Switched Networks

Companion Guide

Cisco | Networking Academy®
Mind Wide Open™

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Switched Networks

Companion Guide

Cisco Networking Academy

Cisco Press
800 East 96th Street
Indianapolis, Indiana 46240 USA

Switched Networks Companion Guide

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

Printed in the United States of America

First Printing May 2014

Library of Congress Control Number: 2014935305

ISBN-13: 978-1-58713-329-9

ISBN-10: 1-58713-329-6

Warning and Disclaimer

This book is designed to provide information about the 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.

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.

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Business Operation Manager, Cisco Press
Jan Cornelssen

Executive Editor
Mary Beth Ray

Managing Editor
Sandra Schroeder

Development Editor
Ellie C. Bru

Project Editor
Mandie Frank

Copy Editor
John Edwards

Technical Editor
Rick McDonald

Editorial Assistant
Vanessa Evans

Designer
Mark Shirar

Composition
Tricia Bronkella

Indexer
Ken Johnson

Proofreader
Debbie Williams

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.

Special Sales

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

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

For questions about sales outside the U.S., please contact international@pearsoned.com.

Feedback Information

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

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

We greatly appreciate your assistance.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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

About the Contributing Authors

Erich Spengler is the Director for the Center for System Security and Information Assurance, based at Moraine Valley CC. Erich is a Professor of Computer Integrated Technologies at Moraine Valley and has been teaching Cisco Academy courses for over 15 years. Erich is an ITQ-certified instructor for Cisco Academy. Erich is an active CISSP and has helped dozens of others earn the CISSP designation.

Erich has over 25 years of professional experience in IT systems and security. Erich's Center has trained over 1000 faculty since 2003 in VMware, CyberSecurity, Cisco, EMC, and Linux.

In his downtime, Erich enjoys spending time with his wife and two daughters.

Wayne Lewis wears three hats: Cisco Academy Manager for the Pacific Center for Advanced Technology Training, NetAcad Contact for the Central Pacific Academy Support and Instructor Training Center, and Professor at Honolulu Community College. Okay . . . four hats: Wayne teaches calculus, linear algebra, and differential equations at the University of Hawaii at Manoa.

Honolulu CC has been an instructor training center for Cisco Academy since 1998, and its instructors are responsible for training many of the initial cohorts of Cisco Academy instructors in countries throughout Asia, Europe, and the Americas. Wayne has been involved in curriculum development and assessment for Cisco Academy since 1999.

Wayne spends his free time doing math (representation theory, algebraic geometry, and several complex variables) and watching marathon sessions of TV series with his family (their favorites to rewatch are South Park, The Office, Monty Python, and Lost).

Dedications

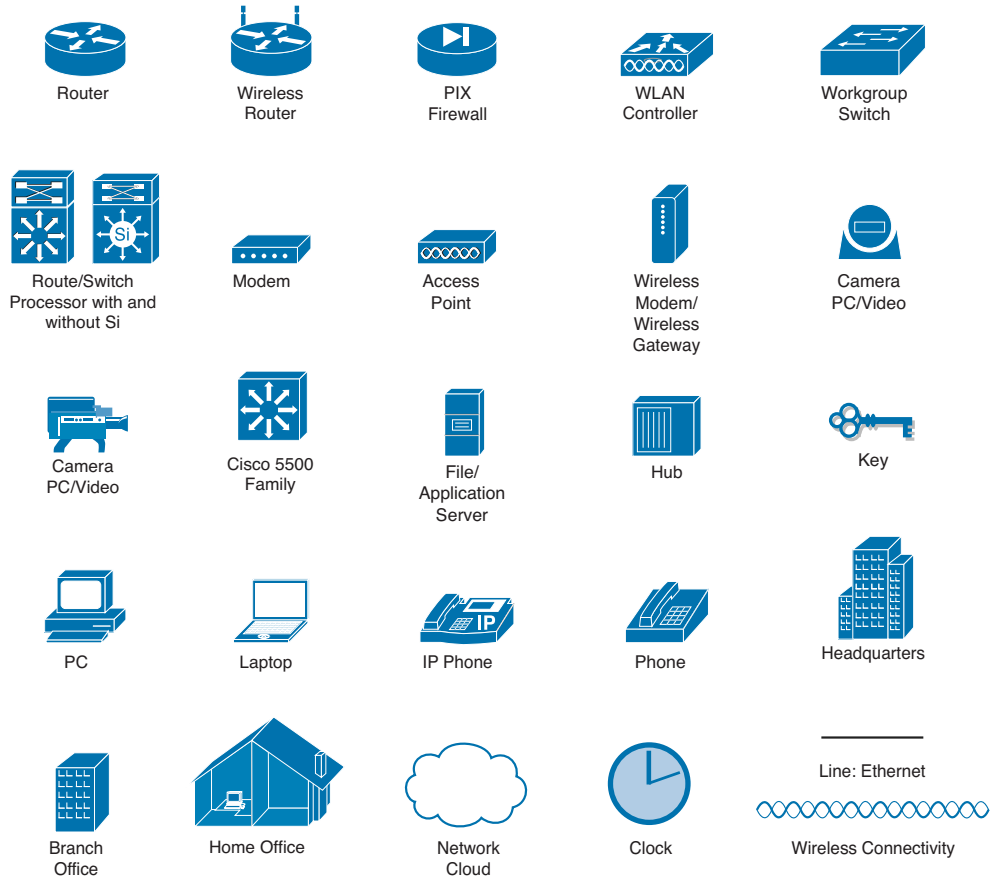
From Erich:
To my wife, Kristi, and daughters, Emily and Lauren, for all your love and support . . . for always doing your best and making me the proudest husband and father in the world.

From Wayne:
To my wife, Leslie, and daughters, Christina and Lenora, for making it all worthwhile.

Contents at a Glance

Contents

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).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

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

As a textbook, this book provides a ready reference to explain the same networking concepts, technologies, protocols, and devices as the online curriculum. This book emphasizes key topics, terms, and activities and provides some alternate explanations and examples as compared with the course. You can use the online curriculum as directed by your instructor and then use this Companion Guide's study tools to help solidify your understanding of all the topics.

Who Should Read This Book

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

Book Features

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

Topic Coverage

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

- **Objectives:** Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives stated in the corresponding chapters of the online curriculum; however, the question format

in the Companion Guide encourages you to think about finding the answers as you read the chapter.

- **"How-to" feature:** When this book covers a set of steps that you need to perform for certain tasks, the text lists the steps as a how-to list. When you are studying, the icon helps you easily refer to this feature as you skim through the book.
- **Notes:** These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.
- **Chapter summaries:** At the end of each chapter is a summary of the chapter's key concepts. It provides a synopsis of the chapter and serves as a study aid.
- **Practice:** At the end of chapter there is a full list of all the Labs, Class Activities, and Packet Tracer Activities to refer back to for study time.

Readability

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

- **Key terms:** Each chapter begins with a list of key terms, along with a page-number reference from inside the chapter. The terms are listed in the order in which they are explained in the chapter. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The Glossary defines all the key terms.
- **Glossary:** This book contains an all-new Glossary with more than 300 terms.

Practice

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

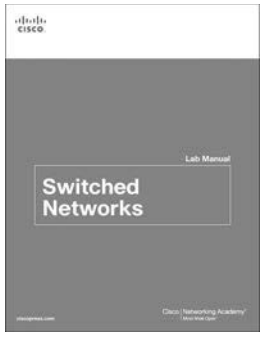
- **Check Your Understanding questions and answer key:** Updated review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. Appendix A, "Answers to 'Check Your Understanding' Questions," provides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

- **Labs and activities:** Throughout each chapter, you will be directed back to the online course to take advantage of the activities created to reinforce concepts. In addition, at the end of each chapter, there is a "Practice" section that collects a list of all the labs and activities to provide practice with the topics introduced in the chapter. The labs and class activities are available in the companion *Switched Networks Lab Manual* (ISBN 978-1-58713-3275). The Packet Tracer Activities PKA files are found in the online course.

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

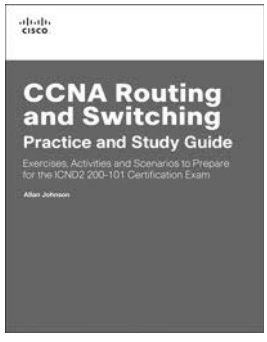
Lab Manual

The supplementary book *Switched Networks Lab Manual*, by Cisco Press (ISBN 978-1-58713-327-5), contains all the labs and class activities from the course.



Practice and Study Guide

Additional Study Guide exercises, activities, and scenarios are available in *CCNA Routing and Switching Practice and Study Guide* (ISBN 978-158713-344-2), by Allan Johnson. The Practice and Study Guide coordinates with the recommended curriculum sequence. The CCNA edition follows the course outlines for *Scaling Networks* and *Connecting Networks*.



About Packet Tracer Software and Activities

Packet Tracer Activity

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

How This Book Is Organized

This book corresponds closely to the Cisco Networking Academy Connecting Networks course and is divided into eight chapters, one appendix, and a glossary of key terms:

- **Chapter 1, "Introduction to Switched Networks":** The role of switched networks in computer networking is examined. LAN design principles are introduced, emphasizing converged networks and features that differentiate switches. Frame-forwarding methods, MAC address table theory, and types of switching domains are explored.
- **Chapter 2, "Basic Switching Concepts and Configuration":** Navigating configuration modes on Cisco switches and performing switch system administration are explored. Port configuration and basic switch security options are introduced.
- **Chapter 3, "VLANs":** VLANs differentiate switches from other networking devices. The various types of VLANs are defined. VLAN trunking theory and configuration are carefully introduced. Security solutions specific to VLANs are explored.
- **Chapter 4, "LAN Redundancy":** Examines the benefits and implementations of Spanning Tree Protocols and First Hop Redundancy Protocols.
- **Chapter 5, "Link Aggregation":** Describes the characteristics, benefits, and implementations of EtherChannel, with PAgP and LACP.
- **Chapter 6, "Inter-VLAN Routing":** Introduces the three major types of inter-VLAN routing: legacy, router-on-a-stick, and multilayer switching. Some new features of Cisco Layer 2 switches related to Layer 3 behavior are explored.
- **Chapter 7, "DHCP":** Describes DHCPv4 and DHCPv6 in great detail. The DHCPv6 content is new to CCNA.

- **Chapter 8, "Wireless LANs":** This chapter goes into considerable detail introducing and analyzing wireless LAN solutions. Topics include wireless LAN operation, wireless LAN security, and wireless LAN configuration.
- **Appendix A, "Answers to 'Check Your Understanding' Questions":** This appendix lists the answers to the "Check Your Understanding" review questions that are included at the end of each chapter.
- **Glossary:** The glossary provides you with definitions for all the key terms identified in each chapter.

This page intentionally left blank

CHAPTER 1

Introduction to Switched Networks

Objectives

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

- How do you describe the convergence of data, voice, and video in the context of switched networks?
- How do you describe a switched network in a small- to medium-sized business?
- How do you explain the process of frame forwarding in a switched network?
- How do you compare a collision domain to a broadcast domain?

Key Terms

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

Converged network *page 3*

Call control *page 6*

Voice messaging *page 6*

Mobility *page 6*

Automated attendant *page 6*

Cisco Borderless Network *page 6*

Hierarchical *page 8*

Modularity *page 8*

Resiliency *page 8*

Flexibility *page 8*

Access *page 8*

Distribution *page 8*

Core *page 8*

Form factor *page 11*

Fixed configuration switch *page 14*

Modular configuration switch *page 14*

Stackable configuration switch *page 15*

Traffic flow analysis *page 16*

Multilayer switch *page 16*

Port density *page 17*

Small form-factor pluggable (SFP) *page 18*

Forwarding rate *page 19*

Power over Ethernet (PoE) *page 19*

Frame forwarding *page 23*

Ingress port *page 24*

Egress port *page 25*

MAC address table *page 25*

Store-and-forward switching *page 29*

Cut-through switching *page 29*

Fragment free switching *page 31*

Collision domain *page 32*

Broadcast domain *page 32*

Introduction (1.0.1.1)

Modern networks continue to evolve to keep pace with the changing way that 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 that LAN switches build forwarding tables and use the MAC address information to efficiently switch data between hosts.

Class Activity 1.0.1.2: Sent or Received Instructions

Individually, or in groups (per the instructor's decision), discuss various ways that 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.

LAN Design (1.1)

In this section, you will explore the design of local-area networks. The Cisco Borderless Network architecture for delivery of services and applications provides a setting for the exploration of switched network design. And you will learn how the fundamental core-distribution-access model applies to switched networks.

Converged Networks (1.1.1)

Converged networks were cutting edge ten years ago, but now they are standard fare for switched environments. The integration of voice, video, and data on a switched infrastructure provides a seamless experience for users. IP phones and video devices are fully integrated into the data network.

Growing Complexity of Networks (1.1.1.1)

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. 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 1-1 illustrates legacy telephone equipment. A business site can 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.

Figure 1-1 Legacy Components

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 1-2 illustrates some of the newer platforms for converged networks that help to provide access to the network anytime, anywhere, and on any device.

Figure 1-2 Converged Network Components

Elements of a Converged Network (1.1.1.2)

To support collaboration, business networks employ converged solutions using voice systems, IP phones, voice gateways, video support, and videoconferencing, as illustrated in Figure 1-3.

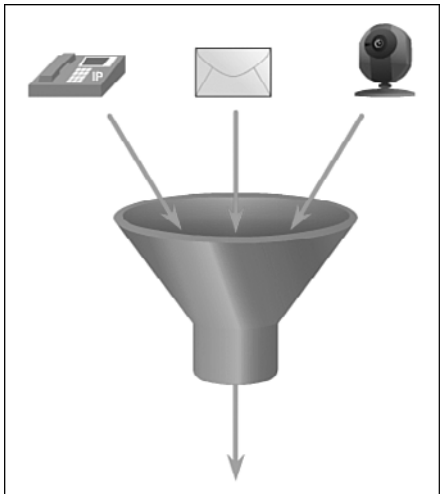


Figure 1-3 Many Types of Traffic on One Network

Including data services, a converged network with collaboration support can 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 superhighway 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.

Video

Video 1.1.1.2: Observing Spanning Tree Protocol Operation

Go to the online course and play the video in the second graphic to view a few of the collaboration services in action.

Cisco Borderless Network (1.1.1.3)

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 1-4. 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 allows users to access resources from any place at any time, while providing optimization, scalability, and security.

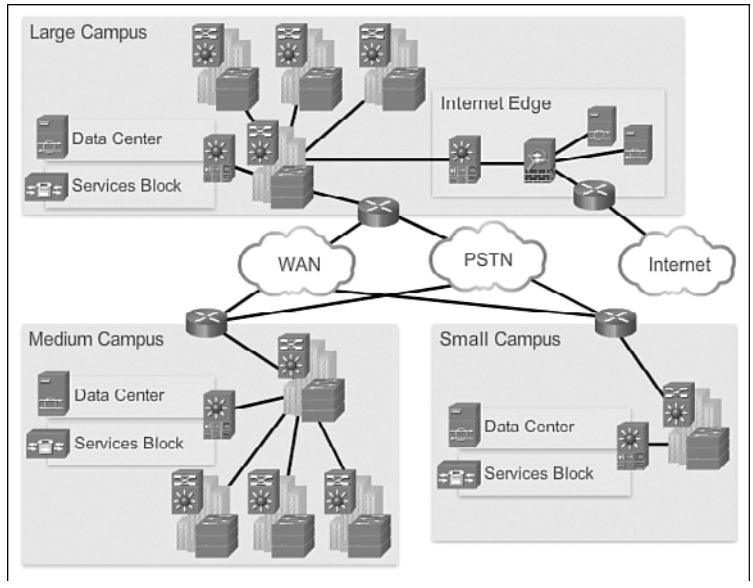


Figure 1-4 Cisco Borderless Network

Video

Video 1.1.1.3: Observing Spanning Tree Protocol Operation

Go to the online course and play the video in the second graphic to learn more about the evolution of the borderless network.

Hierarchy in the Borderless Switched Network (1.1.1.4)

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 model, as shown in Figure 1-5, and the two-tier layer model, as shown in Figure 1-6.

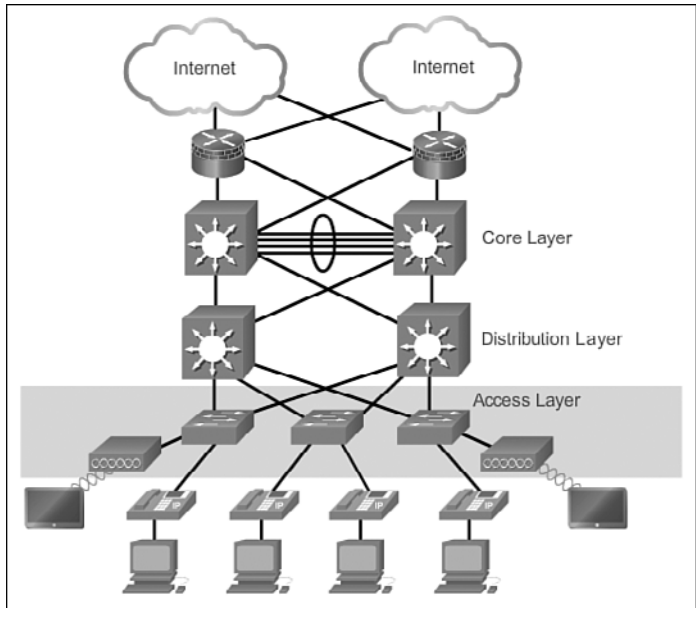


Figure 1-5 Access Layer

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.

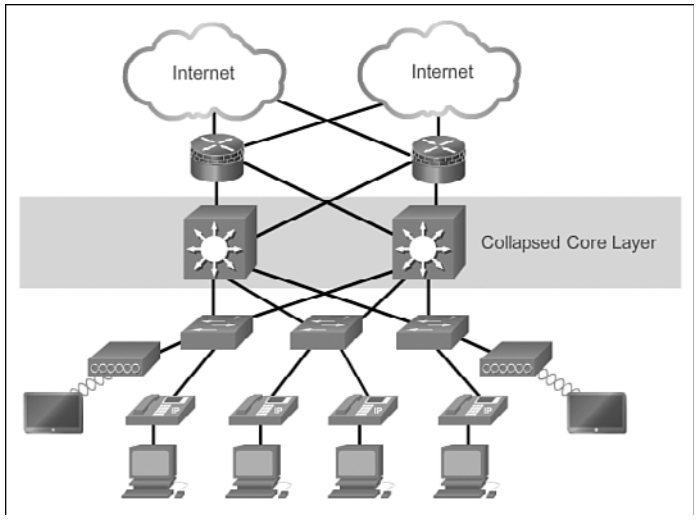


Figure 1-6 Collapsed Core

Access, Distribution, and Core Layers (1.1.1.5)

The access-distribution-core hierarchical network model is the most referenced network model in computer networking. It is simple, but it carries the rudimentary information necessary to convey networking concepts in context.

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 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 1-7 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.

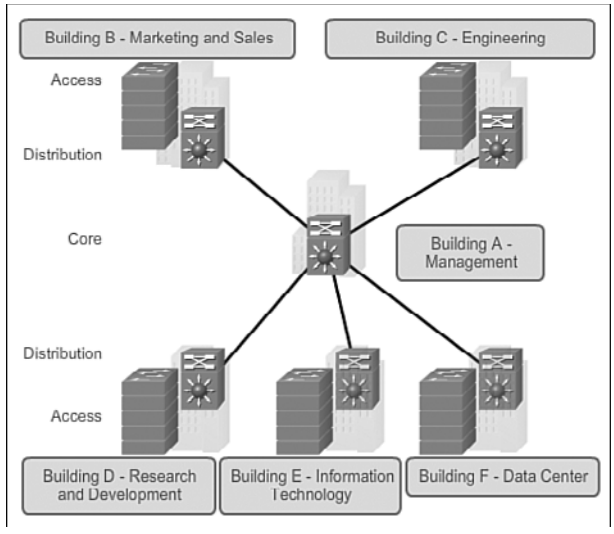


Figure 1-7 Three-Tier Campus Network Design

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 might 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 1-8 shows a two-tier campus network design example for an enterprise campus where the distribution and core layers are collapsed into a single layer.

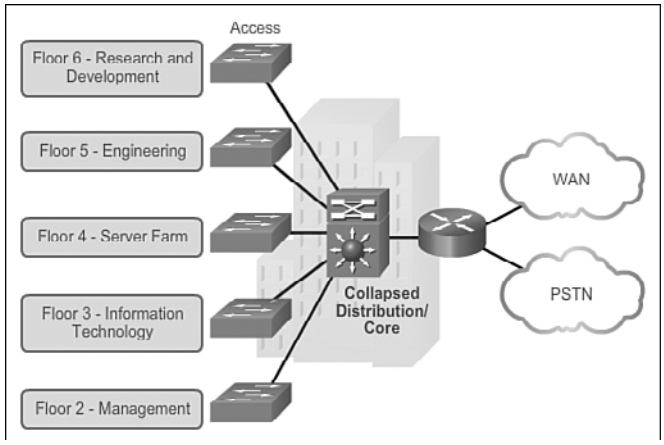


Figure 1-8 Two-Tier Campus Network Design

Interactive Graphic

Activity 1.1.1.6: Identify Switched Network Terminology

Go to the online course to perform this practice activity.

Switched Networks (1.1.2)

In this topic, you will learn about the various types of switches and their *form factors*. A discussion of multilayer switching will put in context our exploration of access layer switches, which are the focus of this course.

Role of Switched Networks (1.1.2.1)

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 1-9, networks have fundamentally changed to switched LANs in a hierarchical network.

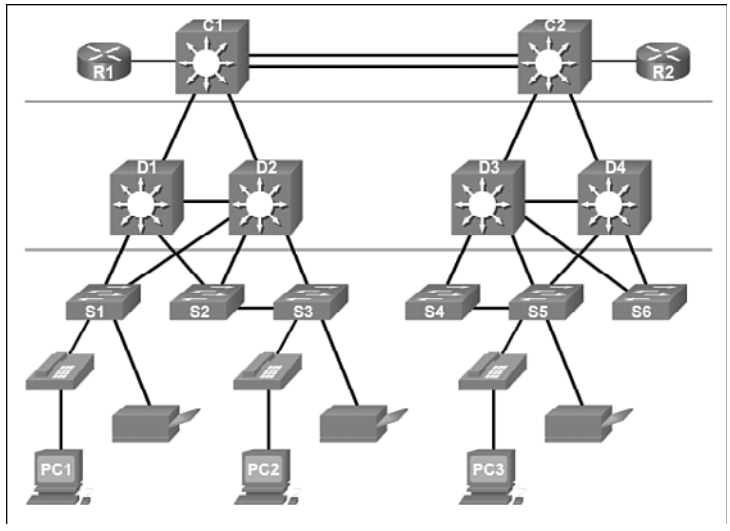


Figure 1-9 Hierarchical Networks

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 1-10 shows the hierarchical design used in the borderless switched network.

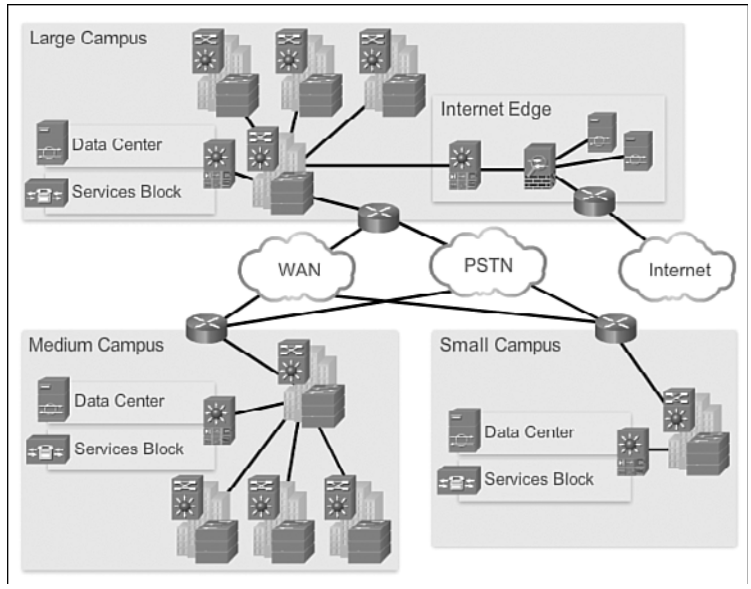


Figure 1-10 Borderless Switched Network

Form Factors (1.1.2.2)

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

- **Cost:** The cost of a switch will depend on the number and speed of the interfaces, supported features, and expansion capability.
- **Port Density:** Network switches must support the appropriate number of devices on the network.
- **Power:** It is now common to power access points, IP phones, and even compact switches using Power over Ethernet (PoE). In addition to PoE considerations, some chassis-based switches support redundant power supplies. PoE will be explored in Section 1.1.3.3.
- **Reliability:** The switch should provide continuous access to the network.
- **Port Speed:** The speed of the network connection is of primary concern to end users.
- **Frame Buffers:** The ability of the switch to store frames is important in a network where there might be congested ports to servers or other areas of the network.

- **Scalability:** The number of users on a network typically grows over time; therefore, the switch should provide the opportunity for growth.

When selecting the type of switch, the network designer must choose between a fixed or a modular configuration, and stackable or nonstackable. 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 1-11 are all 1 rack unit (1U). These options are sometimes referred to as switch form factors.

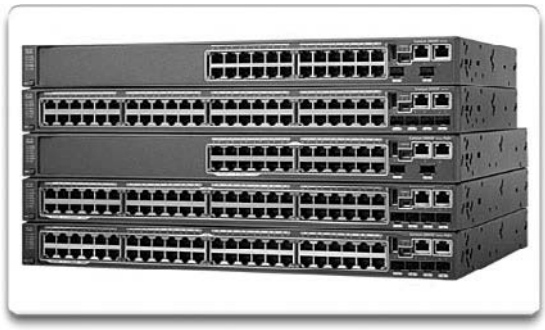


Figure 1-11 Fixed Configuration Switches

Fixed Configuration Switches

Fixed configuration switches do not support features or options beyond those that originally came with the switch. The particular model determines the features and options available; features and options are limited to those that originally come with the switch. 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, as shown in Figure 1-12. 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.

Figure 1-12 Modular Switches

Stackable Configuration Switches

Stackable configuration switches can be interconnected using a special cable that provides high-bandwidth throughput between the switches, as shown in Figure 1-13. 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.

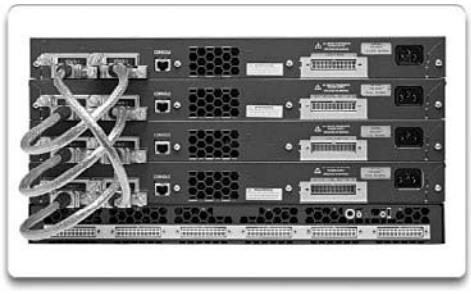


Figure 1-13 Stackable Switches

Traffic Flow (1.1.2.3)

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 might 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.

Multilayer Switching (1.1.2.4)

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

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

The Catalyst 2960 switches shown in Figure 1-14 illustrate the migration to a pure Layer 3 environment. With IOS Releases prior to 15.x, these switches supported only one active switched virtual interface (SVI). With IOS Release 15.x, these switches now support multiple active SVIs, as well as support for static routes! This means that the switch can be remotely accessed through multiple IP addresses on distinct networks.

Figure 1-14 Cisco Catalyst 2960 Series Switches

Packet Tracer Activity

Packet Tracer Activity 1.1.2.5: Comparing 2960 and 3560 Switches

In this activity, you will use various commands to examine three different switching topologies and compare the similarities and differences between the 2960 and 3560 switches. You will also compare the routing table of a 1941 router with a 3560 switch.

Switch Features (1.1.3)

Relative to routers, the features associated with a switch or a product line of switches vary dramatically. It is important for a switch administrator to understand the features available so that well-informed switch-purchasing decisions are made for an organization.

Port Density (1.1.3.1)

The *port density* of a switch refers to the number of ports available on a single switch. Figure 1-15 shows the port density of three different switches.

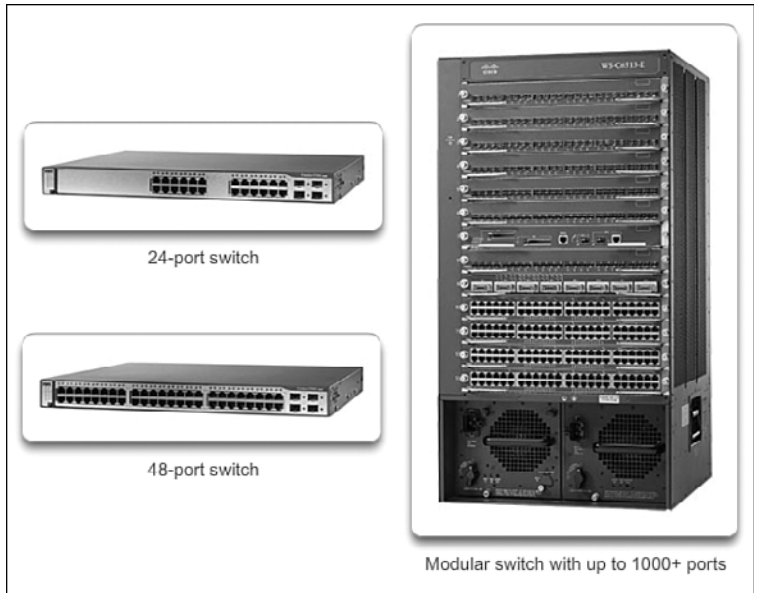


Figure 1-15 Port Densities

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

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

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

The network designer must also consider the issue of uplink bottlenecks. For example, to achieve target performance, a series of fixed configuration switches might 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.

Forwarding Rates (1.1.3.2)

Forwarding rates define the processing capabilities of a switch by rating how much data the switch can process per second. Switch product lines are classified by forwarding rates, as shown in Figure 1-16. 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.

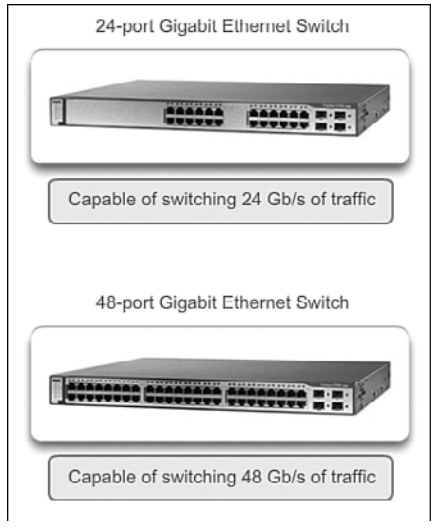


Figure 1-16 Forwarding Rate

Power over Ethernet (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. The highlighted devices in Figure 1-17 have PoE ports.

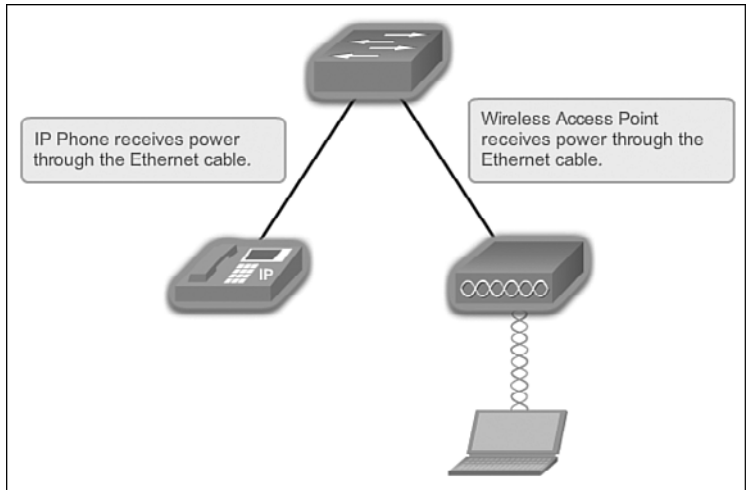


Figure 1-17 Power over Ethernet

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. The highlighted switch in Figure 1-18 represents a Cisco Catalyst 2960-C.

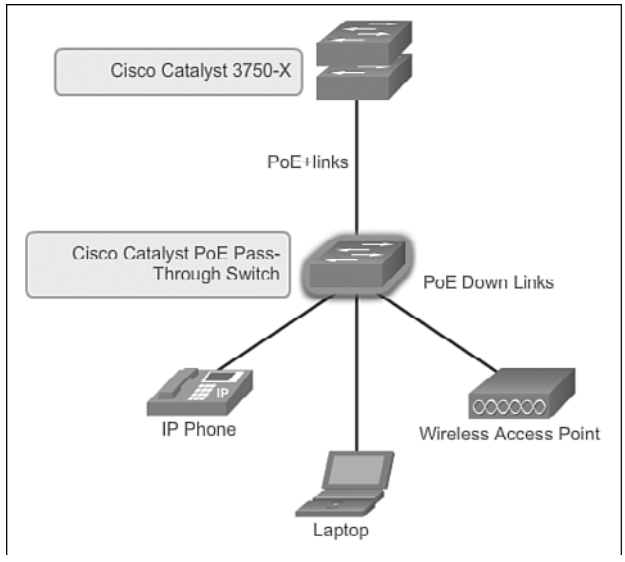


Figure 1-18 PoE Pass-Through

Cisco Catalyst Switch Breakdown (1.1.3.4)

While switches can be categorized in various ways, Cisco Catalyst switches are usually described in terms of the core-distribution-access hierarchy, as shown in Figure 1-19. 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.

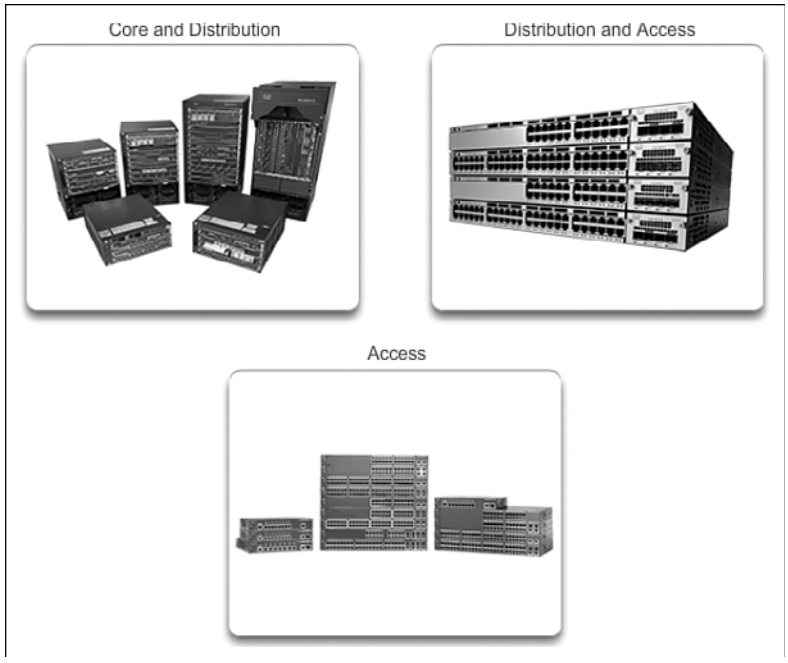


Figure 1-19 Switches in the Hierarchical Design Model

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-terabits-per-second 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 operate 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 and 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 that 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 that 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.

Interactive Graphic

Activity 1.1.3.5: Identify Switch Hardware

Go to the online course to perform this practice activity.

Lab 1.1.3.6: Selecting Switch 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

The Switched Environment (1.2)

In this section you learn about *frame forwarding* of LAN switches and the role of broadcast domains and collision domains in a switched environment.

Frame Forwarding (1.2.1)

Computer networking is enabled by switching. Often people make the mistake of thinking that switching is specific to LANs. In reality, switching is a generic concept that applies to any networking device with interfaces on it. Switching in a generic sense refers only to the use of some sort of table to instruct a networking device what port to use to send out a packet based on the port in which the packet entered, coupled with specific information embedded in the packet. It really is up to your imagination what a generic switch might use to switch packets; it comes down to the set of rules used to build the table.

Switching as a General Concept in Networking and Telecommunications (1.2.1.1)

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*
- Some sort of address embedded in the frames or packets processed by the device

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 LAN 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. In Table 1-1, you see the information that a generic LAN switch might use to forward Ethernet frames.

Table 1-1 Generic LAN Switch

Port Table	
Destination Address	**Port**
EE	1
AA	2
BA	3
EA	4
AC	5
AB	6

With Table 1-1, the following conclusions can be made:

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

Dynamically Populating a Switch MAC Address Table (1.2.1.2)

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 that 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 in Figure 1-20.

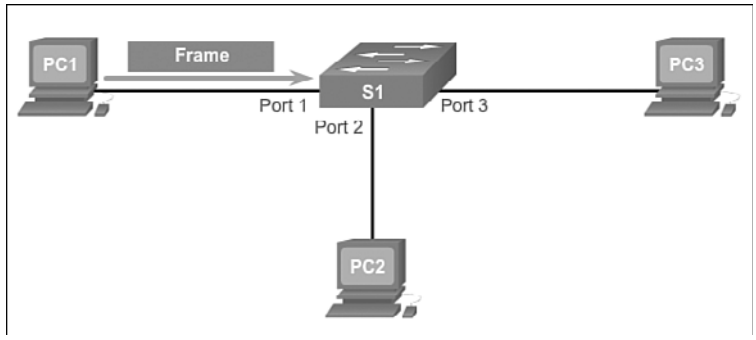


Figure 1-20 Receipt of a Frame

2. The switch examines the source MAC address and compares it to the 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, as shown in Figure 1-21.
   - 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.

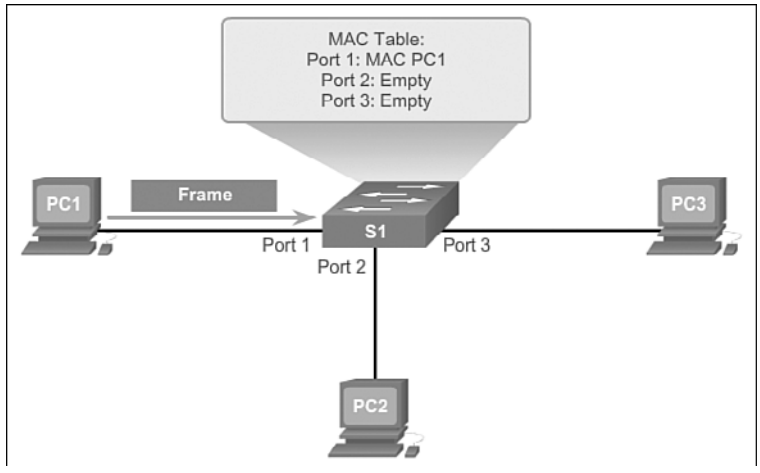


Figure 1-21 Parse Source MAC Address Against MAC Address Table

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, as shown in Figure 1-22.

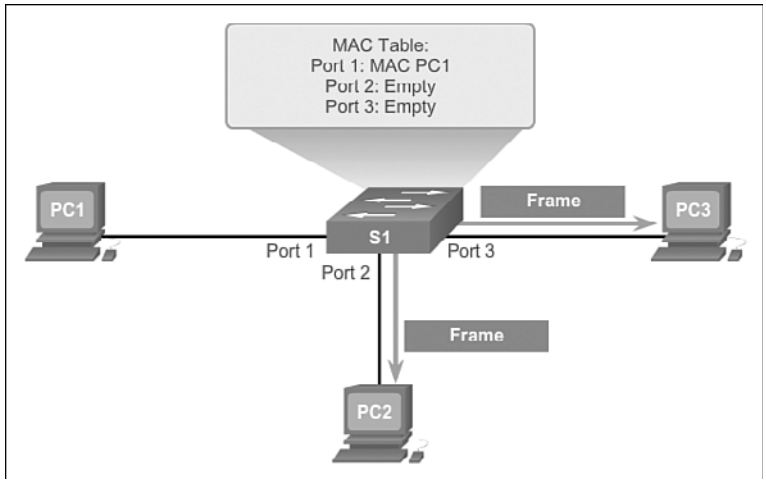


Figure 1-22 Switch Forwards Frame Out All Ports If Destination Is Not in MAC Address Table

4. The destination device (PC 3) replies to the frame with a unicast frame addressed to PC 1, as shown in Figure 1-23.

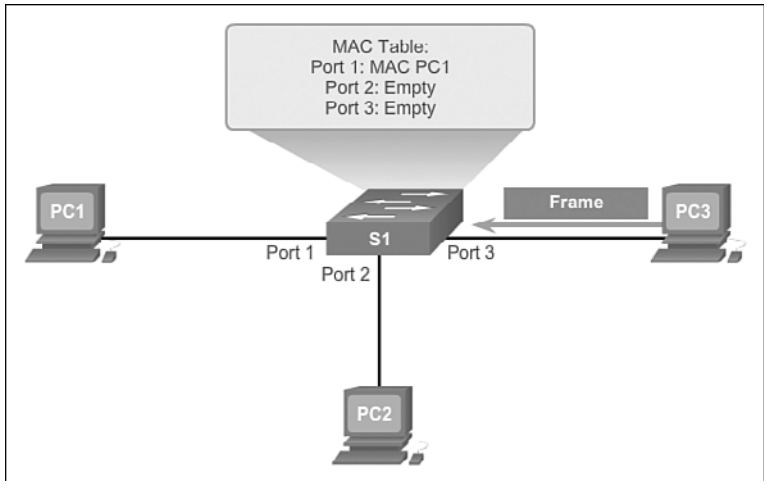


Figure 1-23 Frame Recipient Replies with Unicast Frame

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 are found in the MAC address table, as shown in Figure 1-24.

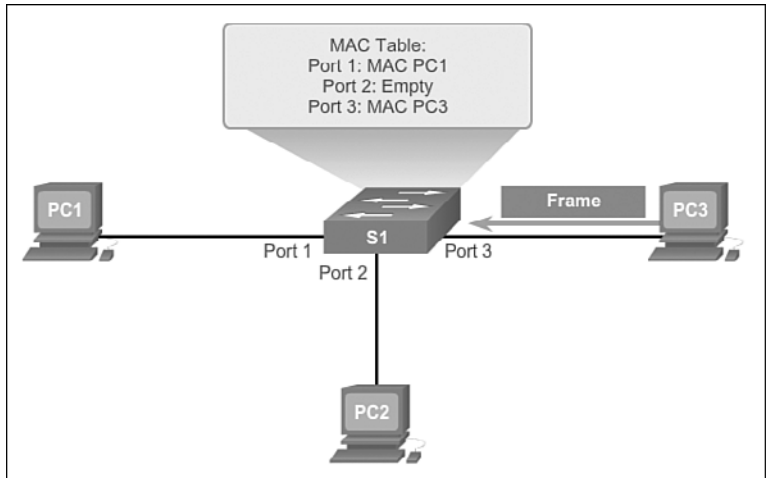


Figure 1-24 Switch Populates MAC Address Table with New Source MAC Address

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, as shown in Figure 1-25.

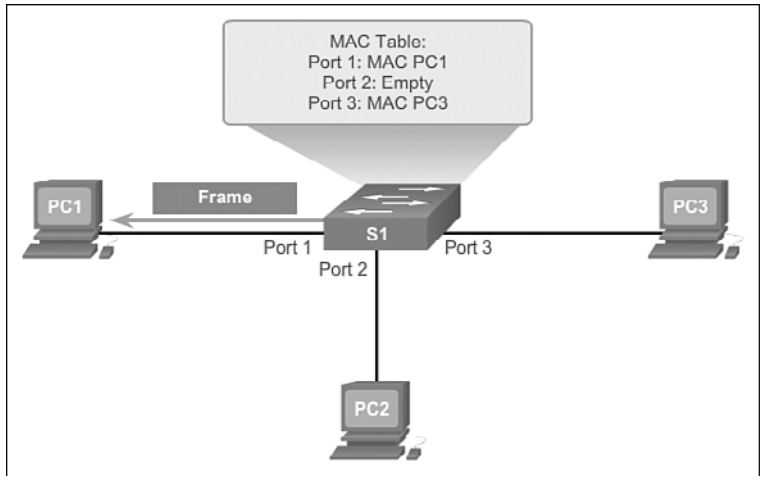


Figure 1-25 Switch Forwards Frame Out All Ports Associated with Original Sender

Switch Forwarding Methods (1.2.1.3)

As networks grew and enterprises began to experience slower network performance, Ethernet bridges (early versions of a switch) were added to networks to limit the size of the collision domains. In the 1990s, advancements in integrated circuit technologies allowed 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 (ASIC). 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***. These switching methods are explored in this section.

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). The CRC was invented by Wesley Peterson at IBM in 1961.

By contrast, the cut-through frame forwarding method begins the forwarding process after the destination MAC address of an incoming frame and the egress port have been determined.

Store-and-Forward Switching (1.2.1.4)

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 Figure 1-26, 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.

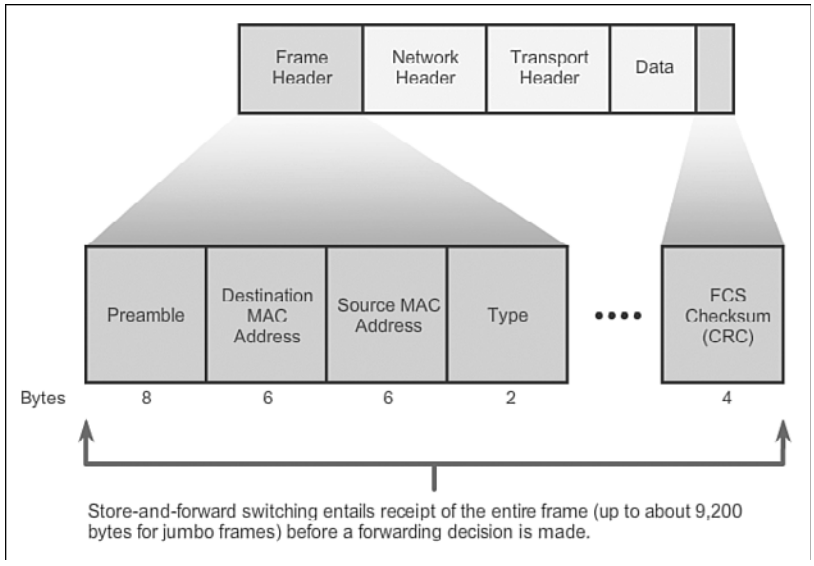


Figure 1-26 Store-and-Forward Switching

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 and therefore does not forward invalid frames. By contrast, a cut-through switch can forward invalid frames because no FCS check is performed.

Cut-Through Switching (1.2.1.5)

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 Figure 1-27, 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.

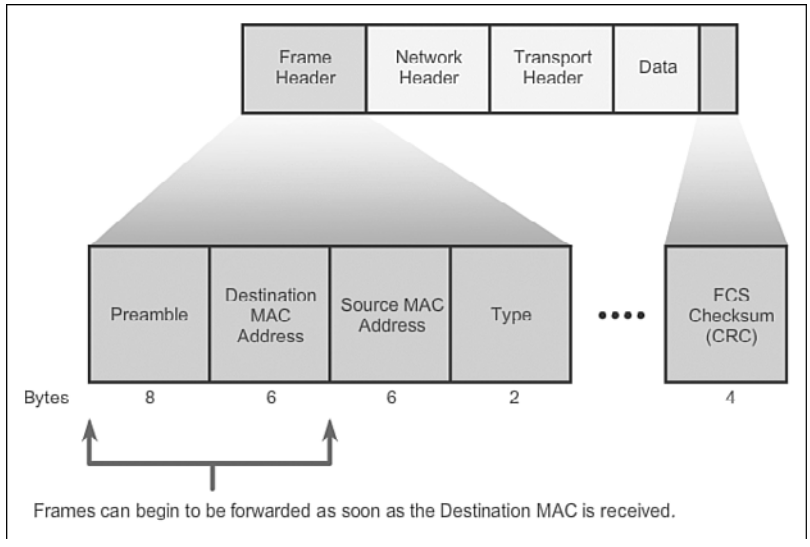


Figure 1-27 Cut-Through Switching

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, the destination MAC address, and the EtherType fields) and examine an additional 40 bytes 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 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 that each frame will be checked into the data field to make sure that 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.

Interactive Graphic

Activity 1.2.1.6: Frame Forwarding Methods

Go to the online course to perform this practice activity.

Interactive Graphic

Activity 1.2.1.7: Switch It!

Go to the online course to perform this practice activity.

Switching Domains (1.2.2)

Access switches determine collision domains. Routers and multilayer switches determine broadcast domains. However, VLANs coincide with broadcast domains in a switched environment, so access switches also contribute to the determination of broadcast domains. In this topic, you will explore the relationship between collision domains and broadcast domains.

Collision Domains (1.2.2.1)

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 can occur.

It is possible, however, to use a switch device, operating at 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 Figure 1-28, each switch port connects to a single PC or server, and each switch port represents a separate collision domain.

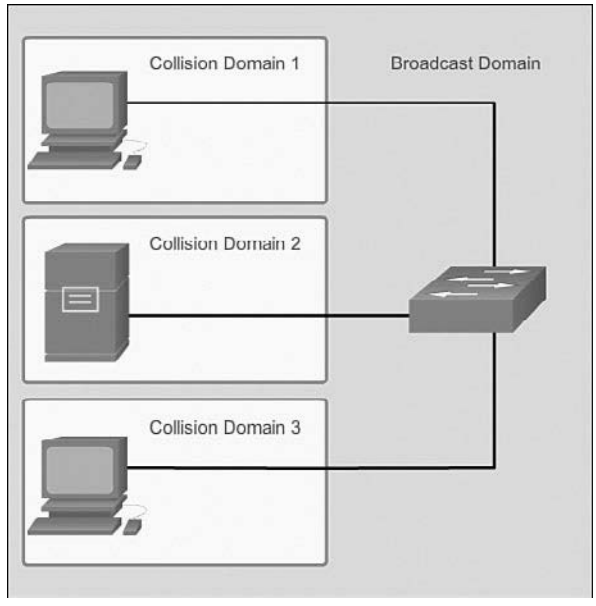


Figure 1-28 Collision Domains and Broadcast Domains

Broadcast Domains (1.2.2.2)

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 1s. A frame with a destination MAC address of all binary 1s, or all Fs in hexadecimal, 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.

Video

Video 1.2.2.2: Broadcast Domains I

Go to the online course and view 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 slowdown in the network performance.

When two switches are connected together, the broadcast domain is increased.

Video

Video 1.2.2.2: Broadcast Domains II

Go to the online course and view 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.

Alleviating Network Congestion (1.2.2.3)

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 can 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 might be congested ports to servers or other parts of the network.
- **Port speed:** Depending on the cost of a switch, it might 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 can 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.

Interactive Graphic

Activity 1.2.2.4: Circle the Domain

Go to the online course to perform this practice activity.

Summary (1.3)

Class Activity 1.3.1.1: 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 one or two PCs
- One instructor end device, preferably represented by a server
- Stream video presentations over a 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 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.

Interactive Graphic

Activity 1.3.1.2: Basic Switch Configurations

Go to the online course to use the Syntax Checker to perform basic switch configurations.

Packet Tracer Activity

Packet Tracer Activity 1.3.1.3: Skills Integration Challenge

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

We have seen that the trend in networks is toward 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 provide 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 is 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 nonstackable. Another consideration is the thickness of the switch, which is expressed in number of rack units. A network administrator might 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, the switch must first use the source MAC address of incoming frames to build 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 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.

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion *Switched Networks Lab Manual* (ISBN 978-1-58713-372-5). The Packet Tracer Activities PKA files are found in the online course.

Class Activities

- Class Activity 1.0.1.2: Sent or Received Instructions
- Class Activity 1.3.1.1: It's Network Access Time

Labs

- Lab 1.1.3.6: Selecting Switch Hardware

Packet Tracer Activities

- Packet Tracer Activity 1.1.2.5: Comparing 2960 and 3560 Switches

Check Your Understanding Questions

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

1. What are the layers of the switch hierarchical design model? (Choose three.)

   A. Access
   B. Data link
   C. Core
   D. Network access
   E. Enterprise
   F. Distribution

2. Which of the following characteristics describe a converged network? (Choose two.)

   A. Support of voice and video, both using the same switch
   B. Separate wiring infrastructure for voice and video traffic
   C. Affordability for small and medium businesses
   D. Cheaper equipment cost

3. When an appropriate switch form factor for a network is being determined, what should be selected when fault tolerance and bandwidth availability are desired but the budget is limited?

   A. Stackable switch
   B. Nonstackable switch
   C. Fixed configuration switch
   D. Modular switch

4. Which cost-effective physical network topology design is recommended when building a three-tier campus network that connects three buildings?

   A. Bus
   B. Mesh
   C. Extended star
   D. Dual-ring

5. When the appropriate switch form factor for a network is being determined, what type of switch should be selected when future expansion is important and cost is not a limiting factor?

   A. Stackable switch
   B. 1-rack-unit switch
   C. Fixed configuration switch
   D. Modular switch

6. Fill in the blank. The technology that allows a switch to deliver power to a device like an IP phone or an access point through the data cable is known as _____.

7. Which of the following statements about Layer 2 Ethernet switches are true? (Choose two.)

   A. Layer 2 switches prevent broadcasts.
   B. Layer 2 switches have multiple collision domains.
   C. Layer 2 switches route traffic between different networks.
   D. Layer 2 switches decrease the number of broadcast domains.
   E. Layer 2 switches can send traffic based on the destination address.

8. A network administrator is researching enterprise-level switches to upgrade the network infrastructure. Which switching feature defines the overall amount of data that the switch can process each second?

   A. Forwarding rate
   B. Wire speed
   C. PoE
   D. Port density

9. Which option best describes a switching method?

   A. Cut-through: makes a forwarding decision after receiving the entire frame
   B. Store-and-forward: forwards the frame immediately after examining its destination MAC address
   C. Cut-through: provides the flexibility to support any mix of Ethernet speeds
   D. Store-and-forward: ensures that the frame is free of physical and data-link errors

10. Which service is provided by an automated attendant feature on a converged network?

    A. Point-to-point video
    B. Call routing
    C. IT management interface
    D. Videoconferencing

11. A medium-sized company wants to add IP phones to its network. Should it consider buying a switch that supports PoE?

    A. Yes, because PoE increases port density.
    B. Yes, because PoE provides more flexibility in placing IP phones.
    C. No, because PoE has no effect on the use of VoIP devices on a network.
    D. Yes, because PoE adds Layer 3 functionality to a switch.

12. Which switching mode describes a switch that transfers a frame as soon as the destination MAC address is read?

A. Fragment free
B. Cut-through
C. Store-and-forward
D. Latency forwarding

CHAPTER 2

Basic Switching Concepts and Configuration

Objectives

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

- How do you configure the initial settings on a Cisco switch?
- How do you configure switch ports to meet network requirements?
- How do you configure the management VLAN switch virtual interface?
- How do you describe basic security attacks in a switched environment?
- How do you describe security best practices in a switched environment?
- How do you configure the port security feature to restrict network access?

Key Terms

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

Port security *page 42*

Secure Shell (SSH) *page 59*

DHCP snooping *page 59*

MAC address flooding *page 66*

DHCP starvation attack *page 69*

Denial of service (DoS) *page 69*

Cisco Discovery Protocol (CDP) *page 70*

Brute force password attack *page 71*

Best practices *page 72*

Security audit *page 74*

Penetration testing *page 74*

Secure MAC address *page 77*

Static secure MAC address *page 77*

Dynamic secure MAC address *page 78*

Sticky secure MAC address *page 78*

Violation mode *page 79*

Protect *page 79*

Restrict *page 79*

Shutdown *page 79*

Error disabled *page 83*

Network Time Protocol (NTP) *page 85*

Introduction (2.0.1.1)

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.

Access layer 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 high-speed connections. *Port security* is one of the security features that Cisco-managed switches provide.

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

Class Activity 2.0.1.2: 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

The student 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.

Basic Switch Configuration (2.1)

Basic switch administration should be mastered by a switch administrator. This includes familiarity with the hardware as well as basic port configuration.

Configure a Switch with Initial Settings (2.1.1)

In this section, you learn the Cisco switch boot sequence, how to recover from a system crash, and how to configure the switch to support remote management.

Switch Boot Sequence (2.1.1.1)

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

1. 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. The switch loads the boot loader software. The boot loader is a small program stored in ROM and is run immediately after the 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. 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 Figure 2-1, 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 to what the current IOS boot file is set.

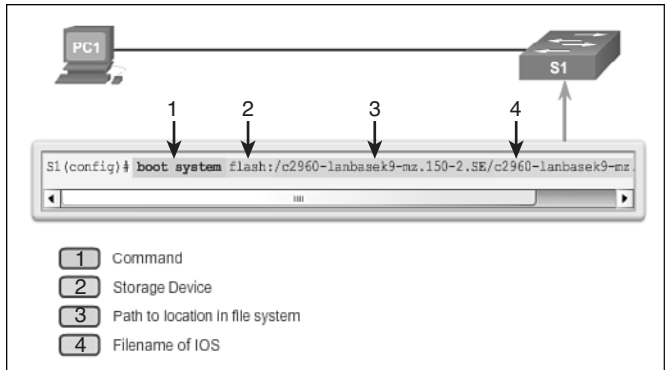


Figure 2-1 Configure BOOT Environment Variable

Recovering From a System Crash (2.1.1.2)

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:

How To

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

Step 2. Unplug the switch power cord, because many Cisco switches do not have an on/off switch.

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 Figure 2-2.

```
Switch# dir flash:
Directory of flash:/

    2   rwx    11607161   Mar 1 2013 03:10:47 +00:00  c2960
lanbasek9-mz.150-2.SE.bin
    3  -rwx        1809   Mar 1 2013 00:02:48 +00:00  config.text
    5  -rwx        1919   Mar 1 2013 00:02:48 +00:00  private-
config.text
    6  -rwx       59416   Mar 1 2013 00:02:49 +00:00  multiple-fs

32514048 bytes total (20841472 bytes free)
Switch#
```

Figure 2-2 Directory Listing in Boot Loader

Note

In this example, the IOS is located in the root of the flash folder.

Switch LED Indicators (2.1.1.3)

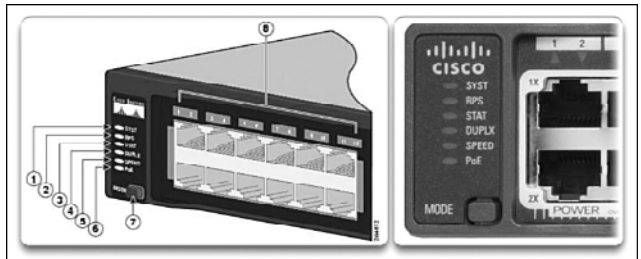
Cisco Catalyst switches have several status LED indicator lights. You can use the switch LEDs to quickly monitor switch activity and its performance. Switches of different models and feature sets will have different LEDs, and their placement on the front panel of the switch can also vary.

Figure 2-3 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 that 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 backup 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 that 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 that 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 that 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 that 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 that the PoE mode is selected and that 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 because of a fault. If the LED is amber, PoE for the port has been disabled.



Catalyst 2960 Switch LEDs			
1	The system LED	5	The port speed LED
2	The RPS LED (if RPS is supported on the switch)	6	The PoE status LED (if PoE is supported on the switch)
3	The port status LED (This is the default mode.)	7	The Mode button
4	The port duplex mode LED	8	The port LEDs

Figure 2-3 Switch LEDs

Preparing for Basic Switch Management (2.1.1.4)

A console cable is used to connect a PC to the console port of a switch, as depicted in Figure 2-4. To remotely manage the switch, it must be initially configured through the console port.

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 Figure 2-4, 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.

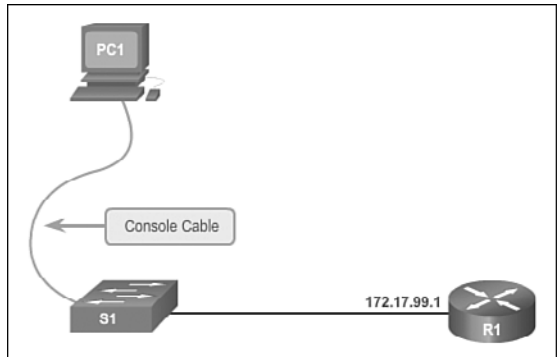


Figure 2-4 Preparing for Remote Management

Configuring Basic Switch Management Access with IPv4 (2.1.1.5)

To configure basic switch management access with IPv4, follow these steps:

How To

Step 1. Configure the management interface.

An IP address and subnet mask are configured on the management SVI of the switch from VLAN interface configuration mode. As shown in Table 2-1, 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.

Table 2-1 Cisco Switch Management Interface

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface vlan 99**
Configure the management interface IP address.	S1(config-if)# **ip address 172.17.99.11 255.255.255.0**
Enable the management interface.	S1(config-if)# **no shutdown**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running configuration file to the startup configuration file.	S1# **copy running-config startup-config**

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 interface FastEthernet 0/1, use the following commands:

```
S1(config)# vlan 99
S1(config-vlan)# name Mgmt
S1(config)# interface f0/1
S1(config-if)# switchport access vlan 99
```

Step 2. Configure the 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 Table 2-2, 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, as shown in Figure 2-5. 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.

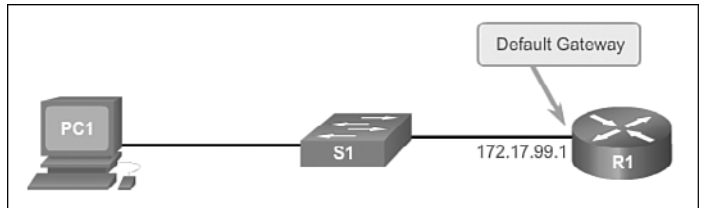


Figure 2-5 Default Gateway

Table 2-2 Configure Default Gateway for Switch

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Configure the default gateway for the switch.	S1(config)# **ip default-gateway 172.17.99.1**
Return to the privileged EXEC mode.	S1(config)# **end**
Save the running configuration file to the startup configuration file.	S1# **copy running-config startup-config**

Step 3. Verify the configuration.

As shown in Figure 2-6, 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 the interface status is "up."

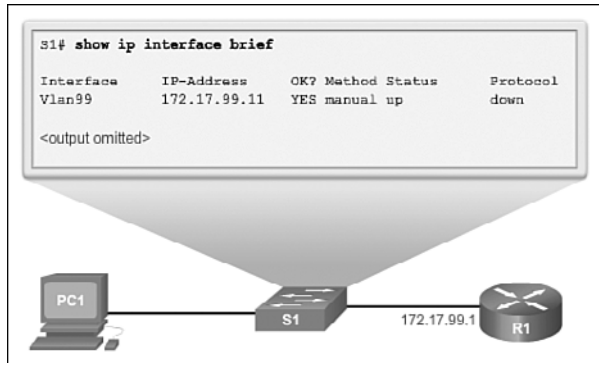


Figure 2-6 Verify Switch Management Interface Configuration

Lab 2.1.1.6: 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

Configure Switch Ports (2.1.2)

In general terms, switches are configured from the physical layer upward. The first set of tasks for switch configuration involves physical layer characteristics, such as duplex, speed, and pinouts.

Duplex Communication (2.1.2.1)

Figure 2-7 illustrates full-duplex and half-duplex communication.

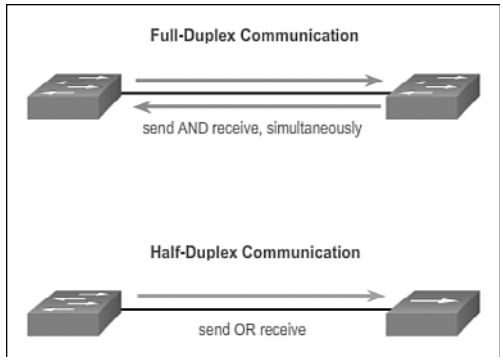


Figure 2-7 Duplex Communication

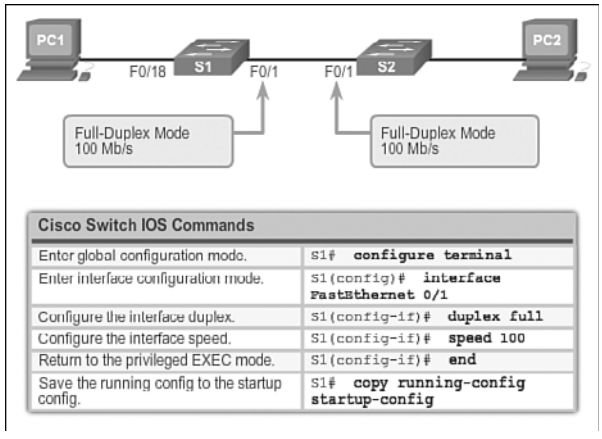
Full-duplex communication improves the performance of a switched LAN. Full-duplex communication increases effective bandwidth by allowing both ends of a connection to transmit and receive data simultaneously. This is also known as bidirectional. This method of optimizing network performance requires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

Unlike full-duplex communication, half-duplex communication is unidirectional. Sending and receiving data do 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 10-Gb 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.

Configure Switch Ports at the Physical Layer (2.1.2.2)

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 2-8, ports 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.



Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface FastEthernet 0/1`
Configure the interface duplex.	`S1(config-if)# duplex full`
Configure the interface speed.	`S1(config-if)# speed 100`
Return to the privileged EXEC mode.	`S1(config-if)# end`
Save the running config to the startup config.	`S1# copy running-config startup-config`

Figure 2-8 Configure Duplex and Speed

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. Autonegotiation is useful when

the speed and duplex settings of the device connecting to the port are unknown or can 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. Autonegotiation failure creates mismatched settings.

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

Interactive Graphic

Activity 2.1.2.2: Configuring Duplex and Speed

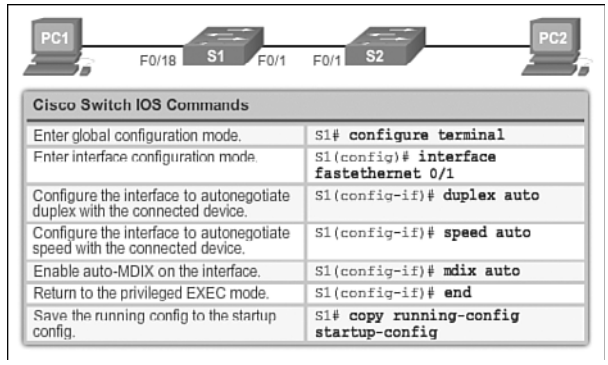
Go to the online course to use the Syntax Checker in the second graphic to configure port F0/1 of switch S1.

Auto-MDIX (2.1.2.3)

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 2-9.



Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface fastethernet 0/1`
Configure the interface to autonegotiate duplex with the connected device.	`S1(config-if)# duplex auto`
Configure the interface to autonegotiate speed with the connected device.	`S1(config-if)# speed auto`
Enable auto-MDIX on the interface.	`S1(config-if)# mdix auto`
Return to the privileged EXEC mode.	`S1(config-if)# end`
Save the running config to the startup config.	`S1# copy running-config startup-config`

Figure 2-9 Configure Auto-MDIX

Note

The auto-MDIX feature is enabled by default on Catalyst 2960 and Catalyst 3560 switches, but it 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 2-10, the output indicates On or Off for the feature.

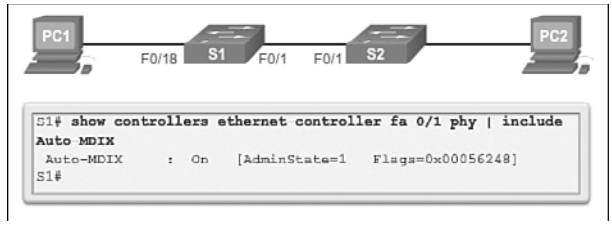


Figure 2-10 Verify Auto-MDIX

Interactive Graphic

Activity 2.1.2.3: Enable Auto-MDIX

Go to the online course to use the Syntax Checker in the third graphic to configure port F0/1 on S2 for auto-MDIX.

Verifying Switch Port Configuration (2.1.2.4)

Table 2-3 describes some of the options for the **show** command that are helpful in verifying common configurable switch features.

Table 2-3 Common Verification Commands

Cisco Switch IOS Commands	
Display interface status configuration.	S1# **show interfaces** [*interface-id*]
Display current startup configuration.	S1# **show startup-config**
Display current operating configuration.	S1# **show running-config**
Display info about flash file system.	S1# **show flash**
Display system hardware and software status.	S1# **show version**
Display history of commands entered.	S1# **show history**
Display IP information about an interface.	S1# **show ip** [*interface-id*]
Display the MAC address table.	S1# **show mac address-table**

Figure 2-11 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 is configured with the management VLAN 99.
- VLAN 99 is configured with an IP address of 172.17.99.11 255.255.255.0.
- Default gateway is set to 172.17.99.1.

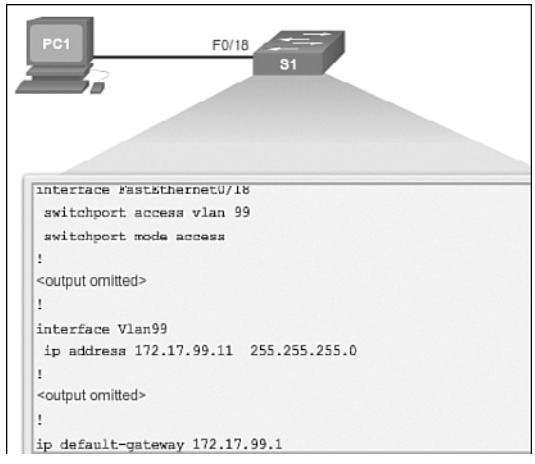


Figure 2-11 Running Configuration

The **show interfaces** command is another commonly used command that 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 2-12 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. Farther down, the output shows that the duplex is full and the speed is 100 Mb/s.

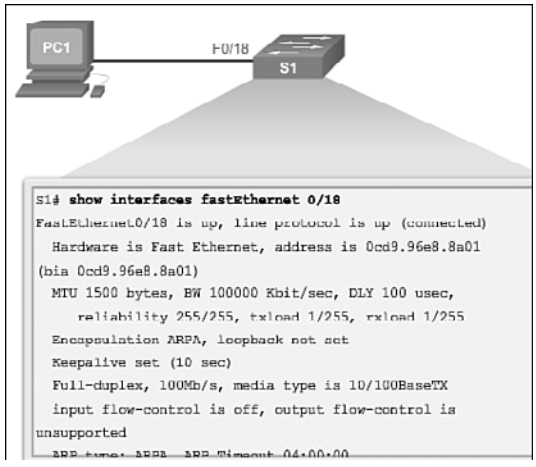


Figure 2-12 Interface Status

Network Access Layer Issues (2.1.2.5)

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. Example 2-1 indicates the summary line to check the status of an interface, and Table 2-4 describes the interface and line protocol status.

Example 2-1 Verify Interface Status

```
R1# show interfaces FastEthernet0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)
MTU 1500 bytes, BW 10000 Kbit, DLY 100 usec,
<output omitted>
```

Table 2-4 Verify Interface Status

Interface Status	Line Protocol Status	Link State
Up	Up	Operational
Down	Down	Interface Problem

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 might be administratively down.
- If the interface is administratively down, it has been manually disabled (the **shutdown** command has been issued) in the active configuration.

Example 2-2 shows an example of the **show interfaces** command output. The example shows counters and statistics for the FastEthernet 0/1 interface.

Example 2-2 Verify Interface Counters

```
S1# show interfaces FastEthernet 0/1
FastEthernet0/1 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0021.d722.9f01 (bia 0021.d722.9f01)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<output omitted>
2295197 packets input, 305539992 bytes, 0 no buffer
Received 1925500 broadcasts (1903 multicasts)
0 runts, 0 giants, 0 throttles
3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 1903 multicast, 0 pause input
0 input packets with dribble condition detected
359464 packets output, 436549843 bytes, 0 underruns
8 output errors, 1790 collisions, 10 interface resets
0 babbles, 235 late collision, 0 deferred
<output omitted>
```

Some media errors are not severe enough to cause the circuit to fail, but do cause network performance issues. Table 2-5 explains some of these common errors, which can be detected by using the **show interfaces** command.

Table 2-5 Network Access Layer Issues

Error Type	Description
Input errors	Total number of errors. It includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
Runts	Packets that are discarded because they are smaller than the minimum packet size for the medium. For example, any Ethernet packet that is less than 64 bytes is considered a runt.
Giants	Packets that are discarded because they exceed the maximum packet size for the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
CRC	CRC errors are generated when the calculated checksum is not the same as the checksum received.
Output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined.
Collisions	Number of messages retransmitted because of an Ethernet collision.
Late collisions	Jammed signal could not reach to ends.

"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.

Troubleshooting Network Access Layer Issues (2.1.2.6)

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 are 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 might be because of a mismatch in speed setting. The speed of an interface is typically autonegotiated; therefore, even if it is manually configured on one interface, the connecting interface should autonegotiate accordingly. If a speed mismatch does occur through misconfiguration or a hardware or software issue, that can 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 can 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 autonegotiated. 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.

Figure 2-13 summarizes switch media issues in a flowchart.

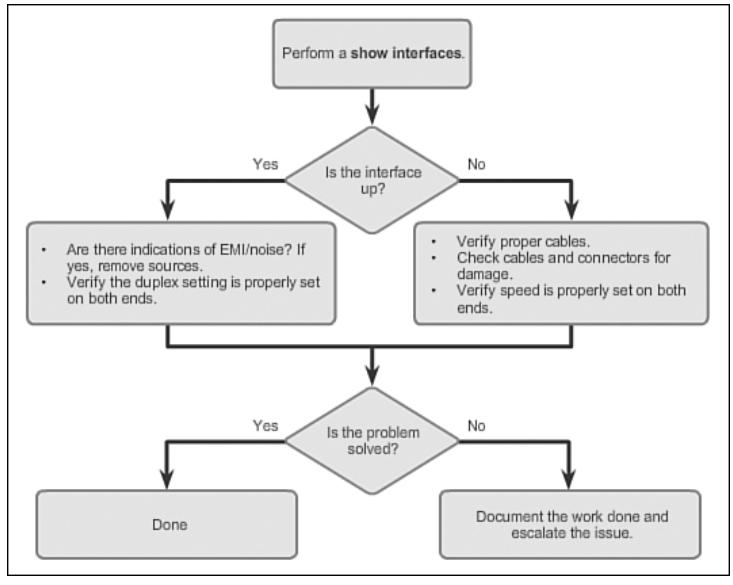


Figure 2-13 Troubleshooting Switch Media Issues

Switch Security: Management and Implementation (2.2)

Switch security is an integral part of network security. The features and technologies available on LAN switches have a wide variety of applications. Security is applied in a layered approach, and switches illustrate this with the configurable security options. In this section, the basic switch security features and technologies are introduced, including *Secure Shell (SSH)*, *DHCP snooping*, and port security.

Secure Remote Access (2.2.1)

Having in mind that network security is applied in layers, a primary consideration is that network administrators need to be able to configure network devices without worrying about hackers seeing what they are doing. In other words, network administrators need secure remote access. Secure Shell makes this possible.

SSH Operation (2.2.1.1)

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 2-14, an attacker can monitor packets using Wireshark. A Telnet stream can be targeted to capture the username and password.

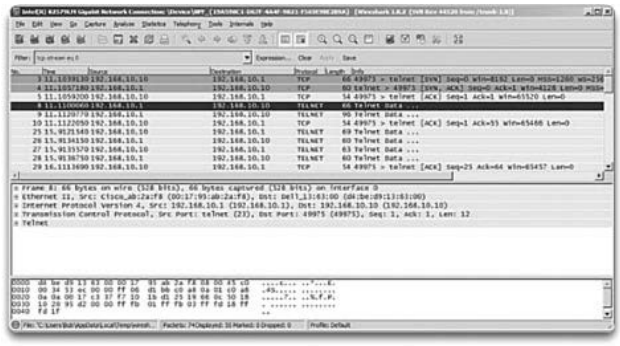


Figure 2-14 Wireshark Telnet Capture

In Figure 2-15, the attacker can capture the username and password of the administrator from the plaintext Telnet session.

Figure 2-16 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 2-17, the username and password are encrypted.

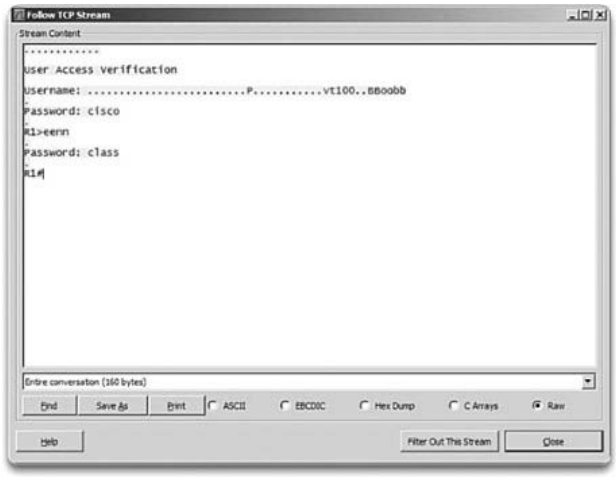


Figure 2-15 Plaintext Username and Password Captured

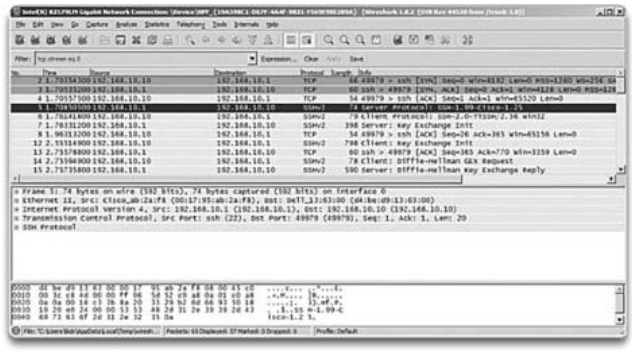


Figure 2-16 Wireshark SSH Capture

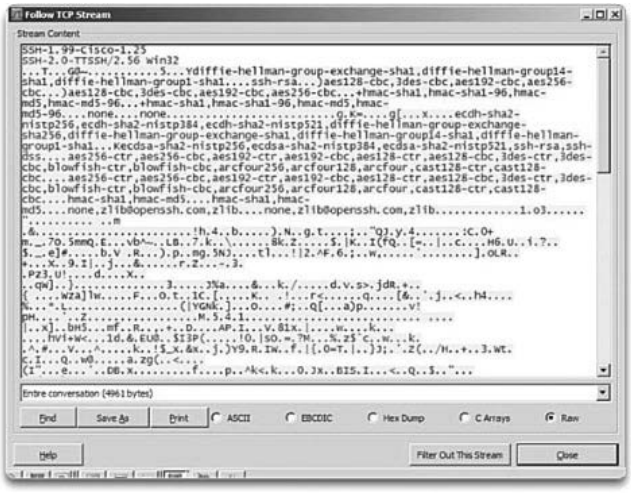


Figure 2-17 Username and Password Encrypted

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 Example 2-3, use the **show version** command on the switch to see which IOS the switch is currently running, and verify that the IOS filename includes the combination "k9", which indicates that it supports cryptographic (encrypted) features and capabilities.

Example 2-3 Cryptographic Image

```
S1# show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE
  SOFTWARE (fc1)
<output omitted>
```

Configuring SSH (2.2.1.2)

Before configuring SSH, be sure that the switch is minimally configured with a unique host name and the correct network connectivity settings.

How To

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 name.

Configure the IP domain name of the network using the **ip domain-name** *domain-name* global configuration mode command. In Figure 2-18, 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 1024 bits (see the sample configuration in Figure 2-18). 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.

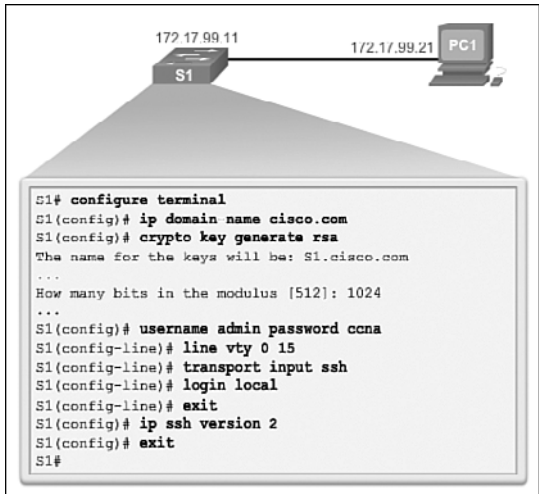


Figure 2-18 Configure SSH for Remote Management

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.

Interactive Graphic

Activity 2.2.1.2: Configure SSH

Go to the online course to use the Syntax Checker in the second graphic to configure SSH on S1.

Verifying SSH (2.2.1.3)

On a PC, an SSH client, such as PuTTY, is used to connect to an SSH server. For the examples in Figures 2-19, 2-20, and 2-21, 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 2-19, the PC initiates an SSH connection to the SVI VLAN IP address of S1.

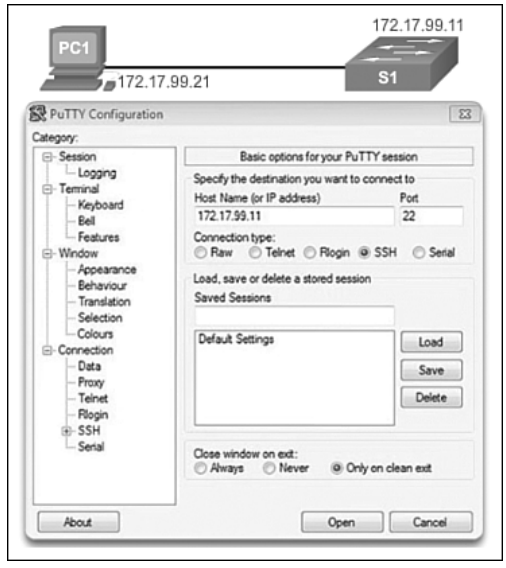


Figure 2-19 Configure PuTTY SSH Client Connection Parameters

In Example 2-4 (and the related graphic in Figure 2-20), 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 through SSH to the CLI on the Catalyst 2960 switch.

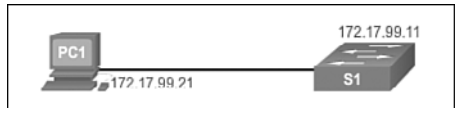


Figure 2-20 Remote Management SSH Connection

Example 2-4 PuTTY Window Text for Remote Management SSH Connection

```
Login as: admin
Using keyboard-interactive
authentication.
Password:

S1> enable
Password:
S1#
```

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 2-21).

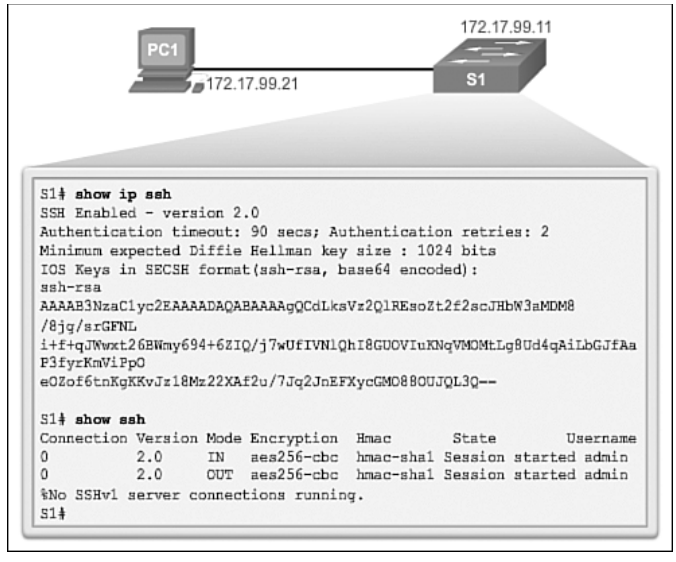


Figure 2-21 Verify SSH Status and Settings

Packet Tracer Activity

Packet Tracer Activity 2.2.1.4: Configuring SSH

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.

Security Concerns in LANs (2.2.2)

Modern networks are especially vulnerable to sophisticated attacks. It is more important than ever to be familiar with the common security attacks associated with the LAN environment. Fortunately, each type of attack has an effective means to mitigate the attack.

Common Security Attacks: MAC Address Flooding (2.2.2.1)

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 is 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 2-22, 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.

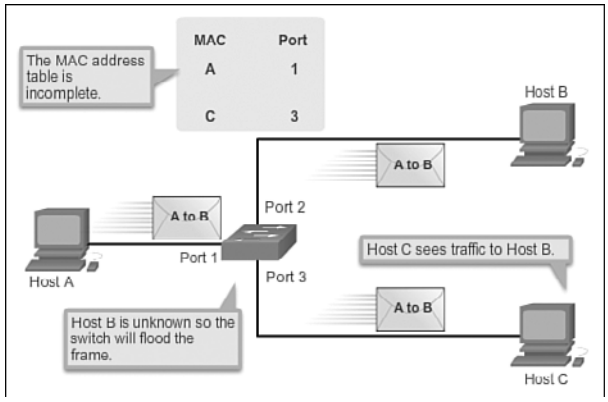


Figure 2-22 Switch Floods Frame for Unknown MAC Address

In Figure 2-23, 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.

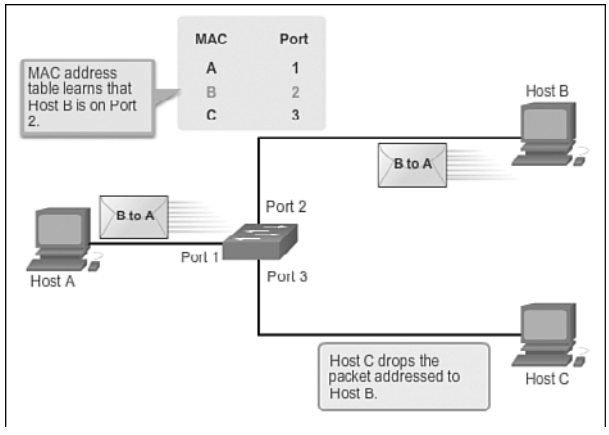


Figure 2-23 Switch Records MAC Address

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 2-24, 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.

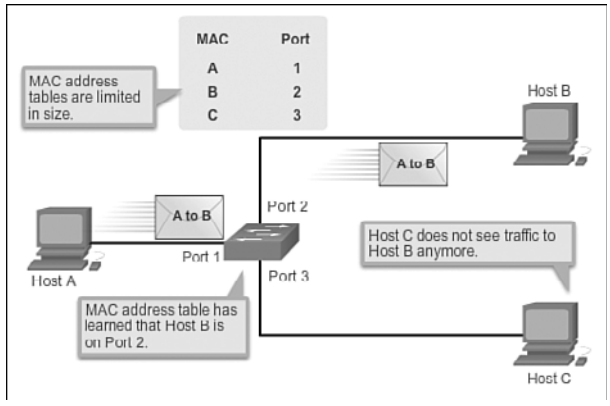


Figure 2-24 Switch Uses MAC Address Table to Forward Traffic

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 2-25, 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 the frames.

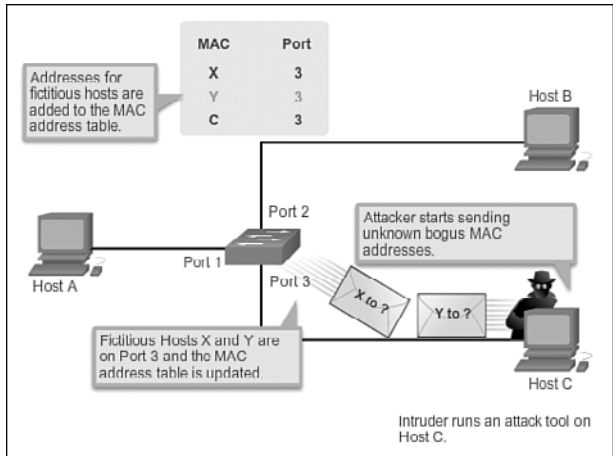


Figure 2-25 MAC Address Flooding Attack

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 2-26, 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.

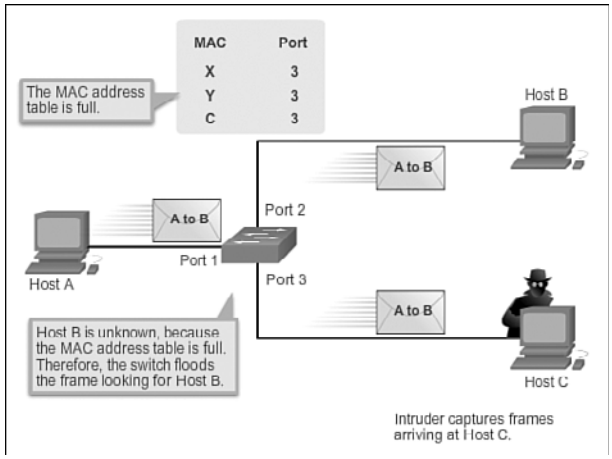


Figure 2-26 Switch Acts Like a Hub

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

Common Security Attacks: DHCP Spoofing (2.2.2.2)

Dynamic Host Control Protocol (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, as shown in Figure 2-27. 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.

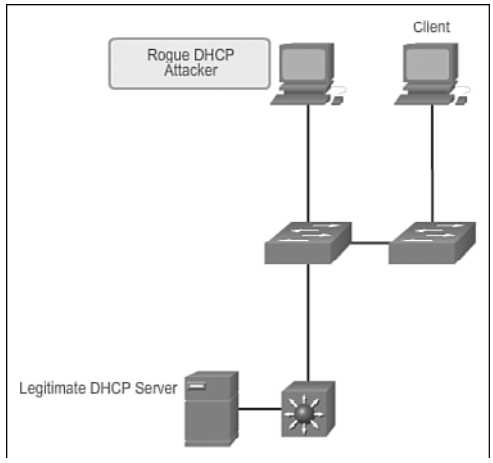


Figure 2-27 DHCP Spoofing

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.

Common Security Attacks: Leveraging CDP (2.2.2.3)

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 autoconfigure 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.

Figure 2-28 is a portion of a Wireshark capture showing the contents of a CDP packet. The Cisco IOS Software version discovered through 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.

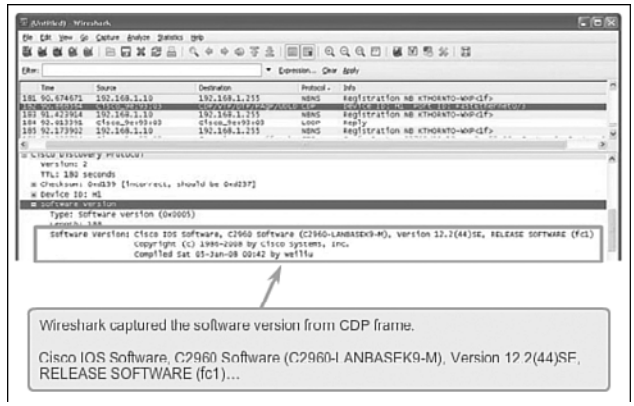


Figure 2-28 CDP Attack

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 uppercase 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.

Interactive Graphic

Activity 2.2.2.4: Identify Common Security Attacks

Go to the online course to perform this practice activity.

Security Best Practices (2.2.3)

Network security *best practices* involve recommended procedures for network administrators to implement in their networks as common practice for ensuring a secure network. Of course, here the focus is on securing the LAN environment.

Best Practices (2.2.3.1)

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, through 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, illustrated in Figure 2-29, 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.

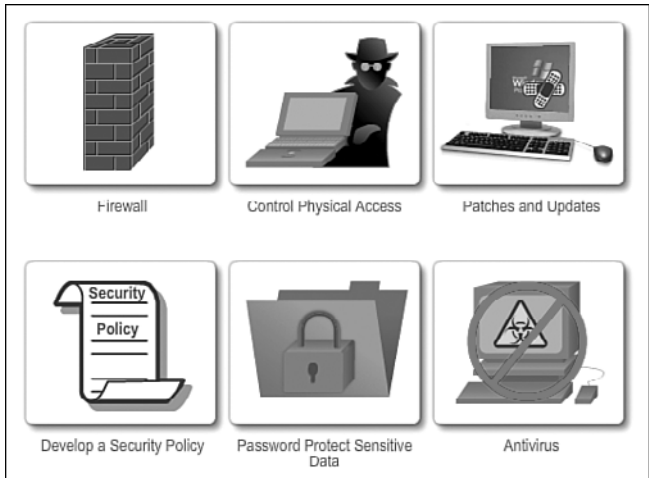


Figure 2-29 Security Best Practices

Network Security Tools and Testing (2.2.3.2)

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 can 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)

Network Security Audits (2.2.3.3)

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, 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 the networking staff to perform network penetration tests.

Switch Port Security (2.2.4)

A number of network attacks in the LAN environment can be mitigated with simple measures applied to switch ports on Cisco switches. DHCP snooping and Cisco port security help to mitigate MAC address flooding and DHCP attacks.

Secure Unused Ports (2.2.4.1)

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 needs to be reactivated, it can be enabled with the **no shutdown** command. Figure 2-30 shows partial output for this configuration.

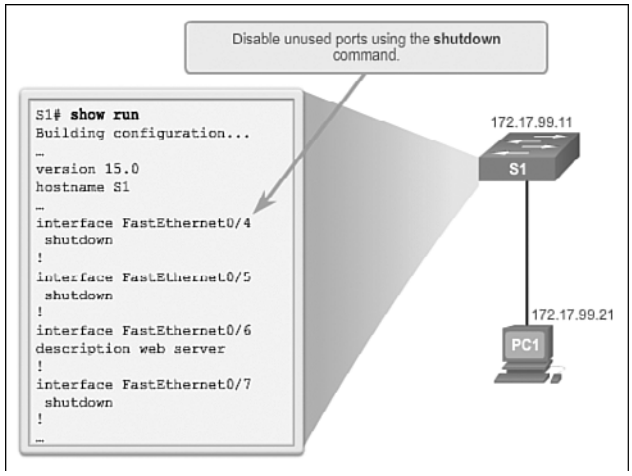


Figure 2-30 Disable Unused Ports

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.

DHCP Snooping (2.2.4.2)

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 acknowledgment 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 Figure 2-31, 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.

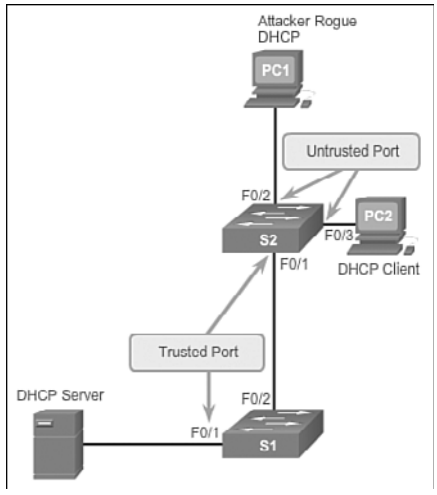


Figure 2-31 DHCP Snooping Operation

DHCP snooping allows the configuration of ports as trusted or untrusted. Trusted ports can send DHCP requests and acknowledgments. Untrusted ports can only forward DHCP requests. DHCP snooping enables the switch to build the DHCP binding table that binds a client MAC address, IP address, VLAN, and port ID.

The following configuration steps, illustrated in Figure 2-32, show how to implement DHCP snooping on a Catalyst 2960 switch:

How To

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.

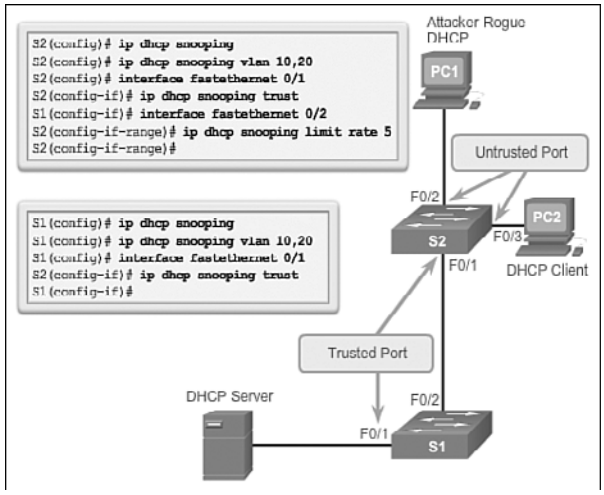


Figure 2-32 DHCP Snooping Configuration

Port Security: Operation (2.2.4.3)

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, 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.

Secure MAC Address Types

There are a number of ways to configure port security. The type of ***secure MAC 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, and 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, 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 as dynamic secure addresses, but are removed from the running configuration.

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

Port Security: Violation Modes (2.2.4.4)

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:

- *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.

Table 2-6 presents which kinds of data traffic are forwarded when one of the security violation modes is configured on a port.

Table 2-6 Port Security Violation Modes

Security Violation Modes				
Violation Mode	**Forwards Traffic**	**Sends Syslog Message**	**Increases Violation Counter**	**Shuts Down Port**
Protect	No	No	No	No
Restrict	No	Yes	Yes	No
Shutdown	No	Yes	Yes	Yes

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

Port Security: Configuring (2.2.4.5)

Table 2-7 summarizes the default port security settings on a Cisco Catalyst switch.

Table 2-7 Port Security Defaults

Feature	Default Setting
Port security	Disabled on a port
Maximum number of secure MAC addresses	1
Restrict	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.
Sticky address learning	Disabled

Figure 2-33 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).

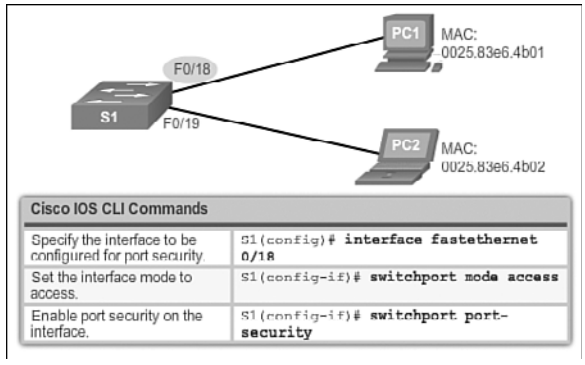
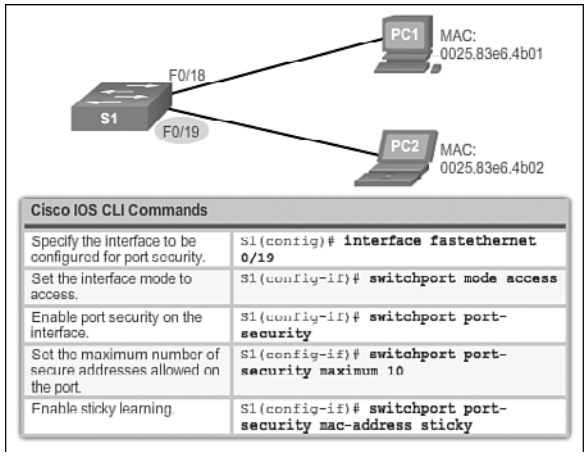


Figure 2-33 Configure Dynamic Port Security

Figure 2-34 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.



Cisco IOS CLI Commands	
Specify the interface to be configured for port security.	`S1(config)# interface fastethernet 0/19`
Set the interface mode to access.	`S1(config-if)# switchport mode access`
Enable port security on the interface.	`S1(config-if)# switchport port-security`
Set the maximum number of secure addresses allowed on the port.	`S1(config-if)# switchport port-security maximum 10`
Enable sticky learning.	`S1(config-if)# switchport port-security mac-address sticky`

Figure 2-34 Configure Sticky Port Security

Port Security: Verifying (2.2.4.6)

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 Example 2-5. By default, there is one MAC address allowed on this port.

Example 2-5 Verify Dynamic MAC Addresses

```
S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging      : Disabled
Maximum MAC Addresses           : 1
Total MAC Addresses             : 1
Configured MAC Addresses        : 0
Sticky MAC Addresses            : 0
Last Source Address:Vlan        : 0025.83e6.4b01:1
Security Violation Count        : 0
```

The output shown in Example 2-6 shows the values for the sticky port security settings. The maximum number of addresses is set to 10, as configured.

Example 2-6 Verify Sticky MAC Addresses

```
S1# show port-security interface fastethernet 0/19
Port Security                : Enabled
Port Status                  : Secure-up
Violation Mode               : Shutdown
Aging Time                   : 0 mins
Aging Type                   : Absolute
SecureStatic Address Aging       : Disabled
Maximum MAC Addresses            : 50
Total MAC Addresses              : 1
Configured MAC Addresses         : 0
Sticky MAC Addresses             : 1
Last Source Address:Vlan         : 0025.83e6.4b02:1
Security Violation Count         : 0
```

Note

The MAC address is identified as a sticky MAC address in Example 2-6.

Sticky MAC addresses are added to the MAC address table and to the running configuration. Port security with sticky MAC addresses retains dynamically learned MAC addresses during a link-down condition. If you enter the **copy running-config startup-config** command, port security with sticky MAC addresses saves dynamically learned MAC addresses in the startup config file and the port does not have to learn addresses from ingress traffic after bootup or a restart. As shown in Example 2-7, the sticky MAC for PC2 has been added to the running configuration for S1.

Example 2-7 Verify Sticky MAC Addresses in Running Configuration

```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 50
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

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 Example 2-8, the secure MAC addresses are listed along with the types.

Example 2-8 Verify Secure MAC Addresses

```
S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type              Ports   Remaining Age
                                                      (mins)
----    -----------       ----              -----   -------------
1       0025.83e6.4b01    SecureDynamic     Fa0/18       -
1       0025.83e6.4b02    SecureSticky      Fa0/19       -
------------------------------------------------------------------
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port
```

Ports in Error-Disabled State (2.2.4.7)

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, similar to those shown in Example 2-9.

Example 2-9 Port Security Violation Messages

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18,
  putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
  caused by MAC address 000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

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** (see Example 2-10). 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.

Example 2-10 Port Status

```
S1# show interface fa0/18 status
Port     Name   Status        Vlan   Duplex  Speed   Type
Fa0/18          err-disabled  1      auto    auto    10/100BaseTX
S1# show port-security interface fastethernet 0/18
Port Security               : Enabled
Port Status                 : Secure-shutdown
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging      : Disabled
Maximum MAC Addresses           : 1
Total MAC Addresses             : 0
Configured MAC Addresses        : 0
Sticky MAC Addresses            : 0
Last Source Address:Vlan        : 000c.292b.4c75:1
Security Violation Count        : 1
```

The administrator should determine what caused the security violation before reenabling the port. If an unauthorized device is connected to a secure port, the port should not be reenabled until the security threat is eliminated. To reenable the port, use the **shutdown** interface configuration mode command (see Example 2-11). Then, use the **no shutdown** interface configuration command to make the port operational.

Example 2-11 Reenabling an Error-Disabled Port

```
S1(config)# interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
  administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/18, changed state to up
```

Network Time Protocol (NTP) (2.2.4.8)

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 want 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 Figure 2-35. Router R2 is configured as an NTP client, while Router R1 serves as an authoritative NTP server.

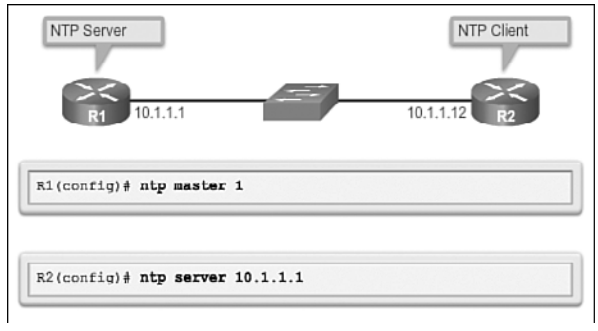


Figure 2-35 Port Status

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.

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. Example 2-12 displays the verification of NTP on Router R2.

Example 2-12 Configuring NTP

```
R2# show ntp associations

  address      ref clock     st   when    poll reach  delay  offset  disp
*~10.1.1.1     .LOCL.         1     13     64   377   1.472  6.071   3.629
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R2# show ntp status
Clock is synchronized, stratum 2, reference is 10.1.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz, precision is 2**17
reference time is D40ADC27.E644C776 (13:18:31.899 UTC Mon Sep 24 2012)
clock offset is 6.0716 msec, root delay is 1.47 msec
root dispersion is 15.41 msec, peer dispersion is 3.62 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000091 s/s
system poll interval is 64, last update was 344 sec ago.***Insert Packet Tracer icon
  here.
```

Packet Tracer Activity

Packet Tracer Activity 2.2.4.9: Configuring Switch Port Security

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.

Packet Tracer Activity

Packet Tracer Activity 2.2.4.10: Troubleshooting Switch Port Security

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 reenable the port.

Lab 2.2.4.11: 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

Summary (2.3)

Class Activity 2.3.1.1: Switch Trio

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

> "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 that you 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 that it is operational or validated.

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

Packet Tracer Activity

Packet Tracer Activity 2.3.1.2: Skills Integration Challenge

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.

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

1. 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. 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. 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 provide a secure (encrypted) management connection to a remote device to prevent the sniffing of unencrypted usernames 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 ten 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, through 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.

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion *Switched Networks Lab Manual* (ISBN 978-1-58713-327-5). The Packet Tracer Activities PKA files are found in the online course.

Class Activities

- Class Activity 2.0.1.2: Stand by Me
- Class Activity 2.3.1.1: Switch Trio

Labs

- Lab 2.1.1.6: Configuring Basic Switch Settings
- Lab 2.2.4.11: Configuring Switch Security Features

Packet Tracer Activities

- Packet Tracer Activity 2.2.1.4: Configuring SSH
- Packet Tracer Activity 2.2.4.9: Configuring Switch Port Security
- Packet Tracer Activity 2.2.4.10: Troubleshooting Switch Port Security
- Packet Tracer Activity 2.3.1.2: Skills Integration Challenge

Check Your Understanding Questions

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

1. Which of the following options correctly associate the command with the paired behavior? (Choose three.)

   A. **switchport port-security violation protect:** Frames with unknown source addresses are dropped and a notification is sent.

   B. **switchport port-security violation restrict:** Frames with unknown source addresses are dropped and no notification is sent.

   C. **switchport port-security violation shutdown:** Frames with unknown source addresses result in the port becoming error-disabled and a notification is sent.

   D. **switchport port-security mac-address sticky:** Allows dynamically learned MAC addresses to be stored in the running configuration.

   E. **switchport port-security maximum:** Defines the number of MAC addresses associated with a port.

2. What advantage does SSH offer over Telnet when remotely connecting to a device?

   A. Encryption

   B. More connection lines

   C. Connection-oriented services

   D. Username and password authentication

3. Which option correctly associates the Layer 2 security attack with the description?

   A. MAC address flooding: broadcast requests for IP addresses with spoofed MAC addresses

   B. DHCP starvation: using Cisco-proprietary protocols to gain information about a switch

   C. CDP attack: the attacker fills the switch MAC address table with invalid MAC addresses

   D. Telnet attack: using brute force password attacks to gain access to a switch

4. The network administrator wants to configure an IP address on a Cisco switch. How does the network administrator assign the IP address?

   A. In privileged EXEC mode
   B. On the switch interface FastEthernet 0/0
   C. On the management VLAN virtual interface
   D. On the physical interface connected to the router or next-hop device

5. Why should a default gateway be assigned to a switch?

   A. So that there can be remote connectivity to the switch through such programs as Telnet and ping
   B. So that frames can be sent through the switch to the router
   C. So that frames generated from workstations and destined for remote networks can pass to a higher level
   D. So that other networks can be accessed from the command prompt of the switch

6. Which of the following tasks does autonegotiation in an Ethernet network accomplish? (Choose two.)

   A. Sets the link speed
   B. Sets the IP address
   C. Sets the link duplex mode
   D. Sets MAC address assignments on the switch port
   E. Sets the ring speed

7. The boot loader can be accessed through a console connection in a sequence of steps. Put the following steps in order.

   A. The boot loader **switch:** prompt appears in the terminal emulation software on the PC.
   B. Unplug the switch power cord.
   C. Connect a PC by console cable to the switch console port. Configure terminal emulation software to connect to the switch.
   D. Continue pressing the **Mode** button until the System LED turns briefly amber and then solid green; then release the **Mode** button.
   E. 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.

8. List three LED indicators on a Cisco Catalyst 2960 switch.

9. What are the default settings for duplex and speed on Cisco Catalyst 2960 and 3560 switches?

10. What feature on Cisco Catalyst 2960 enables switch ports to work with either crossover or straight-through cables?

11. A giant Ethernet frame is one that is greater than how many bytes?

12. An Ethernet frame that is smaller than 64 bytes is called a _____.

13. Assume that a Cisco Catalyst switch has an image that supports SSH. Assume that a host name and domain name are configured, that local authentication is properly configured, and that the vty lines support all protocols. Which command is required to have a functional SSH configuration?

    A. **ip ssh version 2** in global configuration mode
    B. **crypto key generate rsa** in global configuration mode
    C. **transport input ssh** in line VTY configuration mode
    D. **login local** in line vty configuration mode
    E. **ip domain-name** <*domain-name*> in global configuration mode

14. A network administrator has configured VLAN 99 as the management VLAN and has configured it with an IP address and subnet mask. The administrator issues the **show interface vlan 99** command and notices that the line protocol is down. Which action can change the state of the line protocol to up?

    A. Connect a host to an interface associated with VLAN 99.
    B. Configure a default gateway.
    C. Remove all access ports from VLAN 99.
    D. Configure a transport input method on the vty lines.

15. A network administrator plugs a PC into a switch port. The LED for that port changes to solid green. What statement best describes the current status of the port?

    A. There is a duplex mismatch error.
    B. There is a link fault error. This port is unable to forward frames.
    C. The port is operational and ready to transmit packets.
    D. This port has been disabled by management and is unable to forward frames.
    E. The flash memory is busy.

16. Describe a DHCP starvation attack.

17. List three best practices for securing a network. (Several answers are possible.)

18. What is an ideal environment to carry out penetration tests?

    A. On the production network during nonpeak times
    B. Under controlled conditions during business hours on the production network
    C. On an off-line test bed network that mimics the actual production network
    D. On a network environment simulated by software

19. What is the result of issuing the **no switchport port-security mac-address sticky** command on an interface with port security configured?

    A. The sticky secure MAC addresses are removed from the address table and from the running configuration.
    B. The sticky secure MAC addresses remain part of the address table but are removed from the running configuration.
    C. The static secure MAC addresses are removed from the address table and from the running configuration.
    D. The static secure MAC addresses remain part of the address table but are removed from the running configuration.

20. An attacker has bypassed physical security and was able to connect a laptop to an Ethernet interface on a switch. If all the switch ports are configured with port security and the violation mode is set to factory default, which action is taken against the attacker?

    A. Packets with unknown source addresses are dropped, and there is no notification that a security violation has occurred.
    B. Packets with unknown source addresses are dropped, and there is a notification that a security violation has occurred.
    C. Packets with unknown source addresses are dropped, and the interface becomes error-disabled and turns off the port LED.
    D. Packets with unknown source addresses are forwarded, and there is a notification to the syslog server.

CHAPTER 3

VLANs

Objectives

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

- How do you explain the purpose of VLANs in a switched network?
- How do you analyze the forwarding of frames by a switch based on VLAN configuration?
- How do you configure a switch port to be assigned to data and voice VLANs?
- How do you configure a trunk port on a LAN switch?
- How do you configure Dynamic Trunking Protocol (DTP)?
- How do you troubleshoot VLAN and trunk configurations in a switched network?
- How do you configure security features to mitigate attacks in a switched network?
- How do you explain security best practices for a switched network?

Key Terms

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

Virtual Local-Area Network (VLAN) *page 96*

VLAN Trunk *page 96*

Data VLAN *page 99*

User VLAN *page 99*

Default VLAN *page 100*

Native VLAN *page 100*

IEEE 802.1Q *page 100*

Management VLAN *page 101*

Voice VLAN *page 101*

Dynamic Trunking Protocol (DTP) *page 120*

Switch Spoofing Attack *page 138*

Double-Tagging Attack *page 139*

Private VLAN (PVLAN) Edge *page 140*

Protected Port *page 140*

Black Hole VLAN *page 142*

Introduction (3.0.1.1)

Network performance is an important factor in the productivity of an organization. One of the technologies used to improve network performance is the separation of large broadcast domains into smaller ones. By design, routers will block broadcast traffic at an interface. However, routers normally have a limited number of LAN interfaces. A router's primary role is to move information between networks, not provide network access to end devices.

The role of providing access into a LAN is normally reserved for an access layer switch. A ***virtual local-area network (VLAN)*** can be created on a Layer 2 switch to reduce the size of broadcast domains, similar to a Layer 3 device. VLANs are commonly incorporated into network design, making it easier for a network to support the goals of an organization. While VLANs are primarily used within switched local-area networks, modern implementations of VLANs allow them to span MANs and WANs.

This chapter will cover how to configure, manage, and troubleshoot VLANs and ***VLAN trunks***. It will also examine security considerations and strategies relating to VLANs and trunks, and best practices for VLAN design.

Class Activity 3.0.1.2: Vacation Station

You have purchased a three-floor vacation home at the beach for rental purposes. The floor plan is identical on each floor. Each floor offers one digital television for renters to use.

According to the local Internet service provider, only three stations can be offered within a television package. It is your job to decide which television packages you offer your guests.

- Divide the class into groups of three students per group.
- Choose three different stations to make one subscription package for each floor of your rental home.
- Complete the PDF for this activity.
- Share your completed group-reflection answers with the class.

VLAN Segmentation (3.1)

LAN switches and VLANs go hand in hand. When you look at the configuration of a router, you do not see references to VLANs; however, when you look at the configuration of a switch, you see frequent references to VLANs. Modern switches are structured around VLANs. VLANs are to switches as networks are to routers. Almost everything you do on a switch relates to VLANs. So, to a large extent, learning about switching is learning about VLANs. The day in the future when every port on every switch is on a separate Layer 3 network is the day that VLANs are no longer necessary—the need for VLANs is tied to the need to put multiple switch ports in one broadcast domain (in one VLAN).

Overview of VLANs (3.1.1)

This section provides a high-level introduction to VLANs, which sets the stage for the chapter.

VLAN Definitions (3.1.1.1)

Within a switched internetwork, VLANs provide segmentation and organizational flexibility. VLANs provide a way to group devices within a LAN. A group of devices within a VLAN communicate as if they were attached to the same wire. VLANs are based on logical connections, instead of physical connections.

VLANs allow an administrator to segment networks based on factors such as function, project team, or application, without regard for the physical location of the user or device, as seen in Figure 3-1. Devices within a VLAN act as if they are in their own independent network, even if they share a common infrastructure with other VLANs. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations within the VLAN where the packets are sourced. Each VLAN is considered a separate logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a device that supports routing.

A VLAN creates a logical broadcast domain that can span multiple physical LAN segments. VLANs improve network performance by separating large broadcast domains into smaller ones. If a device in one VLAN sends a broadcast Ethernet frame, all devices in the VLAN receive the frame, but devices in other VLANs do not.

VLANs enable the implementation of access and security policies according to specific groupings of users. Each switch port can be assigned to only one VLAN (with the exception of a port connected to an IP phone or to another switch).

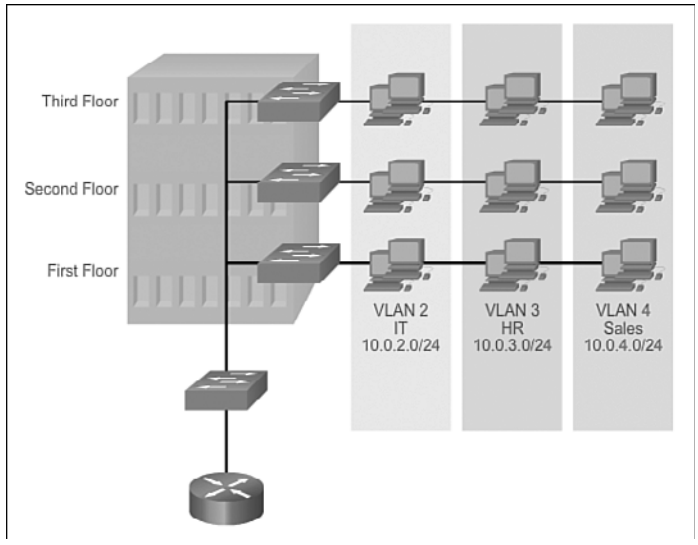


Figure 3-1 Defining VLAN Groups

Benefits of VLANs (3.1.1.2)

User productivity and network adaptability are important for business growth and success. VLANs make it easier to design a network to support the goals of an organization. The primary benefits of using VLANs are as follows:

- **Security:** Groups that have sensitive data are separated from the rest of the network, decreasing the chances of confidential information breaches. As shown in Figure 3-2, faculty computers are on VLAN 10 and completely separated from student and guest data traffic.
- **Cost reduction:** Cost savings result from reduced need for expensive network upgrades and more efficient use of existing bandwidth and uplinks.
- **Better performance:** Dividing flat Layer 2 networks into multiple logical workgroups (broadcast domains) reduces unnecessary traffic on the network and boosts performance.
- **Shrink broadcast domains:** Dividing a network into VLANs reduces the number of devices in the broadcast domain. As shown in Figure 3-2, there are six computers on this network but there are three broadcast domains: Faculty, Student, and Guest.
- **Improved IT staff efficiency:** VLANs make it easier to manage the network because users with similar network requirements share the same VLAN. When a new switch is provisioned, all the policies and procedures already configured for the particular VLAN are implemented when the ports are assigned. It is also easy

for the IT staff to identify the function of a VLAN by giving it an appropriate name. In Figure 3-2, for easy identification, VLAN 10 has been named "Faculty," VLAN 20 is named "Student," and VLAN 30 "Guest."

- **Simpler project and application management:** VLANs aggregate users and network devices to support business or geographic requirements. Having separate functions makes managing a project or working with a specialized application easier; an example of such an application is an e-learning development platform for faculty.

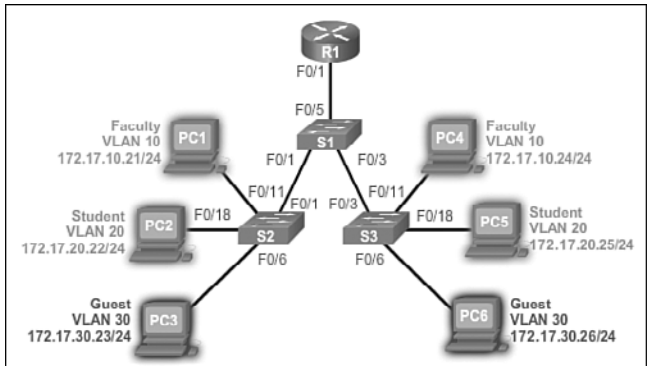


Figure 3-2 Benefits of VLANs

Each VLAN in a switched network corresponds to an IP network; therefore, VLAN design must take into consideration the implementation of a hierarchical network-addressing scheme. Hierarchical network addressing means that IP network numbers are applied to network segments or VLANs in an orderly fashion that takes the network as a whole into consideration. Blocks of contiguous network addresses are reserved for and configured on devices in a specific area of the network, as shown in Figure 3-2.

Types of VLANs (3.1.1.3)

There are a number of distinct types of VLANs used in modern networks. Some VLAN types are defined by traffic classes. Other types of VLANs are defined by the specific function that they serve.

Data VLAN

A ***data VLAN*** is a VLAN that is configured to carry user-generated traffic. A VLAN carrying voice or management traffic would not be a data VLAN. It is common practice to separate voice and management traffic from data traffic. A data VLAN is sometimes referred to as a ***user VLAN***. Data VLANs are used to separate the network into groups of users or devices.

Default VLAN

All switch ports become a part of the default VLAN after the initial bootup of a switch loading the default configuration. Switch ports that participate in the ***default VLAN*** are part of the same broadcast domain. This allows any device connected to any switch port to communicate with other devices on other switch ports. The default VLAN for Cisco switches is VLAN 1. In Example 3-1, the **show vlan brief** command was issued on a switch running the default configuration. Notice that all ports are assigned to VLAN 1 by default.

VLAN 1 has all the features of any VLAN, except it cannot be renamed or deleted. By default, all Layer 2 control traffic is associated with VLAN 1.

Example 3-1 Default VLAN Configuration

```
Switch# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Native VLAN

A ***native VLAN*** is assigned to an 802.1Q trunk port. Trunk ports are the links between switches that support the transmission of traffic associated with more than one VLAN. An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic), as well as traffic that does not come from a VLAN (untagged traffic). Tagged traffic refers to traffic that has a 4-byte tag inserted within the original Ethernet frame header, specifying the VLAN to which the frame belongs. The 802.1Q trunk port places untagged traffic on the native VLAN, which by default is VLAN 1.

Native VLANs are defined in the ***IEEE 802.1Q*** specification to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. A native VLAN serves as a common identifier on opposite ends of a trunk link.

It is a best practice to configure the native VLAN as an unused VLAN, distinct from VLAN 1 and other VLANs. In fact, it is not unusual to dedicate a fixed VLAN to serve the role of the native VLAN for all trunk ports in the switched domain.

Management VLAN

A ***management VLAN*** is any VLAN configured to access the management capabilities of a switch. VLAN 1 is the management VLAN by default. To create the management VLAN, the switch virtual interface (SVI) of that VLAN is assigned an IP address and subnet mask, allowing the switch to be managed through HTTP, Telnet, SSH, or SNMP. Because the out-of-the-box configuration of a Cisco switch has VLAN 1 as the default VLAN, VLAN 1 would be a bad choice for the management VLAN.

In the past, the management VLAN for a 2960 switch was the only active SVI. On 15.x versions of the Cisco IOS for Catalyst 2960 Series switches, it is possible to have more than one active SVI. With Cisco IOS Release 15.x, the particular active SVI assigned for remote management must be documented. While theoretically a switch can have more than one management VLAN, having more than one increases exposure to network attacks.

In Example 3-1, all ports are currently assigned to the default VLAN 1. No native VLAN is explicitly assigned and no other VLANs are active; therefore the network is designed with the native VLAN the same as the management VLAN. This is considered a security risk.

Voice VLANs (3.1.1.4)

A separate VLAN is needed to support Voice over IP (VoIP). VoIP traffic requires

- Assured bandwidth to ensure voice quality
- Transmission priority over other types of network traffic
- Ability to be routed around congested areas on the network
- Delay of less than 150 ms across the network

To meet these requirements, the entire network has to be designed to support VoIP. The details of how to configure a network to support VoIP are beyond the scope of this course, but it is useful to summarize how a ***voice VLAN*** works between a switch, a Cisco IP Phone, and a computer.

In Figure 3-3, VLAN 150 is designed to carry voice traffic. The student computer PC5 is attached to the Cisco IP Phone, and the phone is attached to switch S3. PC5 is in VLAN 20, which is used for student data.

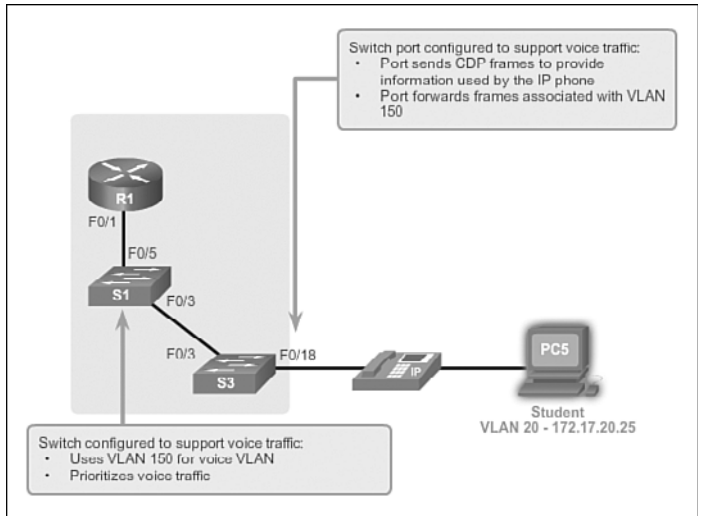


Figure 3-3 Voice VLAN

Packet Tracer Activity

Packet Tracer Activity 3.1.1.5: Who Hears the Broadcast?

In this activity, a 24-port Catalyst 2960 switch is fully populated. All ports are in use. You will observe broadcast traffic in a VLAN implementation and answer some reflection questions.

VLANs in a Multiswitch Environment (3.1.2)

VLAN trunks are the connections in switched networks upon which all control traffic is transmitted and received. VLAN trunks carry data traffic for all VLANs in the switched network, unless restricted manually or with a pruning mechanism. Switches are interconnected with VLAN trunks. This section describes VLAN trunks.

VLAN Trunks (3.1.2.1)

A trunk is a point-to-point link between two network devices that carries more than one VLAN. A VLAN trunk extends VLANs across an entire network. Cisco supports IEEE 802.1Q for coordinating trunks on Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces.

VLANs would not be very useful without VLAN trunks. VLAN trunks allow all VLAN traffic to propagate between switches so that devices that are in the same VLAN, but connected to different switches, can communicate without the intervention of a router.

A VLAN trunk does not belong to a specific VLAN; rather, it is a conduit for multiple VLANs between switches and routers. A trunk could also be used between a network device and server or other device that is equipped with an appropriate 802.1Q-capable NIC. By default, on a Cisco Catalyst switch, all VLANs are supported on a trunk port.

In Figure 3-4, the links between switches S1 and S2, and S1 and S3, are configured to transmit traffic coming from VLANs 10, 20, 30, and 99 across the network. This network could not function without VLAN trunks.

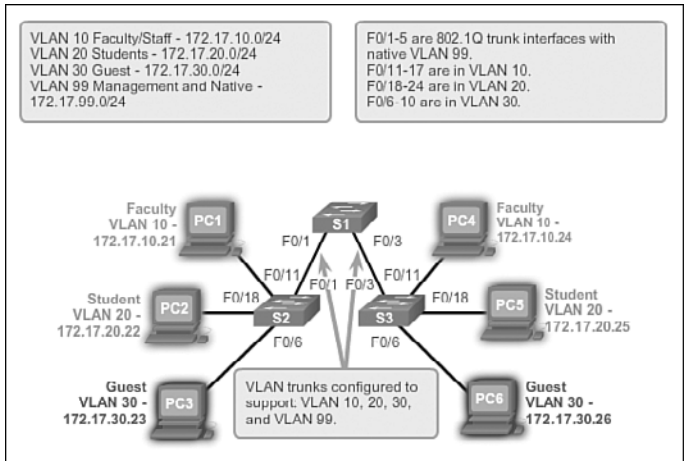


Figure 3-4 VLAN Trunks

Controlling Broadcast Domains with VLANs (3.1.2.2)

The behavior of broadcasts is affected by the presence of a switch. An ingress broadcast frame on a switch will only be forwarded out ports identified with the VLAN with which the frame is associated.

Network Without VLANs

In normal operation, when a switch receives a broadcast frame on one of its ports, it forwards the frame out all other ports except the port where the broadcast was received. In Figure 3-5, the entire network is configured in the same subnet (172.17.40.0/24) and no VLANs are configured. As a result, when the faculty computer (PC1) sends out a broadcast frame, switch S2 sends that broadcast frame out all of its ports. Eventually the entire network receives the broadcast because the network is one broadcast domain.

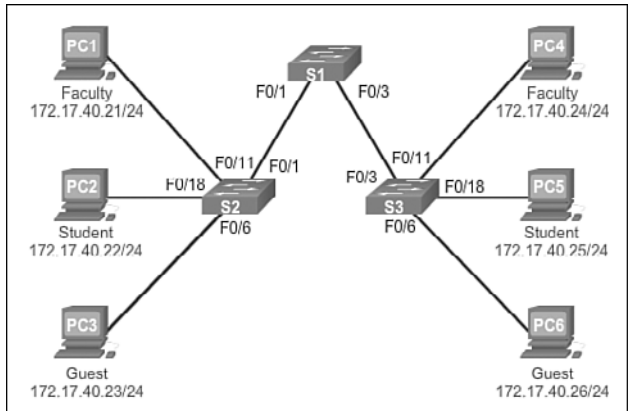


Figure 3-5 VLAN Trunks

Network with VLANs

As shown in Figure 3-6, the network has been segmented using two VLANs. Faculty devices are assigned to VLAN 10 and student devices are assigned to VLAN 20. When a broadcast frame is sent from the faculty computer, PC1, to switch S2, the switch forwards that broadcast frame only to those switch ports configured to support VLAN 10.

The ports that comprise the connection between switches S2 and S1 (ports F0/1), and between S1 and S3 (ports F0/3), are trunks and have been configured to support all the VLANs in the network. Port F0/18 is associated with VLAN 20, so S2 forwards the broadcast out port F0/1 but does not forward the broadcast out port F0/18, as shown in Figure 3-6.

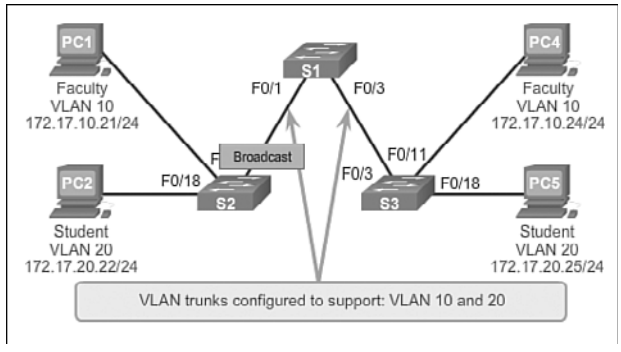


Figure 3-6 Broadcasts with VLAN Segmentation

When S1 receives the broadcast frame on port F0/1, S1 forwards that broadcast frame out of the only other port configured to support VLAN 10, which is port F0/3. When S3 receives the broadcast frame on port F0/3, it forwards the broadcast frame out of the only other port configured to support VLAN 10, which is port F0/11. The broadcast frame arrives at the only other computer in the network configured in VLAN 10, which is faculty computer PC4.

When VLANs are implemented on a switch, the transmission of unicast, multicast, and broadcast traffic from a host in a particular VLAN is restricted to the devices that are in that VLAN.

Tagging Ethernet Frames for VLAN Identification (3.1.2.3)

Catalyst 2960 Series switches are Layer 2 devices. They use the Ethernet frame header information to forward packets. They do not have routing tables. The standard Ethernet frame header does not contain information about the VLAN to which the frame belongs. Thus, when Ethernet frames are placed on a trunk, information about the VLANs to which they belong must be added. This process, called tagging, is accomplished by using the IEEE 802.1Q header, specified in the IEEE 802.1Q standard. The 802.1Q header includes a 4-byte tag inserted within the original Ethernet frame header, specifying the VLAN to which the frame belongs.

When the switch receives a frame on a port configured in access mode and assigned a VLAN, the switch inserts a VLAN tag in the frame header, recalculates the FCS, and sends the tagged frame out of a trunk port.

VLAN Tag Field Details

The VLAN tag field, shown in Figure 3-7, consists of a Type field, a Priority field, a Canonical Format Identifier field, and VLAN ID field:

- **Type:** A 2-byte value called the tag protocol ID (TPID) value. For Ethernet, it is set to hexadecimal 0x8100.
- **Priority:** A 3-bit value that supports level or service implementation.
- **Canonical Format Identifier (CFI):** A 1-bit identifier that enables Token Ring frames to be carried across Ethernet links.
- **VLAN ID (VID):** A 12-bit VLAN identification number that supports up to 4096 VLAN IDs.

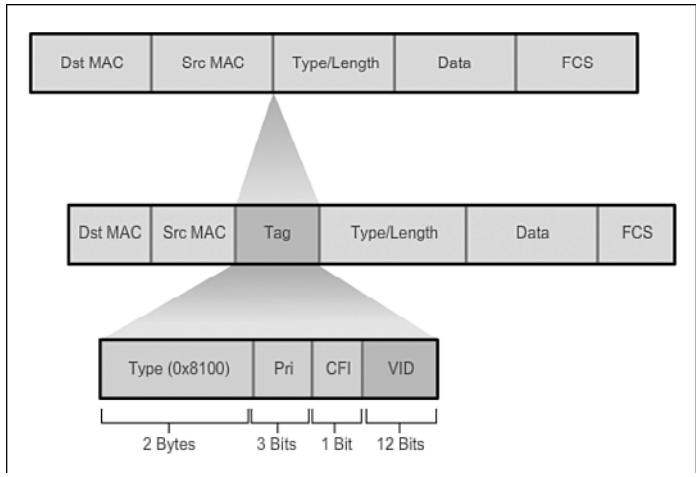


Figure 3-7 802.1Q VLAN Tag

After the switch inserts the Type and tag control information fields, it recalculates the FCS values and inserts the new FCS into the frame.

Native VLANs and 802.1Q Tagging (3.1.2.4)

The behavior of frames in the context of IEEE 802.1Q trunking is a vestige of the original standard, which was created when VLANs were still widely used. Essentially, the behavior is dictated by the assumption that a hub is connected between two switch ports that define a common VLAN trunk.

Tagged Frames on the Native VLAN

Some devices that support trunking add a VLAN tag to native VLAN traffic. Control traffic sent on the native VLAN should not be tagged. If an 802.1Q trunk port receives a tagged frame with the VLAN ID the same as the native VLAN, it drops the frame. Consequently, when configuring a switch port on a Cisco switch, configure devices so that they do not send tagged frames on the native VLAN. Devices from other vendors that support tagged frames on the native VLAN include IP phones, servers, routers, and non-Cisco switches.

Untagged Frames on the Native VLAN

When a Cisco switch trunk port receives untagged frames (which are unusual in a well-designed network), it forwards those frames to the native VLAN. If there are no devices associated with the native VLAN (which is not unusual) and there are no other trunk ports (which is not unusual), the frame is dropped. The default native

VLAN is VLAN 1. When configuring an 802.1Q trunk port, a default Port VLAN ID (PVID) is assigned the value of the native VLAN ID. All untagged traffic coming into or out of the 802.1Q port is forwarded based on the PVID value. For example, if VLAN 99 is configured as the native VLAN, the PVID is 99 and all untagged traffic is forwarded to VLAN 99. If the native VLAN has not been reconfigured, the PVID value is set to VLAN 1.

In Figure 3-8, PC1 is connected by a hub to an 802.1Q trunk link. PC1 sends untagged traffic, which the switches associate with the native VLAN configured on the trunk ports, and forwards accordingly. Tagged traffic on the trunk received by PC1 is dropped. This scenario reflects poor network design for several reasons: It uses a hub, it has a host connected to a trunk link, and it implies that the switches have access ports assigned to the native VLAN. But it illustrates the motivation for the IEEE 802.1Q specification for native VLANs as a means of handling legacy scenarios.

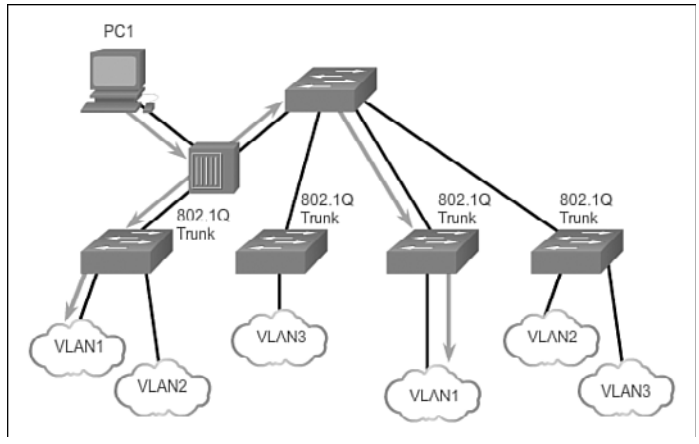


Figure 3-8 Native VLAN Forwarding Behavior

Voice VLAN Tagging (3.1.2.5)

Recall that to support VoIP, a separate voice VLAN is required.

An access port that is used to connect a Cisco IP Phone can be configured to use two separate VLANs: one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone. The link between the switch and the IP phone acts as a trunk to carry both voice VLAN traffic and data VLAN traffic.

The Cisco IP Phone contains an integrated three-port 10/100 switch. The ports provide dedicated connections to these devices:

- Port 1 connects to the switch or other VoIP device.
- Port 2 is an internal 10/100 interface that carries the IP phone traffic.
- Port 3 (access port) connects to a PC or other device.

On the switch, the access is configured to send Cisco Discovery Protocol (CDP) packets that instruct an attached IP phone to send voice traffic to the switch in one of three ways, depending on the type of traffic:

- In a voice VLAN tagged with a Layer 2 class of service (CoS) priority value
- In an access VLAN tagged with a Layer 2 CoS priority value
- In an access VLAN, untagged (no Layer 2 CoS priority value)

In Figure 3-9, the student computer PC5 is attached to a Cisco IP Phone, and the phone is attached to switch S3. VLAN 150 is designed to carry voice traffic, while PC5 is in VLAN 20, which is used for student data.

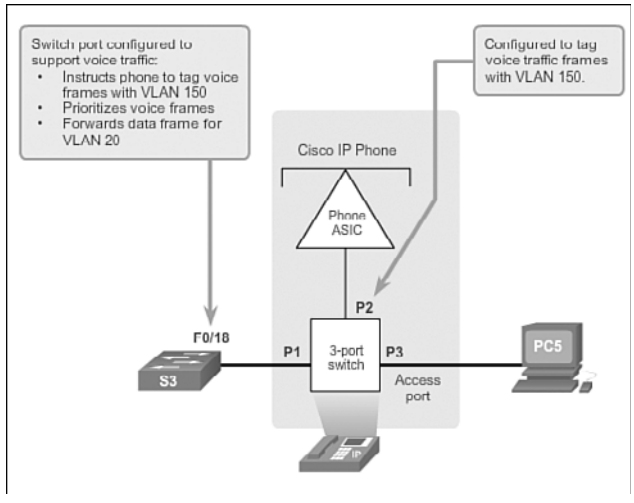


Figure 3-9 Voice VLAN Tagging

Sample Configuration

Example 3-2 shows sample output. A discussion of voice Cisco IOS commands is beyond the scope of this course, but the highlighted areas in the sample output show the F0/18 interface configured with a VLAN configured for data (VLAN 20) and a VLAN configured for voice (VLAN 150).

Example 3-2 Default VLAN Configuration

```
S1# show interfaces f0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (voice)
<output omitted>
```

Interactive Graphic

Activity 3.1.2.6: VLAN Trunks in Action

Go to the online course to perform this practice activity.

Packet Tracer Activity

Packet Tracer Activity 3.1.2.7: Investigating a VLAN Implementation

In this activity, you will observe how broadcast traffic is forwarded by the switches when VLANs are configured and when VLANs are not configured.

VLAN Implementations (3.2)

Network administrators who are responsible for portions of the switched network are familiar with the basic configuration tasks related to creating VLANs, configuring trunk links, associating voice and data VLANs with ports, and securing the VLAN implementation. This section describes the major tasks required to configure VLANs and trunks on switches in the network infrastructure.

VLAN Assignment (3.2.1)

The first step in configuring VLANs is to create the VLANs and to associate switch ports with VLANs.

VLAN Ranges on Catalyst Switches (3.2.1.1)

Different Cisco Catalyst switches support various numbers of VLANs. The number of supported VLANs is large enough to accommodate the needs of most organizations. For example, the Catalyst 2960 and 3560 Series switches support over 4000 VLANs. Normal-range VLANs on these switches are numbered 1 to 1005, and extended-range VLANs are numbered 1006 to 4094. Catalyst 2960 switches running Cisco IOS Release 15.x support extended-range VLANs.

Normal-Range VLANs

Normal range VLANs are usually the ones utilized in switched networks, because most networks do not need over 1000 VLANs!

- Used in small- and medium-sized business and enterprise networks.
- Identified by a VLAN ID between 1 and 1005.
- IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
- IDs 1 and 1002 to 1005 are automatically created and cannot be removed.
- Configurations are stored within a VLAN database file called vlan.dat. The vlan.dat file is located in the flash memory of the switch.
- The VLAN Trunking Protocol (VTP), which helps manage VLAN configurations between switches, can only learn and store normal-range VLANs.

Extended-Range VLANs

Extended range VLANs are primarily used in metropolitan service provider networks requiring over 1000 VLANs to support the various customers.

- Enable service providers to extend their infrastructure to a greater number of customers. Some global enterprises could be large enough to need extended-range VLAN IDs.
- Are identified by a VLAN ID between 1006 and 4094.
- Configurations are not written to the vlan.dat file.
- Support fewer VLAN features than normal-range VLANs.
- Are, by default, saved in the running configuration file.
- VTP does not learn extended-range VLANs.

Note

4096 is the upper bound for the number of VLANs available on Catalyst switches, because there are 12 bits in the VLAN ID field of the IEEE 802.1Q header.

Creating a VLAN (3.2.1.2)

When configuring normal-range VLANs, the configuration details are stored in flash memory on the switch in a file called vlan.dat. Flash memory is persistent and does not require the **copy running-config startup-config** command. However, because other details are often configured on a Cisco switch at the same time that VLANs are created, it is good practice to save running configuration changes to the startup configuration.

Table 3-1 displays the Cisco IOS command syntax used to add a VLAN to a switch and give it a name. Naming each VLAN is considered a best practice in switch configuration.

Table 3-1 Creating a VLAN

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Create a VLAN with a valid ID number.	S1(config)# **vlan vlan-id**
Specify a unique name to identify the VLAN.	S1(config-vlan)# **name vlan-name**
Return to privileged EXEC mode.	S1(config-vlan)# **end**

Figure 3-10 shows how the student VLAN (VLAN 20) is configured on switch S1. In the topology example, the student computer (PC2) has not been associated with a VLAN yet, but it does have an IP address of 172.17.20.22.

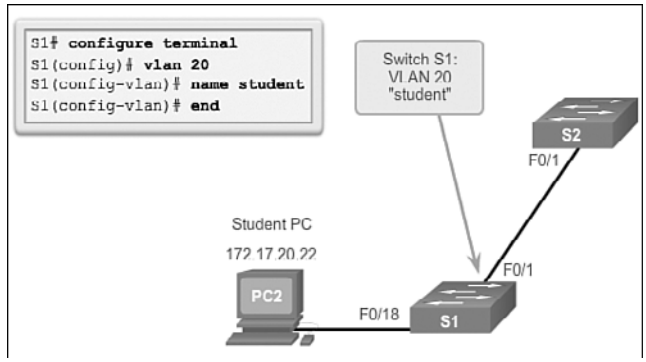


Figure 3-10 Sample VLAN Configuration

Interactive Graphic

Activity 3.2.1.2: Creating and Verifying VLANs

Go to the online course to use the Syntax Checker in the third graphic to create a VLAN and use the **show vlan brief** command to display the contents of the vlan.dat file.

In addition to entering a single VLAN ID, a series of VLAN IDs can be entered separated by commas, or a range of VLAN IDs separated by hyphens using the **vlan** *vlan-id* command. For example, use the following command to create VLANs 100, 102, 105, 106, and 107:

```
S1(config)# vlan 100,102,105-107
```

Assigning Ports to VLANs (3.2.1.3)

After creating a VLAN, the next step is to assign ports to the VLAN. An access port can belong to only one VLAN at a time. One exception to this rule is that of a port connected to an IP phone, in which case there are two VLANs associated with the port: one for voice and one for data.

Table 3-2 displays the syntax for defining a port to be an access port and assigning it to a VLAN. The **switchport mode access** command is optional but strongly recommended as a security best practice. With this command, the interface changes to permanent access mode.

Table 3-2 Assign Ports to VLANs

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface interface-id**
Set the port to access mode.	S1(config-if)# **switchport mode access**
Assign the port to a VLAN.	S1(config-if)# **switchport access vlan vlan-id**
Return to the privileged EXEC mode.	S1(config-if)# **end**

Note

Use the **interface range** command to simultaneously configure multiple interfaces.

In Figure 3-11, VLAN 20 is assigned to port F0/18 on switch S1; therefore, the student computer (PC2) is in VLAN 20. When VLAN 20 is configured on other switches, the network administrator knows to configure the other student computers to be in the same subnet as PC2 (172.17.20.0/24).

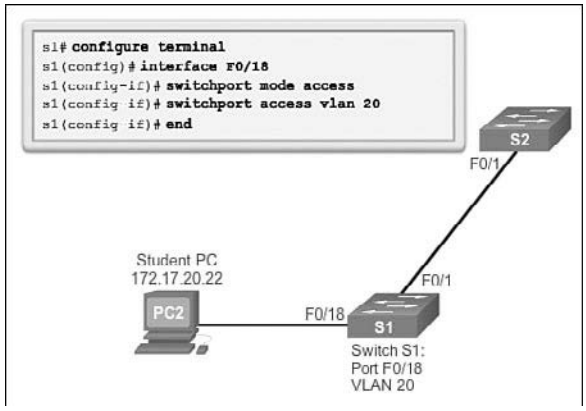


Figure 3-11 Sample Interface Configuration for VLANs

Interactive Graphic

Activity 3.2.1.3: Assigning Ports to VLANs

Go to the online course to use the Syntax Checker in the third graphic to assign a VLAN and use the **show vlan brief** command to display the contents of the vlan.dat file.

The **switchport access vlan** command forces the creation of a VLAN if it does not already exist on the switch. For example, VLAN 30 is not present in the **show vlan brief** output of the switch. If the **switchport access vlan 30** command is entered on any interface with no previous configuration, the switch displays

```
% Access VLAN does not exist. Creating vlan 30
```

Changing VLAN Port Membership (3.2.1.4)

There are a number of ways to change VLAN port membership. Table 3-3 shows the syntax for changing a switch port to VLAN 1 membership with the **no switchport access vlan** interface configuration mode command.

Table 3-3 Removing a VLAN Assignment

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface interface-id**
Remove the VLAN assignment from the port.	S1(config-if)# **no switchport access vlan**
Return to the privileged EXEC mode.	S1(config-if)# **end**

Interface F0/18 was previously assigned to VLAN 20. The **no switchport access vlan** command is entered for interface F0/18. Examine the output in the **show vlan brief** command, as shown in Example 3-3. The **show vlan brief** command displays the VLAN assignment and membership type for all switch ports. The **show vlan brief** command displays one line for each VLAN. The output for each VLAN includes the VLAN name, status, and switch ports.

Example 3-3 Sample VLAN Assignment Removal

```
S1(config)# interface f0/18
S1(config-if)# no switchport access vlan
S1(config-if)# do show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
20   student                           active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

VLAN 20 is still active, even though no ports are assigned to it. In Example 3-4, the **show interfaces f0/18 switchport** output verifies that the access VLAN for interface F0/18 has been reset to VLAN 1.

Example 3-4 Verification of VLAN Assignment Removal

```
S1# show interfaces f0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
<output omitted>
```

A port can easily have its VLAN membership changed. It is not necessary to first remove a port from a VLAN to change its VLAN membership. When an access port has its VLAN membership reassigned to another existing VLAN, the new VLAN membership simply replaces the previous VLAN membership. In Example 3-5, port F0/11 is assigned to VLAN 20.

Example 3-5 Changing VLAN Assignment

```
S1(config)# interface f0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
*Mar  31 09:33:26.058: %SYS-5-CONFIG_I: Configured from console by console
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
20   student                          active    Fa0/11
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
S1#
```

Interactive Graphic

Activity 3.2.1.4: Creating and Verifying VLANs

Go to the online course to use the Syntax Checker in the fifth graphic to change VLAN port membership.

Deleting VLANs (3.2.1.5)

In Example 3-6, the **no vlan** *vlan-id* global configuration mode command is used to remove VLAN 20 from the switch. Switch S1 had a minimal configuration with all ports in VLAN 1 and an unused VLAN 20 in the VLAN database. The **show vlan brief** command verifies that VLAN 20 is no longer present in the vlan.dat file after using the **no vlan 20** command.

Example 3-6 Deleting a VLAN

```
S1(config)# no vlan 20
S1(config)# end
S1#
*Mar  1 07:37:55.785: %SYS-5-CONFIG_I: Configured from console by console
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Caution

Before deleting a VLAN, be sure to first reassign all member ports to a different VLAN. Any ports that are not moved to an active VLAN are unable to communicate with other hosts after the VLAN is deleted and until they are assigned to an active VLAN.

Alternatively, the entire vlan.dat file can be deleted using the **delete flash:vlan.dat** privileged EXEC mode command. The abbreviated command version (**delete vlan.dat**) can be used if the vlan.dat file has not been moved from its default location.

After issuing this command and reloading the switch, the previously configured VLANs are no longer present. This effectively places the switch into its factory default condition concerning VLAN configurations.

Note

For a Catalyst switch, the **erase startup-config** command must accompany the **delete vlan.dat** command prior to reload to restore the switch to its factory default condition.

Verifying VLAN Information (3.2.1.6)

After a VLAN is configured, VLAN configurations can be validated using Cisco IOS **show** commands.

Table 3-4 displays the show vlan command options.

Table 3-4 show vlan Command

Cisco IOS CLI Command Syntax	
show vlan [brief | id *vlan-id* **| name** *vlan-name* **| summary]**	
Display one line for each VLAN with the VLAN name, status, and its ports.	**brief**
Display information about a single VLAN identified by VLAN ID number. For *vlan-id*, the range is 1 to 4094.	**id** *vlan-id*
Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.	**name** *vlan-name*
Display VLAN summary information.	**summary**

Table 3-5 displays the **show interfaces** command options.

Table 3-5 show interfaces Command

Cisco IOS CLI Command Syntax	
show interfaces [*interface-id* **| vlan** *vlan-id***] | switchport**	
Valid interfaces include physical ports (including type, module, and port number) and port channels. The port-channel range is 1 to 6.	*interface-id*
VLAN identification. The range is 1 to 4095.	**vlan** *vlan-id*
Display the administrative and operational status of a switching port, including port blocking and port protection settings.	**switchport**

In Example 3-7, the **show vlan name student** command produces output that is not easily interpreted. The preferable option is to use the **show vlan brief** command. The **show vlan summary** command displays the count of all configured VLANs. The output in Example 3-7 shows seven VLANs.

Example 3-7 Using the **show vlan** Command

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------
20   student                           active    Fa0/11
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------

S1# show vlan summary
Number of existing VLANs           : 7
 Number of existing VTP VLANs      : 7
 Number of existing extended VLANs : 0
```

The **show interfaces vlan** *vlan-id* command displays details that are beyond the scope of this course. The important information appears on the second line in Example 3-8, indicating that VLAN 20 is up.

Example 3-8 Using the **show interfaces vlan** Command

```
S1# show interfaces vlan 20
Vlan 20 is up, line protocol is down
  Hardware is EtherSVI, address is 0021.a1e0.78c1 (bia 0021.a1e0.78c1)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
```

```
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
S1#
```

Interactive Graphic

Activity 3.2.1.6: Using the show interfaces Command

Go to the online course to use the Syntax Checker in the fourth graphic to display the VLAN and switch port information, and verify VLAN assignments and mode.

Packet Tracer Activity

Packet Tracer Activity 3.2.1.7: Configuring VLANs

VLANs are helpful in the administration of logical groups, allowing members of a group to be easily moved, changed, or added. This activity focuses on creating and naming VLANs, and assigning access ports to specific VLANs.

VLAN Trunks (3.2.2)

In this section, the elements of VLAN trunk configuration are explored. Remember that VLAN trunks carry all the control traffic between switches. VLAN trunks enable the communication between switches required for many of the technologies specific to the LAN switched environment.

Configuring IEEE 802.1Q Trunk Links (3.2.2.1)

A VLAN trunk is an OSI Layer 2 link between two switches that carries traffic for all VLANs (unless the allowed VLAN list is restricted manually or dynamically). To enable trunk links, configure the ports on either end of the physical link with parallel sets of commands.

To configure a switch port on one end of a trunk link, use the **switchport mode trunk** command. With this command, the interface changes to permanent trunking

mode. The port enters into a *Dynamic Trunking Protocol (DTP)* negotiation to convert the link into a trunk link even if the interface connecting to it does not agree to the change. DTP is described in the next topic. In this course, the **switchport mode trunk** command is the only method implemented for trunk configuration.

The Cisco IOS command syntax to specify a native VLAN (other than VLAN 1) is shown in Table 3-6.

Table 3-6 802.1Q Trunk Configuration

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface** *interface-id*
Force the link to be a trunk link.	S1(config-if)# **switchport mode trunk**
Specify a native VLAN for 802.1Q trunks.	S1(config-if)# **switchport trunk native vlan** *vlan-id*
Specify the list of VLANs to be allowed on the trunk link.	S1(config-if)# **switchport trunk allowed vlan** *vlan-list*
Return to the privileged EXEC mode.	S1(config-if)# **end**

Use the Cisco IOS **switchport trunk allowed vlan** *vlan-list* command to specify the list of VLANs to be allowed on the trunk link.

In Figure 3-12, VLANs 10, 20, and 30 support the Faculty, Student, and Guest computers (PC1, PC2, and PC3). The native VLAN should also be changed from VLAN 1 and changed to another VLAN such as VLAN 99. By default, all VLANs are allowed across a trunk link. The **switchport trunk allowed vlan** command can be used to limit the allowed VLANs.

In Example 3-9, the F0/1 port on switch S1 is configured as a trunk port, assigns the native VLAN to VLAN 99, and specifies the trunk to only forward traffic for VLANs 10, 20, 30, and 99.

Example 3-9 Sample Trunk Configuration

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30
S1(config-if)# end
```

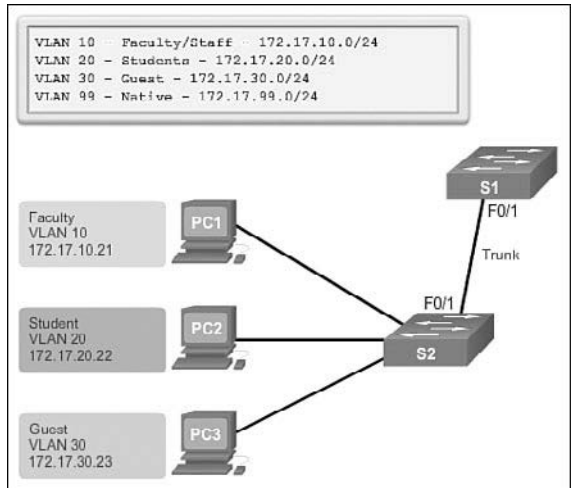


Figure 3-12 Sample Interface Configuration for VLANs

Note

This configuration assumes the use of Cisco Catalyst 2960 switches, which automatically use 802.1Q encapsulation on trunk links. Other switches might require manual configuration of the encapsulation. Always configure both ends of a trunk link with the same native VLAN. If 802.1Q trunk configuration is not the same on both ends, Cisco IOS Software reports errors.

Resetting the Trunk to the Default State (3.2.2.2)

Table 3-7 shows the commands to remove the allowed VLANs and reset the native VLAN of the trunk. When reset to the default state, the trunk allows all VLANs and uses VLAN 1 as the native VLAN.

Table 3-7 Resetting Configured Values on Trunk Links

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface** *interface-id*
Force the link to be a trunk link.	S1(config-if)# **no switchport trunk allowed vlan**
Specify a native VLAN for 802.1Q trunks.	S1(config-if)# **no switchport trunk native vlan**
Return to the privileged EXEC mode.	S1(config-if)# **end**

Example 3-10 shows the commands used to reset all trunking characteristics of a trunking interface to the default settings. The **show interfaces f0/1 switchport** command reveals that the trunk has been reconfigured to a default state.

Example 3-10 Resetting Trunk Link

```
S1(config)# interface f0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

In Example 3-11, the sample output shows the commands used to remove the trunk feature from the F0/1 switch port on switch S1. The **show interfaces f0/1 switchport** command reveals that the F0/1 interface is now in static access mode.

Example 3-11 Return Port to Access Mode

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
```

```
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
```

Verifying Trunk Configuration (3.2.2.3)

Example 3-12 displays the configuration of switch port F0/1 on switch S1. The configuration is verified with the **show interfaces** *interface-id* **switchport** command.

Example 3-12 Verifying Trunk Configuration

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

The top highlighted area shows that port F0/1 has its administrative mode set to **trunk**. The port is in trunking mode. The next highlighted area verifies that the native VLAN is VLAN 99. Farther down in the output, the bottom highlighted area shows that all VLANs are enabled on the trunk.

Interactive Graphic

Activity 3.2.2.3: Configuring and Verifying a VLAN Trunk

Go to the online course to use the Syntax Checker in the second graphic to configure a trunk supporting all VLANs on interface F0/1 with native VLAN 99. Verify the trunk configuration with the **show interfaces f0/1 switchport** command.

Packet Tracer Activity

Packet Tracer Activity 3.2.2.4: Configuring Trunks

Trunks are required to pass VLAN information between switches. A port on a switch is either an access port or a trunk port. Access ports carry traffic from a specific VLAN assigned to the port. A trunk port by default is a member of all VLANs; therefore, it carries traffic for all VLANs. This activity focuses on creating trunk ports and assigning them to a native VLAN other than the default.

Lab 3.2.2.5: Configuring VLANs and Trunking

In this lab, you will complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Create VLANs and Assign Switch Ports
- Part 3: Maintain VLAN Port Assignments and the VLAN Database
- Part 4: Configure an 802.1Q Trunk Between the Switches
- Part 5: Delete the VLAN Database

Dynamic Trunking Protocol (3.2.3)

Networking technologies often involve both manual and automatic implementations. For example, routing, speed/duplex port configuration, and cable selection versus auto-MDIX illustrate this dichotomy of manual versus automatic. In LAN switching, Dynamic Trunking Protocol (DTP) is one of the first examples one encounters of manual versus automatic. With DTP, network administrators have the option to let neighboring switches autonegotiate trunk formation.

Introduction to DTP (3.2.3.1)

Ethernet trunk interfaces support different trunking modes. An interface can be set to trunking or nontrunking, or to negotiate trunking with the neighbor interface. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which operates on a point-to-point basis only between network devices.

DTP is a Cisco-proprietary protocol that is automatically enabled on Catalyst 2960 and Catalyst 3560 Series switches. Switches from other vendors do not support DTP. DTP manages trunk negotiation only if the port on the neighbor switch is configured in a trunk mode that supports DTP.

Caution

Some internetworking devices might forward DTP frames improperly, which can cause misconfigurations. To avoid this, turn off DTP on interfaces on a Cisco switch connected to devices that do not support DTP.

The default DTP configuration for Cisco Catalyst 2960 and 3560 switches is dynamic auto, as shown in Figure 3-13 on interface F0/3 of switches S1 and S3.

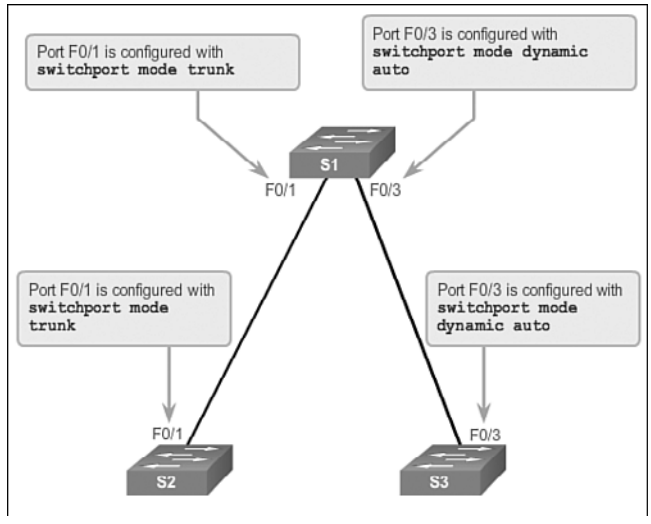


Figure 3-13 Initial DTP Configuration

To enable trunking from a Cisco switch to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration mode commands. This causes the interface to become a trunk, but not generate DTP frames.

In Figure 3-14, the link between switches S1 and S2 becomes a trunk because the F0/1 ports on switches S1 and S2 are configured to ignore all DTP advertisements,

and to come up in and stay in trunk port mode. The F0/3 ports on switches S1 and S3 are set to dynamic auto, so the negotiation results in the access mode state. This creates an inactive trunk link. When configuring a port to be in trunk mode, use the **switchport mode trunk** command. There is no ambiguity about which state the trunk is in; it is always on. With this configuration, it is easy to remember which state the trunk ports are in; if the port is supposed to be a trunk, the mode is set to trunk.

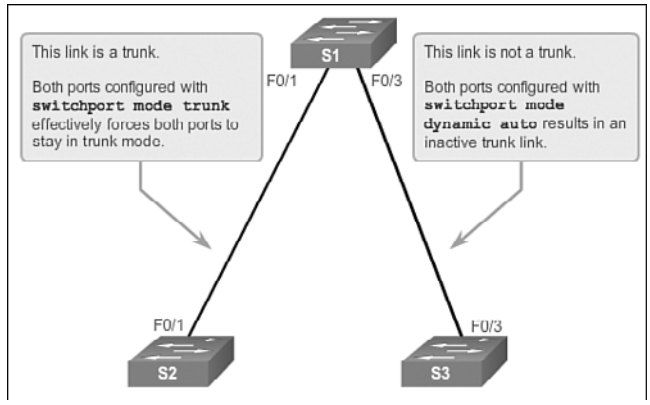


Figure 3-14 DTP Interaction Results

Negotiated Interface Modes (3.2.3.2)

Ethernet interfaces on Catalyst 2960 and Catalyst 3560 Series switches support different trunking modes with the help of DTP:

- **switchport mode access:** Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface, regardless of whether the neighboring interface is a trunk interface.
- **switchport mode dynamic auto:** Makes the interface able to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode. The default switch port mode for all Ethernet interfaces is **dynamic auto**.
- **switchport mode dynamic desirable:** Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode. This is the default switch port mode on older switches, such as the Catalyst 2950 and 3550 Series switches.
- **switchport mode trunk:** Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.

- **switchport nonegotiate:** Prevents the interface from generating DTP frames. You can use this command only when the interface switch port mode is **access** or **trunk**. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

Table 3-8 illustrates the results of the DTP configuration options on opposite ends of a trunk link connected to Catalyst 2960 switch ports.

Table 3-8 DTP-Negotiated Interface Modes

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Access

Configure trunk links statically whenever possible. The default DTP mode is dependent on the Cisco IOS Software version and on the platform. To determine the current DTP mode, issue the **show dtp interface** command, as shown in Example 3-13.

Example 3-13 Verifying DTP Mode

```
S1# show dtp interface f0/1
DTP information for FastEthernet0/1:
  TOS/TAS/TNS:                              TRUNK/ON/TRUNK
  TOT/TAT/TNT:                              802.1Q/802.1Q/802.1Q
  Neighbor address 1:                       0CD996D23F81
  Neighbor address 2:                       000000000000
  Hello timer expiration (sec/state):       12/RUNNING
  Access timer expiration (sec/state):      never/STOPPED
  Negotiation timer expiration (sec/state): never/STOPPED
  Multidrop timer expiration (sec/state):   never/STOPPED
  FSM state:                                S6:TRUNK
  # times multi & trunk                     0
  Enabled:                                  yes
  In STP:
<output omitted>
```

Interactive Graphic

Activity 3.2.3.2: Verifying DTP Mode

Go to the online course to use the Syntax Checker in the third graphic to determine the DTP mode on interface F0/1.

Note

A general best practice is to set the interface to **trunk** and **nonegotiate** when a trunk link is required. On links where trunking is not intended, DTP should be turned off.

Interactive Graphic

Activity 3.2.3.3: Predict DTP Behavior

Go to the online course to perform this practice activity.

Troubleshoot VLANs and Trunks (3.2.4)

A network administrator responsible for portions of the switched infrastructure is able to quickly diagnose and solve problems. Troubleshooting VLANs and VLAN trunks is standard practice in a switched environment.

IP Addressing Issues with VLAN (3.2.4.1)

Each VLAN must correspond to a unique IP subnet. If two devices in the same VLAN have different subnet addresses, they cannot communicate. This is a common problem, and it is easy to solve by identifying the incorrect configuration and changing the subnet address to the correct one.

In Figure 3-15, PC1 cannot connect to the Web/TFTP server shown.

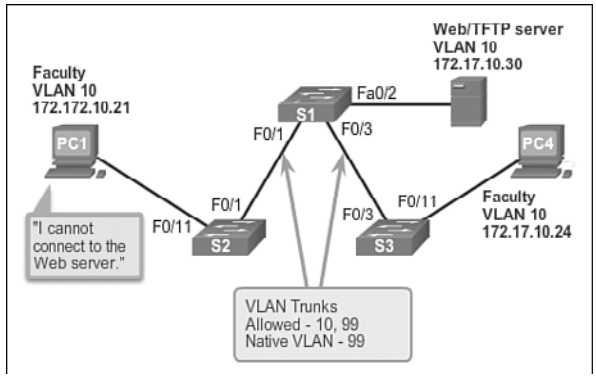


Figure 3-15 IP Issue Within VLAN

A check of the IP configuration settings of PC1 shown in Example 3-14 reveals the most common error in configuring VLANs: an incorrectly configured IP address. PC1 is configured with an IP address of 172.172.10.21, but it should have been configured with 172.17.10.21.

Example 3-14 Problem: Incorrect IP Address

```
PC1> ipconfig
   IPv4 Address. . . . . . . . . . . : 172.172.10.21
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 0.0.0.0
```

The PC1 Fast Ethernet configuration dialog box shows the updated IP address of 172.17.10.21. In Figure 3-16, the output on the bottom reveals that PC1 has regained connectivity to the Web/TFTP server found at IP address 172.17.10.30.

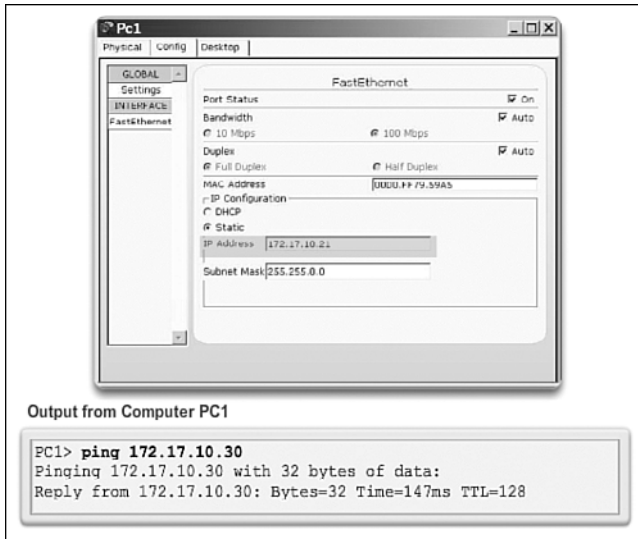


Figure 3-16 Solution: Change PC IP Address

Missing VLANs (3.2.4.2)

If there is still no connection between devices in a VLAN, but IP addressing issues have been ruled out, refer to the flowchart in Figure 3-17 to troubleshoot:

How To

Step 1. Use the **show vlan** command to check whether the port belongs to the expected VLAN. If the port is assigned to the wrong VLAN, use the **switchport access vlan** command to correct the VLAN membership. Use the **show mac address-table** command to check which addresses were learned on a particular port of the switch and to which VLAN that port is assigned.

Step 2. If the VLAN to which the port is assigned is deleted, the port becomes inactive. Use the **show vlan** or **show interfaces switchport** command.

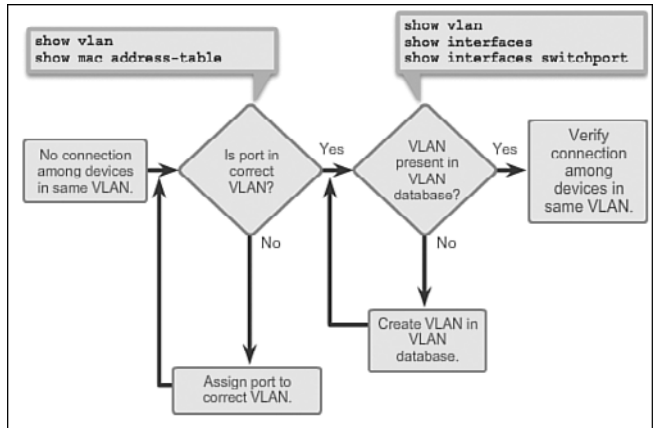


Figure 3-17 Missing VLAN

To display the MAC address table, use the **show macaddress-table** command. Example 3-15 shows MAC addresses that were learned on the F0/1 interface. It can be seen that MAC address 000c.296a.a21c was learned on interface F0/1 in VLAN 10. If this number is not the expected VLAN number, change the port VLAN membership using the **switchport access vlan** command.

Example 3-15 Missing VLAN

```
S1# show mac address-table interface FastEthernet 0/1
          Mac Address Table

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    000c.296a.a21c    DYNAMIC     Fa0/1
  10    000f.34f9.9181    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 2
S1# show interfaces FastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

Each port in a switch belongs to a VLAN. If the VLAN to which the port belongs is deleted, the port becomes inactive. All ports belonging to the VLAN that was deleted are unable to communicate with the rest of the network. Use the **show interface f0/1 switchport** command to check whether the port is inactive. If the port is inactive, it is not functional until the missing VLAN is created using the **vlan** *vlan-id* command.

Introduction to Troubleshooting Trunks (3.2.4.3)

A common task of a network administrator is to troubleshoot trunk link formation or links incorrectly behaving as trunk links. Sometimes a switch port can behave like a trunk port even if it is not configured as a trunk port. For example, an access port might accept frames from VLANs different from the VLAN to which it is assigned. This is called VLAN leaking.

Figure 3-18 displays a flowchart of general trunk troubleshooting guidelines.

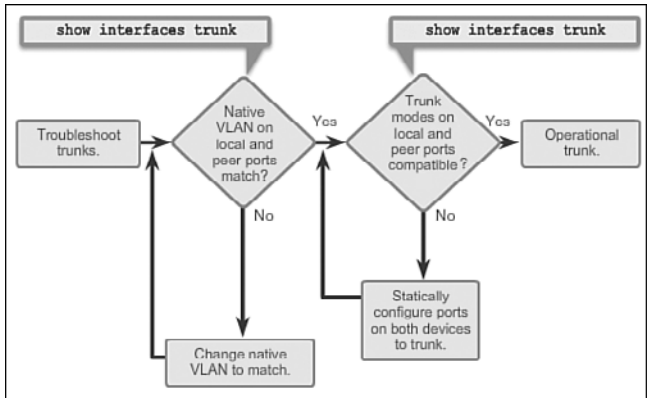


Figure 3-18 Troubleshooting Trunks

To troubleshoot issues when a trunk is not forming or when VLAN leaking is occurring, proceed as follows:

How To

Step 1. Use the **show interfaces trunk** command to check whether the local and peer native VLANs match. If the native VLAN does not match on both sides, VLAN leaking occurs.

Step 2. Use the **show interfaces trunk** command to check whether a trunk has been established between switches. Statically configure trunk links whenever possible. Cisco Catalyst switch ports use DTP by default and attempt to negotiate a trunk link.

To display the status of the trunk and to display the native VLAN used on that trunk link, and to verify trunk establishment, use the **show interfaces trunk** command. Example 3-16 shows that the native VLAN on one side of the trunk link was changed

to VLAN 2. If one end of the trunk is configured as native VLAN 99 and the other end is configured as native VLAN 2, a frame sent from VLAN 99 on one side is received on VLAN 2 on the other side. VLAN 99 leaks into the VLAN 2 segment.

Example 3-16 Troubleshooting Trunks

```
S1# show interfaces f0/1 trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       auto             802.1q         trunking      2
<output omitted>
```

CDP displays a notification of a native VLAN mismatch on a trunk link with this message:

```
*Mar 1 06:45:26.232: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/1 (2), with S2 FastEthernet0/1 (99).
```

Connectivity issues occur in the network if a native VLAN mismatch exists. Data traffic for VLANs, other than the two native VLANs configured, successfully propagates across the trunk link, but data associated with either of the native VLANs does not successfully propagate across the trunk link.

As shown in Example 3-16, native VLAN mismatch issues do not keep the trunk from forming. To solve the native VLAN mismatch, configure the native VLAN to be the same VLAN on both sides of the link.

Common Problems with Trunks (3.2.4.4)

Trunking issues are usually associated with incorrect configurations. When configuring VLANs and trunks on a switched infrastructure, the following types of configuration errors are the most common:

- **Native VLAN mismatches:** Trunk ports are configured with different native VLANs. This configuration error generates console notifications, and causes control and management traffic to be misdirected. This poses a security risk. For example, one port might be configured with VLAN 99 and the other with VLAN 100.
- **Trunk mode mismatches:** One trunk port is configured in a mode that is not compatible for trunking on the corresponding peer port. This configuration error causes the trunk link to stop working. For example, both local and peer switch port modes might be configured as dynamic auto.

- **Allowed VLANs on trunks:** The list of allowed VLANs on a trunk has not been updated with the current VLAN trunking requirements. In this situation, unexpected traffic or no traffic is being sent over the trunk. For example, the list of allowed VLANs might not support current VLAN trunking requirements.

If an issue with a trunk is discovered and if the cause is unknown, start troubleshooting by examining the trunks for a native VLAN mismatch. If that is not the cause, check for trunk mode mismatches, and finally check for the allowed VLAN list on the trunk. The next several sections examine how to fix the common problems with trunks.

Trunk Mode Mismatches (3.2.4.5)

Trunk links are normally configured statically with the **switchport mode trunk** command. Cisco Catalyst switch trunk ports use DTP to negotiate the state of the link. When a port on a trunk link is configured with a trunk mode that is incompatible with the neighboring trunk port, a trunk link fails to form between the two switches.

In the scenario illustrated in Figure 3-19, PC4 cannot connect to the internal web server. The topology indicates a valid configuration. Why is there a problem?

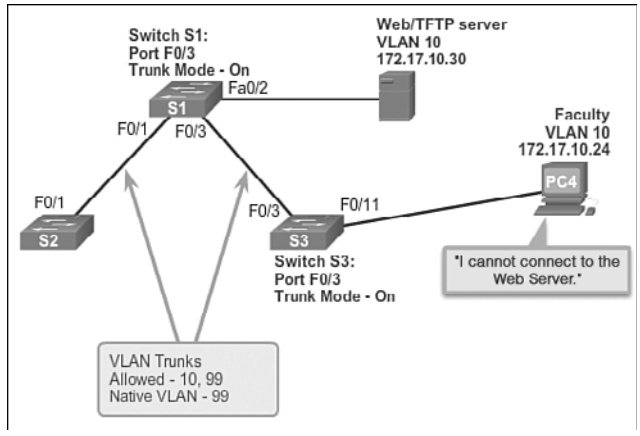


Figure 3-19 Scenario Topology

Check the status of the trunk ports on switch S1 using the **show interfaces trunk** command. The output shown in Example 3-17 reveals that interface Fa0/3 on switch S1 is not currently a trunk link. Examining the F0/3 interface reveals that the switch port is actually in dynamic auto mode. An examination of the trunks on switch S3 reveals that there are no active trunk ports. Further checking reveals that the Fa0/3 interface is also in dynamic auto mode. This explains why the trunk is down.

Example 3-17 Mismatched DTP Modes

```
S1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99

Port        Vlans allowed and active in management domain
Fa0/1       10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,99
S1# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
<output omitted>
S3# show interfaces trunk
S3# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
<output omitted>
```

To resolve the issue, reconfigure the trunk mode of the F0/3 ports on switches S1 and S3, as shown in Example 3-18. After the configuration change, the output of the **show interfaces** command indicates that the port on switch S1 is now in trunking mode. The output from PC4 indicates that it has regained connectivity to the Web/TFTP server found at IP address 172.17.10.30.

Example 3-18 Corrected Trunk Modes

```
S1(config)# interface f0/3
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
<output omitted>
S3(config)# interface f0/3
S3(config-if)# switchport mode trunk
```

```
S3(config-if)# end
S3# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
<output omitted>
S3# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/3       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/3       10,99

Port        Vlans allowed and active in management domain
Fa0/3       10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/3       10,99
PC4> ping 172.17.10.30
Pinging 172.17.10.30 with 32 bytes of data:
Reply from 172.17.10.30: bytes=32 time=147ms TTL=128
<output omitted>
```

Incorrect VLAN List (3.2.4.6)

For traffic from a VLAN to be transmitted across a trunk, it must be allowed on the trunk. To do so, use the **switchport trunk allowed vlan** *vlan-id* command.

In Figure 3-20, VLAN 20 (Student) and PC5 have been added to the network. The documentation has been updated to show that the VLANs allowed on the trunk are 10, 20, and 99. In this scenario, PC5 cannot connect to the student email server.

Check the trunk ports on switch S1 using the **show interfaces trunk** command, as shown in Example 3-19. The command reveals that the interface F0/3 on switch S3 is correctly configured to allow VLANs 10, 20, and 99. An examination of the F0/3 interface on switch S1 reveals that interfaces F0/1 and F0/3 only allow VLANs 10 and 99. Someone updated the documentation but forgot to reconfigure the ports on the S1 switch.

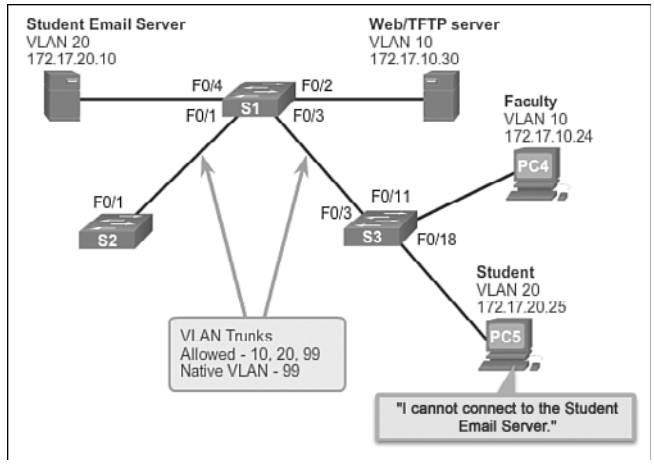


Figure 3-20 Scenario Topology

Example 3-19 Missing VLANs

```
S3# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/3       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/3       10,20,99

Port        Vlans allowed and active in management domain
Fa0/3       10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/3       10,20,99
S1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99
Fa0/3       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99
Fa0/3       10,99
<output omitted>
```

Reconfigure F0/1 and F0/3 on switch S1 using the **switchport trunk allowed vlan 10,20,99** command, as shown in Example 3-20. The output shows that VLANs 10, 20, and 99 are now added to the F0/1 and F0/3 ports on switch S1. The **show interfaces trunk** command is an excellent tool for revealing common trunking problems. PC5 has regained connectivity to the student email server found at IP address 172.17.20.10

Example 3-20 Corrected VLAN List

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk allowed vlan 10,20,99
S1(config-if)# interface f0/3
S1(config-if)# switchport trunk allowed vlan 10,20,99
S1(config-if)# end
S1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99
Fa0/3       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,20,99
Fa0/3       10,20,99
<output omitted>
PC5> ping 172.17.20.10
Pinging 172.17.10.30 with 32 bytes of data:
Reply from 172.17.10.30: bytes=32 time=147ms TTL=128
<output omitted>
```

Packet Tracer Activity

Packet Tracer Activity 3.2.4.7: Troubleshooting a VLAN Implementation—Scenario 1

In this activity, you will troubleshoot connectivity problems between PCs on the same VLAN. The activity is complete when PCs on the same VLAN can ping each other. Any solution you implement must conform to the addressing table.

Packet Tracer Activity

Packet Tracer Activity 3.2.4.8: Troubleshooting a VLAN Implementation—Scenario 2

In this activity, you will troubleshoot a misconfigured VLAN environment. The initial network has errors. Your objective is to locate and correct the errors in the configurations and establish end-to-end connectivity. Your final configuration should match the topology diagram and addressing table. The native VLAN for this topology is VLAN 56.

Lab 3.2.4.9: Troubleshooting VLAN Configurations

In this lab, you will complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Troubleshoot VLAN 10
- Part 3: Troubleshoot VLAN 20

VLAN Security and Design (3.3)

The proliferation of network security certifications indicates that the importance of network security is growing. Every configuration, monitoring, maintenance, and troubleshooting procedure in a switched network must include an analysis of the security implications. VLANs and VLAN technologies play an integral role in the design and implementation of switched networks.

Attacks on VLANs (3.3.1)

A number of attacks are specific to the VLAN infrastructure. In this section, the various types of attacks involving VLANs are explored.

Switch Spoofing Attack (3.3.1.1)

There are a number of different types of VLAN attacks in modern switched networks. The VLAN architecture simplifies network maintenance and improves performance, but it also opens the door to abuse. It is important to understand the general methodology behind these attacks and the primary approaches to mitigate them.

VLAN hopping enables traffic from one VLAN to be seen by another VLAN. Switch spoofing is a type of VLAN hopping attack that works by taking advantage of an incorrectly configured trunk port. By default, trunk ports have access to all VLANs and pass traffic for multiple VLANs across the same physical link, generally between switches.

Figure 3-21 illustrates a *switch spoofing attack*.

In a basic switch spoofing attack, the attacker takes advantage of the fact that the default configuration of the switch port is dynamic auto. The network attacker configures a system to spoof itself as a switch. This spoofing requires that the network attacker be capable of emulating 802.1Q and DTP messages. By tricking a switch into thinking that another switch is attempting to form a trunk, an attacker can gain access to all the VLANs allowed on the trunk port.

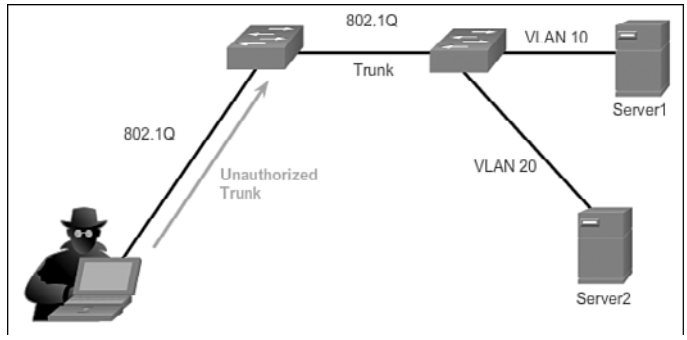


Figure 3-21 Switch Spoofing Attack

The best way to prevent a basic switch spoofing attack is to turn off trunking on all ports, except the ones that specifically require trunking. On the required trunking ports, disable DTP and manually enable trunking.

Double-Tagging Attack (3.3.1.2)

Another type of VLAN attack is a double-tagging (or double-encapsulated) VLAN hopping attack. This type of attack takes advantage of the way that hardware on most switches operates. Most switches perform only one level of 802.1Q deencapsulation, which allows an attacker to embed a hidden 802.1Q tag inside the frame. This tag allows the frame to be forwarded to a VLAN that the original 802.1Q tag did not specify. An important characteristic of the double-encapsulated VLAN hopping attack is that it works even if trunk ports are disabled, because a host typically sends a frame on a segment that is not a trunk link.

A *double-tagging attack*, illustrated in Figure 3-22, follows three steps:

1. The attacker sends a double-tagged 802.1Q frame to the switch. The outer header has the VLAN tag of the attacker, which is the same as the native VLAN of the trunk port. The assumption is that the switch processes the frame received from the attacker as if it were on a trunk port or a port with a voice VLAN (a switch should not receive a tagged Ethernet frame on an access port). For the purposes of this example, assume that the native VLAN is VLAN 10. The inner tag is the victim VLAN, in this case, VLAN 20.
2. The frame arrives on the switch, which looks at the first 4-byte 802.1Q tag. The switch sees that the frame is destined for VLAN 10, which is the native VLAN. The switch forwards the packet out on all VLAN 10 ports after stripping the VLAN 10 tag. On the trunk port, the VLAN 10 tag is stripped, and the packet is not retagged because it is part of the native VLAN. At this point, the VLAN 20 tag is still intact and has not been inspected by the first switch.

3. The second switch looks only at the inner 802.1Q tag that the attacker sent and sees that the frame is destined for VLAN 20, the target VLAN. The second switch sends the frame on to the victim port or floods it, depending on whether there is an existing MAC address table entry for the victim host.

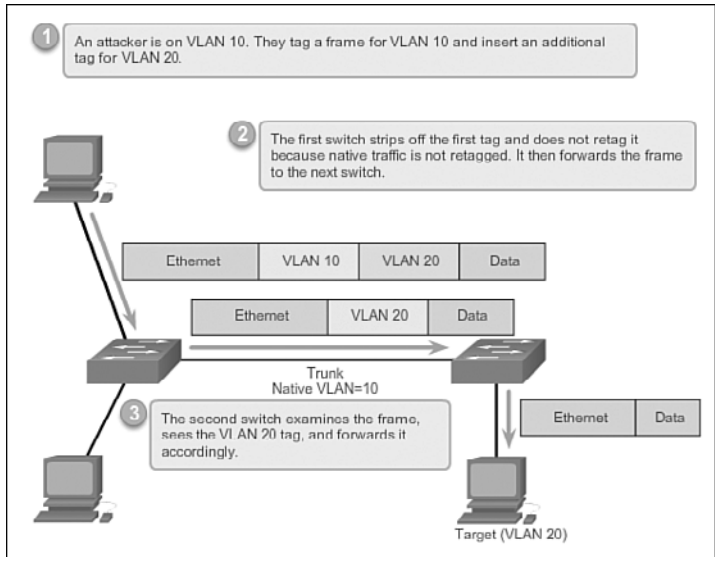


Figure 3-22 Double-Tagging Attack

This type of attack is unidirectional and works only when the attacker is connected to a port residing in the same VLAN as the native VLAN of the trunk port. Thwarting this type of attack is not as easy as stopping basic VLAN hopping attacks.

The best approach to mitigating double-tagging attacks is to ensure that the native VLAN of the trunk ports is different from the VLAN of any user ports. In fact, it is considered a security best practice to use a fixed VLAN that is distinct from all user VLANs in the switched network as the native VLAN for all 802.1Q trunks.

PVLAN Edge (3.3.1.3)

Some applications require that no traffic be forwarded at Layer 2 between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor. In such an environment, the use of the ***Private VLAN (PVLAN) Edge*** feature, also known as ***protected ports***, ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch, as shown in Figure 3-23.

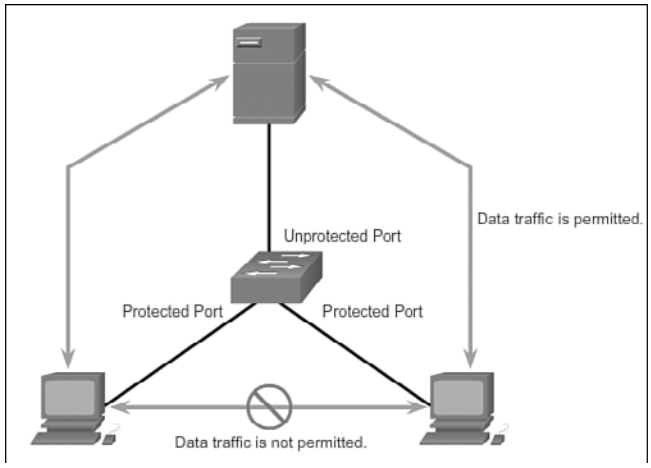


Figure 3-23 Private VLAN Edge

The PVLAN Edge feature has the following characteristics:

- A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port, except for control traffic. Data traffic cannot be forwarded between protected ports at Layer 2.
- Forwarding behavior between a protected port and a nonprotected port proceeds as usual.
- Protected ports must be manually configured.

To configure the PVLAN Edge feature, enter the **switchport protected** command in interface configuration mode, as shown in Example 3-21. To disable protected port, use the **no switchport protected** interface configuration mode command. To verify the configuration of the PVLAN Edge feature, use the **show interfaces** *interface-id* **switchport** global configuration mode command.

Example 3-21 PVLAN Edge

```
S1(config)# interface g0/1
S1(config-if)# switchport protected
S1(config-if)# end
S1# show interfaces g0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
```

```
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<output omitted>
Protected: true
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Interactive Graphic

Activity 3.3.1.3: PVLAN Edge

Go to the online course to use the Syntax Checker in the third graphic to configure the PVLAN Edge feature on interface G0/1 and verify the configuration.

Interactive Graphic

Activity 3.3.1.4: Identify the Type of VLAN Attacks

Go to the online course to perform this practice activity.

VLAN Best Practices (3.3.2)

VLAN best practices refer to those practices that any network administrator responsible for portions of a switched network should employ in his day-to-day work. These comprise standard operating procedures for switch practitioners.

VLAN Design Guidelines (3.3.2.1)

Cisco switches have a factory configuration in which default VLANs are preconfigured to support various media and protocol types. The default Ethernet VLAN is VLAN 1. It is a security best practice to configure all the ports on all switches to be associated with VLANs other than VLAN 1. This is usually done by configuring all unused ports to a ***black hole VLAN*** that is not used for anything on the network. All used ports are associated with VLANs distinct from VLAN 1 and distinct from the black hole VLAN. It is also a good practice to shut down unused switch ports to prevent unauthorized access.

A good security practice is to separate management and user data traffic. The management VLAN, which is VLAN 1 by default, should be changed to a separate, distinct VLAN. To communicate remotely with a Cisco switch for management purposes, the switch must have an IP address configured on the management VLAN. Users in other VLANs would not be able to establish remote access sessions to the switch unless they were routed into the management VLAN, providing an additional layer

of security. Also, the switch should be configured to accept only encrypted SSH sessions for remote management.

All control traffic is sent on VLAN 1. Therefore, when the native VLAN is changed to something other than VLAN 1, all control traffic is tagged on IEEE 802.1Q VLAN trunks (tagged with VLAN ID 1). A recommended security practice is to change the native VLAN to a different VLAN than VLAN 1. The native VLAN should also be distinct from all user VLANs. Ensure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link.

DTP offers four switch port modes: access, trunk, dynamic auto, and dynamic desirable. A general guideline is to disable autonegotiation. As a port security best practice, do not use the dynamic auto or dynamic desirable switch port modes.

Finally, voice traffic has stringent QoS requirements. If user PCs and IP phones are on the same VLAN, each tries to use the available bandwidth without considering the other device. To avoid this conflict, it is good practice to use separate VLANs for IP telephony and data traffic.

Lab 3.2.4.9: Troubleshooting VLAN Configurations

In this lab, you will complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Implement VLAN Security on the Switches

Summary (3.4)

Class Activity 3.4.1.1: VLAN Plan

You are designing a VLAN switched network for your small- to medium-sized business.

Your business owns space on two floors of a high-rise building. The following elements need VLAN consideration and access for planning purposes:

- Management
- Finance
- Sales
- Human Resources
- Network administrator
- General visitors to your business location

You have two Cisco 3560-24PS switches.

Use a word processing software program to design your VLAN-switched network scheme.

Section 1 of your design should include the regular names of your departments, suggested VLAN names and numbers, and which switch ports would be assigned to each VLAN.

Section 2 of your design should list how security would be planned for this switched network.

When your VLAN plan is finished, complete the reflection questions from this activity's PDF.

Save your work. Be able to explain and discuss your VLAN design with another group or with the class.

Packet Tracer Activity

Packet Tracer Activity 3.4.1.2: Skills Integration Challenge

In this activity, two switches are completely configured. On a third switch, you are responsible for assigning IP addressing to the SVI, configuring VLANs, assigning VLANs to interfaces, configuring trunking, and performing basic switch security.

This chapter introduced VLANs. VLANs are based on logical connections, instead of physical connections. VLANs are a mechanism to allow network administrators to create logical broadcast domains that can span across a single switch or multiple switches, regardless of physical proximity. This function is useful to reduce the size of broadcast domains or to allow groups of users to be logically grouped without the need to be physically located in the same place.

There are several types of VLANs:

- Default VLAN
- Management VLAN
- Native VLAN
- User/Data VLANs
- Black Hole VLAN
- Voice VLAN

On a Cisco switch, VLAN 1 is the default Ethernet VLAN, the default native VLAN, and the default management VLAN. Best practices suggest that the native and management VLANs be moved to another distinct VLAN and that unused switch ports be moved to a "black hole" VLAN for increased security.

The **switchport access vlan** command is used to create a VLAN on a switch. After creating a VLAN, the next step is to assign ports to the VLAN. The **show vlan brief** command displays the VLAN assignment and membership type for all switch ports. Each VLAN must correspond to a unique IP subnet.

Use the **show vlan** command to check whether the port belongs to the expected VLAN. If the port is assigned to the wrong VLAN, use the **switchport access vlan** command to correct the VLAN membership. Use the **show mac address-table** command to check which addresses were learned on a particular port of the switch and to which VLAN that port is assigned.

A port on a switch is either an access port or a trunk port. Access ports carry traffic from a specific VLAN assigned to the port. A trunk port by default is a member of all VLANs; therefore, it carries traffic for all VLANs.

VLAN trunks facilitate inter-switch communication by carrying traffic associated with multiple VLANs. IEEE 802.1Q frame tagging differentiates between Ethernet frames associated with distinct VLANs as they traverse common trunk links. To enable trunk links, use the **switchport mode trunk** command. Use the **show interfaces trunk** command to check whether a trunk has been established between switches.

Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which operates on a point-to-point basis only, between network devices. DTP is a Cisco-proprietary protocol that is automatically enabled on Catalyst 2960 and Catalyst 3560 Series switches.

To place a switch into its factory default condition with one default VLAN, use the **delete flash:vlan.dat** and **erase startup-config** commands.

This chapter also examined the configuration, verification, and troubleshooting of VLANs and trunks using the Cisco IOS CLI and explored basic security and design considerations in the context of VLANs.

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion *Switched Networks Lab Manual* (ISBN 978-1-58713-372-5). The Packet Tracer Activities PKA files are found in the online course.

Class Activities

- Class Activity 3.0.1.2: Vacation Station
- Class Activity 3.4.1.1: VLAN Plan

Labs

- Lab 3.2.2.5: Configuring VLANs and Trunking
- Lab 3.2.4.9: Troubleshooting VLAN Configurations

Packet Tracer Activities

- Packet Tracer Activity 3.1.1.5: Who Hears the Broadcast?
- Packet Tracer Activity 3.1.2.7: Investigating a VLAN Implementation
- Packet Tracer Activity 3.2.1.7: Configuring VLANs
- Packet Tracer Activity 3.2.2.4: Configuring Trunks
- Packet Tracer Activity 3.2.4.7: Troubleshooting a VLAN Implementation—Scenario 1
- Packet Tracer Activity 3.2.4.8: Troubleshooting a VLAN Implementation—Scenario 2

Check Your Understanding Questions

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

1. For what reason would a network administrator use the **show interfaces trunk** command on a switch?

   A. To view the native VLAN
   B. To examine DTP negotiation as it occurs
   C. To verify port association with a particular VLAN
   D. To display an IP address for any existing VLAN

2. What is the purpose of the switch command **switchport access vlan 99**?

   A. To enable port security
   B. To make the port operational
   C. To assign the port to a particular VLAN
   D. To designate the VLAN that does not get tagged
   E. To assign the port to the default native VLAN (VLAN 99)

3. Which step should be performed first when deleting a VLAN that has member switch ports?

   A. Reload the switch.
   B. Implement the **delete vlan.dat** command.
   C. Reassign all VLAN member ports to a different VLAN.
   D. Back up the running config.

4. All access ports on a switch are configured with the administrative mode of dynamic auto. An attacker, connected to one of the ports, sends a malicious DTP frame. What is the intent of the attacker?

   A. VLAN hopping attack
   B. DHCP spoofing attack
   C. MAC flooding attack
   D. ARP poisoning attack

5. Which of the following statements accurately describe DTP? (Choose two.)

   A. DTP is a Cisco-proprietary protocol.
   B. DTP supports IEEE 802.1Q.
   C. Cisco switches require DTP to establish trunks.
   D. DTP must be enabled on only one side of the trunk link.
   E. Trunk ports that are configured for dynamic auto will request to enter the trunking state.

6. Match the action to the corresponding command.

   1. Assigns VLAN 10 for untagged traffic
   2. Activates the current interface as trunk
   3. Prohibits VLAN 10 on the trunk interface

   A. Switch(config-if)# **switchport trunk allowed vlan remove 10**
   B. Switch(config-if)# **switchport mode trunk**
   C. Switch(config-if)# **switchport trunk native vlan 10**

7. What is one way to prevent the VLAN hopping attack?

   A. Disable DTP negotiation on all ports.
   B. Change the native VLAN to an unused VLAN.
   C. Designate a different default VLAN.
   D. Remove all user VLANs from the trunk.

8. What security issue is of concern regarding the VLAN configuration of switches?

   A. All interfaces are in the same user VLAN.
   B. The management VLAN is using the same VLAN ID as a user VLAN is using.
   C. The "black hole" VLAN is not configured.
   D. The native VLAN has not been changed from the default setting.

9. In which location are the normal-range VLANs stored on a Cisco switch by default?

   A. Flash memory
   B. Startup config
   C. Running config
   D. RAM

10. Which of the following statements describe the benefits of VLANs? (Choose two.)

    A. VLANs improve network performance by regulating flow control and window size.

    B. VLANs enable switches to route packets to remote networks through VLAN ID filtering.

    C. VLANs reduce network cost by reducing the number of physical ports required on switches.

    D. VLANs improve network security by isolating users that have access to sensitive data and applications.

    E. VLANs divide a network into smaller logical networks, resulting in lower susceptibility to broadcast storms.

11. An administrator is investigating an inoperational trunk link between a Cisco switch and a switch from another vendor. After a few **show** commands, the administrator notices that the switches are not negotiating a trunk. What is a probable cause for this issue?

    A. Both switches are in trunk mode.

    B. Both switches are in nonegotiate mode.

    C. Switches from other vendors do not support DTP.

    D. DTP frames are flooding the entire network.

12. Which distinct type of VLAN is used by an administrator to access and configure a switch?

    A. Default VLAN

    B. Native VLAN

    C. Data VLAN

    D. Management VLAN

This page intentionally left blank

This page intentionally left blank

Index

NUMBERS

A

B

C

D

E

F

G-H

J-K-L

M

N

O

P

Q-R

S

T

U-V

W

X-Y-Z