ROSE-HULMAN
INSTITUTE OF TECHNOLOGY

CSSE 490
Network Security

Day 14: ICMP Wrap Up

Outline

- ❑ Port Numbers
- ❑ TCP v UDP
- ❑ User Datagram Protocol
- ❑ UDP Header
- ❑ Activity

Port Numbers

- 16 bits value
- 0 – 1023: Well-known ports
  - Need sudo privileges to bind to these ports, why?
  - Http runs on port 80, https on 443, ssh on 22, etc…
- 1024 – 49151: Lesser well-know ports
  - SQL Server (1433)
- 49152 – 65535: Private ports

Transport Layer Protocols: TCP vs UDP

	TCP	UDP
Connection	Connection based	Connectionless
Packet Boundary	Stream based	Preserving packet boundaries
Reliability	✓	✗
Ordering	✓	✗
Speed	✗	✓
Broadcast	✗	✓

User Datagram Protocol

- ❑ Very simple protocol
- ❑ Only adds two pieces of information on top of L3 protocols Source port / destination port
- ❑ Src/Dst ports, length, checksum, and data

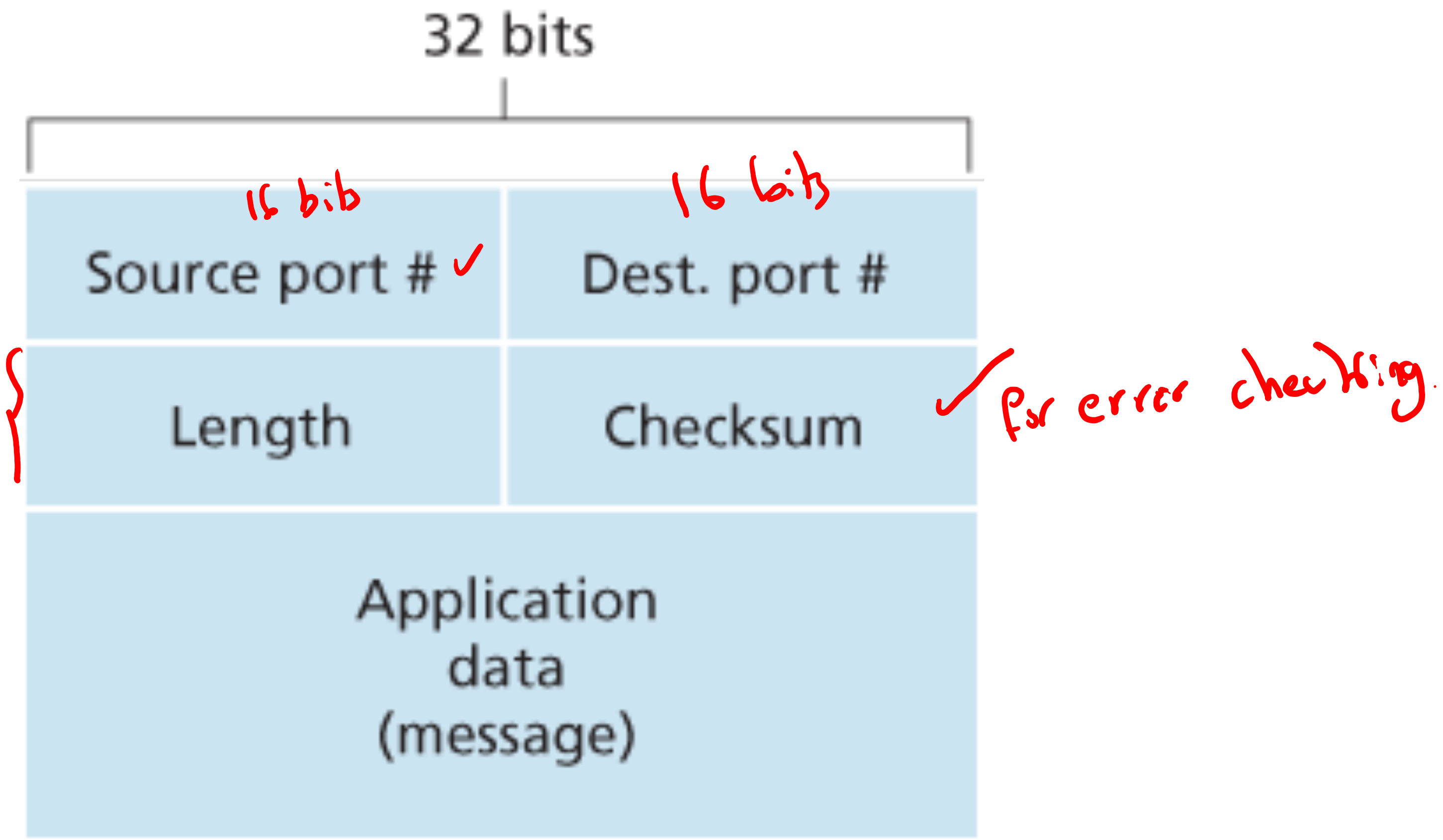
UDP Applications

Speed vs. Reliability
tradeoff.

- Domain Name Service (DNS) ✓
- Video/Audio streaming (e.g., Skype, Zoom) ✓

  except: YouTube, Netflix use TCP
- Real-time applications
- OpenVPN

UDP Header



32 bits

16 bits 16 bits

Source port # ✓	Dest. port #
Length	Checksum
Application data (message)	

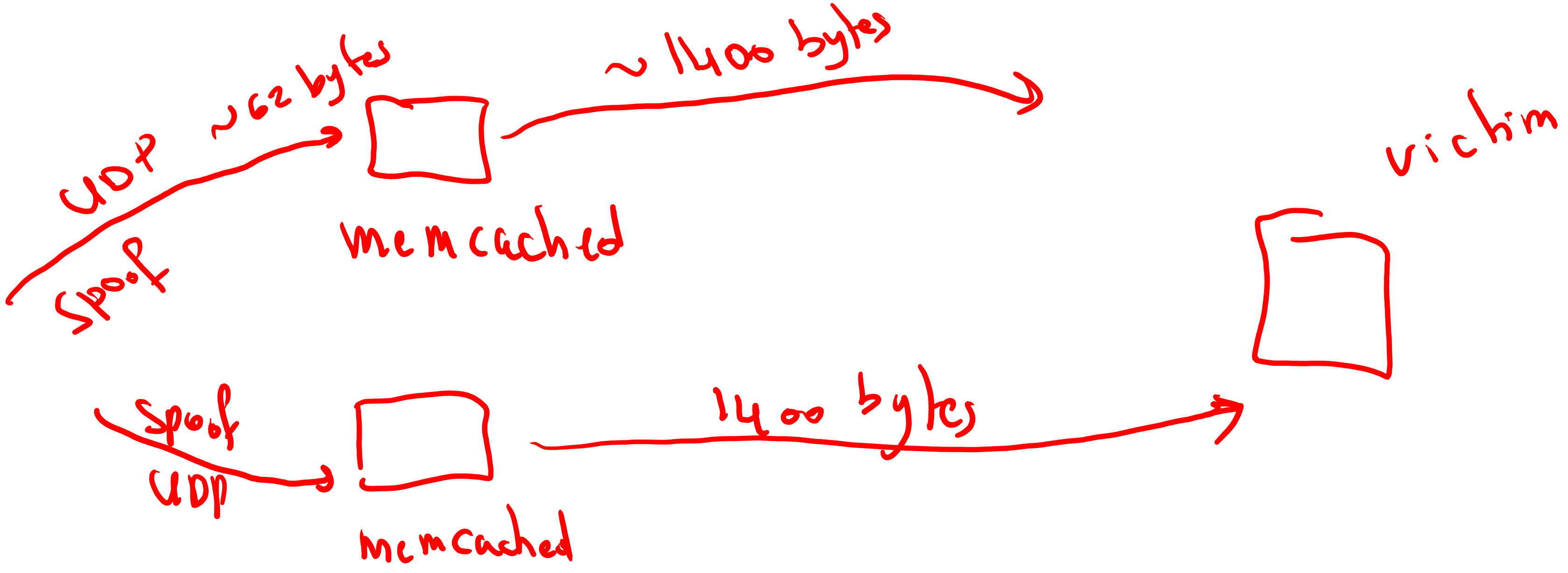
✓ for error checking.

Image from: K&R 2017

Memcrashed

GitHub Survived the Biggest DDoS Attack Ever Recorded

On Wednesday, a 1.3Tbps DDoS attack pummeled GitHub for 15-20 minutes. Here's how it stayed online.



Activity: UDP Attack

Step 1: ~~Write code to discover which UDP ports are enabled~~ gogo

Step 2: Discover the service running on the target port

Step 3: Take down the service (launch a DoS attack) by sending no more than 100 pps

Runs on victim & client

```
bash /proj/csse490/labs/run_server.sh
```