Course Booklet

Switched Networks

ciscopress.com

Cisco | Networking Academy®
Mind Wide Open™

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Switched Networks Course Booklet

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

Printed in the United States of America

First Printing December 2013

Library of Congress data is on file.

ISBN-13: 978-1-58713-326-8

ISBN-10: 1-58713-326-1

Warning and Disclaimer

This book is designed to provide information about Cisco Networking Academy Switched 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.

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Business Operations Manager, Cisco Press
Jan Cornelssen

Executive Editor
Mary Beth Ray

Managing Editor
Sandra Schroeder

Project Editor
Seth Kerney

Editorial Assistant
Vanessa Evans

Cover Designer
Louisa Adair

Interior Designer
Mark Shirar

Composition
Bronkella Publishing, LLC

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.cisco.com/edu.

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.

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

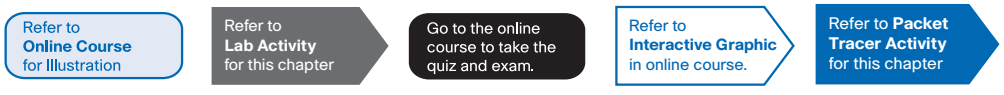
The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **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, and 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: 9781587133299 eBook: 9780133476460)

CHAPTER 0

Introduction to Course

0.0 Switched Networks

0.0.1 Message to the Student

0.0.1.1 Welcome

Welcome to the CCNA R&S Switched Networks course. The goal of this course is to introduce you to fundamental networking concepts and technologies. These online course materials will assist you in developing the skills necessary to plan and implement small networks across a range of applications. The specific skills covered in each chapter are described at the start of each chapter.

You can use your smart phone, tablet, laptop, or desktop to access your course, participate in discussions with your instructor, view your grades, read or review text, and practice using interactive media. However, some media are complex and must be viewed on a PC, as well as Packet Tracer activities, quizzes, and exams.

Refer to **Online Course** for Illustration

0.0.1.2 A Global Community

When you participate in the Networking Academy, you are joining a global community linked by common goals and technologies. Schools, colleges, universities, and other entities in over 160 countries participate in the program. A visualization of the global Networking Academy community is available at http://www.academynetspace.com.

Look for the Cisco Networking Academy official site on Facebook© and LinkedIn©. The Facebook site is where you can meet and engage with other Networking Academy students from around the world. The Cisco Networking Academy LinkedIn site connects you with job postings, and you can see how others are effectively communicating their skills.

Refer to **Online Course** for Illustration

0.0.1.3 More Than Just Information

The NetSpace learning environment is an important part of the overall course experience for students and instructors in the Networking Academy. These online course materials include course text and related interactive media, Packet Tracer simulation activities, real equipment labs, remote access labs, and many different types of quizzes. All of these materials provide important feedback to help you assess your progress throughout the course.

The material in this course encompasses a broad range of technologies that facilitate how people work, live, play, and learn by communicating with voice, video, and other data. Networking and the internet affect people differently in different parts of the world. Although we have worked with instructors from around the world to create these materials, it is important that you work with your instructor and fellow students to make the material in this course applicable to your local situation.

Refer to **Online Course** for Illustration

0.0.1.4 How We Teach

E-doing is a design philosophy that applies the principle that people learn best by doing. The curriculum includes embedded, highly interactive e-doing activities to help stimulate learning, increase knowledge retention, and make the whole learning experience much richer – and that makes understanding the content much easier.

Refer to **Online Course** for Illustration

0.0.1.5 Practice Leads to Mastery

In a typical lesson, after learning about a topic for the first time, you will check your understanding with some interactive media items. If there are new commands to learn, you will practice them with the Syntax Checker before using the commands to configure or troubleshoot a network in Packet Tracer, the Networking Academy network simulation tool. Next, you will do practice activities on real equipment in your classroom or accessed remotely over the internet.

Packet Tracer can also provide additional practice any time by creating your own activities or you may want to competitively test your skills with classmates in multi-user games. Packet Tracer skills assessments and skills integration labs give you rich feedback on the skills you are able to demonstrate and are great practice for chapter, checkpoint, and final exams.

Refer to **Online Course** for Illustration

0.0.1.6 Mind Wide Open

An important goal in education is to enrich you, the student, by expanding what you know and can do. It is important to realize, however, that the instructional materials and the instructor can only facilitate the process. You must make the commitment yourself to learn new skills. The following pages share a few suggestions to help you learn and prepare for transitioning your new skills to the workplace.

Refer to **Online Course** for Illustration

0.0.1.7 Engineering Journals

Professionals in the networking field often keep Engineering Journals in which they write down the things they observe and learn such as how to use protocols and commands. Keeping an Engineering Journal creates a reference you can use at work in your ICT job. Writing is one way to reinforce your learning – along with Reading, Seeing, and Practicing.

A sample entry for implementing a technology could include the necessary software commands, the purpose of the commands, command variables, and a topology diagram indicating the context for using the commands to configure the technology.

Refer to **Online Course** for Illustration

0.0.1.8 Explore the World of Networking

Packet Tracer is a networking learning tool that supports a wide range of physical and logical simulations. It also provides visualization tools to help you understand the internal workings of a network.

The pre-made Packet Tracer activities consist of network simulations, games, activities, and challenges that provide a broad range of learning experiences. These tools will help you develop an understanding of how data flows in a network.

Refer to **Online Course** for Illustration

0.0.1.9 Create Your Own Worlds

You can also use Packet Tracer to create your own experiments and networking scenarios. We hope that, over time, you consider using Packet Tracer - not only for experiencing the pre-built activities, but also to become an author, explorer, and experimenter.

The online course materials have embedded Packet Tracer activities that will launch on computers running Windows® operating systems, if Packet Tracer is installed. This integration may also work on other operating systems using Windows emulation.

Refer to **Online Course** for Illustration

0.0.1.10 How Packet Tracer Helps Master Concepts

Educational Games

Packet Tracer Multi-User games enable you or a team to compete with other students to see who can accurately complete a series of networking tasks the fastest. It is an excellent way to practice the skills you are learning in Packet Tracer activities and hands-on labs.

Cisco Aspire is a single-player, standalone strategic simulation game. Players test their networking skills by completing contracts in a virtual city. The Networking Academy Edition is specifically designed to help you prepare for the CCENT certification exam. It also incorporates business and communication skills ICT employers seek in job candidates.

Performance-Based Assessments

The Networking Academy performance-based assessments have you do Packet Tracer activities like you have been doing all along, only now integrated with an online assessment engine that will automatically score your results and provide you with immediate feedback. This feedback helps you to more accurately identify the knowledge and skills you have mastered and where you need more practice. There are also questions on chapter quizzes and exams that use Packet Tracer activities to give you additional feedback on your progress.

Refer to **Interactive Graphic** in online course.

0.0.1.11 Course Overview

As the course title states, the focus of this course is on learning the architecture, components, and operations of a converged switched network. In this course, you will learn about the hierarchical network design model and how to configure a switch for basic and advanced functionality. You will do the following:

- Describe basic switching concepts and the operation of Cisco switches
- Describe enhanced switching technologies such as VLANs, VLAN Trunking Protocol (VTP), Rapid Spanning Tree Protocol (RSTP), Per VLAN Spanning Tree Protocol (PVSTP), and 802.1q
- Configure and troubleshoot basic operations of a small switched network
- Describe how VLANs create logically separate networks and how routing occurs between them
- Configure and troubleshoot VLANs, trunking on Cisco switches, inter-VLAN routing, VTP, and RSTP
- Describe the operations and benefits of Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) for IPv4 and IPv6

- Configure and troubleshoot DHCP and DNS operations for IPv4 and IPv6
- Describe the purpose of the components in a small wireless network
- Compare and contrast Wi-Fi Protected Access (WPA) security features and the capabilities of open, Wired Equivalent Privacy (WEP), and WPA1/2 networks
- Configure and troubleshoot basic operations of a small wireless network

By the end of this course, you will be able to troubleshoot and resolve common issues with Virtual LANs, VTP, and inter-VLAN routing in a converged network. You will also develop the knowledge and skills needed to implement a WLAN in a small-to-medium network.

Refer to **Interactive Graphic** in online course.

0.1.1.1 Course GUI Tutorial

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

Chapter 0 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 0 Exam

The chapter exam assesses your knowledge of the chapter content.

Your Chapter Notes

CHAPTER 1

Introduction to Switched Networks

1.0 Introduction

1.0.1.1 Introduction

Modern networks continue to evolve to keep pace with the changing way organizations carry out their daily business. Users now expect instant access to company resources from anywhere and at any time. These resources not only include traditional data but also video and voice. There is also an increasing need for collaboration technologies that allow real-time sharing of resources between multiple remote individuals as though they were at the same physical location.

Different devices must seamlessly work together to provide a fast, secure, and reliable connection between hosts. LAN switches provide the connection point for end users into the enterprise network and are also primarily responsible for the control of information within the LAN environment. Routers facilitate the movement of information between LANs and are generally unaware of individual hosts. All advanced services depend on the availability of a robust routing and switching infrastructure on which they can build. This infrastructure must be carefully designed, deployed, and managed to provide a necessary stable platform.

This chapter begins an examination of the flow of traffic in a modern network. It examines some of the current network design models and the way LAN switches build forwarding tables and use the MAC address information to efficiently switch data between hosts.

Refer to **Lab Activity** for this chapter

1.0.1.2 Class Activity - Sent or Received

Sent or Received Instructions

Individually, or in groups (per the instructor's decision), discuss various ways hosts send and receive data, voice, and streaming video.

Develop a matrix (table) listing network data types that can be sent and received. Provide five examples.

Note For an example of the matrix, see the document prepared for this modeling activity.

Save your work in either hard- or soft-copy format. Be prepared to discuss your matrix and statements in a class discussion

Refer to **Interactive Graphic** in online course.

1.1 LAN Design

1.1.1 Converged Networks

1.1.1.1 Growing Complexity of Networks

Our digital world is changing. The ability to access the Internet and the corporate network is no longer confined to physical offices, geographical locations, or time zones. In today's globalized workplace, employees can access resources from anywhere in the world and information must be available at any time, and on any device, as shown in Figure 1. These requirements drive the need to build next-generation networks that are secure, reliable, and highly available.

Data networks originally served the purpose of transporting data between workstations and servers. As networks became more reliable, voice and video traffic was integrated with data traffic creating a converged network. A converged network is one where data, voice, and video are integrated. Next generation converged networks must not only support current expectations and equipment, but must also be able to integrate legacy platforms.

Legacy Equipment

Legacy equipment can hinder convergence. Figure 2 illustrates legacy telephone equipment. A business site may contain equipment that supports both legacy PBX telephone systems and IP-based phones. This sort of equipment is rapidly migrating toward IP-based phone switches.

Advanced Technology

Although converged networks have existed for some time now, they were initially only feasible in large enterprise organizations because of the network infrastructure and complex management requirements. There were high network costs associated with convergence because more expensive switch hardware was required to support the additional bandwidth. Converged networks also required extensive management in relation to QoS, because voice and video data traffic needed to be classified and prioritized on the network. Few individuals had the expertise in voice, video, and data networks to make convergence feasible and functional.

Over time convergence has become easier to implement and manage, and less expensive to purchase. Figure 3 illustrates some of the newer platforms for converged networks that help to provide access to the network anytime, anywhere, and on any device.

Refer to **Online Course** for Illustration

1.1.1.2 Elements of a Converged Network

To support collaboration, business networks employ converged solutions using voice systems, IP phones, voice gateways, video support, and video conferencing (Figure 1). Including data services, a converged network with collaboration support may include features such as the following:

- **Call control**- Telephone call processing, caller ID, call transfer, hold, and conference
- **Voice messaging**- Voicemail

- **Mobility**- Receive important calls wherever you are
- **Automated attendant**- Serve customers faster by routing calls directly to the right department or individual

One of the primary benefits of transitioning to the converged network is that there is just one physical network to install and manage. This results in substantial savings over the installation and management of separate voice, video, and data networks. Such a converged network solution integrates IT management so that any moves, additions, and changes are completed with an intuitive management interface. A converged network solution also provides PC softphone application support, as well as point-to-point video, so that users can enjoy personal communications with the same ease of administration and use as a voice call.

The convergence of services onto the network has resulted in an evolution in networks from a traditional data transport role, to a super-highway for data, voice, and video communication. This one physical network must be properly designed and implemented to allow the reliable handling of the various types of information that it must carry. A structured design is required to allow management of this complex environment.

In Figure 2, play the video to view a few of the collaboration services in action.

Refer to **Online Course** for Illustration

1.1.1.3 Cisco Borderless Network

With the increasing demands of the converged network, the network must be developed with an architectural approach that embeds intelligence, simplifies operations, and is scalable to meet future demands. One of the more recent developments in network design is the Cisco Borderless Network.

The Cisco Borderless Network is a network architecture combining innovation and design that allows organizations to support a borderless network that can connect anyone, anywhere, anytime, on any device - securely, reliably, and seamlessly. This architecture is designed to address IT and business challenges, such as supporting the converged network and changing work patterns.

The Cisco Borderless Network provides the framework to unify wired and wireless access, including policy, access control, and performance management across many different device types. Using this architecture, the borderless network is built on a hierarchical infrastructure of hardware that is scalable and resilient, as shown in Figure 1. By combining this hardware infrastructure with policy-based software solutions, the Cisco Borderless Network provides two primary sets of services: network services and user and endpoint services, all managed by an integrated management solution. It enables different network elements to work together and allow users to access resources from any place at any time, while providing optimization, scalability, and security.

In Figure 2, play the video to learn more about the evolution of the borderless network.

Refer to **Online Course** for Illustration

1.1.1.4 Hierarchy in the Borderless Switched Network

Creating a borderless switched network requires that sound network design principles are used to ensure maximum availability, flexibility, security, and manageability. The borderless switched network must deliver on current requirements and future required services

and technologies. Borderless switched network design guidelines are built upon the following principles:

- **Hierarchical**- Facilitates understanding the role of each device at every tier, simplifies deployment, operation, and management, and reduces fault domains at every tier
- **Modularity**- Allows seamless network expansion and integrated service enablement on an on-demand basis
- **Resiliency**- Satisfies user expectations for keeping the network always on
- **Flexibility**- Allows intelligent traffic load sharing by using all network resources

These are not independent principles. Understanding how each principle fits in the context of the others is critical. Designing a borderless switched network in a hierarchical fashion creates a foundation that allows network designers to overlay security, mobility, and unified communication features. Two time-tested and proven hierarchical design frameworks for campus networks are the three-tier layer, as shown in Figure 1, and the two-tier layer model, as shown in Figure 2.

The three critical layers within these tiered designs are the access, distribution, and core layers. Each layer can be seen as a well-defined, structured module with specific roles and functions in the campus network. Introducing modularity into the campus hierarchical design further ensures that the campus network remains resilient and flexible enough to provide critical network services. Modularity also helps to allow for growth and changes that occur over time.

Refer to **Online Course** for Illustration

1.1.1.5 Access, Distribution, and Core Layers

Access Layer

The access layer represents the network edge, where traffic enters or exits the campus network. Traditionally, the primary function of an access layer switch is to provide network access to the user. Access layer switches connect to distribution layer switches, which implement network foundation technologies such as routing, quality of service, and security.

To meet network application and end-user demand, the next-generation switching platforms now provide more converged, integrated, and intelligent services to various types of endpoints at the network edge. Building intelligence into access layer switches allows applications to operate on the network more efficiently and securely.

Distribution Layer

The distribution layer interfaces between the access layer and the core layer to provide many important functions, including:

- Aggregating large-scale wiring closet networks
- Aggregating Layer 2 broadcast domains and Layer 3 routing boundaries
- Providing intelligent switching, routing, and network access policy functions to access the rest of the network

- Providing high availability through redundant distribution layer switches to the end-user and equal cost paths to the core
- Providing differentiated services to various classes of service applications at the edge of the network

Core Layer

The core layer is the network backbone. It connects several layers of the campus network. The core layer serves as the aggregator for all of the other campus blocks and ties the campus together with the rest of the network. The primary purpose of the core layer is to provide fault isolation and high-speed backbone connectivity.

Figure 1 shows a three-tier campus network design for organizations where the access, distribution, and core are each separate layers. To build a simplified, scalable, cost-effective, and efficient physical cable layout design, the recommendation is to build an extended-star physical network topology from a centralized building location to all other buildings on the same campus.

In some cases where extensive physical or network scalability does not exist, maintaining separate distribution and core layers is not required. In smaller campus locations where there are fewer users accessing the network or in campus sites consisting of a single building, separate core and distribution layers may not be needed. In this scenario, the recommendation is the alternate two-tier campus network design, also known as the collapsed core network design.

Figure 2 shows a two-tier campus network design example for an enterprise campus where the distribution and core layers are collapsed into a single layer.

Refer to **Interactive Graphic** in online course.

1.1.1.6 Activity - Identify Switched Network Terminology

Refer to **Online Course** for Illustration

1.1.2 Switched Networks

1.1.2.1 Role of Switched Networks

The role of switched networks has evolved dramatically in the last two decades. It was not long ago that flat Layer 2 switched networks were the norm. Flat Layer 2 data networks relied on the basic properties of Ethernet and the widespread use of hub repeaters to propagate LAN traffic throughout an organization. As shown in Figure 1, networks have fundamentally changed to switched LANs in a hierarchical network. A switched LAN allows more flexibility, traffic management, and additional features, such as:

- Quality of service
- Additional security
- Support for wireless networking and connectivity
- Support for new technologies, such as IP telephony and mobility services
- Layer 3 functionality

Figure 2 shows the hierarchical design used in the borderless switched network.

Refer to **Online Course** for Illustration

1.1.2.2 Form Factors

There are various types of switches used in business networks. It is important to deploy the appropriate types of switches based on network requirements. Figure 1 highlights some common business considerations when selecting switch equipment.

When selecting the type of switch, the network designer must choose between a fixed or a modular configuration, and stackable or non-stackable. Another consideration is the thickness of the switch, which is expressed in number of rack units. This is important for switches that are mounted in a rack. For example, the fixed configuration switches shown in Figure 2 are all 1 rack unit (1U). These options are sometimes referred to as switch form factors.

Fixed Configuration Switches

Fixed configuration switches do not support features or options beyond those that originally came with the switch (Figure 2). The particular model determines the features and options available. For example, a 24-port gigabit fixed switch cannot support additional ports. There are typically different configuration choices that vary in how many and what types of ports are included with a fixed configuration switch.

Modular Configuration Switches

Modular configuration switches offer more flexibility in their configuration. Modular configuration switches typically come with different sized chassis that allow for the installation of different numbers of modular line cards (Figure 3). The line cards actually contain the ports. The line card fits into the switch chassis the way that expansion cards fit into a PC. The larger the chassis, the more modules it can support. There can be many different chassis sizes to choose from. A modular switch with a single 24-port line card could have an additional 24-port line card added to bring the total number of ports up to 48.

Stackable Configuration Switches

Stackable configuration switches can be interconnected using a special cable that provides high-bandwidth throughput between the switches (Figure 4). Cisco StackWise technology allows the interconnection of up to nine switches. Switches can be stacked one on top of the other with cables connecting the switches in a daisy chain fashion. The stacked switches effectively operate as a single larger switch. Stackable switches are desirable where fault tolerance and bandwidth availability are critical and a modular switch is too costly to implement. Using cross-connected connections, the network can recover quickly if a single switch fails. Stackable switches use a special port for interconnections. Many Cisco stackable switches also support StackPower technology, which enables power sharing among stack members.

Refer to **Online Course** for Illustration

1.1.2.3 Traffic Flow

To select the appropriate switch for a network, you need to have specifications that detail the target traffic flows. Companies need a network that can meet evolving requirements. A business may start with a few PCs interconnected so that they can share data. As the business adds more employees, devices, such as PCs, printers, and servers, are added to the network. Accompanying the new devices is an increase in network traffic. Some companies also rely on converged VoIP phone systems, which add more traffic.

To select the appropriate switches, it is important to perform and record traffic flow analyses regularly. Traffic flow analysis is the process of measuring the bandwidth usage on a network, and then analyzing the data for performance tuning, capacity planning, and

making hardware improvement decisions. Analyzing the various traffic sources and their impact on the network allows you to more accurately tune and upgrade the network to achieve the best possible performance.

There are many ways to monitor traffic flow on a network. Individual switch ports can be manually monitored to record bandwidth utilization over time. Traffic flow analysis tools can automatically record traffic flow data in a database and perform an associated trend analysis. While the software is collecting data, you can see how every interface is performing at any given point in time on the network. This gives the network administrator a visual means of identifying traffic flow patterns.

Refer to **Online Course** for Illustration

1.1.2.4 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. Eventually the term multilayer switch will be redundant.

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 **Packet Tracer Activity** for this chapter

1.1.2.5 Packet Tracer - Comparing 2960 and 3560 Switches

Background/Scenario

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.

Refer to **Online Course** for Illustration

1.1.3 Switch Features

1.1.3.1 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 typically support up to 48 ports on a single device. They have options for up to four additional ports for small form-factor pluggable (SFP) devices. High-port densities allow for better use of limited space and power. If there are two switches that each contain 24 ports, they would be able to support up to 46 devices, because at least one port per switch is lost with the connection of each switch to the rest

of the network. In addition, two power outlets are required. Alternatively, if there is a single 48-port switch, 47 devices can be supported, with only one port used to connect the switch to the rest of the network, and only one power outlet needed to accommodate the single switch.

Modular switches can support very high-port densities through the addition of multiple switch port line cards. For example, some Catalyst 6500 switches can support in excess of 1,000 switch ports.

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

The network designer must also consider the issue of uplink bottlenecks. For example, to achieve target performance, a series of fixed configuration switches may require many ports for bandwidth aggregation between switches. 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

1.1.3.2 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 Ethernet 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 **Online Course** for Illustration

1.1.3.3 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 relatively new 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

1.1.3.4 Cisco Catalyst Switch Breakdown

While switches can be categorized in various ways, Cisco Catalyst switches are usually described in terms of the core-distribution-access hierarchy. The core and distribution layers often include the same types of switches, depending on the size of the network. Similarly, the distribution and access layers often include the same types of switches.

In general, the core and distribution layers incorporate four types of switches:

- **Cisco Catalyst 6500 Series Switches**- These switches scale to 4-terabit capacity with the Virtual Switching System, with up to 160 gigabits per slot; the switches are 100 Gigabit Ethernet ready, and support enhanced security, manageability, and wireless control.
- **Cisco Catalyst 4500E Series Switches**- These switches support modularity, offering 1.6-terabit capacity with the Virtual Switching System; these switches offer high availability bolstered by Control Plane Policing (CPP), and are ideal for collapsed distribution-access and small to medium distribution deployments.
- **Cisco Catalyst 4500-X Series Switches**- These switches are fixed aggregation switches for space-constrained environments, in a 1 RU form factor, and operating at 1.6 terabits per second capacity.
- **Cisco Catalyst 3750-X Series Switches**- These switches are stackable fixed-configuration switches for smaller, restrictive deployments, with advanced Layer 3 and Layer 2 switching and security services, and support for Gigabit and 10 Gigabit Ethernet aggregation, including comprehensive support for Borderless Networks services.

The distribution and access layers typically incorporate the following types of switches:

- **Cisco Catalyst 4500E Series Switches**- These switches come with high capacity (848 gigabits) and density (240 full Power Over Ethernet Plus ports), with 60 Watt Universal Power Over Ethernet to power a large range of devices, and high availability with Stateful Switchover (SSO).
- **Cisco Catalyst 3750-X Series Switches**- These switches are stackable fixed-configuration switches, with StackWise Plus and StackPower for high availability and operational efficiency, service and network modules for service upgrades, and full Power Over Ethernet Plus and comprehensive Borderless Networks services.
- **Cisco Catalyst 3560-X Series Switches**- These switches are fixed-configuration switches for campus and branch deployments, with high-availability and advanced security features, service and network modules for service upgrades, and full Power Over Ethernet Plus and comprehensive Borderless Networks services.
- **Cisco Catalyst 3560 and 3560-C Series Compact Switches**- These are sleek quiet switches that deliver comprehensive access services outside the wiring closet, support for Power Over Ethernet Plus, Cisco EnergyWise, and advanced QoS, as well as providing a unique PoE pass-through capability that eliminates the need for power outlets.

The access layer normally incorporates the following types of switches:

- **Cisco Catalyst 2960 Series Switches**- These are stackable fixed-configuration Layer 2 switches which are a cost-effective solution for mid-sized organizations and branch offices, and provide full Power Over Ethernet Plus and baseline Borderless Networks services
- **Cisco Catalyst 2960 and 2960-C Series Compact Switches**- These are sleek quiet switches that deliver baseline access services outside the wiring closet, with support for Power Over Ethernet Plus, Cisco EnergyWise, and advanced QoS, and provide unique PoE pass-through capability eliminates the need for power outlets.

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

Refer to **Interactive Graphic** in online course.

1.1.3.5 Activity - Identify Switch Hardware

Refer to **Lab Activity** for this chapter

1.1.3.6 Lab - Selecting Switching Hardware

In this lab, you will complete the following objectives:

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

Refer to **Online Course** for Illustration

1.2 The Switched Environment

1.2.1 Frame Forwarding

1.2.1.1 Switching as a General Concept in Networking and Telecommunications

The concept of switching and forwarding frames is universal in networking and telecommunications. Various types of switches are used in LANs, WANs, and the public switched telephone network (PSTN). The fundamental concept of switching refers to a device making a decision based on two criteria:

- Ingress port
- Destination address

The decision on how a switch forwards traffic is made in relation to the flow of that traffic. The term ingress is used to describe where a frame enters the device on a port. The term egress is used to describe frames leaving the device from a particular port.

When a switch makes a decision, it is based on the ingress port and the destination address of the message.

A LAN switch maintains a table that it uses to determine how to forward traffic through the switch. Click the Play button in the figure to see an animation of the switching process. In this example:

- If a message enters switch port 1 and has a destination address of EA, then the switch forwards the traffic out port 4.
- If a message enters switch port 5 and has a destination address of EE, then the switch forwards the traffic out port 1.
- If a message enters switch port 3 and has a destination address of AB, then the switch forwards the traffic out port 6.

The only intelligence of the LAN switch is its ability to use its table to forward traffic based on the ingress port and the destination address of a message. With a LAN switch, there is only one master switching table that describes a strict association between addresses and ports; therefore, a message with a given destination address always exits the same egress port, regardless of the ingress port it enters.

Cisco LAN switches forward Ethernet frames based on the destination MAC address of the frames.

Refer to **Online Course** for Illustration

1.2.1.2 Dynamically Populating a Switch MAC Address Table

Switches use MAC addresses to direct network communications through the switch to the appropriate port toward the destination. A switch is made up of integrated circuits and the accompanying software that controls the data paths through the switch. For a switch to know which port to use to transmit a frame, it must first learn which devices exist on each port. As the switch learns the relationship of ports to devices, it builds a table called a MAC address, or content addressable memory (CAM) table. CAM is a special type of memory used in high-speed searching applications.

LAN switches determine how to handle incoming data frames by maintaining the MAC address table. A switch builds its MAC address table by recording the MAC address of each device connected to each of its ports. The switch uses the information in the MAC address table to send frames destined for a specific device out the port which has been assigned to that device.

A switch populates the MAC address table based on source MAC addresses. When a switch receives an incoming frame with a destination MAC address that is not found in the MAC address table, the switch forwards the frame out of all ports (flooding) except for the ingress port of the frame. When the destination device responds, the switch adds the source MAC address of the frame and the port where the frame was received to the MAC address table. In networks with multiple interconnected switches, the MAC address table contains multiple MAC addresses for a single port connected to the other switches.

The following steps describe the process of building the MAC address table:

1. The switch receives a frame from PC 1 on Port 1 (Figure 1).
2. The switch examines the source MAC address and compares it to MAC address table.
   - If the address is not in the MAC address table, it associates the source MAC address of PC 1 with the ingress port (Port 1) in the MAC address table (Figure 2).
   - If the MAC address table already has an entry for that source address, it resets the aging timer. An entry for a MAC address is typically kept for five minutes.

3. After the switch has recorded the source address information, the switch examines the destination MAC address.
   - If the destination address is not in the MAC table or if it's a broadcast MAC address, as indicated by all Fs, the switch floods the frame to all ports, except the ingress port (Figure 3).
4. The destination device (PC 3) replies to the frame with a unicast frame addressed to PC 1 (Figure 4).
5. The switch enters the source MAC address of PC 3 and the port number of the ingress port into the address table. The destination address of the frame and its associated egress port is found in the MAC address table (Figure 5).
6. The switch can now forward frames between these source and destination devices without flooding, because it has entries in the address table that identify the associated ports (Figure 6).

Refer to **Online Course** for Illustration

1.2.1.3 Switch Forwarding Methods

As networks grew and enterprises began to experience slower network performance, Ethernet bridges (an early version of a switch) were added to networks to limit the size of the collision domains. In the 1990s, advancements in integrated circuit technologies allowed for LAN switches to replace Ethernet bridges. These LAN switches were able to move the Layer 2 forwarding decisions from software to application-specific-integrated circuits (ASICs). ASICs reduce the packet-handling time within the device, and allow the device to handle an increased number of ports without degrading performance. This method of forwarding data frames at Layer 2 was referred to as store-and-forward switching. This term distinguished it from cut-through switching.

As shown in Figure 1, the store-and-forward method makes a forwarding decision on a frame after it has received the entire frame and checked the frame for errors using a mathematical error-checking mechanism known as a cyclic redundancy check (CRC).

By contrast, the cut-through method, as shown in Figure 2 begins the forwarding process after the destination MAC address of an incoming frame and the egress port has been determined.

Refer to **Online Course** for Illustration

1.2.1.4 Store-and-Forward Switching

Store-and-forward switching has two primary characteristics that distinguish it from cut-through: error checking and automatic buffering.

Error Checking

A switch using store-and-forward switching performs an error check on an incoming frame. After receiving the entire frame on the ingress port, as shown in the figure, the switch compares the frame-check-sequence (FCS) value in the last field of the datagram against its own FCS calculations. The FCS is an error checking process that helps to ensure that the frame is free of physical and data-link errors. If the frame is error-free, the switch forwards the frame. Otherwise the frame is dropped.

Automatic Buffering

The ingress port buffering process used by store-and-forward switches provides the flexibility to support any mix of Ethernet speeds. For example, handling an incoming frame traveling into a 100 Mb/s Ethernet port that must be sent out a 1 Gb/s interface would require using the store-and-forward method. With any mismatch in speeds between the ingress and egress ports, the switch stores the entire frame in a buffer, computes the FCS check, forwards it to the egress port buffer and then sends it.

A store-and-forward switch drops frames that do not pass the FCS check, therefore does not forward invalid frames. By contrast, a cut-through switch may forward invalid frames because no FCS check is performed.

Refer to **Online Course** for Illustration

1.2.1.5 Cut-Through Switching

An advantage to cut-through switching is the ability of the switch to start forwarding a frame earlier than store-and-forward switching. There are two primary characteristics of cut-through switching: rapid frame forwarding and fragment free.

Rapid Frame Forwarding

As indicated in the figure, a switch using the cut-through method can make a forwarding decision as soon as it has looked up the destination MAC address of the frame in its MAC address table. The switch does not have to wait for the rest of the frame to enter the ingress port before making its forwarding decision.

With today's MAC controllers and ASICs, a switch using the cut-through method can quickly decide whether it needs to examine a larger portion of a frame's headers for additional filtering purposes. For example, the switch can analyze past the first 14 bytes (the source MAC address, destination MAC, and the EtherType fields), and examine an additional 40 bytes in order to perform more sophisticated functions relative to IPv4 Layers 3 and 4.

The cut-through switching method does not drop most invalid frames. Frames with errors are forwarded to other segments of the network. If there is a high error rate (invalid frames) in the network, cut-through switching can have a negative impact on bandwidth; thus, clogging up bandwidth with damaged and invalid frames.

Fragment Free

Fragment free switching is a modified form of cut-through switching in which the switch waits for the collision window (64 bytes) to pass before forwarding the frame. This means each frame will be checked into the data field to make sure no fragmentation has occurred. Fragment free mode provides better error checking than cut-through, with practically no increase in latency.

The lower latency speed of cut-through switching makes it more appropriate for extremely demanding, high-performance computing (HPC) applications that require process-to-process latencies of 10 microseconds or less.

Refer to **Interactive Graphic** in online course.

1.2.1.6 Activity - Frame Forwarding Methods

Refer to **Interactive Graphic** in online course.

1.2.1.7 Activity - Switch It!

Refer to **Online Course** for Illustration

1.2.2 Switching Domains

1.2.2.1 Collision Domains

In hub-based Ethernet segments, network devices compete for the medium, because devices must take turns when transmitting. The network segments that share the same bandwidth between devices are known as collision domains, because when two or more devices within that segment try to communicate at the same time, collisions may occur.

It is possible, however, to use a switch device, operating the OSI data link layer, to divide a network into segments and reduce the number of devices that compete for bandwidth. When a switch is used, each port represents a new segment. Each new segment is a new collision domain. More bandwidth is available to the devices on the segment, and collisions in one collision domain do not interfere with the other segments. This is also known as microsegmentation.

As shown in the figure, each switch port connects to a single PC or server, and each switch port represents a separate collision domain.

Refer to **Online Course** for Illustration

1.2.2.2 Broadcast Domains

Although switches filter most frames based on MAC addresses, they do not filter broadcast frames. For other devices on the LAN to receive broadcast frames, switches must flood these frames out all ports except the one on which the broadcast was received. A collection of interconnected switches forms a single broadcast domain. Only a network layer device, such as a router, can divide a Layer 2 broadcast domain. Routers are used to segment both collision and broadcast domains.

When a device sends a Layer 2 broadcast, the destination MAC address in the frame is set to all binary ones. A frame with a destination MAC address of all binary ones is received by all devices in the broadcast domain.

The Layer 2 broadcast domain is referred to as the MAC broadcast domain. The MAC broadcast domain consists of all devices on the LAN that receive broadcast frames from a host.

Click Play in the figure to see this in the first half of the animation.

When a switch receives a broadcast frame, it forwards the frame out each of its ports, except the ingress port where the broadcast frame was received. Each device connected to the switch receives a copy of the broadcast frame and processes it. Broadcasts are sometimes necessary for initially locating other devices and network services, but they also reduce network efficiency. Network bandwidth is used to propagate the broadcast traffic. Too many broadcasts and a heavy traffic load on a network can result in congestion: a slow-down in the network performance.

When two switches are connected together, the broadcast domain is increased, as seen in the second half of the animation. In this case, a broadcast frame is forwarded to all connected ports on switch S1. Switch S1 is connected to switch S2. The frame is then also propagated to all devices connected to switch S2.

Refer to **Online Course** for Illustration

1.2.2.3 Alleviating Network Congestion

LAN switches have special characteristics that make them effective at alleviating network congestion. First, they allow the segmentation of a LAN into separate collision domains.

Each port of the switch represents a separate collision domain and provides the full bandwidth to the device or devices that are connected to that port. Second, they provide full-duplex communication between devices. A full-duplex connection can carry transmitted and received signals at the same time. Full-duplex connections have dramatically increased LAN network performance, and are required for 1 Gb/s Ethernet speeds and higher.

Switches interconnect LAN segments (collision domains), use a table of MAC addresses to determine the segment to which the frame is to be sent, and can lessen or eliminate collisions entirely. Following are some important characteristics of switches that contribute to alleviating network congestion:

- **High port density**- Switches have high-port densities: 24- and 48-port switches are often just 1 rack unit (1.75 inches) in height and operate at speeds of 100 Mb/s, 1 Gb/s, and 10 Gb/s. Large enterprise switches may support many hundreds of ports.
- **Large frame buffers**- The ability to store more received frames before having to start dropping them is useful, particularly when there may be congested ports to servers or other parts of the network.
- **Port speed**- Depending on the cost of a switch, it may be possible to support a mixture of speeds. Ports of 100 Mb/s, and 1 or 10 Gb/s are common (100 Gb/s is also possible).
- **Fast internal switching**- Having fast internal forwarding capabilities allows high performance. The method that is used may be a fast internal bus or shared memory, which affects the overall performance of the switch.
- **Low per-port cost**- Switches provide high-port density at a lower cost. For this reason, LAN switches can accommodate network designs featuring fewer users per segment, therefore, increasing the average available bandwidth per user.

Refer to **Interactive Graphic** in online course.

1.2.2.4 Activity - Circle the Domain

1.3 Summary

Refer to **Online Course** for Illustration

Refer to **Lab Activity** for this chapter

1.3.1.1 Class Activity - It's Network Access Time

It's Network Access Time

Use Packet Tracer for this activity. Internet connectivity is not required in this design. Work with a classmate to create two network designs to accommodate the following scenarios:

Scenario 1 - Classroom Design (LAN)

- 15 student end devices represented by 1 or 2 PCs
- 1 instructor end device preferably represented by a server
- Stream video presentations over LAN connection

Scenario 2 - Administrative Design (WAN)

- All requirements as listed in Scenario 1
- Access to and from a remote administrative server for video presentations and pushed updates for network application software

Both the LAN and WAN designs should fit on to one Packet Tracer file screen. All intermediary devices should be labeled with the switch model (or name) and the router model (or name).

Save your work and be ready to justify your device decisions and layout to your instructor and the class.

Refer to **Interactive Graphic** in online course.

1.3.1.2 Basic Switch Configurations

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

We have seen that the trend in networks is towards convergence using a single set of wires and devices to handle voice, video, and data transmission. In addition, there has been a dramatic shift in the way businesses operate. No longer are employees constrained to physical offices or by geographic boundaries. Resources must now be seamlessly available anytime and anywhere. The Cisco Borderless Network architecture enables different elements, from access switches to wireless access points, to work together and allow users to access resources from any place at any time.

The traditional three-layer hierarchical design model divides the network into core, distribution, and access layers, and allows each portion of the network to be optimized for specific functionality. It provides modularity, resiliency, and flexibility, which provides a foundation that allows network designers to overlay security, mobility, and unified communication features. In some networks, having a separate core and distribution layer is not required. In these networks, the functionality of the core layer and the distribution layer are often collapsed together.

There are various types of switches used in business networks. It is important to deploy the appropriate types of switches based on network requirements. When selecting the type of switch, the network designer must choose between a fixed or modular configuration, and stackable or non-stackable. Another consideration is the thickness of the switch, which is expressed in number of rack units. A network administrator may choose to implement a multilayer switch. 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. Other switch features that should be considered include port density, forwarding rates, power capabilities (such as PoE), and scalability features.

Cisco LAN switches use ASICs to forward frames based on the destination MAC address. Before this can be accomplished, it must first use the source MAC address of incoming frames to build up a MAC address table in content-addressable memory (CAM). If the destination MAC address is contained in this table, the frame is forwarded only to the specific destination port. In cases where the destination MAC address is not found in the MAC address table, the frames are flooded out all ports, except the one on which the frame was received.

Switches use either store-and-forward or cut-through switching. Store-and-forward reads the entire frame into a buffer and checks the CRC before forwarding the frame. Cut-through switching only reads the first portion of the frame and starts forwarding it as soon as the destination address is read. Although this is extremely fast, no error checking is done on the frame before forwarding.

Every port on a switch forms a separate collision domain allowing for extremely high-speed full-duplex communication. Switch ports do not block broadcasts and connecting switches together can extend the size of the broadcast domain often resulting in degraded network performance.

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

CHAPTER 2

Basic Switching Concepts and Configuration

2.0 Basic Switching Concepts and Configuration

2.0.1.1 Introduction

Switches are used to connect multiple devices together on the same network. In a properly designed network, LAN switches are responsible for directing and controlling the data flow at the access layer to networked resources.

Cisco switches are self-configuring and no additional configurations are necessary for them to function out of the box. However, Cisco switches run Cisco IOS, and can be manually configured to better meet the needs of the network. This includes adjusting port speed, bandwidth, and security requirements.

Additionally, Cisco switches can be managed both locally and remotely. To remotely manage a switch it needs to have an IP address and default gateway configured. These are just two of the configurations discussed in this chapter.

Switches operate at the access layer where client network devices connect directly to the network and IT departments want uncomplicated network access for the users. It is one of the most vulnerable areas of the network because it is so exposed to the user. Switches need to be configured to be resilient to attacks of all types while they are protecting user data and allowing for high speed connections. Port security is one of the security features Cisco managed switches provide.

This chapter examines some of the basic switch configuration settings required to maintain a secure, available, switched LAN environment.

Refer to **Lab Activity** for this chapter

2.0.1.2 Class Activity – Stand By Me

Stand By Me

When you arrived to class today, you were given a number by your instructor to use for this introductory class activity.

When class begins, your instructor will ask certain students with specific numbers to stand. Your job is to record the standing students' numbers for each scenario.

Scenario 1 Students with numbers starting with the number 5 should stand. Record the numbers of the standing students.

Scenario 2 Students with numbers ending in B should stand. Record the numbers of the standing students.

Scenario 3 Students with the number 505C should stand. Record the number of the standing student.

At the end of this activity, divide into small groups and record answers to the Reflection questions on the PDF for this activity.

Save your work and be prepared to share it with another student or the entire class.

Refer to **Interactive Graphic** in online course.

2.1 Basic Switch Configuration

2.1.1 Configure a Switch with Initial Settings

2.1.1.1 Switch Boot Sequence

After a Cisco switch is powered on, it goes through the following boot sequence:

1. First, the switch loads a power-on self-test (POST) program stored in ROM. POST checks the CPU subsystem. It tests the CPU, DRAM, and the portion of the flash device that makes up the flash file system.
2. Next, the switch loads the boot loader software. The boot loader is a small program stored in ROM and is run immediately after POST successfully completes.
3. The boot loader performs low-level CPU initialization. It initializes the CPU registers, which control where physical memory is mapped, the quantity of memory, and its speed.
4. The boot loader initializes the flash file system on the system board.
5. Finally, the boot loader locates and loads a default IOS operating system software image into memory and hands control of the switch over to the IOS.

The boot loader finds the Cisco IOS image and attempts to automatically boot by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable file it can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of the file system, the search begins at the first top-level directory. The search proceeds through the directory from the lowest level subdirectory, up the tree. If the search is unsuccessful, the next top-level directory is located and the bottom up search pattern is repeated. On Catalyst 2960 Series switches, the image file is normally contained in a directory that has the same name as the image file (excluding the .bin file extension).

The IOS operating system then initializes the interfaces using the Cisco IOS commands found in the configuration file, startup-config, which is stored in NVRAM.

In the figure, the BOOT environment variable is set using the **`boot system`** global configuration mode command. Notice that the IOS is located in a distinct folder and the folder path is specified. Use the **`show bootvar`** command (**`show boot`** in older IOS versions) to see what the current IOS boot file is set to.

Refer to **Online Course** for Illustration

2.1.1.2 Recovering From a System Crash

The boot loader provides access into the switch if the operating system cannot be used because of missing or damaged system files. The boot loader has a command-line that provides access to the files stored in flash memory.

The boot loader can be accessed through a console connection following these steps:

Step 1. Connect a PC by console cable to the switch console port. Configure terminal emulation software to connect to the switch.

Step 2. Unplug the switch power cord.

Step 3. Reconnect the power cord to the switch and, within 15 seconds, press and hold down the **Mode** button while the System LED is still flashing green.

Step 4. Continue pressing the **Mode** button until the System LED turns briefly amber and then solid green; then release the **Mode** button.

Step 5. The boot loader **`switch:`** prompt appears in the terminal emulation software on the PC.

The **`boot loader`** command line supports commands to format the flash file system, reinstall the operating system software, and recover from a lost or forgotten password. For example, the **`dir`** command can be used to view a list of files within a specified directory as shown in the figure.

Note Notice that in this example, the IOS is located in the root of the flash folder.

Refer to **Online Course** for Illustration

2.1.1.3 Switch LED Indicators

Cisco Catalyst switches have several status LED indicator lights. You can use the switch LEDs to quickly monitor switch activity and its performance. Switches of different models and feature sets will have different LEDs and their placement on the front panel of the switch may also vary.

The figure shows the switch LEDs and the Mode button for a Cisco Catalyst 2960 switch. The Mode button is used to toggle through port status, port duplex, port speed, and PoE (if supported) status of the port LEDs. The following describes the purpose of the LED indicators, and the meaning of their colors:

- **System LED**- Shows whether the system is receiving power and is functioning properly. If the LED is off, it means the system is not powered on. If the LED is green, the system is operating normally. If the LED is amber, the system is receiving power but is not functioning properly.
- **Redundant Power System (RPS) LED**- Shows the RPS status. If the LED is off, the RPS is off or not properly connected. If the LED is green, the RPS is connected and ready to provide back-up power. If the LED is blinking green, the RPS is connected but is unavailable because it is providing power to another device. If the LED is amber, the RPS is in standby mode or in a fault condition. If the LED is blinking amber, the internal power supply in the switch has failed, and the RPS is providing power.
- **Port Status LED**- Indicates that the port status mode is selected when the LED is green. This is the default mode. When selected, the port LEDs will display colors with different meanings. If the LED is off, there is no link, or the port was administratively shut down. If the LED is green, a link is present. If the LED is blinking green, there is activity and the port is sending or receiving data. If the LED is alternating green-amber, there is a link fault. If the LED is amber, the port is blocked to ensure a loop does not exist in the forwarding domain and is not forwarding data (typically, ports

will remain in this state for the first 30 seconds after being activated). If the LED is blinking amber, the port is blocked to prevent a possible loop in the forwarding domain.

- **Port Duplex LED**- Indicates the port duplex mode is selected when the LED is green. When selected, port LEDs that are off are in half-duplex mode. If the port LED is green, the port is in full-duplex mode.
- **Port Speed LED**- Indicates the port speed mode is selected. When selected, the port LEDs will display colors with different meanings. If the LED is off, the port is operating at 10 Mb/s. If the LED is green, the port is operating at 100 Mb/s. If the LED is blinking green, the port is operating at 1000 Mb/s.
- **Power over Ethernet (PoE) Mode LED**- If PoE is supported; a PoE mode LED will be present. If the LED is off, it indicates the PoE mode is not selected and that none of the ports have been denied power or placed in a fault condition. If the LED is blinking amber, the PoE mode is not selected but at least one of the ports has been denied power, or has a PoE fault. If the LED is green, it indicates the PoE mode is selected and the port LEDs will display colors with different meanings. If the port LED is off, the PoE is off. If the port LED is green, the PoE is on. If the port LED is alternating green-amber, PoE is denied because providing power to the powered device will exceed the switch power capacity. If the LED is blinking amber, PoE is off due to a fault. If the LED is amber, PoE for the port has been disabled.

Refer to **Online Course** for Illustration

2.1.1.4 Preparing for Basic Switch Management

To prepare a switch for remote management access, the switch must be configured with an IP address and a subnet mask. Keep in mind, that to manage the switch from a remote network, the switch must be configured with a default gateway. This is very similar to configuring the IP address information on host devices. In the figure, the switch virtual interface (SVI) on S1 should be assigned an IP address. The SVI is a virtual interface, not a physical port on the switch.

SVI is a concept related to VLANs. VLANs are numbered logical groups to which physical ports can be assigned. Configurations and settings applied to a VLAN are also applied to all the ports assigned to that VLAN.

By default, the switch is configured to have the management of the switch controlled through VLAN 1. All ports are assigned to VLAN 1 by default. For security purposes, it is considered a best practice to use a VLAN other than VLAN 1 for the management VLAN.

Note that these IP settings are only for remote management access to the switch; the IP settings do not allow the switch to route Layer 3 packets.

Refer to **Online Course** for Illustration

2.1.1.5 Configuring Basic Switch Management Access with IPv4

Step 1. **Configure Management Interface**An IP address and subnet mask is configured on the management SVI of the switch from VLAN interface configuration mode. As shown in Figure 1, the `interface vlan 99` command is used to enter interface configuration mode. The `ip address` command is used to configure the IP address. The `no shutdown` command enables the interface. In this example, VLAN 99 is configured with IP address 172.17.99.11.The SVI for VLAN 99 will not appear as “up/up” until VLAN 99 is created and there is a device connected

to a switch port associated with VLAN 99. To create a VLAN with the vlan_id of 99, and associate it to an interface, use the following commands:

```
S1(config)# vlan vlan_id
S1(config-vlan)# name vlan_name
S1(config-vlan)# exit
S1(config)# interface interface_id
S1(config-if)# switchport access vlan vlan_id
```

Step 2. **Configure Default Gateway**

The switch should be configured with a default gateway if it will be managed remotely from networks not directly connected. The default gateway is the router the switch is connected to. The switch will forward its IP packets with destination IP addresses outside the local network to the default gateway. As shown in Figure 2, R1 is the default gateway for S1. The interface on R1 connected to the switch has IP address 172.17.99.1. This address is the default gateway address for S1.

To configure the default gateway for the switch, use the **ip default-gateway** command. Enter the IP address of the default gateway. The default gateway is the IP address of the router interface to which the switch is connected. Use the **copy running-config startup-config** command to back up your configuration.

Step 3. **Verify Configuration**

As shown in Figure 3, the **show ip interface brief** command is useful when determining the status of both physical and virtual interfaces. The output shown confirms that interface VLAN 99 has been configured with an IP address and subnet mask and that it is operational.

Refer to **Lab Activity** for this chapter

2.1.1.6 Lab - Configuring Basic Switch Settings

In this lab, you will complete the following objectives:

- Part 1: Cable the Network and Verify the Default Switch Configuration
- Part 2: Configure Basic Network Device Settings
- Part 3: Verify and Test Network Connectivity
- Part 4: Manage the MAC Address Table

Refer to **Online Course** for Illustration

2.1.2 Configure Switch Ports

2.1.2.1 Duplex Communication

The figure illustrates full-duplex and half-duplex communication.

Full-duplex communication improves the performance of a switched LAN. Full-duplex communication increases effective bandwidth by allowing both ends of a connection to transmit and receive data simultaneously. This is also known as bidirectional. This method of optimizing network performance requires micro-segmentation. A micro-segmented

LAN is created when a switch port has only one device connected and is operating at full-duplex. This results in a micro size collision domain of a single device. However, because there is only one device connected, a micro-segmented LAN is collision free.

Unlike full-duplex communication, half-duplex communication is unidirectional. Sending and receiving data does not occur at the same time. Half-duplex communication creates performance issues because data can flow in only one direction at a time, often resulting in collisions. Half-duplex connections are typically seen in older hardware, such as hubs. Full-duplex communication has replaced half-duplex in most hardware.

Most Ethernet and Fast Ethernet NICs sold today offer full-duplex capability. Gigabit Ethernet and 10Gb NICs require full-duplex connections to operate. In full-duplex mode, the collision detection circuit on the NIC is disabled. Frames that are sent by the two connected devices cannot collide because the devices use two separate circuits in the network cable. Full-duplex connections require a switch that supports full-duplex configuration, or a direct connection using an Ethernet cable between two devices.

Standard, shared hub-based Ethernet configuration efficiency is typically rated at 50 to 60 percent of the stated bandwidth. Full-duplex offers 100 percent efficiency in both directions (transmitting and receiving). This results in a 200 percent potential use of the stated bandwidth.

Refer to **Online Course** for Illustration

2.1.2.2 Configure Switch Ports at the Physical Layer

Duplex and Speed

Switch ports can be manually configured with specific duplex and speed settings. Use the **`duplex`** interface configuration mode command to manually specify the duplex mode for a switch port. Use the **`speed`** interface configuration mode command to manually specify the speed for a switch port. In Figure 1, port F0/1 on switch S1 and S2 are manually configured with the **`full`** keyword for the **`duplex`** command, and the **`100`** keyword for the **`speed`** command.

The default setting for both duplex and speed for switch ports on Cisco Catalyst 2960 and 3560 switches is auto. The 10/100/1000 ports operate in either half- or full-duplex mode when they are set to 10 or 100 Mb/s, but when they are set to 1000 Mb/s (1 Gb/s), they operate only in full-duplex mode. Auto-negotiation is useful when the speed and duplex settings of the device connecting to the port are unknown or may change. When connecting to known devices, such as servers, dedicated workstations, or network devices, best practice is to manually set the speed and duplex settings.

When troubleshooting switch port issues, the duplex and speed settings should be checked.

Note Mismatched settings for the duplex mode and speed of switch ports can cause connectivity issues. Auto-negotiation failure creates mismatched settings.

All fiber optic ports, such as 100BASE-FX ports, operate only at one preset speed and are always full-duplex.

Use the Syntax Checker in Figure 2 to configure port F0/1 of switch S1.

Refer to **Online Course** for Illustration

2.1.2.3 Auto-MDIX

Until recently, certain cable types (straight-through or crossover) were required when connecting devices. Switch-to-switch or switch-to-router connections required using different Ethernet cables. Using the automatic medium-dependent interface crossover (auto-MDIX) feature on an interface eliminates this problem. When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately. When connecting to switches without the auto-MDIX feature, straight-through cables must be used to connect to devices such as servers, workstations, or routers and crossover cables must be used to connect to other switches or repeaters.

With auto-MDIX enabled, either type of cable can be used to connect to other devices, and the interface automatically adjusts to communicate successfully. On newer Cisco routers and switches, the **`mdix auto`** interface configuration mode command enables the feature. When using auto-MDIX on an interface, the interface speed and duplex must be set to **`auto`** so that the feature operates correctly.

The commands to enable auto-MDIX are shown in Figure 1.

Note The auto-MDIX feature is enabled by default on Catalyst 2960 and Catalyst 3560 switches, but is not available on the older Catalyst 2950 and Catalyst 3550 switches.

To examine the auto-MDIX setting for a specific interface, use the **`show controllers ethernet-controller`** command with the **`phy`** keyword. To limit the output to lines referencing auto-MDIX, use the **`include Auto-MDIX`** filter. As shown in Figure 2, the output indicates On or Off for the feature.

Use the Syntax Checker in Figure 3 to configure the FastEthernet 0/1 interface on S2 for auto-MDIX.

Refer to **Online Course** for Illustration

2.1.2.4 Verifying Switch Port Configuration

Figure 1 describes some of the options for the **`show`** command that are helpful in verifying common configurable switch features.

Figure 2 shows sample abbreviated output from the **`show running-config`** command. Use this command to verify that the switch has been correctly configured. As seen in the output for S1, some key information is shown:

- Fast Ethernet 0/18 interface configured with the management VLAN 99
- VLAN 99 configured with an IP address of 172.17.99.11 255.255.255.0
- Default gateway set to 172.17.99.1

The **`show interfaces`** command is another commonly used command, which displays status and statistics information on the network interfaces of the switch. The **`show interfaces`** command is frequently used when configuring and monitoring network devices.

Figure 3 shows the output from the **`show interfaces fastEthernet 0/18`** command. The first line in the figure indicates that the FastEthernet 0/18 interface is up/up meaning that it is operational. Further down the output shows that the duplex is full and the speed is 100 Mb/s.

Refer to **Online Course** for Illustration

2.1.2.5 Network Access Layer Issues

The output from the **show interfaces** command can be used to detect common media issues. One of the most important parts of this output is the display of the line and data link protocol status. Figure 1 indicates the summary line to check the status of an interface.

The first parameter (FastEthernet0/1 is up) refers to the hardware layer and, essentially, reflects whether the interface is receiving the carrier detect signal from the other end. The second parameter (line protocol is up) refers to the data link layer and reflects whether the data link layer protocol keepalives are being received.

Based on the output of the **show interfaces** command, possible problems can be fixed as follows:

- If the interface is up and the line protocol is down, a problem exists. There could be an encapsulation type mismatch, the interface on the other end could be error-disabled, or there could be a hardware problem.
- If the line protocol and the interface are both down, a cable is not attached or some other interface problem exists. For example, in a back-to-back connection, the other end of the connection may be administratively down.
- If the interface is administratively down, it has been manually disabled (the **shutdown** command has been issued) in the active configuration.

Figure 2 shows an example of **show interfaces** command output. The example shows counters and statistics for the FastEthernet0/1 interface.

Some media errors are not severe enough to cause the circuit to fail, but do cause network performance issues. Figure 3 explains some of these common errors which can be detected with using the **show interfaces** command.

"Input errors" is the sum of all errors in datagrams that were received on the interface being examined. This includes runts, giants, CRC, no buffer, frame, overrun, and ignored counts. The reported input errors from the **show interfaces** command include the following:

- **Runt Frames**- Ethernet frames that are shorter than the 64-byte minimum allowed length are called runts. Malfunctioning NICs are the usual cause of excessive runt frames, but they can be caused by the same issues as excessive collisions.
- **Giants**- Ethernet frames that are longer than the maximum allowed length are called giants. Giants are caused by the same issues as those that cause runts.
- **CRC errors**- On Ethernet and serial interfaces, CRC errors usually indicate a media or cable error. Common causes include electrical interference, loose or damaged connections, or using the incorrect cabling type. If you see many CRC errors, there is too much noise on the link and you should inspect the cable for damage and length. You should also search for and eliminate noise sources, if possible.

"Output errors" is the sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined. The reported output errors from the **show interfaces** command include the following:

- **Collisions**- Collisions in half-duplex operations are completely normal and you should not worry about them, as long as you are pleased with half-duplex operations. However, you should never see collisions in a properly designed and configured network that uses full-duplex communication. It is highly recommended that you use full-duplex unless you have older or legacy equipment that requires half-duplex.
- **Late collisions**- A late collision refers to a collision that occurs after 512 bits of the frame (the preamble) have been transmitted. Excessive cable lengths are the most common cause of late collisions. Another common cause is duplex misconfiguration. For example, you could have one end of a connection configured for full-duplex and the other for half-duplex. You would see late collisions on the interface that is configured for half-duplex. In that case, you must configure the same duplex setting on both ends. A properly designed and configured network should never have late collisions.

Refer to **Online Course** for Illustration

2.1.2.6 Troubleshooting Network Access Layer Issues

Most issues that affect a switched network are encountered during the original implementation. Theoretically, after it is installed, a network continues to operate without problems. However, cabling gets damaged, configurations change, and new devices are connected to the switch that require switch configuration changes. Ongoing maintenance and troubleshooting of the network infrastructure is required.

To troubleshoot these issues when you have no connection or a bad connection between a switch and another device, follow this general process:

Use the **show interfaces** command to check the interface status.

If the interface is down:

- Check to make sure that the proper cables are being used. Additionally, check the cable and connectors for damage. If a bad or incorrect cable is suspected, replace the cable.
- If the interface is still down, the problem may be due to a mismatch in speed setting. The speed of an interface is typically auto-negotiated; therefore, even if it is manually configured on one interface, the connecting interface should auto-negotiate accordingly. If a speed mismatch does occur through misconfiguration or a hardware or software issue, then that may result in the interface going down. Manually set the same speed on both connection ends if a problem is suspected.

If the interface is up, but issues with connectivity are still present:

- Using the **show interfaces** command, check for indications of excessive noise. Indications may include an increase in the counters for runts, giants, and CRC errors. If there is excessive noise, first find and remove the source of the noise, if possible. Also, verify that the cable does not exceed the maximum cable length and check the type of cable that is used. For copper cable, it is recommended that you use at least Category 5.

- If noise is not an issue, check for excessive collisions. If there are collisions or late collisions, verify the duplex settings on both ends of the connection. Much like the speed setting, the duplex setting is usually auto-negotiated. If there does appear to be a duplex mismatch, manually set the duplex on both connection ends. It is recommended to use full-duplex if both sides support it.

Refer to **Online Course** for Illustration

2.2 Switch Security: Management and Implementation

2.2.1 Secure Remote Access

2.2.1.1 SSH Operation

Secure Shell (SSH) is a protocol that provides a secure (encrypted) management connection to a remote device. SSH should replace Telnet for management connections. Telnet is an older protocol that uses unsecure plaintext transmission of both the login authentication (username and password) and the data transmitted between the communicating devices. SSH provides security for remote connections by providing strong encryption when a device is authenticated (username and password) and also for the transmitted data between the communicating devices. SSH is assigned to TCP port 22. Telnet is assigned to TCP port 23.

In Figure 1, an attacker can monitor packets using Wireshark. A Telnet stream can be targeted to capture the username and password.

In Figure 2, the attacker can capture the username and password of the administrator from the plaintext Telnet session.

Figure 3 shows the Wireshark view of an SSH session. The attacker can track the session using the IP address of the administrator device.

However, in Figure 4, the username and password are encrypted.

To enable SSH on a Catalyst 2960 switch, the switch must be using a version of the IOS software including cryptographic (encrypted) features and capabilities. In Figure 5, use the **`show version`** command on the switch to see which IOS the switch is currently running, and IOS filename that includes the combination "k9" supports cryptographic (encrypted) features and capabilities.

Refer to **Online Course** for Illustration

2.2.1.2 Configuring SSH

Before configuring SSH, the switch must be minimally configured with a unique hostname and the correct network connectivity settings.

Step 1. **Verify SSH support.** Use the **`show ip ssh`** command to verify that the switch supports SSH. If the switch is not running an IOS that supports cryptographic features, this command is unrecognized.

Step 2. **Configure the IP domain.**

Configure the IP domain name of the network using the **ip domain-name** domain-name global configuration mode command. In Figure 1, the domain-name value is **cisco.com**.

Step 3. **Generate RSA key pairs.**

Generating an RSA key pair automatically enables SSH. Use the **crypto key generate rsa** global configuration mode command to enable the SSH server on the switch and generate an RSA key pair. When generating RSA keys, the administrator is prompted to enter a modulus length. Cisco recommends a minimum modulus size of 1,024 bits (see the sample configuration in Figure 1). A longer modulus length is more secure, but it takes longer to generate and to use.

Note To delete the RSA key pair, use the **crypto key zeroize rsa** global configuration mode command. After the RSA key pair is deleted, the SSH server is automatically disabled.

Step 4. **Configure user authentication.**

The SSH server can authenticate users locally or using an authentication server. To use the local authentication method, create a username and password pair using the **username** username **password** password global configuration mode command. In the example, the user **admin** is assigned the password **ccna**.

Step 5. **Configure the vty lines.**

Enable the SSH protocol on the vty lines using the **transport input ssh** line configuration mode command. The Catalyst 2960 has vty lines ranging from 0 to 15. This configuration prevents non-SSH (such as Telnet) connections and limits the switch to accept only SSH connections. Use the **line vty** global configuration mode command and then the **login local** line configuration mode command to require local authentication for SSH connections from the local username database.

Step 6. **Enable SSH version 2.**By default, SSH supports both versions 1 and 2. When supporting both versions, this is shown in the **show ip ssh** output as supporting version 1.99. Version 1 has known vulnerabilities. For this reason, it is recommended to enable only version 2. Enable SSH version using the **ip ssh version 2** global configuration command.Use the Syntax Checker in Figure 2 to configure SSH on switch S1.

Refer to **Online Course** for Illustration

2.2.1.3 Verifying SSH

On a PC, an SSH client, such as PuTTY, is used to connect to an SSH server. For the examples in Figures 1 to 3, the following have been configured:

- SSH enabled on switch S1
- Interface VLAN 99 (SVI) with IP address 172.17.99.11 on switch S1
- PC1 with IP address 172.17.99.21

In Figure 1, the PC initiates an SSH connection to the SVI VLAN IP address of S1.

In Figure 2, the user has been prompted for a username and password. Using the configuration from the previous example, the username **admin** and password **ccna** are entered. After entering the correct combination, the user is connected via SSH to the CLI on the Catalyst 2960 switch.

To display the version and configuration data for SSH on the device that you configured as an SSH server, use the **show ip ssh** command. In the example, SSH version 2 is enabled. To check the SSH connections to the device, use the **show ssh** command (see Figure 3).

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

2.2.1.4 Packet Tracer - Configuring SSH

Background/Scenario

SSH should replace Telnet for management connections. Telnet uses insecure plaintext communications. SSH provides security for remote connections by providing strong encryption of all transmitted data between devices. In this activity, you will secure a remote switch with password encryption and SSH.

Refer to **Online Course** for Illustration

2.2.2 Security Concerns in LANs

2.2.2.1 Common Security Attacks: MAC Address Flooding

Basic switch security does not stop malicious attacks. Security is a layered process that is essentially never complete. The more aware the team of networking professionals within an organization are regarding security attacks and the dangers they pose, the better. Some types of security attacks are described here, but the details of how some of these attacks work are beyond the scope of this course. More detailed information is found in the CCNA WAN Technologies course and the CCNA Security course.

MAC Address Flooding

The MAC address table in a switch contains the MAC addresses associated with each physical port and the associated VLAN for each port. When a Layer 2 switch receives a frame, the switch looks in the MAC address table for the destination MAC address. All Catalyst switch models use a MAC address table for Layer 2 switching. As frames arrive on switch ports, the source MAC addresses are recorded in the MAC address table. If an entry exists for the MAC address, the switch forwards the frame to the correct port. If the MAC address does not exist in the MAC address table, the switch floods the frame out of every port on the switch, except the port where the frame was received.

The MAC address flooding behavior of a switch for unknown addresses can be used to attack a switch. This type of attack is called a MAC address table overflow attack. MAC address table overflow attacks are sometimes referred to as MAC flooding attacks, and CAM table overflow attacks. The figures show how this type of attack works.

In Figure 1, host A sends traffic to host B. The switch receives the frames and looks up the destination MAC address in its MAC address table. If the switch cannot find the destination MAC in the MAC address table, the switch then copies the frame and floods (broadcasts) it out of every switch port, except the port where it was received.

In Figure 2, host B receives the frame and sends a reply to host A. The switch then learns that the MAC address for host B is located on port 2 and records that information into the MAC address table.

Host C also receives the frame from host A to host B, but because the destination MAC address of that frame is host B, host C drops that frame.

As shown in Figure 3, any frame sent by host A (or any other host) to host B is forwarded to port 2 of the switch and not broadcast out every port.

MAC address tables are limited in size. MAC flooding attacks make use of this limitation to overwhelm the switch with fake source MAC addresses until the switch MAC address table is full.

As shown in Figure 4, an attacker at host C can send frames with fake, randomly-generated source and destination MAC addresses to the switch. The switch updates the MAC address table with the information in the fake frames. When the MAC address table is full of fake MAC addresses, the switch enters into what is known as fail-open mode. In this mode, the switch broadcasts all frames to all machines on the network. As a result, the attacker can see all of the frames.

Some network attack tools can generate up to 155,000 MAC entries on a switch per minute. Depending on the switch, the maximum MAC address table size varies.

As shown in Figure 5, as long as the MAC address table on the switch remains full, the switch broadcasts all received frames out of every port. In this example, frames sent from host A to host B are also broadcast out of port 3 on the switch and seen by the attacker at host C.

One way to mitigate MAC address table overflow attacks is to configure port security.

Refer to **Online Course** for Illustration

2.2.2.2 Common Security Attacks: DHCP Spoofing

DHCP is the protocol that automatically assigns a host a valid IP address out of a DHCP pool. DHCP has been in use for nearly as long as TCP/IP has been the main protocol used within industry for allocating clients IP addresses. Two types of DHCP attacks can be performed against a switched network: DHCP starvation attacks and DHCP spoofing.

In DHCP starvation attacks, an attacker floods the DHCP server with DHCP requests to use up all the available IP addresses that the DHCP server can issue. After these IP addresses are issued, the server cannot issue any more addresses, and this situation produces a denial-of-service (DoS) attack as new clients cannot obtain network access. A DoS attack is any attack that is used to overload specific devices and network services with illegitimate traffic, thereby preventing legitimate traffic from reaching those resources.

In DHCP spoofing attacks, an attacker configures a fake DHCP server on the network to issue DHCP addresses to clients. The normal reason for this attack is to force the clients to use false Domain Name System (DNS) or Windows Internet Naming Service (WINS) servers and to make the clients use the attacker, or a machine under the control of the attacker, as their default gateway.

DHCP starvation is often used before a DHCP spoofing attack to deny service to the legitimate DHCP server, making it easier to introduce a fake DHCP server into the network.

To mitigate DHCP attacks, use the DHCP snooping and port security features on the Cisco Catalyst switches. These features are covered in a later topic.

Refer to **Online Course** for Illustration

2.2.2.3 Common Security Attacks: Leveraging CDP

The Cisco Discovery Protocol (CDP) is a proprietary protocol that all Cisco devices can be configured to use. CDP discovers other Cisco devices that are directly connected, which allows the devices to auto-configure their connection. In some cases, this simplifies configuration and connectivity.

By default, most Cisco routers and switches have CDP-enabled on all ports. CDP information is sent in periodic, unencrypted broadcasts. This information is updated locally in the CDP database of each device. Because CDP is a Layer 2 protocol, CDP messages are not propagated by routers.

CDP contains information about the device, such as the IP address, IOS software version, platform, capabilities, and the native VLAN. This information can be used by an attacker to find ways to attack the network, typically in the form of a denial-of-service (DoS) attack.

The figure is a portion of a Wireshark capture showing the contents of a CDP packet. The Cisco IOS software version discovered via CDP, in particular, would allow the attacker to determine whether there were any security vulnerabilities specific to that particular version of IOS. Also, because CDP is not authenticated, an attacker could craft bogus CDP packets and send them to a directly-connected Cisco device.

It is recommended that you disable the use of CDP on devices or ports that do not need to use it by using the **`no cdp run`** global configuration mode command. CDP can be disabled on a per port basis.

Telnet Attacks

The Telnet protocol is insecure and can be used by an attacker to gain remote access to a Cisco network device. There are tools available that allow an attacker to launch a brute force password-cracking attack against the vty lines on the switch.

Brute Force Password Attack

The first phase of a brute force password attack starts with the attacker using a list of common passwords and a program designed to try to establish a Telnet session using each word on the dictionary list. If the password is not discovered by the first phase, a second phase begins. In the second phase of a brute force attack, the attacker uses a program that creates sequential character combinations in an attempt to guess the password. Given enough time, a brute force password attack can crack almost all passwords used.

To mitigate against brute force password attacks use strong passwords that are changed frequently. A strong password should have a mix of upper and lowercase letters and should include numerals and symbols (special characters). Access to the vty lines can also be limited using an access control list (ACL).

Telnet DoS Attack

Telnet can also be used to launch a DoS attack. In a Telnet DoS attack, the attacker exploits a flaw in the Telnet server software running on the switch that renders the Telnet service unavailable. This sort of attack prevents an administrator from remotely accessing switch management functions. This can be combined with other direct attacks on the network as part of a coordinated attempt to prevent the network administrator from accessing core devices during the breach.

Vulnerabilities in the Telnet service that permit DoS attacks to occur are usually addressed in security patches that are included in newer Cisco IOS revisions.

Note It is a best practice to use SSH, rather than Telnet for remote management connections.

Refer to **Interactive Graphic** in online course.

2.2.2.4 Activity - Identify Common Security Attacks

Refer to **Online Course** for Illustration

2.2.3 Security Best Practices

2.2.3.1 Best Practices

Defending your network against attack requires vigilance and education. The following are best practices for securing a network:

- Develop a written security policy for the organization.
- Shut down unused services and ports.
- Use strong passwords and change them often.
- Control physical access to devices.
- Avoid using standard insecure HTTP websites, especially for login screens; instead use the more secure HTTPS.
- Perform backups and test the backed up files on a regular basis.
- Educate employees about social engineering attacks, and develop policies to validate identities over the phone, via email, and in person.
- Encrypt and password-protect sensitive data.
- Implement security hardware and software, such as firewalls.
- Keep software up-to-date by installing security patches weekly or daily, if possible.

These methods are only a starting point for security management. Organizations must remain vigilant at all times to defend against continually evolving threats. Use network security tools to measure the vulnerability of the current network.

Refer to **Online Course** for Illustration

2.2.3.2 Network Security Tools and Testing

Network security tools help a network administrator test a network for weaknesses. Some tools allow an administrator to assume the role of an attacker. Using one of these tools, an administrator can launch an attack against the network and audit the results to determine how to adjust security policies to mitigate those types of attacks. Security auditing and penetration testing are two basic functions that network security tools perform.

Network security testing techniques may be manually initiated by the administrator. Other tests are highly automated. Regardless of the type of testing, the staff that sets up and conducts the security testing should have extensive security and networking knowledge. This includes expertise in the following areas:

- Network security
- Firewalls
- Intrusion prevention systems

- Operating systems
- Programming
- Networking protocols (such as TCP/IP)

Refer to **Online Course** for Illustration

2.2.3.3 Network Security Audits

Network security tools allow a network administrator to perform a security audit of a network. A security audit reveals the type of information an attacker can gather simply by monitoring network traffic.

For example, network security auditing tools allow an administrator to flood the MAC address table with fictitious MAC addresses. This is followed by an audit of the switch ports as the switch starts flooding traffic out of all ports. During the audit, the legitimate MAC address mappings are aged out and replaced with fictitious MAC address mappings. This determines which ports are compromised and not correctly configured to prevent this type of attack.

Timing is an important factor in performing the audit successfully. Different switches support varying numbers of MAC addresses in their MAC table. It can be difficult to determine the ideal number of spoofed MAC addresses to send to the switch. A network administrator also has to contend with the age-out period of the MAC address table. If the spoofed MAC addresses start to age out while performing a network audit, valid MAC addresses start to populate the MAC address table, and limiting the data that can be monitored with a network auditing tool.

Network security tools can also be used for penetration testing against a network. Penetration testing is a simulated attack against the network to determine how vulnerable it would be in a real attack. This allows a network administrator to identify weaknesses within the configuration of networking devices and make changes to make the devices more resilient to attacks. There are numerous attacks that an administrator can perform, and most tool suites come with extensive documentation detailing the syntax needed to execute the desired attack.

Because penetration tests can have adverse effects on the network, they are carried out under very controlled conditions, following documented procedures detailed in a comprehensive network security policy. An off-line test bed network that mimics the actual production network is the ideal. The test bed network can be used by networking staff to perform network penetration tests.

Refer to **Online Course** for Illustration

2.2.4 Switch Port Security

2.2.4.1 Secure Unused Ports

Disable Unused Ports

A simple method that many administrators use to help secure the network from unauthorized access is to disable all unused ports on a switch. For example, if a Catalyst 2960 switch has 24 ports and there are three Fast Ethernet connections in use, it is good practice to disable the 21 unused ports. Navigate to each unused port and issue the Cisco IOS **`shutdown`** command. If a port later on needs to be reactivated, it can be enabled with the **`no shutdown`** command. The figure shows partial output for this configuration.

It is simple to make configuration changes to multiple ports on a switch. If a range of ports must be configured, use the **interface range** command.

```
Switch(config)# interface range type module/first-number - last-number
```

The process of enabling and disabling ports can be time-consuming, but it enhances security on the network and is well worth the effort.

Refer to **Online Course** for Illustration

2.2.4.2 DHCP Snooping

DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted. Trusted ports can source all DHCP messages, including DHCP offer and DHCP acknowledgement packets; untrusted ports can source requests only. Trusted ports host a DHCP server or can be an uplink toward the DHCP server. If a rogue device on an untrusted port attempts to send a DHCP offer packet into the network, the port is shut down. This feature can be coupled with DHCP options in which switch information, such as the port ID of the DHCP request, can be inserted into the DHCP request packet.

As shown in Figures 1 and 2, untrusted ports are those not explicitly configured as trusted. A DHCP binding table is built for untrusted ports. Each entry contains a client MAC address, IP address, lease time, binding type, VLAN number, and port ID recorded as clients make DHCP requests. The table is then used to filter subsequent DHCP traffic. From a DHCP snooping perspective, untrusted access ports should not send any DHCP server messages.

These steps illustrate how to configure DHCP snooping on a Catalyst 2960 switch:

Step 1. Enable DHCP snooping using the **ip dhcp snooping** global configuration mode command.

Step 2. Enable DHCP snooping for specific VLANs using the **ip dhcp snooping vlan** number command.

Step 3. Define ports as trusted at the interface level by defining the trusted ports using the **ip dhcp snooping trust** command.

Step 4. (Optional) Limit the rate at which an attacker can continually send bogus DHCP requests through untrusted ports to the DHCP server using the **ip dhcp snooping limit rate** rate command.

Refer to **Online Course** for Illustration

2.2.4.3 Port Security: Operation

Port Security

All switch ports (interfaces) should be secured before the switch is deployed for production use. One way to secure ports is by implementing a feature called port security. Port security limits the number of valid MAC addresses allowed on a port. The MAC addresses of legitimate devices are allowed access, while other MAC addresses are denied.

Port security can be configured to allow one or more MAC addresses. If the number of MAC addresses allowed on the port is limited to one, then only the device with that specific MAC address can successfully connect to the port.

If a port is configured as a secure port and the maximum number of MAC addresses is reached, any additional attempts to connect by unknown MAC addresses will generate a security violation. Figure 1 summarizes these points.

Secure MAC Address Types

There are a number of ways to configure port security. The type of secure address is based on the configuration and includes:

- **Static secure MAC addresses**- MAC addresses that are manually configured on a port by using the **switchport port-security mac-address** mac-address interface configuration mode command. MAC addresses configured in this way are stored in the address table and are added to the running configuration on the switch.
- **Dynamic secure MAC addresses**- MAC addresses that are dynamically learned and stored only in the address table. MAC addresses configured in this way are removed when the switch restarts.
- **Sticky secure MAC addresses**- MAC addresses that can be dynamically learned or manually configured, then stored in the address table and added to the running configuration.

Sticky Secure MAC addresses

To configure an interface to convert dynamically learned MAC addresses to sticky secure MAC addresses and add them to the running configuration, you must enable sticky learning. Sticky learning is enabled on an interface by using the **switchport port-security mac-address sticky** interface configuration mode command.

When this command is entered, the switch converts all dynamically learned MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. All sticky secure MAC addresses are added to the address table and to the running configuration.

Sticky secure MAC addresses can also be manually defined. When sticky secure MAC addresses are configured by using the **switchport port-security mac-address sticky** mac-address interface configuration mode command, all specified addresses are added to the address table and the running configuration.

If the sticky secure MAC addresses are saved to the startup configuration file, then when the switch restarts or the interface shuts down, the interface does not need to relearn the addresses. If the sticky secure addresses are not saved, they will be lost.

If sticky learning is disabled by using the **no switchport port-security mac-address sticky** interface configuration mode command, the sticky secure MAC addresses remain part of the address table, but are removed from the running configuration.

Figure 2 shows the characteristics of sticky secure MAC addresses.

Note that port security feature will not work until port security is enabled on the interface using the **switchport port-security** command.

Refer to **Online Course** for Illustration

2.2.4.4 Port Security: Violation Modes

It is a security violation when either of these situations occurs:

- The maximum number of secure MAC addresses have been added to the address table for that interface, and a station whose MAC address is not in the address table attempts to access the interface.
- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

An interface can be configured for one of three violation modes, specifying the action to be taken if a violation occurs. The figure presents which kinds of data traffic are forwarded when one of the following security violation modes are configured on a port:

- **Protect**- When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed, or the number of maximum allowable addresses is increased. There is no notification that a security violation has occurred.
- **Restrict**- When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed, or the number of maximum allowable addresses is increased. In this mode, there is a notification that a security violation has occurred.
- **Shutdown**- In this (default) violation mode, a port security violation causes the interface to immediately become error-disabled and turns off the port LED. It increments the violation counter. When a secure port is in the error-disabled state, it can be brought out of this state by entering the **`shutdown`** and **`no shutdown`** interface configuration mode commands.

To change the violation mode on a switch port, use the **`switchport port-security violation`** {**`protect`** | **`restrict`** | **`shutdown`**} interface configuration mode command.

Refer to **Online Course** for Illustration

2.2.4.5 Port Security: Configuring

Figure 1 summarizes the default port security settings on a Cisco Catalyst switch.

Figure 2 shows the Cisco IOS CLI commands needed to configure port security on the Fast Ethernet F0/18 port on the S1 switch. Notice that the example does not specify a violation mode. In this example, the violation mode is shutdown (the default mode).

Figure 3 shows how to enable sticky secure MAC addresses for port security on Fast Ethernet port 0/19 of switch S1. As stated earlier, the maximum number of secure MAC addresses can be manually configured. In this example, the Cisco IOS command syntax is used to set the maximum number of MAC addresses to 10 for port 0/19. The violation mode is set to shutdown, by default.

Refer to **Online Course** for Illustration

2.2.4.6 Port Security: Verifying

Verify Port Security

After configuring port security on a switch, check each interface to verify that the port security is set correctly, and check to ensure that the static MAC addresses have been configured correctly.

Verify Port Security Settings

To display port security settings for the switch or for the specified interface, use the **show port-security [interface** interface-id**]** command. The output for the dynamic port security configuration is shown in Figure 1. By default, there is one MAC address allowed on this port.

The output shown in Figure 2 shows the values for the sticky port security settings. The maximum number of addresses is set to 10, as configured.

Note The MAC address is identified as a sticky MAC.

Sticky MAC addresses are added to the MAC address table and to the running configuration. As shown in Figure 3, the sticky MAC for PC2 has been added to the running configuration for S1.

Verify Secure MAC Addresses

To display all secure MAC addresses configured on all switch interfaces, or on a specified interface with aging information for each, use the **show port-security address** command. As shown in Figure 4, the secure MAC addresses are listed along with the types.

Refer to **Online Course** for Illustration

2.2.4.7 Ports in Error Disabled State

When a port is configured with port security, a violation can cause the port to become error disabled. When a port is error disabled, it is effectively shut down and no traffic is sent or received on that port. A series of port security related messages display on the console (Figure 1).

Note The port protocol and link status is changed to down.

The port LED will change to orange. The **show interfaces** command identifies the port status as **err-disabled** (Figure 2). The output of the **show port-security interface** command now shows the port status as **secure-shutdown**. Because the port security violation mode is set to `shutdown`, the port with the security violation goes to the error disabled state.

The administrator should determine what caused the security violation before re-enabling the port. If an unauthorized device is connected to a secure port, the port should not be re-enabled until the security threat is eliminated. To re-enable the port, use the **shutdown** interface configuration mode command (Figure 3). Then, use the **no shutdown** interface configuration command to make the port operational.

Refer to **Online Course** for Illustration

2.2.4.8 Network Time Protocol (NTP)

Having the correct time within networks is important. Correct time stamps are required to accurately track network events such as security violations. Additionally, clock synchronization is critical for the correct interpretation of events within syslog data files as well as for digital certificates.

Network Time Protocol (NTP) is a protocol that is used to synchronize the clocks of computer systems over packet-switched, variable-latency data networks. NTP allows network devices to synchronize their time settings with an NTP server. A group of NTP clients that

obtain time and date information from a single source will have more consistent time settings.

A secure method of providing clocking for the network is for network administrators to implement their own private network master clocks, synchronized to UTC, using satellite or radio. However, if network administrators do not wish to implement their own master clocks because of cost or other reasons, other clock sources are available on the Internet. NTP can get the correct time from an internal or external time source including the following:

- Local master clock
- Master clock on the Internet
- GPS or atomic clock

A network device can be configured as either an NTP server or an NTP client. To allow the software clock to be synchronized by an NTP time server, use the **ntp server** ip-address command in global configuration mode. A sample configuration is shown in the Figure 1. Router R2 is configured as an NTP client, while router R1 serves as an authoritative NTP server.

To configure a device as having an NTP master clock to which peers can synchronize themselves, use the **ntp master** [stratum] command in global configuration mode. The stratum value is a number from 1 to 15 and indicates the NTP stratum number that the system will claim. If the system is configured as an NTP master and no stratum number is specified, it will default to stratum 8. If the NTP master cannot reach any clock with a lower stratum number, the system will claim to be synchronized at the configured stratum number, and other systems will be willing to synchronize to it using NTP.

Figure 2 displays the verification of NTP. To display the status of NTP associations, use the **show ntp associations** command in privileged EXEC mode. This command will indicate the IP address of any peer devices that are synchronized to this peer, statically configured peers, and stratum number. The **show ntp status** user EXEC command can be used to display such information as the NTP synchronization status, the peer that the device is synchronized to, and in which NTP strata the device is functioning.

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

2.2.4.9 Packet Tracer - Configuring Switch Port Security

Background/Scenario

In this activity, you will configure and verify port security on a switch. Port security allows you to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port.

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

2.2.4.10 Packet Tracer - Troubleshooting Switch Port Security

Background/Scenario

The employee who normally uses PC1 brought his laptop from home, disconnected PC1 and connected the laptop to the telecommunication outlet. After reminding him of the security policy that does not allow personal devices on the network, you now must reconnect PC1 and re-enable the port.

Refer to **Lab Activity** for this chapter

2.2.4.11 Lab - Configuring Switch Security Features

In this lab, you will complete the following objectives:

- Part 1: Set Up the Topology and Initialize Devices
- Part 2: Configure Basic Device Settings and Verify Connectivity
- Part 3: Configure and Verify SSH Access on S1
- Part 4: Configure and Verify Security Features on S1

Refer to **Online Course** for Illustration

2.3 Summary

Refer to **Lab Activity** for this chapter

2.3.1.1 Class Activity – Switch Trio

Switch Trio

You are the network administrator for a small- to medium-sized business. Corporate headquarters for your business has mandated that on all switches in all offices, security must be implemented. The memorandum delivered to you this morning states:

"By Monday, April 18, 20xx, the first three ports of all configurable switches located in all offices must be secured with MAC addresses — one address will be reserved for the printer, one address will be reserved for the laptop in the office, and one address will be reserved for the office server.

If a port's security is breached, we ask you to shut it down until the reason for the breach can be certified.

Please implement this policy no later than the date stated in this memorandum. For questions, call 1.800.555.1212. Thank you. The Network Management Team"

Work with a partner in the class and create a Packet Tracer example to test this new security policy. After you have created your file, test it with, at least, one device to ensure it is operational or validated.

Save your work and be prepared to share it with the entire class.

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

2.3.1.2 Packet Tracer - Skills Integration Challenge

Background/Scenario

The network administrator asked you to configure a new switch. In this activity, you will use a list of requirements to configure the new switch with initial settings, SSH, and port security.

Refer to **Online Course** for Illustration

2.3.1.3 Summary

When a Cisco LAN switch is first powered on it goes through the following boot sequence:

1. First, the switch loads a power-on self-test (POST) program stored in ROM. POST checks the CPU subsystem. It tests the CPU, DRAM, and the portion of the flash device that makes up the flash file system.
2. Next, the switch loads the boot loader software. The boot loader is a small program stored in ROM and is run immediately after POST successfully completes.
3. The boot loader performs low-level CPU initialization. It initializes the CPU registers, which control where physical memory is mapped, the quantity of memory, and its speed.
4. The boot loader initializes the flash file system on the system board.
5. Finally, the boot loader locates and loads a default IOS operating system software image into memory and hands control of the switch over to the IOS.

The specific Cisco IOS file that is loaded is specified by the BOOT environmental variable. After the Cisco IOS is loaded it uses the commands found in the startup-config file to initialize and configure the interfaces. If the Cisco IOS files are missing or damaged, the boot loader program can be used to reload or recover from the problem.

The operational status of the switch is displayed by a series of LEDs on the front panel. These LEDs display such things as port status, duplex, and speed.

An IP address is configured on the SVI of the management VLAN to allow for remote configuration of the device. A default gateway belonging to the management VLAN must be configured on the switch using the **`ip default-gateway`** command. If the default gateway is not properly configured, remote management is not possible. It is recommended that Secure Shell (SSH) be used to provided a secure (encrypted) management connection to a remote device to prevent the sniffing of unencrypted user names and passwords which is possible when using protocols such as Telnet.

One of the advantages of a switch is that it allows full-duplex communication between devices effectively doubling the communication rate. Although it is possible to specify the speed and duplex settings of a switch interface, it is recommended that the switch be allowed to set these parameters automatically to avoid errors.

Switch port security is a requirement to prevent such attacks as MAC Address Flooding and DHCP Spoofing. Switch ports should be configured to allow only frames with specific source MAC addresses to enter. Frames from unknown source MAC addresses should be denied and cause the port to shut down to prevent further attacks.

Port security is only one defense against network compromise. There are 10 best practices that represent the best insurance for a network:

- Develop a written security policy for the organization.
- Shut down unused services and ports.
- Use strong passwords and change them often.
- Control physical access to devices.

- Avoid using standard insecure HTTP websites, especially for login screens. Instead use the more secure HTTPS.
- Perform backups and test the backed up files on a regular basis.
- Educate employees about social engineering attacks, and develop policies to validate identities over the phone, via email, and in person.
- Encrypt sensitive data and protect it with a strong password.
- Implement security hardware and software, such as firewalls.
- Keep IOS software up-to-date by installing security patches weekly or daily, if possible.

These methods are only a starting point for security management. Organizations must remain vigilant at all times to defend against continually evolving threats.

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

Chapter 2 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 2 Exam

The chapter exam assesses your knowledge of the chapter content.

Your Chapter Notes