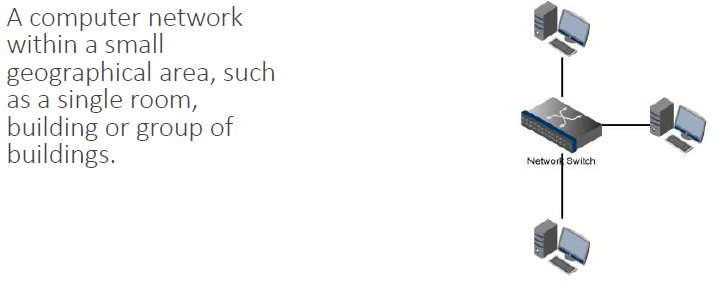
# Client-Server Network

* Network is Composed of Clients and Servers
* Servers Provide Resources
* Clients Receive Resources
* Servers Provided Centralized Control Over Network Resources (files, printers, authentication, etc.)

# Peer-to-Peer Network

* All Computers on the Network Are Peers
* No Dedicated Servers
* There Is No Centralized Control over Shared Resources
* Any Individual Machine Can Share Its Resources as It Pleases
* All Computers on the Network Can Act as Either a Client (Receive Resources) or a Server (Provide Resources)

# Local Area Network (LAN)



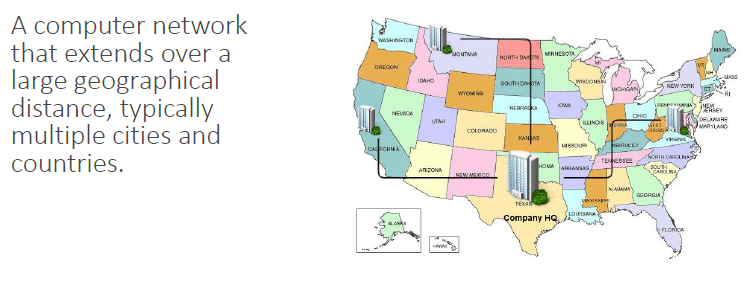
# Campus Area Network (CAN)

# 

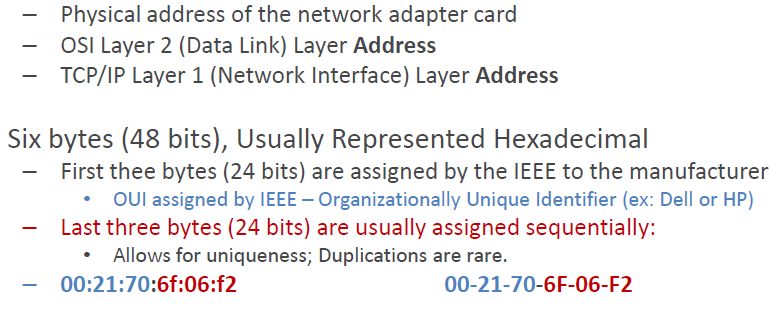
# Metropolitan Area Network (MAN)

# 

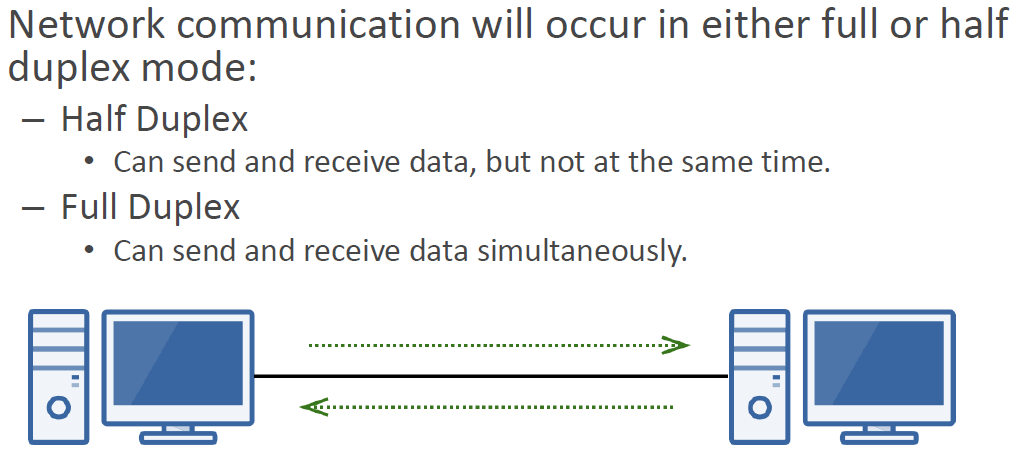
# Wide Area Network (WAN)



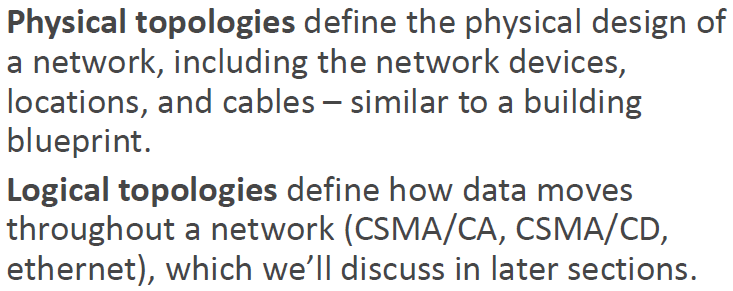
# MAC Addresses



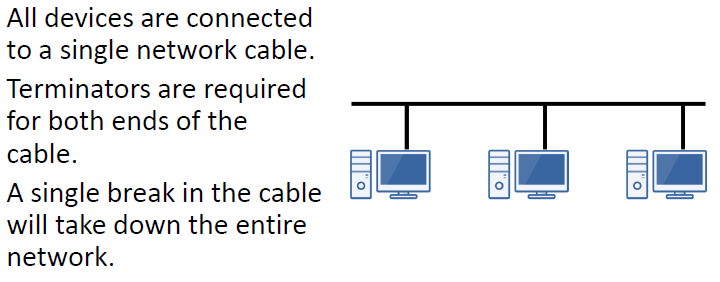
# Duplex Communication



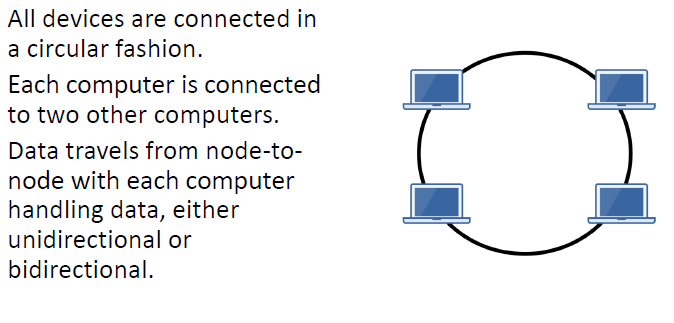
# Physical & Logical Network Topologies



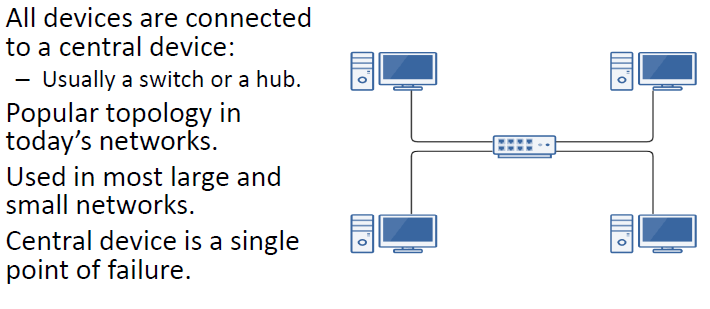
# Bus Topology

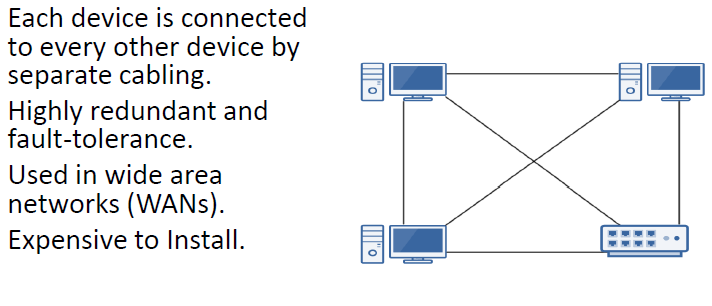


# Ring Topology



# Star Topology

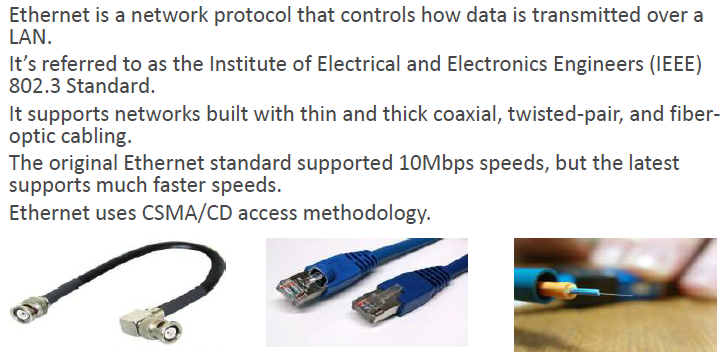


Mesh Topology

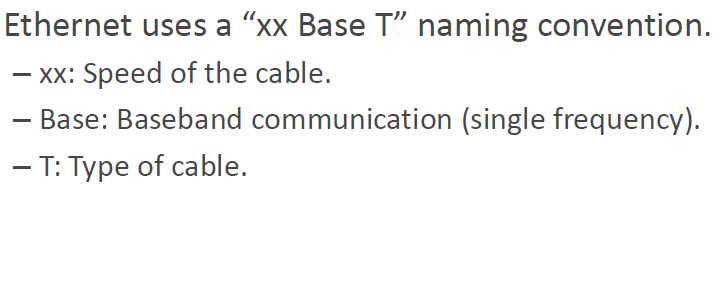
# Types of Network Cabling



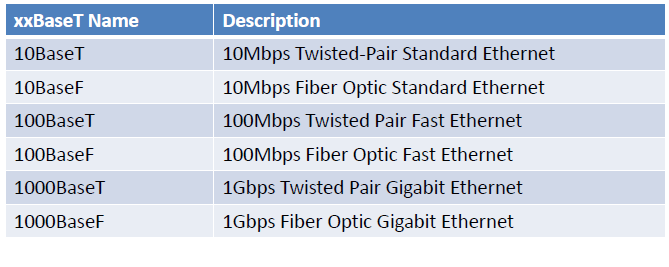
# Ethernet



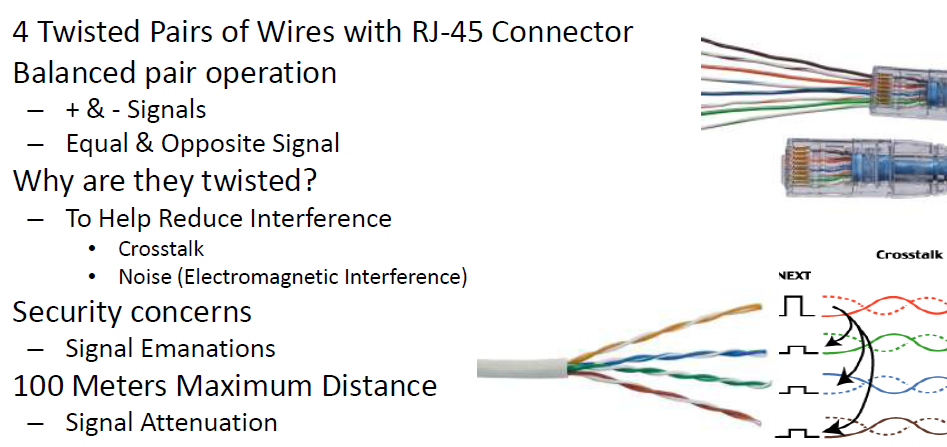
# Ethernet xxBaseT Naming



# Ethernet xxBaseT Naming



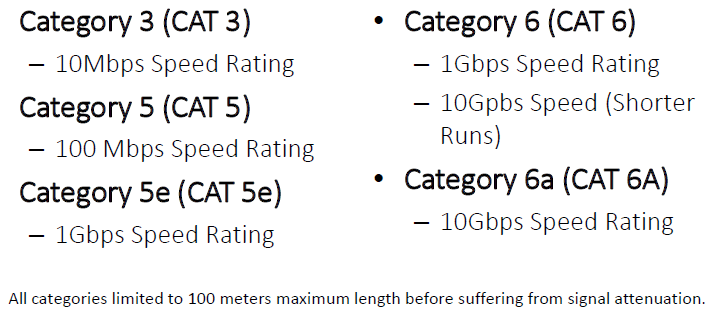
# Twisted Pair Copper Cabling



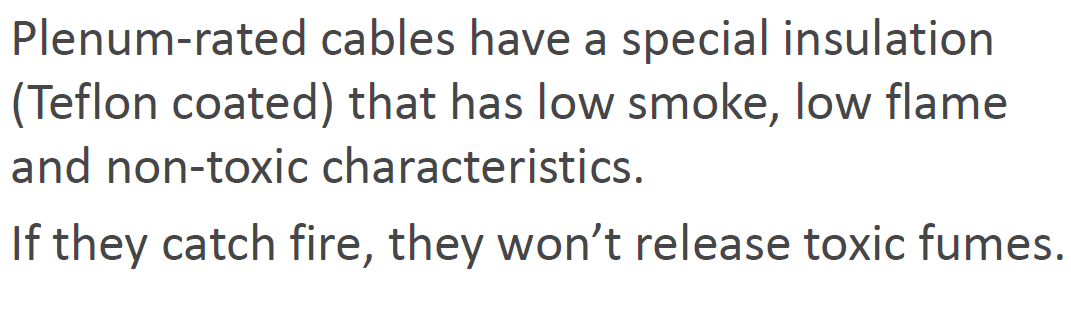
# Shielded vs. Unshielded Twisted Pair

# 

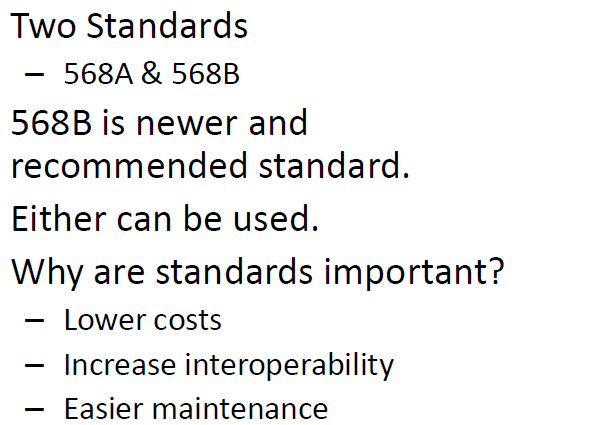
# Twisted Pair Copper Cabling Categories



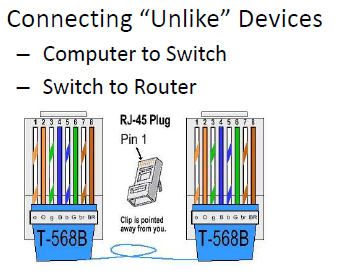
# Plenum-Rated Cable



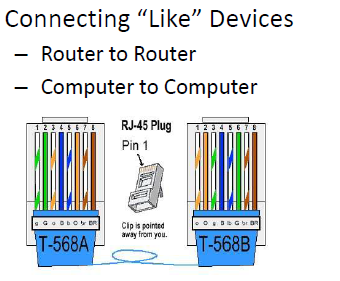
# Twisted Pair Wiring Standards



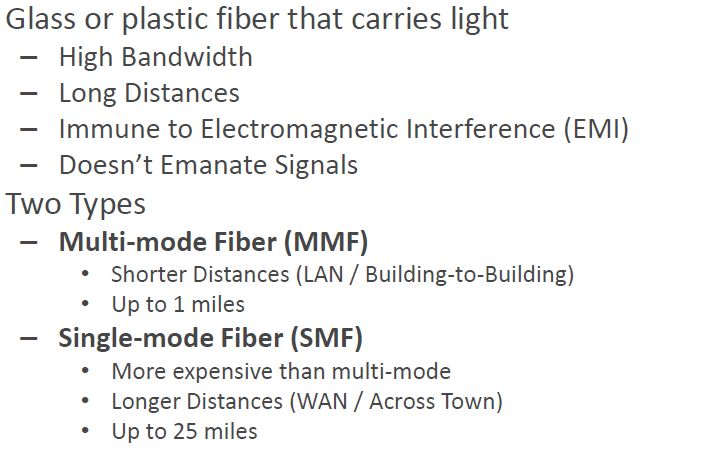
# Straight-Through Cable



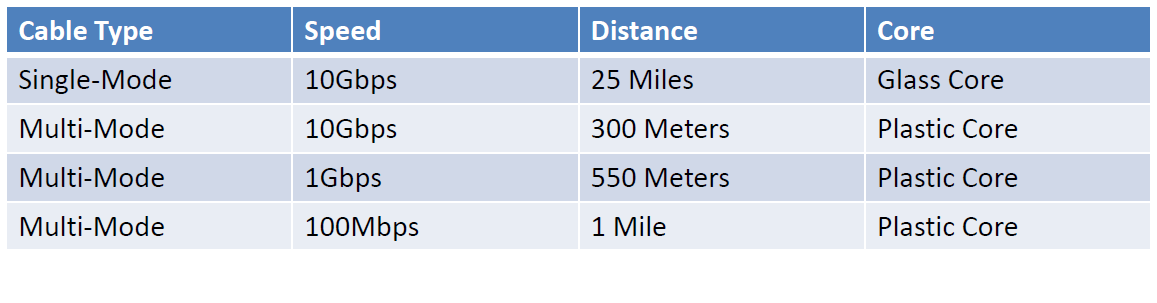
# Crossover Cable



# Fiber Optic Cabling



# Fiber Optic Cable Characteristics



# The OSI Model

# 

# The OSI Model

# 

# OSI Layer 1: Physical Layer

# 

# OSI Layer 2: Data Link Layer

# 

# OSI Layer 3: Network Layer

# 

# OSI Layer 4: Transport Layer

# 

# OSI Layer 5: Session Layer

# 

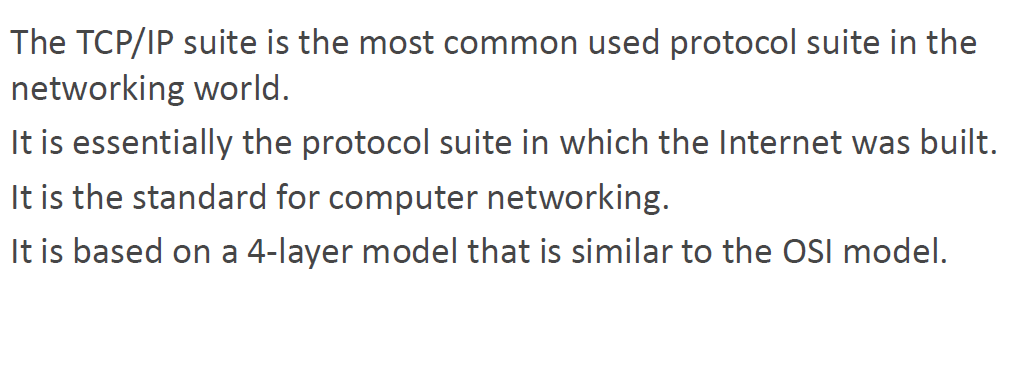
# OSI Layer 6: Presentation Layer

# 

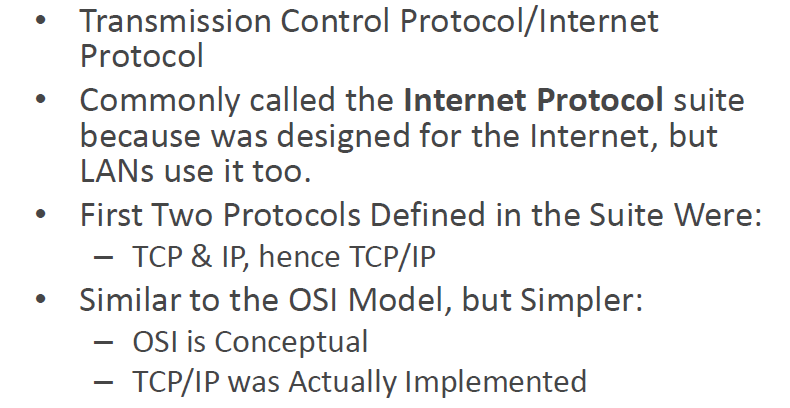
# OSI Layer 7: Application Layer

# 

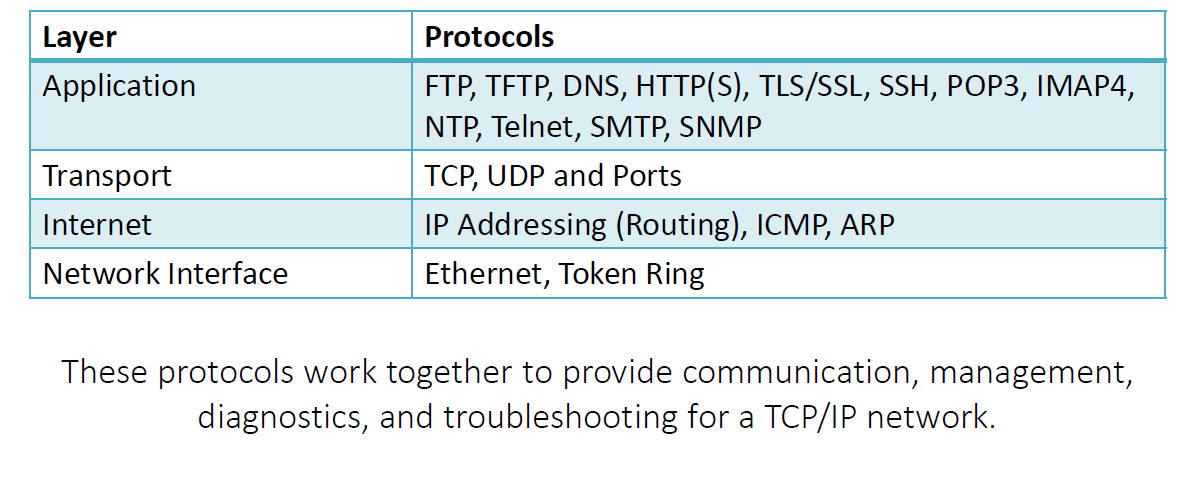
# The TCP/IP Model



# TCP/IP Model



# The TCP/IP Model





# Internet Control Message Protocol (ICMP)

# 

# Address Resolution Protocol (ARP)

# 

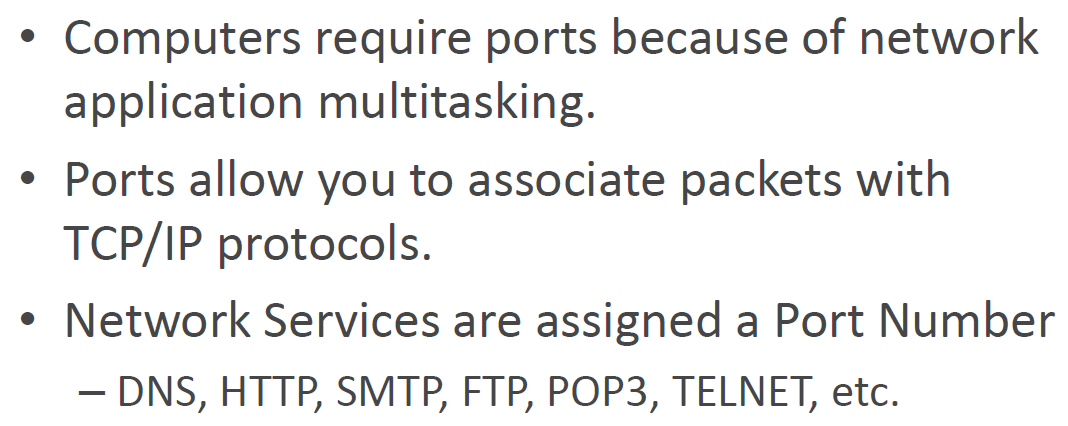
# Transmission Control Protocol (TCP)

# 

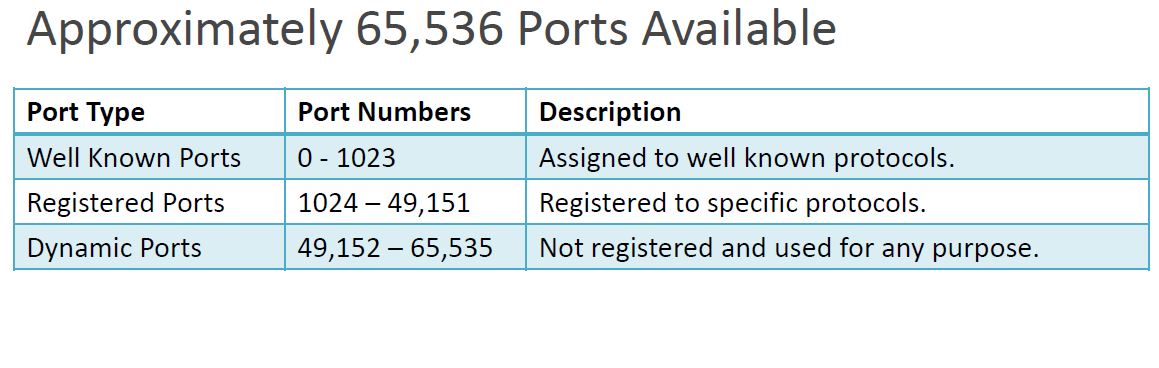
# User Datagram Protocol (UDP)

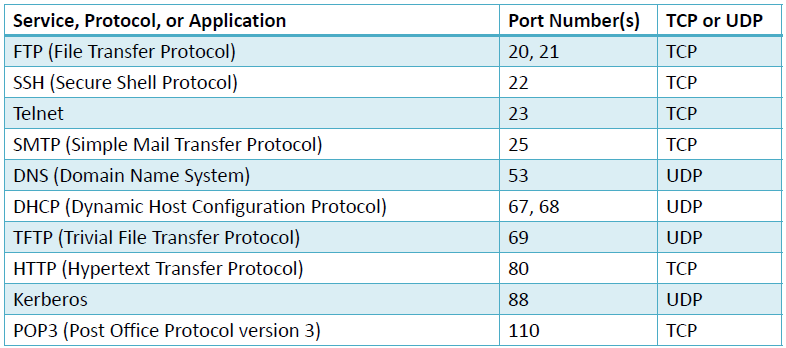
# 

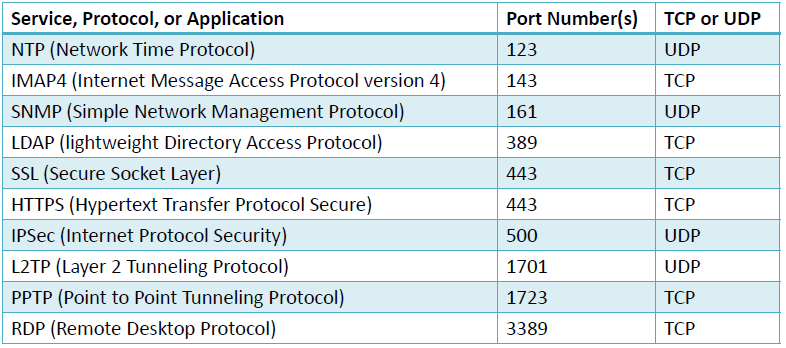
**TCP/UDP Ports**



**Types of Ports**



**Well Known Port Numbers**

**Well Known Port Numbers**

# Ports in Action

# 

# Browser Application Protocols

# 

# File Transfer Application Protocols

# 

# Mail Application Protocols

# 

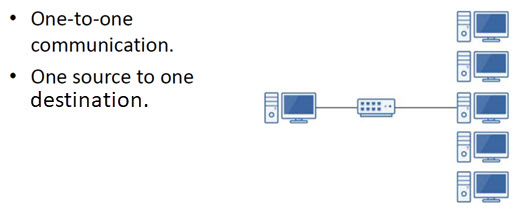
# Management Protocols

* **DNS – Domain Name Services** 
  + Converts domain name to IP addresses
  + Google.com 74.125.224.52
  + NSLOOKUP Command
* **NTP – Network Time Protocol** 
  + Automatically synchronized clocks on network devices
* **SNMP – Simple Network Management Protocol** 
  + SNMP v1, SNMP v2, SNMP v3
  + Collects and manipulates network information
  + Used for network management and maintenance
  + v1 – The original; clear text data
  + v3 – Encrypted data

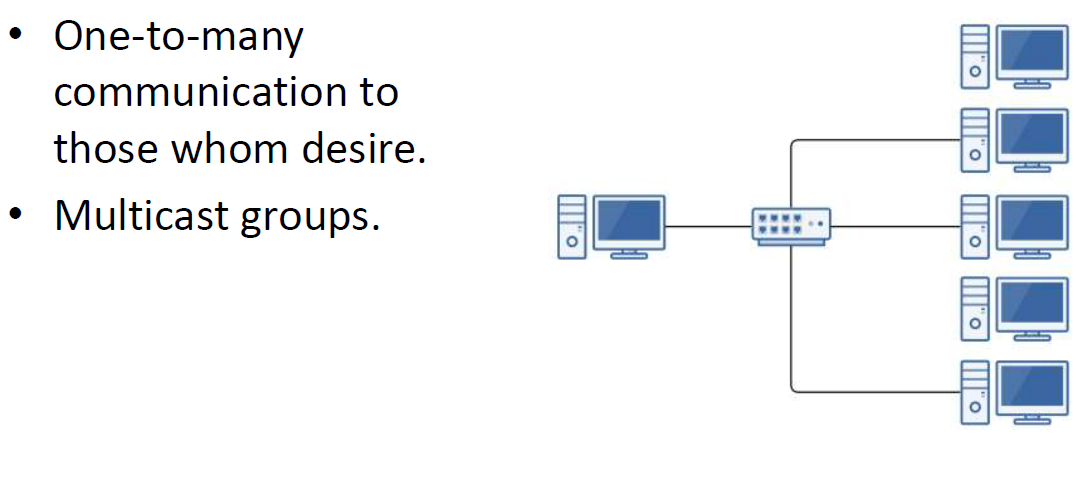
# Remote Communication Protocols

# 

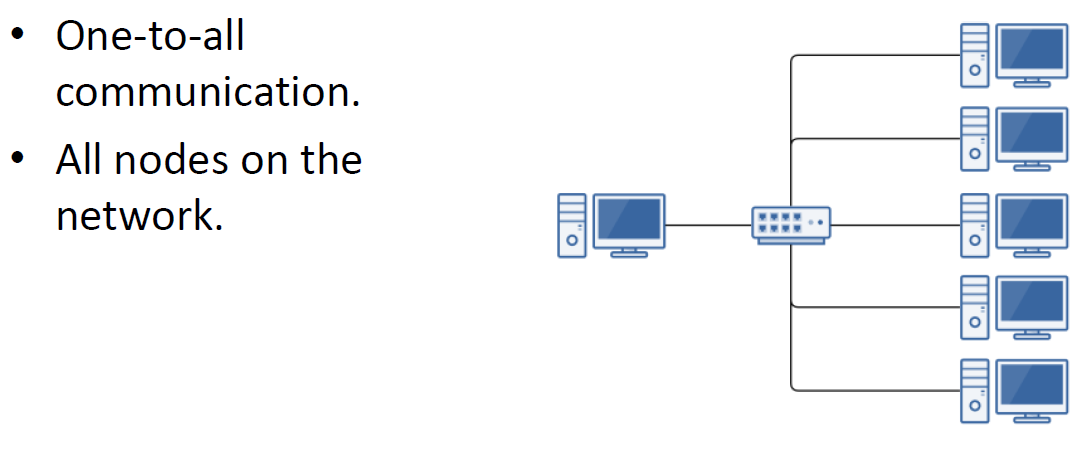
# Unicast Communication



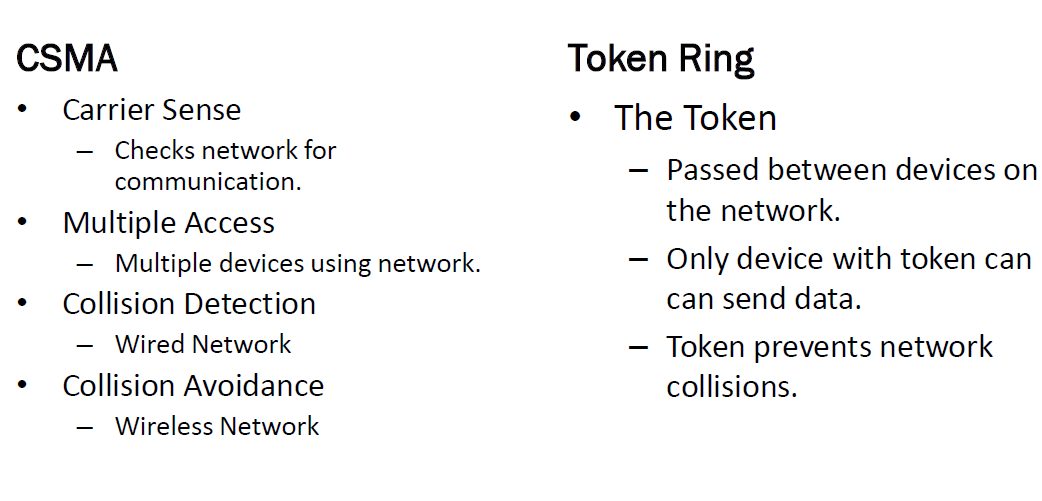
# Multicast Communication



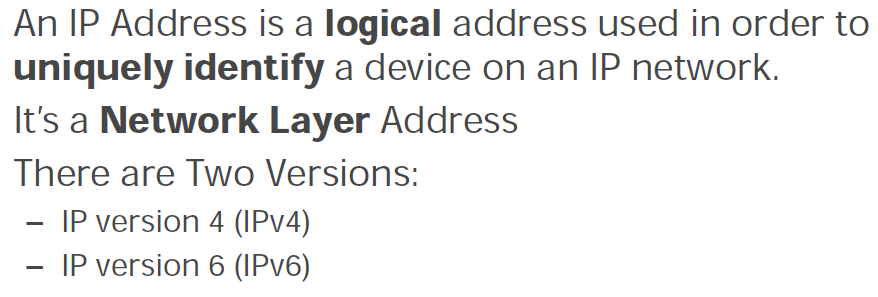
# Broadcast Communication



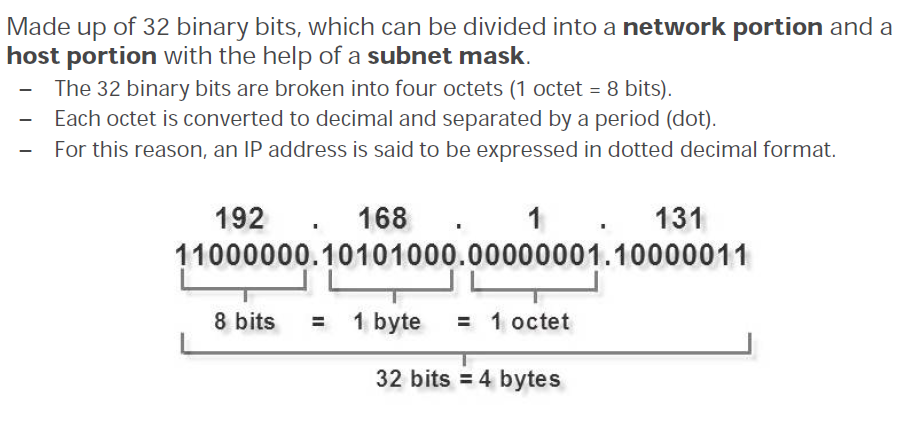
# Network Access Methods: CSMA & Token Ring



# IP Addressing



# IPv4 Addressing



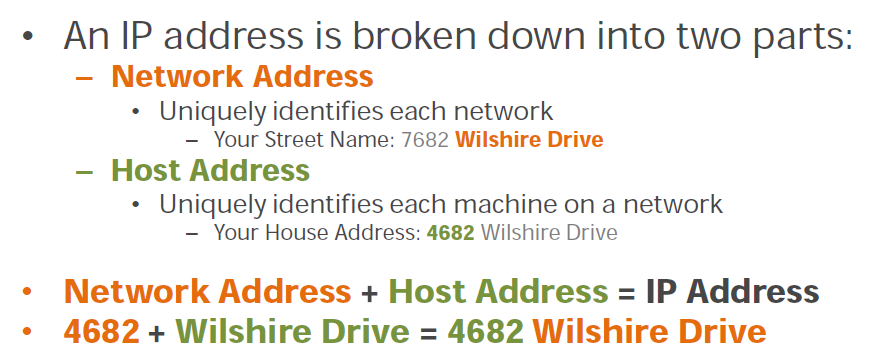
# IPv4 Addressing

# 

# IPv4 Addressing

# 

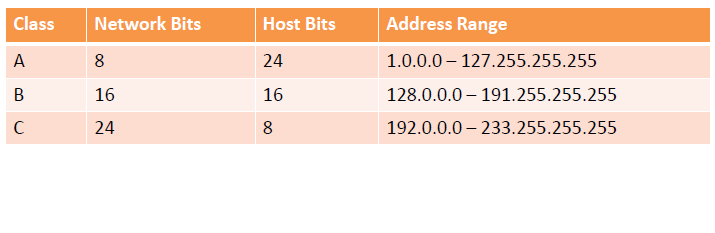
# IPv4 Host & Network Address



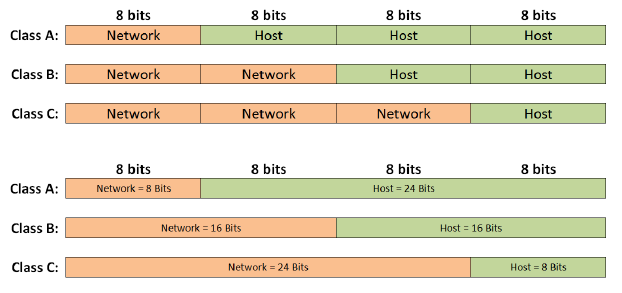
# IPv4 Addressing

# 

# IPv4 Address Classes



# IPv4 Network & Host Bits



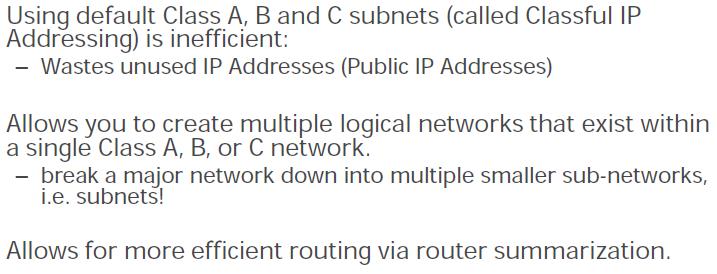
# IPv4 Addresses & Subnet Masks

# 

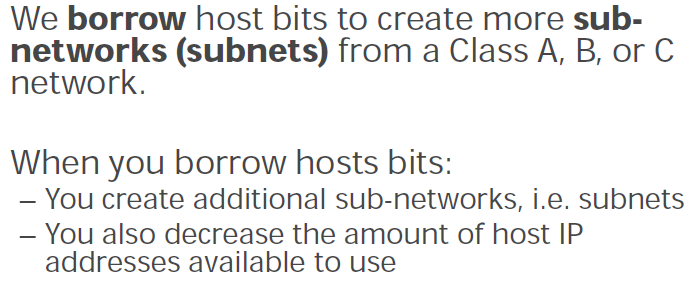
# IPv4 CIDR Notation

# 

# Reason for Subnetting IPv4 Addresses



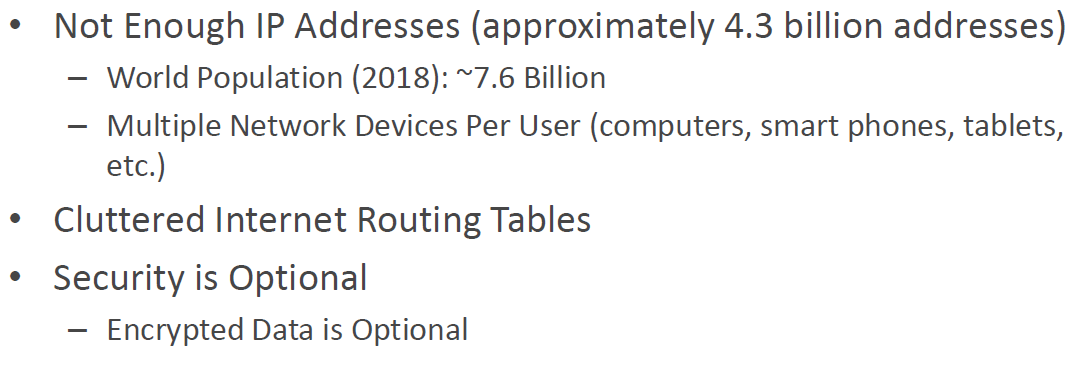
# Process of Subnetting



# Creating Subnets Visualized

# 

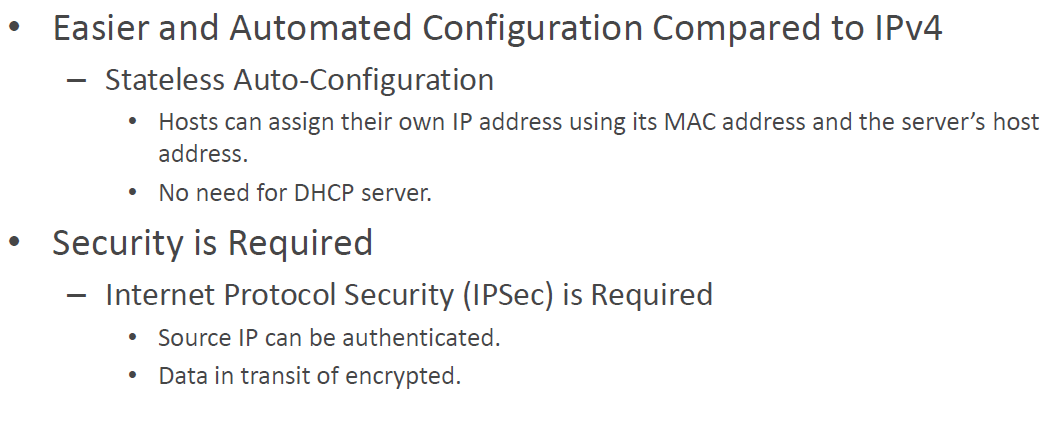
# Disadvantages of IPv4



# IPv6 Solutions to IPv4 Problems

# 

# IPv6 Solutions to IPv4 Problems



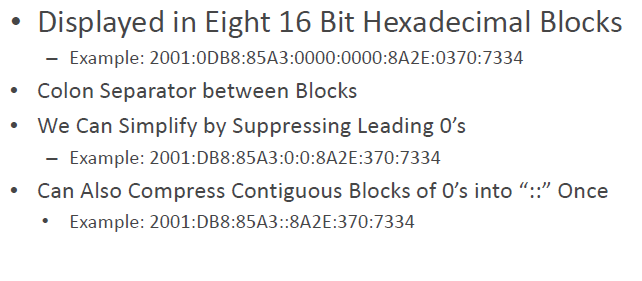
# IPv4 vs IPv6

# 

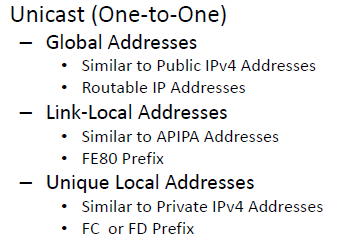
# Reasons IPv4 is Still Used



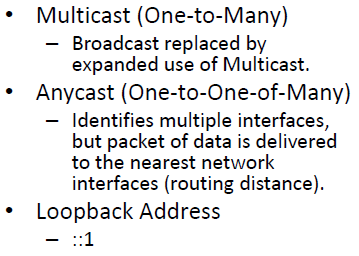
# IPv6 Addressing



# Types of IPv6 Addresses



# Types of IPv6 Addresses



# IPv4 to IPv6 Transition

# 

# Dual Stack IP

* When both IPv4 and IPv6 protocols exist within an operating system.
* Can be used independently or together.

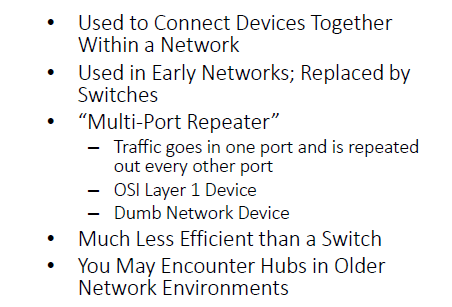
# IPv4-Mapped Addresses

* Dual IP stack can map IPv4 addresses to IPv6 Addresses.
* First 80 bits are 0, next 16 are 1 (shown as ffff), and last 32 bits are populated with the IPv4 address
* Example ::ffff:192.168.1.100

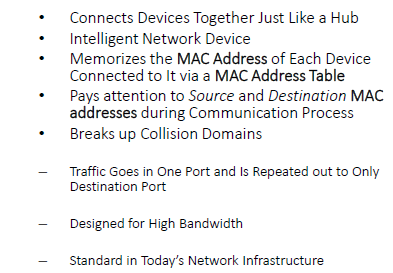
# IPv4 to IPv6 Tunneling

* IPv6 packets are encapsulated inside IPv4 datagram.
* Microsoft utilizes the Teredo virtual adapter to accomplish this.
* You can use ipconfig /all in command prompt to see if your system is using Teredo.

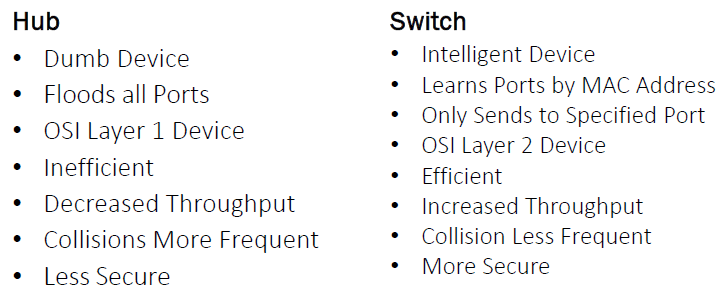
# Hubs



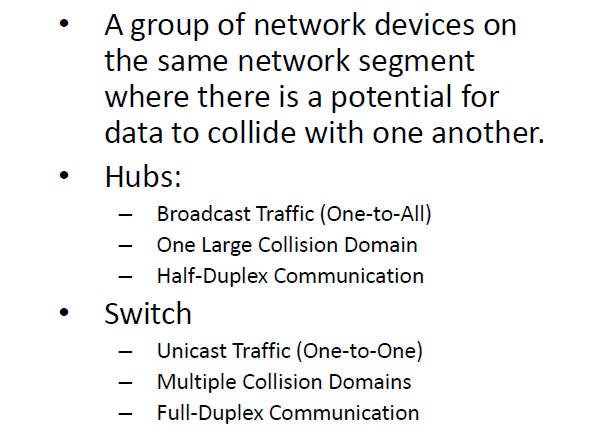
# Switch



# Hub versus Switch



# Collision Domains



# CSMA/CD

Carrier Sense Multiple Access/Collision Detection (CSMA/CD)

* Typically used with hubs (half duplex communication) where there is one large collision domain.
* Can be used with switches if a half-duplex device is connected to it, such as a hub.

Helps hosts decide when to send packets on a shared network segment and to detect collisions.

# CSMA/CD Process

1. Host checks for the presence of a digital signal on the wire.
2. If a digital signal isn’t detected, the host will begin sending a frame of data.
3. If another host begins transmitting and a collision occur, the transmitting host will send a jam signal that causes all hosts on the network segment to stop sending data.
4. After a random period of time, hosts retransmit their packets.

# Layer 3 Switches

Provide Layer 2 Switching & Layer 3 Routing.

* OSI Layer 2 (Data Link): Switching via MAC Addresses
* OSI Layer 3 (Network): Routing via IP Addresses

Managed Switch Capability

Used in Conjunction with VLANs

Provides:

* VLAN Switching
* IP Routing between VLANs

One Device Instead of Router & Switch

# Virtual LANs (VLANs)

Essential LANs within a LAN

Break up a large “physical” LAN into several smaller “logical” LANs.

Accomplished with managed switches.

Assign specific switch interfaces (ports) to specific virtual LANs.

* Human Resource VLAN (Interfaces 1, 2, 3)
* Accounting VLAN (Interfaces 4, 5, 6)

# Virtual LANs (VLANs) Visualized



# Benefits of Virtual LANs (VLANs)

* Reduces Broadcast Domains
* Segments Network by Role
* Increases Security
* Devices Cannot Communicate with Other VLANS
* Group Devices by Need, Not Physical Location

# Unmanaged Switches

* Completely unmanaged.
* Unbox it, plug it in, and it works without any administration.

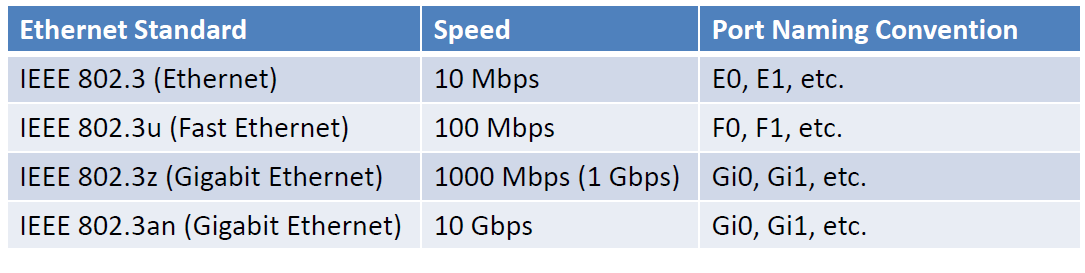
# Managed Switches

Can be configured and managed by network administrators, typically via Telnet or SSH.

* Configure static entries in the MAC table.
* Configure half or full duplex on specific ports.
* Monitor switch performance with SNMP.
* Create virtual LANs (VLANs)
* Configure Port Mirroring

Much more expensive than unmanaged switches.

# Switch Speed Standards



# Transmission Speeds

Many switches can “auto-sense” to detect the transmission speed capabilities of connected devices.

* **10/100**: Autosensing switch capable of 10 Mbps or 100 Mbps speed.
* **100/1000**: Autosensing switch capable of 100 Mbps or 1 Gbps speed.
* **1000/10000**: Autosensing switch capable of 1 Gbps or 10 Gbps speed.
* **10/100/1000/10000:** Autosensing switch capable of 10 Mbps, 100 Mbps, 1 Gbps, or 10 Gbps speed.

# Switch Uplink Port

* The switch uplink port is a special port used to connect a switch to another switch or router.
* Usually used connect to the next “higher” device in the network topology, i.e. smaller LAN to larger network in a building or campus setting.
* You can bundle uplink ports to increase your uplink speed using the *link aggregation control protocol* (LACP).

# Router

* Used to Connect Different Networks Together
* Routes Traffic Between Networks using IP Addresses
* Uses Intelligent Decisions (Routing Protocols) to Find the Best Way to Get a Packet of Information from One Network to Another.
* OSI Layer 3 Device
  + Layer 3 = Router
  + Layer 2 = Switch
  + Layer 1 = Hub

# Static vs Dynamic Routing

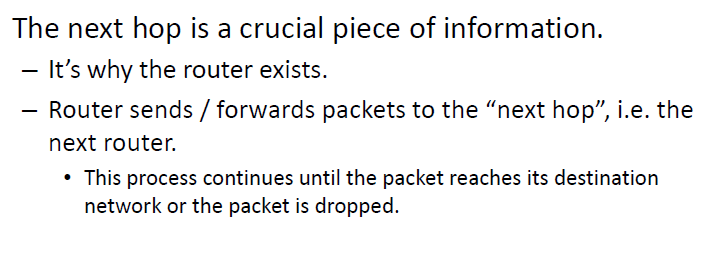
**Static Routing**

* Manual Process
* You manually tell your router where to route traffic
* Often seen as the “default” route on the Internet

**Dynamic Routing**

* Automatic & Hands Off
* Routers are able to make changes to the route on the fly
* All routing decisions are handled by the protocol
* RIP, RIPv2, OSPF

# The Next Hop



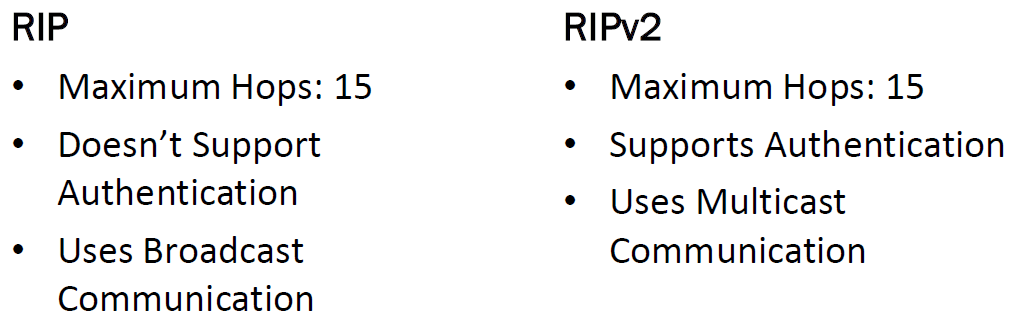
# Link State Routing Protocol: OSPF

* Open Shortest Path First (OSPF)
* Information passed between routers is related to the current connectivity
  + If the link is up, then the packet can go there.
  + If the link is down, the packet can’t go there.
* Requires all routers to know about the paths reachable by all other routers in a network.
  + Where it is, how fast it is, etc.
* Uses “cost” metrics to determine “best” route by including link state and speed.

# Distance Vector Routing Protocol: RIP

* Router Information Protocol: RIP and RIPv2
* Find the best path to a remote network by judging distance.
  + How many “hops” away is another network?
* Distance = Hops
  + Each time a packet goes through a router, it equals a “hop.”
  + 15 hops maximum distance.
* Vector = Which Direction
  + The vector with the fewest hops is the best route.

# RIP versus RIPv2



# Network Address Translation

NAT translates private IP addresses to public IP addresses, allowing us to map multiple private IP addresses to a single public IP.

# DHCP

* Dynamic Host Configuration Protocol (DHCP) Server
* Automatically Assigns IP Addresses to Hosts
* Makes Administering a Network Much Easier
* The Alternative is Static IP addressing

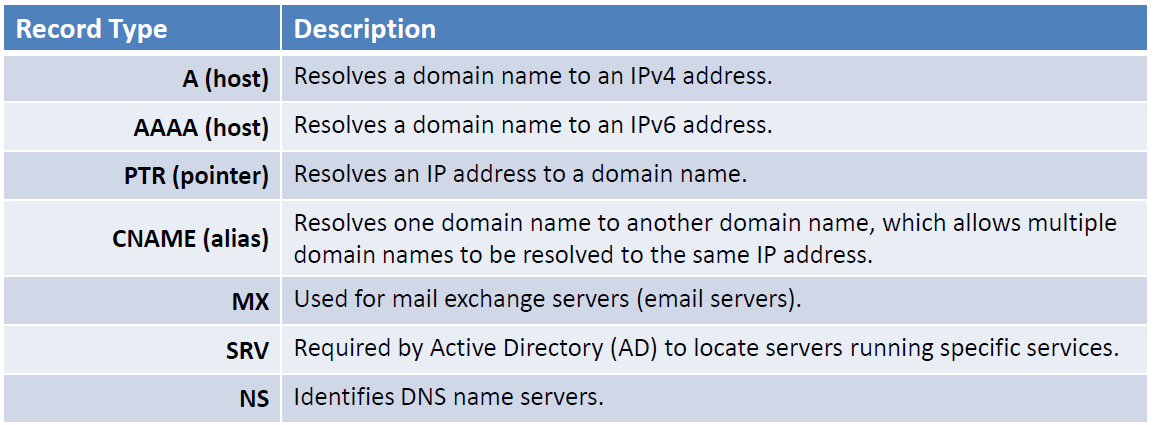
# DHCP IP Address Leasing Process

1. Client requests an IP address by broadcasting a “**DHCP Discover**” message on its local subnet.
2. When the DHCP server receives the request, it’ll respond with a “**DHCP Offer**” message containing an IP address and lease information.
3. If no DHCP server is available, the client will use Automatic Private IP Addressing (APIPA) alternate configuration, if it’s configured.
4. The client then accepts the “DHCP Offer” by replying with a “**DHCP Request**” message to the DHCP server.
5. The DHCP server assigns client the address and sends a “**DHCP Ack**” message in response, finalizing the DHCP IP address lease.

# DNS Hierarchy

|  |  |
| --- | --- |
| **Root DNS Servers** |  |
| **Top Level Domain DNS Servers** | .com, .mil, .edu, .net, .org |
| **Second Level Domain DNS Servers** | Microsoft.com |
| **Third Level Domain DNS Servers** | Technet.Microsoft.com |

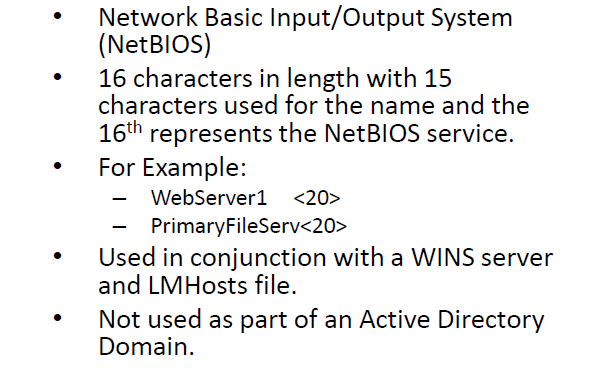
# Common DNS Records



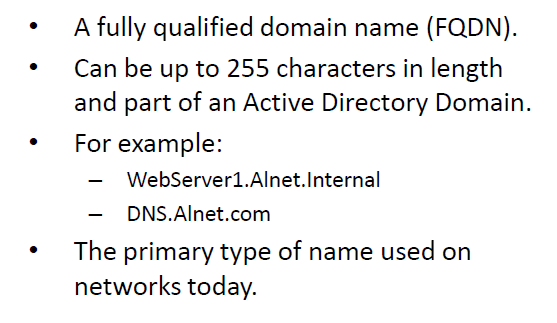
# Name Resolution Process

1. Host Cache/Hosts File
2. DNS Server
3. NetBIOS Cache
4. WINS Server
5. Broadcast
6. LMHosts File

# NetBIOS Names



# Host Names



# Name Resolution Step 1: Host Cache/Hosts File

Your computer caches DNS query responses in DNS cache and it always checks there first.

We can view a computer’s DNS cache with the following command:

* ipconfig /displaydns

Windows has a “Hosts” file where you can manually map domain names / host names to IP addresses.

* Any entry in the “Hosts” file is added to the DNS Cache
* C:\WINDOWS\System32\drivers\etc

# Name Resolution Step 2: DNS Server

If your computer cannot find the domain name / host name in its Host Cache, it will query its configured DNS server in it’s TCP/IP settings.

# Name Resolution Step 3: NetBIOS Cache

* The next step in the name resolution process is NetBIOS cache.
* NetBIOS names resolved by WINS server names are placed in a NetBIOS cache.
* We can use the following command to view a computer’s netBIOS cache:
  + nbtstat -c

# Name Resolution Step 4: WINS Server

If a NetBIOS name isn’t in the computer’s NetBIOS cache, the computer will then query the WINS server.

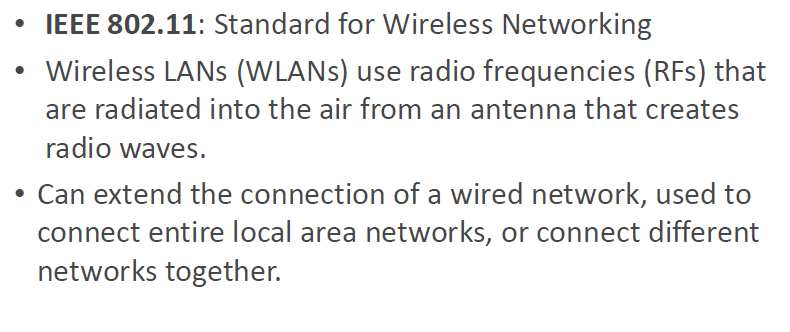
# Name Resolution Step 5: Broadcast

If WINS doesn’t resolve a NetBIOS name, the computer will attempt to resolve the name using a network broadcast over its local subnet.

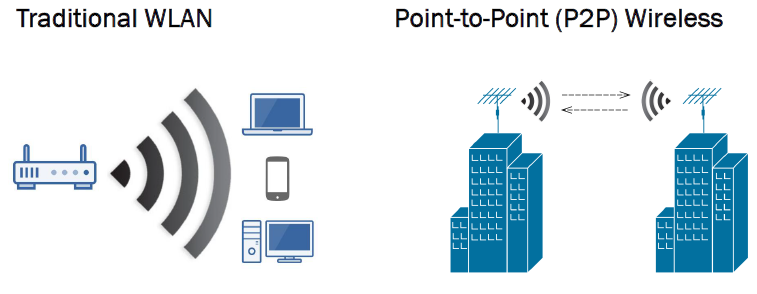
# Name Resolution Step 6: LMHosts File

* The last step is to look up the NetBIOS name in the LMHosts file if all other steps have failed to resolve the name’s IP address.
* However, newer Windows operating systems don’t include a working LMHosts file:
  + Windows 7 and Newer
  + Windows Server 2008 and Newer
  + You have to manually create an LMHosts file on these operating systems
  + C:\WINDOWS\System32\drivers\etc

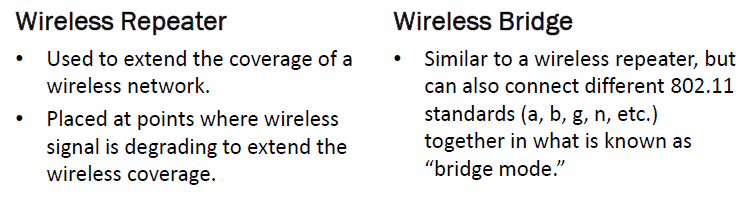
# Wireless Networking



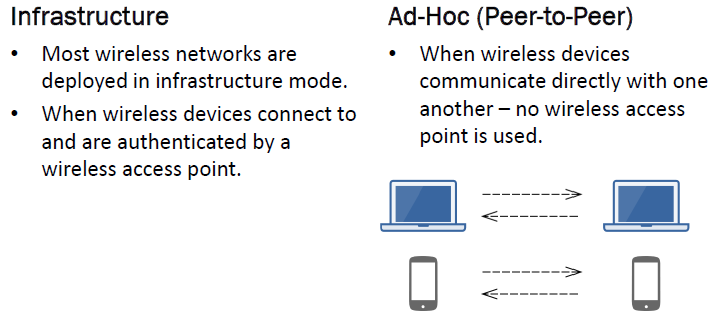
# Depicting Wireless Networks



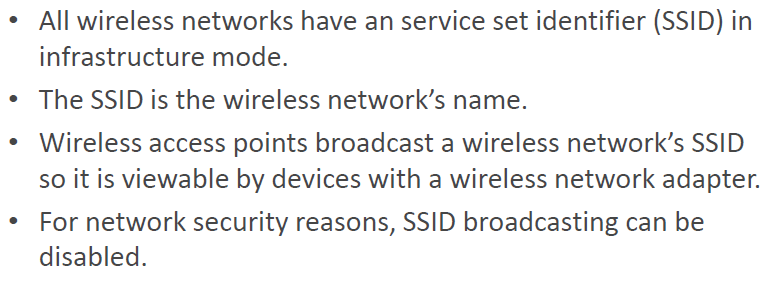
# Wireless Repeater vs. Wireless Bridge



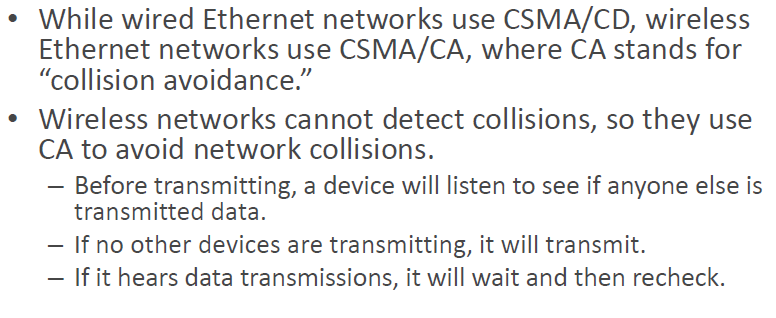
# Wireless Network Modes



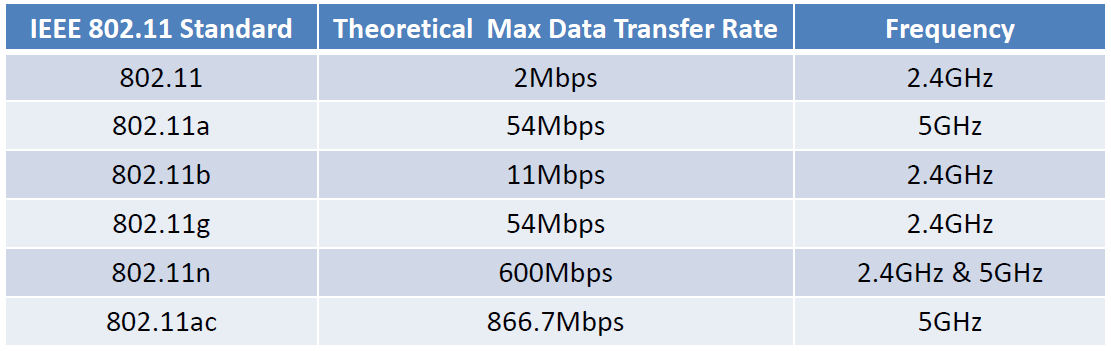
# Service Set Identifier (SSID)



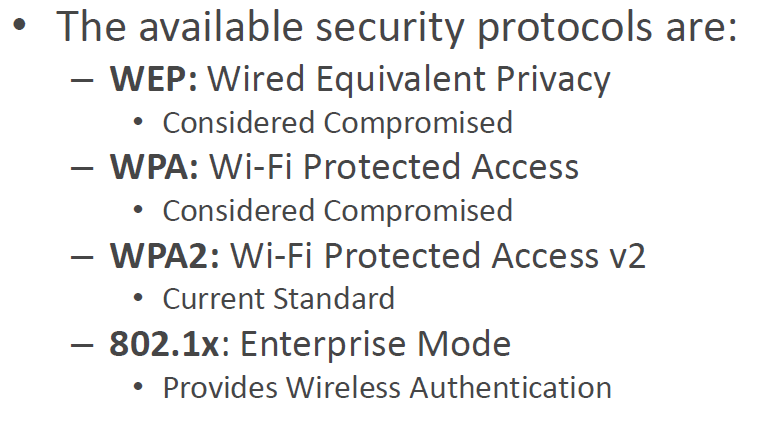
# Wireless Network CSMA/CA



# Wireless 802.11 Standards



# Wireless Network Security Standards



# Wired Equivalent Privacy (WEP)

* The original security protocol used to secure wireless networks.
* Has significant vulnerabilities (weak encryption and key management) and software is easily attainable to crack WEP-protected networks in minutes.

# Wi-Fi Protected Access (WPA)

* WPA was created as an interim replacement for WEP after WEP’s vulnerabilities became widely known and exploited.
* Was never designed to be a long-term solution, just an interim solution until WPA2 became available.
* It was cracked in Nov 2008.

# Wi-Fi Protected Access v2 (WPA2)

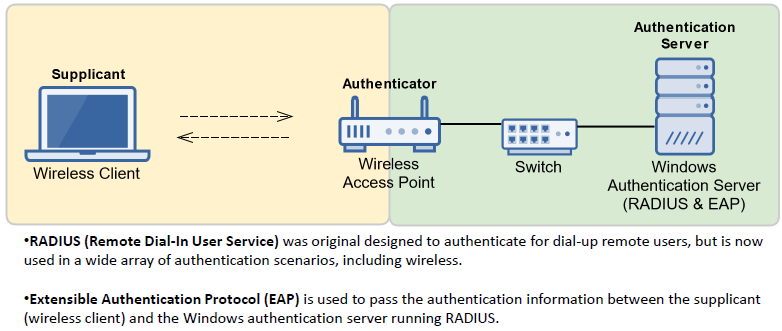
* WPA2 is the permanent replacement for WEP and WPA.
* WPA2 used Advanced Encryption Standard (AES) encryption instead of RC4 (used by WEP & WPA).
* AES is the encryption standard for the U.S. government and is used worldwide.

# WPA2 Modes

WPA2 supports two modes:

* **WPA2 Personal Mode (WPA2-PSK)** 
  + Pre-shared key for home use.
* **WPA2 Enterprise Mode (WPA2 with 802.1)** 
  + 802.1x provides authentication services via a Windows Server before users are granted access to the wireless network.

# 802.1x Fundamentals



# Wide Area Networks (WANs)

WANs connect smaller networks together

* Typically Covers a Relatively Broad Geographic Area
* Uses Transmission Facilities Provided by Common Carriers
* You Usually Lease a WAN Infrastructure from a Service Provider

Common WAN Technologies

* Circuit Switching
* Packet Switched Virtual Circuits
* Leased Lines
* Cell Relay

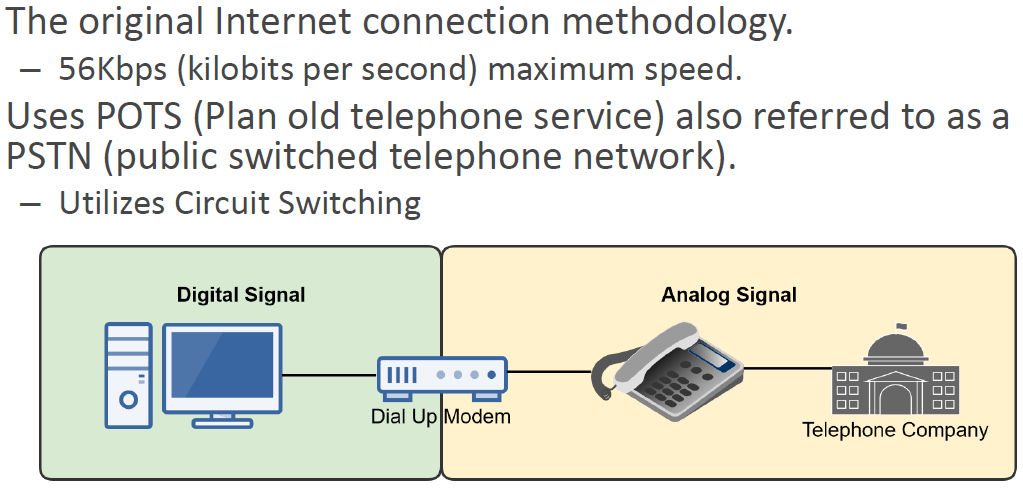
# Circuit Switching

* Designed in 1878, was originally designed for telephone calls.
* Uses a dedicated point-to-point connection (circuit) using a telecommunications network.
* A circuit guarantees you full bandwidth of the circuit and remains connected for the duration of your call.
* The circuit functions as if the nodes were physically connected as with a dedicated electrical circuit.

# Packet Switching

* Uses virtual switches that provide end-to-end connectivity.
* Data is moved in packets based on the destination address in each packet.
* Unlike circuit switching, packet switching shares bandwidth and connection with others.
* This method of data transmission is the core technology for the Internet and most LANs.

# Dial Up Connection



# ISDN

* Integrated Services Digital Network (ISDN)
* The original high speed Internet connection.
* A POTS network system that operates via circuit-switched technology.
* Can simultaneously transmit data and phone conversations digitally over normal telephone wires.
  + With dial-up you could not make phone calls while accessing the Internet.
  + With ISDN, you can make phone calls and access the Internet simultaneously.

# ISDN Basic Rate Interface (BRI)

* Uses two data (bearer or B) channels that operate at 64Kbps for a total data transfer rate of 128Kbps for uploads and downloads.
* Also has a 16Kbps D channel that transmits control information.

# ISDN Primary Rate Interface (PRI)

A high-speed form of ISDN –provided on T1 or E1 trunk lines.

* T1: USA, Canada, Japan & E1: Europe

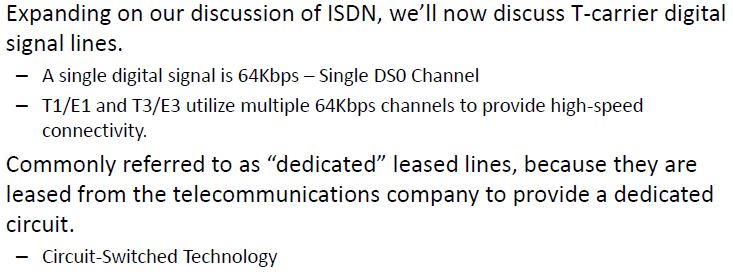
T1 trunk line is divided into 24 channels of 64Kbps capacity (1.544Mbps):

* 23 64Kbps B Channels and 1 64Kbps D Channel

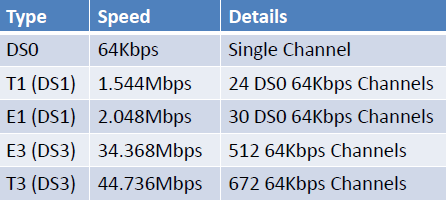
E1 trunk line is divided into 32 channels of 64Kbps capacity (2.048Mbps):

* 30 64Kbps B Channels and 2 64Kbps D Channel

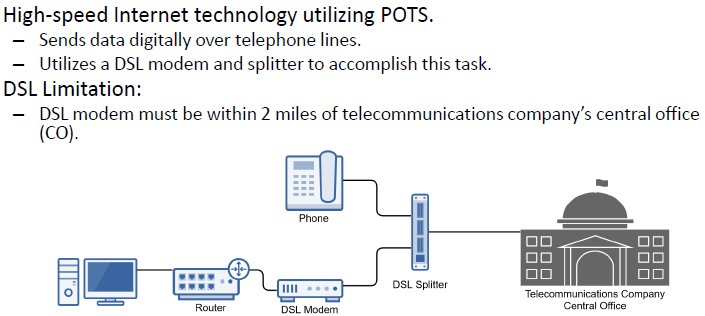
# T-Carrier & E-Carrier Digital Signal Lines



# Comparing T1, E1, T3, and E3 Speeds



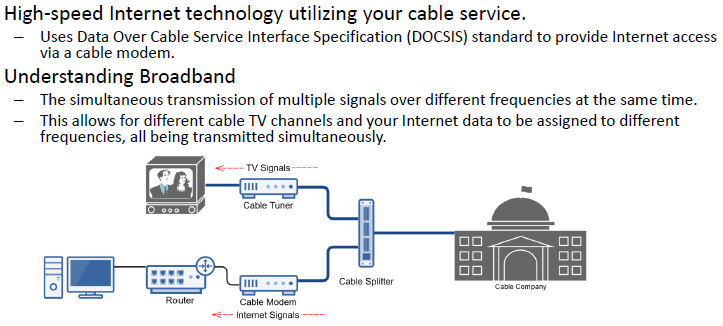
# Digital Subscriber Line (DSL)



# SDSL versus ADSL

# 

# Broadband Cable



# Broadband Cable DOCSIS Standards

# 

# X.25

* The original packet switching technology designed in the 1970s.
* 2400bps – 2Mbps data transfer rate.

# Frame Relay

* Advancement of X.25 designed in 1990s.
* Has a base price based on its Committed Information Rate (CIR).
* Puts data in a variable-sized unit called a frame.
* T1 (1.544Mbps) & T3 (44.736Mbps) data transfer rates.
* Discontinued by major Internet service providers from 2007 through 2016.

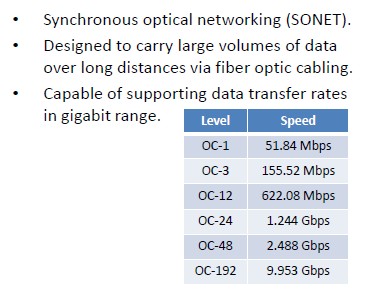
# ATM

* Asynchronous Transfer Mode.
* An advanced packet switching technology, called “cell-based” switching technology.
* Utilizes fixed length packets (53 bytes).
* Can be used with Fiber Distributed data interface (FDDI), Synchronous Optical Network (SONET), and other high-speed WAN technologies.
* Speeds on ATM networks can reach 10Gbps.

# FDDI

* Fiber distributed data interface (FDDI).
* Standard for transmitting on fiber optic cables at 100Mbps.
* Was primarily used on backbone networks, but was made obsolete by Fast Ethernet in the 1990s, which offers the same speeds at a much lower cost.

# SONET/OCx



# Intranet & Extranet

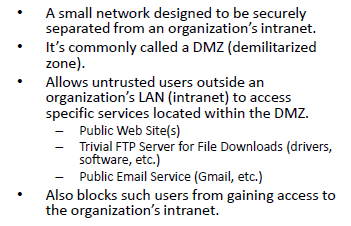
**Intranet**

* An organization’s internal private network that only the organization’s employees can access.
* Used for internal business activities such as HR, accounting, R&D, etc.

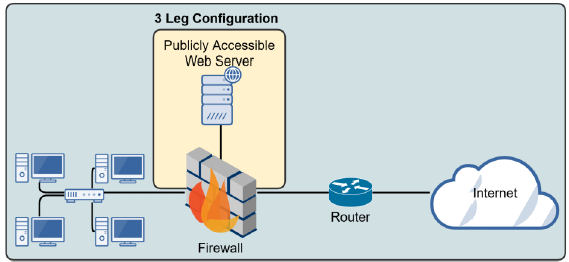
**Extranet**

* A portion of an organization’s private network that only business partners can access.
* Used for business partner activities such as ordering supplies, etc. via a business partner web portal.

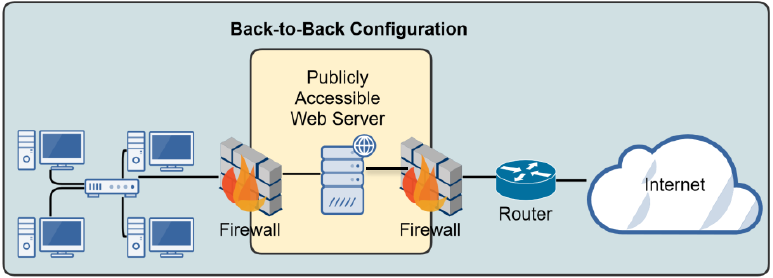
# Perimeter Network: DMZ



# 3-Leg DMZ Configuration



# Back-to-Back DMZ Configuration



# Firewalls

* Protects Your LAN from Malicious Activity on the Internet
* Prevents Unwanted Network Traffic on Different Networks from Accessing Your Network and vice Versa
* Essentially Controls the Flow of Information in and out of Your Network
* You Create Network Access Rule Sets to Setup and Maintain a Firewall
* A Firewall Can Be a Standalone Network Device or Software on a Computer System, Meaning Network-Based or Host-Based

# 1st Generation: Packet Filtering Firewall

The original type of firewall and most basic type of firewall. Filters packets based on IP addresses and ports.

# 2nd Generation: Stateful Inspection Firewall

* Analyzes packets similar to a packet filtering firewall; however, it also make intelligent decisions tracking each communication session.
* Determine the legitimacy of a requested session by monitoring the 3-way handshake between packets.
* Hackers can alter the 3-way handshake process attempting to cause denial of service (DoS) attack.
* If the firewall believes an attack is occurring, it will block the traffic.

# 3rd Generation: Application Layer Firewall

* Filters packets based on an application or service.
* It “understands” certain applications and protocols (FTP, DNS, HTTP, etc.) and is able to detect if an unwanted application or service is attempting to bypass the firewall using a protocol of a different port.

# Intrusion Detection & Prevention Systems

Are designed to detect attacks on a network and respond passively or actively.

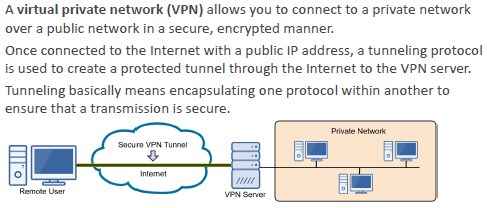
Basic firewalls will try to block network attacks using ACLs (rules) while IDS/IPS try to detect the attacks.

* IDS is **Passive**, meaning its response is logging and notifying.
* IPS is **Active**, meaning it’ll change the network environment to stop an attack, such as changing ACLs or closing processes, sessions or ports.

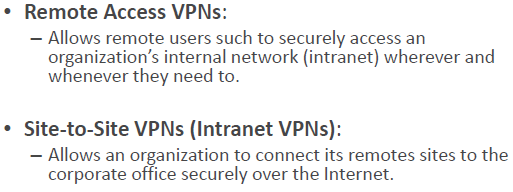
# Proxy Servers

* Acts on behalf of computers within a LAN to retrieve web content from the Internet.
* Specifically, proxy servers can provide the following services:
  + Filtering
  + Content Checking
  + Caching

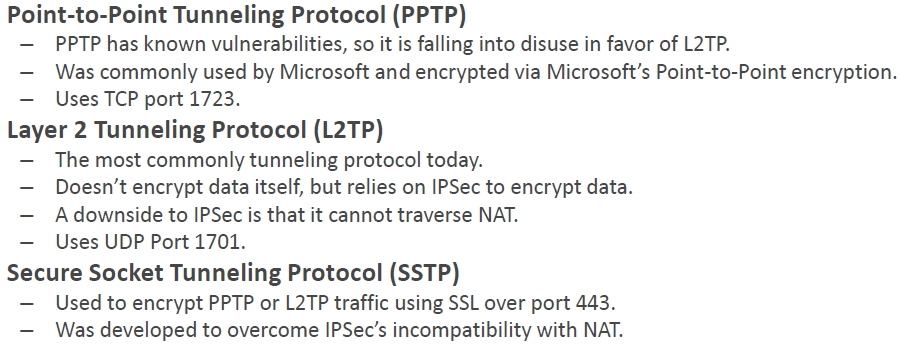
# Virtual Private Network (VPN)



# Types of VPN



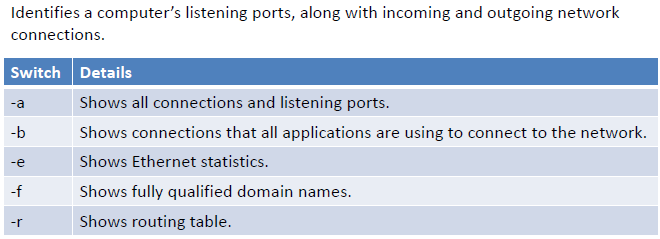
# VPN Tunneling Protocols



# IPConfig

# C:\Users\jrjpb\AppData\Local\Temp\1\SNAGHTML1bc4561.PNG

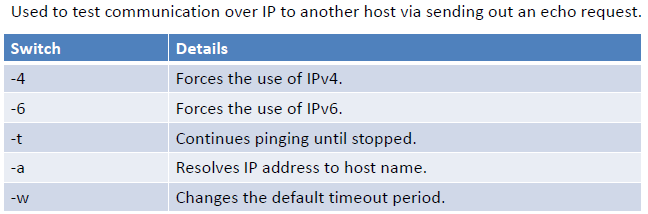
# Netstat



# PathPing

# 

# Ping



# Tracert

