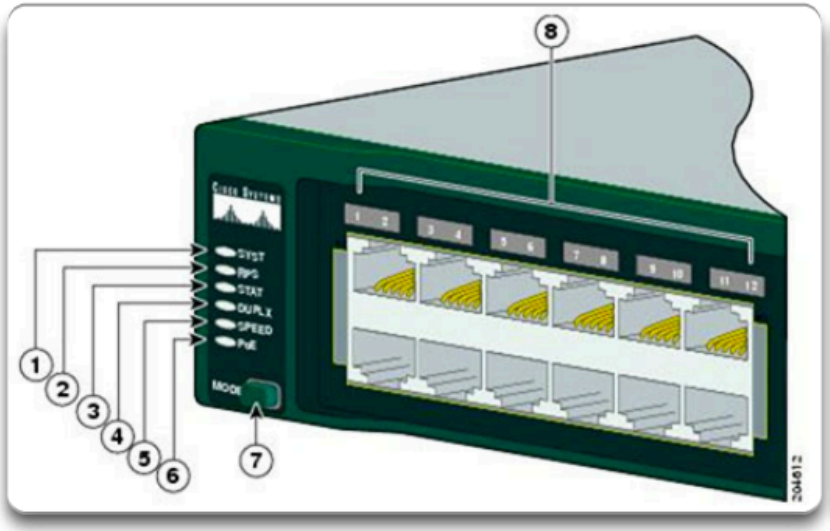
Chapter 2: Basic Switching Concepts and Configuration

Switched Networks

Cisco | Networking Academy®
Mind Wide Open™

Switch LED Indicators

Cisco Catalyst 2960 Switch Modes



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

Preparing for Basic Switch Management

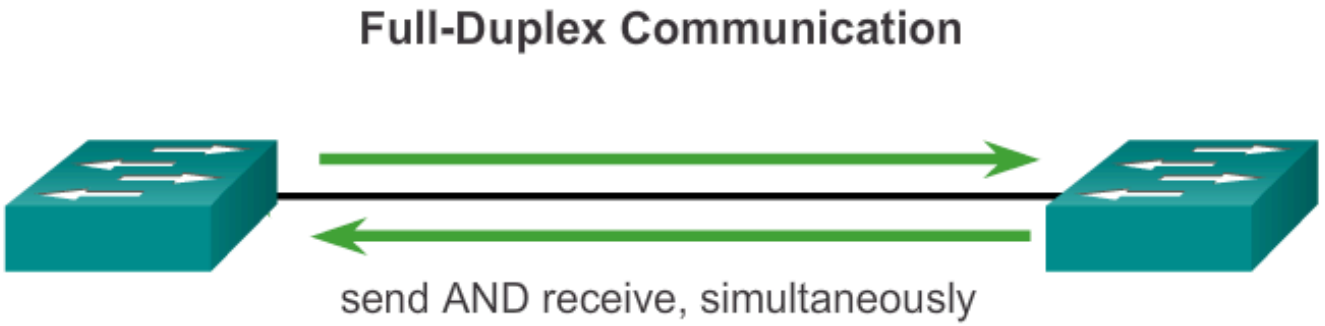
- To remotely manage a Cisco switch, it must be configured to access the network.
- An IP address and a subnet mask must be configured.
- If managing the switch from a remote network, a default gateway must also be configured.
- The IP information (address, subnet mask, gateway) must be assigned to a 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.

Configuring Basic Switch Management Access

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**

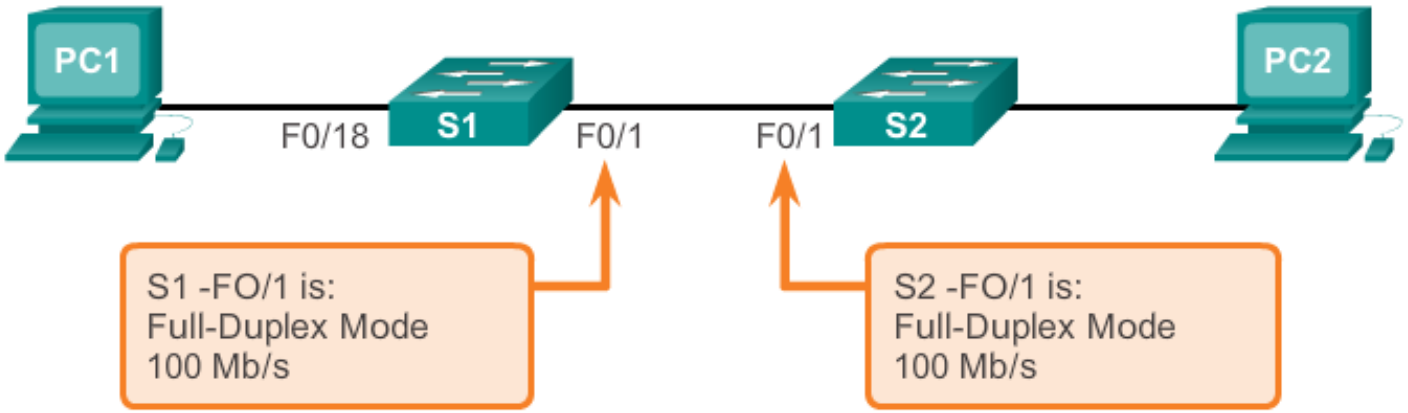
Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Configure the default gateway for the switch.	S1(config)# **ip default-gateway 172.17.99.**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config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

Duplex Communication



Configure Switch Ports at the Physical Layer

Configure Duplex and Speed



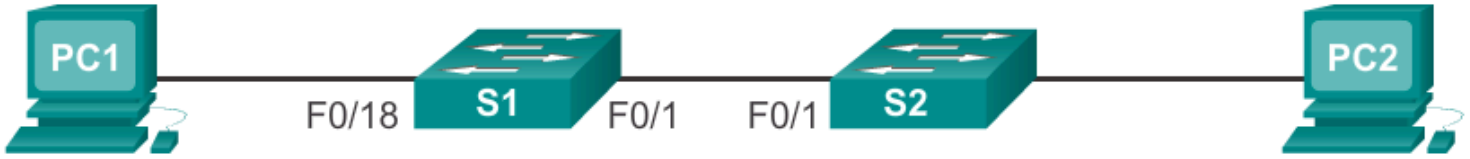
Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface fastethernet 0/1**
Configure the interface duplex.	S1(config-if)# **duplex full**
Configure the interface speed.	S1(config-if)# **speed 100**
Return to the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

Auto-MDIX Feature

- Certain cable types (straight-through or crossover) were 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 configures the connection appropriately.
- When using auto-MDIX on an interface, the interface speed and duplex must be set to **auto**.

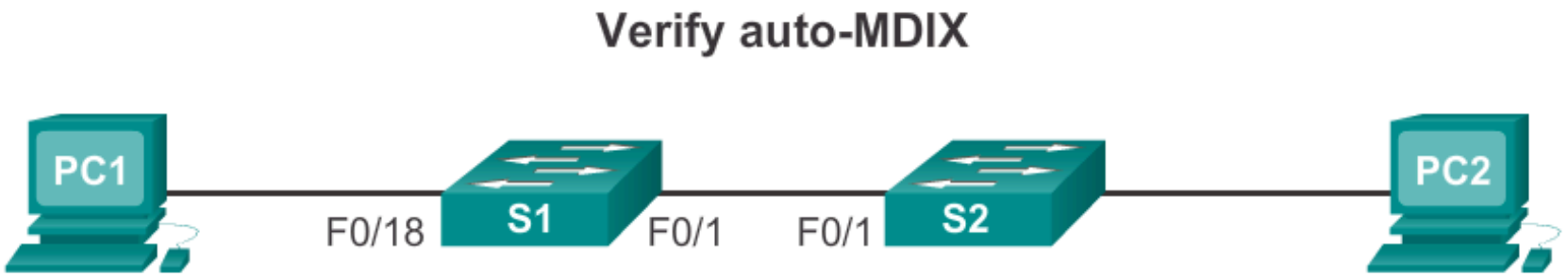
Auto-MDIX Feature (cont.)

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`

Auto-MDIX Feature (cont.)




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

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**

Display Interface Status and Statistics

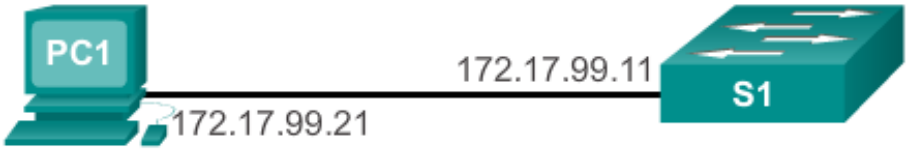
- Output of a **`show interfaces`** command

```
S1# show interfaces 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>
```

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 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 of its strong encryption features, SSH should replace Telnet for management connections.
- By default, SSH uses TCP port 22 and Telnet uses TCP port 23.

SSH Operation (cont.)



172.17.99.11 - PuTTY

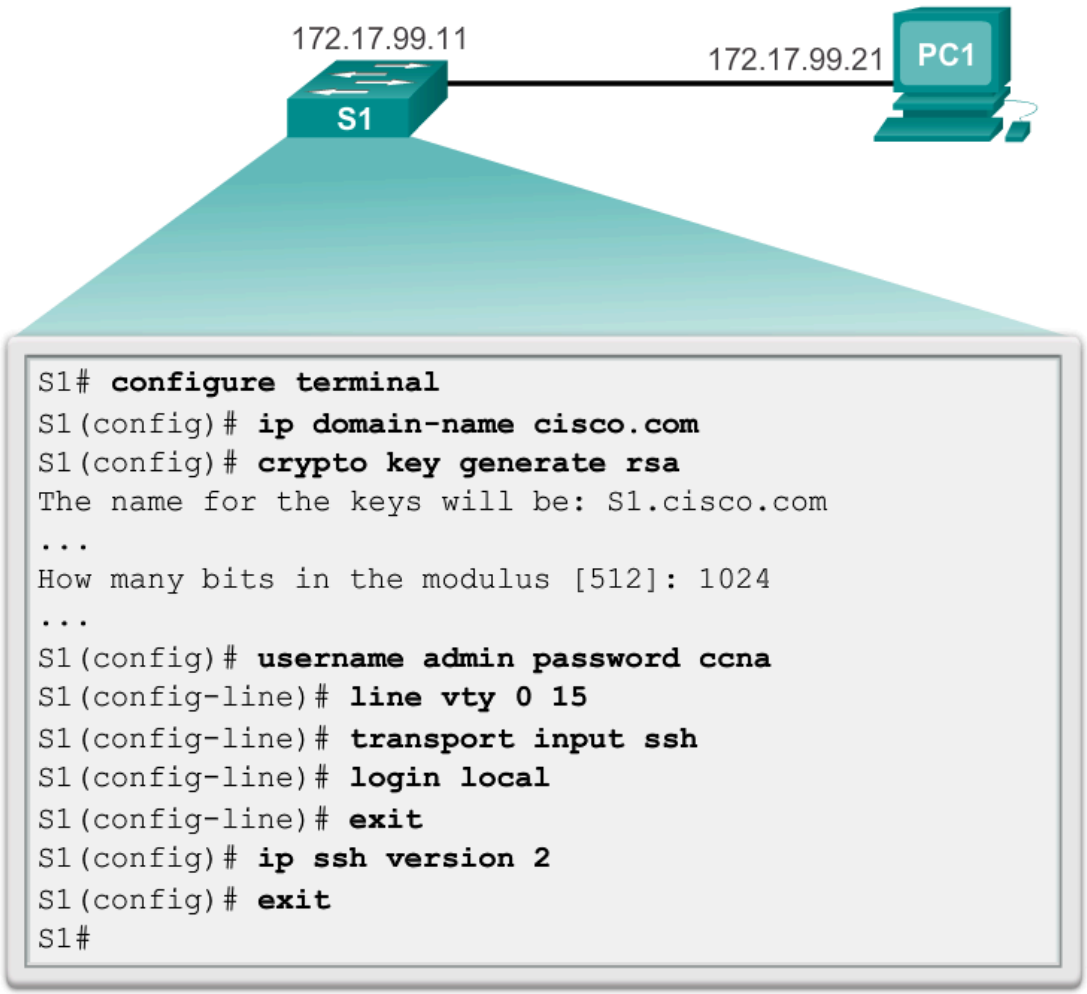
```
Login as: admin
Using keyboard-interactive
authentication.
Password:

S1>enable
Password:
S1#
```

Secure Remote Access

Configuring SSH

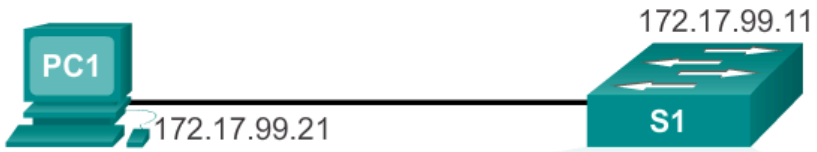
Configure SSH for Remote Management



Secure Remote Access

Verifying SSH

Verify SSH Status and Settings

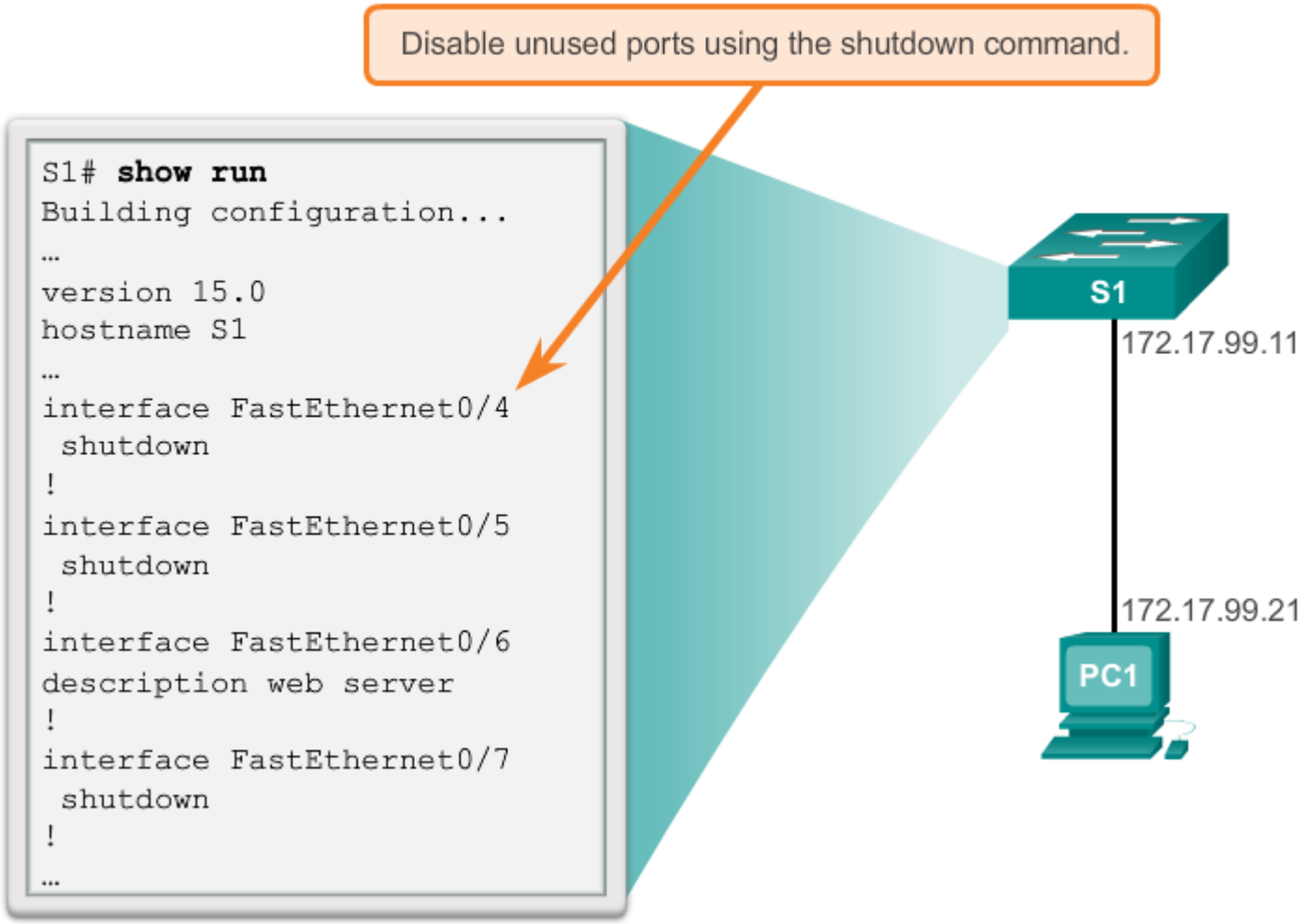



```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAa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

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

Secure Unused Ports

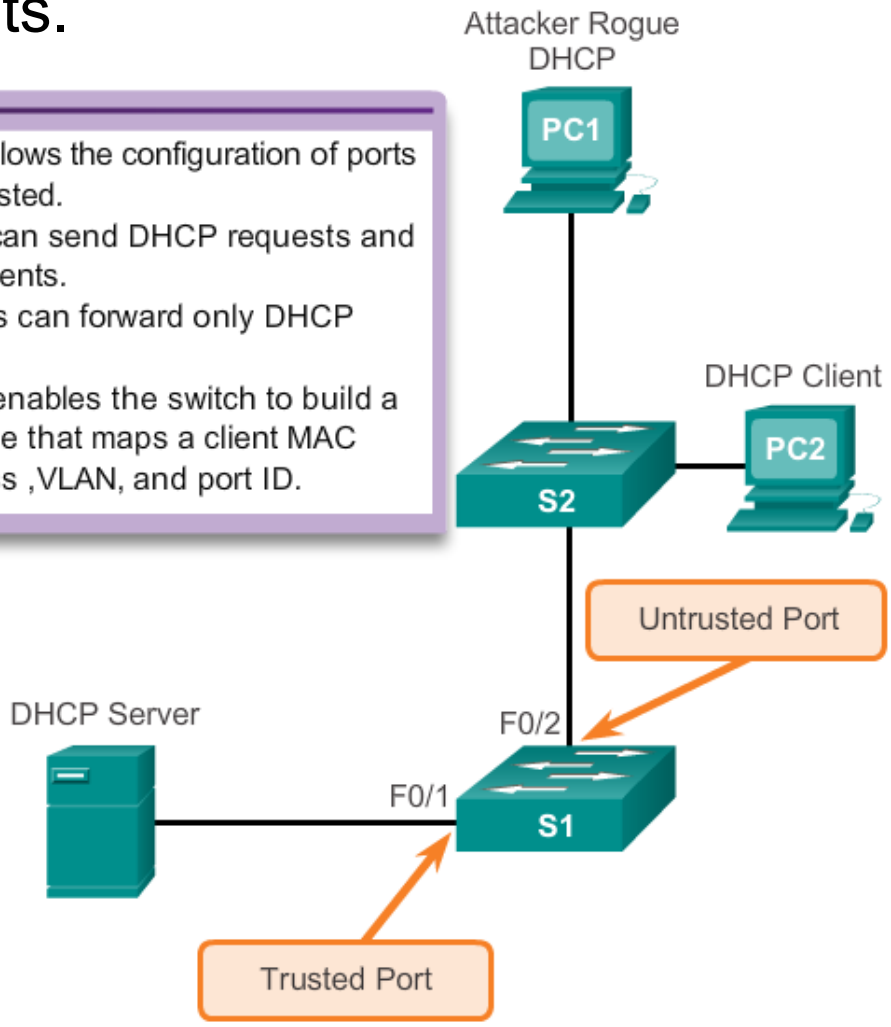
Disabling unused ports is a simple, yet efficient security practice.



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 acknowledgements.
  - 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
```

Port Security: Operation

- Port security limits the number of valid MAC addresses allowed on a port.
- 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

Port Security: Violation Modes

- The IOS software 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 be taken when a violation is detected:
  - Protect
  - Restrict
  - Shutdown

Port Security: Configuring

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.

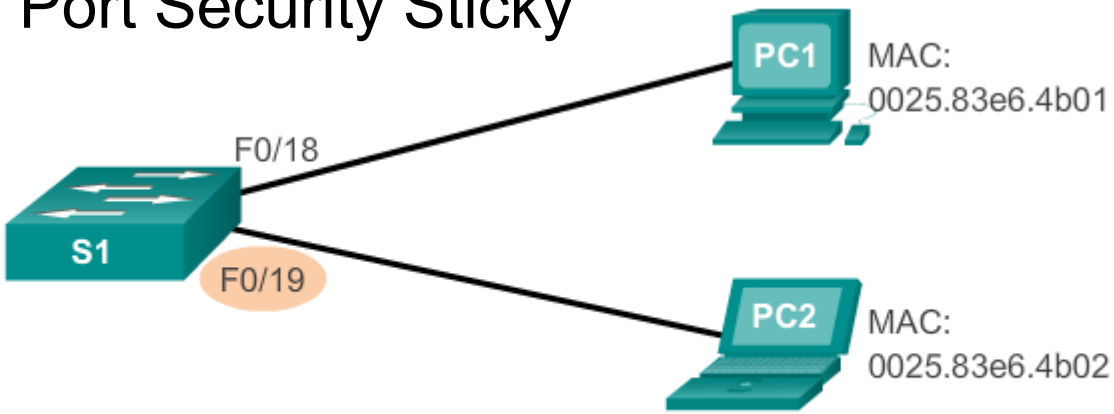
Port Security: Configuring (cont.)

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.

Port Security: Configuring (cont.)

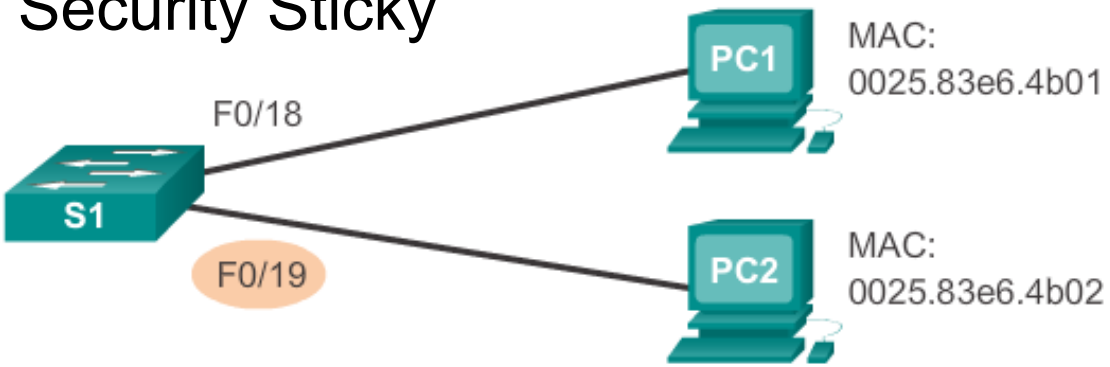
Configuring Port Security Sticky



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.

Port Security: Verifying

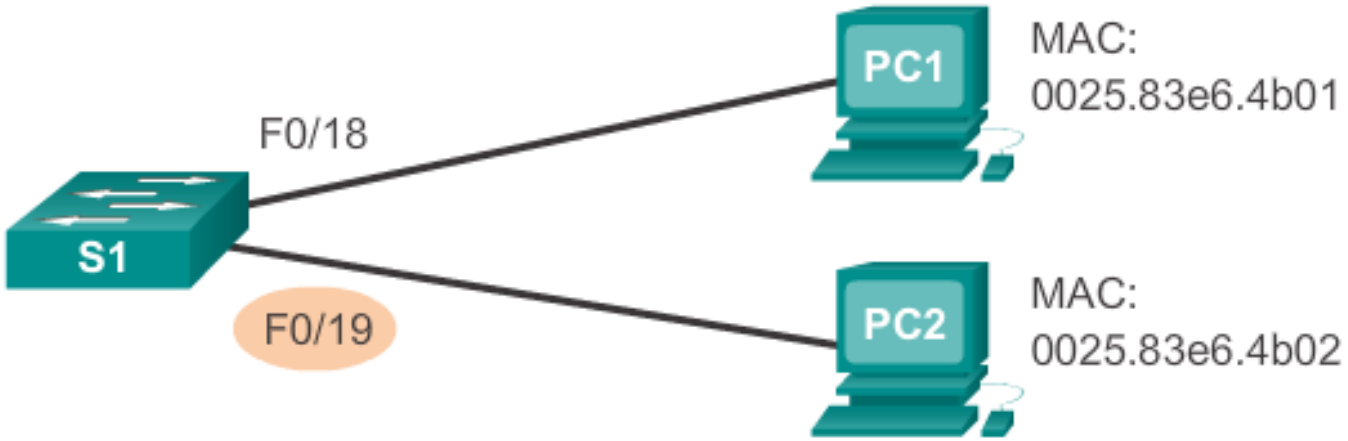
Verifying Port Security Sticky




```
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
```

Port Security: Verifying (cont.)

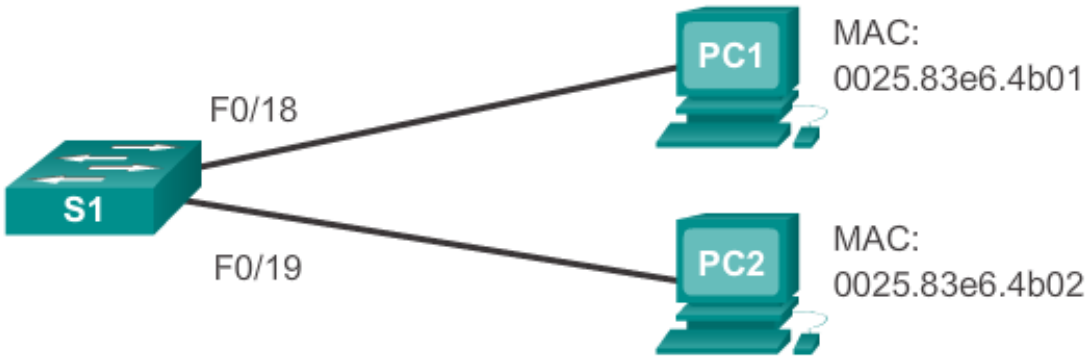
Verifying Port Security Sticky – Running Configuration




```
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
```

Port Security: Verifying (cont.)

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
```

Ports in Error-Disabled State

- A port security violation can put a switch in error-disabled state.
- A port in error-disabled state 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
```

Ports In Error Disabled State (cont.)

The **`show interface`** command also reveals a switch port on the 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
```

Ports In Error Disabled State (cont.)

A shutdown (or no shutdown) interface 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
```

Network Time Protocol (NTP)

- Having the correct time within networks is important.
- Correct time stamps are required to accurately track network events such as security violations.
- Clock synchronization is also critical for the interpretation of events within syslog data files as well as for digital certificates
- Network Time Protocol (NTP) is a protocol that is used to synchronize the clocks of computer systems over the network
- NTP allows network devices to synchronize their time settings with an NTP server.

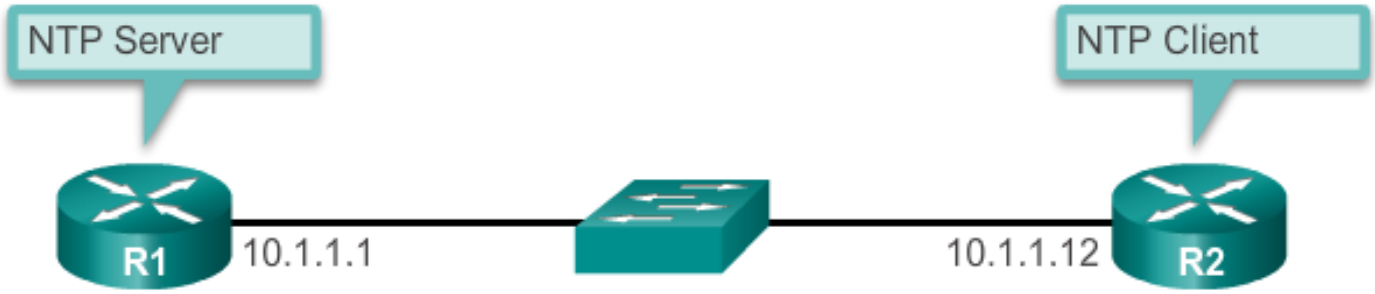
Network Time Protocol (NTP) (cont.)

- Some administrator prefer to maintain their own time source for increased security. However, public time sources are available on the Internet for general use.

- 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.

Network Time Protocol (NTP) (cont.)

- R2 is configured as a NTP client, receiving time updates from the server, R1.




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

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