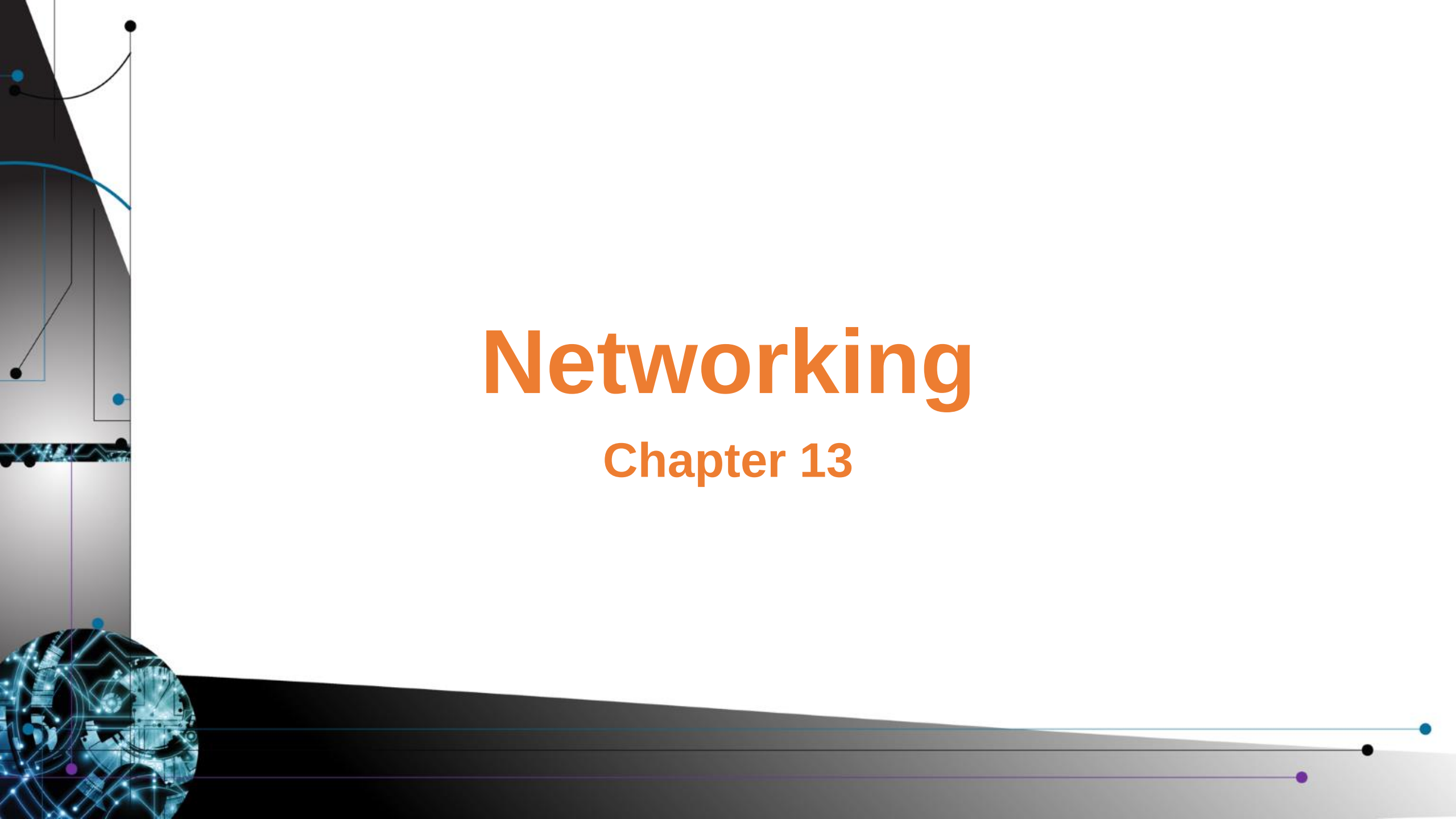


Networking

Chapter 13

This presentation covers:

- Being Proactive
- Networking Overview
- Network Media Overview
- Wireless Networks Overview
- Cloud Technologies

Qualities of a Good Technician

"Soft skills" as they are known across many industries are essential

Being Proactive

- Think of ways to improve a situation, anticipates problems, and fixes them before being told
- Follow up after a service call
- Provide a list of recommended solutions or procedural changes to the supervisor rather than waiting for the supervisor to delineate what changes must occur
- Have a list of “standard” software loaded on the computer such as the operating system, service pack level, and any applications that are standard throughout the institution
- Being proactive saves both the technician and the customer

Networking Overview

Networks Examples

- A network of roads and interstate highways
- A telephone network
- The electrical network that provides electricity to our homes
- The cellular network that allows cell phones/smartphones to connect to one another
- The air traffic control network
- Your network of friends and family

Types of Networks

Computers can attach to different types of networks:

- PAN (personal area network) – small wireless network such as a Bluetooth keyboard and mouse connecting to a PC
- LAN (local area network) – Share resources in a single area such as a room, home, or building
- MAN (metropolitan area network) – Spans a city such as multiple community college campuses
- WAN (wide area network) – Spans across a large geographic area

Types of Networks (cont.)

- WLAN (wireless LAN) – access point with wireless devices attached
- WWAN (wireless WAN) – can use a mix of technologies such as cellular or WiMax over a large geographic area
- WMN (wireless mesh network) – good for emergency situations for connectivity among rescue workers or in smart devices

Attaching to Different Types of Networks

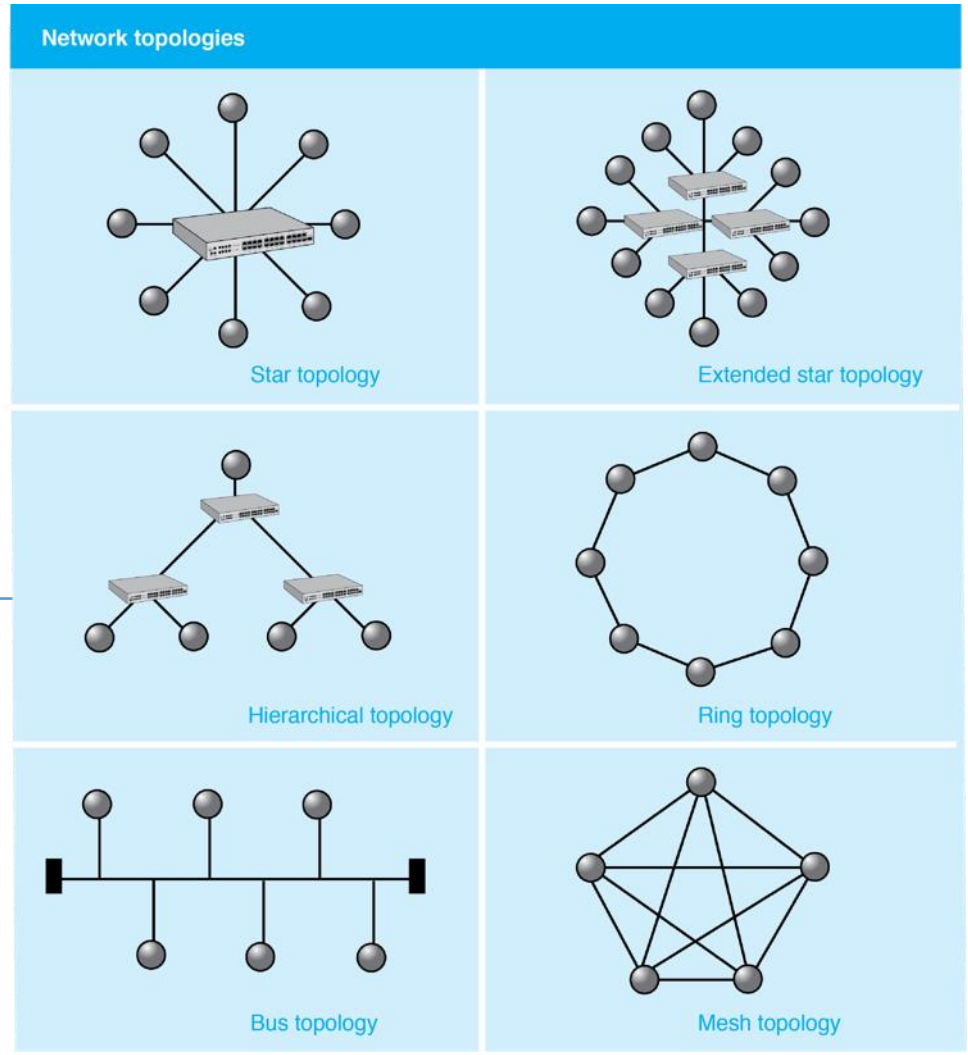
Computers can attach to different types of networks:

- A server-based network: computer users participate in a domain and log in to a main computer called a server where they are authenticated (authorized to use the network)
- A workgroup: Windows computers in a peer-to-peer network are known as a workgroup or
- A Microsoft HomeGroup: Microsoft calls a workgroup a HomeGroup in Windows 7, 8, and 10 (removed version 1803 and higher)
  - HomeGroup network is assigned a single password, and other devices within that HomeGroup simply need that password to access resources like files and photos.

Network Topologies

The physical network topology is how the network is wired

Network Topologies



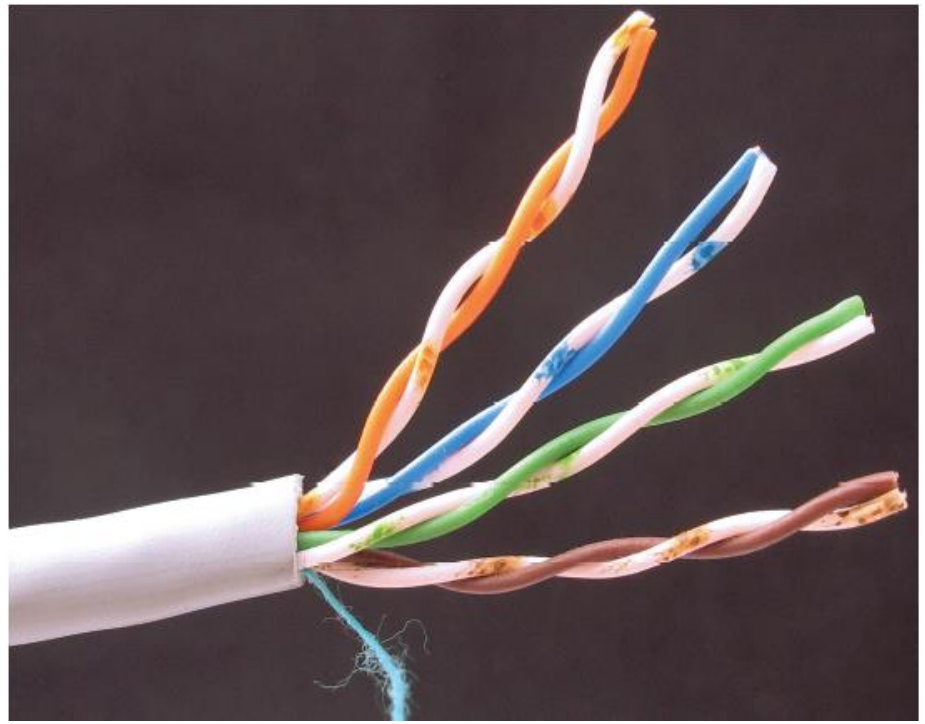
Network Media Overview

Copper Media

- Copper media is the most common cabling used to connect devices to the network
- Also used to connect network devices
- Copper media comes in two major types
  - Twisted pair
  - Coaxial

Twisted Pair Cable

- Twisted pair cable is named because each of the four pairs of conductors entwines around each other
- Twisted pair cable comes in two types
  - Shielded: STP (shielded twisted pair)
  - Unshielded: UTP (unshielded twisted pair)



UTP Cable

Twisted Pair Cable

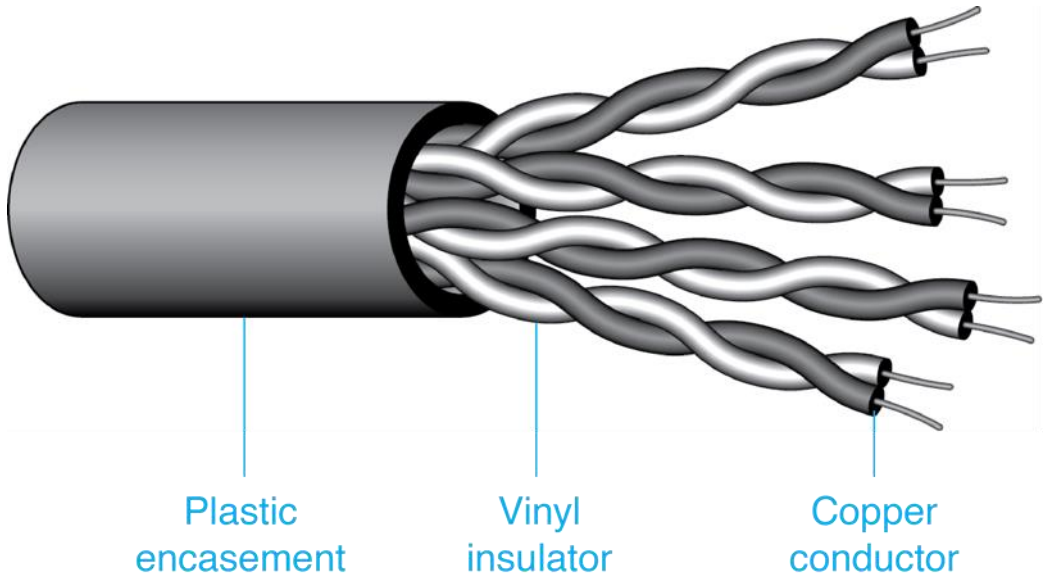
Shielded: STP (shielded twisted pair)

- Has extra foil that provides more shielding
- Used in industrial settings, such as a factory, where extra shielding is needed to prevent outside interference from interfering with the data on the cable

Twisted Pair Cable

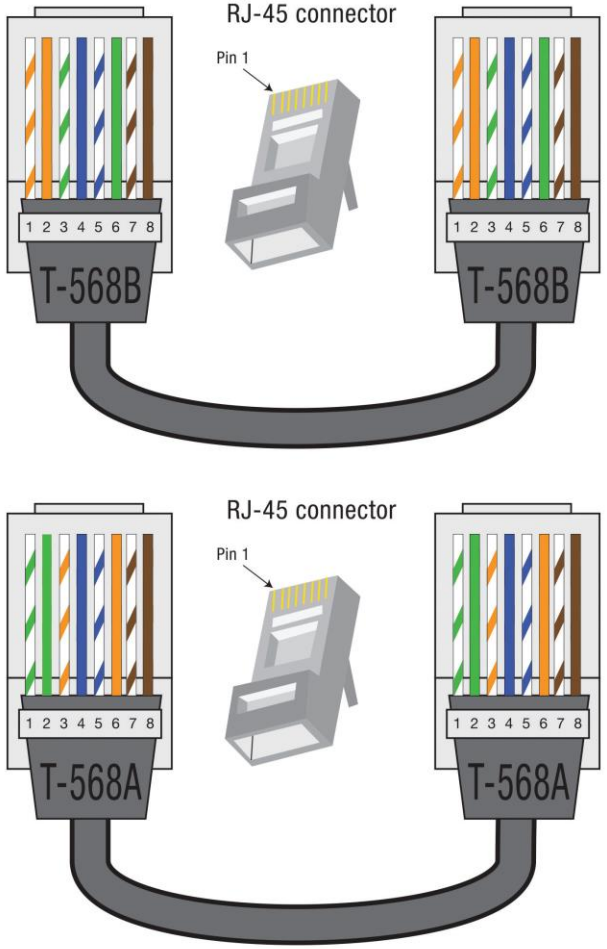
Unshielded: UTP (unshielded twisted pair)

- UTP is the most common
- Measured in gauges
- Most common are categories 5e, 6, and 7 – these are known as CAT 5e, CAT 6, CAT 7, etc.



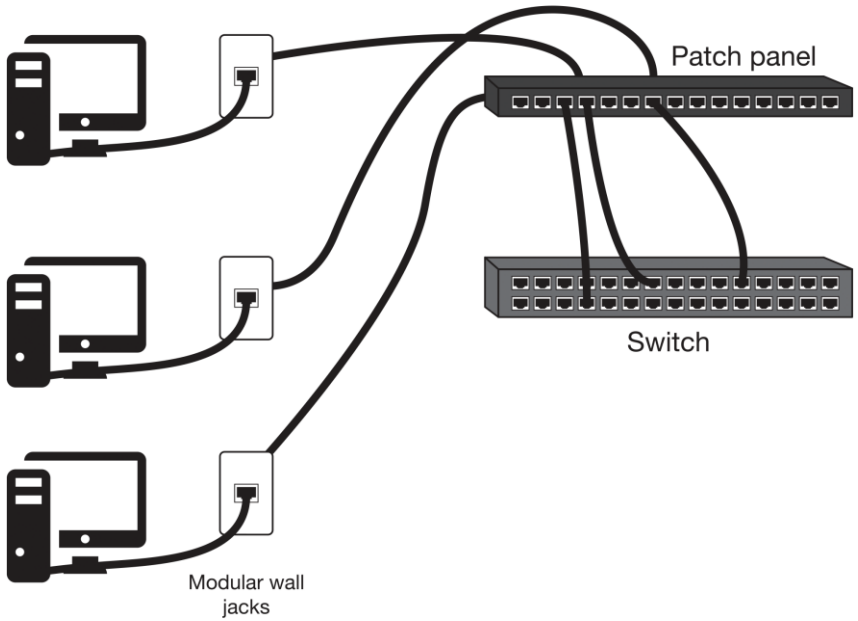
Twisted Pair Cable

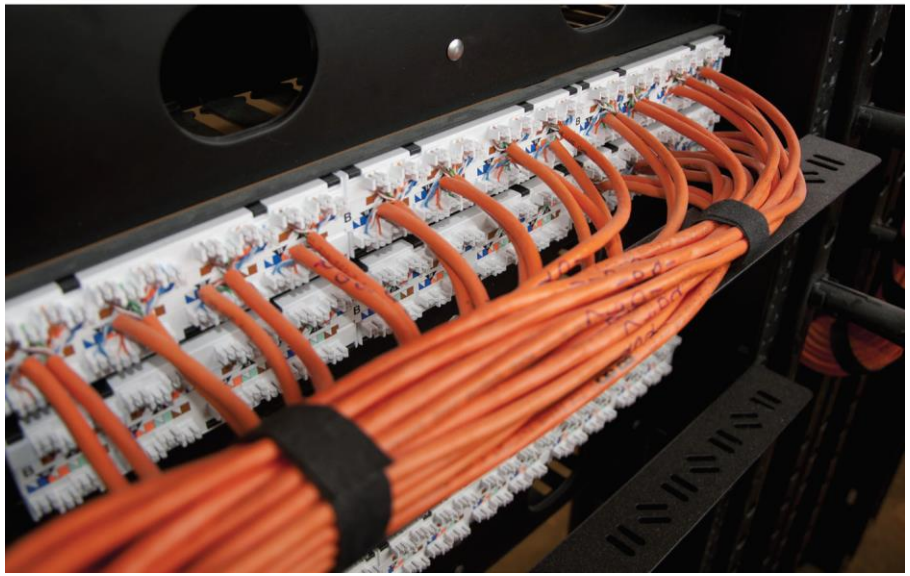
- Two wiring standards
  - T-568A
  - T-568B
- For most cabling both ends are wired the same.
- For a crossover cable between like devices like 2 PCs or two switches, one end is T-568A and the other end is T-568B.



Twisted Pair Cabling

> Corporate wiring is through a patch panel



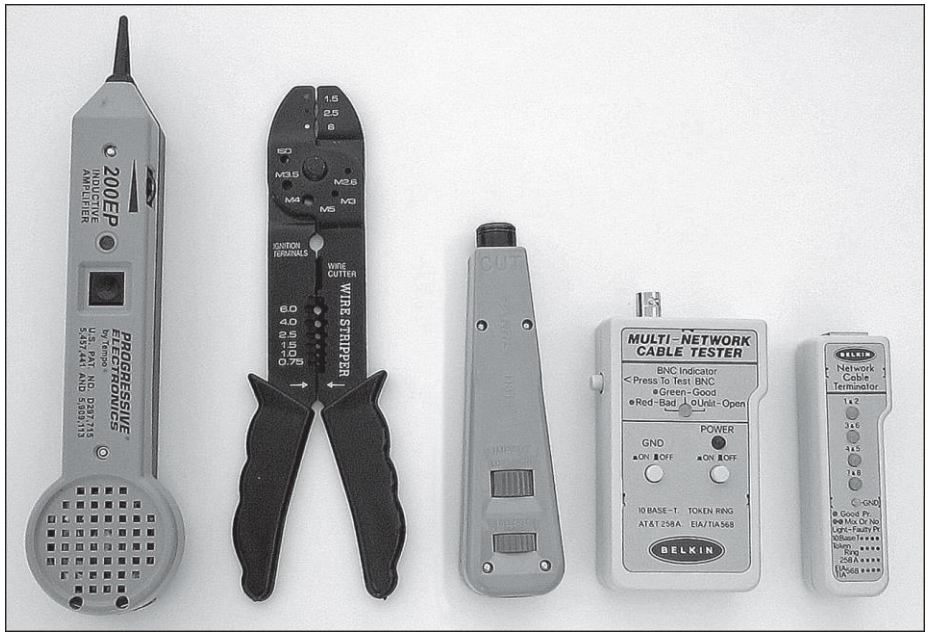


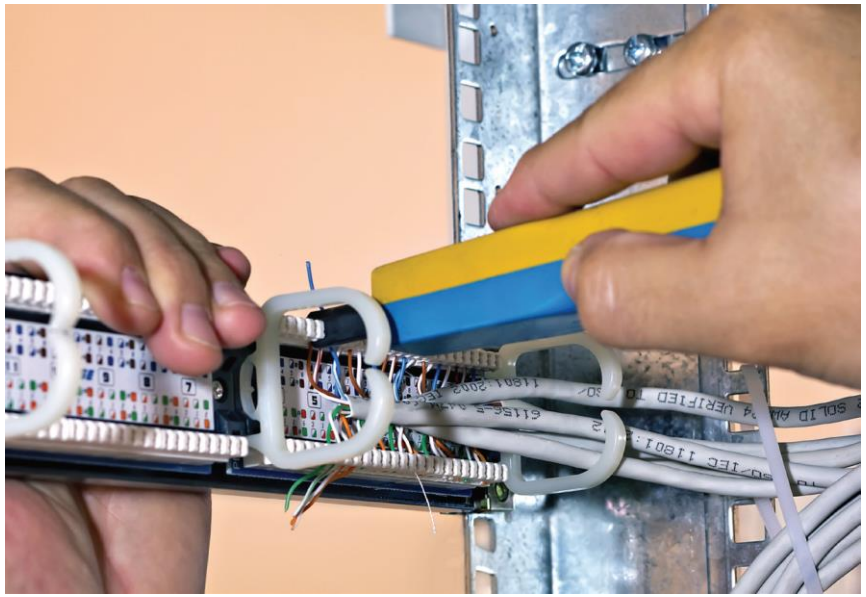
Protecting Your Network and Cable Investment

- Network devices should be locked in a secure room or cabinet when possible
- Network cable can be pulled through walls and over ceilings but should be installed in conduit or raceways if possible
- A professional cable management system can help keep network cables organized
- Ensure network cabling is not a trip or other safety hazard in any location

Network cabinets

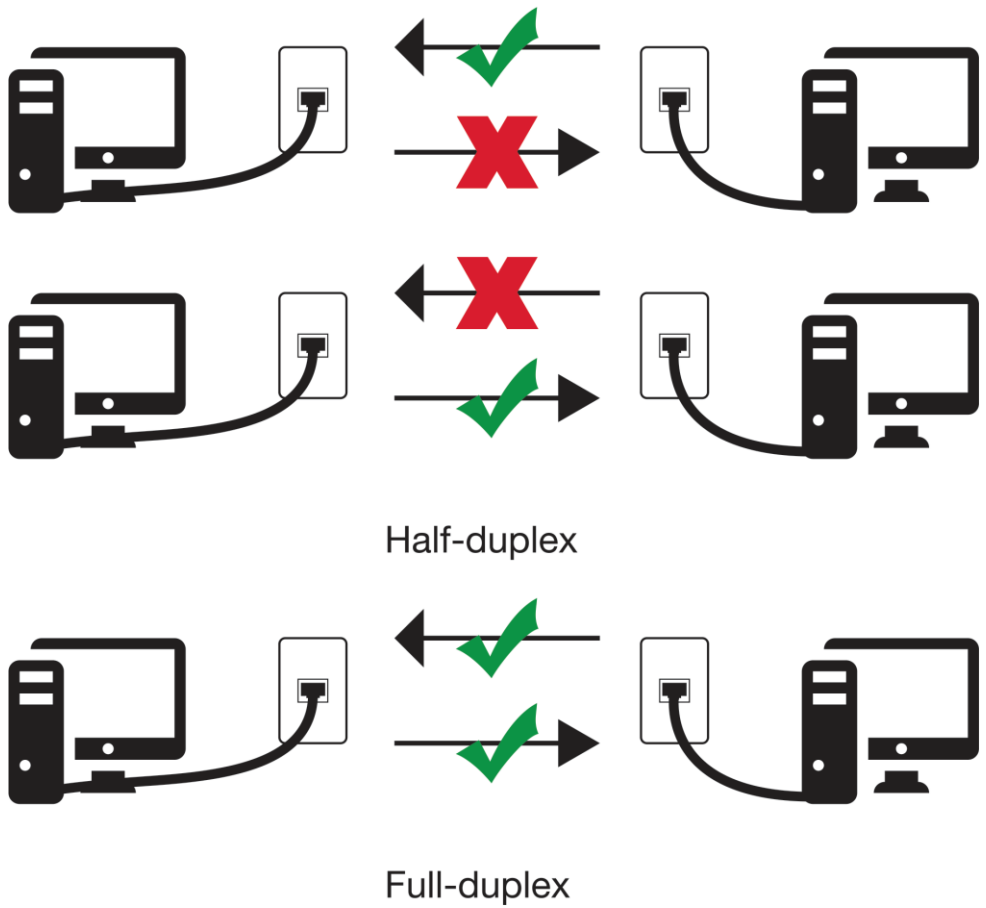
Network and Troubleshooting Tools





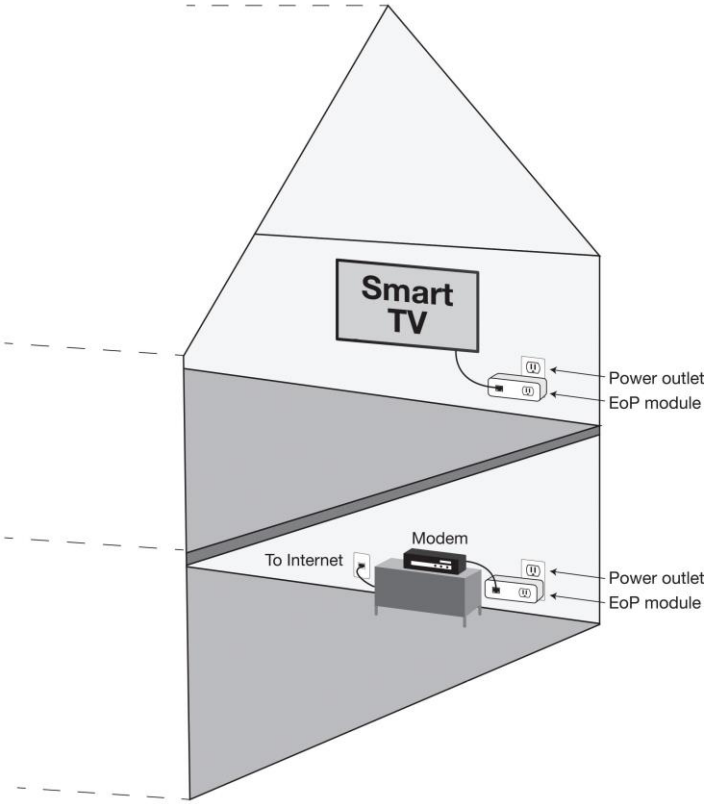
Ethernet Concepts

- Ethernet is the most common type of LAN
- Issues related to Ethernet include full-duplex and half-duplex transmissions, network slowdowns, and increasing bandwidth



Ethernet Over Power (EoP)

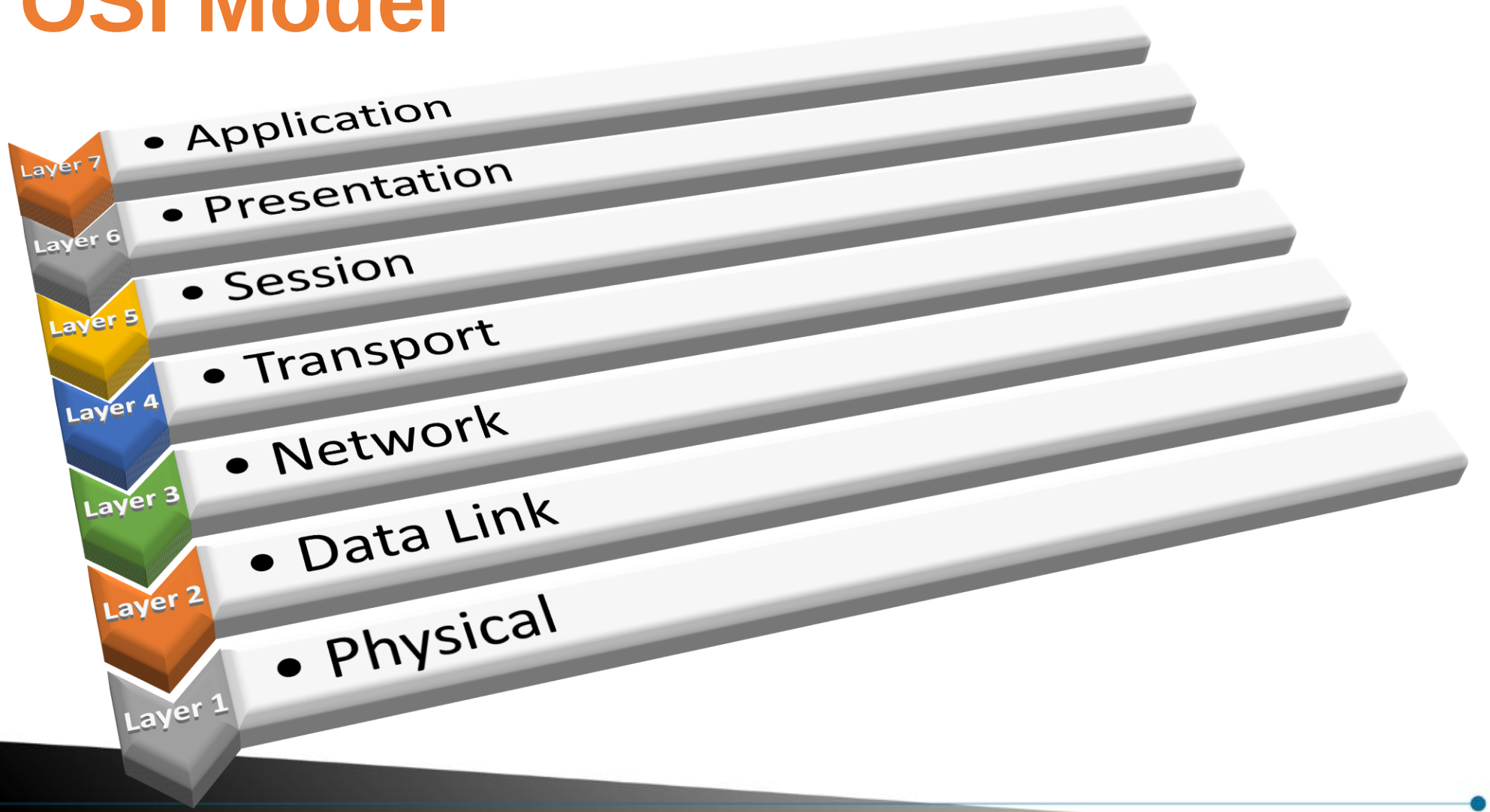
- Also called powerline communication
- A network is created by using EoP modules plugged in to power outlets to extend wired Ethernet or wireless networks.



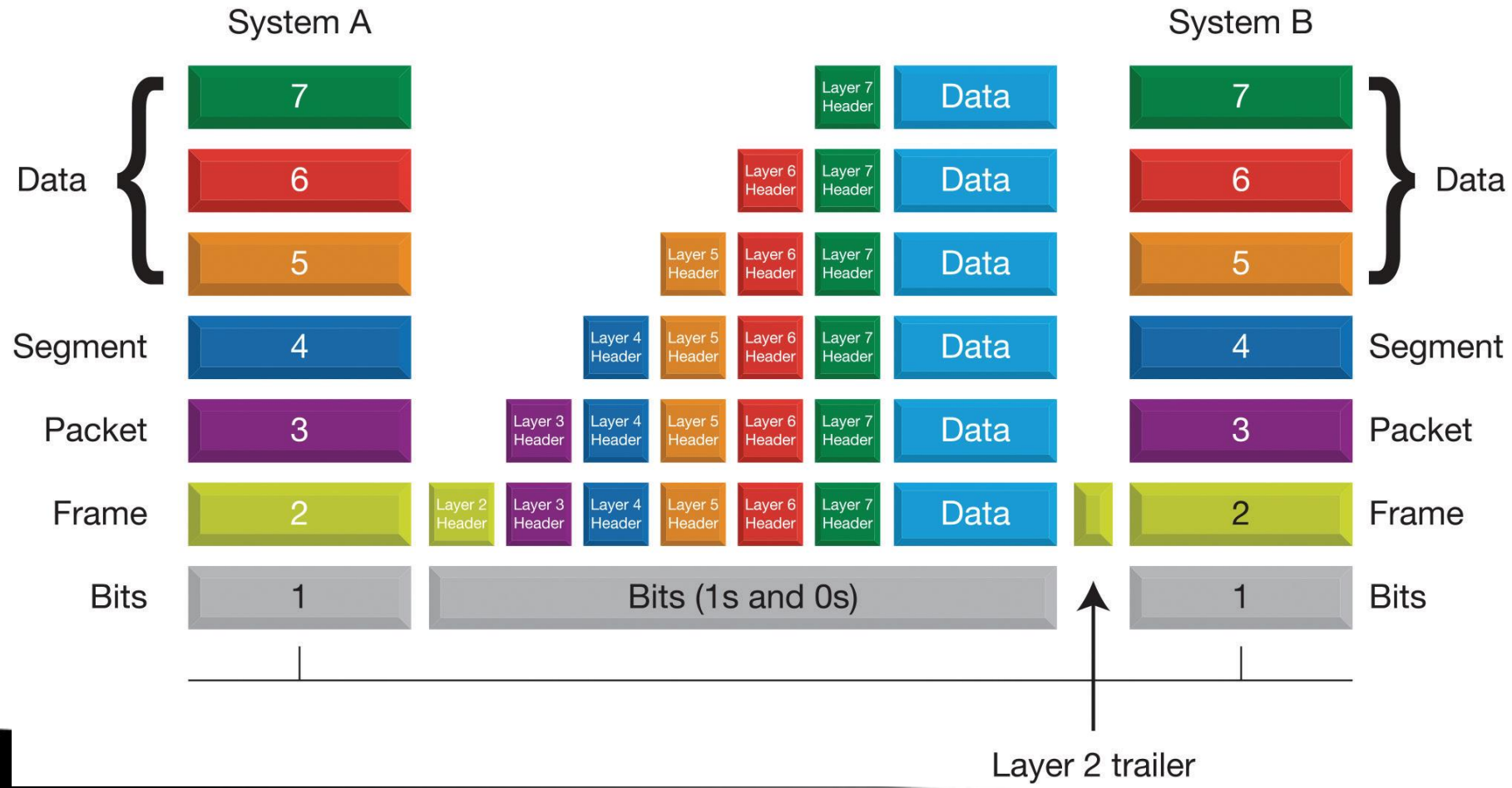
The OSI Model

- The International Organization for Standardization (ISO) developed a model for network communications known as the OSI (Open Systems Interconnect) model
- It is a standard for information transfer across the network
- The model sets several guidelines, including:
  - (1) how the different transmission media are arranged and interconnected
  - (2) how network devices that use different languages communicate with one another
  - (3) how a network device contacts another net-work device
  - (4) how and when data gets transmitted across the network
  - (5) how data is sent to the correct device
  - (6) how it is known if the network data was received properly

The OSI Model

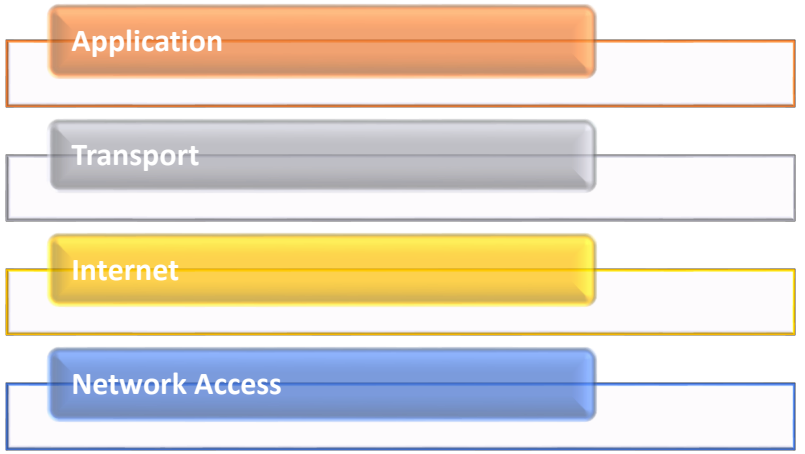


The OSI Model

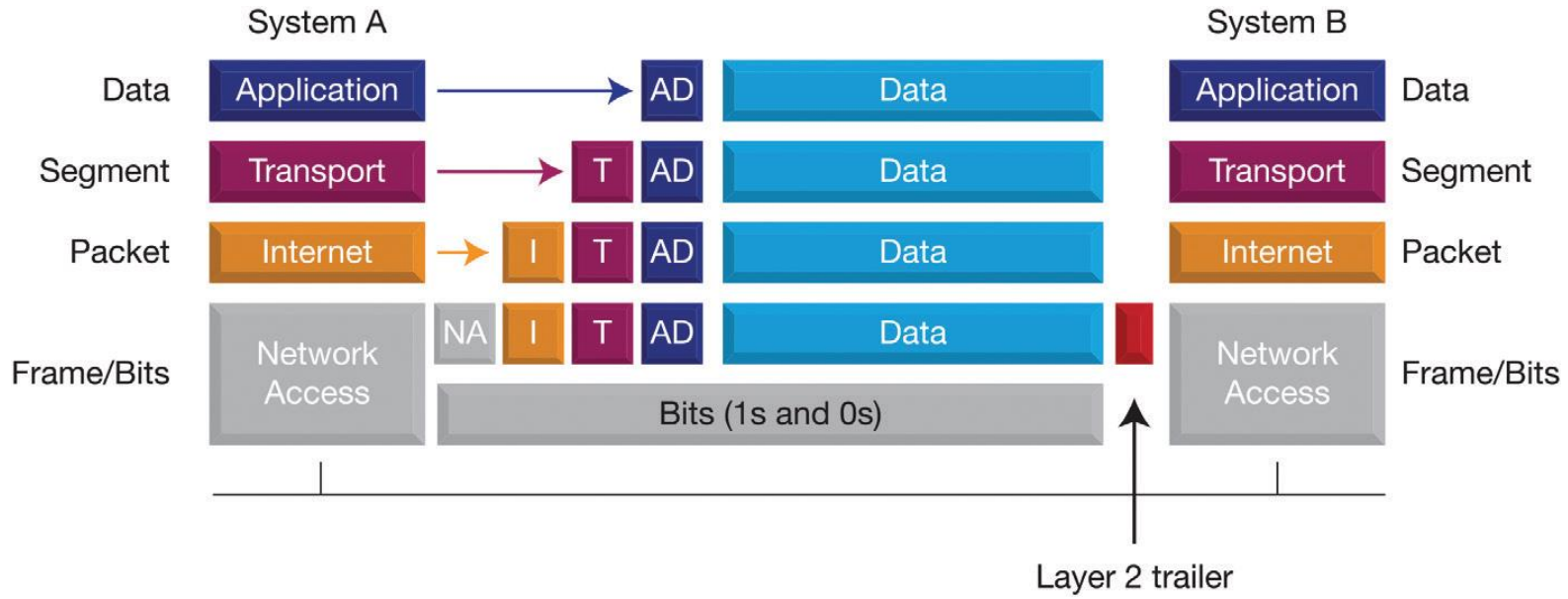


The TCP/IP Model

- A network protocol is a data communication language
- A protocol suite is a group of protocols that are designed to work together
- Transmission Control Protocol/ Internet Protocol (TCP/IP) is the protocol suite used in networks today



The TCP/IP Model



The TCP/IP Model

- It is the most common network protocol and is required when accessing the Internet
- The TCP/IP protocol suite consists of many protocols, including: Transmission Control Protocol (TCP), Internet Protocol (IP), Dynamic Host Configuration Protocol (DHCP), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP), to name a few

Network Addressing

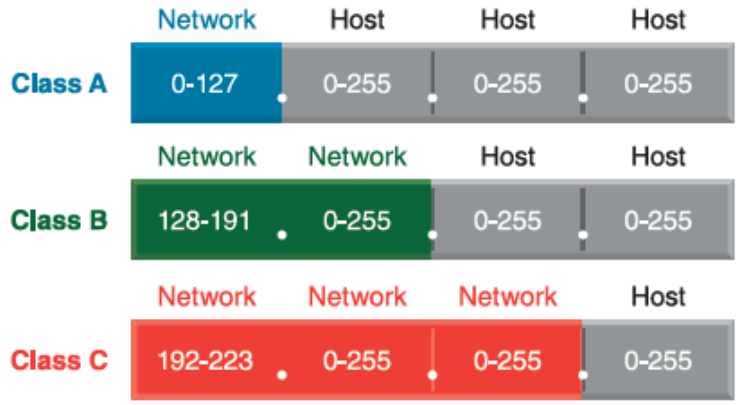
Network adapters normally have two types of addresses assigned to them:

- A MAC address: a 48-bit unique number that is burned into a chip located on a NIC and is represented in hexadecimal
- An IP address can be IPv4 (32 bits) or IPv6 (128 bits)
  - An IP address: is broken into two major parts
  - The network number: the portion of an IP address that represents which network the computer is on
  - The host number/address: represents the specific computer on the network

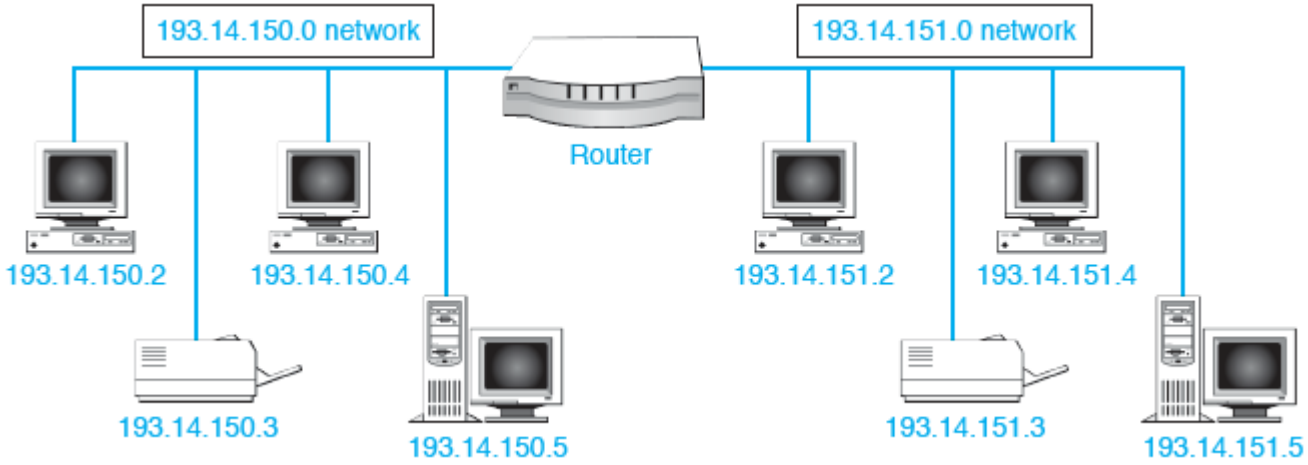
```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : gateway.2wire.net
   Link-local IPv6 Address . . . . . : fe80::13e:4586:5807:95f7%10
   IPv4 Address. . . . . . . . . . . : 192.168.1.64
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.254
```

Using IP Addresses



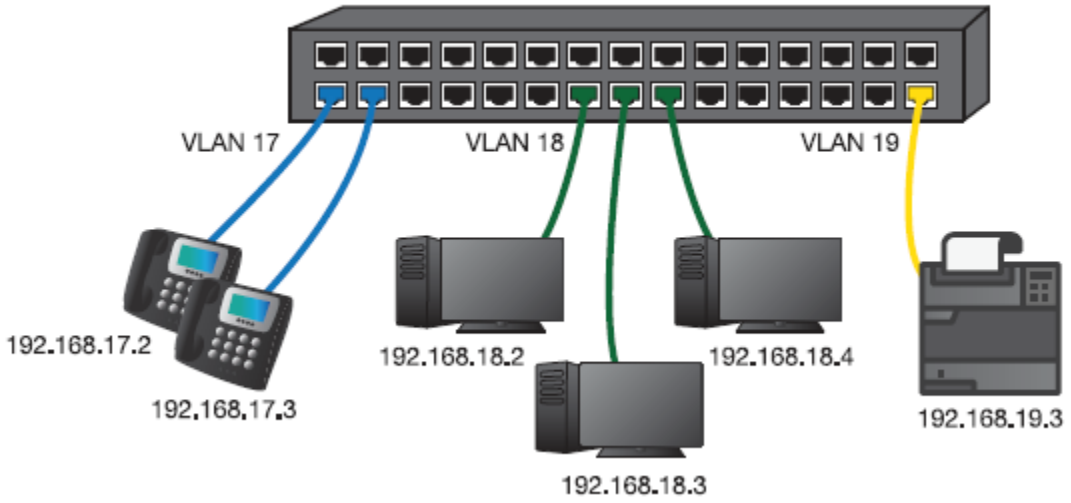
Classes of IP addresses



Two networks

VLANs

Some corporate switches can be programed with virtual LANs (VLANs). VLANs can be thought of as network numbers. Each VLAN number creates its own network.



Wireless Networks Overview

Wireless Networks

- Transmit data over air using either infrared (1- to 400THz range) or radio frequencies (2.4GHz or 5GHz range)
- Operate at Layers 1 and 2 of the OSI model

Bluetooth

- Wireless technology for PANs
- Devices include audio/visual products, automotive accessories, keyboards, mice, phones, printer adapters, and other small wireless devices
- Works in the 2.4GHz range, similarly to business wireless networks
- Has three classes of devices (1, 2, and 3) that have a range of less than 30 feet (less than 10 meters), 33 feet (10 meters), and 328 feet (100 meters)
- Newest version (5) supports longer distances, but not defined as to the max.

Wireless Network Standards

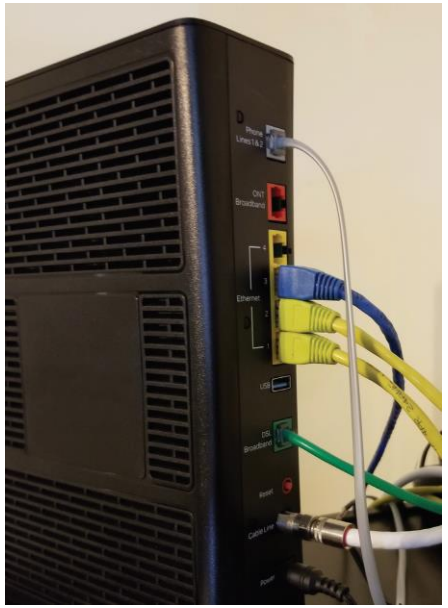
- 802.11a: Came after the 802.11b standard. Has speeds up to 54Mb/s but is incompatible with 802.11b. Operates in the 5GHz range.
- 802.11b: Operates in the 2.4000 and 2.4835GHz radio frequency ranges, with speeds up to 11Mb/s.
- 802.11e: Provides standards related to quality of service.
- 802.11g: Operates in the 2.4GHz range, with speeds up to 54Mb/s, and is backward compatible with 802.11b.

Wireless Network Standards, cont'd

- 802.11i: Relates to wireless network security and includes AES (Advanced Encryption Standard) for protecting data.
- 802.11n: Operates in the 2.4 and 5GHz ranges and is backward compatible with the older 802.11a, b, and g equipment. Speeds up to 600Mb/s using MIMO antennas. Maximum of 4 simultaneous data streams.
- 802.11ac: Operates only in the 5GHz range, which makes it backward compatible with 802.11n and 802.11a. Speeds up to 6.93Gb/s. Maximum of 8 simultaneous data streams using MU-MIMO antennas.
- 802.11ad: Also known as WiGig and works in the 60GHz range. Speeds up to 6.76Gb/s.

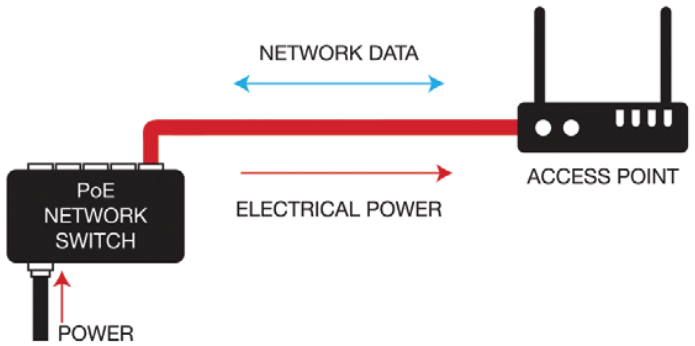
Wireless Devices

- AP (access point) – coordinates wireless connectivity for multiple devices
- Bridge – connects two or more networks
- NIC – allows a device to connect to a wireless network
- Router – connects a wireless network to another network (commonly a wired network or the Internet)

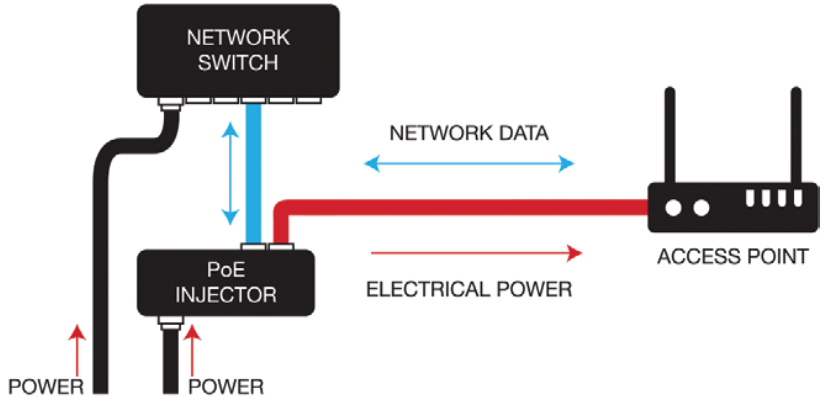


Power over Ethernet (PoE)

- Used in corporate environment to provide power to devices such as access points or IP phones



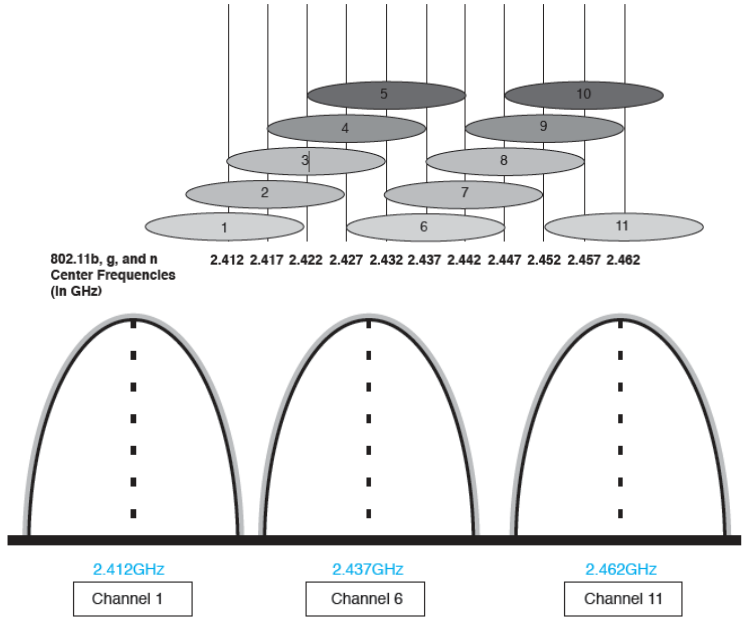
Power Over Ethernet (PoE)

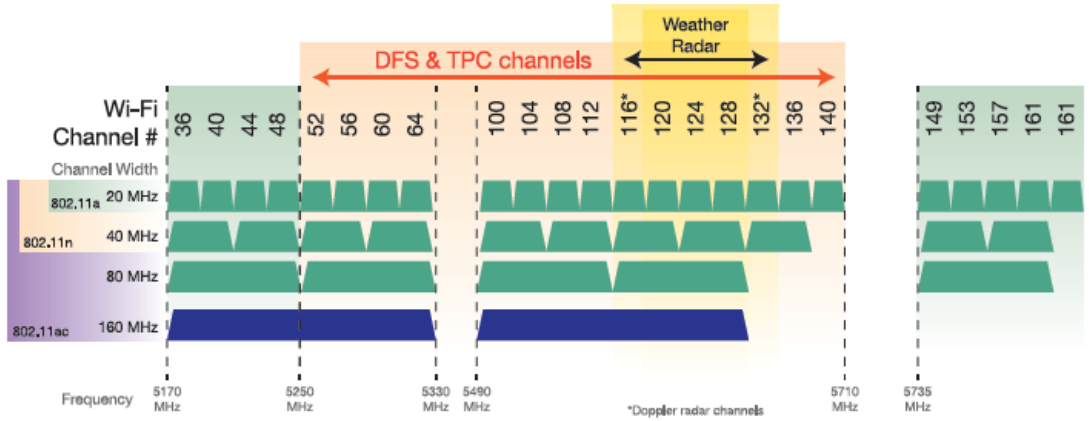


Power Over Ethernet injector

Wireless Channels

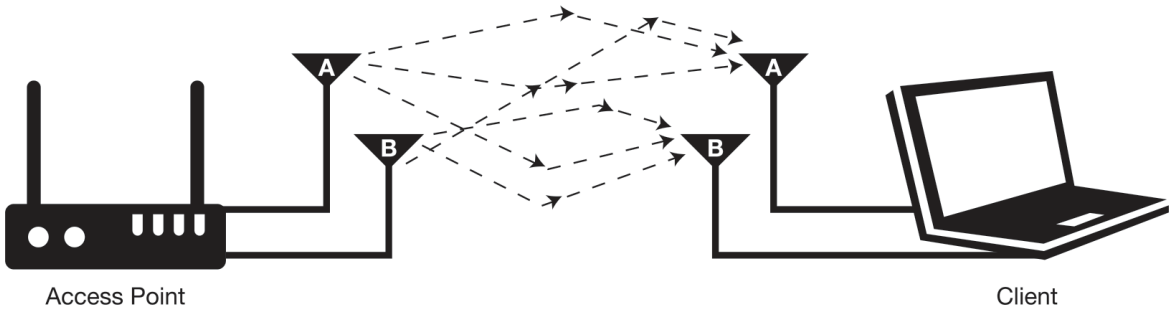
- Specific frequency used to create the wireless network
- Only devices on the same frequency are on the wireless network
  - Think of a radio channel



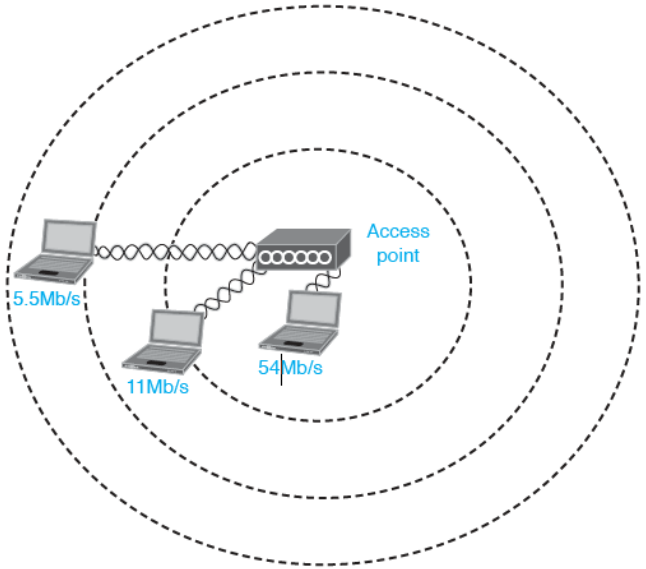


Wireless Transmissions

- Today's access points use multiple 2.4 GHz and/or 5 GHz MIMO antennas.



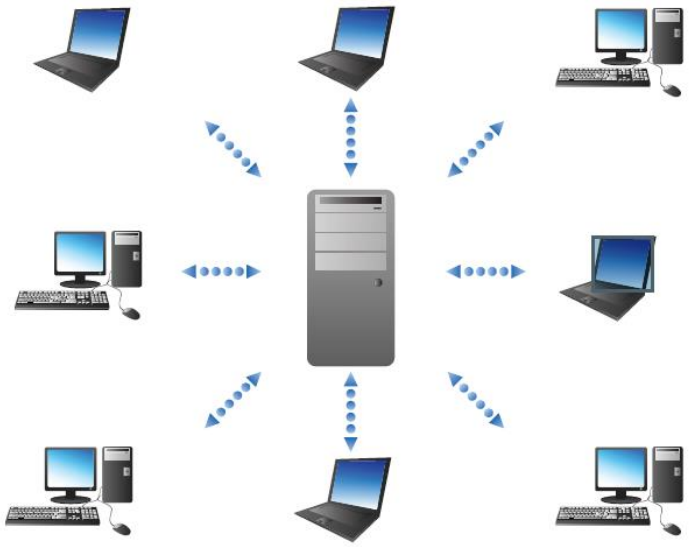
- The further away you are from the PA, the slower your device transmits.



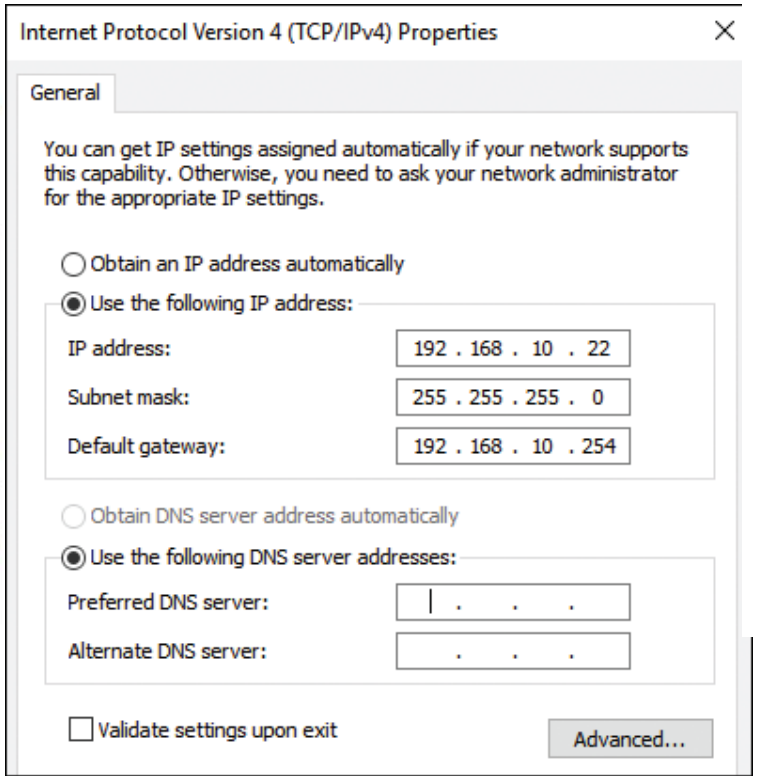
Wireless Security Options

End-User Device Configuration Overview

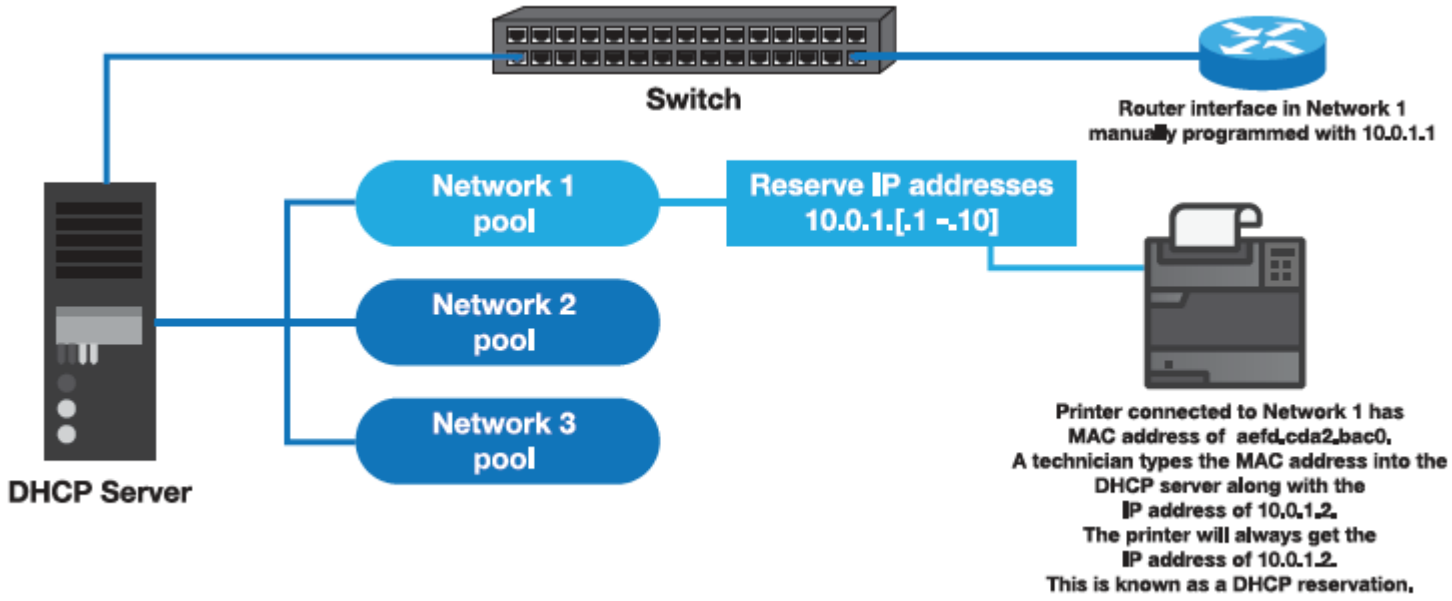
- Give the device a unique name and optionally join a workgroup or domain.
- Configure IP addressing – DHCP (automatic) or statically configure
- Optionally enable file and print sharing
- If a wireless device is being configured, you have to select the wireless network or configure the SSID and possibly enter security parameters.



IP Addressing Configuration



Static IP address configuration



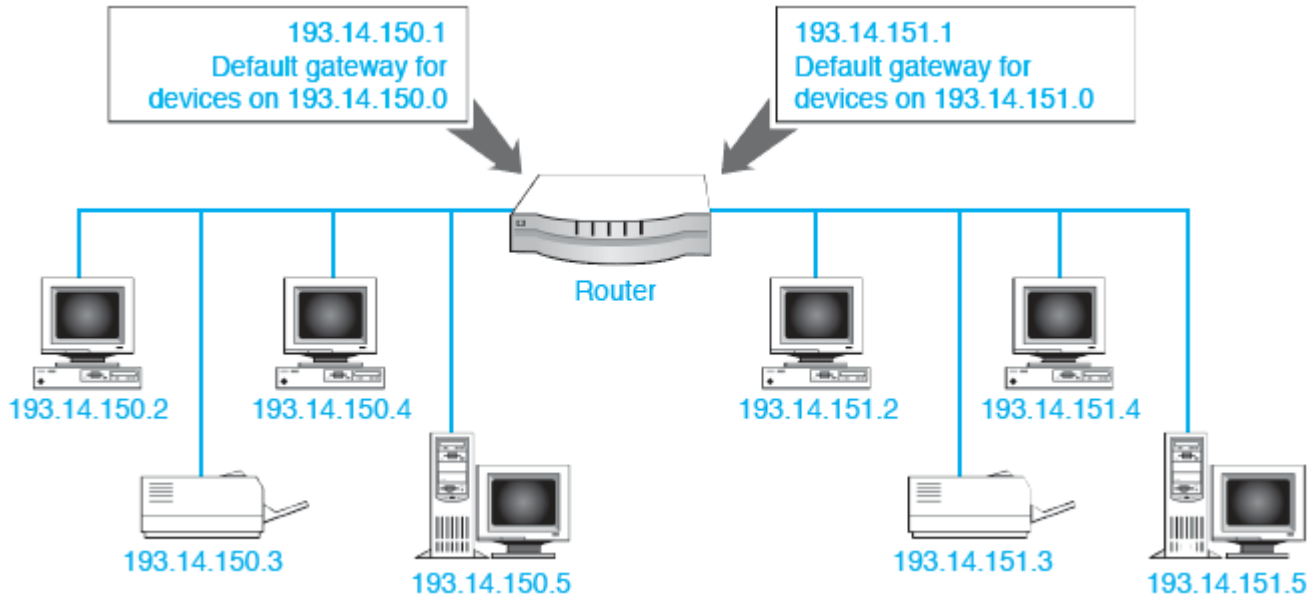
DHCP addressing

APIPA

- When a Windows computer is set up for DHCP and does not receive an IP address, an automatic private IP address (APIPA) is applied.
- APIPA addresses start with 169.254.x.x
- Check that the computer has connectivity (cable plugged in).
- Try using ipconfig /release and ipconfig /renew to reach the DHCP server again.

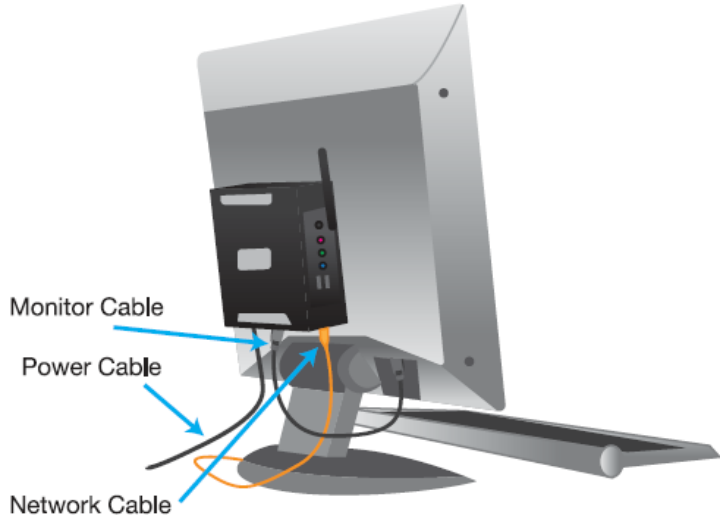
Default Gateway

- The default gateway address is used to allow a network device to reach a device on a different network.
- The default gateway address is the IP address of the router connected to the LAN.
- The default gateway address is ALWAYS a different IP address in the same network address range.



Thin Client Installation

- A thin client runs its applications from a server.
- Image management software is used to install an OS and drivers
- Configuration information commonly needed to deploy
  - MAC and/or IP address
  - Monitor settings
  - Domain/username
  - Drivers



Thick Client Installation

- A thick client has applications installed locally
- Image management software is used to install an OS and drivers
- Some unique apps might have to be installed manually
- Configuration options
  - Network printer and/or local printer
  - Application account settings
  - Computer settings including desktop icons and/or wireless options

Wireless Device Configuration Options

- Basic QoS
- Blacklist
- Channel ID
- DMZ
- DHCP
- Firmware
- NAT/DNAT
- Port forwarding/port triggering
- SSID
- UPnP
- Security Options (covered more in Chapter 18)

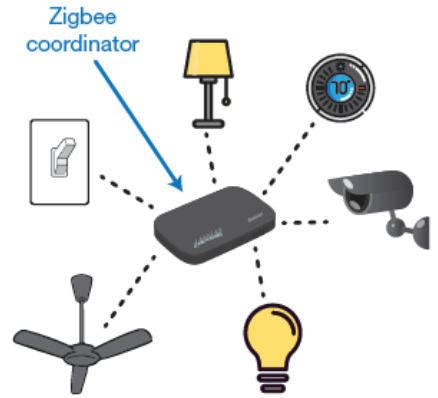
IoT and Smart Devices

- Can be on the wired Ethernet, 802.11 wireless, Zigbee wireless, Z-Wave wireless, or proprietary wired or wireless network

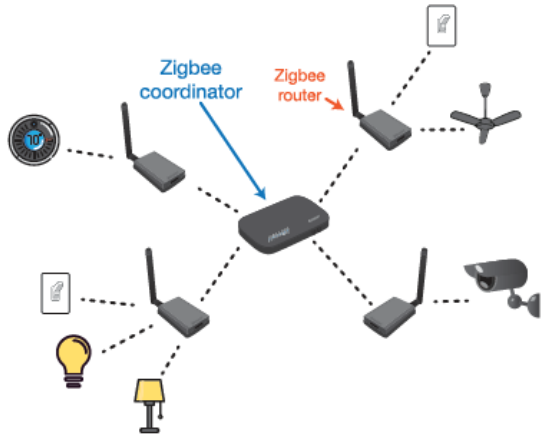
Standard	Frequency	Data rate	Range	Security
Zigbee	915 MHz and 2.4 GHz	Up to 250 kbps	Up to 328 feet (100 meters)	128-bit AES encryption
Z-Wave	908.4, 908.42, and 916 MHz (United States, Canada, and Mexico)	Up to 250 kbps	Up to 328 feet (100 meters)	Proprietary and improved with Security2 (S2)

Zigbee

- PAN ID and Channel ID must be the same for all devices on the same network.
- Does not have a maximum number of hops (how many devices the signal has to go through to reach the destination)



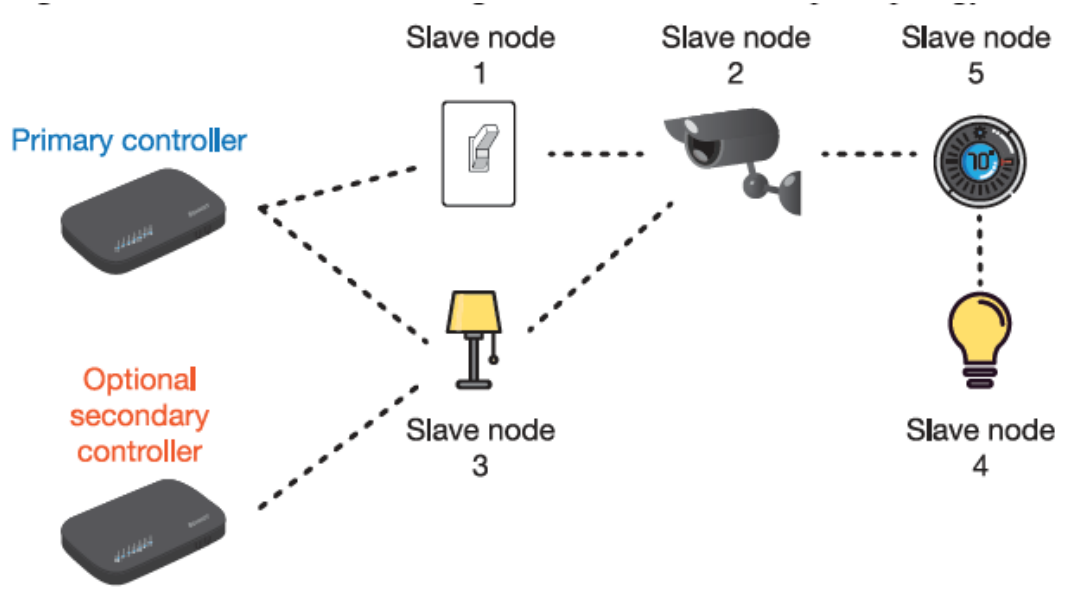
A Zigbee coordinator registers and receives data from the Zigbee end devices.



A Zigbee router extends the Zigbee network.

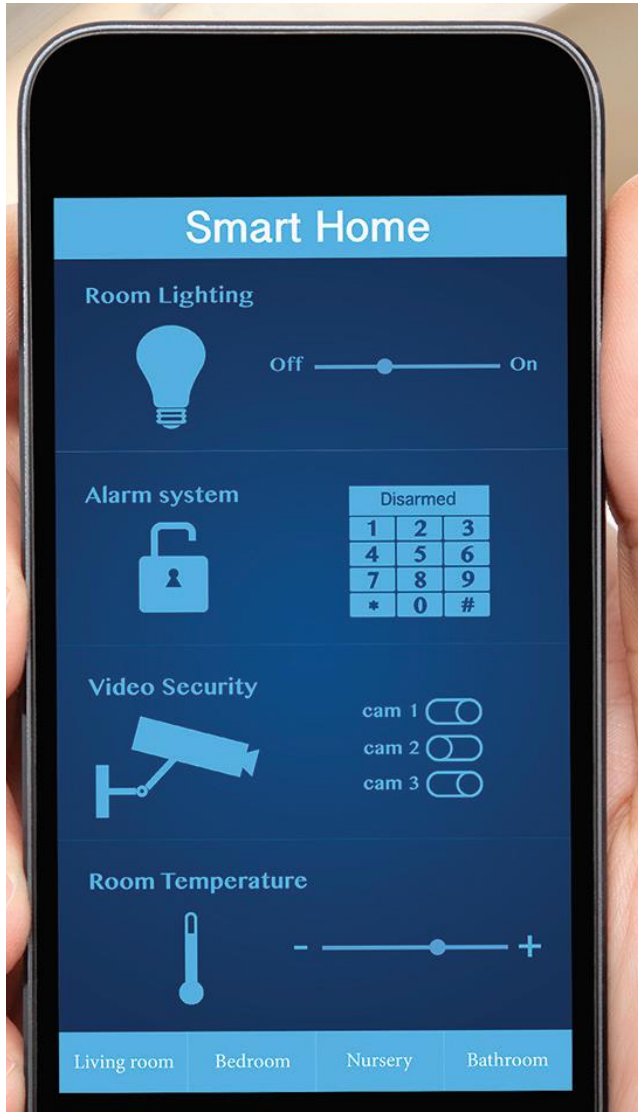
Z-Wave

- Limit of 232 devices
- Maximum of 4 hops between one device and a controller



IoT Devices

- Smart thermostat – remotely control and provides data on energy consumption
- Light Switch – programmed and set on a timer, motion-activated, and/or controlled by voice and/or an app.
- Security camera – can provide remote monitoring and be motion-activated
- Door lock – allows keyless entry
- Voice-enabled smart speakers or digital assistants



Network Troubleshooting

- Use the `ping` command to see if you can reach other devices on the same network or remote network.
- Use the `ping` command followed by a specific URL like `www.pearsoned.com` to see if DNS is working.
- Use the `ipconfig` or `ifconfig` command to see if the device has an IP address and default gateway.
- Use the `tracert` command to see how far the device can reach.
- Use the `nslookup` command when troubleshooting DNS issues

```
C:\Users\Cheryl>tracert comptia.org
Tracing route to comptia.org [198.134.5.6] over a maximum of 30
hops:
1 <1 ms <1 ms <1 ms vankman1 [192.168.1.1]
2 8 ms 7 ms 8 ms 10.126.208.1
3 10 ms 8 ms 7 ms 72-31-92-20.net.bhntampa.com [72.31.92.20]
4 11 ms 14 ms 12 ms ten0-6-0-11.tamp27-car1.bhn.net [71.44.3.186]
5 17 ms 16 ms 19 ms hun0-4-0-3.tamp20-car1.bhn.net [72.31.117.170
6 22 ms 19 ms 18 ms ten0-8-0-0.orld71-CAR1.bhn.net [71.44.1.211]
7 17 ms 16 ms 19 ms 72-31-217-88.net.bhntampa.com [72.31.217.88]
8 23 ms 19 ms 14 ms 10.bu-ether15.orldfljo00w-bcr00.tbone.rr.com
[66.109.6.98]
9 36 ms 31 ms 31 ms bu-ether18.atlngamq47w-bcr01.tbone.rr.com
[66.109.1.72]
10 23 ms 23 ms 24 ms 0.ae2.pr1.atl20.tbone.rr.com [107.14.17.188]
11 26 ms 29 ms 23 ms 67.106.215.89.ptr.us.xo.net [67.106.215.89]
12 50 ms 51 ms 50 ms 207.88.13.54.ptr.us.xo.net [207.88.13.54]
13 52 ms 56 ms 49 ms 207.88.12.174.ptr.us.xo.net [207.88.12.174]
14 50 ms 51 ms 51 ms 207.88.12.31.ptr.us.xo.net [207.88.12.31]
15 49 ms 57 ms 55 ms ae0d0.mcr1.chicago-il.us.xo.net
[216.156.0.162]
16 54 ms 52 ms 53 ms 216.55.11.62
17 52 ms 60 ms 52 ms 198.134.5.6
Trace complete.
```

Network Troubleshooting (cont.)

- Use the `net` command to manage network devices from a command prompt or through a script.

Command	Description
`net help`	Used to get help for the `net` commands. You can also use `net help` followed by the command (`net help computer`) or `net computer /help` or `net computer /?`.
`net computer`	Used to add or remove a computer from a Microsoft domain.
`net config`	Used to display information about the server or workstation service.
`net share`	Used to create, remove, or view network share resources
`net start`	Used to start a network service.
`net stop`	Used to stop a network service.
net use	Used to map a drive letter to a network resource.
net user	Used to manage user accounts.
`net view`	Used to view network devices.

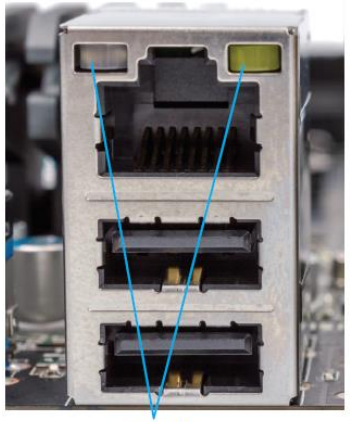
Network Troubleshooting (cont.)

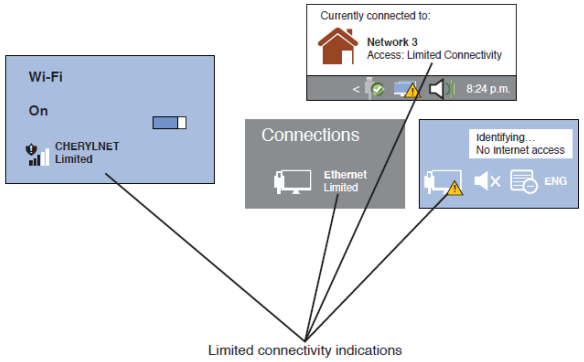
- Use the `netdom` command to manage network workstations from a command prompt or through a script.

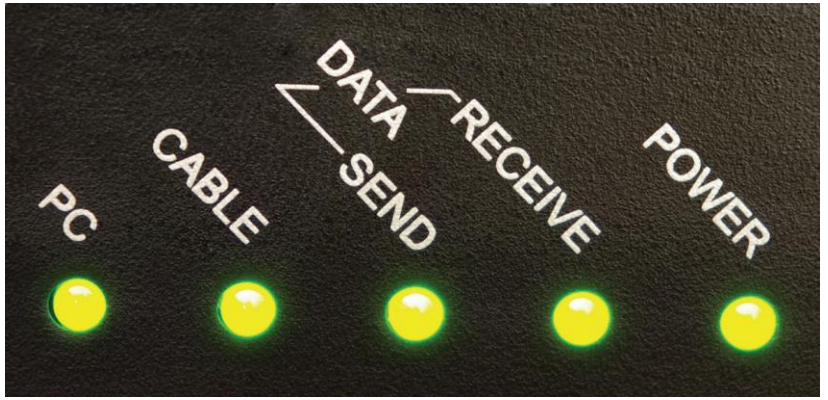
Command	Description
`netdom add`	Used to add a workstation account to the domain
`netdom join`	Used to join a workstation to a domain
`netdom remove`	Used to remove a workstation from the domain
`netdom renamecomputer`	Used to rename a computer and its domain account
`netdom reset`	Used to reset the connection between a workstation and a network domain controller
`netdom resetpwd`	Used to reset the computer account password
`netdom verify`	Used to verify the connection between a workstation and a Microsoft domain controller

Network Troubleshooting (cont.)

- Check NIC status lights for cabling or NIC issues
- Look for connectivity indicators for wired or wireless Internet connectivity
- Check Internet router modem lights







Network Servers

- Authentication – verify credentials
- DHCP – provide IP addressing information to clients
- DNS – translate domain names to IP addresses
- End-point management – discover devices, distribute software, update, configure, manage, and re-image

Network Servers (Cont.)

- Mail – manage, control, and route email
- Print – manage one or more printers
- Proxy – act as a go-between between an application and a remote server
- Syslog – log information reported by network devices as a historical record
- Web – provide web-based content

Important TCP/IP Protocols

- AFP (Apple Filing Protocol) – file services for macOS on port 548
- DHCP (Dynamic Host Configuration Protocol) – IP addressing information on port 67/68
- DNS (Domain Name System) – translate Internet names and URLs to IP addresses on port 53
- FTP (File Transfer Protocol) – unsecure file storage on port 21 and optionally port 20
- HTTP (Hypertext Transfer Protocol) – view information through a browser on port 80
- HTTPS (HTTP over SSL – Secure Sockets Layer) – encrypted HTTP communication on port 443

Important TCP/IP Protocols (cont.)

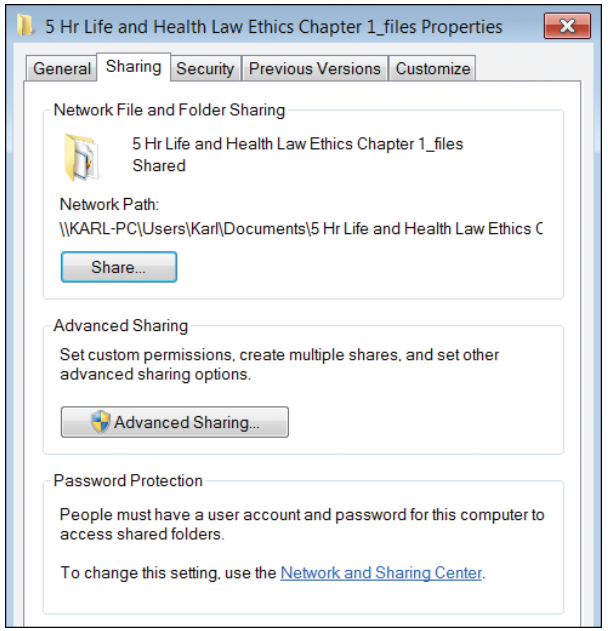
- IMAP (Internet Message Access Protocol) – email retrieval on port 143
- LDAP (Lightweight Directory Access Protocol) – records related to directory services on port 389
- NetBT (NetBIOS over TCP/IP) – supports outdated apps that rely on the NetBIOS API on ports 137-139
- POP3 (Post Office Protocol) – email retrieval on port 110
- RDP (Remote Desktop Protocol) – remote computer connectivity on port 3389

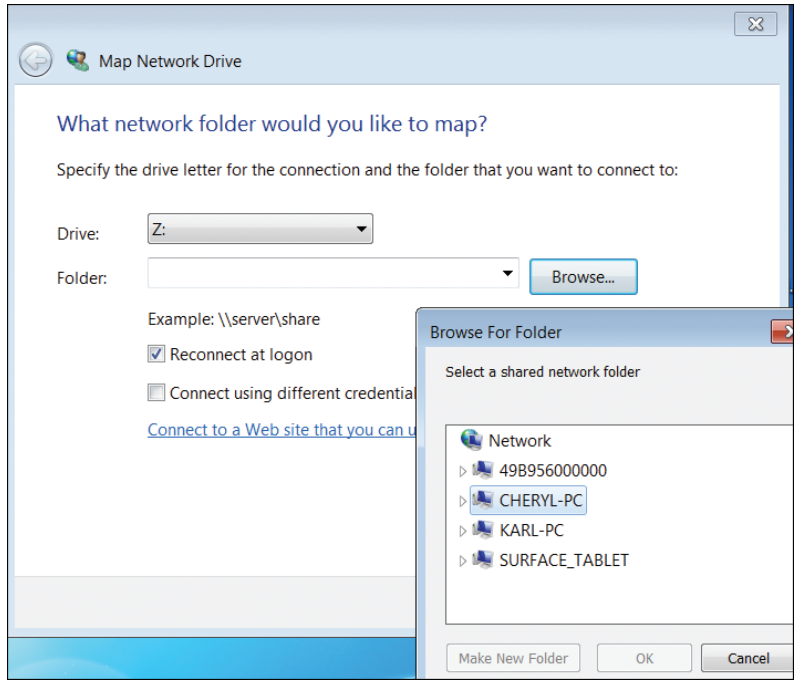
Important TCP/IP Protocols (cont.)

- SSH (Secure Shell) – Secure connectivity and file transfer on port 22
- SMB (Server Message Block) – access to shared network devices, files/folders, and printers on port 445
- SLP (Service Location Protocol) – announce and discover services on port 427
- SMTP (Simple Mail Transfer Protocol) transmits email on port 25
- SNMP (Simple Network Management Protocol) monitor, communicate, and manage network devices on ports 161/162
- Telnet – unsecure remote connectivity on port 23

Shared Folders

> Use Windows Explorer or File Explorer to share a folder.





Ways to Connect to the Internet

- Cable
- Cellular
- Dial-up – uses traditional phone network
- DSL
- ISDN – uses traditional phone network
- Line-of-sight wireless
- Satellite

Computer Terms

Refer to the glossary terms at the end of the textbook chapter. Review Chapter 13 and become familiar with the terms.

This PPT deck was developed

to support instruction of

The Complete CompTIA A+ Guide to IT Hardware and Software 8th Ed.