Basic Switching Concepts and Configuration

Objectives

After completing this course, students will be able to

- Identify the steps a switch takes after power is applied.
- Describe the function of the boot loader if the operating system is corrupt or missing.
- Explain how the switch LEDs help with troubleshooting.
- Explain the steps taken to configure a Cisco switch with an IP address, subnet mask, and default gateway.
- Identify what interface is used to apply an IP address to a Cisco switch.
- Explain the functionality available once a switch has an IP address and the default gateway.
- Enumerate the types of customization can be applied to a switch port.
- Enumerate the tools that can be used to troubleshoot a Layer 1 or 2 problems.
- List the steps required to configure a switch for SSH access.
- Explain the common security attacks that affect switches.
- What mitigation tools could be used on a Cisco switch to prevent or react to a security attack?
- Understand the best practices for switch security.
- Identify the steps required to configure switch security.

Introduction

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

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

Additionally, Cisco switches can be managed both locally and remotely. To remotely manage a switch, it needs to have

- an IP address
- default gateway configured.

Switches operate at the access layer where client network devices connect directly to the network. Switches need to be configured to be resilient to attacks of all types while they are protecting user data and allowing for high speed connections. Port security is one of the security features Cisco managed switches provide.

Basic Switch Configuration

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

Switch Boot Sequence

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

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

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

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

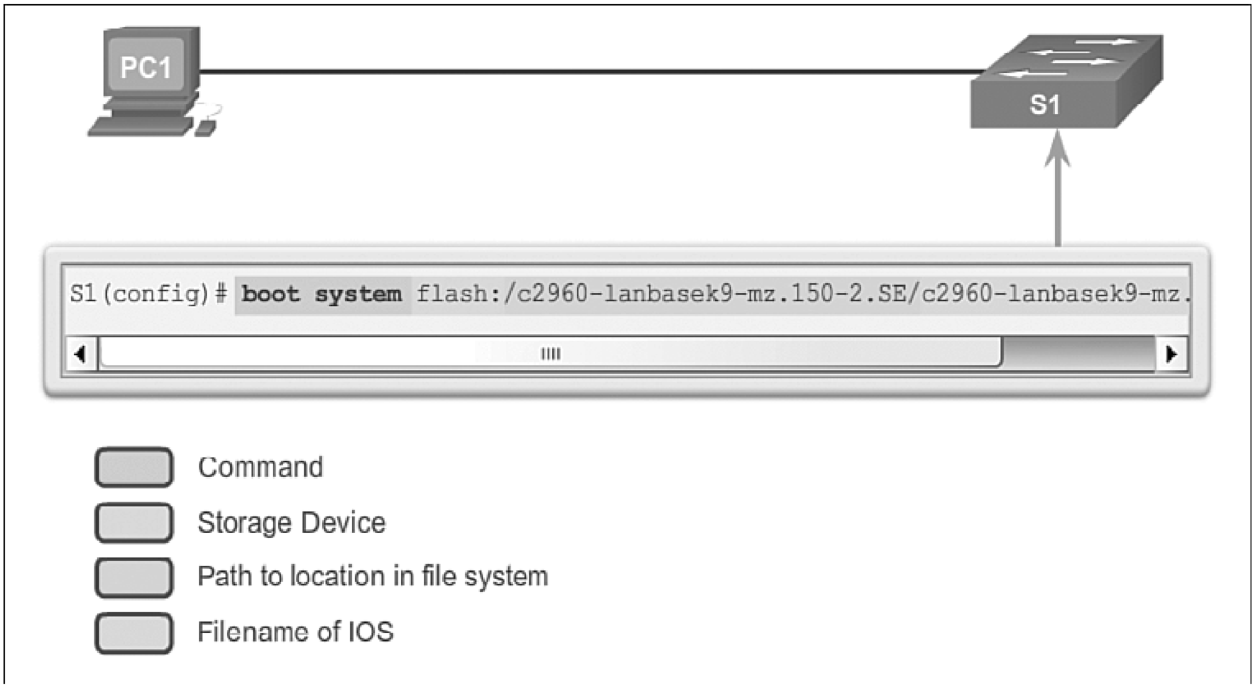
Step 4. The boot loader initializes the flash file system on the system board.

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

The boot loader finds the Cisco IOS image on the switch using the following process: The switch attempts to automatically boot by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable file it can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory. On Catalyst 2960 Series switches, the image file is normally contained in a directory that has the same name as the image file (excluding the .bin file extension).

The IOS operating system then initializes the interfaces using the Cisco IOS commands found in the configuration file, startup configuration, which is stored inNVRAM. In Figure 2-1, the BOOT environment variable is set using the **boot system** global configuration mode command. Use the **show bootvar** command (**show boot** in older IOS versions) to see the current IOS boot file version.

How To



```
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

The boot loader provides access into the switch if the operating system cannot be used because of missing or damaged system files. The boot loader has a command line that provides access to files stored in flash memory. The boot loader can be accessed through a console connection using these steps:

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

Step 2. Unplug the switch power cord.

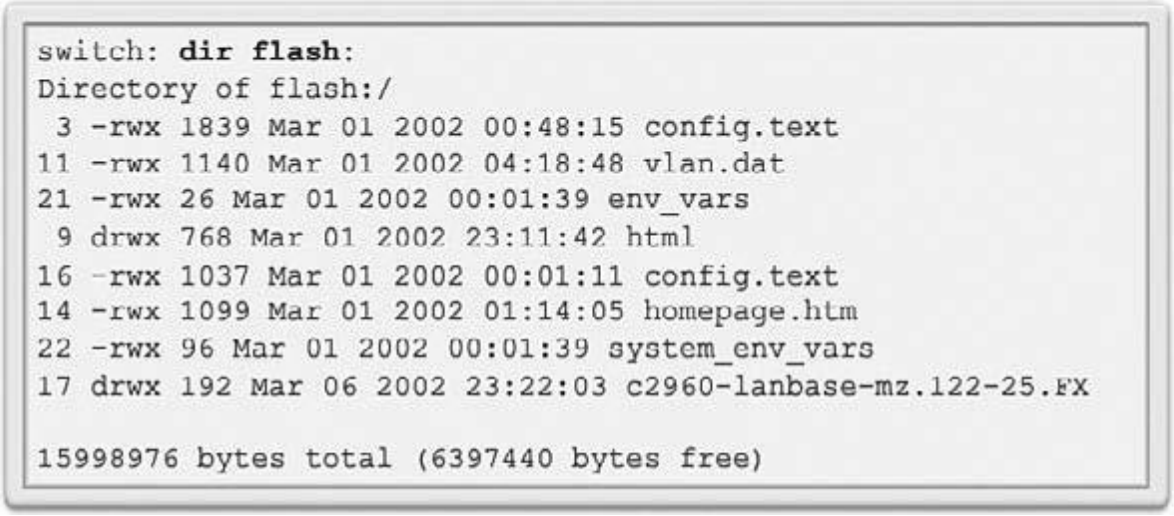
Step 3. Reconnect the power cord to the switch and within 15 seconds press and hold down the Mode button while the System LED is still flashing green.

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

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

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

How To



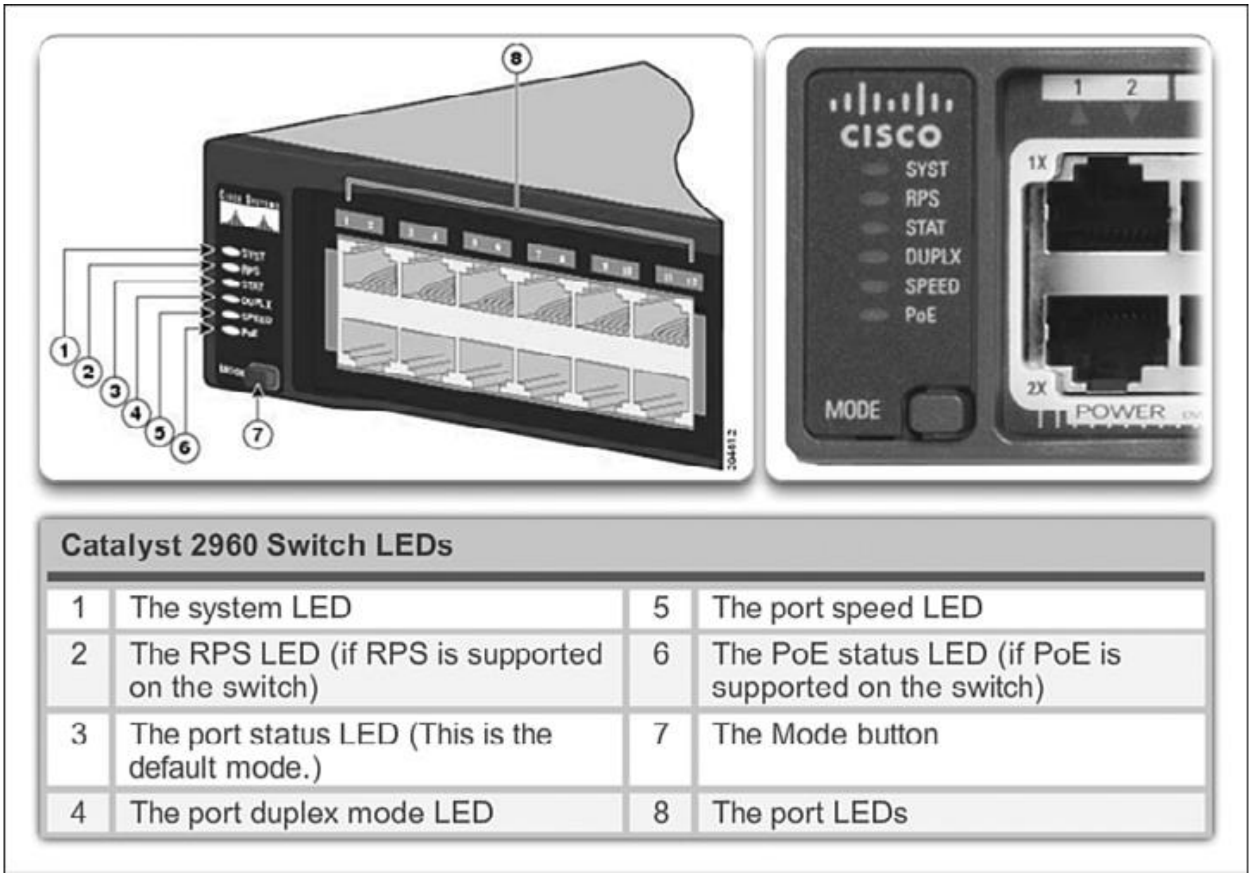
```
switch: dir flash:
Directory of flash:/
 3 -rwx 1839 Mar 01 2002 00:48:15 config.text
11 -rwx 1140 Mar 01 2002 04:18:48 vlan.dat
21 -rwx 26 Mar 01 2002 00:01:39 env_vars
 9 drwx 768 Mar 01 2002 23:11:42 html
16 -rwx 1037 Mar 01 2002 00:01:11 config.text
14 -rwx 1099 Mar 01 2002 01:14:05 homepage.htm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

15998976 bytes total (6397440 bytes free)
```

Figure 2-2 Directory Listing in Boot Loader

Switch LED Indicators

Cisco Catalyst switches have several status LED indicator lights. You can use the switch LEDs to quickly monitor switch activity and its performance. Switches of different models and feature sets will have different LEDs, and their placement on the front panel of the switch may also vary. Figure 2-3 shows the switch LEDs and the Mode button for a Cisco Catalyst 2960 switch. The Mode button is used to toggle through port status, port duplex, port speed, and PoE (if supported) status of the port LEDs.



Catalyst 2960 Switch LEDs

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

Figure 2-3 Cisco 2960 Switch LEDs

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

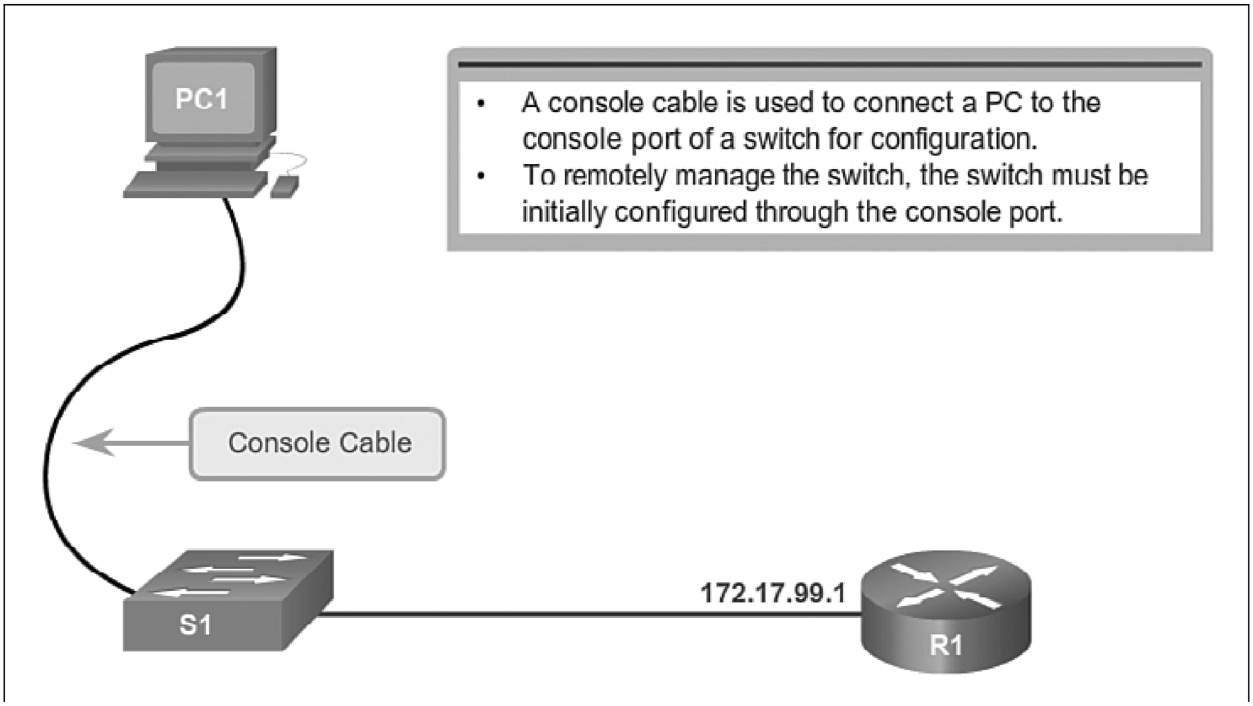
Table 2-1 Purpose of Cisco Switch LEDs

System LED	Shows whether the system is receiving power and is functioning properly. If the LED is off, it means the system is not powered. If the LED is green, the system is operating normally. If the LED is amber, the system is receiving power but is not functioning properly.
Redundant Power	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

System (RPS) LED	connected and ready to provide backup power. If the LED is blinking green, the RPS is connected but is unavailable because it is providing power to another device. If the LED is amber, the RPS is in standby mode or in a fault condition. If the LED is blinking amber, the internal power supply in the switch has failed, and the RPS is providing power.
Port Status LED	Indicates that the port status mode is selected when the LED is green. This is the default mode. When selected, the port LEDs will display colors with different meanings. If the LED is off, there is no link, or the port was administratively shut down. If the LED is green, a link is present. If the LED is blinking green, there is activity and the port is sending or receiving data. If the LED is alternating green-amber, there is a link fault. If the LED is amber, the port is blocked to ensure a loop does not exist in the forwarding domain and is not forwarding data (typically, ports will remain in this state for the first 30 seconds after being activated). If the LED is blinking amber, the port is blocked to prevent a possible loop in the forwarding domain.
Port Duplex LED	Indicates the port duplex mode is selected when the LED is green. When selected, port LEDs that are off are in half-duplex mode. If the port LED is green, the port is in full-duplex mode.
Port Speed LED	Indicates the port speed mode is selected. When selected, the port LEDs will display colors with different meanings. If the LED is off, the port is operating at 10 Mb/s. If the LED is green, the port is operating at 100 Mb/s. If the LED is blinking green, the port is operating at 1000 Mb/s.
Power over Ethernet (PoE) Mode LED	If PoE is supported, a PoE mode LED will be present. If the LED is off, it indicates the PoE mode is not selected and none of the ports have been denied power or placed in a fault condition. If the LED is blinking amber, the PoE mode is not selected but at least one of the ports has been denied power, or has a PoE fault. If the LED is green, it indicates the PoE mode is selected and the port LEDs will display colors with different meanings. If the port LED is off, PoE is off. If the port LED is green, PoE is being provided to a device. If the port LED is alternating green-amber, PoE is denied because providing power to the powered device will exceed the switch power capacity. If the LED is blinking amber, PoE is off due to a fault. If the LED is amber, PoE for the port has been disabled .

Preparing for Basic Switch Management

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



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

Figure 2-4 Preparing for Remote Switch Management

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

By default, the switch is configured to have the management of the switch controlled through VLAN 1. All ports are assigned to VLAN 1 by default. For security purposes, it is considered a best practice to use a VLAN other than VLAN 1 for the management VLAN. Furthermore, it is also a best practice to use a VLAN that is not used by end devices such as users and printers.

Note

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

Configuring Basic Switch Management Access with IPv4

Step 1. Configure the Management Interface.

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

Table 2-2 Configure the Switch Management Interface

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

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

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

Note

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

How To

Step 2. Configure the Default Gateway.

The switch should be configured with a default gateway if the switch will be managed remotely from networks not directly connected. The default gateway is the first Layer 3 device (such as a router) on the same management VLAN network to which the switch connects. The switch will forward IP packets with destination IP addresses outside the local network to the default gateway. As shown in Table 2-3 and Figure 2-5, R1 is the default gateway for S1. The interface on R1 connected to the switch has IP address 172.17.99.1. This address is the default gateway

address for S1.

Table 2-3 Commands to Configure a Switch Default Gateway

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

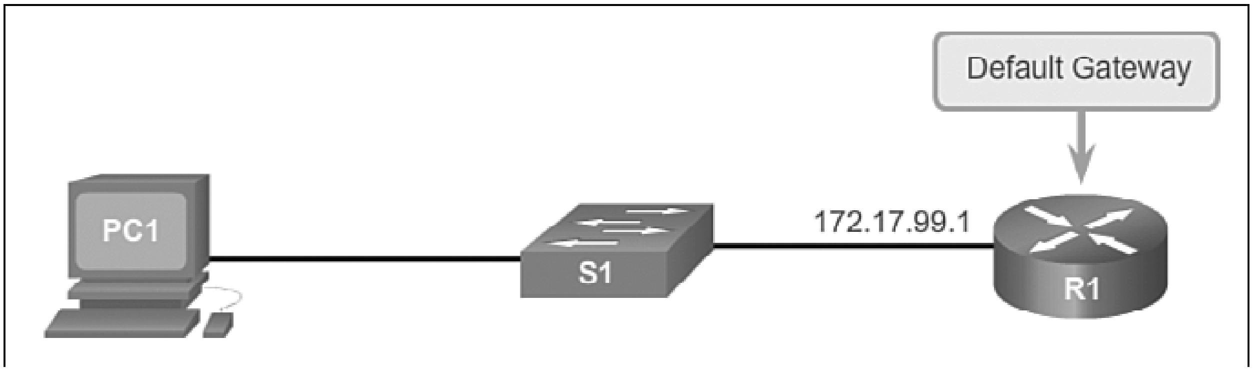
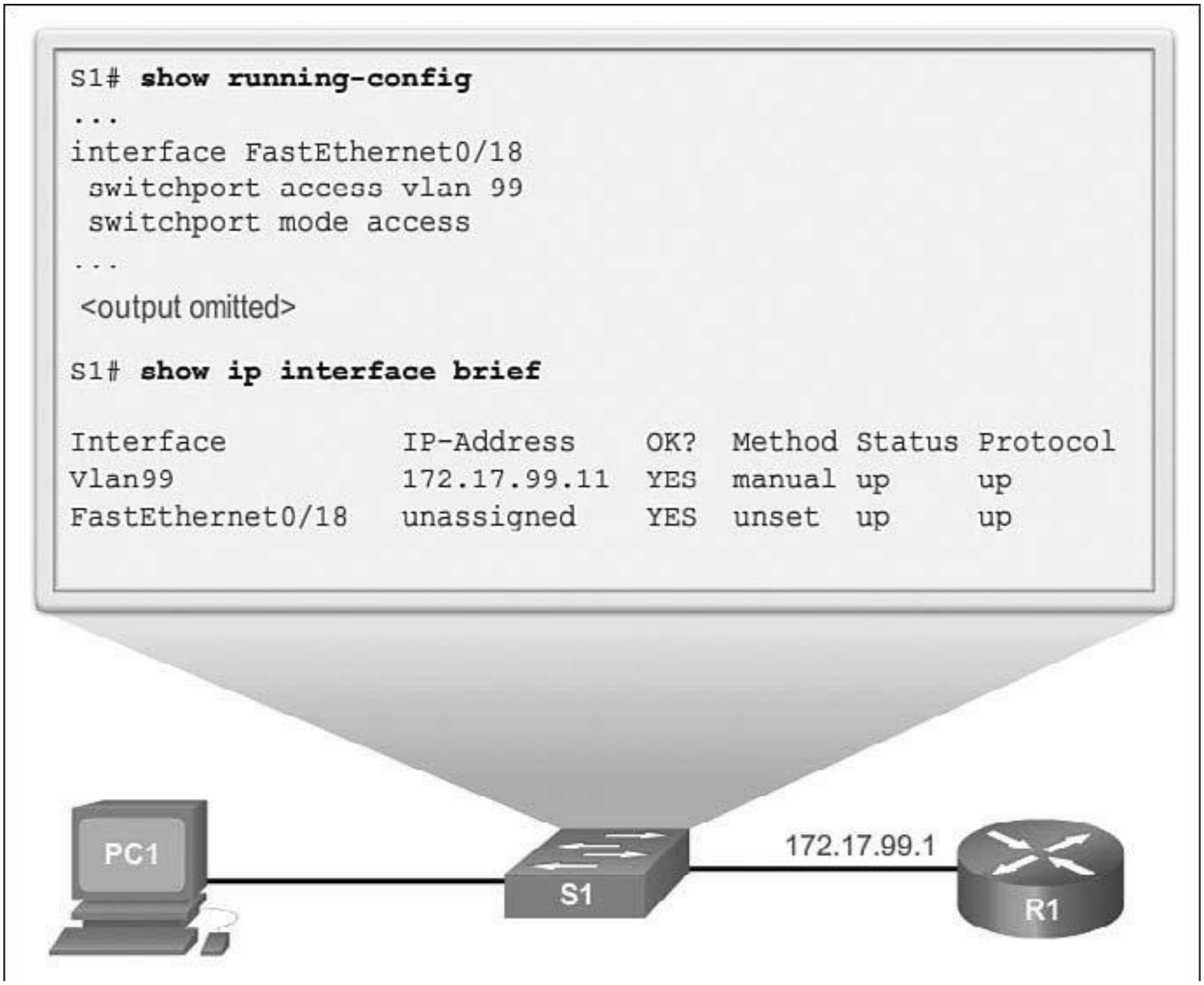


Figure 2-5 Configuring the Switch Default Gateway

To configure the default gateway for the switch, use the **ip default-gateway** command. Enter the IP address of the default gateway. The default gateway is the IP address of the router interface to which the switch connects. Use the following command to backup the configuration: **copy running-config startup-config**.

Step 3. Verify the Configuration.

As shown in Figure 2-6, the **show ip interface brief** command is useful when determining the status of both physical and virtual interfaces. The output shown in Figure 2-6 confirms that interface VLAN 99 has been configured with an IP address and a subnet mask, and that FastEthernet port Fa0/18 has been assigned to the VLAN 99 management interface. Both interfaces are now “up/up” and operational.



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

S1# show ip interface brief

Interface           IP-Address     OK?  Method Status  Protocol
vlan99              172.17.99.11   YES  manual up      up
FastEthernet0/18    unassigned     YES  unset  up      up
```

Figure 2-6 Verifying the Switch Management Interface Configuration

Configure Switch Ports

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

Duplex Communication

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

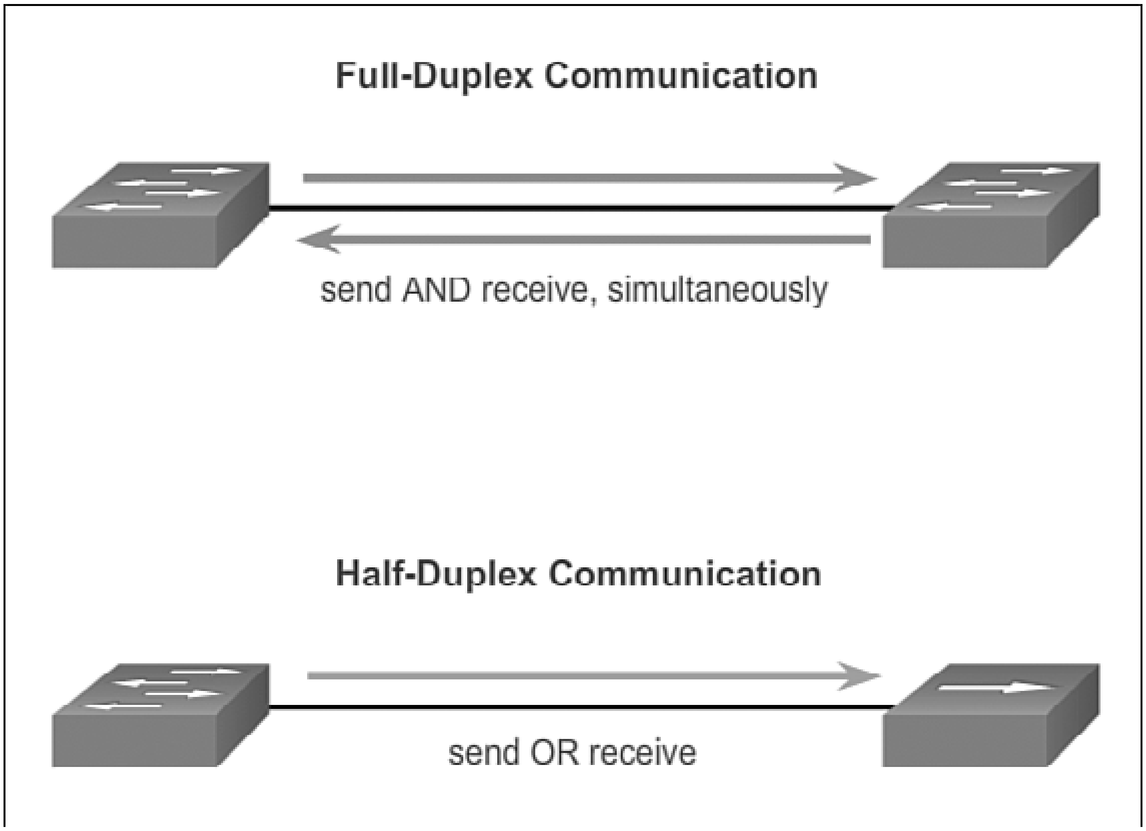

Full-Duplex Communication
send AND receive, simultaneously
Half-Duplex Communication
send OR receive

Figure 2-7 Duplex Modes

Full-duplex communication improves the performance of a switched LAN. Full-duplex communication increases effective bandwidth by allowing both ends of a connection to transmit and receive data simultaneously. This is also known as bidirectional communication. This method of optimizing network performance requires micro-segmentation. A micro-segmented LAN is created when a switch port has only one device connected and is operating at full-duplex. This results in a micro size collision domain of a single device. Because there is only one device connected, a micro-segmented LAN is collision free. Unlike full-duplex communication, half-duplex communication is unidirectional. Sending and receiving data does not occur at the same time. Half-duplex communication creates performance issues because data can flow in only one direction at a time, often resulting in collisions. Half-duplex connections are typically seen in older hardware, such as hubs. Full-duplex communication has replaced half-duplex in most hardware.

Most Ethernet and Fast Ethernet NICs sold today offer full-duplex capability. Gigabit Ethernet and 10Gb NICs require full-duplex connections to operate. In full-duplex mode, the collision detection circuit on the NIC is disabled. Frames that are sent by the two connected devices cannot collide because the devices use two separate circuits in the network cable. Full-duplex connections require a switch that supports full-duplex configuration, or a direct connection using an Ethernet cable between two devices. Standard, shared hub-based Ethernet configuration efficiency is typically rated at 50 to 60 percent of the stated bandwidth. Full-duplex offers 100 percent efficiency in both directions (transmitting and receiving). This results in a 200 percent potential use of the stated bandwidth.

Configure Switch Ports at the Physical Layer

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

Duplex and Speed

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

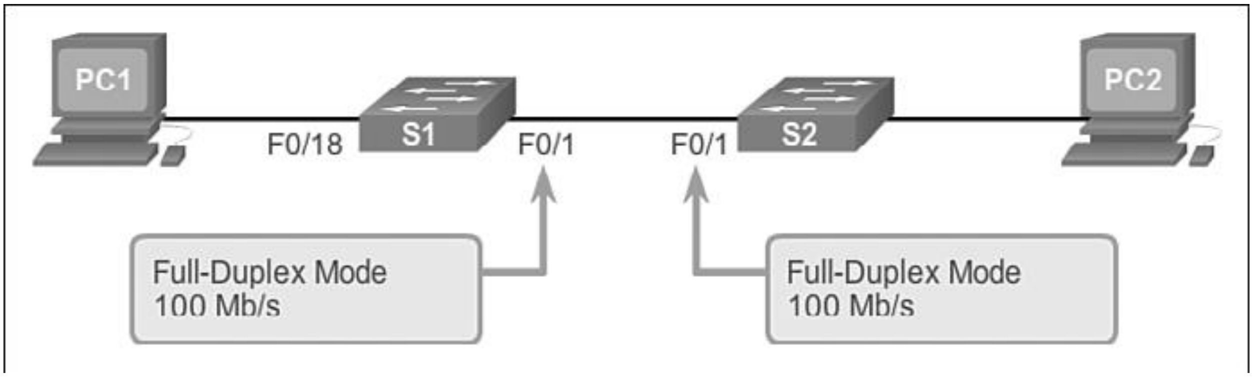


Figure 2-8 Manually Configure Duplex and Speed

Table 2-4 Cisco Switch Port Configuration

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

Save the running config to the startup config.	S1# **copy running-config startup-config**

The default setting for both duplex and speed for switch ports on Cisco Catalyst 2960 and 3560 switches is auto. The 10/100/1000 ports operate in either half- or full-duplex mode when they are set to 10 or 100 Mb/s, but when they are set to 1000 Mb/s (1 Gb/s), they operate only in full-duplex mode. When troubleshooting switch port issues, the duplex and speed settings should be checked.

Note

Mismatched settings for the duplex mode and speed of switch ports can cause connectivity issues. Auto negotiation failure creates mismatched settings. Cisco recommends using the **auto** command for duplex and manually configuring interface speed using the **speed** command in order to avoid connectivity issues between devices. All fiber optic ports, such as 100BASE-FX ports, operate only at one preset speed and are always full-duplex.

Auto-MDIX

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

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

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

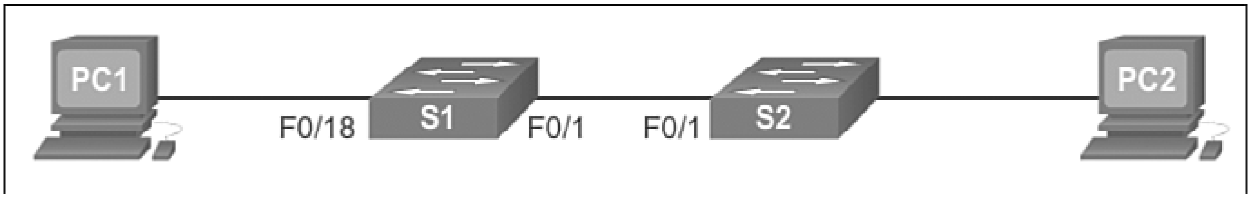


Figure 2-9 Configure Auto-MDIX

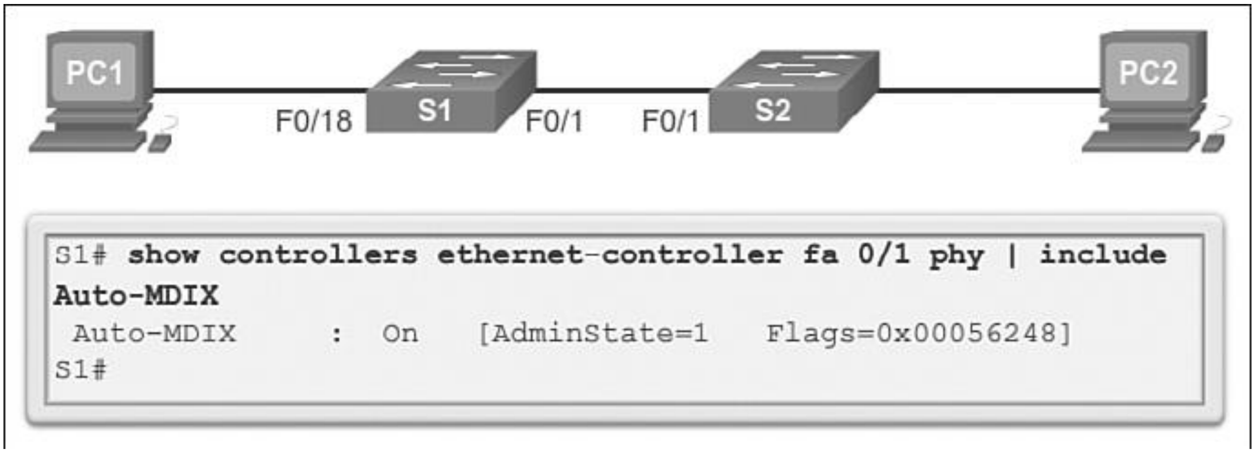
Table 2-5 Cisco Switch Auto-MDIX Commands

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

Note

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

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



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

Figure 2-10 Verify Auto-MDIX

Verifying Switch Port Configuration

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

Table 2-6 Switch Verification Commands

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

show interfaces command

- commonly used command which displays status and statistics information on the network interfaces of the switch
- frequently used when configuring and monitoring network devices.

Network Access Layer Issues

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

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

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

Table 2-7 Verify the Status of a Switch Interface

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

The first parameter (FastEthernet0/1 is up) refers to the hardware layer and, essentially, reflects whether the interface is receiving the carrier detect signal from the other end. The second parameter (line protocol is up) refers to the data link layer and reflects whether the data link layer protocol keepalives are being received. Based on the output of the **show interfaces** command, possible problems can be fixed as follows:

- If the interface is up and the line protocol is down, a problem exists. There could be an encapsulation type mismatch, the interface on the other end could be error-disabled, or there could be a hardware problem.

- If the line protocol and the interface are both down, a cable is not attached or some other interface problem exists. For example, in a back-to-back connection (a connection where the transmitter of one device connects directly to the receiver of another device without a transmission media between the two devices), one end of the connection may be administratively down.

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

Some media errors are not severe enough to cause the circuit to fail but do cause network performance issues. Table 2-8 explains some of these common errors that can be detected using the **show interfaces** command.

Table 2-8 Network Access Layer Issues

Input Errors	Total number of errors. It includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
Runts	Packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, any Ethernet pack that is less than 64 bytes is considered a runt.
Giants	Packets that are discarded because they exceed the maximum packet size for the medium. For example, any Ethernet packet that is greater than 1,518 bytes is considered a giant.
CRC errors	CRC errors are generated when the calculated checksum is not the same as the checksum received.
Output Errors	The sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined.
Collisions	The number of messages retransmitted because of an Ethernet collision.
Late Collisions	A collision that occurs after 512 bits of the frame have been transmitted.

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

- **Runt Frames:** Ethernet frames that are shorter than the 64-byte minimum allowed length are called runts. Malfunctioning NICs are the usual cause of excessive runt frames, but they can be caused by improperly or unterminated cables which can also cause excessive collisions.

- **Giants:** Ethernet frames that are longer than the maximum allowed length are called giants. Giants are caused by the same issues as those that cause runts.

- **CRC errors:** On Ethernet and serial interfaces, CRC errors usually indicate a media or cable error. Common causes include electrical interference, loose or damaged connections, or using the incorrect cabling type. If you see many CRC errors, there is too much noise on the link and you should inspect the cable for damage and length. You should also search for and eliminate noise sources, if possible.

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

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

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

Troubleshooting Network Access Layer Issues

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

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

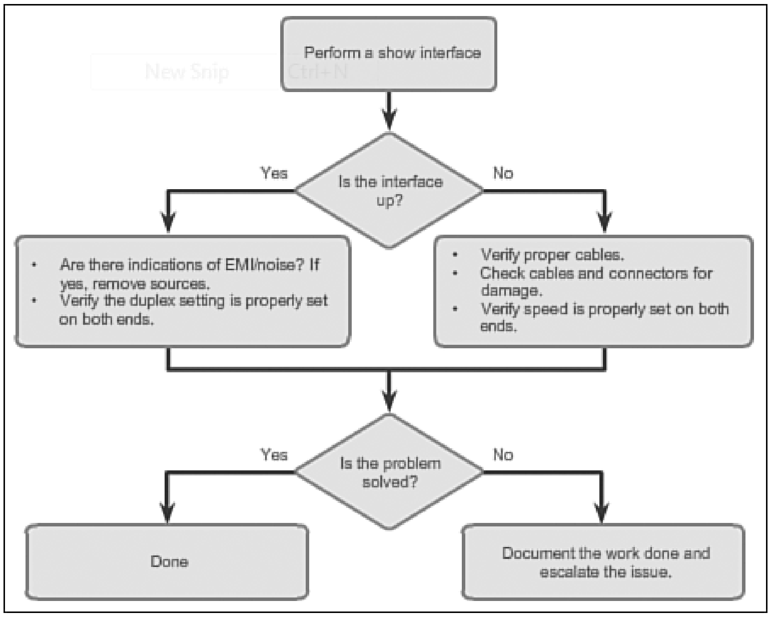

Perform a show interface
Yes
Is the interface up?
No
Are there indications of EMI/noise? If yes, remove sources.
Verify the duplex setting is properly set on both ends.
Verify proper cables.
Check cables and connectors for damage.
Verify speed is properly set on both ends.
Yes
Is the problem solved?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

Figure 2-11 Troubleshooting Switch Media Issues

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

If the interface is down:

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

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

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

- Using the **show interfaces** command, check for indications of excessive noise.

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

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

Switch Security: Management and Implementation

Learning the different methods used to secure a switch is important, the types of attacks that can be launched on, toward, or through a switch.

Secure Remote Access

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

SSH Operation

Secure Shell (SSH) is a protocol that provides a secure (encrypted) connection to a remote device. SSH should replace Telnet for management connections.

Telnet is an older protocol that uses insecure plaintext transmission of both the login authentication (username and password) and the data transmitted between the communicating devices. SSH provides security for remote connections by providing strong encryption when a device is authenticated (username and password) and also for the transmitted data between the communicating devices.

SSH is assigned to TCP port 22.

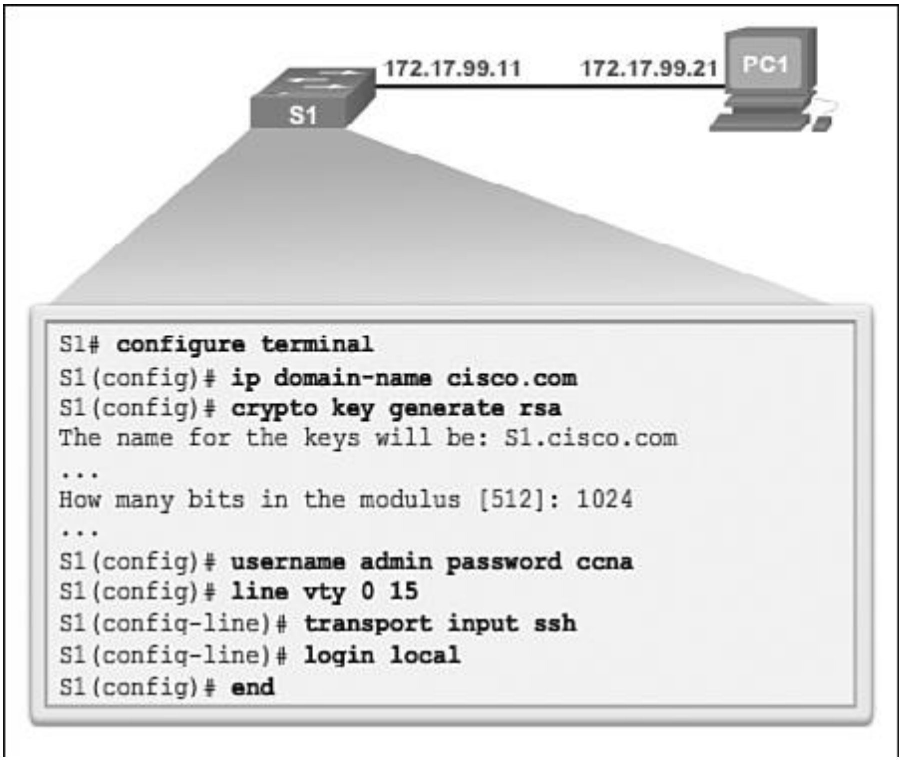
Telnet is assigned to TCP port 23.

Configuring SSH

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

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

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



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

Figure 2-12 Configure SSH for Remote Management

- **Generate RSA key pairs:** Generating an RSA key pair automatically enables SSH. Use the **crypto key generate rsa** global configuration mode command to enable the SSH server on the switch and generate an RSA key pair. When generating RSA keys, the administrator is prompted to enter a modulus length. Cisco recommends a minimum modulus size of 1024 bits (refer to the sample configuration in Figure 2-12). A longer modulus length is more secure, but it takes longer to generate and use.

Note

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

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

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

Security Concerns in LANs

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

Common Security Attacks: MAC Address Flooding

Basic switch security does not stop malicious attacks. Security is a layered process that is essentially never complete. The more aware networking professionals within an organization are regarding security attacks and the dangers they pose, the better.

MAC Address Flooding

All Catalyst switch models use a MAC address table for Layer 2 switching. The MAC address table in a switch contains the MAC addresses associated with each physical port and the associated VLAN for each port. As a frame arrives on a switchport, the source MAC address is recorded in the MAC address table. The switch then examines the received destination MAC address and looks in the MAC address table to see if it contains the destination MAC address. If an entry already exists for the destination MAC address, the switch forwards the frame to the correct port. If the destination MAC address does not exist in the MAC address table, the switch floods the frame out of every port on the switch, except the port where the frame was received.

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

In Figure 2-13, host A sends traffic to host B. The switch receives the frames and looks up the destination MAC address in its MAC address table. If the switch cannot find the destination MAC in the MAC address table, the switch then copies the frame and floods (broadcasts) it out of every switch port, except the port where it was received.

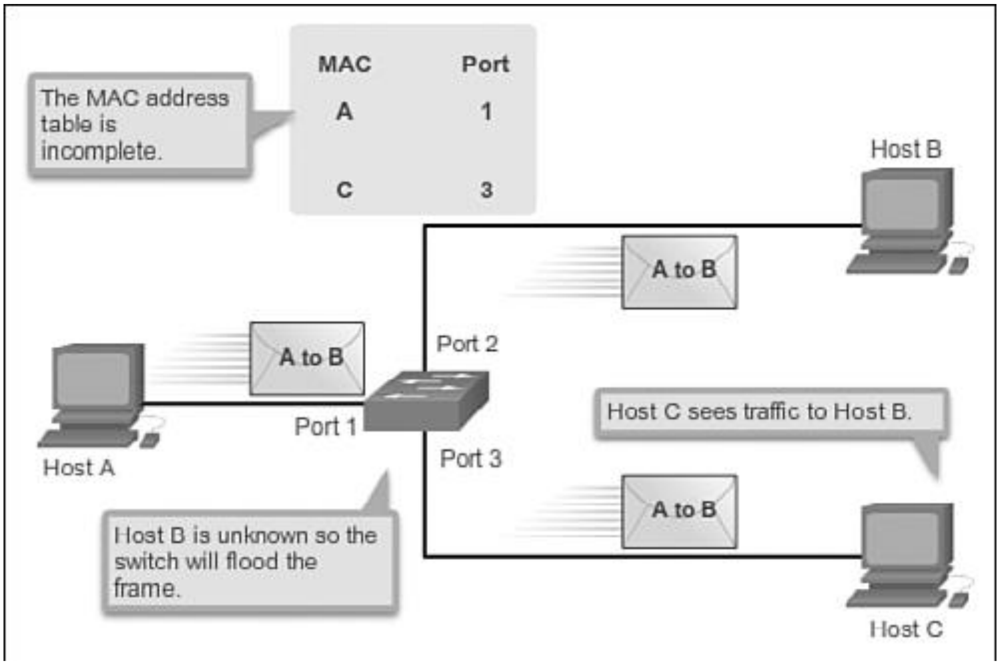

The MAC address table is incomplete.
MAC
Port
A
1
C
3
Host B
A to B
Port 2
A to B
Host C sees traffic to Host B.
Port 1
Host A
Port 3
A to B
Host B is unknown so the switch will flood the frame.
Host C

Figure 2-13 MAC Address Flooding - Switch Floods Frame for Unknown MAC

In Figure 2-14, host B receives the frame and sends a reply to host A. The switch then learns that the MAC address for host B is located on port 2 and records that information into the MAC address table.

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

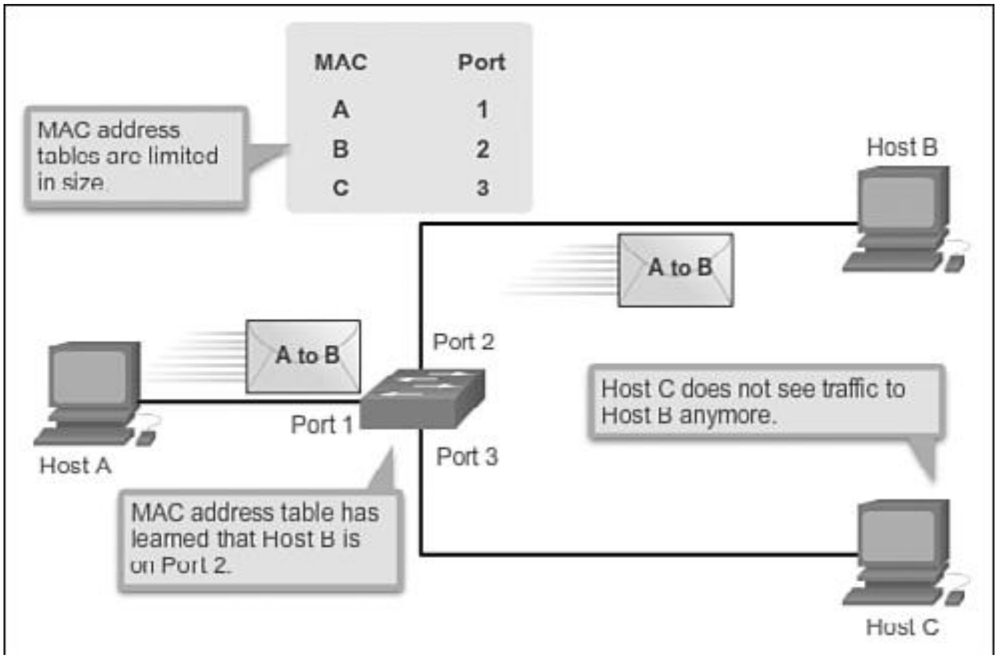

MAC
Port
A
1
B
2
C
3
MAC address tables are limited in size.
Host B
A to B
Port 2
A to B
Host C does not see traffic to Host B anymore.
Port 1
Port 3
Host A
MAC address table has learned that Host B is on Port 2.
Host C

Figure 2-14 MAC Address Flooding - Switch Records MAC Address

As shown in Figure 2-15, any frame sent by host A (or any other host) to host B is forwarded to port 2 of the switch and not broadcasted out every port.

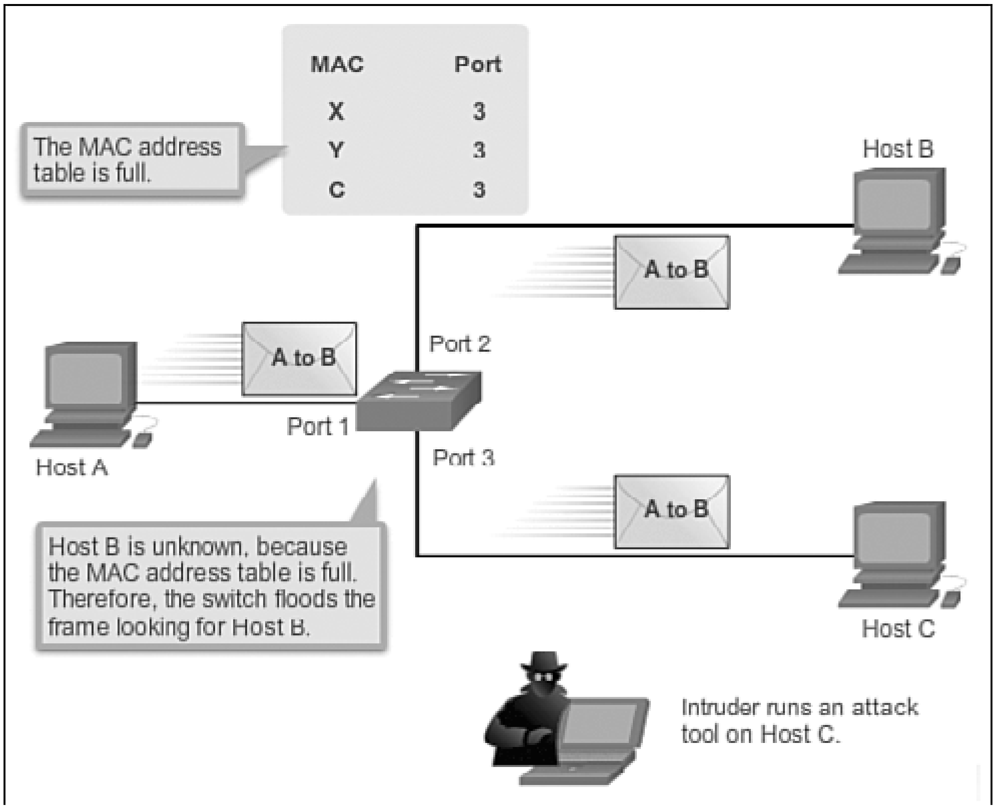

MAC
Port
X 3
Y 3
C 3
The MAC address table is full.
Host B
A to B
Port 2
A to B
Port 1
Host A
Port 3
A to B
Host B is unknown, because the MAC address table is full. Therefore, the switch floods the frame looking for Host B.
Host C
Intruder runs an attack tool on Host C.

Figure 2-15MAC Address Flooding - Switch Uses MAC Address Table to Forward

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

As shown in Figure 2-16, an attacker at host C can send frames with fake, randomly generated source and destination MAC addresses to the switch. The switch updates the MAC address table with the information in the fake frames. When the MAC address table is full of fake MAC addresses, the switch enters into what is known as fail-open mode. In this mode, the switch broadcasts all frames to all machines on the network. As a result, the attacker can see all of the frames.

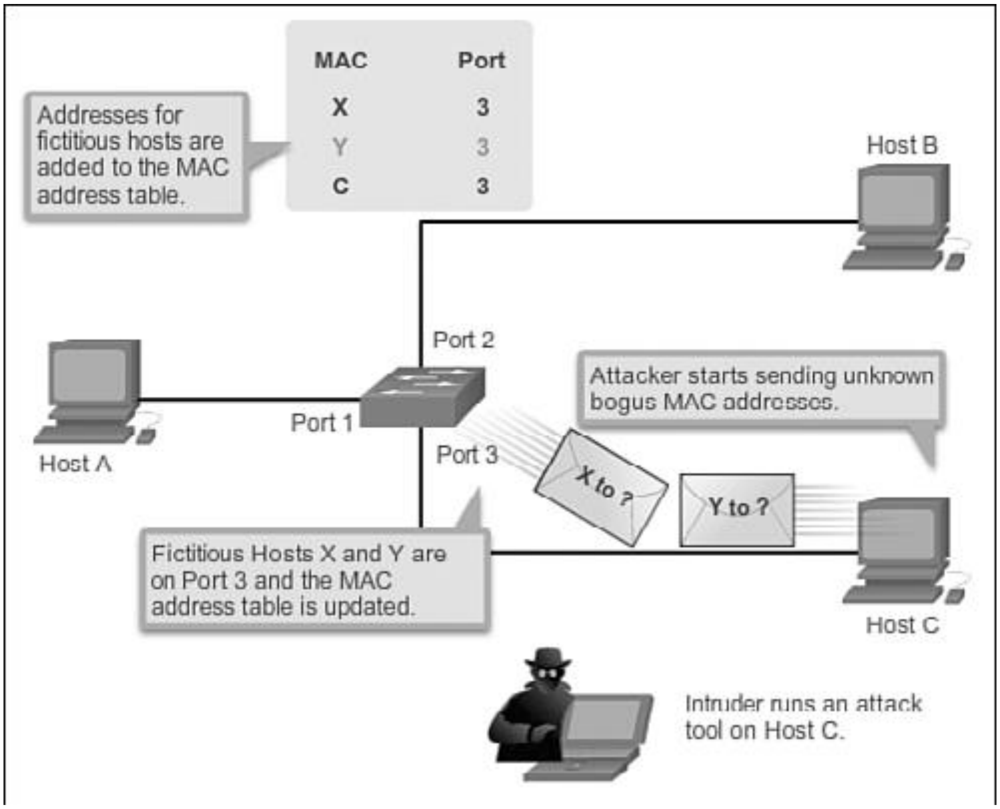

MAC
Port
X 3
Y 3
C 3
Addresses for fictitious hosts are added to the MAC address table.
Host B
Port 2
Port 1
Host A
Port 3
Attacker starts sending unknown bogus MAC addresses.
X to ?
Y to ?
Fictitious Hosts X and Y are on Port 3 and the MAC address table is updated.
Host C
Intruder runs an attack tool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

Figure 2-16MAC Address Flooding Attack - Attacker Launches Attack

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

As shown in Figure 2-17, as long as the MAC address table on the switch remains full, the switch broadcasts all received frames out of every port except the ingress port. In this example, frames sent from host A to host B are also broadcast out of port 3 on the switch and seen by the attacker at host C.

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

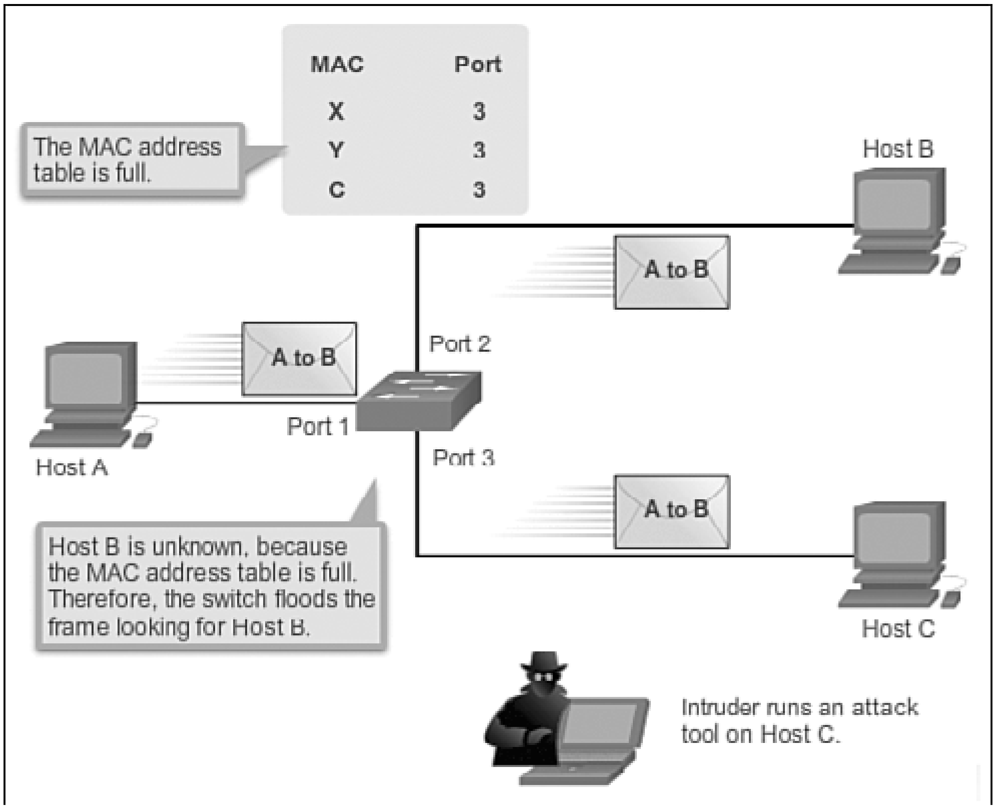

MAC
Port
X 3
Y 3
C 3
The MAC address table is full.
Host B
A to B
Port 2
A to B
Host A
Port 1
Port 3
A to B
Host B is unknown, because the MAC address table is full. Therefore, the switch floods the frame looking for Host B.
Host C
Intruder runs an attack tool on Host C.

Figure 2-17MAC Address Flooding Attack - Attacker Sees Broadcasts

Common Security Attacks: DHCP Spoofing

DHCP is the protocol that automatically assigns a host a valid IP address out of a DHCP pool. DHCP has always been the main protocol used within industry for allocating clients IP addresses. Two types of DHCP attacks can be performed against a switched network: DHCP starvation attacks and DHCP spoofing, as shown in Figure 2-21.

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

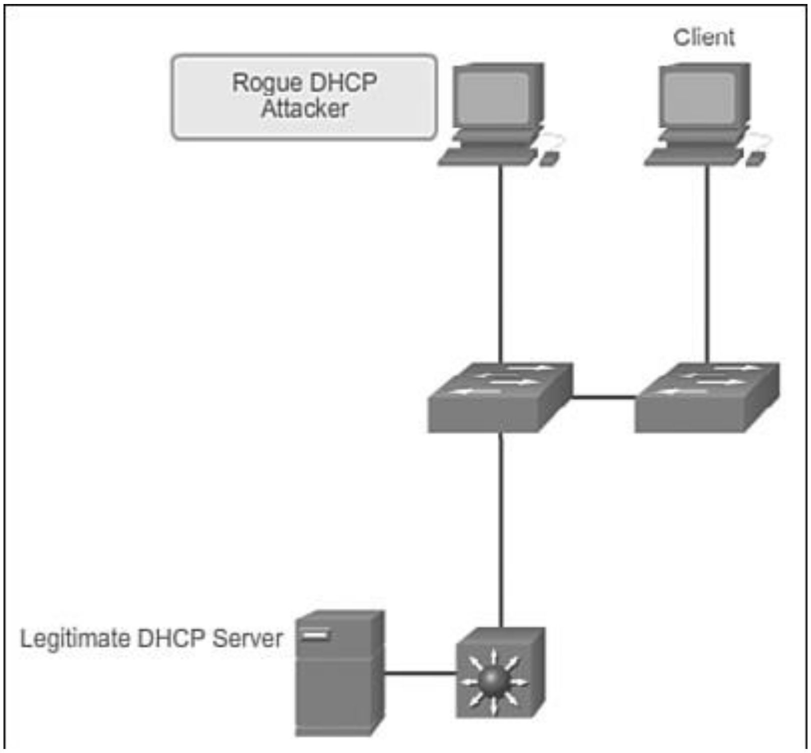


Figure 2-18 DHCP Spoofing and Starvation Attack

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

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

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

Common Security Attacks: Leveraging CDP

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

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

Telnet Attacks

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

Brute Force Password Attack

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

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

Telnet DoS Attack

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

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

Note

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

Security Best Practices

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

Best Practices

The following are best practices for securing a network:

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

Network Security Tools and Testing

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

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

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

Network Security Audits

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

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

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

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

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

Switch Port Security

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

Secure Unused Ports

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

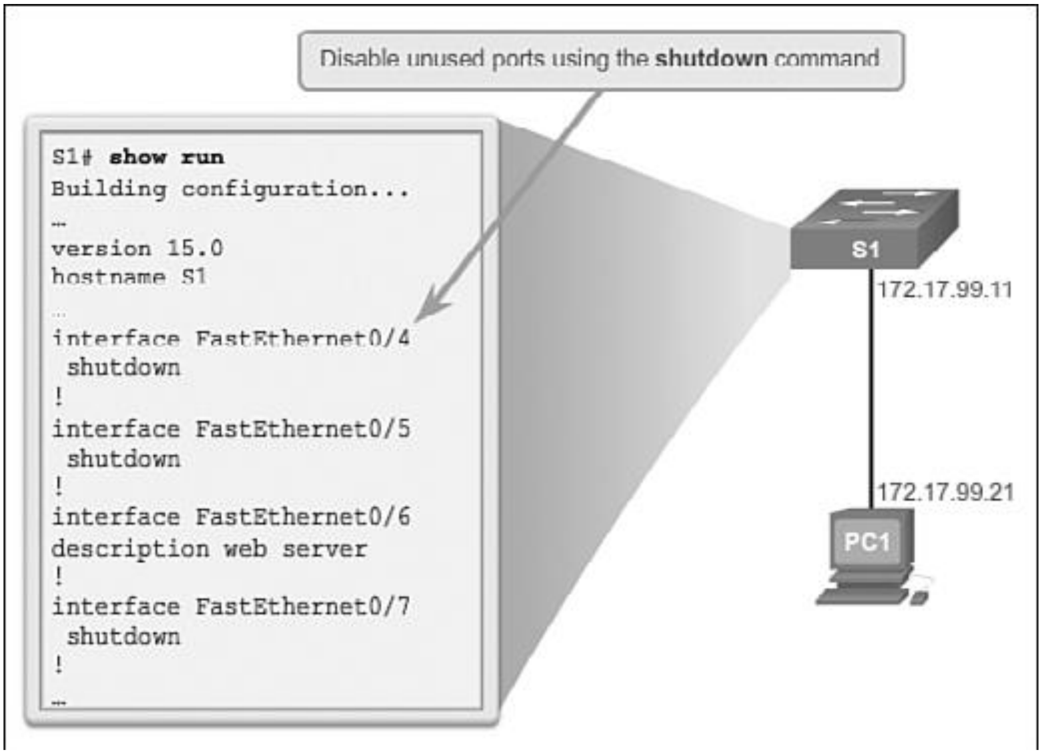
Disable Unused Ports

A simple method that many administrators use to help secure the network from unauthorized access is to disable all unused ports on a switch. For example, if a Catalyst 2960 switch has 24 ports and there are three Fast Ethernet connections in use, it is good practice to disable the 21 unused ports. Navigate to each unused port and issue the Cisco IOS **shutdown** command. If a port later on needs to be reactivated, it can be enabled with the **no shutdown** command. Figure 2-19 shows partial output for this configuration.

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

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

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



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 2-19 Disable Unused Switch Ports

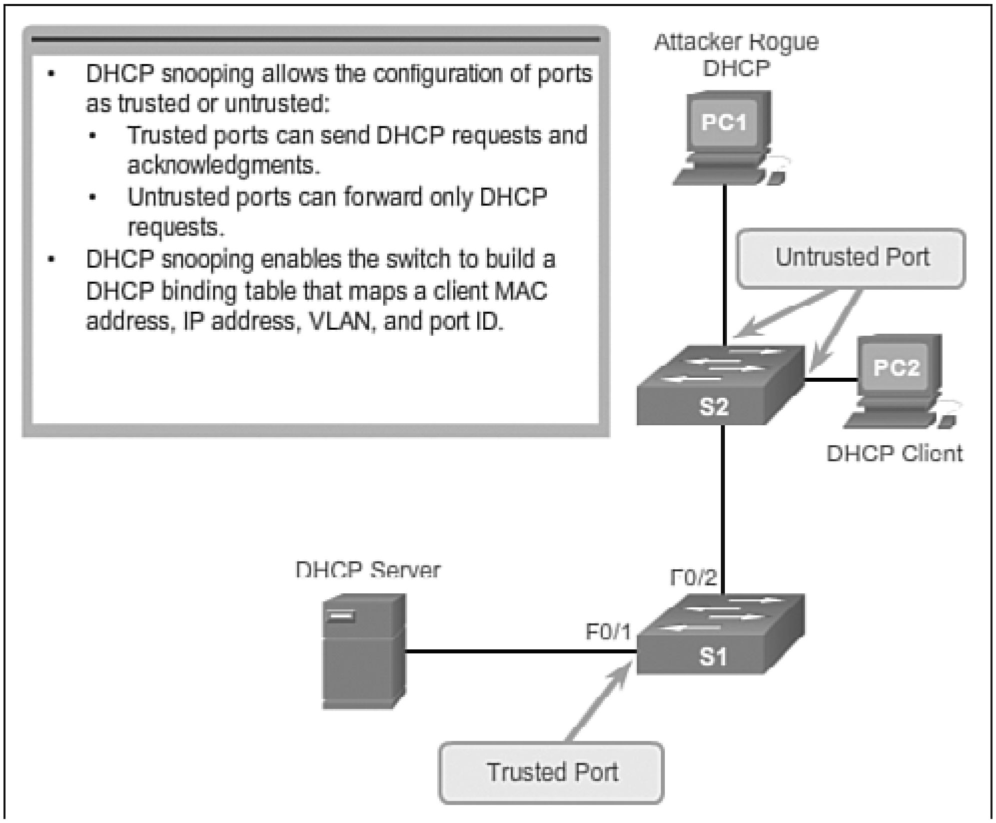
DHCP Snooping

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

As part of the DHCP configuration process, switch ports can be identified as trusted and untrusted.

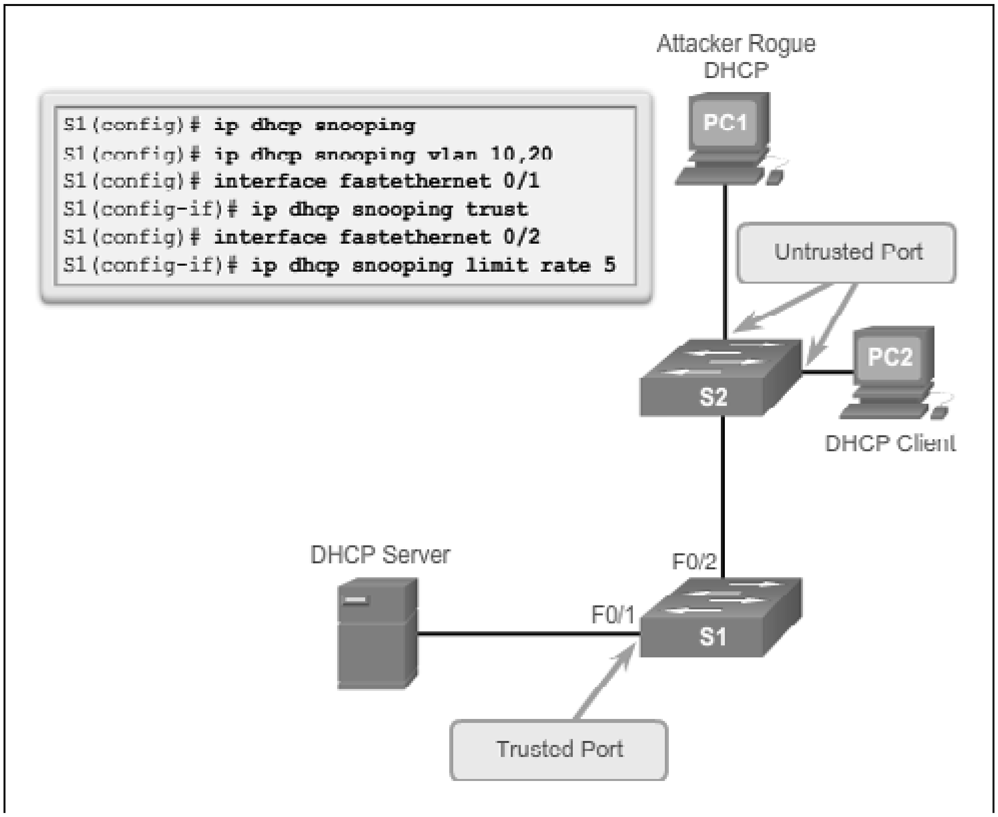
Trusted ports can source any type of DHCP message; ***untrusted ports*** can source DHCP requests only. This configuration protects the network from someone attacking a device by acting as a rogue DHCP server. Trusted ports host a DHCP server or can be an uplink toward the DHCP server. If a rogue device on an untrusted port attempts to send a DHCP response packet into the network, the port is shut down. This feature can be coupled with DHCP options in which switch information, such as the port ID of the DHCP request, can be inserted into the DHCP request packet.

As shown in Figures 2-20 and 2-21, untrusted ports are those not explicitly configured as trusted. A DHCP binding table is built for untrusted ports. Each entry contains a client MAC address, IP address, lease time, binding type, VLAN number, and port ID recorded as clients make DHCP requests. The table is then used to filter subsequent DHCP traffic. From a DHCP snooping perspective, untrusted access ports should not send any DHCP server responses.



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

Figure 2-20DHCP Snooping Operation



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

Figure 2-21DHCP Snooping Configuration

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

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

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

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

Optional Limit the rate at which an attacker can continually send bogus DHCP

Step 4. requests through untrusted ports to the DHCP server using the **ip dhcp snooping limit rate** *rate* command.

Port Security: Operation

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

Port Security

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

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

Note

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

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

Secure MAC Address Types

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

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

- ***Dynamic secure MAC addresses:*** MAC addresses that are dynamically learned and stored only in the address table. MAC addresses configured in this way are removed when the switch restarts.

- ***Sticky secure MAC addresses:*** MAC addresses that can be dynamically learned or manually configured stored in the address table, and added to the running configuration.

Sticky Secure MAC addresses

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

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

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

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

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

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

Note

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

- Learned dynamically, converted to sticky secure MAC addresses stored in the running-config.
- Removed from the running-config if port security is disabled.
- Lost when the switch reboots (power cycled).
- Saving sticky secure MAC addresses in the startup-config makes them permanent, and the switch retains them after a reboot.
- Disabling sticky learning converts sticky MAC addresses to dynamic secure addresses and removes them from the running-config.

Port Security: Violation Modes

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

- The maximum number of secure MAC addresses have been added to the address table for that interface, and a station whose MAC address is not in the address table attempts to access the interface.

- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

An interface can be configured for one of three violation modes, specifying the action to be taken if a violation occurs. Table 2-9 presents which kinds of data traffic are forwarded when one of the following security violation modes are configured on a port:

- **Protect:** When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed or the number of maximum allowable addresses is increased. There is no notification that a security violation has occurred.

- **Restrict:** When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed or the number of maximum allowable addresses is increased. In this mode, there is a notification that a security violation has occurred.

- **Shutdown:** In this (default) violation mode, a port security violation causes the interface to immediately become error-disabled and turns off the port LED. It increments the violation counter. When a secure port is in the error-disabled state, it can be brought out of this state by entering the **shutdown** and **no shutdown** interface configuration mode commands.

Security violations occur in these situations:

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

Table 2-9 Security Violations Modes

Violation Mode	**Forwards Traffic**	**Sends Syslog Message**	**Displays Error Message**	**Increases Violation Counter**	**Shuts Down Port**
Protect	No	No	No	No	No

Restrict	No	Yes	No	Yes	No
Shutdown	No	No	No	Yes	Yes

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

Port Security: Configuring

Table 2-10 summarizes the default port security configuration on a Cisco Catalyst switch.

Table 2-10 Port Security Default Settings

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

Figure 2-22 shows the topology used when configuring F0/18 on the S1 switch. Table 2-11 shows the Cisco IOS CLI commands needed to configure port security on the Fast Ethernet F0/18 port on the S1 switch. Notice that the example does not specify a violation mode. In this example, the violation mode is the default mode of shutdown.

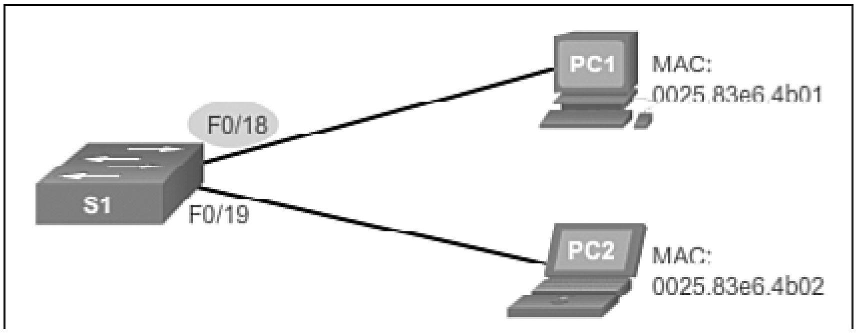


Figure 2-22 Port Security Configuration Topology

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

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

Table 2-12 shows the commands needed to enable sticky secure MAC addresses for

port security on Fast Ethernet port 0/19 of switch S1. As stated earlier, a specific maximum number of secure MAC addresses can be manually configured. In this example, the Cisco IOS command syntax is used to set the maximum number of MAC addresses to 50 for port 0/19. The violation mode is set to the default mode of shutdown.

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

Specify the interface to be configuredfor port security.	S1(config)# **interface fastethernet 0/19**
Set the interface mode to access.	S1(config-if)# **switchport mode access**
Enable port security on the interface.	S1(config-if)# **switchport port-security**
Set the maximum number of secure addresses allowed on the port.	S1(config-if)# **switchport port-security maximum 50**
Enable sticky learning.	S1(config-if)# **switchport port-security mac-address sticky**

Port Security: Verifying

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

Verify Port Security

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

Verify Port Security Settings

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

```
S1# show port-security interface fastethernet 0/18

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

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

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

Note

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

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

```
S1# show run | begin FastEthernet 0/19
        interface FastEthernet0/19
        switchport mode access
        switchport port-security

        switchport port-security maximum 50
        switchport port-security mac-address sticky
        switchport port-security sticky 0025.83e6.4b02
```

Verify Secure MAC Addresses

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

S1# **show port-security address**

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age(mins)
1	0025.83e6.4b01	SecureDynamic	Fa0/18	-
1	0025.83e6.4b02	SecureSticky	Fa0/19	-

Ports in Error Disabled State

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

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state

Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.

Sep 20 06:44:53.973: %LINEPROTO-5-PPDOWN: Line protocol on
Interface FastEthernet0/18, changed state to down

Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to down
```

Note

Notice in the output how the port protocol and link status changed to down. Another indication that a port security violation has occurred is that the switch port LED will change to orange. The **show interfaces** command identifies the port status as err-disabled as shown in the following output. The output of the **show port-security interface** command now shows the port status as secure-shutdown.

Because the port security violation mode is set to shutdown, the port with the security violation goes to the error disabled state.

```
S1# show interfaces fastethernet 0/18 status
```

Port	Name	Status	Vlan Duplex	Speed	Type
Fa0/18	err-disabled	1	auto	auto	10/100BaseTX

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

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

```
S1(config)# interface FastEthernet 0/18
S1(config-if)# shutdown

Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface
FastEthernet0/18, changed state to administratively down
S1(config-if)# no shutdown
```

```
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to up

Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/18, changed state to up
```

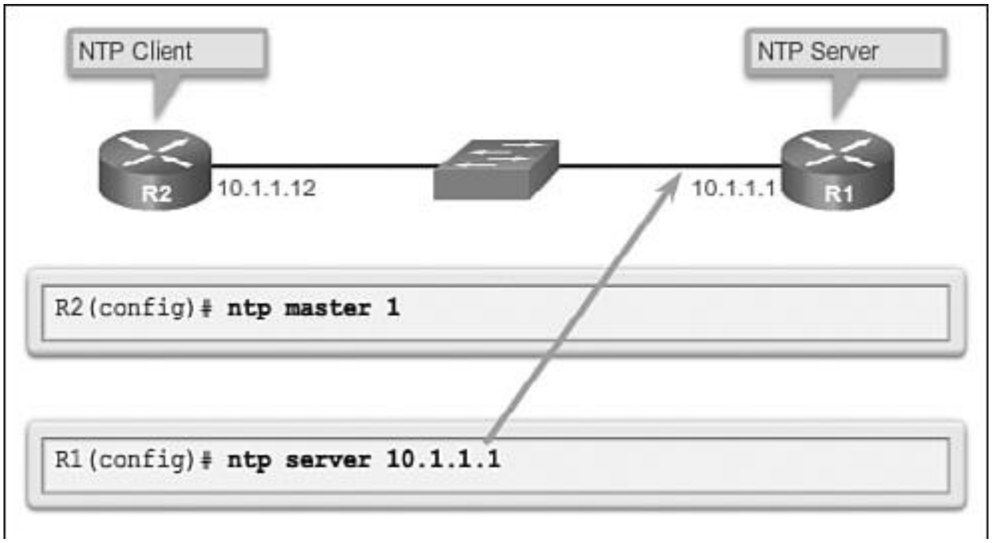
Network Time Protocol (NTP)

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 2-23. Router R2 is configured as an NTP client, while router R1 serves as an authoritative NTP server.



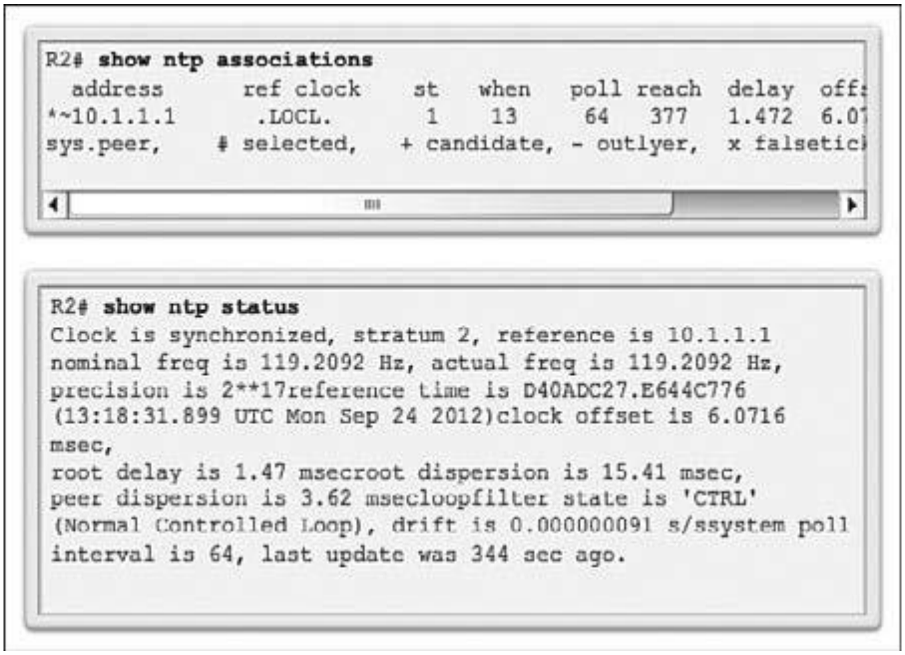
```
R2(config)# ntp master 1
```

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

Figure 2-23 Configuring NTP

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

Figure 2-24 displays the verification of NTP. To display the status of NTP associations, use the **show ntp associations** command in privileged EXEC mode. This command will indicate the IP address of any peer devices that are synchronized to this peer, statically configured peers, and stratum number. The **show ntp status** user EXEC command can be used to display such information as the NTP synchronization status, the peer that the device is synchronized to, and in which NTP strata the device is functioning.



```
R2# show ntp associations
  address        ref clock     st    when    poll reach   delay   off
*~10.1.1.1        .LOCL.        1     13      64    377   1.472   6.0
sys.peer,     # selected,    + candidate, - outlyer,   x falsetic
```

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

Figure 2-24 Verifying NTP