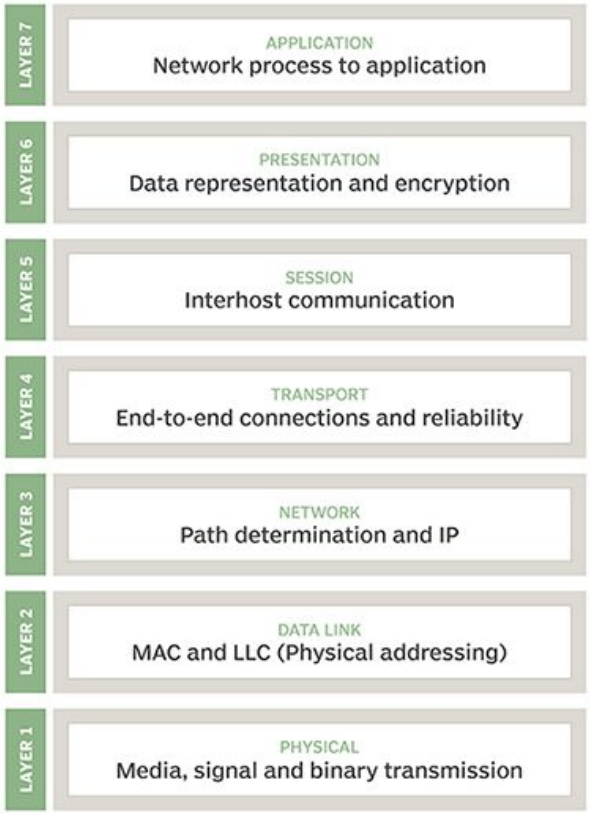
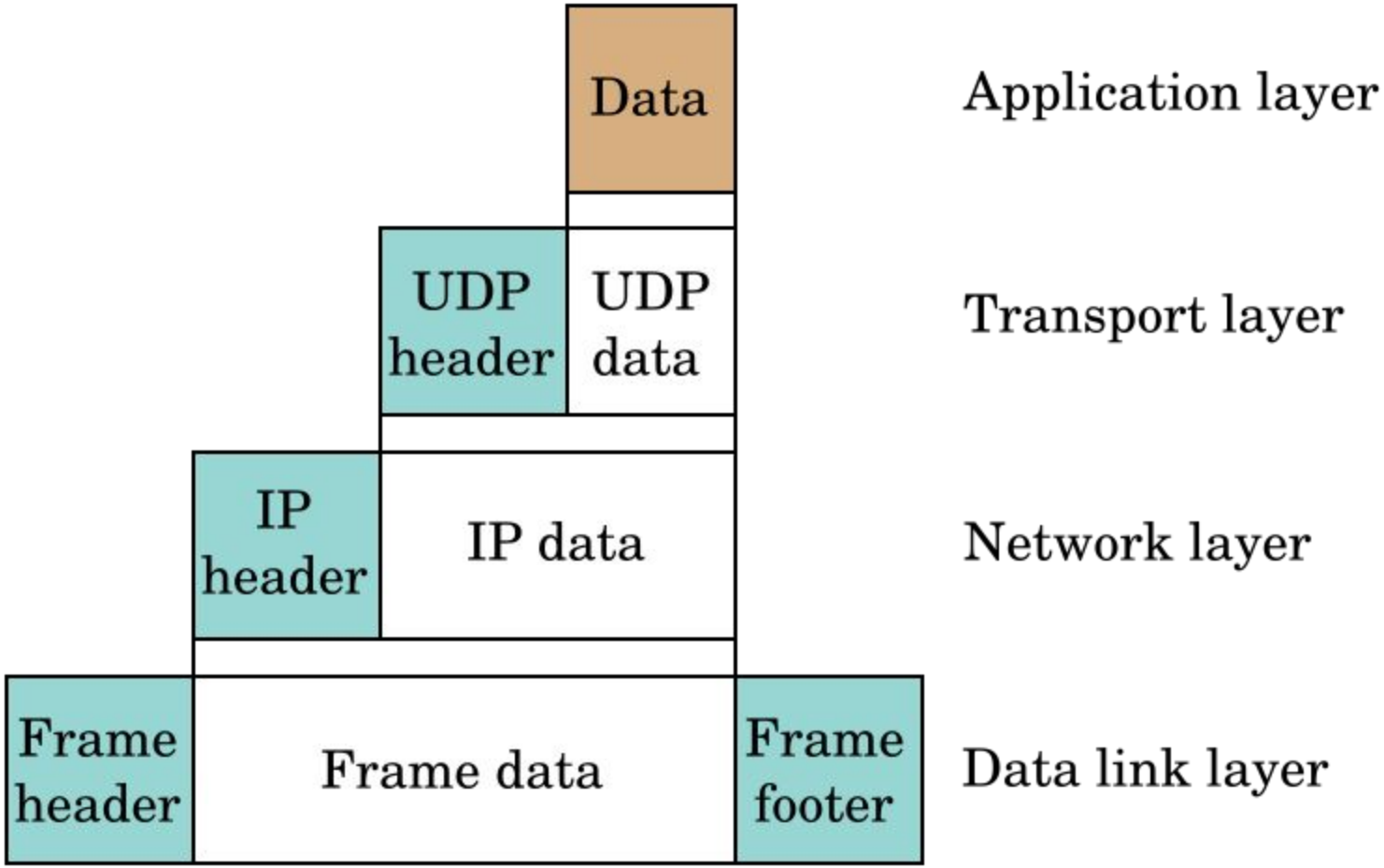
UNLV CYBER SECURITY CLUB

Network Traffic Analysis



- Layer 7: **DATA**
  - HTTP(S), DHCP, DNS, TSL/SSL, FTP, TELNET
- Layer 4: **SEGMENTS**
  - TCP, UDP, port numbers
- Layer 3: **PACKETS**
  - IP(v4/v6), ICMP
- Layer 2: **FRAMES**
  - MAC, ARP, Ethernet
- Layer 1: **BITS**
  - Copper cables, fiber optics, hubs


Data
Application layer
UDP header
UDP data
Transport layer
IP header
IP data
Network layer
Frame header
Frame data
Frame footer
Data link layer

Addressing Schemes

Transport Layer: PORTS

Network Layer: IP ADDRESSES

Data Link Layer: MAC ADDRESSES

Quick Explanation of Other Protocols

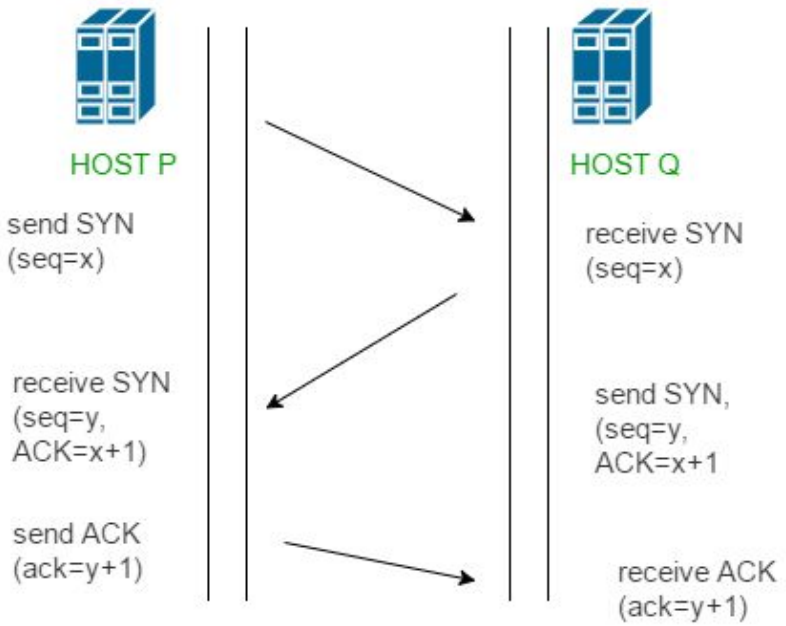
File Transfer Protocol (FTP)

Telnet

- uses TCP port 23
- bidirectional interactive communication (CLI)

Internet Control Message Protocol (ICMP)

- layer 3, no port number
- includes ping, traceroute
- used for diagnostic / error control purposes



TCP 3-WAY HANDSHAKE

- establishes synchronized connections between a client & server

Address Resolution Protocol (ARP)

- computers can communicate via IP addresses
  - but in order for them to communicate at Layer3, they need to be able to communicate at both Layer2 and Layer1
- layer 2 communication ➔ MAC addresses

- question: if I know the IP address of a server that I want to talk to, but I **don't** know the MAC address, how can I **find the MAC address of the server**?
- answer: ARP

Types of HTTP Authentication

- Basic Auth
- Cookies
  - helps prevent XSRF (Cross-Site Request Forgery)
- Tokens
  - JSON Web Tokens
  - helps prevent XSS (Cross-Site Scripting)
- Signatures
- One-Time Passwords
  - Time-based
  - HMAC-based

HTTP Basic Authentication

- Basic Auth
  - username and password
  - doesn’t require cookies, etc.
  - client sends an Authorization HTTP header
  - structure
    - username:password
    - base64 encoded

```
curl --header “Authorization: Basic user:pass” https://website.com
```

Internet Control Message Protocol (ICMP)

- Layer3 protocol
- DOES NOT exist on a TCP/UDP port
- commonly used ICMP is ping
  - echo request / echo reply
  - just sends empty bytes
  - Time to Live (TTL): how long the packet is going to attempt to find the other computer before it’s dropped

FTP Methods

- Like with what we've seen for HTTP, FTP has its own methods that define behavior/action

https://en.wikipedia.org/wiki/List_of_FTP_commands