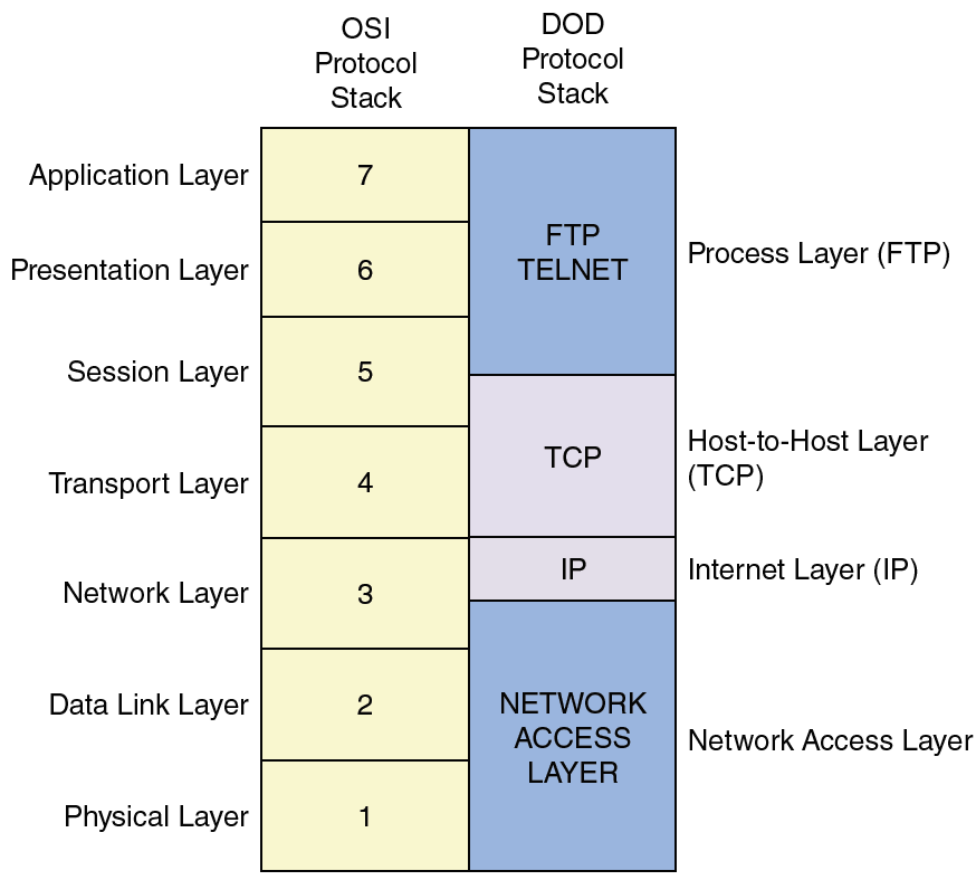
NETWORKING BASICS

Prof. Yasser Mostafa Kadah – www.k-space.org

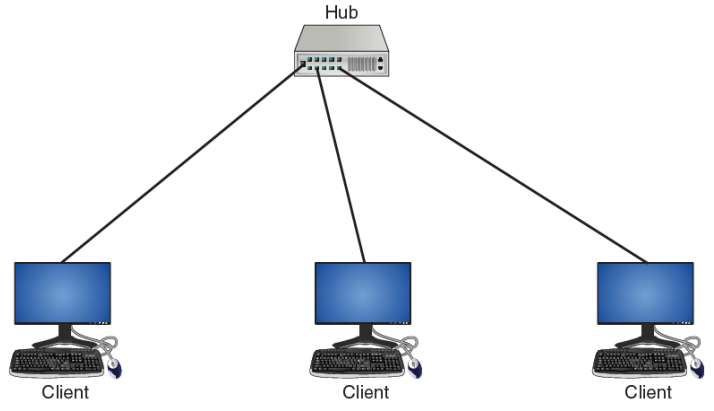
Network Communication Model Layers



Layer Number	Layer Name	Description	Function
Layer 7	Application Layer	The top layer, Application, provides the user interface to allow network services.	Provides services for user applications.
Layer 6	Presentation Layer	The Presentation Layer is concerned with how the data is represented and formatted for the user.	Is used for translation, compression, and encryption.
Layer 5	Session Layer	This layer has the responsibility of permitting the two parties on the network to hold ongoing communications across the network.	Allows devices to establish and manage sessions.
Layer 4	Transport Layer	The Transport Layer is responsible for ensuring that error-free data is given to the user.	Provides connection establishment, management, and termination as well as acknowledgments and retransmissions.
Layer 3	Network Layer	The Network Layer picks the route the packet is to take and handles the addressing of the packets for delivery.	Makes logical addressing, routing, fragmentation and reassembly available.
Layer 2	Data Link Layer	The Data Link Layer is responsible for dividing the data into packets. Some additional duties of the Data Link Layer include error detection and correction (for example, if the data is not received properly, the Data Link Layer would request that it be retransmitted).	Performs physical addressing, data framing, error detection and handling.
Layer 1	Physical Layer	The job of this layer is to send the signal to the network or receive the signal from the network.	Involved with encoding and signaling, data transmission, and reception.

Hubs

- Hub is older device for connecting multiple Ethernet devices on network, typically by using shielded twisted-pair (STP) copper cables to make them function as single network segment
- Hubs work at Physical Layer (Layer 1) of the OSI model
  - This means that they do not read any of data passing through them and are ignorant of source and destination of the frames
  - Hub will only receive incoming frames, regenerate the electrical signal, and then send frames out to all other devices connected to hub
- Because hub repeats all frames to all of its attached network devices, it not only increases network traffic but also can be security risk
  - Hubs are rarely used today, and many organizations restrict or even prohibit their use

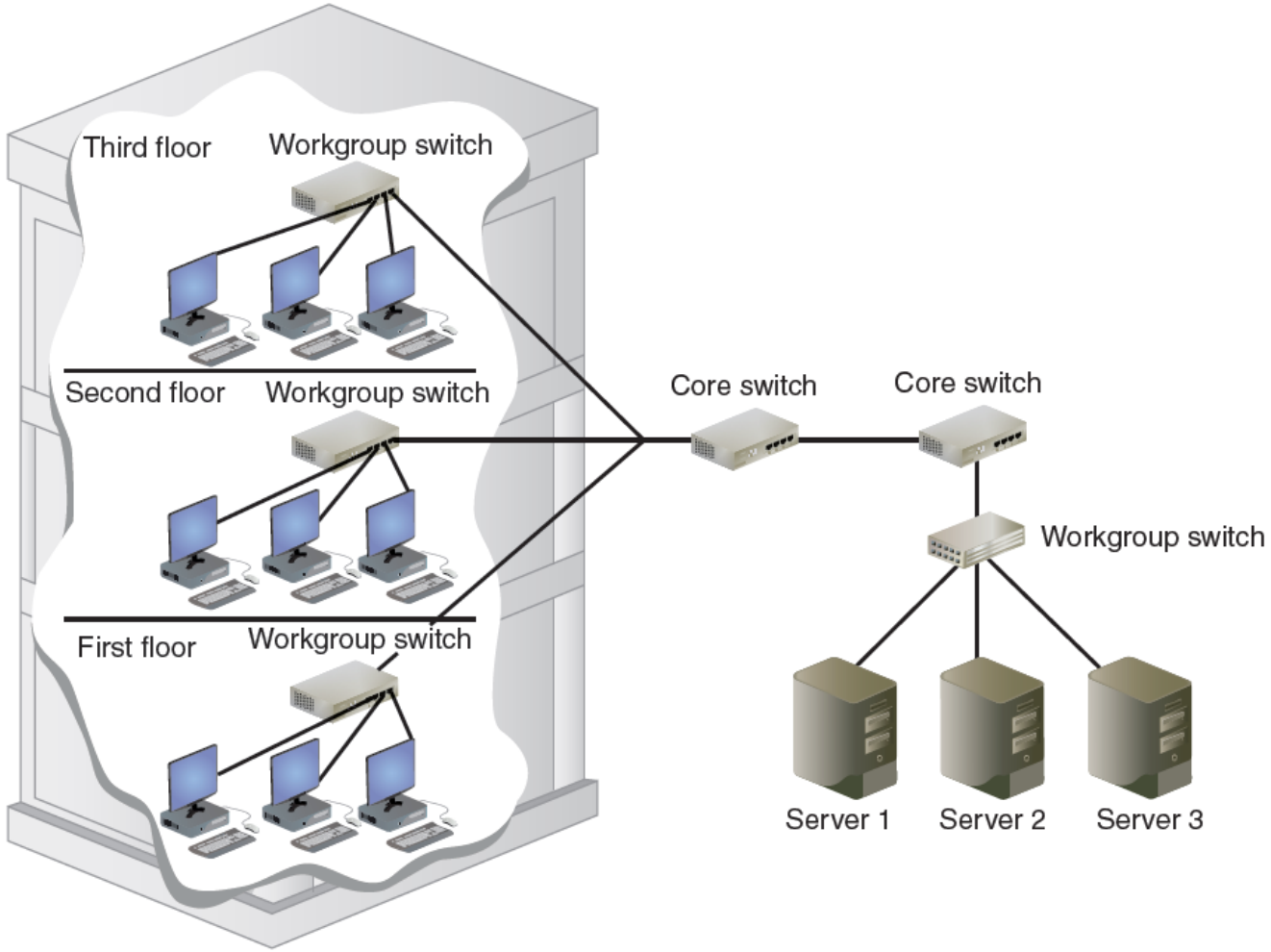


Switches

- Network switch is device that connects network segments together with degree of "intelligence"
- Operating at Data Link Layer (Layer 2), switch can learn which device is connected to each of its ports, and forward only frames intended for that specific device (unicast) or frames sent to all devices (broadcast)
- Each device connected to the switch has unique media access control (MAC) address (also called the hardware address)
- Switch learns by examining MAC address that is included in frames that it receives and then associates its port with that MAC address of the device connected to that port
  - This improves network performance and provides better security

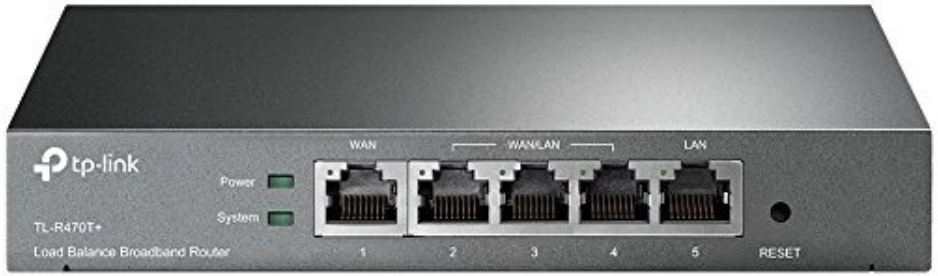
Network Division with Core and Workgroup Switches

- In most network environments, networks are divided or segmented by using switches to divide network into hierarchy
  - Core switches reside at top of hierarchy and carry traffic between switches, while workgroup switches are connected directly to devices on the network
  - Core switches must work faster than workgroup switches because core switches must handle traffic of several workgroup switches



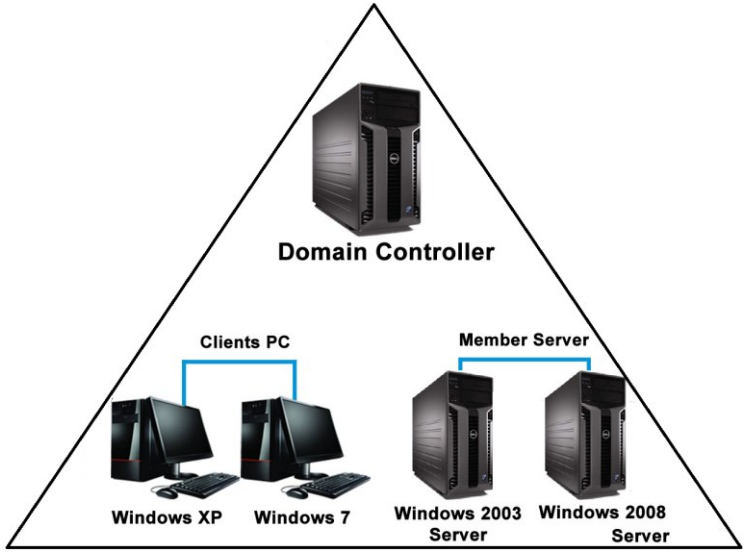
Routers

- Operating at Network Layer (Layer 3), router is network device that can forward packets across computer networks
- When router receives incoming packet, it reads destination address and then, using information in its routing table, sends packet to next network toward its destination
- Routers can also perform security function
  - Can be configured to filter out specific types of network traffic
  - For example, router can be set to disallow incoming packets that have invalid addresses or to disallow packets from specific addresses



Domain Controllers

- In network using Microsoft Windows software, domain is collection of devices that all share central directory database containing accounts and security information for resources in that domain
- Domain controller is server that manages security-related elements on network for user
  - Allows for security to be centralized and more easily managed
- Windows domain controller is generally suited for organizations when more than 10 client computers are being used



Servers

- Servers play crucial role in client-server computing environment with several different types of services and servers along with different protocols
  - Print services: Multiple users share printers across network
    - Single centrally located higher-speed (and more feature-rich) printer to serve printing needs of all users in office or computer lab resulting in significant cost savings
  - File services: Ability to share user-created files by storing them in central location where they can be accessed by other users who have permission
    - Conserve storage space as well as prevent different versions of the same file circulating (with one user updating one version while another user updates another version)
  - Application services: Processes that run software for network clients and thus enable clients to share processing power across network
  - Communication services: Help users communicate using variety of tools such as e-mail, telephony, and instant messaging
- These different network services can be provided through server dedicated to that function
  - Print server, database server, application server, communication server

Server Management

- Load balancing
  - Technology that can help to evenly distribute work across network
    - Requests received can be allocated across multiple devices such as servers to balance loads
  - To the user, this distribution is transparent and appears as if single server is providing resources
    - Probability of overloading single server is reduced
    - Each networked computer can benefit from having optimized resources
    - Network downtime can be reduced
  - Performed by software running on computer or as dedicated hardware device (Layer 4–7 router)
- Managing Storage
  - Several different technologies available that can provide enhanced storage capabilities such as storage virtualization, which hides physical resources of storage (such as specific hard drive) from user and all storage devices are "pooled" and appear as one large repository of storage

Protocols

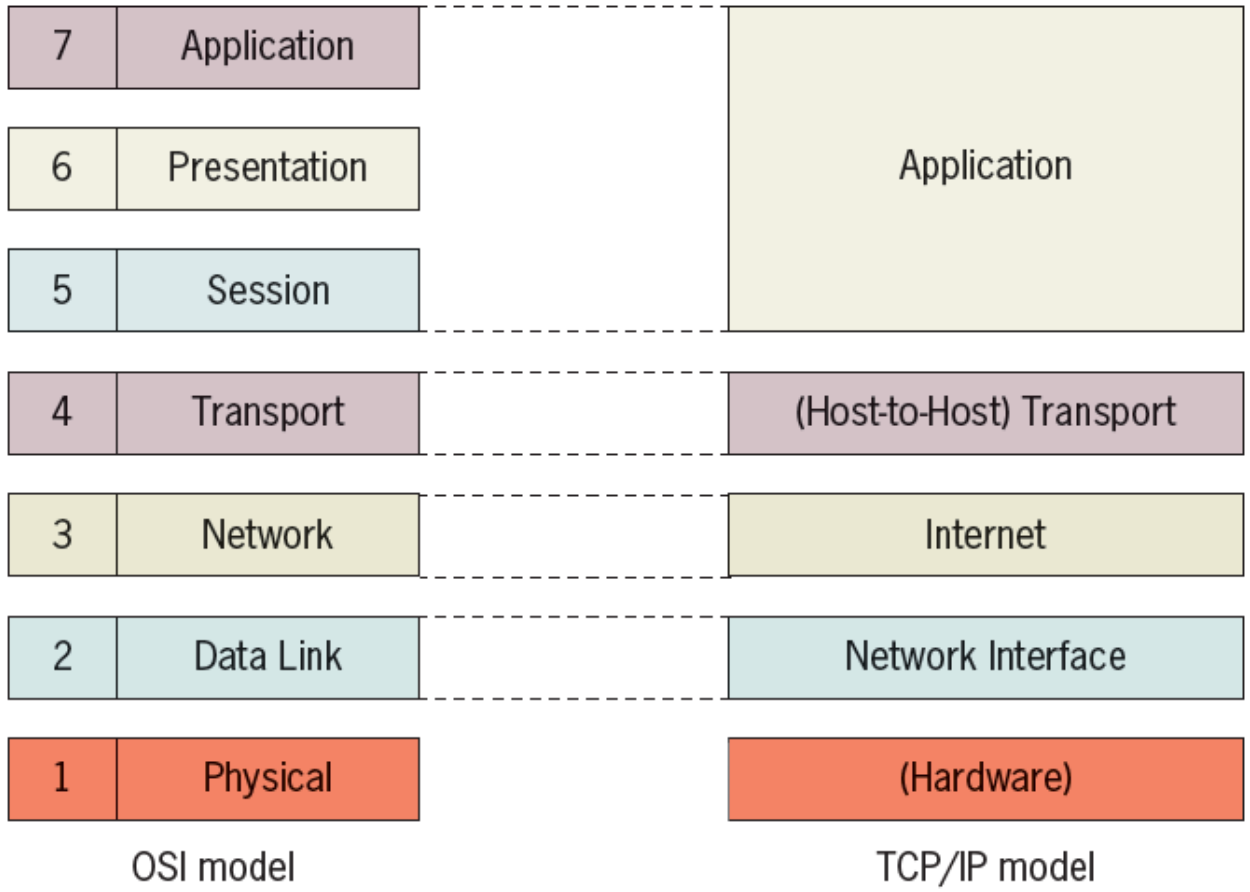
- Computer networks have protocols, or rules for communication that are essential for proper communication to take place between network devices
- Three common protocols are in use
  - Transmission Control Protocol/Internet Protocol (TCP/IP)
  - Wireless protocols,
  - Remote Desktop Protocol (RDP).

Transmission Control Protocol/Internet Protocol (TCP/IP)

- Most common protocol suite used today for local area networks (LANs) as well as Internet
- Combination of several protocols function together or protocol suite
  - Two major protocols that make up its name: Transmission Control Protocol (TCP) and Internet Protocol (IP)
  - IP is protocol that functions primarily at OSI Network Layer (Layer 3) to provide addressing and routing
    - IP is responsible for addressing packets and sending them on correct route to destination
  - TCP is main Transport Layer (Layer 4) protocol responsible for establishing connections and reliable data transport between devices
    - TCP is responsible for reliable packet transmission

Transmission Control Protocol/Internet Protocol (TCP/IP)

- TCP/IP uses its own four-layer architecture that includes Network Interface, Internet, Transport, and Application layers
  - Physical Layer is omitted because TCP/IP views Network Interface Layer as point of connection between TCP/IP protocol and networking hardware
- TCP/IP architecture gives framework for dozens of various protocols that comprise suite and also includes several high-level applications that are part of TCP/IP
  - Basic TCP/IP protocols include Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) and File Transfer Protocol (FTP)

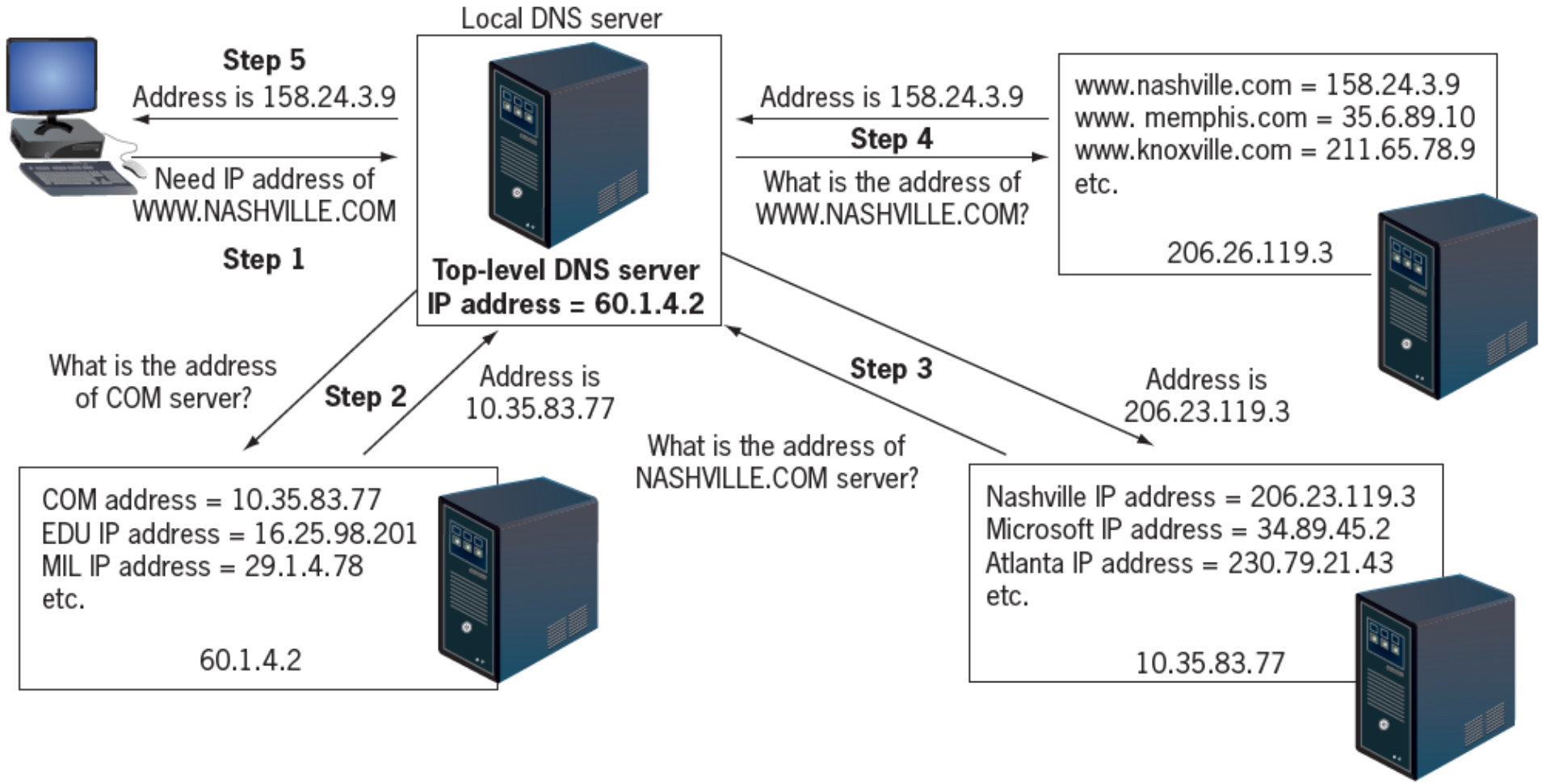


Domain Name System (DNS)

- TCP/IP protocol that resolves (maps) IP address (such as 69.132.133.179) to its equivalent symbolic name (www.mywebsite.com)
- DNS is database, organized as hierarchy or tree, of name of each site on Internet and its corresponding IP address
- Storing entire DNS database in one location would present several problems
  - Cause bottleneck and slow down the Internet with all users trying to access one copy of database
  - If something happened to this one database, then entire Internet would be affected
- DNS database is divided and distributed to many different servers on Internet, each of which is responsible for different areas of Internet

DNS Lookup

- Resolving IP address to symbolic name



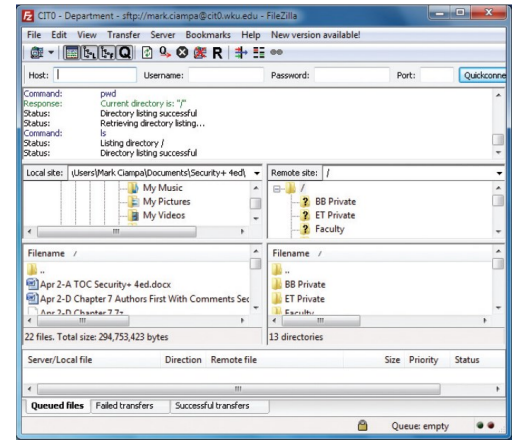
Dynamic Host Configuration Protocol (DHCP)

- Each device on computer network must have unique name or number
  - Because no two devices share same name or number, packets can be transmitted through network addressed to device that has that unique identifier
- Computers on TCP/IP network use logical address, called IP address, is assigned to each host
- IP address is made up of four bytes (called octets), each contain eight bits (total 32 bits) indicating numbers for computer network and host on that network (defined by subnet mask)
  - Each octet is number from 1 to 254
  - Subnet mask of 255.255.255.0 means that first 3 octets define network and last one defines host
- Assigning IP addresses to each device can be done in one of two ways: static or dynamic
  - Static IP: assigned manually (IP address that does not change)
    - On large network, this can be very time-consuming process and may cause IP conflicts if done incorrectly
  - Dynamic IP: automatically distributed using protocol in TCP/IP suite known as DHCP
    - When computer attaches to network, it requests IP address from DHCP server
    - IP address is leased to host and once computer is off network or lease expires, IP address becomes free and can be given to another computer

Type of Address	First Octet	Second Octet	Third Octet	Fourth Octet
IP address	192	168	1	1
Subnet mask	255	255	255	0

File Transfer Protocol (FTP)

- FTP is popular method by which computer files can be transferred from one system to another over Internet or other computer network
  - FTP links to FTP server same way that HTTP links to Web server
- There are several different methods for using FTP on a local host computer:
  - From a command prompt: FTP commands can by typed at operating system prompt
  - Using Web browser: Instead of URL with protocol http://, FTP protocol is entered with preface of ftp://.
  - Using FTP client: Separate FTP client application can be installed that displays files on local host as well as remote server, and these files can be dragged and dropped between devices
- FTP servers can be configured to allow unauthenticated users to transfer files, known as anonymous FTP (also called blind FTP)



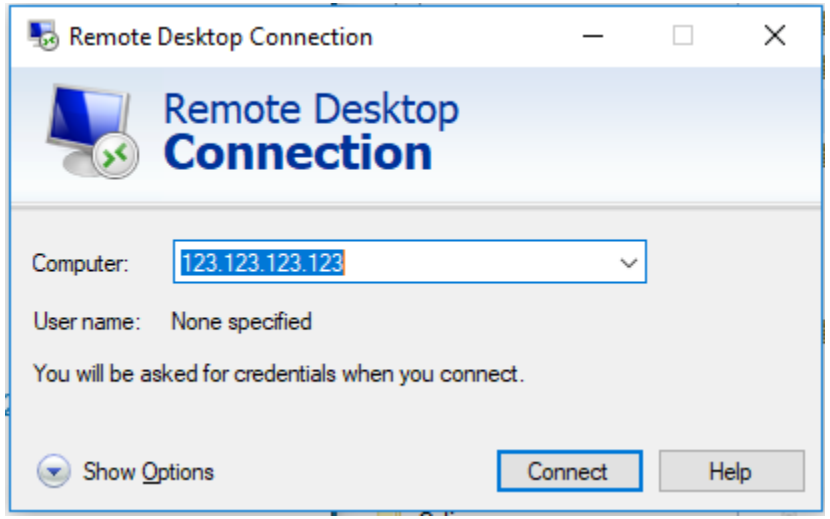
Wireless Protocols

- Wireless data communications are replacing need to be tethered by cable to network to surf Web, check e-mail, or access inventory records
  - Wireless communication has made mobility possible to degree never before possible or rarely even imagined whereby users can access same resources standing on street corner or walking across college campus as they can while sitting at desk
- Although wireless voice communication started revolution in 1990s, wireless data communications have been driving force in twenty-first century
- Among reasons wireless local area networks (WLANs) have been so successful is because from outset these networks were based on set of standards
  - WLAN standards IEEE 802.11
    - High speed, wide coverage area, interference reduction, strong level of wireless security

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

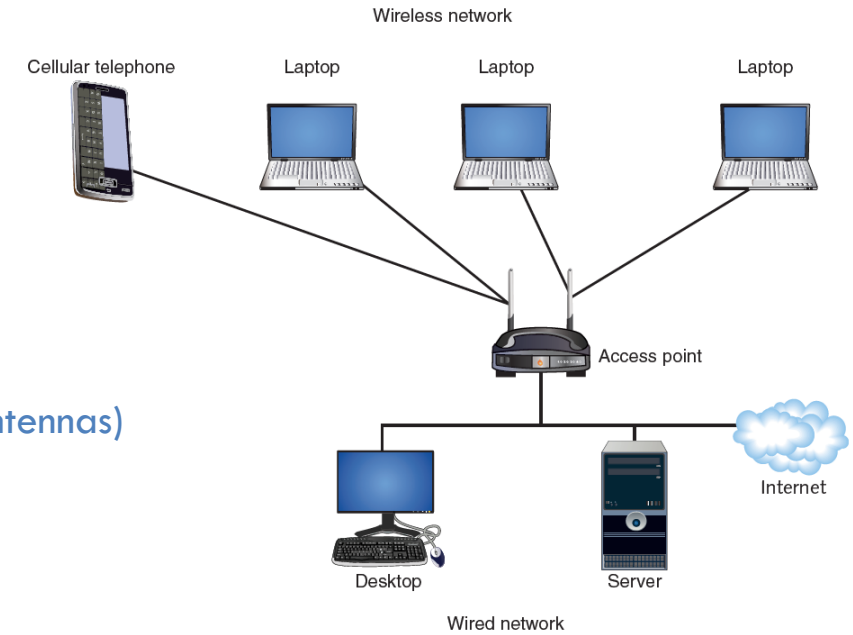
Remote Desktop Protocol (RDP)

- Proprietary Microsoft protocol that allows user to access another remote computer over network and perform tasks on it as if they were sitting at remote computer
  - It provides remote display and input capabilities over network connections for Windows-based applications running on server
- RDP is designed to support different types of networks and protocols



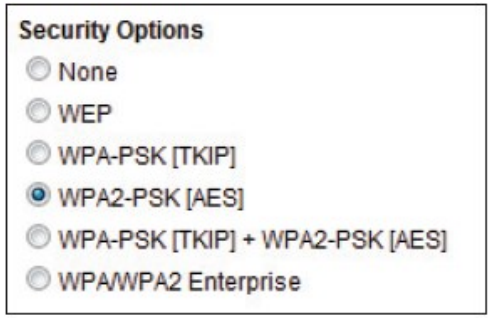
Basic Network Setup

- Client Connections
  - Wired network needs network interface card (NIC) or client network adapter (RJ-45 connection)
  - Wireless network needs wireless client network interface card
- Network Hardware
  - Internet (broadband) Modem (modulator-demodulator)
  - Router (configured to enable DHCP server and if needed port forwarding)
  - Wireless Access Point (AP)
    - Ad hoc mode: devices send/receive network traffic only between themselves
    - Infrastructure mode: ability to access remote computers and Internet
    - Serves as bridge between the wireless and wired networks
    - Acts as "base station" for wireless network where all wireless devices transmit to AP, which in turn redirects signal to other wireless devices or Internet
    - Use antennas that radiate out signal in all directions (called omnidirectional antennas)



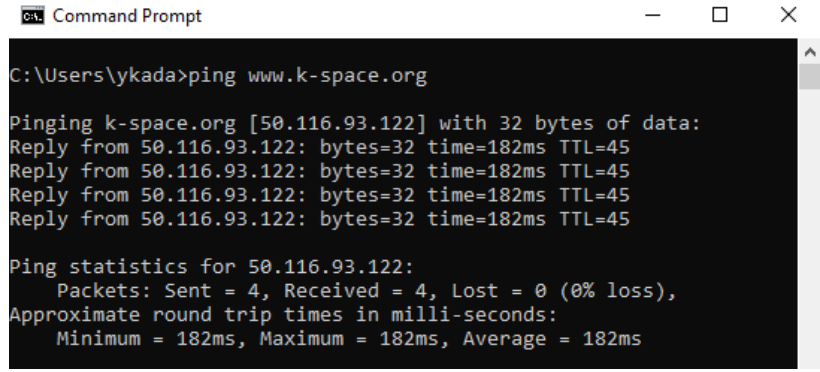
Access Point Security

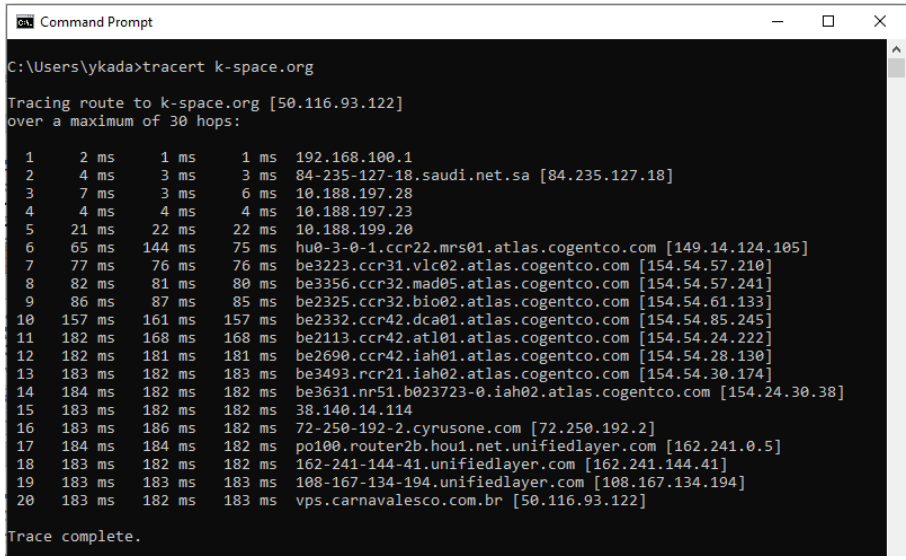
- Unlike wired networks restricted to cable in wall or buried underground, wireless networks do not have these boundaries and hence vulnerable targets for attackers
  - Attacker can easily intercept unencrypted wireless transmission and read private contents, steal passwords or even change message
  - Attackers with radio frequency jammer can flood network with wireless data and bring it to crash
- Recommended security settings on APs must be used to secure wireless network
  - Turn on Wi-Fi Protected Access 2 (WPA2)
  - Disable Service Set Identifier (SSID)
  - Center antenna placement
  - Reduce power levels
  - Create guest network



Network Troubleshooting

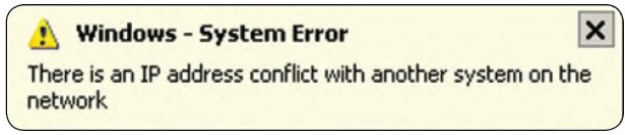
- Connectivity Problems
  - Almost half of all network problems are result of cabling or network devices (check physical damage/malfunction)
  - When network fails, it is important to take systematic approach to problem solving
    - Examining obvious solutions first before more technically advanced areas
  - If network loses connectivity to Internet, first check that network devices, like routers or APs, are receiving power
  - Another obvious check is whether Internet Service Provider (ISP) may be experiencing network problems
  - If all internal network devices are checked and are properly functioning, then use command-line utility 'ping' to check for connectivity outside organization
    - If sending ping command to two or more web sites results in message of 100% packet loss, then it may be indication connectivity problem is with ISP
  - To confirm problem is with ISP, command-line utility 'tracert' can be used, which displays route (path) that packet travels
    - Sending tracert command to web site can show where transmission stopped and if that device belonged to ISP



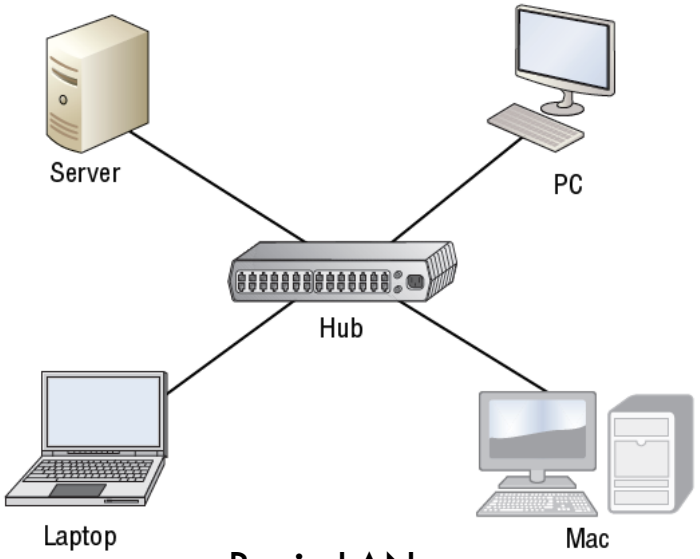


Network Troubleshooting

- IP Settings
  - Common cause of network problems that mainly result from incorrect selection of static IPs
    - Incorrect IP address
    - Same IP address assigned to two devices (IP conflict)
  - To help identify this problem, command-line utility 'ipconfig/all' can be used
    - Lists all of IP settings for device, such as IP address, address of DHCP server, and address of router

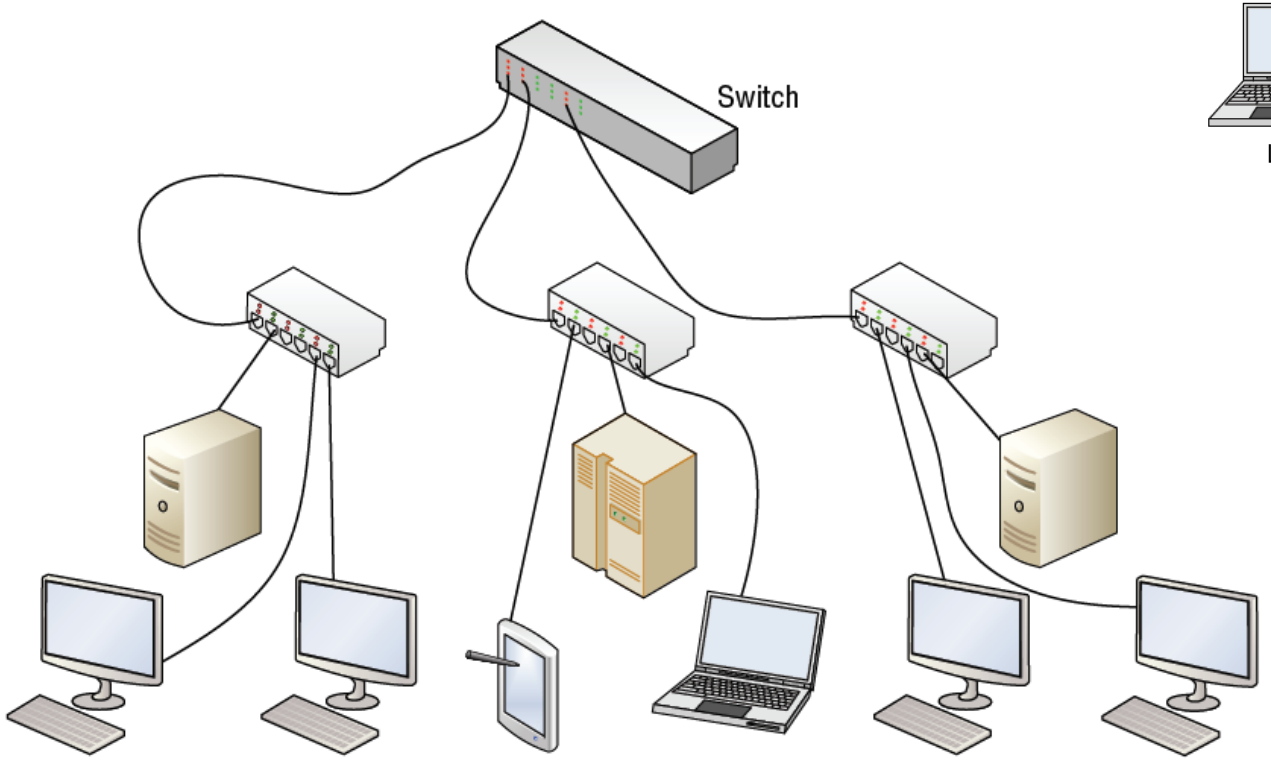


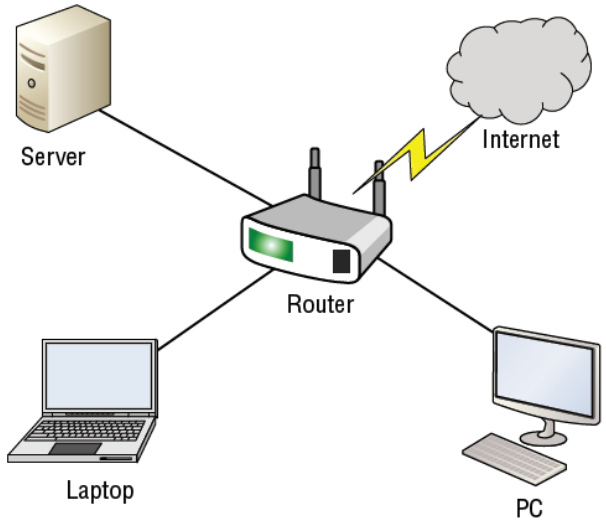
Local Area Network Types



Basic LAN

Advanced LAN

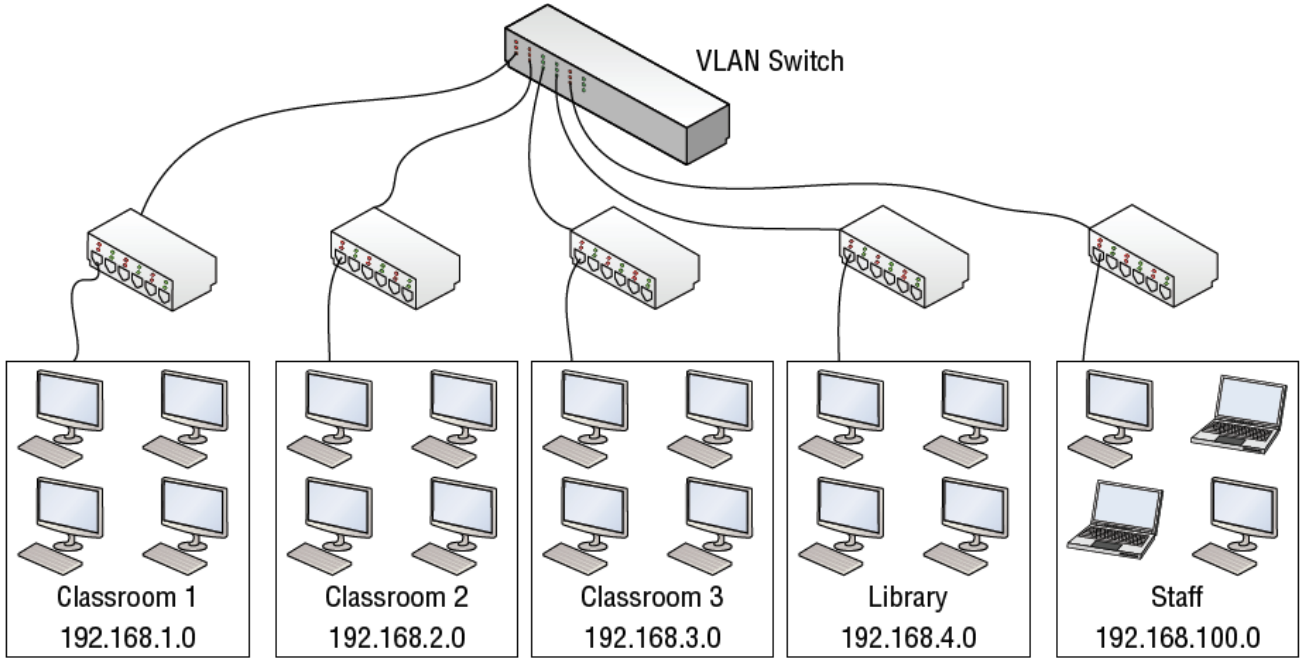




Intermediate LAN

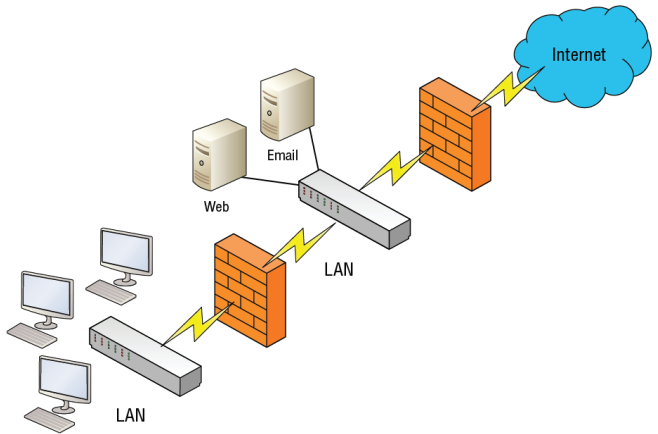
Virtual LAN (VLAN)

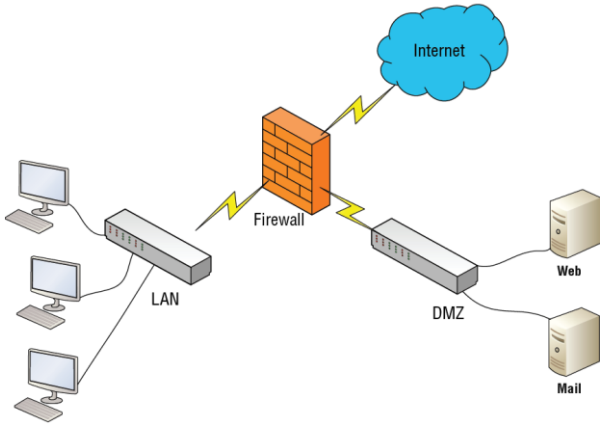
- Group of hosts with common set of requirements that communicate as if they were connected together in normal fashion on one switch, regardless of their physical location
  - VLAN is implemented to segment network, reduce collisions, organize network, boost performance, and increase security
- Like subnetting, VLAN compartmentalizes network and can isolate traffic
  - But unlike subnetting, VLAN can be set up in physical manner such as port-based VLAN



Perimeter Network (Demilitarized Zone) [DMZ]

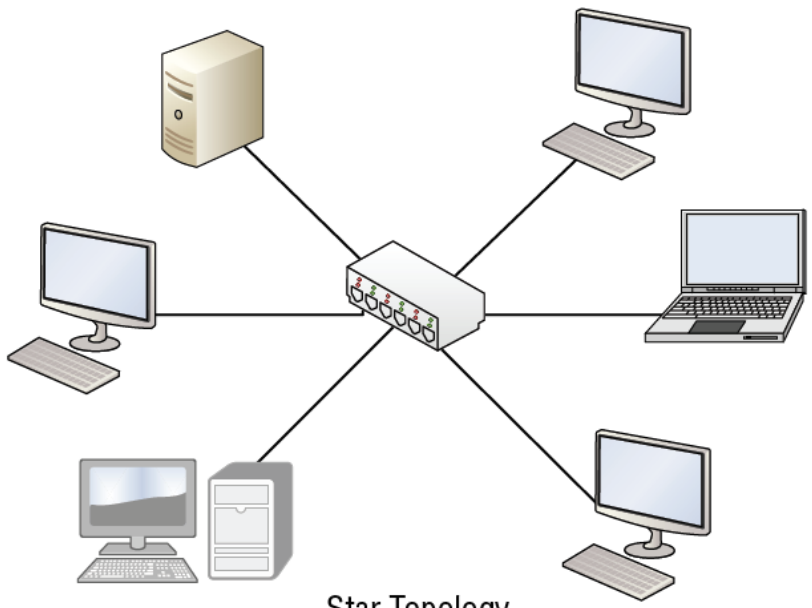
- Small network set up separately from company's private LAN and Internet
  - Called perimeter network because it is usually on edge of LAN, but DMZ has become much more popular term
- DMZ allows users outside of company LAN to access specific services located on DMZ (e.g., email, web)
  - However, those users are blocked from gaining access to company LAN
  - Users on LAN will quite often connect to DMZ as well, but without having to worry about outside attackers gaining access to their private LAN
- Back-to-Back Configuration: DMZ situated in between two firewall devices
- 3-leg Perimeter Configuration: DMZ is usually attached to separate connection of company firewall
  - Firewall would have three connections: one to company LAN, one to DMZ, and one to Internet



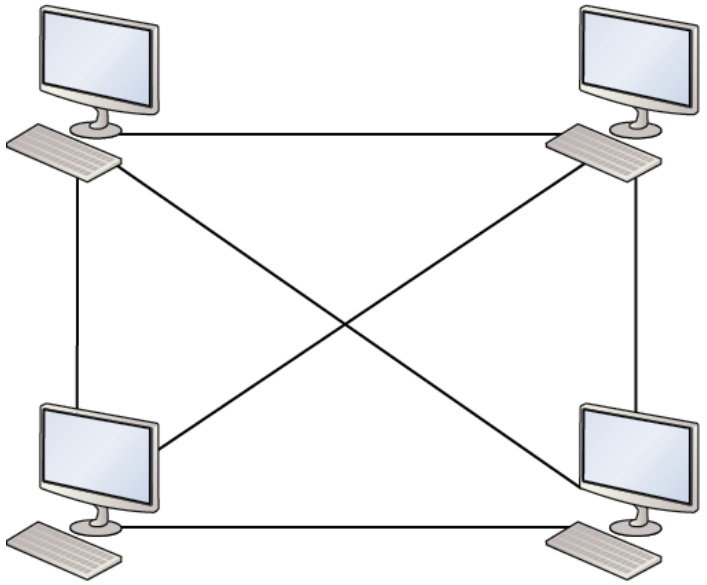


Network Physical Topology

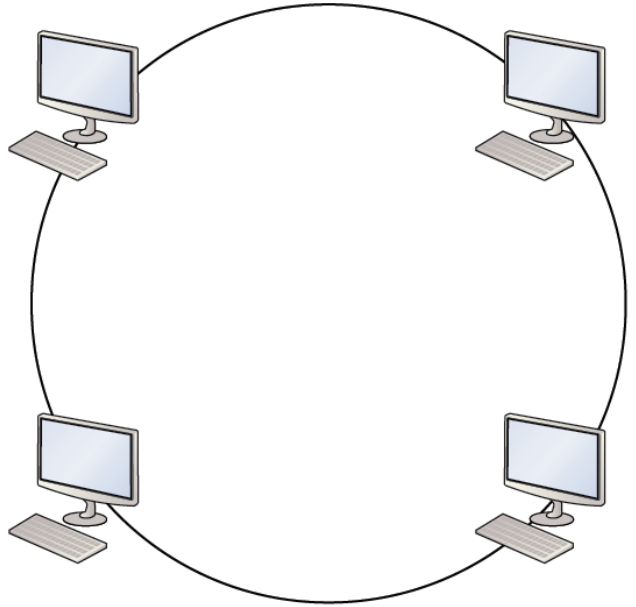
- By far, most common topology is star topology where each computer is individually connected to central connecting device (hub, switch, or router)
  - This type of topology is usually use when implementing networks
- Other topologies were introduced to minimize problem of data collisions
  - Modern ethernet technologies effectively minimize collisions
  - Cost and maintenance



Star Topology



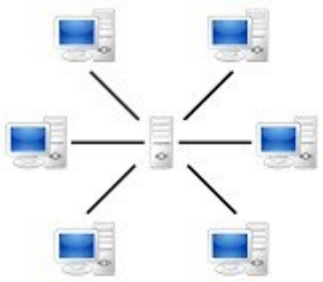
Mesh Topology



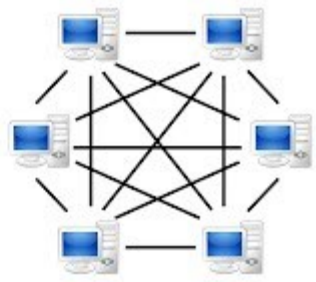
Ring Topology

Client/Server vs. Peer-to-Peer Models

- Most common types of distributed networks
  - Every device or workstation has its own processing power
- Client/server model architecture distributes applications/processing between servers
  - Extremely common in today's LANs, as with most applications used when connecting to Internet
  - Examples: web browser (client) and web server, mail client and mail server
  - Sometimes, it is more efficient to not use server, particularly with very small number of users
- Peer-to-peer (P2P) networking: each computer treated as equal in ability to serve and access data
  - Usually works well enough for smaller organizations
  - One peer usually acts as sort of pseudo-server, but additional resources, such as files, databases, printers, and so on, could be added to any other computer on network
  - Main disadvantage:no centralized user database



Server-based



P2P-network

Reference Material

- Mark Ciampa, Mark Revels, *Introduction to Healthcare Information Technology*, Cengage Learning, 2012.
  - Chapter 4
- Crystal Panek, *Networking Fundamentals*, Sybex, 2020.
  - Chapter 15