Advanced Networking Concepts
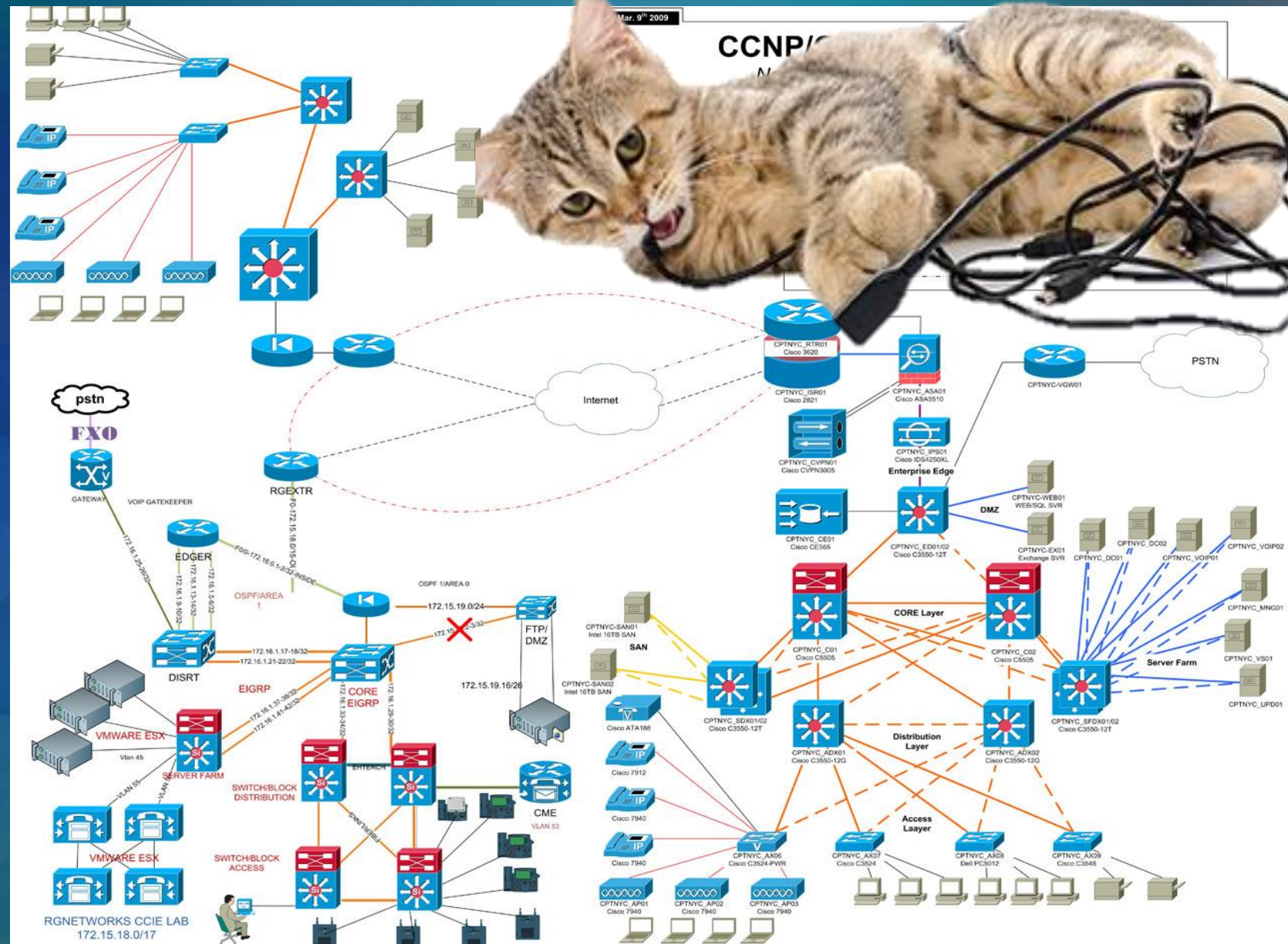
Cyber Defense
Kevin Cleary
Monday, March 25, 2019

The Internet

- The Internet is governed by a series of <u>protocols</u> that form the rules for how communications should happen

- The Internet is a network of networks.
  - There is no centralized point.
  - There are no boundaries.

- Information sent from one location on the internet to another is broken down into smaller, more manageable pieces called "<u>packets</u>".

The TCP/IP Protocol Stack

Application

Transport

Network

Physical (Hardware)

At what layers do we primarily deal with Security?

All Layers!

The TCP/IP Protocol Stack

Application

Transport

Network

Physical (Hardware)

The OSI Model

Application

Presentation

Session

Transport

Network

Data Link

Physical (Hardware)
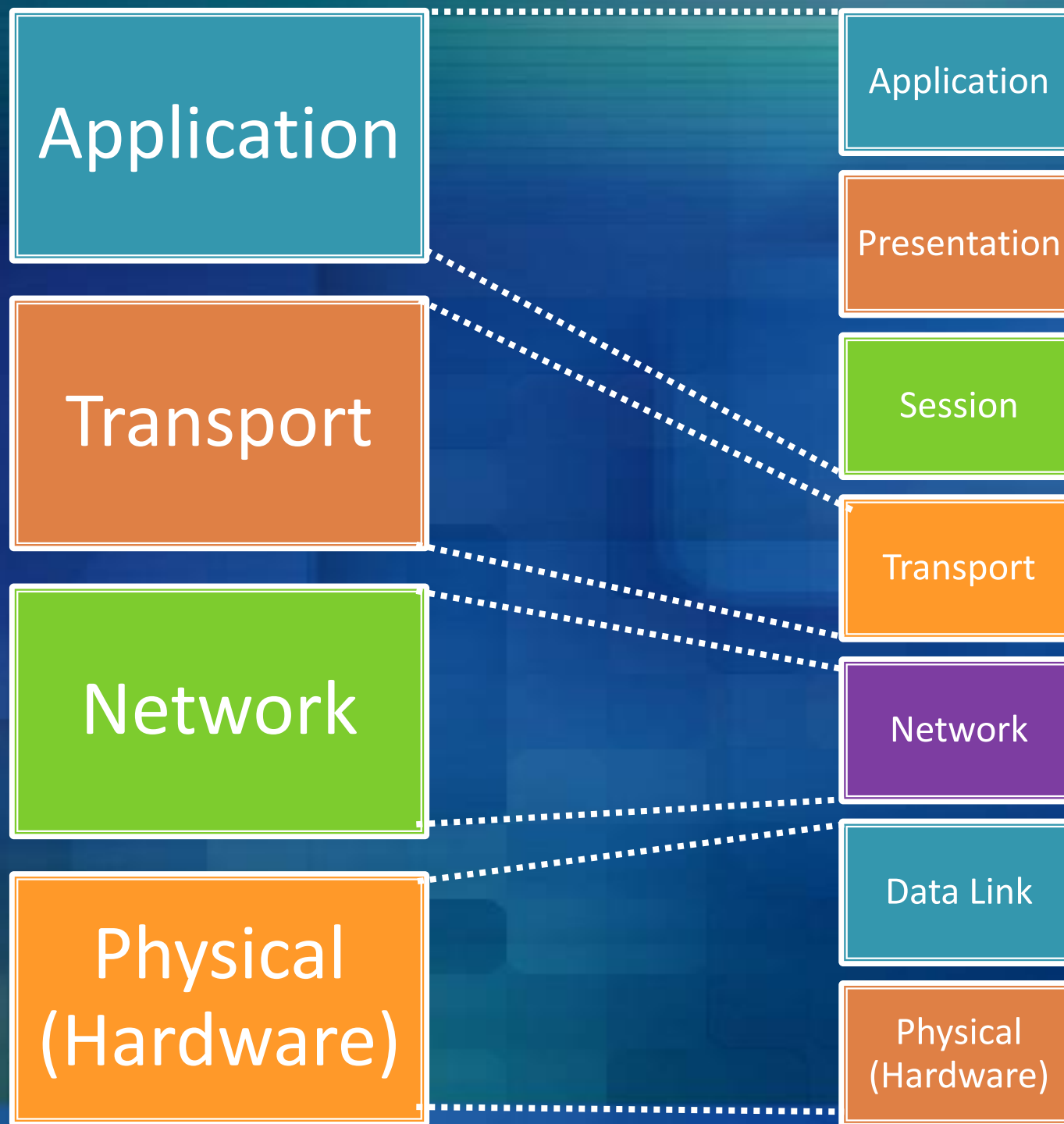
Protocol Stacks

- The protocol stack used by every computer on the Internet 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 the applications assemble and make sense of newly arrived packets.

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 | 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…. |

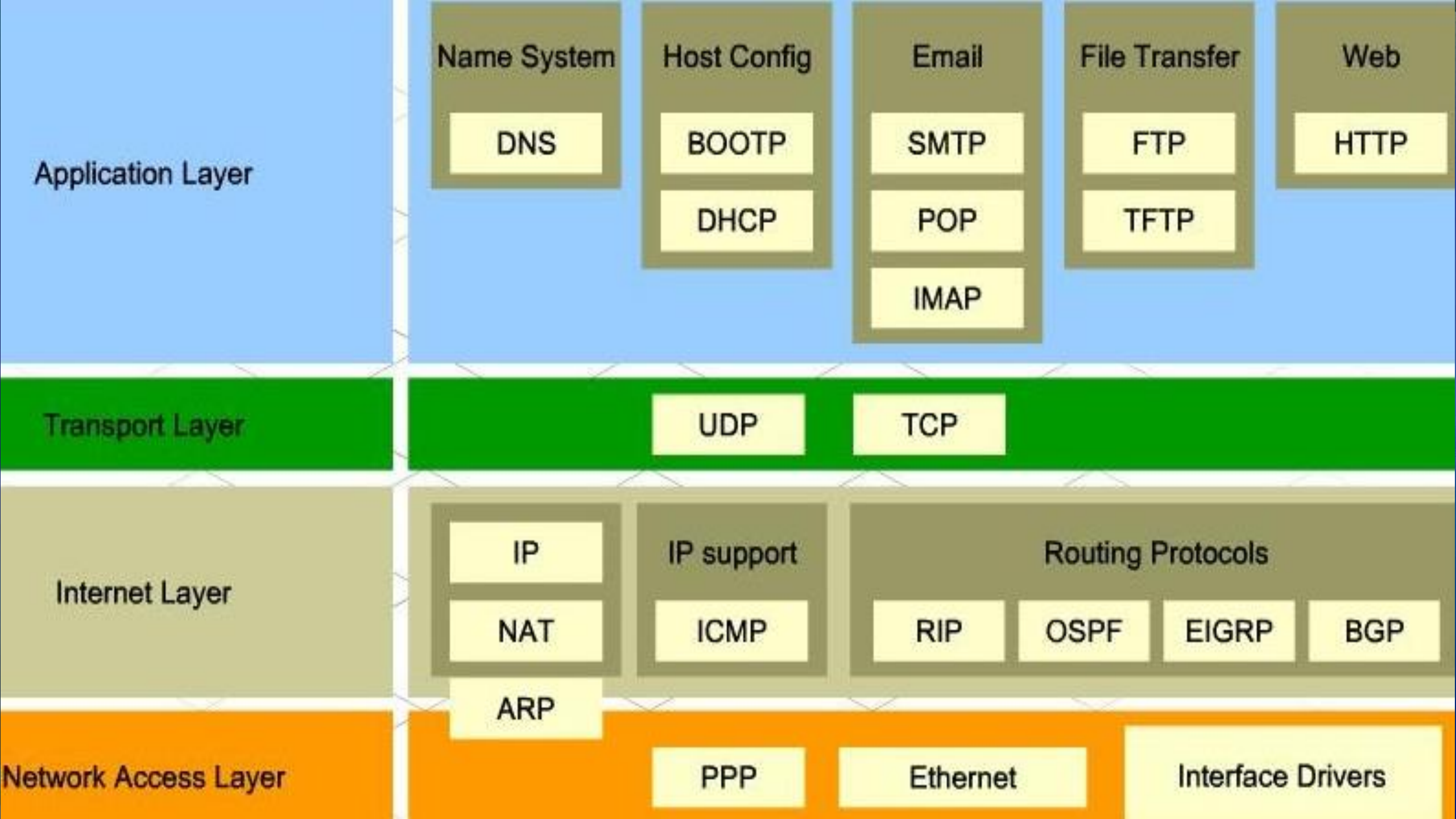Data Flow of the Internet Protocol Suite
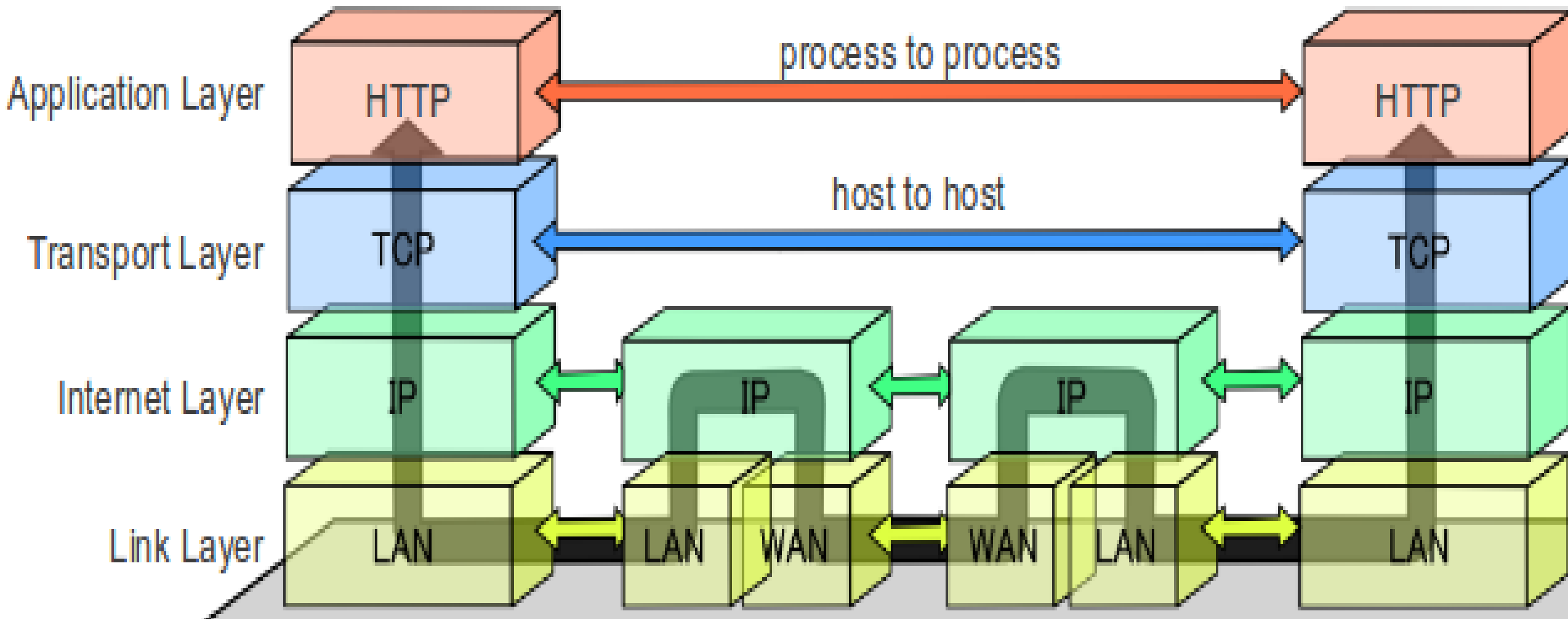
Protocol Stacks

- When an applications whishes to send a message over the Internet it hands the message down the protocol stack. Each protocol within the stack has some task.

- 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 IP layer takes care of steering these packets.

- The Hardware physical transmits packets (frames).

The Transport Layer

- The Transport layer, using the Transmission Control Protocol (TCP) takes care of breaking application information in to chunks, known as "packets" and assigning those packets 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
  - Number of packets sent
  - The number the packet in the series being sent.
  - On the receiving end the TCP protocol helps to <u>arrange packets</u> as they arrive in the correct order for the applications.

Protocol Stacks

- IP is an <u>unreliable</u>, <u>connectionless</u>, <u>packet switched</u> 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".)
- The Transport layer is a <u>connection-oriented</u>, <u>message switched</u>, <u>reliable</u>, byte stream service.
  - Connection-oriented means that two applications using TCP must first establish a connection before exchanging data (a handshake).
  - TCP is reliable because for each packet received, an acknowledgement is sent to the sender.
  - A cousin of TCP, User Datagram Protocol (UDP) is commonly used for streaming. A connectionless, unreliable protocol

Application Layer	Name System	Host Config	Email	File Transfer	Web
	DNS	BOOTP	SMTP	FTP	HTTP
		DHCP	POP	TFTP	
			IMAP		

Transport Layer   UDP   TCP

Internet Layer	IP	IP support	Routing Protocols			
	NAT	ICMP	RIP	OSPF	EIGRP	BGP
	ARP					

Network Access Layer   PPP   Ethernet   Interface Drivers

Packet Routing at the IP 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.

TCP/IP Packet

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol=6 (TCP)	Header Checksum	
Source Address				
Destination Address				
Options				Padding
Source Port			Destination Port	
Sequence Number				
Acknowledgement Number				

IP Header

TCP

| Data Offset		U R G	A C K	P S H	R S T	S Y N	F I N	Window	
Checksum								Urgent Pointer	
TCP Options									Padding
TCP Data									

Protocol Stacks

- Each layer places its information in the "packet header".
  - This is information needed to deliver and re-order the packet once it has arrived to its destination.

IP Header	Transport Header	Packet Data

← 20 Bytes → ← 20 Bytes →

Local Area Networks

- 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.
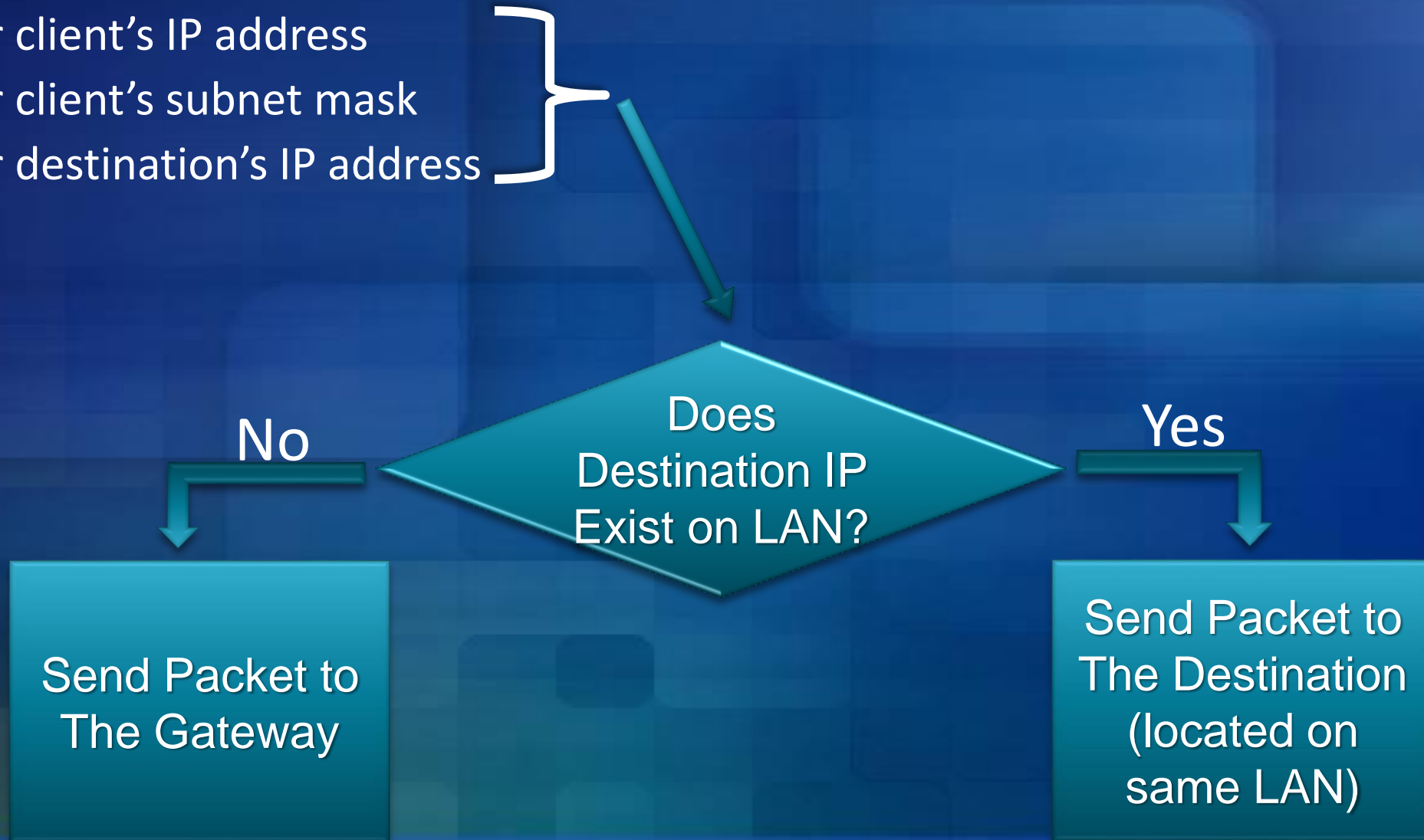

LAN
(Local Area Network)
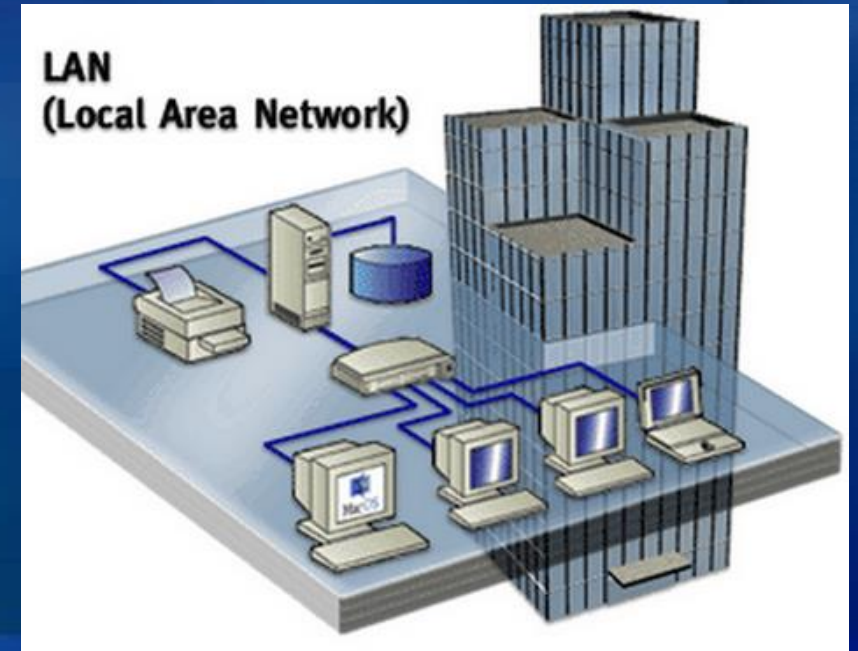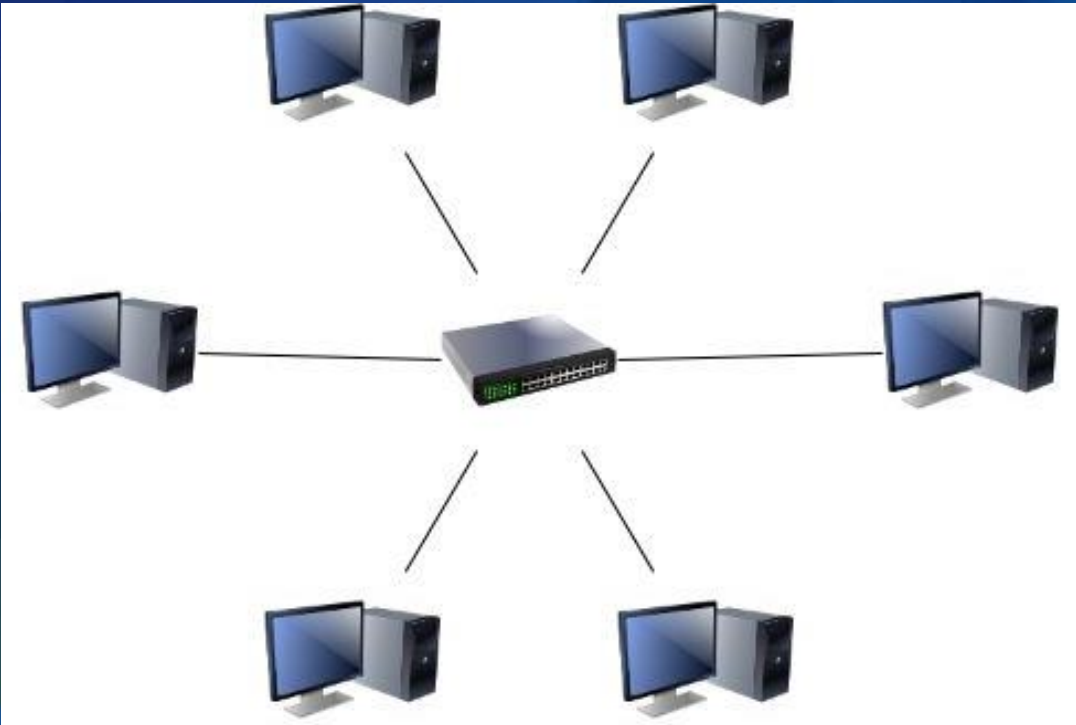
IP Client Information

- For the IP layer to route packets correctly, a device must be configured with:
  - IP address: Every IP address on the internet is unique*. An address takes the form of:
    - 4 x 8 bit (32 bit) numbers represented in decimal notation separated by '.'s. For example 128.205.34.66. – IPV4
    - 8 x 16 bit (128 bit) alphanumeric addresses in decimal notation separated by '.'s. For example 2001:0000:3238:DFE1:63:0000:0000:FEFB – IPV6
    - IP addresses (To and From) are placed in packet headers, similar to how one would label an envelop.
  - Subnet Mask – used to determine the boundaries of a Local Area Network (LAN).
    - A subnet mask resembles an IP address. Ex 255.255.255.0
  - Gateway IP Address – where packets destined for outside our LAN are handed off.

* -some IP ranges are designated as internal ranges and are repeatable

The Flow of Internet Data

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

Does Destination IP Exist on LAN?

No → **Send Packet to The Gateway**

Yes → **Send Packet to The Destination (located on same LAN)**

The Flow of Internet Data

- 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 <u>Firewall</u> and <u>Monitoring</u> measures.
- Routers maintain multiple connections to one another.
- 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.

Wide Area Networks

LANs are connected together to form WANs

- LANs get connected to WANs through routers.
- 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.

Network Segmentation

- **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
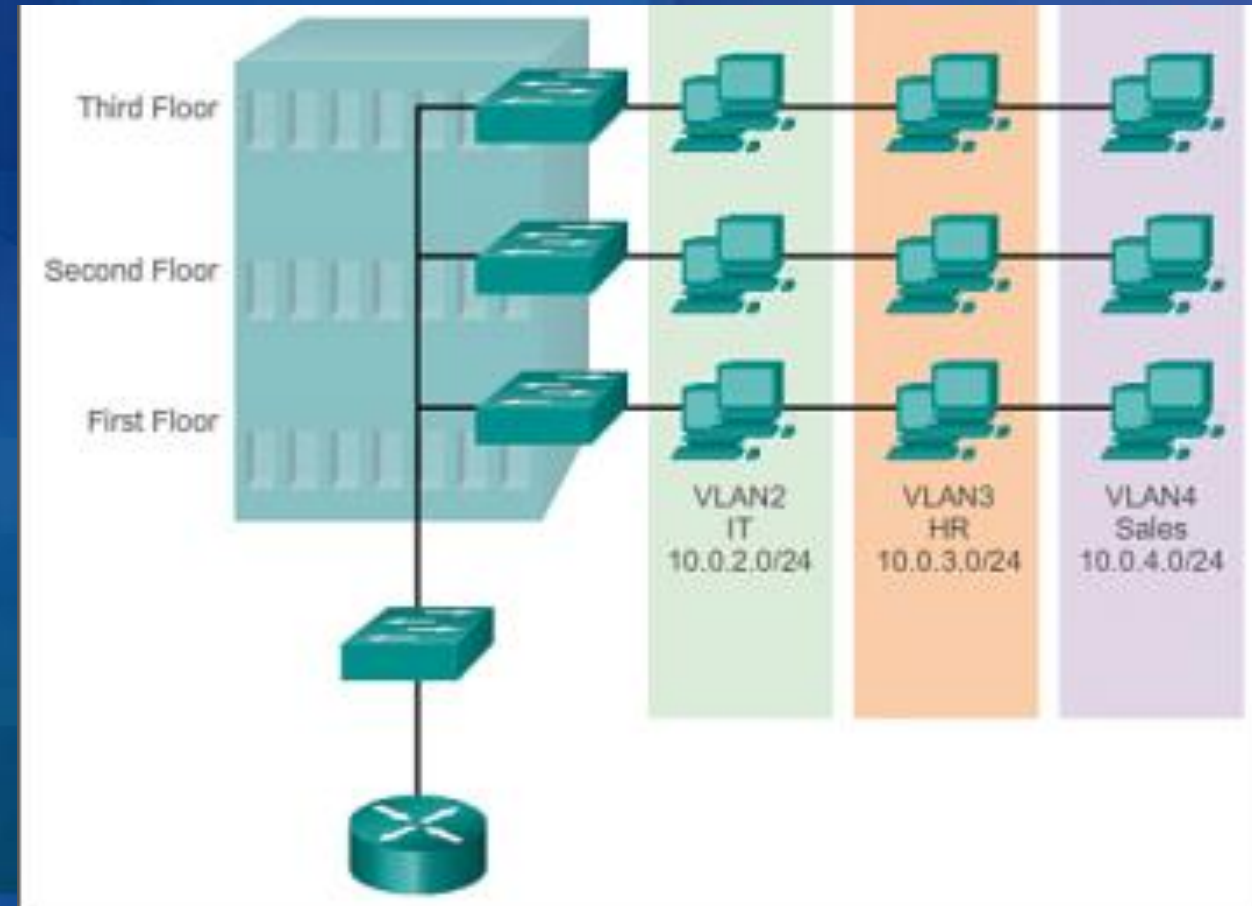
Network Segmentation

- Demilitarized Zone (DMZ) - a perimeter network or screened subnetwork
  - A separate network for services that may require less restive access and firewall rules.
  - Exposes an organization's external-facing services to an untrusted network, such as the Internet.
  - This provides an additional layer of security to the LAN as it restricts the ability of hackers to directly access internal servers and data via the internet.
- Multiple DMZ networks should exist, based on access needs
- Enterprise services should be placed on separate subnetworks based on type of service and need for access.

Local Area Network

Wide Area Network WAN
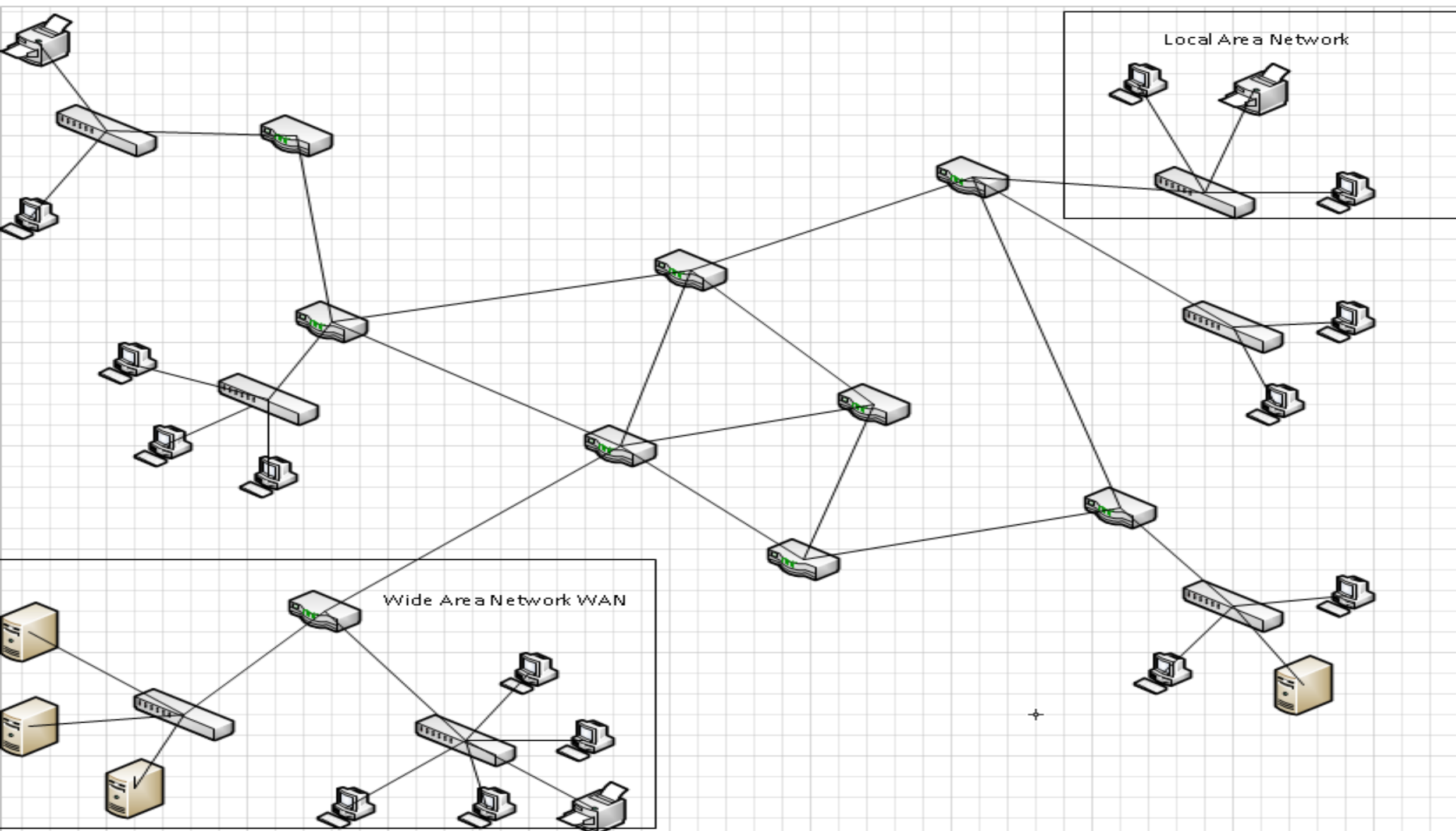
The Hardware Layer

- The "hardware" layer (sometimes called the "Link Layer") of the internet is in charge of transmitting data over a physical medium.

- The physical medium for transmitting data can take on many forms and is implemented with a wide variety of technologies, both wired and wireless.

The Hardware Layer

- All machines have a hardware address called a "MAC" address, or "Media Access Control Address".
  - address is hardcoded on the network interface card (NIC) and usually* cannot be changed.
  - MAC address is used when delivering messages within subnet.
- 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 <u>on your own subnet</u>.
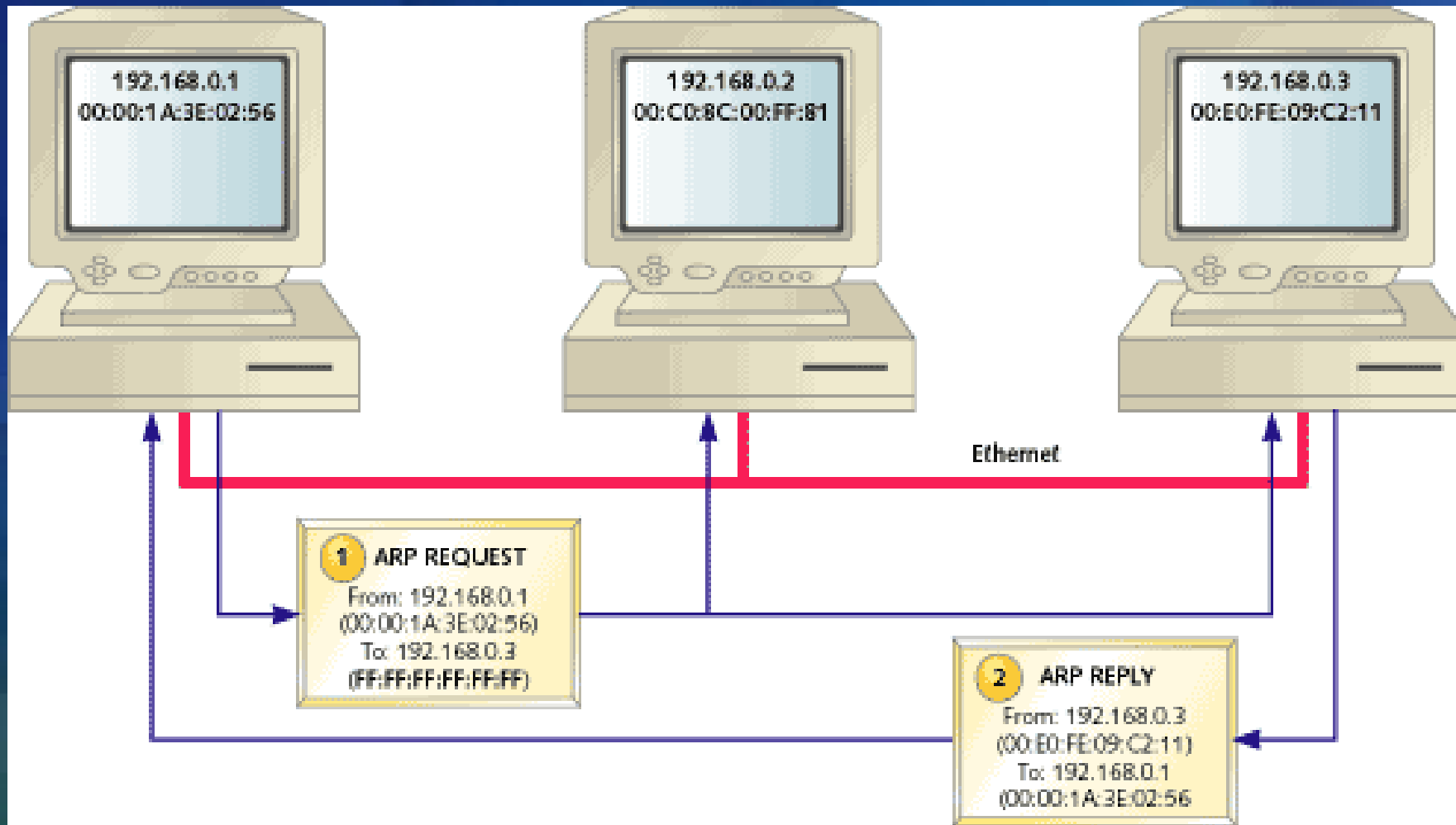
Connecting It All

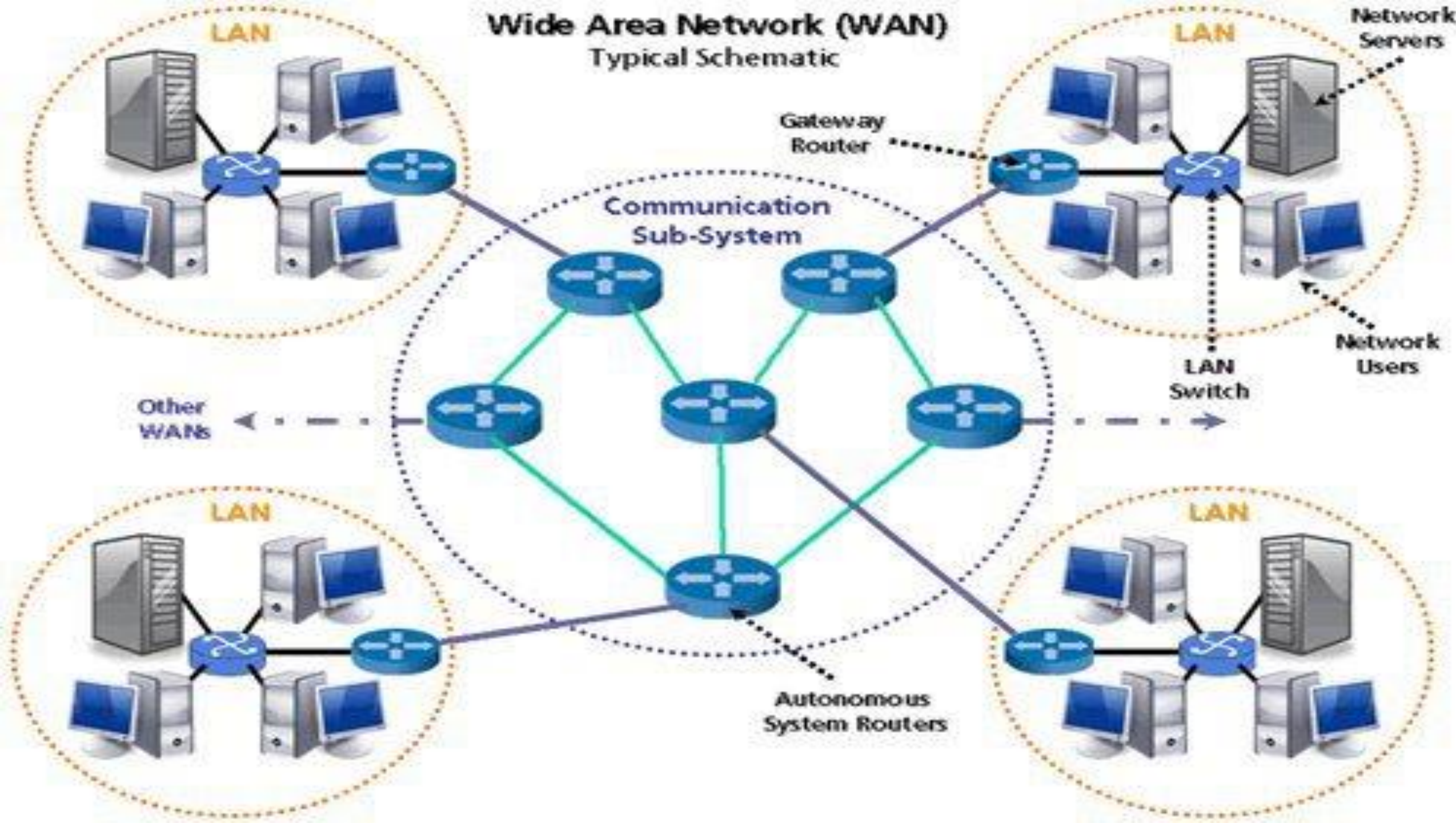|	LANs	WANs
Wired	Ethernet (NICs and Switches) • 1 GB/S • 10GB/S	Modem DSL/ISDN Cable Fiber Optic
Wireless	Wifi (802.11 B/G/N/AC/AD/AH)	Satellite (Microwaves) 4G (Cell service) Infra-red

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

Connecting to LANs - Ethernet

- Ethernet can be thought of as:
  - Hardware communication devices
  - Topologies of devices being used
- Common Ethernet speeds are
  - 1,000Mb/s (1000Base-T) - gigabit.
  - 1,000Gb/s (10GBase-T) - 10 gigabit.
- Most Ethernet devices such as network interface cards and switches have the ability to negotiate the highest available speed.
- Power over Ethernet (PoE) allows the transmission of power through an Ethernet network cable.   This is useful for things like VOIP phones.
- Can connect using:
  - Copper (RJ45 and SFP+)
  - Fiber

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.

Home Networks

- What are home routers?
  - A Switch?
  - A Gateway?
  - A Firewall?
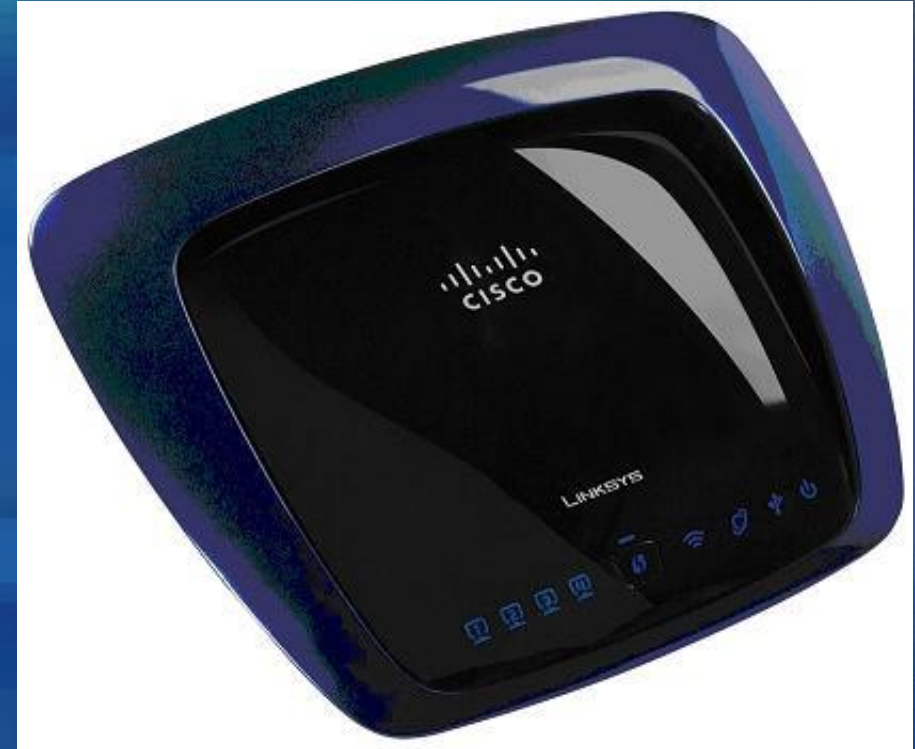 - A Server?
  - A DSL/Cable Modem?

Home Routers

- Most Home Routers will function as a Network Address Translation Firewall (NAT).
  - NAT allows a single device, such as a home router, to act as an agent between the Internet (public network) and a local (private) network.
  - Only a single, unique, IP address is required to represent an entire group of internal or private computers, such as a home network.
  - In a home setup, a NAT firewall allows several home devices to share a single IP provided by an ISP
  - NATs help to hide the internal setup of your network.

Home Networks

Home Routers provide a combination of:

- IP address routing (gateway)
- Network address translation (NAT)
- DHCP functions
- DNS
- Firewall functions
- LAN connectivity like a Network switch
- Modem Functionality
- Some allow you to connect an external USB or E-Sata drive as a means of providing shared storage.

Home Networks

- Home Routers are connected to the internet through an Internet Service Provider (ISP).
  - An ISP provides you a way to connect to their own WAN, providing access to the Internet.
  - An ISP will provide you a modem or home router to connect through their preferred transmission medium.
    - Sometimes these devices must be connected to a local switch to form your own LAN

Home Routers

- Most Home Routers will function as a Network Address translation Firewall, or NAT.