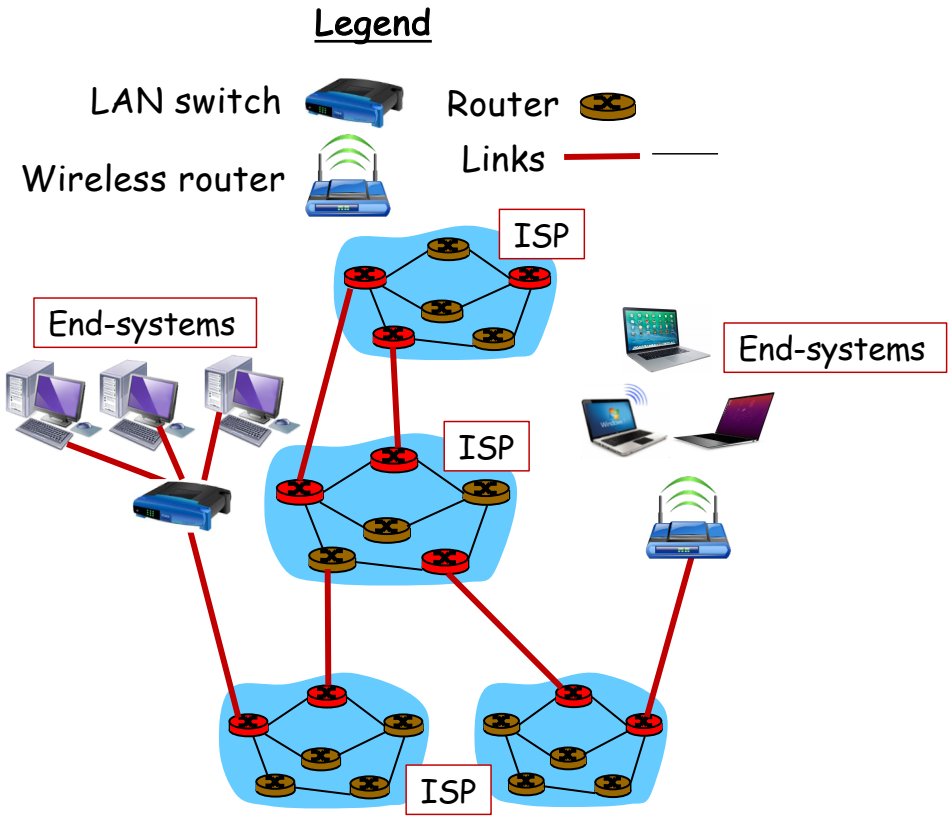
Lecture 1 – Networking Essentials

CPSC-456 Network Security Fundamentals

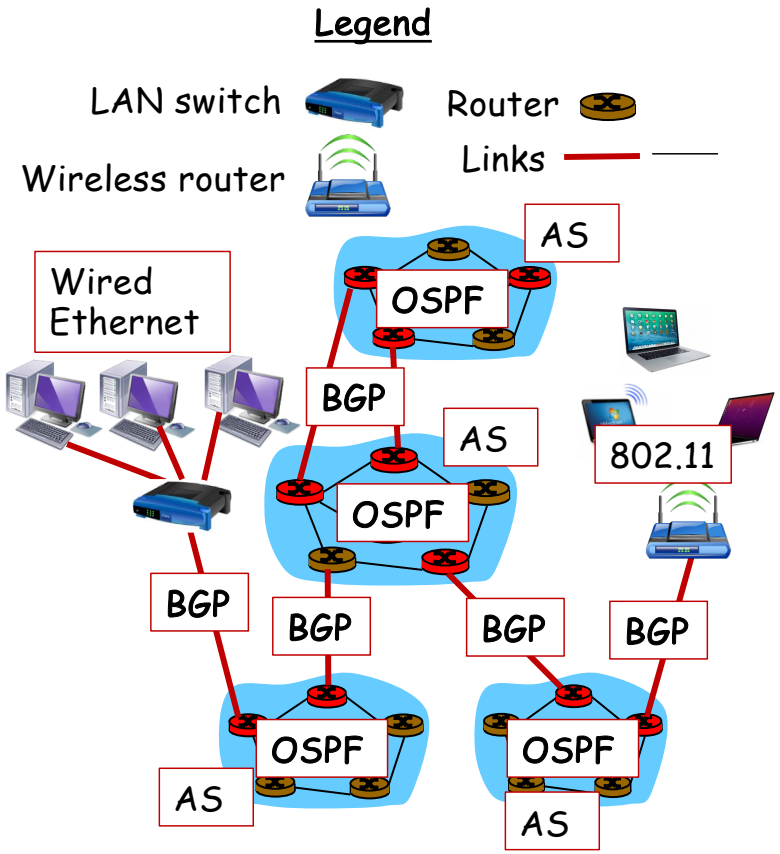
The Internet Infrastructure

- A network of networks.
- Components:
  - Network edge:
    - End-systems (e.g., server, personal computers, etc.) and applications relying on the Internet services.
  - Network Core: networks of routers inter-connecting the end-systems:
    - Internet Service Provider Networks (ISPs): connect end-systems to the Internet.
    - Backbone: networks which route data between ISP networks.
    - Local Area Network (LAN): network interconnecting systems within a limited range e.g., home, school, etc.



Dominant Protocols on the Internet

- Dominant Internet Protocols:
  - Local area networks (LANs):
    - 802.3: Wired Ethernet
    - 802.11: Wireless Ethernet
  - Internet:
    - Domain Name Service (DNS): resolves domain names to IP addresses.
    - Open Shortest Path First (OSPF) protocol: routes traffic within Internet networks a.k.a. Autonomous Systems (ASs).
    - Border Gateway Protocol: routes traffic between autonomous systems.

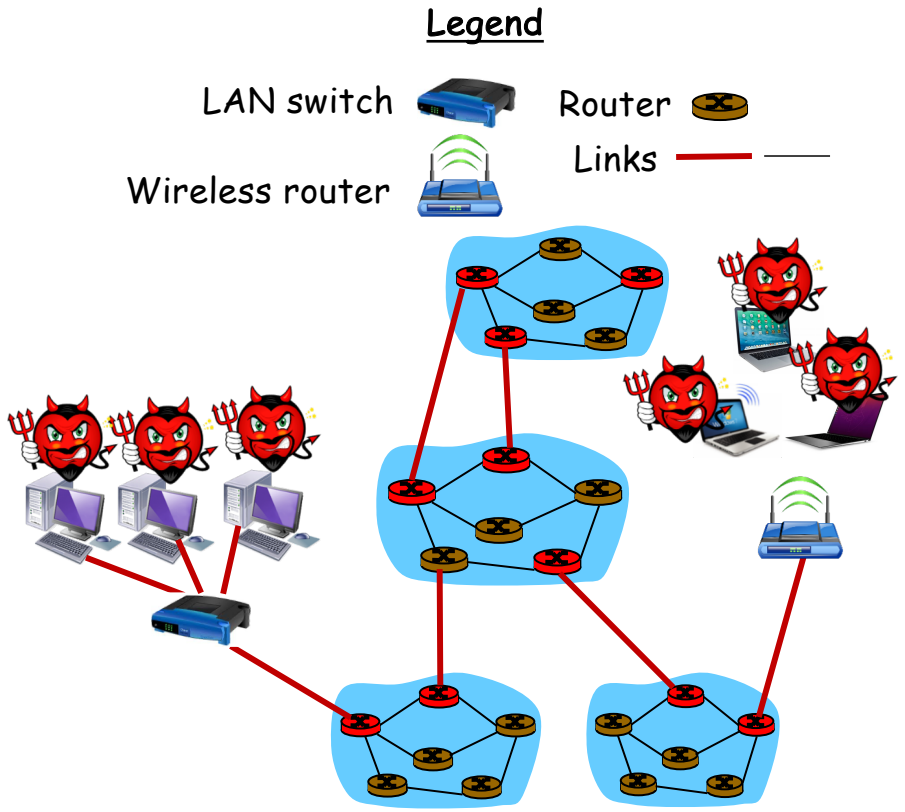


Threat Model for the Internet (1)

- A threat model (definition adapted from owasp.org):
  - A structured representation of all the information that affects the security of an application/system/network.
  - A view of the system and its environment through security glasses.
- Threat model for Internet (Next slide).

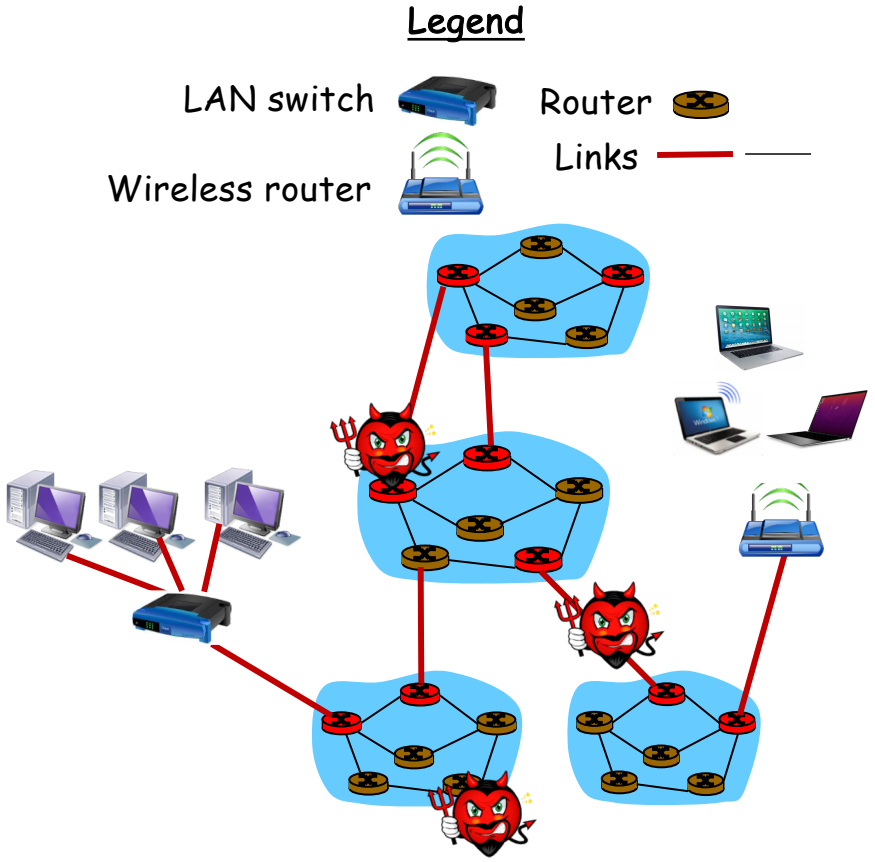
Threat Model for the Internet (2)

- Threats:
  - Malicious end-systems: e.g., systems affected by malware or used by attackers.



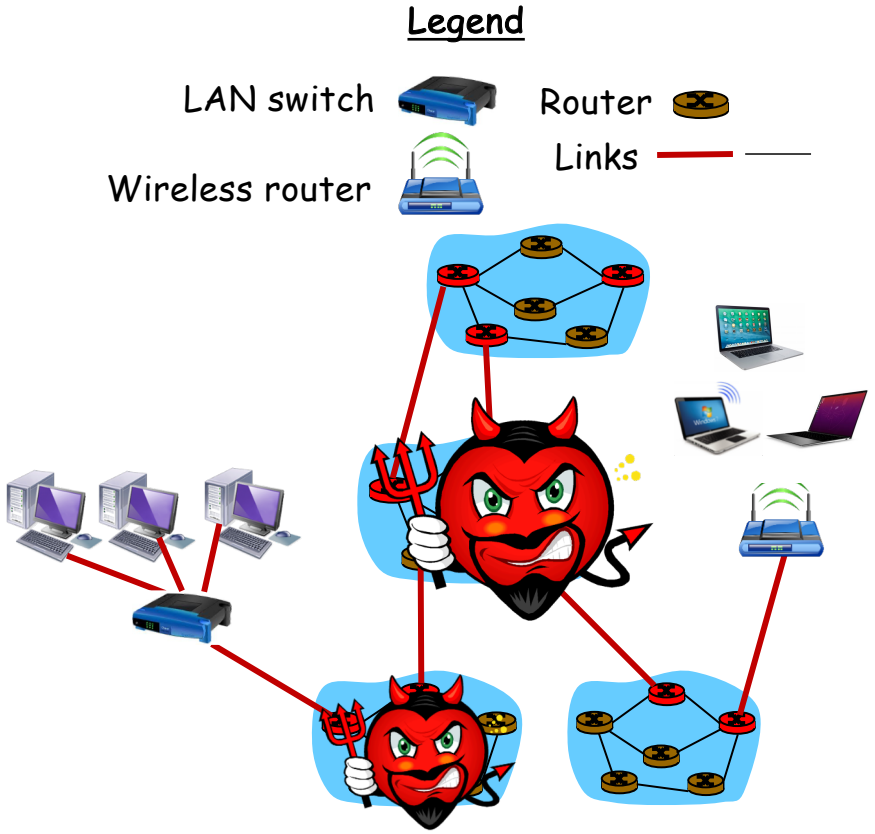
Threat Model for the Internet (3)

- Threats:
  - Compromised routers and Link: tapped link, backdoored routers, etc.



Threat Model for the Internet (4)

- Threats:
  - Malicious ISPs and Backbone Networks.



Overview: What is Networking?

- A network is simply a collection of computers or other hardware devices that are connected, either physically or logically, using special hardware and software that allows the devices to exchange information and cooperate.

- Networking is the process involved in designing, implementing, upgrading, managing, and otherwise working with networks and network technologies.

Overview: Benefits and Cost of Networking

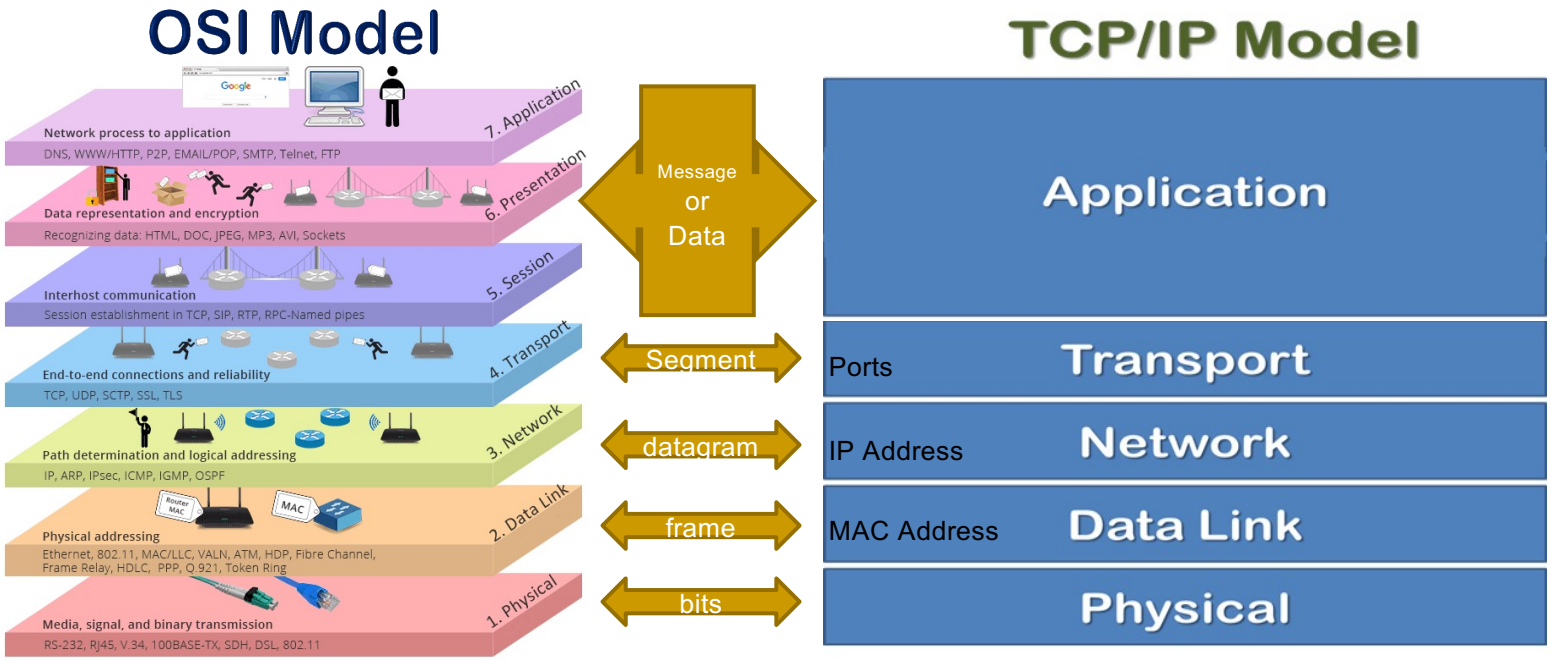
Advantages:

- **Data Sharing**
  - Eliminates *sneakernet* (shoe-based network)
- **Hardware/Internet Access Sharing**
  - e.g., printer, scanner, etc.
  - Special hardware devices allow the bandwidth of the connection to be easily shared among various devices as permitted
- **Data Security and Management**
  - Centralize data on shared servers
- **Performance Enhancement and Balancing**
  - Distribute computational task to various nodes on the network

Disadvantages:

- **Additional Overhead Cost**
  - Requires additional network device(s) and software configuration
  - Administration cost for maintenance and management
- **Undesirable Sharing**
  - Malware can also be transferred within the network
- **Data Security Concerns**
  - Poorly secured network can put data at risk and expose to other potential problems such as unauthorized access and even hold hostage

Conceptual View of OSI and TCP/IP Models

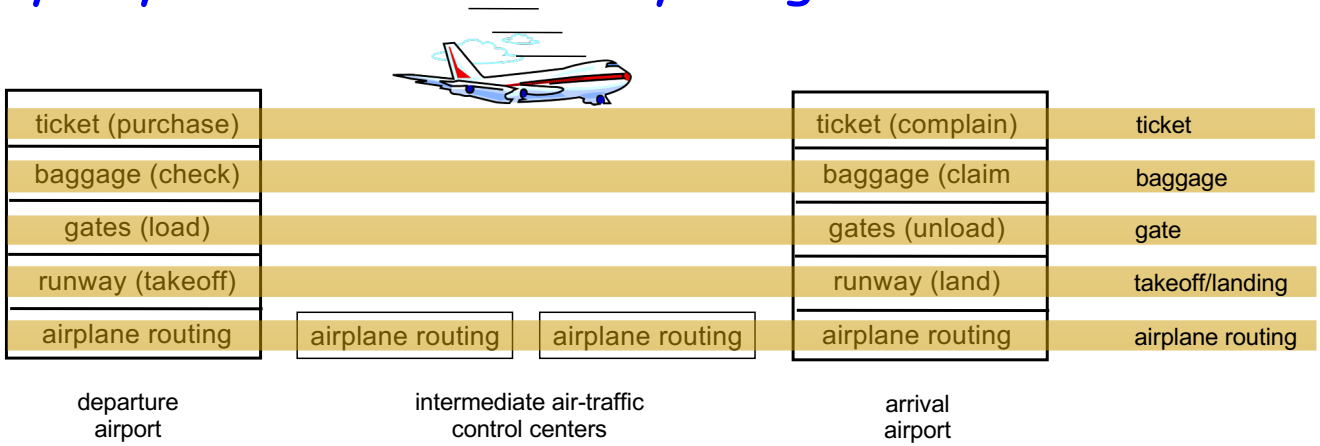


Why is this useful to understand such frameworks?

It can help troubleshoot an application/protocol(s)/network configuration (path), particularly when there are no errors involved, but the expected behavior is not achieved.

Image source: https://community.fs.com/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html

Why Layer? Motivation: Layering of Airline Services



Layers: each layer implements a service

- Via its own internal-layer actions
- Relying on services provided by layer below

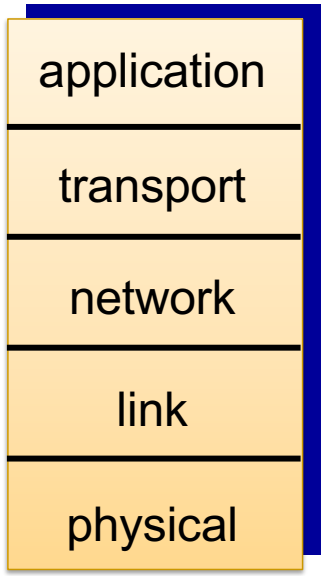
- Layering of services *helps modularize system design* e.g., can change implementation of one layer without affecting implementation of other layers:
  - E.g., in the airline example, we can change the ticketing service without affecting other services.

Why Layer? Motivation: Layering of Network Protocols

- Dealing with complex systems:
  - Explicit structure allows identification, relationship of complex system's pieces
    - layered *reference model* for discussion
  - Modularization eases maintenance, updating of system:
    - Change of implementation of layer's service transparent to rest of system
    - e.g., Change in gate procedure doesn't affect rest of system
    - Example: network application developers can develop applications without worrying about how the data is routed, the types of links used on the network, etc.

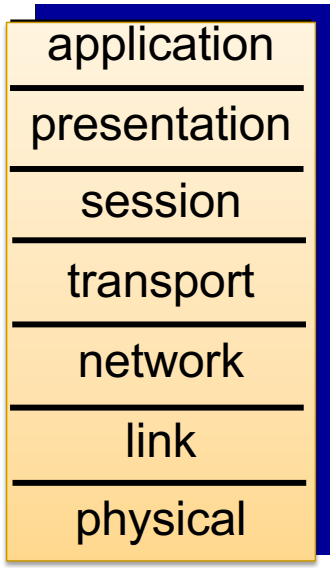
Network Model: The TCP/IP Layered Stack

- *Used on the Internet. Comprises of the following layers:*
  - *Application:* supporting network applications
    - FTP, SMTP, HTTP(S)
  - *Transport:* process-process data transfer
    - TCP, UDP
  - *Network:* routing of datagrams from source to destination
    - IP, routing protocols
  - *Link:* data transfer between neighboring network elements
    - Ethernet, 802.11 (WiFi), PPP
  - *Physical:* bits "on the wire"



Network Model: The OSI Layered Stack

- *Extends the TCP/IP Stack with the two more layers:*
  - *presentation:* allow applications to interpret meaning of data, e.g., encryption, compression, machine-specific conventions
  - *session:* synchronization, checkpointing, recovery of data exchange
- TCP/IP stack is "missing" these layers:
  - In TCP/IP stack, if the application needs the services of these missing layers, it is up to the application developer to implement these services in his/her application.



Networking Standards: Layer 1 Devices

Ethernet Hub

- Also sometimes referred to as **repeater**
- Collision domain (CSMA/CD)
- One-way traffic (half-duplex)
- No knowledge of addresses

Ethernet Repeater

- Layer 1 device
- Also called signal **extender**
- Extend signal attenuation limit of a given media

Network Interface Card

- Wireless/wired network interface

Network Standards: Types of Network

Local Area Network (LAN)

- Network of computers connected relatively close together, i.e., room or building

Campus Area Network (CAN)

- Like LAN, but spans multiple buildings in the same location

Wide Area Network (WAN)

- Network that connects devices or other networks over a greater distance than LANs
- Distance between devices can be measure in miles.

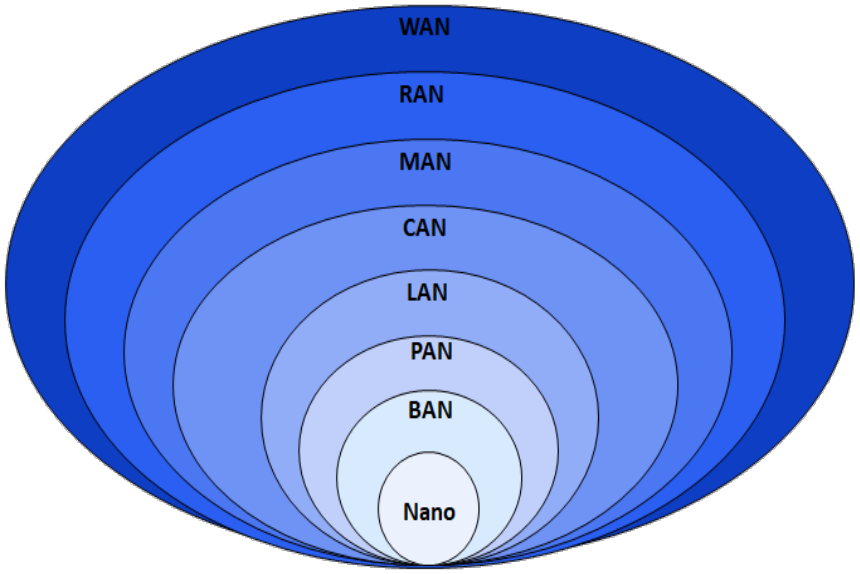


Image source: https://en.wikipedia.org/wiki/Computer_network

Networking Standards: Layer 2 Devices

Ethernet Switch

- Layer 2 device like a Bridge
- Also referred to as a smart hub
- Learns MAC addresses to forward network traffic to a given port
- Allows simultaneous communication between connected devices (full duplex

Ethernet Bridge

- Segment a network into multiple collision domains
- Replaced by switches

Bridge

Wireless Bridge

- Layer 2 device

Networking Standards: Layer 3 Devices

Ethernet Router

- Sometimes referred to as **gateway**
- Forwards traffic to another network until it reaches the destination network

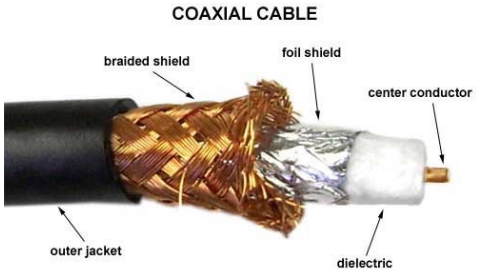
Router Firewall

- Works as a packet filter router
- Forwards traffic to another network until it reaches the destination network
- Allow or deny incoming or outgoing traffic

Networking Standards: Medium

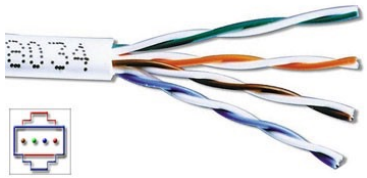
802.3 Wired Ethernet

- Copper
  - Twisted-pair (STP and UTP)
  - Coaxial
- Fiber optic



Shielded twisted pair (STP)

Unshielded twisted pair (UTP)



802.11 Wireless Ethernet (WLAN)

- Radio

Image sources: https://medium.com/the-cabin-coder/lesson-3-topology-and-cables-f93fa0f01031; https://www.microsoft.com/en-us/p/wifi-explore-speedtest-wifi-scan/9nmzl3wg81wb?activetab=pivot:overviewtab

Networking Standards: Medium

Common Name	Speed	Alternative Name	Name of IEEE Standard	Cable Type, Maximum Length
Ethernet	10Mbps	10BASE-T	802.3	Copper, 100 m
Fast Ethernet	100Mbps	100BASE-TX	802.3u	Copper, 100 m
Gigabit Ethernet	1000Mbps	1000BASE-LX	802.3z	Fiber, 550 m
Gigabit Ethernet	1000Mbps	1000BASE-T	802.3ab	Copper, 100 m
10GigE (Gigabit Ethernet)	10Gbps	10GBASE-T	802.3an	Copper, 100 m

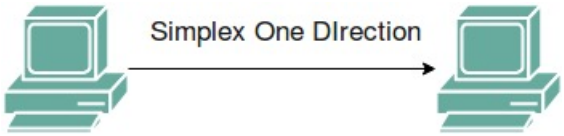
Image sources: http://ptgmedia.pearsoncmg.com/imprint_downloads/informit/learninglabs/9780134213736/ch29.html

Networking Standards: Transmission Modes

Simplex

- One-way communication

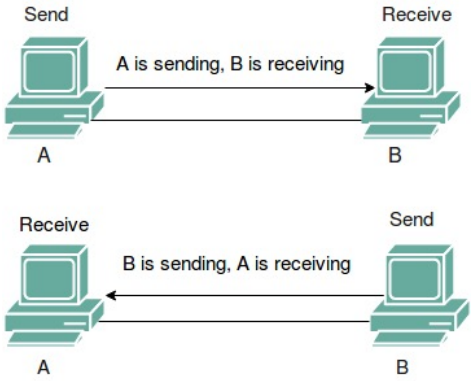
e.g., Airports Flight Information Display Systems (FIDS), campus information display units



Half-Duplex

- Two-way communication, but not at the same time

e.g., hubs, walkie-talkie



Full-Duplex

- Two-way communication at the same time

e.g., bridges, switches, routers, cell phone, etc.

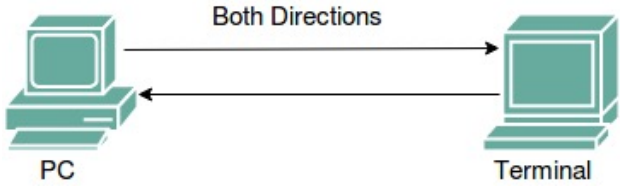
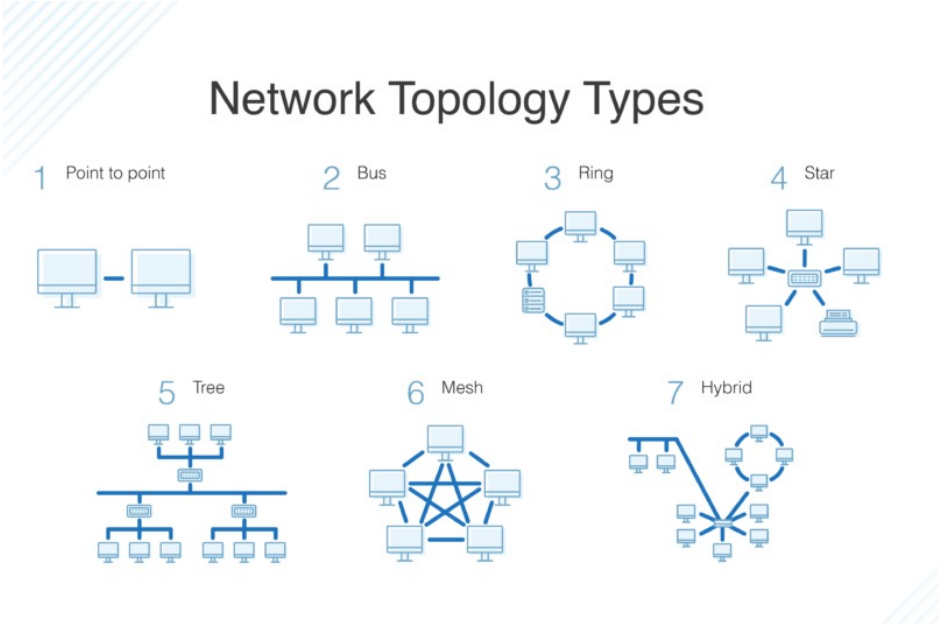


Image sources:https://www.geeksforgeeks.org/transmission-modes-computer-networks/

Network Topologies: How They Are Put/Work Together

A Network Topology refers to how various nodes, devices, and their connections on your network are *physically* or *logically* arranged in relation to each other.



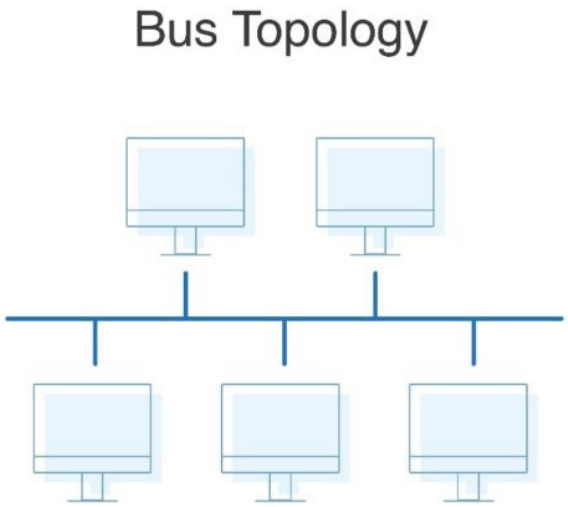
source: https://www.dnsstuff.com/what-is-network-topology

Network Topologies: Bus

A bus topology connects all the devices on a single shared channel. It is sometimes called a "line or backbone topology."

A node typically contends with other nodes before it can send data to the network.

- Simple & cost-effective for small networks
- If shared channel fails, it brings down the entire network
- Only one node can send at any given time (Half-duplex)
- Not ideal for high volume network traffic

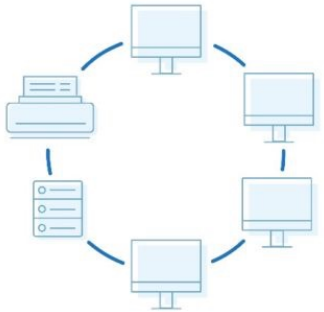


source: https://www.dnsstuff.com/what-is-network-topology

Network Topologies: Ring

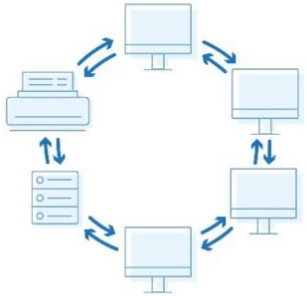
A ring topology connects all the devices in a circle (or ring). Typically, a token is used to pick which node gets to start sending data.

Ring Topology



The data can travel through the ring network in either one direction (single-ring) or both directions (dual-ring), with each device having exactly two neighbors.

Dual Ring Topology

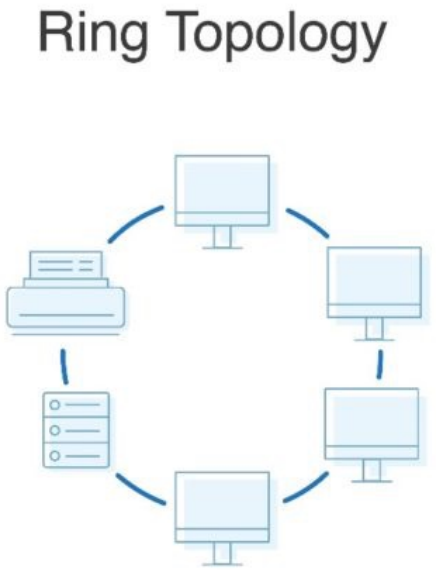


source: https://www.dnsstuff.com/what-is-network-topology

Network Topologies: Ring

- No packet collision: Data is passed from an adjacent node to the other neighbor node in a circular fashion until it reaches its destination.
- Easy node configuration

- Like the bus topology, only one node can send data at a time
- Failure of one node can bring down the entire network
- Failure in one connection will bring down the network
- Must interrupt the network to a add/remove network device

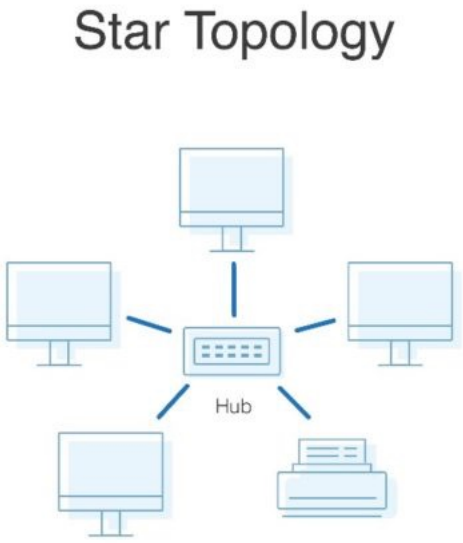


source: https://www.dnsstuff.com/what-is-network-topology

Network Topologies: Star

A star topology is the *most* common network topology today. It is laid out so every node in the network is directly connected to a central hub via coaxial, twisted-pair, or fiber-optic cable.

The node at the center manages data transmission as information is sent from any node on the network to pass through the central device to reach its destination.

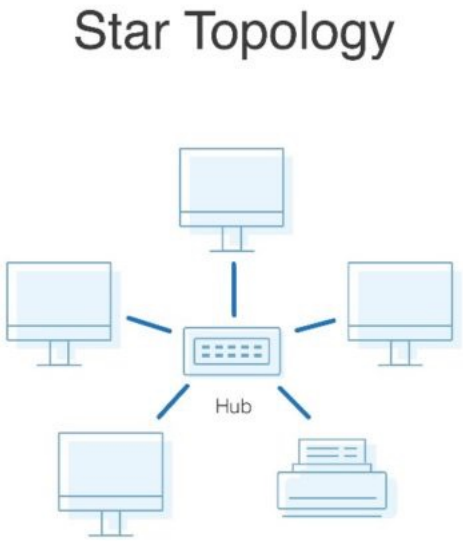


source: https://www.dnsstuff.com/what-is-network-topology

Network Topologies: Star

- Other network devices can be added or removed without interruption to the network operation
- Offers fault-tolerance: If an attached node goes down or a break on its network cable, it does not bring down the entire network
- Cost-effective (less connections needed) compared to other topologies such as Mesh or Full-Mesh

- If the central device goes down, all connected devices will loose connectivity
- Overhead to maintain the central device

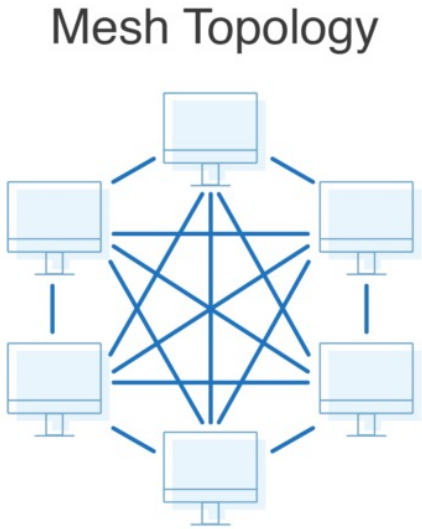


source: https://www.dnsstuff.com/what-is-network-topology

Network Topologies: Mesh

A mesh topology is an intricate and elaborate structure of point-to-point connections where the nodes are interconnected.

Mesh networks can be full or partial mesh. Partial mesh topology is mostly interconnected with a few nodes with only two or three connections. In a full mesh topology is every node is directly connected to the other nodes.

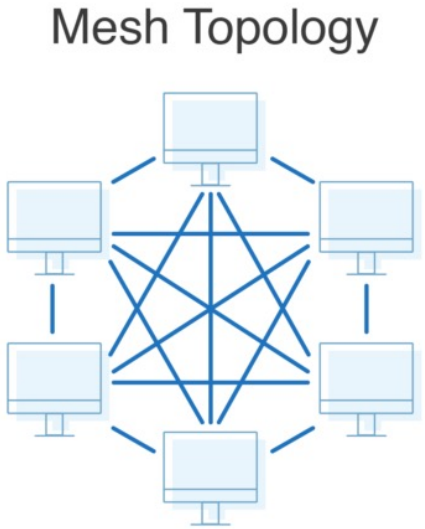


source: https://www.dnsstuff.com/what-is-network-topology

Network Topologies: Mesh

- Provides more fault tolerance when one or more hosts/links fail but will not bring down the network
- Reliable to deliver data to destination in any available path

- Complex layout makes it harder to troubleshoot
- Costs the most of needed resources
- Labor-intensive setup



source: https://www.dnsstuff.com/what-is-network-topology

Network Topologies: How Network Devices Are Used

Router: Bridges two or more networks; Operates on Network layer (L3)

- physical: star topology
- logical: mesh topology

Ethernet Switch: Forward packets to devices within LAN. Operates on Link Layer (L2)

- physical & logical: star topology

Ethernet Hub: Broadcasts packets to all connected device. Operates on Physical Layer (L1)

- physical: star topology
- logical: bus topology

Wireless Access Point (or Bridge): Connects two network segments; Operates on Link Layer (L2)

- physical & logical: star topology