CHAPTER 1

Introduction to Scaling Networks

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- How is the hierarchical network used in small business?
- What are the recommendations for designing a network that is scalable?
- What features in switch hardware are necessary to support small- to medium-sized business network requirements?
- What types of routers are available for small- to medium-sized business networks?
- What are the basic configuration settings for a Cisco IOS device?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

hierarchical network *page 3*

Cisco Enterprise Architecture *page 3*

enterprise network *page 4*

reliability *page 5*

access layer *page 6*

distribution layer *page 6*

core layer *page 6*

Enterprise Campus *page 8*

port density *page 8*

redundancy *page 8*

Server Farm and Data Center Module *page 8*

Services Module *page 8*

Enterprise Edge *page 9*

Service Provider Edge *page 9*

failure domain *page 9*

multilayer switch *page 10*

cluster *page 11*

EtherChannel *page 11*

Spanning Tree Protocol (STP) *page 12*

link aggregation *page 13*

load-balancing *page 14*

wireless access point (AP) *page 15*

link-state routing protocol *page 15*

Open Shortest Path First (OSPF) *page 15*

Single-Area OSPF *page 16*

Multiarea OSPF *page 16*

Enhanced Interior Gateway Routing Protocol (EIGRP) *page 17*

distance vector routing protocol *page 17*

Protocol Dependent Modules page 17

fixed configuration page 19

modular configuration page 19

stackable configuration page 19

forwarding rates page 22

wire speed page 22

Power over Ethernet (PoE) page 23

application-specific integrated circuit (ASIC) page 25

branch router page 28

network edge router page 28

service provider router page 29

Cisco IOS page 30

in-band management page 31

out-of-band management page 31

Introduction (1.0.1.1)

As a business grows, so do its networking requirements. Businesses rely on the network infrastructure to provide mission-critical services. Network outages can result in lost revenue and lost customers. Network designers must design and build an enterprise network that is scalable and highly available.

This chapter introduces strategies that can be used to systematically design a highly functional network, such as the ***hierarchical network*** design model, the ***Cisco Enterprise Architecture***, and appropriate device selections. The goals of network design are to limit the number of devices impacted by the failure of a single network device, provide a plan and path for growth, and create a reliable network.

Class Activity 1.0.1.2: Network by Design

Your employer is opening a new branch office.

You have been reassigned to the site as the network administrator, where your job will be to design and maintain the new branch network.

The network administrators at the other branches used the Cisco three-layer hierarchical model when designing their networks. You decide to use the same approach.

To get an idea of what using the hierarchical model can do to enhance the design process, you research the topic.

Implementing a Network Design (1.1)

Effective network design implementation requires a solid understanding of the current state of recommended network models and their ability to scale as the network grows.

Hierarchical Network Design (1.1.1)

The hierarchical network model and the Cisco Enterprise Architecture are models to consider when designing a network. This section reviews the importance of scalability and how these models can effectively address that need.

The Need to Scale the Network (1.1.1.1)

Businesses increasingly rely on their network infrastructure to provide mission-critical services. As businesses grow and evolve, they hire more employees, open branch offices, and expand into global markets. These changes directly affect the requirements of a network. A large business environment with many users, locations, and systems is referred to as an *enterprise*. The network that is used to support the business enterprise is called an ***enterprise network***.

In Figure 1-1, the following steps occur as the network grows from a small company to a global enterprise:

1. The company begins as a small, single-location company.
2. The company increases its number of employees.
3. The company grows to multiple locations in the same city.
4. The enterprise grows to multiple cities.
5. The enterprise hires teleworkers.
6. The enterprise expands to other countries (not all enterprises are international).
7. The enterprise centralizes network management in a Network Operations Center (NOC).

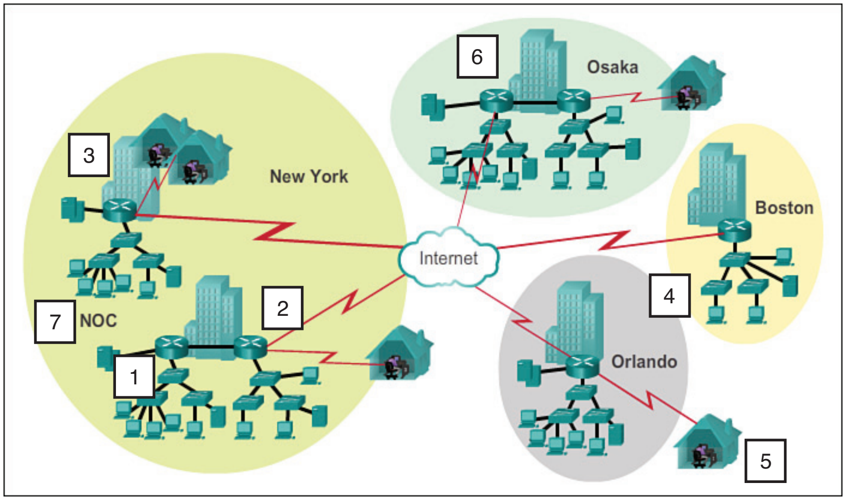

Figure 1-1 Scaling the Network as the Business Grows

An enterprise network must support the exchange of various types of network traffic, including data files, email, IP telephony, and video applications for multiple business units. All enterprise networks must

- Support critical applications
- Support converged network traffic

- Support diverse business needs
- Provide centralized administrative control

Enterprise Business Devices (1.1.1.2)

Users expect enterprise networks, such as the example shown in Figure 1-2, to be up 99.999 percent of the time. Outages in the enterprise network prevent the business from performing normal activities, which can result in a loss of revenue, customers, data, and opportunities.

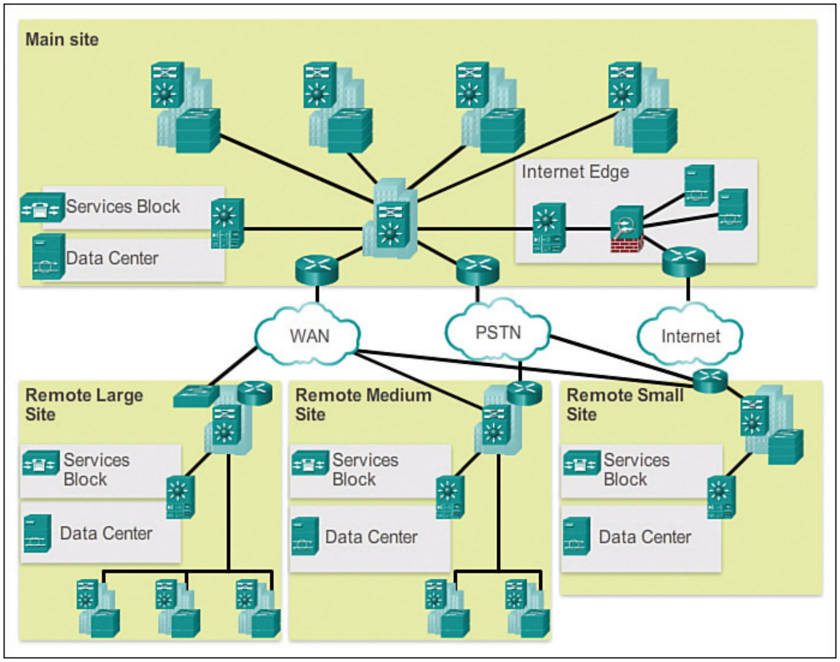

Figure 1-2 Large Enterprise Network Design

To obtain this level of ***reliability***, high-end, enterprise-class equipment is commonly installed in the enterprise network. Designed and manufactured to more stringent standards than lower-end devices, enterprise equipment moves large volumes of network traffic.

Enterprise-class equipment is designed for reliability, with features such as redundant power supplies and failover capabilities. *Failover capability* refers to the ability of a device to switch from a nonfunctioning module, service, or device to a functioning one with little or no break in service.

Purchasing and installing enterprise-class equipment does not eliminate the need for proper network design.

Hierarchical Network Design (1.1.1.3)

To optimize bandwidth on an enterprise network, the network must be organized so that traffic stays local and is not propagated unnecessarily onto other portions of the network. Using the three-layer hierarchical design model helps organize the network.

This model divides the network functionality into three distinct layers, as shown in Figure 1-3:

- Access layer
- Distribution layer
- Core layer

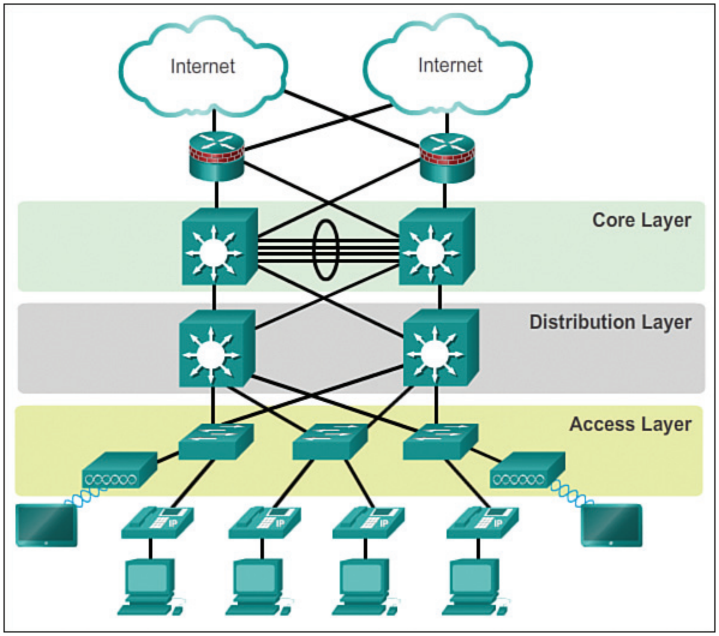

Figure 1-3 Hierarchical Design Model

Each layer is designed to meet specific functions.

The ***access layer*** provides connectivity for the users. The ***distribution layer*** is used to forward traffic from one local network to another. Finally, the ***core layer*** represents a high-speed backbone layer between dispersed networks. User traffic is initiated at the access layer and passes through the other layers if the functionality of those layers is required.

Even though the hierarchical model has three layers, some smaller enterprise networks might implement a two-tier hierarchical design. In a two-tier hierarchical design, the core and distribution layers are collapsed into one layer, reducing cost and complexity, as shown in Figure 1-4.

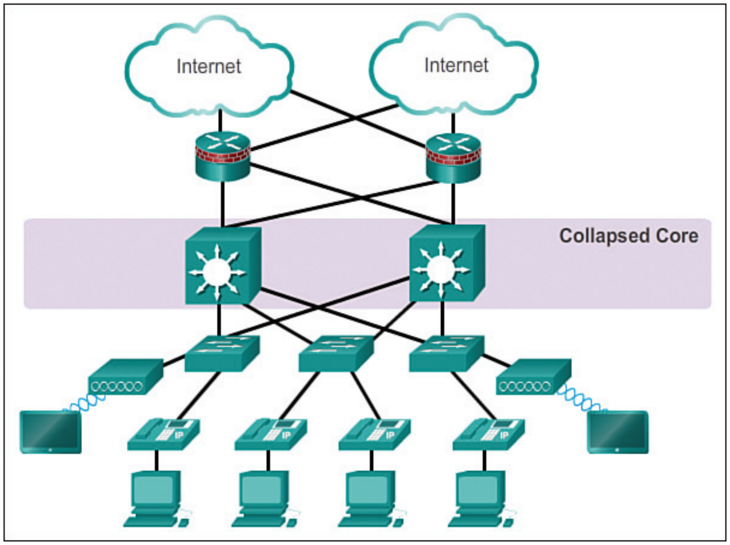

Figure 1-4 Collapsed Core

Cisco Enterprise Architecture (1.1.1.4)

The Cisco Enterprise Architecture divides the network into functional components while still maintaining the core, distribution, and access layers. As Figure 1-5 shows, the primary Cisco Enterprise Architecture modules include

- Enterprise Campus
- Enterprise Edge
- Service Provider Edge
- Remote

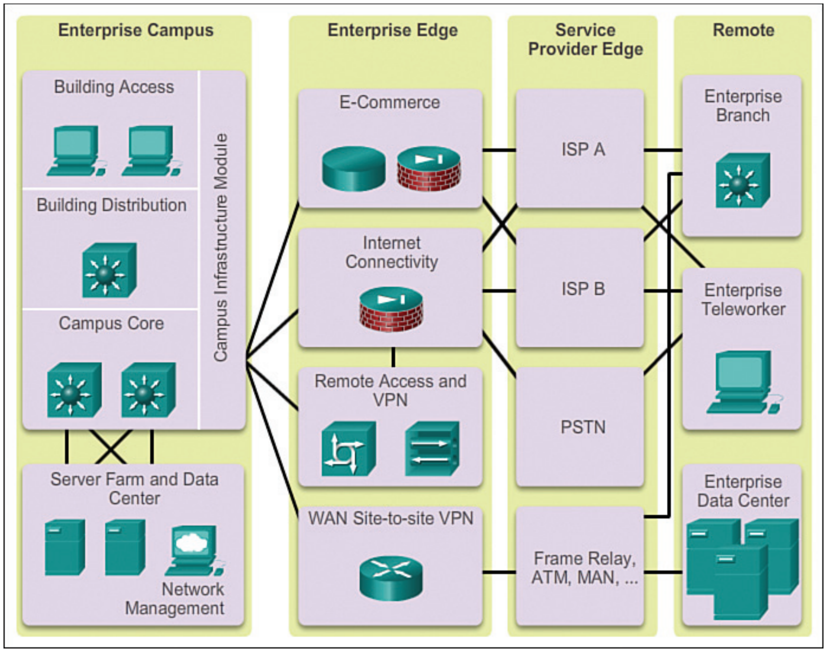

Figure 1-5 Enterprise Architecture

Enterprise Campus

The ***Enterprise Campus*** consists of the entire campus infrastructure, to include the access, distribution, and core layers. The access layer module contains Layer 2 or Layer 3 switches to provide the required ***port density***. Implementation of VLANs and trunk links to the building distribution layer occurs here. ***Redundancy*** to the building distribution switches is important. The distribution layer module aggregates building access using Layer 3 devices. Routing, access control, and QoS are performed at this distribution layer module. The core layer module provides high-speed interconnectivity between the distribution layer modules, data center server farms, and the enterprise edge. Redundancy, fast convergence, and fault tolerance are the focus of the design in this module.

In addition to these modules, the Enterprise Campus can include other submodules such as

- ***Server Farm and Data Center Module***: This area provides high-speed connectivity and protection for servers. It is critical to provide security, redundancy, and fault tolerance. The network management systems monitor performance by monitoring device and network availability.
- ***Services Module***: This area provides access to all services, such as IP Telephony services, wireless controller services, and unified services.

Enterprise Edge

The ***Enterprise Edge*** consists of the Internet, VPN, and WAN modules connecting the enterprise with the service provider's network. This module extends the enterprise services to remote sites and enables the enterprise to use Internet and partner resources. It provides QoS, policy reinforcement, service levels, and security.

Service Provider Edge

The ***Service Provider Edge*** provides Internet, Public Switched Telephone Network (PSTN), and WAN services.

All data that enters or exits the Enterprise Composite Network Model (ECNM) passes through an edge device. This is the point where all packets can be examined and a decision made whether the packet should be allowed on the enterprise network. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) can also be configured at the enterprise edge to protect against malicious activity.

Failure Domains (1.1.1.5)

A well-designed network not only controls traffic but also limits 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 device that initially fails determines the impact of a failure domain. For example, a malfunctioning switch on a network segment normally affects only the hosts on that segment. However, if the router that connects this segment to others fails, the impact is much greater.

The use of redundant links and reliable enterprise-class equipment minimizes the chance of disruption in a network. Smaller failure domains reduce the impact of a failure on company productivity. They also simplify the troubleshooting process, thereby shortening the downtime for all users.

Failure domains often include other, smaller failure domains. For example, Figure 1-6 shows the following failure domains:

1. If the Edge Router fails, it will impact every device connected to it.
2. If S1 fails, it will impact H1, H2, H3, and AP1.
3. If S2 fails, it will impact S3, H4, H5, and H6.
4. If AP1 fails, it will impact H1.
5. If S3 fails, it will impact H5 and H6.

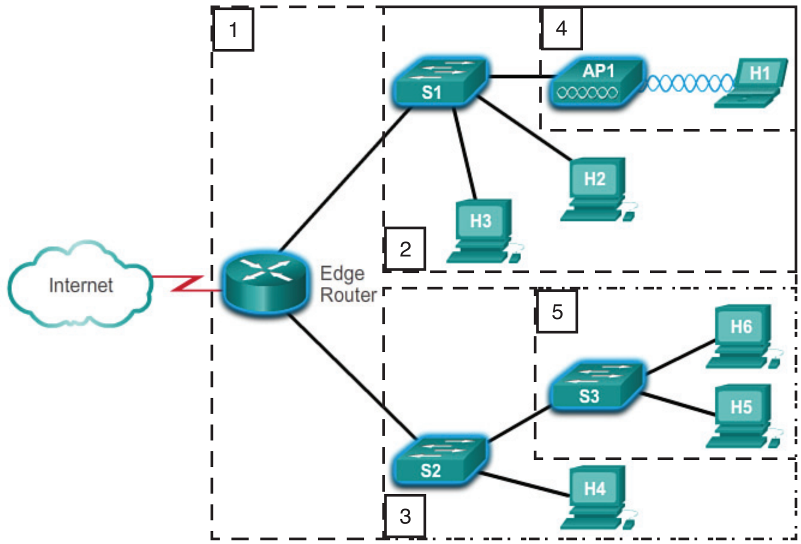

Figure 1-6 Failure Domain Examples

Limiting the Size of Failure Domains

Because a failure at the core layer of a network can have a potentially large impact, the network designer often concentrates on efforts to prevent failures. These efforts can greatly increase the cost of implementing the network. In the hierarchical design model, it is easiest and usually least expensive 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, thus affecting 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. This configuration is referred to as a building, or departmental, switch block. Each switch block acts independently of the others. As a result, the failure of a single device does not cause the network to go down. Even the failure of an entire switch block does not affect a significant number of end users.

Interactive Graphic

Activity 1.1.1.6: Identify Cisco Enterprise Architecture Modules

Go to the course online to perform this practice activity.

Expanding the Network (1.1.2)

A solid network design is not all that is needed for network expansion. This section reviews the features necessary to ensure that the network scales well as the company grows.

Design for Scalability (1.1.2.1)

To support an enterprise network, the network designer must develop a strategy to enable the network to be available and to scale effectively and easily. Included in a basic network design strategy are the following recommendations:

- Use expandable, modular equipment or clustered devices that can be easily upgraded to increase capabilities. Device modules can be added to the existing equipment to support new features and devices without requiring major equipment upgrades. Some devices can be integrated in a ***cluster*** to act as one device to simplify management and configuration.
- Design a hierarchical network to include modules that can be added, upgraded, and modified, as necessary, without affecting the design of the other functional areas of the network. For example, you can create a separate access layer that can be expanded without affecting the distribution and core layers of the campus network.
- Create an IPv4 or IPv6 address strategy that is hierarchical. Careful address planning eliminates the need to re-address the network to support additional users and services.
- Choose routers or multilayer switches to limit broadcasts and filter other undesirable traffic from the network. Use Layer 3 devices to filter and reduce traffic to the network core.

Figure 1-7 shows examples of some more advanced network requirements.

Advanced network design requirements shown in Figure 1-7 include

- Implementing redundant links in the network between critical devices and between access layer and core layer devices.
- Implementing multiple links between equipment, with either link aggregation (***EtherChannel***) or equal-cost load balancing, to increase bandwidth. Combining multiple Ethernet links into a single, load-balanced EtherChannel configuration increases available bandwidth. EtherChannel implementations can be used when budget restrictions prohibit purchasing high-speed interfaces and fiber runs.
- Implementing wireless connectivity to allow for mobility and expansion.
- Using a scalable routing protocol and implementing features within that routing protocol to isolate routing updates and minimize the size of the routing table.

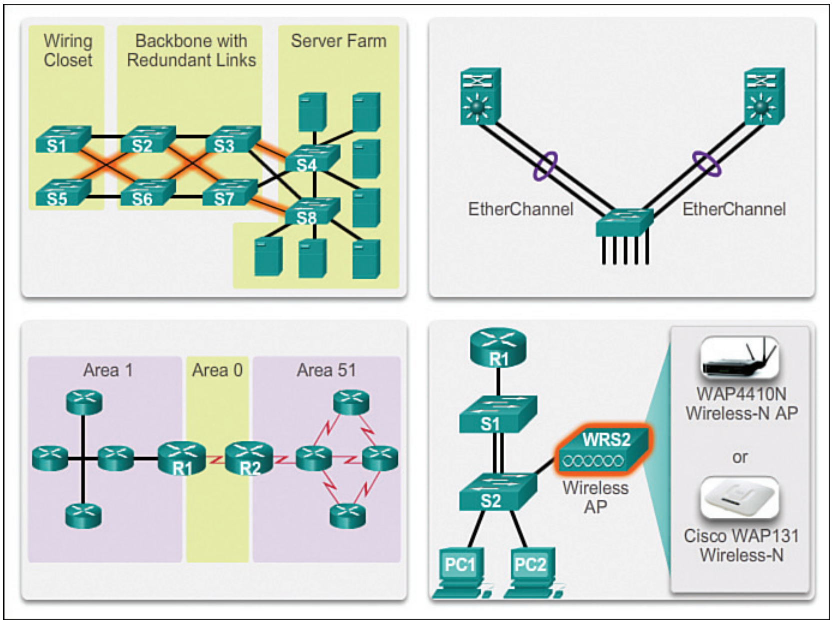

Figure 1-7 Design for Scalability

Planning for Redundancy (1.1.2.2)

Redundancy is a critical design feature for most company networks.

Implementing Redundancy

For many organizations, the availability of the network is essential to supporting business needs. Redundancy is an important part of network design for preventing disruption of network services by minimizing the possibility of a single point of failure. One method of implementing redundancy is by installing duplicate equipment and providing failover services for critical devices.

Another method of implementing redundancy is using redundant paths, as shown in Figure 1-8.

Redundant paths offer alternate physical paths for data to traverse the network. Redundant paths in a switched network support high availability. However, because of the operation of switches, redundant paths in a switched Ethernet network can cause logical Layer 2 loops. For this reason, ***Spanning Tree Protocol (STP)*** is required.

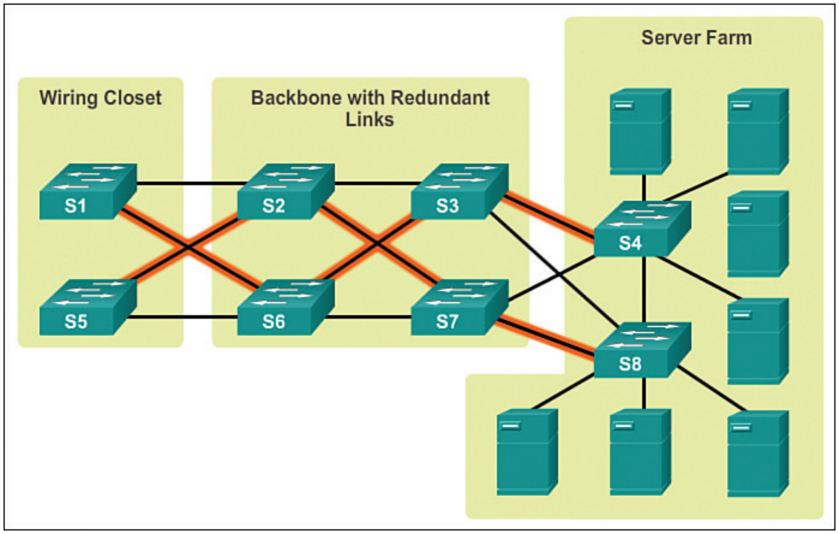

Figure 1-8 LAN Redundancy

STP allows for the redundancy required for reliability but eliminates the switching loops. It does this by providing a mechanism for disabling redundant paths in a switched network until the path is necessary, such as when failures occur. STP is an open standard protocol, used in a switched environment to create a loop-free logical topology.

More details about LAN redundancy and the operation of STP are covered in Chapter 2, "LAN Redundancy."

Increasing Bandwidth (1.1.2.3)

Bandwidth demand continues to grow as users increasingly access video content and migrate to IP phones. EtherChannel can quickly add more bandwidth.

Implementing EtherChannel

In hierarchical network design, some links between access and distribution switches might need to process a greater amount of traffic than other links. As traffic from multiple links converges onto a single, outgoing link, it is possible for that link to become a bottleneck. ***Link aggregation*** allows an administrator to increase the amount of bandwidth between devices by creating one logical link made up of several physical links. EtherChannel is a form of link aggregation used in switched networks, as shown in Figure 1-9.

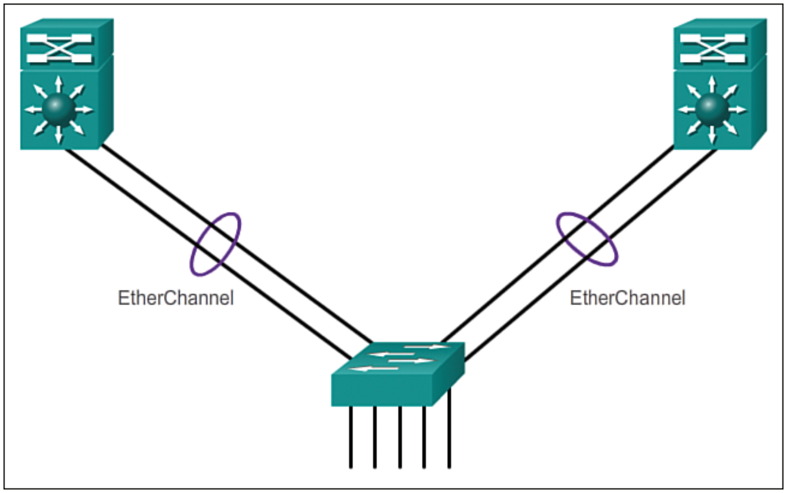

Figure 1-9 Advantages of EtherChannel

EtherChannel uses the existing switch ports; therefore, additional costs to upgrade the link to a faster and more expensive connection are not necessary. The EtherChannel is seen as one logical link using an EtherChannel interface. Most configuration tasks are done on the EtherChannel interface, instead of on each individual port, ensuring configuration consistency throughout the links. Finally, the EtherChannel configuration takes advantage of load balancing between links that are part of the same EtherChannel, and depending on the hardware platform, one or more *load-balancing* methods can be implemented.

EtherChannel operation and configuration will be covered in more detail in Chapter 3, "Link Aggregation."

Expanding the Access Layer (1.1.2.4)

Except in the most secure setting, today's users expect wireless access to the networks.

Implementing Wireless Connectivity

The network must be designed to be able to expand network access to individuals and devices, as needed. An increasingly important aspect of extending access layer connectivity is through wireless connectivity. Providing wireless connectivity offers many advantages, such as increased flexibility, reduced costs, and the ability to grow and adapt to changing network and business requirements.

To communicate wirelessly, end devices require a wireless NIC that incorporates a radio transmitter/receiver and the required software driver to make it operational.

Additionally, a wireless router or a ***wireless access point*** (AP) is required for users to connect, as shown in Figure 1-10.

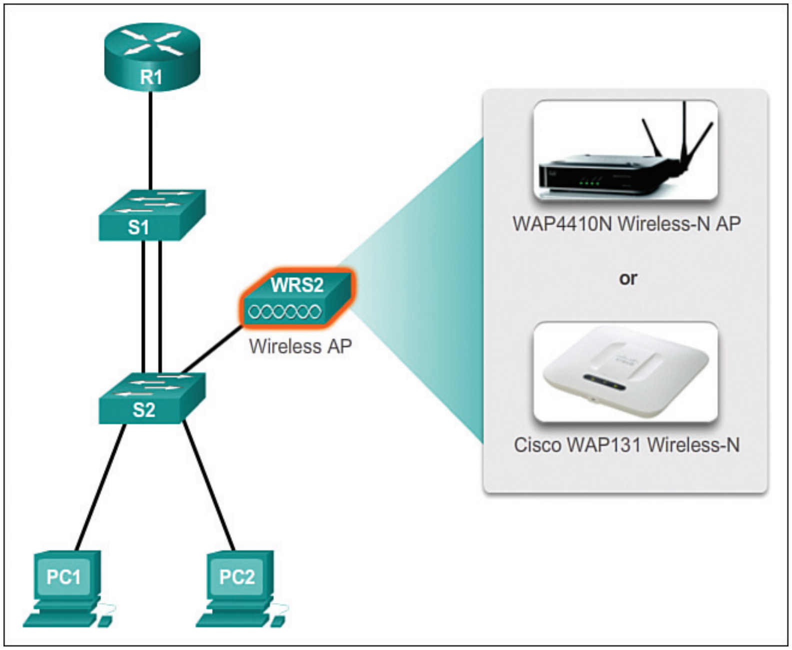

Figure 1-10 Wireless LANs

There are many considerations when implementing a wireless network, such as the types of wireless devices to use, wireless coverage requirements, interference considerations, and security considerations.

Wireless operation and implementation will be covered in more detail in Chapter 4, "Wireless LANs."

Fine-tuning Routing Protocols (1.1.2.5)

Routing protocol configuration is usually rather straightforward. However, to take full advantage of a protocol's feature set, it is often necessary to modify the configuration.

Managing the Routed Network

Enterprise networks and ISPs often use more advanced protocols, such as link-state protocols, because of their hierarchical design and ability to scale for large networks.

Link-state routing protocols such as ***Open Shortest Path First (OSPF)***, as shown in Figure 1-11, work well for larger hierarchical networks, where fast convergence is important.

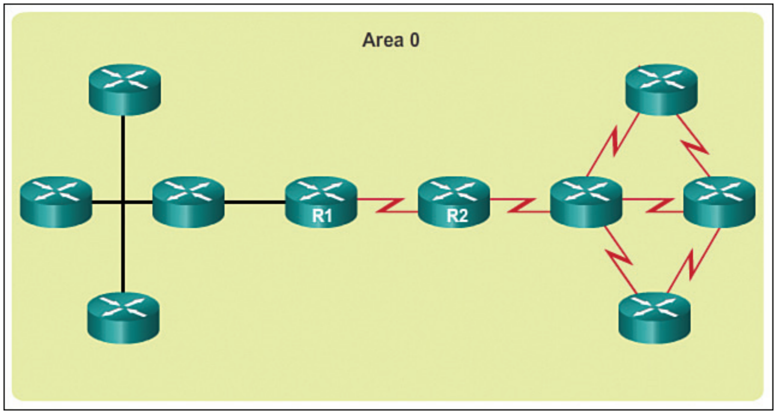

Figure 1-11 Single-Area OSPF

OSPF routers establish and maintain neighbor adjacency or adjacencies with other connected OSPF routers. When routers initiate an adjacency with neighbors, an exchange of link-state updates begins. Routers reach a FULL state of adjacency when they have synchronized views on their link-state database. With OSPF, link-state updates are sent when network changes occur.

OSPF is a popular link-state routing protocol that can be fine-tuned in many ways. Chapter 5, "Adjust and Troubleshoot ***Single-Area OSPF***," will cover some of the more advanced features of OSPF configuration and troubleshooting.

Additionally, OSPF supports a two-layer hierarchical design, or ***multiarea OSPF***, as shown in Figure 1-12.

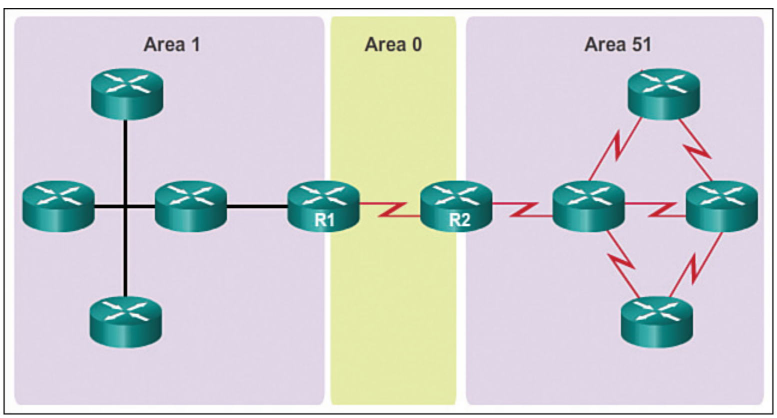

Figure 1-12 Multiarea OSPF

All OSPF networks begin with Area 0, also called the backbone area. As the network is expanded, other nonbackbone areas can be created. All nonbackbone areas must directly connect to area 0. Chapter 6, "Multiarea OSPF," introduces the benefits, operation, and configuration of multiarea OSPF.

Another popular routing protocol for larger networks is ***Enhanced Interior Gateway Routing Protocol (EIGRP)***. Cisco developed EIGRP as a proprietary ***distance vector routing protocol*** with enhanced capabilities. Although configuring EIGRP is relatively simple, the underlying features and options of EIGRP are extensive and robust. For example, EIGRP uses multiple tables to manage the routing process using ***Protocol Dependent Modules (PDM)***, as shown in Figure 1-13.

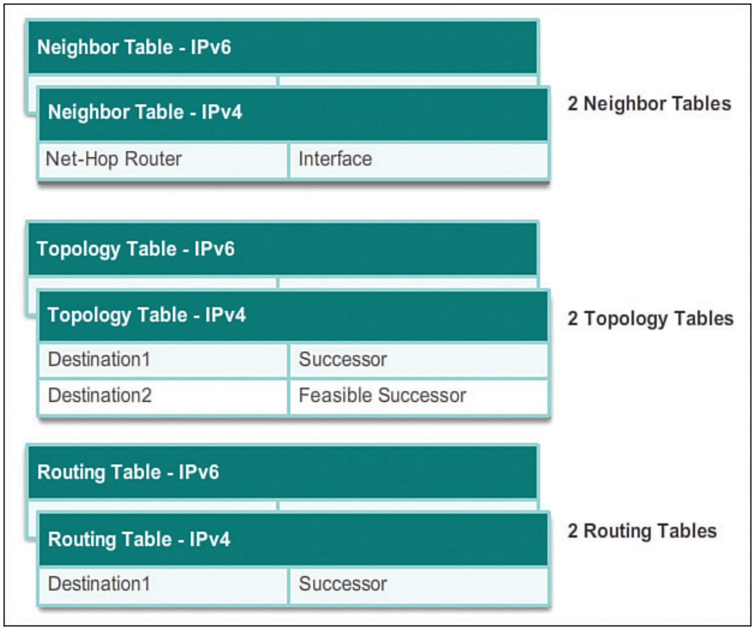

Figure 1-13 EIGRP Protocol Dependent Modules (PDM)

EIGRP contains many features that are not found in any other routing protocols. It is an excellent choice for large, multiprotocol networks that employ primarily Cisco devices.

Chapter 7, "EIGRP," introduces the operation and configuration of the EIGRP routing protocol, while Chapter 8, "EIGRP Advanced Configurations and Troubleshooting," covers some of the more advanced configuration options of EIGRP.

Interactive Graphic

Activity 1.1.2.6: Identify Scalability Terminology

Go to the course online to perform this practice activity.

Selecting Network Devices (1.2)

A basic understanding of switch and router hardware is essential to implementing network designs that scale.

Switch Hardware (1.2.1)

Cisco switches address the needs at the access, distribution, and core layers. Many models scale well with the network as it grows.

Switch Platforms (1.2.1.1)

When designing a network, it is important to select the proper hardware to meet current network requirements, as well as to allow for network growth. Within an enterprise network, both switches and routers play a critical role in network communication.

There are five categories of switches for enterprise networks, as shown in Figure 1-14:

- **Campus LAN Switches:** To scale network performance in an enterprise LAN, there are core, distribution, access, and compact switches. These switch platforms vary from fanless switches with eight fixed ports to 13-blade switches supporting hundreds of ports. Campus LAN switch platforms include the Cisco 2960, 3560, 3750, 3850, 4500, 6500, and 6800 Series.
- **Cloud-Managed Switches:** The Cisco Meraki cloud-managed access switches enable virtual stacking of switches. They monitor and configure thousands of switch ports over the web, without the intervention of onsite IT staff.
- **Data Center Switches:** A data center should be built based on switches that promote infrastructure scalability, operational continuity, and transport flexibility. The data center switch platforms include the Cisco Nexus Series switches and the Cisco Catalyst 6500 Series switches.
- **Service Provider Switches:** Service provider switches fall under two categories: aggregation switches and Ethernet access switches. Aggregation switches are carrier-grade Ethernet switches that aggregate traffic at the edge of a network. Service provider Ethernet access switches feature application intelligence, unified services, virtualization, integrated security, and simplified management.
- **Virtual Networking:** Networks are becoming increasingly virtualized. Cisco Nexus virtual networking switch platforms provide secure multitenant services by adding virtualization intelligence technology to the data center network.

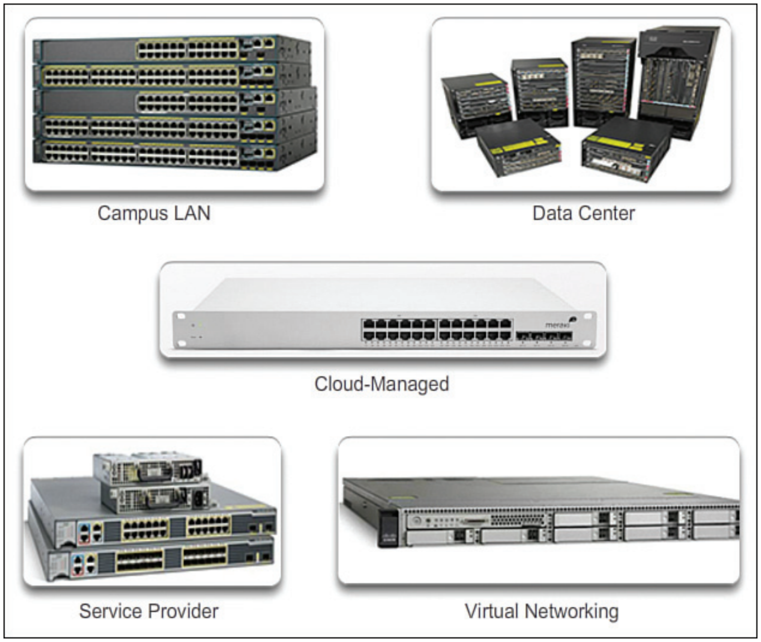

Figure 1-14 Switch Platforms

When selecting switches, network administrators must determine the switch form factors. This includes the *fixed configuration* shown in Figure 1-15, the *modular configuration* shown in Figure 1-16, the *stackable configuration* shown in Figure 1-17, or the nonstackable configuration.

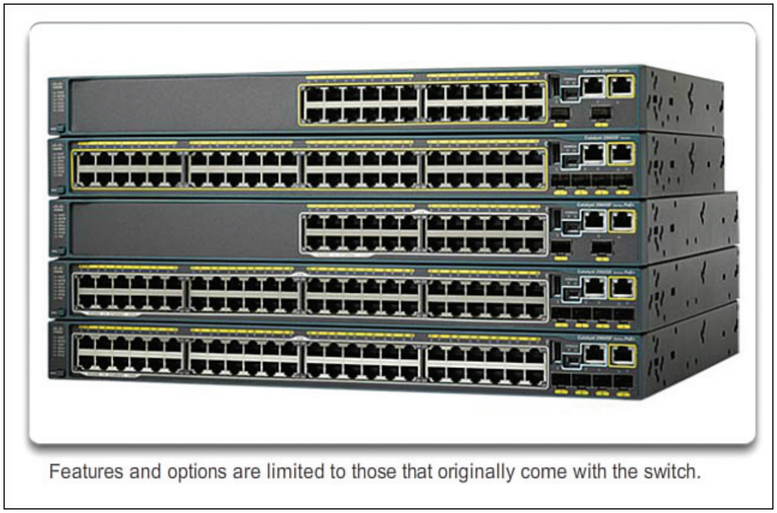

Figure 1-15 Fixed Configuration Switches

Figure 1-16 Modular Configuration Switches

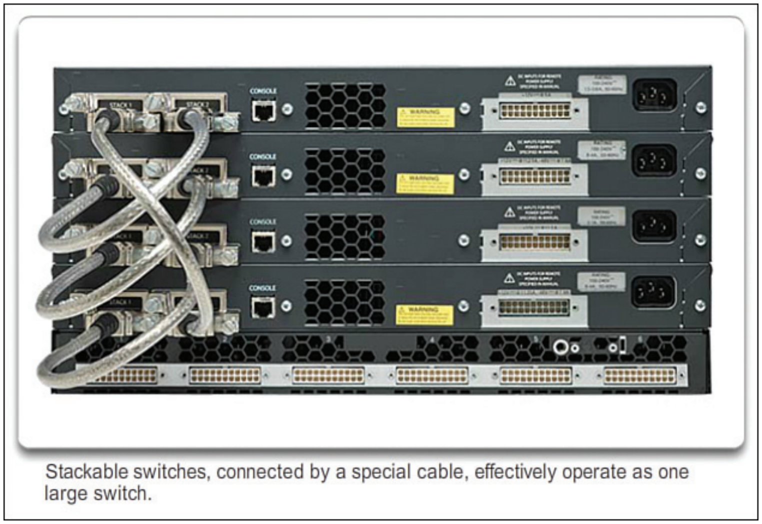

Figure 1-17 Stackable Configuration Switches

The height of the switch, which is expressed in the number of rack units, is also important for switches that are mounted in a rack. For example, the fixed configuration switches shown in Figure 1-15 are all one rack unit (1U) high.

In addition to these considerations, the following list highlights other common business considerations when selecting switch equipment:

- **Cost:** The cost of a switch will depend on the number and speed of the interfaces, supported features, and expansion capability.
- **Port Density:** Network switches must support the appropriate number of devices on the network.
- **Power:** It is now common to power access points, IP phones, and even compact switches using Power over Ethernet (PoE). In addition to PoE considerations, some chassis-based switches support redundant power supplies.
- **Reliability:** The switch should provide continuous access to the network.
- **Port Speed:** The speed of the network connection is of primary concern to end users.
- **Frame Buffers:** The ability of the switch to store frames is important in a network where there might be congested ports to servers or other areas of the network.
- **Scalability:** The number of users on a network typically grows over time; therefore, the switch should provide the opportunity for growth.

Port Density (1.2.1.2)

The port density of a switch refers to the number of ports available on a single switch. Figure 1-18 shows the port density of three different switches.

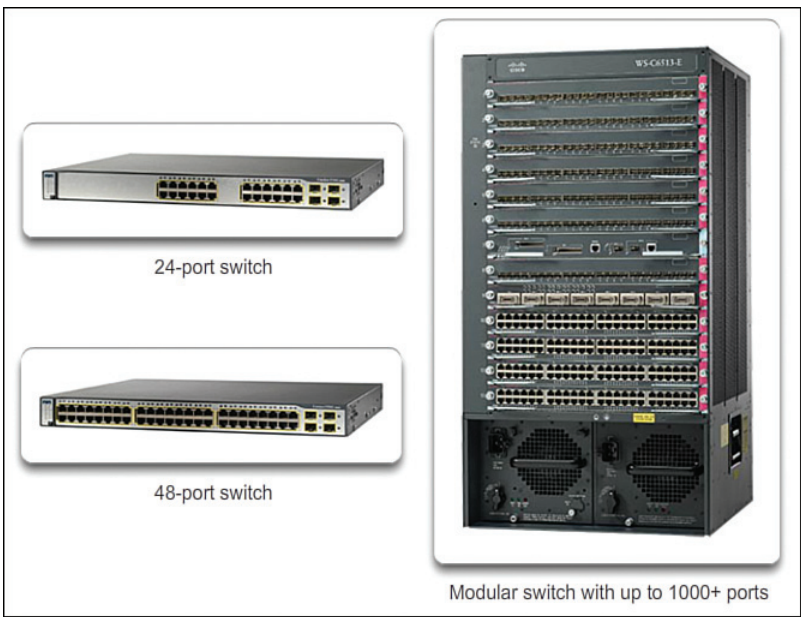

Figure 1-18 Port Densities

Fixed configuration switches typically support up to 48 ports on a single device. They have options for up to four additional ports for small form-factor pluggable (SFP) devices. High-port densities allow for better use of limited space and power. If there are two switches that each contain 24 ports, they would be able to support up to 46 devices, because at least one port per switch is lost with the connection of each switch to the rest of the network. In addition, two power outlets are required. Alternatively, if there is a single 48-port switch, 47 devices can be supported, with only one port used to connect the switch to the rest of the network, and only one power outlet needed to accommodate the single switch.

Modular switches can support very high-port densities through the addition of multiple switch port line cards. For example, some Catalyst 6500 switches can support in excess of 1000 switch ports.

Large enterprise networks that support many thousands of network devices require high-density, modular switches to make the best use of space and power. Without using a high-density modular switch, the network would need many fixed configuration switches to accommodate the number of devices that need network access. This approach can consume many power outlets and a lot of closet space.

The network designer must also consider the issue of uplink bottlenecks: A series of fixed configuration switches can consume many additional ports for bandwidth aggregation between switches, for the purpose of achieving target performance. With a single modular switch, bandwidth aggregation is less of an issue, because the backplane of the chassis can provide the necessary bandwidth to accommodate the devices connected to the switch port line cards.

Forwarding Rates (1.2.1.3)

Forwarding rates define the processing capabilities of a switch by rating how much data the switch can process per second. Switch product lines are classified by forwarding rates, as shown in Figure 1-19.

Entry-level switches have lower forwarding rates than enterprise-level switches. Forwarding rates are important to consider when selecting a switch. If the switch forwarding rate is too low, it cannot accommodate full wire-speed communication across all of its switch ports. ***Wire speed*** is the data rate that each Ethernet port on the switch is capable of attaining. Data rates can be 100 Mb/s, 1 Gb/s, 10 Gb/s, or 100 Gb/s.

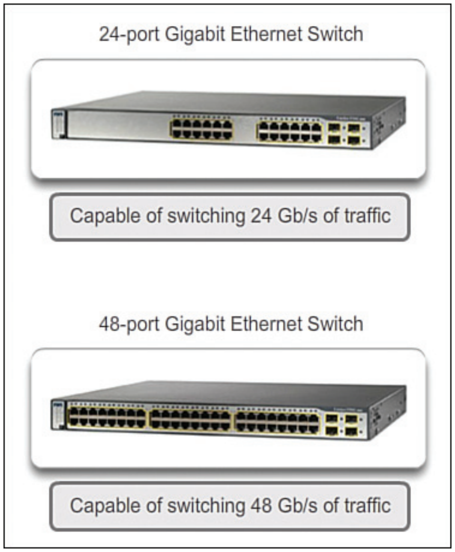

Figure 1-19 Forwarding Rate

For example, a typical 48-port gigabit switch operating at full wire speed generates 48 Gb/s of traffic. If the switch only supports a forwarding rate of 32 Gb/s, it cannot run at full wire speed across all ports simultaneously. Fortunately, 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. This means that less expensive, lower-performing switches can be used at the access layer, and more expensive, higher-performing switches can be used at the distribution and core layers, where the forwarding rate has a greater impact on network performance.

Power over Ethernet (1.2.1.4)

Power over Ethernet (PoE) allows the switch to deliver power to a device over the existing Ethernet cabling. This feature can be used by IP phones and some wireless access points, as shown in Figure 1-20.

PoE allows more flexibility when installing wireless access points and IP phones, allowing them to be installed anywhere that there is an Ethernet cable. A network administrator should ensure that the PoE features are required, because switches that support PoE are expensive.

The relatively new Cisco Catalyst 2960-C and 3560-C Series compact switches support PoE pass-through, as shown in Figure 1-21.

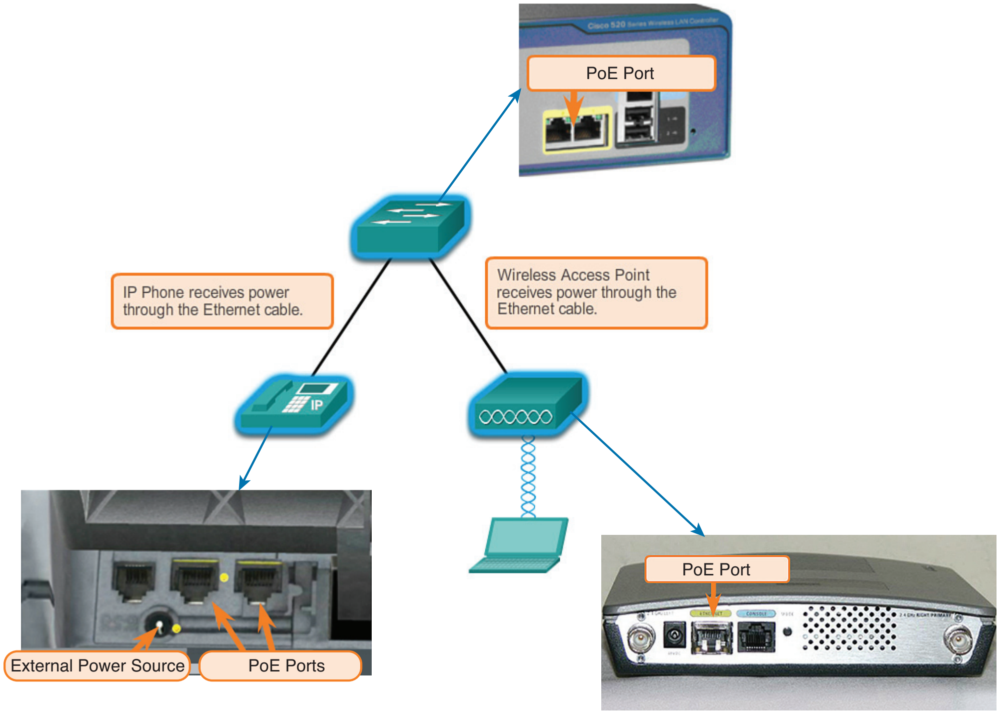

Figure 1-20 Power over Ethernet

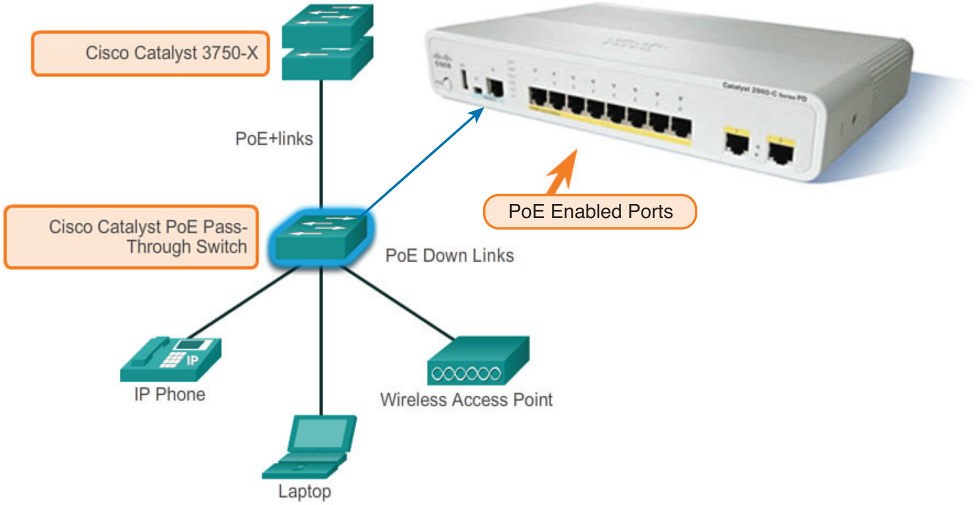

Figure 1-21 PoE Pass-Through

PoE pass-through allows a network administrator to power PoE devices connected to the switch, as well as the switch itself, by drawing power from certain upstream switches.

Multilayer Switching (1.2.1.5)

Multilayer switches are typically deployed in the core and distribution layers of an organization's switched network. Multilayer switches are characterized by their ability to build a routing table, support a few routing protocols, and forward IP packets at a rate close to that of Layer 2 forwarding. Multilayer switches often support specialized hardware, such as ***application-specific integrated circuits (ASIC)***. ASICs, along with dedicated software data structures, can streamline the forwarding of IP packets independent of the CPU.

There is a trend in networking toward a pure Layer 3 switched environment. When switches were first used in networks, none of them supported routing; now, almost all switches support routing. It is likely that soon all switches will incorporate a route processor because the cost of doing so is decreasing relative to other constraints. Eventually the term *multilayer switch* will be redundant.

As shown in Figure 1-22, the Catalyst 2960 switches illustrate the migration to a pure Layer 3 environment.

Figure 1-22 Cisco Catalyst 2960 Series Switches

With IOS versions prior to 15.x, these switches supported only one active switched virtual interface (SVI). The Catalyst 2960 also supports multiple active SVIs. This means that the switch can be remotely accessed through multiple IP addresses on distinct networks.

Interactive Graphic

Activity 1.2.1.6: Selecting Switch Hardware

Go to the course online to perform this practice activity.

Packet Tracer Activity

Packet Tracer Activity 1.2.1.7: Comparing 2960 and 3560 Switches

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.

Lab 1.2.1.8: Selecting Switching Hardware

In this lab, you will complete the following objectives:

- Part 1: Explore Cisco Switch Products
- Part 2: Select an Access Layer Switch
- Part 3: Select a Distribution/Core Layer Switch

Router Hardware (1.2.2)

Like switches, routers can play a role in the access, distribution, and core layers of the network. In many small networks like branch offices and a teleworker's home network, all three layers are implemented within a router.

Router Requirements (1.2.2.1)

In the distribution layer of an enterprise network, routing is required. Without the routing process, packets cannot leave the local network.

Routers play a critical role in networking by interconnecting multiple sites within an enterprise network, providing redundant paths, and connecting ISPs on the Internet. Routers can also act as a translator between different media types and protocols. For example, a router can accept packets from an Ethernet network and reencapsulate them for transport over a serial network.

Routers use the network portion of the destination IP address to route packets to the proper destination. They select an alternate path if a link goes down or traffic is congested. All hosts on a local network specify the IP address of the local router interface in their IP configuration. This router interface is the default gateway.

Routers also serve the following beneficial functions, as shown in Figure 1-23:

- Provide broadcast containment
- Connect remote locations
- Group users logically by application or department
- Provide enhanced security

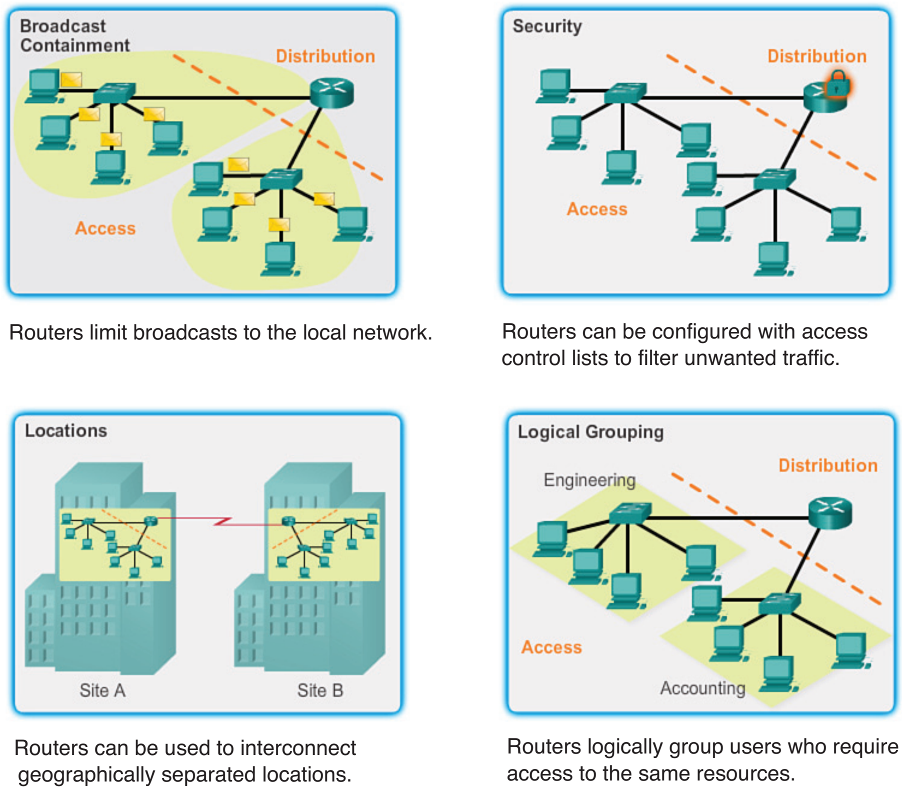

Figure 1-23 Router Functions

With the enterprise and the ISP, the ability to route efficiently and recover from network link failures is critical to delivering packets to their destination.

Cisco Routers (1.2.2.2)

As the network grows, it is important to select the proper routers to meet its requirements. As shown in Figure 1-24, there are three categories of routers:

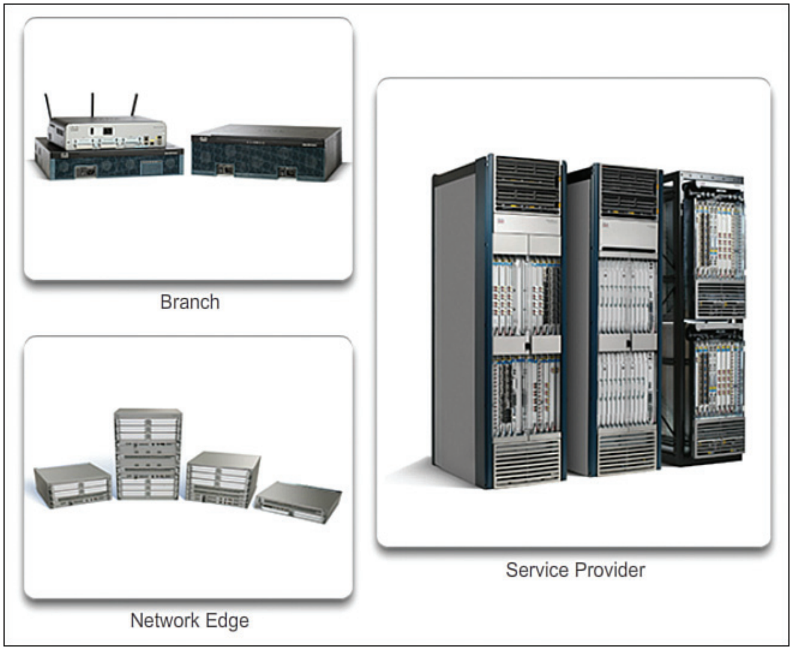

Figure 1-24 Router Platforms

- ***Branch Routers***: Branch routers optimize branch services on a single platform while delivering an optimal application experience across branch and WAN infrastructures. Maximizing service availability at the branch requires networks designed for 24x7x365 uptime. Highly available branch networks must ensure fast recovery from typical faults, while minimizing or eliminating the impact on service, and provide simple network configuration and management.
- ***Network Edge Routers***: Network edge routers enable the network edge to deliver high-performance, highly secure, and reliable services that unite campus, data center, and branch networks. Customers expect a high-quality media experience and more types of content than ever before. Customers want interactivity, personalization, mobility, and control for all content. Customers also want to access content anytime and anyplace they choose, over any device, whether at home, at work, or on the go. Network edge routers must deliver enhanced quality of service and nonstop video and mobile capabilities.

- ***Service Provider Routers***: Service provider routers differentiate the service portfolio and increase revenues by delivering end-to-end scalable solutions and subscriber-aware services. Operators must optimize operations, reduce expenses, and improve scalability and flexibility to deliver next-generation Internet experiences across all devices and locations. These systems are designed to simplify and enhance the operation and deployment of service-delivery networks.

Router Hardware (1.2.2.3)

Routers also come in many form factors, as shown in Figure 1-25. Network administrators in an enterprise environment should be able to support a variety of routers, from a small desktop router to a rack-mounted or blade model.

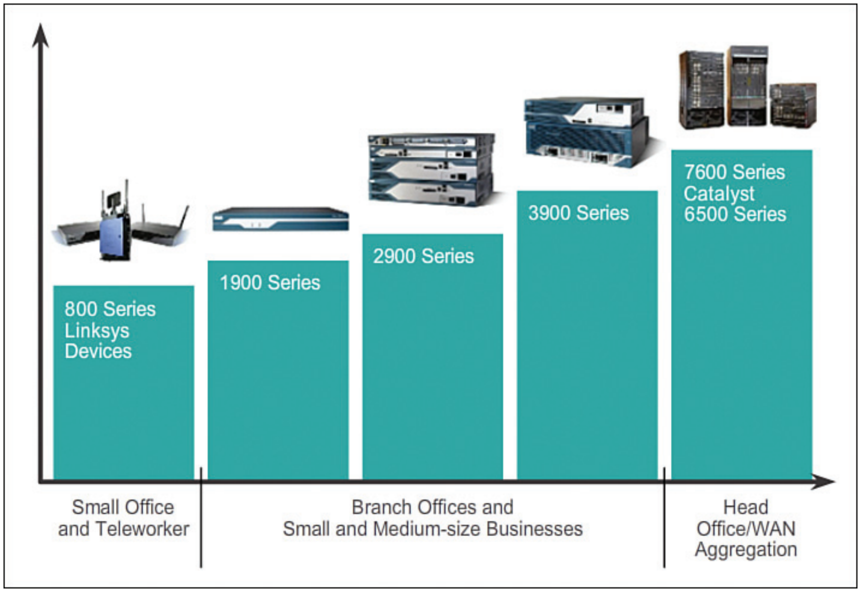

Figure 1-25 Routing Devices

Routers can also be categorized as fixed configuration or modular. With the fixed configuration, the desired router interfaces are built in. Modular routers come with multiple slots that allow a network administrator to change the interfaces on the router. As an example, a Cisco 1841 router comes with two Fast Ethernet RJ-45 interfaces built in and two slots that can accommodate many different network interface modules. Routers come with a variety of different interfaces, such as Fast Ethernet, Gigabit Ethernet, Serial, and Fiber-Optic.

Interactive Graphic

Activity 1.2.2.4: Identify the Router Category

Go to the course online to perform this practice activity.

Managing Devices (1.2.3)

Routers and switches all come with Cisco IOS Software. Network administrators are responsible for managing these devices. This includes initial configuration, verification, and troubleshooting tasks as well as maintaining up-to-date images and backing up the configuration files.

Managing IOS Files and Licensing (1.2.3.1)

With such a wide selection of network devices to choose from in the Cisco product line, an organization can carefully determine the ideal combination to meet the needs of the employees and the customers.

When selecting or upgrading a ***Cisco IOS*** device, it is important to choose the proper IOS image with the correct feature set and version. IOS refers to the package of routing, switching, security, and other internetworking technologies integrated into a single multitasking operating system. When a new device is shipped, it comes preinstalled with the software image and the corresponding permanent licenses for the customer-specified packages and features.

For routers, beginning with Cisco IOS Software Release 15.0, Cisco modified the process to enable new technologies within the IOS feature sets, as shown in Figure 1-26.

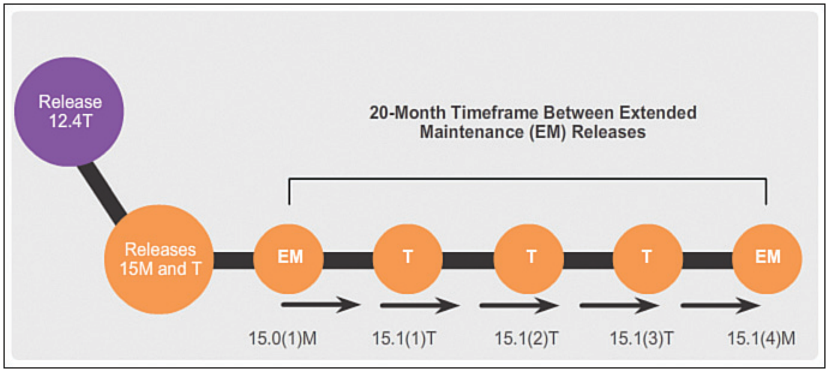

Figure 1-26 Cisco IOS Software 15 Release Family

Chapter 9, “IOS Images and Licensing,” covers more information on managing and maintaining the Cisco IOS licenses.

In-Band Versus Out-of-Band Management (1.2.3.2)

Regardless of the Cisco IOS network device being implemented, there are two methods for connecting a PC to that network device for configuration and monitoring tasks. These methods include out-of-band and ***in-band management***, as shown in Figure 1-27.

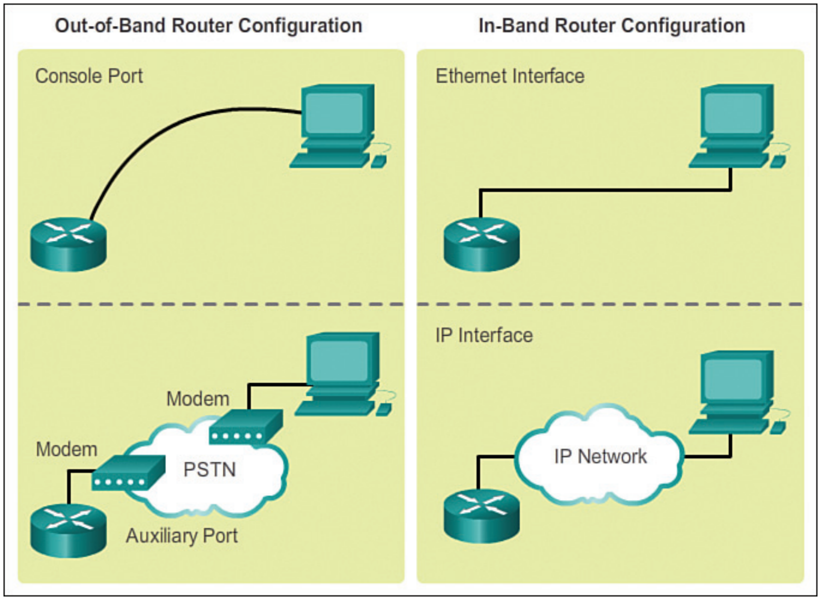

Figure 1-27 In-Band Versus Out-of-Band Configuration Options

Out-of-band management is used for initial configuration or when a network connection is unavailable. Configuration using out-of-band management requires

- Direct connection to console or AUX port
- Terminal emulation client

In-band management is used to monitor and make configuration changes to a network device over a network connection. Configuration using in-band management requires

- At least one network interface on the device to be connected and operational
- Telnet, SSH, or HTTP to access a Cisco device

Basic Router CLI Commands (1.2.3.3)

A basic router configuration includes the host name for identification, passwords for security, assignment of IP addresses to interfaces for connectivity, and basic routing. Assuming that the physical interfaces are connected to the network, Example 1-1 shows the commands entered to enable a router with OSPF. Verify and save configuration changes using the **copy running-config startup-config** command.

Example 1-1 Enabling a Router with OSPF

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exec-timeout 0 0
R1(config-line)# line vty 0 4
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 shutdown
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 shutdown
R1(config-if)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 172.16.1.0 0.0.0.255 area 0
R1(config-router)# network 172.16.3.0 0.0.0.3 area 0
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0
R1(config-router)# end
R1# copy running-config startup-config
```

Example 1-2 shows the results of the configuration commands that were entered in Example 1-1. To clear the router configuration, use the **erase startup-config** command and then the **reload** command.

Example 1-2 Router Running Configuration

```
R1# show running-config
Building configuration...
```

```
Current configuration : 1242 bytes
!
Version 15.1
Service timestamps debug datetime msec
Service timestamps log datetime msec
Service password-encryption
!
hostname R1
!
enable secret class
!
<output omitted>
!
interface GigabitEthernet0/0
 description Link to LAN 1
 ip address 172.16.1.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 description Link to R2
 ip address 172.16.3.1 255.255.255.252
 clock rate 128000
 no shutdown
!
interface Serial0/0/1
 description Link to R3
 ip address 192.168.10.5 255.255.255.252
 no shutdown
!
router ospf 10
 router-id 1.1.1.1
 network 172.16.1.0 0.0.0.255 area 0
 network 172.16.3.0 0.0.0.3 area 0
 network 192.168.10.4 0.0.0.3 area 0
!
banner motd ^C Authorized Access Only! ^C
!
line console 0
 password cisco
 login
 exec-timeout 0 0
Line aux 0
line vty 0 4
 password cisco
 login
```

Basic Router show Commands (1.2.3.4)

Here are some of the most commonly used IOS commands to display and verify the operational status of the router and related network functionality. These commands are divided into several categories.

The following show commands are related to routing:

- **show ip protocols:** As shown in Example 1-3, this command displays information about the routing protocols configured. If OSPF is configured, this includes the OSPF process ID, the router ID, networks the router is advertising, the neighbors the router is receiving updates from, and the default administrative distance, which is 110 for OSPF.

Example 1-3 show ip protocols Command

```
R1# show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.255 area 0
    172.16.3.0 0.0.0.3 area 0
    192.168.10.4 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:11:48
    2.2.2.2              110      00:11:50
    3.3.3.3              110      00:11:50
  Distance: (default is 110)
```

- **show ip route:** As shown in Example 1-4, this command displays routing table information, including routing codes, known networks, administrative distance and metrics, how routes were learned, next hop, static routes, and default routes.

Example 1-4 show ip route Command

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C       172.16.1.0/24 is directly connected, GigabitEthernet0/0
L       172.16.1.1/32 is directly connected, GigabitEthernet0/0
O       172.16.2.0/24 [110/65] via 172.16.3.2, 01:43:03, Serial0/0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
L       172.16.3.1/32 is directly connected, Serial0/0/0
O    192.168.1.0/24 [110/65] via 192.168.10.6, 01:43:03, Serial0/0/1
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C       192.168.10.4/30 is directly connected, Serial0/0/1
L       192.168.10.5/32 is directly connected, Serial0/0/1
O       192.168.10.8/30 [110/128] via 172.16.3.2, 01:43:03, Serial0/0/0
                        [110/128] via 192.168.10.6, 01:43:03, Serial0/0/1
```

- **show ip ospf neighbor:** As shown in Example 1-5, this command displays information about OSPF neighbors that have been learned, including the Router ID of the neighbor, the priority, the state (Full = adjacency has been formed), the IP address, and the local interface that learned of the neighbor.

Example 1-5 show ip ospf neighbor Command

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State       Dead Time   Address         Interface
2.2.2.2           0   FULL/  -    00:00:34    172.16.3.2      Serial0/0/0
3.3.3.3           0   FULL/  -    00:00:34    192.168.10.6    Serial0/0/1
```

The following show commands are related to interfaces:

- **show interfaces:** As shown in Example 1-6, this command displays interfaces with line (protocol) status, bandwidth, delay, reliability, encapsulation, duplex, and I/O statistics. If specified without a specific interface designation, all interfaces will be displayed. If a specific interface is specified after the command, information about that interface only will be displayed.

Example 1-6 show interfaces Command

```
R1# show interfaces
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 00e0.8fb2.de01 (bia 00e0.8fb2.de01)
  Description: Link to LAN 1
  Internet address is 172.16.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Description: Link to R2
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
<output omitted>
Serial0/0/1 is up, line protocol is up (connected)
  Hardware is HD64570
  Description: Link to R3
  Internet address is 192.168.10.5/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
```

- **show ip interfaces:** As shown in Example 1-7, this command displays interface information, including protocol status, IP address, whether a helper address is configured, and whether an ACL is enabled on the interface. If specified without a specific interface designation, all interfaces will be displayed. If a specific interface is specified after the command as shown in Example 1-7, information about that interface only will be displayed.

Example 1-7 show ip interface Command

```
R1# show ip interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 172.16.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5 224.0.0.6
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  IPv4 WCCP Redirect outbound is disabled
  IPv4 WCCP Redirect inbound is disabled
  IPv4 WCCP Redirect exclude is disabled
```

- **show ip interface brief:** As shown in Example 1-8, this command displays all interfaces with IP addressing information and interface and line protocol status.

Example 1-8 show ip interface brief Command

```
R1# show ip interface brief
Interface            IP-Address      OK?  Method   Status                    Protocol
GigabitEthernet0/0   172.16.1.1      YES  manual   up                        up
GigabitEthernet0/1   unassigned      YES  unset    administratively down     down
Serial0/0/0          172.16.3.1      YES  manual   up                        up
Serial0/0/1          192.168.10.5    YES  manual   up                        up
Vlan1                unassigned      YES  unset    administratively down     down
```

- **show protocols:** As shown in Example 1-9, this command displays information about the routed protocol that is enabled and the protocol status of interfaces.

Example 1-9 show protocols Command

```
R1# show protocols
Global values:
  Internet Protocol routing is enabled
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
Vlan1 is administratively down, line protocol is down
```

Other connectivity-related commands include the **show cdp neighbors** command shown in Example 1-10.

Example 1-10 show cdp neighbors Command

```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID  Local Intrfce   HoldtmeCapability      Platform    Port ID
S1         Gig 0/0           126         S        2960        Gig 1/1
R2         Ser 0/0/0         136         R        C1900       Ser 0/0/0
R3         Ser 0/0/1         133         R        C1900       Ser 0/0/0
```

This command displays information on directly connected devices, including Device ID, local interface that the device is connected to, capability (R = router, S = switch), platform, and Port ID of the remote device. The details option includes IP addressing information and the IOS version.

Basic Switch CLI Commands (1.2.3.5)

Basic switch configuration includes the host name for identification, passwords for security, and assignment of IP addresses for connectivity. In-band access requires the switch to have an IP address. Example 1-11 shows the commands entered to enable a switch.

Example 1-11 Enable a Switch with a Basic Configuration

```
Switch# enable
Switch# configure terminal
Switch(config)# hostname S1
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)# service password-encryption
S1(config)# banner motd $ Authorized Access Only! $
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.5 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# 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)# end
S1# copy running-config startup-config
```

Example 1-12 shows the results of the configuration commands that were entered in Example 1-11.

Example 1-12 Switch Running Configuration

```
S1# show running-config
<some output omitted>
version 15.0
```

```
service password-encryption
!
hostname S1
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
!
interface Vlan1
 ip address 192.168.1.5 255.255.255.0
!
ip default-gateway 192.168.1.1
!
banner motd ^C Authorized Access Only ^C
!
line con 0
 exec-timeout 0 0
 password 7 1511021F0725
 login
line vty 0 4
 password 7 1511021F0725
 login
line vty 5 15
 login
!
end
```

Verify and save the switch configuration using the **copy running-config startup-config** command. To clear the switch configuration, use the **erase startup-config** command and then the **reload** command. It might also be necessary to erase any VLAN information using the **delete flash:vlan.dat** command. When switch configurations are in place, view the configurations using the **show running-config** command.

Basic Switch show Commands (1.2.3.6)

Switches make use of common IOS commands for configuration, to check for connectivity, and to display current switch status. For example, the following commands are useful for gathering some important information:

- **show port-security interface:** Displays any ports with security activated. To examine a specific interface, include the interface ID, as shown in Example 1-13. Information included in the output: the maximum addresses allowed, current count, security violation count, and action to be taken.

Example 1-13 show port-security interface Command

```
S1# show port-security interface fa0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0024.50d1.9902:1
Security Violation Count   : 0
```

- **show port-security address:** As shown in Example 1-14, this command displays all secure MAC addresses configured on all switch interfaces.

Example 1-14 show port-security address Command

```
S1# show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                        Ports   Remaining Age
                                                               (mins)
----    -----------       ----                        -----   -------------
   1    0024.50d1.9902    SecureDynamic                Fa0/2        -
--------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1536
```

- **show interfaces:** As shown in Example 1-15, this command displays one or all interfaces with line (protocol) status, bandwidth, delay, reliability, encapsulation, duplex, and I/O statistics.

Example 1-15 show interfaces Command

```
S1# show interfaces fa0/2
FastEthernet0/2 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 001e.14cf.eb04 (bia 001e.14cf.eb04)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 2000 bits/sec, 3 packets/sec
     59 packets input, 11108 bytes, 0 no buffer
     Received 59 broadcasts (59 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 59 multicast, 0 pause input
     0 input packets with dribble condition detected
     886 packets output, 162982 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

- **show mac-address-table:** As shown in Example 1-16, this command displays all MAC addresses that the switch has learned, how those addresses were learned (dynamic/static), the port number, and the VLAN assigned to the port.

Example 1-16 show mac address-table Command

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

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    001e.4915.5405    DYNAMIC     Fa0/3
   1    001e.4915.5406    DYNAMIC     Fa0/4
   1    0024.50d1.9901    DYNAMIC     Fa0/1
   1    0024.50d1.9902    STATIC      Fa0/2
   1    0050.56be.0e67    DYNAMIC     Fa0/1
   1    0050.56be.c23d    DYNAMIC     Fa0/6
   1    0050.56be.df70    DYNAMIC     Fa0/3
Total Mac Addresses for this criterion: 27
```

Like the router, the switch also supports the **show cdp neighbors** command.

The same in-band and out-of-band management techniques that apply to routers also apply to switch configuration.

Summary (1.3)

Class Activity 1.3.1.1: Layered Network Design Simulation

As the network administrator for a very small network, you want to prepare a simulated-network presentation for your branch manager to explain how the network currently operates.

The small network includes the following equipment:

- One 2911 Series router
- One 3560 switch
- One 2960 switch
- Four user workstations (PCs or laptops)
- One printer

Interactive Graphic

Activity 1.3.1.2: Basic Switch Configurations

Go to the course online to perform this practice activity.

Packet Tracer Activity

Packet Tracer Activity 1.3.1.3: Skills Integration Challenge

As a recently hired LAN technician, your network manager has asked you to demonstrate your ability to configure a small LAN. Your tasks include configuring initial settings on two switches using the Cisco IOS and configuring IP address parameters on host devices to provide end-to-end connectivity. You are to use two switches and two hosts/PCs on a cabled and powered network.

The hierarchical network design model divides network functionality into the access layer, the distribution layer, and the core layer. The Cisco Enterprise Architecture further divides the network into functional components.

A well-designed network controls traffic and limits the size of failure domains. Routers and multilayer switches can be deployed in pairs so that the failure of a single device does not cause service disruptions.

A network design should include an IP addressing strategy, scalable and fast-converging routing protocols, appropriate Layer 2 protocols, and modular or clustered devices that can be easily upgraded to increase capacity.

A mission-critical server should have a connection to two different access layer switches. It should have redundant modules when possible and a power backup source. It might be appropriate to provide multiple connections to one or more ISPs.

Security monitoring systems and IP telephony systems must have high availability and often have special design considerations.

The network designer should specify a router from the appropriate category: branch router, network edge router, or service provider router. It is important to also deploy the appropriate type of switches for a given set of requirements, switch features and specifications, and expected traffic flow.

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion *Introduction to Scaling Networks Lab Manual* (ISBN 978-1-58713-325-1). The Packet Tracer Activities PKA files are found in the online course.

Class Activities

- Class Activity 1.0.1.2: Network by Design
- Class Activity 1.3.1.1: Layered Network Design Simulation

Labs

- Lab 1.2.1.8: Selecting Switching Hardware

Packet Tracer Activity

Packet Tracer Activities

- Packet Tracer 1.2.1.7: Comparing 2960 and 3560 Switches
- Packet Tracer 1.3.1.3: Skills Integration Challenge

Check Your Understanding Questions

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix “Answers to ‘Check Your Understanding’ Questions” lists the answers.

1. What are the expected features of modern enterprise networks? (Choose two.)
   - A. Support for 90 percent reliability
   - B. Support for limited growth
   - C. Support for converged network traffic
   - D. Support for distributed administrative control
   - E. Support for critical applications
2. Which of the following methods help to prevent the disruption of network services? (Choose two.)
   - A. Changing the routing protocols at regular intervals
   - B. Using redundant connections to provide alternate physical paths
   - C. Installing duplicate equipment to provide failover services
   - D. Removing switches that cause loops
   - E. Using VLANs to segment network traffic
3. Which feature could be used in a network design to increase the bandwidth by combining multiple physical links into a single logical link?
   - A. VLANs
   - B. Trunk ports
   - C. EtherChannel
   - D. Subinterfaces
4. Which network design solution will best extend access layer connectivity to host devices?
   - A. Implementing EtherChannel
   - B. Implementing redundancy
   - C. Implementing routing protocols
   - D. Implementing wireless connectivity

5. How much traffic is a 48-port gigabit switch capable of generating when operating at full wire speed?

   A. 44 Gb/s, because of overhead requirements

   B. 48 Gb/s, by providing full bandwidth to each port

   C. 24 Gb/s, because this is the maximum forwarding rate on Cisco switches

   D. 1 Gb/s, because data can only be forwarded from one port at a time

6. Which type of router would an enterprise use to allow customers to access content anytime and anyplace, regardless of whether they are at home or work?

   A. Service provider routers

   B. Network edge routers

   C. Branch routers

   D. Modular routers

7. What is a characteristic of out-of-band device management?

   A. It requires a terminal emulation client.

   B. It requires Telnet, SSH, or HTTP to access a Cisco device.

   C. It requires at least one network interface on the device to be connected and operational.

   D. Out-of-band device management requires a direct connection to a network interface.

8. The number of ports available on a single switch is referred to as ________.

9. Among the beneficial functions of a router are enhanced network security and containment of ________ traffic.

10. Indicate the design model layer described by the following network functions:

    The ________ layer provides connectivity for the users.

    The ________ layer forwards traffic from one local network to another.

    The ________ layer provides a high-speed backbone link between dispersed networks.