CHAPTER 2

Basic Switching Concepts and Configuration

Objectives

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

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

Key Terms

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

Port security	*page 42*
Secure Shell (SSH)	*page 59*
DHCP snooping	*page 59*
MAC address flooding	*page 66*
DHCP starvation attack	*page 69*
Denial of service (DoS)	*page 69*
Cisco Discovery Protocol (CDP)	*page 70*
Brute force password attack	*page 71*
Best practices	*page 72*
Security audit	*page 74*
Penetration testing	*page 74*
Secure MAC address	*page 77*
Static secure MAC address	*page 77*
Dynamic secure MAC address	*page 78*
Sticky secure MAC address	*page 78*
Violation mode	*page 79*
Protect	*page 79*
Restrict	*page 79*
Shutdown	*page 79*
Error disabled	*page 83*
Network Time Protocol (NTP)	*page 85*

Introduction (2.0.1.1)

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

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

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

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

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

Class Activity 2.0.1.2: Stand by Me

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

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

Scenario 1

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

Scenario 2

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

Scenario 3

The student with the number 505C should stand. Record the number of the standing student.

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

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

Basic Switch Configuration (2.1)

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

Configure a Switch with Initial Settings (2.1.1)

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

Switch Boot Sequence (2.1.1.1)

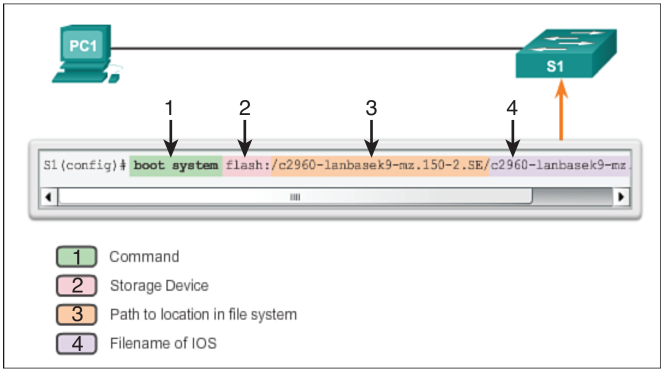
After a Cisco switch is powered on, it goes through the following boot sequence:

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

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

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

In Figure 2-1, the BOOT environment variable is set using the **boot system** global configuration mode command. Notice that the IOS is located in a distinct folder and the folder path is specified. Use the **show bootvar** command (**show boot** in older IOS versions) to see to what the current IOS boot file is set.



```
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 the files stored in flash memory.

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

How To

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

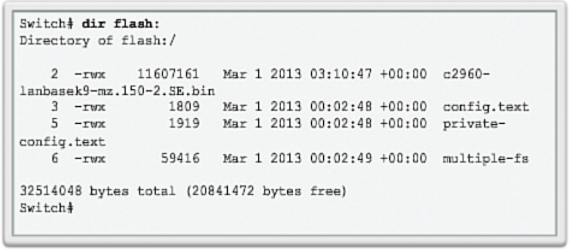
Step 2. Unplug the switch power cord, because many Cisco switches do not have an on/off switch.

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

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

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

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



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

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

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

Figure 2-2 Directory Listing in Boot Loader

Note

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

Switch LED Indicators (2.1.1.3)

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

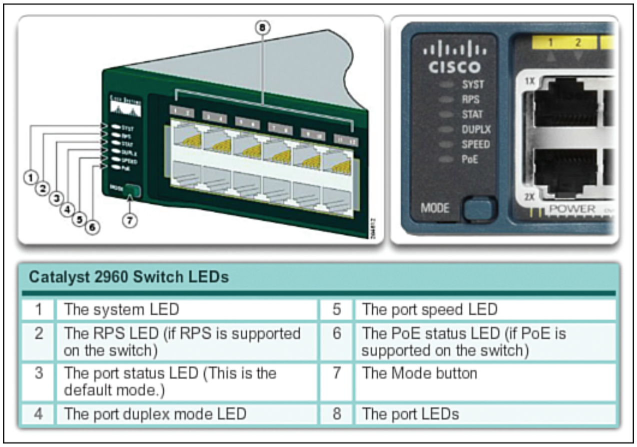
Figure 2-3 shows the switch LEDs and the **Mode** button for a Cisco Catalyst 2960 switch. The **Mode** button is used to toggle through port status, port duplex, port speed, and PoE (if supported) status of the port LEDs. The following describes the purpose of the LED indicators and the meaning of their colors:

- **System LED:** Shows whether the system is receiving power and is functioning properly. If the LED is off, it means that the system is not powered on. If the LED is green, the system is operating normally. If the LED is amber, the system is receiving power but is not functioning properly.

- **Redundant Power System (RPS) LED:** Shows the RPS status. If the LED is off, the RPS is off or not properly connected. If the LED is green, the RPS is connected and ready to provide backup power. If the LED is blinking green, the RPS is connected but is unavailable because it is providing power to another device. If the LED is amber, the RPS is in standby mode or in a fault condition. If the LED is blinking amber, the internal power supply in the switch has failed, and the RPS is providing power.

- **Port Status LED:** Indicates that the port status mode is selected when the LED is green. This is the default mode. When selected, the port LEDs will display colors with different meanings. If the LED is off, there is no link, or the port was administratively shut down. If the LED is green, a link is present. If the LED is blinking green, there is activity and the port is sending or receiving data. If the LED is alternating green-amber, there is a link fault. If the LED is amber, the port is blocked to ensure that a loop does not exist in the forwarding domain and is not forwarding data (typically, ports will remain in this state for the first 30 seconds after being activated). If the LED is blinking amber, the port is blocked to prevent a possible loop in the forwarding domain.

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



Catalyst 2960 Switch LEDs

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

Figure 2-3 Switch LEDs

Preparing for Basic Switch Management (2.1.1.4)

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

To prepare a switch for remote management access, the switch must be configured with an IP address and a subnet mask. Keep in mind that to manage the switch from a remote network, the switch must be configured with a default gateway. This is very similar to configuring the IP address information on host devices. In Figure 2-4, the switch virtual interface (SVI) on S1 should be assigned an IP address. The SVI is a virtual interface, not a physical port on the switch.

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

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

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

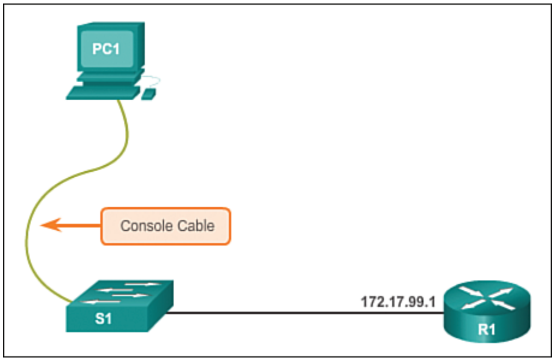


Figure 2-4 Preparing for Remote Management

Configuring Basic Switch Management Access with IPv4 (2.1.1.5)

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

How To

Step 1. Configure the management interface.

An IP address and subnet mask are configured on the management SVI of the switch from VLAN interface configuration mode. As shown in Table 2-1, the **interface vlan 99** command is used to enter interface configuration mode. The **ip address** command is used to configure the IP address. The **no shutdown** command enables the interface. In this example, VLAN 99 is configured with IP address 172.17.99.11.

Table 2-1 Cisco Switch Management Interface

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

The SVI for VLAN 99 will not appear as "up/up" until VLAN 99 is created and there is a device connected to a switch port associated with VLAN 99. To create a VLAN with the vlan_id of 99 and associate it to interface FastEthernet 0/1, use the following commands:

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

Step 2. Configure the default gateway.

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

To configure the default gateway for the switch, use the **ip default-gateway** command, as shown in Figure 2-5. Enter the IP address of the default gateway. The default gateway is the IP address of the router interface to which the switch is connected. Use the **copy running-config startup-config** command to back up your configuration.

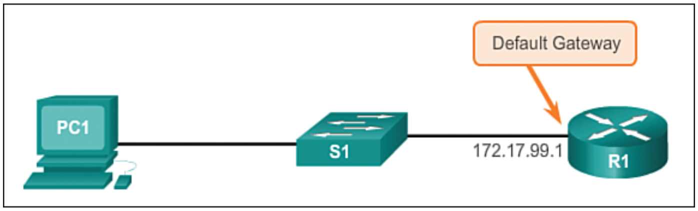


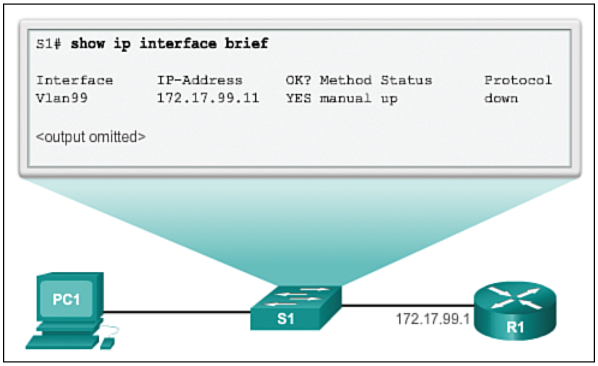
Figure 2-5 Default Gateway

Table 2-2 Configure Default Gateway for Switch

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

Step 3. Verify the configuration.

As shown in Figure 2-6, the **show ip interface brief** command is useful when determining the status of both physical and virtual interfaces. The output shown confirms that interface VLAN 99 has been configured with an IP address and subnet mask and that the interface status is "up."



```
S1# show ip interface brief

Interface     IP-Address     OK? Method Status      Protocol
Vlan99        172.17.99.11   YES manual up          down

<output omitted>
```

Figure 2-6 Verify Switch Management Interface Configuration

Lab 2.1.1.6: Configuring Basic Switch Settings

In this lab, you will complete the following objectives:

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

Configure Switch Ports (2.1.2)

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

Duplex Communication (2.1.2.1)

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

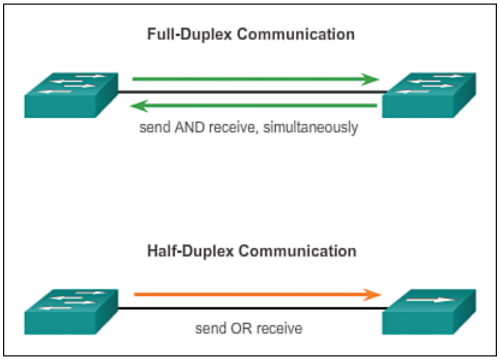

Full-Duplex Communication
send AND receive, simultaneously
Half-Duplex Communication
send OR receive

Figure 2-7 Duplex Communication

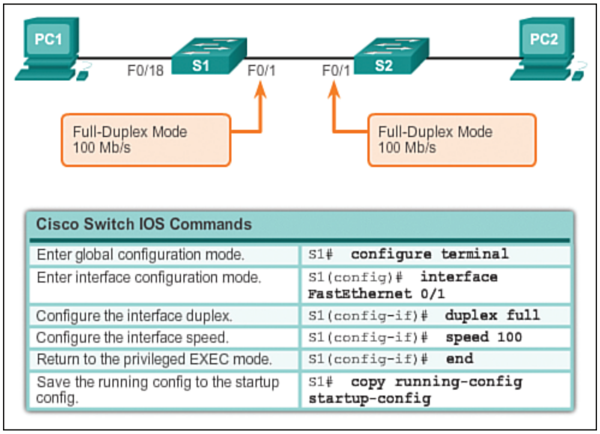
Full-duplex communication improves the performance of a switched LAN. Full-duplex communication increases effective bandwidth by allowing both ends of a connection to transmit and receive data simultaneously. This is also known as bidirectional. This method of optimizing network performance requires microsegmentation. A microsegmented LAN is created when a switch port has only one device connected and is operating at full-duplex. This results in a micro-size collision domain of a single device. However, because there is only one device connected, a microsegmented LAN is collision free.

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

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

Configure Switch Ports at the Physical Layer (2.1.2.2)

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



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

Figure 2-8 Configure Duplex and Speed

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

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

Note

Mismatched settings for the duplex mode and speed of switch ports can cause connectivity issues. Autonegotiation failure creates mismatched settings.

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

Interactive Graphic

Activity 2.1.2.2: Configuring Duplex and Speed

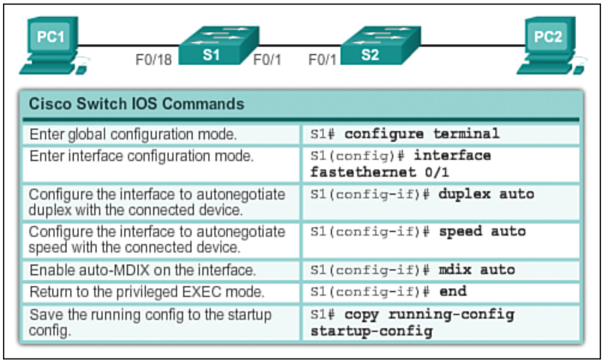
Go to the online course to use the Syntax Checker in the second graphic to configure port F0/1 of switch S1.

Auto-MDIX (2.1.2.3)

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

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

The commands to enable auto-MDIX are shown in Figure 2-9.



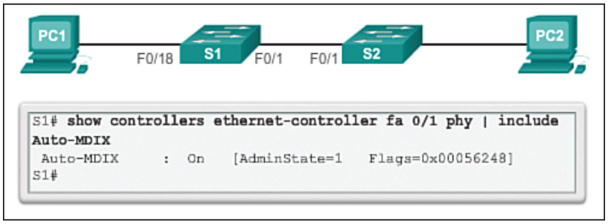
Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface fastethernet 0/1`
Configure the interface to autonegotiate duplex with the connected device.	`S1(config-if)# duplex auto`
Configure the interface to autonegotiate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

Figure 2-9 Configure Auto-MDIX

Note

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

To examine the auto-MDIX setting for a specific interface, use the **show controllers ethernet-controller** command with the **phy** keyword. To limit the output to lines referencing auto-MDIX, use the **include Auto-MDIX** filter. As shown in Figure 2-10, the output indicates On or Off for the feature.



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

Verifying Switch Port Configuration (2.1.2.4)

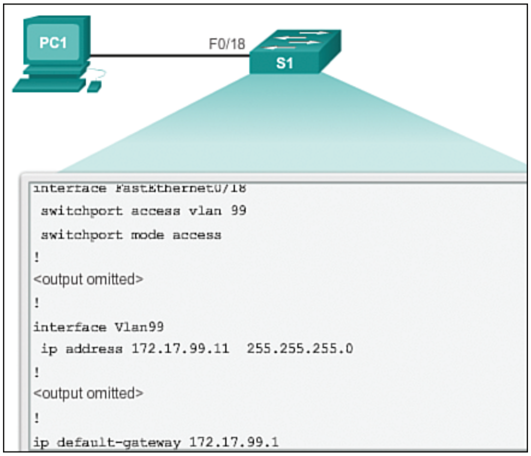
Table 2-3 describes some of the options for the **show** command that are helpful in verifying common configurable switch features.

Table 2-3 Common Verification Commands

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

Figure 2-11 shows sample abbreviated output from the **show running-config** command. Use this command to verify that the switch has been correctly configured. As seen in the output for S1, some key information is shown:

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

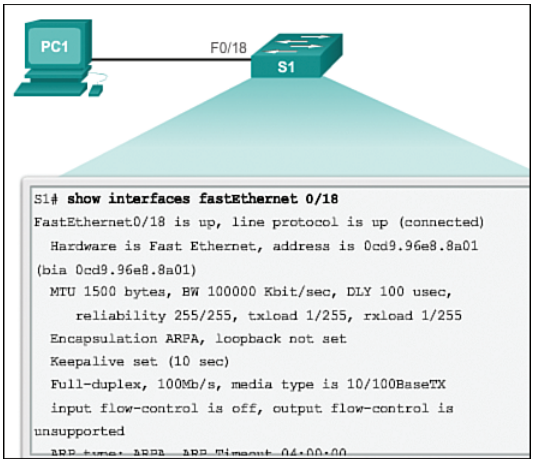


```
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
!
<output omitted>
!
interface Vlan99
 ip address 172.17.99.11  255.255.255.0
!
<output omitted>
!
ip default-gateway 172.17.99.1
```

Figure 2-11 Running Configuration

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

Figure 2-12 shows the output from the **show interfaces fastEthernet 0/18** command. The first line in the figure indicates that the FastEthernet 0/18 interface is up/up, meaning that it is operational. Farther down, the output shows that the duplex is full and the speed is 100 Mb/s.



```
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
```

Figure 2-12 Interface Status

Network Access Layer Issues (2.1.2.5)

The output from the **show interfaces** command can be used to detect common media issues. One of the most important parts of this output is the display of the line and data-link protocol status. Example 2-1 indicates the summary line to check the status of an interface, and Table 2-4 describes the interface and line protocol status.

Example 2-1 Verify Interface Status

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

Table 2-4 Verify Interface Status

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

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

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

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

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

Example 2-2 Verify Interface Counters

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

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

Table 2-5 Network Access Layer Issues

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

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

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

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

- **Collisions:** Collisions in half-duplex operations are completely normal and you should not worry about them, as long as you are pleased with half-duplex operations. However, you should never see collisions in a properly designed and configured network that uses full-duplex communication. It is highly recommended that you use full-duplex unless you have older or legacy equipment that requires half-duplex.

- **Late collisions:** A late collision refers to a collision that occurs after 512 bits of the frame (the preamble) have been transmitted. Excessive cable lengths are the most common cause of late collisions. Another common cause is duplex misconfiguration. For example, you could have one end of a connection configured for full-duplex and the other for half-duplex. You would see late collisions on the interface that is configured for half-duplex. In that case, you must configure the same duplex setting on both ends. A properly designed and configured network should never have late collisions.

Troubleshooting Network Access Layer Issues (2.1.2.6)

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

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

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

If the interface is down:

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

- If the interface is still down, the problem might be because of a mismatch in speed setting. The speed of an interface is typically autonegotiated; therefore, even if it is manually configured on one interface, the connecting interface should autonegotiate accordingly. If a speed mismatch does occur through misconfiguration or a hardware or software issue, that can result in the interface going down. Manually set the same speed on both connection ends if a problem is suspected.

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

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

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

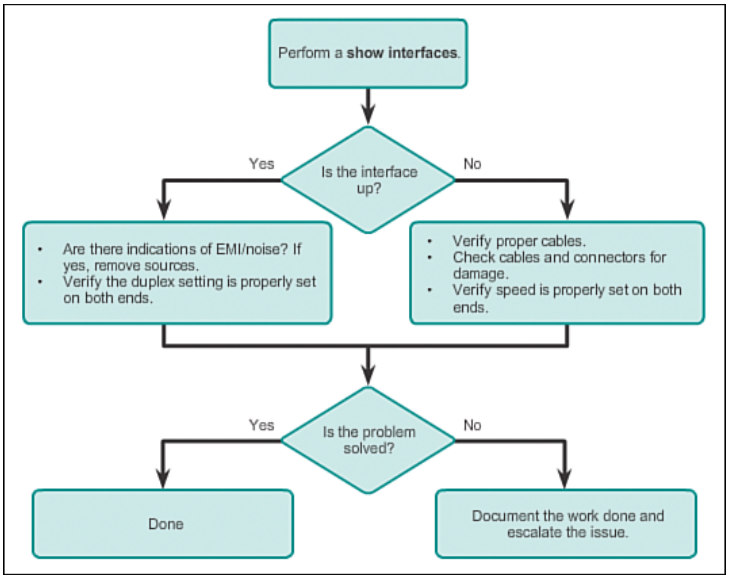

Perform a show interfaces.
Is the interface up?
Yes
No
• Are there indications of EMI/noise? If yes, remove sources.
• Verify the duplex setting is properly set on both ends.
• Verify proper cables.
• Check cables and connectors for damage.
• Verify speed is properly set on both ends.
Is the problem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

Figure 2-13 Troubleshooting Switch Media Issues

Switch Security: Management and Implementation (2.2)

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

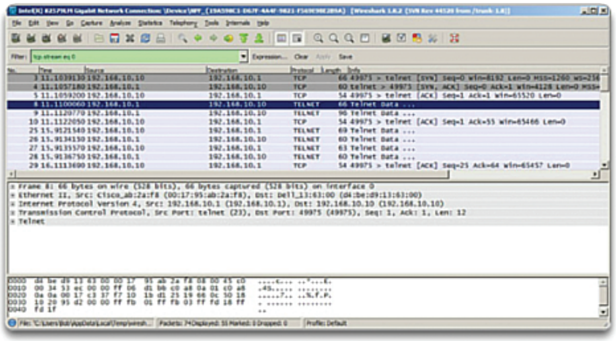
Secure Remote Access (2.2.1)

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

SSH Operation (2.2.1.1)

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

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



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.stream eq 0
Expression... Clear Apply Save

```
No.  Time       Source          Destination     Protocol Length Info
 3 11.1039130 192.168.10.10   192.168.10.1    TCP      66 49975 > telnet [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=256
 4 11.1057180 192.168.10.1    192.168.10.10   TCP      60 telnet > 49975 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=
 5 11.1059200 192.168.10.10   192.168.10.1    TCP      54 49975 > telnet [ACK] Seq=1 Ack=1 Win=65520 Len=0
 8 11.1100060 192.168.10.1    192.168.10.10   TELNET   66 Telnet Data ...
 9 11.1120770 192.168.10.1    192.168.10.10   TELNET   96 Telnet Data ...
10 11.1122050 192.168.10.10   192.168.10.1    TCP      54 49975 > telnet [ACK] Seq=1 Ack=55 Win=65466 Len=0
25 15.9121540 192.168.10.10   192.168.10.1    TELNET   69 Telnet Data ...
26 15.9134150 192.168.10.1    192.168.10.10   TELNET   60 Telnet Data ...
27 15.9135570 192.168.10.10   192.168.10.1    TELNET   63 Telnet Data ...
28 15.9136750 192.168.10.1    192.168.10.10   TELNET   60 Telnet Data ...
29 16.1113690 192.168.10.10   192.168.10.1    TCP      54 49975 > telnet [ACK] Seq=25 Ack=64 Win=65457 Len=0

+ Frame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
+ Ethernet II, Src: Cisco_ab:2a:f8 (00:17:95:ab:2a:f8), Dst: Dell_13:63:00 (d4:be:d9:13:63:00)
+ Internet Protocol Version 4, Src: 192.168.10.1 (192.168.10.1), Dst: 192.168.10.10 (192.168.10.10)
+ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 49975 (49975), Seq: 1, Ack: 1, Len: 12
+ Telnet

0000  d4 be d9 13 63 00 00 17  95 ab 2a f8 08 00 45 c0   ....c... ..*...E.
0010  00 34 53 ec 00 00 ff 06  d1 bb c0 a8 0a 01 c0 a8   .4S..... ........
0020  0a 0a 00 17 c3 37 f7 10  1b d1 25 19 66 0c 50 18   .....7.. ..%.f.P.
0030  10 20 95 d2 00 00 ff fb  01 ff fb 03 ff fd 18 ff   . ...... ........
0040  fd 1f                                              ..
```

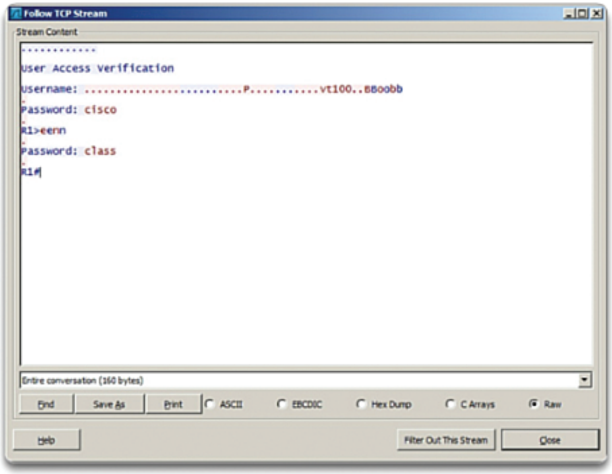
File: "C:\Users\Bob\AppData\Local\Temp\wiresh... Packets: 74 Displayed: 55 Marked: 0 Dropped: 0 Profile: Default

Figure 2-14 Wireshark Telnet Capture

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

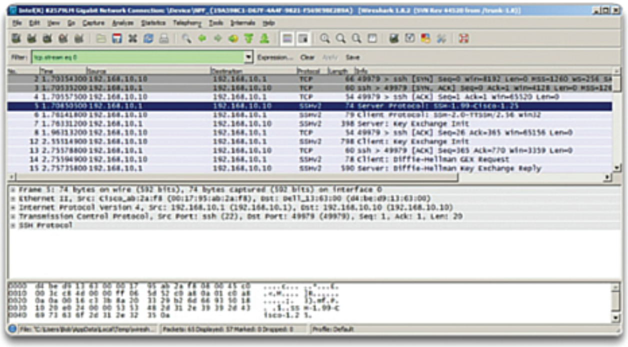
Figure 2-16 shows the Wireshark view of an SSH session. The attacker can track the session using the IP address of the administrator device.

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



```
............
User Access Verification
Username: .........................P...........vt100..BBoobb
Password: cisco
R1>eenn
Password: class
R1#
```

Figure 2-15 Plaintext Username and Password Captured



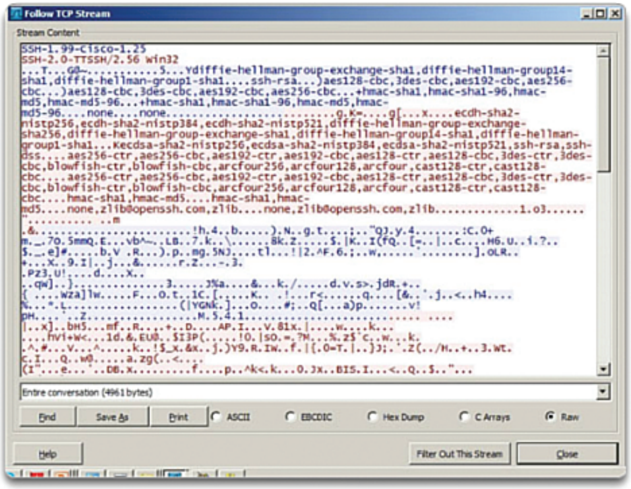
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.stream eq 0
Expression... Clear Apply Save

```
No.  Time        Source         Destination    Protocol Length Info
 2 1.70354300 192.168.10.10  192.168.10.1   TCP      66 49979 > ssh [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=256 SA
 3 1.70535200 192.168.10.1   192.168.10.10  TCP      60 ssh > 49979 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=126
 4 1.70557500 192.168.10.10  192.168.10.1   TCP      54 49979 > ssh [ACK] Seq=1 Ack=1 Win=65520 Len=0
 5 1.70650500 192.168.10.1   192.168.10.10  SSHv2    74 Server Protocol: SSH-1.99-Cisco-1.25
 6 1.76141800 192.168.10.10  192.168.10.1   SSHv2    79 Client Protocol: SSH-2.0-TTSSH/2.56 Win32
 7 1.76331200 192.168.10.1   192.168.10.10  SSHv2   398 Server: Key Exchange Init
 8 1.96313200 192.168.10.10  192.168.10.1   TCP      54 49979 > ssh [ACK] Seq=26 Ack=365 Win=65156 Len=0
12 2.55514900 192.168.10.10  192.168.10.1   SSHv2   798 Client: Key Exchange Init
13 2.75578800 192.168.10.1   192.168.10.10  TCP      60 ssh > 49979 [ACK] Seq=365 Ack=770 Win=3359 Len=0
14 2.75594900 192.168.10.10  192.168.10.1   SSHv2    78 Client: Diffie-Hellman GEX Request
15 2.75735800 192.168.10.1   192.168.10.10  SSHv2   590 Server: Diffie-Hellman Key Exchange Reply

+ Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
+ Ethernet II, Src: Cisco_ab:2a:f8 (00:17:95:ab:2a:f8), Dst: Dell_13:63:00 (d4:be:d9:13:63:00)
+ Internet Protocol Version 4, Src: 192.168.10.1 (192.168.10.1), Dst: 192.168.10.10 (192.168.10.10)
+ Transmission Control Protocol, Src Port: ssh (22), Dst Port: 49979 (49979), Seq: 1, Ack: 1, Len: 20
+ SSH Protocol

0000  d4 be d9 13 63 00 00 17  95 ab 2a f8 08 00 45 c0   ....c... ..*...E.
0010  00 3c c8 4d 00 00 ff 06  5d 52 c0 a8 0a 01 c0 a8   .<.M.... ]R......
0020  0a 0a 00 16 c3 3b 8a 20  33 29 b2 6d 66 93 50 18   .....;.  3).mf.P.
0030  10 20 e0 24 00 00 53 53  48 2d 31 2e 39 39 2d 43   . .$..SS H-1.99-C
0040  69 73 63 6f 2d 31 2e 32  35 0a                     isco-1.2 5.
```

Figure 2-16 Wireshark SSH Capture



```
SSH-1.99-Cisco-1.25
SSH-2.0-TTSSH/2.56 Win32
...T...G0~...........5...Ydiffie-hellman-group-exchange-sha1,diffie-hellman-group14-
sha1,diffie-hellman-group1-sha1....ssh-rsa...)aes128-cbc,3des-cbc,aes192-cbc,aes256-
cbc...)aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc...+hmac-sha1,hmac-sha1-96,hmac-
md5,hmac-md5-96...+hmac-sha1,hmac-sha1-96,hmac-md5,hmac-
md5-96....none....none.............................g.K=....g[...x....ecdh-sha2-
nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-
sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-
group1-sha1...Kecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,ssh-
dss....aes256-ctr,aes256-cbc,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,3des-ctr,3des-
cbc,blowfish-ctr,blowfish-cbc,arcfour256,arcfour128,arcfour,cast128-ctr,cast128-
cbc....aes256-ctr,aes256-cbc,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,3des-ctr,3des-
cbc,blowfish-ctr,blowfish-cbc,arcfour256,arcfour128,arcfour,cast128-ctr,cast128-
cbc....hmac-sha1,hmac-md5....hmac-sha1,hmac-
md5....none,zlib@openssh.com,zlib....none,zlib@openssh.com,zlib.............1.o3......
"..........  ..m
.&........................!h.4..b.....).N..g.t....;.."QJ.y.4........:C.O+
m._.7O.5mmQ.E...vb^~..LB..7.k..\......8k.Z.....$.|K..I(fQ..[=..|..c....H6.U..i.?..
$._.e]#.....b.V .R...).p..mg.5NJ....tl...!|2.^F.6.;..W,....'........].OLR..
+...X..9.I|..j...&......r.Z...-.3.
.Pz3.U!....d....X..
..qw]..}..............3.....J%a....&...k./.....d.v.s>.jdR.+..
{ ....Wza]lw.....F...O.t..1C.[.....K.. .!...r<......q....[&..'.j..<..h4....
%...*.L..................(|YGNk.]...O....#;..Q[...a)p.......v!
pH....'..Z..................M.5.4.1...................................  ....
|..x]..bH5...mf..R...,.+..D....AP.I...V.81x.|....W....k...
.....hVi+W<...1d.&.EU0..$I3P(.....!O.|SO.=.?M...%.Z$`c..W...k.
.^.#...V...^.....k..!$_x.&x..j.)Y9.R.IW..f.|(.O=T.|..}J;.'.Z(../H..+..3.Wt.
c.I...Q..W0.....a.zg(..<....
(I"...e...'..DB.x.........f....p..^k<.k...0.Jx..BIS.I...<..Q..$.."...
```

Figure 2-17 Username and Password Encrypted

To enable SSH on a Catalyst 2960 switch, the switch must be using a version of the IOS software including cryptographic (encrypted) features and capabilities. In Example 2-3, use the **show version** command on the switch to see which IOS the switch is currently running, and verify that the IOS filename includes the combination “k9”, which indicates that it supports cryptographic (encrypted) features and capabilities.

Example 2-3 Cryptographic Image

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

Configuring SSH (2.2.1.2)

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

Step 1. Verify SSH support.

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

Step 2. Configure the IP domain name.

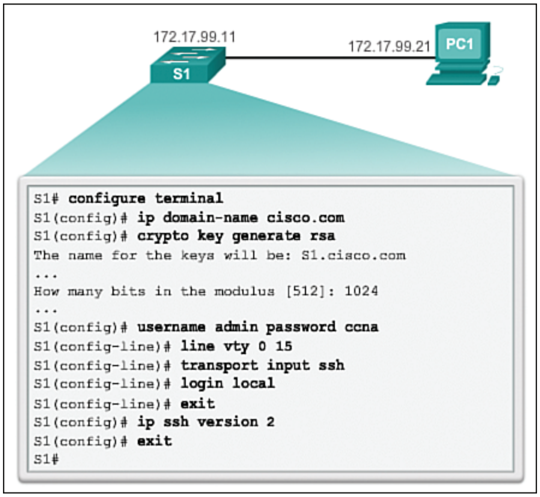
Configure the IP domain name of the network using the **ip domain-name** *domain-name* global configuration mode command. In Figure 2-18, the *domain-name* value is **cisco.com**.

Step 3. Generate RSA key pairs.

Generating an RSA key pair automatically enables SSH. Use the **crypto key generate rsa** global configuration mode command to enable the SSH server on the switch and generate an RSA key pair. When generating RSA keys, the administrator is prompted to enter a modulus length. Cisco recommends a minimum modulus size of 1024 bits (see the sample configuration in Figure 2-18). A longer modulus length is more secure, but it takes longer to generate and to use.

Note

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



```
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)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
S1(config)# ip ssh version 2
S1(config)# exit
S1#
```

Figure 2-18 Configure SSH for Remote Management

Step 4. Configure user authentication.

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

Step 5. Configure the vty lines.

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

Step 6. Enable SSH version 2.

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

Interactive Graphic

Activity 2.2.1.2: Configure SSH

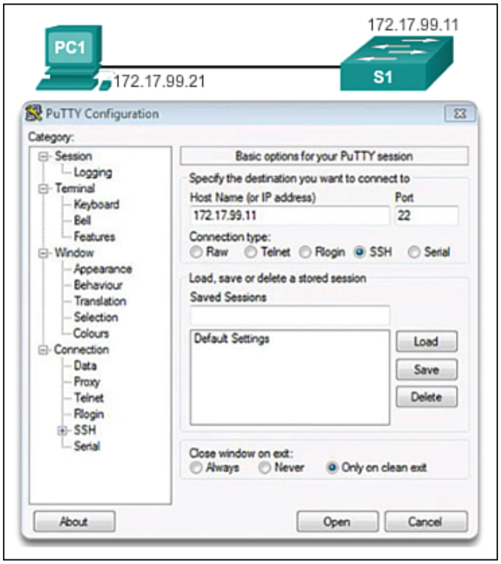
Go to the online course to use the Syntax Checker in the second graphic to configure SSH on S1.

Verifying SSH (2.2.1.3)

On a PC, an SSH client, such as PuTTY, is used to connect to an SSH server. For the examples in Figures 2-19, 2-20, and 2-21, the following have been configured:

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

In Figure 2-19, the PC initiates an SSH connection to the SVI VLAN IP address of S1.



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

Load, save or delete a stored session

Saved Sessions

Default Settings

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

Figure 2-19 Configure PuTTY SSH Client Connection Parameters

In Example 2-4 (and the related graphic in Figure 2-20), the user has been prompted for a username and password. Using the configuration from the previous example, the username **admin** and password **ccna** are entered. After entering the correct combination, the user is connected through SSH to the CLI on the Catalyst 2960 switch.

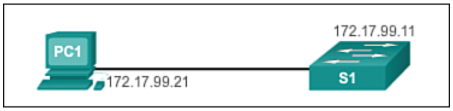


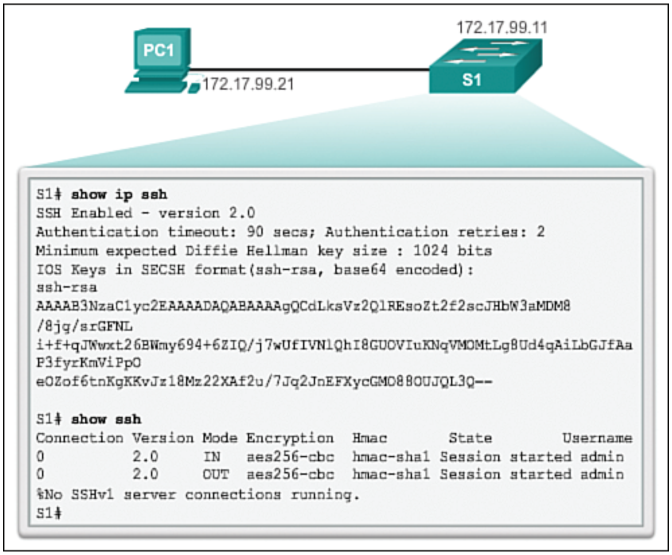
Figure 2-20 Remote Management SSH Connection

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

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

S1> enable
Password:
S1#
```

To display the version and configuration data for SSH on the device that you configured as an SSH server, use the **show ip ssh** command. In the example, SSH version 2 is enabled. To check the SSH connections to the device, use the **show ssh** command (see Figure 2-21).



```
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
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2Q1REsoZt2f2scJHbW3aMDM8
/8jq/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 2-21 Verify SSH Status and Settings

Packet Tracer
□ Activity

Packet Tracer Activity 2.2.1.4: Configuring SSH

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

Security Concerns in LANs (2.2.2)

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

Common Security Attacks: MAC Address Flooding (2.2.2.1)

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

MAC Address Flooding

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

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

In Figure 2-22, host A sends traffic to host B. The switch receives the frames and looks up the destination MAC address in its MAC address table. If the switch cannot find the destination MAC in the MAC address table, the switch then copies the frame and floods (broadcasts) it out of every switch port, except the port where it was received.

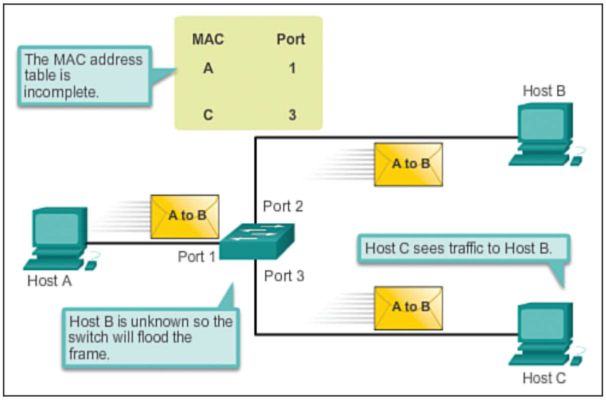

The MAC address table is incomplete.
MAC
Port
A
1
C
3
Host B
A to B
A to B
Port 2
Port 1
Port 3
Host A
Host C sees traffic to Host B.
A to B
Host B is unknown so the switch will flood the frame.
Host C

Figure 2-22 Switch Floods Frame for Unknown MAC Address

In Figure 2-23, host B receives the frame and sends a reply to host A. The switch then learns that the MAC address for host B is located on port 2 and records that information into the MAC address table.

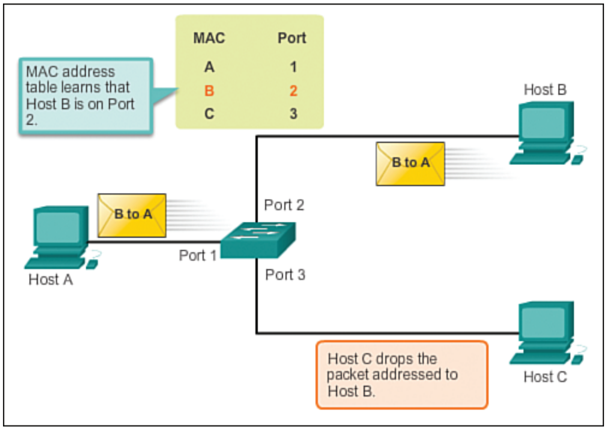
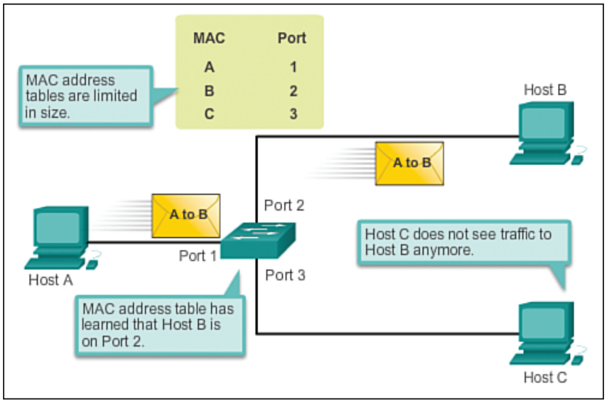

MAC address table learns that Host B is on Port 2.
MAC
Port
A
1
B
2
C
3
Host B
B to A
B to A
Port 2
Port 1
Port 3
Host A
Host C drops the packet addressed to Host B.
Host C

Figure 2-23 Switch Records MAC Address

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

As shown in Figure 2-24, any frame sent by host A (or any other host) to host B is forwarded to port 2 of the switch and not broadcast out every port.



MAC	Port
A	1
B	2
C	3

MAC address tables are limited in size.

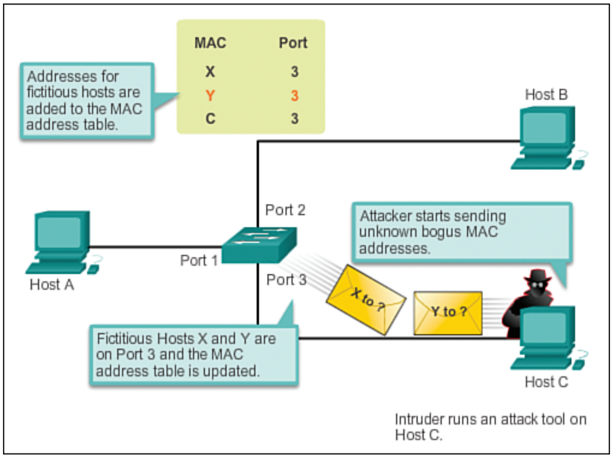
Host C does not see traffic to Host B anymore.

MAC address table has learned that Host B is on Port 2.

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

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

As shown in Figure 2-25, an attacker at host C can send frames with fake, randomly generated source and destination MAC addresses to the switch. The switch updates the MAC address table with the information in the fake frames. When the MAC address table is full of fake MAC addresses, the switch enters into what is known as fail-open mode. In this mode, the switch broadcasts all frames to all machines on the network. As a result, the attacker can see all the frames.



MAC	Port
X	3
Y	3
C	3

Addresses for fictitious hosts are added to the MAC address table.

Attacker starts sending unknown bogus MAC addresses.

Fictitious Hosts X and Y are on Port 3 and the MAC address table is updated.

Intruder runs an attack tool on Host C.

Figure 2-25 MAC Address Flooding Attack

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

As shown in Figure 2-26, as long as the MAC address table on the switch remains full, the switch broadcasts all received frames out of every port. In this example, frames sent from host A to host B are also broadcast out of port 3 on the switch and seen by the attacker at host C.

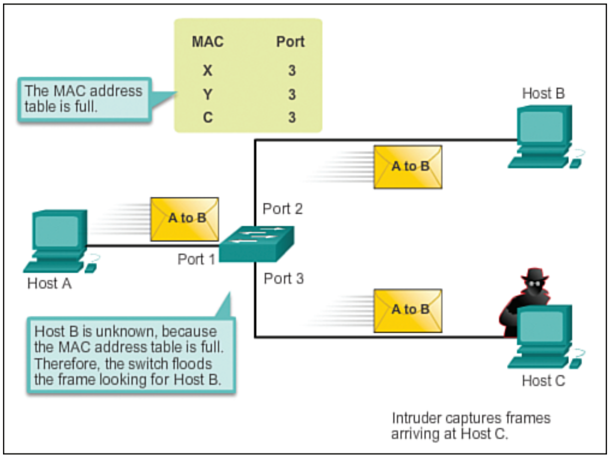

MAC
Port
X
3
Y
3
C
3
The MAC address table is full.
Host B
A to B
Port 2
A to B
Port 1
Host A
Port 3
A to B
Host B is unknown, because the MAC address table is full. Therefore, the switch floods the frame looking for Host B.
Host C
Intruder captures frames arriving at Host C.

Figure 2-26 Switch Acts Like a Hub

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

Common Security Attacks: DHCP Spoofing (2.2.2.2)

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

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

In DHCP spoofing attacks, an attacker configures a fake DHCP server on the network to issue DHCP addresses to clients, as shown in Figure 2-27. The normal reason for this attack is to force the clients to use false Domain Name System (DNS) or Windows Internet Naming Service (WINS) servers and to make the clients use the attacker, or a machine under the control of the attacker, as their default gateway.

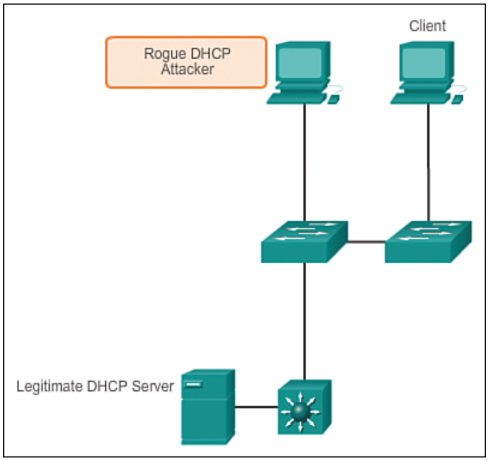


Figure 2-27 DHCP Spoofing

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

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

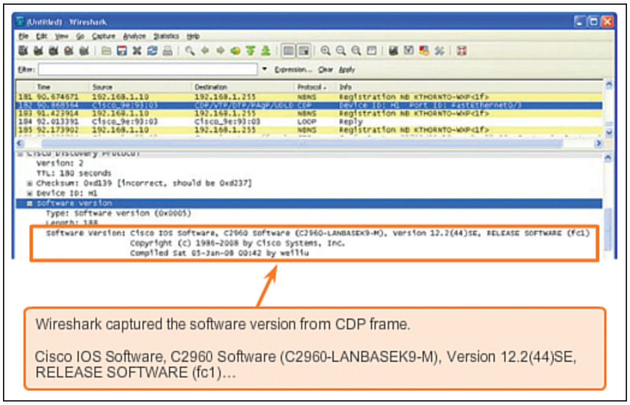
Common Security Attacks: Leveraging CDP (2.2.2.3)

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

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

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

Figure 2-28 is a portion of a Wireshark capture showing the contents of a CDP packet. The Cisco IOS Software version discovered through CDP, in particular, would allow the attacker to determine whether there were any security vulnerabilities specific to that particular version of IOS. Also, because CDP is not authenticated, an attacker could craft bogus CDP packets and send them to a directly connected Cisco device.



(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 90.868364   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 2-28 CDP Attack

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

Telnet Attacks

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

Brute Force Password Attack

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

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

Telnet DoS Attack

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

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

Note

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

Interactive Graphic

Activity 2.2.2.4: Identify Common Security Attacks

Go to the online course to perform this practice activity.

Security Best Practices (2.2.3)

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

Best Practices (2.2.3.1)

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

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

These methods, illustrated in Figure 2-29, are only a starting point for security management. Organizations must remain vigilant at all times to defend against continually evolving threats. Use network security tools to measure the vulnerability of the current network.

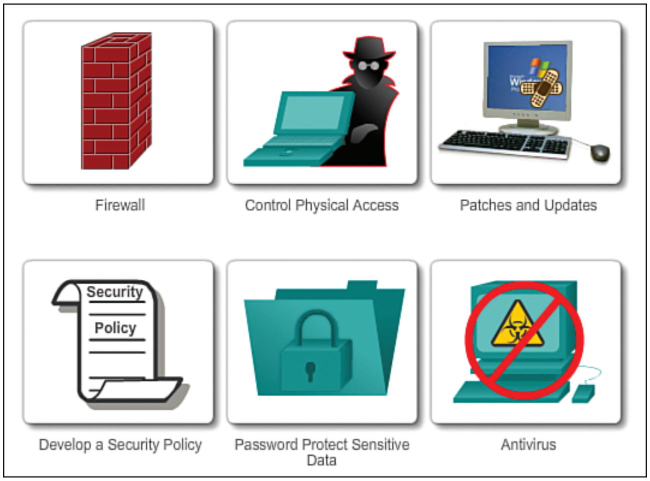


Figure 2-29 Security Best Practices

Network Security Tools and Testing (2.2.3.2)

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

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

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

Network Security Audits (2.2.3.3)

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

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

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

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

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

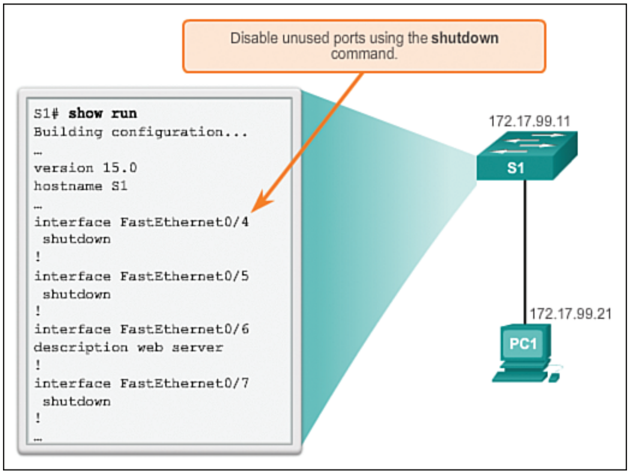
Switch Port Security (2.2.4)

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

Secure Unused Ports (2.2.4.1)

A simple method that many administrators use to help secure the network from unauthorized access is to disable all unused ports on a switch. For example, if a

Catalyst 2960 switch has 24 ports and there are three Fast Ethernet connections in use, it is good practice to disable the 21 unused ports. Navigate to each unused port and issue the Cisco IOS **shutdown** command. If a port later needs to be reactivated, it can be enabled with the **no shutdown** command. Figure 2-30 shows partial output for this configuration.



Disable unused ports using the **shutdown** command.

```
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 2-30 Disable Unused Ports

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

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

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

DHCP Snooping (2.2.4.2)

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

As shown in Figure 2-31, untrusted ports are those not explicitly configured as trusted. A DHCP binding table is built for untrusted ports. Each entry contains a client MAC address, IP address, lease time, binding type, VLAN number, and port ID recorded as clients make DHCP requests. The table is then used to filter subsequent

DHCP traffic. From a DHCP snooping perspective, untrusted access ports should not send any DHCP server messages.

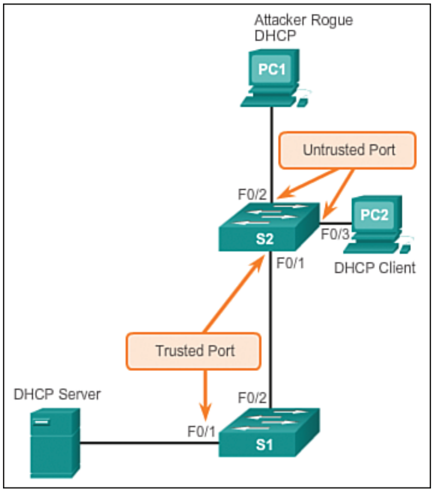


Figure 2-31 DHCP Snooping Operation

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

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

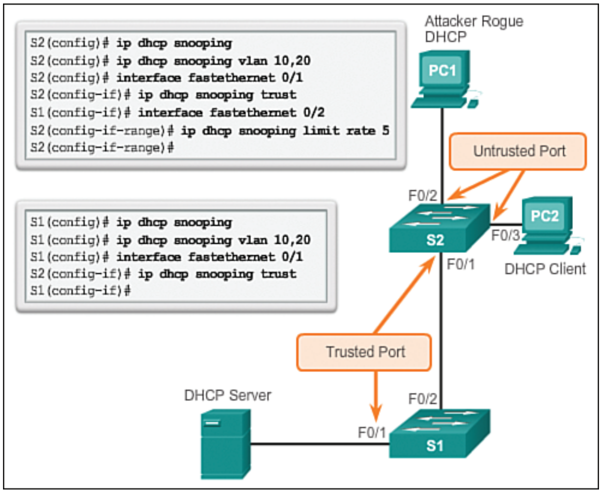
How To

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

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

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

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



```
S2(config)# ip dhcp snooping
S2(config)# ip dhcp snooping vlan 10,20
S2(config)# interface fastethernet 0/1
S2(config-if)# ip dhcp snooping trust
S1(config-if)# interface fastethernet 0/2
S2(config-if-range)# ip dhcp snooping limit rate 5
S2(config-if-range)#
```

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10,20
S1(config)# interface fastethernet 0/1
S2(config-if)# ip dhcp snooping trust
S1(config-if)#
```

Figure 2-32 DHCP Snooping Configuration

Port Security: Operation (2.2.4.3)

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

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

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

Secure MAC Address Types

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

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

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

Sticky Secure MAC Addresses

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

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

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

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

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

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

Port Security: Violation Modes (2.2.4.4)

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

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

An interface can be configured for one of three ***violation modes***, specifying the action to be taken if a violation occurs:

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

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

Table 2-6 Port Security Violation Modes

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

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

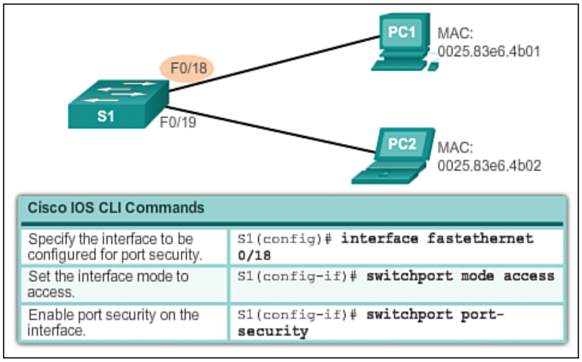
Port Security: Configuring (2.2.4.5)

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

Table 2-7 Port Security Defaults

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

Figure 2-33 shows the Cisco IOS CLI commands needed to configure port security on the Fast Ethernet F0/18 port on the S1 switch. Notice that the example does not specify a violation mode. In this example, the violation mode is shutdown (the default mode).

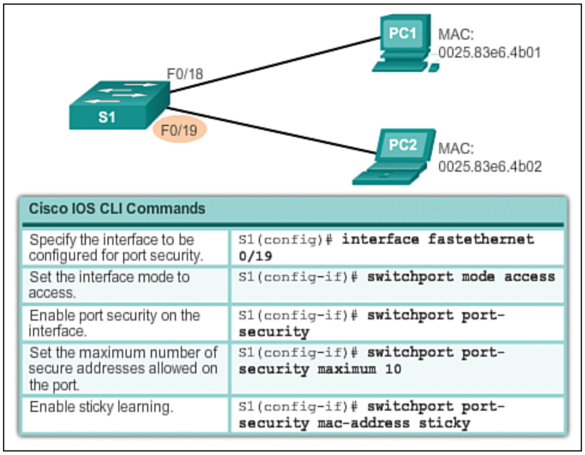


Cisco IOS CLI Commands

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`

Figure 2-33 Configure Dynamic Port Security

Figure 2-34 shows how to enable sticky secure MAC addresses for port security on Fast Ethernet port 0/19 of switch S1. As stated earlier, the maximum number of secure MAC addresses can be manually configured. In this example, the Cisco IOS command syntax is used to set the maximum number of MAC addresses to 10 for port 0/19. The violation mode is set to shutdown, by default.



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

Figure 2-34 Configure Sticky Port Security

Port Security: Verifying (2.2.4.6)

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

Verify Port Security Settings

To display port security settings for the switch or for the specified interface, use the **show port-security** [**interface** *interface-id*] command. The output for the dynamic port security configuration is shown in Example 2-5. By default, there is one MAC address allowed on this port.

Example 2-5 Verify Dynamic MAC Addresses

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

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

Example 2-6 Verify Sticky MAC Addresses

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

Note

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

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

Example 2-7 Verify Sticky MAC Addresses in Running Configuration

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

Verify Secure MAC Addresses

To display all secure MAC addresses configured on all switch interfaces, or on a specified interface with aging information for each, use the **show port-security address** command. As shown in Example 2-8, the secure MAC addresses are listed along with the types.

Example 2-8 Verify Secure MAC Addresses

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

Ports in Error-Disabled State (2.2.4.7)

When a port is configured with port security, a violation can cause the port to become ***error disabled***. When a port is error disabled, it is effectively shut down and no traffic is sent or received on that port. A series of port security–related messages display on the console, similar to those shown in Example 2-9.

Example 2-9 Port Security Violation Messages

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

Note

The port protocol and link status is changed to down.

The port LED will change to orange. The **show interfaces** command identifies the port status as **err-disabled** (see Example 2-10). The output of the **show port-security interface** command now shows the port status as **secure-shutdown**. Because the port security violation mode is set to shutdown, the port with the security violation goes to the error-disabled state.

Example 2-10 Port Status

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

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

Example 2-11 Reenabling an Error-Disabled Port

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

Network Time Protocol (NTP) (2.2.4.8)

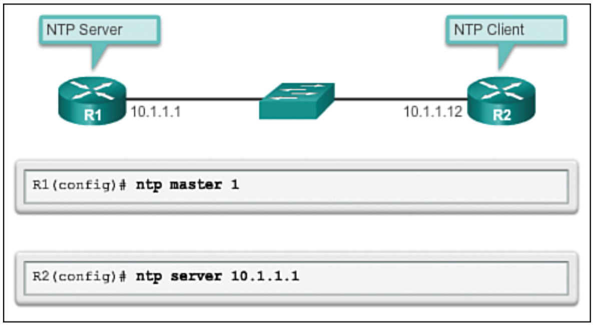
Having the correct time within networks is important. Correct time stamps are required to accurately track network events such as security violations. Additionally, clock synchronization is critical for the correct interpretation of events within syslog data files as well as for digital certificates.

Network Time Protocol (NTP) is a protocol that is used to synchronize the clocks of computer systems over packet-switched, variable-latency data networks. NTP allows network devices to synchronize their time settings with an NTP server. A group of NTP clients that obtain time and date information from a single source will have more consistent time settings.

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

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

A network device can be configured as either an NTP server or an NTP client. To allow the software clock to be synchronized by an NTP time server, use the **ntp server** *ip-address* command in global configuration mode. A sample configuration is shown in Figure 2-35. Router R2 is configured as an NTP client, while Router R1 serves as an authoritative NTP server.



```
R1(config)# ntp master 1
```

```
R2(config)# ntp server 10.1.1.1
```

Figure 2-35 Port Status

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

To display the status of NTP associations, use the **show ntp associations** command in privileged EXEC mode. This command will indicate the IP address of any peer devices that are synchronized to this peer, statically configured peers, and stratum number. The **show ntp status** user EXEC command can be used to display such information as the NTP synchronization status, the peer that the device is synchronized to, and in which NTP strata the device is functioning. Example 2-12 displays the verification of NTP on Router R2.

Example 2-12 Configuring NTP

```
R2# show ntp associations


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

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

Packet Tracer
□ **Activity**

Packet Tracer Activity 2.2.4.9: Configuring Switch Port Security

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

Packet Tracer
□ **Activity**

Packet Tracer Activity 2.2.4.10: Troubleshooting Switch Port Security

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

Lab 2.2.4.11: Configuring Switch Security Features

In this lab, you will complete the following objectives:

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

Summary (2.3)

Class Activity 2.3.1.1: Switch Trio

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

> "By Monday, April 18, 20xx, the first three ports of all configurable switches located in all offices must be secured with MAC addresses—one address will be reserved for the printer, one address will be reserved for the laptop in the office, and one address will be reserved for the office server.
>
> If a port's security is breached, we ask that you shut it down until the reason for the breach can be certified.
>
> Please implement this policy no later than the date stated in this memorandum. For questions, call 1.800.555.1212. Thank you. The Network Management Team."

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

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

Packet Tracer
□ Activity

Packet Tracer Activity 2.3.1.2: Skills Integration Challenge

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

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

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

4. The boot loader initializes the flash file system on the system board.
5. The boot loader locates and loads a default IOS operating system software image into memory and hands control of the switch over to the IOS.

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

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

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

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

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

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

- Develop a written security policy for the organization.
- Shut down unused services and ports.
- Use strong passwords and change them often.
- Control physical access to devices.
- Avoid using standard insecure HTTP websites, especially for login screens. Instead use the more secure HTTPS.
- Perform backups and test the backed-up files on a regular basis.

- Educate employees about social engineering attacks, and develop policies to validate identities over the phone, through email, and in person.
- Encrypt sensitive data and protect it with a strong password.
- Implement security hardware and software, such as firewalls.
- Keep IOS software up to date by installing security patches weekly or daily, if possible.

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

Practice

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

Class Activities

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

Labs

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

Packet Tracer
□ **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 'Check Your Understanding' Questions" lists the answers.

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

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

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

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

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

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

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

   A. Encryption

   B. More connection lines

   C. Connection-oriented services

   D. Username and password authentication

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

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

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

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

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

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

   A. In privileged EXEC mode

   B. On the switch interface FastEthernet 0/0

   C. On the management VLAN virtual interface

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

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

   A. So that there can be remote connectivity to the switch through such programs as Telnet and ping

   B. So that frames can be sent through the switch to the router

   C. So that frames generated from workstations and destined for remote networks can pass to a higher level

   D. So that other networks can be accessed from the command prompt of the switch

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

   A. Sets the link speed

   B. Sets the IP address

   C. Sets the link duplex mode

   D. Sets MAC address assignments on the switch port

   E. Sets the ring speed

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

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

   B. Unplug the switch power cord.

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

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

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

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

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

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

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

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

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

    A. **ip ssh version 2** in global configuration mode

    B. **crypto key generate rsa** in global configuration mode

    C. **transport input ssh** in line VTY configuration mode

    D. **login local** in line vty configuration mode

    E. **ip domain-name** <*domain-name*> in global configuration mode

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

    A. Connect a host to an interface associated with VLAN 99.

    B. Configure a default gateway.

    C. Remove all access ports from VLAN 99.

    D. Configure a transport input method on the vty lines.

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

    A. There is a duplex mismatch error.

    B. There is a link fault error. This port is unable to forward frames.

    C. The port is operational and ready to transmit packets.

    D. This port has been disabled by management and is unable to forward frames.

    E. The flash memory is busy.

16. Describe a DHCP starvation attack.

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

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

    A. On the production network during nonpeak times

    B. Under controlled conditions during business hours on the production network

    C. On an off-line test bed network that mimics the actual production network

    D. On a network environment simulated by software

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

    A. The sticky secure MAC addresses are removed from the address table and from the running configuration.

    B. The sticky secure MAC addresses remain part of the address table but are removed from the running configuration.

    C. The static secure MAC addresses are removed from the address table and from the running configuration.

    D. The static secure MAC addresses remain part of the address table but are removed from the running configuration.

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

    A. Packets with unknown source addresses are dropped, and there is no notification that a security violation has occurred.

    B. Packets with unknown source addresses are dropped, and there is a notification that a security violation has occurred.

    C. Packets with unknown source addresses are dropped, and the interface becomes error-disabled and turns off the port LED.

    D. Packets with unknown source addresses are forwarded, and there is a notification to the syslog server.