Networks

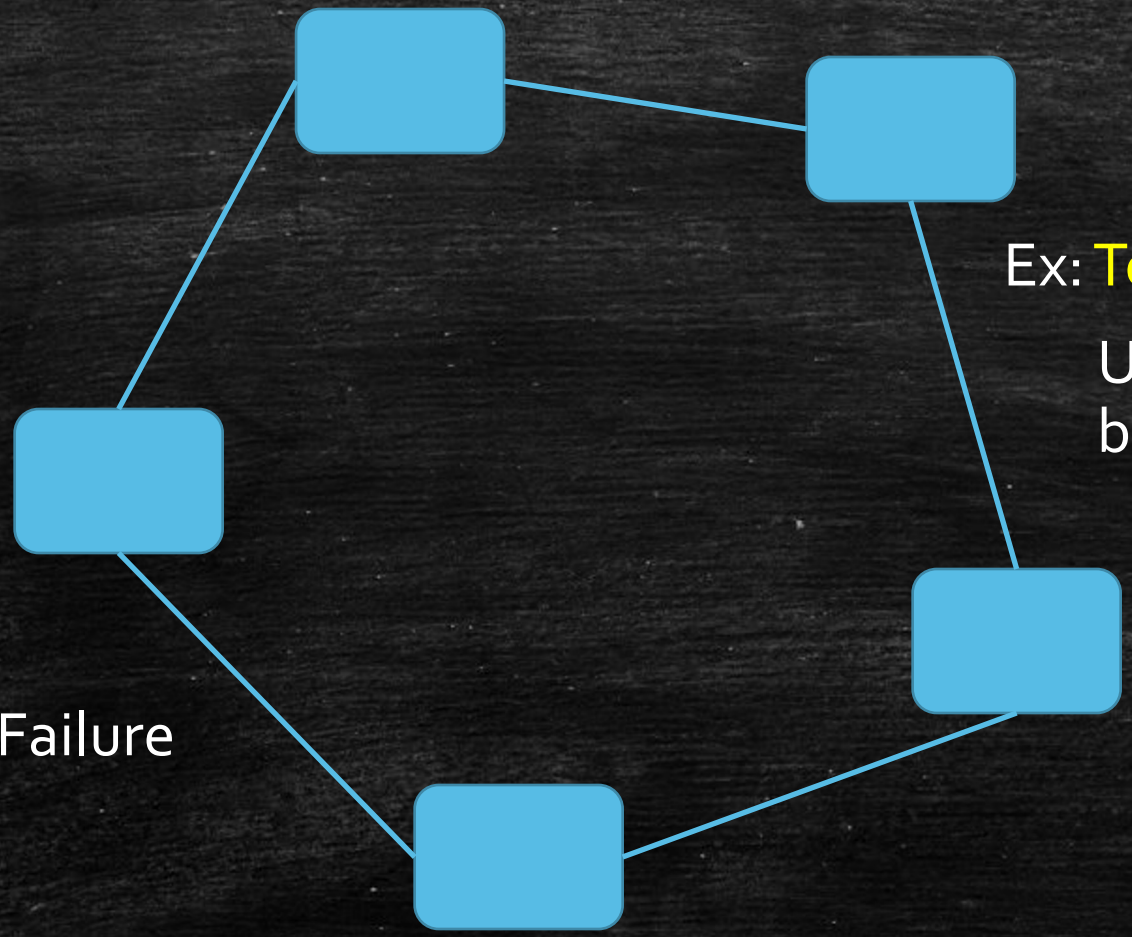
Connecting in a Digital World

Network Topology

- An important distinction first:
  - Physical Network (Physical layout/connection of hardware)
  - Logical Network (how does data flow)

  - 4 Types of Network Topologies
    - Bus (1 cable – everyone hears everything)
    - Ring (More common in fiber) (Each neighbor connected to two neighbors)
      - Anywhere a break, all communications die (Single point of failure)
    - Star (Also a SPF issue)
    - Full Mesh – Everyone is connected to everyone
      - (N(N-1))/2 = number of connections required

Ring Networks

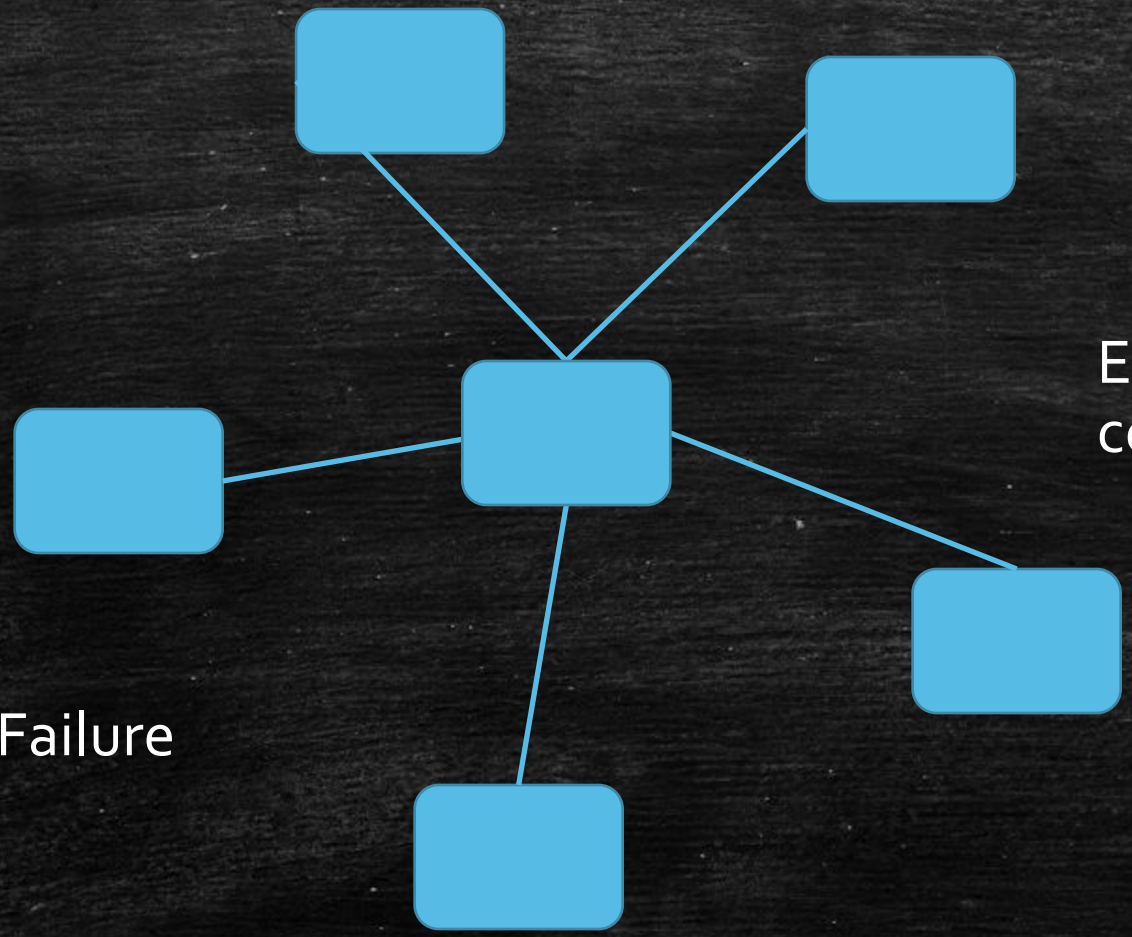


Ex: Token Ring (uses 3-Byte "Token")

Used originally by businesses, but eclipsed by Ethernet

Single Point of Failure

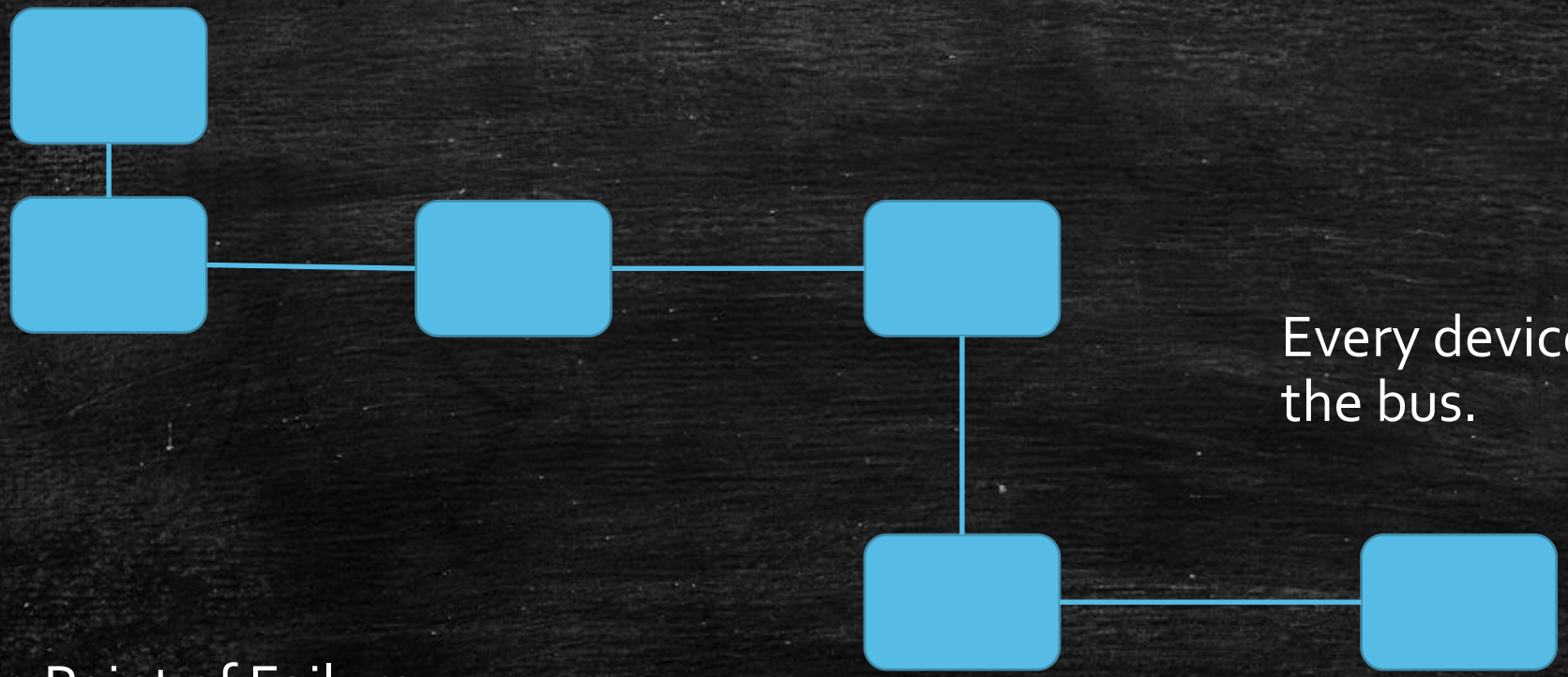
Star Networks



Every device is connected to a central hub of some kind.

Single Point of Failure

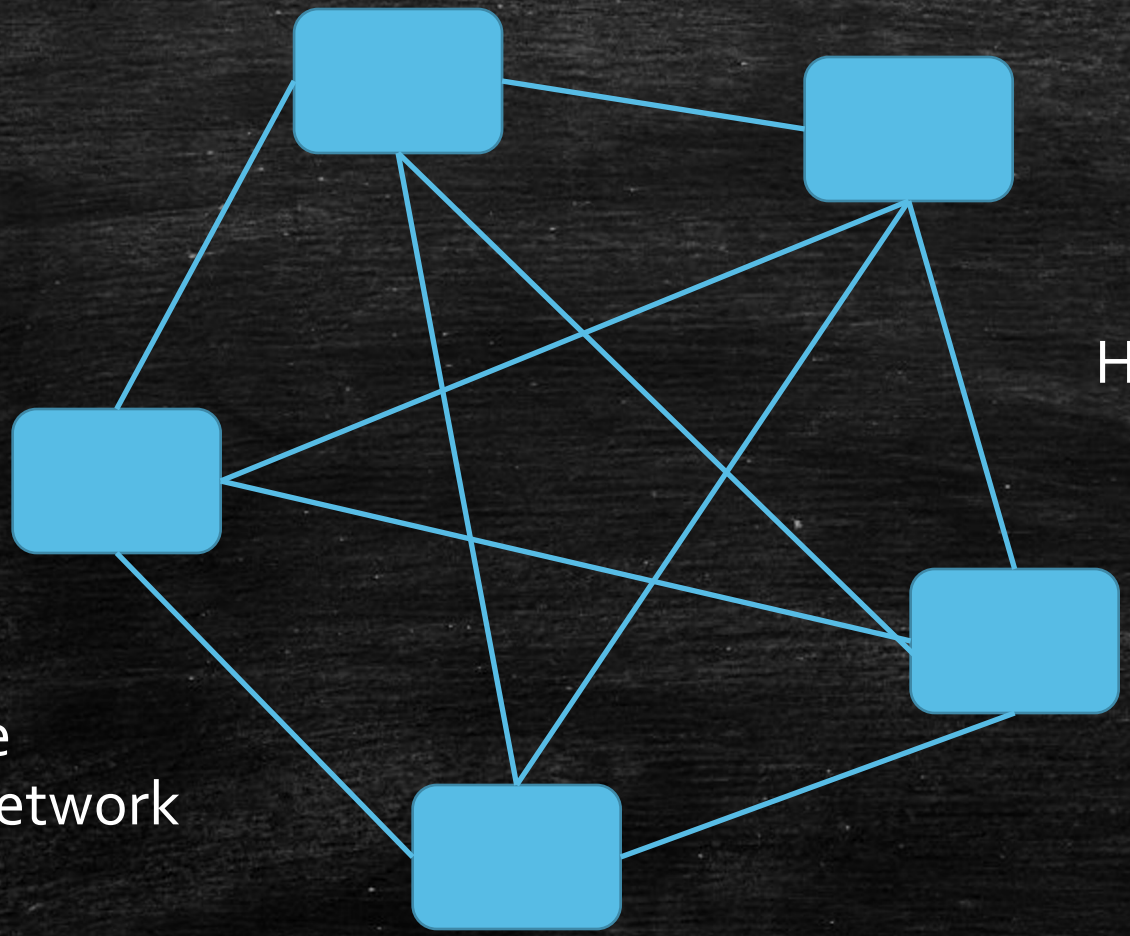
Bus Networks



Every device “hears” what is on the bus.

Single Point of Failure

Mesh Networks



How Many Connections?

$$\frac{n(n-1)}{2}$$

Example: (5*4)/2 = 10

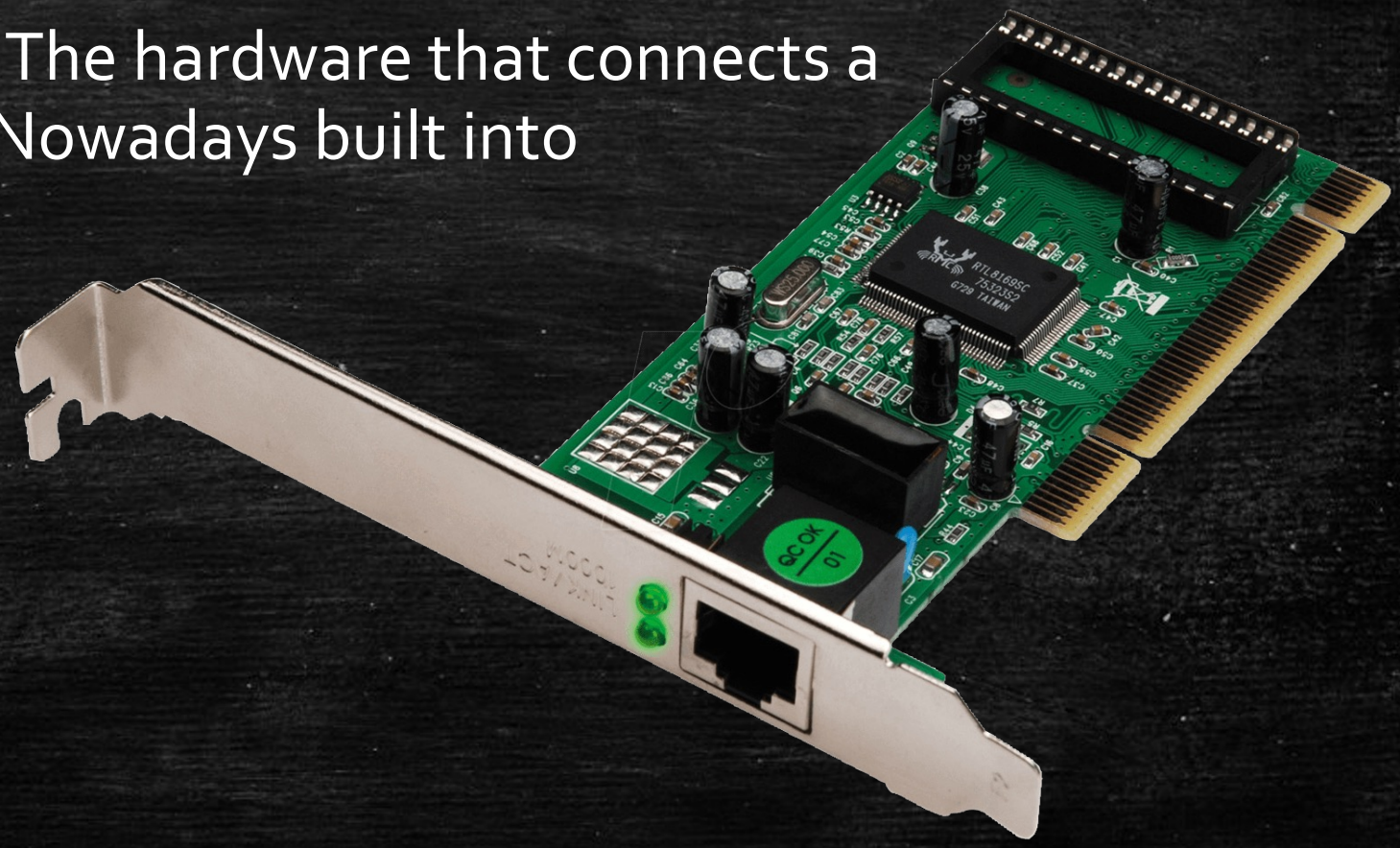
Most Expensive
But Fail-Safe Network

Network Topology - Hardware

- Switches
- Hubs
- Bridges
- Routers
- Firewalls

Networking - Hardware

- Network Interface – The software that accesses networking hardware.
- Network Interface Card – The hardware that connects a computer to a network. (Nowadays built into motherboards)



Networking - Switch

"Switches Build Networks"

Layer 2

Networking - Switch

Smart vs. Dumb Switches

Smart Switches have software that provides significant services

AKA
Switching Hub
Bridging Hub
MAC Bridge

A switch is more intelligent than an Ethernet hub, which simply retransmits packets out of every port of the hub except the port on which the packet was received, unable to distinguish different recipients, and achieving an overall lower network efficiency.

Networking - Routers

"Routers Connect Networks"

Networking - Routers

"Routers Connect Networks"

Networking - Firewalls

Network Security

Block Unwanted Traffic

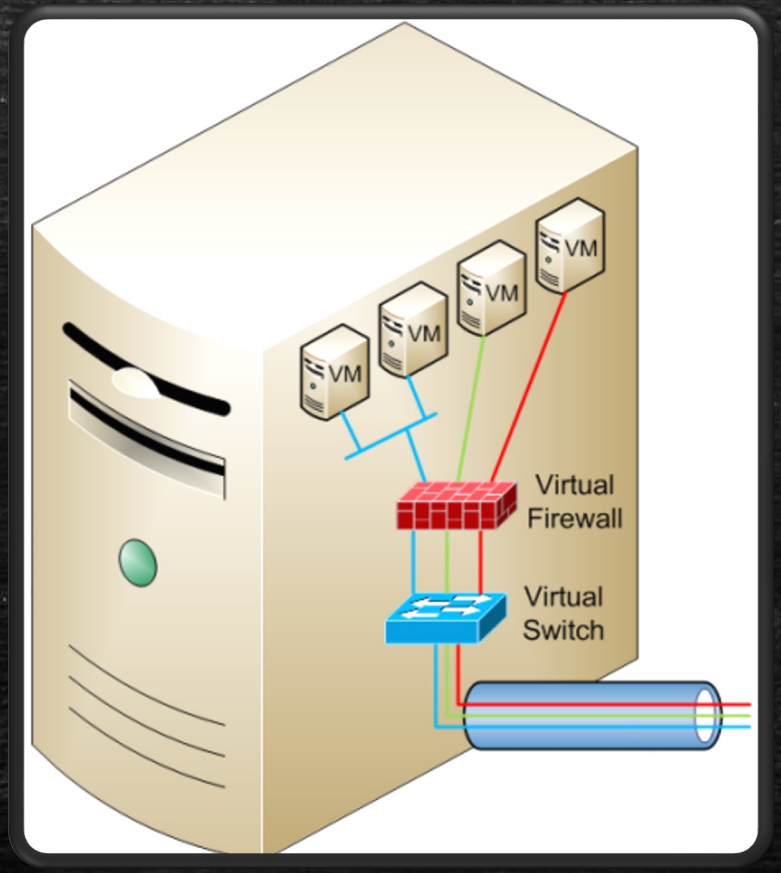
- In or Out
- Whitelist
- Blacklist

Networking - Firewalls

Network Security

Host-Based Firewalls

- In or Out
- Whitelist
- Blacklist



Secures One Host

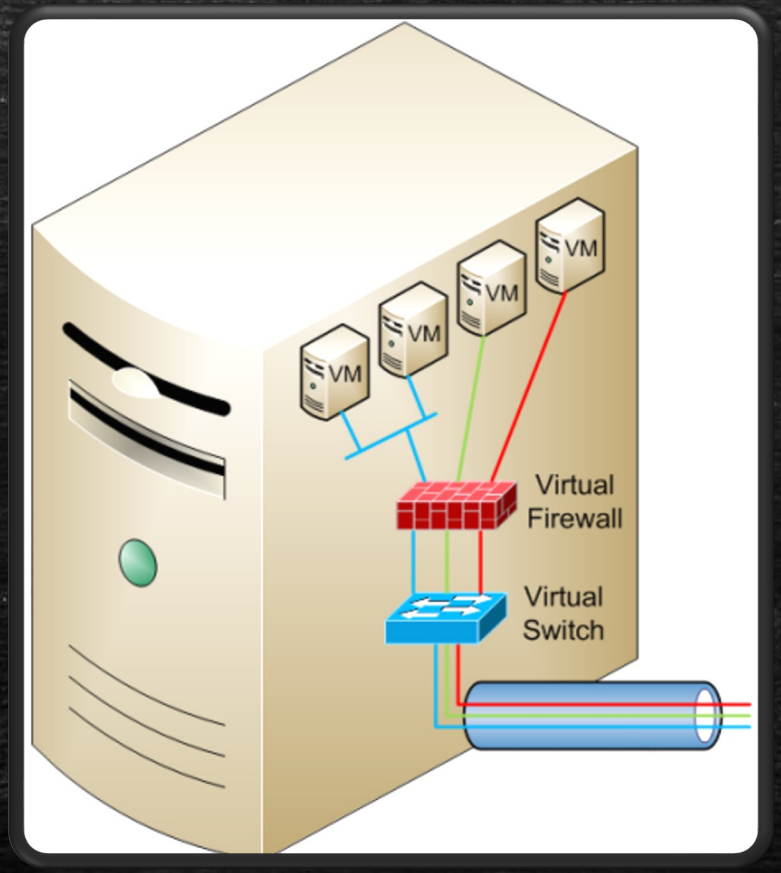
- Often File Servers
- Comes with OS or as an add-on
- Filters/Restricts Packet Flows

Networking - Firewalls

Network Security

Host-Based Firewalls

- In or Out
- Whitelist
- Blacklist



Secures One Host

- Often File Servers
- Comes with OS or as an add-on
- Filters/Restricts Packet Flows

Networking – Open Systems Interconnection Model

Abstract Model: Seven Layers

- Layer 7: Application
- Layer 6: Presentation
- Layer 5: Session
- Layer 4: Transport
- Layer 3: Network
- Layer 2: Data Link
- Layer 1: Physical

Networking – Protocol Data Units

What Data Units PDUs are at each level?

Host Layers

- Layer 7: Data
- Layer 6: Data
- Layer 5: Data
- Layer 4: Segment, Datagram

Media Layers

- Layer 3: Packet
- Layer 2: Frame
- Layer 1: Symbol

Networking – Open Systems Interconnection Model

Abstract Model: Seven Layers

- Layer 7: Application
- Layer 6: Presentation
- Layer 5: Session
- Layer 4: Transport — TCP
- Layer 3: Network — IP
- Layer 2: Data Link
- Layer 1: Physical

} "Language" of the Internet TCI/IP

- Layer 7: User and this level (7) interact with the software application.
- Layer 6: Controls the syntax of data exchange between application-layer entities. Maps between network formats and file formats the application can use.
- Layer 5: Controls the dialogue between two computers: (full-duplex, half-duplex, simplex operations. Gracefully closes sessions managed at Layer 4/TCP.
- Layer 4: Functional/procedural transmission of variable-length data sequences from a source to a destination, maintaining quality of service. TCP or UDP layer.
- Layer 3: Functional transmission of packets between different networks. (Internet Protocol (IP) layer.
- Layer 2: Defines connection between two nodes. Some error detection. Defines flow between them. Medium Access Control (MAC) and Logical Link Control (LLC) sub-layers.
- Layer 1: Transmission/Reception of unstructured raw data between a device and a physical transmission medium. Electrical, Radio, or optical signaling.

Network Terminology

- Packet - A network packet is a formatted unit of data carried by a packet-switched network
- Internet Protocol - (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries.
  Its routing function enables internetworking, and essentially establishes the Internet.
- Transmission Control Protocol - one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network.

Network Terminology

- User Datagram Protocol – Connectionless packet transfer. Checksum only, no handshakes. Fast for large real-time data (i.e. video transmission/broadcast).
- Dynamic Host Configuration Protocol – DHCP Servers assign IP addresses to devices wishing to join or communicate on a UDP/IP network. (Opposite of assigning a manual IP address.)
- Domain Name Service- Translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. DNS Servers look up the IP addresses so we do not have to track them.

Network Terminology

- User Datagram Protocol – Connectionless packet transfer. Checksum only, no handshakes. Fast for large real-time data (i.e. video transmission/broadcast).
- Dynamic Host Configuration Protocol – DHCP Servers assign IP addresses to devices wishing to join or communicate on a UDP/IP network. (Opposite of assigning a manual IP address.)
- Domain Name Service- Translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. DNS Servers look up the IP addresses so we do not have to track them.
- IPv4/IPv6 – fourth/sixth versions of IP. Connectionless protocol for packet switched networks. Best effort. Does not guarantee delivery. (Hence TCP)
  - IPv4 uses 32 bits: 255.255.255.255 (4.3 Billion addresses)
  - IPv6 uses 128 bits: 8 words separated by ':' (3.4×10^{38} addresses)
    - Example:
    - FE80:0000:0000:0000:0202:B3FF:FE1E:8329 FULL ADDRESS
    - FE80::0202:B3FF:FE1E:8329 COLLAPSED ADDRESS (0's omitted)

Network Terminology

- File Server – A computer attached to a network that provides a location for shared disk access.
- Web Server - A computer attached to the World Wide Web that provides content. Web servers respond to web requests over port 80 (unsecure), and port 443 (SSL).

- Secure Socket Layer (SSL) – Predecessor to TLS – Stateful - provides encrypted data transmission from point-to-point. (Symmetric Key encryption using public private key exchange to establish the session) Can be defeated with man-in-the-middle attacks, truncation attacks, and other attacks. OFFICIALLY DEPRECATED by the Internet Engineering Task Force (IETF)

Network Terminology

- Transport Layer Security (TLS) – Replaced SSL. Stateful connection.
  - Provides:
    - Data privacy using symmetric encryption
    - Authentication using public/private keys (PKI)
    - Reliable Data – Message Authentication Codes (MAC ID) to detect unauthorized loss or *alteration* of the data.