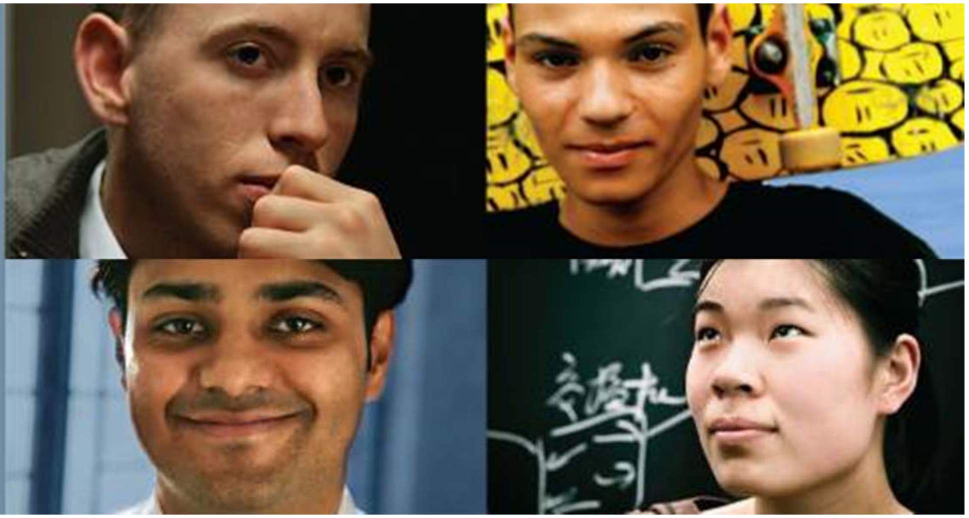
Chapter 2: Introduction to Switched Networks



Routing and Switching

Cisco | Networking Academy®
Mind Wide Open™

Chapter 2

2.0 Introduction

2.1 Basic Switch Configuration

2.2 Switch Security: Management and Implementation

Chapter 2: Objectives

Upon completion of this chapter, you will be able to:

- Explain the advantages and disadvantages of static routing.
- Configure initial settings on a Cisco switch.
- Configure switch ports to meet network requirements.
- Configure the management switch virtual interface.
- Describe basic security attacks in a switched environment.
- Describe security best practices in a switched environment.
- Configure the port security feature to restrict network access.

Basic Switch Configuration

Switch Boot Sequence

1. Power-on self test (POST).
2. Run boot loader software.
3. Boot loader performs low-level CPU initialization.
4. Boot loader initializes the flash file system
5. Boot loader locates and loads a default IOS operating system software image into memory and passes control of the switch over to the IOS.

Basic Switch Configuration

Switch Boot Sequence (cont.)

To find a suitable Cisco IOS image, the switch goes through the following steps:

Step 1. It attempts to automatically boot by using information in the BOOT environment variable.

Step 2. If this variable is not set, the switch performs a top-to-bottom search through the flash file system. It loads and executes the first executable file, if it can.

Step 3. The IOS software then initializes the interfaces using the Cisco IOS commands found in the configuration file and startup configuration, which is stored in NVRAM.

Note: The **`boot system`** command can be used to set the BOOT environment variable.

Basic Switch Configuration

Recovering from a System Crash

- The boot loader can also be used to manage the switch if the IOS cannot be loaded.
- The boot loader can be accessed through a console connection by:
  1. Connecting a PC by console cable to the switch console port. Unplug the switch power cord.
  2. Reconnecting the power cord to the switch and press and hold the **Mode** button.
  3. The System LED turns briefly amber and then solid green. Release the **Mode** button.
- The boot loader **`switch:prompt`** appears in the terminal emulation software on the PC.

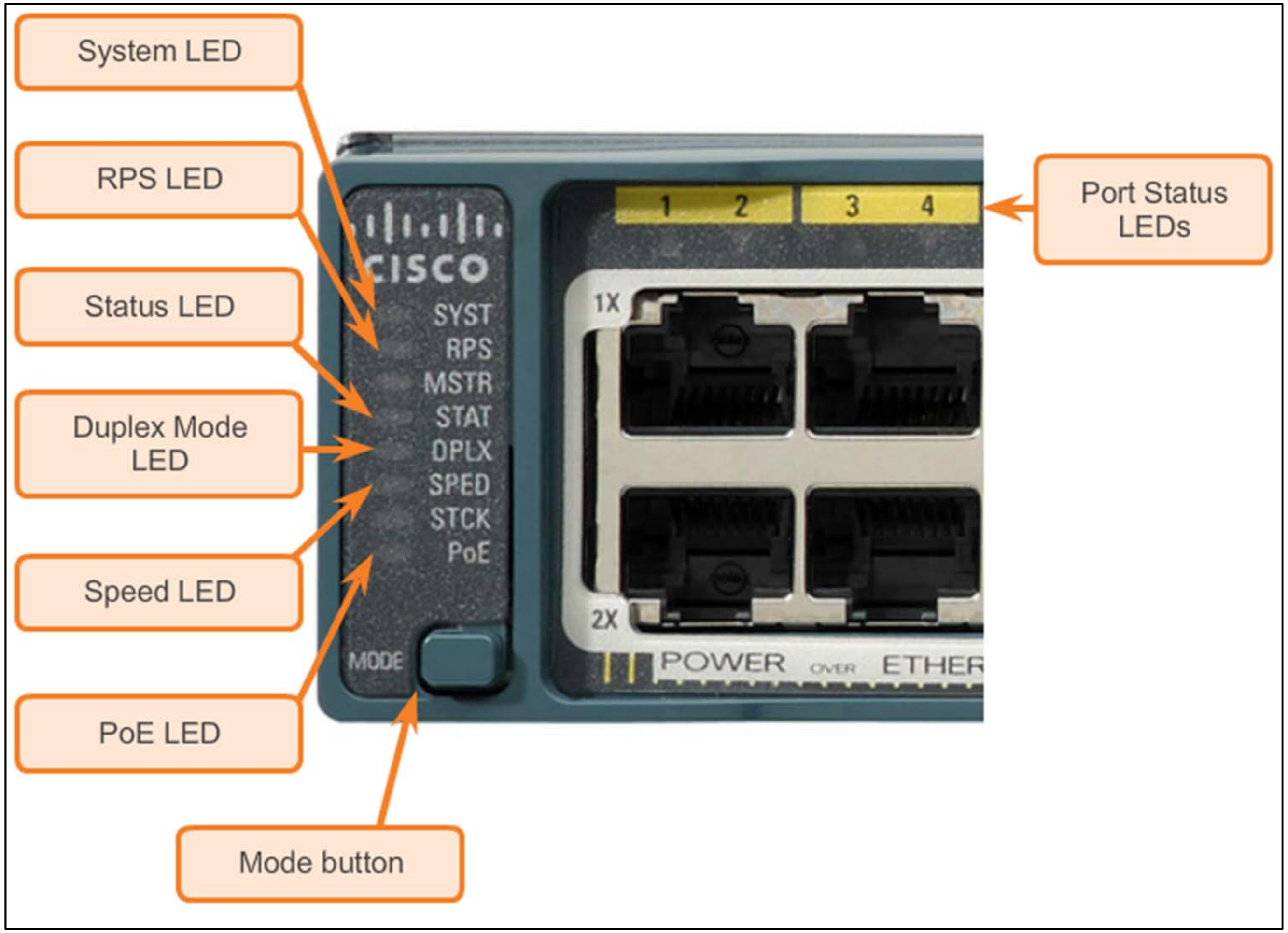
Basic Switch Configuration

Switch LED Indicators

- Each port on Cisco Catalyst switches have status LED indicator lights.
- By default, these LED lights reflect port activity, but they can also provide other information about the switch through the **Mode** button.
- The following modes are available on Cisco Catalyst 2960 switches:
  - System LED
  - Redundant Power System (RPS) LED
  - Port Status LED
  - Port Duplex LED
  - Port Speed LED
  - Power over Ethernet (PoE) Mode LED

Basic Switch Configuration

Cisco Catalyst 2960 Switch Modes



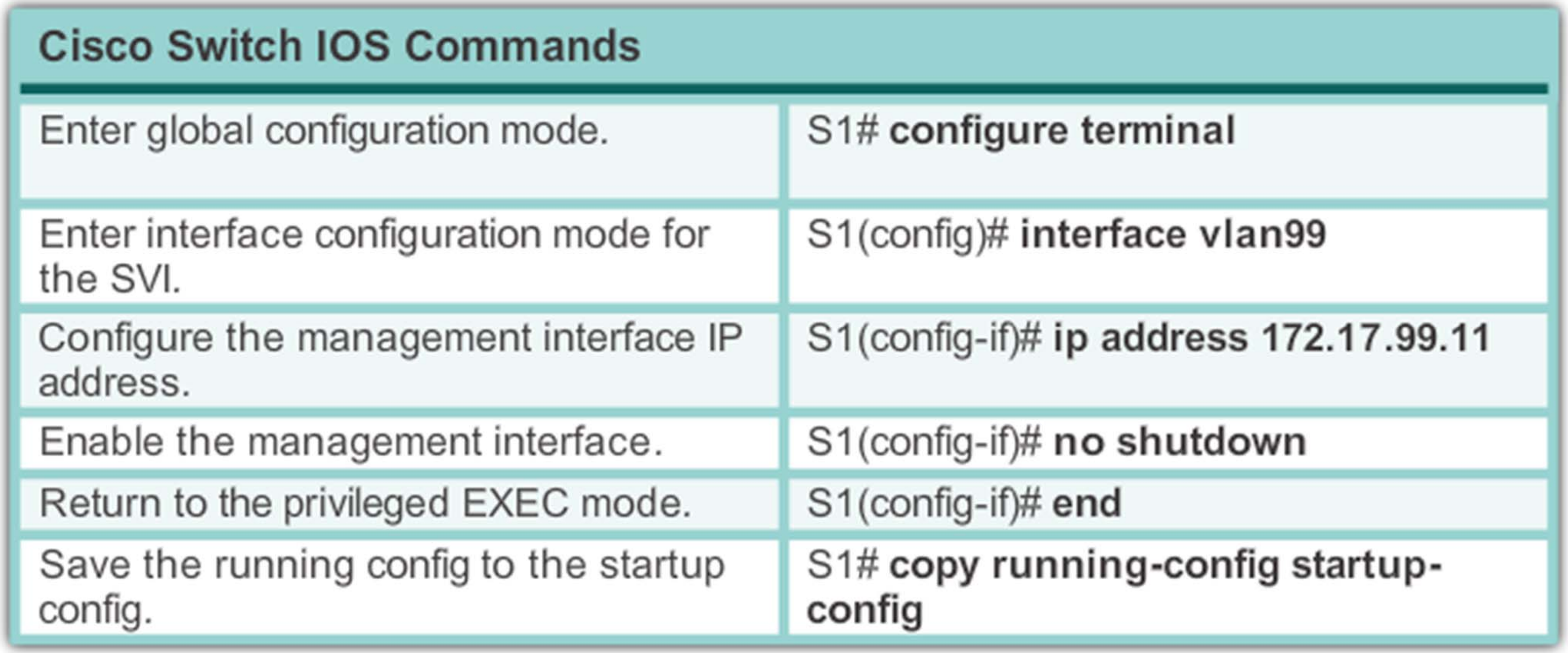
Basic Switch Configuration

Preparing for Basic Switch Management

- To remotely manage a Cisco switch, it must be configured to access the network.
- An IP address and a subnet mask must be configured.
- If managing the switch from a remote network, a default gateway must also be configured.
- The IP information (address, subnet mask, gateway) is to be assigned to a switch switch virtual interface (SVI).
- Although these IP settings allow remote management and remote access to the switch, they do not allow the switch to route Layer 3 packets.

Basic Switch Configuration

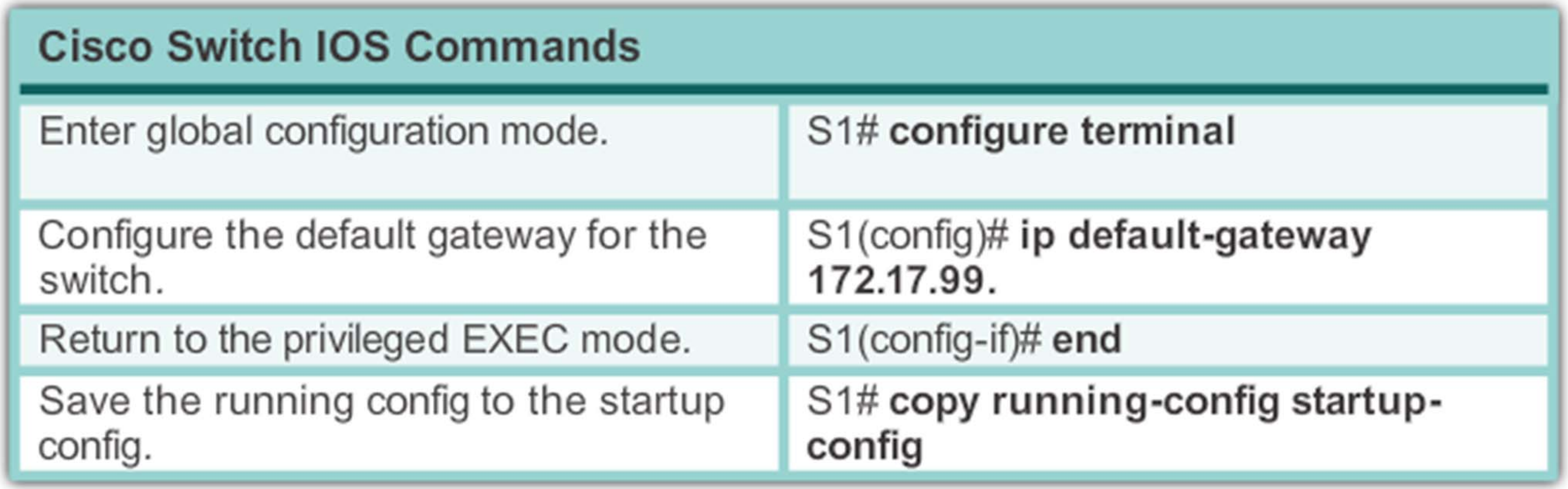
Preparing for Basic Switch Management (cont.)



Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode for the SVI.	S1(config)# **interface vlan99**
Configure the management interface IP address.	S1(config-if)# **ip address 172.17.99.11**
Enable the management interface.	S1(config-if)# **no shutdown**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

Basic Switch Configuration

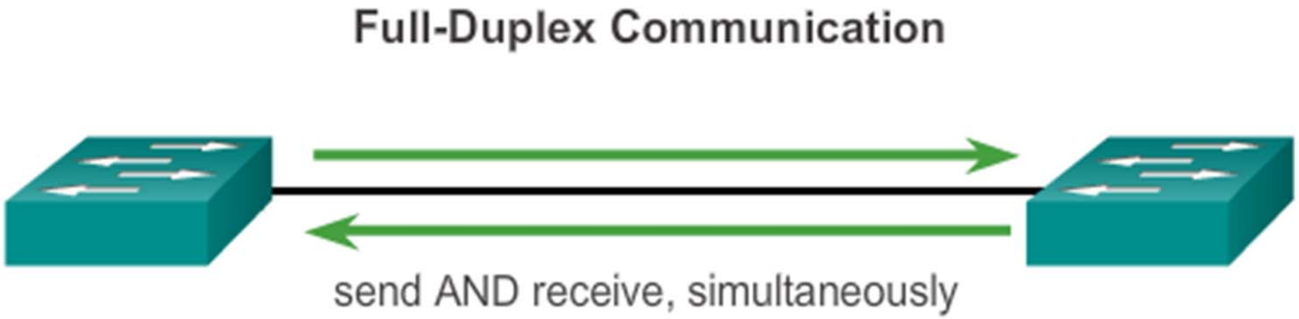
Preparing for Basic Switch Management (cont.)

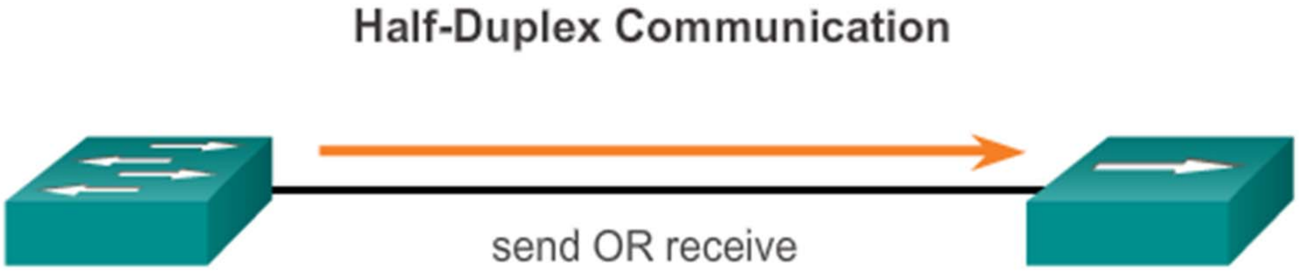


Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Configure the default gateway for the switch.	S1(config)# **ip default-gateway 172.17.99.**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

Configuring Switch Ports

Duplex Communication

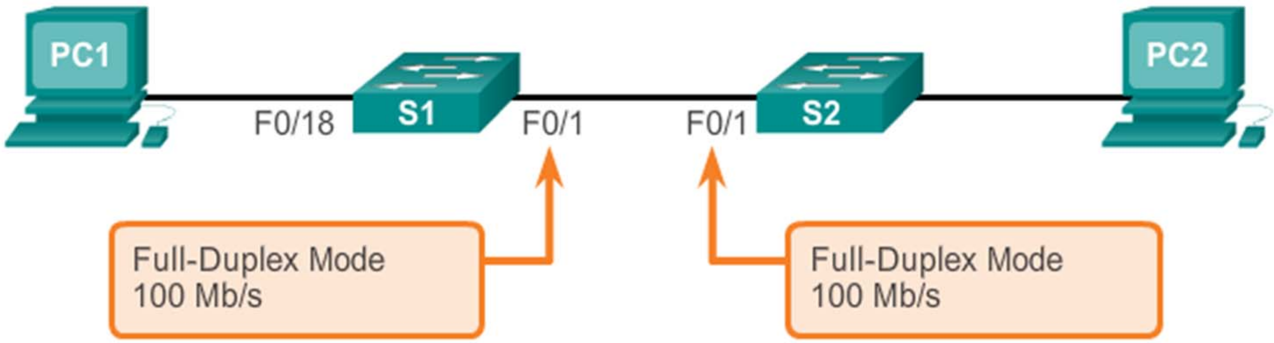


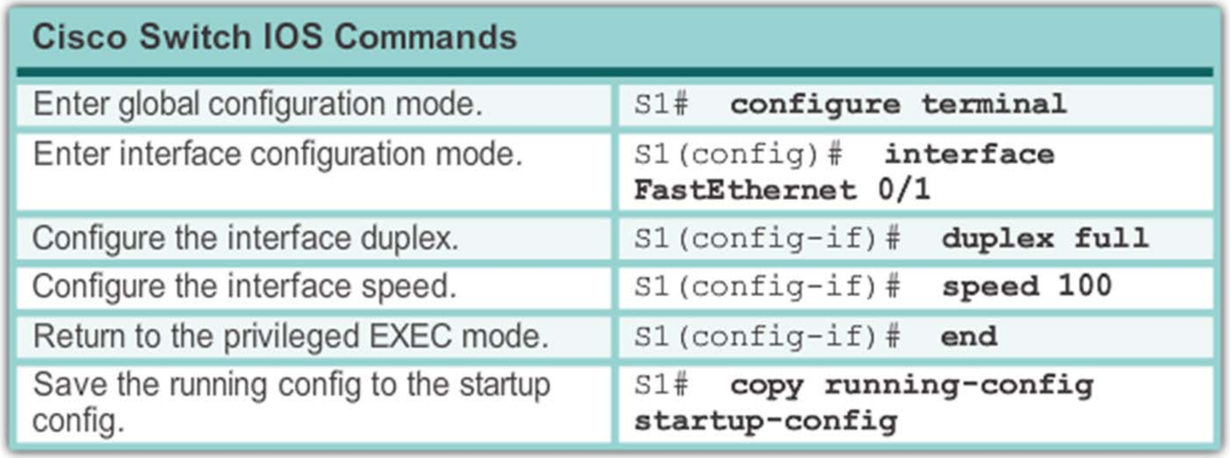


Configuring Switch Ports

Configuring Switch Ports at the Physical Layer

Configure Duplex and Speed





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`

Configuring Switch Ports

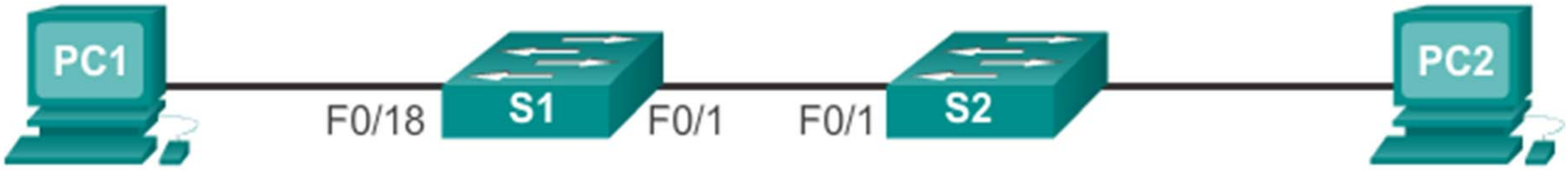
Auto-MDIX Feature

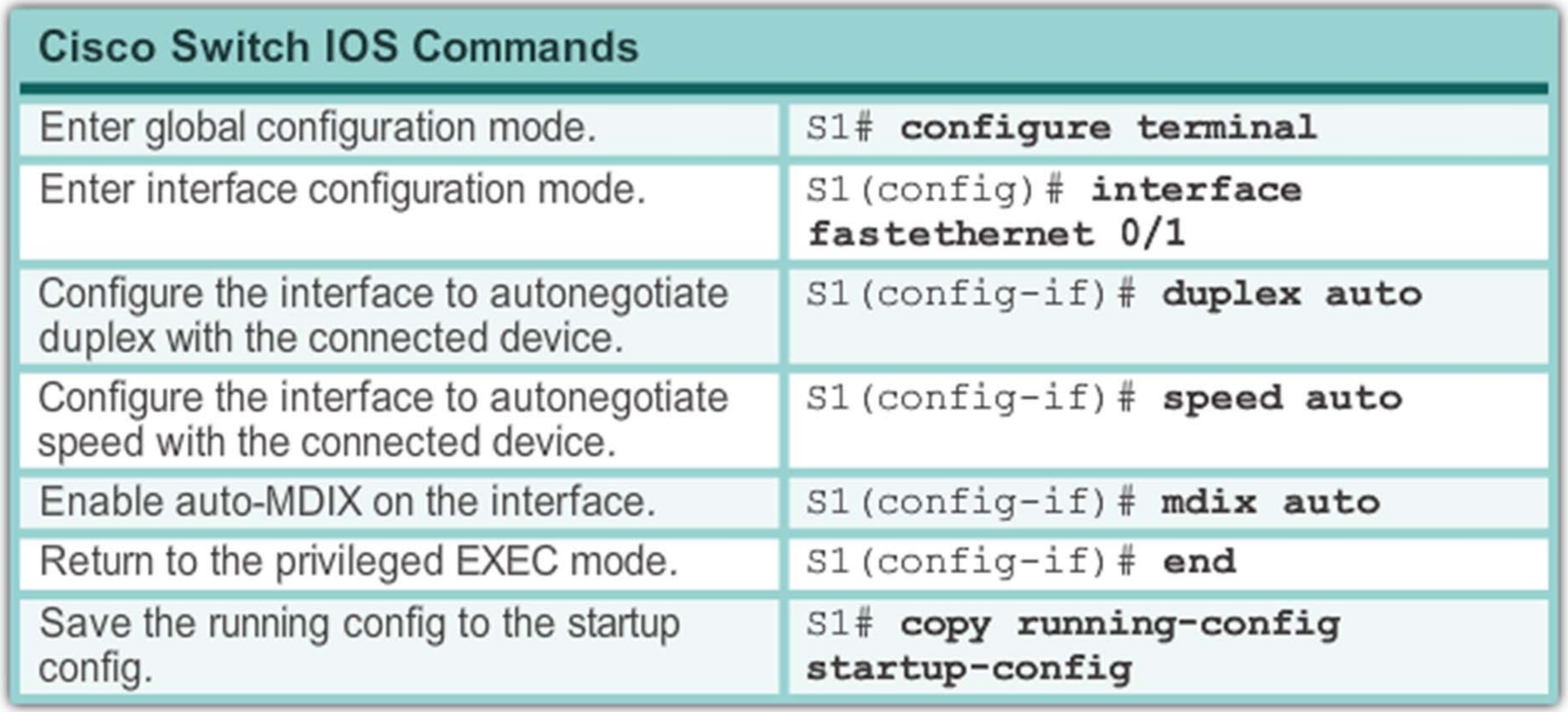
- Certain cable types (straight-through or crossover) were historically required when connecting devices.
- The automatic medium-dependent interface crossover (auto-MDIX) feature eliminates this problem.
- When auto-MDIX is enabled, the interface automatically detects and appropriately configures the connection.
- When using auto-MDIX on an interface, the interface speed and duplex must be set to **auto**.

Configuring Switch Ports

Auto-MDIX Feature (cont.)

Configure auto-MDIX



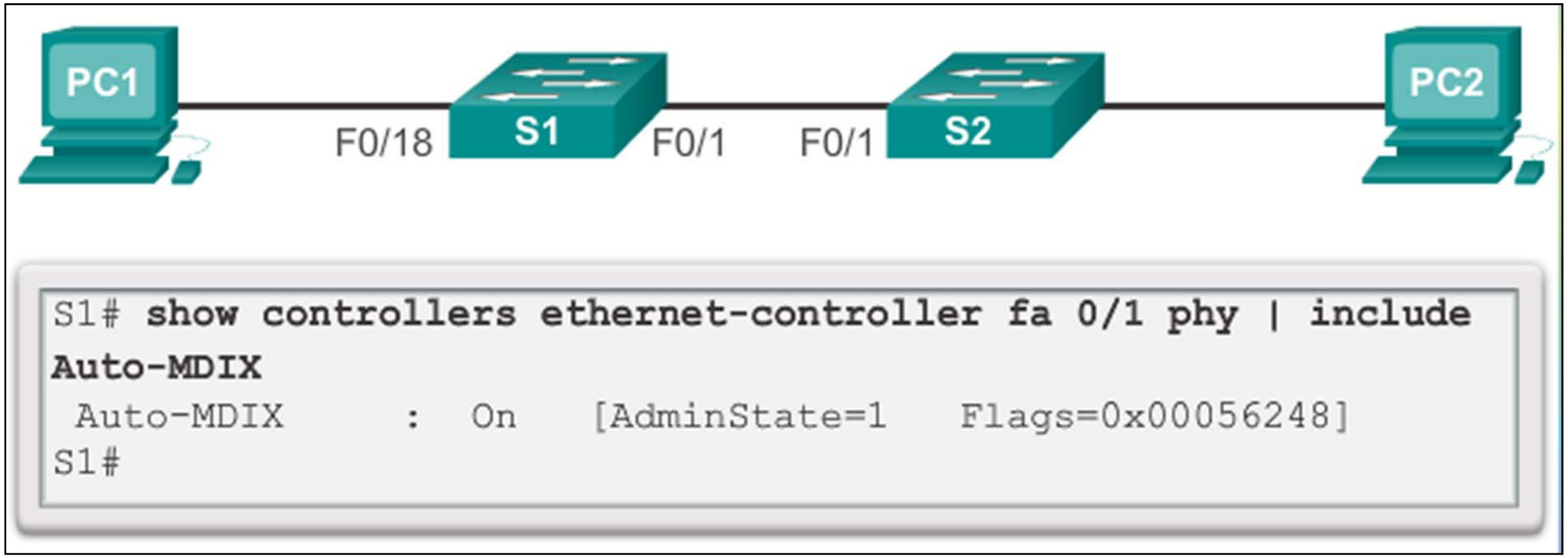


Cisco Switch IOS Commands

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`

Configuring Switch Ports

Auto-MDIX Feature (cont.)

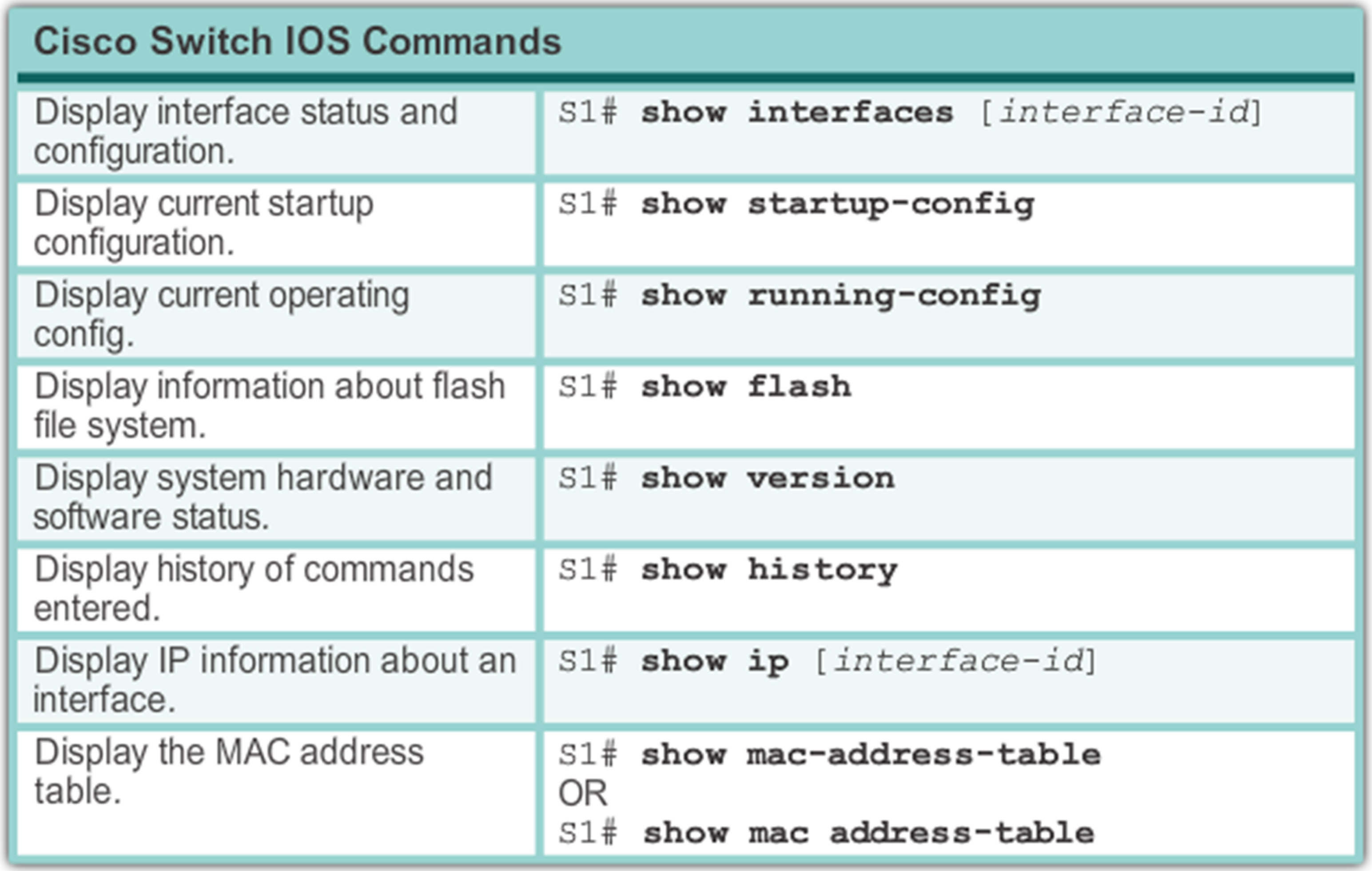


```
S1# show controllers ethernet-controller fa 0/1 phy | include
Auto-MDIX
 Auto-MDIX      :   On    [AdminState=1    Flags=0x00056248]
S1#
```

Configuring Switch Ports

Verifying Switch Port Configuration

Verification Commands



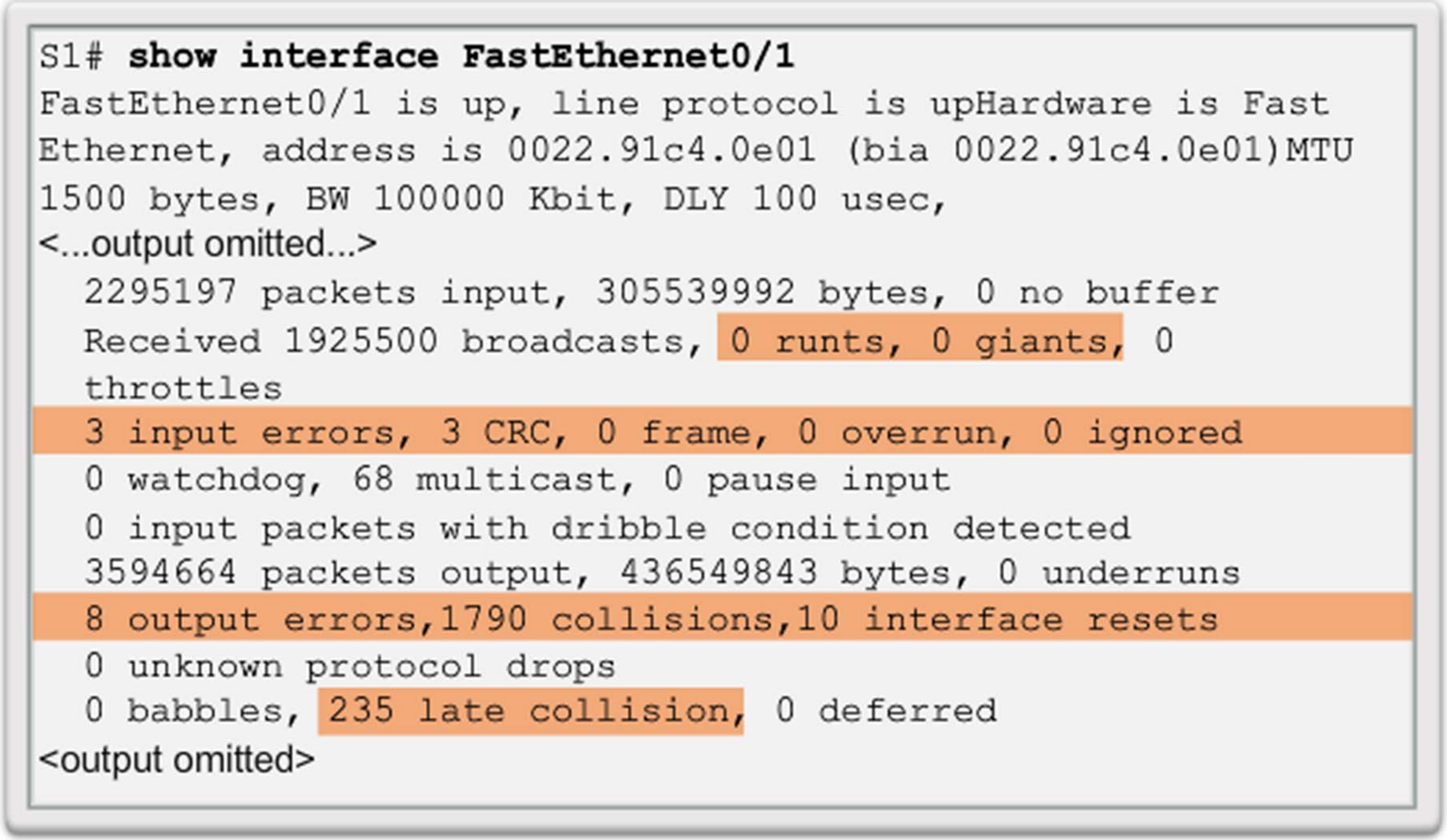
Cisco Switch IOS Commands	
Display interface status and configuration.	`S1# show interfaces [interface-id]`
Display current startup configuration.	`S1# show startup-config`
Display current operating config.	`S1# show running-config`
Display information about flash file system.	`S1# show flash`
Display 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`
	OR
	`S1# show mac address-table`

Configuring Switch Ports

Network Access Layer Issues

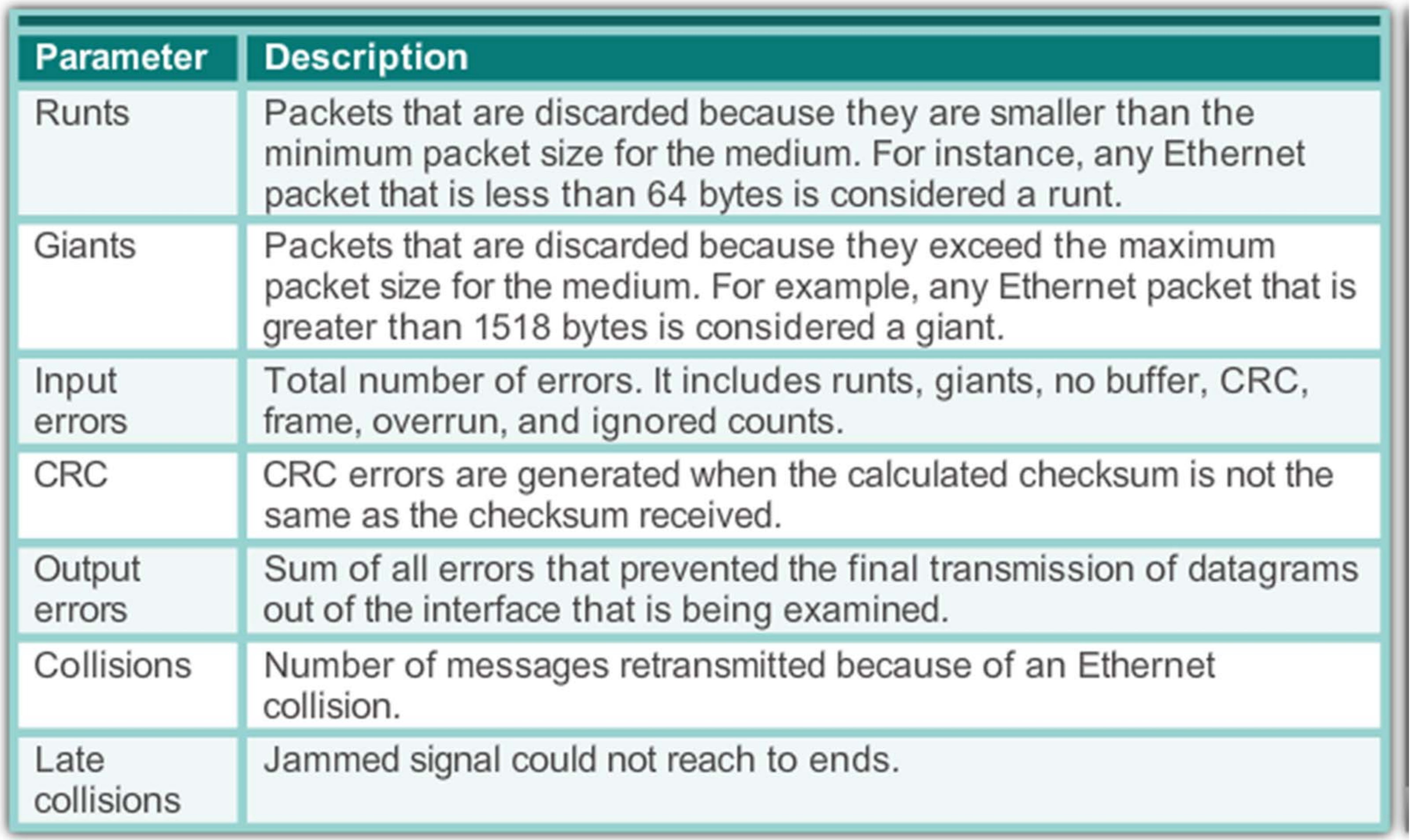
Display interface status and statistics.



```
S1# show interface FastEthernet0/1
FastEthernet0/1 is up, line protocol is upHardware is Fast
Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)MTU
1500 bytes, BW 100000 Kbit, DLY 100 usec,
<...output omitted...>
   2295197 packets input, 305539992 bytes, 0 no buffer
   Received 1925500 broadcasts, 0 runts, 0 giants, 0
   throttles
   3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 68 multicast, 0 pause input
   0 input packets with dribble condition detected
   3594664 packets output, 436549843 bytes, 0 underruns
   8 output errors,1790 collisions,10 interface resets
   0 unknown protocol drops
   0 babbles, 235 late collision, 0 deferred
<output omitted>
```

Configuring Switch Ports

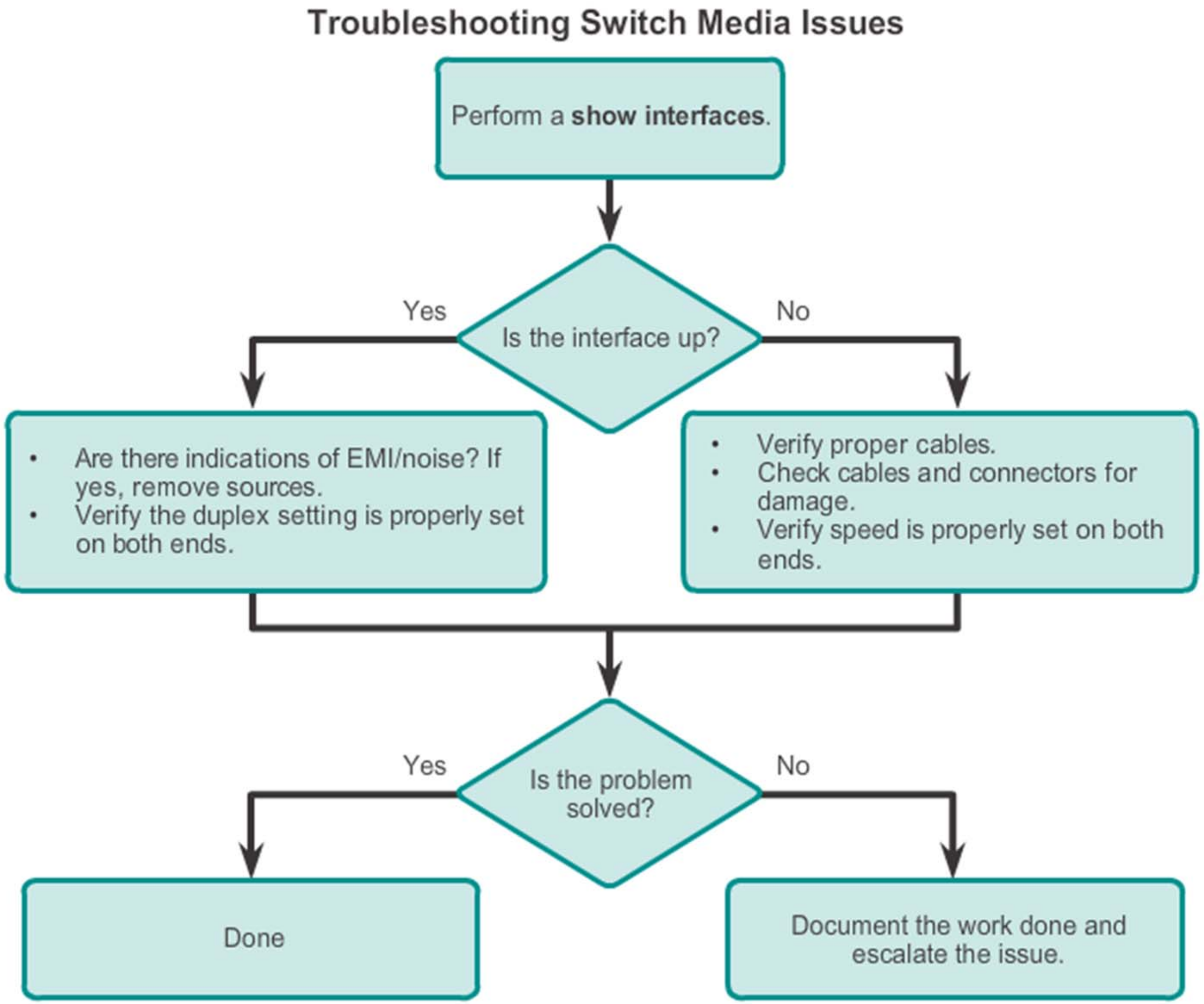
Network Access Layer Issues (cont.)



Parameter	Description
Runts	Packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, 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.
Input errors	Total number of errors. It includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
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.

Configuring Switch Ports

Troubleshooting Switch Media (Connection) Issues


Troubleshooting Switch Media Issues
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.

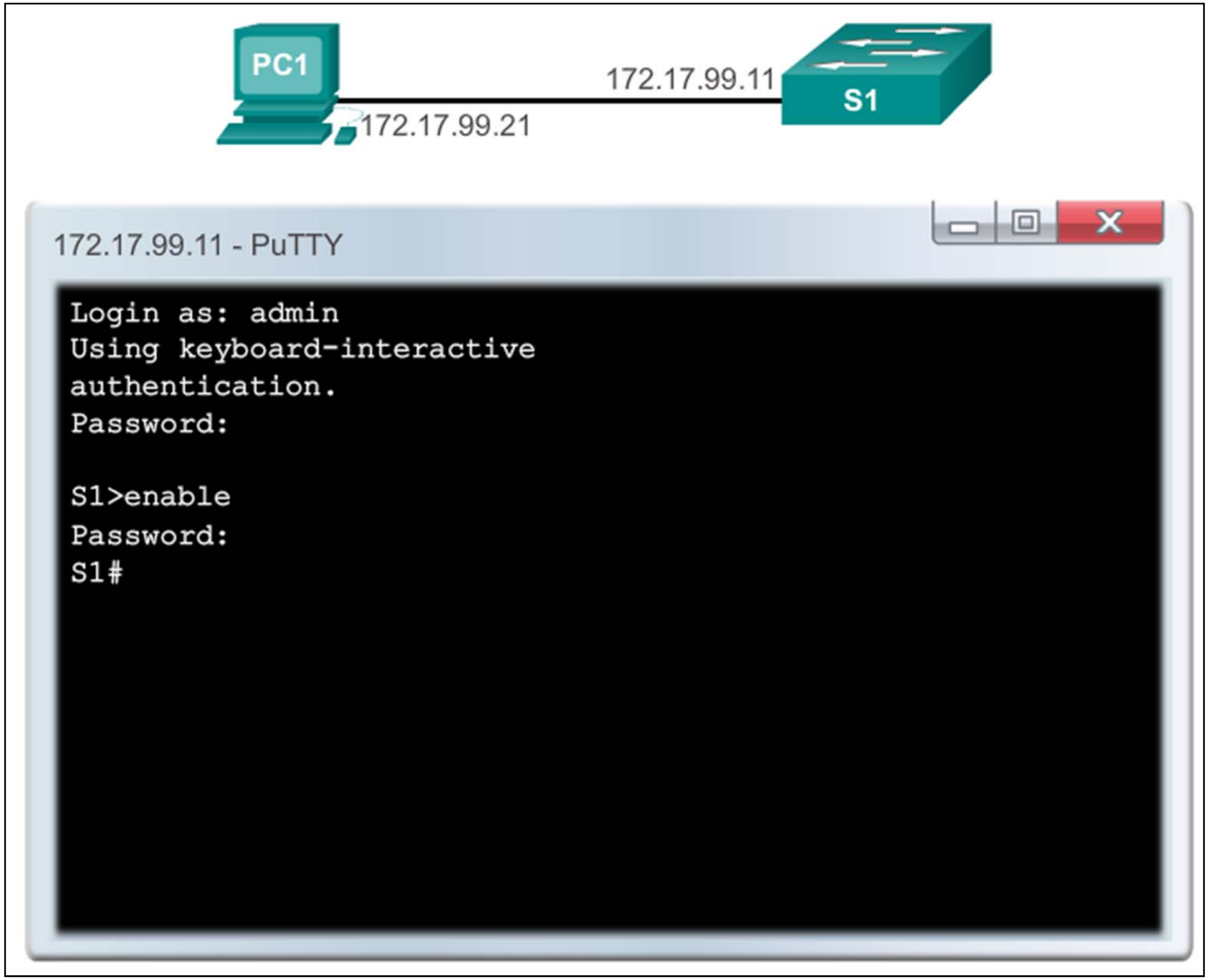
Secure Remote Access

SSH Operation

- Secure Shell (SSH) is a protocol that provides a secure (encrypted), command-line based connection to a remote device.
- SSH is commonly used in UNIX-based systems.
- The Cisco IOS software also supports SSH.
- A version of the IOS software, including cryptographic (encrypted) features and capabilities, is required to enable SSH on Catalyst 2960 switches.
- Because its strong encryption features, SSH should replace Telnet for management connections.
- SSH uses TCP port 22, by default. Telnet uses TCP port 23.

Secure Remote Access

SSH Operation (cont.)

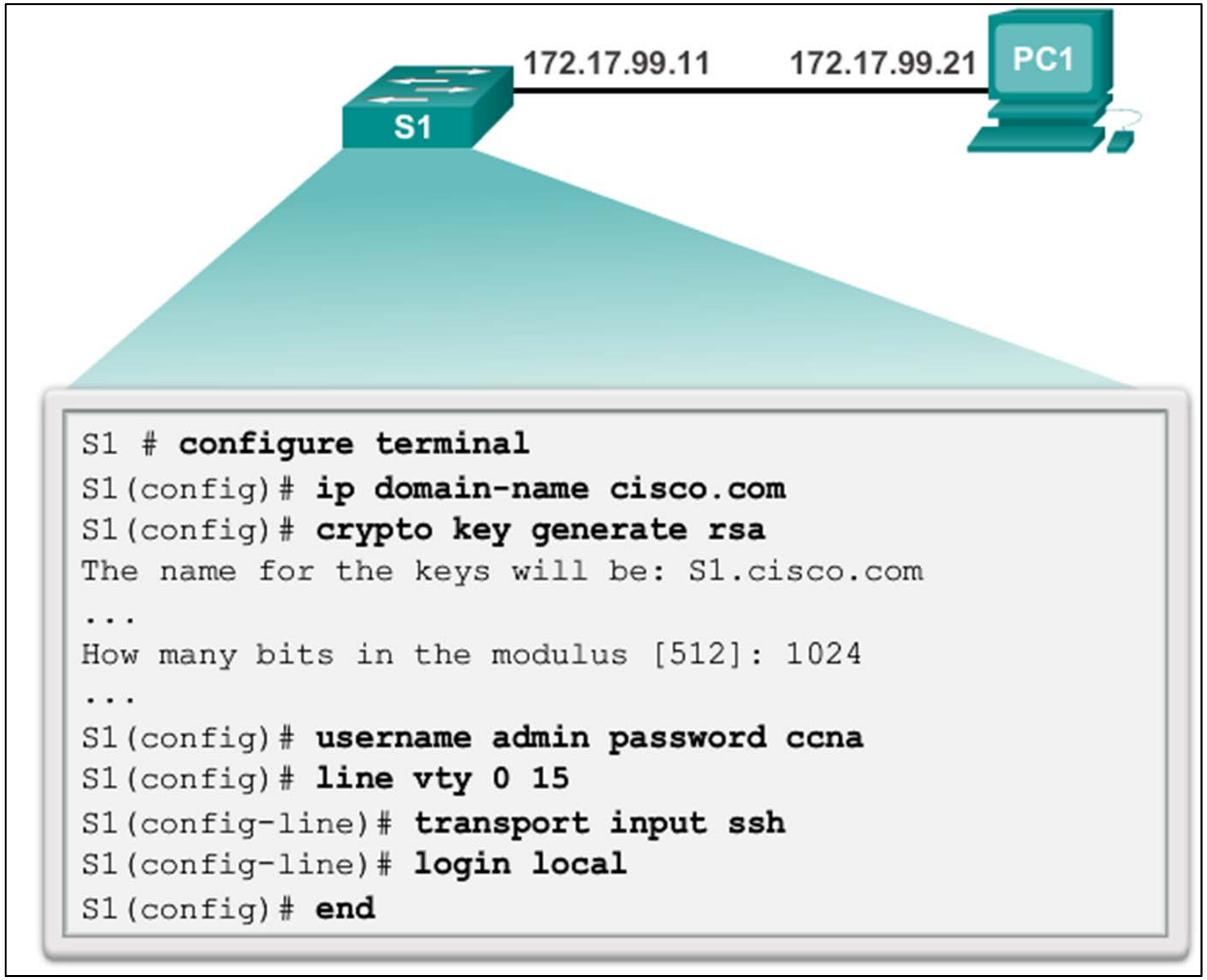


```
Login as: admin
Using keyboard-interactive
authentication.
Password:

S1>enable
Password:
S1#
```

Secure Remote Access

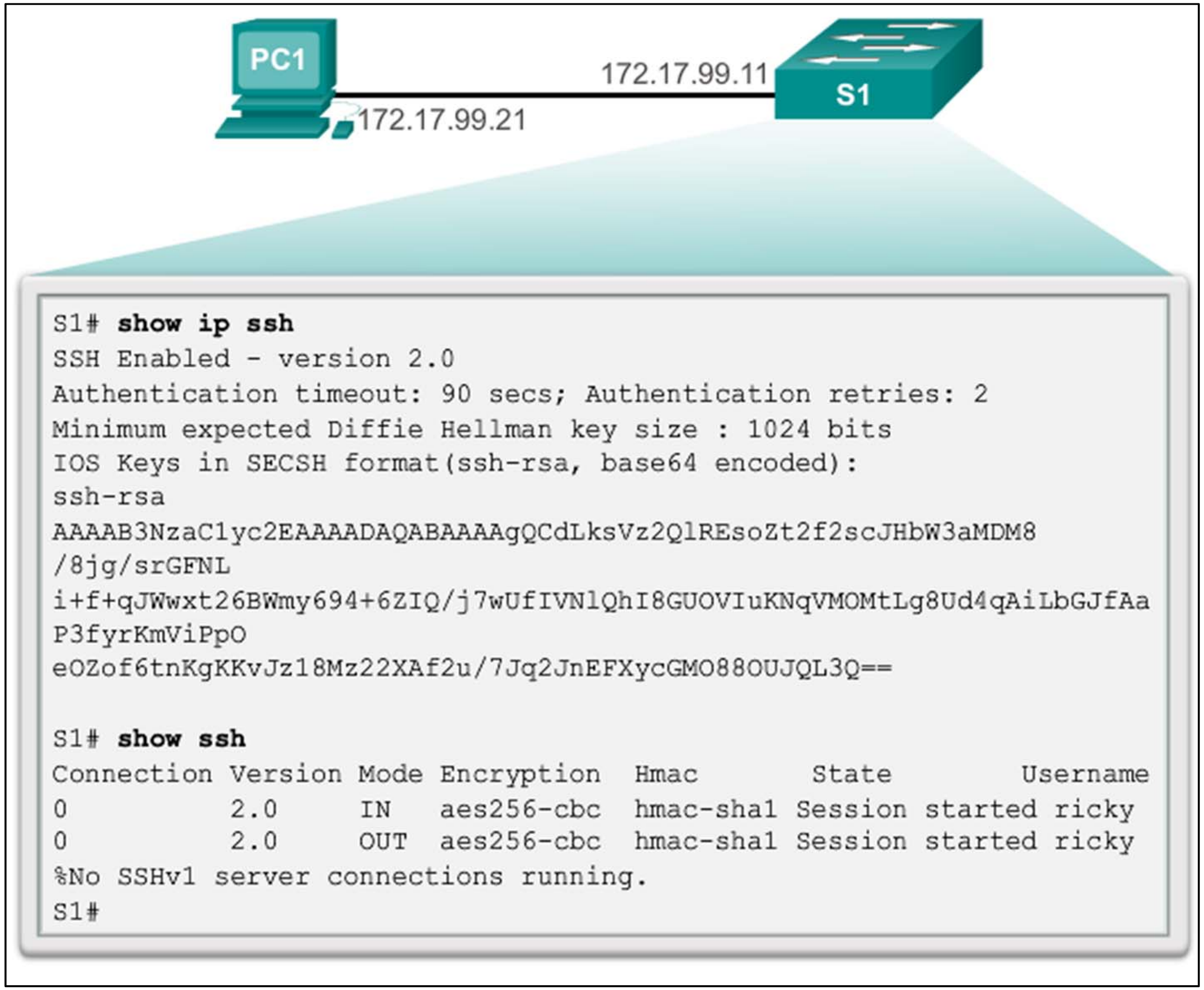
Configuring SSH



```
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
```

Secure Remote Access

Verifying SSH



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

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

Security Concerns in LANs

MAC Address Flooding

- Switches automatically populate their CAM tables by watching traffic entering their ports.
- Switches forward traffic trough all ports if it cannot find the destination MAC in its CAM table.
- Under such circumstances, the switch acts as a hub. Unicast traffic can be seen by all devices connected to the switch.
- An attacker could exploit this behavior to gain access to traffic normally controlled by the switch by using a PC to run a MAC flooding tool.
- Such tool is a program created to generate and send out frames with bogus source MAC addresses to the switch port.
- As these frames reach the switch, it adds the bogus MAC address to its CAM table, taking note of the port the frames arrived.

Security Concerns in LANs

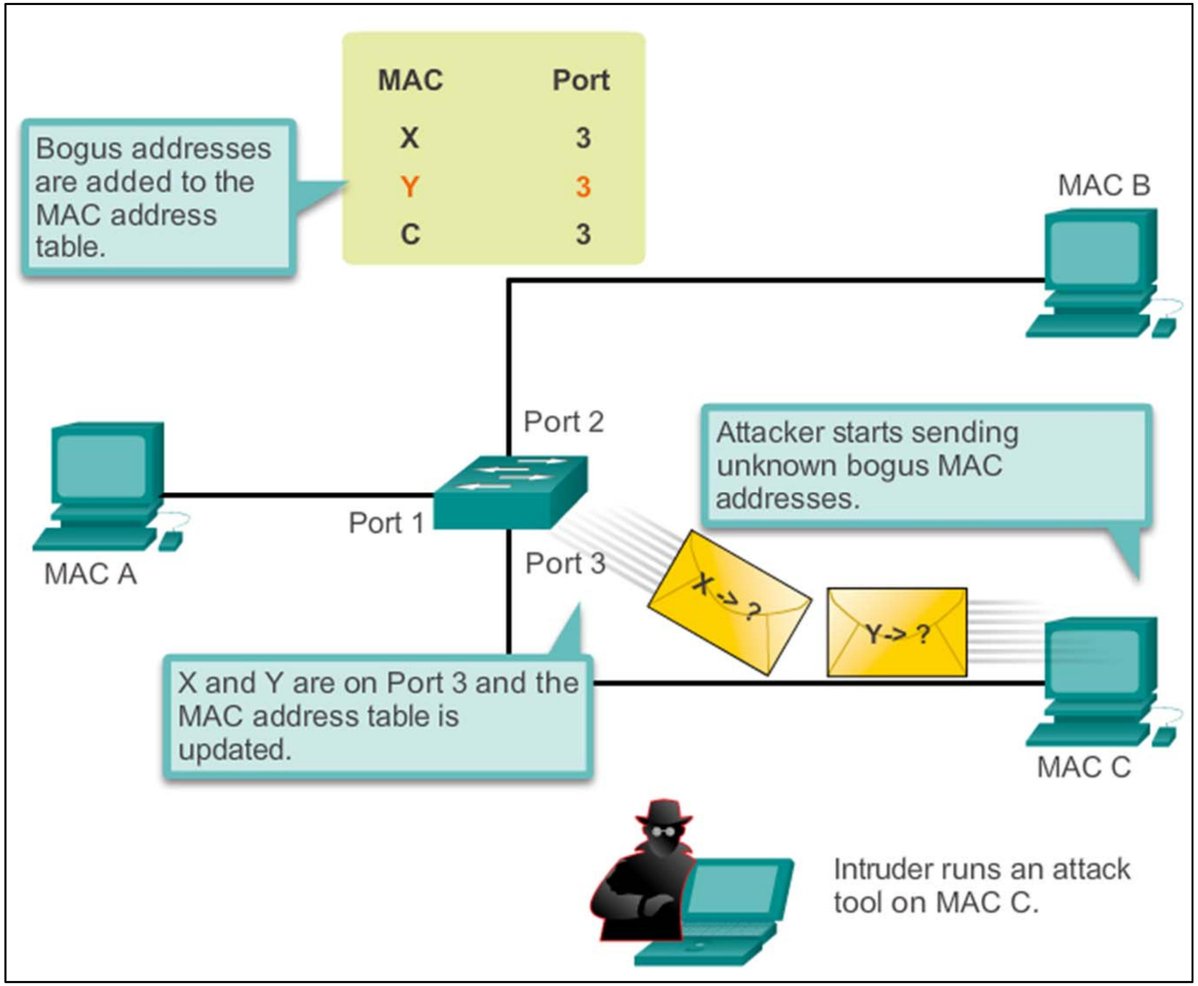
MAC Address Flooding (cont.)

- Eventually the CAM table fills out with bogus MAC addresses.
- The CAM table now has no room for legit devices present in the network and, therefore, never finds their MAC addresses in the CAM table.
- All frames are now forwarded to all ports, allowing the attacker to access traffic to other hosts.

Security Concerns in LANs

MAC Address Flooding (cont.)

An attacker flooding the CAM table with bogus entries.



MAC	Port
X	3
Y	3
C	3

Bogus addresses are added to the MAC address table.

Attacker starts sending unknown bogus MAC addresses.

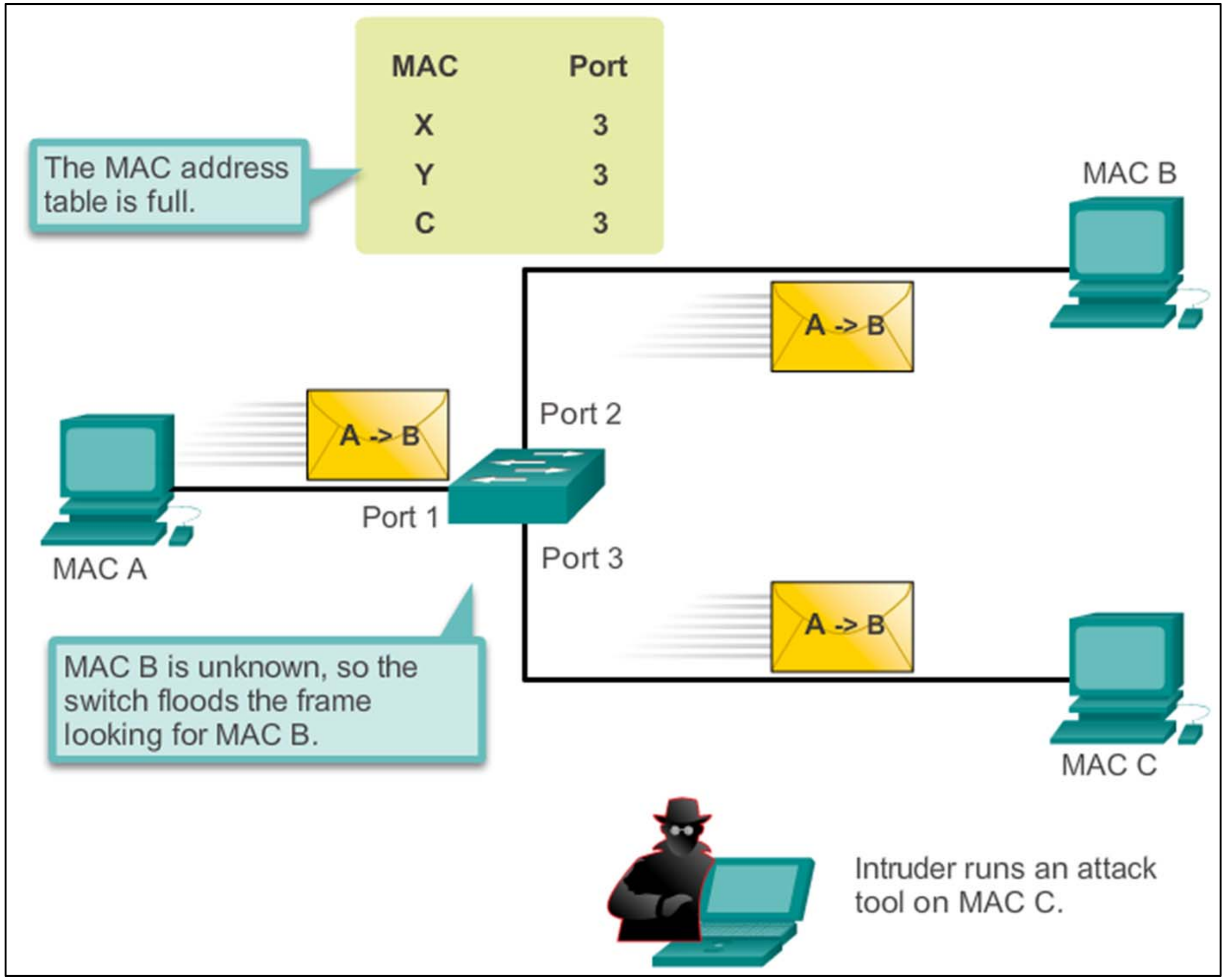
X and Y are on Port 3 and the MAC address table is updated.

Intruder runs an attack tool on MAC C.

Security Concerns in LANs

MAC Address Flooding (cont.)

The switch now behaves as a hub.



MAC	Port
X	3
Y	3
C	3

The MAC address table is full.

MAC B is unknown, so the switch floods the frame looking for MAC B.

Intruder runs an attack tool on MAC C.

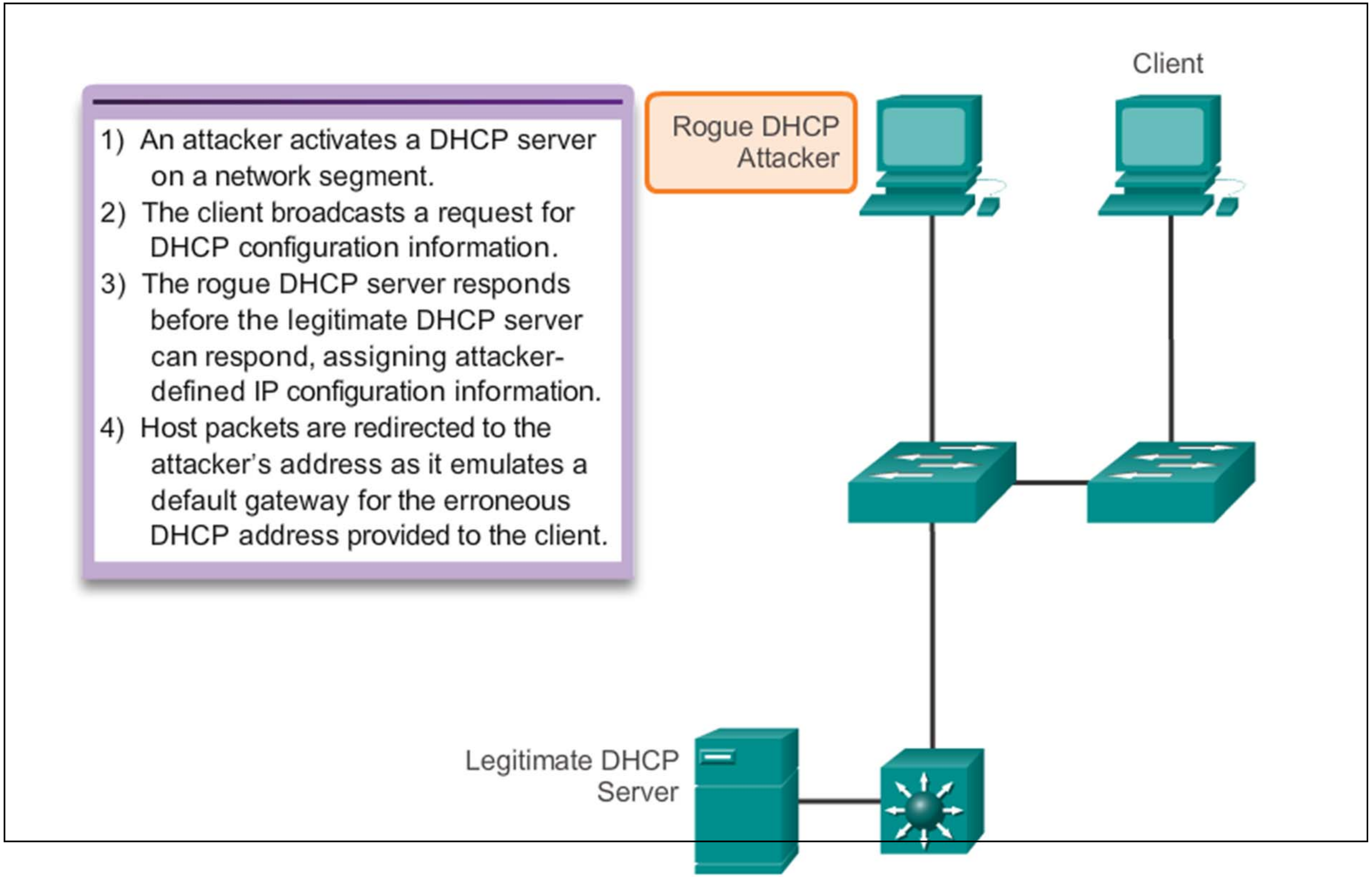
Security Concerns in LANs

DHCP Spoofing

- DHCP is a network protocol used to automatically assign IP information.
- Two types of DHCP attacks are:
  - DHCP spoofing
  - DHCP starvation
- In DHCP spoofing attacks, a fake DHCP server is placed in the network to issue DHCP addresses to clients.
- DHCP starvation is often used before a DHCP spoofing attack to deny service to the legitimate DHCP server.

Security Concerns in LANs

DHCP Spoof Attack



1) An attacker activates a DHCP server on a network segment.
2) The client broadcasts a request for DHCP configuration information.
3) The rogue DHCP server responds before the legitimate DHCP server can respond, assigning attacker-defined IP configuration information.
4) Host packets are redirected to the attacker's address as it emulates a default gateway for the erroneous DHCP address provided to the client.

Security Concerns in LANs

Leveraging Cisco Discovery Protocol

- The Cisco Discovery Protocol is a Layer 2 Cisco proprietary protocol used to discover other directly connected Cisco devices.
- The Cisco Discovery Protocol is designed to allow the devices to auto-configure their connections.
- If an attacker is listening to Cisco Discovery Protocol messages, it could learn important information about the device model and running software version.

Note: Cisco recommends disabling CDP when not in use.

Security Concerns in LANs

Leveraging Telnet

- The Telnet protocol is insecure and should be replaced by SSH.
- An attacker can use Telnet as part of other attacks:
  - Brute force password attack
  - Telnet DOS attack
- When passwords cannot be captured, attackers will try as many combinations of characters as possible. This attempt to guess the password is known as brute force password attack.
- Telnet can be used to test the guessed password against the system.

Security Concerns in LANs

Leveraging Telnet (cont.)

- 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.

Security Best Practices

10 Best Practices

- 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.
- Use HTTPS instead of HTTP.
- Perform backup operations on a regular basis.
- Educate employees about social engineering attacks.
- Encrypt and password-protect sensitive data.
- Implement firewalls.
- Keep software up-to-date.

Security Best Practices

Network Security Tools: Options

- Network security tools are important to network administrators.
- Network security tools allow an administrator to test the strength of the security measures implemented.
- An administrator can launch an attack against the network and analyze the results. This is also 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.

Security Best Practices

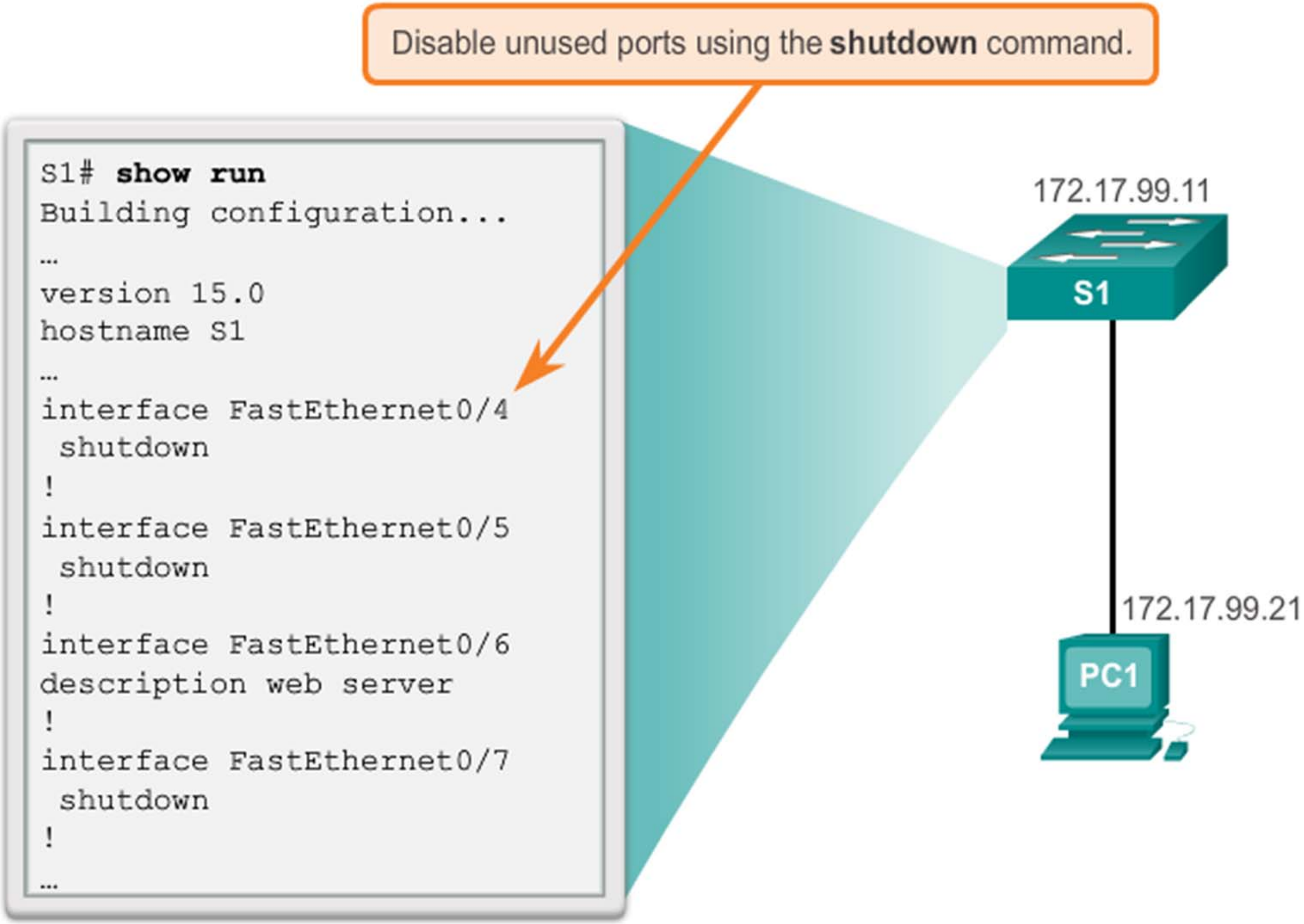
Network Security Tools: Audits

- Network security tools can be used to audit the network.
- By monitoring the network, an administrator can assess what type of information an attacker would be able to gather. For example, by attacking and flooding the CAM table of a switch, an administrator learn which switch ports are vulnerable to MAC flooding and can correct the issue.
- Network security tools can also be used as penetration test tools. Penetration testing is a simulated attack and helps to determine how vulnerable the network is when under a real attack.
- Weaknesses within the configuration of networking devices can be identified based on penetration test results.
- Changes can be made to make the devices more resilient to attacks.
- Such tests can damage the network and should be carried out under very controlled conditions.
- An offline test bed network that mimics the actual production network is ideal.

Switch Port Security

Secure Unused Ports

Disabling unused ports is a simple, yet efficient security guideline.



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

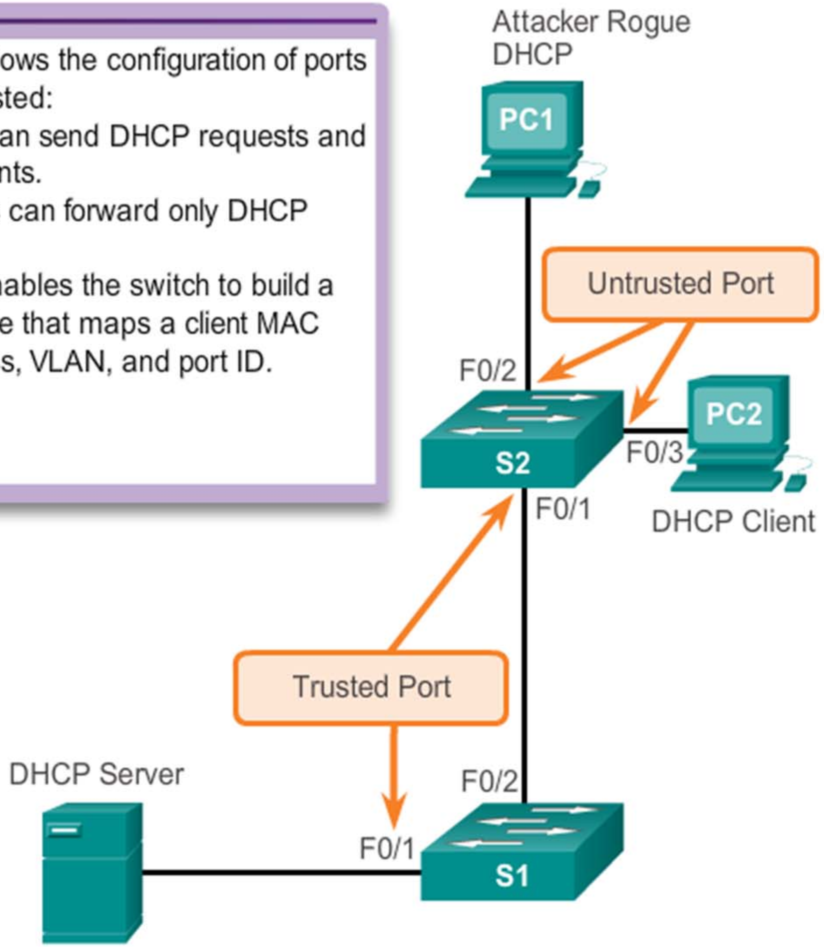
```
S1# show run
Building configuration...
…
version 15.0
hostname S1
…
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
description web server
!
interface FastEthernet0/7
 shutdown
!
…
```

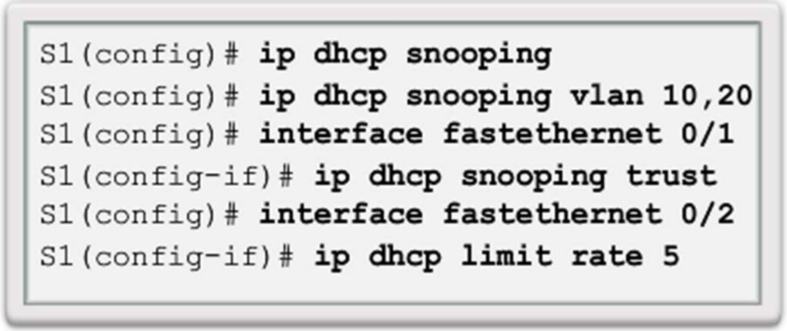
Switch Port Security

DHCP Snooping

DHCP Snooping specifies which switch ports can respond to DHCP requests

- 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.





```
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 limit rate 5
```

Switch Port Security

Port Security: Operation

- 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.
- Any additional attempts to connect by unknown MAC addresses generate a security violation.
- Secure MAC addresses can be configured in a number of ways:
  - Static secure MAC addresses
  - Dynamic secure MAC addresses
  - Sticky secure MAC addresses

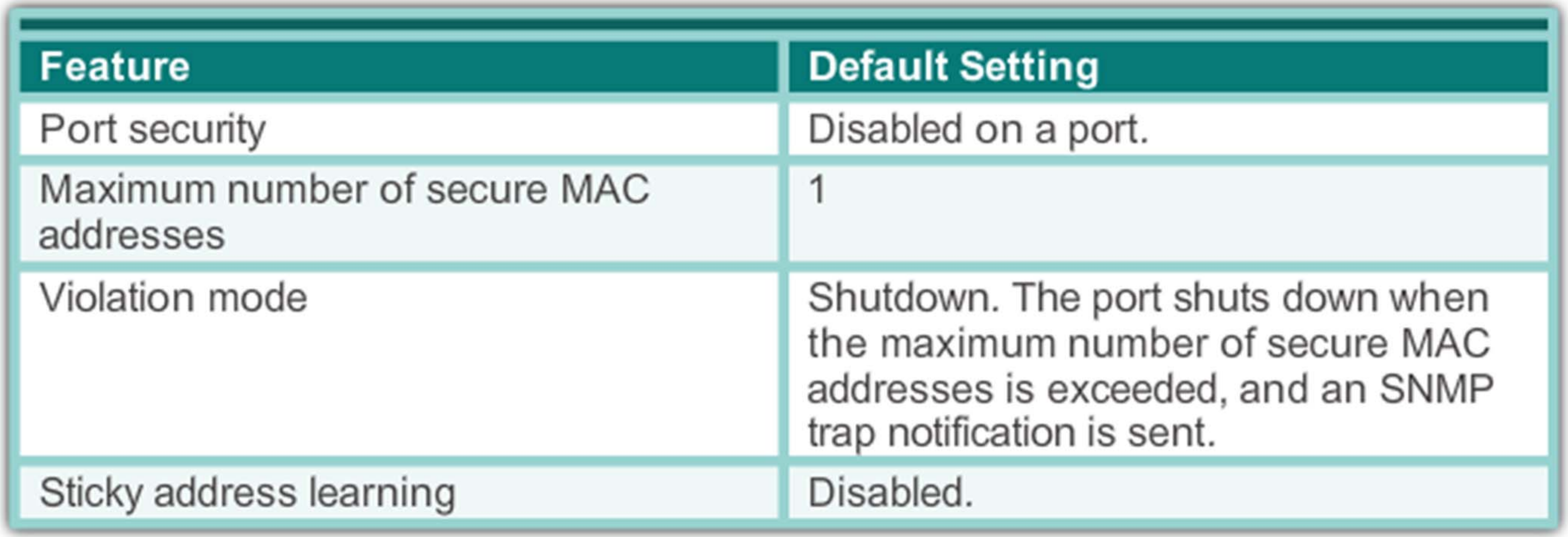
Switch Port Security

Port Security: Violation Modes

- IOS considers a security violation when either of these situations occurs:
  - The maximum number of secure MAC addresses for that interface have been added to the CAM, 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.
- There are three possible actions to take when a violation is detected:
  - Protect
  - Restrict
  - Shutdown

Switch Port Security

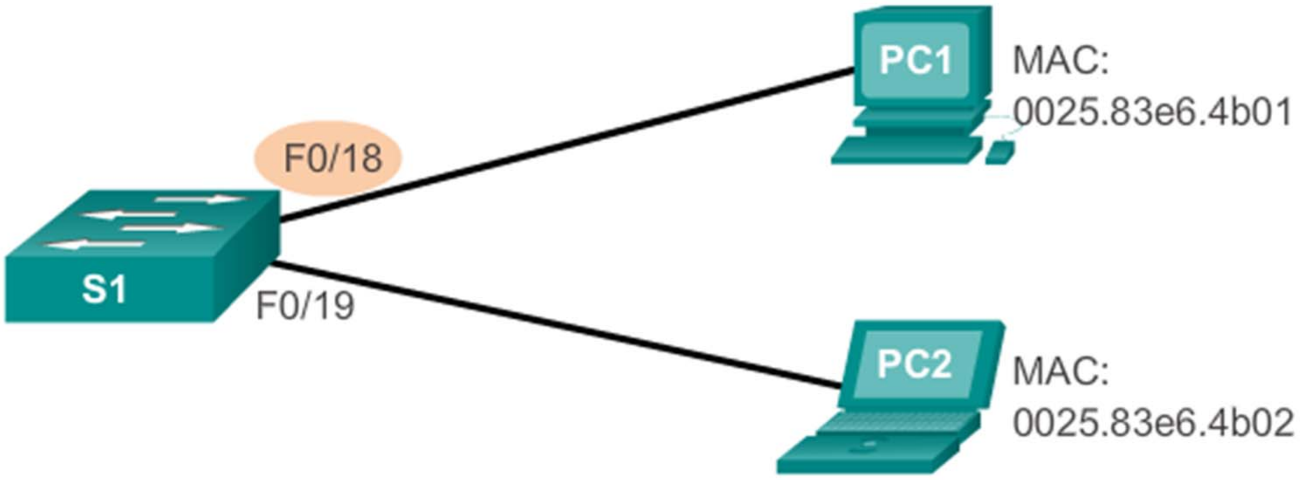
Dynamic Port Security Defaults

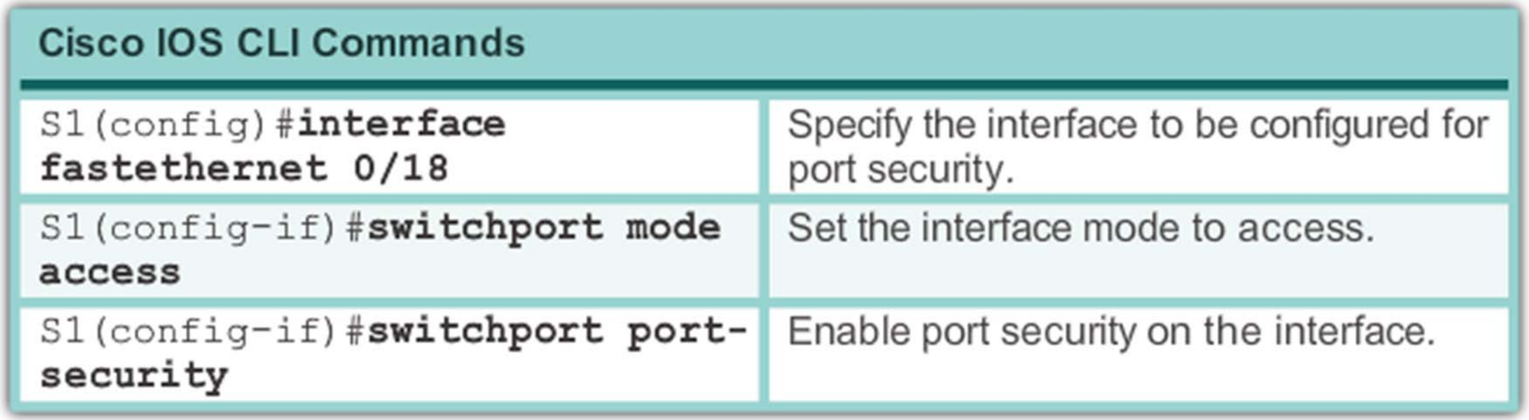


Feature	Default Setting
Port security	Disabled on a port.
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.
Sticky address learning	Disabled.

Switch Port Security

Configuring Dynamic Port Security

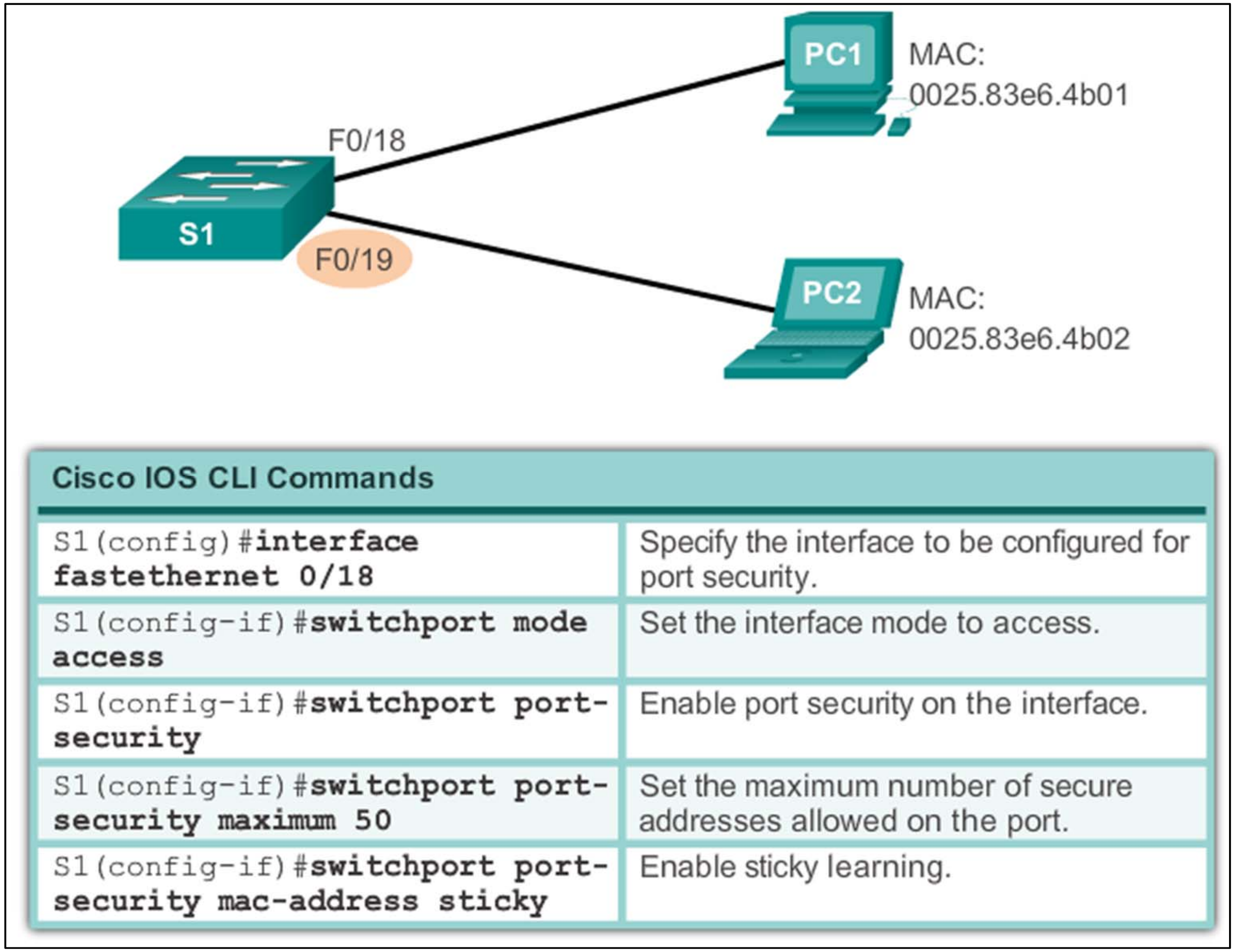




Cisco IOS CLI Commands	
S1(config)#**interface fastethernet 0/18**	Specify the interface to be configured for port security.
S1(config-if)#**switchport mode access**	Set the interface mode to access.
S1(config-if)#**switchport port-security**	Enable port security on the interface.

Switch Port Security

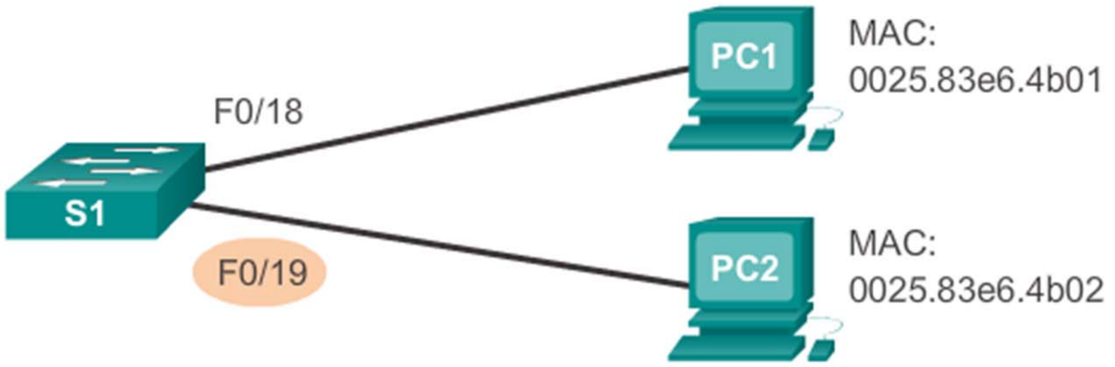
Configuring Port Security Sticky

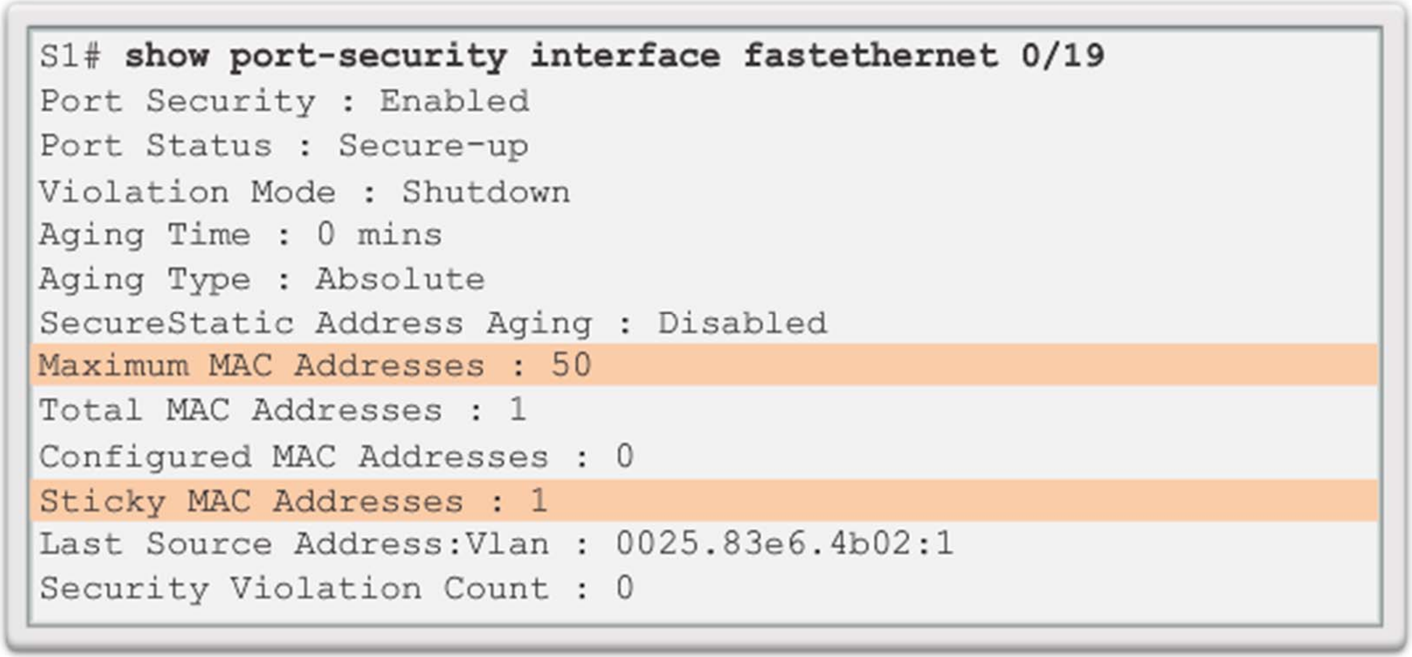


Cisco IOS CLI Commands	
S1(config)#**interface fastethernet 0/18**	Specify the interface to be configured for port security.
S1(config-if)#**switchport mode access**	Set the interface mode to access.
S1(config-if)#**switchport port-security**	Enable port security on the interface.
S1(config-if)#**switchport port-security maximum 50**	Set the maximum number of secure addresses allowed on the port.
S1(config-if)#**switchport port-security mac-address sticky**	Enable sticky learning.

Switch Port Security

Verifying Port Security Sticky

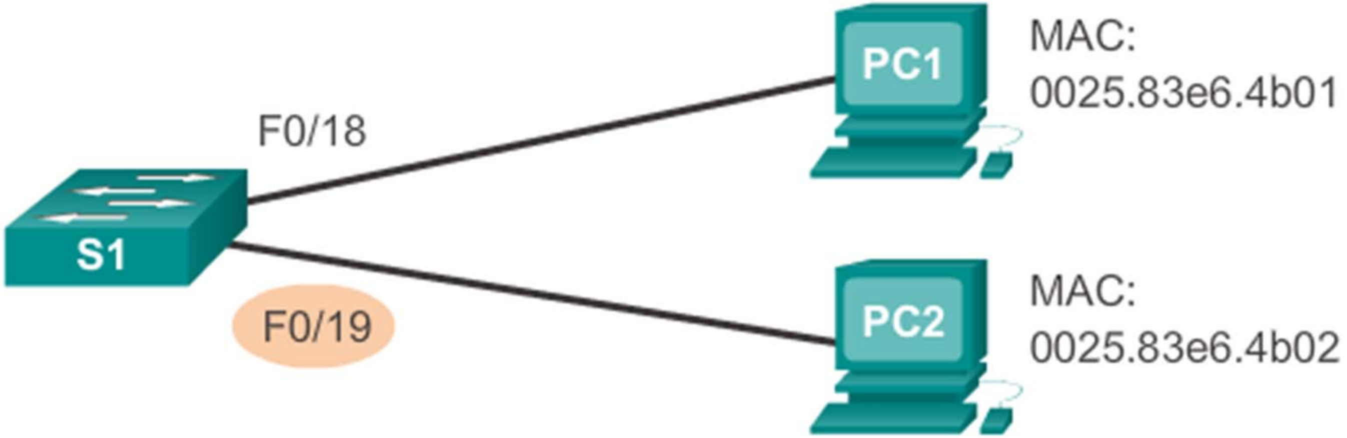


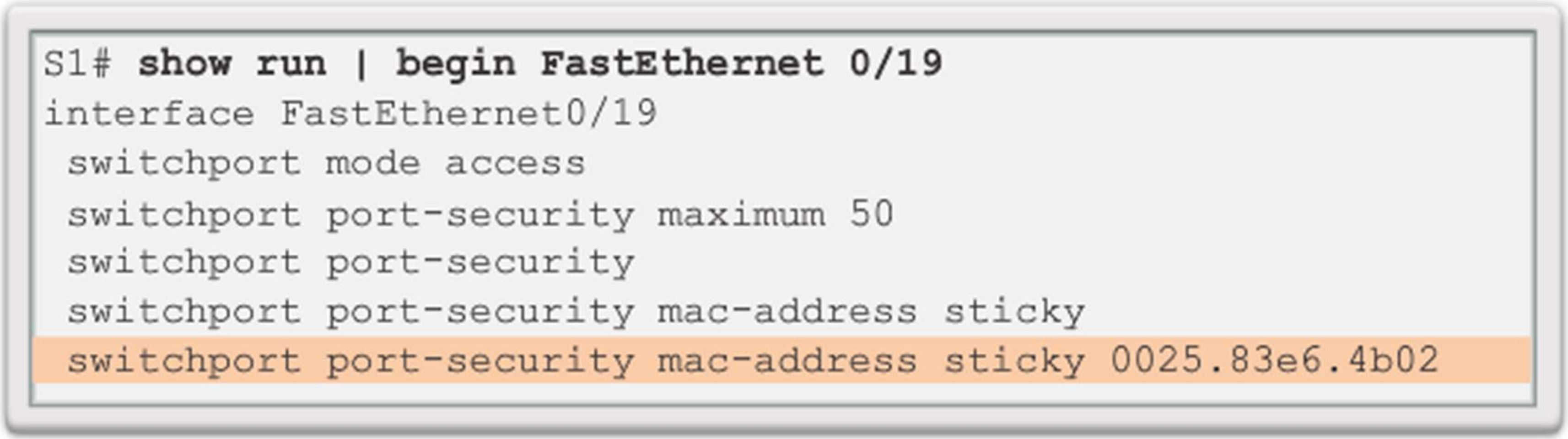


```
S1# show port-security interface fastethernet 0/19
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 50
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses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

Switch Port Security

Verifying Port Security Stick – Running Configuration

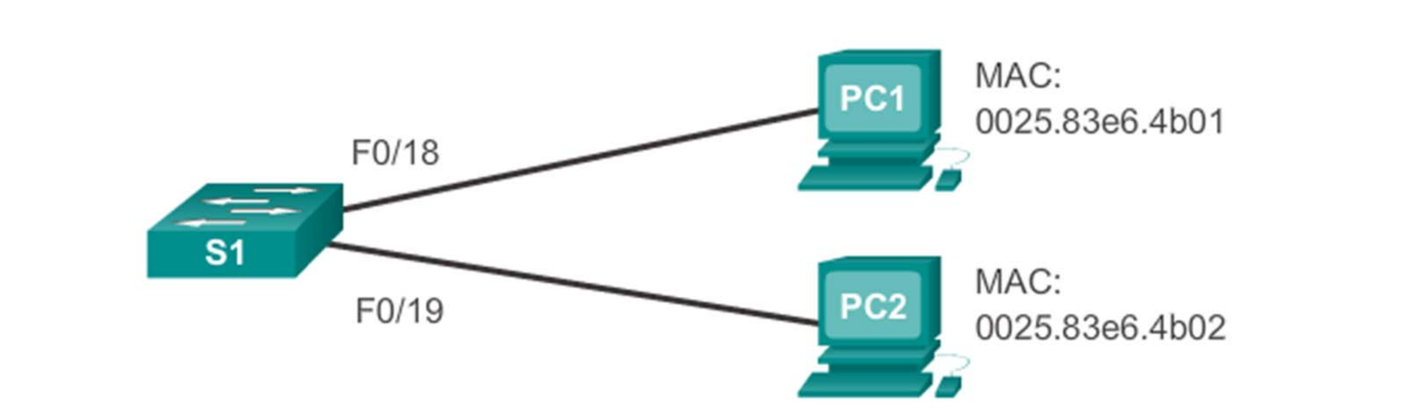


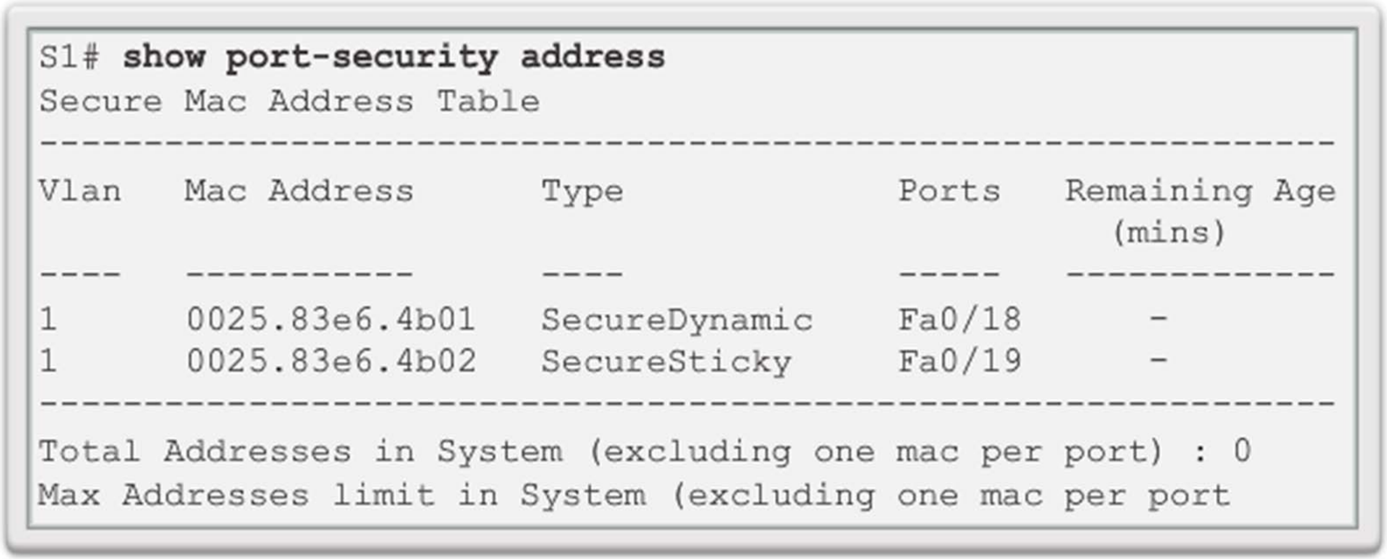


```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 50
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

Switch Port Security

Verifying Port Security – Secure MAC Addresses



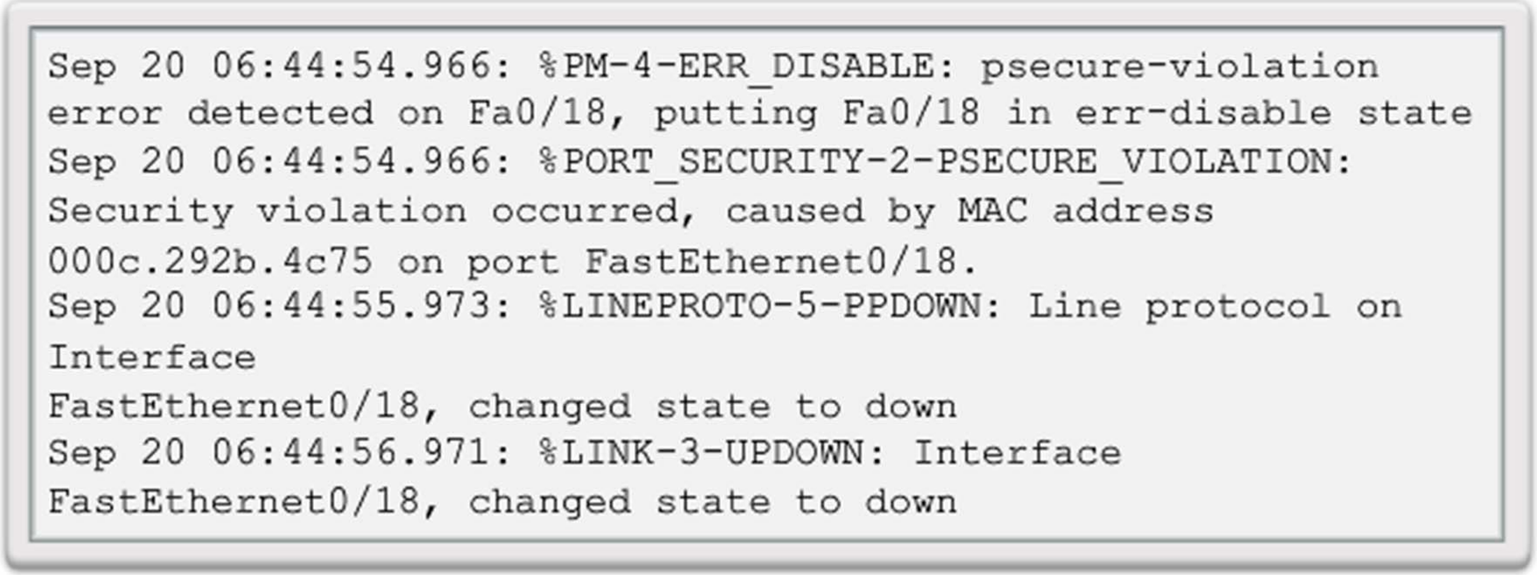


```
S1# show port-security address
Secure Mac Address Table
-------------------------------------------------------------
Vlan    Mac Address       Type              Ports    Remaining Age
                                                       (mins)
----    -----------       ----              -----    -------------
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
```

Switch Port Security

Ports in Error Disabled State

- A port security violation can put a switch in error disabled state.
- A port in error disabled is effectively shutdown.
- The switch communicates these events through console messages.

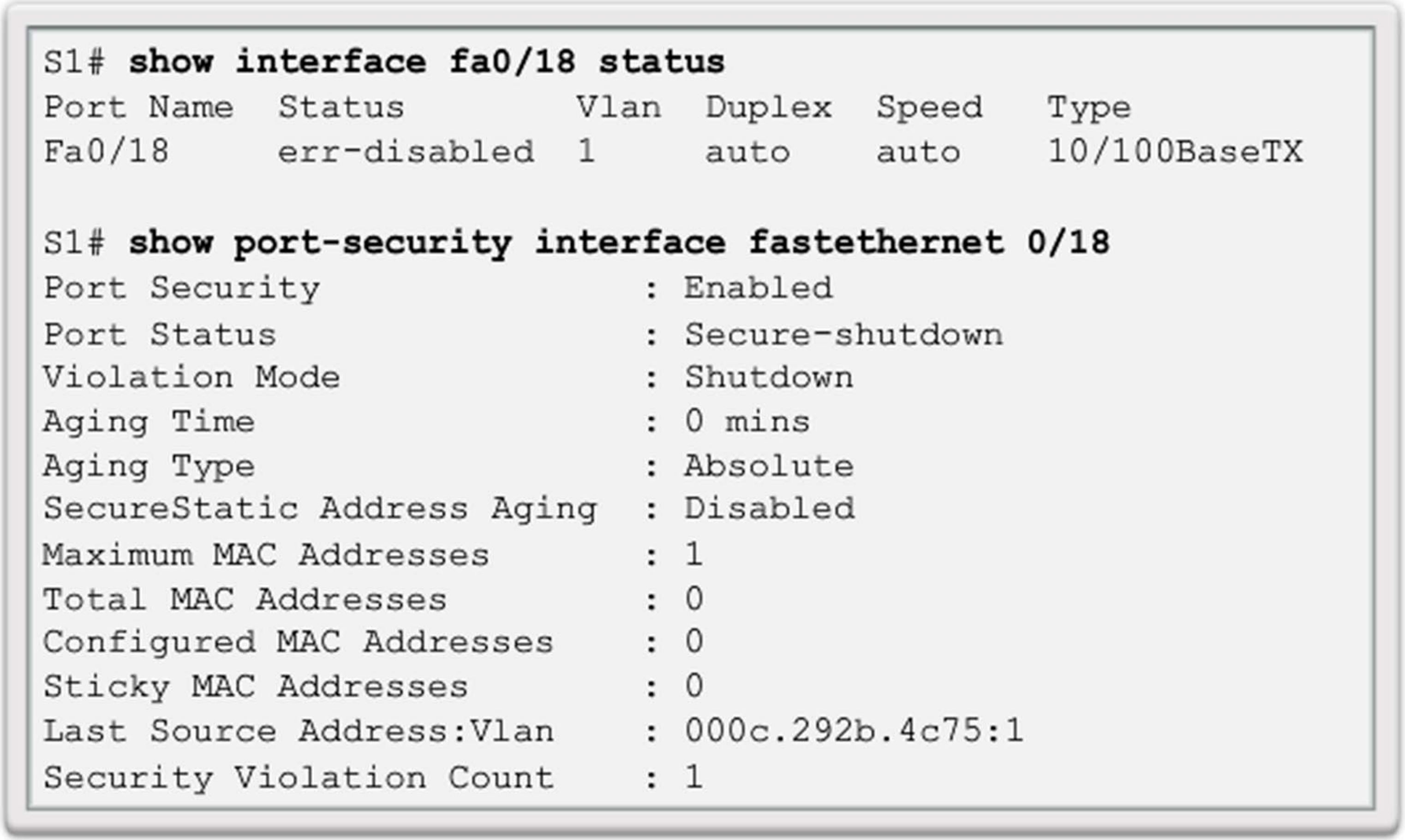


```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: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

Switch Port Security

Ports in Error Disabled State (cont.)

The **`show interface`** command also reveals a switch port on error disabled state.



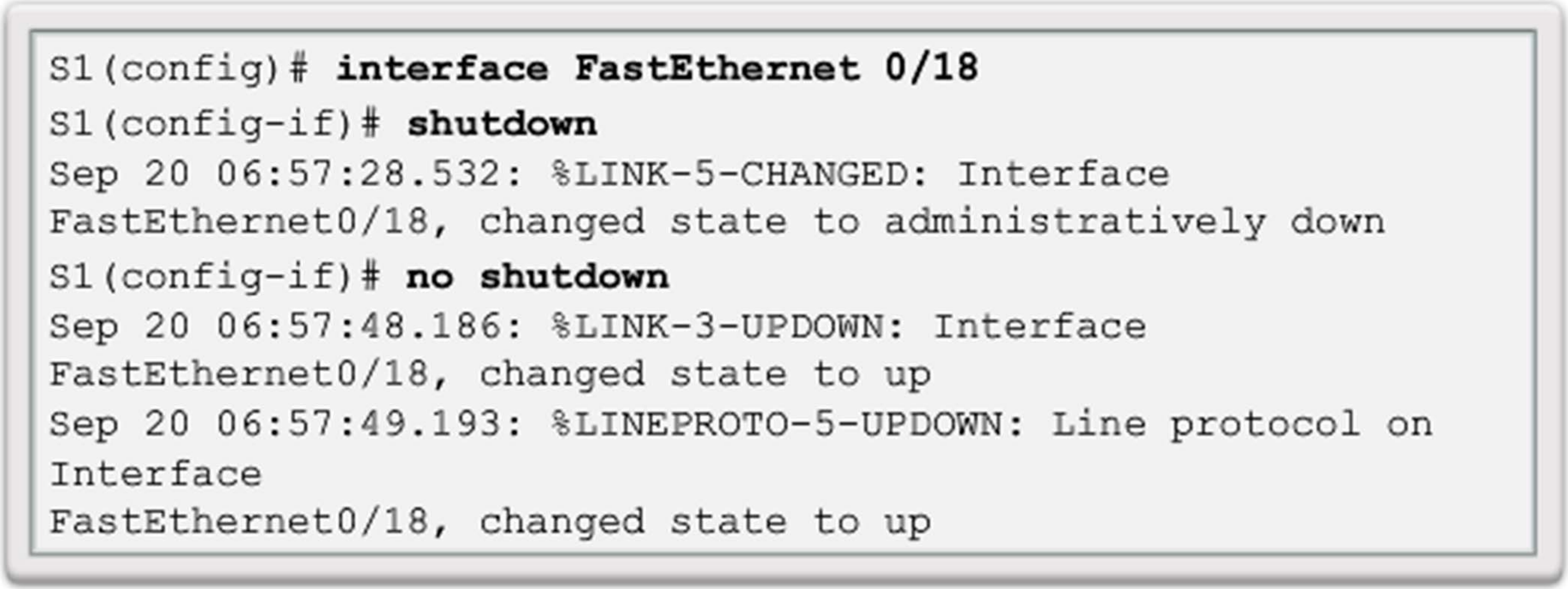
```
S1# show interface fa0/18 status
Port Name  Status        Vlan  Duplex  Speed  Type
Fa0/18     err-disabled  1     auto    auto   10/100BaseTX

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
```

Switch Port Security

Ports in Error Disabled State (cont.)

A **`shutdown`** or **`no shutdown`** interface configuration mode command must be issued to re-enable the 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
```

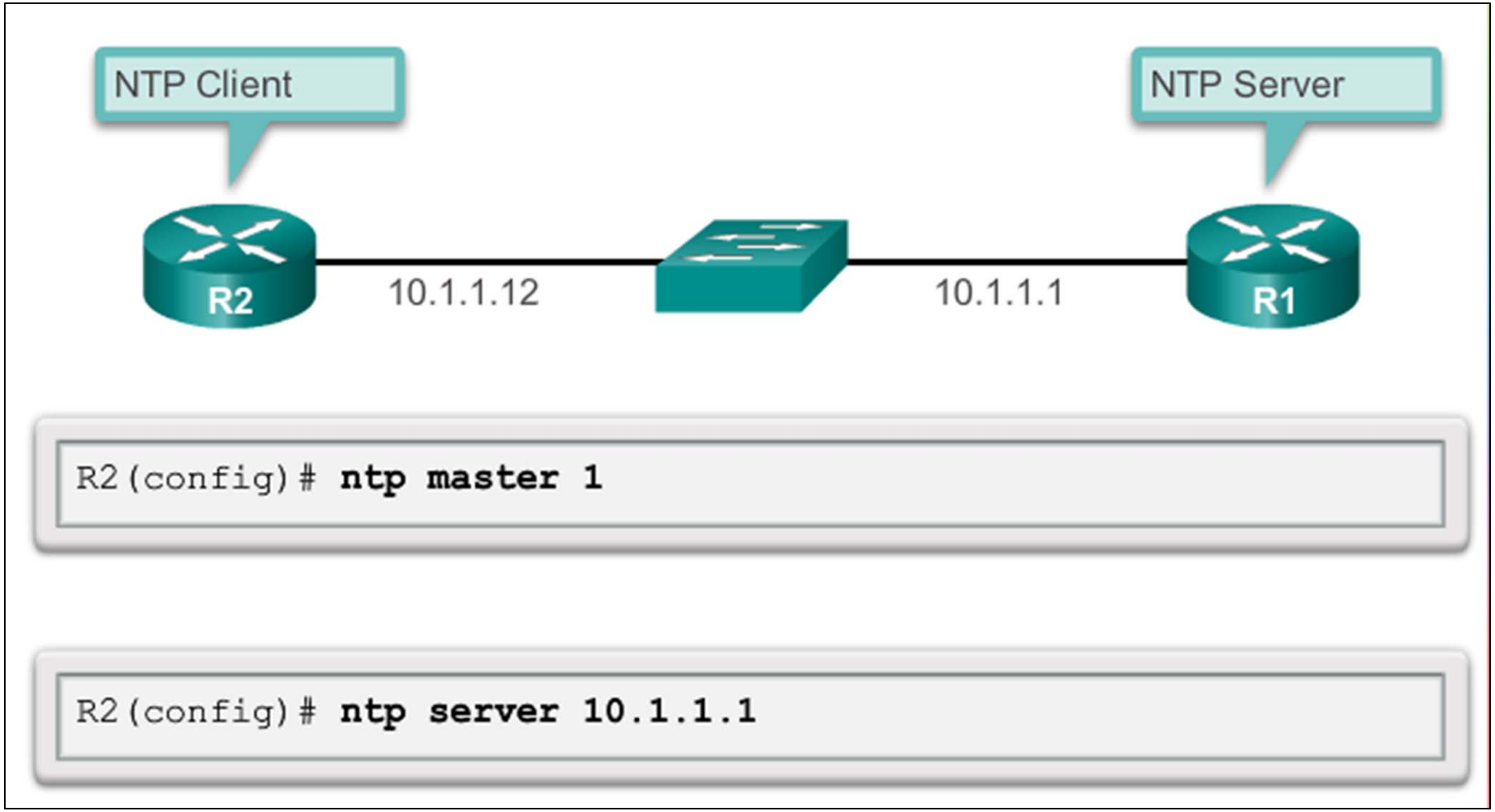
Switch Port Security

Network Time Protocol

- The Network Time Protocol (NTP) is used to synchronize the clocks of computer systems data networks.
- NTP can get the correct time from an internal or external time source.
- Time sources can be:
  - 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.
- See slide notes for more information on NTP.

Switch Port Security

Configuring NTP

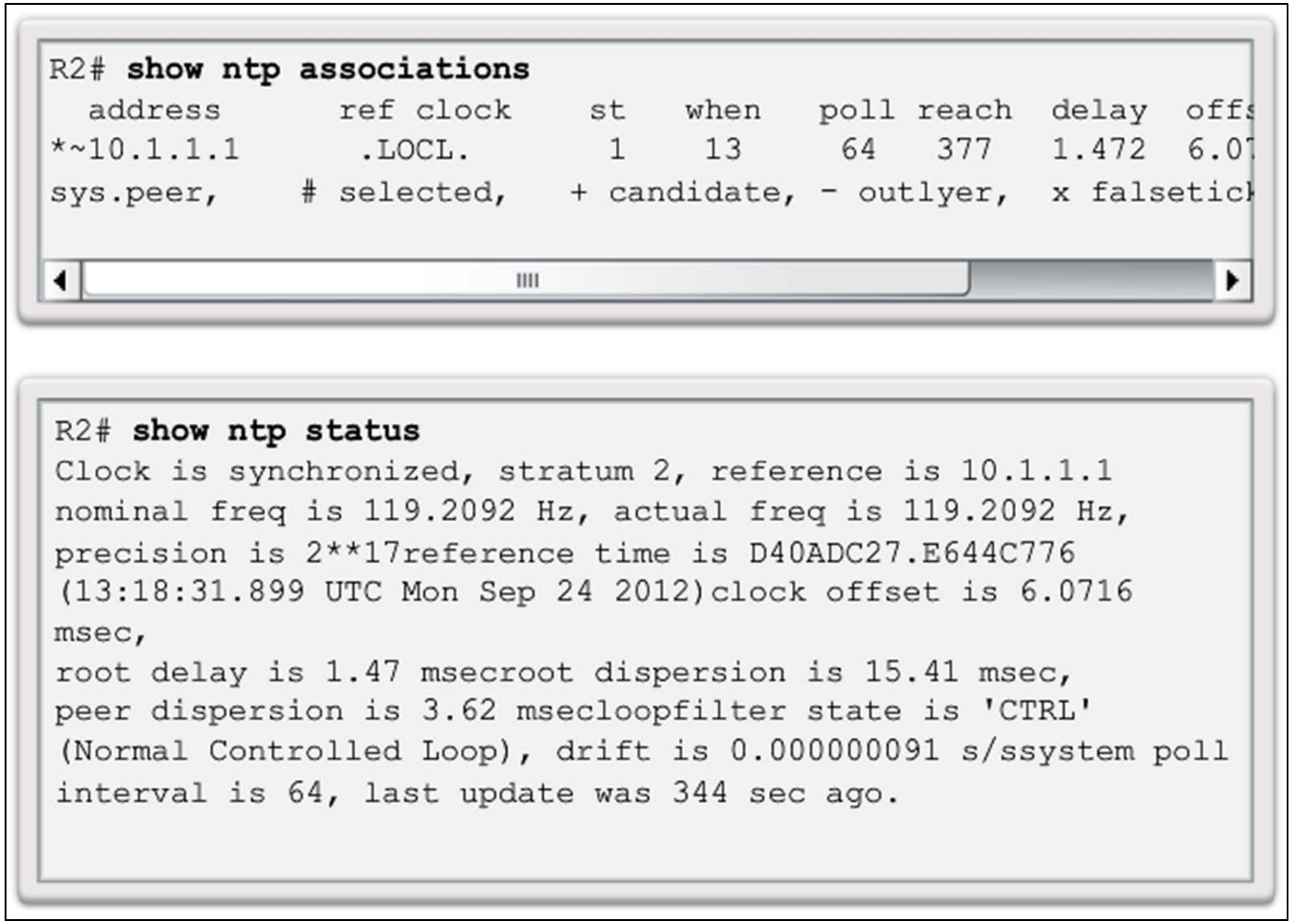


```
R2(config)# ntp master 1
```

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

Switch Port Security

Verifying NTP



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

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

Chapter 2: Summary

In this chapter, you learned:

- Cisco LAN switch boot sequence.
- Cisco LAN switch LED modes.
- How to remotely access and manage a Cisco LAN switch through a secure connection.
- Cisco LAN switch port duplex modes.
- Cisco LAN switch port security, violation modes, and actions.
- Best practices for switched networks.

Cisco | Networking Academy®

Mind Wide Open™