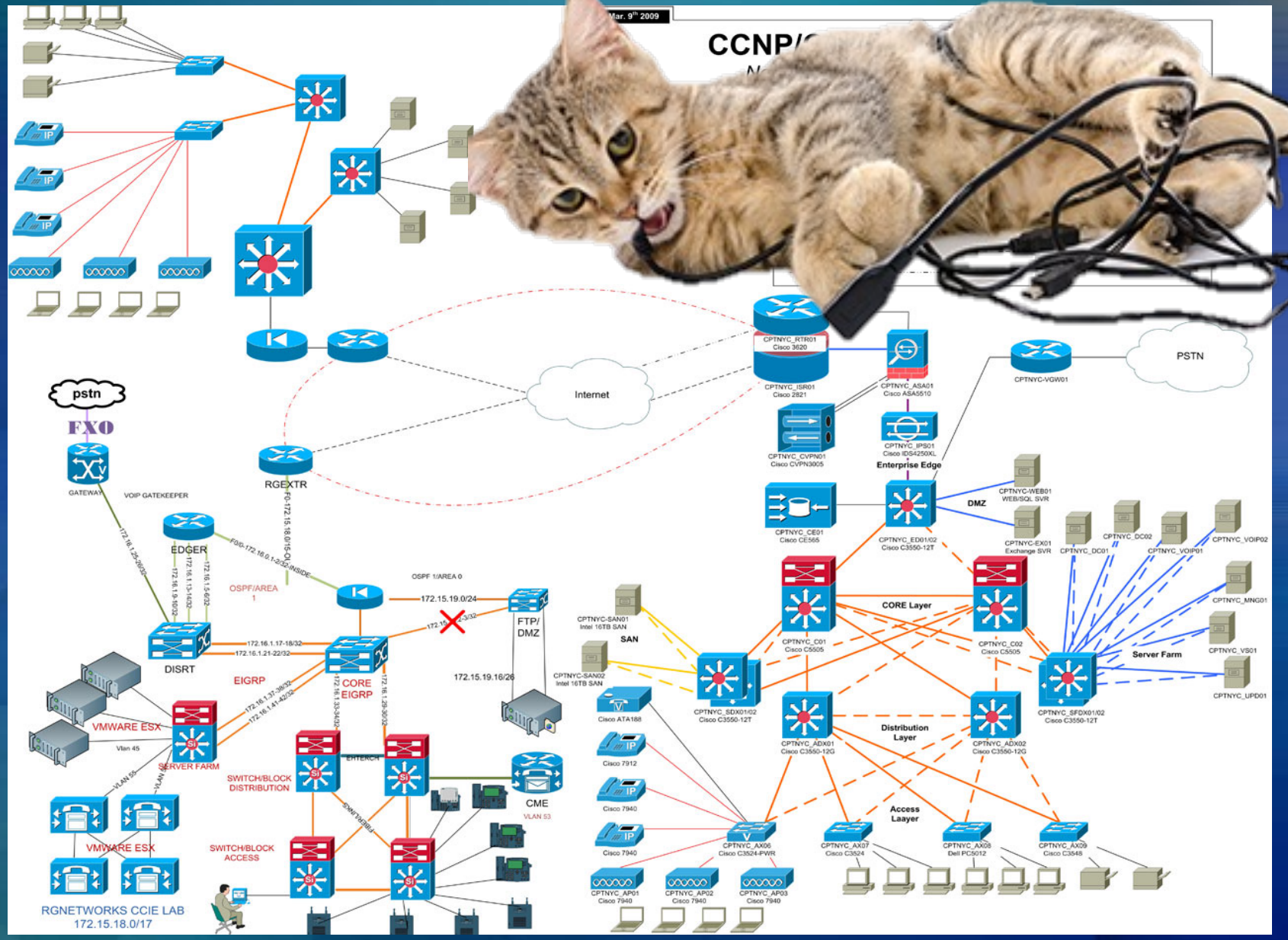
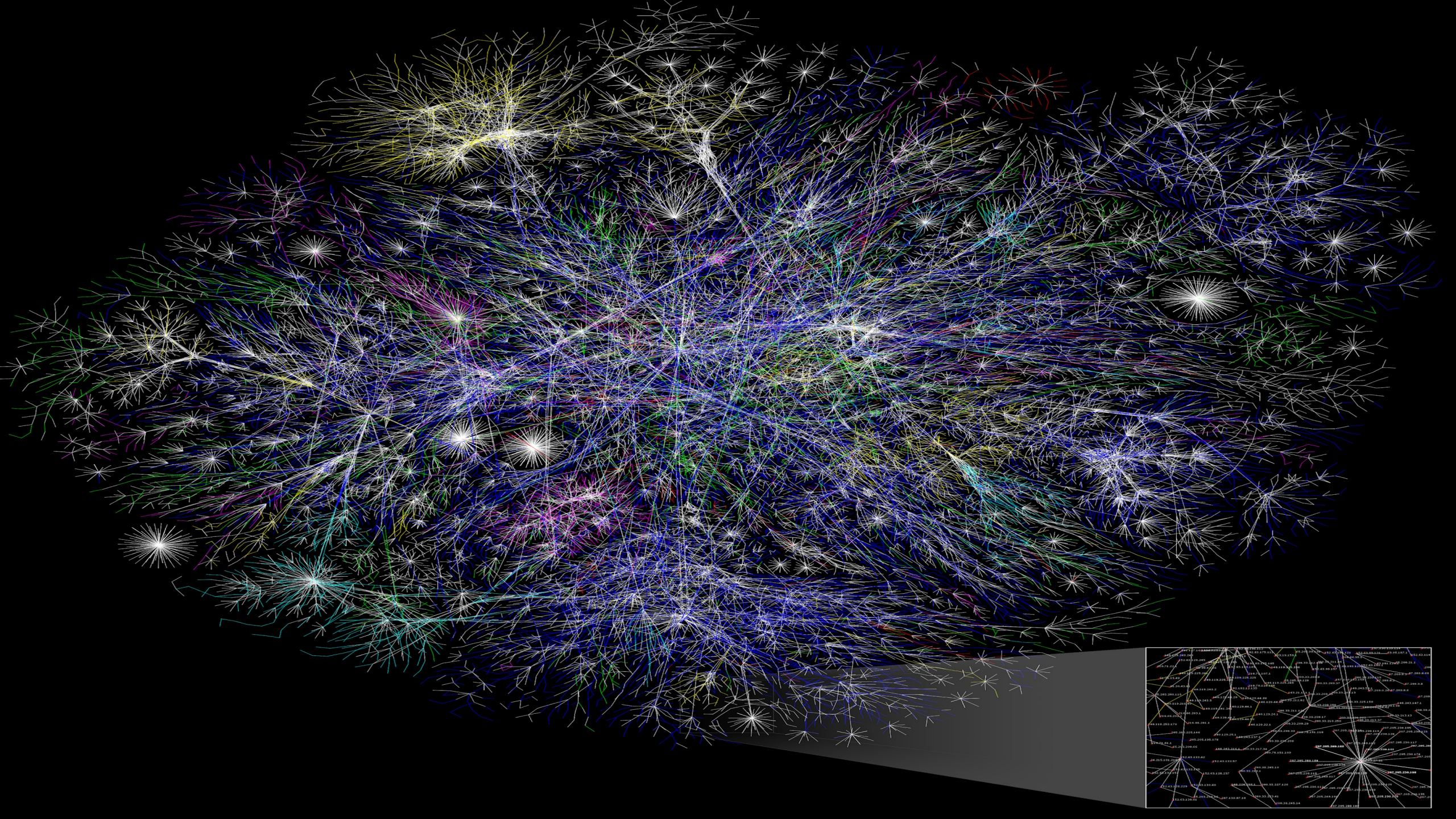
Advanced Networking Concepts



Systems Security

Kevin Cleary

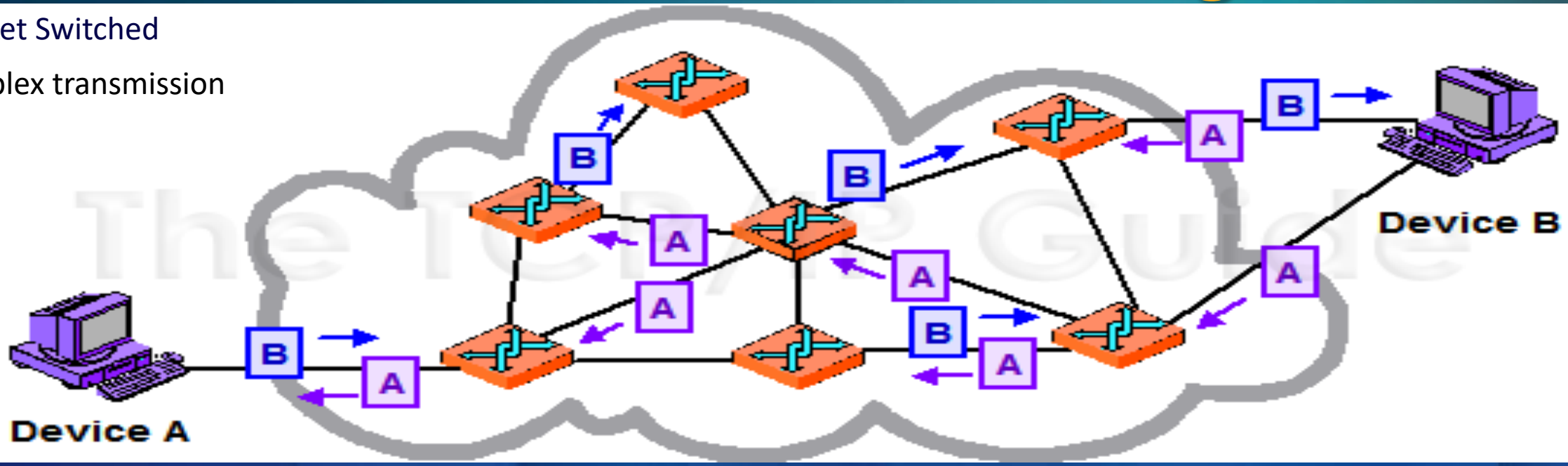
Thursday, November 3, 2022



Packet Vs Circuit Switching

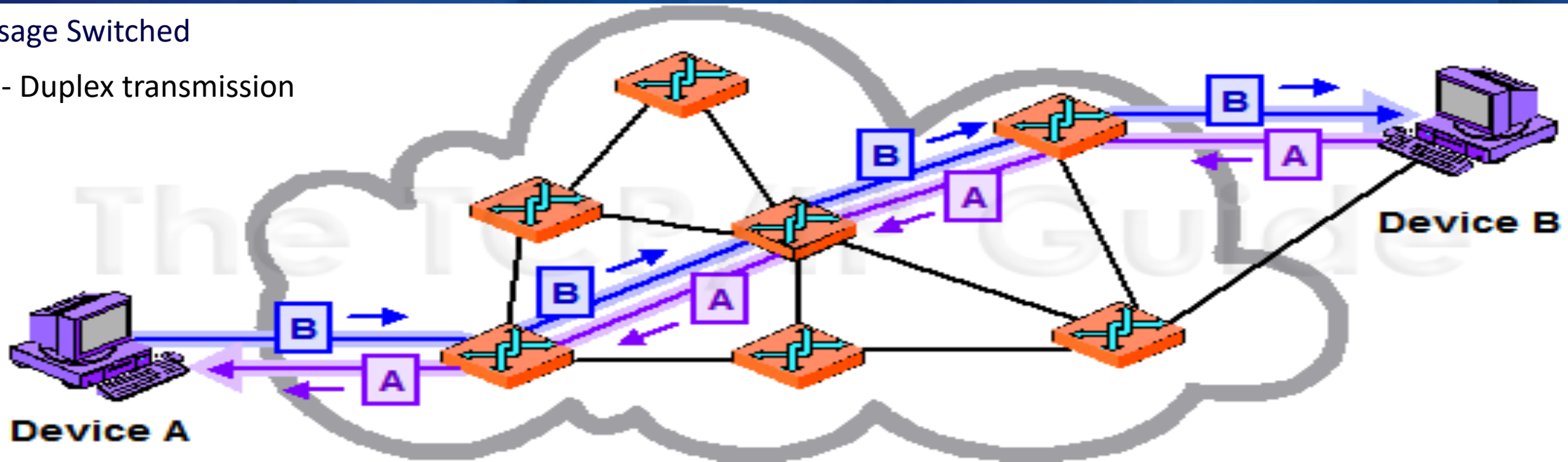
Packet Switched

Duplex transmission

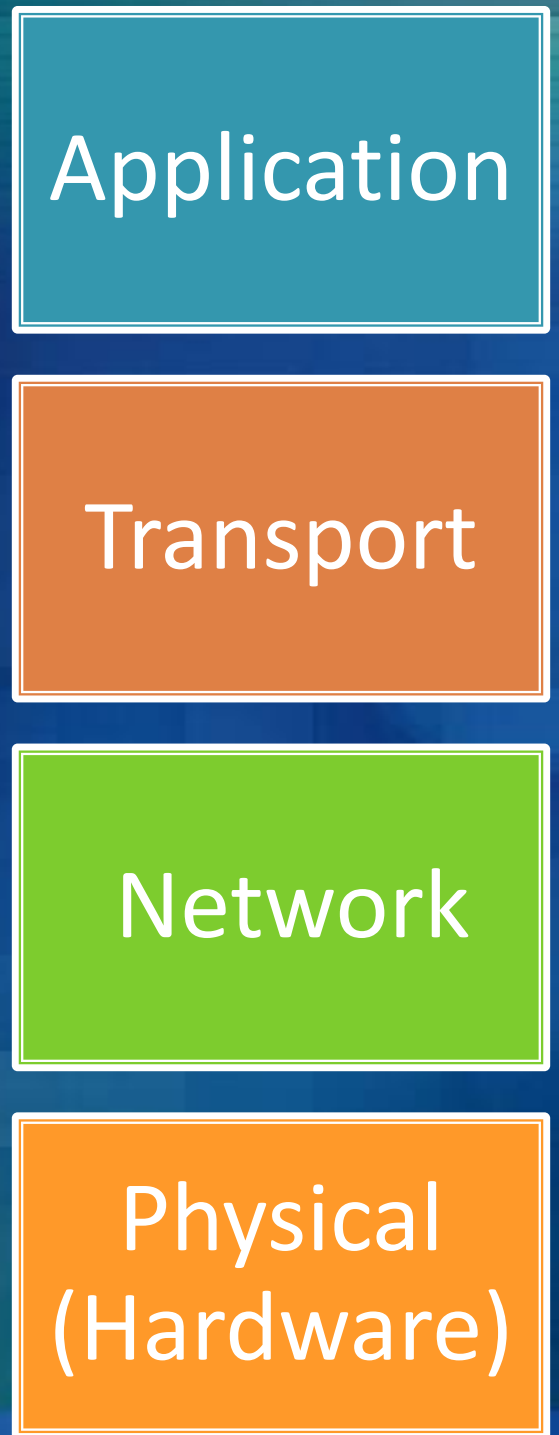


Message Switched

Half - Duplex transmission



The TCP/IP Protocol Stack



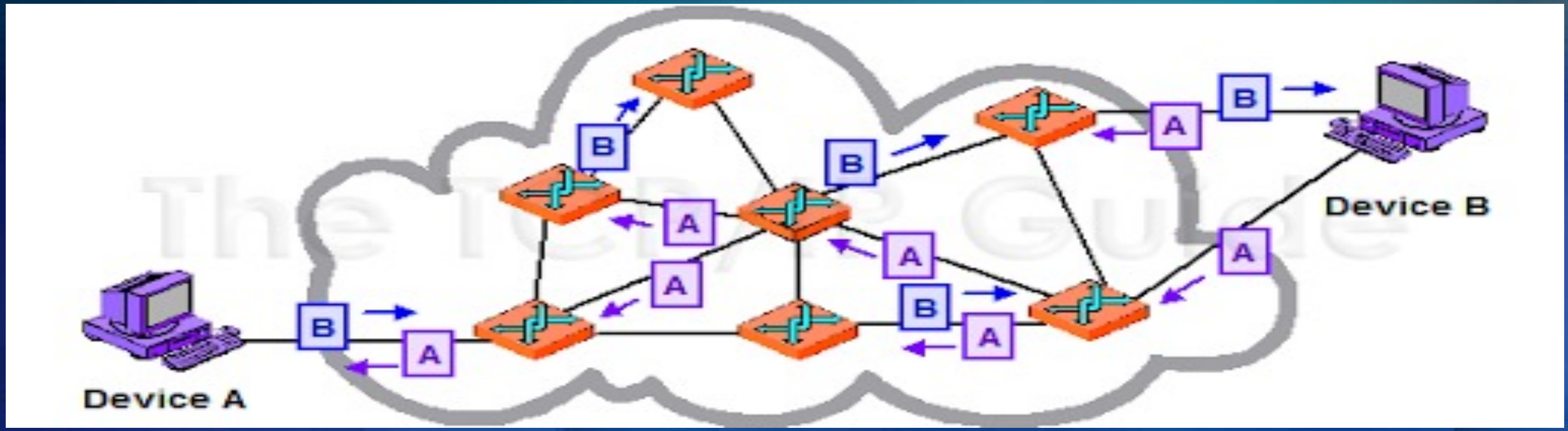
At what layers do we primarily deal with Security?

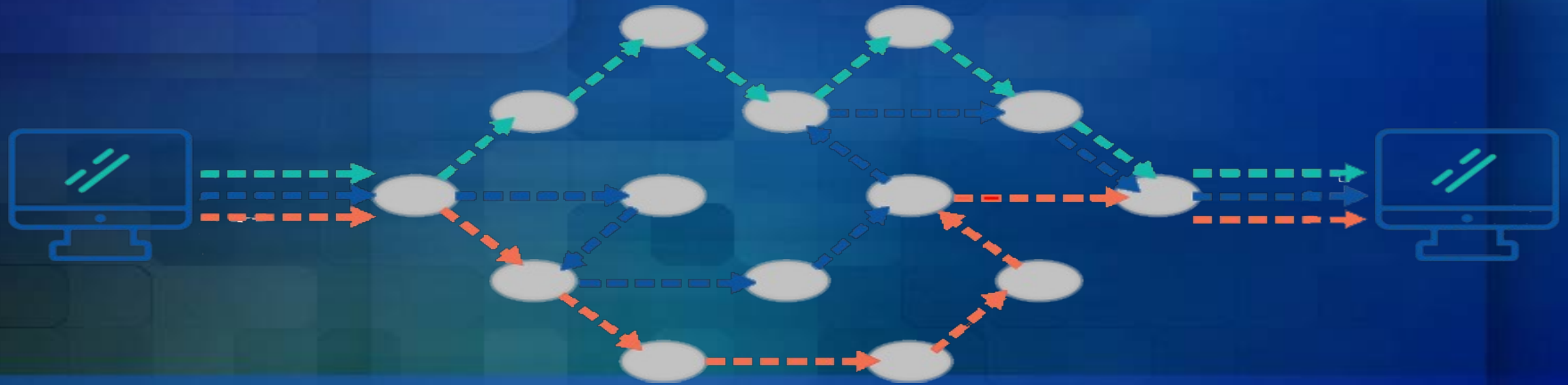
All Layers!

Protocol Stacks

- Protocol stack used by most devices is known as TCP/IP.
  - The stack includes:
    - Network (Internet) - packet switched
    - Transport Layer - circuit switching
- The TCP/IP protocol stack takes care of how computer communications get routed to the correct computer and how packets are reassemble so that they make sense to our applications.
  - Messages travel down and then up the protocol stack.
  - Each protocol within the stack has a set task.
  - transport layer provides management overhead to ensure messages are sent and received in a reliable way, ensuring integrity and authenticity.
  - The IP layer takes care of steering these packets in an efficient, redundant way across many multiple, heterogeneous networks.
- The Hardware layer physical transmits packets wrapped in frames.

The Flow of Internet Data at the Network Layer

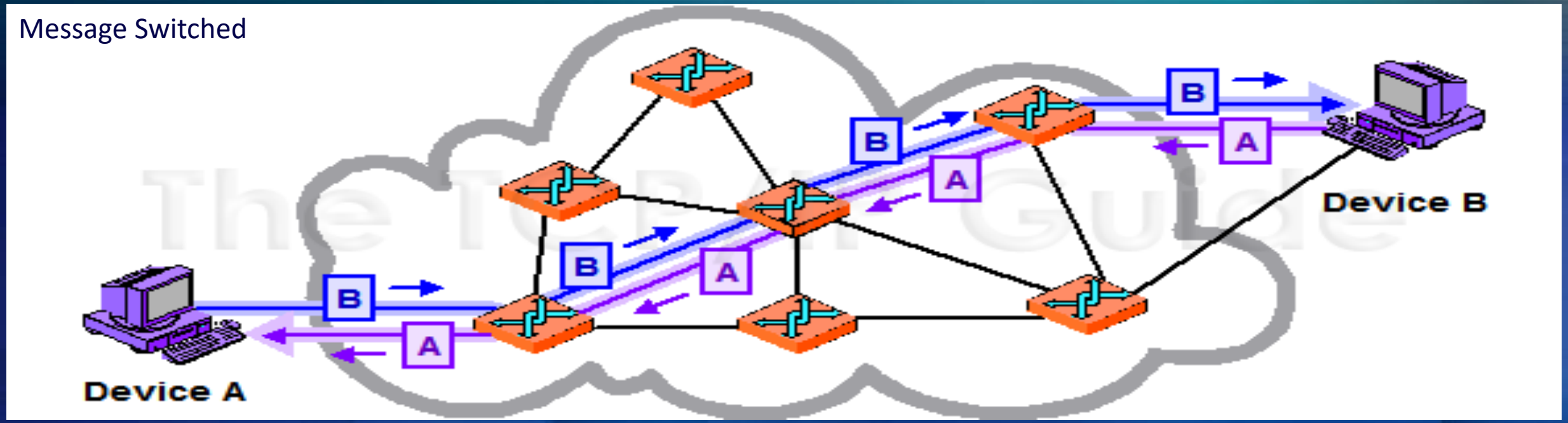




The Network Layer

- IP is an unreliable, connectionless, packet switched protocol.
  - IP's job is to send and route packets to other routers / computers.
  - IP packets are independent entities and may arrive out of order or not at all.
  - IP does not guarantee packet delivery.
  - A series of diagnostic tools exist at the IP layer, the Internet Control Messaging Protocol ICMP. (“ping” and “traceroute”.)
- Advantages:
  - More tolerant to failures
  - Better utilization of an internet connection
- Disadvantages:
  - Packets may arrive out of order
  - Packets may not arrive at all!
  - Controlled chaos from a messaging perspective

The Flow of Internet Data at the Transport Layer



Breaking a Message Down Into Packets

Episode IV, A NEW HOPE It is a period of civil war. Rebel spaceships, striking from a hidden base, have won their first victory against the evil Galactic Empire. During the battle, Rebel spies managed to steal secret plans to the Empire's ultimate weapon, the DEATH STAR, an armored space station with enough power to destroy an entire planet. Pursued by the Empire's sinister agents, Princess Leia races home aboard her starship, custodian of the stolen plans that can save her people and restore freedom to the galaxy....

Episode IV, A NEW HOPE It is a period of civil war. Rebel spaceships, striking from a hidden base, have won

1 /4

their first victory against the evil Galactic Empire. During the battle, Rebel spies managed to steal secret plans

2/4

to the Empire's ultimate weapon, the DEATH STAR, an armored space station with enough power to destroy

3 /4

an entire planet. Pursued by the Empire's sinister agents, Princess Leia races home aboard her starship, custodian of the stolen plans that can save her people and restore freedom to the galaxy....

4 /4

The Transport Layer

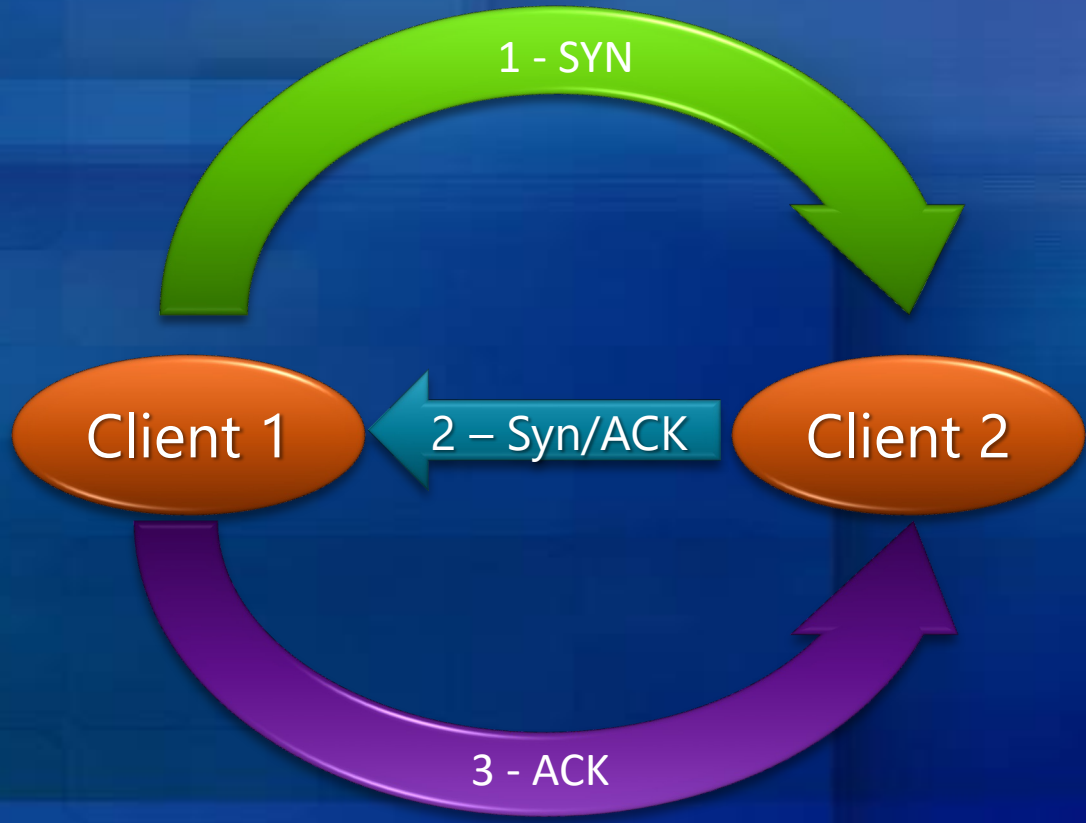
- Your application passes information on to the Transport layer to be broken up in to manageable chunks called packets.
  - Information is added to the packet headers for re-assembly.
    - Sequencing numbers
    - Session IDs
- The Transport layer is a connection-oriented, message switched, reliable, byte stream service.
  - Connection-oriented means:
    - semi-permanent connection is established before any useful data can be transferred
    - a stream of data is delivered in the same order as it was sent
  - TCP must first establish a connection before exchanging data (a handshake).
  - For each packet received, an acknowledgement is sent to the sender.
- Three way handshake to establish a connection
  - TCP SYN, SYN ACK, ACK / SYN-ACK-ACK

The Transport Layer

- The Transport layer, using the Transmission Control Protocol (TCP) takes care of breaking application messages into chunks, known as **packets** and assigning information such as:
  - Port number - help to separate what data is destined to which applications.
    - Email and Web browsers have a specific, unique port number
    - The builds a socket. Ex – 192.168.100.2:25
  - Number of packets sent.
  - The number the packet in the series being sent.
  - Packet sequencing numbers.
  - On the receiving end the TCP protocol helps to arrange packets as they arrive in the correct order for the applications.
  - Provides SSL for whole-session encryption
- A cousin of TCP, User Datagram Protocol (UDP) is commonly used for streaming. A connectionless, unreliable protocol

The Transport Layer

- TCP header flags:
  - Three way handshake to establish a connection
    - SYN – requests synchronization with new sequencing numbers
    - SYN ACK
    - ACK / SYN-ACK-ACK – acknowledges synchronization or shutdown request.
  - RST causes immediate disconnection
  - FIN requests graceful shutdown



The TCP/IP Protocol Stack

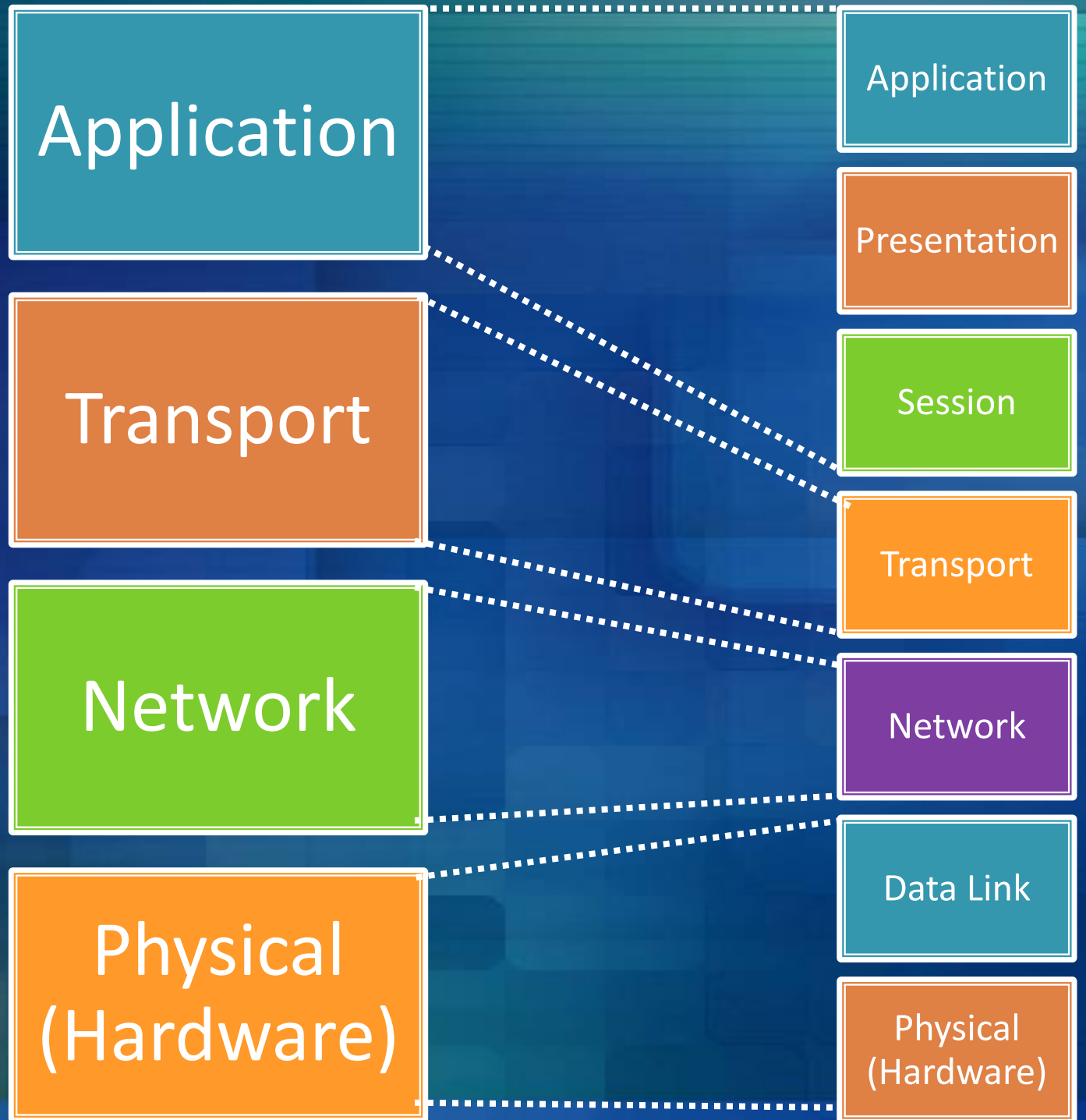
"Please do not throw sausage pizza away"

- Application
- Transport
- Network
- Physical (Hardware)

The OSI Model

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical (Hardware)

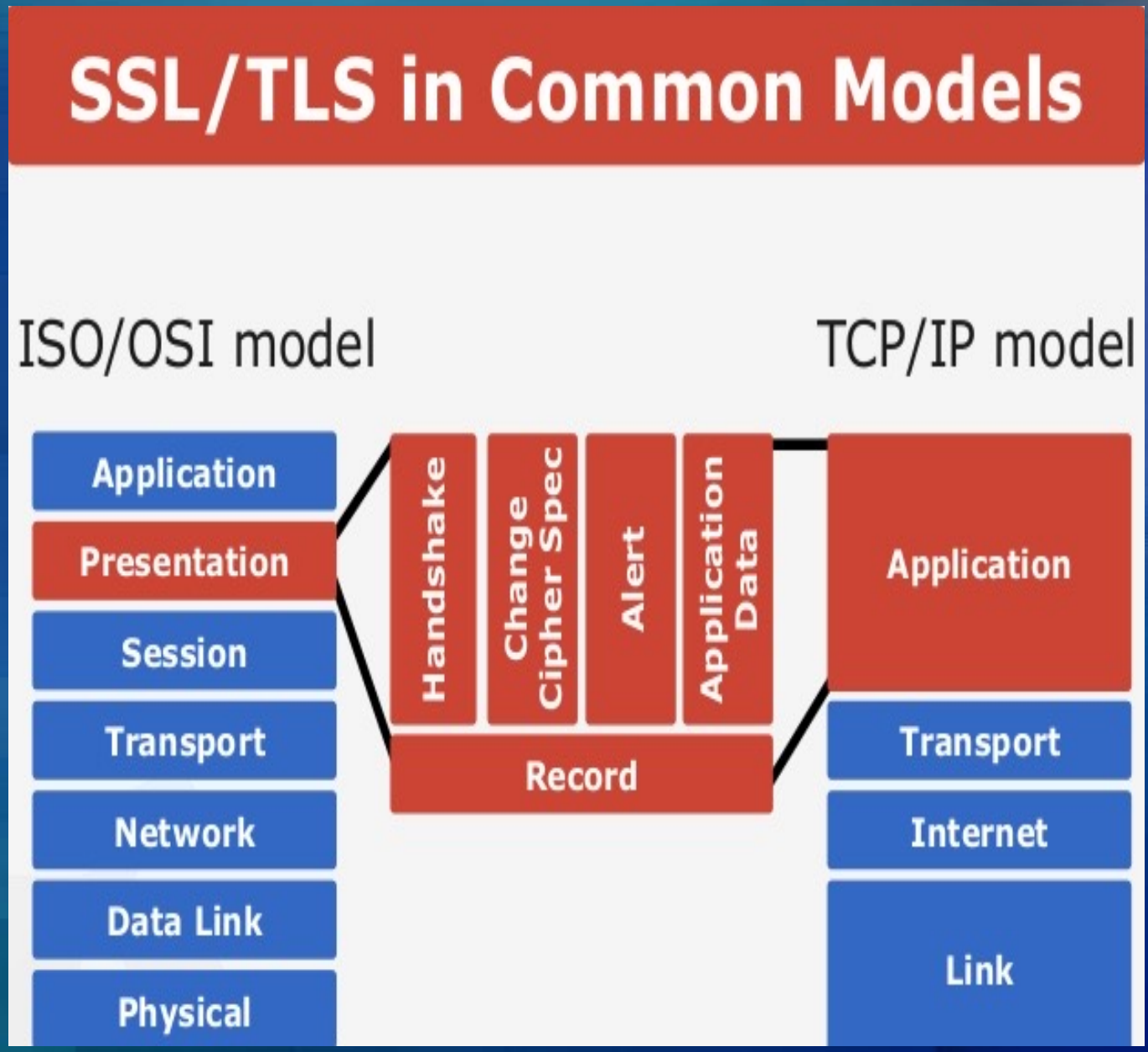
The TCP/IP Protocol Stack



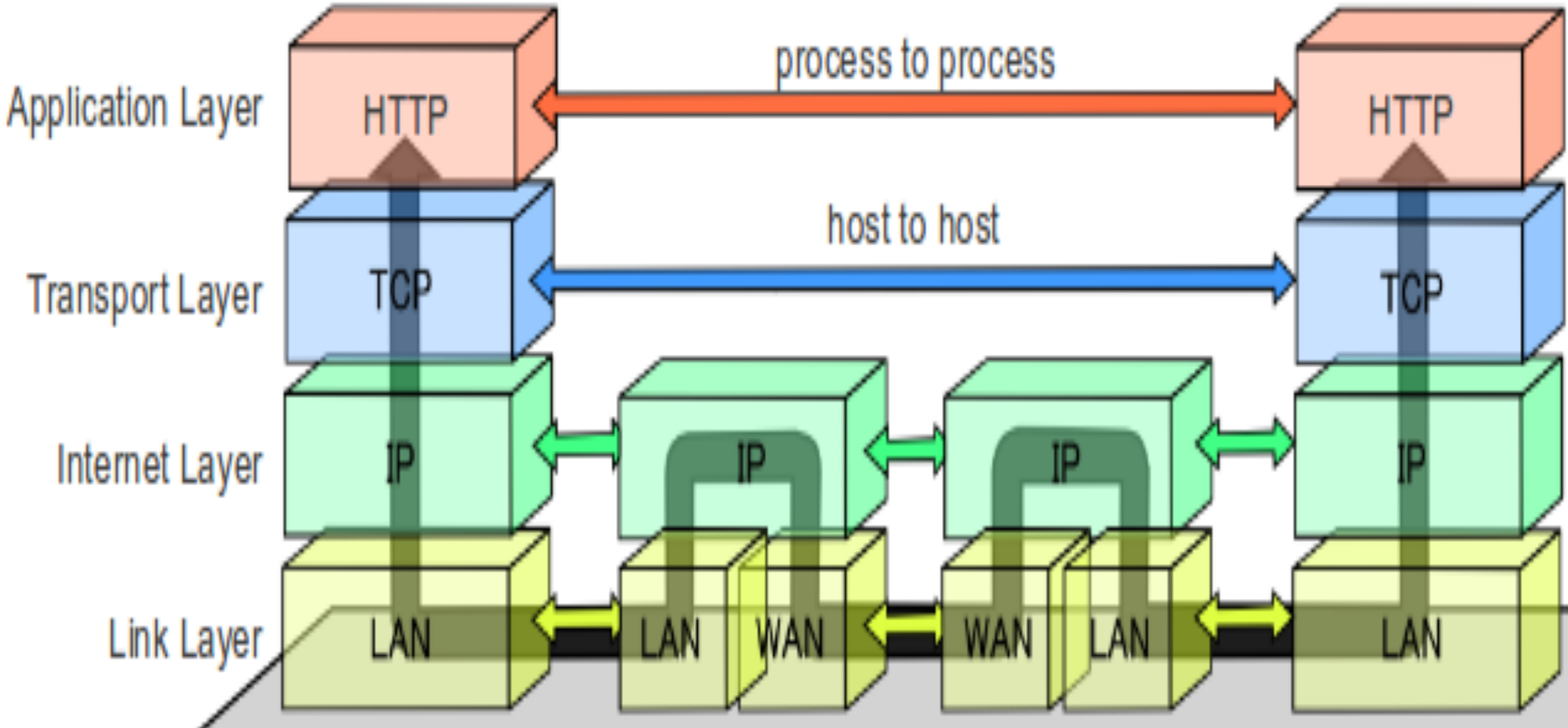
The OSI Model

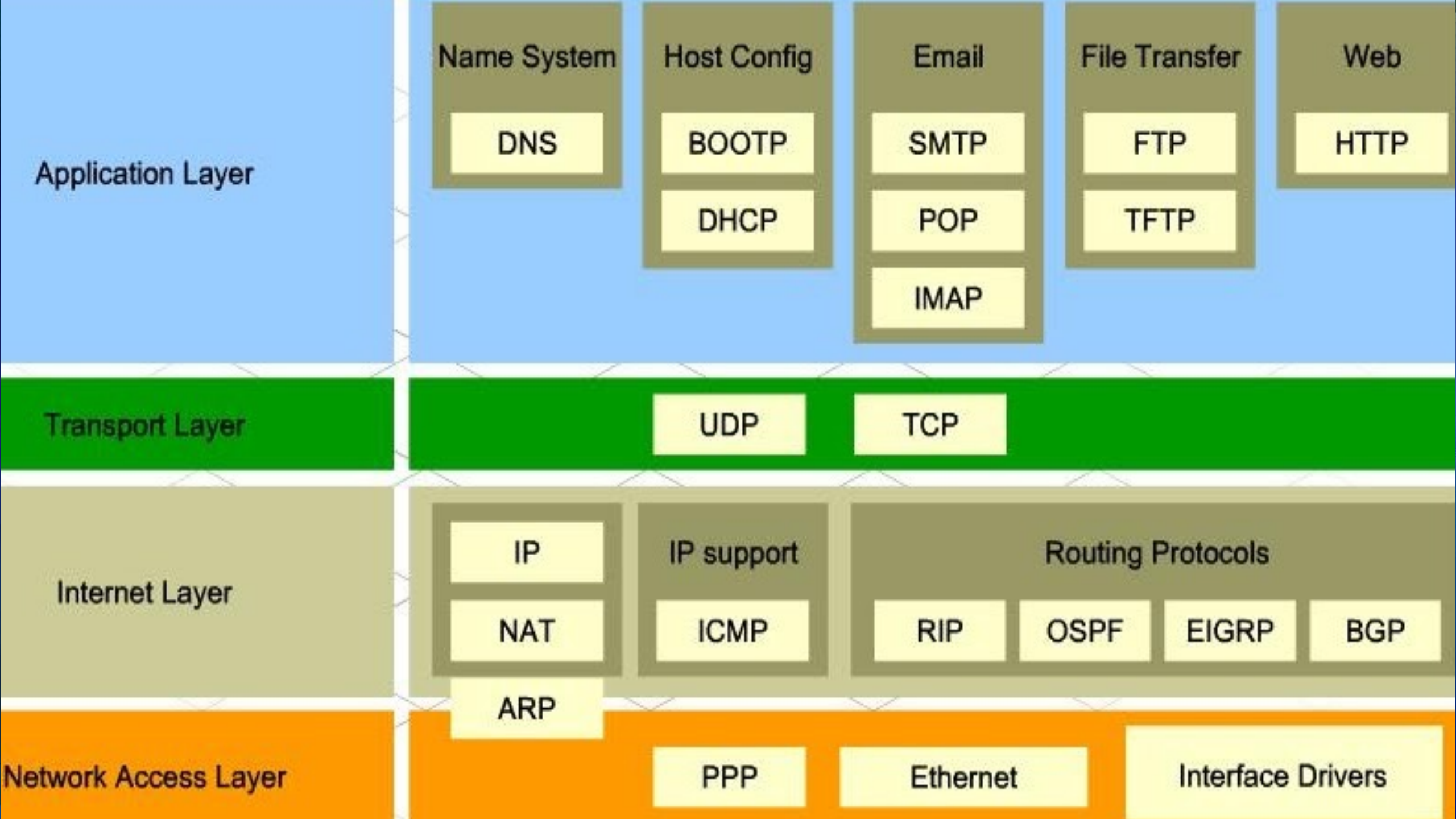
A Word on TLS Encryption and OSI

- Transport Layer Security (TLS) has replaced Secure Sockets Layer (SSL) to provide end to end encrypted connections.
- This all happens at the *Presentation* and *Application* layers, atop the TCP in order to encrypt Application Layer protocols such as HTTP(s), FTP(s), SMTP(s), IMAP(s), etc
- What does this mean for things like firewalls?



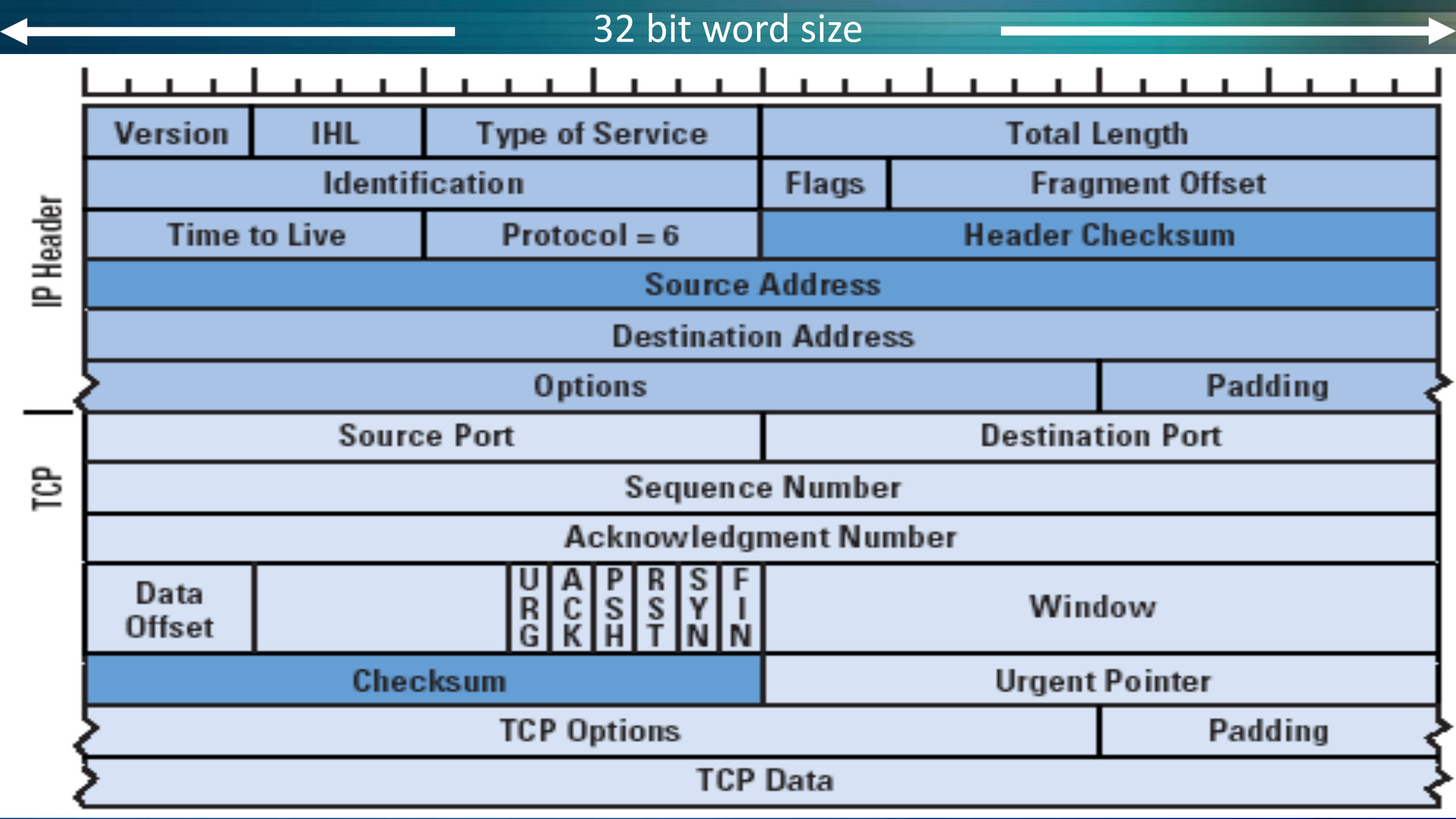
Data Flow of the Internet Protocol Suite




Application Layer
Name System
DNS
Host Config
BOOTP
DHCP
Email
SMTP
POP
IMAP
File Transfer
FTP
TFTP
Web
HTTP
Transport Layer
UDP
TCP
Internet Layer
IP
NAT
ARP
IP support
ICMP
Routing Protocols
RIP
OSPF
EIGRP
BGP
Network Access Layer
PPP
Ethernet
Interface Drivers

Protocol Stacks

- Each layer of the protocol stack places information and metadata into “packet headers”.
  - This is information needed to deliver and re-order the packet once it has arrived to its destination.
  - Packet data payload is variable length up to the maximum allowable size of a packet. Maximum allowable size is known as the Maximum transmission unit (MTU)
    - Not to be confused with the frame size at the data link layer.
    - Commonly 1500 bytes – 40 bytes of header and 1460 bytes for data
    - “Jumbo” frame MTU can grow as large as 9000 bytes.
  - Header information is very important when it comes to packet capture and analysis done by intrusion detection systems.


32 bit word size
IP Header
TCP
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol = 6
Header Checksum
Source Address
Destination Address
Options
Padding
Source Port
Destination Port
Sequence Number
Acknowledgment Number
Data Offset
URG
ACK
PSH
RST
SYN
FIN
Window
Checksum
Urgent Pointer
TCP Options
Padding
TCP Data

```
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 1133, Seq: 1, Ack: 302, Len: 732
    Source Port: 80
    Destination Port: 1133
    [Stream index: 0]
    [TCP Segment Len: 732]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 733    (relative sequence number)]
    Acknowledgment number: 302    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  ▼ Flags: 0x018 (PSH, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·····AP···]
    Window size value: 6432
    [Calculated window size: 6432]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x187c [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▼ [SEQ/ACK analysis]
      [iRTT: 0.002143000 seconds]
      [Bytes in flight: 732]
      [Bytes sent since last PSH flag: 732]
    TCP payload (732 bytes)
```

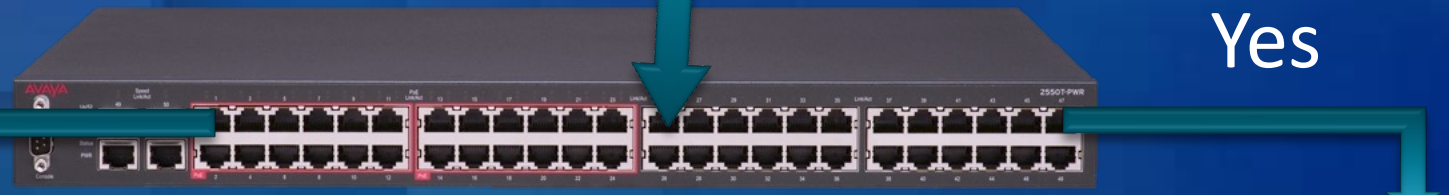
```
▼ Internet Protocol Version 4, Src: 10.10.10.1, Dst: 10.10.10.11
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 772
    Identification: 0x519d (20893)
  ▼ Flags: 0x02 (Don't Fragment)
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xbe37 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.10.1
    Destination: 10.10.10.11
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

Packet Routing at the Network Layer

- IP packet routing is similar to mailing a letter.
- The steps you take in mailing a letter include…
  - Sealing your message in to an envelope.
  - Looking up the address to write on the envelope.
  - Determine if you can hand deliver your message or if it needs to be given to the mail man.
  - If the mailman must deliver the message you must hand the message off to them. The mailman works with other mailmen to then deliver your envelope.
  - Wait for a response.

The Flow of Internet Data

- The IP layer determines if the client you're sending a packet to resides on your LAN by looking at:
  - Your client's IP address
  - Your client's subnet mask
  - Your destination's IP address



No

Yes

Send Packet to The Gateway

Send Packet to
The Destination
(located on same LAN)

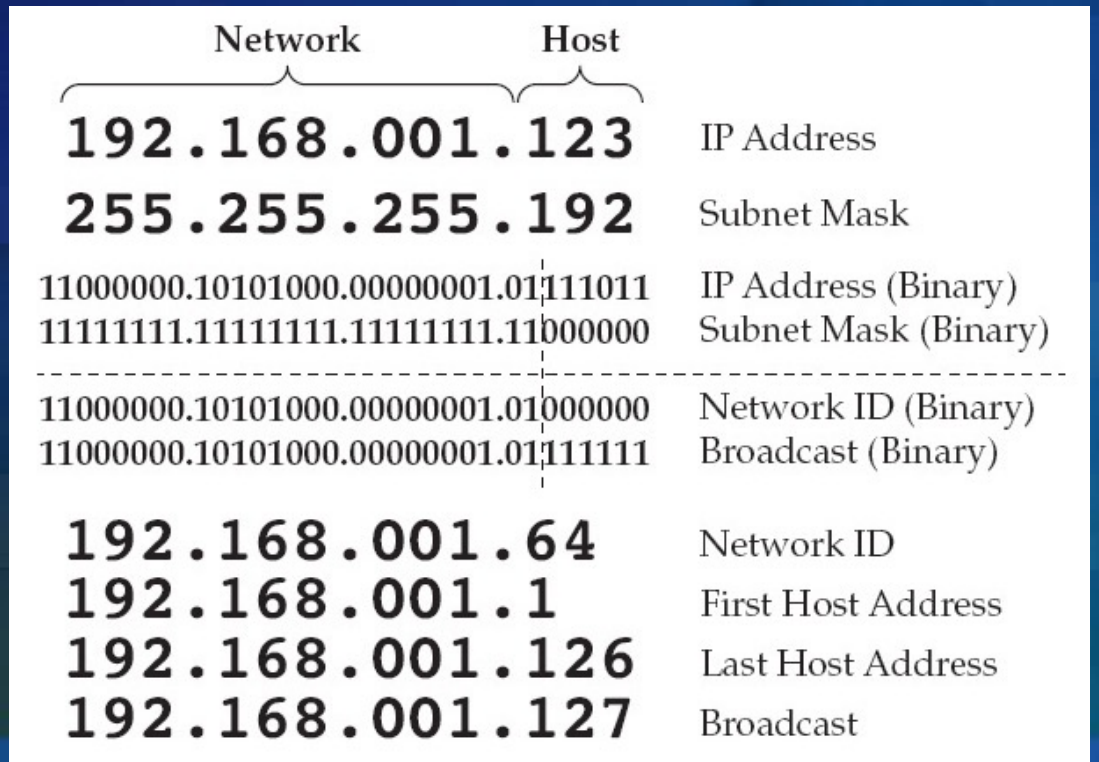
Network – IP Client Information

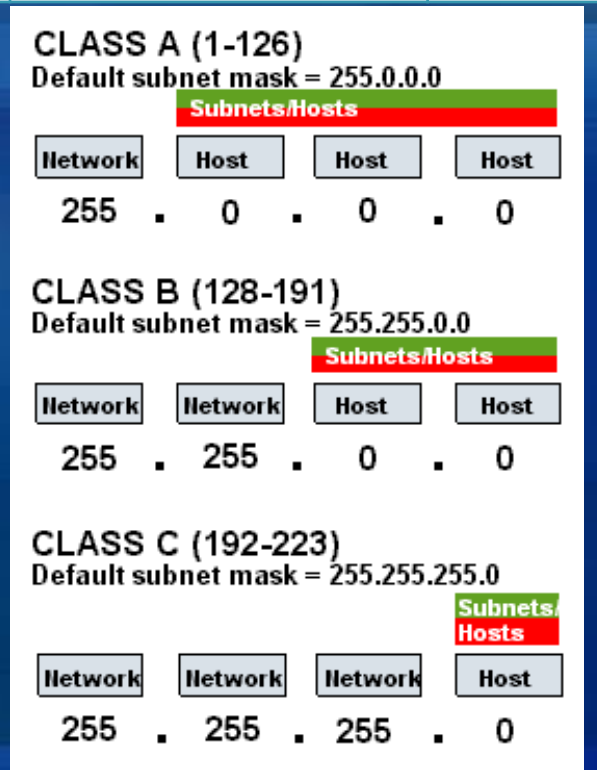
- To route packets correctly, a device must be configured with:
  - IP address: Every IP address on the internet is unique*:
    - IPV4 - 4 x 8 bit (32 bit) numbers represented in decimal notation separated by ‘.’s. For example 128.205.34.66.
    - IPV6 - 8 x 16 bit (128 bit) alphanumeric addresses in decimal notation separated by ‘.’s. For example 2001:0000:3238:DFE1:63:0000:0000:FEFB
    - IP addresses (To and From) are placed in packet headers, similar to an envelop.
  - Subnet Mask – used to determine the boundaries of a Local Area Network.
    - A subnet mask resembles an IP address. Ex 255.255.255.0
  - Gateway IP Address – where packets destined outside LAN are handed off.
- Some IP ranges are designated as **internal** ranges and are repeatable
  - 192.168.0.0 - 192.168.255.255 (65,536 IP addresses) - private
  - 172.16.0.0 - 172.31.255.255 (1,048,576 IP addresses) - private
  - 10.0.0.0 - 10.255.255.255 (16,777,216 IP addresses) – private
  - 127.0.0.1 -127.255.255.255 – loopback (testing and troubleshooting)

Network – Subnetwork Ranges

- Networks usually come in several sizes (number of addresses that can be assigned to hosts)

Class	Range	Network Address	Host Address	Number of Hosts
A	1.0.0.0 – 126.0.0.0	xxx	xxx.xxx.xxx	16,777,214
B	128.0.0.0 - 191.255.0.0	xxx.xxx	xxx.xxx	65,534
C	192.0.1.0-223.255.255.255	xxx.xxx.xxx	xxx	254

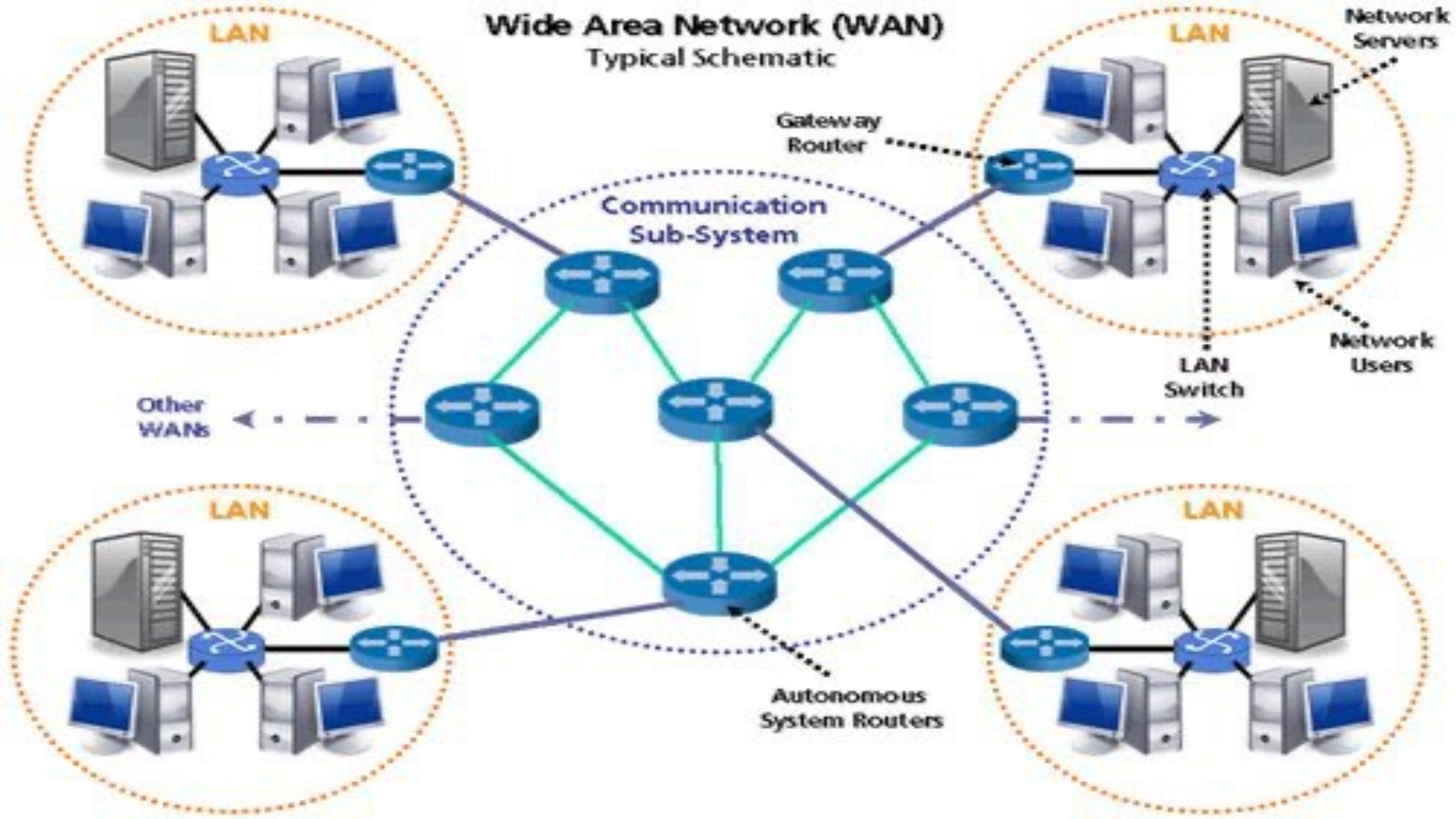




Subnetwork Ranges

- But… subnet defaults can be adjusted!
  - https://www.calculator.net/ip-subnet-calculator.html
- In practice, by adjusting the subnet mask, we can have much more granular control over the size, number and topology of our networks.
- More subnets means more segmentation!!! (more to come on that)

Subnet Mask	Network bits	# of Host per Subnet
255.255.255.252	/30	2
255.255.255.248	/29	6
255.255.255.240	/28	14
255.255.255.224	/27	30
255.255.255.192	/26	62
255.255.255.128	/25	126
255.255.255.0	/24	254
255.255.254.0	/23	510
255.255.252.0	/22	1,022
255.255.248.0	/21	2,046
255.255.240.0	/20	4,094
255.255.224.0	/19	8,190
255.255.192.0	/18	16,382
255.255.128.0	/17	32,766
255.255.0.0	/16	65,534
255.254.0.0	/15	131,070
255.252.0.0	/14	262,142
255.248.0.0	/13	524,286
255.240.0.0	/12	1,048,574
255.224.0.0	/11	2,097,150
255.192.0.0	/10	4,194,302
255.128.0.0	/9	8,288,606
255.0.0.0	/8	16,777,216

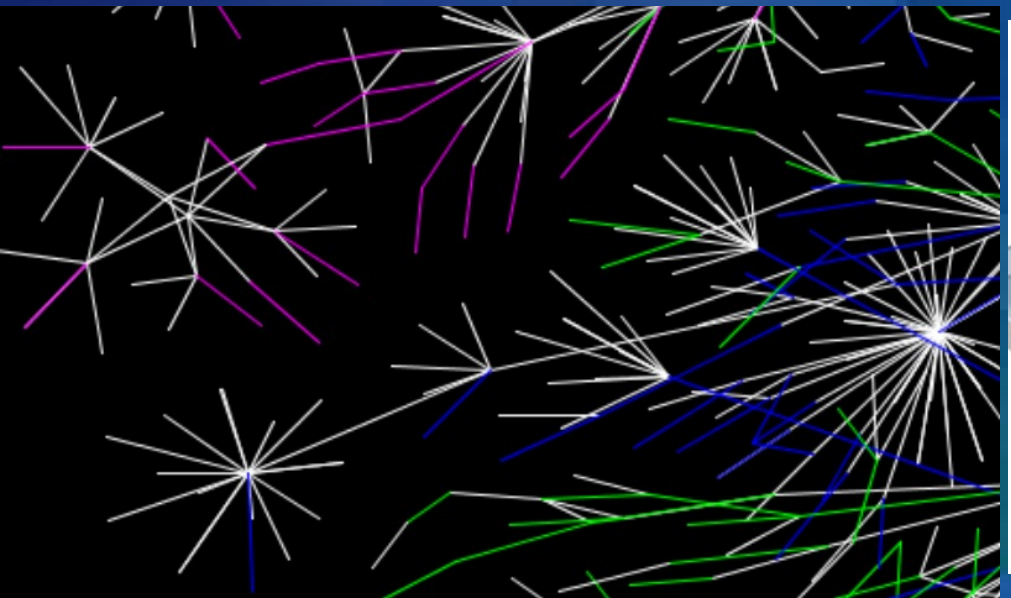

Wide Area Network (WAN)
Typical Schematic
LAN
LAN
Network Servers
Gateway Router
Communication Sub-System
Network Users
LAN Switch
Other WANs
LAN
LAN
Autonomous System Routers

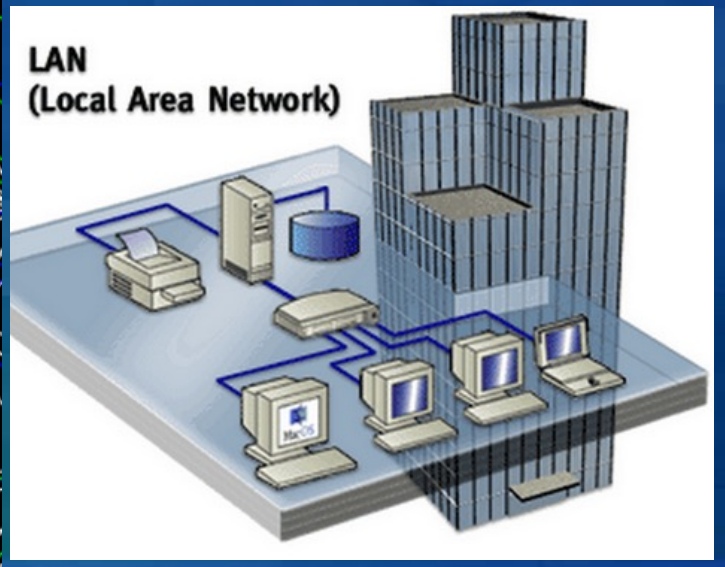
The Flow of Internet Data at the Network Layer

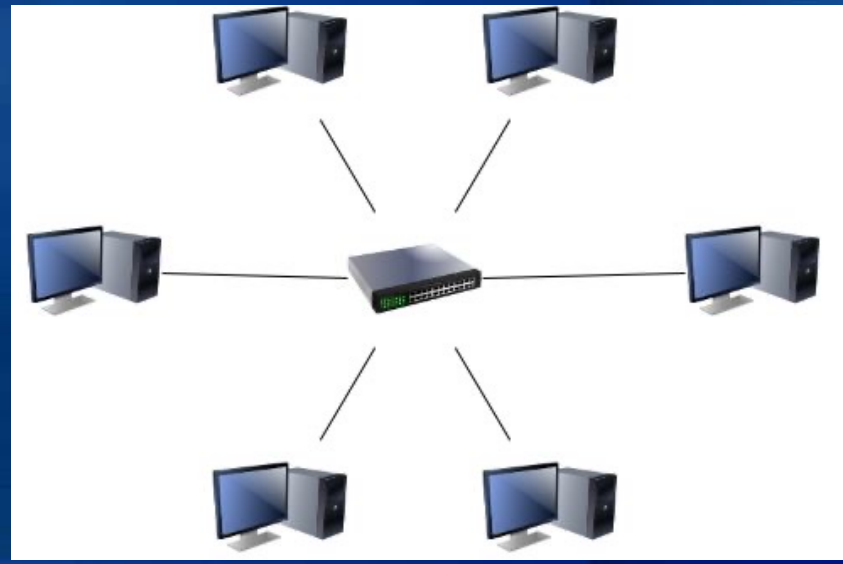
- Gateways will communicate with one or more other gateways and devices called “routers”.
  - Routers are usually connected between subnets and take care of handing off massive amounts of packets.
  - Gateways make convenient locations for Firewall and Monitoring measures.
- Routers maintain multiple connections to one another.
  - Use the following protocols – RIP, OSPF, IS-IS, IGRP, BGP.
- Routers constantly keep track of other routers around them.
  - They will look at things like link speeds, delay times, network congestion.
  - Routers are connected to “backbones”. Backbones are the information super highways of the internet.
- Routers have a role in security but are not security devices.
- Key security control at the network layer is through Firewalls!

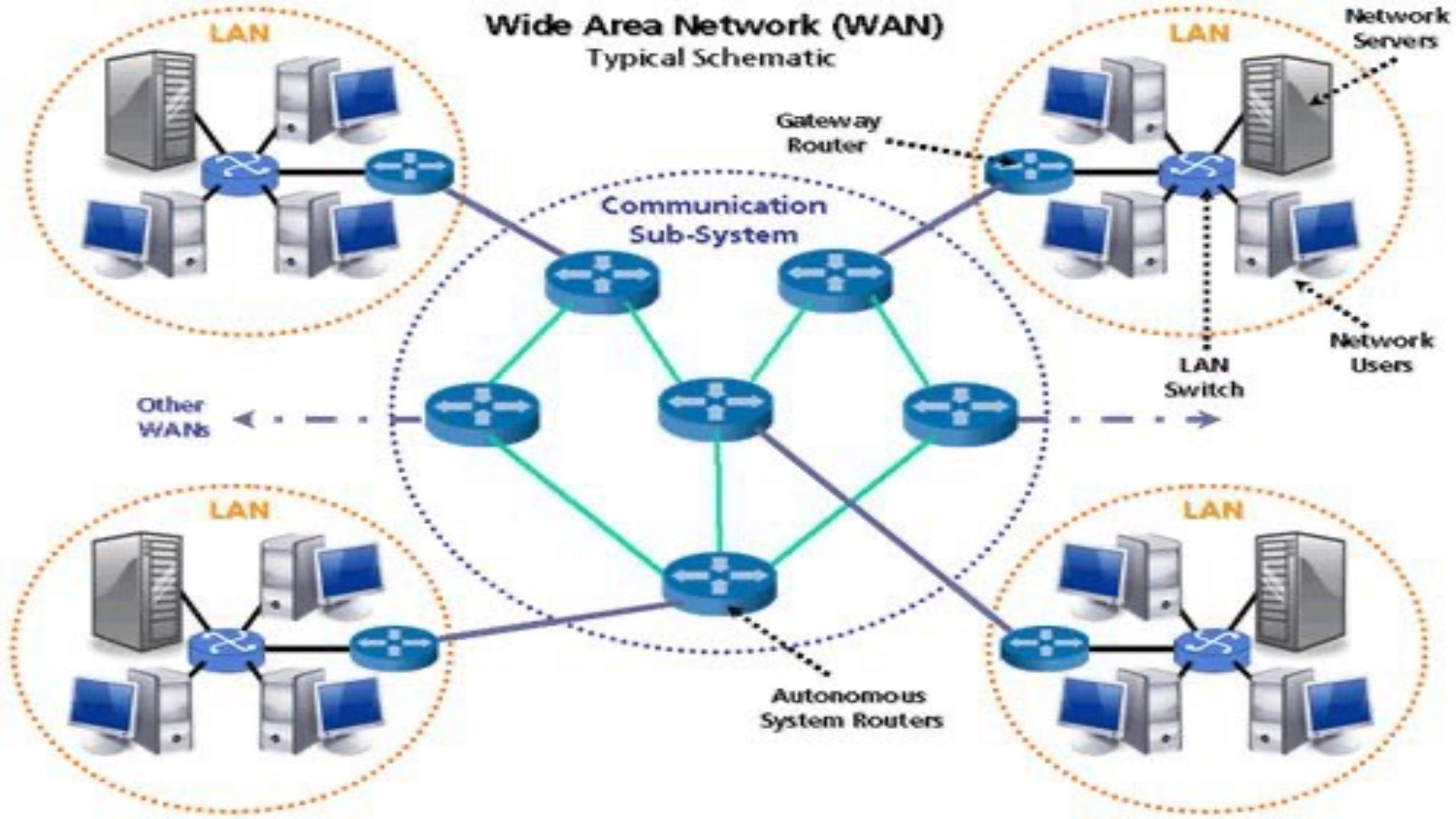
Local Area Networks (Subnets)

- LANs are the most basic type of network.
  - These small networks are the building blocks of the Internet!
  - Can be thought of as a “local neighborhood” of computers or devices.
  - All devices on the same LAN communicate directly with one another across a “switch” (collision domain).
  - LAN communication DOES NOT require a gateway.
  - Tend to be more “local”







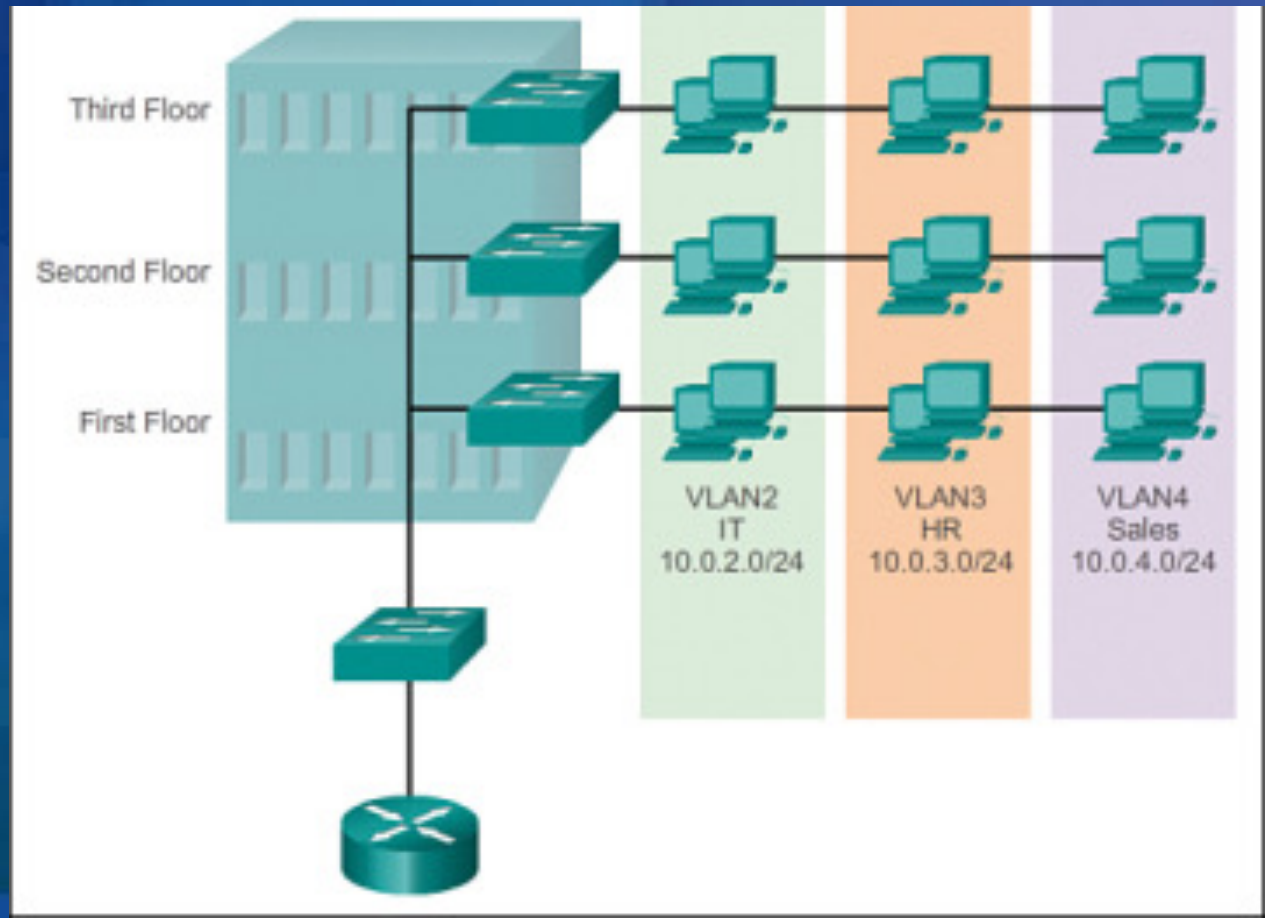

Wide Area Network (WAN)
Typical Schematic
LAN
LAN
Network Servers
Gateway Router
Communication Sub-System
Network Users
LAN Switch
Other WANs
LAN
LAN
Autonomous System Routers

Wide Area Networks

- LANs are interconnected together to form WANs
- LANs get connected to WANs through routers and gateways.
  - Which make them ore expensive to configure and manage.
- The “Internet” is one big WAN.
- We can connect LANs to WANs through both wireless and Wired Connections.
- WANs can span much larger geographic distances than LANs.
- WANs typically boast higher speed connections for each LAN member.
- It’s typical and necessary for enterprise IT operations to have many LANs interconnected.
- WANs may be defined by their geographic reach
  - CAN – Campus Area Network
  - PAN – Personal Area Network
  - MAN – Metropolitan Area Network
  - * but these are just fancy names for WANs.

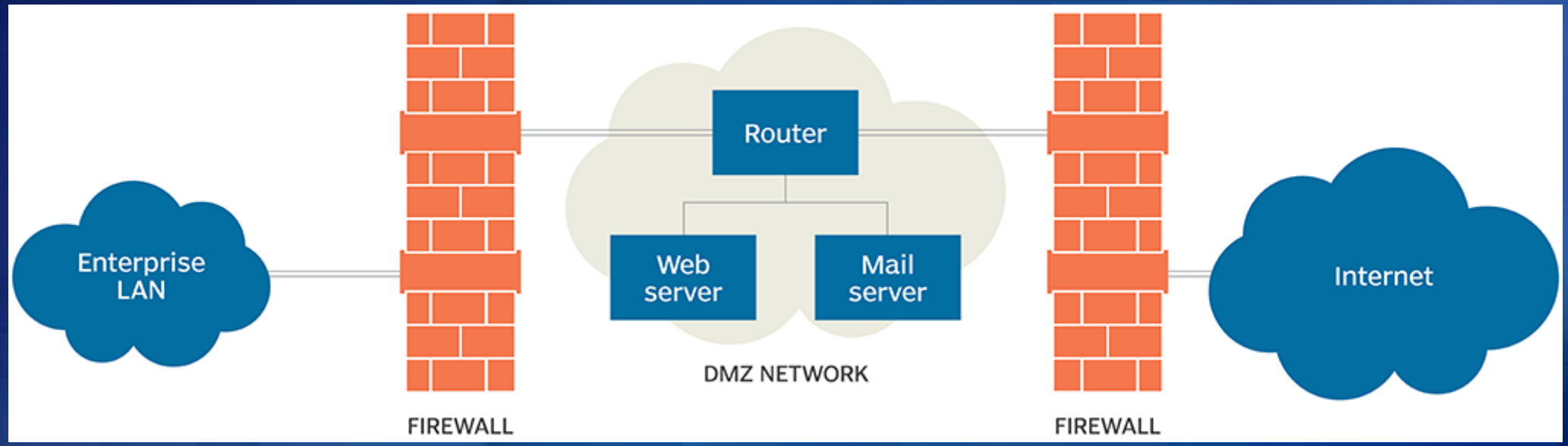
Network Segmentation and Topology

- Network and LAN segmentation is a fundamental security concept.
- Segmenting a network:
  - Limits the broadcast reach of devices on a subnetwork
  - Enables additional firewalls to be placed at the boundary of each network
- LANs can be organized by :
  - Geographic area
  - Device type / Function
  - Administrative boundary
  - Data or work classification
  - Department or entity
  - Type of service.
- Air-Gapping is the ultimate in Network segmentation!



Network Segmentation and Topology

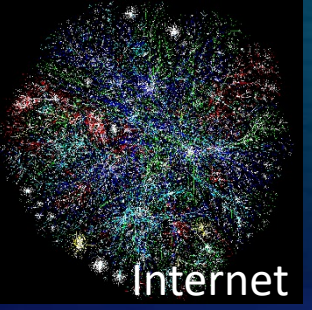
- Demilitarized Zone (DMZ) - a perimeter or screened subnetwork
  - Networks considered less secure but not totally insecure land in the DMZ



  - DON’T DO THIS
  - The only thing a DMZ is good for is Honeypots!


Trust No One!

Network Segmentation and Topology



Border or
Choke Router

Next Gen
Firewall

WAN

LAN

LAN

LAN

LAN

Multi-tier Firewall Strategy

Network Segmentation and Topology

- What about:

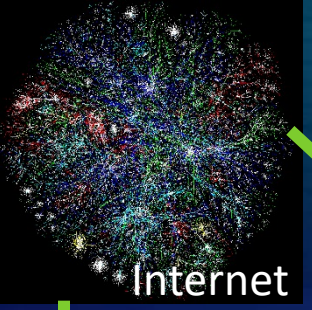
Guest Networks

WiFi

Smartphones

0-Trust Architecture

Network Segmentation and Topology



Border or
Choke Router

Next Gen
Firewall

WAN

LAN

LAN

LAN

LAN

VPN

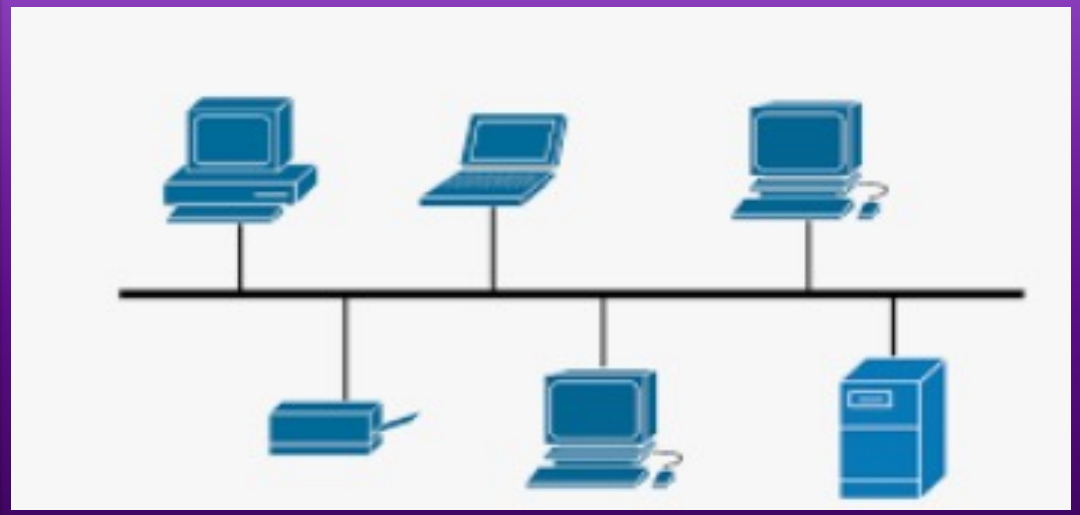
Network Segmentation and Topology

- Multiple “Edge” networks should exist, based on access needs
  - Separate networks (edge and internal) for discrete services.
  - Sensitive servers are not directly open to the world
  - Traffic into a server or service is handled via proxy servers or load balancers which then interact with back-end servers.
  - Provides a layer of security as this restricts the ability of bad actors to directly access internal servers and data via the Internet.
  - Pinhole firewall rules should be leveraged to provide only the minimum requires access – **Remember the importance of “Least Privilege”.**
- Enterprise services should be placed on separate subnetworks based on type of service and need for access.
- Disparate WFH clients should tunnel into secure network segments through VPN connections. (Full Tunnel vs Split Tunnel)

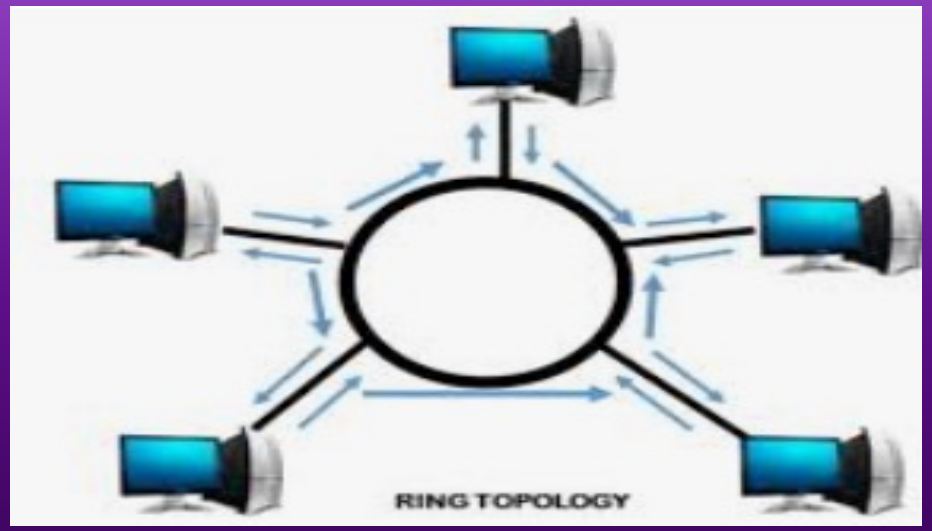
The Data Link (Hardware) Layer

- The “hardware“ layer (AKA “Data Link Layer”) is in charge of transmitting data over a physical medium (wired or wireless).
- The physical medium for transmitting data can take on many forms and is implemented with a wide variety of technologies.

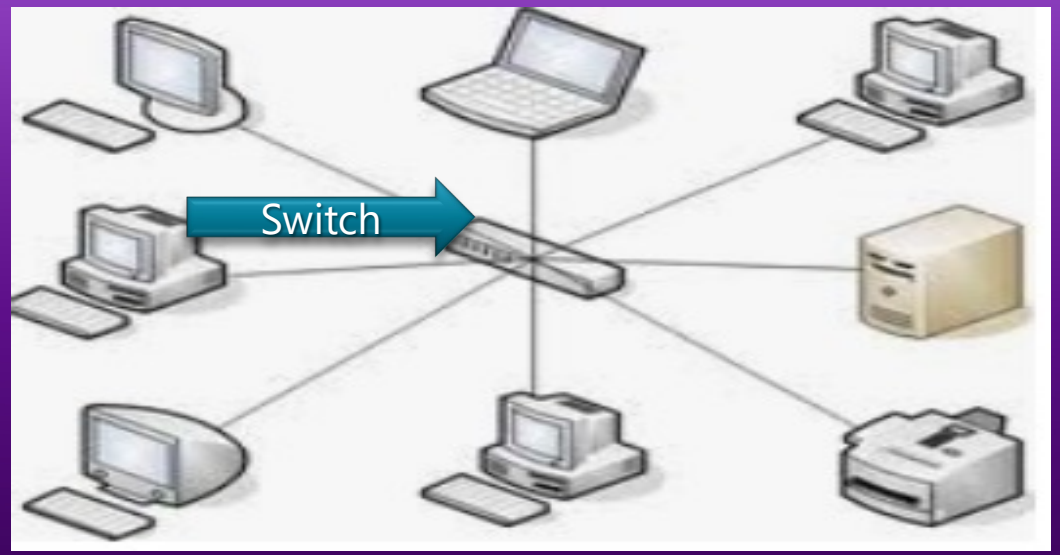
Connecting to LANs - Ethernet



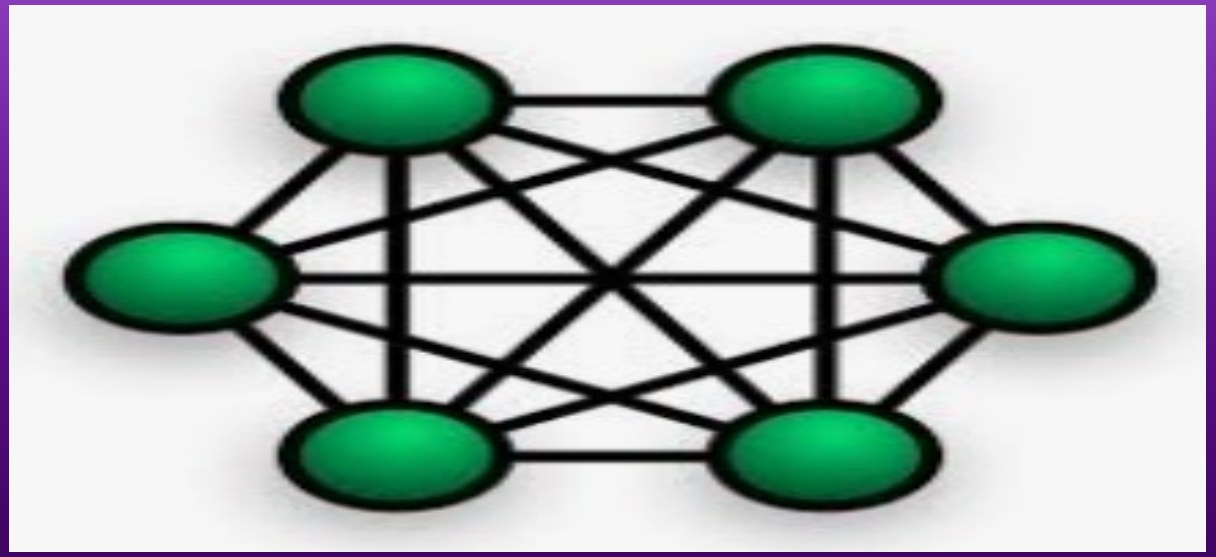
Bus (deprecated)



Ring (deprecated)



Star (Ethernet)



Mesh (WiFi)

Connecting to LANs - Ethernet

- Switches - devices that physically connect multiple computers together to form a subnet.
  - Switches use a star topology and work by joining electrical pathways together, so that devices can talk to each other.
  - Hubs look similar to switches but use a ring topology, relying on each member node to pass along a packet of information.
  - More advanced switches support Virtual Local Area Networks (VLANS), SPANing, TAPing, port filtering, etc…
  - VLANs give us the ability for nearly unlimited network segmentation and network level isolation, without needing multiple switches.

Securing Layer 2 Switches

- Secured remote access and management
- Physical security
- VLAN configuration and segregation
- Port-based Network Access Control (NAC) for authorized devices
- Port activation, deactivation and re-vlan based on IDS monitoring.
- Port level security:
  - MAC address flooding (limit # of MACs / port)
  - DHCP spoofing (using trusted ports)
  - Storm control (Broadcast, multicast, unicast)
  - Quality of Service (QoS) queues
  - Dynamic ARP inspection (discard ARP packets with invalid MAC address to IP address bindings).
  - Switch loop protection

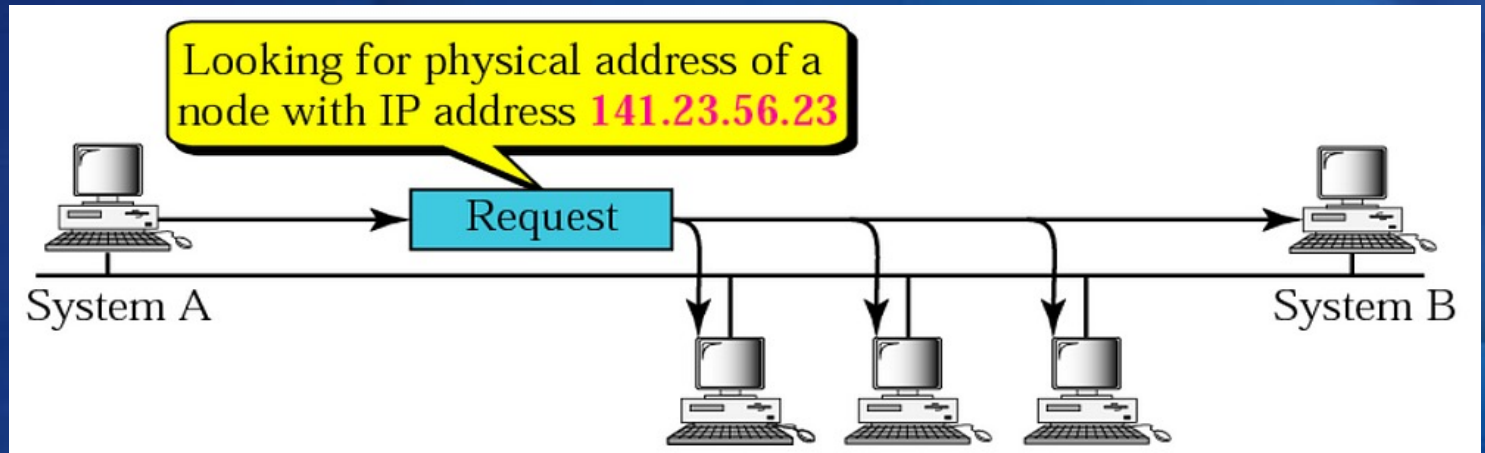
The Data Link (Hardware) Layer

- All network interface cards (NICs) have a hardware address called a "MAC" address, or "Media Access Control Address".
  - hardcoded on the NIC and *usually* cannot be changed.
  - MAC address is used when delivering messages within subnet, by the switch.
- Possible for a MAC address to have multiple IP addresses bound to it.
- The binding between MAC and IP address is handled through "Address Resolution Protocol" (ARP).

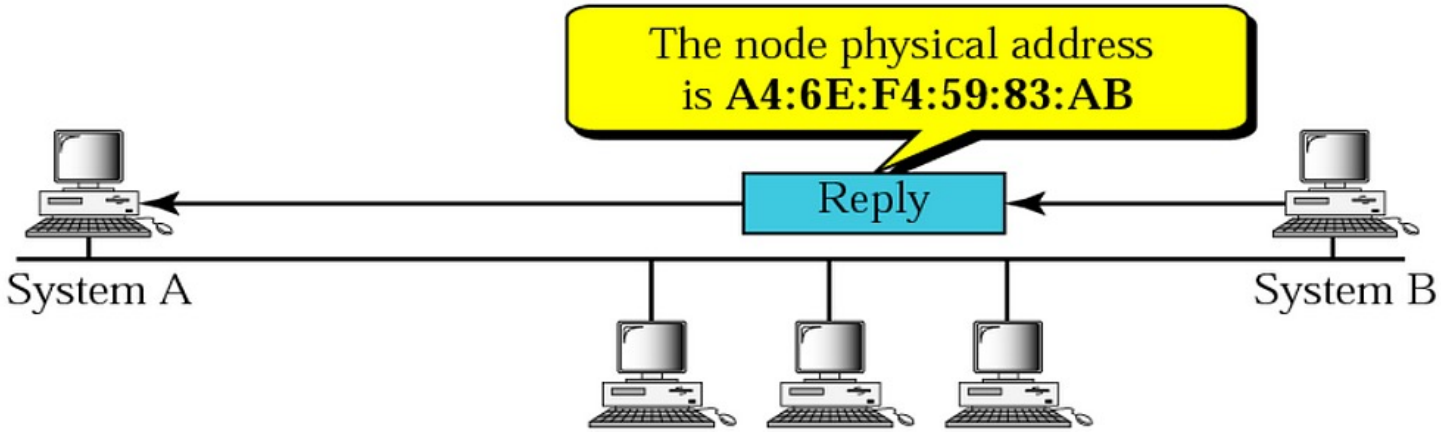
```
Media State . . . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : Intel(R) 82579LM Gigabit Network Connection #2
Physical Address. . . . . . . . . : D4-BE-D9-95-EA-C7
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

The Hardware Layer

- Your machine will only use ARP to communicate with other devices on your own subnet.



a. ARP request is broadcast



b. ARP reply is unicast