NETWORKING
A Beginner’s Guide

Understanding Network Jobs

- Network Administrator
  - Creating, maintaining, and removing user accounts
  - Ensuring necessary backups are made
  - Managing the "keys" to the network, such as the administrative accounts and passwords
  - Managing network security policies
  - Adding new networking equipment (servers, routers, hubs, etc…)
  - Monitoring the network for utilization levels and potential problems
  - Troubleshooting network problems (usually quickly!)

Networking Jobs

- Network Engineer
  - More deeply involved in the bits and bytes of the network
  - Typically degreed in electrical engineering
  - Expected to be experts in the network operating systems with which they work
  - Troubleshooters of last resort
  - Diagnose and fix the most vexing problems
  - At least 5 years of experience, with certifications (e.g. Cisco)

Networking Jobs

- Network Architect/Designer
  - Usually work for companies that sell and support networks for large companies
  - Design networks
  - Need to combine important qualities to be successful
    - Understanding business needs
    - Knowledge of networking products
    - Knowledge of how various products interact

The Business of Networking

- The Corporate Perspective
  - What Does the Company Need?
    - For Each Key Area of the Business, ask:
      - What is their function for the company?
      - How do their objectives tie into the company objectives?
      - What are the key short-term and long-term goals?
      - What are the chief challenges to overcome in achieving their objectives?
      - How might IT pay a role in supporting their objectives?
      - How is the work in their area accomplished?

Networking Jobs

- Many opportunities
- Demand for trained, capable networking people is extremely high
- Salaries are top-notch
- Jobs are – for the most part – fun, stimulating, and rewarding in many ways

Laying the Foundation

- Bits, Nibbles, and Bytes
  - Binary Digit – bit (0 or 1)
  - Byte – string of eight bits together
  - Kilobit – string of 1,000 bits together
- Understanding Binary Numbers
  - We use the base-10 numbering system
  - Computers use the base-2 numbering system

Understanding Binary Numbers

- 1 represents *on,* 0 represents *off*
- Values of the lowest eight positions used in the binary numbering system:
  - 128 64 32 16 8 4 2 1
  - So, suppose that you encounter the following binary number:
  - 1 0 1 0 1 1 0 1

Binary Numbers

- 128 64 32 16 8 4 2 1
- 1 0 1 0 1 1 0 1
- Represents:
  - (128x1)+(64x0)+(32x1)+(16x0)+(18x1)+(4x1)+(2x0)+(1x1)
- Which = 173, therefore the base -2 binary number 10101101 represents 173 in base-10

Terminology to Describe Network Speeds

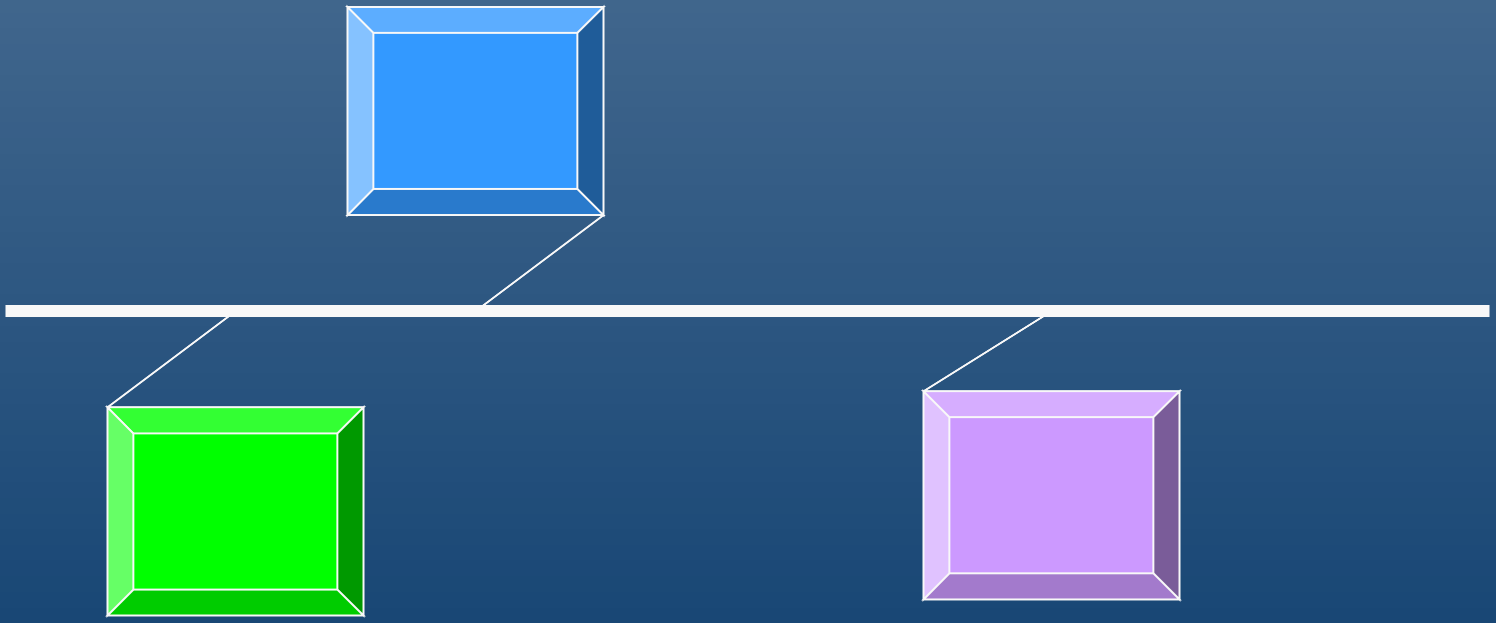
- Networking is almost entirely about moving data from one point to another.
- Broadly speaking this is *bandwidth* – which is a measure of the amount of data that a connection can carry in a given period of time
- Common measurement of *bandwidth* is *bits per second*, abbreviated as *bps*
- Kbps – thousands of bits per second
- Mbps – millions of bits per second
- Gbps – billions of bits per second

Understanding Networks

- Network Relationship Types
  - Peer-to-Peer (P2P): is a relationship in which computers on the network communicate with each other as equals. Each computer is also responsible for setting up and maintaining it own security.
  - Client/Server: is a relationship which a distinction exists between the computers that make available network resources (*servers*) and the computers that use the resources (*clients/workstations*)

A peer-to-peer network

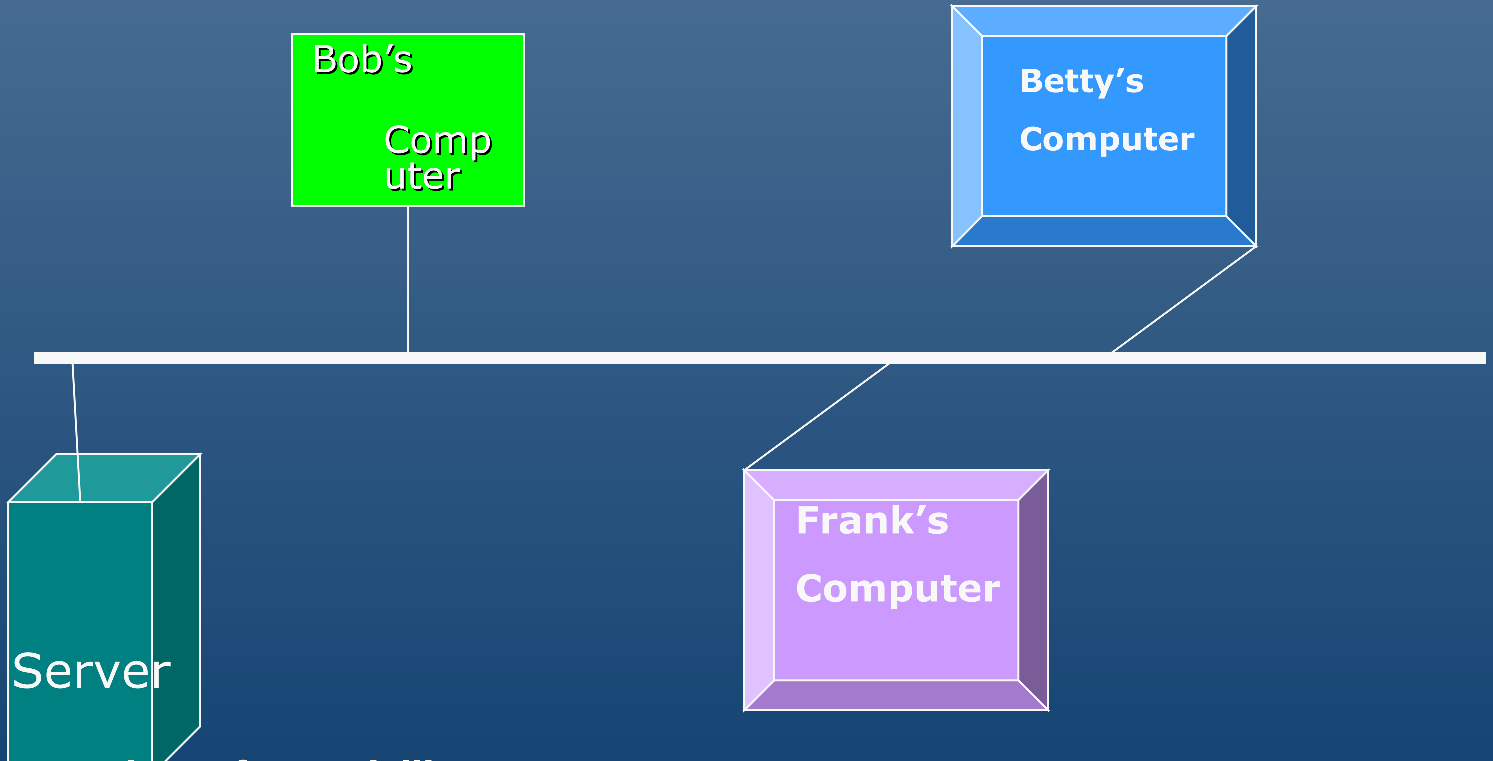
Frank’s computer
- Accounting system (shared)
- Documents (private)



Bob’s computer
- Customer proposals (private)
- Marketing software (shared)

Betty’s computer
- Employee reviews (private)
- HR Software(private)

Client/Server Network keeps resources centralized



- Accounting software (all)
- Documents (Frank only)
- HR software (Betty only)
- Employee reviews (Betty only
- Marketing software (all)

Pros for Peer-to-Peer Networks

- Use less expensive computer hardware
- Easy to administer
- No Network Operating System (NOS) required
- More built-in redundancy

Cons for Peer-to-Peer Networks

- Might hurt user’s performance
- Not very secure
- Hard to back up
- Hard to maintain version control

Pros for Client/Server Networks

- Very secure
- Better performance
- Centralized backup
- Very reliable

Cons for Client/Server Networks

- Require professional administration
  - Even for small client/server networks, you need professional administration. Either you hire someone to fill this position, or you contract the services
- More hardware intensive
  - You need a server – “beefy computer”
  - You need a network operating system
  - You need client liceses

In a Nutshell

- Choose peer-to-peer network for smaller networks with fewer than 10-15 users
- Choose a client/server network for anything larger

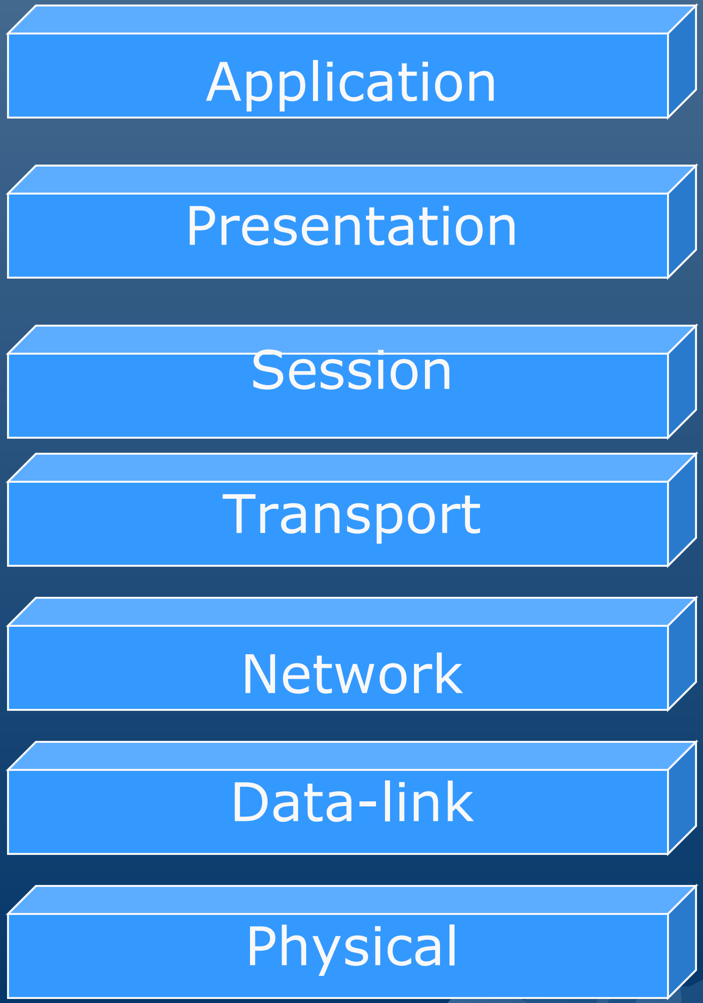
Network Features

- File Sharing
- Printer Sharing
- Application Services
- E-mail
- Remote Access
- Wide Area Networks (WAN)
- Internet and Intranet
- Network Security

The Open Systems Interconnection (OSI) Model

- The OSI model defines all the methods and protocols needed to connect one computer to any other over a network.
- The OSI model offers an excellent way to understand and visualize how computers network to each other.
- The OSI model separates the methods and protocols needed for a network connection into seven different *layers*.

The Seven Layers of the OSI Model



Application

Presentation

Session

Transport

Network

Data-link

Physical

Physical Layer

- The first layer, *the physical layer*, defines the properties of the physical medium used to make a network connection
- The physical connection can be either point-to-point, or multipoint
- It can consist of *half-duplex* (one direction at a time) or *full-duplex* (both directions simultaneously) transmissions.
- The bits can be transmitted either in series or in parallel (most networks use a serial stream of bits)
- A NIC (*network interface card*) is an example of the physical layer

Data-Link Layer

- The *data-link layer*, Layer 2, defines standards that assign meaning to the bits carried by the physical layer
- Includes error detection and correction to ensure a reliable data stream
- The data elements cared by the data-link layer are called *frames*

Data-Link Layer (continued)

- The *data-link layer* is subdivided into two sublayers
  - Logical link control (LLC)
  - Media access control (MAC)
- If used, the LLC layer performs tasks such as call setup and termination
- The MAC sublayer handles frame assembly, disassembly, error dection and correction, and addressing
- The most common MAC protocols are 802.3 Ethernet and 802.5 Token Ring
- On most systems, drivers for the NIC perform the work done at the data-link layer

Network Layer

- The *network layer*, Layer 3, is where a lot of action goes on for most networks.
- The *network layer* defines how data *packets* get from one point to another on a network and what goes into each packet.
- The network layer defines different packet protocols, such as Internet Protocol (IP) and Internet Protocol Exchange (IPX)

Network Layer (continued)

- *Routers* – hardware devices that examine each packet and, from their source and destination addresses, send the packets to their proper destination
- The *network layer* is also known as the *packet layer*.

Transport Layer

- The *transport layer*, Layer 4, manages the flow of information from one network node to another.
- It insures that the packets are decoded in the proper sequence and that all packets are received.
- It identifies each computer or node on a network uniquely.
- Examples of transport layer protocols include Transmission Control Protocol (TCP) and Sequenced Packet Exchange (SPX) – each used in concert with IP and IPX, respectively.

Session Layer

- The *session layer*, Layer 5, defines the connection from a user computer to a network server, or from a peer computer on a network to another peer computer.
- These virtual connections are referred to as *sessions*.

Presentation Layer

- The *presentation layer*, Layer 6, takes the data supplied by the lower-level layers and transforms it so it can be presented to the system.
- The functions that can take place at the presentation layer can include data compression and decompression, as well as data encryption and decryption

Application Layer

- The *application layer*, Layer 7, controls how the operating system and its applications interact with the network.
- An example of software at the application layer is the network client software you use, such as Windows Client for Microsoft Networks, the Windows Client for Novell Networks, or Novell’s Client32 software.

How Data Travels Through the OSI Layers

- Data flows from an application program or the operating system, through the protocols and devices that make up the seven layers until the data arrives at the physical layer and is transmitted over the network connection.
- The computer at the receiving end reverses this process

Understanding How Data Travels

- At each stage of the OSI Model, the data is “wrapped” with new control information related to the work done at that particular layer, leaving the previous layers’ information intact and wrapped within the new control information.
- The control information is different for each layer, but includes *headers, trailers, preambles*, and *postambles.*

Network Hardware Components

- Servers – any computer that performs network functions for other computers
  - File and print servers
  - Application servers
  - E-mail servers
  - Internet servers
  - Remote access servers

Network Hardware Components

- Hubs – sometimes called a *concentrator*, is a device that connects a number of network cables coming from client computers to a network.
  - All the network connections on a hub share a single *collision domain*, which means they “talk” over a single logical wire and are subject to interference from other computers connected to the same hub.

Network Hardware Components

- Switch – a *switch* is wired very similarly to a hub, and looks like a hub.
  - However, on a switch, all of the network connections are on their own collision domain. The switch makes each network connection a private one.
  - Often switches will be used to connect many hubs to a single network backbone.

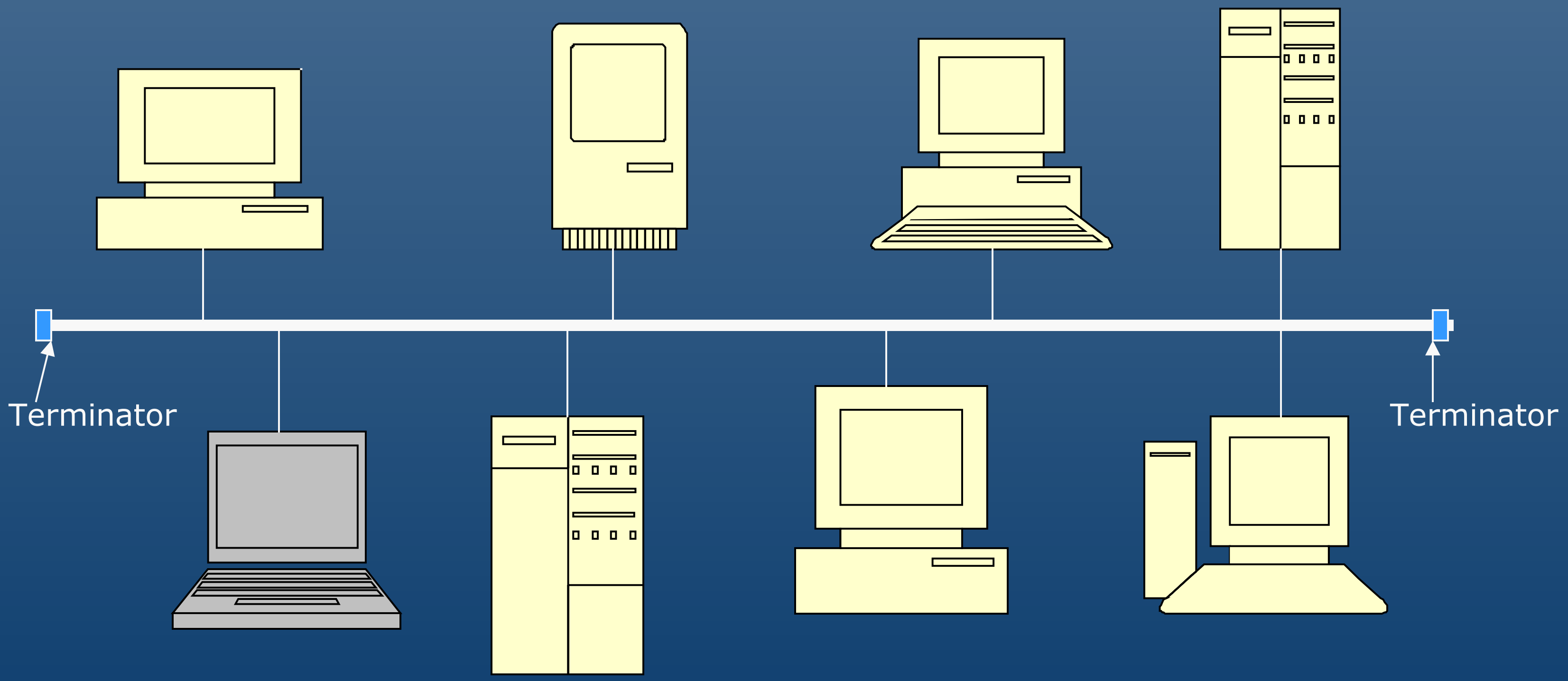
Network Hardware Components

- Cabling and Cable Plants
  - The most common network cable for LANs is Category 5 (Cat-5) twisted-pair cable.
  - Cat-5 cable is used to support 100Base-T Ethernet networks.
  - The term *cable plants* refers to the entire installation of all your network cable (e.g., cable, connectors, wall plates, patch panels, etc.)
- Workstation Hardware
  - NIC (network interface card)

Understanding Cable Topologies

- *Topology* basically means shape, the term network topology refers to the shape of a network
  - *Bus Topology is a network when one single network cable is used from one end of the network to the other, with different network devices (called* nodes) *connected to the cable at different locations.*

A Simple Bus Topology Network



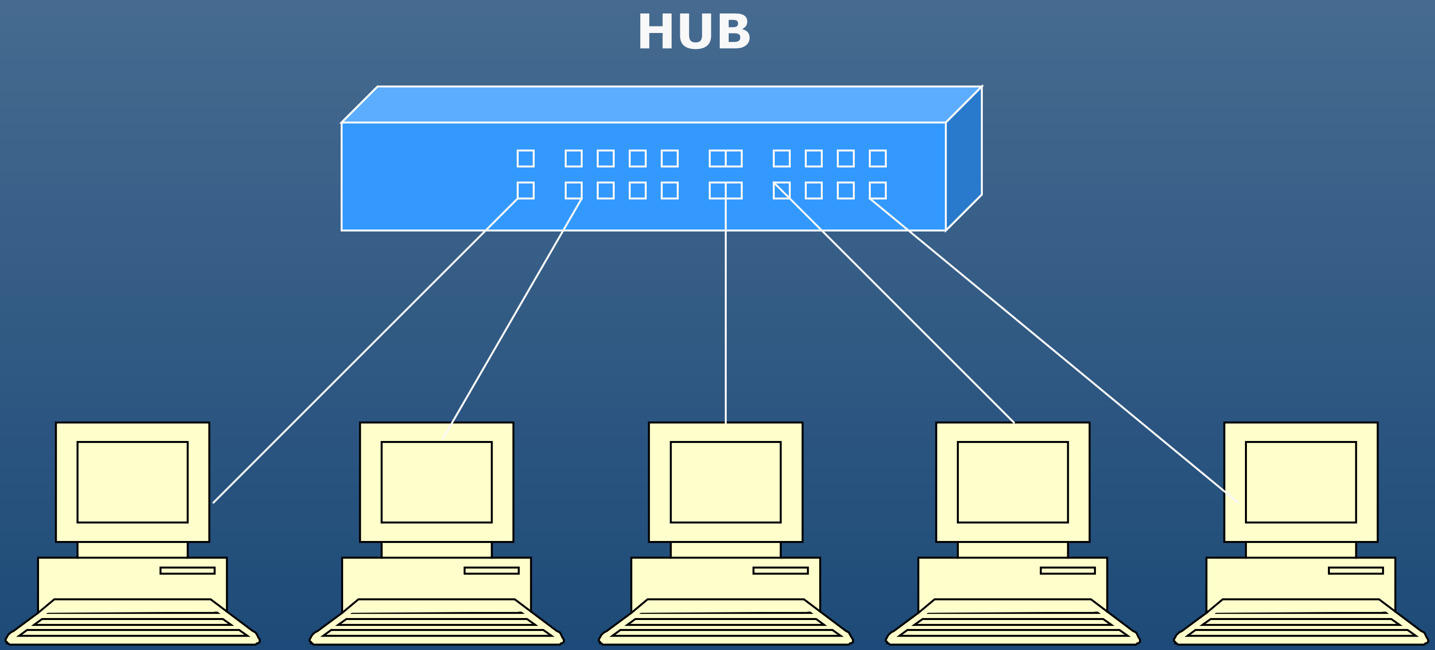
Bus Topology

- Different types of bus networks have different specifications, which include:
  - How many nodes can be in a single segment
  - How many segments can be used through the use of *repeaters* (electrically boost the signal on the cable)
  - How close the nodes can be to each other
  - The total length of a segment
  - Which coax cable type is required
  - How the ends of the bus must be terminated

Star Topology

- A *star topology* is one which a central unit, called a *hub* or *concentrator*, hosts a set of network cables that radiate out to each node on the network.
  - All network traffic used on any network connections to the hub is echoed to all the other connected nodes on that particular hub.
  - Because of this, all the bandwidth of any single node’s connection is shared with all other node’s connections

A Star Topology Network



Ring Topology

- A ring topology is actually not a physical arrangement of a network cable, as you might guess. Instead, rings are a logical arrangement, with the cables wired in a star, with each node connected on its own cable to the MAU (multistation access unit/hub)
- Electrically the network behaves like a ring.
- Ring topology LANs are based on Token Ring instead of Ethernet

Basic Cable Types

- Unshielded Twisted Pair (UTP)
  - The most common used today
- Shielded Twisted Pair (STP)
  - Has a braided metal shield surrounding the twisted pairs to further reduce the chance of interference from electrical sources outside the cable
- Fiber Optic
  - Uses a glass strand and carries the data signals as light instead of electricity
  - Can span great distances
- Coaxial
  - Consists of a central copper conductor wrapped in plastic insulation, which is surrounded by a braided wire shield and finally wrapped in a plastic cable sheath

Installing and Maintaining Network Cabling

- A proper cable plant installation should include:
  - Proper cable and connectors for the type of network, including documentation of what components were used
  - Complete labeling of all parts of the network – very important for troubleshooting
  - An *as-built* drawing of the building showing all the cabling routes and locations
  - A certification report showing that all the installed cables operate properly - using a special network test device

Understanding Network Hardware

- Repeaters
- Hubs and concentrators
- Switches
- Bridges
- Routers
- Gateways
- Firewalls
- Short-haul modems for short inter-building connections

Network Hardware

- Repeaters
  - Extend the distance that network traffic can travel
  - Mostly used on 10-Base2 networks (Thin Ethernet), but are available for virtually any network connection
  - Only to be used on the same type of media, such as Token Ring twisted pair to Token Ring twisted pair

Network Hardware

- Hubs and concentrators
  - Used to connect nodes to one another
  - Echo all data for each port to all the other ports on the hub
  - Hubs have *automatic partitioning*, where the hub can automatically *partition* or “cut off” any node having trouble from the other nodes
  - Can be purchased in a variety of sizes (2-100)
  - Are becoming increasing sophisticated: with auto-sensing different connection speeds, built-in bridging, routing and switching functions

Network Hardware

- Switches
  - Switch connections from one port to another rapidly
  - Think of them as a train yard with many trains coming in on some tracks and leaving on other tracks, and the switch being the yard manager – instead of trains being switched its packets.
  - Because switches form one-to-one connections between any two ports, all the ports coming into a switch are not all part of a single collision domain.
  - Switches are inexpensive and blazingly fast. For LAN connections, switches make more sense than routers.

Network Hardware

- Bridges
  - Bridges are more intelligent versions of repeaters. They can connect two network segments together, but they have the intelligence to pass traffic from one segment to another *only when that traffic is destined for the other segment.*
  - Used to segment networks into smaller pieces
  - Sometimes used to span different networking systems (e.g., coaxial Thin Ethernet to twisted-pair Token Ring)
  - Operate on Layer 2 (data-link layer) and they examine the MAC address of each packet they encounter to determine whether they should forward the packet to the other network

Network Hardware

- Routers
  - Routers are more intelligent bridges.
  - They operate on Layer 3 (network layer)
  - Routers can connect both similar and dissimilar networks, and are often used for WAN links
  - Routers become a node on a network, and have their own network address
  - They have fast (sometimes limited) microprocessors, and lots of memory
  - To learn about the networks to which they're connected, they use a process called *discovery (listening to traffic on its ports and sending out advertisement packets letting other devices know of the router's presence)*

Network Hardware

- Gateways
  - Gateways are application-specific interfaces that link all seven layers of the OSI Model when they are dissimilar at any or all levels.
  - The primary use for gateways today is for handling e-mail. POP3 and SMTP are two examples of mail-handling protocols that are handled by gateways.
  - Sometimes email servers handle the task of a gateway.

Networking Hardware

- Firewalls
  - Firewalls are hardware devices that enforce your network security policies.
  - Firewalls are often installed hand in hand with routers.
  - Generally firewalls are computers that sit between the Internet and the LAN
  - Two basic types: network-based (operating at the packet level using *packet filtering*) and application-based (*proxy firewall* ~ using a technique called *network address translation [NAT]*)