CHAPTER 1

Introduction to Switched Networks

Objectives

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

- How do switched networks support small to medium-sized businesses?
- How has the convergence of data, voice, and video affected switched networks?
- What benefits are provided by creating networks based on a structured hierarchical design model?
- What are the two most commonly used Cisco hierarchical design models?
- What are the layers found in the Cisco hierarchical design model?
- What switch form factors are available?
- How do Layer 2 switches build and use a MAC address table to forward data?
- What is the difference between a collision domain and a broadcast domain?

Key Terms

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

converged network	*page 3*
hierarchical	*page 6*
modularity	*page 6*
resiliency	*page 7*
flexibility	*page 7*
access layer	*page 8*
distribution layer	*page 8*
core layer	*page 8*
three-tier campus network design	*page 8*
two-tier campus network design	*page 9*
collapsed core network design	*page 9*
fixed configuration switch	*page 13*
modular configuration switch	*page 13*
stackable configuration switch	*page 13*
ingress	*page 15*
egress	*page 15*
MAC address table	*page 16*
application-specific-integrated circuit (ASIC)	*page 19*
store-and-forward switching	*page 19*
cut-through switching	*page 19*
frame-check-sequence (FCS)	*page 20*
collision domain	*page 22*
microsegmentation	*page 23*
broadcast domain	*page 23*

Introduction (1.0.1.1)

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

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

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

Class Activity 1.0.1.2: Sent or Received Instructions

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

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

Note

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

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

LAN Design (1.1)

Hiring managers want networking professionals, even entry level ones, to be able to design a LAN. Why is this so important? If someone knows how to design something, it means that person knows and understands the components that comprise the object. By knowing how to design a LAN, a network professional knows the network components and how those components interact with one another. The professional would also know what products to buy to expand the network.

Converged Networks (1.1.1)

The words *converged network* can mean several things to a network engineer: (1) a single network designed to handle voice, video, and data; (2) an internal network where the Layer 3 devices, such as routers, have a complete routing table to be able to accurately and efficiently send data to a remote destination; and (3) a switch network that has completed calculations that result in a single path through the switch network. In this chapter, we explore the first description.

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, geographic 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.

These next generation networks must not only support current expectations and equipment, but must also be able to integrate legacy platforms. Figure 1-1 shows some common legacy devices that must often be incorporated into network design. Figure 1-2 illustrates some of the newer platforms (converged networks) that help to provide access to the network anytime, anywhere, and on any device.

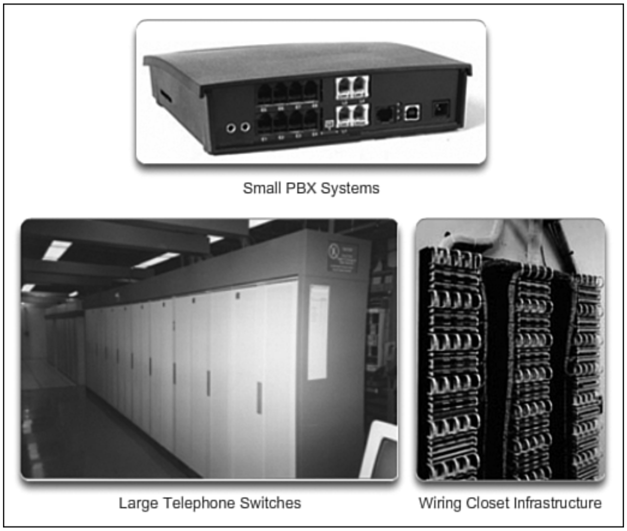


Figure 1-1 Legacy Components

Unified Communication - Media Convergence Server
Cisco Catalyst 2960 LAN Base Switches
Cisco Unified IP Phones

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 video conferencing (Figure 1-3). Including data services, a converged network with collaboration support may include features such as the following:

- **Call control:** Telephone call processing, caller ID, call transfer, hold, and conference
- **Voice messaging:** Voicemail
- **Mobility:** Receive important calls wherever you are
- **Automated attendant:** Serve customers faster by routing calls directly to the right department or individual

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

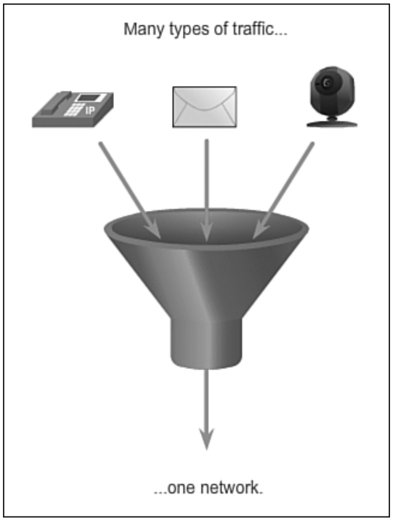


Figure 1-3 Network Traffic Convergence

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

Play the online video to view a few of the collaboration services in action.

Video

Video 1.1.1.2: A Typical Work Day Transformed with People-Centric Collaboration

Go to course section 1.1.1.2. Click on the second graphic, and play the video to see how people can work more efficiently with collaboration tools.

Borderless Switched Networks (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 illustrated by the Cisco Borderless Network architecture illustrated in Figure 1-4.

The Cisco Borderless Network is a network architecture that combines several innovations and design considerations to allow organizations to connect anyone, anywhere, anytime, and 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.

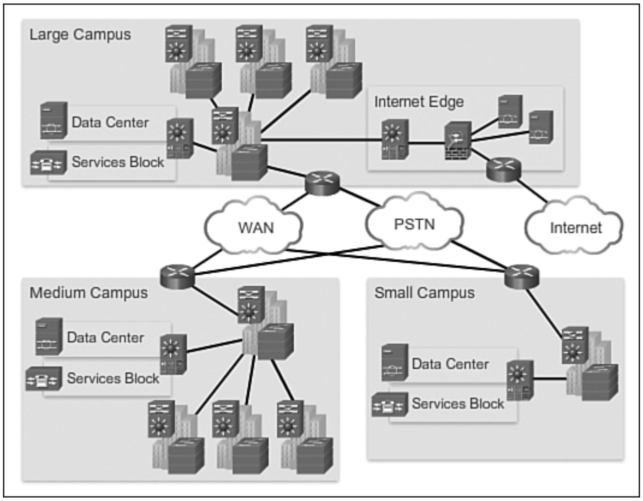


Figure 1-4 Borderless Switched Networks

The Cisco Borderless Network is built on an infrastructure of scalable and resilient hardware and software. It 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, providing optimization, scalability, and security to collaboration and virtualization.

Play the online video to learn more about the evolution of the Cisco Borderless Network.

Video

Video 1.1.1.3: Evolution of Borderless Networks

Go to course section 1.1.1.3. Click on the second graphic and play the video to see how a borderless network affects businesses.

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 and the two-tier layer models, as illustrated in Figure 1-5.

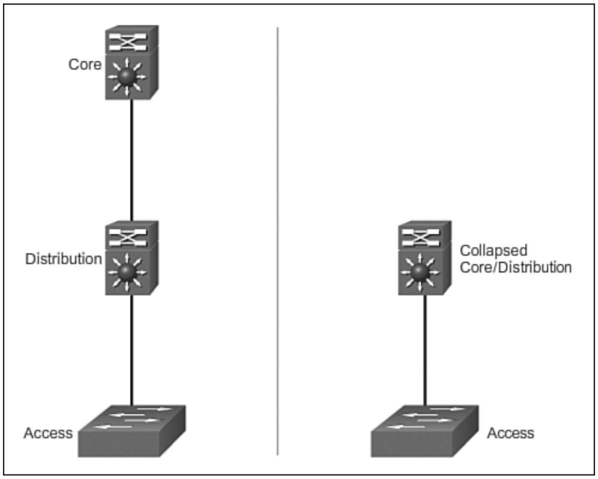


Figure 1-5 Switch Network Design Models

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.

Core Distribution Access (1.1.1.5)

There are three layers of distribution access:

- Access layer
- Distribution layer
- Core layer

These will be discussed in greater detail in this section.

Access Layer

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

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

Distribution Layer

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

- Aggregating large-scale wiring closet networks
- Aggregating Layer 2 broadcast domains and Layer 3 routing boundaries
- Providing intelligent switching, routing, and network access policy functions to access the rest of the network
- Providing high availability through redundant distribution layer switches to the end-user and equal cost paths to the core
- Providing differentiated services to various classes of service applications at the edge of the network

Core Layer

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

Figure 1-6 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.

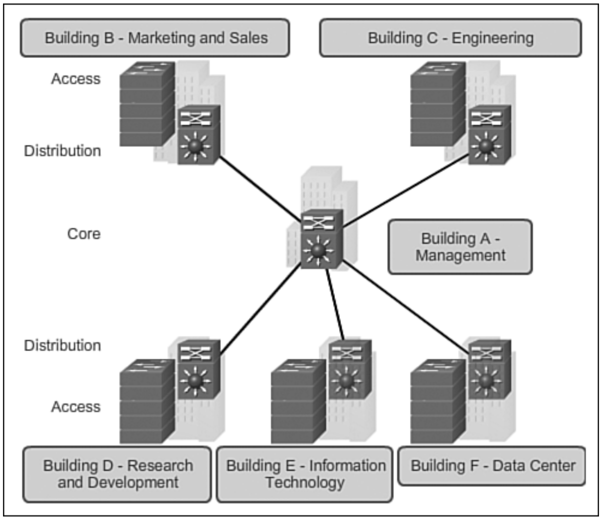


Figure 1-6 Three-Tier Campus Network Design

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

Figure 1-7 shows a two-tier campus network design example for an enterprise campus where the distribution and core layers are collapsed into a single layer.

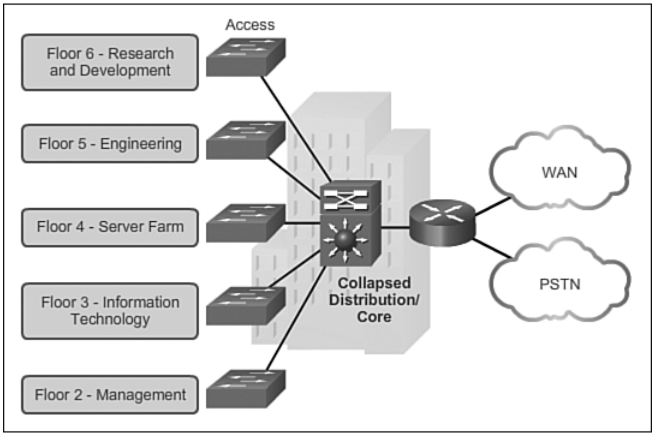

Access
Floor 6 - Research and Development
Floor 5 - Engineering
Floor 4 - Server Farm
Floor 3 - Information Technology
Floor 2 - Management
Collapsed Distribution/ Core
WAN
PSTN

Figure 1-7 Two-Tier Campus Network Design

Interactive Graphic

Activity 1.1.1.6 Part 1: Identify Switched Network Terminology

This activity is found in the course in the first graphic in 1.1.1.6. Go to the online course to match the term with the switch characteristic.

Interactive Graphic

Activity 1.1.1.6 Part 2: Identify Switched Network Layer Functions

Go to the course online and click on the second graphic. Perform the practice activity by matching specific characteristics to one of the three layers of the switch network design model.

Switched Networks (1.1.2)

Switched networks are important when deploying wired LANs. A network professional today must be well-versed in switches and LAN technology in order to add commonly deployed devices such as PCs, printers, video cameras, phones, copiers, and scanners. Sharing and accessing network devices is common in both the home and business network.

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 1-8, networks have fundamentally changed to switched LANs in a hierarchical network. A switched LAN allows more flexibility, traffic management, and additional features, such as:

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

Figure 1-9 shows the hierarchical design used in the borderless switched network.

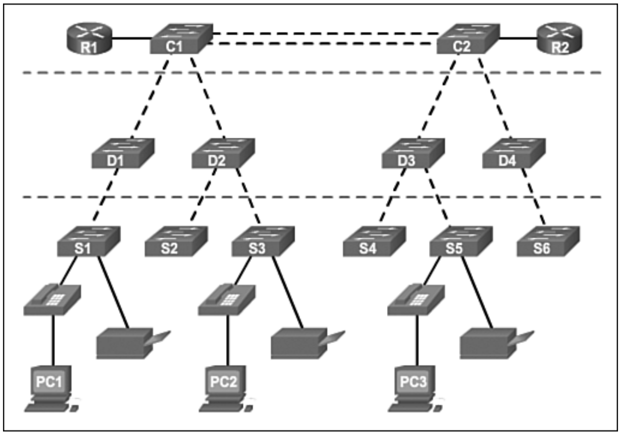


Figure 1-8 Hierarchical Networks

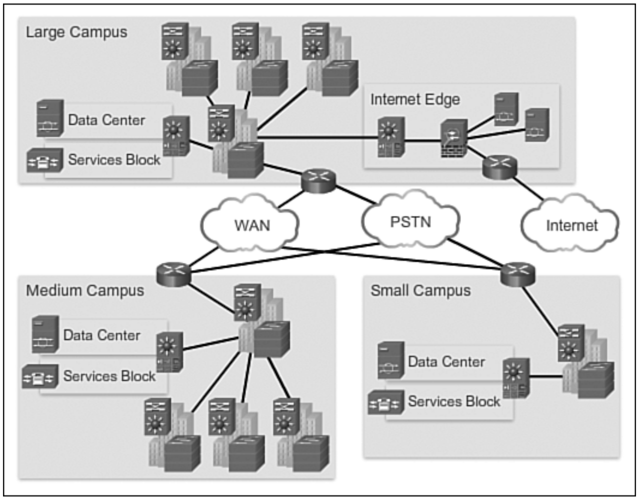


Figure 1-9 Three-Tier Design in Borderless Switched Networks

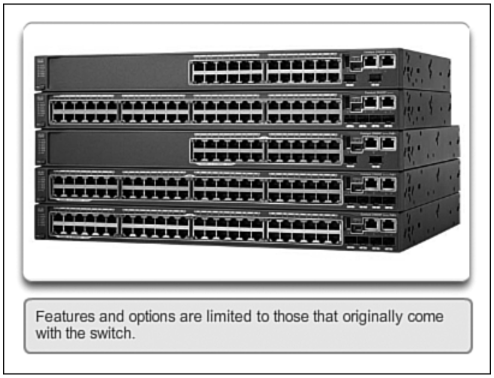
Form Factors (1.1.2.2)

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

Table 1-1 Business Considerations for Switch Selection

Switch Feature	Business Consideration
Cost	The cost of a switch will depend on the number and speed of the interfaces, supported features, and expansion capability.
Port density	Network switches must support the appropriate number of devices on the network.
Power	It is now common to power access points, IP phones, and even compact switches using Power over Ethernet (PoE). In addition to PoE considerations, some chassis-based switches support redundant power supplies.
Reliability	The switch should provide continuous access to the network.
Port speed	The speed of the network connection is of primary concern to the end users.
Frame buffers	The capability of the switch to store frames is important in a network where there may 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 non-stackable. Another consideration is the thickness of the switch, which is expressed in number of rack units. This is important for switches that are mounted in a rack. For example, the fixed configuration switches shown in Figure 1-10 are all 1 rack unit (1U). These options are sometimes referred to as switch form factors.



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

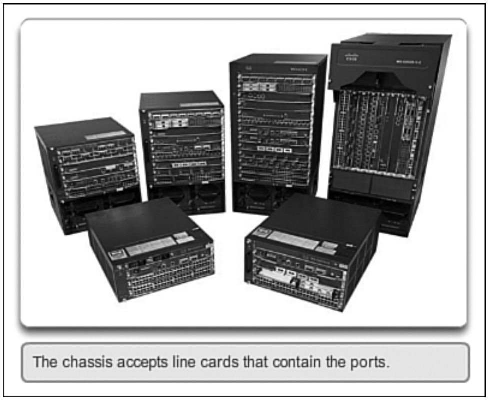
Figure 1-10 Fixed Configuration Switches

Fixed Configuration Switches

Fixed configuration switches do not support features or options beyond those that originally came with the switch (refer to Figure 1-10). The particular model determines the features and options available. For example, a 24-port gigabit fixed switch cannot support additional ports. There are typically different configuration choices that vary in how many and what types of ports are included with a fixed configuration switch.

Modular Configuration Switches

Modular configuration switches offer more flexibility in their configuration. Modular configuration switches typically come with different sized chassis that allow for the installation of different numbers of modular line cards (Figure 1-11). 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 24-port line card supports an additional 24-port line card, to bring the total number of ports up to 48.

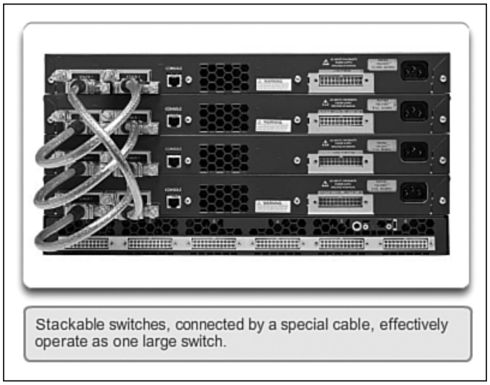


The chassis accepts line cards that contain the ports.

Figure 1-11 Modular Configuration Switches

Stackable Configuration Switches

Stackable configuration switches can be interconnected using a special cable that provides high-bandwidth throughput between the switches (Figure 1-12). 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.



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

Figure 1-12 Stackable Configuration Switches

Interactive Graphic

Activity 1.1.2.3: Identify Switch Hardware

Go to the online course to match the term to the switch selection criteria.

The Switched Environment (1.2)

One of the most exciting functions of networking is the switched environment because businesses are always adding devices to the wired network, and they will do so through a switch. Learning how switches operate is important to someone entering the networking profession.

Frame Forwarding (1.2.1)

On Ethernet networks, frames contain a source MAC address and a destination MAC address. Switches receive a frame from the source device and quickly forward it toward the destination device.

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
- Destination address

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

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

A LAN switch maintains a table that it uses to determine how to forward traffic through the switch.

Interactive Graphic

Activity 1.2.1.1: LAN Switch Forwarding Operation

Go to the course online to see an animation of how a switch forwards a frame based on the destination MAC address. Click the Play button to begin.

In the animated example:

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

The only intelligence of the LAN switch is its capability 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 outbound port toward the destination. A switch is made up of integrated circuits and 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 table,*** or content addressable memory (CAM) table. CAM is a special type of memory used in high-speed searching applications.

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

An easy way to remember how a switch operates is the following saying: A switch learns on "source" and forwards based on "destination." This means that a switch populates the MAC address table based on source MAC addresses. As frames enter the switch, the switch "learns" the source MAC address of the received frame and adds the MAC address to the MAC address table or refreshes the age timer of an existing MAC address table entry.

To forward the frame, the switch examines the destination MAC address and compares it to addresses found in the MAC address table. If the address is in the table, the frame is forwarded out the port associated with the MAC address in the table. When the destination MAC address 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. 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:

How To

Step 1. The switch receives a frame from PC 1 on Port 1 (Figure 1-13).

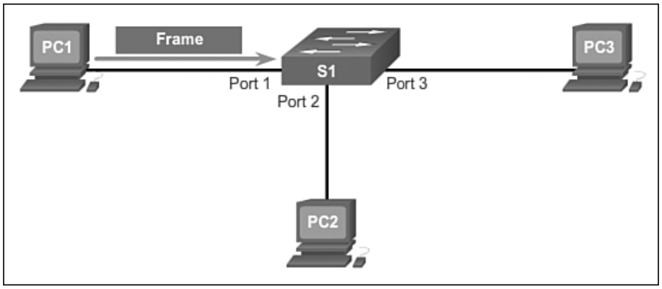


Figure 1-13 Building a MAC Address Table: PC1 Sends Frame to Port 1

Step 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 (Figure 1-14).
- 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.

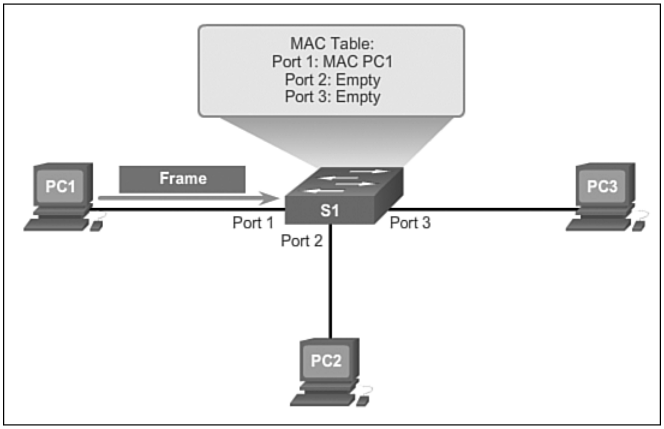


Figure 1-14 Building a MAC Address Table: S1 Adds MAC Address Heard Through Port 1

Step 3. After the switch has recorded the source address information, the switch examines the destination MAC address.

- If the destination address is not in the MAC table or if it's a broadcast MAC address, as indicated by all Fs, the switch floods the frame to all ports, except the ingress port (Figure 1-15).

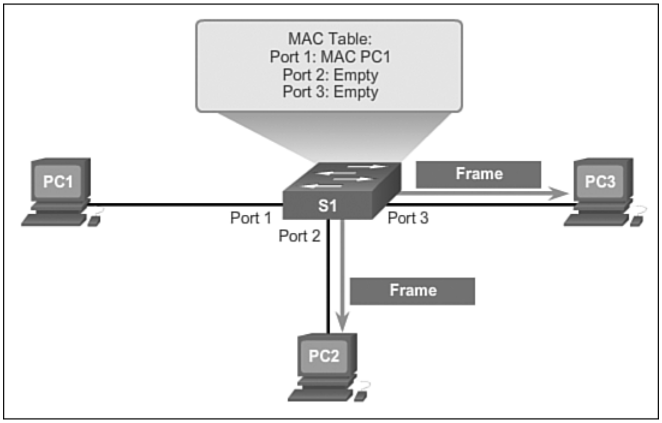


Figure 1-15 Building a MAC Address Table: S1 Broadcasts the Frame

Step 4. The destination device (PC 3) replies to the frame with a unicast frame addressed to PC 1 (Figure 1-16).

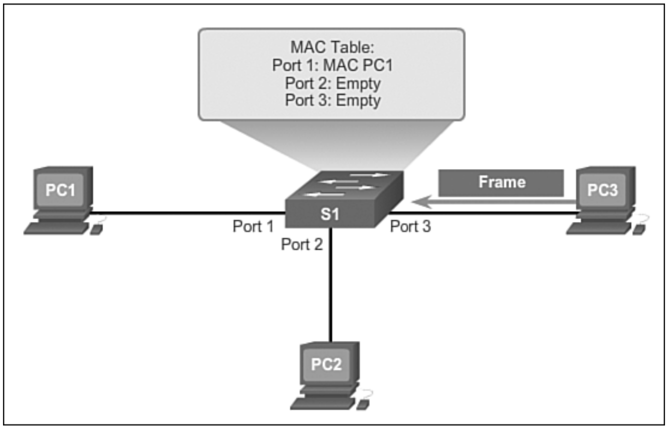


Figure 1-16 Building a MAC Address Table: PC3 Sends a Reply Frame

Step 5. The switch enters the source MAC address of PC 3 and the port number of the ingress port into the address table. The destination address of the frame and its associated egress port is found in the MAC address table (Figure 1-17).

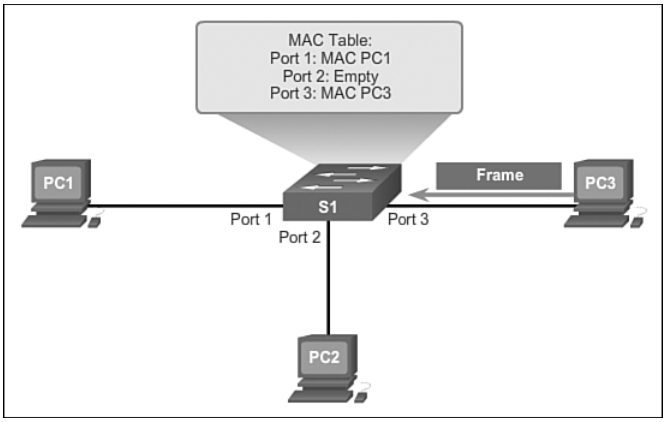


Figure 1-17 Building a MAC Address Table: S1 Adds the MAC Address for PC3

Step 6. The switch can now forward frames between these source and destination devices without flooding because it has entries in the address table that identify the associated ports (Figure 1-18).

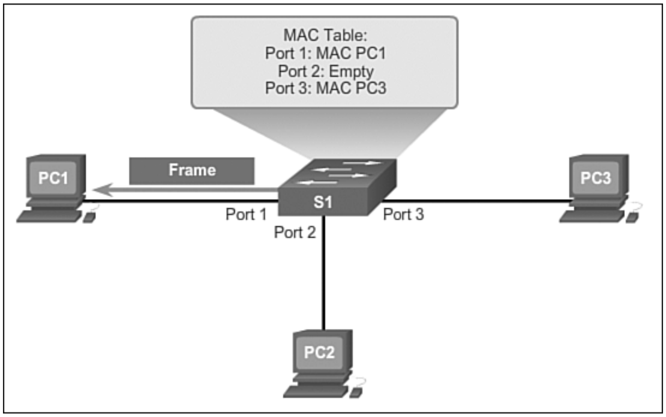


Figure 1-18 Building a MAC Address Table: S1 Sends the Frame to Port 1

Switch Forwarding Methods (1.2.1.3)

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

As shown in the online video, the store-and-forward method makes a forwarding decision on a frame after it has received the entire frame and then checked the frame for errors.

Video

Video 1.2.1.3: Store-and-Forward Switching

Go to the course online to see an animation of how a store-and-forward switch works.

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

Video

Video 1.2.1.3: Cut-Through Switching

Go to the course online. Click on the second graphic to see an animation of how a cut-through switch works.

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 1-19, 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.

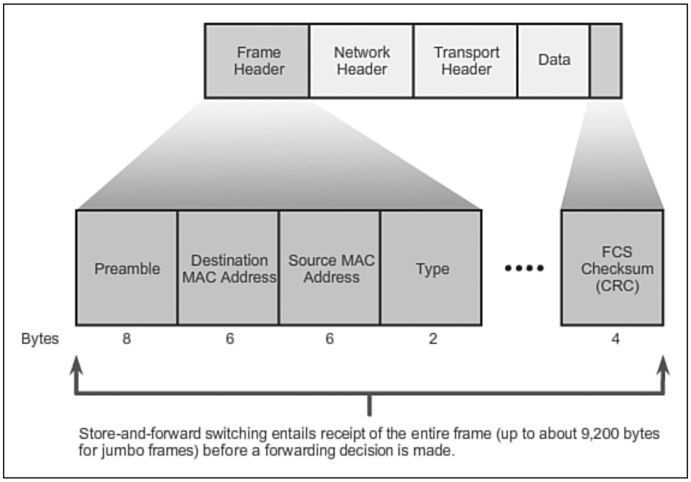

Frame Header
Network Header
Transport Header
Data
Preamble
Destination MAC Address
Source MAC Address
Type
FCS Checksum (CRC)
Bytes
8
6
6
2
4
Store-and-forward switching entails receipt of the entire frame (up to about 9,200 bytes for jumbo frames) before a forwarding decision is made.

Figure 1-19 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 the frame to the egress port buffer and then sends the frame.

Store-and-forward switching is Cisco's primary LAN switching method.

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

Cut-Through Switching (1.2.1.5)

An advantage to cut-through switching is the capability 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 invalid frame processing.

Rapid Frame Forwarding

As indicated in Figure 1-20, 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.

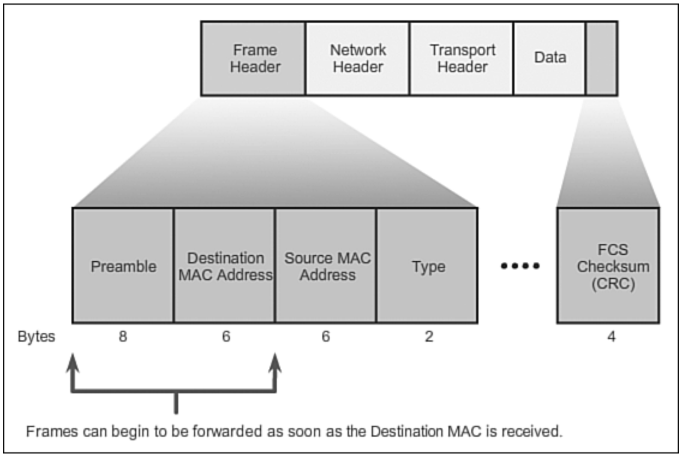


Figure 1-20 Cut-Through Switching

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, destination MAC, and the EtherType fields), and examine an additional 40 bytes in order to perform more sophisticated functions relative to IPv4 Layers 3 and 4.

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

Fragment Free

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

With a lower latency speed advantage of cut-through switching, it is 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 indicate whether each given action is performed by store-and-forward or cut-through switching. Use the online curriculum to check your answer.

Interactive Graphic

Activity 1.2.1.7: Switch It!

Go to the course outline to perform this practice activity where you have multiple scenarios of frames going through a switch. Select how the switch will handle the frame.

Switching Domains (1.2.2)

Two commonly misunderstood terms used with switching are collision domains and broadcast domains. This section tries to explain these two important concepts that affect LAN performance.

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 may occur.

It is possible, however, to use networking devices such as switches, which operate at the data link layer of the OSI model to divide a network into segments and reduce the number of devices that compete for bandwidth. Each port on a switch is a new segment because the devices plugged into the ports do not compete with each other for bandwidth. The result is that each port represents a new collision domain. More bandwidth is available to the devices on a segment, and collisions in one collision domain do not interfere with the other segments. This is also known as *microsegmentation*.

As shown in the Figure 1-21, each switch port connects to a single PC or server, and each switch port represents a separate collision domain.

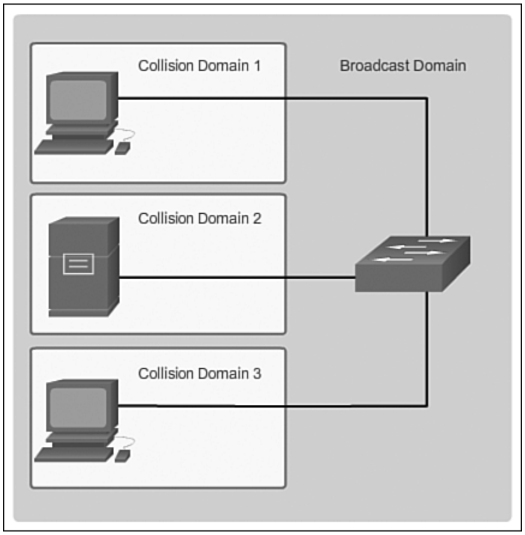


Figure 1-21 Collision Domains

Broadcast Domains (1.2.2.2)

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

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

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

Interactive Graphic

Activity 1.2.2.2: Broadcast Domains

Go to the online curriculum, and click Play to see this in the first half of the animation.

Watch how a switch broadcasts a frame out all ports except the port that received the frame.

When a switch receives a broadcast frame, the switch forwards the frame out each of the switch 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, as shown in the top broadcast domain in Figure 1-22. 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.

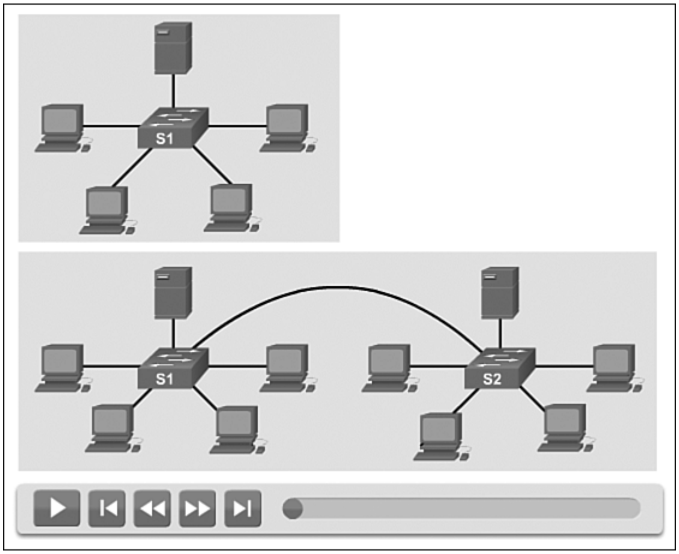


Figure 1-22 Broadcast Domains

When two switches are connected together, the broadcast domain is increased, as seen in the second (bottom) broadcast domain shown in Figure 1-22. 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. Table 1-2 shows some important characteristics of switches that contribute to alleviating network congestion.

Table 1-2 Switch Characteristics That Help with Congestion

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

Interactive Graphic

Activity 1.2.2.4: Circle the Domain

Go to the online course to view nine network topologies. On each graphic, draw a circle around the devices that make up each broadcast or collision domain as directed.

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 1 or 2 PCs
- 1 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 to one Packet Tracer file screen. All intermediary devices should be labeled with the switch model (or name) and the router model (or name).

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

Interactive Graphic

Activity 1.3.1.2: Basic Switch Configurations

Configuring switches is a common practice for LAN technicians, and practice is the key to becoming proficient. This Syntax Checker activity reviews basic switch configurations from the first course.

Go to the course outline to perform this practice activity.

Packet Tracer
□ Activity

Packet Tracer Activity 1.3.1.3: Skills Integration Challenge

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

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 provides a foundation that allows network designers to overlay security, mobility, and unified communication features. In some networks, having a separate core and distribution layer is not required. In these networks, the functionality of the core layer and the distribution layer are often collapsed together.

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 for extremely high-speed full-duplex communication. Switch ports do not block broadcasts, and connecting switches together can extend the size of the broadcast domain often resulting in degraded network performance.

Practice

The following activities provide practice with the topics introduced in this chapter. The Class Activities are available in the companion *Routing and Switching Essential Lab Manual* (978-1-58713-320-6). 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

Packet Tracer
□ Activity

Packet Tracer Activities

Packet Tracer Activity1.3.1.3: Skills Integration Challenge

Check Your Understanding Questions

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

1. Which three options correctly associate a layer of the hierarchical design model with the function of that layer? (Choose three.)

   A. Core - end device connectivity

   B. Distribution - aggregation and traffic control

   C. Access - end device connectivity

   D. Distribution - high speed backbone

   E. Access - aggregation of traffic

   F. Core - high speed backbone

2. Which hierarchical network design goal is to provide a way for the network to always be accessible?

   A. hierarchical

   B. modularity

   C. resiliency

   D. flexibility

3. Which two layers of the hierarchical network design model are commonly combined into a single layer in a small-to-medium sized network architecture? (Choose two.)

   A. access

   B. data link

   C. network

   D. distribution

   E. application

   F. core

4. What is convergence as it relates to network design?

   A. Implementation of an access-distribution-core layer design model for all sites in a corporation

   B. A centralized point in the network design where all traffic aggregates before transmission to the destination

   C. The combining of voice and video with traditional network traffic

   D. Designing a network in such a way that each tier has a specific function and upgrade path

5. What are three benefits of a converged network? (Choose three.)

   A. Voice and data support staff are combined.

   B. Network design is simplified.

   C. Network configuration is simplified.

   D. Voice, video, and data traffic use one physical network.

   E. Maintenance is simpler than hierarchical networks.

   F. Network moves, adds, and changes are simplified.

6. Which two terms are correctly defined? (Choose two.)

   A. Internal switching rate - processing capability of a switch that quantifies how much data it can process per second

   B. Port density - capability to use multiple switch ports concurrently for higher throughput data communication

   C. Rack unit - number of ports that can fit in a specific switch

   D. Cut-through switching - the transmission of a frame after the destination MAC address has been examined and processed

   E. Modular configuration switch - only support features or options that ship with the device

7. A switch that uses MAC addresses to forward frames operates at which layer of the OSI model?

   A. Layer 1

   B. Layer 2

   C. Layer 3

   D. Layer 4

8. A switch has just been powered on. PC1 connects to port 1; PC2 connects to port 2. If PC1 sends data to PC2, how will the switch process the frame?

   A. The switch forwards the frame based on the MAC address of PC2.

   B. The switch adds the MAC address of PC1 (that is received on the ingress port) to the switch MAC address table.

   C. The switch forwards the frame to all switch ports including ports 1 and 2.

   D. The switch adds the IP address of PC2 (that is sent through the egress port) to the switch MAC address table.

9. What function is most likely to be provided by a Cisco access layer switch?

   A. PoE

   B. Routing

   C. Link aggregation

   D. Fault isolation

10. Use the abbreviated MAC addresses in the MAC address table to determine the correct answer. A PC connected to port Gi0/3 sends data to a PC connected to port Gi0/5. When the switch receives the data, what will the switch do to process the frame?

Port	MAC address
Gi0/3	AA
Gi0/7	AB

   A. Add the destination MAC address to the switch MAC address table.

   B. Forward the data out all ports except for port Gi0/3.

   C. Forward the data to port Gi0/3.

   D. Forward the data out all ports.

   E. Add both the source and destination MAC addresses to the switch MAC address table.

11. Use the abbreviated MAC addresses in the MAC address table to determine the correct answer. A PC connected to port Gi0/4 sends data to a PC connected to port Gi0/3. When the switch receives the data, what will the switch do first to process the frame?

Port	MAC address
Gi0/3	AA
Gi0/7	AB

A. Add the source MAC address to the switch MAC address table.

B. Forward the data out all ports except for port 4.

C. Forward the data to port 5.

D. Forward the data out all ports.

E. Add both the source and destination MAC addresses to the switch MAC address table.

F. Add the destination MAC address to the switch MAC address table.

CHAPTER 2

Basic Switching Concepts and Configuration

Objectives

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

- What are the steps a switch takes after power is applied?
- What is the function of the boot loader if the operating system is corrupt or missing?
- How might the switch LEDs help with troubleshooting?
- What are the steps taken to configure a Cisco switch with an IP address, subnet mask, and default gateway?
- What interface is used to apply an IP address to a Cisco switch?
- What functionality is available once a switch has an IP address and default gateway?
- What type of customization can be applied to a switch port?
- What tools can be used to troubleshoot a Layer 1 or 2 problem?
- What steps are required to configure a switch for SSH access?
- What are some common security attacks that affect switches?
- What mitigation tools could be used on a Cisco switch to prevent or react to a security attack?
- What are best practices for switch security?
- What steps are required to configure switch security?
- What is the purpose of NTP?

Key Terms

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

boot loader *page 36*

switch virtual interface (SVI) *page 40*

automatic medium-dependent interface crossover (auto-MDIX) *page 46*

runt *page 51*

giant *page 51*

CRC error *page 52*

late collision *page 52*

Secure Shell (SSH) *page 55*

MAC address table overflow attack *page 60*

MAC flooding attack *page 60*

DHCP starvation attack *page 63*

denial-of-service (DoS) attack *page 63*

DHCP spoofing attacks *page 63*

Cisco Discovery Protocol (CDP) *page 64* *brute force password attack* *page 65*

Telnet DoS attack *page 65*

security audit *page 67*

penetration testing *page 67*

DHCP snooping *page 69*

trusted port *page 69*

untrusted port *page 69*

port security *page 71*

static secure MAC address *page 71*

dynamic secure MAC address *page 72*

sticky secure MAC address *page 72*

Network Time Protocol (NTP) *page 78*

Introduction (2.0.1.1)

Switches are used to connect multiple devices 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 and bandwidth, as well as implementing security requirements.

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

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

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

Class Activity 2.0.1.2: Stand by Me

Scenario

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

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

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

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

Scenario 3: Students with the number 504C 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 contained in the online course.

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

Basic Switch Configuration (2.1)

Switches are one of the most numerous devices installed onto the corporate network infrastructure. Configuring them can be fun and challenging. Knowing how switches normally boot and load an operating system is also important.

Switch Boot Sequence (2.1.1.1)

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

How To

Step 1. First, the switch loads a power-on self-test (POST) program stored in ROM. POST checks the CPU subsystem. It tests the CPU, DRAM, and the portion of the flash device that makes up the flash file system.

Step 2. Next, the switch loads the boot loader software. The *boot loader* is a small program stored in ROM and is run immediately after POST successfully completes.

Step 3. The boot loader performs low-level CPU initialization. It initializes the CPU registers that control where physical memory is mapped, the quantity of memory, and memory speed.

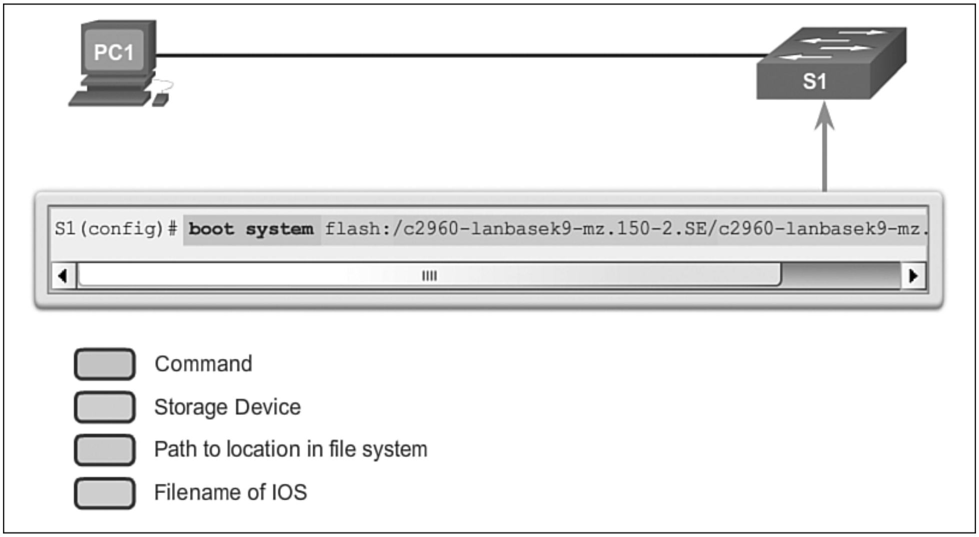
Step 4. The boot loader initializes the flash file system on the system board.

Step 5. Finally, the boot loader locates and loads a default IOS operating system software image into memory and hands control of the switch over to the IOS.

The boot loader finds the Cisco IOS image on the switch using the following process: The switch 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 a directory, each encountered subdirectory is completely searched before continuing the search in the original directory. 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 configuration, which is stored in NVRAM.

In Figure 2-1, the BOOT environment variable is set using the **boot system** global configuration mode command. Use the **show bootvar** command (**show boot** in older IOS versions) to see the current IOS boot file version.



```
S1(config)# boot system flash:/c2960-lanbasek9-mz.150-2.SE/c2960-lanbasek9-mz.
```

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 files stored in flash memory.

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

How To

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

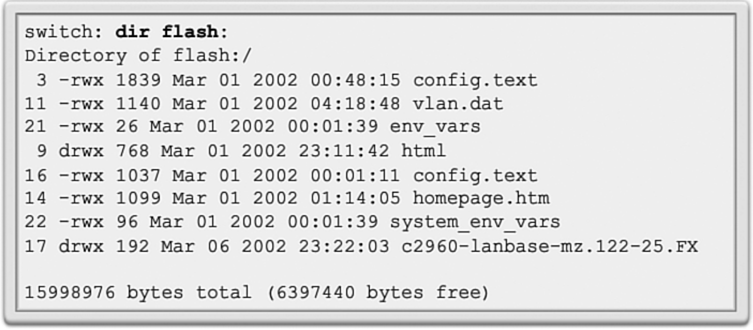
Step 2. Unplug the switch power cord.

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

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

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

The **boot loader** command line supports commands to format the flash file system, reinstall the operating system software, and recover from a lost or forgotten password. For example, the **dir** command can be used to view a list of files within a specified directory as shown in Figure 2-2.



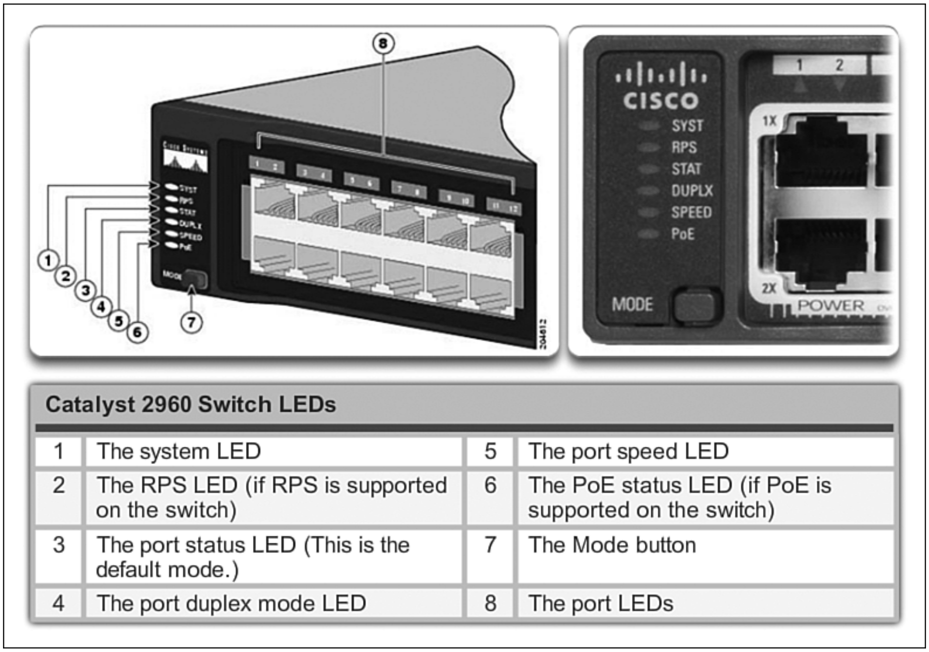
```
switch: dir flash:
Directory of flash:/
 3 -rwx 1839 Mar 01 2002 00:48:15 config.text
11 -rwx 1140 Mar 01 2002 04:18:48 vlan.dat
21 -rwx 26 Mar 01 2002 00:01:39 env_vars
 9 drwx 768 Mar 01 2002 23:11:42 html
16 -rwx 1037 Mar 01 2002 00:01:11 config.text
14 -rwx 1099 Mar 01 2002 01:14:05 homepage.htm
22 -rwx 96 Mar 01 2002 00:01:39 system_env_vars
17 drwx 192 Mar 06 2002 23:22:03 c2960-lanbase-mz.122-25.FX

15998976 bytes total (6397440 bytes free)
```

Figure 2-2 Directory Listing in Boot Loader

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 may 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.



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 Cisco 2960 Switch LEDs

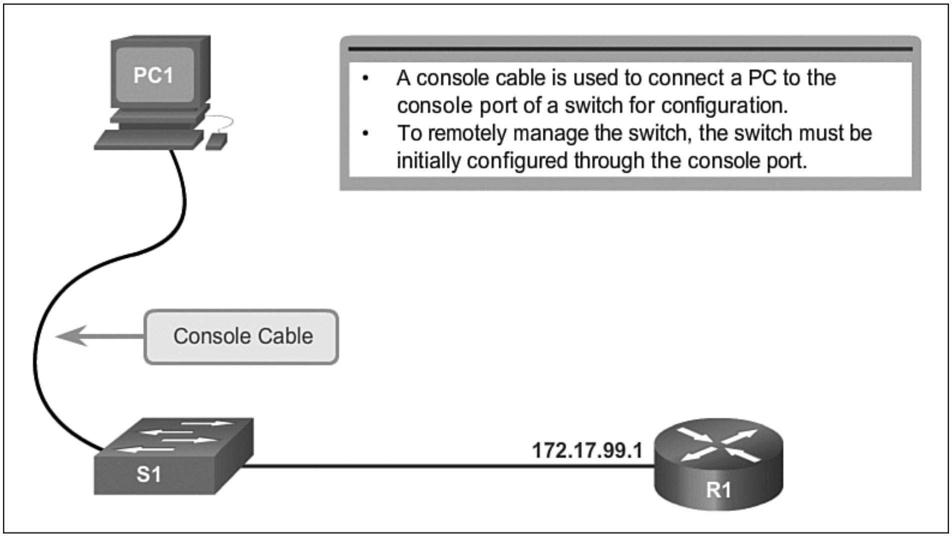
Table 2-1 contains the purpose of the Cisco 2960 switch LED indicators, and the meaning of their colors.

Table 2-1 Purpose of Cisco Switch LEDs

System LED	Shows whether the system is receiving power and is functioning properly. If the LED is off, it means the system is not powered. 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 a loop does not exist in the forwarding domain and is not forwarding data (typically, ports will remain in this state for the first 30 seconds after being activated). If the LED is blinking amber, the port is blocked to prevent a possible loop in the forwarding domain.
Port Duplex LED	Indicates the port duplex mode is selected when the LED is green. When selected, port LEDs that are off are in half-duplex mode. If the port LED is green, the port is in full-duplex mode.
Port Speed LED	Indicates the port speed mode is selected. When selected, the port LEDs will display colors with different meanings. If the LED is off, the port is operating at 10 Mb/s. If the LED is green, the port is operating at 100 Mb/s. If the LED is blinking green, the port is operating at 1000 Mb/s.
Power over Ethernet (PoE) Mode LED	If PoE is supported, a PoE mode LED will be present. If the LED is off, it indicates the PoE mode is not selected and none of the ports have been denied power or placed in a fault condition. If the LED is blinking amber, the PoE mode is not selected but at least one of the ports has been denied power, or has a PoE fault. If the LED is green, it indicates the PoE mode is selected and the port LEDs will display colors with different meanings. If the port LED is off, PoE is off. If the port LED is green, PoE is being provided to a device. If the port LED is alternating green-amber, PoE is denied because providing power to the powered device will exceed the switch power capacity. If the LED is blinking amber, PoE is off due to a fault. If the LED is amber, PoE for the port has been disabled.

Preparing for Basic Switch Management (2.1.1.4)

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.



- A console cable is used to connect a PC to the console port of a switch for configuration.
- To remotely manage the switch, the switch must be initially configured through the console port.

Figure 2-4 Preparing for Remote Switch Management

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. Furthermore, it is also a best practice to use a VLAN that is not used by end devices such as users and printers.

Note

These IP settings are only for remote management access to the switch; assigning an IP address to the switch does not allow the switch to route Layer 3 packets.

Configuring Basic Switch Management Access with IPv4 (2.1.1.5)

Step 1. Configure the Management Interface.

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

Table 2-2 Configure the Switch Management Interface

Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode for the SVI.	`S1(config)# interface vlan 99`
Configure the management interface IP address.	`S1(config-if)# ip address 172.17.99.11 255.255.0.0`
Enable the management interface.	`S1(config-if)# no shutdown`
Return to privileged EXEC mode.	`S1(config-if)# end`
Save the running config to the startup config.	`S1# copy running-config startup-config`

- In this example, VLAN 99 is configured with the IP address and mask of 172.17.99.11. To create a VLAN with the *vlan_id* of 99 and associate it to an interface, use the following commands:

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

Note

The SVI for VLAN 99 will not appear as “up/up” until VLAN 99 is created, the IP address assigned to the SVI, the **no shutdown** command entered, and either (1) a device is connected to an access port associated with VLAN 99 (not a best practice) or (2) a trunk link (covered in the VLAN chapter) connects to another network device such as a switch.

Step 2. Configure the Default Gateway.

- The switch should be configured with a default gateway if the switch will be managed remotely from networks not directly connected. The default gateway is the first Layer 3 device (such as a router) on the same management VLAN network to which the switch connects. The switch will forward IP packets with destination IP addresses outside the local network to the default gateway. As shown in Table 2-3 and Figure 2-5, 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.

Table 2-3 Commands to Configure a Switch Default Gateway

Enter global configuration mode.	`S1# configure terminal`
Configure the switch default gateway.	`S1(config)# ip default-gateway 172.17.99.1`
Return to privileged EXEC mode.	`S1(config)# end`
Save the running config to the startup config.	`S1# copy running-config startup-config`

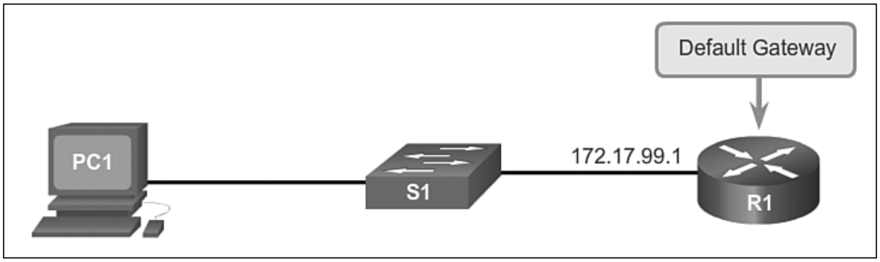
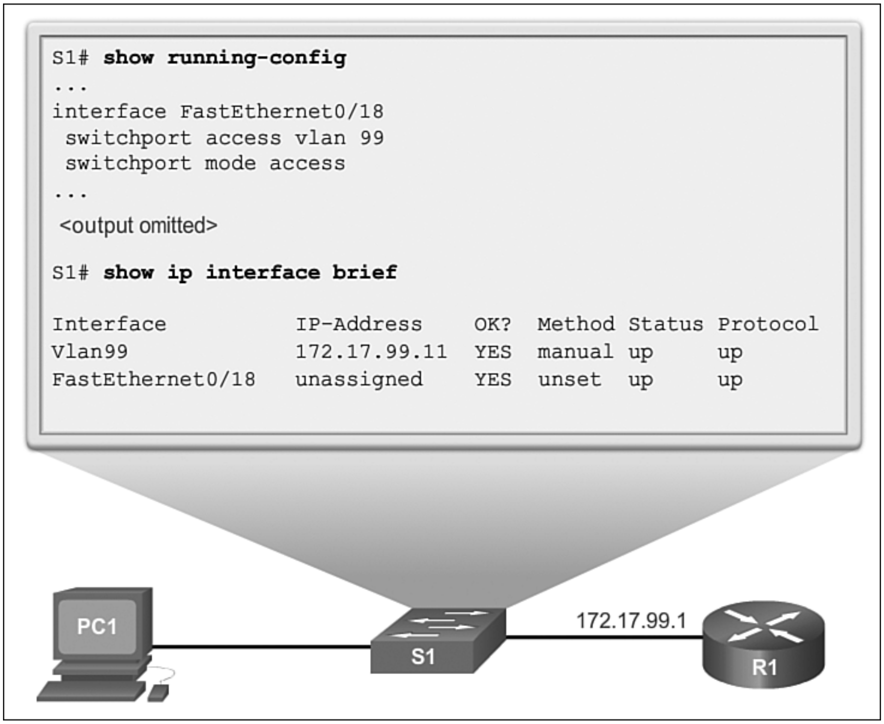


Figure 2-5 Configuring the Switch Default Gateway

- To configure the default gateway for the switch, use the **ip default-gateway** command. Enter the IP address of the default gateway. The default gateway is the IP address of the router interface to which the switch connects. Use the following command to backup the configuration: **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 in Figure 2-6 confirms that interface VLAN 99 has been configured with an IP address and a subnet mask, and that FastEthernet port Fa0/18 has been assigned to the VLAN 99 management interface. Both interfaces are now “up/up” and operational.



```
S1# show running-config
...
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
...
 <output omitted>

S1# show ip interface brief

Interface          IP-Address    OK?  Method Status Protocol
Vlan99             172.17.99.11  YES  manual up     up
FastEthernet0/18   unassigned    YES  unset  up     up
```

Figure 2-6 Verifying the Switch Management Interface Configuration

Lab 2.1.1.6: Basic Switch Configuration

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)

Port configuration starts with the basics of duplex and speed. Sometimes switch ports must manually have their duplex mode and speed manually configured. Most of the time the technician simply connects a cable and lets the network device and switch automatically negotiate these parameters. There are also times when things go awry and there are issues. This section helps you with these basic concepts.

Duplex Communication (2.1.2.1)

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

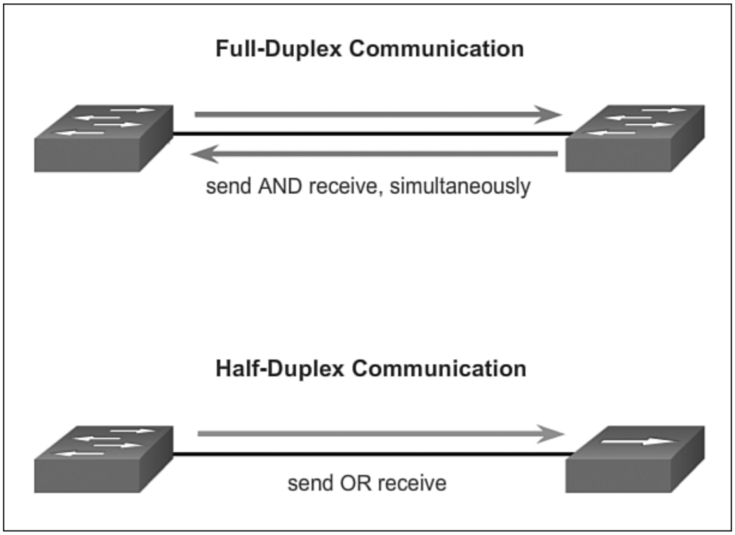

Full-Duplex Communication
send AND receive, simultaneously
Half-Duplex Communication
send OR receive

Figure 2-7 Duplex Modes

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 communication. This method of optimizing network performance requires micro-segmentation. A micro-segmented LAN is created when a switch port has only one device connected and is operating at full-duplex. This results in a micro size collision domain of a single device. Because there is only one device connected, a micro-segmented LAN is collision free.

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

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

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

Configure Switch Ports at the Physical Layer (2.1.2.2)

Just as a network card in a PC can have specific conditions such as duplex and speed set, so too can a switch port. This section examines how to configure specific parameters on a Cisco switch port and introduces auto-MDIX.

Duplex and Speed

Switch ports can be manually configured with specific duplex and speed settings. Use the **duplex** interface configuration mode command to manually specify the duplex mode for a switch port. Use the **speed** interface configuration mode command to manually specify the speed for a switch port. In Figure 2-8 and Table 2-4, port F0/1 on switch S1 and S2 are manually configured with the **full** keyword for the **duplex** command and the **100** keyword for the **speed** command.

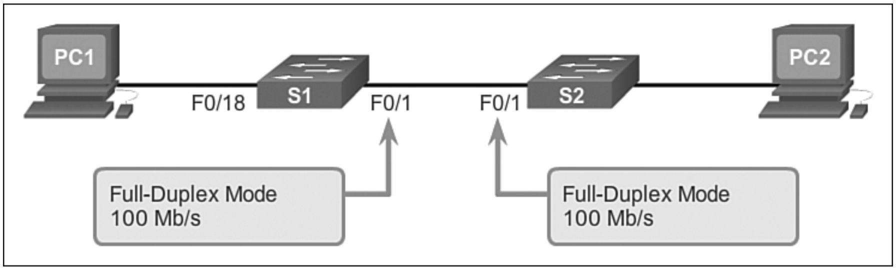


Figure 2-8 Manually Configure Duplex and Speed

Table 2-4 Cisco Switch Port Configuration

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

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

Note

Mismatched settings for the duplex mode and speed of switch ports can cause connectivity issues. Auto negotiation failure creates mismatched settings. Cisco recommends using the **auto** command for duplex and manually configuring interface speed using the **speed** command in order to avoid connectivity issues between devices.

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: Configure Switch Port Duplex and Speed

Access the second figure in the online course to use the Syntax Checker to practice configuring port Fa0/1 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. Crossover cables must be used to connect a switch to another switch or repeater.

With auto-MDIX enabled, either type of cable can be used to connect to other devices, and the interface automatically corrects for any incorrect cabling. 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.

Figure 2-9 shows the topology, and Table 2-5 shows the commands to enable auto-MDIX.

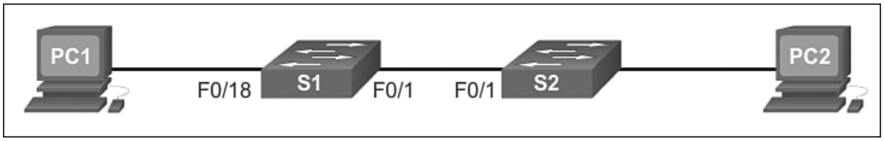


Figure 2-9 Configure Auto-MDIX

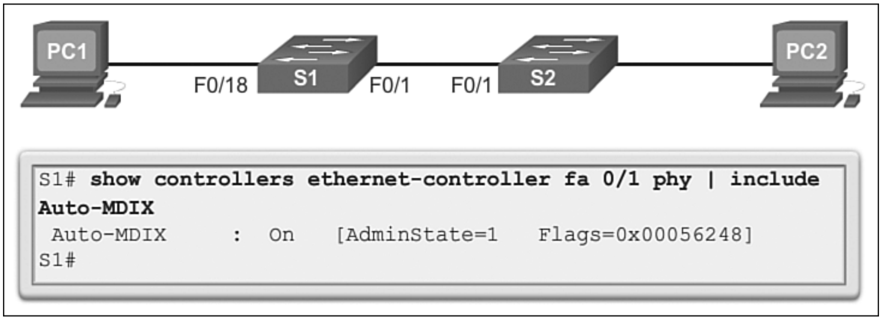
Table 2-5 Cisco Switch Auto-MDIX Commands

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

Note

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

To examine the auto-MDIX setting for a specific interface, use the **show controllers ethernet-controller** command with the argument *`interface-id`* and 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.



```
S1# show controllers ethernet-controller fa 0/1 phy | include
Auto-MDIX
 Auto-MDIX      :  On    [AdminState=1    Flags=0x00056248]
S1#
```

Figure 2-10 Verify Auto-MDIX

Interactive Graphic

Activity 2.1.2.3: Enable Auto-MDIX

Go to the online course and select the third graphic to use the Syntax Checker to practice configuring the FastEthernet 0/1 interface on S2 for auto-MDIX.

Verifying Switch Port Configuration (2.1.2.4)

Table 2-6 describes some of the options for the **show** command that are helpful in verifying common configurable switch features.

Table 2-6 Switch Verification Commands

Display interface status and configuration.	`S1# show interfaces [interface-id]`
Display current startup configuration.	`S1# show startup-config`
Display current operating configuration.	`S1# show running-config`
Display information about the flash file system.	`S1# show flash:`
Display status of system hardware and software.	`S1# show version`
Display a 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`
	OR
	`S1# show mac address-table`

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

- Fast Ethernet 0/18 interface configured with the management VLAN 99
- VLAN 99 configured with an IP address of 172.17.99.11 255.255.0.0
- Default gateway set to 172.17.99.1

```
S1# show running-config
Building configuration…

Current configuration : 1664 bytes
!
<output omitted>
!
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
!
<output omitted>
!
interface Vlan99
 ip address 172.17.99.11 255.255.0.0
!
<output omitted>
!
ip default-gateway 172.17.99.1
!
<output omitted>
```

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

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

```
S1# show interfaces fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
 Hardware is Fast Ethernet, address is 0cd9.96e8.8a01 (bia 0cd9.96e8.8a01)
 MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 Full-duplex, 100Mb/s, media type is 10/100BaseTX
 input flow-control is off, output flow-control is unsupported
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input 00:00:01, output 00:00:06, 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
   25994 packets input, 2013962 bytes, 0 no buffer
   Received 22213 broadcasts (21934 multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 21934 multicast, 0 pause input
   0 input packets with dribble condition detected
   7203 packets output, 771291 bytes, 0 underruns
<output omitted>
```

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. The following output and Table 2-7 indicate the summary line to check the status of an interface.

```
S1# show interfaces fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
 Hardware is Fast Ethernet, address is 0022.91c4.0301 (bia 0022.91c4.0e01)
 MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
<output omitted>
```

Table 2-7 Verify the Status of a Switch Interface

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 (a connection where the transmitter of one device connects directly to the receiver of another device without a transmission media between the two devices), one end of the connection may be administratively down.
- If the interface is administratively down, it has been manually disabled (the **shutdown** command has been issued) in the active configuration.

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

```
S1# 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 100000 Kbit, DLY 100 usec,
<output omitted>
  2295197 packets input, 305539992 bytes, 0 no buffer
  Received 1925500 broadcasts, 0 runts, 0 giants, 0 throttles
  3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 68 multicast, 0 pause input
  0 input packets with dribble condition detected
  3594664 packets output, 436549843 bytes, 0 underruns
  8 output errors, 1790 collisions, 10 interface resets
  0 unknown protocol drops
  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 2-8 explains some of these common errors that can be detected using the **show interfaces** command.

Table 2-8 Network Access Layer Issues

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 instance, any Ethernet pack 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 1,518 bytes is considered a giant.

continues

Table 2-8 (continued)

CRC errors	CRC errors are generated when the calculated checksum is not the same as the checksum received.
Output Errors	The sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined.
Collisions	The number of messages retransmitted because of an Ethernet collision.
Late Collisions	A collision that occurs after 512 bits of the frame have been transmitted.

"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 improperly or unterminated cables which can also cause 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 an 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 can tolerate the performance when half-duplex mode is used. 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 is required.

To troubleshoot these issues when you have no connection or a bad connection between a switch and another device, follow this general process, as shown in Figure 2-11, and explained thereafter.

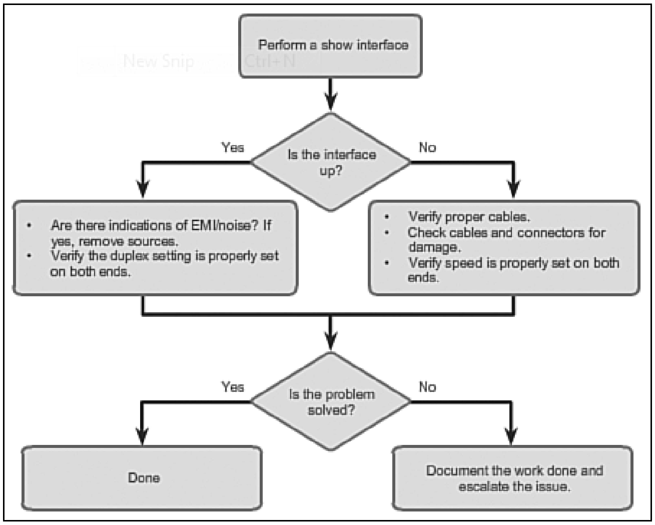

Perform a show interface
New Snip
Ctrl+N
Is the interface up?
Yes
No
• Are there indications of EMI/noise? If yes, remove sources.
• Verify the duplex setting is properly set on both ends.
• Verify proper cables.
• Check cables and connectors for damage.
• Verify speed is properly set on both ends.
Is the problem solved?
Yes
No
Done
Document the work done and escalate the issue.

Figure 2-11 Troubleshooting Switch Media Issues

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

If the interface is down:

- Check to make sure that the proper cables are being used. Additionally, check the cable and connectors for damage. If a bad or incorrect cable is suspected, replace the cable.

- If the interface is still down, the problem may be due to a mismatch in speed setting. The speed of an interface is typically auto-negotiated; therefore, even if speed is manually configured on one interface, the connecting interface should auto-negotiate accordingly. If a speed mismatch does occur through misconfiguration or a hardware or software issue, then that may result in the interface going down. Manually set the same speed on both connection ends if an auto negotiation problem is suspected.

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

- Using the **show interfaces** command, check for indications of excessive noise. Indications may include an increase in the counters for runts, giants, and CRC errors. If there is excessive noise, first find and remove the source of the noise, if possible. Also, verify that the cable does not exceed the maximum cable length and check the type of cable that is used. For copper cable, it is recommended that you use at least Category 5.
- If noise is not an issue, check for excessive collisions. If there are collisions or late collisions, verify the duplex settings on both ends of the connection. Much like the speed setting, the duplex setting is usually auto-negotiated. If there does appear to be a duplex mismatch, manually set the duplex on both connection ends. It is recommended to use full-duplex if both sides support it.

Switch Security: Management and Implementation (2.2)

When you take a new switch out of the box, the first thing the network engineer does is secure the switch and assign it an IP address, subnet mask, and default gateway so the switch can be managed from a remote location. Learning the different methods used to secure a switch is important. Also important is learning the types of attacks that can be launched on, toward, or through a switch. By understanding the attacks and the available tools and countermeasures, a technician can be better prepared to secure the switch and make use of the tools and security commands.

Secure Remote Access (2.2.1)

There are different methods that can be used to secure a switch including Telnet and SSH. Telnet has already been covered, but SSH is a much better method used to securely manage the switch from a remote location.

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 insecure 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.

Look at the online course, and select the first graphic to see how an attacker can monitor packets using a product such as Wireshark. A Telnet stream can be targeted to capture the username and password.

In the following output, you can see how the attacker can capture the username and password of the administrator from the plaintext Telnet session.

```
...........
User Access verification
username: ..................P.........vt100..BBoobb
.
Password: cisco
.
R1> eenn
.
Password: class
.
R1#
```

Click on the third graphic in the online course to see a Wireshark view of an SSH session. The attacker can track the session using the IP address of the administrator device.

However, if a Wireshark capture is made on the SSH session, the fourth graphic in the online course shows how the username and password are encrypted.

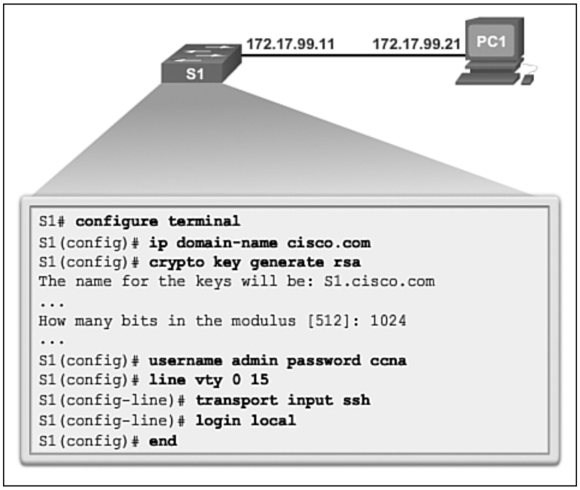
To enable SSH on a Catalyst 2960 switch, the switch must be using a version of the IOS software including cryptographic (encrypted) features and capabilities. In the following output, use the **show version** command on the switch to see which IOS the switch is currently running, and IOS filename that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

```
S1> show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M),
Version 15.0(@)SE, RELEASE SOFTWARE (fc1)

<output omitted>
```

Configuring SSH (2.2.1.2)

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

- **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.
- **Configure the IP domain:** Configure the IP domain name of the network using the **ip domain-name** *domain-name* global configuration mode command. In Figure 2-12, the *domain-name* value is **cisco.com**.



```
S1# configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin password ccna
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config)# end
```

Figure 2-12 Configure SSH for Remote Management

- **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 (refer to the sample configuration in Figure 2-12). A longer modulus length is more secure, but it takes longer to generate and 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.

- **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**.
- **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.

Interactive Graphic

Activity 2.2.1.2: Configure SSH

Go to the online course and select the second graphic to use the Syntax Checker to configure SSH on switch S1.

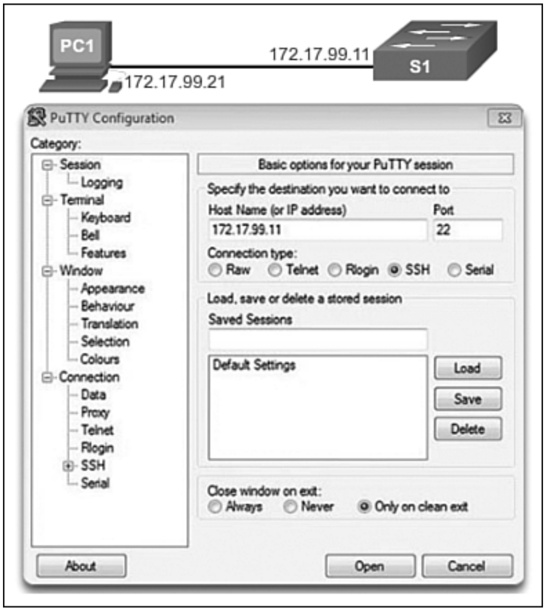
Verifying SSH (2.2.1.3)

On a PC, an SSH client, such as PuTTY, is used to connect to an SSH server. For the examples in Figures 2-16 to 2-18, 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 2-13, the PC initiates an SSH connection to the SVI VLAN IP address of S1.

In Figure 2-14, the user has been prompted for a username and password. Using the configuration from the previous example, the username **admin** and password **ccna** are entered. After entering the correct combination, the user is connected via SSH to the CLI on the Catalyst 2960 switch.



Specify the destination you want to connect to

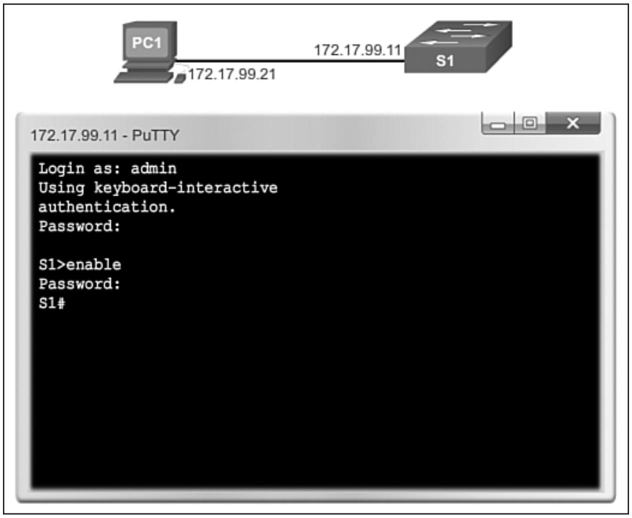
Host Name (or IP address): 172.17.99.11

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Close window on exit: ○ Always ○ Never ● Only on clean exit

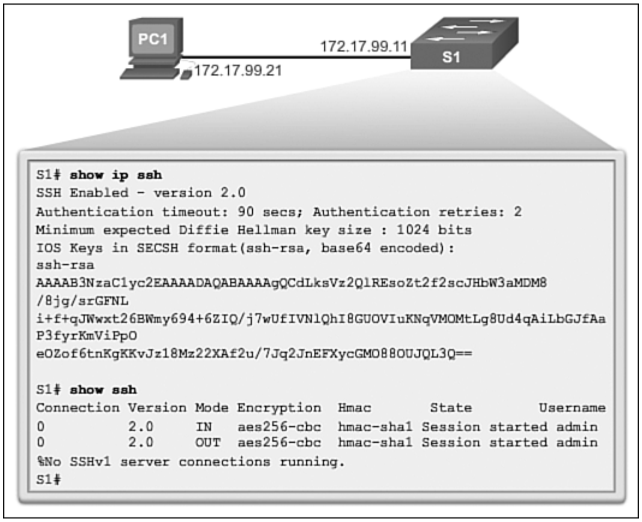
Figure 2-13 Configure PuTTY with SSH Client Connection Parameters



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

S1>enable
Password:
S1#
```

Figure 2-14 Remote Management SSH Connection

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 2-15).



```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAa
P3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q==

S1# show ssh
Connection Version Mode Encryption  Hmac       State         Username
0          2.0     IN   aes256-cbc  hmac-sha1 Session started admin
0          2.0     OUT  aes256-cbc  hmac-sha1 Session started admin
%No SSHv1 server connections running.
S1#
```

Figure 2-15 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)

Wired LANs are a common source of attack because so much information can be gained about the wired network using free downloadable tools. By examining downloaded frames, attackers can determine IP addresses of network devices, protocols being used, valid server names and IP addresses, etc. With this information an attacker can launch further attacks or even insert a rogue device. This section introduces the types of attacks and countermeasures to be performed on a wired LAN.

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 networking professionals within an organization are regarding security attacks and the dangers they pose, the better. Some types of security attacks are described here, but the details of how some of these attacks work are beyond the scope of this course. More detailed information is found in the CCNA WAN Protocols course and the CCNA Security course.

MAC Address Flooding

All Catalyst switch models use a MAC address table for Layer 2 switching. The MAC address table in a switch contains the MAC addresses associated with each physical port and the associated VLAN for each port. As a frame arrives on a switch port, the source MAC address is recorded in the MAC address table. The switch then examines the received destination MAC address and looks in the MAC address table to see if it contains the destination MAC address. If an entry already exists for the destination MAC address, the switch forwards the frame to the correct port. If the destination 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 following figures show how this type of attack works.

In Figure 2-16, 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.

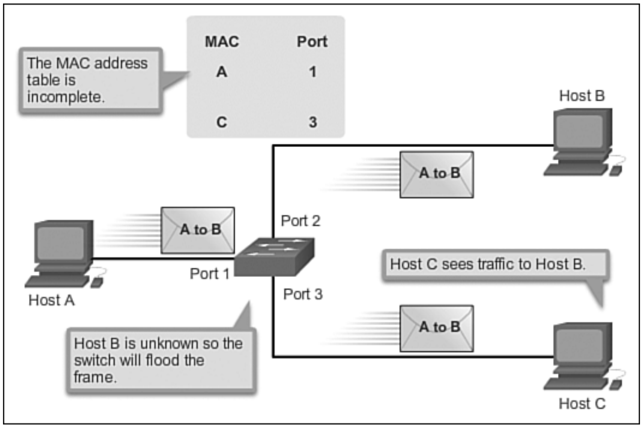

The MAC address table is incomplete.
MAC
Port
A
1
C
3
Host B
A to B
Port 2
A to B
Port 1
Host A
Host C sees traffic to Host B.
Port 3
A to B
Host B is unknown so the switch will flood the frame.
Host C

Figure 2-16 MAC Address Flooding - Switch Floods Frame for Unknown MAC

In Figure 2-17, host B receives the frame and sends a reply to host A. The switch then learns that the MAC address for host B is located on port 2 and records that information into the MAC address table.

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

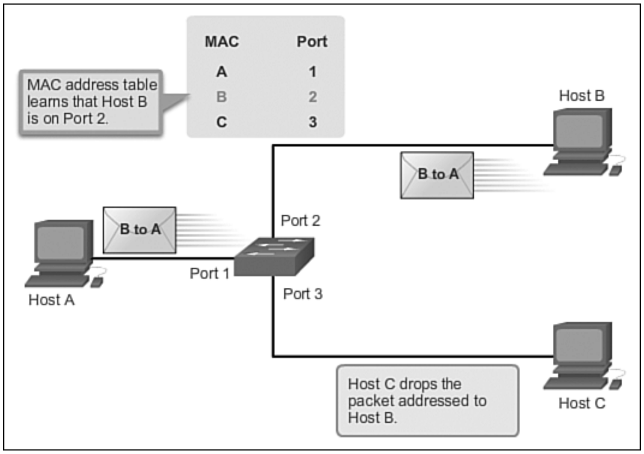

MAC
Port
A 1
B 2
C 3
MAC address table learns that Host B is on Port 2.
Host B
B to A
B to A
Port 2
Port 1
Port 3
Host A
Host C drops the packet addressed to Host B.
Host C

Figure 2-17 MAC Address Flooding - Switch Records MAC Address

As shown in Figure 2-18, any frame sent by host A (or any other host) to host B is forwarded to port 2 of the switch and not broadcasted out every port.

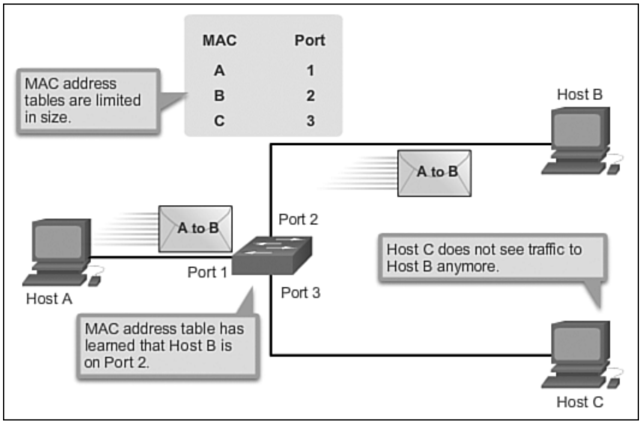

MAC
Port
A 1
B 2
C 3
MAC address tables are limited in size.
Host B
A to B
A to B
Port 2
Port 1
Port 3
Host A
Host C does not see traffic to Host B anymore.
MAC address table has learned that Host B is on Port 2.
Host C

Figure 2-18 MAC Address Flooding - 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 2-19, an attacker at host C can send frames with fake, randomly-generated source and destination MAC addresses to the switch. The switch updates the MAC address table with the information in the fake frames. When the MAC address table is full of fake MAC addresses, the switch enters into what is known as fail-open mode. In this mode, the switch broadcasts all frames to all machines on the network. As a result, the attacker can see all of the frames.

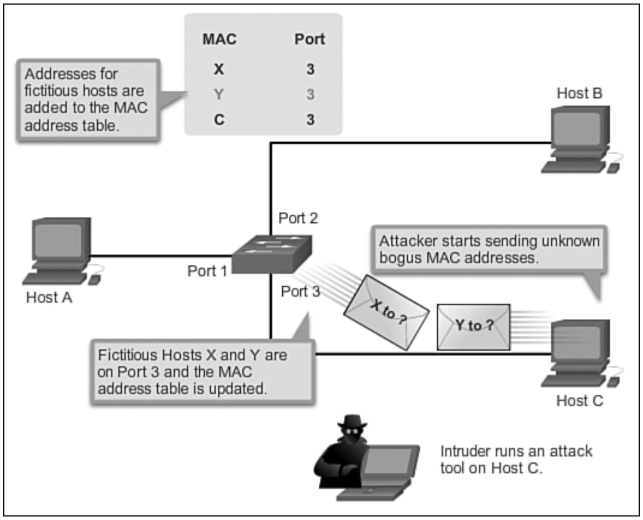

MAC
Port
X 3
Y 3
C 3
Addresses for fictitious hosts are added to the MAC address table.
Host B
Port 2
Attacker starts sending unknown bogus MAC addresses.
Port 1
Host A
Port 3
X to ?
Y to ?
Fictitious Hosts X and Y are on Port 3 and the MAC address table is updated.
Host C
Intruder runs an attack tool on Host C.

Figure 2-19 MAC Address Flooding Attack - Attacker Launches Attack

Some network attack tools can generate up to 155,000 MAC entries on a switch per minute. The maximum MAC address table size is switch model-dependent.

As shown in Figure 2-20, as long as the MAC address table on the switch remains full, the switch broadcasts all received frames out of every port except the ingress port. In this example, frames sent from host A to host B are also broadcast out of port 3 on the switch and seen by the attacker at host C.

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

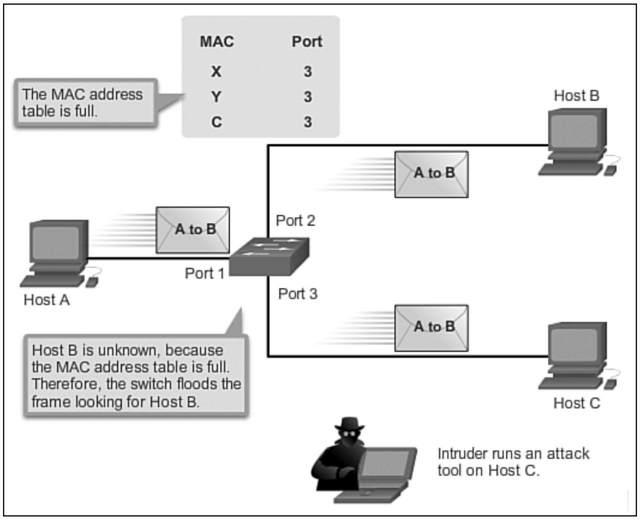

MAC
Port
X 3
Y 3
C 3
The MAC address table is full.
Host B
A to B
A to B
Port 2
Port 1
Host A
Port 3
A to B
Host B is unknown, because the MAC address table is full. Therefore, the switch floods the frame looking for Host B.
Host C
Intruder runs an attack tool on Host C.

Figure 2-20 MAC Address Flooding Attack - Attacker Sees Broadcasts

Common Security Attacks: DHCP Spoofing (2.2.2.2)

DHCP is the protocol that automatically assigns a host a valid IP address out of a DHCP pool. DHCP has always 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, as shown in Figure 2-21.

In ***DHCP starvation attacks***, an attacker floods the DHCP server with DHCP requests to use 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.

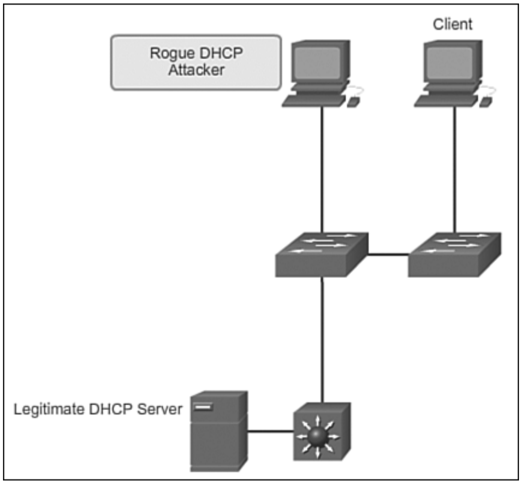


Figure 2-21 DHCP Spoofing and Starvation Attack

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

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

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

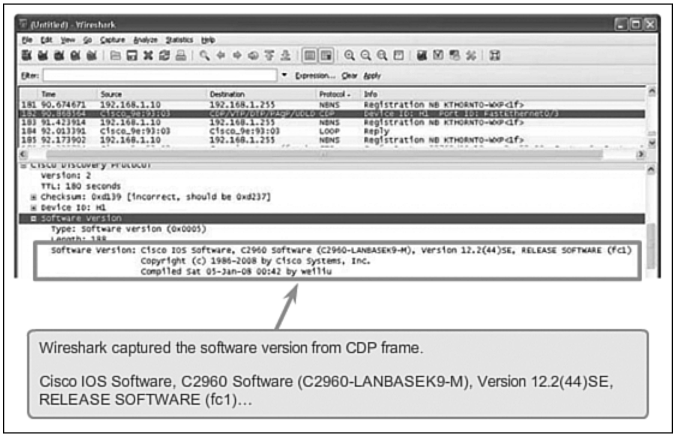
Common Security Attacks: Leveraging CDP (2.2.2.3)

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 auto-configure their connection. In some cases, this simplifies configuration and connectivity.

By default, most Cisco routers and switches have CDP enabled on all ports. CDP information is sent in periodic, unencrypted broadcasts. This information is updated locally in the CDP database of each device. Even though CDP is a Layer 2 protocol, all Cisco devices can use CDP to communicate and share device information with an adjacent Cisco device; however, this information cannot be shared beyond a single, adjacent Cisco device.

CDP contains information about the device, such as the IP address, 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 DoS attack.

Figure 2-22 shows a portion of a Wireshark capture showing the contents of a CDP packet. The Cisco IOS software version discovered via CDP, in particular, would allow the attacker to determine whether there were any security vulnerabilities specific to that particular version of IOS. Also, because CDP is not authenticated, an attacker could craft bogus CDP packets and send them to a directly-connected Cisco device.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
    Time        Source            Destination              Protocol  Info
181 90.674671   192.168.1.10      192.168.1.255            NBNS      Registration NB KTHORNTO-WXP<1f>
182 90.888364   Cisco_9e:93:03    CDP/VTP/DTP/PAgP/UDLD    CDP       Device ID: H1  Port ID: FastEthernet0/3
183 91.423914   192.168.1.10      192.168.1.255            NBNS      Registration NB KTHORNTO-WXP<1f>
184 92.013391   Cisco_9e:93:03    Cisco_9e:93:03           LOOP      Reply
185 92.173902   192.168.1.10      192.168.1.255            NBNS      Registration NB KTHORNTO-WXP<1f>

⊟ Cisco Discovery Protocol
    Version: 2
    TTL: 180 seconds
  ⊞ Checksum: 0xd139 [incorrect, should be 0xd237]
  ⊞ Device ID: H1
  ⊟ Software Version
      Type: Software version (0x0005)
      Length: 188
      Software Version: Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)SE, RELEASE SOFTWARE (fc1)
                        Copyright (c) 1986-2008 by Cisco Systems, Inc.
                        Compiled Sat 05-Jan-08 00:42 by weiliu
```

Wireshark captured the software version from CDP frame.

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)SE, RELEASE SOFTWARE (fc1)...

Figure 2-22 Wireshark CDP Packet Capture

Note

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

A ***brute force password attack*** tries to crack a password on another device. 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) that designates what IP address(es) are allowed access to the vty lines.

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: Common Security Attacks

Go to the online course to perform the practice activity where you match the type of attack to the description.

Security Best Practices (2.2.3)

With so many devices being attached to the wired network, network security is even more important today. Security starts the moment you take a network device, such as a switch, out of the box for the first time. Now that some of the common attacks have been covered, next is what a network administrator can do to protect and counteract those attacks.

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, via email, and in person.
- Encrypt and password-protect sensitive data.
- Implement security hardware and software, such as firewalls.
- Keep software up-to-date by installing security patches weekly or daily, if possible.

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

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

- Network security
- Firewalls
- Intrusion prevention systems
- Operating systems
- Programming
- Networking protocols (such as TCP/IP)

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 amount of spoofed MAC addresses to send to the switch. A network administrator also has to contend with the age-out period of the MAC address table. If the spoofed MAC addresses start to age out while performing a network audit, valid MAC addresses start to populate the MAC address table, and limiting the data that can be monitored with a network auditing tool.

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

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

Switch Port Security (2.2.4)

Port security is the process of enabling specific commands on switch ports to protect against unauthorized wired devices being attached to the network. An easy way for an intruder to gain access to a corporate network is to plug into an unused Ethernet jack or to unplug an authorized device and use that connector. Cisco provides ways to protect against such behavior.

Secure Unused Ports (2.2.4.1)

The first step in port security is to be aware of ports that are not currently being used on the switch.

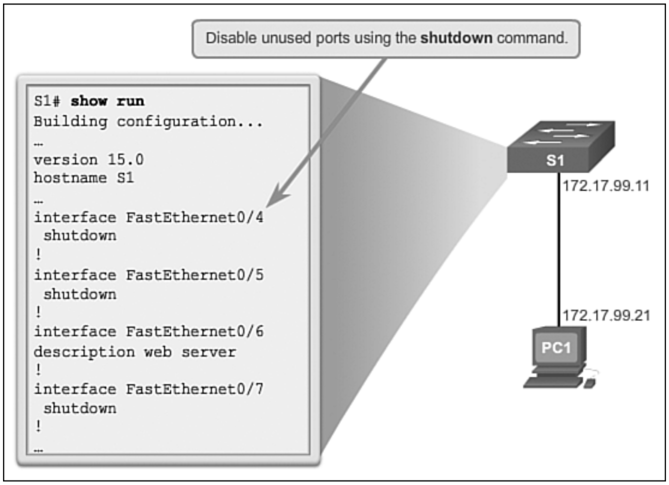
Disable Unused Ports

A simple method that many administrators use to help secure the network from unauthorized access is to disable all unused ports on a switch. For example, if a Catalyst 2960 switch has 24 ports and there are three Fast Ethernet connections in use, it is good practice to disable the 21 unused ports. Navigate to each unused port and issue the Cisco IOS **shutdown** command. If a port later on needs to be reactivated, it can be enabled with the **no shutdown** command. Figure 2-23 shows partial output for this configuration.

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

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

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



```
S1# show run
Building configuration...
…
version 15.0
hostname S1
…
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
description web server
!
interface FastEthernet0/7
 shutdown
!
…
```

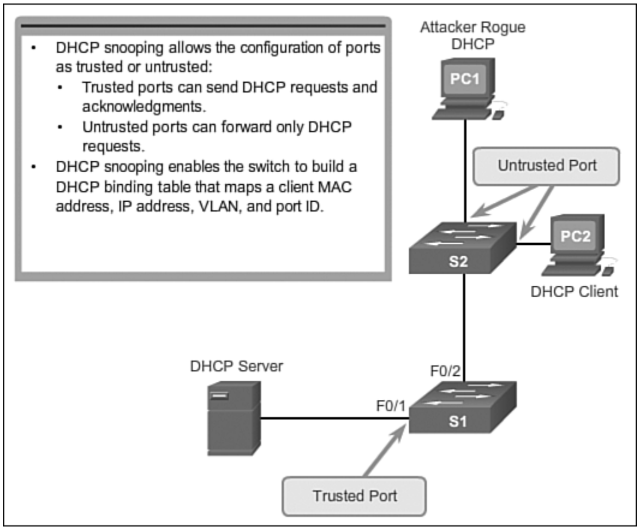
Figure 2-23 Disable Unused Switch Ports

DHCP Snooping (2.2.4.2)

DHCP snooping is a Cisco Catalyst feature that determines which devices attached to switch ports can respond to DHCP requests. DHCP snooping can be used to prevent unauthorized DHCP messages that contain information such as IP address-related data being provided to legitimate network devices.

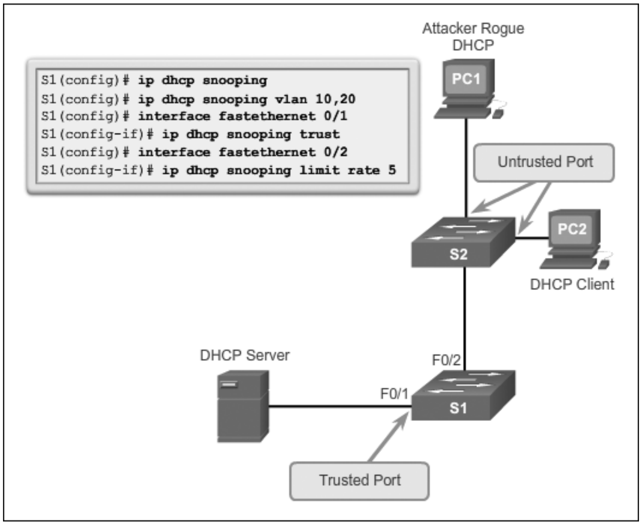
As part of the DHCP configuration process, switch ports can be identified as trusted and untrusted. *Trusted ports* can source any type of DHCP message; *untrusted ports* can source DHCP requests only. This configuration protects the network from someone attacking a device by acting as a rogue DHCP server. 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 response packet into the network, the port is shut down. This feature can be coupled with DHCP options in which switch information, such as the port ID of the DHCP request, can be inserted into the DHCP request packet.

As shown in Figures 2-24 and 2-25, 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 responses.



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

Figure 2-24 DHCP Snooping Operation



```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10,20
S1(config)# interface fastethernet 0/1
S1(config-if)# ip dhcp snooping trust
S1(config)# interface fastethernet 0/2
S1(config-if)# ip dhcp snooping limit rate 5
```

Figure 2-25 DHCP Snooping Configuration

These steps illustrate how to configure 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.

Optional Step 4. 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.

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. Cisco *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

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

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

Note

Remember that when implementing port security on a switch port to:

- Turn port security on before doing any other commands.
- Specify a single MAC address or a group of valid MAC addresses allowed on the port.
- Specify that a port automatically shuts down if unauthorized MAC addresses are detected.

Secure MAC Address Types

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

- *Static secure MAC addresses:* MAC addresses that are manually configured on a port by using the **switchport port-security mac-address** `mac-address` interface configuration mode command. MAC addresses configured in this way are stored in the address table and are added to the running configuration on the switch.

- *Dynamic secure MAC addresses:* MAC addresses that are dynamically learned and stored only in the address table. MAC addresses configured in this way are removed when the switch restarts.
- *Sticky secure MAC addresses:* MAC addresses that can be dynamically learned or manually configured stored in the address table, and added to the running configuration.

Sticky Secure MAC addresses

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

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

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

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

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

The following list shows the characteristics of sticky secure MAC addresses.

Note

On a switch port, **switchport port-security** commands will not function until port security is enabled.

- Learned dynamically, converted to sticky secure MAC addresses stored in the running-config.
- Removed from the running-config if port security is disabled.
- Lost when the switch reboots (power cycled).

- Saving sticky secure MAC addresses in the startup-config makes them permanent, and the switch retains them after a reboot.
- Disabling sticky learning converts sticky MAC addresses to dynamic secure addresses and removes them from the running-config.

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. Table 2-9 presents which kinds of data traffic are forwarded when one of the following security violation modes are configured on a port:

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

Security violations occur in these situations:

- A station with MAC address that is not in the address table attempts to access the interface when the table is full.
- An address is being used on two secure interfaces in the same VLAN.

Table 2-9 Security Violations Modes

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	No	No	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 2-10 summarizes the default port security configuration on a Cisco Catalyst switch.

Table 2-10 Port Security Default Settings

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

Figure 2-26 shows the topology used when configuring F0/18 on the S1 switch. Table 2-11 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 the default mode of shutdown.

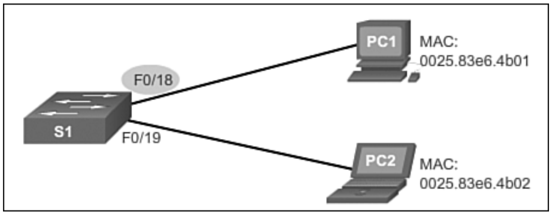


Figure 2-26 Port Security Configuration Topology

Table 2-11 Cisco Switch IOS CLI Commands for Dynamic Port Security

Specify the interface to be configured for port security.	`S1(config)# interface fastethernet 0/18`
Set the interface mode to access.	`S1(config-if)# switchport mode access`
Enable port security on the interface.	`S1(config-if)# switchport port-security`

Table 2-12 shows the commands needed to enable sticky secure MAC addresses for port security on Fast Ethernet port 0/19 of switch S1. As stated earlier, a specific 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 50 for port 0/19. The violation mode is set to the default mode of shutdown.

Table 2-12 Cisco Switch IOS CLI Commands for Sticky Port Security

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 50`
Enable sticky learning.	`S1(config-if)# switchport port-security mac-address sticky`

Port Security: Verifying (2.2.4.6)

Many students make the mistake of forgetting to enable port security before doing the specific port security options. For any configuration step, verification is important. It is especially important when configuring port security.

Verify Port Security

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

Verify Port Security Settings

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

```
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
```

Taking a look at the port after the configuration has been applied shows the values for the sticky port security settings. The maximum number of addresses is set to 50 as configured.

```
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 in the previous output as 0025.83e6.4b02:1 is identified as a sticky MAC address.

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

```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security
 switchport port-security maximum 50
 switchport port-security mac-address sticky
 switchport port-security 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 the output, the secure MAC addresses are listed along with the types.

```
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    -
--------------------------------------------------------
```

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 as shown.

```
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 06:44:53.973: %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

Notice in the output how the port protocol and link status changed to down.

Another indication that a port security violation has occurred is that the switch port LED will change to orange. The **show interfaces** command identifies the port status as `err-disabled` as shown in the following output. 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.

```
S1# show interfaces fastethernet 0/18 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 re-enabling the port. If an unauthorized device is connected to a secure port, the port should not be re-enabled until the security threat is eliminated. To re-enable the port, use the **shutdown** interface configuration mode command. Then, use the **no shutdown** interface configuration command to make the port operational, as shown in the following output.

```
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)

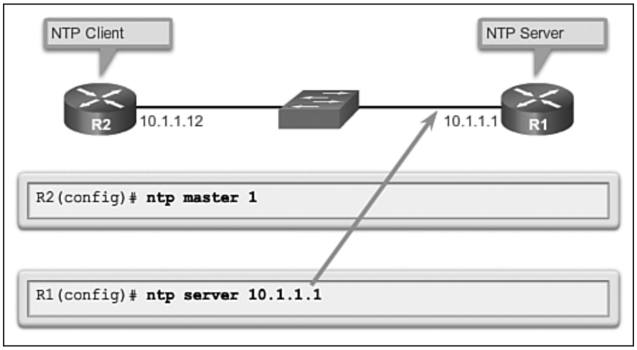
Having the correct time within networks is important. Correct time stamps are required to accurately track network events such as security violations. Additionally, clock synchronization is critical for the correct interpretation of events within syslog data files as well as for digital certificates.

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 2-27. Router R2 is configured as an NTP client, while router R1 serves as an authoritative NTP server.



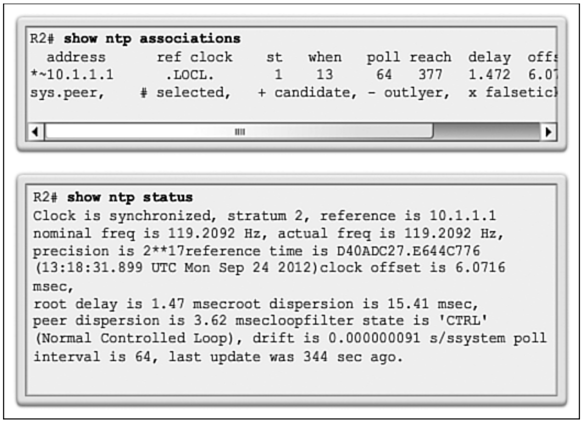
```
R2(config)# ntp master 1
```

```
R1(config)# ntp server 10.1.1.1
```

Figure 2-27 Configuring NTP

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

Figure 2-28 displays the verification of NTP. To display the status of NTP associations, use the **show ntp associations** command in privileged EXEC mode. This command will indicate the IP address of any peer devices that are synchronized to this peer, statically configured peers, and stratum number. The **show ntp status** user EXEC command can be used to display such information as the NTP synchronization status, the peer that the device is synchronized to, and in which NTP strata the device is functioning.



```
R2# show ntp associations
  address       ref clock    st   when   poll reach  delay  offs
*~10.1.1.1       .LOCL.       1    13     64   377   1.472  6.07
sys.peer,    # selected,   + candidate, - outlyer,  x falsetick
```

```
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**17reference time is D40ADC27.E644C776
(13:18:31.899 UTC Mon Sep 24 2012)clock offset is 6.0716
msec,
root delay is 1.47 msecroot dispersion is 15.41 msec,
peer dispersion is 3.62 msecloopfilter state is 'CTRL'
(Normal Controlled Loop), drift is 0.000000091 s/ssystem poll
interval is 64, last update was 344 sec ago.
```

Figure 2-28 Verifying NTP

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 ingress traffic on a switch port 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 re-enable 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)

Now that you are getting the sense of what network administrators do to configure basic features and security features on a switch, you are ready to look back and review all you have learned. Then perform the activity and skills integration challenge to prove to yourself you are ready to move to the next chapter.

Class Activity 2.3.1.1: Switch Trio

Scenario

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

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

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

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

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

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

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:

Step 1. First, the switch loads a power-on self-test (POST) program stored in ROM. POST checks the CPU subsystem. It tests the CPU, DRAM, and the portion of the flash device that makes up the flash file system.

Step 2. Next, the switch loads the boot loader software. The boot loader is a small program stored in ROM and is run immediately after POST successfully completes.

Step 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.

Step 4. The boot loader initializes the flash file system on the system board.

Step 5. Finally, the boot loader locates and loads a default IOS operating system software image into memory and hands control of the switch over to the IOS.

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

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

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

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

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

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

- Develop a written security policy for the organization.
- Shut down unused services and ports.

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

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

NTP is used to synchronize the date and time among network devices. NTP clients can synchronize their time settings with an NTP server. Clock synchronization is important when using system log messages for verification and troubleshooting.

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion *Routing and Switching Essentials Lab Manual* (9781587133206). You can find the Packet Tracer Activities PKA files 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: Basic Switch Configuration

Lab 2.2.4.11: Configuring Switch Security Features

Packet Tracer
□ Activity

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 the 'Check Your Understanding' Questions," lists the answers.

1. Which three 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 is the effect of entering the following command on a Fast Ethernet switch port?

   ```
   SW1(config-if)# duplex full
   ```

   A. The connected device communicates in two directions, but only one direction at a time.

   B. The switch port returns to its default configuration.

   C. If the device connected to this port is also set for full duplex, the device participates in collision-free communication.

   D. The efficiency of this configuration is typically rated at 50 to 60 percent.

   E. The connected device should be configured as half duplex.

3. Which two 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 switch port

   E. Sets the ring speed

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

   A. So that there can be remote connectivity to the switch via 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

5. 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 FastEthernet0/0

   C. On the management VLAN

   D. On the physical interface connected to the router or next-hop device

6. 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 proprietary Cisco 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.

7. What is an advantage of using SSH over Telnet when remotely connecting to a switch?

   A. Encryption

   B. More connection lines

   C. Connection-oriented services

   D. Username and password authentication

8. Consider the configuration. Which two commands are not needed on the switch in order for a remote network administrator to access the switch using SSH?

   A. `Switch(config)#` **`ip domain-name mydomain.com`**

   B. `Switch(config)#` **`crypto key generate rsa`**

   C. `Switch(config)#` **`ip ssh version 2`**

   D. `Switch(config)#` **`line vty 0 15`**

   E. `Switch(config-if)#` **`transport input ssh`**

9. What is an advantage of having the correct date and time on a network device?

   A. Network administrators are provided with correct timestamps on log messages.

   B. When working at the console prompt, the network administrator has a good idea how long the configuration or troubleshooting process is taking.

   C. Other devices can use CDP to discover neighbor device information if the time and date are synchronized between the two devices.

   D. Secure remote connectivity can be accomplished if the date and time are accurate.

10. What is the purpose of DHCP snooping?

    A. Ensures devices are configured for automatic IP address assignment

    B. Prevents unauthorized DHCP servers

    C. Prevents DHCP messages from going across a trunk

    D. Prevents DHCP messages from being sent to another network

11. What is a Cisco best practice for deploying switches?

    A. When a server connects to a switch, the switch port should have the port speed manually configured, but the autonegotiation feature used for duplex.

    B. A compound word should be used as a password on an infrastructure network device such as a switch.

    C. Telnet should be used whenever possible on the switch vty lines.

    D. The enable secret password should be used when configuring a switch to use SSH on the vty lines.

12. When would auto-MDIX be best to use?

    A. When a switch connects to a router

    B. When a switch connects to another switch

    C. When any device connects to an access layer switch

    D. When the cable type is unknown

CHAPTER 3

VLANs

Objectives

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

- What is a VLAN and what benefits are provided by implementing VLANs?
- What are the different types of VLANs?
- When would you use a trunk?
- How does a trunk work?
- What is the purpose of the native VLAN?
- How do you configure VLANs and trunks?
- What is DTP and when should you use it?
- What commands would be used to troubleshoot VLANs and trunks?
- What types of security issues are related to VLANs and trunks and how would you mitigate these issues?
- What are the best practices to use when implementing VLANs and trunks?

Key Terms

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

VLAN	*page 90*
data VLAN	*page 93*
default VLAN	*page 93*
native VLAN	*page 94*
trunk	*page 94*
management VLAN	*page 95*
voice VLAN	*page 96*
tagging	*page 101*
vlan.dat	*page 106*
VLAN Trunking Protocol (VTP)	*page 106*
Dynamic Trunking Protocol (DTP)	*page 120*
VLAN leaking	*page 127*
VLAN hopping	*page 134*
switch spoofing	*page 134*
double-tagging	*page 135*
Private VLAN (PVLAN) Edge	*page 136*
black hole VLAN	*page 138*

Introduction (3.0.1.1)

Network performance is a key 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, Layer 3 devices such as 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 WLANs, 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

Scenario

You have purchased a vacation home at the beach for rental purposes. There are three identical floors on each level of the home. Each floor offers one digital television for renters to use.

According to the local Internet service provider, only three stations may 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)

One way of breaking a larger network into smaller sections is by implementing VLANs. VLANs allow segmentation, or breaking a large network into smaller ones.

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 shown 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.

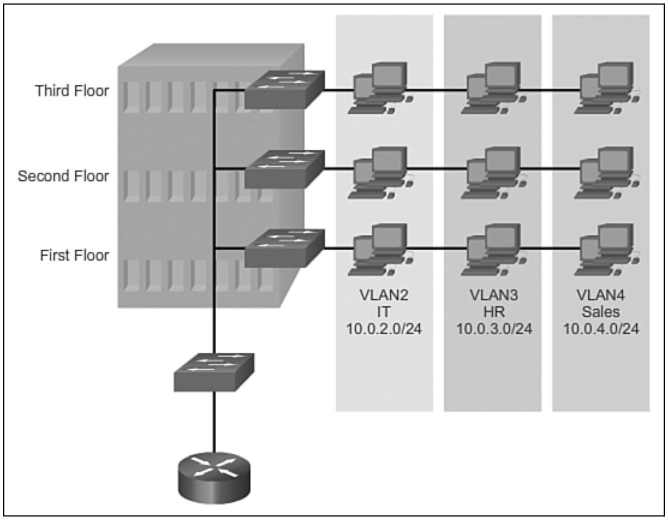


Figure 3-1 VLAN Groups

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).

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.

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. A hierarchical network addressing scheme 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.

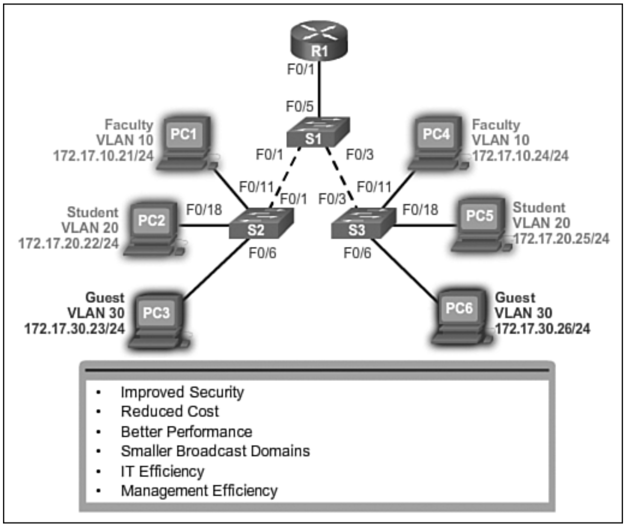


Figure 3-2 Benefits of VLANs

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.

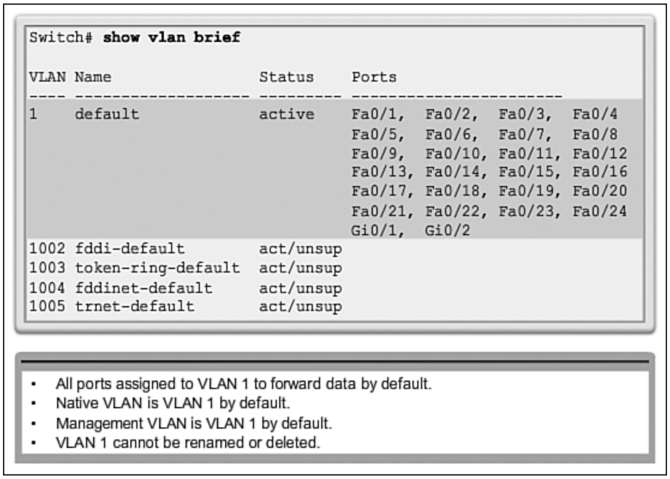
Data VLAN

A ***data VLAN*** is a VLAN that is configured to carry user-generated traffic. A VLAN carrying voice or management traffic would not be part of 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 boot up 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 Figure 3-3, 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. In Figure 3-3, all ports are currently assigned to the default VLAN 1.



```
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
```

- All ports assigned to VLAN 1 to forward data by default.
- Native VLAN is VLAN 1 by default.
- Management VLAN is VLAN 1 by default.
- VLAN 1 cannot be renamed or deleted.

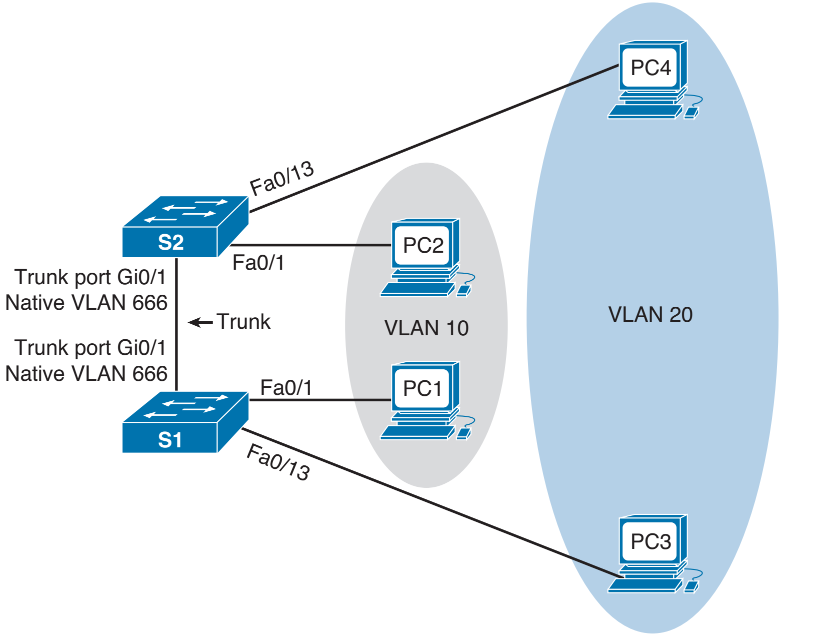
Figure 3-3 Default VLAN 1

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). 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. Look at Figure 3-4.



Traffic from VLANs 10 and 20 cross the trunk. A tag is added with the VLAN number before the data leaves the switch port. An unused VLAN number is configured as the native VLAN.

Figure 3-4 Native VLAN

PC1 and PC2 are in VLAN 10. PC3 and PC4 are in VLAN 20. Traffic from both VLANs crosses the trunk link that is configured between the two switches. If PC1 was sending traffic to PC2, as the data leaves the S1 Gi0/1 port, the S1 switch would "tag" the traffic with VLAN 10. When S2 receives the tag, the switch removes it and sends the data on to PC2. The native VLAN should be an unused VLAN, as shown in Figure 3-4. If any devices were configured in the native VLAN, the switches would not tag the traffic before it is placed on the trunk link.

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 via HTTP, Telnet, SSH, or SNMP.

Note

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 15.x, the particular active SVI assigned for remote management must be documented. Although theoretically a switch can have more than one management VLAN, having more than one increases exposure to network attacks.

Note

If the native VLAN is the same as the management VLAN, a security risk exists. The native VLAN, when used, and the management VLAN should always be a VLAN number distinct from any other VLANs.

Voice VLANs (3.1.1.4)

A separate VLAN known as a ***voice 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
- Capability 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 3-5, 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.

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.

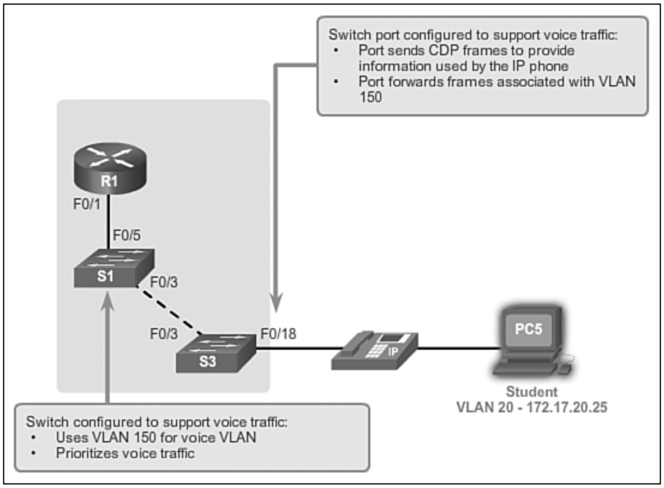

Switch port configured to support voice traffic:
• Port sends CDP frames to provide information used by the IP phone
• Port forwards frames associated with VLAN 150
R1
F0/1
F0/5
S1
F0/3
F0/3
S3
F0/18
IP
PC5
Student
VLAN 20 - 172.17.20.25
Switch configured to support voice traffic:
• Uses VLAN 150 for voice VLAN
• Prioritizes voice traffic

Figure 3-5 Voice VLAN

VLANs in a Multiswitched Environment (3.1.2)

Even a small business might have more than one switch. Multiple switch configuration and design influences network performance. Trunks are commonly used to connect a switch to a switch or to another network device such as a router.

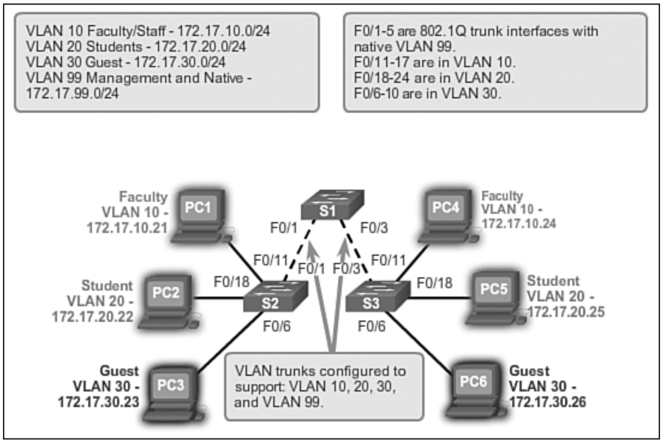
VLAN Trunks (3.1.2.1)

A VLAN trunk, or trunk, is a point-to-point link between two network devices that carries more than one VLAN. A VLAN trunk extends VLANs across two or more network devices. 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 which 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 3-6, 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.



VLAN 10 Faculty/Staff - 172.17.10.0/24
VLAN 20 Students - 172.17.20.0/24
VLAN 30 Guest - 172.17.30.0/24
VLAN 99 Management and Native - 172.17.99.0/24

F0/1-5 are 802.1Q trunk interfaces with native VLAN 99.
F0/11-17 are in VLAN 10.
F0/18-24 are in VLAN 20.
F0/6-10 are in VLAN 30.

VLAN trunks configured to support: VLAN 10, 20, 30, and VLAN 99.

Figure 3-6 Trunks

Controlling Broadcast Domains with VLANs (3.1.2.2)

Recall that a broadcast domain includes all of the devices that receive a broadcast. When a switch is bought, removed from the packaging, and powered on, all devices attached to the switch are part of the same network or broadcast domain. When VLANs are implemented, each VLAN is its own broadcast domain. Let's examine that concept because VLANs are commonly implemented in business.

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.

Interactive Graphic

Activity 3.1.2.2: Traffic Without VLAN Segmentation

Go to the online curriculum and access the first graphic. Press the Play button in order to see what happens when PC1 sends a Layer 2 broadcast.

In the animation, 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.

Network with VLANs

Interactive Graphic

Activity 3.1.2.2: Traffic with VLAN Segmentation

Go to the course outline and access the second graphic to see how the traffic changes when segmentation has been implemented.

As shown in the animation, 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.

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 that 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.

Figure 3-7 shows a network design without using segmentation compared to how it looks with VLAN segmentation, as shown in Figure 3-8. Notice how the network with the VLAN segmentation design has different network numbers for the two VLANs. Also notice how a trunk must be used to carry multiple VLANs across a single link. By implementing a trunk, any future VLAN or any PC related to assembly line production can be carried between the two switches.

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

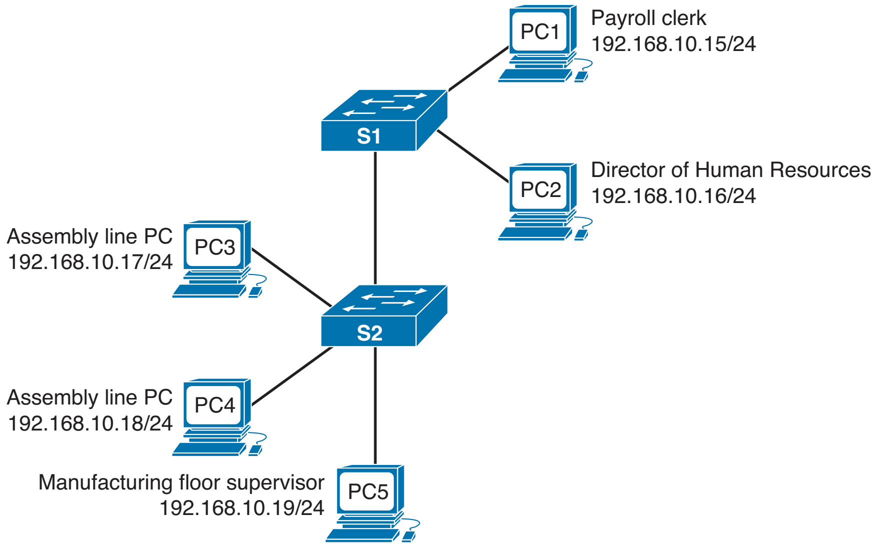


Figure 3-7 Network without Segmentation

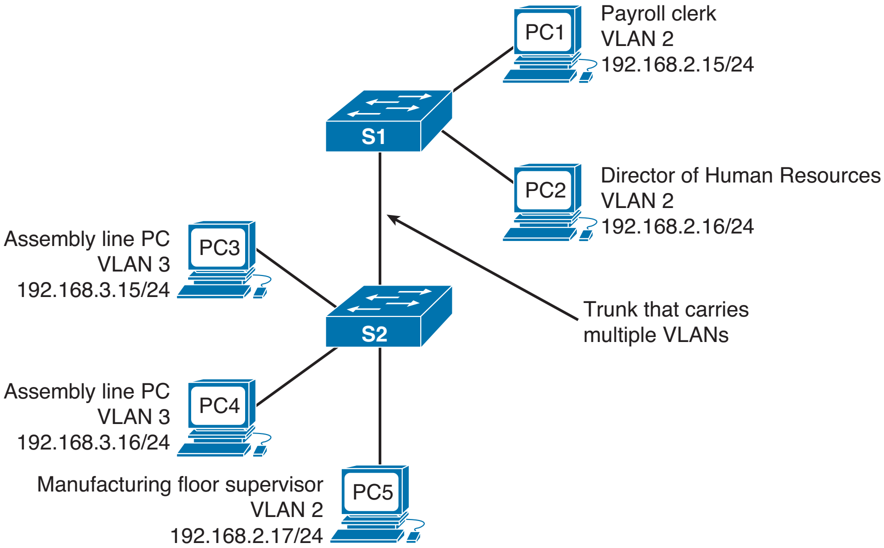


Figure 3-8 Networks with Segmentation

Tagging Ethernet Frames for VLAN Identification (3.1.2.3)

Layer 2 devices use the Ethernet frame header information to forward packets. 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, as shown in Figure 3-9.

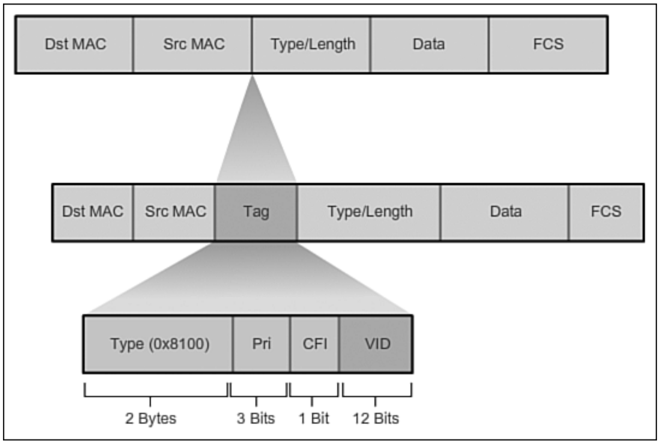


Figure 3-9 Fields in an Ethernet 802.1Q Frame

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 consists of a Type field, a tag control information field, and the FCS field:

- **Type:** A 2-byte value called the tag protocol ID (TPID) value. For Ethernet, it is set to hexadecimal 0x8100.
- **User 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.

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)

Native VLANs frequently baffle students. Keep in mind that all trunks have a native VLAN whether you configure it or not. It is best if you control the VLAN ID used as the native VLAN on a trunk. You will learn why in this section.

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), the switch 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, then the frame is dropped. The default native VLAN is VLAN 1 on a Cisco switch. 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 in 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 3-10, 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 forward 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. A better designed network without a hub is shown in Figure 3-11.

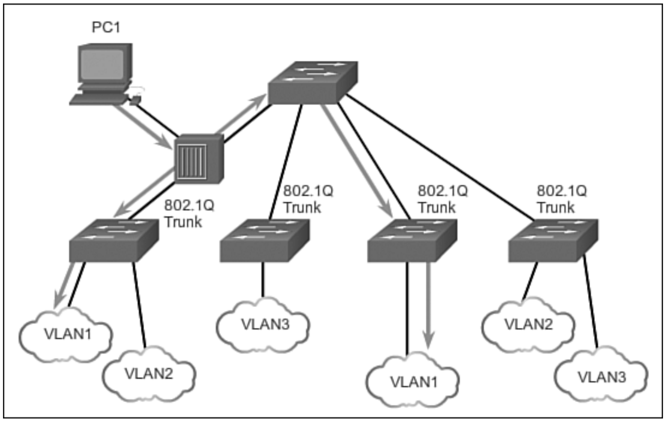


Figure 3-10 Native VLAN on 802.1Q Trunk

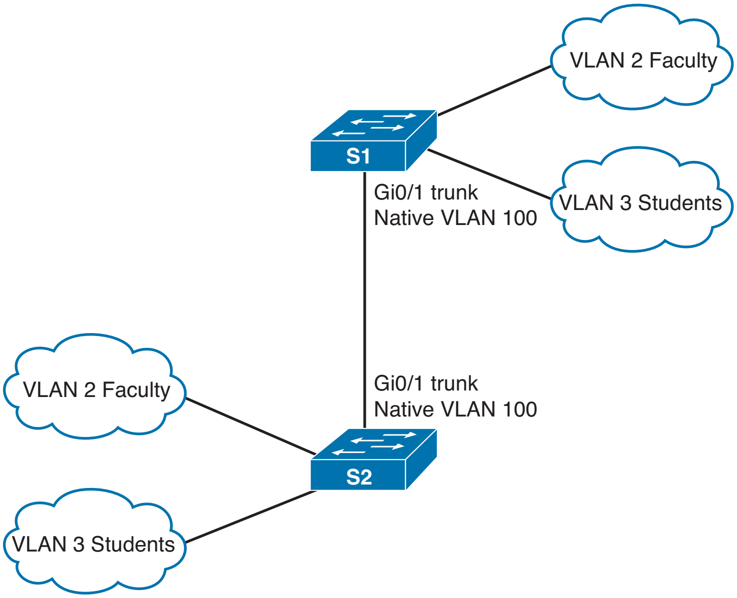


Figure 3-11 Better Native VLAN Design

Voice VLAN Tagging (3.1.2.5)

As shown in Figure 3-12, the F0/18 port on S3 is configured to be in voice mode so that voice frames will be tagged with VLAN 150. Data frames coming through the Cisco IP phone from PC5 are left untagged. Data frames destined for PC5 coming from port F0/18 are tagged with VLAN 20 on the way to the phone. The phone strips the VLAN tag before the data is forwarded to PC5.

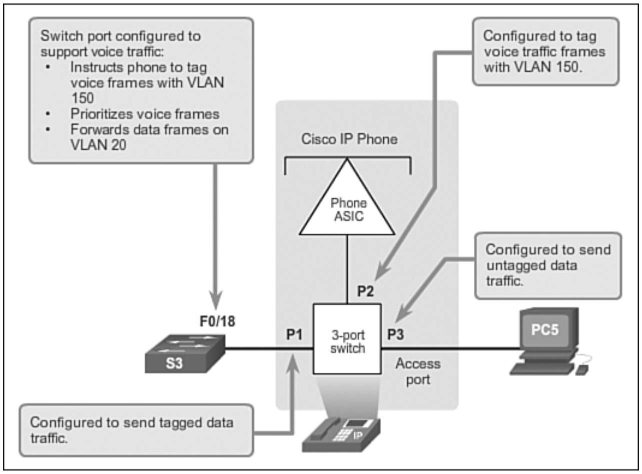

Switch port configured to support voice traffic:
• Instructs phone to tag voice frames with VLAN 150
• Prioritizes voice frames
• Forwards data frames on VLAN 20
Configured to tag voice traffic frames with VLAN 150.
Cisco IP Phone
Phone ASIC
Configured to send untagged data traffic.
P2
F0/18
P1
3-port switch
P3
PC5
S3
Access port
Configured to send tagged data traffic.
IP

Figure 3-12 Voice VLAN Tagging

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.

When the switch port has been configured with a voice VLAN, the link between the switch and the IP phone acts as a trunk to carry both the tagged voice traffic and untagged data traffic. Communication between the switch and IP phone is facilitated by the Cisco Discovery Protocol (CDP).

Sample Configuration

Look at the sample output.

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (voice)
<output omitted>
```

A discussion of voice Cisco IOS commands are 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).

Interactive Graphic

Activity 3.1.2.6: Predict Switch Behavior

Go to the online curriculum and select the three graphics to practice with VLANs and trunks.

Packet Tracer
□ Activity

Packet Tracer Activity 3.1.2.7: Investigating a VLAN Implementation

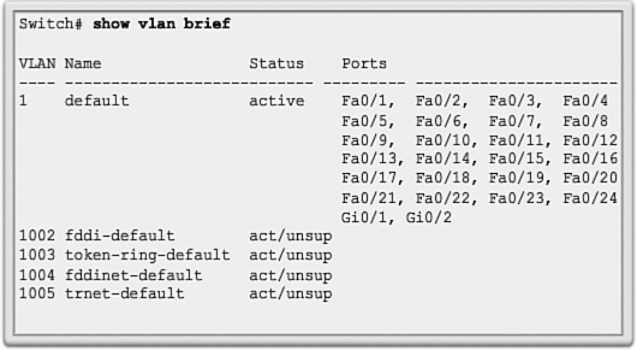
In this activity, you will observe how broadcast traffic is forwarded by the switches when VLANs are configured and when VLANs are not configured.

VLAN Implementations (3.2)

VLANs allow multiple networks to exist on one or more switches. Companies commonly use VLANs to separate a user network from other networks such as a voice network, printer/copier network, and guest network.

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 more than 4000 VLANs. Normal range VLANs on these switches are numbered 1 to 1005 and extended range VLANs are numbered 1006 to 4094. Figure 3-13 illustrates the available VLAN IDs on a Catalyst 2960 switch running Cisco IOS Release 15.x.



```
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
```

Figure 3-13 Normal VLAN ID Range

Normal Range 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)*** is a Cisco-proprietary Layer 2 protocol used to manage VLAN configurations between switches; VTP can learn and store only normal range VLANs.

Extended Range VLANs

- 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

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

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.

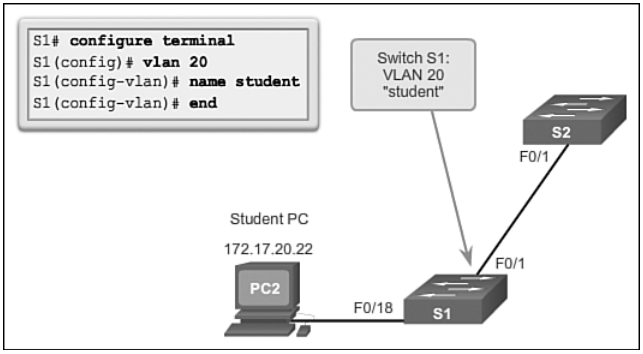
Note

Naming each VLAN is considered a best practice in switch configuration.

Table 3-1 Commands Used to Create a VLAN

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

Figure 3-14 shows how the student VLAN (VLAN 20) is configured on switch S1. In the topology example, the student computer (PC1) has not been associated with a VLAN yet, but it does have an IP address of 172.17.20.22.



```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```

Figure 3-14 Sample VLAN Configuration

Interactive Graphic

Activity 3.2.1.2: VLAN Creation and Verification

Go to the online course and click on the third graphic to use the Syntax Checker 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.

Note

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

Table 3-2 Commands Used to Assign Ports to VLANs

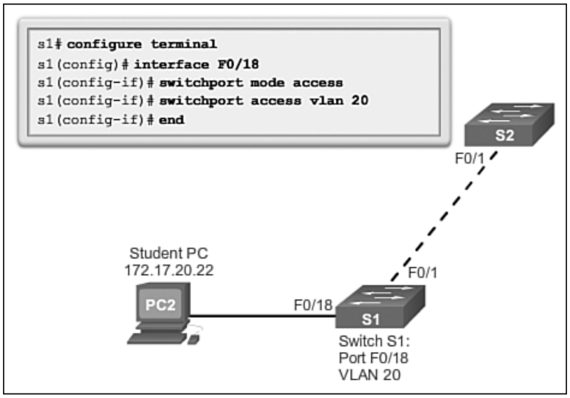
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode for a particular port number.	S1(config)# **interface** *interface_id*
Set the port to access mode.	S1(config-if)# **switchport mode access**
Assign the port to a particular VLAN.	S1(config-if)# **switchport access vlan** *vlan-id*
Return to the privileged EXEC mode.	S1(config-if)# **end**

In Figure 3-15, 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).

Interactive Graphic

Activity 3.2.1.3: Assign Ports to a VLAN and Verify

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



```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```

Figure 3-15 Sample VLAN Interface Configuration

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, then the switch displays the following:

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

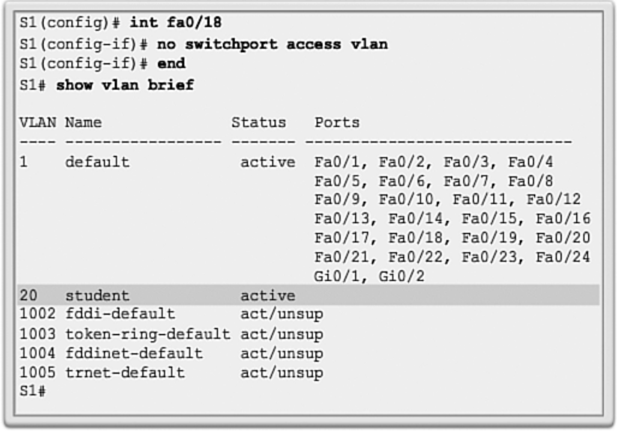
Changing VLAN Port Membership (3.2.1.4)

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 Remove **VLAN** Configuration Commands

Enter global configuration mode.	`S1#` **`configure terminal`**
Enter interface configuration mode for a particular port number.	`S1(config)#` **`interface`** *`interface_id`*
Assign the port to a particular VLAN.	`S1(config-if)#` **`no switchport access vlan`** *`vlan-id`*
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 that immediately follows as shown in Figure 3-16. 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.



```
S1(config)# int fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
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, Fa0/11, 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
S1#
```

Figure 3-16 Sample Interface Removal of a VLAN

VLAN 20 is still active, even though no ports are assigned to it. The **show interfaces fa0/18 switchport** output verifies that the access VLAN for interface F0/18 has been reset to VLAN 1.

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
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 the following output, port F0/11 is assigned to VLAN 20.

```
S1# config t
S1(config)# interface fastethernet0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
S1(config-if)# end
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, Gig1/1
                                                Gig1/2
20   VLAN0020                         active    Fa0/11
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

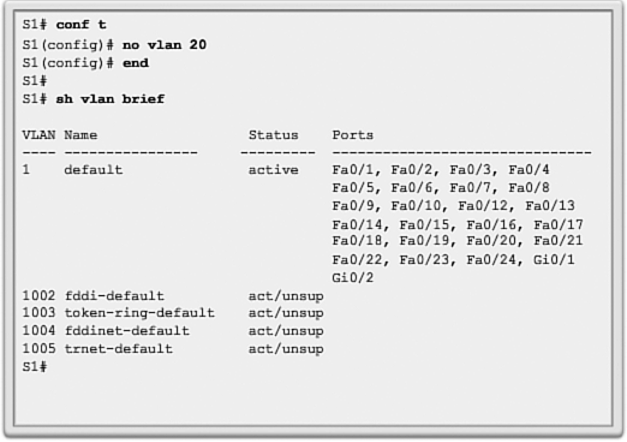
Interactive Graphic

Activity 3.2.1.4: Changing VLAN Port Membership

Go to the online curriculum and click on the fifth graphic to use the Syntax Checker to change VLAN port membership.

Deleting VLANs (3.2.1.5)

In Figure 3-17, 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.



```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh 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
S1#
```

Figure 3-17 Deleting a VLAN

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 Cisco Catalyst switch, the **erase startup-config** command must accompany the **delete vlan.dat** command prior to using the **reload** command 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 shows common **show vlan** command options.

Table 3-4 The `show vlan` Command Options

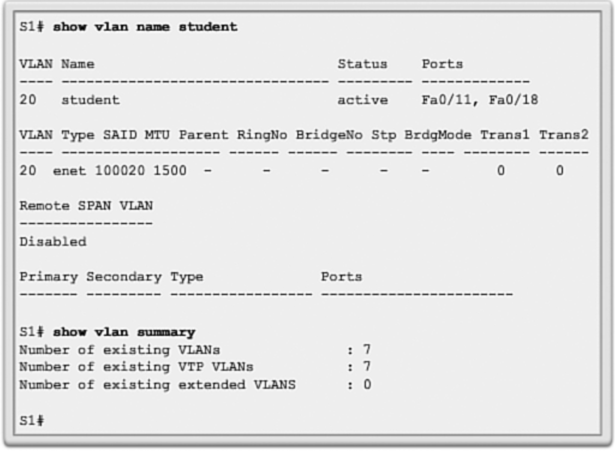
show vlan [**brief** | **id** *vlan-id* | **name** *vlan-name* | **summary**]	
Display one line for each VLAN with the VLAN name, status, and associated ports.	**brief**
Display information about a single VLAN identified by the VLAN ID number, which can be a number between 1 and 4094.	**id** *vlan-id*
Display information about a single VLAN identified by a 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 shows common **show interfaces** command options.

Table 3-5 The `show interfaces` Command Options

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, which is a number from 1 to 4094.	**vlan** *vlan-id*
Display the administrative and operational status of a switch port, including port blocking and port protection settings.	**switchport**

In Figure 3-18, 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 Figure 3-18 shows seven VLANs.



```
S1# show vlan name student

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------
20   student                          active    Fa0/11, Fa0/18

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

S1#
```

Figure 3-18 Using the **show vlan** Command

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 the output, indicating that VLAN 20 is up.

```
S1# show interfaces vlan 20
Vlan 20 is up, line protocol is down
 Hardware is EtherSVI, address is 001c.57ec.0641 (bia 001c.57ec.0641)
 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
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 multicast)
   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
<output omitted>
```

Interactive Graphic

Activity 3.2.1.6: Using the show interfaces **Command**

Go to the online curriculum and select the fourth graphic to use the Syntax Checker to display the switch port information using the **show interfaces** *interface-id* **switchport** command. This command can be used to verify VLAN assignments and mode.

Packet Tracer □ Activity

Packet Tracer Activity 3.2.1.6: 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)

Trunks are commonly used between switches and other network devices such as a router, another switch, or a server. A network technician must be very familiar with configuring a trunk and ensuring it works properly.

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. In the example, VLAN 99 is configured as the native VLAN using the **switchport trunk native vlan 99** command.

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

Table 3-6 Switch Port Trunk Commands

Enter global configuration mode.	`S1#` **`configure terminal`**
Enter interface configuration mode for a particular port number.	`S1(config)#` **`interface`** *`interface_id`*
Optionally, put the trunk in the appropriate trunking mode if the switch supports more than one mode.	`S1(config-if)#` **`switchport trunk encapsulation`** `[`**`dot1q`** `|` **`isl`**`]`
Force the link to be a trunk link.	`S1(config-if)#` **`switchport mode trunk`**
Specify a native VLAN for untagged 802.1Q frames.	`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`**

In Figure 3-19, VLANs 10, 20, and 30 support the Faculty, Student, and Guest computers (PC1, PC2, and PC3). The F0/1 port on switch S1 is configured as a trunk port and forwards traffic for VLANs 10, 20, and 30. VLAN 99 is configured as the native VLAN.

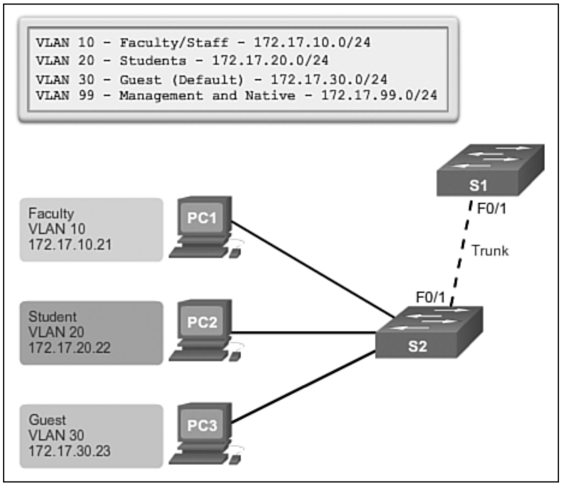

VLAN 10 - Faculty/Staff - 172.17.10.0/24
VLAN 20 - Students - 172.17.20.0/24
VLAN 30 - Guest (Default) - 172.17.30.0/24
VLAN 99 - Management and Native - 172.17.99.0/24
S1
F0/1
Trunk
F0/1
S2
Faculty VLAN 10 172.17.10.21
PC1
Student VLAN 20 172.17.20.22
PC2
Guest VLAN 30 172.17.30.23
PC3

Figure 3-19 Sample VLAN Design

Look at the configuration of port F0/1 on switch S1 as a trunk port. The native VLAN is changed to VLAN 99 and the allowed VLAN list is restricted to 10, 20, and 30. If the native VLAN is not allowed on the trunk link, the trunk will not allow any data traffic for the native VLAN.

```
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
```

Note

This configuration assumes the use of Cisco Catalyst 2960 switches, which automatically use 802.1Q encapsulation on trunk links. Other switches may 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 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 Configures Values on Trunk Lines

Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode for a particular port number.	S1(config)# **interface** *interface_id*
Set trunk to allow all VLANs.	S1(config-if)# **no switchport trunk allowed vlan**
Reset the native VLAN to the default.	S1(config-if)# **no switchport trunk native vlan**
Configure the port in access mode.	S1(config-if)# **switchport mode access**
Optionally, remove the trunk mode if it was entered.	S1(config-if)# **no switchport trunk encapsulation** [**dot1q** | **isl**]
Return to the privileged EXEC mode.	S1(config-if)# **end**

The command to reset the switch port to an access port and, in effect, delete the trunk configuration is also shown.

The following output 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.

```
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>
```

The following 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.

```
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)

The following output displays the configuration of switch port F0/1 on switch S1. The configuration is verified with the **show interfaces** `interface-ID` **switchport** command.

```
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 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. Further 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 Trunk

Go to the online curriculum and select the second graphic to use the Syntax Checker 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

VLAN 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)

The *Dynamic Trunking Protocol (DTP)* is used to negotiate forming a trunk between two Cisco devices. DTP causes increased traffic, and is enabled by default, but may be disabled.

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 3-20 on interface F0/3 of switches S1 and S3.

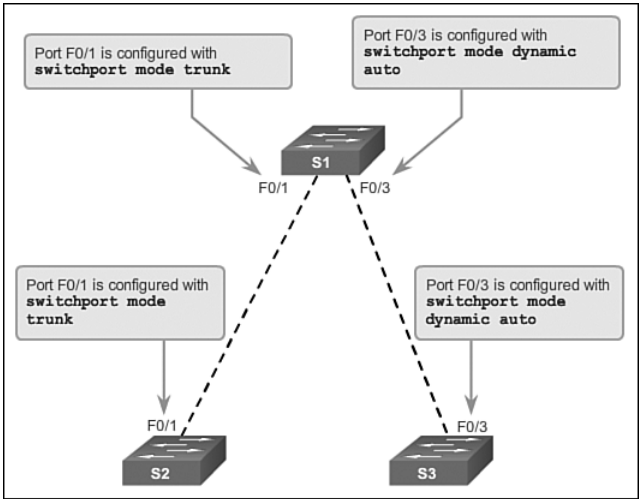

Port F0/1 is configured with **switchport mode trunk**
Port F0/3 is configured with **switchport mode dynamic auto**
S1
F0/1
F0/3
Port F0/1 is configured with **switchport mode trunk**
Port F0/3 is configured with **switchport mode dynamic auto**
F0/1
F0/3
S2
S3

Figure 3-20 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 3-21, 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, 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.

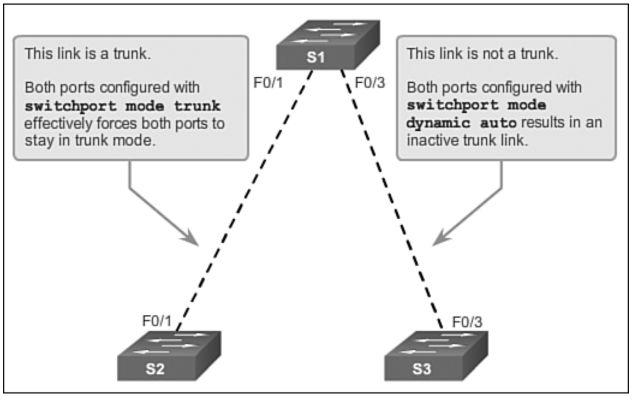

This link is a trunk.
Both ports configured with **switchport mode trunk** effectively forces both ports to stay in trunk mode.
S1
F0/1
F0/3
This link is not a trunk.
Both ports configured with **switchport mode dynamic auto** results in an inactive trunk link.
F0/1
F0/3
S2
S3

Figure 3-21 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 switchport mode for newer Cisco switch Ethernet interfaces is **dynamic auto**. Note that if two Cisco switches are left to the common default setting of **auto**, a trunk will never form.

- **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 switchport 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 switchport 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

Note

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 the following output.

```
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:                                    no
<output omitted>
```

Interactive Graphic

Activity 3.2.3.2: Configuring and Verifying DTP

Go to the curriculum and click on the third graphic in order to use the Syntax Checker 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 course outline to perform this practice activity where you will select whether a link will become a trunk link or an access link.

Troubleshoot VLANs and Trunks (3.2.4)

When first learning about switches, students have trouble knowing where to start troubleshooting. Pay particular attention to the **show** commands in this section to verify your configurations using the described techniques instead of simply using the **show running-configuration** command.

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 3-22, PC1 cannot connect to the web/TFTP server shown.

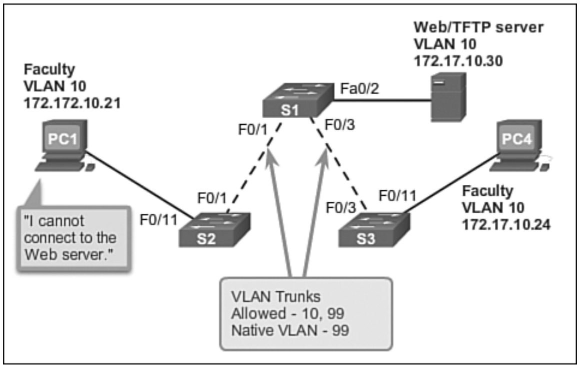
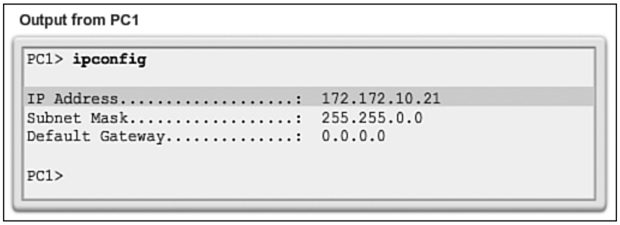


Figure 3-22 IP Issue Within a VLAN

A check of the IP configuration settings of PC1 shown in Figure 3-23 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.

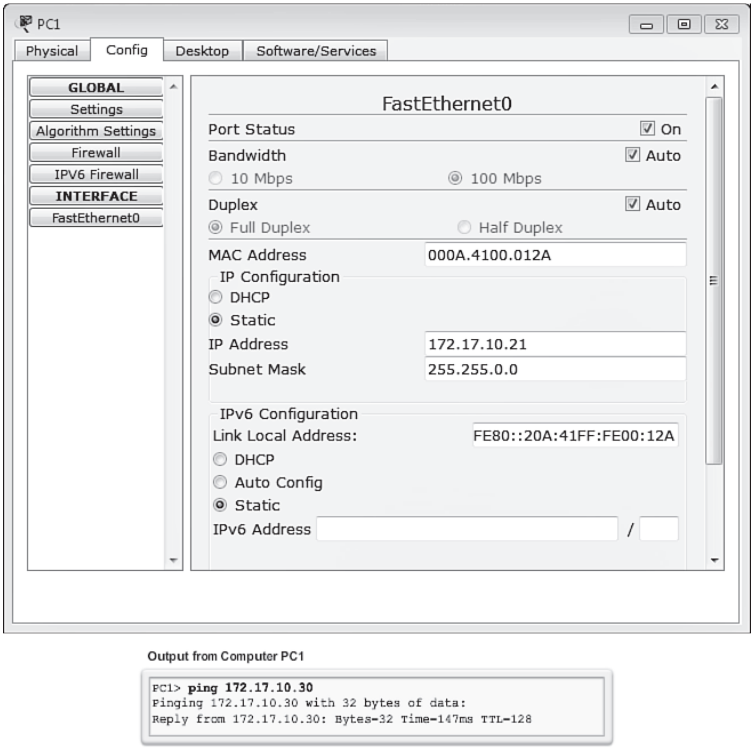


Output from PC1

```
PC1> ipconfig

IP Address..................:  172.172.10.21
Subnet Mask.................:  255.255.0.0
Default Gateway.............:  0.0.0.0

PC1>
```

Figure 3-23 Incorrect IP Address Problem

The PC1 Fast Ethernet configuration dialog box shows the updated IP address of 172.17.10.21. In Figure 3-24, the output on the bottom reveals that PC1 has regained connectivity to the web/TFTP server found at IP address 172.17.10.30.



FastEthernet0

Port Status ☑ On

Bandwidth ☑ Auto

○ 10 Mbps ● 100 Mbps

Duplex ☑ Auto

● Full Duplex ○ Half Duplex

MAC Address 000A.4100.012A

IP Configuration

○ DHCP

● Static

IP Address 172.17.10.21

Subnet Mask 255.255.0.0

IPv6 Configuration

Link Local Address: FE80::20A:41FF:FE00:12A

○ DHCP

○ Auto Config

● Static

IPv6 Address /

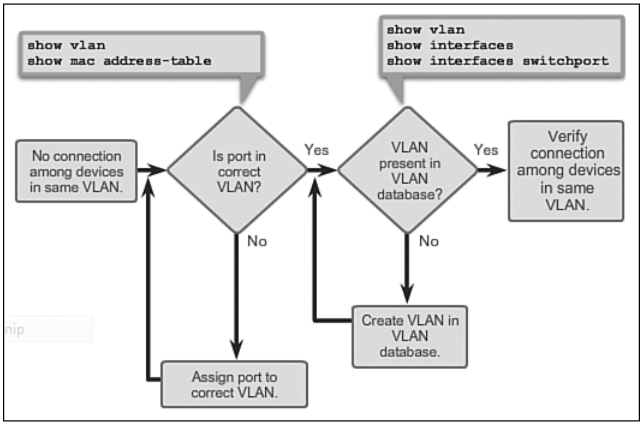
Output from Computer PC1

```
PC1> 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
```

Figure 3-24 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, see the flowchart in Figure 3-25 to troubleshoot.



```
show vlan
show mac address-table
```

```
show vlan
show interfaces
show interfaces switchport
```

No connection among devices in same VLAN.
Is port in correct VLAN?
Yes
No
VLAN present in VLAN database?
Yes
No
Verify connection among devices in same VLAN.
Create VLAN in VLAN database.
Assign port to correct VLAN.

Figure 3-25 Missing VLAN Flowchart

- As shown in Figure 3-25, 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 on a particular port. 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, as shown in the following output.

```
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
```

- **Total Mac Addresses for this criterion:** If the VLAN to which the port is assigned is deleted, the port becomes inactive. Use the **show vlan** or **show interfaces switchport** command to verify whether a VLAN is active.

```
S1# show interfaces fastethernet0/1 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
<output omitted>
```

In the previous example of a MAC address table, the output shows the 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.

Note

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 may 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***, which is caused by a mismatched native VLAN or misconfigured trunk.

Figure 3-26 displays a flowchart of general trunk troubleshooting guidelines.

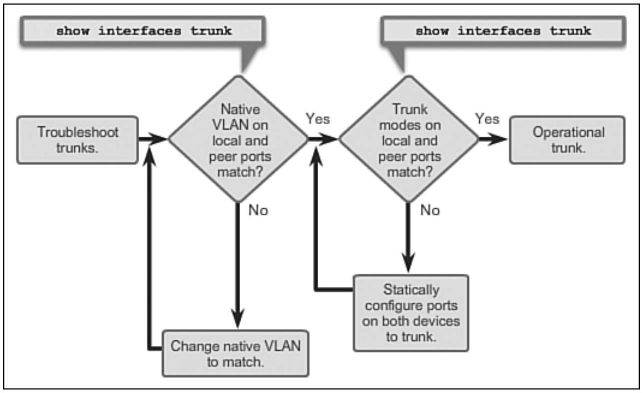

show interfaces trunk
show interfaces trunk
Troubleshoot trunks.
Native VLAN on local and peer ports match?
Yes
Trunk modes on local and peer ports match?
Yes
Operational trunk.
No
No
Statically configure ports on both devices to trunk.
Change native VLAN to match.

Figure 3-26 Trunk Troubleshooting Flowchart

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

- 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.
- 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, determine the native VLAN used on that trunk link and verify trunk establishment using the **show interfaces trunk** command. The following output 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.

```
SW1# 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.

Note

The previous output indicates that there is an active trunk despite the native VLAN mismatch. Configure the native VLAN to be the same VLAN on both sides of the link to correct this behavior so that VLAN leaking does not occur.

Common Problems with Trunks (3.2.4.4)

Trunking issues are usually associated with incorrect configurations, shown in Table 3-9.

Table 3-9 Common Problems with Trunks

Problem	Result	Example
Native VLAN mismatch	Poses a security risk and creates unintended results	One port is defined as native VLAN 99 and the opposite trunk end is defined as native VLAN 100.
Trunk mode mismatch	Causes loss of network connectivity	One end of the trunk is configured as trunk mode “off” and the other as trunk mode “on.”
Allowed VLANs on trunks	Causes unexpected traffic or no traffic to be sent over the trunk	The list of allowed VLANs does not support current VLAN trunking requirements.

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.
- **Trunk mode mismatches:** One trunk port is configured with trunk mode off and the other with trunk mode on. This configuration error causes the trunk link to stop working.
- **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 sent over the trunk.

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 two 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 Figure 3-27, PC4 cannot connect to the internal web server. The topology indicates a valid configuration. Why is there a problem?

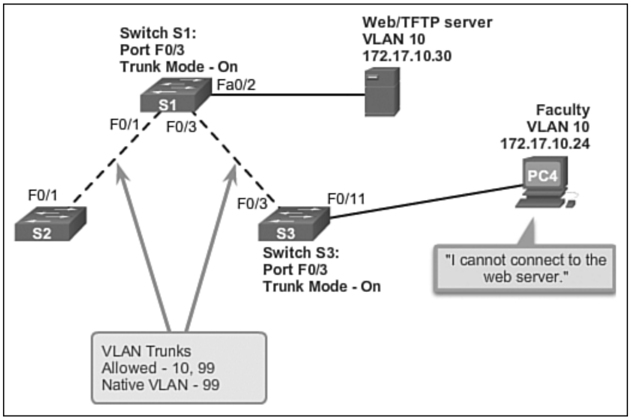


Figure 3-27 Trunk Scenario Topology

Check the status of the trunk ports on switch S1 using the **show interfaces trunk** command. The following output 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.

Output from Switch S1:

```
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>
```

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 as shown in the output.

Output from Switch S3:

```
S3# show interfaces trunk


S3#
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 the following output. 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.

Output from Switch S1:

```
S1# config terminal
S1(config)# interface fastethernet0/3
```

```
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1# show interfaces fa0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
<output omitted>
```

Output from Switch S3:

```
S3# config terminal
S3(config)# interface fastethernet0/3
S3(config-if)# switchport mode trunk
S3(config-if)# end
S3# show interfaces fa0/3 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
```

Output from Computer PC4:

```
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 3-28, 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.

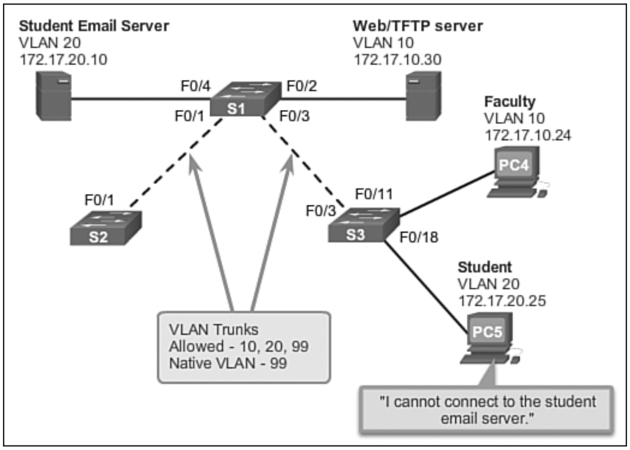


Figure 3-28 Incorrect VLAN List Scenario Topology

Check the trunk ports on switch S3 using the **show interfaces trunk** command as shown in the output that follows.

Output from Switch S3:

```
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
```

The command reveals that the interface F0/3 on switch S3 is correctly configured to allow VLANs 10, 20, and 99 as shown in the output.

An examination of the F0/3 interface on switch S1 reveals that interfaces F0/1 and F0/3 allow only VLANs 10 and 99. Someone updated the documentation but forgot to reconfigure the ports on the S1 switch, as shown in the output.

Output from Switch S1:

```
S1# show interfaces trunk
Port         Mode     Encapsulation     Status     Native vlan
Fa0/1        on       802.1q
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 the following output. 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.

Output from Switch S1:

```
S1# config terminal
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# show interface trunk
Port         Mode     Encapsulation    Status     Native vlan
Fa0/1        on       802.1q
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 has regained connectivity to the student email server found at IP address 172.17.20.10.

Output from Computer PC5:

```
PC5> ping 172.17.20.10
Pinging 172.17.20.10 with 32 bytes of data:
Reply from 172.17.20.10: 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)

Learning what attacks can occur and how to design the switch network to mitigate these attacks is important to a network technician. Because VLANs are commonly configured in a business environment, VLANs are a common security target.

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.

Interactive Graphic

Activity 3.3.1.1: Switch Spoofing Attack

Go to the online curriculum, and click the Play button in the graphic to see an animation of 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.

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 de-encapsulation, 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 as shown in Figure 3-29. 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.

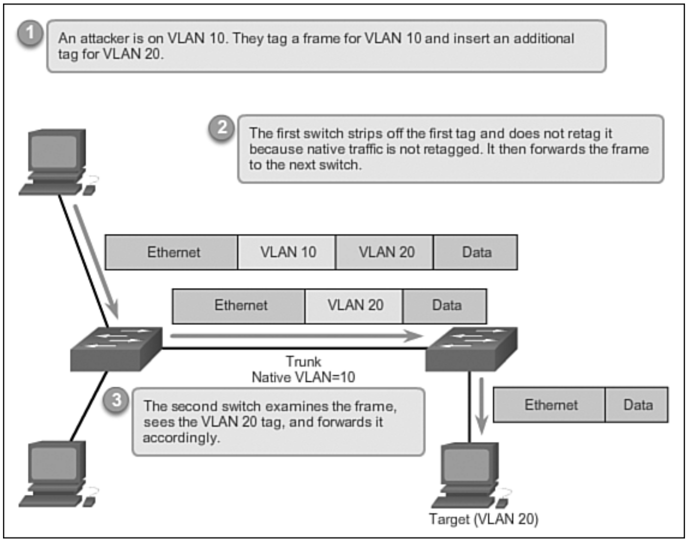

1
An attacker is on VLAN 10. They tag a frame for VLAN 10 and insert an additional tag for VLAN 20.
2
The first switch strips off the first tag and does not retag it because native traffic is not retagged. It then forwards the frame to the next switch.
Ethernet
VLAN 10
VLAN 20
Data
Ethernet
VLAN 20
Data
Trunk
Native VLAN=10
3
The second switch examines the frame, sees the VLAN 20 tag, and forwards it accordingly.
Ethernet
Data
Target (VLAN 20)

Figure 3-29 Double-Tagging Attack

A double-tagging VLAN hopping attack follows three steps:

Step 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, it is VLAN 20.

Step 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.

Step 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.

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 3-30.

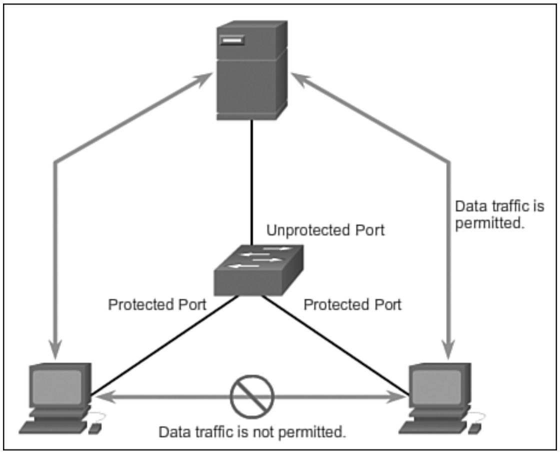


Figure 3-30 PVLAN Edge

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 the output that follows.

```
S1(config)# interface g0/1
S1(config-if)# switchport protected
S1(config-if)# end
S1# show interfaces g0/1 switchport
Name: G0/1
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
```

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.

Interactive Graphic

Activity 3.3.1.3: Configure and Verify the PVLAN Edge Feature

Go to the online curriculum, and click on the third graphic to use the Syntax Checker 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 Attack

Go to the course outline to perform this practice activity. Drag the type of attack to the description.

Design Best Practices for VLANs (3.3.2)

Because VLANs are a common security target, designing VLANs with security in mind is being proactive. Here are some best practices to use before you create the first VLAN on a switch.

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 3.3.2.2: Implementing VLAN Security

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)

This chapter thoroughly covered VLANs: how to design and create VLANs and how to transmit those VLANs to other network devices such as other switches using a trunk link. Security risks associated with VLANs and how to mitigate those risks with some proactive designs and configurations were also covered. This section helps you to determine if you learned the main points as well as the finer details of the chapter.

Class Activity 3.4.1.1: VLAN Plan

Scenario

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 or 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 1 default VLAN, use the command **delete flash:vlan.dat** and **erase startup-config.**

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 *Introduction to Routing and Switching Essentials Lab Manual* (978-1-58713-320-6). You can find the Packet Tracer Activities PKA files 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

Lab 3.3.2.2: Implementing VLAN Security

Packet Tracer Activities

Packet Tracer Activity

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 3.2.1.6: 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

Packet Tracer Activity 3.4.1.2: 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 the 'Check Your Understanding' Questions," lists the answers.

1. What is the difference between an access port and a trunk port?

    A. A trunk port belongs to a single VLAN; an access port provides access for multiple VLANs between switches.

    B. An access port can have a native VLAN, but a trunk port cannot.

    C. An access port can have only one device attached.

    D. Multiple VLANs traverse a trunk port, but an access port can belong to a single VLAN.

2. Switch S1 and Switch S2 are both configured with ports in the Faculty, Students, Voice, Guest, Printing, and Admin VLANs. Each VLAN contains 12 users. How many subnets are needed to address the VLANs?

    A. 1

    B. 2

    C. 4

    D. 6

    E. 8

    F. 12

    G. 24

3. What mechanism is used to achieve the separation between different VLANs as they cross a trunk link?

   A. VLAN tagging using 802.1Q protocol

   B. VLAN tagging using 802.1p protocol

   C. VLAN multiplexing

   D. VLAN set as a native VLAN

4. What are two options to consider when configuring a trunk link between two switches? (Choose two.)

   A. The **switchport nonegotiate** command must be configured for trunks that use DTP.

   B. Port security cannot be configured on the trunk interfaces.

   C. The native VLAN must be the same on both ends of the trunk.

   D. Different encapsulation types can be configured on both ends of the trunk link.

   E. Trunk ports can be configured only on Gigabit Ethernet interfaces.

5. A 24-port switch has been configured to support three VLANs named Sales, Marketing, and Finance. Each VLAN spans four ports on the switch. The network administrator has deleted the Marketing VLAN from the switch. What two statements describe the status of the ports associated with this VLAN? (Choose two.)

   A. The ports are inactive.

   B. The ports are administratively disabled.

   C. The ports will become trunks to carry data from all remaining VLANs.

   D. The ports will remain part of the Marketing VLAN until reassigned to another VLAN.

   E. The ports were released from the Marketing VLAN and automatically reassigned to VLAN 1.

6. Which three statements are true about hosts that are configured in the same VLAN? (Choose three.)

   A. Hosts in the same VLAN must be on the same IP subnet.

   B. Hosts in different VLANs can communicate with the aid of only the Layer 2 switch.

   C. Hosts in the same VLAN share the same broadcast domain.

   D. Hosts in the same VLAN share the same collision domain.

   E. Hosts in the same VLAN comply with the same security policy.

   F. Hosts in the same VLAN must be on the same physical segment.

7. Refer to Figure 3-8. Host PC3 is unable to transfer data because it does not have the MAC address of the destination host. If PC3 sends out an ARP request broadcast, which of the other hosts will see the message?

   A. Only PC3

   B. Only PC4

   C. Only PC4 and PC5

   D. PC1, PC2, PC4, and PC5

   E. PC1, PC2, PC3, PC4, and PC5

8. With each listed characteristic on the right, indicate in the blank on the left whether it reflects a normal range VLAN, an extended range VLAN, or VLAN 1. Use N for normal range VLAN, E for extended range VLAN, and 1 for VLAN 1.

   _______ 1–1005

   _______ 1006–4094

   _______ Stored in vlan.dat

   _______ Default management VLAN

   _______ Default native VLAN

   _______ All ports are a member of by default

   _______ Stored in running configuration file

9. Refer to the following configuration. Host 1 is connected to interface Fa0/4 with IP address 192.168.1.22/28. Host 2 is connected to interface Fa0/5 with IP address 192.168.1.33/28. Host 3 is connected to interface F0/6 with IP address 192.168.1.30/28. Select the three statements that describe the success of pinging from one host to another. (Choose three.)

```
Switch(config)# vlan 10
Switch(config-vlan)# name Faculty
Switch(config-vlan)# vlan 20
Switch(config-vlan)# name Staff
Switch(config-vlan)# interface range fa0/4 , fa0/6
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# interface fa0/5
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
```

A. Host 1 can ping Host 2.

B. Host 1 cannot ping Host 2.

C. Host 1 can ping Host 3.

D. Host 1 cannot ping Host 3.

E. Host 2 can ping Host 3.

F. Host 2 cannot ping Host 3.

10. Which three options accurately associate the Catalyst switch command with the result? (Choose three.)

A. **show vlan id** *`vlan-id`*: displays information about a specific VLAN.

B. **show vlan**: displays detailed information about all VLANs on the switch.

C. **show vlan brief:** displays detailed information about all VLANs on the switch.

D. **show interfaces fa0/1 switchport**: displays information about a specific port.

E. **show interfaces fa0/1**: displays VLAN information about a specific port.

11. Match the commands with the correct descriptions.

________ **switchport mode trunk**

________ **switchport mode dynamic desirable**

________ **switchport nonegotiate**

________ **switchport mode access**

A. Configures the port to negotiate a trunk

B. Configures the trunk to not send DTP packets

C. Configures the port as a permanent 802.1Q trunk

D. Disables trunk mode

12. Match the problem definition with the correct problem description.

_______ Native VLAN mismatch

_______ Trunk mode mismatch

_______ Incorrect VLAN list

_______ VLAN subnet conflict

A. Both switches are configured to dynamic auto and will not negotiate a link.

B. Not all the VLANs needed are allowed to traverse a trunk.

C. PCs on the same VLAN are not sharing the same address space.

D. The VLAN configured for untagged frames is not the same on two switches connected by a trunk.

13. The _____________ protocol is an industry standard for trunking.

14. Which Layer 2 security issue sends a frame destined for one VLAN to a different VLAN by adding more than one VLAN ID to the header?

A. Double-tagging

B. Switch spoofing

C. PVLAN edge

D. Plaintext vty access

15. Which two design considerations are best practices for switch VLAN design? (Choose two.)

A. Unused ports should be left to the default configuration.

B. The native VLAN should be an unused VLAN.

C. All unused ports should be configured as a part of the black hole VLAN.

D. All unused ports should be configured as a part of the native VLAN.

E. A server should always be configured as a protected port.

F. The management VLAN should be a VLAN not used by any type of user traffic.

G. Disable DTP messages.