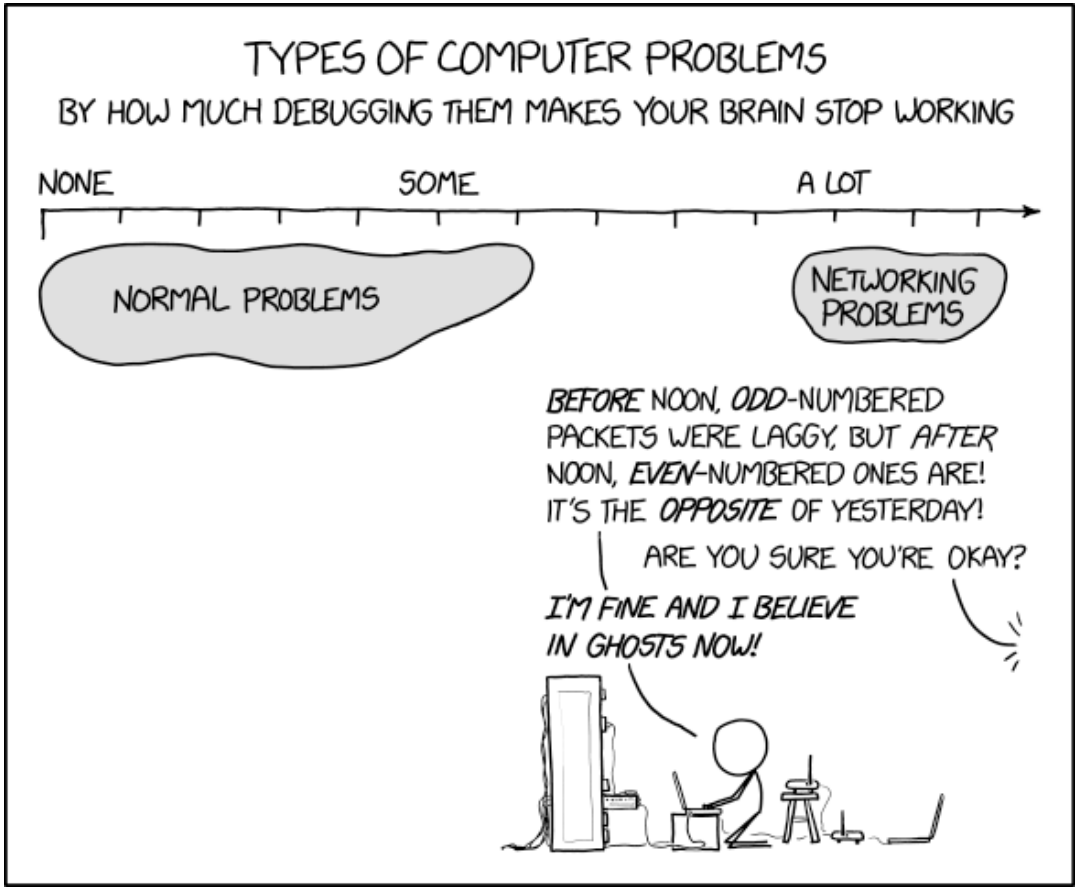
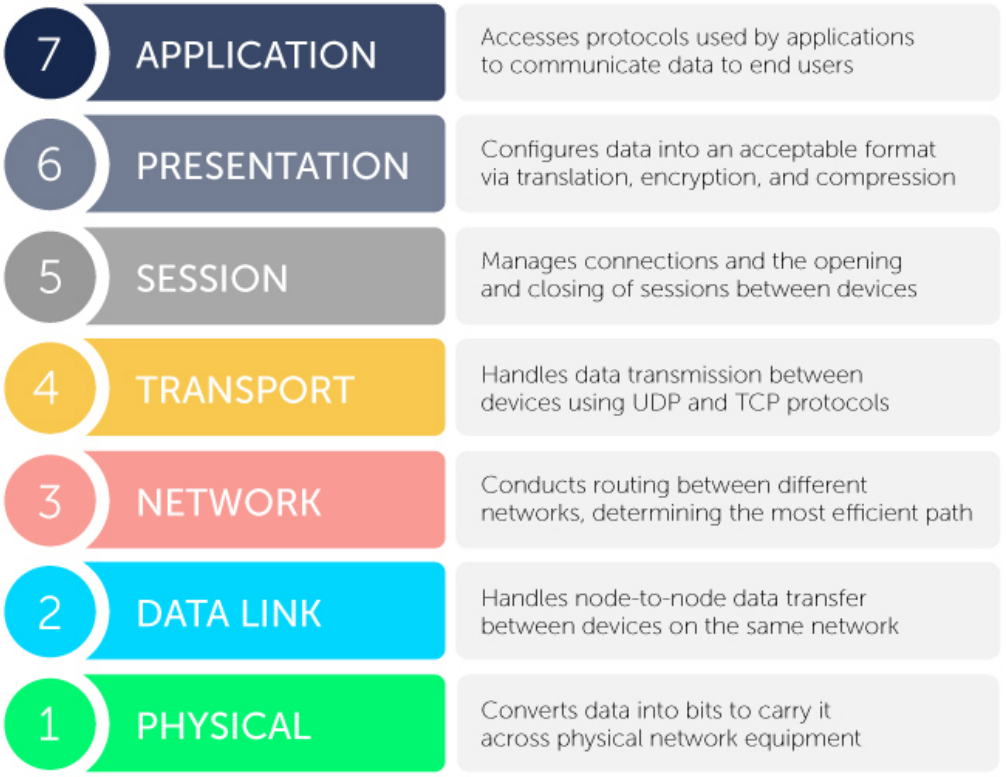
CSCI 3330 Cybersecurity



Word of the day

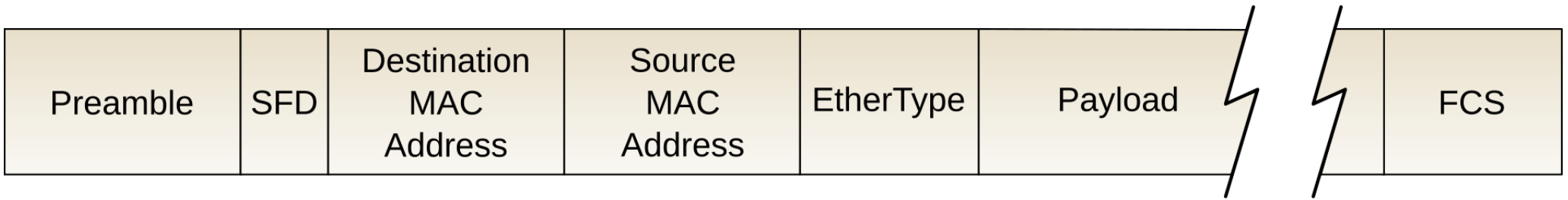
WART n. A small, crocky feature that sticks out of an otherwise clean design. Something conspicuous for localized ugliness, especially a special-case exception to a general rule. For example, in some versions of csh(1), single quotes literalize every character inside them except !. In ANSI C, the ?? syntax used for obtaining ASCII characters in a foreign environment is a wart.

Network layers (OSI model)

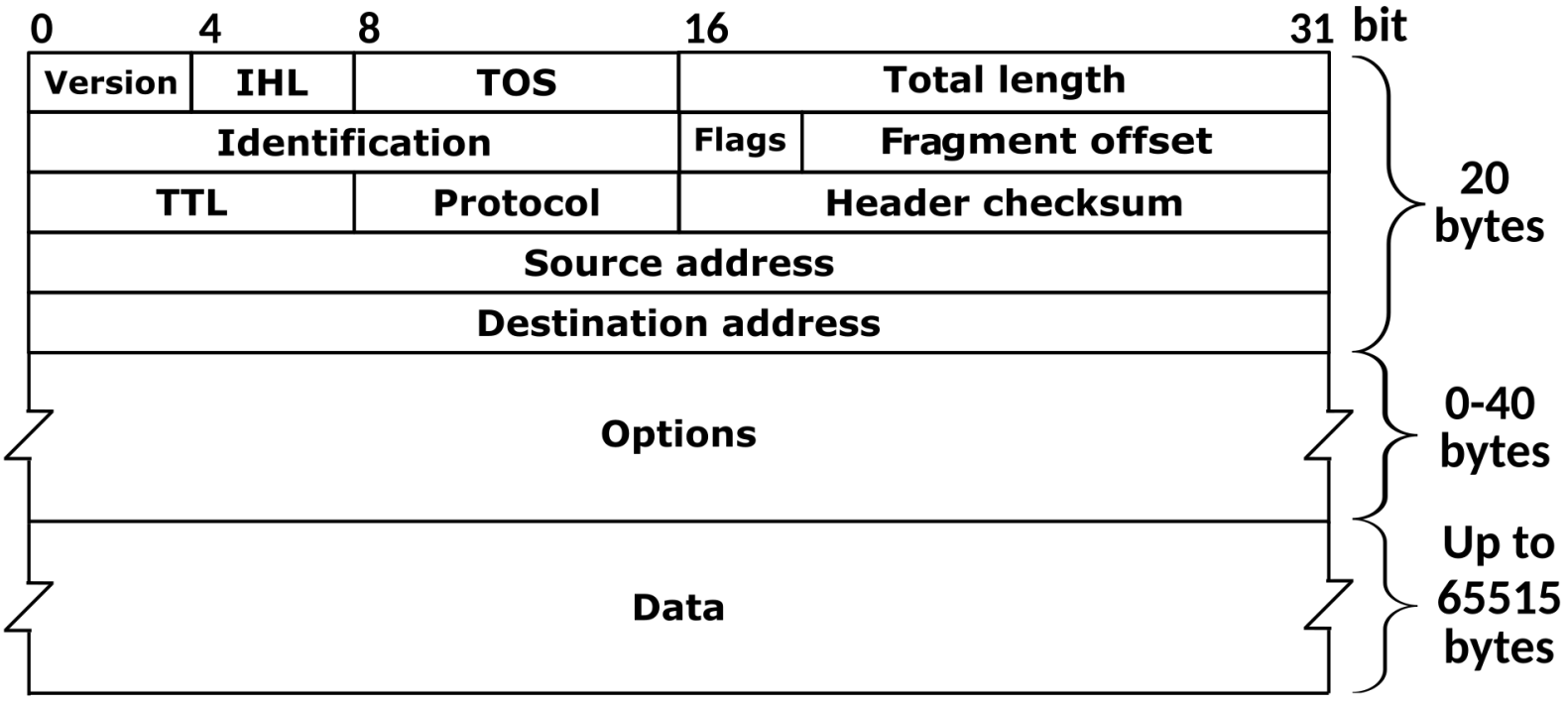


- Layer 8: user layer / political layer / etc.
- Often the most problematic layer…

Ethernet: Layer 2



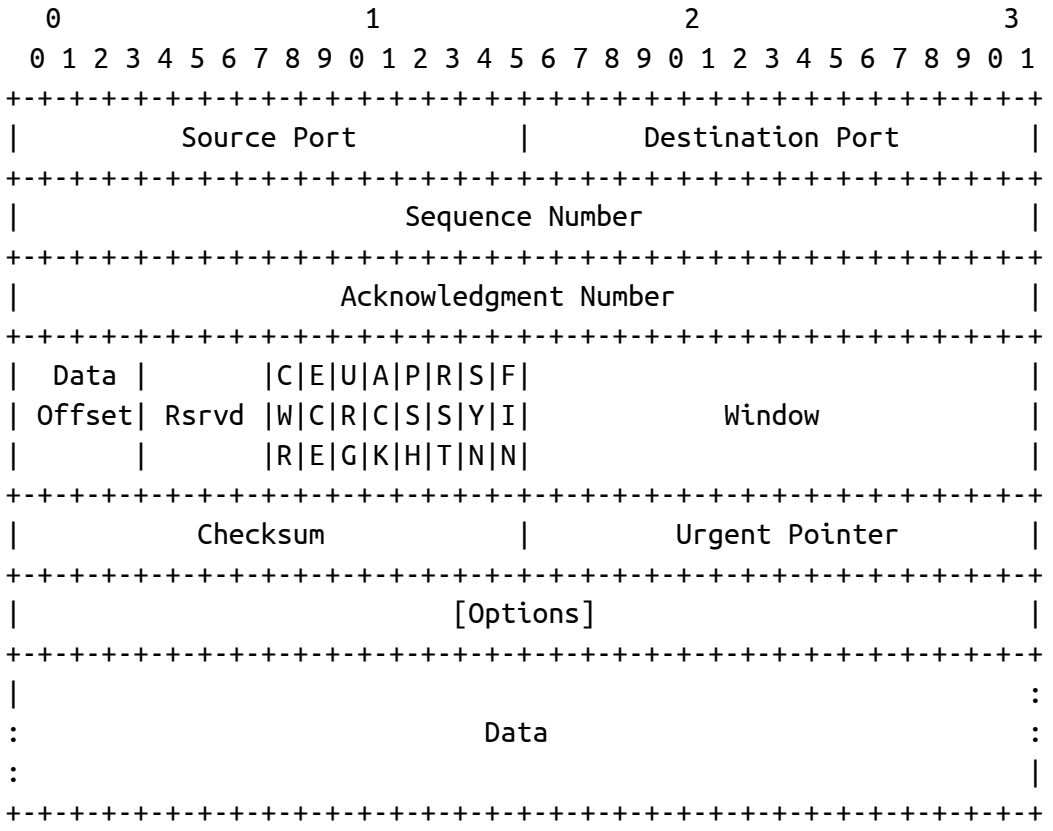
Internet protocol (IP): Layer 3



Notable fields

- Total length (max 65515)
- TTL (time to live)
- Identification / fragment offset
  - Fragments are keyed by (src addr, dst addr, protocol #, and IP id)

Transmission Control Protocol (TCP): Layer 4



Notable fields

- Sequence / acknowledgment #s
- Flags
  - SYN / ACK / FIN / RST
- Source/destination ports
  - Open ports / closed ports / filtered

Three-way handshake

- SYN: Send ISN to server
- SYNACK: ACK client’s ISN, send ISN to client
- ACK: Ack server’s ISN

Layer 7: application layer

- HTTP
- FTP
- ssh
- DNS

In between the layers

- ARP (layer 2, glues together layers 2 and 3)
- ICMP (layer 3, provides errors, etc.)

Layer 2: switch vs. hub

- Hub transmits all traffic on all ports
- Switch transmits only on needed port

Address Resolution Protocol (ARP)

- Used for addresses on your subnet
- IP to MAC address translation

ARP request

- Which MAC address has IP address 1.2.3.4?
- ARP response:
  - I do at MAC address XXX!

Internet Control Message Protocol (ICMP)

- ping (ICMP echo request/reply)
- traceroute (ICMP TTL exceeded)
- ICMP reassembly time exceeded: not all fragments found

Holistic view

- Putting it all together…

Wireshark

- Packet sniffer
- Free, open source

Three pillars of Information Security

- AKA CIA triad

Assignment 4

- Deadline: October 13, 2025, 10:00pm
- Advanced SQL information inference https://tildesites.bowdoin.edu/~j.knockel/csci3330f25/assignment4.pdf