Course Booklet

Scaling Networks

Version 6

ciscopress.com

Cisco | Networking Academy
Mind Wide Open

Scaling Networks v6 Course Booklet

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing May 2017

Library of Congress Control Number: 2017936409

ISBN-13: 978-1-58713-430-2

ISBN-10: 1-58713-430-6

Warning and Disclaimer

This book is designed to provide information about Cisco Networking Academy Scaling Networks course. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Editor-in-Chief
Mark Taub

Alliances Manager, Cisco Press
Ron Fligge

Executive Editor
Mary Beth Ray

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Editorial Assistant
Vanessa Evans

Cover Designer
Chuti Prasertsith

Indexer
Erika Millen

Composition
codeMantra

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, Please visit www.netacad.com

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Reader Services

Register your copy at www.ciscopress.com/title/9781587134302 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account*. Enter the product ISBN 9781587134302 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

CISCO™

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Contents at a Glance

Contents

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

About This Course Booklet

Your Cisco Networking Academy Course Booklet is designed as a study resource you can easily read, highlight, and review on the go, wherever the Internet is not available or practical:

- The text is extracted directly, word-for-word, from the online course so you can highlight important points and take notes in the "Your Chapter Notes" section.
- Headings with the exact page correlations provide a quick reference to the online course for your classroom discussions and exam preparation.
- An icon system directs you to the online curriculum to take full advantage of the images imbedded within the Networking Academy online course interface and reminds you to perform the labs, Class activities, Interactive activities, Packet Tracer activities, watch videos, and take the chapter quizzes and exams.

The *Course Booklet* is a basic, economical paper-based resource to help you succeed with the Cisco Networking Academy online course.

Companion Guide

Looking for more than the online curriculum? The Companion Guide is fully aligned to Networking Academy's online course chapters and offers additional book-based pedagogy to reinforce key concepts, enhance student comprehension, and promote retention. Using this full-fledged textbook, students can focus scarce study time, organize review for quizzes and exams, and get the day-to-day reference answers they're looking for.

The Companion Guide also offers instructors additional opportunities to assign take-home reading or vocabulary homework, helping students prepare more for in-class lab work and discussions.

Available in print and all major eBook formats (book: 9781587134340; eBook: 9780134760896).

CHAPTER 1

LAN Design

Refer to **Online Course** for Illustration

1.0 Introduction to LAN Design

There is a tendency to discount the network as just simple plumbing, to think that all you have to consider is the size and the length of the pipes or the speeds and feeds of the links, and to dismiss the rest as unimportant. Just as the plumbing in a large stadium or high rise has to be designed for scale, purpose, redundancy, protection from tampering or denial of operation, and the capacity to handle peak loads, the network requires similar consideration. As users depend on the network to access the majority of the information they need to do their jobs and to transport their voice or video with reliability, the network must be able to provide resilient, intelligent transport.

As a business grows, so does 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.

The campus local area network (LAN) is the network that supports devices people use within a location to connect to information. The campus LAN can be a single switch at a small remote site up to a large multi-building infrastructure, supporting classrooms, office space, and similar places where people use their devices. The campus design incorporates both wired and wireless connectivity for a complete network access solution.

This chapter discusses strategies that can be used to systematically design a highly functional network, such as the hierarchical network design model 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.

Refer to **Online Course** for Illustration

1.0.1.2 Class Activity - 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.

1.1 Campus Wired LAN Designs

1.1.1 Cisco Validated Designs

Refer to **Video** in online course

1.1.1.1 The Need to Scale the Network

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.

Click the Play button in the figure to view an animation of a small network expanding into a larger network.

A 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

The LAN is the networking infrastructure that provides access to network communication services and resources for end users and devices spread over a single floor or building. You create a campus network by interconnecting a group of LANs that are spread over a small geographic area. Campus network designs include small networks that use a single LAN switch, up to very large networks with thousands of connections.

Refer to **Interactive Graphic** in online course

1.1.1.2 Hierarchical Design Model

The campus wired LAN uses a hierarchical design model to break the design up into modular groups or layers. Breaking the design up into layers allows each layer to implement specific functions, which simplifies the network design and therefore the deployment and management of the network.

The campus wired LAN enables communications between devices in a building or group of building, as well as interconnection to the WAN and internet edge at the network core.

A hierarchical LAN design includes the following three layers, as shown in Figure 1:

- Access layer
- Distribution layer
- Core layer

Each layer is designed to meet specific functions.

The access layer provides endpoints and users direct access to the network. The distribution layer aggregates access layers and provides connectivity to services. Finally, the core layer provides connectivity between distribution layers for large LAN environments. 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 may 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 2.

In flat or meshed network architectures, changes tend to affect a large number of systems. Hierarchical design helps constrain operational changes to a subset of the network, which makes it easy to manage as well as improve resiliency. Modular structuring of the network into small, easy-to-understand elements also facilitates resiliency via improved fault isolation.

1.1.2 Expanding the Network

1.1.2.1 Design for Scalability

Refer to **Online Course** for Illustration

To support a large, medium or small 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, creating 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.

As shown in the figure, more advanced network design requirements 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.
- Using a scalable routing protocol and implementing features within that routing protocol to isolate routing updates and minimize the size of the routing table.
- Implementing wireless connectivity to allow for mobility and expansion.

Refer to **Online Course** for Illustration

1.1.2.2 Planning for Redundancy

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

STP eliminates Layer 2 loops when redundant links are used between switches. 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 the chapter titled “STP”.

Refer to **Online Course** for Illustration

1.1.2.3 Failure Domains

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 minimize 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.

In the figure, click each highlighted network device to view the associated failure domain.

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.

Refer to **Online Course** for Illustration

1.1.2.4 Increasing Bandwidth

Implementing EtherChannel

In hierarchical network design, some links between access and distribution switches may 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 the figure.

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 the chapter titled “Etherchannel and HSRP”.

Refer to **Online Course** for Illustration

1.1.2.5 Expanding the Access Layer

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 the figure.

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.

Refer to **Interactive Graphic** in online course

1.1.2.6 Fine-tuning Routing Protocols

Managing the Routed Network

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

Link-state routing protocols such as Open Shortest Path First (OSPF), as shown in Figure 1, works well for larger hierarchical networks where fast convergence is important. 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. Single Area OSPF configuration and concepts will be covered in Chapter 8.

Additionally, OSPF supports a two-layer hierarchical design, referred to as multiarea OSPF, as shown in Figure 2. All multiarea OSPF networks must have an Area 0, also called the backbone area. Non-backbone areas must be directly connected to area 0. Chapter 9 titled “Multiarea OSPF” introduces the benefits, operation, and configuration of Multiarea OSPF. Chapter 10, “OSPF Tuning and Troubleshooting”, will cover the more advanced features of 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, as shown in Figure 3. EIGRP contains many features that are not found in any other routing protocols. It is an excellent choice for large, multi-protocol networks that employ primarily Cisco devices.

Chapter 6 titled “EIGRP” introduces the operation and configuration of the EIGRP routing protocol, while chapter 7 titled “EIGRP Tuning and Troubleshooting” covers some of the more advanced configuration options of EIGRP.

Refer to **Interactive Graphic** in online course

1.1.2.7 Activity - Identify Scalability Terminology

1.2 Selecting Network Devices

1.2.1 Switch Hardware

Refer to **Interactive Graphic** in online course

1.2.1.1 Switch Platforms

When designing a network, it is important to select the proper hardware to meet current network requirements, as well as 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:

- **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, 3650, 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 multi-tenant services by adding virtualization intelligence technology to the data center network.

When selecting switches, network administrators must determine the switch form factors. This includes fixed configuration (Figure 2), modular configuration (Figure 3), stackable (Figure 4), or non-stackable. The thickness 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 2 are all one rack units (1U).

In addition to these considerations, Figure 5 highlights other common business considerations when selecting switch equipment.

Refer to **Online Course** for Illustration

1.2.1.2 Port Density

The port density of a switch refers to the number of ports available on a single switch. The figure shows the port density of three different switches.

Fixed configuration switches support a variety of port density configurations. The Cisco Catalyst 3850 24 port and 48 port switches are shown on the left in the figure. The 48 port switch has an option for four additional ports for small form-factor pluggable (SFP) devices.

Modular switches can support very high-port densities through the addition of multiple switch port line cards. The modular Catalyst 6500 switch shown on the right in the figure can support in excess of 1,000 switch ports.

Large 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 may 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.

Refer to **Online Course** for Illustration

1.2.1.3 Forwarding Rates

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 the figure. 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.

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.

Refer to **Interactive Graphic** in online course

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. Click the highlighted icons in Figure 1 to view PoE ports on each device.

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 Cisco Catalyst 2960-C and 3560-C Series compact switches support 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. Click the highlighted icon in Figure 2 to view a Cisco Catalyst 2960-C.

Refer to **Online Course** for Illustration

1.2.1.5 Multilayer Switching

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 (ASICs). 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.

As shown in the figure, the Catalyst 2960 switches illustrate the migration to a pure Layer 3 environment. With IOS versions prior to 15.x, these switches supported only one active switched virtual interface (SVI). With IOS 15.x, these switches now support multiple active SVIs. This means that the switch can be remotely accessed via multiple IP addresses on distinct networks.

Refer to **Interactive Graphic** in online course

1.2.1.6 Activity - Selecting Switch Hardware

Refer to **Packet Tracer Activity** for this chapter

1.2.1.7 Packet Tracer - 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.

1.2.2 Router Hardware

Refer to **Online Course** for Illustration

1.2.2.1 Router Requirements

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 connecting homes and businesses to the Internet, 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 re-encapsulate 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 or path goes down. 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. The ability to route efficiently and recover from network link failures is critical to delivering packets to their destination.

Routers also serve other beneficial functions:

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

Click each highlighted area in the figure for more information on the functions of routers.

Refer to **Online Course** for Illustration

1.2.2.2 Cisco Routers

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

- **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.

Refer to **Online Course** for Illustration

1.2.2.3 Router Hardware

Routers also come in many form factors, as shown in the figure. 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.

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 1941 router comes with two Gigabit 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.

Click here to see a comprehensive list of Cisco routers.

Refer to **Interactive Graphic** in online course

1.2.2.4 Activity – Identify the Router Category

1.2.3 Managing Devices

Refer to **Online Course** for Illustration

1.2.3.1 Managing IOS Files and Licensing

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 the figure.

Refer to **Online Course** for Illustration

1.2.3.2 In-Band versus Out-of-Band Management

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 the figure.

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, HTTP, or HTTPS to access a Cisco device

Note Telnet and HTTP are less secure and are not recommended.

Refer to **Interactive Graphic** in online course

1.2.3.3 Basic Router CLI Commands

A basic router configuration includes the hostname for identification, passwords for security, assignment of IP addresses to interfaces for connectivity, and basic routing. Figure 1 shows the commands entered to enable a router with RIPv2. Verify and save configuration changes using the **copy running-config startup-config** command. Figure 2 shows the results of the configuration commands that were entered in Figure 1. To clear the router configuration, use the **erase startup-config** command and then the **reload** command.

Use the Syntax Checker in Figure 3 to practice your basic router configuration skills.

Refer to **Interactive Graphic** in online course

1.2.3.4 Basic Router Show Commands

Here are some of the most commonly used IOS commands to display and verify the operational status of the router and related IPv4 network functionality. Similar commands are available for IPv6 by replacing **ip** with **ipv6**. These commands are divided into several categories.

Routing Related:

- **show ip protocols -** Displays information about the routing protocols configured. If RIP is configured, this includes the version of RIP, networks the router is advertising, whether or not automatic summarization is in effect, the neighbors the router is receiving updates from, and the default administrative distance, which is 120 for RIP. (Figure 1)
- **show ip route -** Displays routing table information, including: routing codes, known networks, administrative distance and metrics, how routes were learned, next hop, static routes, and default routes. (Figure 2)

Interface Related:

- **show interfaces -** 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. (Figure 3)
- **show ip interfaces -** Displays interface information, including: protocol status, the IPv4 address, if 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, information about that interface only will be displayed. (Figure 4)
- **show ip interface brief -** Displays all interfaces with IPv4 addressing information and interface and line protocols status. (Figure 5)
- **show protocols -** Displays information about the routed protocol that is enabled, and the protocol status of interfaces. (Figure 6)

Other connectivity related commands include the **show cdp neighbors** command (Figure 7). This command displays information on directly connected Cisco devices including Device ID, the local interface the device is connected to, capability (R = router, S = switch), the platform, and Port ID of the remote device. The **details** option includes IP addressing information and the IOS version.

Use the Syntax Checker in Figure 8 to verify router configurations using these **show** commands.

Refer to **Interactive Graphic** in online course

1.2.3.5 Basic Switch CLI commands

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

Figure 2 shows the results of the configuration commands that were entered in Figure 1. 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 may also be necessary to erase any VLAN information using the command **delete flash:vlan.dat.** When switch configurations are in place, view the configurations using the **show running-config** command.

Refer to **Interactive Graphic** in online course

1.2.3.6 Basic Switch Show Commands

Switches make use of common IOS commands for configuration, to check for connectivity and to display current switch status. Click buttons 1 to 4 for sample outputs of the commands and the important pieces of information that an administrator can gather from it.

Interface / Port Related:

- **show port-security -** Displays any ports with security activated. To examine a specific interface, include the interface ID. Information included in the output: the maximum addresses allowed, current count, security violation count, and action to be taken. (Figure 1)
- **show port-security address -** Displays all secure MAC addresses configured on all switch interfaces. (Figure 2)
- **show interfaces -** Displays one or all interfaces with line (protocol) status, bandwidth, delay, reliability, encapsulation, duplex, and I/O statistics. (Figure 3)
- **show mac-address-table -** 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. (Figure 4)

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 applies to switch configuration.

1.3 Summary

Refer to **Online Course** for Illustration

1.3.1.1 Class Activity - 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

Refer to **Interactive Graphic** in online course

1.3.1.2 Basic Switch Configuration

Refer to **Packet Tracer Activity** for this chapter

1.3.1.3 Packet Tracer - Skills Integration Challenge

Background/Scenario

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.

Refer to **Online Course** for Illustration

1.3.1.4 Summary

The hierarchical network design model divides network functionality into the access layer, the distribution layer, and the core layer. The campus wired LAN enables communications between devices in a building or group of buildings, as well as interconnection to the WAN and internet edge at the network core.

A well-designed network controls traffic and limits the size of failure domains. Routers and 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 may 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.

It is important to deploy the appropriate type of routers and switches for a given set of requirements, features and specifications, and expected traffic flow.

Go to the online course to take the quiz and exam.

Chapter 1 Quiz

This quiz is designed to provide an additional opportunity to practice the skills and knowledge presented in the chapter and to prepare for the chapter exam. You will be allowed multiple attempts and the grade does not appear in the gradebook.

Chapter 1 Exam

The chapter exam assesses your knowledge of the chapter content.

Your Chapter Notes

Index

D

E

F

G-H

I

J-K-L

M

N

O

P

Q-R

S

T

U

V

W-X-Y-Z