Syn flood

DDOS

Internet of Things DOS

3> Which TCP client or server call will result in the first "SYN" packet?

4> TCP Handshaking and the speed of light

The moon is 1.3 light seconds distant. The TCP client is on the Earth and a lunar console runs a TCP server. Assume a new TCP connection is required each time.

3.1 Save the astronaut. How many seconds elapse between wanting to send a CLOSEAIRLOCK message and the server receiving the data?

```
fd=socket(...)
connect(fd,...,...)
write(fd,"CLOSEAIRLOCK!",13);
```

3.2 How many seconds elapse between requesting data from the server and receiving the result?

```
fd=socket(...)
connect(fd,...,...)
write(fd,"READTEMP!",9);
bytes=read(fd,buffer,256);
```

5> TCP and web performance

HTTP/1.0
If the client-server round trip time is 10 ms. What is the minimum time required to display a page with an image? Assume HTTP/1.0 (and that the image requires a separate request).

6> Better... Faster...

Performance improvements in HTTP/1.1

Improvements in HTTP/2.0

Why did Google create QUIC ?

7> Remote Procedure Calls

```
void updateScoreBoard(char*name, int score) {
  char mesg[256];
  sprintf(mesg, "newscore,%100s,%d",name,score);

  write( fd, mesg, strlen(mesg+1));
  // Why did I also send the null byte?
}
// You could also send the message size
// My protocol! So I'll choose bigendian binary format
uint16_t mesglen = htons( strlen(mesg) );
write( fd, & mesglen, sizeof(mesglen) );
write( fd, mesg , strlen(mesg) );
```

8> Subverting protocols

Case study: Heartbleed April 2014

```
  /* simplified */
 sock_fd = accept(server_fd);
 while(1) {
   secureread(sock_fd, &request, &reqsize);

   switch(request->request_type) {
     case HEARTBEAT:
         // echo the client message back
         securewrite(sock_fd,
                     request->content,
                     request->content_length
         );
         break;
     case (...):
         ...
     break;
   }
   free(mesg);
}
```

Change ONE character to fix this program to print
20 dashes.

```
#include <stdio.h>
int main()
{
  int a;
  int b = 20;
  for( a = 0; a < b; a-- )
    putchar('-');
  return 0;
}
```

Actually there are THREE solutions (again,
changing only ONE character). Find all three.

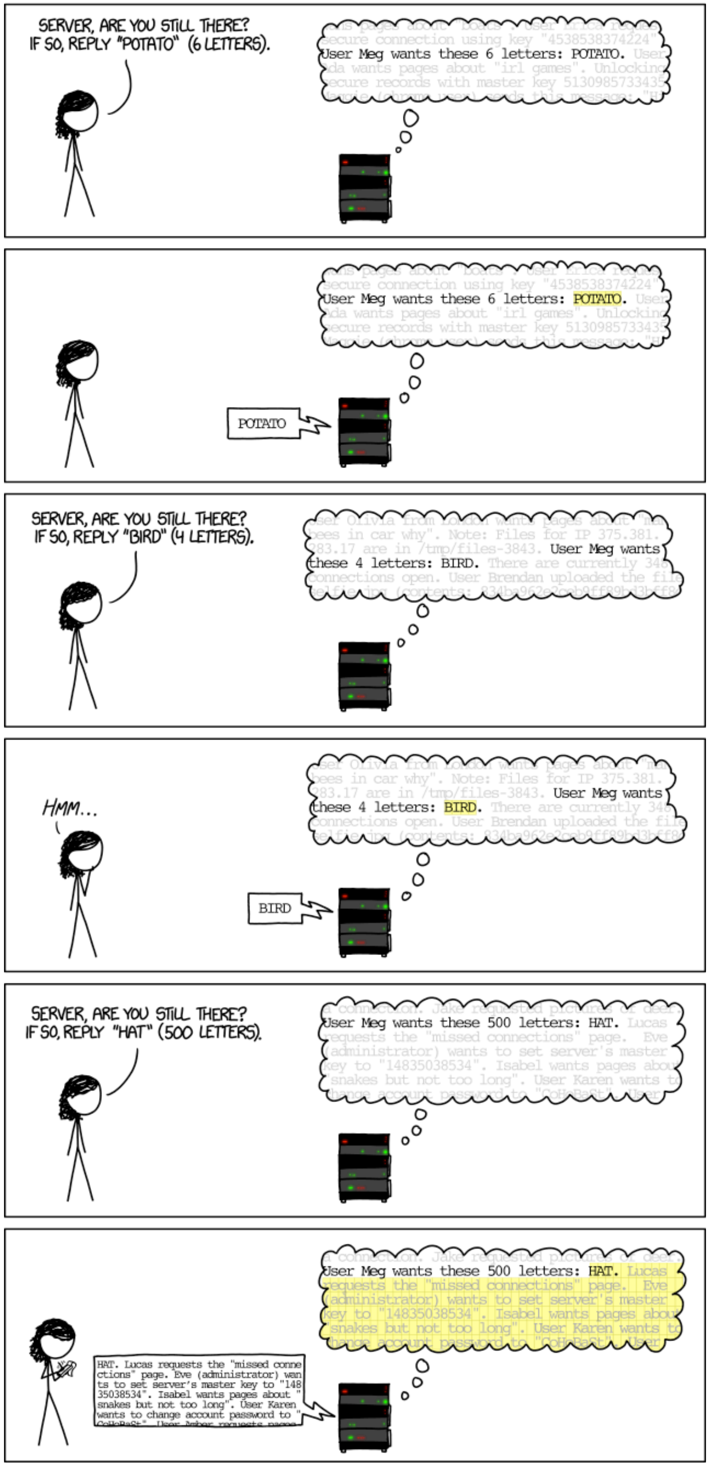
Bonus: Change one character to print 21 dashes.

Heartbleed

Heartbleed is a security bug disclosed in April 2014 in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. Heartbleed may be exploited regardless of whether the party using a vulnerable OpenSSL instance for TLS is a server or a client. It results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension, thus the bug's name derives from "heartbeat". The vulnerability is classified as a buffer over-read.

17% of all web servers were vulnerable
In June 2014, 300,000 systems still vulnerable.

HOW THE HEARTBLEED BUG WORKS:


SERVER, ARE YOU STILL THERE? IF SO, REPLY "POTATO" (6 LETTERS).
ants pages about "boats". User Erica reques secure connection using key "4538538374224" User Meg wants these 6 letters: POTATO. User Ada wants pages about "irl games". Unlocking secure records with master key 5130985733435 Maggie (chrome user) sends this message: "H
ants pages about "boats". User Erica reques secure connection using key "4538538374224" User Meg wants these 6 letters: POTATO. User Ada wants pages about "irl games". Unlocking secure records with master key 5130985733435 Maggie (chrome user) sends this message: "H
POTATO
SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).
User Olivia from London wants pages about "ma bees in car why". Note: Files for IP 375.381. 283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ceb9ff89bd3bff8
HMM...
User Olivia from London wants pages about "ma bees in car why". Note: Files for IP 375.381. 283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ceb9ff89bd3bff8
BIRD
SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User Amber requests pages