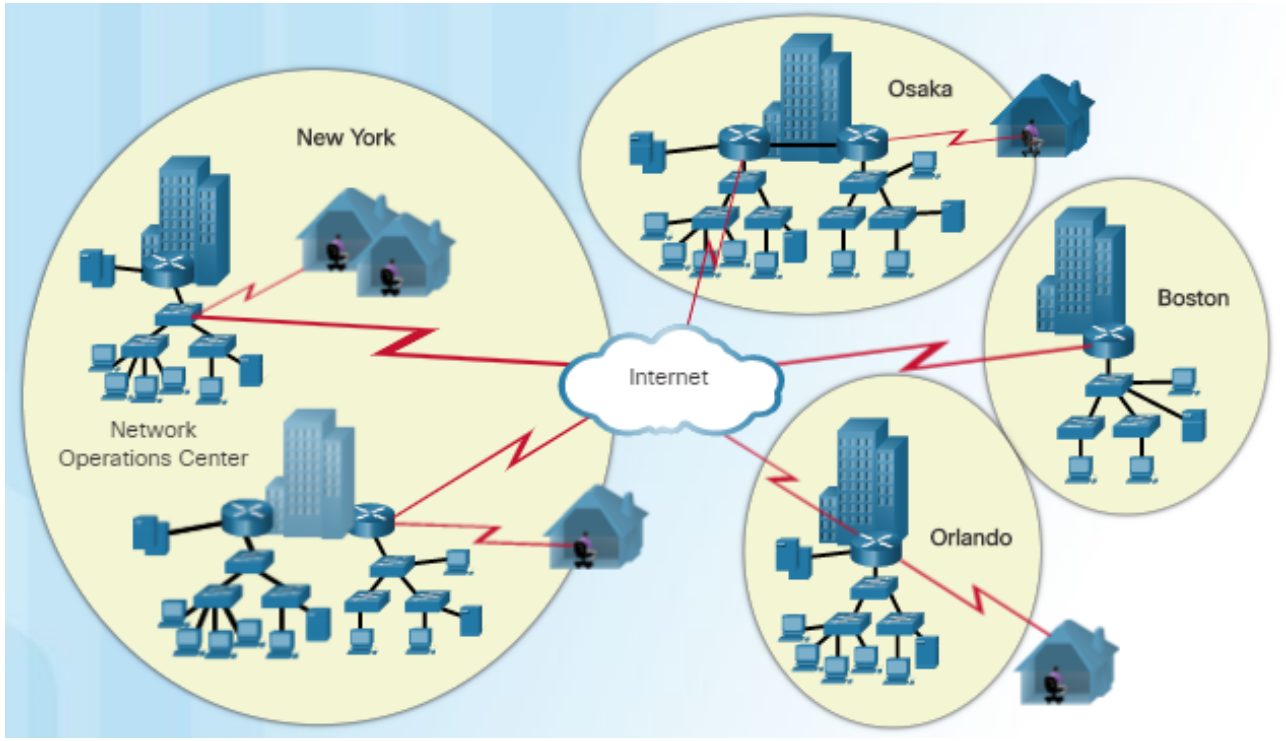
Distributed Networks

Platform Technologies

Based on CCNA Routing and Switching Scaling Networks v6.0

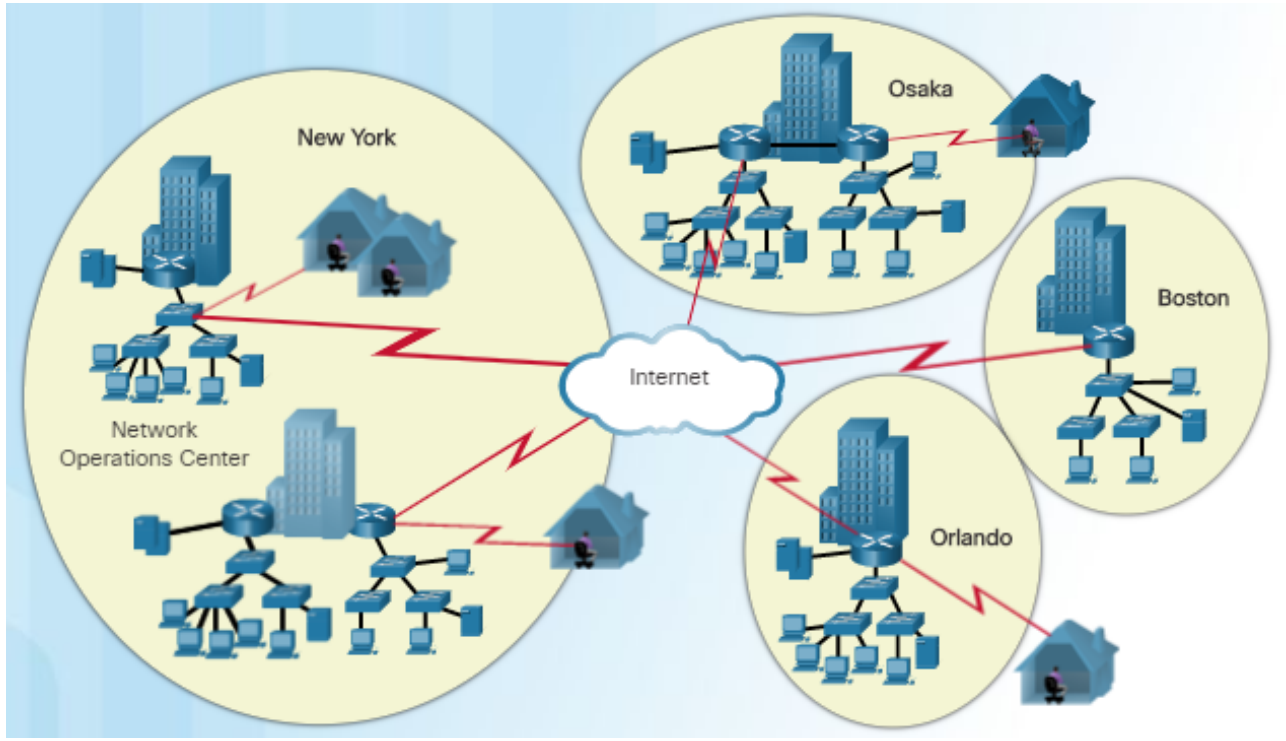
Scaling Networks with LANs

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



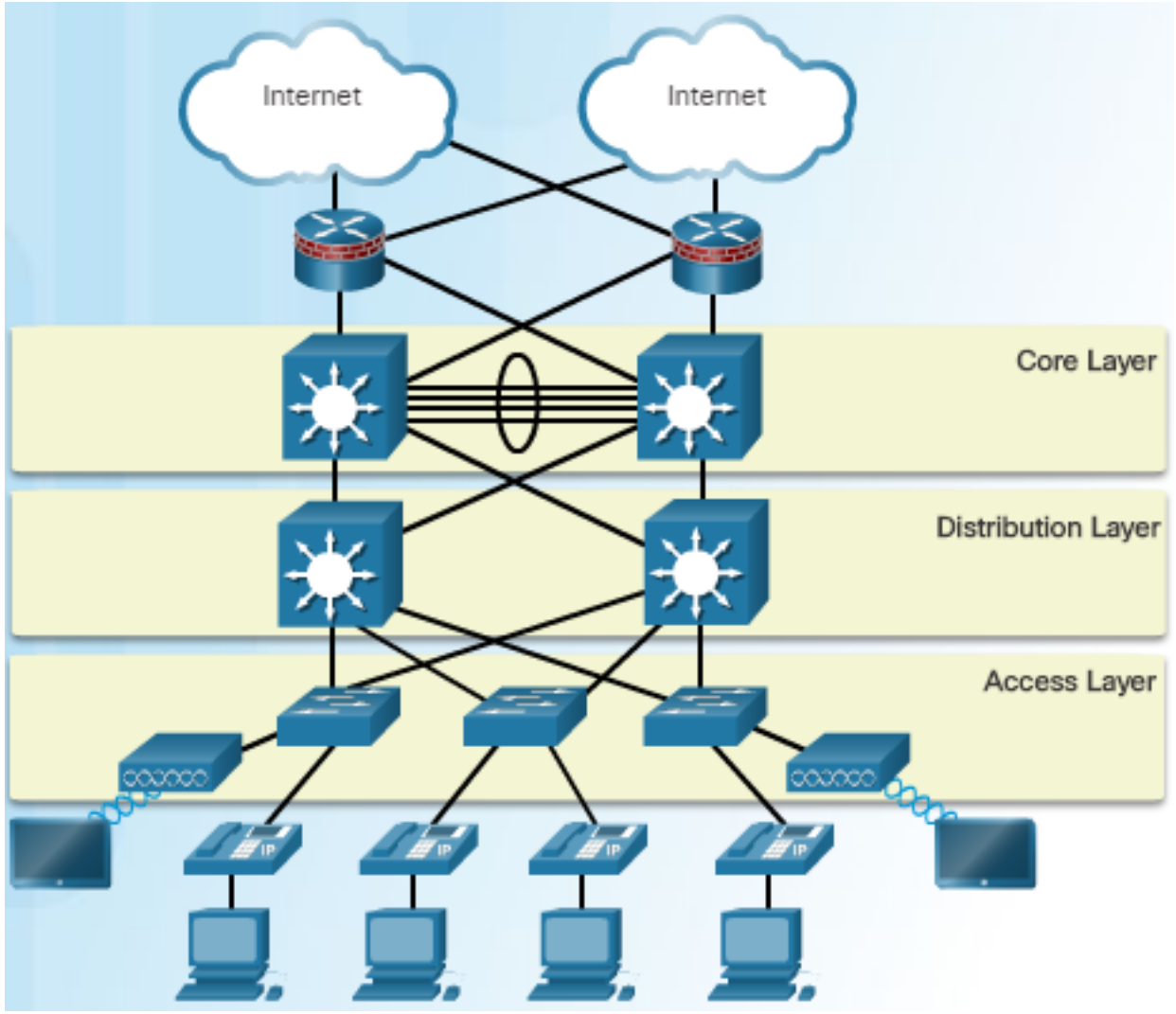
The Need to Scale a Network

- 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



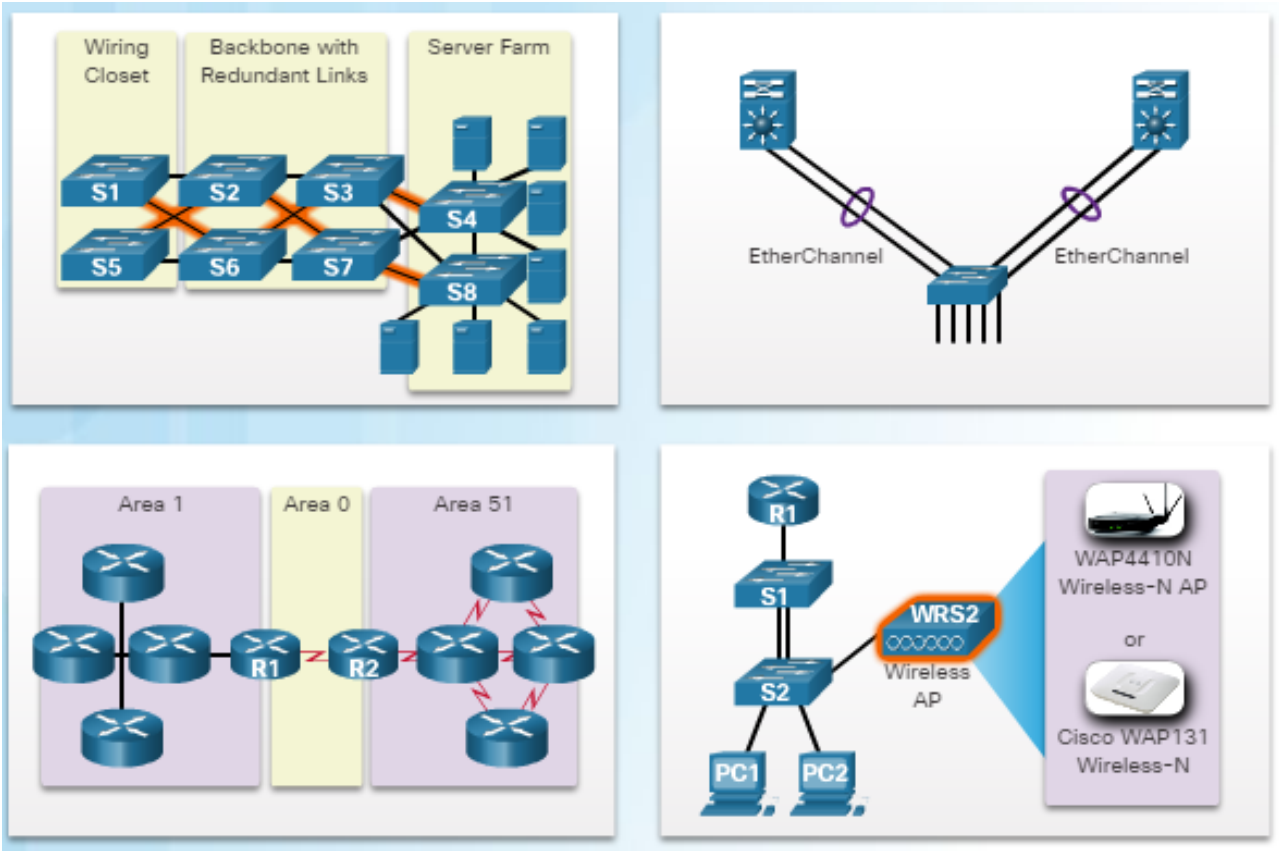
Hierarchical Design Model

- 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



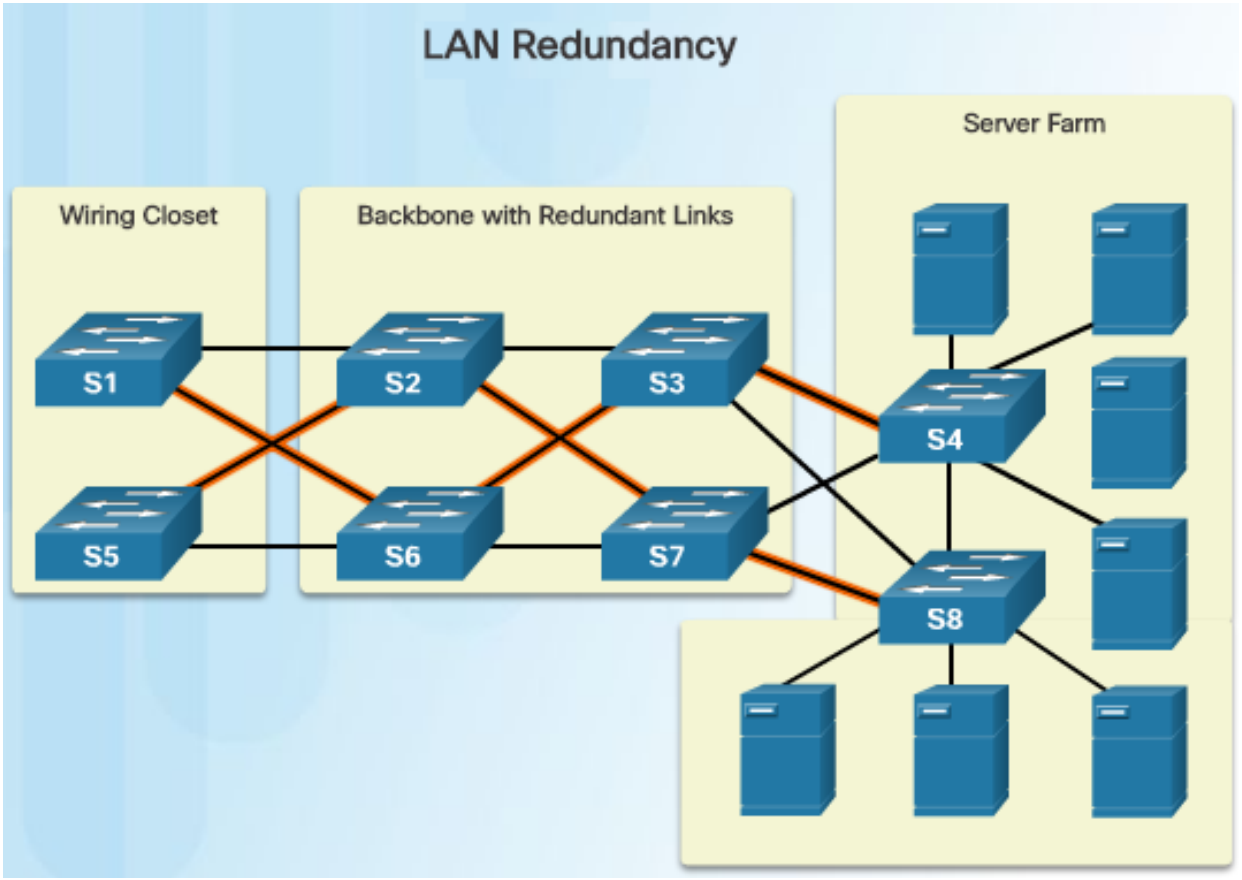
Design for Scalability

- 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.



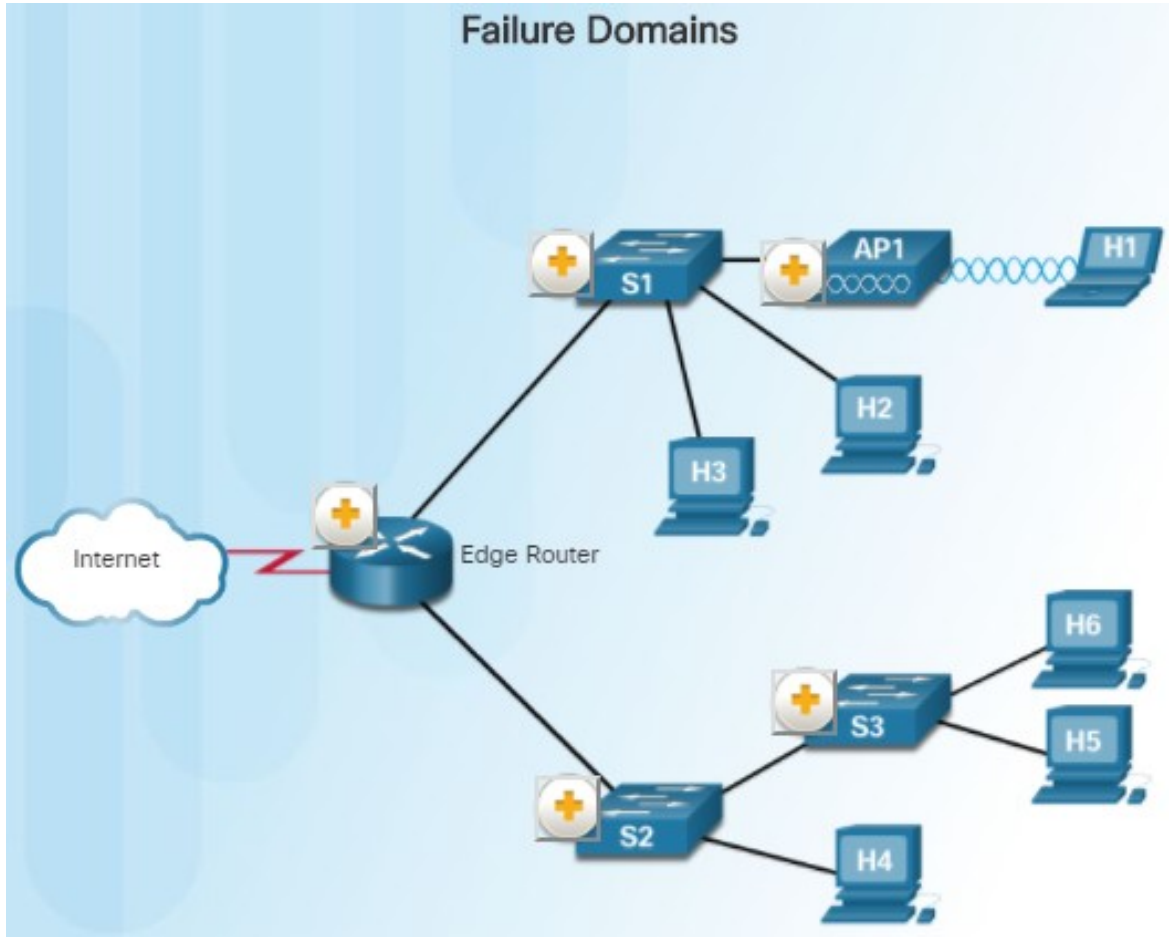
Planning for Redundancy

- 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.



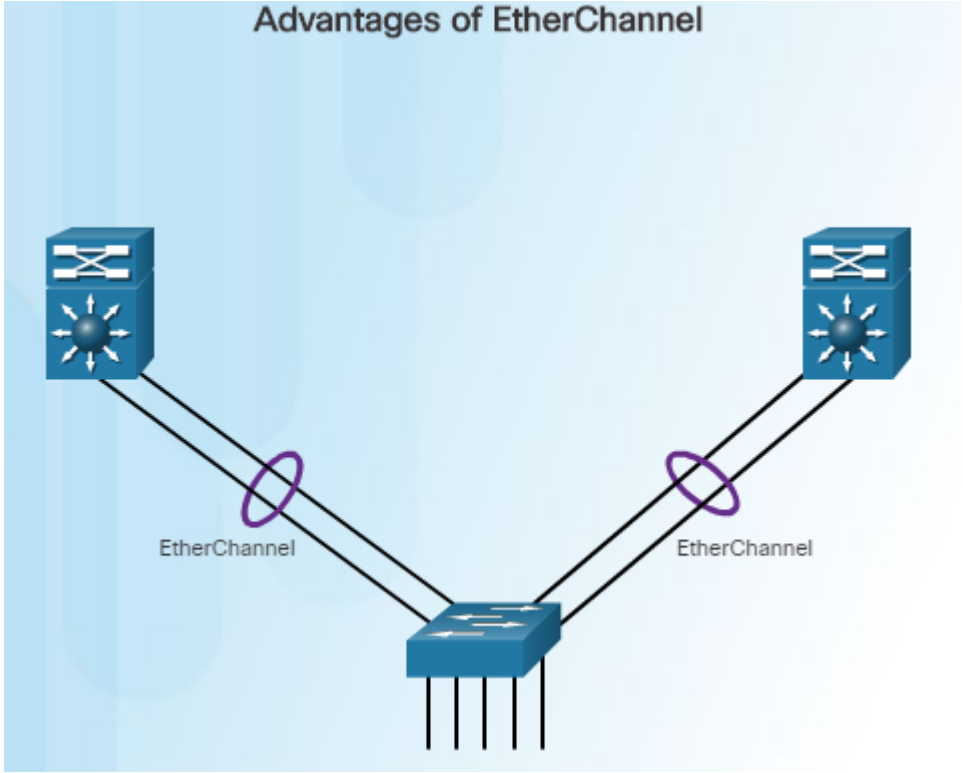
Failure Domains

- 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.



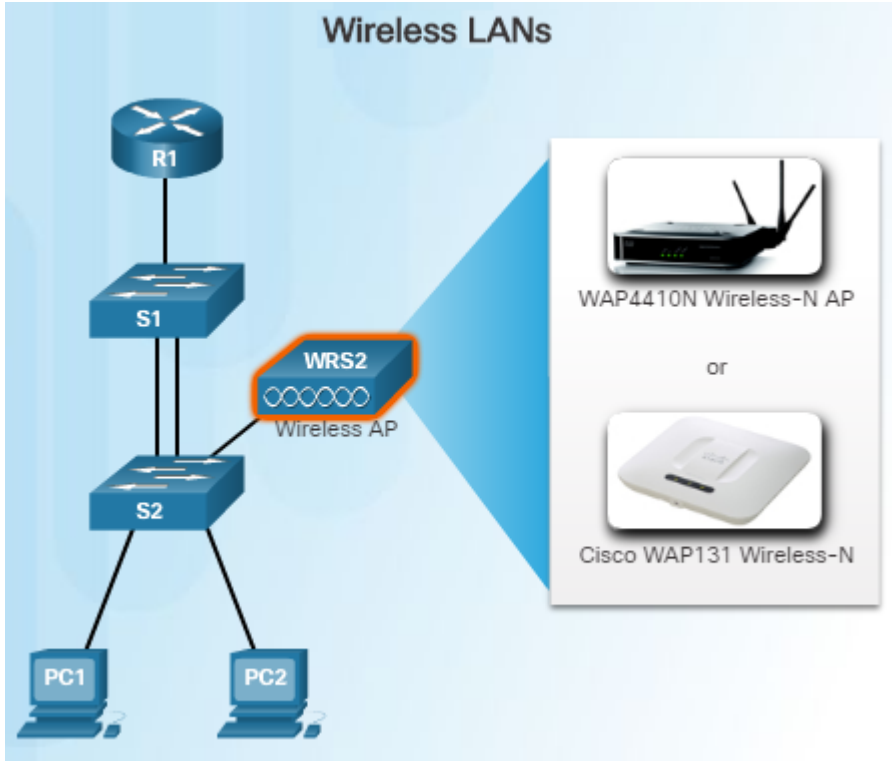
Increasing Bandwidth

- 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.



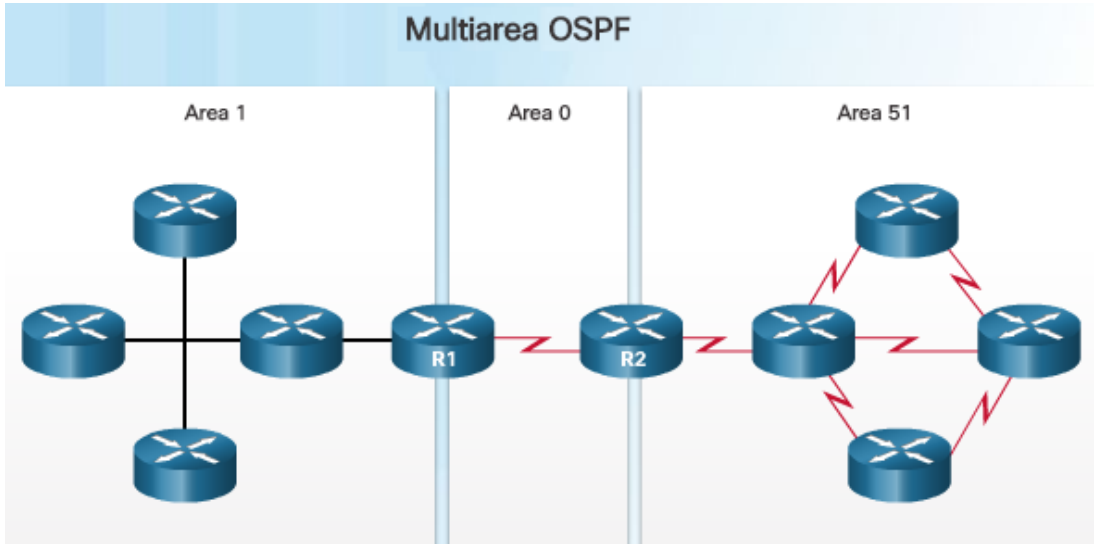
Expanding the Access Layer

- 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

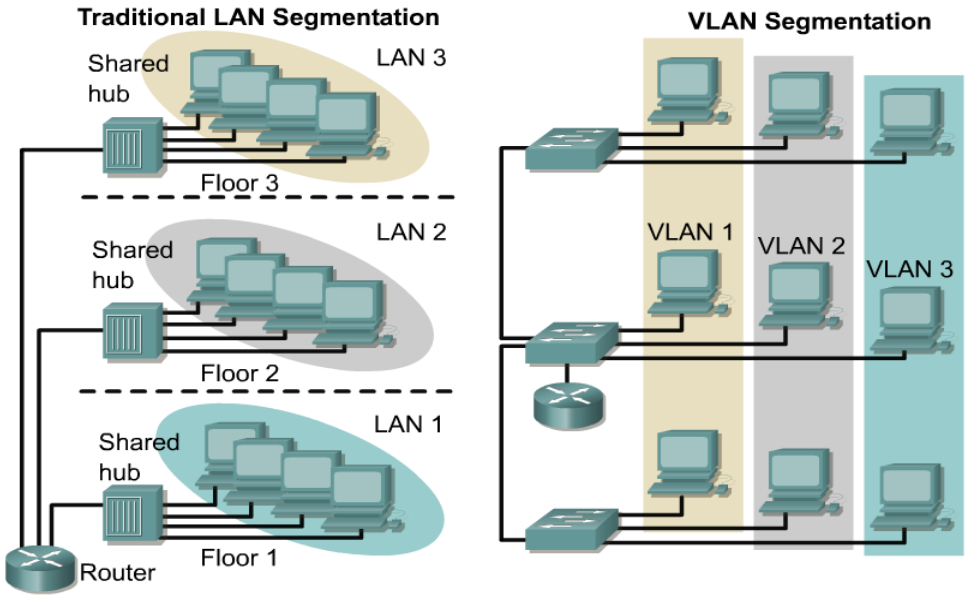
- Advanced routing protocols, such as OSPF and EIGRP are used in large networks.
- Link-state routing protocols such as OSPF works well for larger hierarchical networks where fast convergence is important.
- OSPF supports a two-layer hierarchical design, referred to as multiarea OSPF.
- Single Area OSPF has one area – Area 0.
- Multiarea OSPF requires an Area 0 (backbone area)
- Non-backbone areas must be directly connected to Area 0.

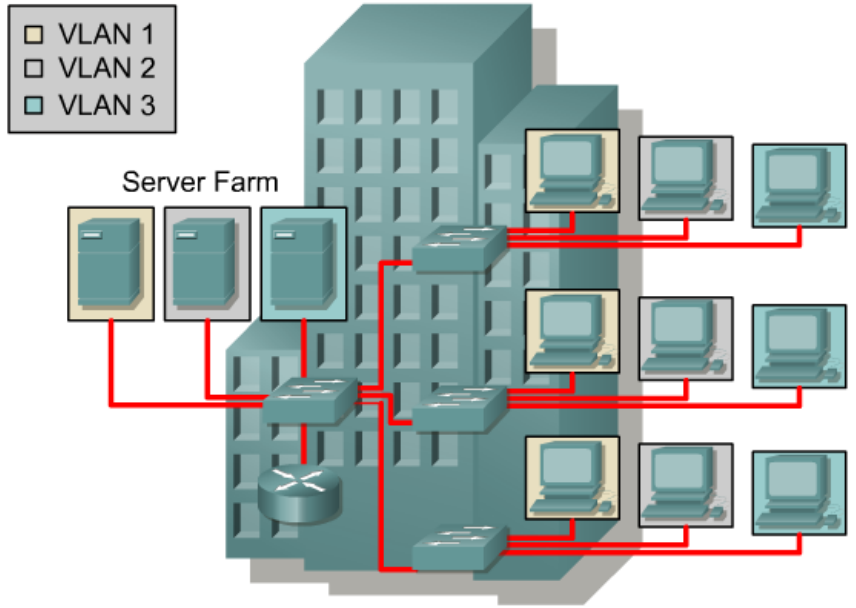


Scaling Networks with VLANs

Virtual LANs (VLANs)

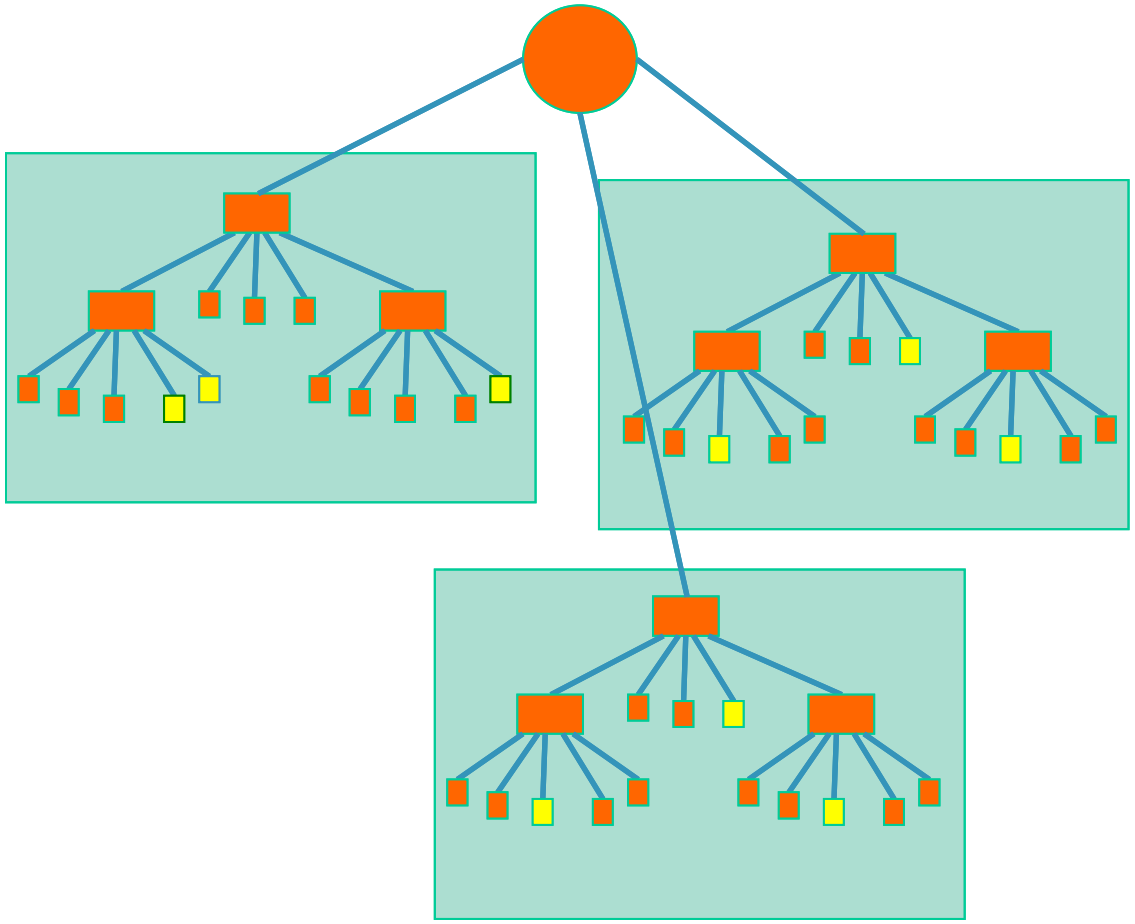
- VLANs provide segmentation based on broadcast domains.
- VLANs logically segment switched networks based on the functions, project teams, or applications of the organization regardless of the physical location or connections to the network.
- All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location.





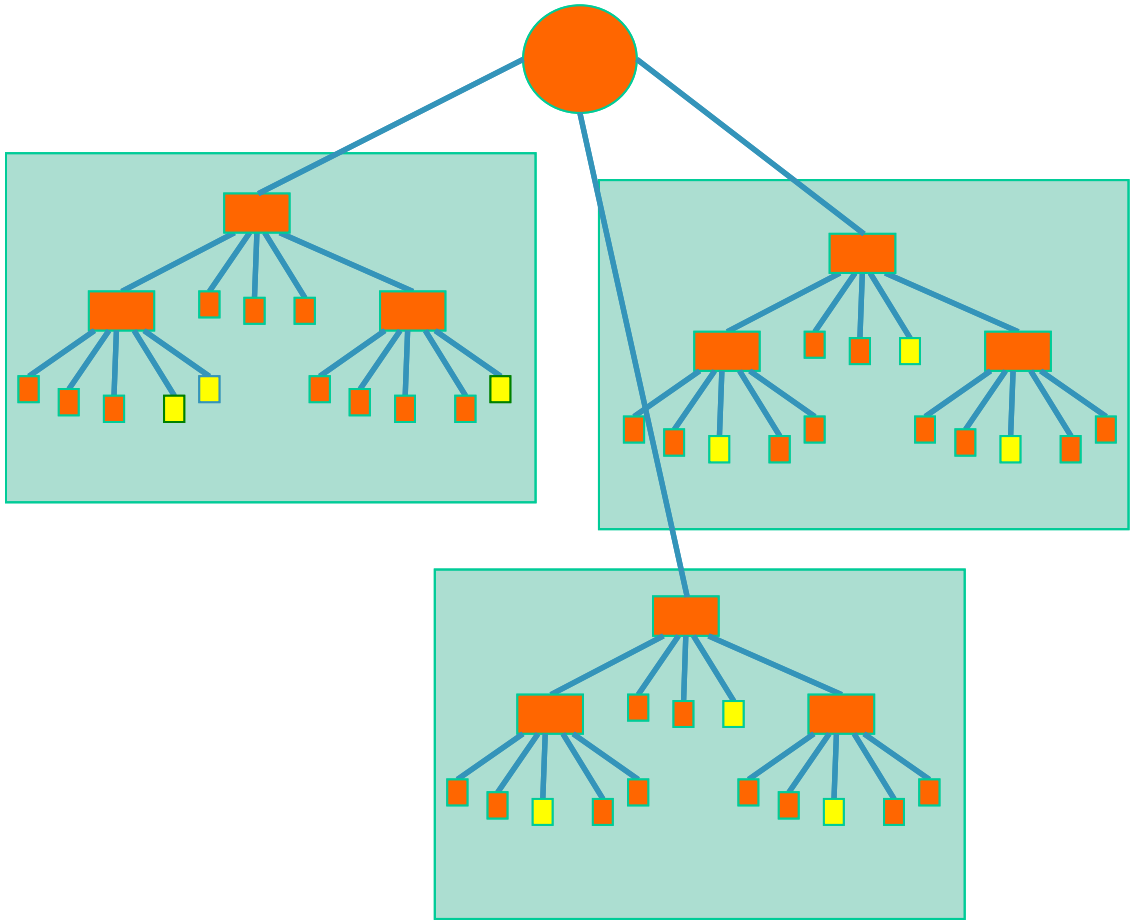
Virtual LANs (VLANs)

- VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.
- Allows us to split switches into separate (virtual) switches
- **Edge ports**, where end nodes are connected, are configured as members of a VLAN



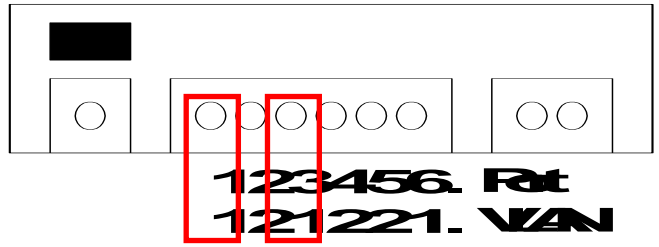
Virtual LANs (VLANs)

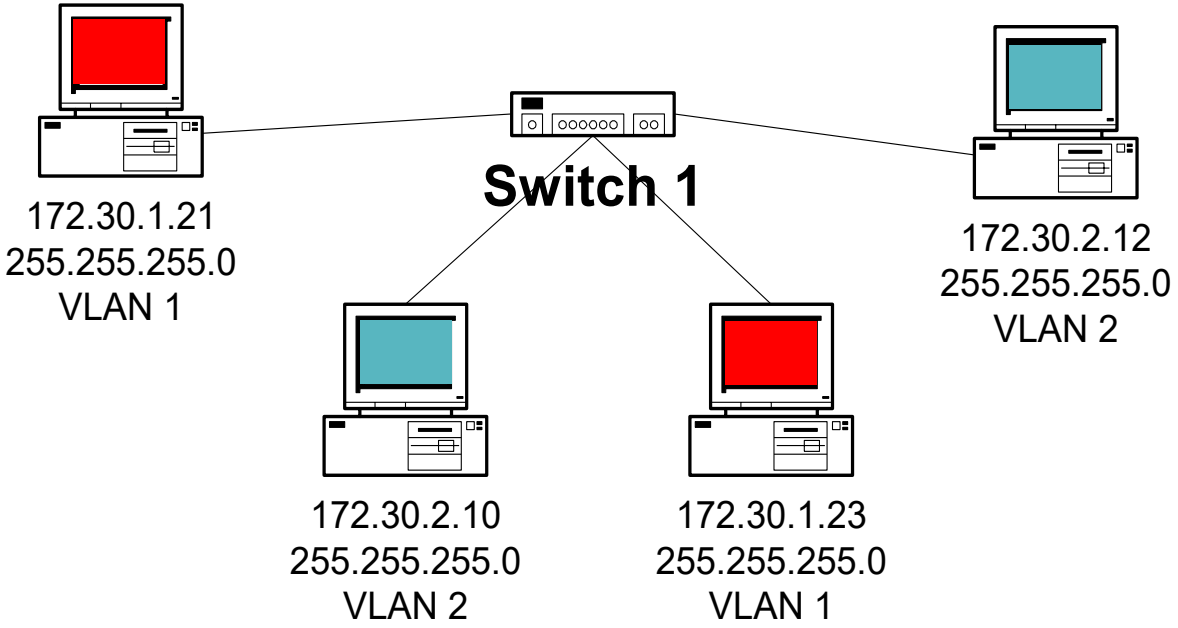
- Two or more VLANs in a single switch
- The switch behaves as several virtual switches, sending traffic only within VLAN members.
- Switches may not bridge any traffic between VLANs, as this would violate the integrity of the VLAN domain.
- Inter-VLAN traffic must be routed (i.e. go through a router) because they are separate subnets



Virtual LANs (VLANs)

- VLANs are assigned to switch ports.
- There is no “VLAN” assignment done on the host.
- In order for a host to be a part of that VLAN, it must be assigned an IP address that belongs to the proper subnet.
- Remember: VLAN = Subnet

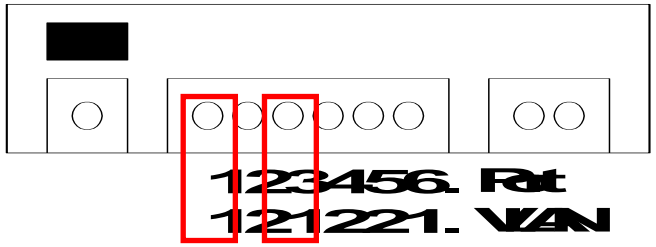




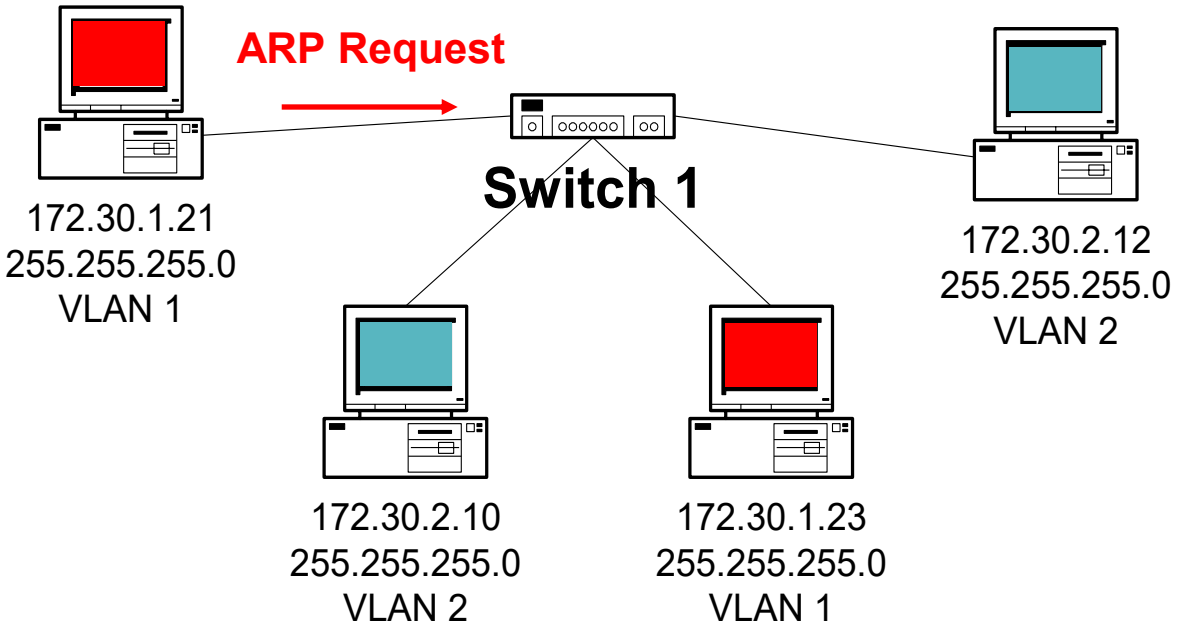
Two **VLANs** = Two **subnets**

- Two Subnets

Virtual LANs (VLANs)



- VLANs separate broadcast domains == subnets.
  - e.g. without VLAN the ARP would be seen on all subnets.
- Assigning a host to the correct VLAN is a 2-step process:
  - Connect the host to the correct port on the switch.
  - Assign to the host the correct IP address depending on the VLAN membership

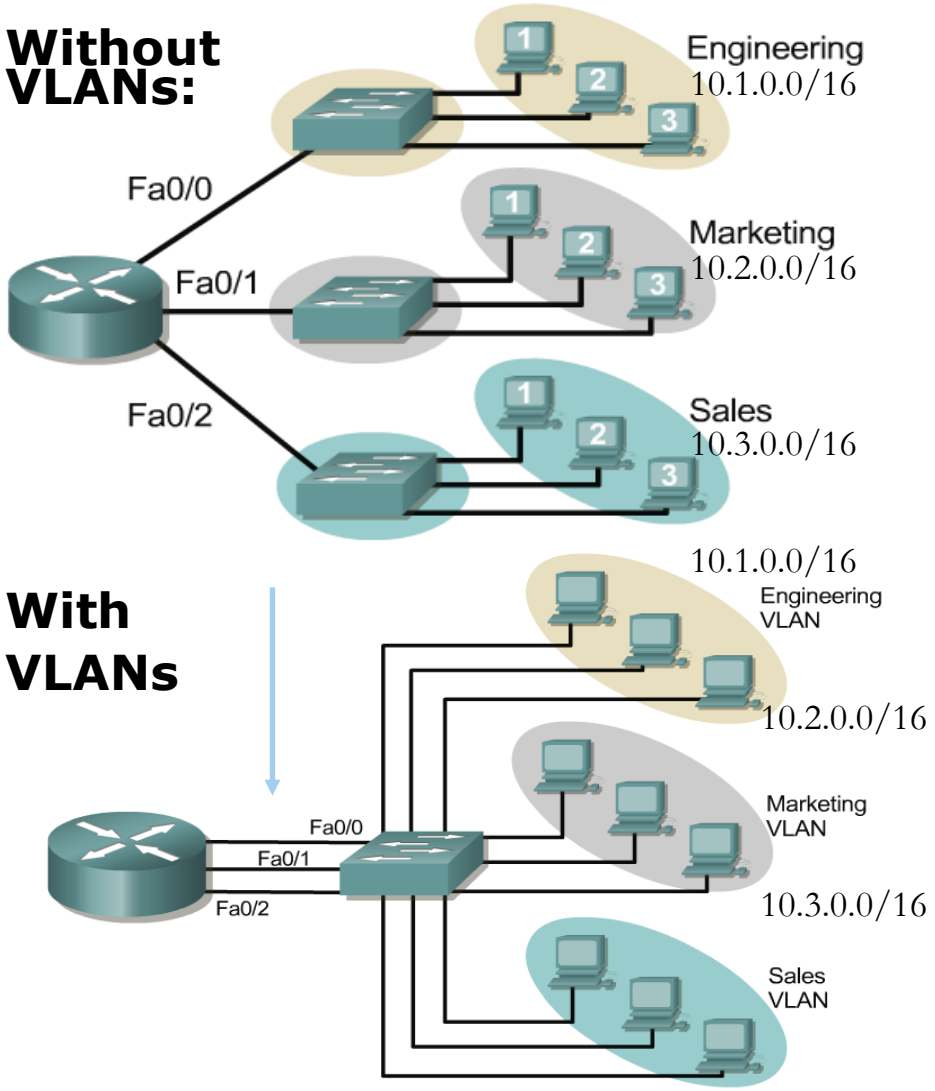


Two **VLANs** = Two **subnets**

- Two Subnets

Broadcast Domains with VLANs and Routers

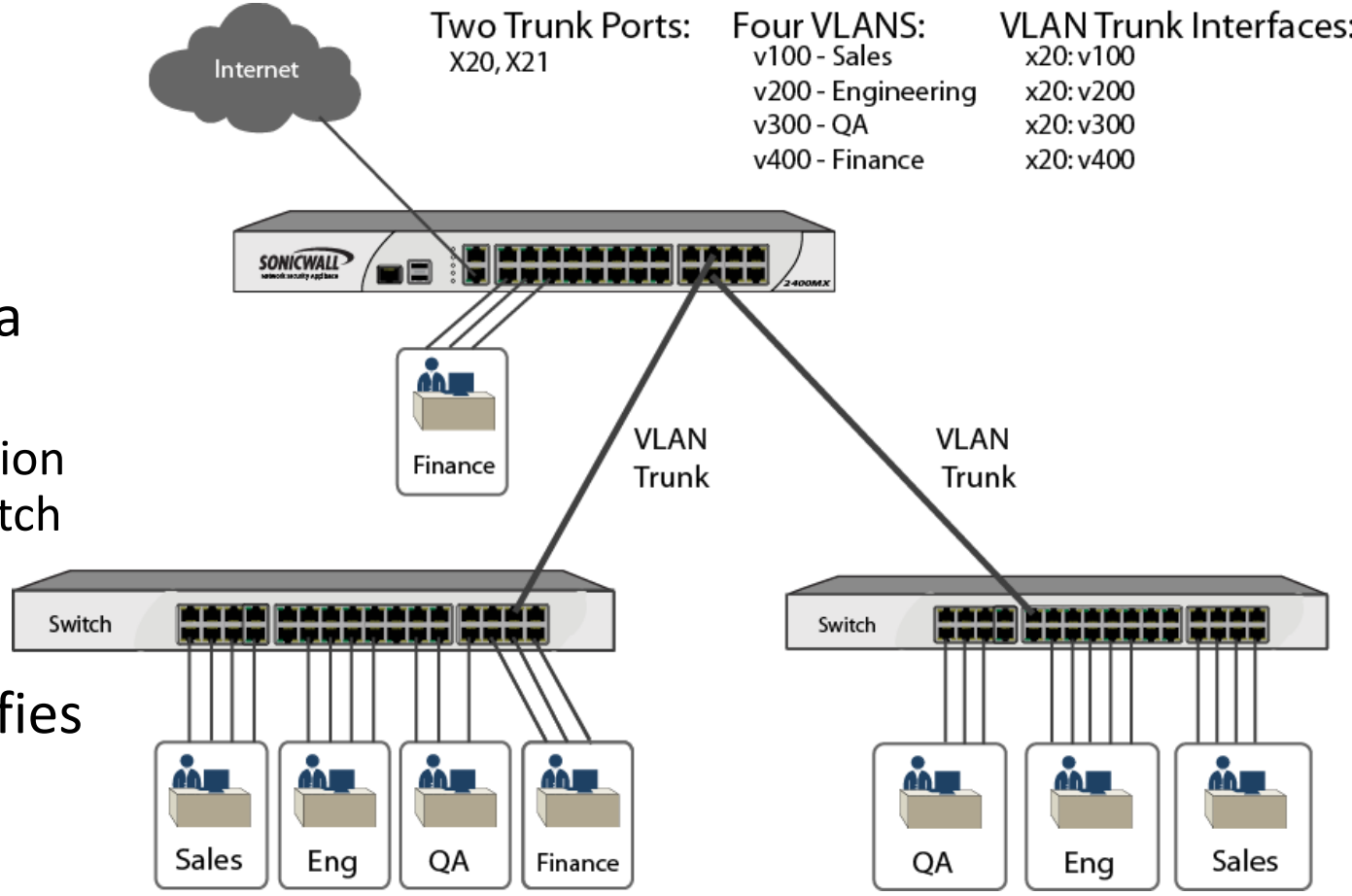
- Without VLANs, each group is on a different IP network and on a different switch.
- Using VLANs, switch is configured with the ports on the appropriate VLAN.
- Still, each group on a different IP network; however, they are all on the same physical switch.
- What are the broadcast domains in each?



One link per VLAN or a single VLAN Trunk

VLANs Across Switches

- Two switches can exchange traffic from one or more VLANs
- Inter-switch links are configured as **trunks**, carrying frames from all or a subset of a switch's VLANs
  - Trunking is the point to point connection between more than one Ethernet switch and some other network devices like switch or a router.
- Each frame carries a tag that identifies which VLAN it belongs to



Increase Complexity with VLANs

- You can no longer “just replace” a switch
  - Now you have VLAN configuration to maintain
  - Field technicians need more skills
- You have to make sure that all the switch-to-switch trunks are carrying all the necessary VLANs
  - Need to keep in mind when adding/removing VLANs
- Do not build “VLAN spaghetti”
  - Extending a VLAN to multiple buildings across trunk ports
  - Bad idea because:
    - Broadcast traffic is carried across all trunks from one end of the network to another
    - Broadcast storm can spread across the extent of the VLAN
    - Maintenance and troubleshooting nightmare

Good Reasons to use VLANs

- You want to segment your network into multiple subnets, but can’t buy enough switches
  - Hide sensitive infrastructure like IP phones, building controls, etc.
- Separate control traffic from user traffic
  - Restrict who can access your switch management address

Bad Reasons to use VLANs

- Because you can, and you feel cool ☺
- Because they will completely secure your hosts (or so you think)
- Because they allow you to extend the same IP network over multiple separate buildings

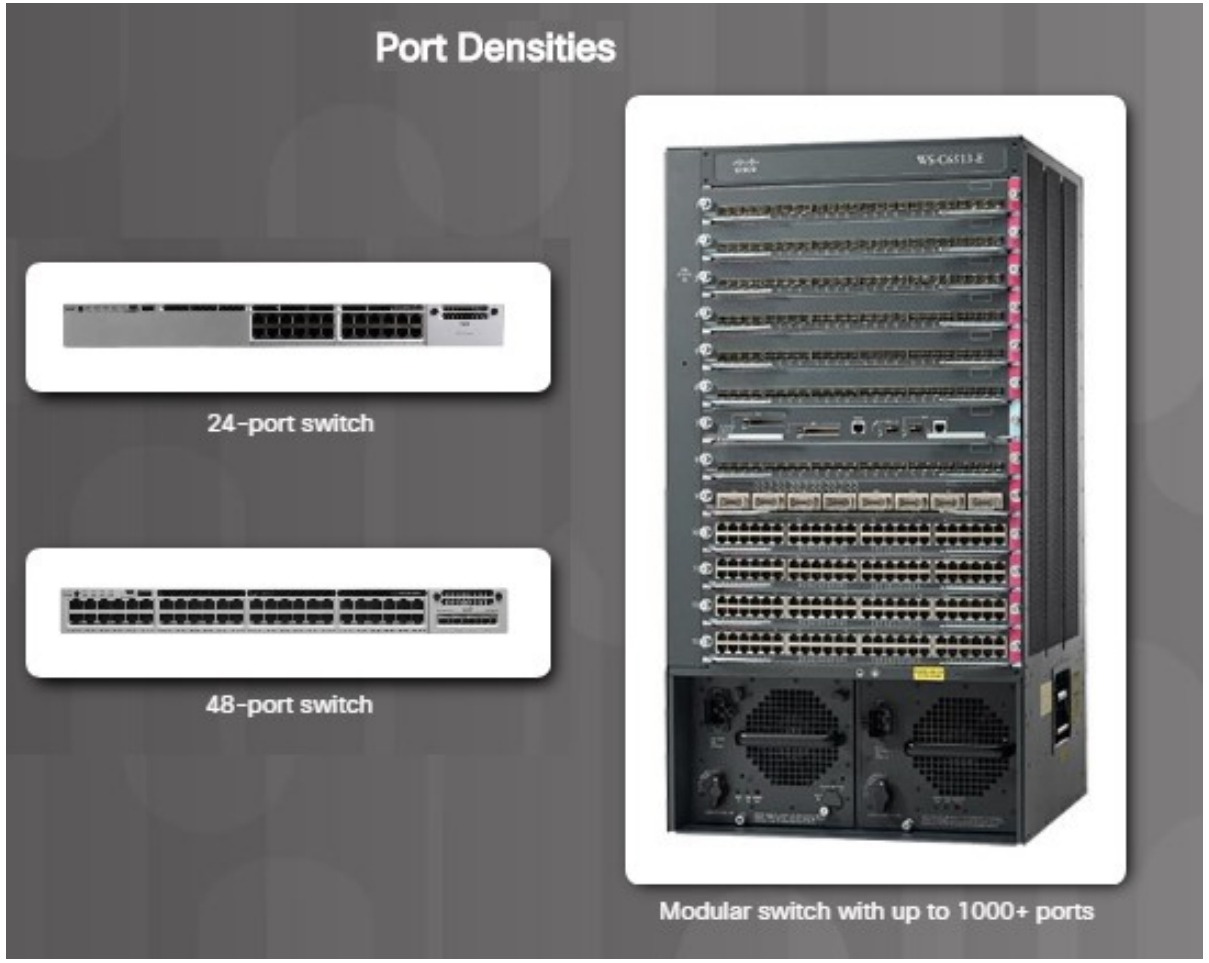
Selecting Network Devices

Switch Hardware Platforms

- 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

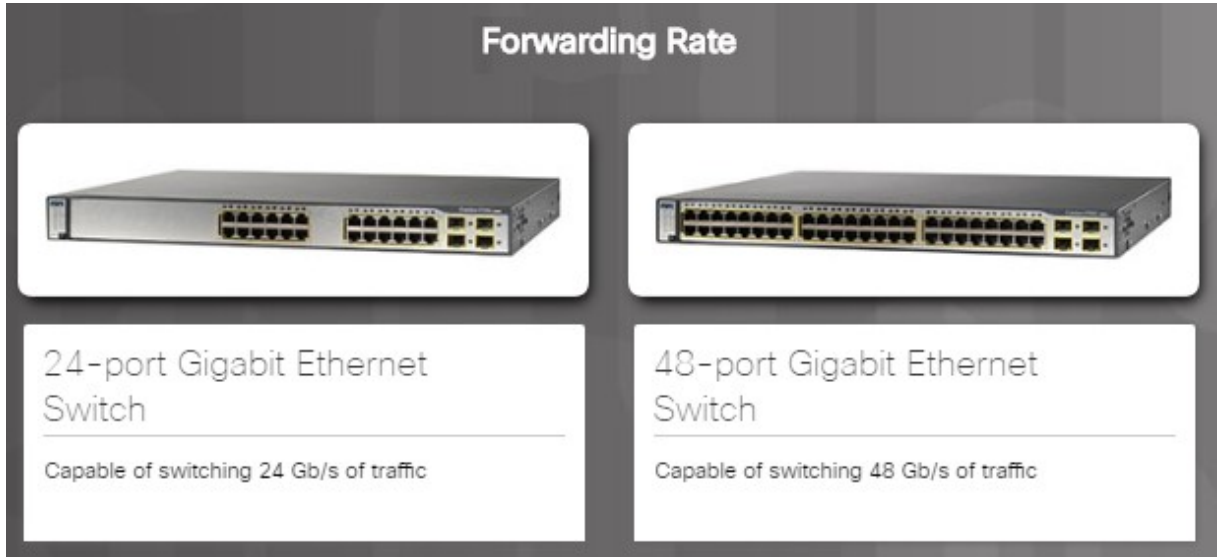
Port Density

- 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:
- 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.



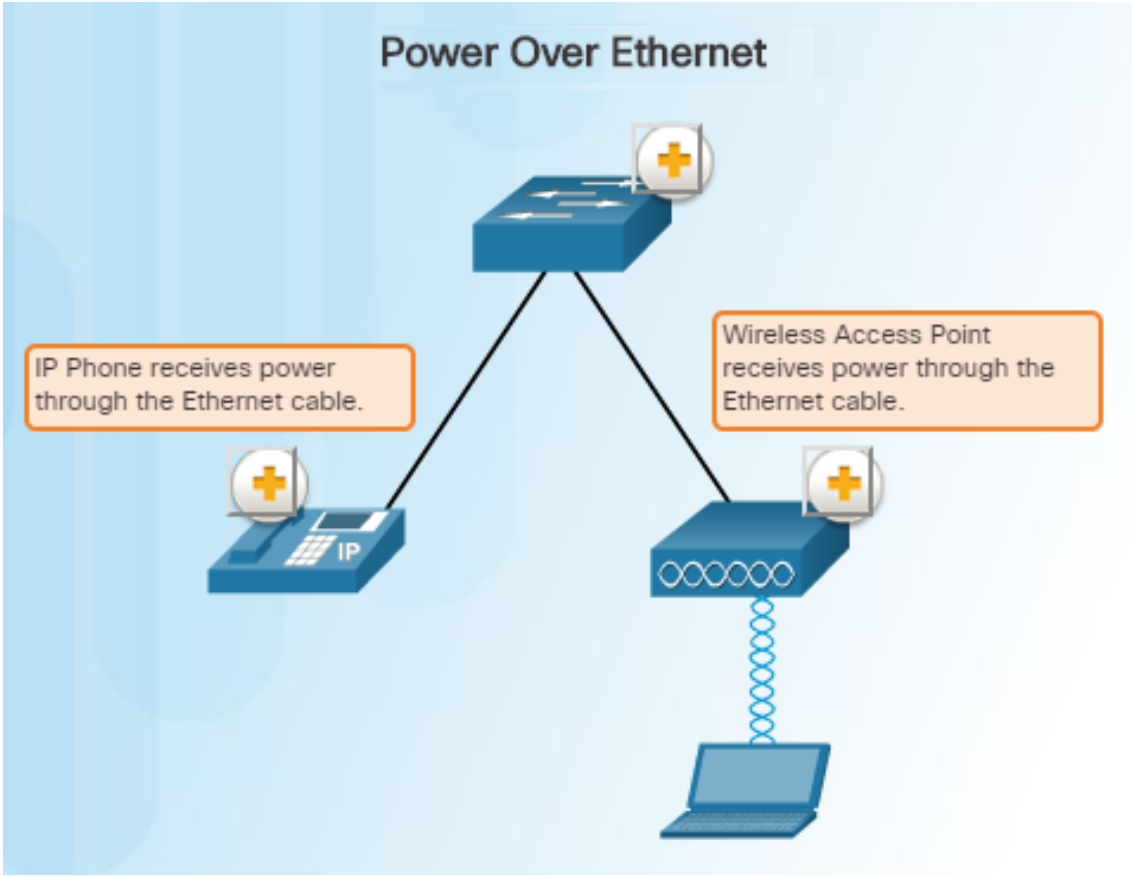
Forwarding Rates

- Forwarding 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

- PoE allows the switch to deliver power to a device over 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.
- PoE pass-through devices can power PoE devices as well as the switch itself by drawing power from certain upstream switches.

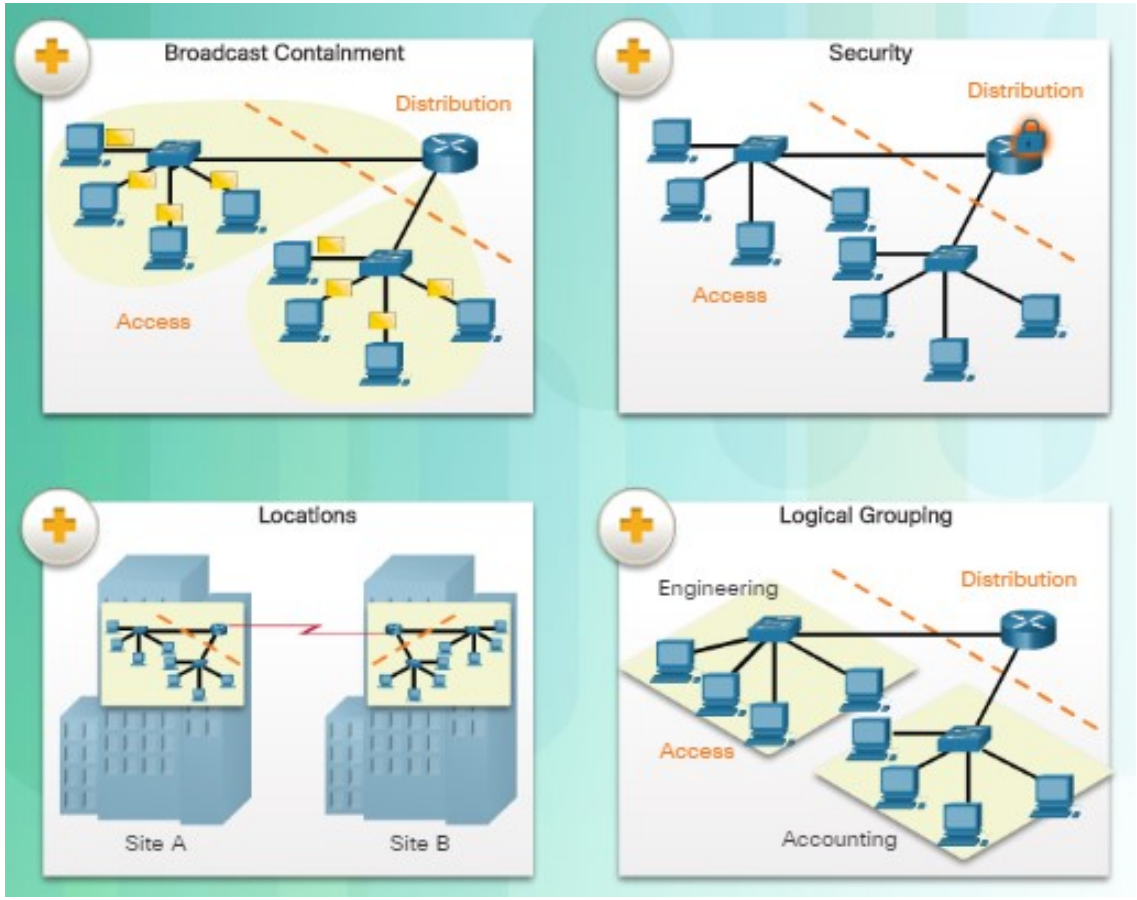


Multilayer Switching

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

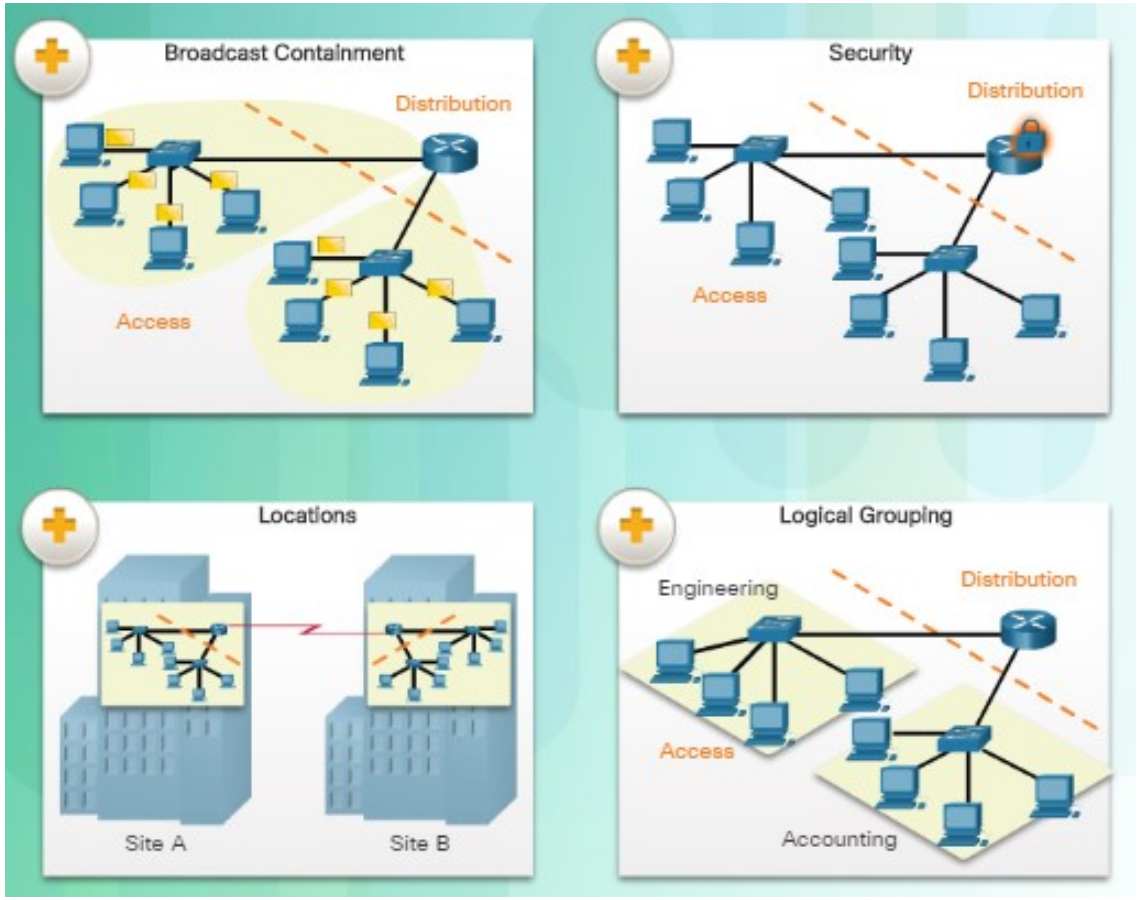
Router Hardware

- 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

- 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.



Managing Devices

- 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.