# Chapter 1: LAN Design

Chapter 1 - Sections & Objectives

- 1.1 Campus Wired LAN Designs

  - Explain why it is important to design a scalable hierarchical network.

    - Describe hierarchical small business network designs.

    - Explain considerations for designing a scalable network.

- 1.2 Campus Network Device Selection

  - Select network devices based on feature compatibility and network requirements.

    - Select the appropriate switch hardware features to support network requirements in small to medium-sized business networks.

    - Describe the types of routers available for small to medium-sized business networks.

    - Configure basic settings on a Cisco IOS device.
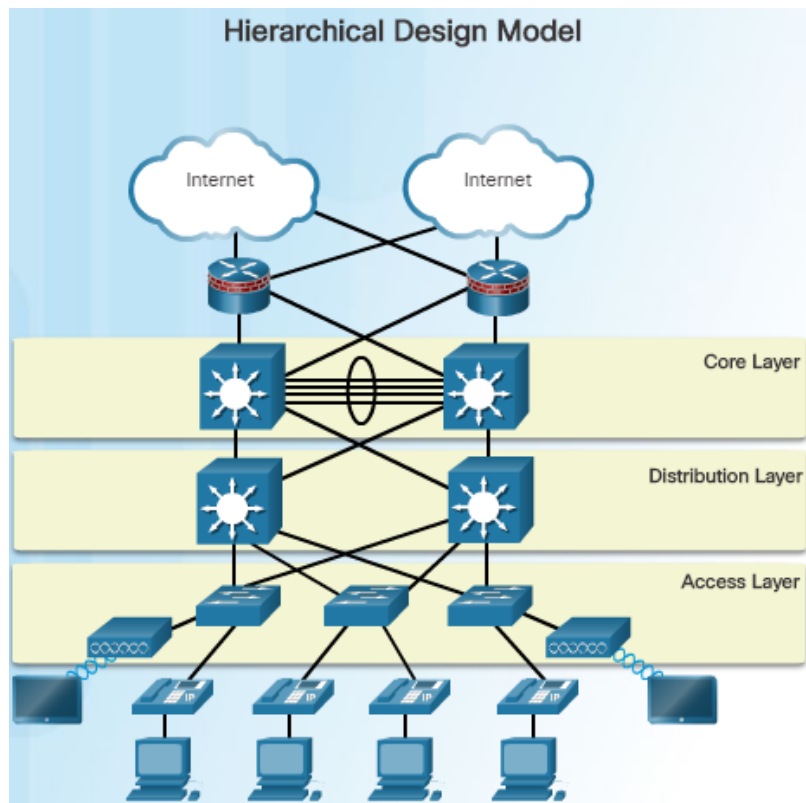
1.1 Campus Wired LAN Designs

The Need to Scale the Network
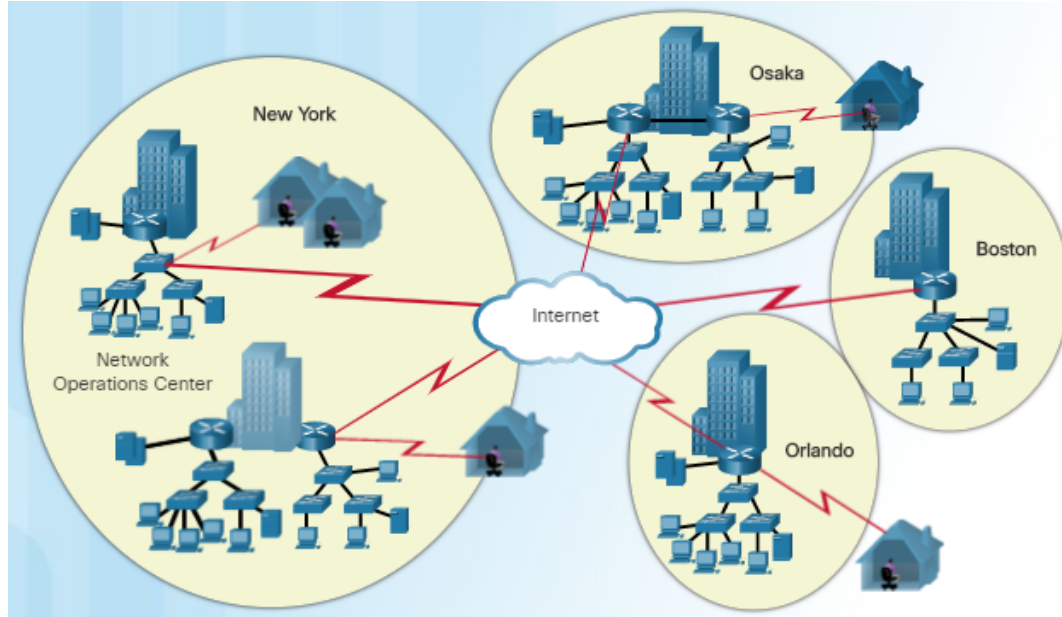
- A company with a small network with one site and a connection to the Internet might grow into an enterprise with a central location with numerous remote sites across the globe.

- All enterprise networks must:
  - Support the exchange of various types of network traffic
  - Support critical applications
  - Support converged network traffic
  - Support diverse business needs
  - Provide centralized administrative control

- The LAN is the networking infrastructure that provides access to network resources for end users over a single floor or a building.

Hierarchical Design Model

Hierarchical Design Model

- The campus wired LAN uses a hierarchical design model to break the design up into modular layers.

- Breaking the design up into layers allows each layer to implement specific functions, which simplifies the network design for easier deployment and management.

- A hierarchical LAN design includes three layers as shown in the figure:

  - Access layer

  - Distribution layer

  - Core layer

- Some smaller enterprise networks implement a two-tier hierarchical design and collapse the core and distribution layers into one layer.

Design for Scalability
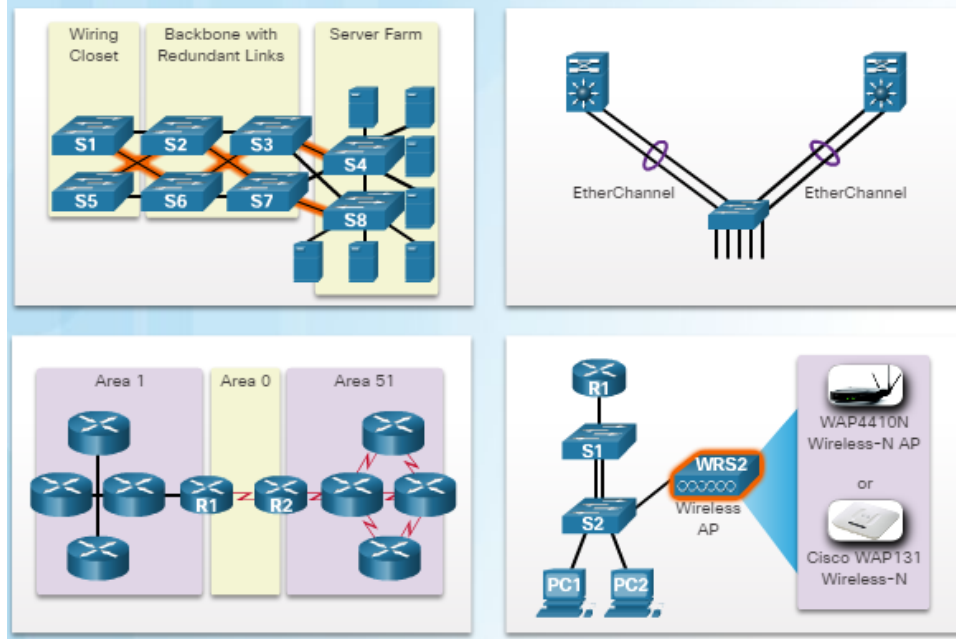
- The network designer must develop a strategy to enable the network to be available and scale easily and effectively.

- Use expandable, modular equipment or clustered devices that can be easily upgraded to increase capabilities.

- Design a hierarchical network to include modules that can be added, upgraded, and modified as needed.

- Create an IPv4 or IPv6 address strategy that is hierarchical.

- Choose routers or multilayer switches to limit broadcasts and filter undesirable traffic from the network.

- Implement redundant links between critical devices and between access and core layers.

Planning for Redundancy
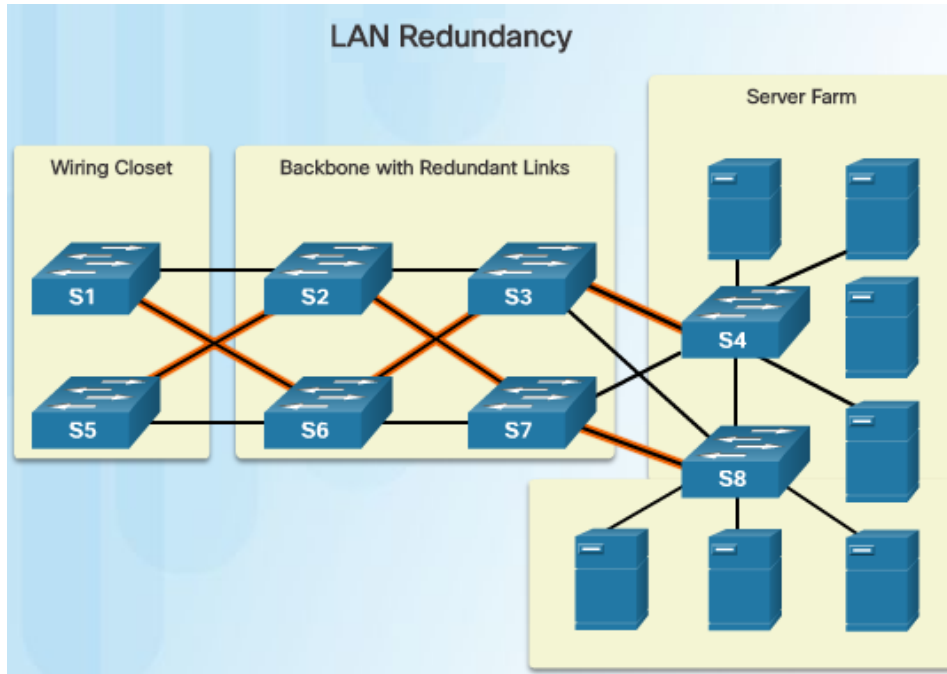
LAN Redundancy

- Redundancy is an important part of the network design for preventing disruption of network services.

- Minimize the possibility of a single point of failure by recognizing these facts:
  - Installing duplicate equipment and providing failover services for critical devices is necessary.
  - Redundant paths offer alternate physical paths for data to traverse the network.
  - Spanning Tree Protocol (STP) is required with redundant paths in a switched Ethernet network to prevent Layer 2 loops.

- STP provides a mechanism for disabling redundant paths in a switched network until the path is necessary such as when a failure occurs.
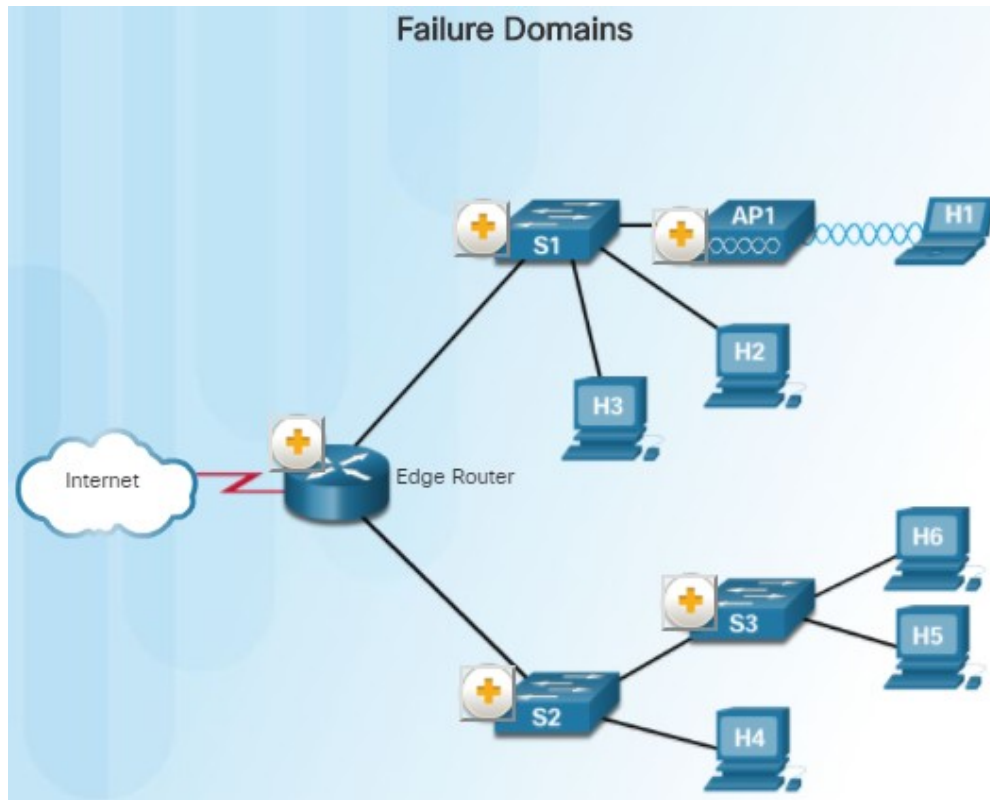
Failure Domains
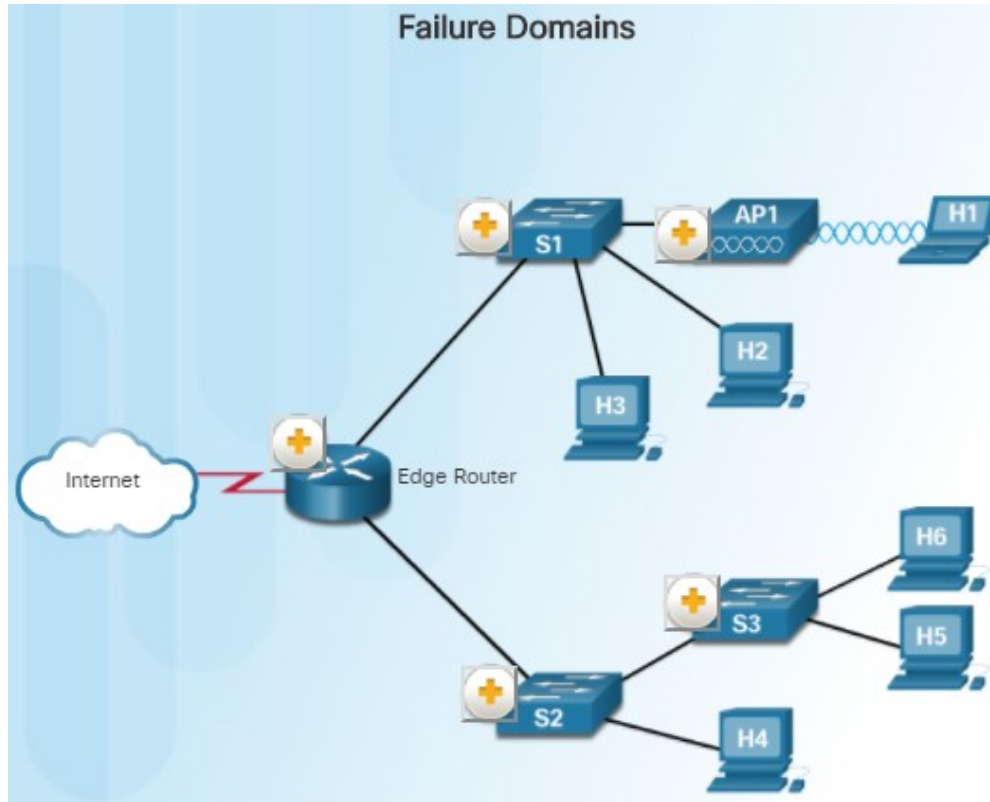
Failure Domains

- A well-designed network should limit the size of failure domains.

- A failure domain is the area of a network that is impacted when a critical device or network service experiences problems.

- The function of the devices that fail will determine the impact of the failure domain.

- Use redundant links and reliable enterprise-class equipment to minimize the disruption in a network.

- Smaller failure domains reduce the impact of a failure but also make troubleshooting easier.

Failure Domains (Cont.)

Failure Domains

- In the hierarchical design model, it is usually easier to control the size of a failure domain in the distribution layer.

- In the distribution layer, network errors can be contained to a smaller area which will impact fewer users.

- When using Layer 3 devices at the distribution layer, every router functions as a gateway for a limited number of access layer users.

- Switch Block Deployment

  - Routers or multilayer switches are usually deployed in pairs with access layer switches evenly divided between them.

  - Each switch block acts independently of the others, which reduces the impact of failures.

Increasing Bandwidth

Advantages of EtherChannel
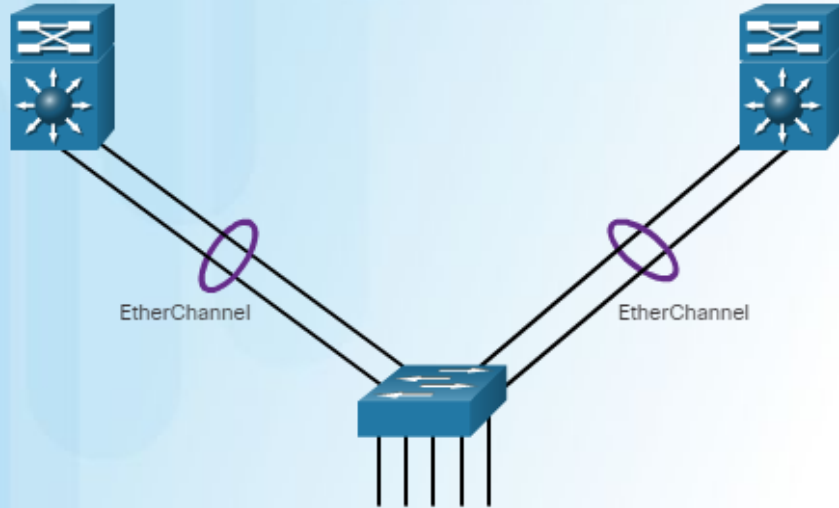
- In a hierarchical network design, some links between access and distribution layer switches may need to process a greater amount of traffic than other links do.

- As multiple links converge into a single link, it is possible for this link to become a bottleneck.

- EtherChannel is a form of link aggregation that will allow the network administrator to increase the amount of bandwidth between devices by creating one logical link out of several physical links.

- EtherChannel uses existing switch ports.

- The EtherChannel configuration takes advantage of load balancing between links that are part of the same EtherChannel.

Expanding the Access Layer

Wireless LANs

WAP4410N Wireless-N AP

or

Cisco WAP131 Wireless-N
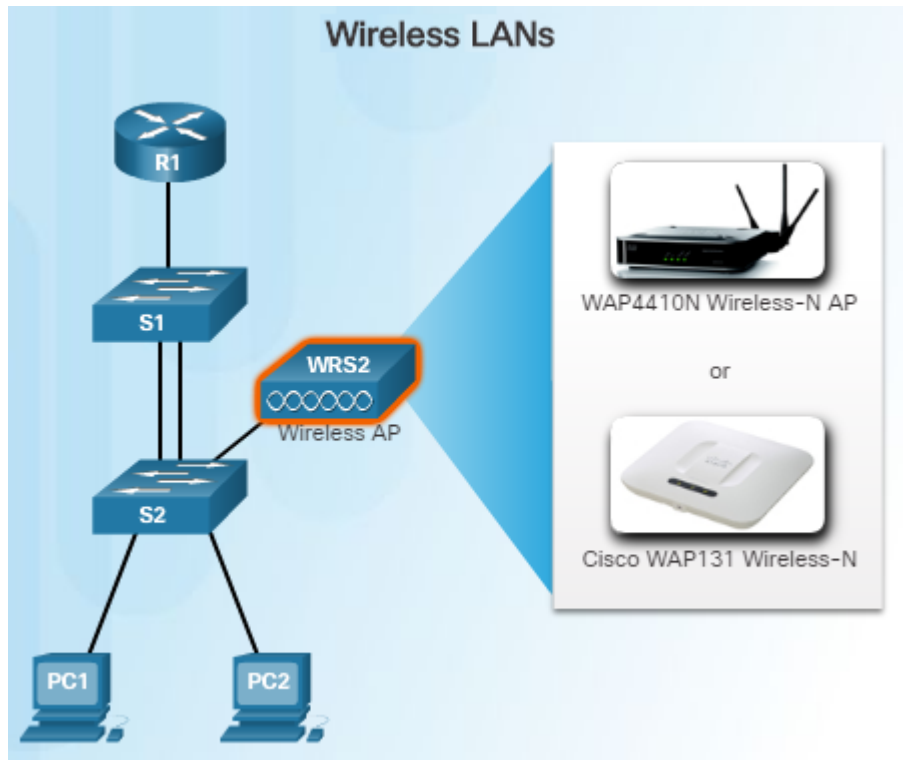
- Wireless connectivity is an important aspect of extending access layer connectivity.

- The network must be designed to be able to expand network access to individuals and devices, as needed.

- Advantages of wireless connectivity include increased flexibility, reduced cost, and the ability to adapt to changing network and business requirements.

- End devices require a wireless NIC that incorporates a radio transmitter/receiver, appropriate software drivers, and also a wireless access point (AP) to connect to.

Fine-tuning Routing Protocols

Multiarea OSPF

Area 1 | Area 0 | Area 51

R1   R2
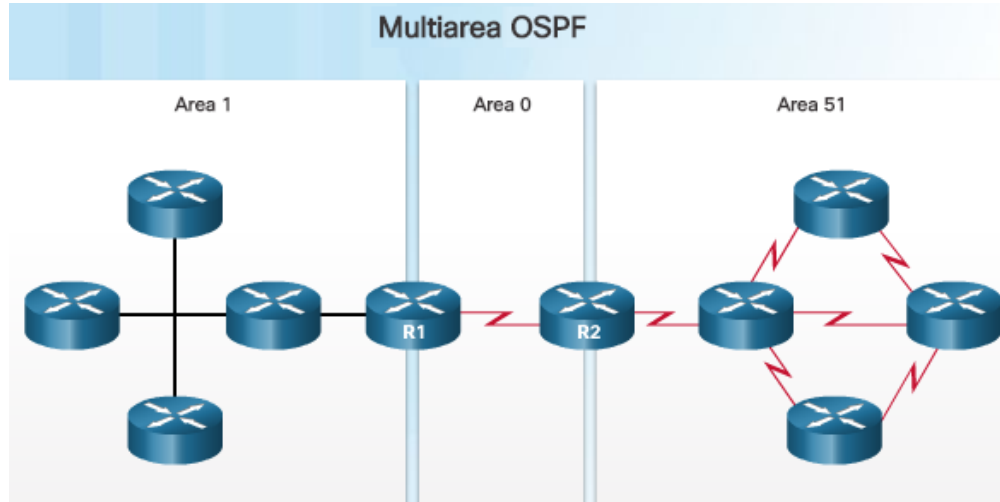
- OSPF supports a two-layer hierarchical design, referred to as multiarea OSPF.

- Multiarea OSPF requires an Area 0 (backbone area)

- Non-backbone areas must be directly connected to Area 0.

- Advanced routing protocols, such as OSPF and EIGRP are used in large networks.

- Link-state routing protocols such as OSPF works well for larger hierarchical networks where fast convergence is important.

- Single Area OSPF has one area – Area 0.

- Cisco's proprietary distance vector routing protocol, called EIGRP, is another popular routing protocol. It is designed for larger networks using primarily Cisco routers.

- Although the configuring EIGRP is simple, the underlying features and options of EIGRP are extensive and robust.

1.2 Selecting Network Devices

Switch Platforms

Modular Configuration Switches

- The chassis accepts line cards that contain the ports

- Selecting the proper hardware to meet the current network requirements is critical when designing a network.

- There are five categories of switches for enterprise networks:

  - Campus LAN switches

  - Cloud-managed switches

  - Data center switches

  - Service provider switches

  - Virtual networking

- Various factors to consider when selecting switches include these:

  - Fixed vs. modular configuration

  - Stackable vs. nonstackable

  - Thickness of the switch (rack units)

  - Cost, port density, power, reliability

Port Density

Port Densities

24-port switch

48-port switch

Modular switch with up to 1000+ ports
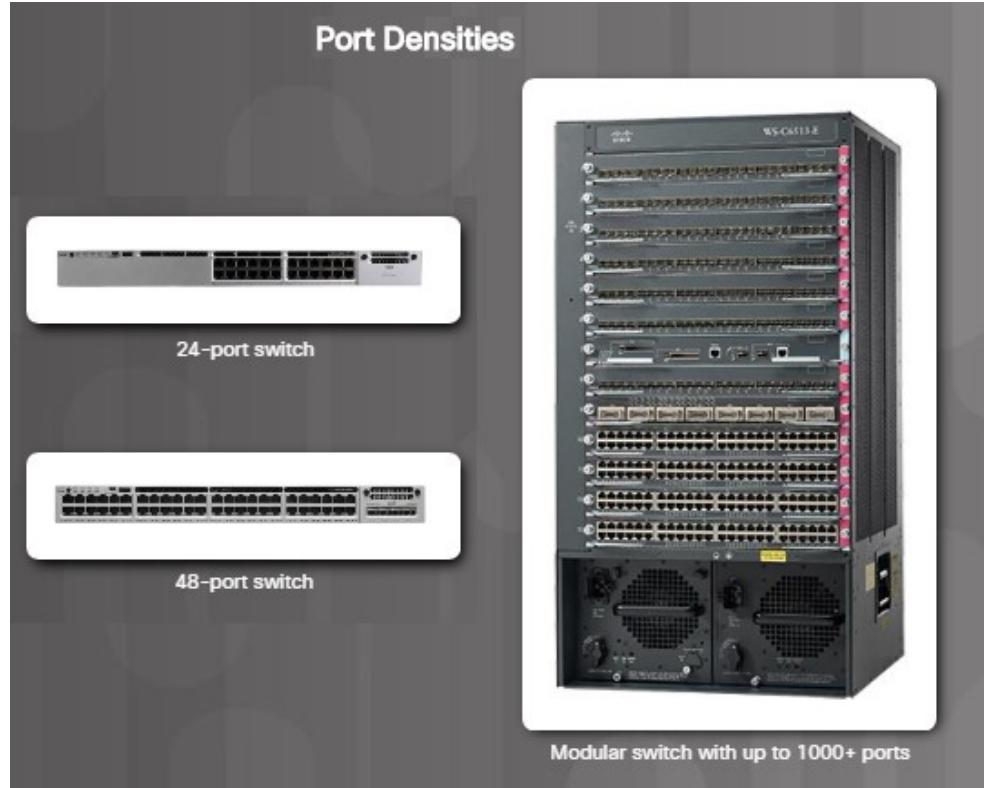
- The port density of a switch refers to the number of ports on a single switch.

- Fixed configuration switches support a variety of port density configurations:
  - Cisco Catalyst 3850 24 port and 48 port switches (see figure)
  - The 48 port switch has an option for four additional ports for pluggable SFP devices.

- The modular Catalyst 6500 switch shown in the figure can support over 1,000 switch ports.

- Modular switches are usually more appropriate in large networks in order to reduce space and power issues.

Forwarding Rates

Forwarding Rate

24-port Gigabit Ethernet Switch

Capable of switching 24 Gb/s of traffic

48-port Gigabit Ethernet Switch

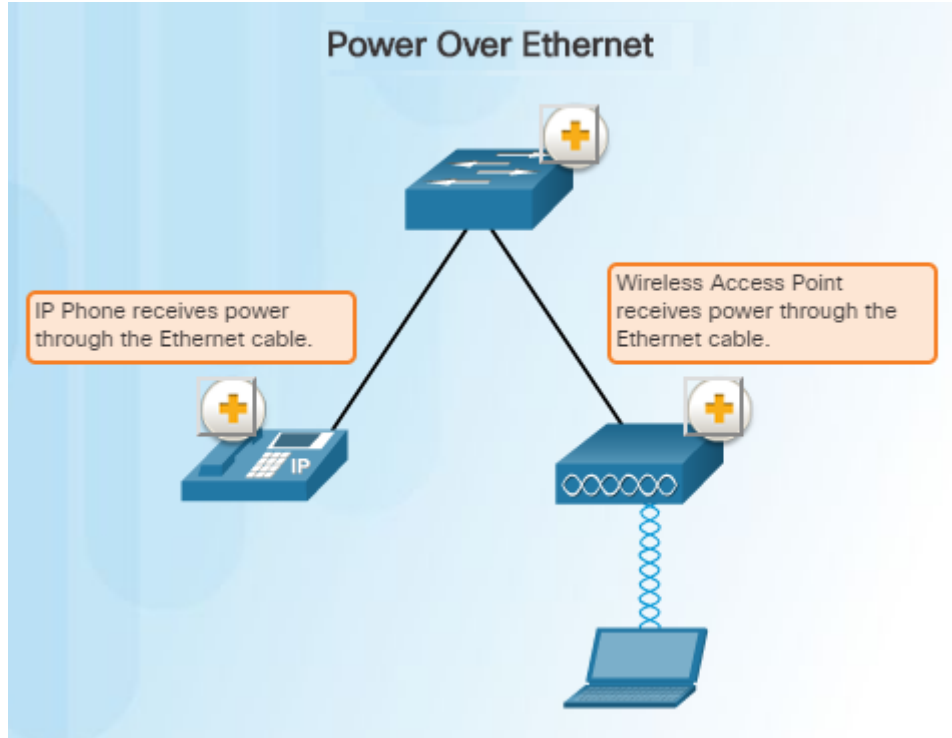Capable of switching 48 Gb/s of traffic
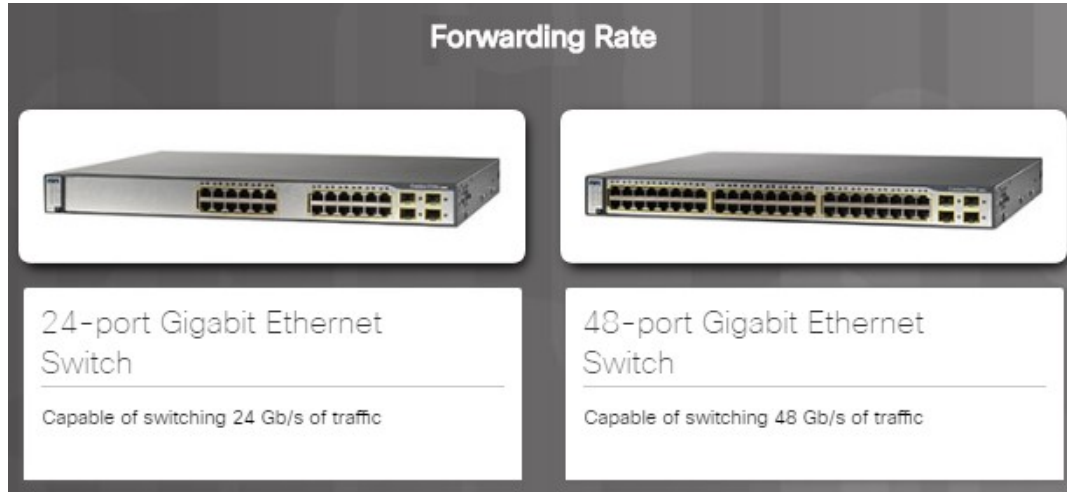
- Switch product lines are classified by forwarding rates.

- Forwarding rates define the processing capabilities of a switch by rating how much data the switch can process per second.

- Entry-level switches have lower forwarding rates than enterprise-level switches.

- Forwarding Rates are an important factor when selecting a switch because if the rate is too low, it will not be able to support full wire-speed communication across all of its switch ports.

- Access layer switches typically do not need to operate at full wire speed because they are physically limited by their uplinks to the distribution layer.

- Higher performing switches are needed at the distribution and core layers.

Power over Ethernet

Power Over Ethernet

IP Phone receives power through the Ethernet cable.

Wireless Access Point receives power through the Ethernet cable.

- PoE allows the switch to deliver power to a device over the existing Ethernet cabling.

- This eliminates the need for a power cable to the networked device such an IP phone or wireless access point.

- PoE allows more flexibility when installing wireless access points and IP phones by allowing them to be installed anywhere that there is an Ethernet cable.

- The Cisco Catalyst 2960-C and 3560-C Series compact switches support PoE pass-through.

- PoE pass-through devices can power PoE devices as well as the switch itself by drawing power from certain upstream switches.

Multilayer Switching

Cisco Catalyst 2960 Series Switches

- Multilayer switches are typically deployed in the core and distribution layer.

- Multilayer switches can do the following:
  - Build a routing table and support routing protocols
  - Forward IP packets at a rate close to that of Layer 2 forwarding

- Multilayer switches often support specialized hardware called application-specific integrated circuits (ASICs).

- ASICs along with dedicated software can streamline the forwarding of IP packets independent of the CPU.

- There is a trend in networking toward a pure Layer 3 switched environment.

Router Requirements
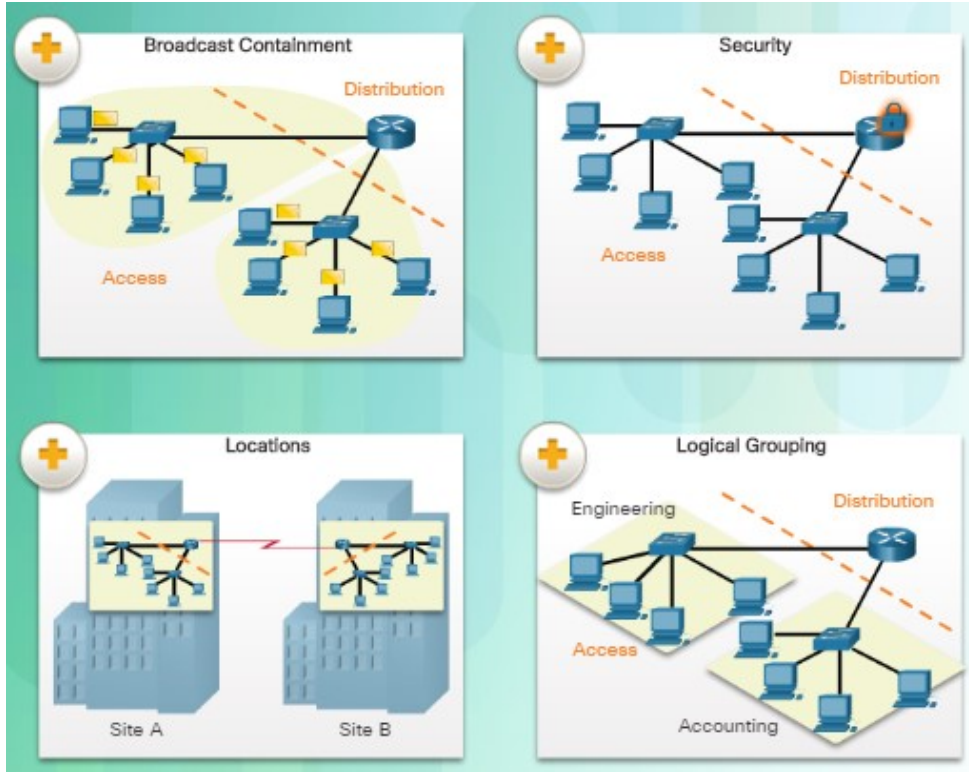
- Routing is required within the distribution layer of an enterprise network. Without routing, packets could not leave the local network.

- Routers are critical networking devices because they are responsible for:

  - Connecting businesses and homes to the Internet

  - Interconnecting multiple sites within an enterprise network

  - Connecting ISPs on the Internet

  - Translating between different media types and protocols

  - Finding alternate paths if a link or path goes down

Router Requirements (Cont.)
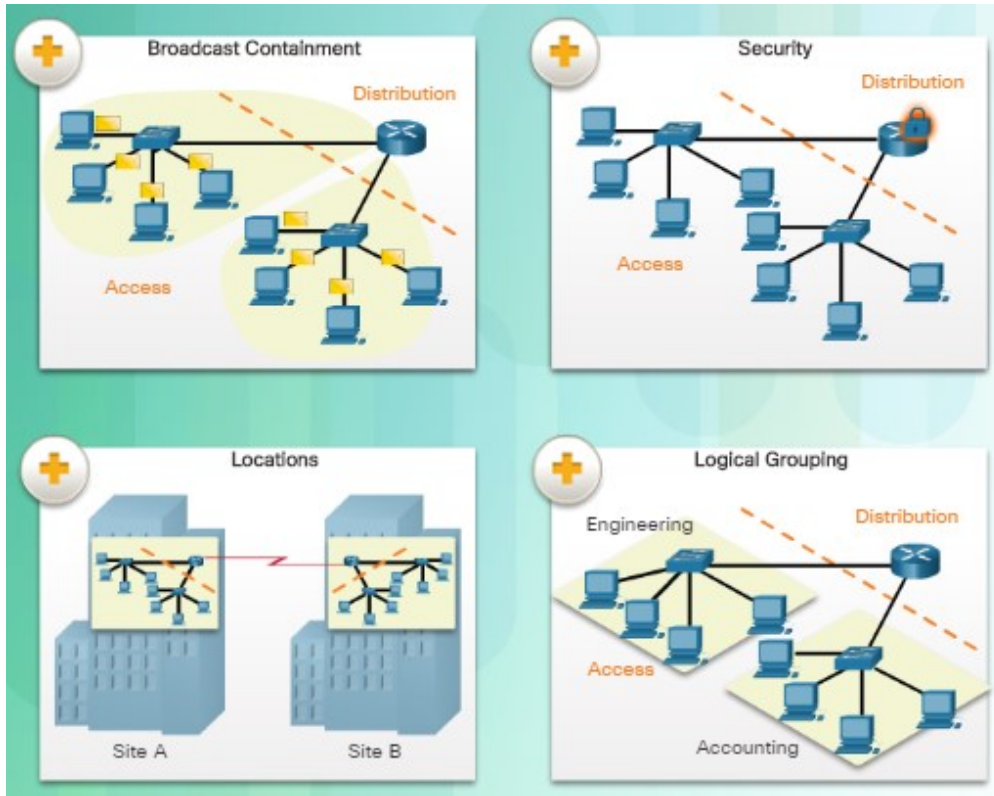
- Routers also serve other important functions:

  - Provide broadcast containment by limiting broadcasts to the local network

  - Group users logically by application or department

  - Provide enhanced security through the use of access control lists in order to filter unwanted traffic.

  - Interconnect geographically separated locations.

In-band versus Out-of-band Management

Out-of-Band Router Configuration | In-Band Router Configuration

Console Port

Ethernet Interface

Auxiliary Port

IP Interface

Modem

Modem

PSTN
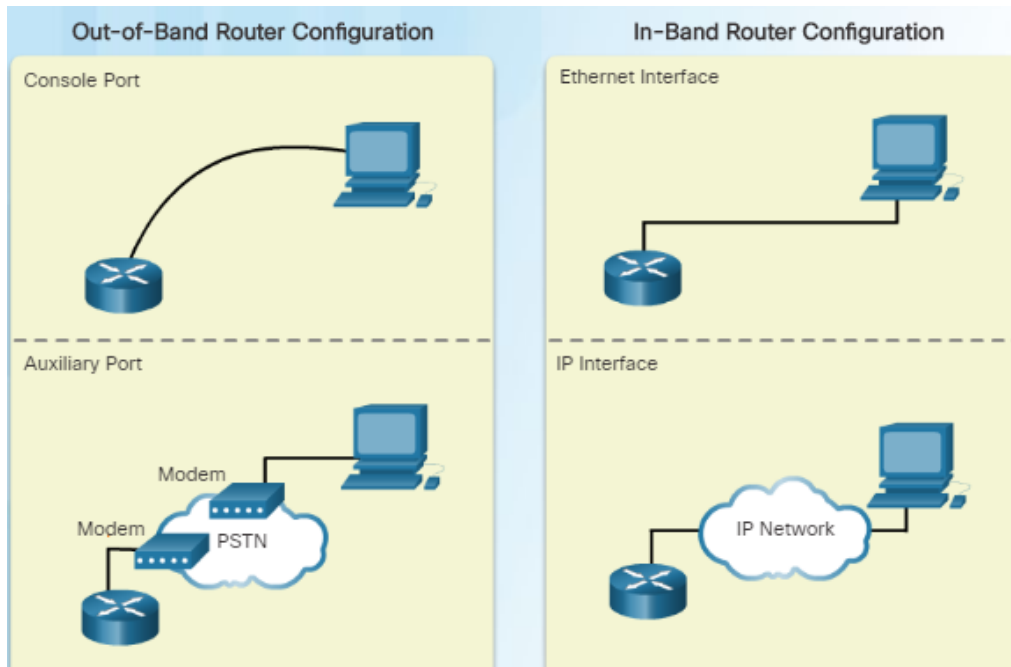
IP Network

- There are two methods for connecting a PC to a network device for configuration and monitoring tasks:

  - Out-of-band management through the use of the console or AUX port is used for the initial configuration or when a network connection is not available.

  - In-band management is used to configure or monitor the device remotely through a network connection using either SSH or HTTPs.

    - A reachable and operational network interface is required.

    - For security reasons, the use of Telnet and HTTP are not recommended.

Basic Router CLI Commands

Enable a Router with RIPv2

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exec-timeout 0 0
R1(config-line)# line vty 0 15
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)# banner motd $ Authorized Access Only! $
R1(config)# interface GigabitEthernet0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 172.16.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface Serial0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ip address 172.16.3.1 255.255.255.252
R1(config-if)# clock rate 128000
R1(config-if)# no shut
R1(config-if)# interface Serial0/0/1
R1(config-if)# description link to R3
R1(config-if)# ip address 192.168.10.5 255.255.255.252
R1(config-if)# no shut
R1(config-if)# exit
R1(config)# router rip
```

- As shown in the figure to the left, a basic router configuration includes as follows:

  - Hostname for identification

  - Passwords for security

  - Assignment of IP addresses to interfaces for connectivity

  - Basic routing

- Verify and save configuration changes with the **copy running-config startup-config** command

- To clear the router configuration, use the **erase startup-config** and **reload** commands.

Basic Router Show Commands

```
R1# show protocols
Global values:
  Internet Protocol routing is enabled
  Embedded-Service-Engine0/0 is administratively down, line protocol is down
  GigabitEthernet0/0 is up, line protocol is up
  Internet address is 172.16.1.1/24
  GigabitEthernet0/1 is administratively down, line protocol is down
  Serial0/0/0 is up, line protocol is up
  Internet address is 172.16.3.1/30
  Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.10.5/30
```

- The following are some of the most common show commands:

- Routing Related:

  - **show ip protocols** –Displays information about the routing protocols configured

  - **show ip route** – Displays detailed routing table information including routing codes, known networks, administrative distance and metrics, how routes were learned, next hop, static routes, and default routes

- Interface Related:

  - **show interfaces** – Displays interfaces with line status, bandwidth, delay, reliability, encapsulation, duplex, and I/O statistics

Basic Router Show Commands (Cont.)

```
R1# show protocols
Global values:
  Internet Protocol routing is enabled
  Embedded-Service-Engine0/0 is administratively down, line protocol is down
  GigabitEthernet0/0 is up, line protocol is up
  Internet address is 172.16.1.1/24
  GigabitEthernet0/1 is administratively down, line protocol is down
  Serial0/0/0 is up, line protocol is up
  Internet address is 172.16.3.1/30
  Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.10.5/30
```

- **show ip interfaces** – Displays interface information including protocol status, IPv4 address, if a helper address is configured, and whether an ACL is enabled on the interface

- **show ip interface brief** –Displays all interfaces with IPv4 addressing information and interface and line protocol status

- **show protocols** – Displays information about the routed protocol that is enabled, and the protocol status of the interfaces

- Other connectivity related commands include **show cdp neighbors**. This command displays information on directly connected Cisco devices including Device ID, the local interface the device is connected to, capability, the platform, and Port ID of the remote device. The **details** option provides the IP address.

Basic Switch CLI Commands

```
                        Enable Switch
Switch# enable
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname S1
S1(config)# banner motd %Unauthorized access prohibited%
S1(config)# enable password cisco
S1(config)# enable secret class
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# interface vlan 1
S1(config-if)# ip address 192.168.1.5 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.1.1
S1(config)# interface fa0/2
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# interface fa0/3
S1(config-if)# speed 10
S1(config-if)# duplex half
S1(config)# end
00:12:31: %SYS-5-CONFIG_I: Configured from console by console
S1#
```

- Basic switch configuration includes these:

  - Hostname for identification

  - Passwords for security

  - Assignment of IP addresses for connectivity. In band-access requires the switch to have an IP address.

- See the figure on the left for the commands used to enable and configure the switch.

- Use the **copy running-config startup-config** command to verify and save the switch configuration.

- Use the **erase startup-config** and **reload** commands to clear the switch configuration.

Basic Switch Show Commands

```
S1# show port-security interface fastethernet 0/19
Port Security             : Enabled
Port Status               : Secure-up
Violation Mode            : Shutdown
Aging Time                : 0 mins
Aging Type                : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses     : 50
Total MAC Addresses       : 1
Configured MAC Addresses  : 0
Sticky MAC Addresses      : 1
Last Source Address:Vlan  : 0025.83e6.4b02:1
Security Violation Count  : 0
```

```
S1# show mac-address-table
        Mac Address Table
-------------------------------------------

Vlan    Mac Address      Type       Ports
----    --------------   --------   -----
All     0014.6954.2480   STATIC     CPU
All     0100.0ccc.cccc   STATIC     CPU
All     0100.0ccc.cccd   STATIC     CPU
All     0100.0cdd.dddd   STATIC     CPU
 1      000b.be02.a841   DYNAMIC    Fa0/1
 1      000c.2999.758e   DYNAMIC    Fa0/2
 1      000c.29c4.9e26   DYNAMIC    Fa0/3
 1      000c.29ff.0744   DYNAMIC    Fa0/1
 1      0014.6a46.e1c8   DYNAMIC    Fa0/2
 1      0014.6a46.e1c9   DYNAMIC    Fa0/3
 1      0016.763f.935d   DYNAMIC    Fa0/3
Total Mac Addresses for this criterion: 11
```

- Switches make use of common IOS commands for configuration, to check for connectivity, and to display current switch status. Here are some very useful commands:

  - **show port-security** – Displays any ports with security activated. Include the interface ID to examine a specific interface.

  - **show port-security address** – Displays all secure MAC addresses configured on all switch interfaces.

  - **show interfaces** – Displays one or all interfaces with line protocol status, bandwidth, delay, reliability, encapsulation, duplex, and I/O statistics.

  - **show mac-address-table** – Displays all MAC addresses that the switch has learned, how they were learned, port number, and the VLAN assigned to the port.

- Cisco switches also support the **show cdp neighbors command.**

cisco

Packet Tracer – Comparing 2960 and 3560 Switches

Topology
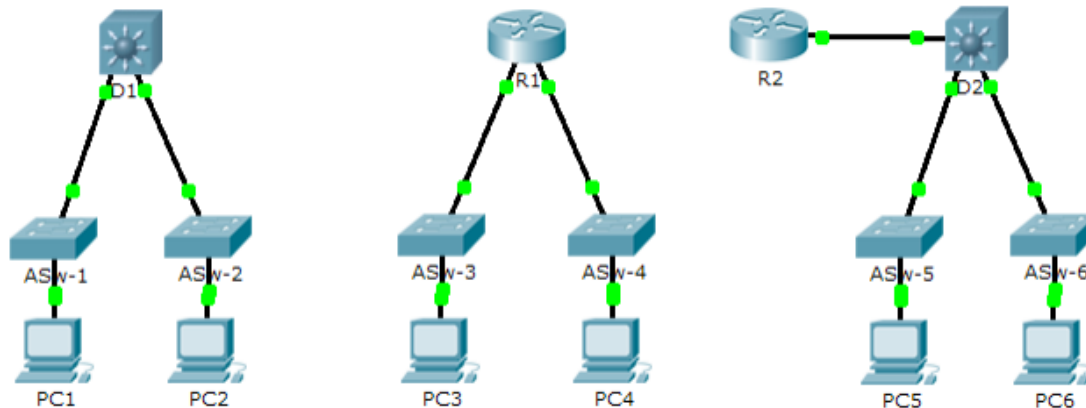
Objective

Part 1: Compare Layer 2 and Layer 3 Switches

**Part 2: Compare a Layer 3 Switch and a Router**

Background

In this activity, you will use various commands to examine three different switching topologies and compare the similarities and differences between the 2960 and 3560 switches. You will also compare the routing table of a 1941 router with a 3560 switch.

- This Packet Tracer activity will allow you to use various commands to compare and examine three different switching topologies and compare the 2960 and 3560 switches.

- You will also compare the routing table of a 1941 router and a 3560 switch.

Packet Tracer – Skills Integration Challenge

Packet Tracer – Skills Integration Challenge

Topology
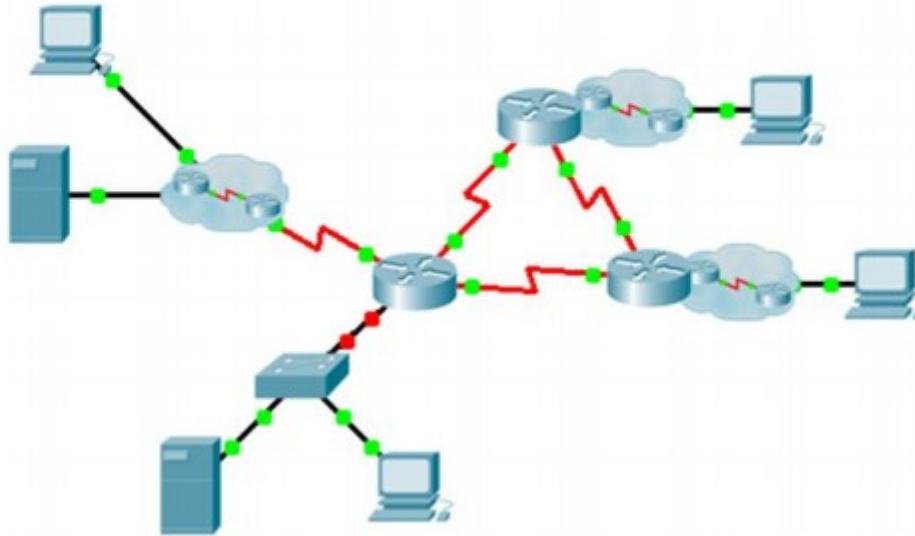
- This Packet Tracer activity will require you to practice many of the skills that you have acquired so far during your CCNA studies.

- You will first complete the documentation for the network before implementing various requirements.

- Finally, you will be required to use your documentation to verify your implementation by testing end-to-end connectivity.