Scaling Networks v6

Companion Guide

Cisco | Networking Academy®
Mind Wide Open™

Scaling Networks v6

Companion Guide

Cisco Networking Academy

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Scaling Networks v6 Companion Guide

Cisco Networking Academy

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

Printed in the United States of America

First Printing August 2017

Library of Congress Control Number: 2017946462

ISBN-13: 978-1-58713-434-0

ISBN-10: 1-58713-434-9

Warning and Disclaimer

This book is designed to provide information about the 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.

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

Editor-in-Chief
Mark Taub

Alliances Manager, Cisco Press
Ron Fligge

Product Line Manager
Brett Bartow

Executive Editor
Mary Beth Ray

Managing Editor
Sandra Schroeder

Development Editor
Ellie C. Bru

Senior Project Editor
Tonya Simpson

Copy Editor
Kitty Wilson

Technical Editor
Rick McDonald

Editorial Assistant
Vanessa Evans

Cover Designer
Ockomon House

Composition
codeMantra

Indexer
Erika Millen

Proofreader
Abigail Manheim

Trademark Acknowledgments

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

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.

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.**

About the Contributing Authors

Bob Vachon is a professor at Cambrian College in Sudbury, Ontario, Canada, where he teaches network infrastructure courses. He has worked and taught in the computer networking and information technology field since 1984. Since 2002, he has collaborated on various CCNA, CCNA Security, CCNP, Cybersecurity, and IoT projects for the Cisco Networking Academy as team lead, lead author, and subject matter expert. He enjoys playing guitar and being outdoors.

Allan Johnson entered the academic world in 1999, after 10 years as a business owner/operator, to dedicate his efforts to his passion for teaching. He holds both an MBA and an MEd in training and development. He taught CCNA courses at the high school level for seven years and has taught both CCNA and CCNP courses at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team, providing services to Networking Academy instructors worldwide and creating training materials. He now works full time for Cisco Networking Academy as curriculum lead.

Contents at a Glance

Contents

Reader Services

Register your copy at www.ciscopress.com/title/9781587134340 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 9781587134340 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.

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.

Introduction

Scaling Networks v6 Companion Guide is the official supplemental textbook for the Cisco Network Academy CCNA Routing & Switching Scaling Networks course. Cisco Networking Academy is a comprehensive program that delivers information technology skills to students around the world. The curriculum emphasizes real-world practical application, while providing opportunities for you to gain the skills and hands-on experience needed to design, install, operate, and maintain networks in small to medium-sized businesses, as well as enterprise and service provider environments.

This book provides a ready reference that explains the same networking concepts, technologies, protocols, and devices as the online curriculum. This book emphasizes key topics, terms, and activities and provides some alternate explanations and examples than are available in the course. You can use the online curriculum as directed by your instructor and then use this book's study tools to help solidify your understanding of all the topics.

Who Should Read This Book

The book, as well as the course, is designed as an introduction to data network technology for those pursuing careers as network professionals as well as those who need only an introduction to network technology for professional growth. Topics are presented concisely, starting with the most fundamental concepts and progressing to a comprehensive understanding of network communication. The content of this text provides the foundation for additional Cisco Networking Academy courses and preparation for the CCNA Routing and Switching certification.

Book Features

The educational features of this book focus on supporting topic coverage, readability, and practice of the course material to facilitate your full understanding of the course material.

Topic Coverage

The following features give you a thorough overview of the topics covered in each chapter so that you can make constructive use of your study time:

- **Objectives:** Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives stated in the corresponding chapters of the online curriculum; however, the question format in this book encourages you to think about finding the answers as you read the chapter.

- **Notes:** These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.
- **Chapter summaries:** At the end of each chapter is a summary of the chapter's key concepts. It provides a synopsis of the chapter and serves as a study aid.
- **Practice:** At the end of chapter is a full list of the labs, class activities, and Packet Tracer activities to refer to for study time.

Readability

The following features have been updated to assist your understanding of the networking vocabulary:

- **Key terms:** Each chapter begins with a list of key terms, along with a page-number reference from within the chapter. The terms are listed in the order in which they are explained in the chapter. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The Glossary defines all the key terms.
- **Glossary:** This book contains an all-new Glossary with more than 250 terms.

Practice

Practice makes perfect. This new Companion Guide offers you ample opportunities to put what you learn into practice. You will find the following features valuable and effective in reinforcing the instruction that you receive:

- **"Check Your Understanding" questions and answer key:** Updated review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. Appendix A, "Answers to the 'Check Your Understanding' Questions," provides an answer key to all the questions and includes an explanation of each answer.

Packet Tracer
□ Activity

Video

- **Labs and activities:** Throughout each chapter, you will be directed back to the online course to take advantage of the activities created to reinforce concepts. In addition, at the end of each chapter, there is a practice section that collects a list of all the labs and activities to provide practice with the topics introduced in the chapter. The labs, class activities, and Packet Tracer instructions are available in the companion *Scaling Networks v6 Labs & Study Guide* (ISBN 9781587134333). The Packet Tracer PKA files are found in the online course.

- **Page references to online course:** After headings, you will see, for example, (1.1.2.3). This number refers to the page number in the online course so that you can easily jump to that spot online to view a video, practice an activity, perform a lab, or review a topic.

Lab Study Guide

The supplementary book *Scaling Networks v6 Labs & Study Guide*, by Allan Johnson (ISBN 9781587134333), includes a Study Guide section and a Lab section for each chapter. The Study Guide section offers exercises that help you learn the concepts, configurations, and troubleshooting skill crucial to your success as a CCNA exam candidate. Some chapters include unique Packet Tracer activities available for download from the book's companion website. The Labs and Activities section contains all the labs, class activities, and Packet Tracer instructions from the course.

Packet Tracer
□ **Activity**

About Packet Tracer Software and Activities

Interspersed throughout the chapters you'll find many activities to work with the Cisco Packet Tracer tool. Packet Tracer allows you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available in the course. Packet Tracer software is available only through the Cisco Networking Academy website. Ask your instructor for access to Packet Tracer.

How This Book Is Organized

This book corresponds closely to the Cisco Academy Scaling Networks course and is divided into 10 chapters, one appendix, and a Glossary of key terms:

- **Chapter 1, "LAN Design":** 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.
- **Chapter 2, "Scaling VLANs":** This chapter examines the implementation of inter-VLAN routing using a Layer 3 switch. It also describes issues encountered when implementing VTP, DTP and inter-VLAN routing.

- **Chapter 3, "STP":** This chapter focuses on the protocols used to manage Layer 2 redundancy. It also covers some of the potential redundancy problems and their symptoms.
- **Chapter 4, "EtherChannel and HSRP":** This chapter describes EtherChannel and the methods used to create an EtherChannel. It also focuses on the operations and configuration of Hot Standby Router Protocol (HSRP), a first-hop redundancy protocol. Finally, the chapter examines a few potential redundancy problems and their symptoms.
- **Chapter 5, "Dynamic Routing":** This chapter introduces dynamic routing protocols. It explores the benefits of using dynamic routing protocols, how different routing protocols are classified, and the metrics routing protocols use to determine the best path for network traffic. In addition, the characteristics of dynamic routing protocols and the differences between the various routing protocols are examined.
- **Chapter 6, "EIGRP":** This chapter introduces EIGRP and provides basic configuration commands to enable it on a Cisco IOS router. It also explores the operation of the routing protocol and provides more detail on how EIGRP determines the best path.
- **Chapter 7, "EIGRP Tuning and Troubleshooting":** This chapter describes EIGRP tuning features, the configuration mode commands to implement these features for both IPv4 and IPv6, and the components and commands used to troubleshoot OSPFv2 and OSPFv3.
- **Chapter 8, "Single-Area OSPF":** This chapter covers basic single-area OSPF implementations and configurations.
- **Chapter 9, "Multiarea OSPF":** This chapter discusses basic multiarea OSPF implementations and configurations.
- **Chapter 10, "OSPF Tuning and Troubleshooting":** This chapter describes OSPF tuning features, the configuration mode commands to implement these features for both IPv4 and IPv6, and the components and commands used to troubleshoot OSPFv2 and OSPFv3.
- **Appendix A, "Answers to the Review Questions":** This appendix lists the answers to the "Check Your Understanding" review questions that are included at the end of each chapter.
- **Glossary:** The Glossary provides you with definitions for all the key terms identified in each chapter.

This page intentionally left blank

CHAPTER 1

LAN Design

Objectives

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

- What are the appropriate hierarchical network designs for small businesses?
- What are the considerations for designing a scalable network?
- What switch hardware features are appropriate to support network requirements in small to medium-sized business networks?
- 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.

mission-critical services	*Page 3*
enterprise network	*Page 3*
network operations center (NOC)	*Page 5*
hierarchical design model	*Page 6*
access layer	*Page 7*
distribution layer	*Page 7*
core layer	*Page 7*
collapsed core design	*Page 7*
multilayer switch	*Page 9*
Redundant links	*Page 9*
link aggregation	*Page 9*
redundancy	*Page 10*
Spanning Tree Protocol (STP)	*Page 10*
failure domain	*Page 11*
wireless access point (AP)	*Page 12*
building switch block	*Page 13*
departmental switch block	*Page 13*
EtherChannel	*Page 13*
port channel interface	*Page 14*
load balancing	*Page 14*
Open Shortest Path First (OSPF)	*Page 15*
Enhanced Interior Gateway Routing Protocol (EIGRP)	*Page 15*
link-state routing protocol	*Page 15*
single-area OSPF	*Page 15*
multiarea OSPF	*Page 15*
distance vector routing protocol	*Page 16*
form factor	*Page 17*

Power over Ethernet (PoE) *Page 17*

campus LAN switch *Page 17*

cloud-managed switch *Page 18*

data center switch *Page 18*

service provider switch *Page 18*

virtual networking switch *Page 18*

fixed configuration *Page 19*

modular configuration *Page 19*

stackable configuration *Page 19*

rack unit *Page 20*

supervisor engine *Page 21*

port density *Page 21*

small form-factor pluggable (SFP) *Page 22*

forwarding rates *Page 22*

wire speed *Page 22*

application-specific integrated circuits (ASIC) *Page 24*

branch router *Page 27*

network edge router *Page 28*

service provider router *Page 28*

Cisco Internetwork Operating System (IOS) *Page 29*

IOS image *Page 30*

out-of-band management *Page 30*

in-band management *Page 30*

PuTTY *Page 31*

TeraTerm *Page 31*

Introduction (1.0.1.1)

There is a tendency to discount a 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, a network requires similar consideration. As users depend on a 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.

Class Activity 1.0.1.2: Network by Design

Refer to *Scaling Networks v6 Labs & Study Guide* and the online course to complete this activity.

Your employer is opening a new branch office. You have been reassigned to the site as the network administrator, and 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.

Campus Wired LAN Designs (1.1)

Enterprise networks come in all sizes. There are small networks consisting of a few hosts, medium-sized networks consisting of a few hundred hosts, and large networks consisting of thousands of hosts. Besides the number of hosts these networks must support, consideration must be given to the applications and services that must be supported to meet the organizational goals.

Fortunately, proven methods are available to design all types of networks. The Cisco Enterprise Architecture is an example of a proven campus network design.

In this section, you will learn why it is important to design a scalable hierarchical network.

Cisco Validated Designs (1.1.1)

Networks must be scalable, which means they must be able to accommodate an increase or a decrease in size. The focus of this topic is to discover how the hierarchical design model is used to help accomplish this task.

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.

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. A campus network is created 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. For example, in Figure 1-1, the company is located in a single location with one connection to the Internet.

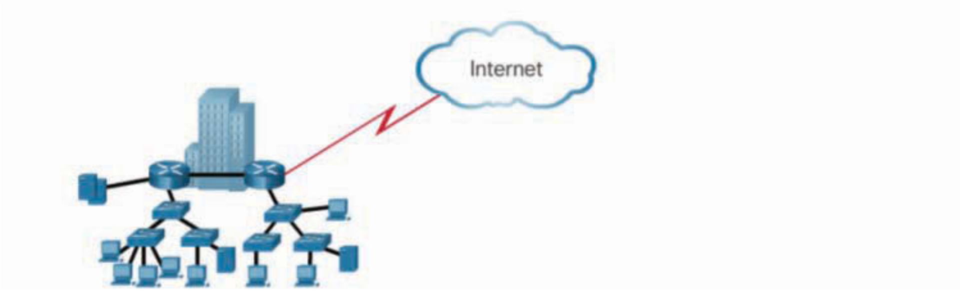


Figure 1-1 A Small, Single-Location Company

In Figure 1-2, the company grows to multiple locations in the same city.

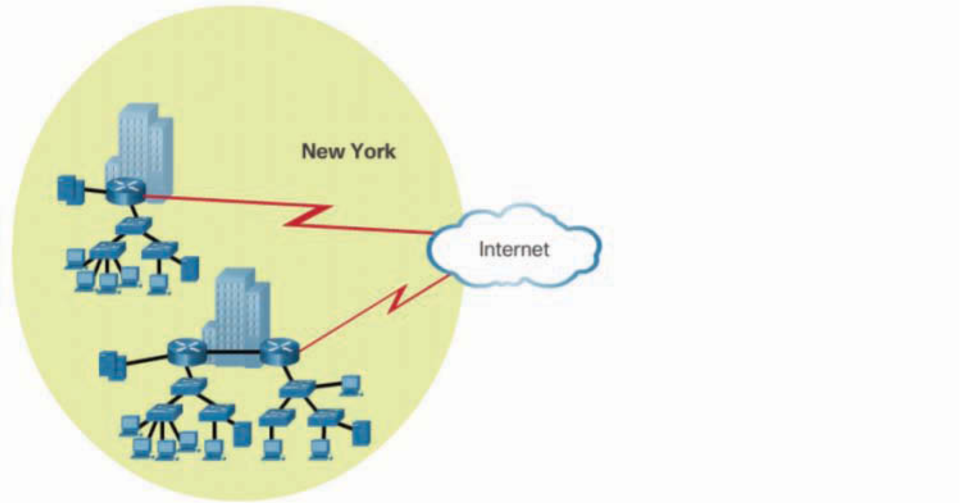


Figure 1-2 The Company Grows to Multiple Locations in the Same City

In Figure 1-3, the company continues to grow and expands to more cities. It also hires and connects teleworkers.

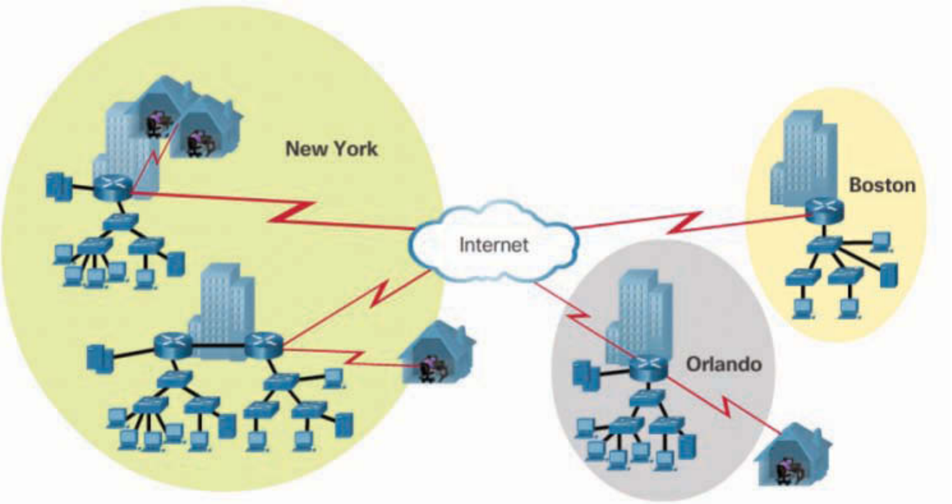


Figure 1-3 Enterprise Grows to Multiple Cities and Adds Teleworkers

In Figure 1-4, the company expands to other countries and centralizes management in a *network operations center (NOC)*.

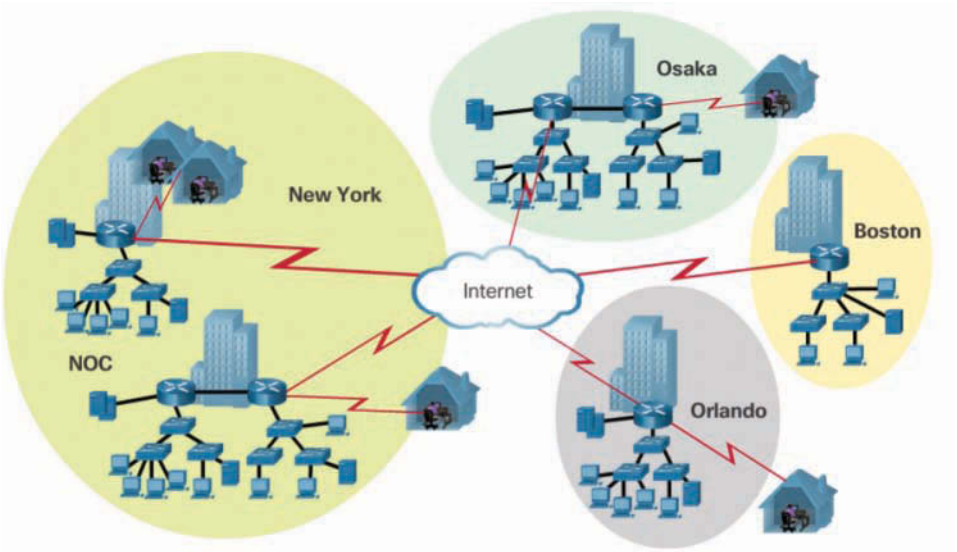


Figure 1-4 Enterprise Becomes Global and Centralizes Network Operations

In addition to supporting physical growth, a network must also support the exchange of all types of network traffic, including data files, email, IP telephony, and video applications for multiple business units.

Specifically, all enterprise networks must:

- Support mission-critical services and applications
- Support converged network traffic
- Support diverse business needs
- Provide centralized administrative control

To help campus LANs meet these requirements, a ***hierarchical design model*** is used.

Hierarchical Design Model (1.1.1.2)

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.

Early networks used a flat or meshed network design, in which large numbers of hosts were connected in the same network. Changes affected many hosts in this type of network architecture.

Campus wired LANs now use a hierarchical design model that divides network design into modular groups or layers. Dividing (or *breaking*) the network design into layers enables each layer to implement specific functions. This simplifies the network design and the deployment and management of the network.

A hierarchical LAN design consists of the following three layers, as shown in Figure 1-5:

- Access layer
- Distribution layer
- Core layer

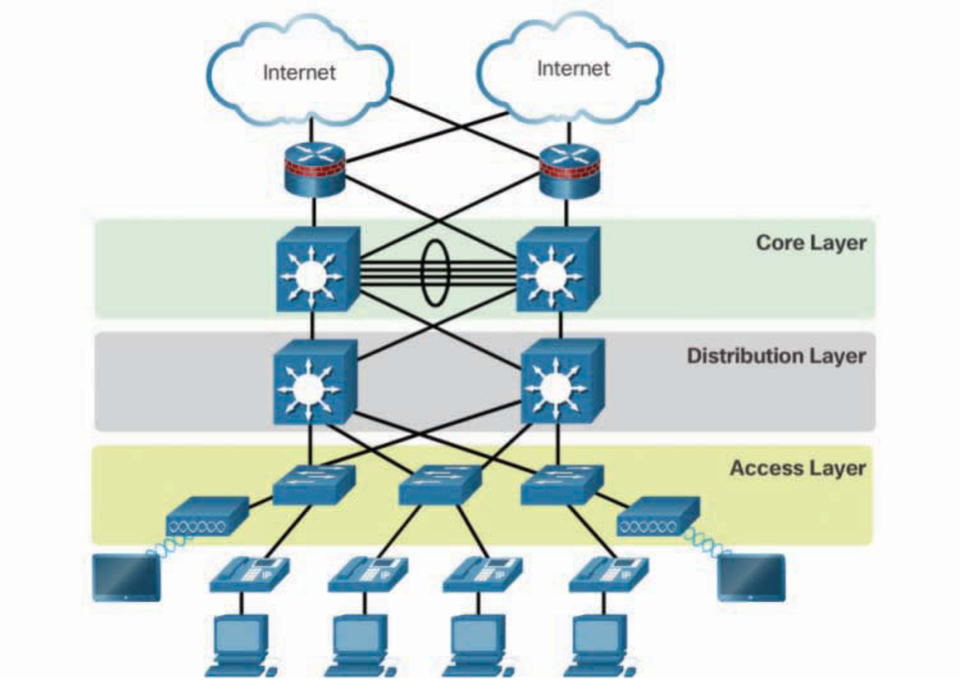


Figure 1-5 Hierarchical Design Model

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.

Medium-sized to large enterprise networks commonly implement the three-layer hierarchical design model. However, some smaller enterprise networks may implement a two-tier hierarchical design, referred to as a *collapsed core 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 1-6.

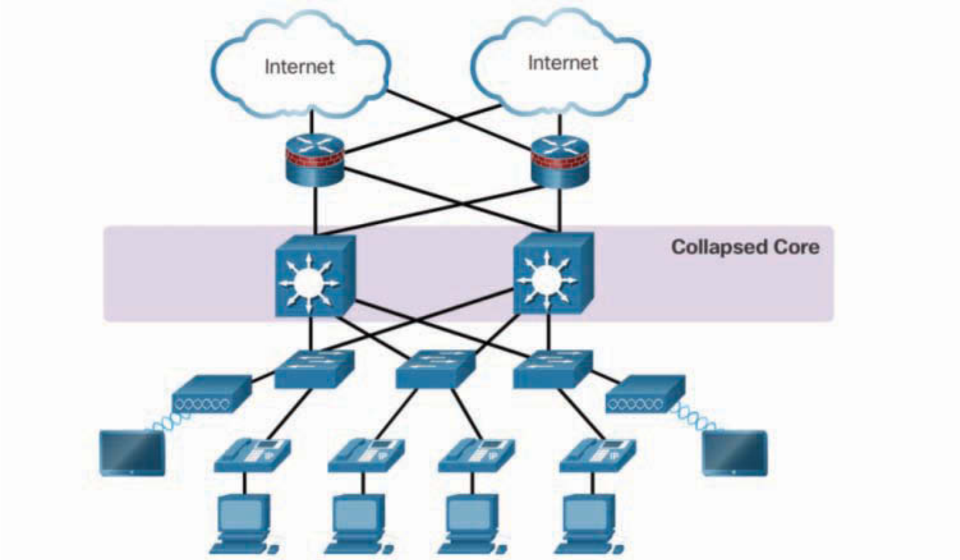


Figure 1-6 Collapsed Core

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 and improves resiliency. Modular structuring of the network into small, easy-to-understand elements also facilitates resiliency via improved fault isolation.

Expanding the Network (1.1.2)

Networks must be scalable, which means they must be able to accommodate an increase or a decrease in size. The focus of this topic is to discover how the hierarchical design model is used to help accomplish this task.

Design for Scalability (1.1.2.1)

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, you might 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.
- Use a router or *multilayer switch* 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 Figure 1-7, more advanced network design requirements include:

A. *Redundant links*—Implementing redundant links in the network between critical devices and between access layer and core layer devices.

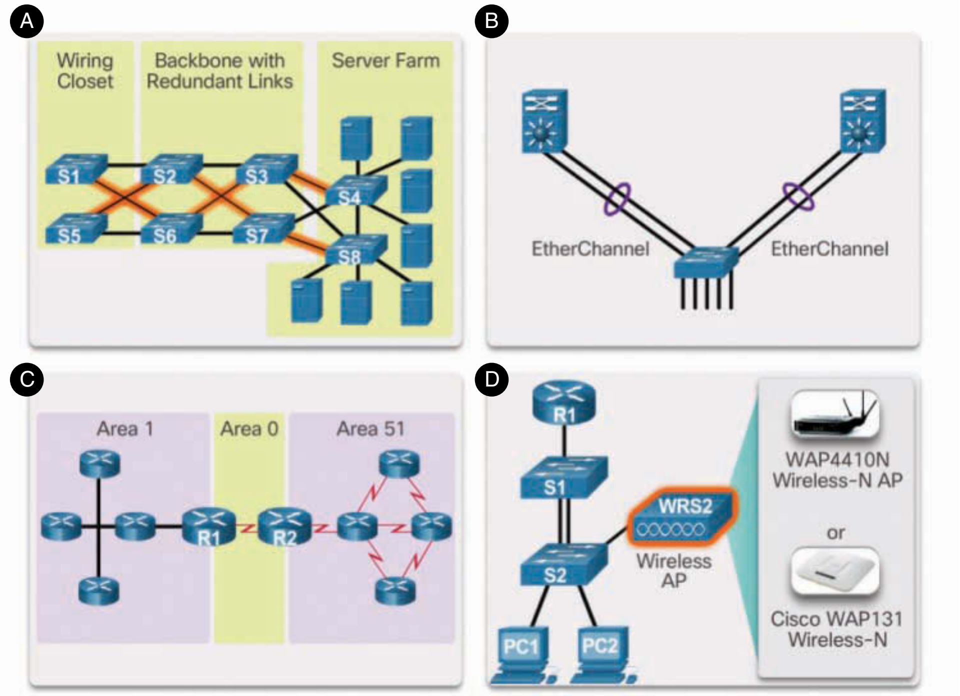


Figure 1-7 Design for Scalability

B. *Link aggregation*—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 the available bandwidth. EtherChannel implementations can be used when budget restrictions prohibit purchasing high-speed interfaces and fiber runs.

C. **Scalable routing protocols**—Using a scalable routing protocol such as multiarea OSPF and implementing features within that routing protocol to isolate routing updates and minimize the size of the routing table.

D. **Wireless mobility**—Implementing wireless connectivity to allow for mobility and expansion.

Planning for Redundancy (1.1.2.2)

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 to install duplicate equipment and provide 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, 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.

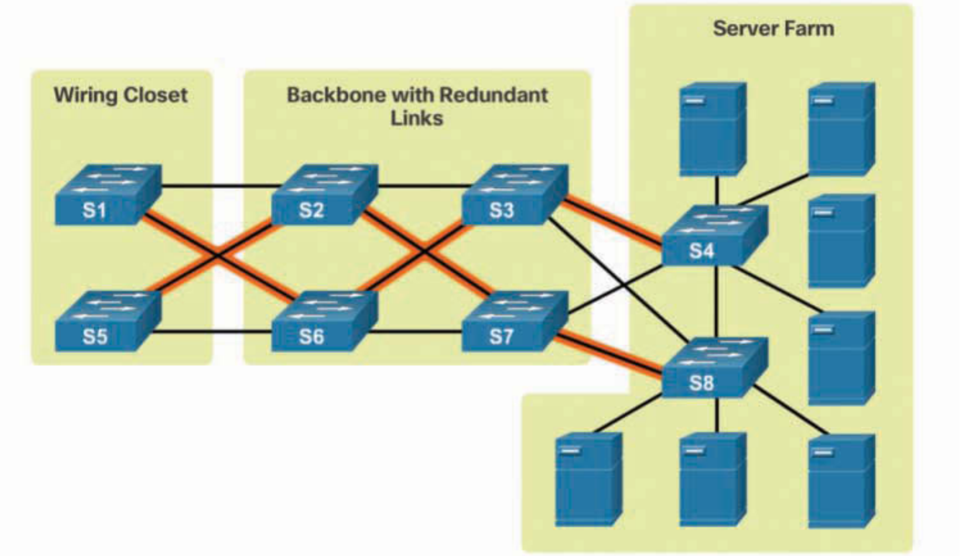


Figure 1-8 LAN Redundancy

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.

Chapter 3, "STP," provides more details about LAN redundancy and the operation of STP.

Failure Domains (1.1.2.3)

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.

Figure 1-9 shows an example of the failure domain for a router.

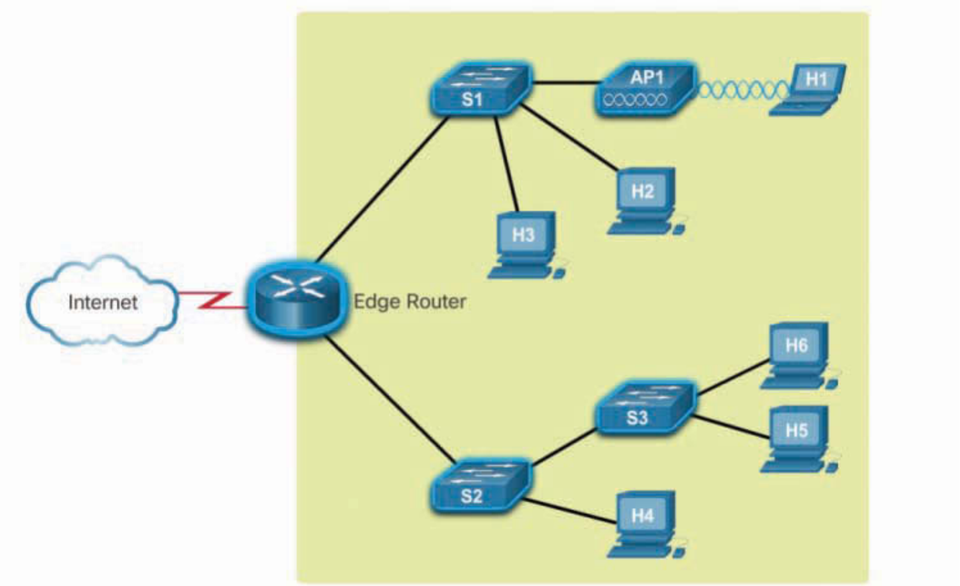


Figure 1-9 Failure Domain—Router

Figure 1-10 shows an example of the failure domain for a switch.

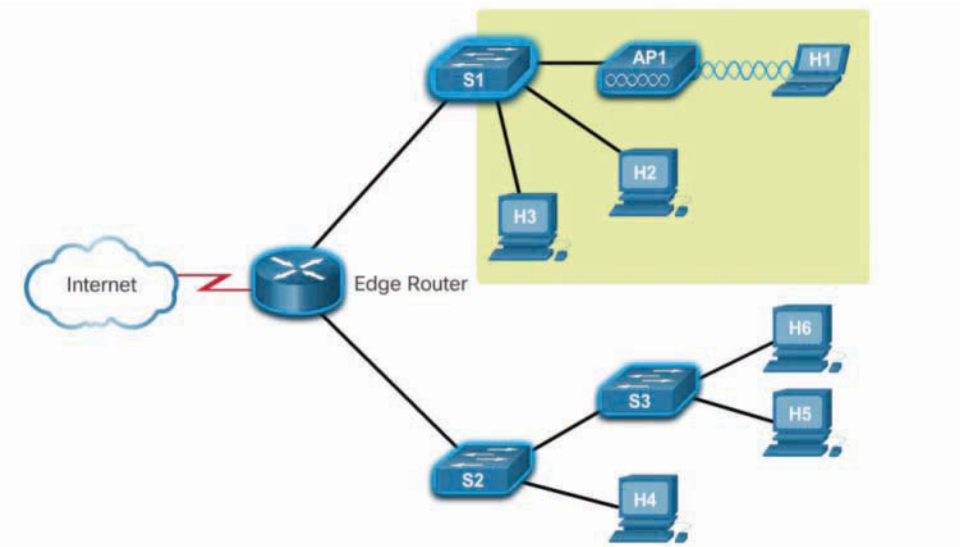


Figure 1-10 Failure Domain—Switch

Figure 1-11 shows an example of the failure domain for a *wireless access point (AP)*.

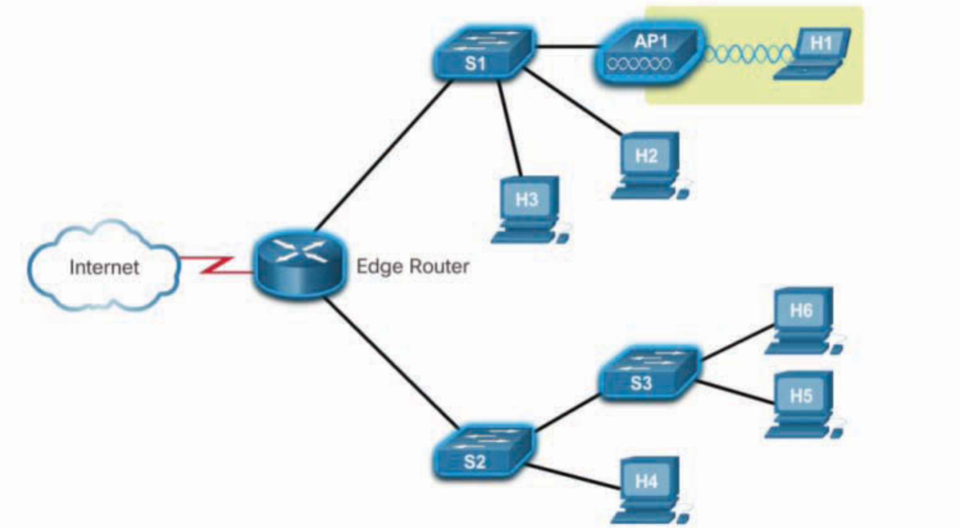


Figure 1-11 Failure Domain—Wireless Access Point

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. Limiting the size of failure domains in the distribution layer confines network errors to a smaller area and thereby affects 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.

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 switch block*** or a ***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.

Increasing Bandwidth (1.1.2.4)

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 by grouping several physical links together. ***EtherChannel*** is a form of link aggregation used in switched networks, as shown in Figure 1-12.

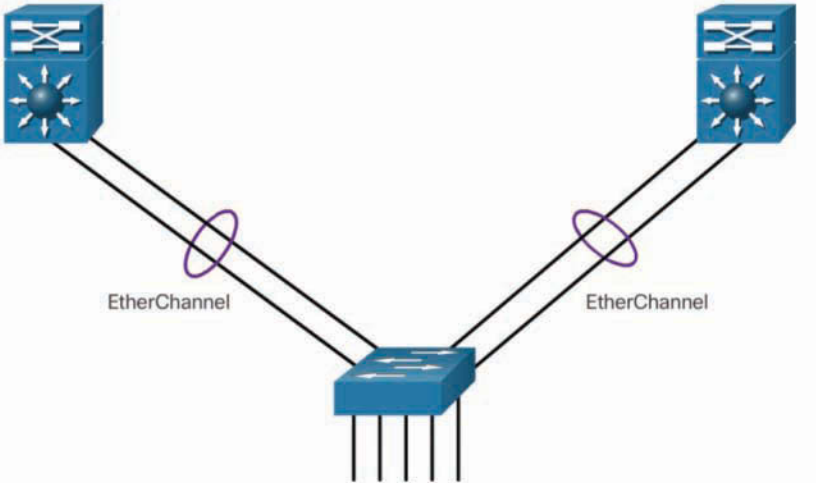


Figure 1-12 Advantages of EtherChannel

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.

On a Cisco Catalyst switch, an EtherChannel is configured as a ***port channel interface***. Most configuration tasks are done on the port channel interface instead of on each individual port to ensure 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 are covered in more detail Chapter 4, "EtherChannel and HSRP."

Expanding the Access Layer (1.1.2.5)

A 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 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 network interface card (NIC) that incorporates a radio transmitter/receiver and the required software driver to make it operational. In addition, a wireless router or a wireless access point (AP) is required for users to connect, as shown in Figure 1-13.

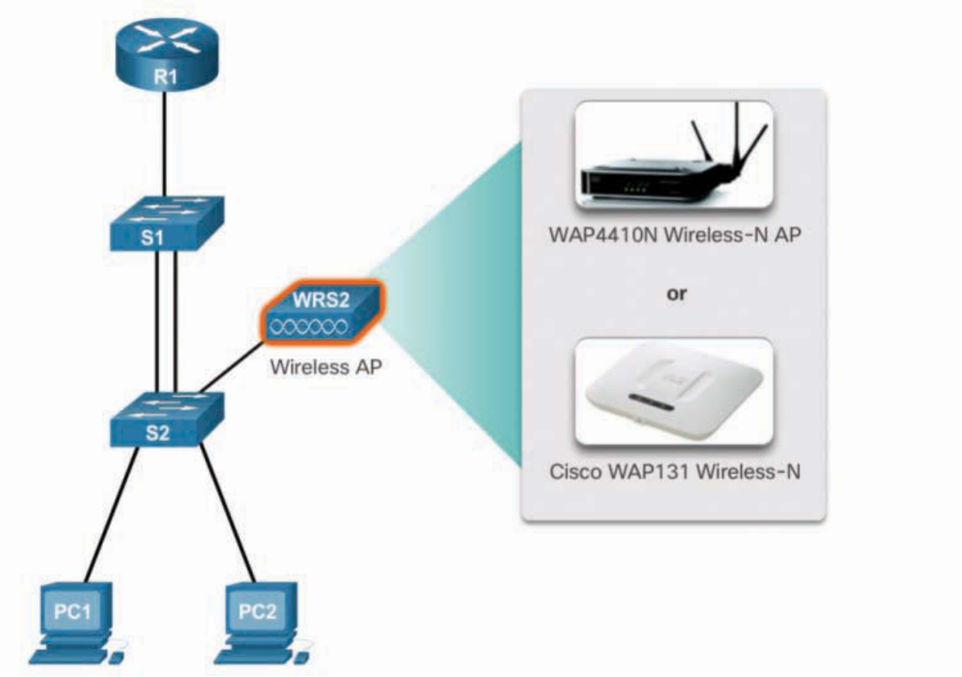


Figure 1-13 Wireless LANs

Implementing a wireless network involves many considerations, such as the types of wireless devices to use, wireless coverage requirements, interference considerations, and security considerations.

Fine-tuning Routing Protocols (1.1.2.6)

Advanced routing protocols, such as *Open Shortest Path First (OSPF)* and *Enhanced Interior Gateway Routing Protocol (EIGRP)*, are used in large networks.

A *link-state routing protocol* such as OSPF, as shown in Figure 1-14, works well for larger hierarchical networks where fast convergence is important.

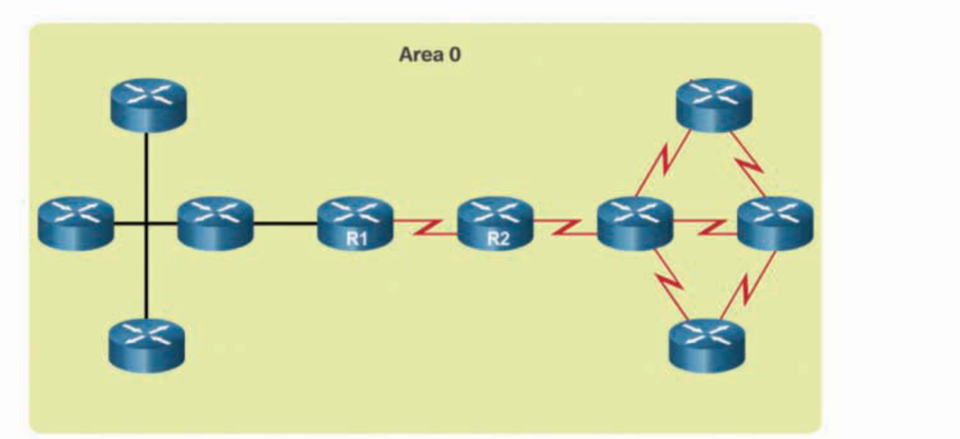


Figure 1-14 Single-Area OSPF

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. *Single-area OSPF* configuration and concepts are covered in Chapter 8, “Single-Area OSPF.”

In addition, OSPF supports a two-layer hierarchical design, referred to as *multiarea OSPF*, as shown in Figure 1-15.

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, “Multiarea OSPF,” introduces the benefits, operation, and configuration of multiarea OSPF. Chapter 10, “OSPF Tuning and Troubleshooting,” covers more advanced features of OSPF.

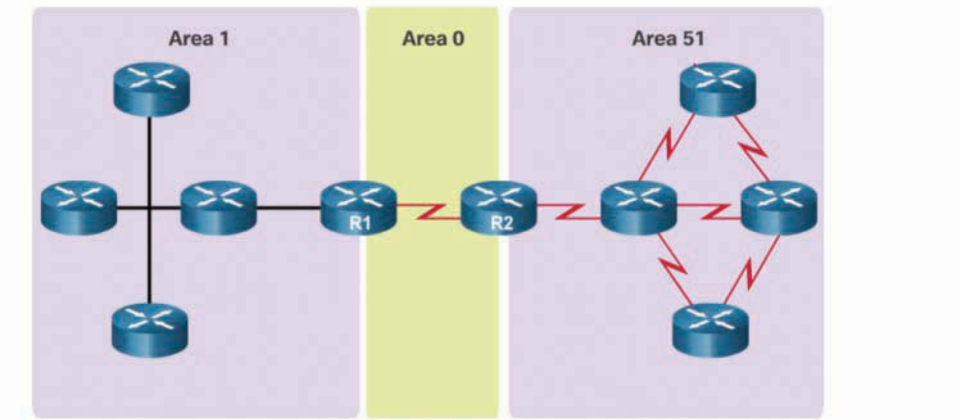
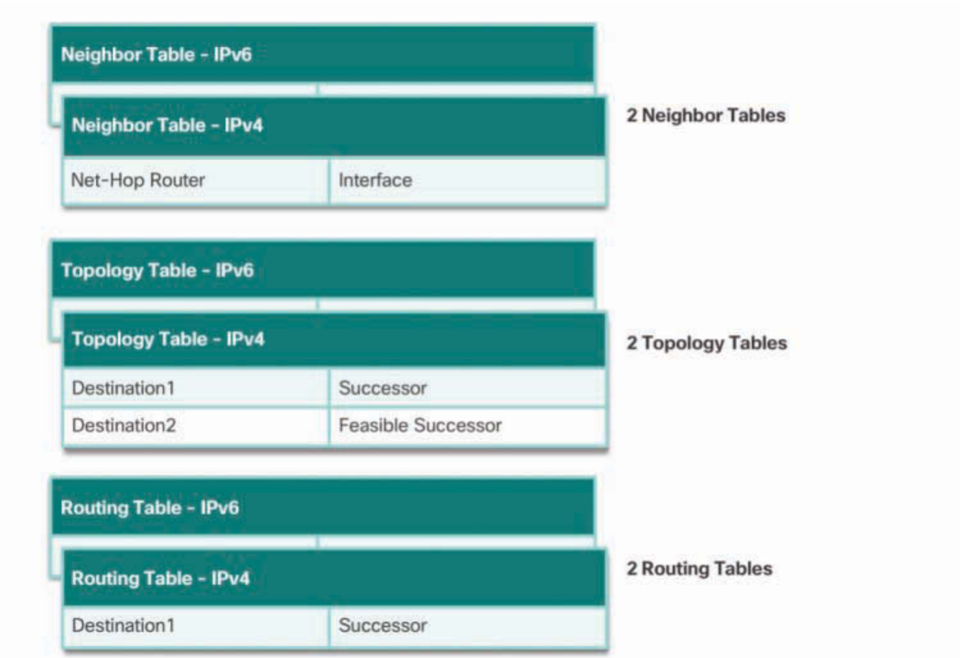


Figure 1-15 Multiarea OSPF

Another popular routing protocol for larger networks is 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 protocol-dependent modules (PDM), which enable support for IPv4 and IPv6 routing tables, as shown in Figure 1-16.


Neighbor Table - IPv6

Neighbor Table - IPv4	
Net-Hop Router	Interface

2 Neighbor Tables

Topology Table - IPv6

Topology Table - IPv4	
Destination1	Successor
Destination2	Feasible Successor

2 Topology Tables

Routing Table - IPv6

Routing Table - IPv4	
Destination1	Successor

2 Routing Tables

Figure 1-16 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 use primarily Cisco devices.

Chapter 6, "EIGRP," introduces the operation and configuration of the EIGRP routing protocol, and Chapter 7, "EIGRP Tuning and Troubleshooting," covers some of the more advanced configuration options of EIGRP.

Interactive Graphic

Activity 1.1.2.7: Identify Scalability Terminology

Refer to the online course to complete this activity.

Selecting Network Devices (1.2)

Switches and routers are core network infrastructure devices. Therefore, selecting them appears to be a fairly simple task. However, many different models of switches and routers are available. Different models provide various numbers of ports, different forwarding rates, and unique feature support.

In this section, you will learn how to select network devices based on feature compatibility and network requirements.

Switch Hardware (1.2.1)

Various types of switch platforms are available. Each platform differs in terms of physical configuration and *form factor*, the number of ports, and the features supported, including *Power over Ethernet (PoE)* and routing protocols.

The focus of this topic is on how to select the appropriate switch hardware features to support network requirements in small to medium-sized business networks.

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 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 1-17:

- *Campus LAN switch*—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.

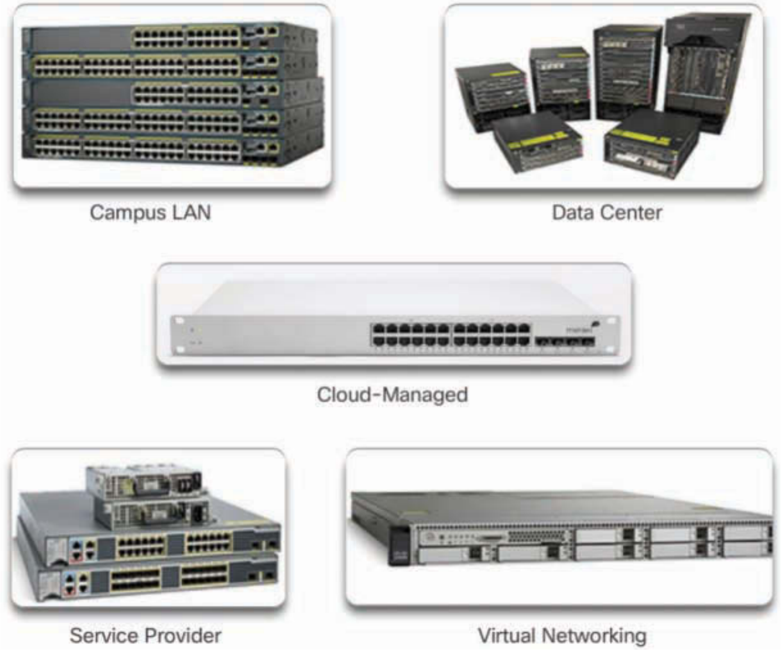
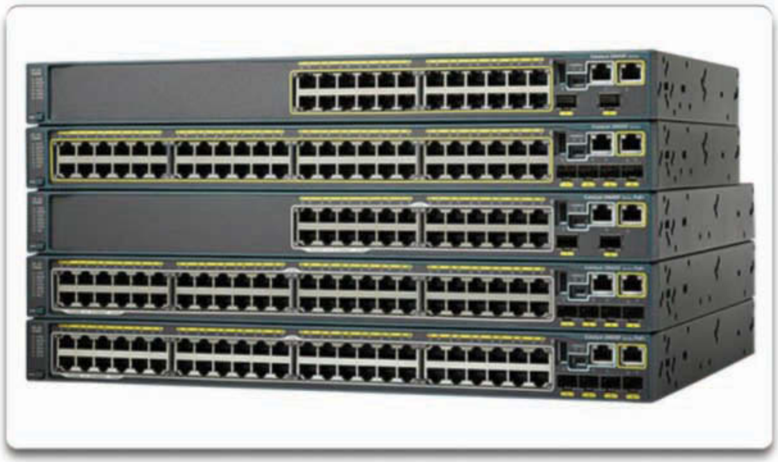


Figure 1-17 Switch Platforms

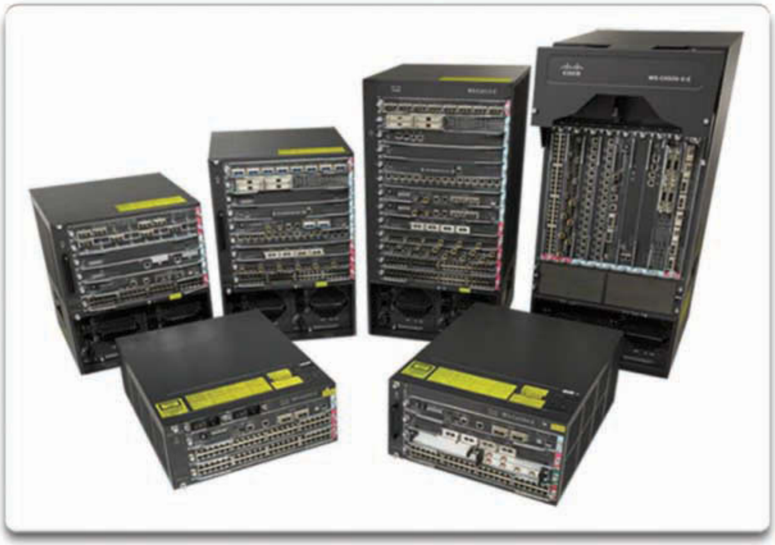
- ***Cloud-managed switch***—The Cisco Meraki cloud-managed access switches enable virtual stacking of switches. They monitor and configure thousands of switch ports over the web, without the intervention of onsite IT staff.
- ***Data center switch***—A data center should be built based on switches that 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 switch***—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 switch***—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.

When selecting switches, network administrators must determine the switch form factors. These include *fixed configuration* (Figure 1-18), *modular configuration* (Figure 1-19), or *stackable configuration* (Figure 1-20).



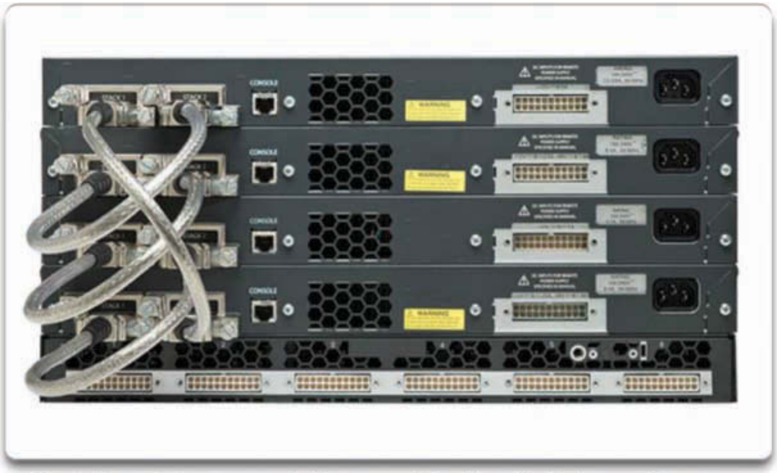
Features and options are limited to those that originally come with the switch.

Figure 1-18 Fixed Configuration Switches



The chassis accepts line cards that contain the ports.

Figure 1-19 Modular Configuration Switches



Stackable switches, connected by a special cable, effectively operate as one large switch.

Figure 1-20 Stackable Configuration Switches

The amount of space that a device occupies in a network rack is also an important consideration. *Rack unit* is a term used to describe the thickness of a rack-mountable network device. Defined in EIA-310, a unit (U) describes a device with a standard height of 4.45 centimeters (1 3/4 inches) and width of 48.26 centimeters (19 inches). For example, the fixed configuration switches shown in Figure 1-18 are all one rack unit (1U).

Besides the device form factor, other device selection considerations must be made. Table 1-1 describes some of these considerations.

Table 1-1 Considerations When Selecting Network Devices

Consideration	Description
Cost	The cost of a switch depends on the number and speed of the interfaces, supported features, and expansion capability.
Port density	The port density describes how many ports are available on the switch. Network switches must support the appropriate number of devices on the network.
Port speed	The speed of the network connection is of primary concern to end users.
Forwarding rate	This rate defines the processing capabilities of a switch by rating how much data the switch can process per second. For instance, distribution layer switches should provide higher forwarding rates than access layer switches.

Consideration	Description
Size of frame buffers	Switches with large frame buffers are better able to store frames when there are congested ports to servers or other areas of the network.
PoE support	Power over Ethernet (PoE) is used to power access points, IP phones, security cameras, and even compact switches. Demand for PoE is increasing.
Redundant power	Some stackable and modular chassis-based switches support redundant power supplies.
Reliability	Switches should provide continuous access to the network. Therefore, select switches with reliable redundant features including redundant power supplies, fans, and *supervisor engines*.
Scalability	The number of users on a network typically grows over time. Therefore, select switches that provide the opportunity for growth.

Some of these considerations are now described in more detail.

Port Density (1.2.1.2)

The *port density* of a switch refers to the number of ports available on a single switch. Figure 1-21 shows the port densities of three different switches.

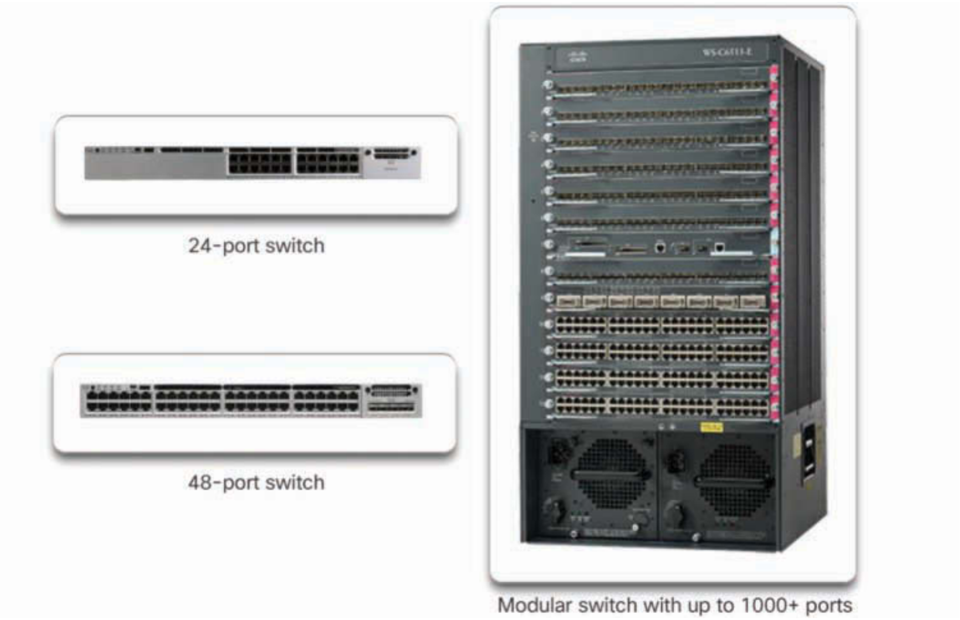


Figure 1-21 Port Densities

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 4 additional ports for ***small form-factor pluggable (SFP)*** devices. SFPs are small compact, hot-pluggable transceivers used on some switches to provide flexibility when choosing network media. SPF transceivers are available for copper and fiber Ethernet, Fibre Channel networks, and more.

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 1000 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 high-density modular switches, a network would need many fixed configuration switches to accommodate the number of devices that need network access—and this approach can consume many power outlets and a lot of closet space.

A 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 problematic 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 1-22.

Forwarding rates are an important consideration when selecting a switch. If its forwarding rate is too low, a switch cannot accommodate full wire-speed communication across all of its switch ports. ***Wire speed*** is a term used to describe 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 supports a forwarding rate of only 32 Gb/s, it cannot run at full wire speed across all ports simultaneously.

Access layer switches are usually physically limited by their uplinks to the distribution layer. However, they typically do not need to operate at full wire speed. Therefore, less expensive, lower-performing switches can be used at the access layer. The 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.

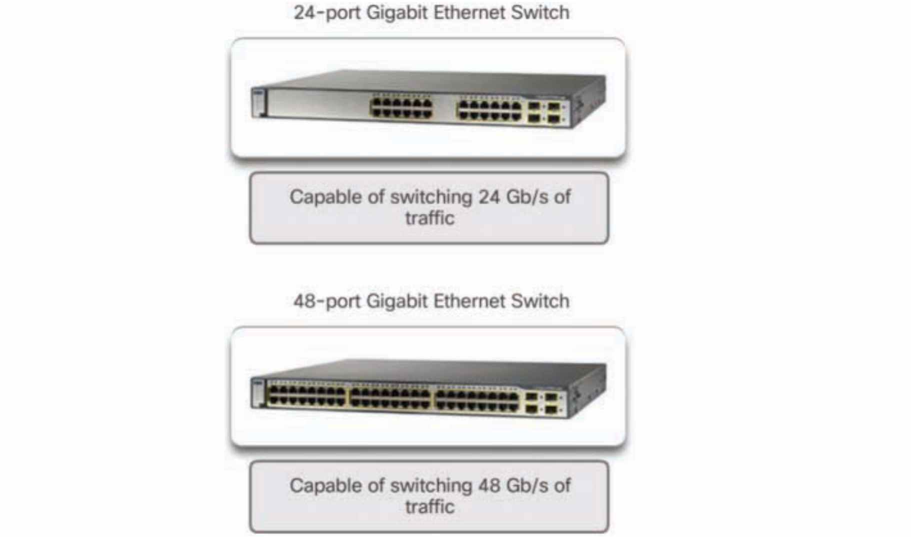

24-port Gigabit Ethernet Switch
Capable of switching 24 Gb/s of traffic
48-port Gigabit Ethernet Switch
Capable of switching 48 Gb/s of traffic

Figure 1-22 Forwarding Rate

Power over Ethernet (1.2.1.4)

PoE allows a 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. Figure 1-23 shows PoE ports on various devices.

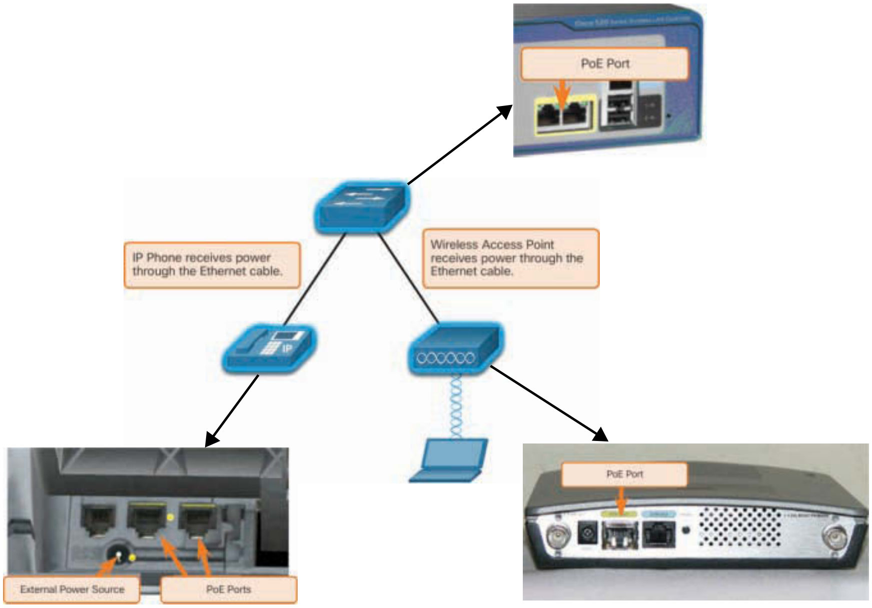

PoE Port
IP Phone receives power through the Ethernet cable.
Wireless Access Point receives power through the Ethernet cable.
IP
External Power Source
PoE Ports
PoE Port

Figure 1-23 Power over Ethernet

PoE increases flexibility when installing wireless access points and IP phones because these devices can be installed anywhere that there is an Ethernet cable. Therefore, 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. Figure 1-24 shows the PoE ports on a Cisco Catalyst 2960-C.

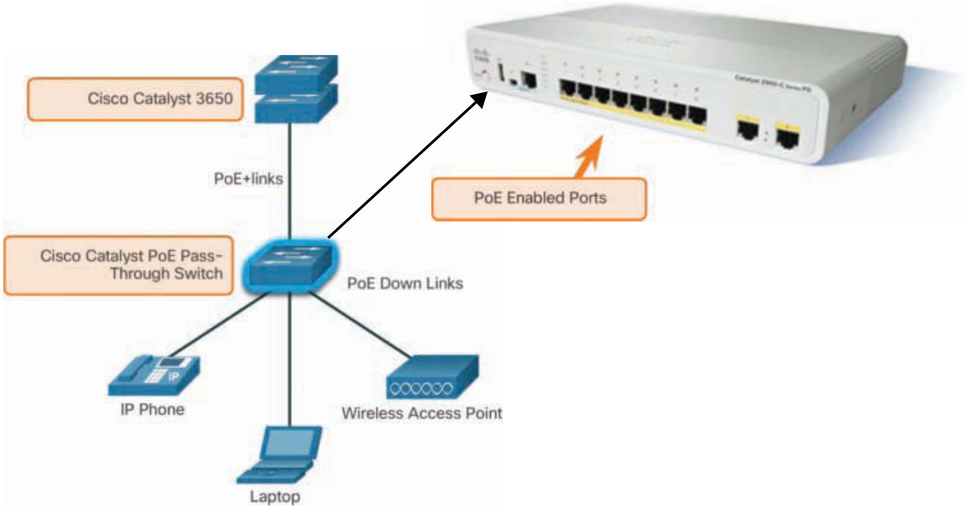


Figure 1-24 PoE Pass-through

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 capability 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 independently 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 is decreasing relative to other constraints.

As shown in Figure 1-25, 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 a Catalyst 2960 switch can be remotely accessed via multiple IP addresses on distinct networks.

Figure 1-25 Cisco Catalyst 2960 Series Switches

Interactive Graphic

Activity 1.2.1.6: Selecting Switch Hardware

Refer to the online course to complete this activity.

Packet Tracer □ **Activity**

Packet Tracer 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.

Router Hardware (1.2.2)

Various types of router platforms are available. Like switches, routers differ in physical configuration and form factor, the number and types of interfaces supported, and the features supported.

The focus of this topic is on how to describe the types of routers available to support network requirements in small to medium-sized business networks.

Router Requirements (1.2.2.1)

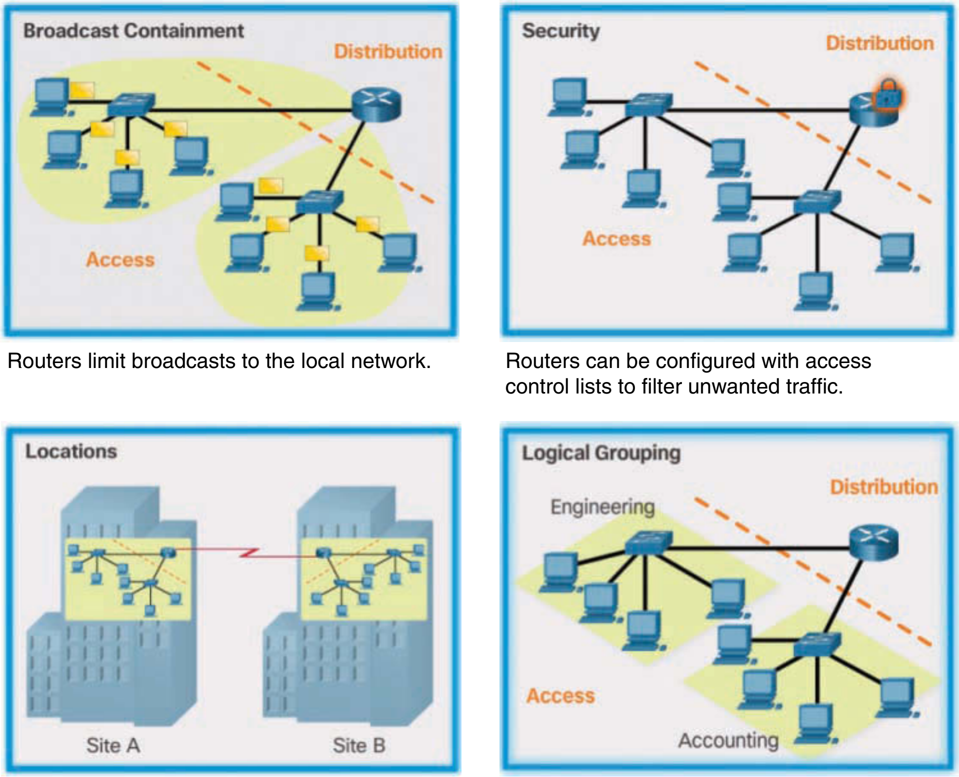
In the distribution layer of an enterprise network, routing is required. Without the routing process, packets cannot leave the local network.

Routers play a critical role in networking by determining the best path for sending packets. They connect multiple IP networks by connecting homes and businesses to the Internet. They are also used to interconnect multiple sites within an enterprise network, providing redundant paths to destinations. A router 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, as shown in Figure 1-26:

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



Routers limit broadcasts to the local network.

Routers can be configured with access control lists to filter unwanted traffic.

Routers can be used to interconnect geographically separated locations.

Routers logically group users who require access to the same resources.

Figure 1-26 Router Functions

Cisco Routers (1.2.2.2)

As a network grows, it is important to select the proper routers to meet its requirements. As shown Figure 1-27, there are three categories of routers:

- *Branch router*—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 they must provide simple network configuration and management.

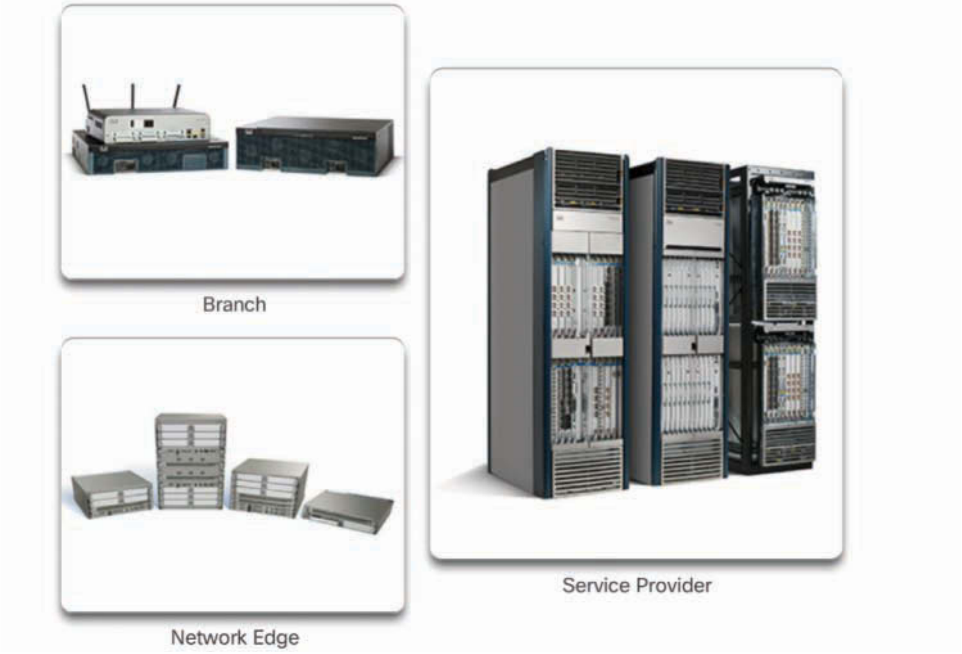


Figure 1-27 Router Platforms

- *Network edge router*—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 router*—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 are available in many form factors, as shown in Figure 1-28. 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.

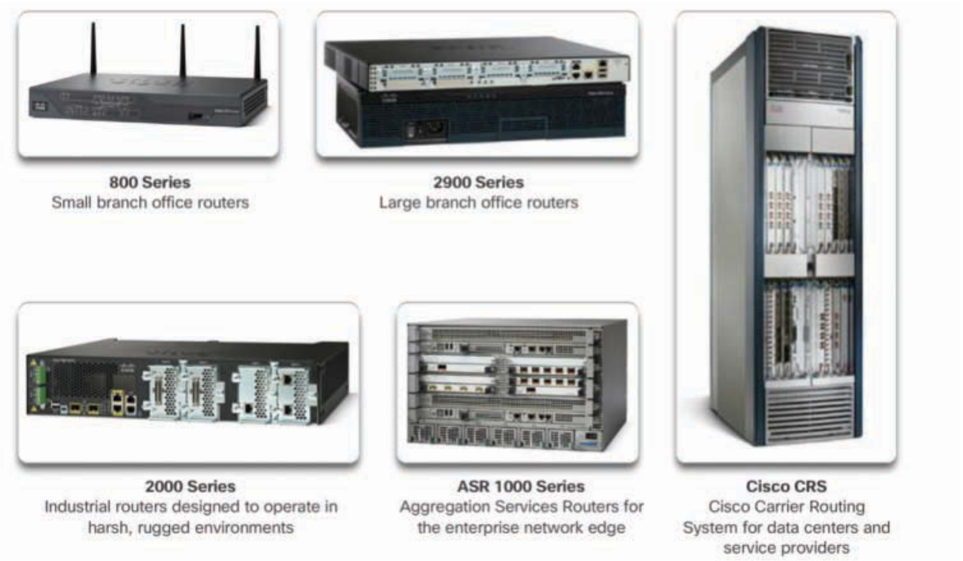

800 Series
Small branch office routers
2900 Series
Large branch office routers
2000 Series
Industrial routers designed to operate in harsh, rugged environments
ASR 1000 Series
Aggregation Services Routers for the enterprise network edge
Cisco CRS
Cisco Carrier Routing System for data centers and service providers

Figure 1-28 A Sampling of Cisco Routers

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. For example, a Cisco 1941 router is a small modular router. It comes with two built-in Gigabit Ethernet RJ-45 interfaces, and it also has 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.

Visit www.cisco.com/c/en/us/products/routers/product-listing.html for a comprehensive list of Cisco routers.

Interactive Graphic

Activity 1.2.2.4: Identify the Router Category

Refer to the online course to complete this activity.

Managing Devices (1.2.3)

Regardless of the form factor and the features each IOS device supports, it requires the *Cisco Internetwork Operating System (IOS)* to be operational.

The focus of this topic is on the Cisco IOS, how to manage it, and how to configure basic settings on Cisco IOS routers and switches.

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 employees and 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. The IOS image 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 1-29.

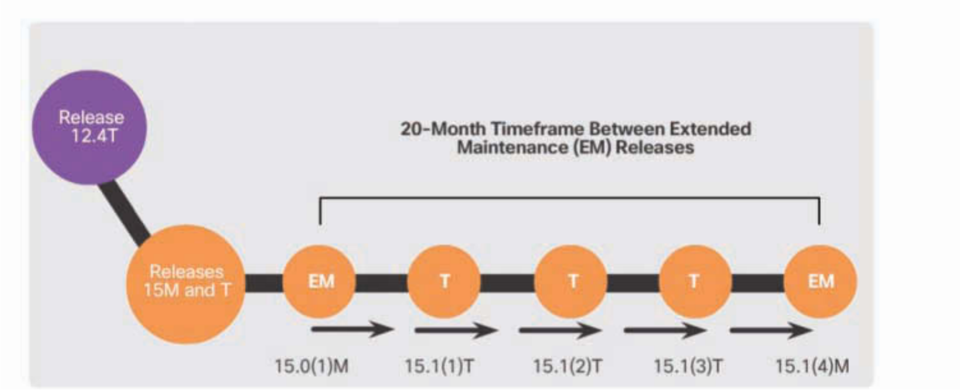


Figure 1-29 Cisco IOS Software Release 15 Family

In this figure, EM (or Extended Maintenance) releases are released approximately every 16 to 20 months. The T releases are between EM releases and are ideal for the very latest features and hardware support before the next EM release becomes available.

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: ***out-of-band management*** and ***in-band management*** (see Figure 1-30).

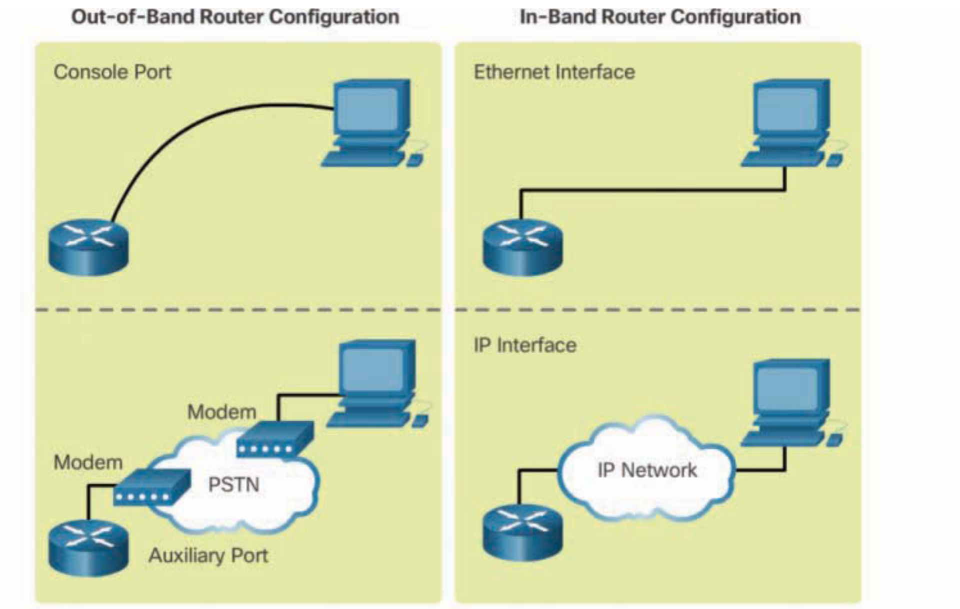


Figure 1-30 In-Band versus Out-of-Band Configuration Options

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

- A direct connection to a console or an AUX port
- A terminal emulation client (such as *PuTTY* or *TeraTerm*)

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 than the others listed here and are not recommended.

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.

Example 1-1 shows the commands entered to enable a router with RIPv2. Verify and save configuration changes by using the **copy running-config startup-config** command.

Example 1-1 Enabling a Router with RIPv2

```
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)#
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)# exit
R1(config)#
R1(config)# 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)# exit
R1(config)#
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 172.16.0.0
R1(config-router)# network 192.168.10.0
R1(config-router)# end
R1#
R1# copy running-config startup-config
```

Example 1-2 shows the results of the configuration commands 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 rip
 version 2
 network 172.16.1.0
 network 192.168.10.0
!
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)

A variety of IOS commands are commonly used to display and verify the operational status of the router and related IPv4 network functionality. Similar commands are available for IPv6; they replace **ip** with **ipv6**.

The following list describes routing-related and interface-related IOS router commands:

- **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 automatic summarization is in effect, the neighbors the router is receiving updates from, and the default administrative distance, which is 120 for RIP (see Example 1-3).

Example 1-3 The **show ip protocols** Command

```
R1# show ip protocols

Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 26 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface              Send  Recv  Triggered RIP  Key-chain
    GigabitEthernet0/0     2     2
    Serial0/0/0            2     2
    Serial0/0/1            2     2
    Interface              Send  Recv  Triggered RIP  Key-chain
 Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
   172.16.0.0
   192.168.10.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.3.2           120      00:00:25
  Distance: (default is 120)
```

- **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 (see Example 1-4).

Example 1-4 The **show ip route** Command

```
R1# show ip route | begin Gateway
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
C        172.16.3.0/30 is directly connected, Serial0/0/0
L        172.16.3.1/32 is directly connected, Serial0/0/0
R        172.16.5.0/24 [120/1] via 172.16.3.2, 00:00:25, Serial0/0/0
      192.168.10.0/24 is variably subnetted, 2 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
```

- **show interfaces**—Displays interface information and status, including the line (protocol) status, bandwidth, delay, reliability, encapsulation, duplex, and I/O statistics. If specified without a specific interface designation, all interfaces are displayed. If a specific interface is specified after the command, information about that interface only is displayed (see Example 1-5).

Example 1-5 The **show interfaces** Command

```
R1# show interfaces gigabitethernet 0/0
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
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
<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—**Displays IP-related interface information, including protocol status, the IPv4 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 are displayed. If a specific interface is specified after the command, information about that interface only is displayed (see Example 1-6).

Example 1-6 The **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—**Displays a summary status of all interfaces, including IPv4 addressing information and interface and line protocols status (see Example 1-7).

Example 1-7 The **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—**Displays information about the routed protocol that is enabled and the protocol status of interfaces (see Example 1-8).

Example 1-8 The **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
```

- **show cdp neighbors—**Tests the Layer 2 connection and provides information about directly connected CDP enabled Cisco devices (see Example 1-9).

Example 1-9 The **show cdp neighbors** Command

```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  D - Remote, C - CVTA, M - Two-port MAC Relay
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce    Holdtme    Capability    Platform    Port ID
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 tests the Layer 2 connection and displays information on directly connected Cisco devices. The information it provides includes the device ID, the local interface the device is connected to, capability (R = router, S = switch), the platform, and the 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 1-10 shows the commands entered to enable a switch.

Example 1-11 shows the results of the configuration commands that were entered in Example 1-10. Verify and save the switch configuration by 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 by using the command **delete flash:vlan.dat**. When switch configurations are in place, view the configurations by using the **show running-config** command.

Example 1-10 Enabling 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-line)# exit
S1(config)#
S1(config)# service password-encryption
S1(config)# banner motd $ Authorized Access Only! $
S1(config)#
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)# exit
S1(config)# ip default-gateway 192.168.1.1
S1(config)#
S1(config)# interface fa0/2
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
S1# copy running-config startup-config
```

Example 1-11 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

S1#
```

Basic Switch Show Commands (1.2.3.6)

Switches make use of the following common IOS commands for configuration, to check for connectivity, and to display current switch status:

- **show port-security interface**—Displays any ports that have security activated. To examine a specific interface, include the interface ID. Information included in the output includes the maximum addresses allowed, the current count, the security violation count, and action to be taken (see Example 1-12).

Example 1-12 The **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**—Displays all secure MAC addresses configured on all switch interfaces (see Example 1-13).

Example 1-13 The **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**—Displays one or all interfaces with line (protocol) status, bandwidth, delay, reliability, encapsulation, duplex, and I/O statistics (see Example 1-14).

Example 1-14 The **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—**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 (see Example 1-15).

Example 1-15 The **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
   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/
Total Mac Addresses for this criterion: 11
S1#
```

Like routers, switches also support the **show cdp neighbors** command.

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