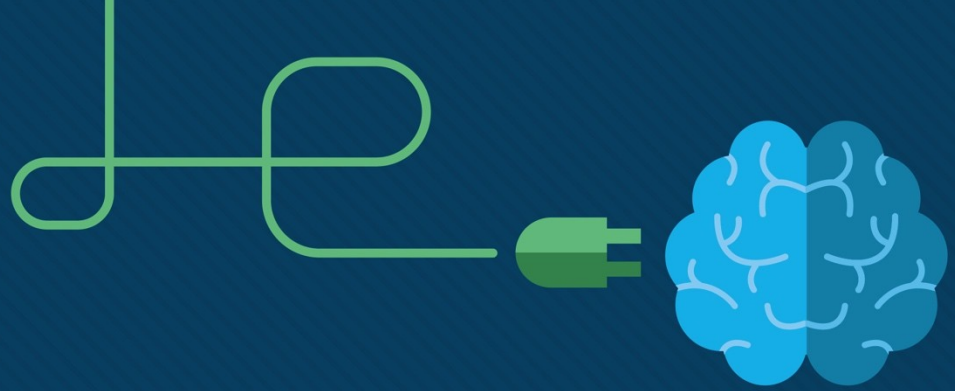
Chapter 5: Networking Concepts

IT Essentials 8.0 Planning Guide



Chapter 5: Networking Concepts

IT Essentials v8.0

Chapter 5 - Sections & Objectives

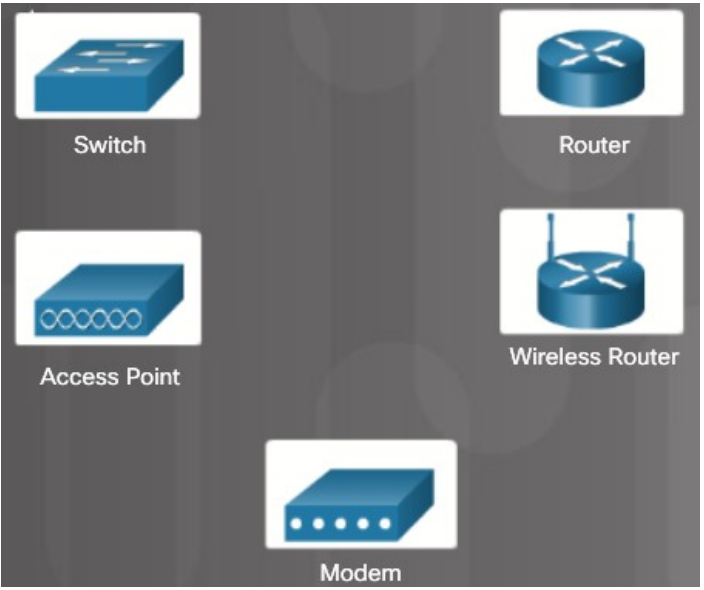
- 5.1 Network Components and Types
  - Explain components and types of computer networks.
    - Describe the types of networks.
    - Describe internet connection types.
- 5.2 Network Protocols, Standards, and Services
  - Explain networking protocols, standards and services.
    - Explain the purpose and characteristics of transport layer protocols.
    - Explain the significance of application port numbers.
    - Explain wireless protocols.
    - Explain network services.

Chapter 5 - Sections & Objectives (Cont.)

- 5.3 Network Devices
  - Explain the purpose of devices on a network.
    - Explain basic network devices.
    - Explain security devices.
    - Explain other network devices.
- 5.4 Network Cables
  - Explain the characteristics of network cables.
    - Describe networking tools and their purpose.
    - Explain the purpose and characteristics of common types of copper network cables and connectors.
    - Explain the purpose and characteristics of common types of fiber network cables and connectors.

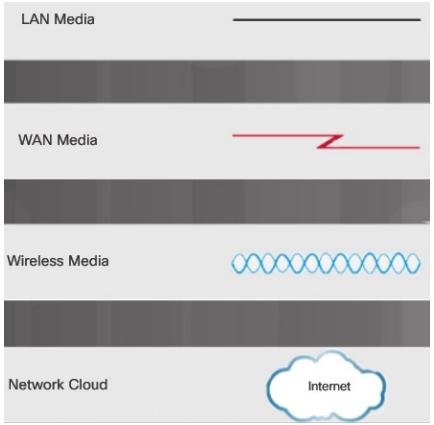
5.1 Network Components and Types

Network Icons



Intermediary Device Icons

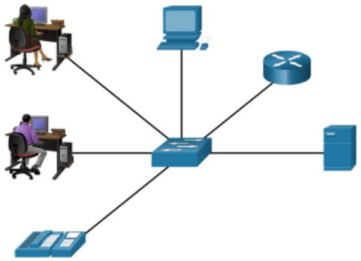
Network Media Icons



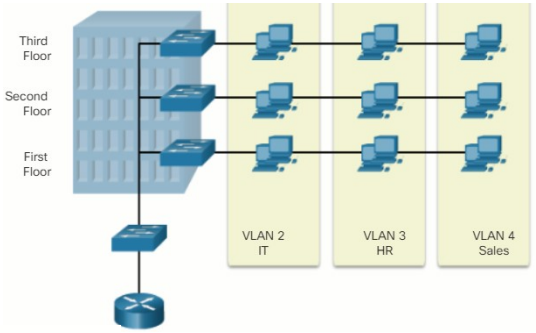
Host Device Icons

Network Topologies and Description

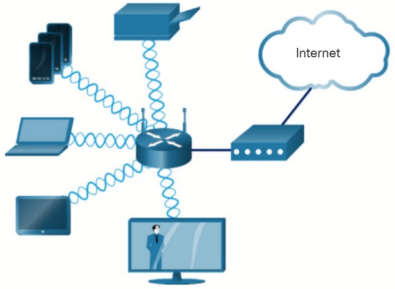
- **PAN (personal area network)** – Commonly uses Bluetooth to connect mice, keyboards, phones, and tablets.



- **LAN (local area network)** – A wired network consisting of a switch and network devices in a limited geographical area.



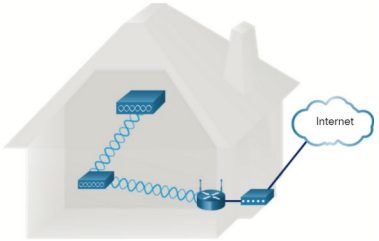
- **VLAN (virtual LAN)** – Extends beyond a traditional LAN and groups users based on administratively defined boundaries such as department or floor.

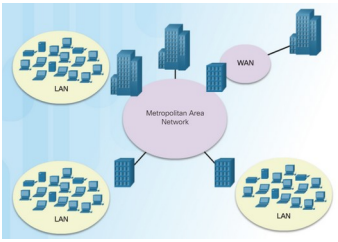


- **WLAN (wireless LAN)** – Connects multiple wireless devices and uses an access point.

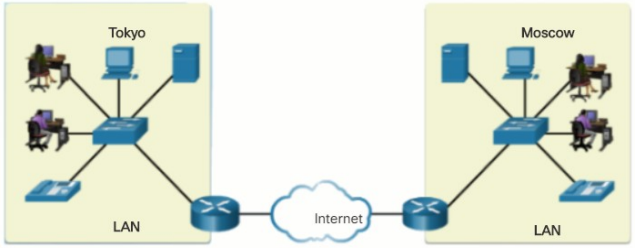
Network Topologies and Description (Cont.)

- **WMN (wireless mesh network)** – Connects multiple wireless access points together to expand the wireless network.



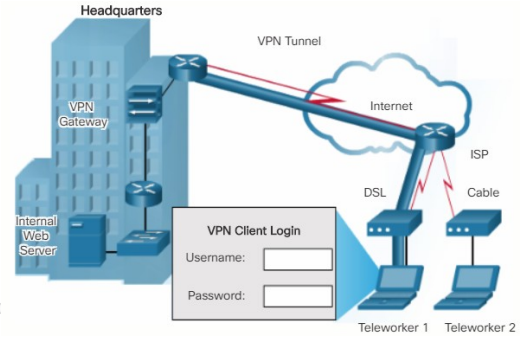


- **MAN (metropolitan area network)** – A network that spans a city.



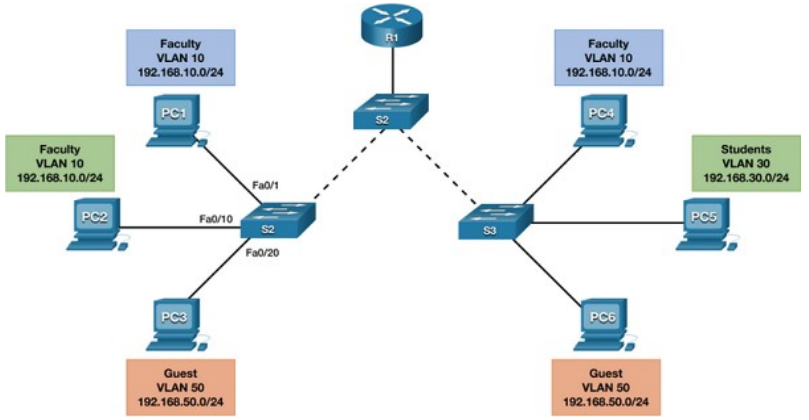
- **WAN (wide area network)** – A network that spans a large geographical area.

- **VPN (virtual private network)** – A method of connecting to a network such as a company network across an unsecure network.



VLANs

- They provide segmentation and organizational flexibility in a switched network.
- A group of devices within a VLAN communicate as if each device was attached to the same switch.
- VLANs are based on logical connections, instead of physical connections, and they can be segmented based on factors such as function, team, or application.
- For example, a faculty member computer (PC1) is connected to S2 on VLAN 10.
- PC1 could communicate with another faculty member using PC4 connected to S3.
- Notice how both hosts are configured on network address 192.168.10.0/24.
- By default, all switch ports are assigned to VLAN 1.
- However, you can assign the PCs to different VLANs by configuring their interconnecting port.



VLANs (Cont.)

- Figure 2 displays a sample configuration of switch S2.
- Notice that we first create the VLANs and assign them names.
- This makes it easier to work with the VLANs.
- Next, we configure the ports connecting to the PCs to the corresponding VLANs.
- Once the VLAN information is configured on the other switches, the faculty member using PC1 would be able to communicate with PC4 because they are on the same VLANs.
- If the faculty member wanted to send something to PC5 which is assigned to VLAN 30, then the services of a router would be required.
- VLANs help reduce excessive broadcast traffic and implement access and security policies between groups of users.

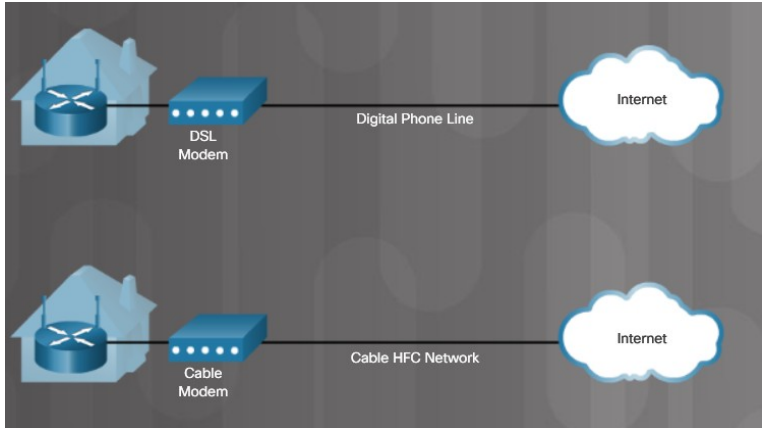
```
S2(config)# vlan 10
S2(config-vlan)# name Faculty
S2(config-vlan)# exit
S2(config)#
S2(config)# vlan 30
S2(config-vlan)# name Students
S2(config-vlan)# exit
S2(config)#
S2(config)# vlan 50
S2(config-vlan)# name Guest
S2(config-vlan)# exit
S2(config)#
S2(config)# interface fastethernet 0/1
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 10
S2(config-if)# exit
S2(config)#
S2(config)# interface range fa0/10
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# exit
S2(config)#
S2(config)# interface range fa0/20
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 50
S2(config-if)# exit
S2(config)#
```

Brief History of Connection Technologies

- **Analog telephone access (dialup)** – uses an analog modem to call another modem.
- **ISDN (Integrated Services Digital Network)** – more bandwidth than dialup. Can carry voice, video, and data.
- **Broadband** – uses different frequencies to send multiple signals over media.

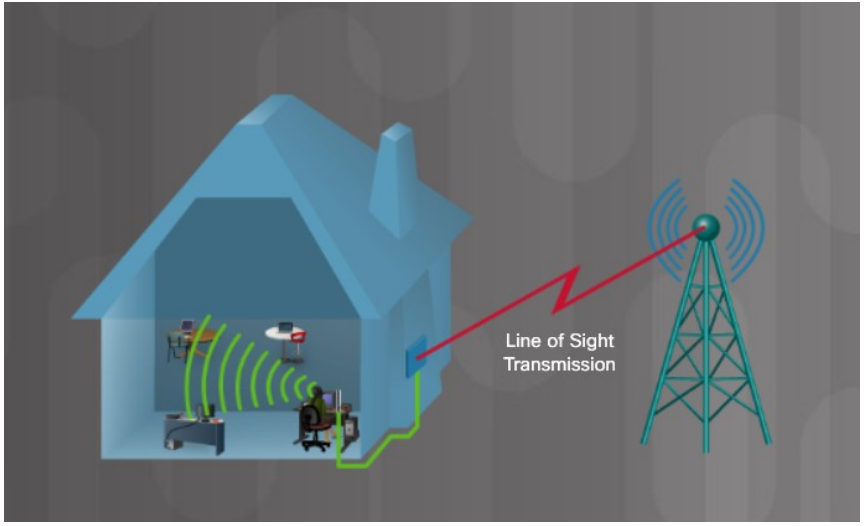
DSL, Cable, and Fiber

- **DSL (digital subscriber line)** – always on technology that uses phone lines; voice and data carried on different frequencies; requires a filter on the port that connects to a phone.
  - Very high-speed DSL (VDSL) attains much higher bit rates than DSL. A symmetric link can carry as much as 26 Mbps in both directions while an asymmetric link can carry as much as 52 Mbps download and 6 Mbps upload. VDSL2 can carry as much as 100 Mbps in both directions.
- **Cable** – Uses a cable modem to connect to a traditional cable TV network; shares the network with multiple subscribers.
- **Fiber** – High bandwidth connection used in backbone networks, large enterprise environments, large data centers, and now part of some home internet connections.
  - In the figure, the cable connection includes a HFC network in which fiber is used in the last mile to the user's home, and at the user's home the network switches back to copper coaxial cable (FTTC).
  - Fiber to the premises (FTTP) brings the fiber to the customer's building.



Line of Sight Wireless Internet Service

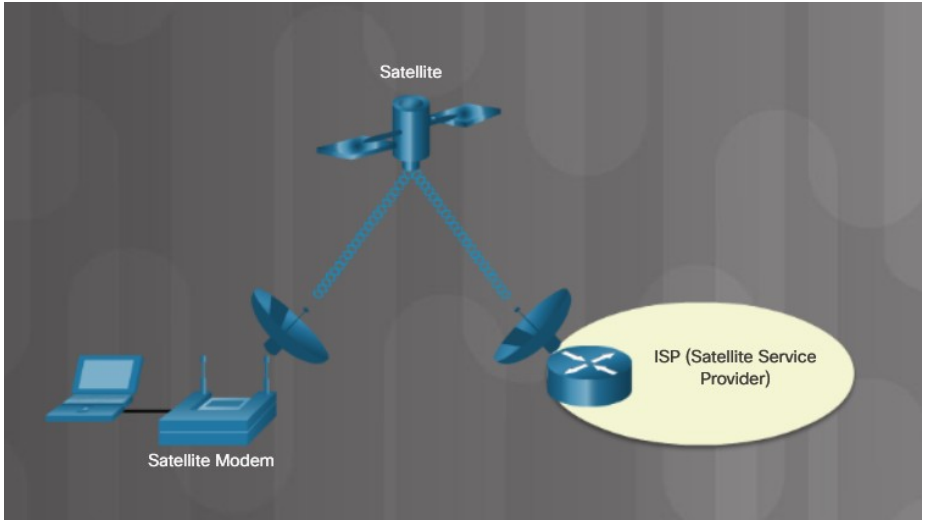
- **Line of site wireless** – always on technology that uses radio signals for connecting to the internet.
  - Clear path required
  - Weather affects signal strength and performance



Satellite

- **Satellite** – broadband technology for remote areas
  - Uses a satellite dish
  - Not a good solution for time-sensitive applications like gaming, Voice over Internet Protocol (VoIP), and video conferencing

- **Low Earth Orbit (LEO)** – far more satellites orbiting the Earth in low Earth orbit
  - Can support up to approximately 100 Mbps
  - Much lower latency than standard satellite, between 100 and 200 ms

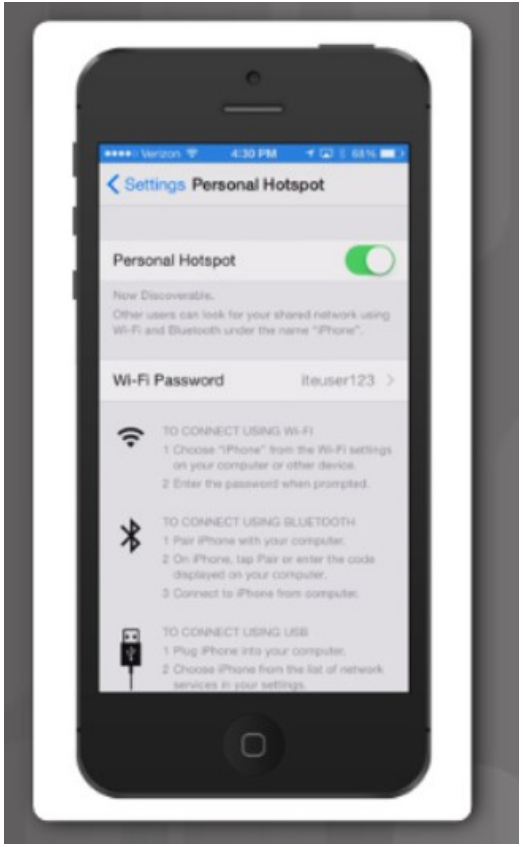


Cellular

- **Cellular**– relies on cell towers to create a network used by cell phones and connectivity to the internet

Mobile Hotspot and Tethering

- Cell phone option that allows another device to connect to the internet using Wi-Fi, Bluetooth, or USB cable
  - The other device is using the phone's cellular connection to connect to the internet
  - Called tethering or a hotspot
- A mobile hotspot is when a cell phone allows Wi-Fi devices to connect and use the mobile data network.



5.2 Networking Protocols, Standards, and Services

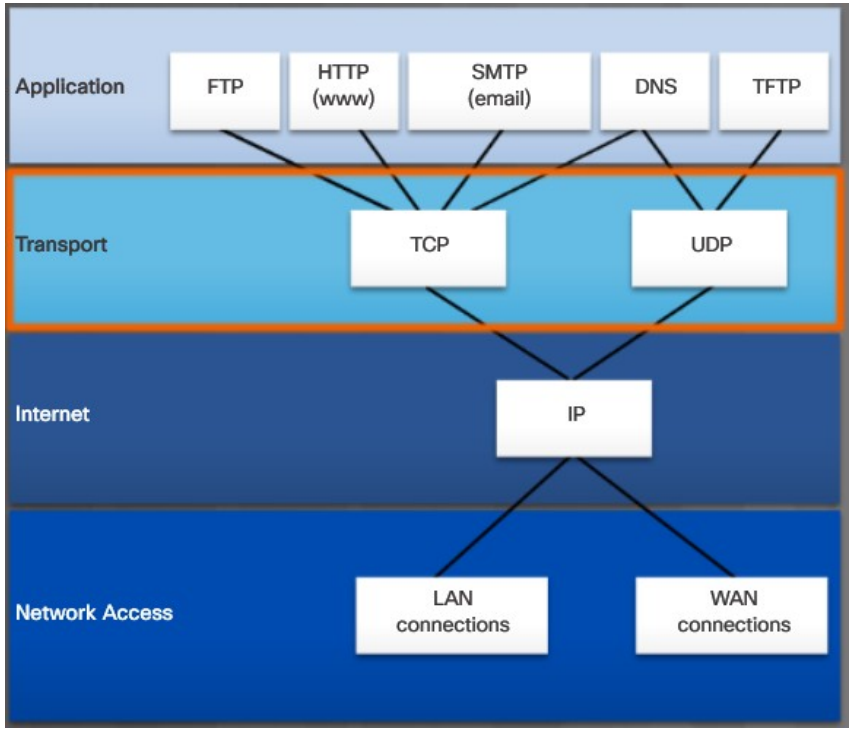
Transport Layer Protocols

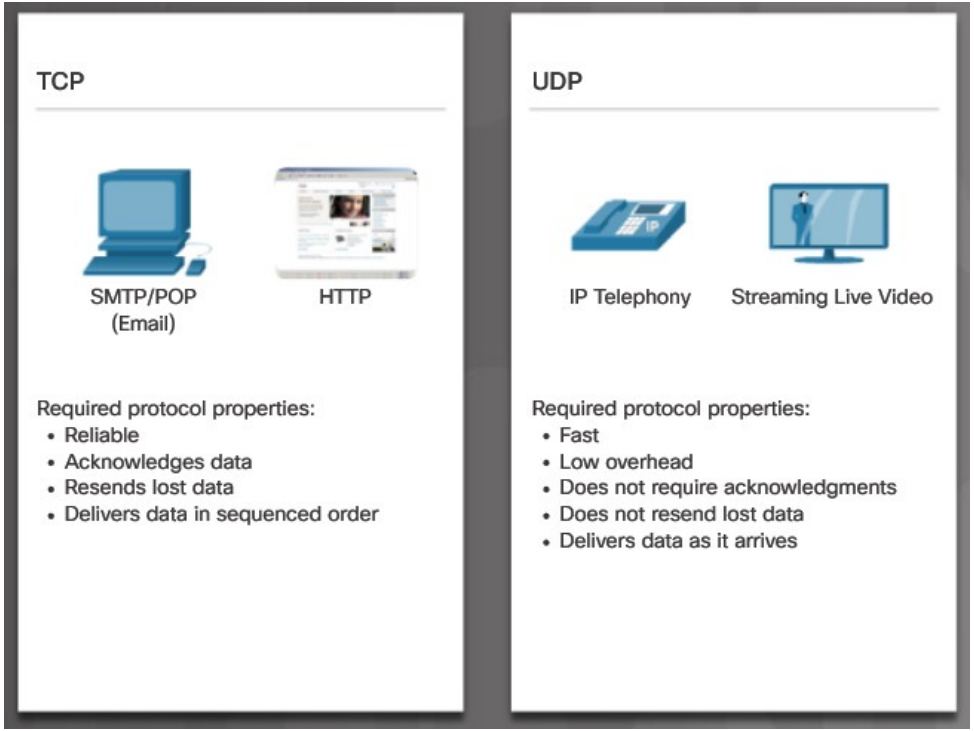
Video Explanation: Transport Layer Protocols

In this video explanation, you will learn about Transport Layer protocols:

- TCP
- UDP
- Sequence numbers

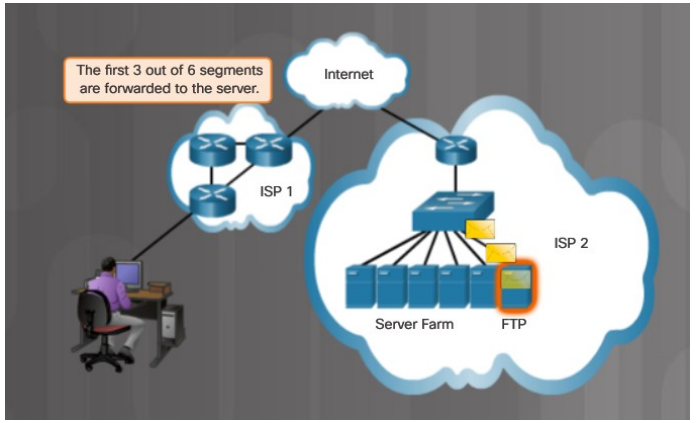
The TCP/IP Model

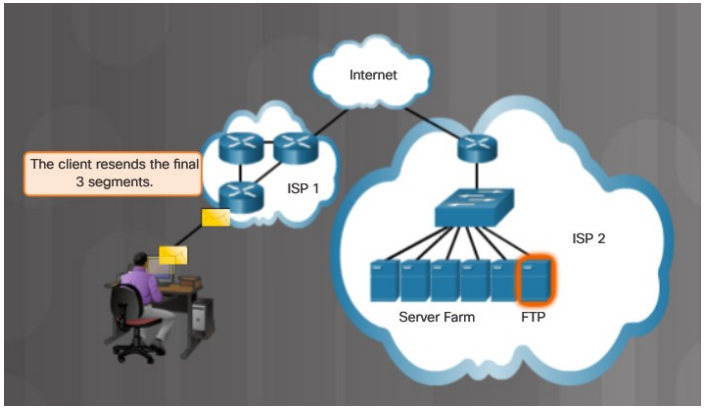




TCP

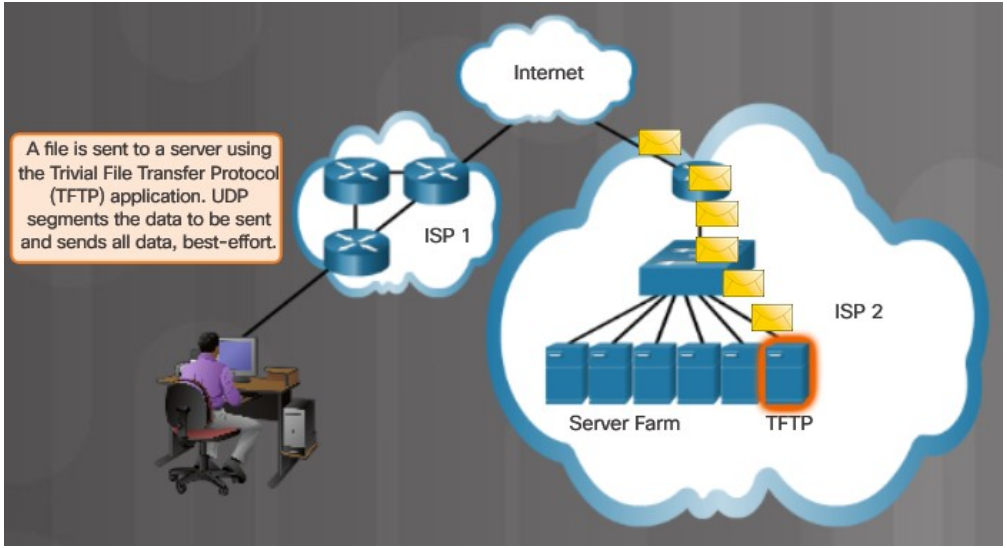
- Three basic operations of reliability
  - Numbering and tracking of data segments
  - Acknowledgment of received data
  - Retransmitting any unacknowledged data after a period of time.





UDP

- Very little overhead or data checking
- Best-effort delivery protocol (unreliable)
  - No acknowledgment that the data is received by the destination



Video Explanation – Application Port Numbers

Video Explanation: Application Port Numbers

In this video explanation, you will learn about application port numbers:

- Source Port
- Destination Port
- Well Known Port Numbers

Classify Application Port Numbers

World Wide Web Protocols

Port	Transport Protocol	Application Protocol	Description
53	TCP, UDP	DNS	The Domain Name Service (DNS) protocol finds the IP address associated with a registered Internet domain for Web, Email, and other Internet services. It uses UDP for requests and information transfer between DNS servers. TCP will be used for DNS responses if required.
80	TCP	HTTP	Hypertext Transfer Protocol (HTTP) provides a set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the World Wide Web
443	TCP, UDP	HTTPS	The browser uses encryption and authenticates your connection with webserver.

Email and Identity Management Protocols

Port	Transport Protocol	Application Protocol	Description
25	TCP	SMTP	Simple Mail Transfer Protocol is used to send email from clients to an email server. It may also be used to relay email messages from source to destination email servers.
110	TCP	POP3	Post Office Protocol 3 is used by email clients to retrieve messages from an email server.
143	TCP	IMAP	Internet Message Access Protocol is used to retrieve email messages from a server. It is more advanced than POP3 and offers a number of advantages.
389	TCP, UDP	LDAP	Lightweight Directory Access Protocol is used to maintain user identity directory information that can be shared across networks and systems. It can be used to manage information about users and network resources. It can be used to authenticate users on multiple computers.

Remote Access Protocols

Port	Transport Protocol	Application Protocol	Description
22	TCP	SSH	Secure Shell or Secure Socket Shell provides a strong authentication and encrypted data transport between a client and remote computer. Like Telnet, it provides a command line on the remote computer.
23	TCP	Telnet	Telnet is an insecure remote access protocol that provides a command line on a remote computer. SSH is preferred for security reasons.
3389	TCP, UDP	RDP	Remote desktop protocol was developed by Microsoft to provide remote access to the graphical desktop of a remote machine. It is useful for tech support situations, however it should be used with caution because it provides a remote user with complete control of the destination computer.

Classify Application Port Numbers (Cont.)

Network Operations Protocols

Port	Transport Protocol	Application Protocol	Description
67/68	UDP	DHCP	Dynamic Host Configuration Protocol automatically provides IP addresses to network hosts and provides a way to manage those addresses. The DHCP server uses UDP port 67 and the client host uses UDP port 68.
137-139	UDP, TCP	NetBIOS (NetBT)	NetBIOS over TCP/IP provides a system through which older computer applications can communicate over large TCP/IP networks. Different NetBT functions use different protocols and ports in this range.
161/162	UDP	SNMP	Simple Network Management Protocol enables network administrators to monitor network operations from centralized monitoring stations.
427	UDP, TCP	SLP	Service Location Protocol allows computers and other devices to locate services on a LAN without previous configuration. Usually uses UDP, but can use TCP.
445	UDP, TCP	SMB	Server Message Block (SMB) is a client/server file sharing protocol that describes the structure of shared network resources, such as directories, files, printers, and serial ports. SMB file-sharing and print services have become the mainstay of Microsoft networking.

File Transport and Management Protocols

Port	Transport Protocol	Application Protocol	Description
20	TCP	FTP	File transfer protocol. Used to transfer files between computers. Considered insecure, SSH file transfer protocol (SFTP, TCP port 22) should be used.
21	TCP	FTP	FTP uses TCP port 21 to establish a connection between the client and FTP server. In order to start a data transfer session.
69	UDP	TFTP	Trivial File Transfer Protocol utilizes less overhead than FTP.
445	TCP	SMB/CIFS	Server Message Block or Common Internet File System allow for sharing of files, printers, and other resources between nodes on a network.
548	TCP, UDP	AFP	Apple Filing Protocol is a proprietary protocol developed by Apple to enable file services for macOS and classic Mac OS.

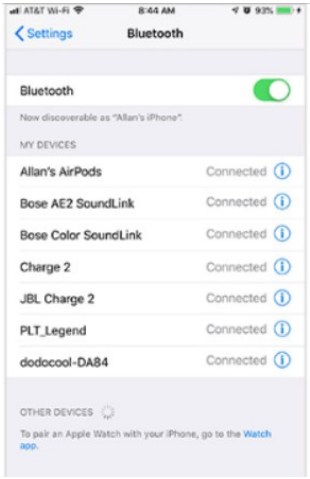
WLAN Protocols

Comparing 802.11 Standards

IEEE Standard	Maximum Speed	Maximum Indoor Range	Frequency	Backwards Compatible
802.11a (Wi-Fi 2)	54 Mbps	115 ft (35 m)	5 GHz	–
802.11b (Wi-Fi 1)	11 Mbps	115 ft (35 m)	2.4 GHz	–
802.11g (Wi-Fi 3)	54 Mbps	125 ft (38 m)	2.4 GHz	802.11b
802.11n (Wi-Fi 4)	600 Mbps	230 ft (70 m)	2.4 GHz, 5 GHz	802.11a/b/g
802.11ac (Wi-Fi 5)	6.9 Gbps	115 ft (35 m)	5 GHz	802.11a/n
802.11ax (Wi-Fi 6)	9.6 Gbps	150 ft (46m)	2.4 GHz, 5 GHz	802.11a/b/g/n/ac
802.11ax (Wi-Fi 6e)	9.6 Gbps	150 ft (46m)	1 GHz, 6 GHz	802.11a/b/g/n/ac

Bluetooth, NFC, and RFID

- Bluetooth
  - Up to 7 devices to create a PAN
  - 802.15.1
  - 2.4 to 2.485 GHz radio frequency range
- RFID
  - Passive or active tags used to identify items
    - **Passive** – rely on RFID reader to activate and read
    - **Active** – have a battery to broadcast the ID up to 100 meters
  - 125 MHz to 960 MHz radio frequency range
- NFC (Near Field Communication)
  - Devices must be in close proximity to exchange data
  - Used for payments, printing, public parking, etc.



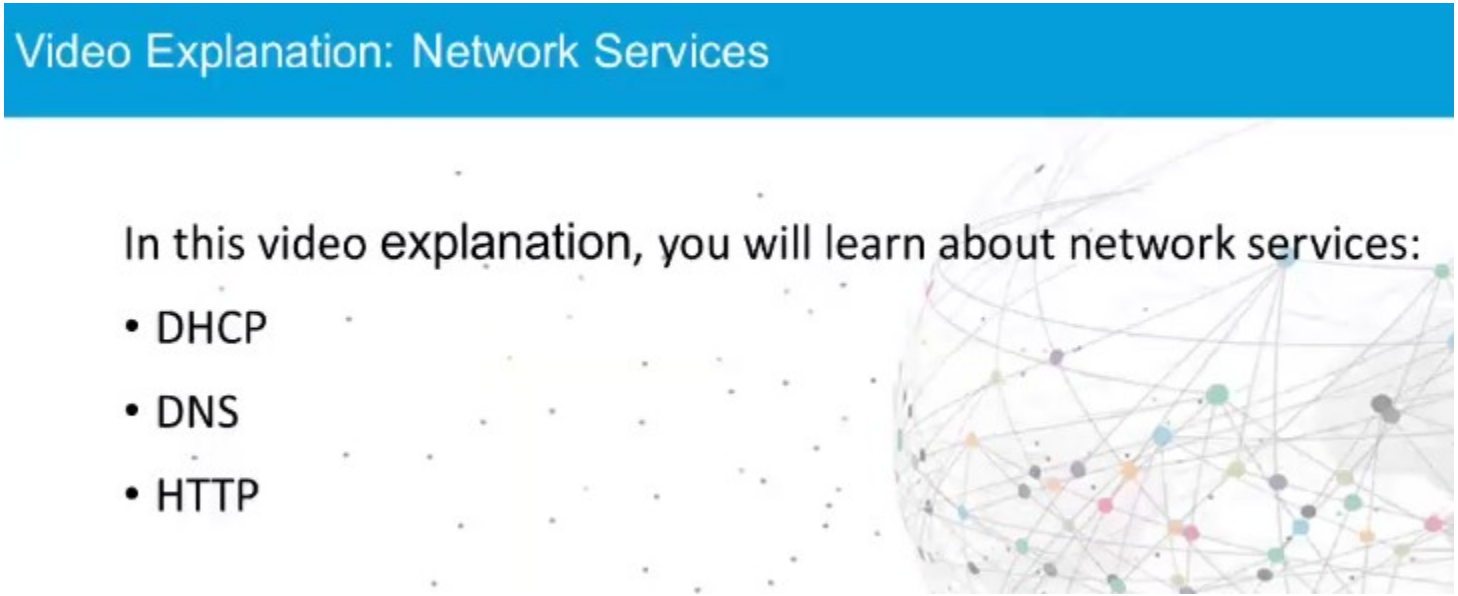
Zigbee and Z-Wave

- Zigbee
  - Requires a ZigBee Coordinator to manage client devices connected in a wireless mesh network.
  - Devices commonly managed from a cell phone app
  - IEEE 802.15.4 standard
  - 868 MHz to 2.4 GHz range up to 20 meters, 65,000 devices, and data speeds up to 250 kb/s
- Z-Wave
  - Proprietary standard, but public version available
  - 232 devices can connect to a wireless mesh network with data speeds up to 100 kb/s.

Cellular Generations

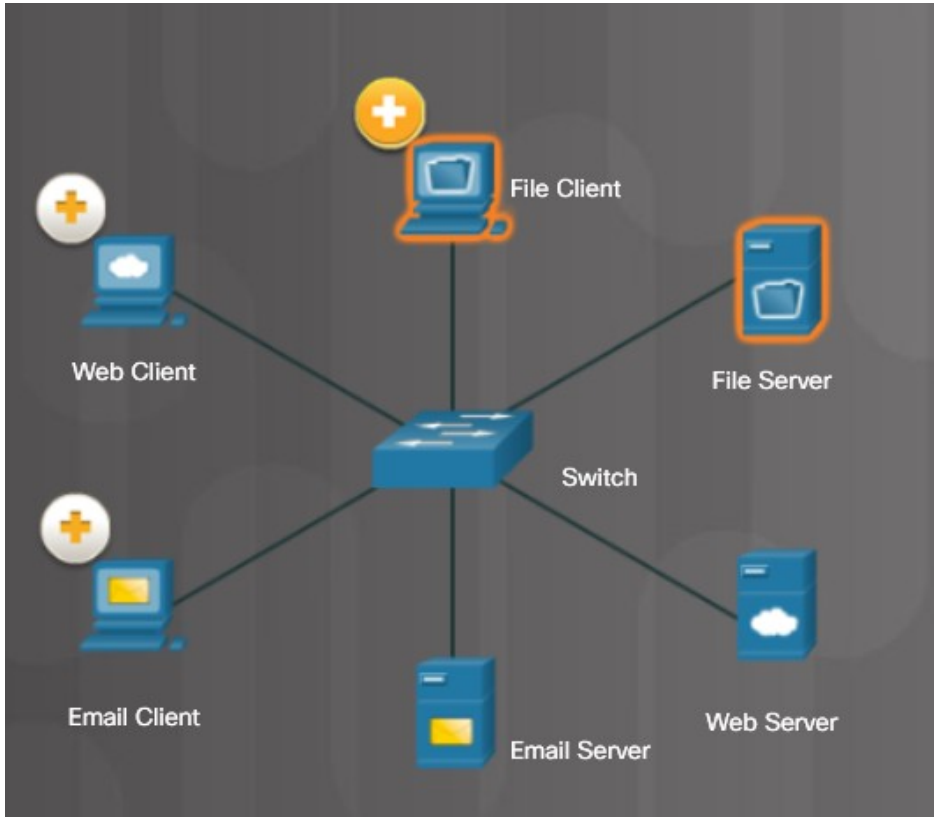
- **1G/2G** – First generation was analog calls only. 2G introduced digital voice, conference calls, and caller ID with speeds less than 9.6 Kb/s
- **2.5G** – supports web browsing, short audio and video clips with speeds up to 237 Kb/s.
- **3G** – full motion **video and streaming music** at speeds up to 2 Mb/s.
- **3.5G** – supports high-quality streaming video, high-quality video conferencing, and VoIP, at speeds up to 16 Mb/s.
- **4G** - IPv6, IP-based voice, gaming services, high quality multimedia at speeds up to 672 Mb/s.
- **LTE (Long Term Evolution)** – means it meets the 4G speed standards and improves connectivity while in motion. Speeds up to 100 Mb/s when mobile and up to 1 Gb/s when stationary.
- **5G** – supports augmented reality (AR), virtual reality (VR), smart homes, smart cars, and data transfer between devices. Download speeds up to 3 Gb/s; upload speeds up to 1.5 Gb/s.
- **6G** – is currently in development. As of late 2022, no standard yet exists. It will support even faster speeds required for AR/VR applications, AI applications, and instantaneous communications.

Video Explanation – Network Services



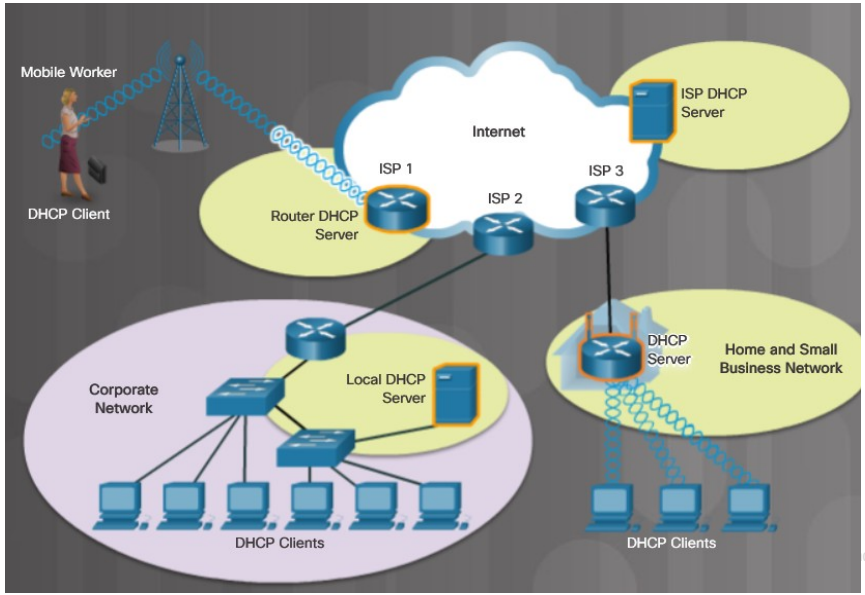
Client – Server Roles

- File Client and Server
- Web Client and Server
- Email Client and Server



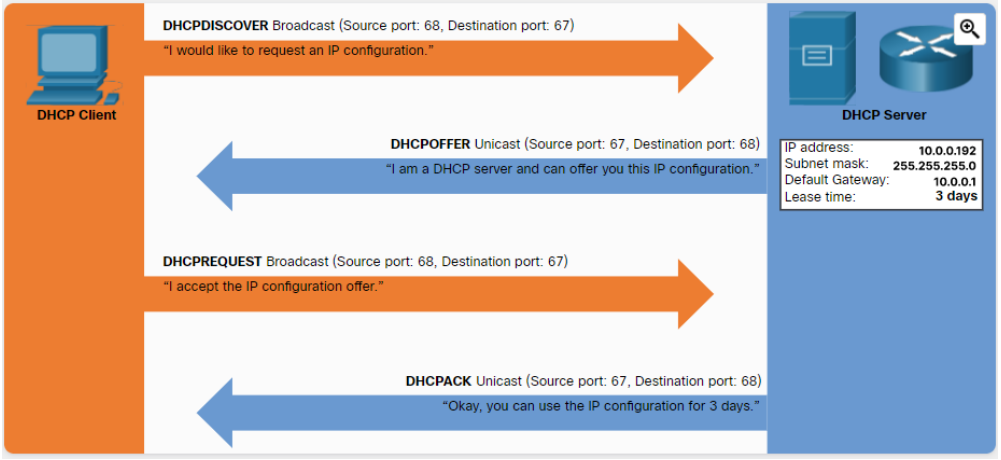
DHCP Server

- A host needs IP address information before it can send data on the network.
- DHCP is the service used by ISPs, network administrators, and wireless routers to automatically assign IP addressing information to hosts, as shown in the figure.



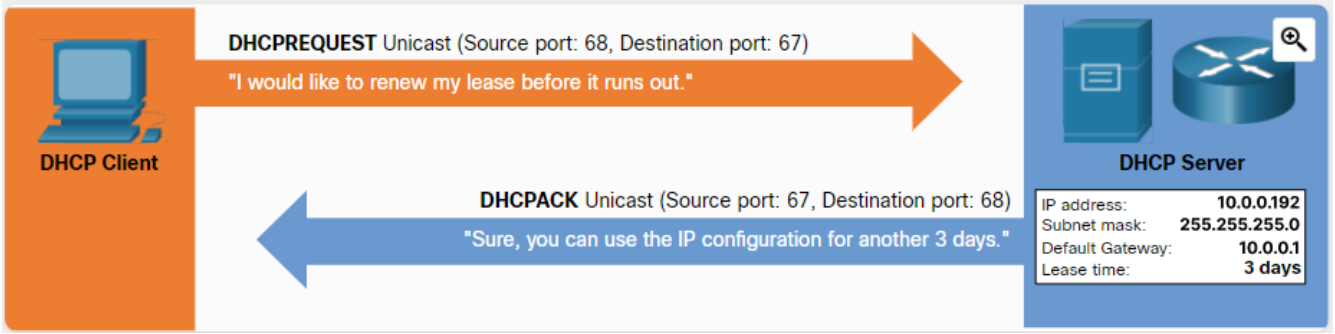
DHCP Server (Cont.)

- DHCP works in a client/server mode, where DHCP clients request available IP configurations from a DHCP server.
- A DHCP server is configured with a scope (i.e., a pool or a range) of addresses that it can lease to requesting DHCP clients.
- As shown in the figure, when the DHCP client boots (or otherwise wants to join a network), it initiates the following four-step process to obtain a lease.



DHCP Server (Cont.)

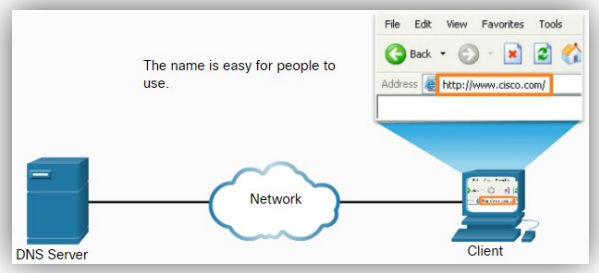
- The client must contact the DHCP server periodically to extend the lease.
- This lease mechanism ensures that moved or power-off clients do not keep addresses that they no longer need.
- When a lease expires, the DHCP server returns the address to the pool where it can be reallocated as necessary.



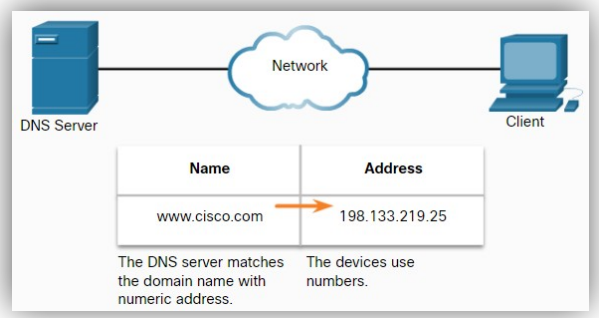
DNS Server

- A DNS server translates domain names such as cisco.com to an IP address.
- The five steps in the DNS resolution process are:

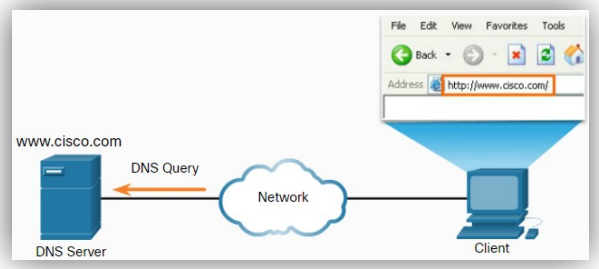
Step 1



Step 2



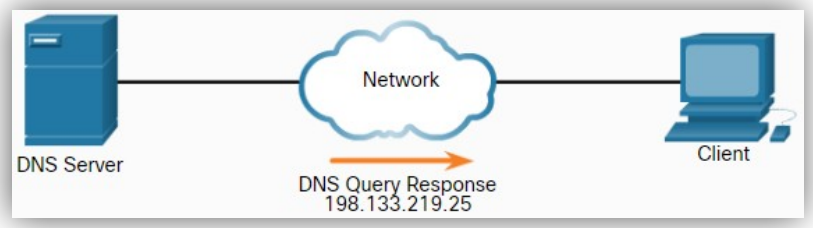
Step 3



DNS Server (Cont.)

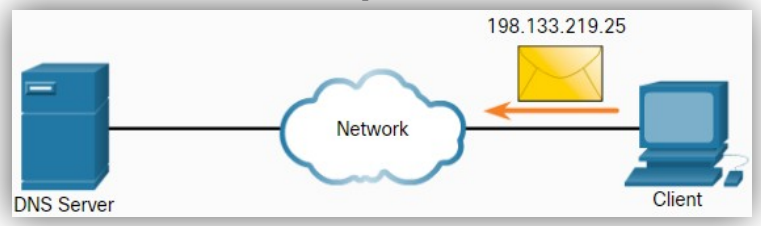
- The five steps in the DNS resolution process are:

Step 4



The number is returned back to the client for use in making requests of the server.

Step 5

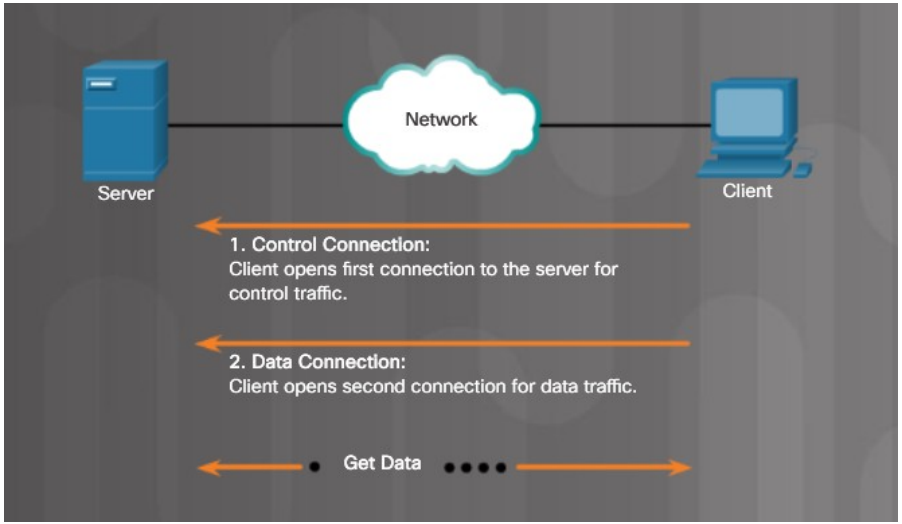


A domain name is resolved to its numeric network device address by the DNS protocol.

Print Server

- A print server
  - Can control multiple printers
  - Provides client access to print resources
  - Allows centralized print job administration
  - Provides feedback to network clients

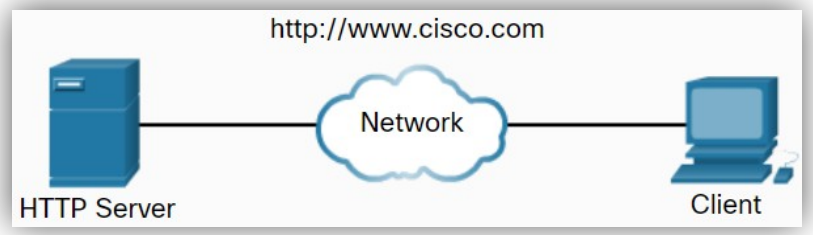
File Server



- A file server allows clients to access files using a specific protocol
  - FTP (File Transfer Protocol)
  - FTPS (File Transfer Protocol Secure)
  - SFTP (Secure Shell File Transfer Protocol)
  - SCP (Secure Copy)

Web Server

- A web server provides web resources using these protocols
  - Hypertext Transfer Protocol (HTTP) operating on TCP port 80
  - Secure HTTP (HTTPS) using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) operating on TCP port 443
- How a web page is opened in a browser:
  - For this example, use the http://www.cisco.com/index.html URL.
  - First, the browser interprets the three parts of the URL:
    1. **http** (the protocol or scheme)
    2. **www.cisco.com** (the server name)
    3. **index.html** (the specific filename requested)

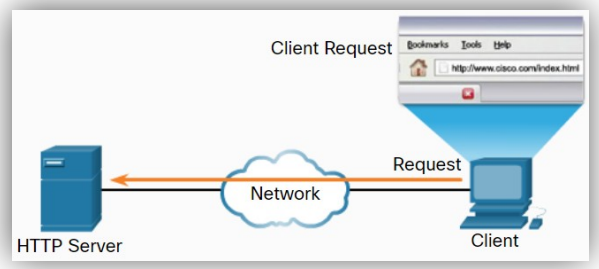


- The browser then checks with a DNS to convert www.cisco.com into a numeric address, which it uses to connect to the server.

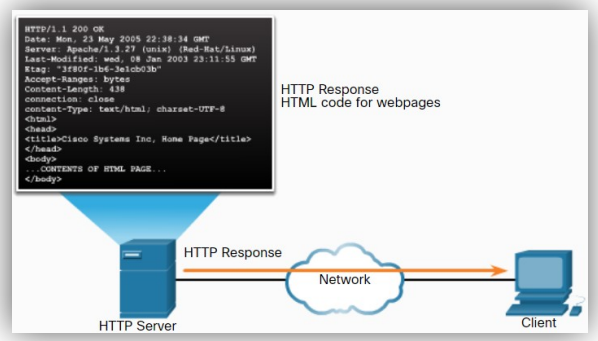
Web Server (Cont.)

- Step 1: Using HTTP requirements, the browser sends a GET request to the server and asks for the index.html file.
- Step 2: The server sends the HTML code for this web page back to the client's browser.
- Step 3: The browser interprets the HTML code and formats the page for the browser window.

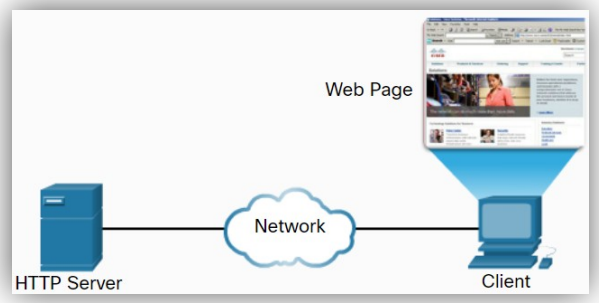
Step 1



Step 2

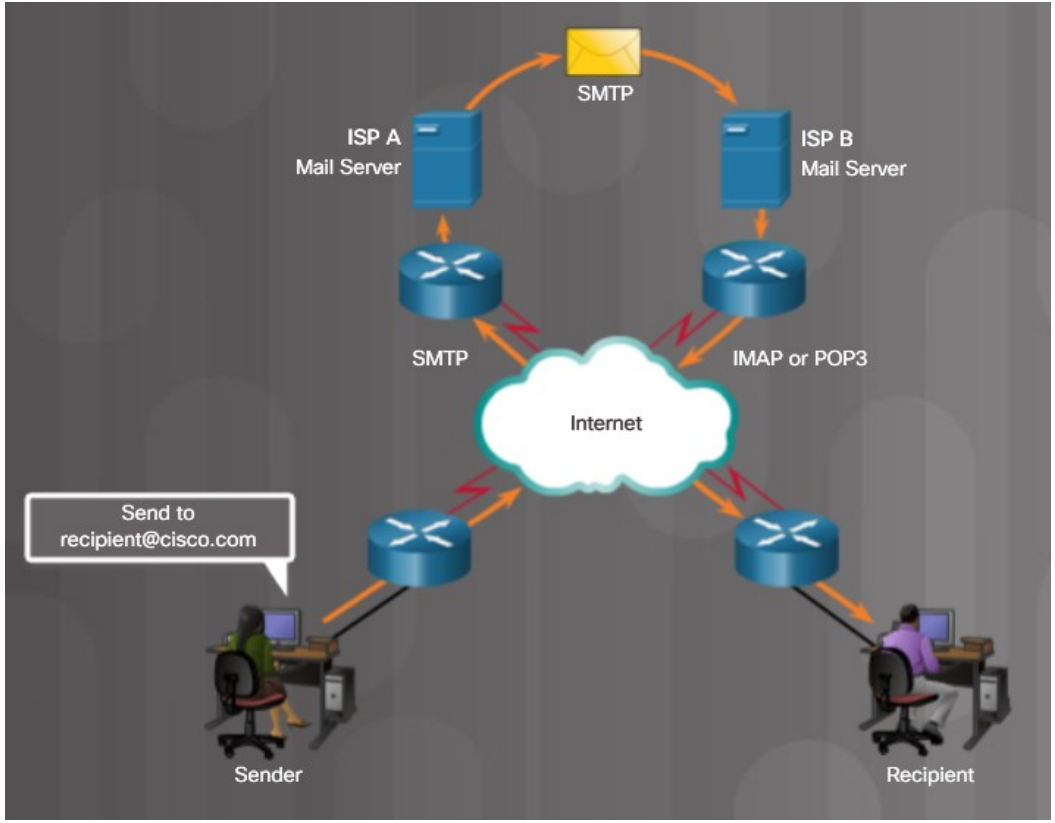


Step 3



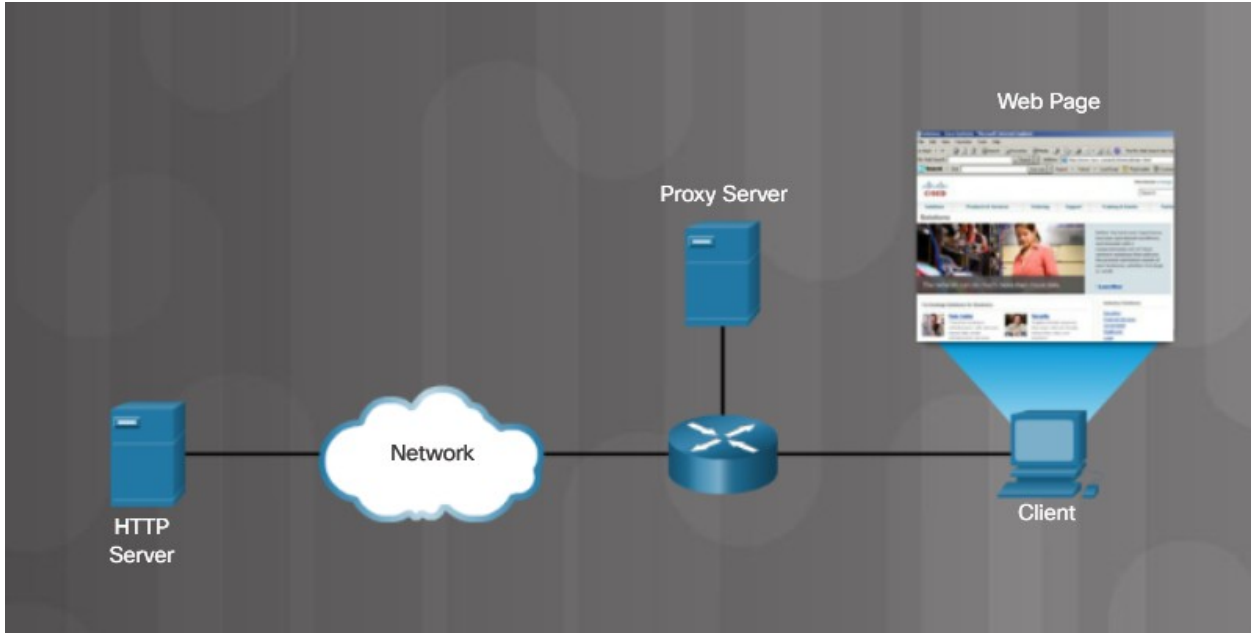
Mail Server

- Email messages are stored in databases on mail servers
  - Client communicates with server in order to reach a different client
  - Protocol used to send email
    - Simple Mail Transfer Protocol (SMTP)
  - Protocols used to retrieve email
    - Post Office Protocol (POP)
    - Internet Message Access Protocol (IMAP)



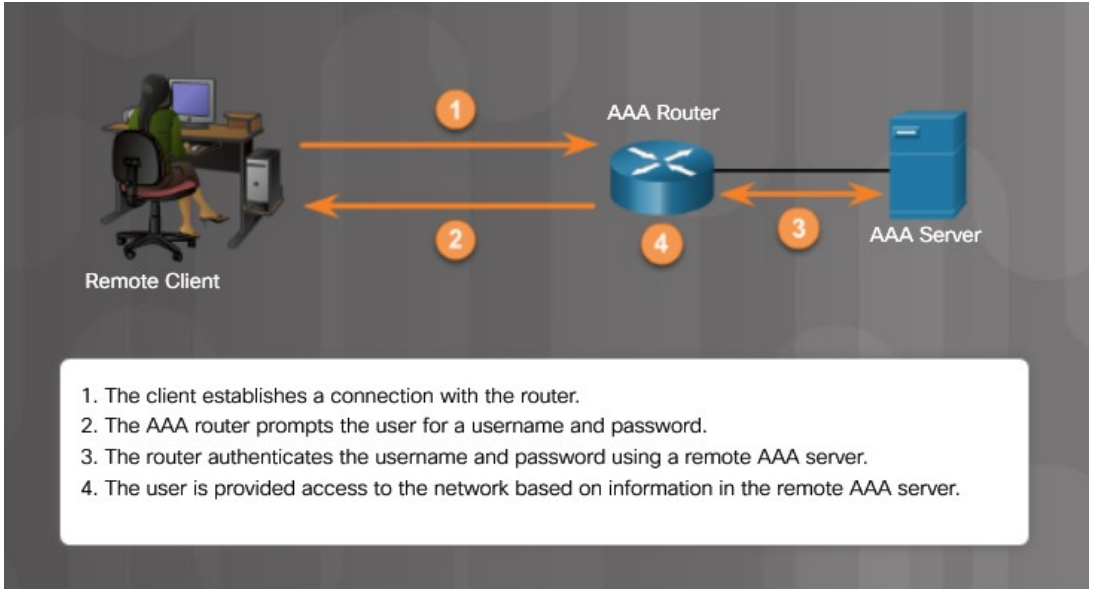
Proxy Server

- Proxy servers act on behalf of a client, thus hiding the real internal host
- Used to cache frequently accessed web pages



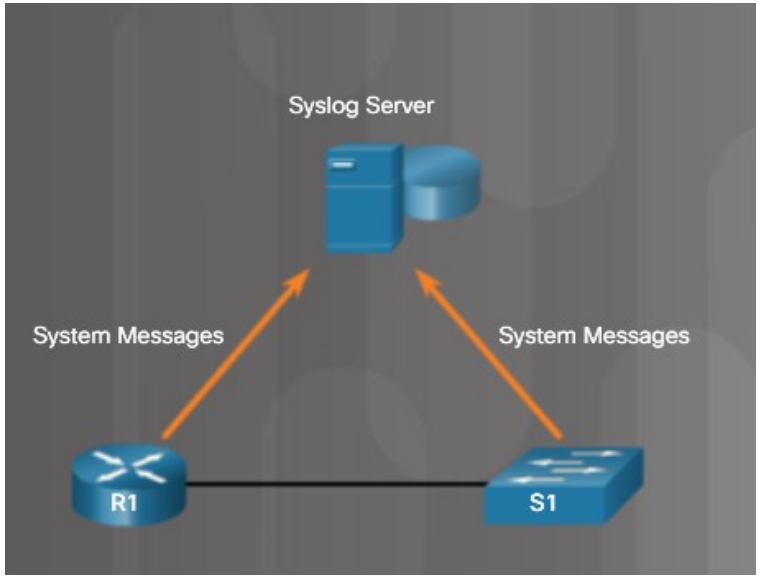
Authentication Server

- Authentication, Authorization, and Accounting (AAA) - Allows access to a network device or a particular network



Syslog Server

- Syslog stores network messages sent by networking devices.



Load Balancer

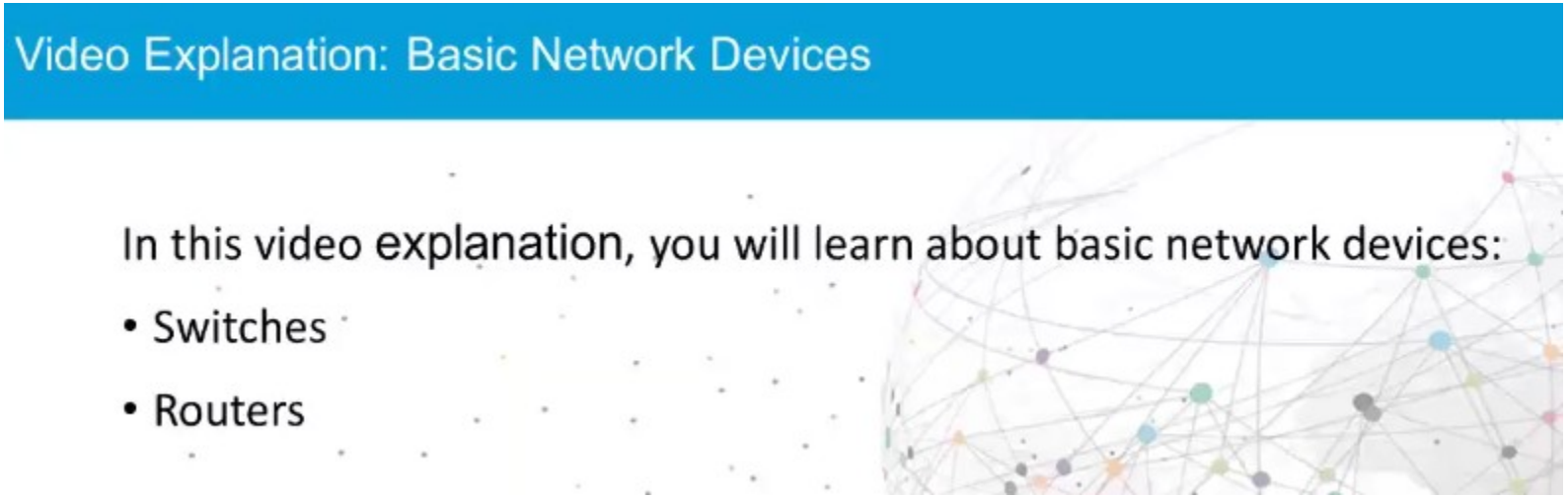
- Some network servers can experience very heavy loads.
- Some examples include streaming media servers, web servers, and email servers.
- Often, multiple servers are providing one service in order to provide timely content.
- A load balancer can be used distribute the demand of requests.
- It is placed in front of the servers to ensure each server is being used as much as the others.
- This prevents things like network timeouts and slow responses.

Scada

- A Supervisory Control and Data Acquisition (SCADA) system is used in an industrial control system (ICS).
- This type of system provides automation for critical services such as national security, water treatment plants, or power suppliers.
- SCADA software runs on a computer to gather data from the devices used by the ICS.
- The SCADA manages the devices remotely typically through the use of satellite or cellular communications.

5.3 Basic Network Devices

Video Explanation - Basic Network Devices

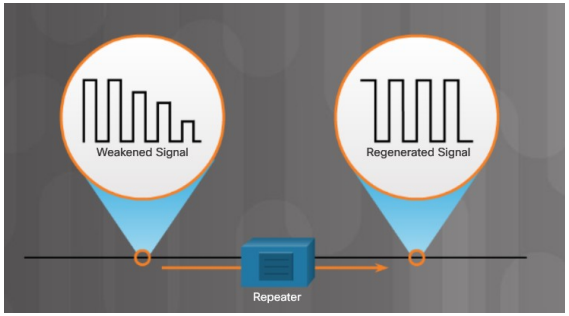


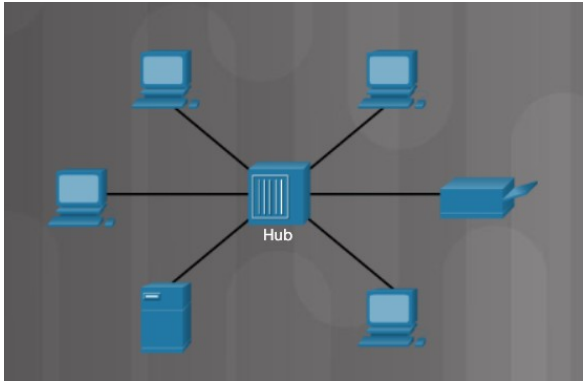
Network Interface Card

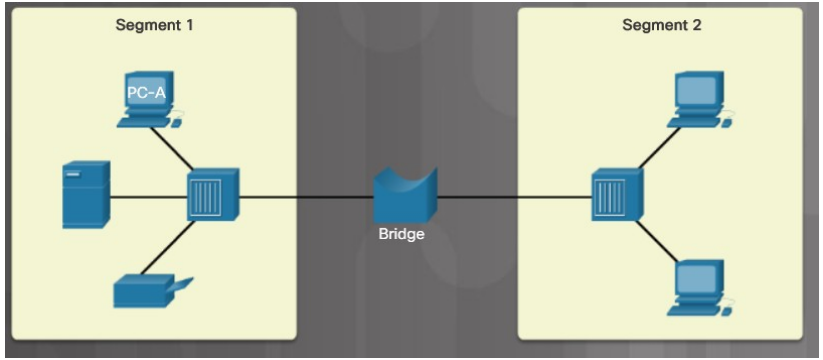
- Todays computers have wired and/or wireless network capability.

Repeaters, Bridges, and Hubs

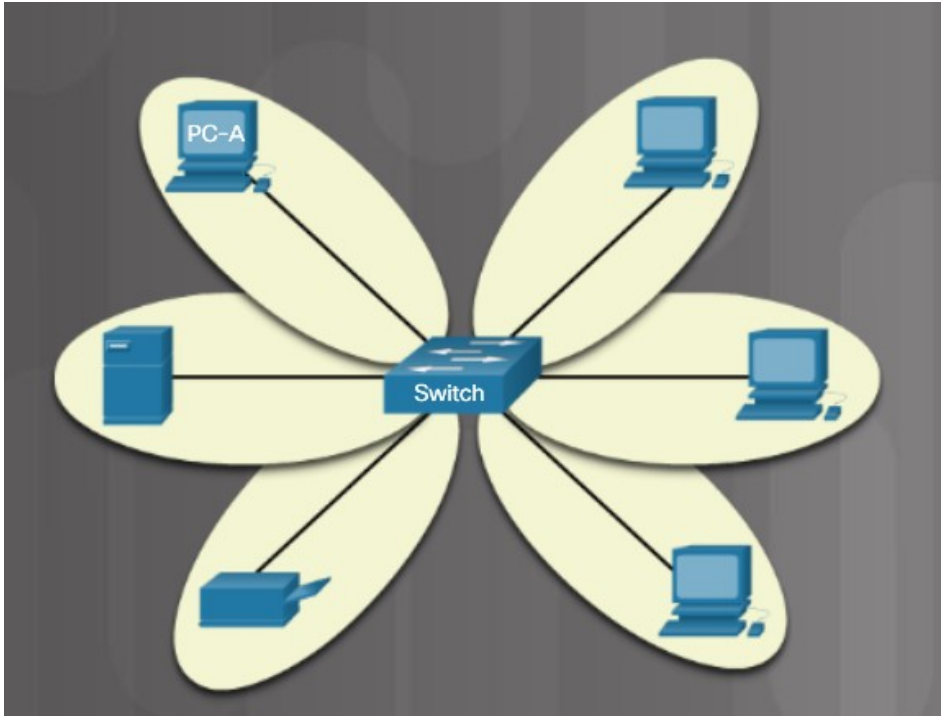
- **Repeaters** – Also called extenders because they regenerate the signal so it can be sent further.
- **Hub** – Receives data on one port and sends to all other ports.
- **Bridge** – Divides a network into two or more segments and tracks which device is on each segment.







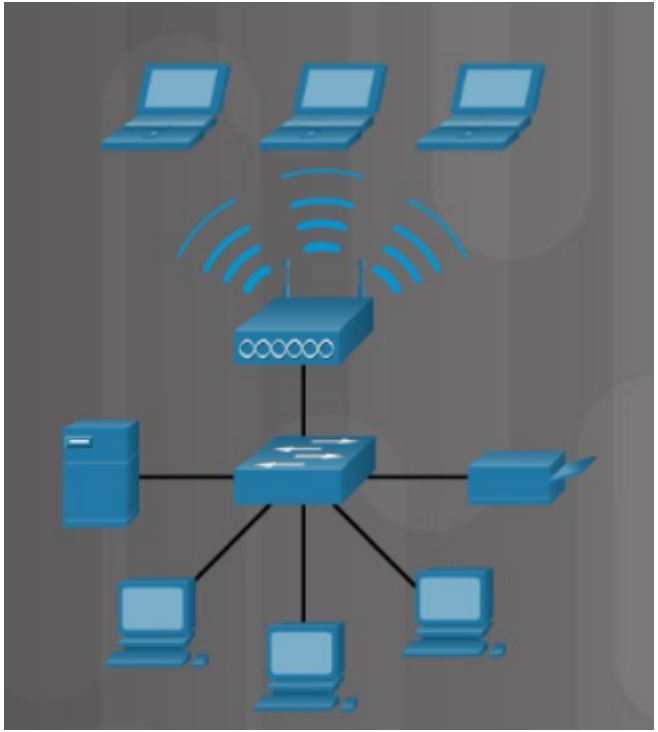
Switches



- Ethernet switches record MAC addresses for each device connected to the switch.
  - Data is sent to a specific device if the MAC address of that device is in the MAC address table.
  - Managed switches are used in a company environment and have additional features.
  - Unmanaged switches are used in home or a small business network.

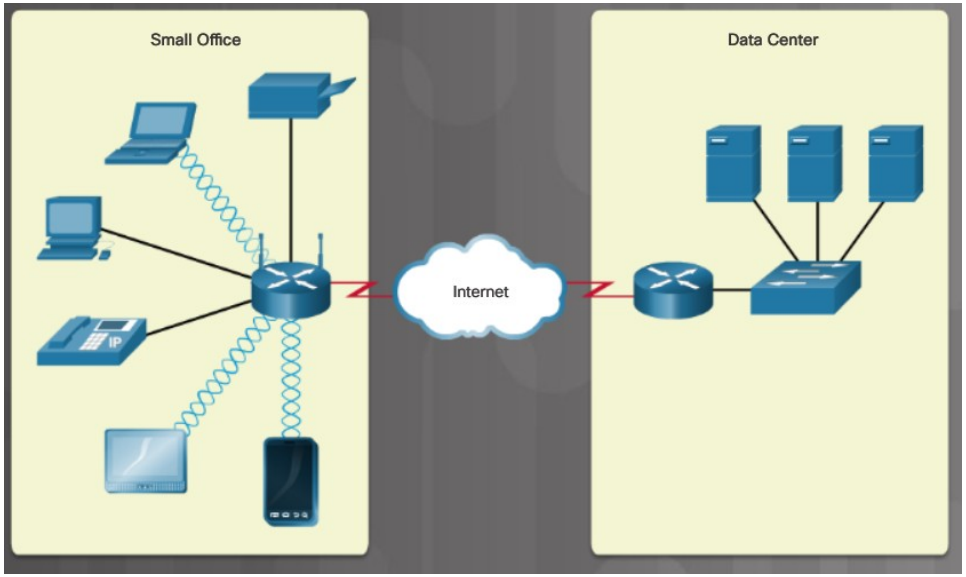
Wireless Access Points

- **Wireless access points (APs)** – provide access to a wireless network for a limited range.



Routers

- Routers connect networks.
  - Use an IP address to forward traffic to other networks
  - Can be a multipurpose device (integrated router) that includes switching and wireless capabilities



Video Explanation – Security Devices

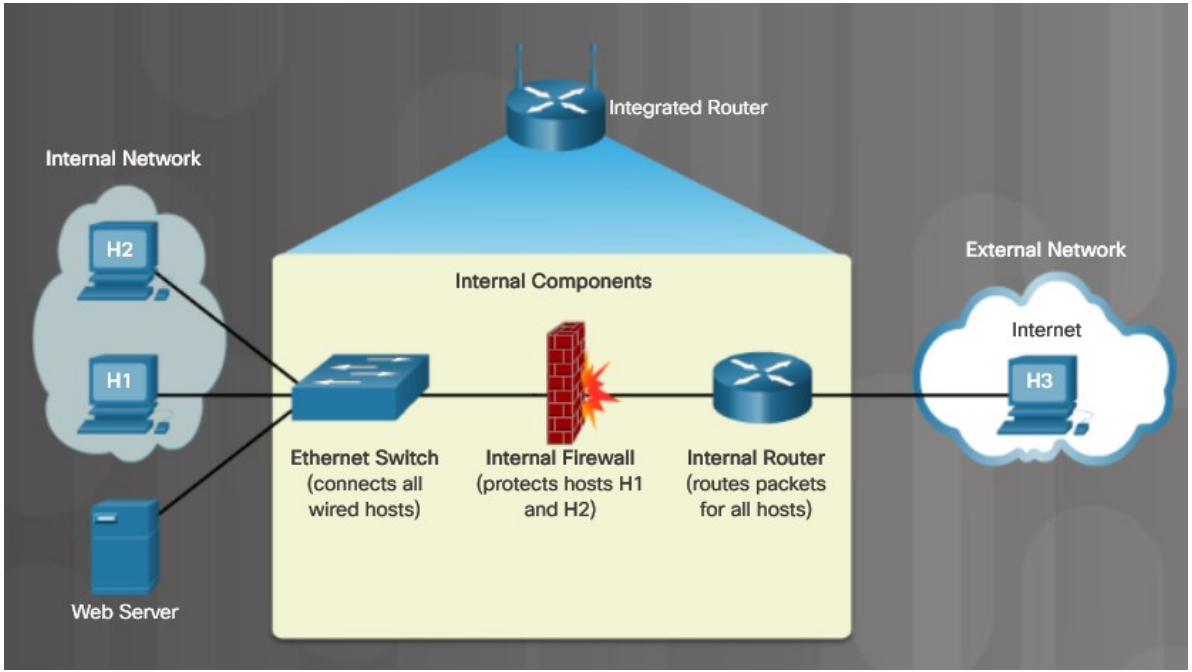
Video Explanation: Security Devices

In this video explanation, you will learn about security devices:

- Firewall
- Integrated Router
- ACLs
- IDS
- IPS

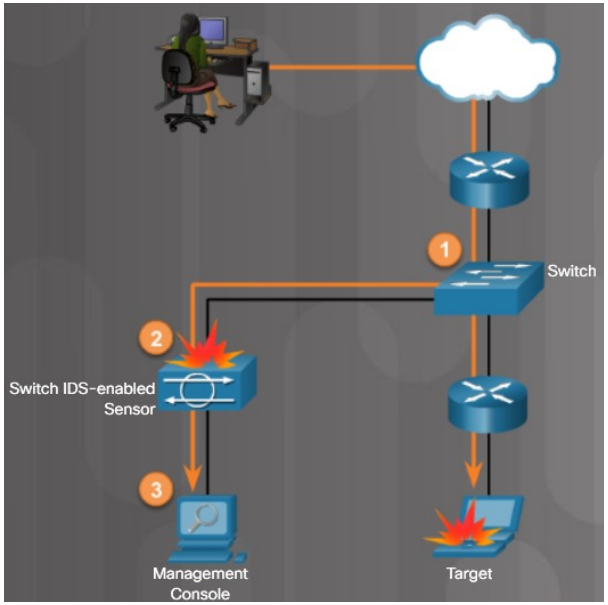
Firewalls

- A firewall protects data and devices connected to a network.
- Firewalls use access control lists (ACLs) which are rules used to determine whether data is permitted (allowed through) or denied.

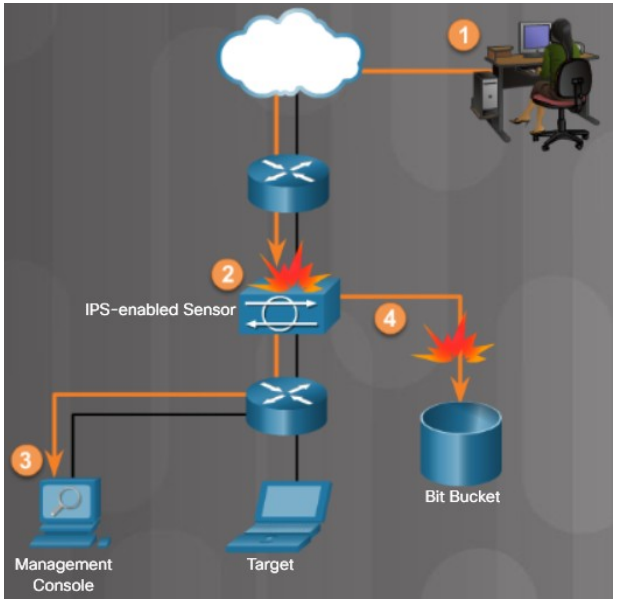


IDS and IPS

An Intrusion Detection System (IDS) monitors traffic and is a passive system.



An Intrusion Prevention System (IPS) actively monitors traffic and takes action when needed.

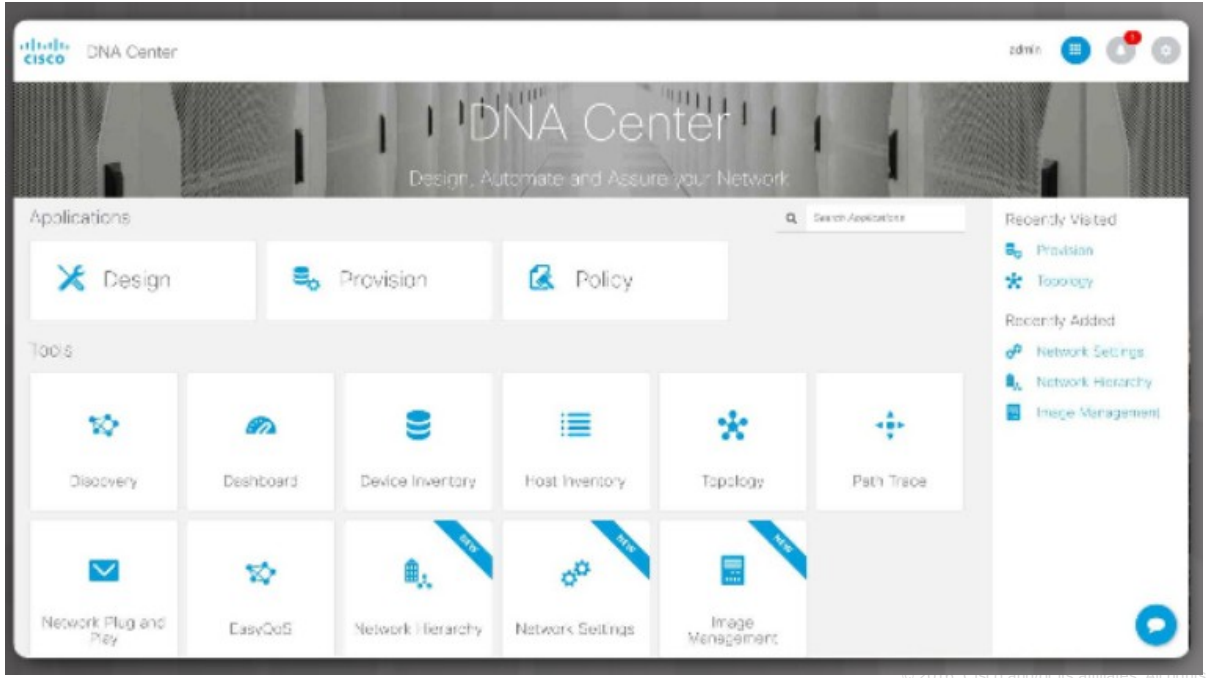


UTMs

- Universal Threat Management (UTM) is an all-in-one security appliance. Features are vendor-specific, but could include:
  - Firewall services
  - IDS/IPS services
  - Additional security services against Zero Day, Denial of Service (DoS) Distributed Denial of Service (DDoS), and spyware
  - Proxy and email filtering
  - Network access control
  - VPN services

Endpoint Management Server

- An endpoint management server monitors end devices such as PCs, laptops, servers, tablets, printers, etc.



Spam Management

- The DNS service is commonly abused by threat actors to assist in their SPAM email campaigns.
- For this reason, DNS servers now use TXT resource records to implement the anti-spam security features detailed in the table.

DNS SPAM Management Feature	Description
Sender Policy Framework (SPF)	• The SPF is a special TXT resource record that identifies SMTP email servers authorized to send emails for an organization. • The RR includes the IP address and email server domain name that receiving servers use to determine legitimacy of emails. • There can only be one SPF RR per domain. • The SPF can also indicate how to process unknown servers including rejecting them, flagging them, or accepting them.
DomainKeys Identified Mail (DKIM)	• DKIM is more advanced than SPF because it leverages cryptographic authentication using digital signatures instead of a list of authorized SMTP servers. • The TXT RR contains the public encryption key of the sending domain that external email servers use to validate the authenticity of the sending email server. • DKIM can replace or be used with SPF.
Domain-based Message Authentication, Reporting, and Conformance (DMARC)	• DMARC is a TXT RR that further enhances SPF and DKIM. • It specifies additional policy information for non-compliant SPF and DKIM DNS queries.

Legacy and Embedded Systems

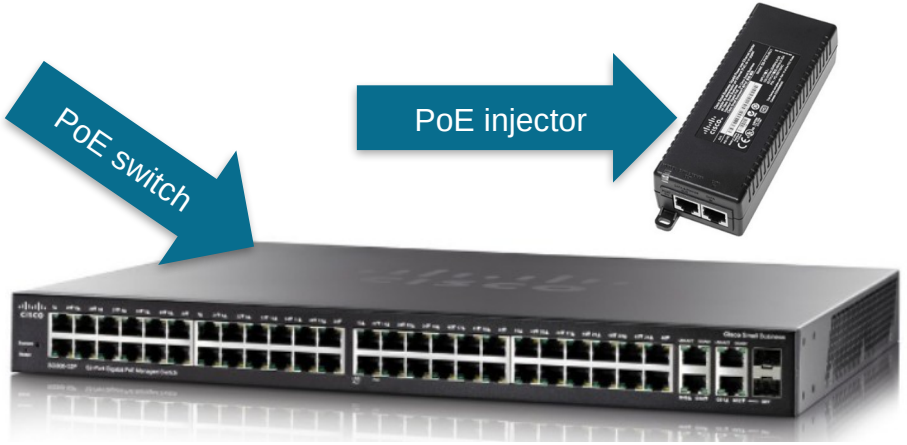
- A legacy system is a device on the network no longer supported, but still in operation.
- An embedded system is a device built into something else such as an appliance. Embedded microchips are contained in legacy systems and embedded systems.
- Legacy systems and embedded systems could be a security risk.

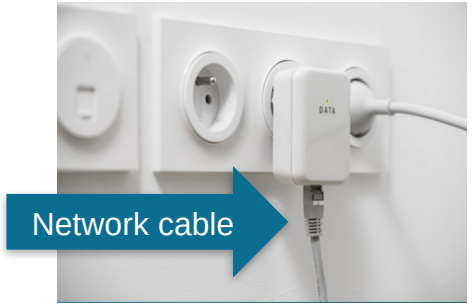
Patch Panel

A centralized place where network cables attach to the back. Patch cables are used to make a connection to another patch panel which connects to a different wiring closet, or to a device such as a switch mounted nearby.

Power over Ethernet and Ethernet over Power

- PoE devices like PoE switches, PoE injectors, IP cameras, Voice over IP (VoIP) phones, and wireless access points (WAPs) are the top five most popular devices.
- Power can also be inserted in the middle of a cable run using a PoE injector.
- There are several IEEE standards for PoE:
  - 802.3af – Can supply up to 13 watts as 350mA at 48 volts.
  - 802.3at (PoE+) – Can supply up to 25 watts as 600 mA.
  - 802.3bt (PoE++ or 4PPoE) – Can supply 51 watts (Type 3) or 73 watts (Type 4)





Ethernet over Power (powerline networking) uses existing electrical wiring to create a network.

Cloud-based Network Controller

- A cloud-based network controller is a remote device used to manage network devices like access points or switches.

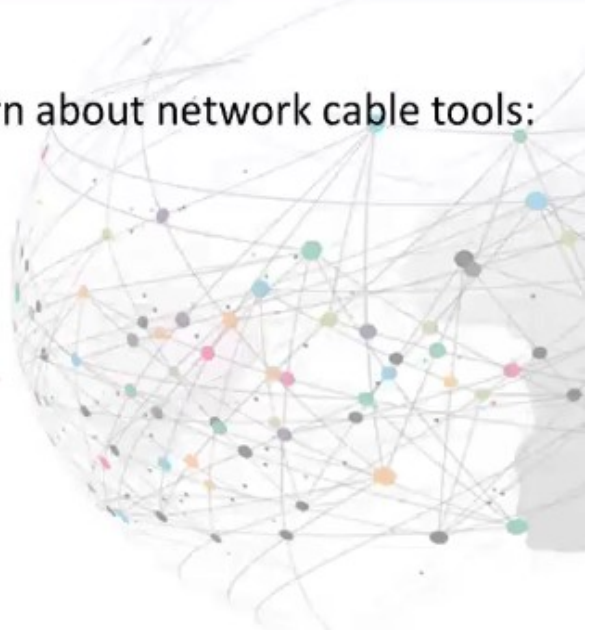
5.4 Network Cables

Video Explanation – Network Cable Tools

Video Explanation: Network Cable Tools

In this video explanation, you will learn about network cable tools:

- Network Cable Crimper
- Wire Strippers
- Cable Connectors
- Punch Down Tool
- Network Cable Tester
- Toner and Probe



Network Tools and Descriptions

- Wire cutters or side cutters

- Wire strippers

- Crimper – used to securely attach an RJ-45 connector

- Punch down tool – used to terminate wires into termination

Network Tools and Descriptions (Cont.)

- Multimeter

- Tone Generator

- Loopback adapter – used to check a port

- Cable Tester

- Wi-Fi analyzer

Network Taps

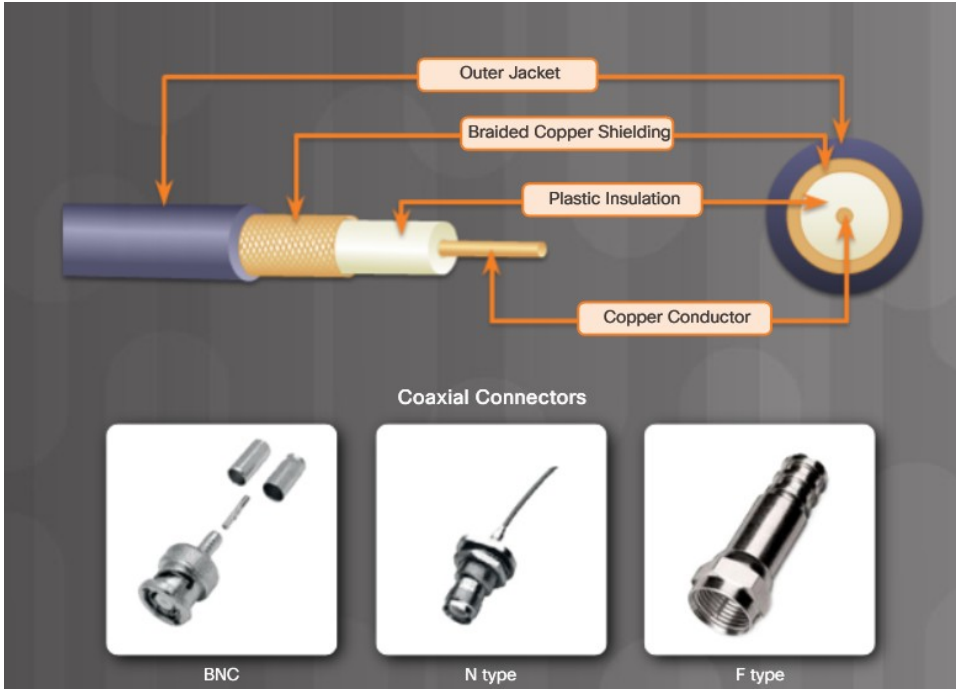
- Sometimes it is necessary to capture network traffic to analyze it, and this can often be done with software such as Wireshark.
- If this is not possible, a network tap can be used to capture the cable signals and send them to analyzing software.
- A network tap can be passive or active (powered):
  - **Passive test access point (TAP)** - This type of TAP is a box with network ports to carry signals in and out. Inside, an inductor or optical splitter is used to copy the signal and send it out a monitor port. The monitor port receives all the traffic from the cable.
  - **Active TAP** - This type of TAP regenerates the signal. Due to the complexity of gigabit signaling, a passive TAP is unable to be used. Also, some fiber links may become corrupt using an optical splitter, so an active TAP is used instead.
- Network sniffing can also be completed using a special port on a network switch, knowning as a switched port analyzer (SPAN)/mirror port.
- A mirror receives a copy of the traffic that are addressed to a specific port or all other ports.

Cable Types

- Cable types used in networking
  - Twisted-pair
  - Coaxial
  - Fiber-optic

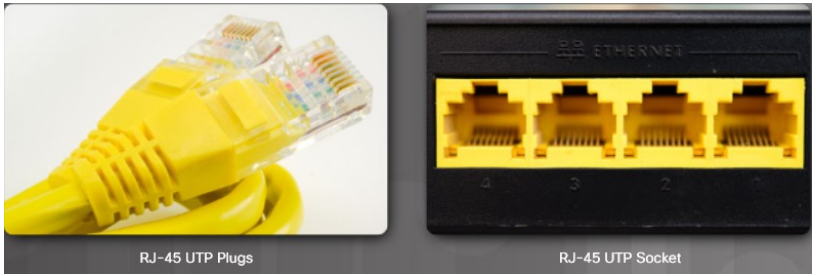
Coaxial Cables

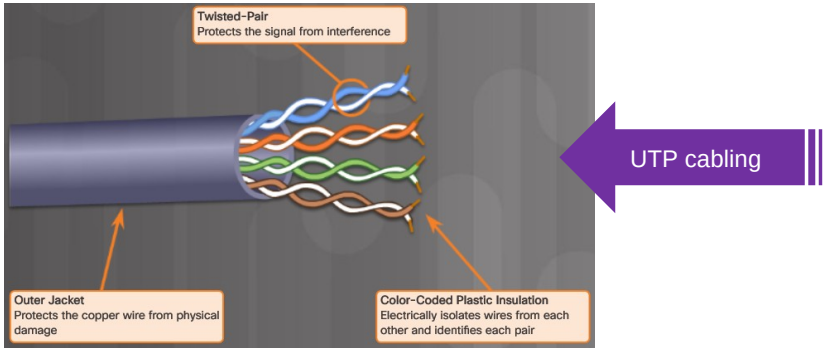
- Coaxial cable
  - Copper or aluminum
  - Used in cable TV systems and satellite communication systems
  - Harder to install, more expensive, and harder to troubleshoot than twisted-pair cabling

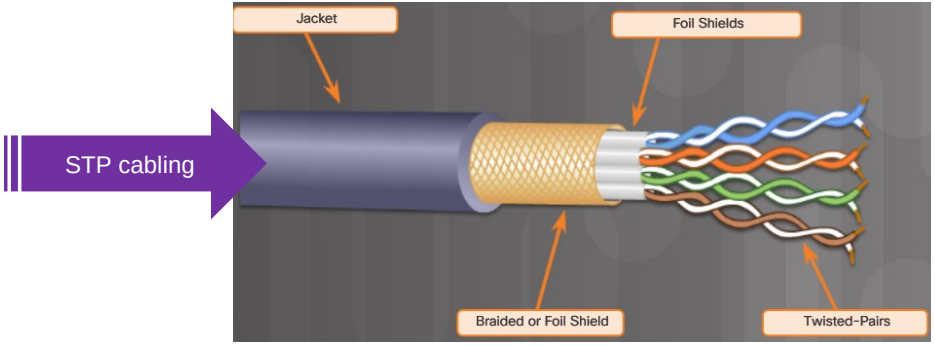


Twisted-Pair Cables

- Twisted-pair cabling types
  - Unshielded twisted-pair (UTP)
  - Shielded twisted-pair (STP)
- UTP
  - Most common
  - Four pairs of color-coded wires
  - Prone to electromagnetic interference (EMI) and radio frequency interference (RFI)
- STP
  - Better protection against EMI and RFI
  - More expensive and harder to install







Twisted-Pair Category Ratings

Speed	Features
100 Mb/s at 100 MHz	• The first widely adopted 4 pair UTP that replaced Cat 3 UTP in Ethernet LANs. • Manufactured with higher standard than Cat 3 to allow for higher data transfer rates.

Cat 5 UTP

Cat 5e UTP

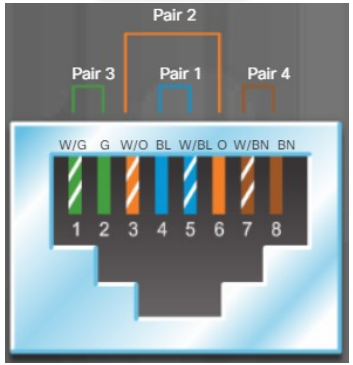
Speed	Features
1 Gb/s at 100 MHz	• Manufactured with higher standard than Cat 5 to allow for higher data transfer rates. • More twists per foot than Cat 5 to better prevent EMI and RFI from outside sources.

Speed	Features
1 Gb/s at 250 MHz (Cat 6a – 500 MHz)	• Manufactured with higher standard than Cat 5e to allow for higher data transfer rates. • More twists per foot than Cat 5e to better prevent EMI and RFI from outside sources. • May have a plastic divider to separate pairs of wires inside the cable to better prevent EMI and RFI. • Good choice for customers using applications that require large amounts of bandwidth, such as videoconferencing or gaming. • Cat 6a has better insulation and performance than Cat6.

Cat 6 UTP

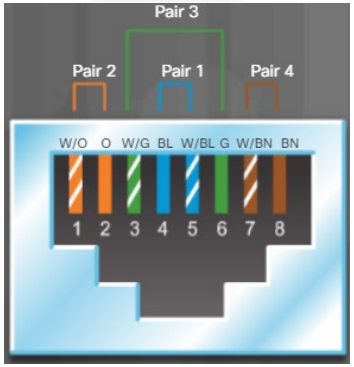
Twisted-Pair Wire Schemes

T568A



Color Labels	
W/G	Green with white stripe
G	Green
W/O	Orange with white stripe
BL	Blue
W/BL	Blue with white stripe
O	Orange
W/BN	Brown with white stripe
BN	Brown

T568B



Color Labels	
W/O	Orange with white stripe
O	Orange
W/G	Green with white stripe
BL	Blue
W/BL	Blue with white stripe
G	Green
W/BN	Brown with white stripe
BN	Brown

When creating a cable to connect a network device to a wall jack or from the patch panel to a switch, make both ends of the cable the same standard.

Video Explanation – Build and Test a Network Cable

Video Demonstration: Build and Test a Network Cable

In this video demonstration, you will learn to build and test a network cable:

- **Step 1**: Cut the cable to length.
- **Step 2**: Strip the cable to expose the wires.
- **Step 3**: Untwist the wire pairs and remove the string and separator if necessary.
- **Step 4**: Organize the wires in the correct color code and trim the wires to length.
- **Step 5**: Place the wire ends into the RJ-45 connector.
- **Step 6**: Ensure the wire ends reach the end of the RJ-45 connector.
- **Step 7**: Crimp the RJ-45 connector to the cable.
- **Step 8**: Test the cable for continuity.

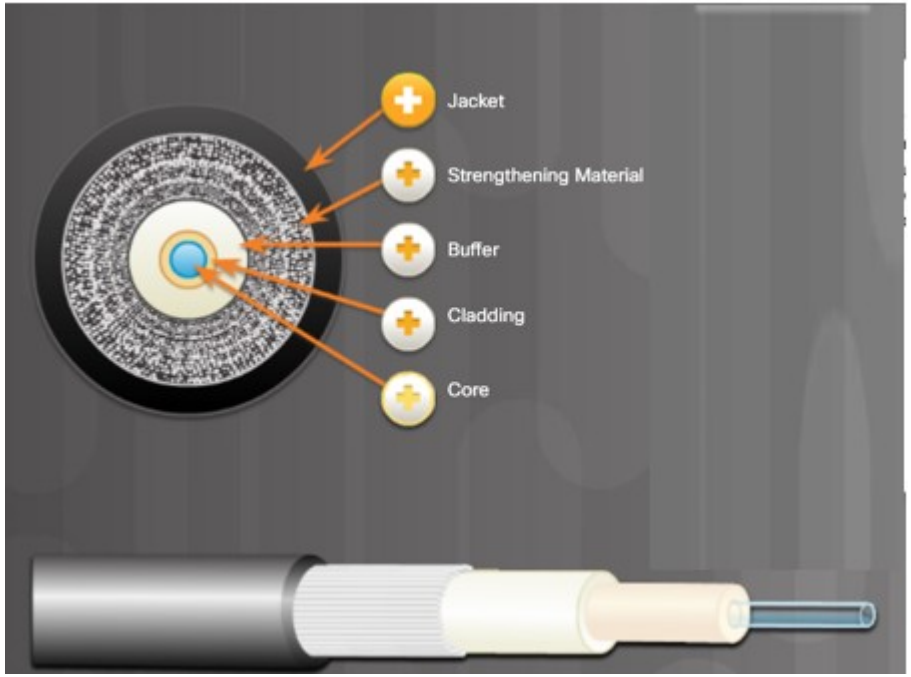
Lab – Build and Test Network Cables

- In this lab, you will build and test a straight-through Unshielded Twisted-Pair (UTP) Ethernet network cable.

Note: With a straight-through cable, the color of wire used by pin 1 on one end is the same color used by pin 1 on the other end, and similarly for the remaining seven pins. The cable will be constructed using either TIA/EIA T568A or T568B standards for Ethernet. This determines which color wire is to be used on each pin. Straight-through cables are normally used to connect a host directly to a switch or a wall plate in an office area.

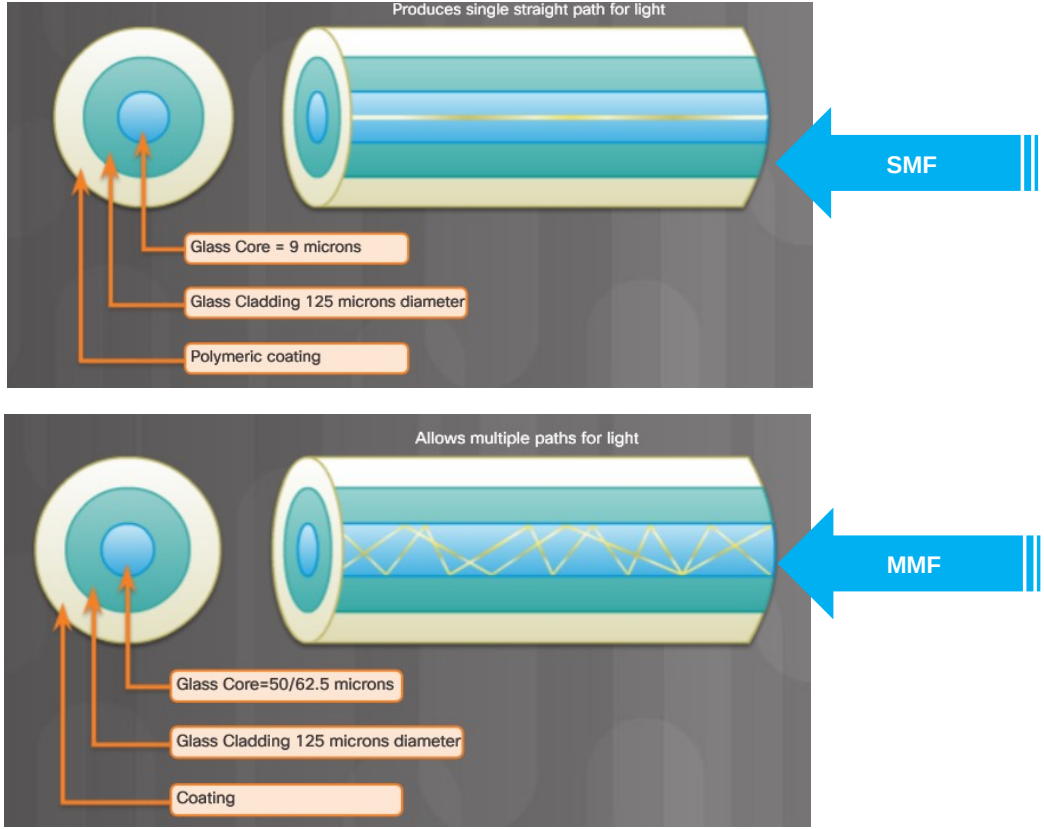
Fiber-Optic Cables

- Fiber-Optic cables
  - Use light to transmit signals
  - Not affected by EMI or RFI

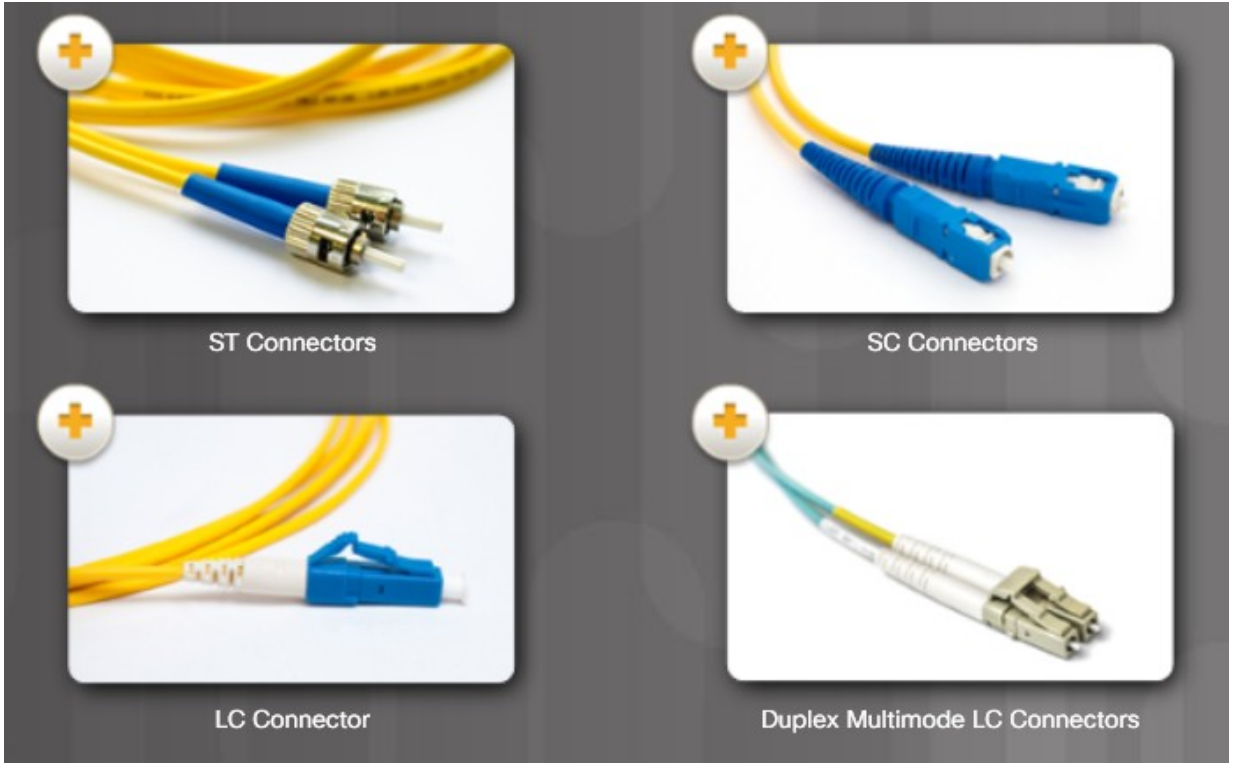


Types of Fiber Media

- Single-mode fiber (SMF)
  - Small core
  - Uses laser technology to send one beam of light
  - Long distances
- Multimode fiber (MMF)
  - Larger core
  - Uses LEDs to send light
  - Light is injected at different angles
  - Cheaper
  - Bandwidth up to 10 Gb/s up to 550 meters



Fiber-Optic Connectors



5.5 Chapter Summary

Chapter 5: Network Concepts

- Explain components and types of computer networks.
- Explain networking protocols, standards and services.
- Explain the purpose of devices on a network.
- Explain the characteristics of network cables.