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

Security Concerns in LANs

MAC Address Flooding

- Switches automatically populate their CAM tables by watching traffic entering their ports
- Switches will forward traffic trough all ports if it can’t 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.

Security Concerns in LANs

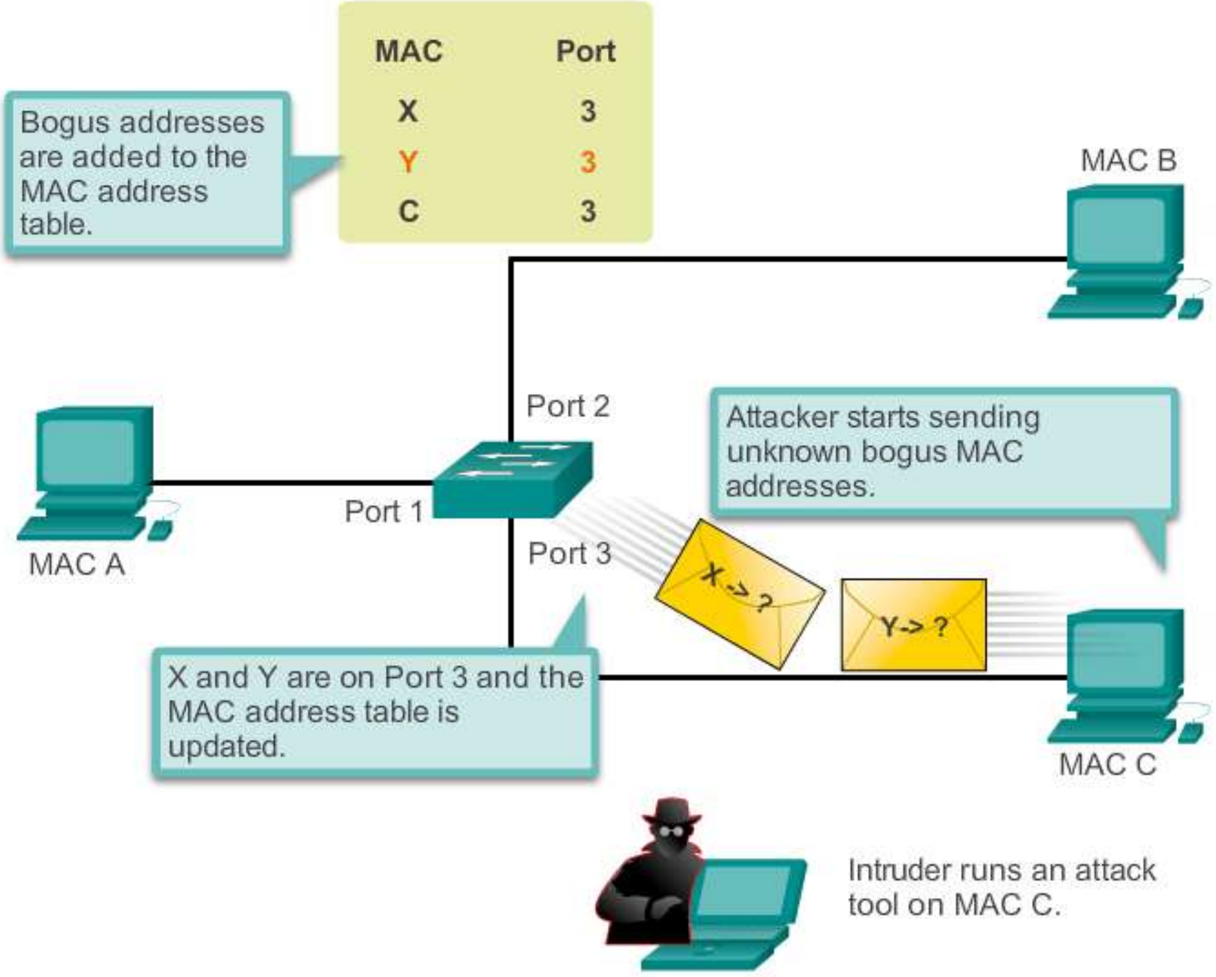
MAC Address Flooding

- 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
- 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 will never find 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

- 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.

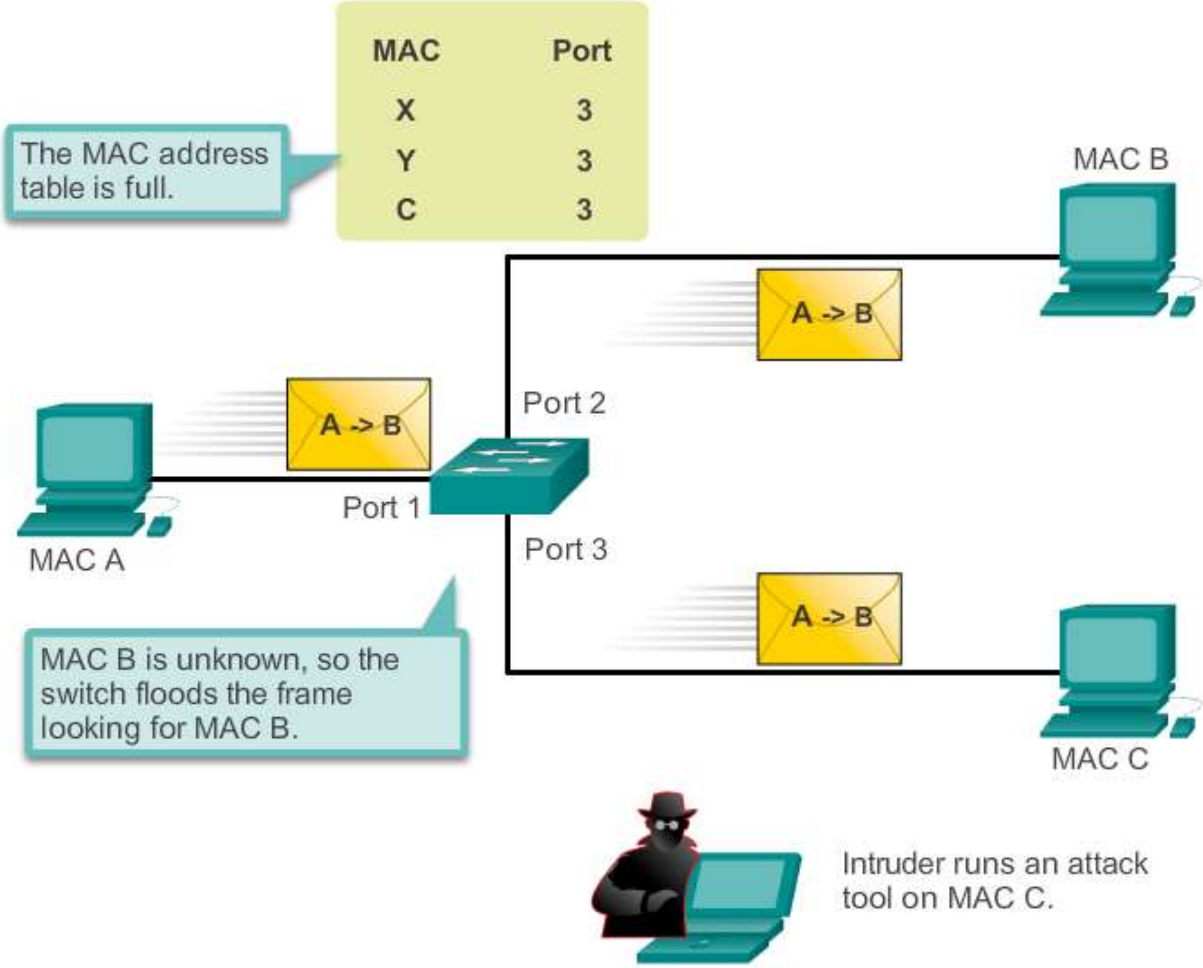
X and Y are on Port 3 and the MAC address table is updated.

Intruder runs an attack tool on MAC C.

Security Concerns in LANs

MAC Address Flooding

- 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

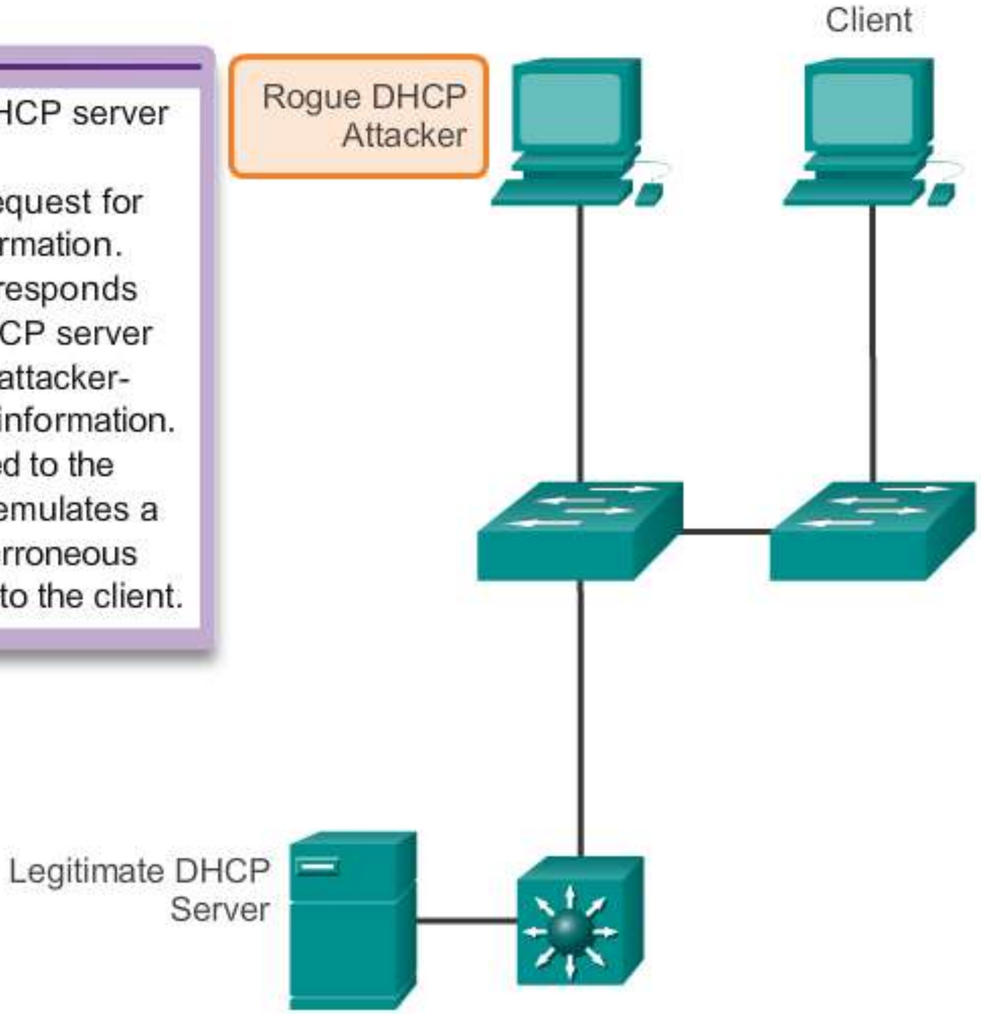
- DHCP is a network protocol used to assign IP info automatically
- Two types of DHCP attacks are:
  - DHCP spoofing
  - DHCP starvation
- In DHCP spoofing attacks, a fake DHCP server is placed in the network to issue DHCP addresses to clients.
- DHCP starvation is often used before a DHCP spoofing attack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

Security Concerns in LANs

DHCP Spoofing

- DHCP Spoof Attack

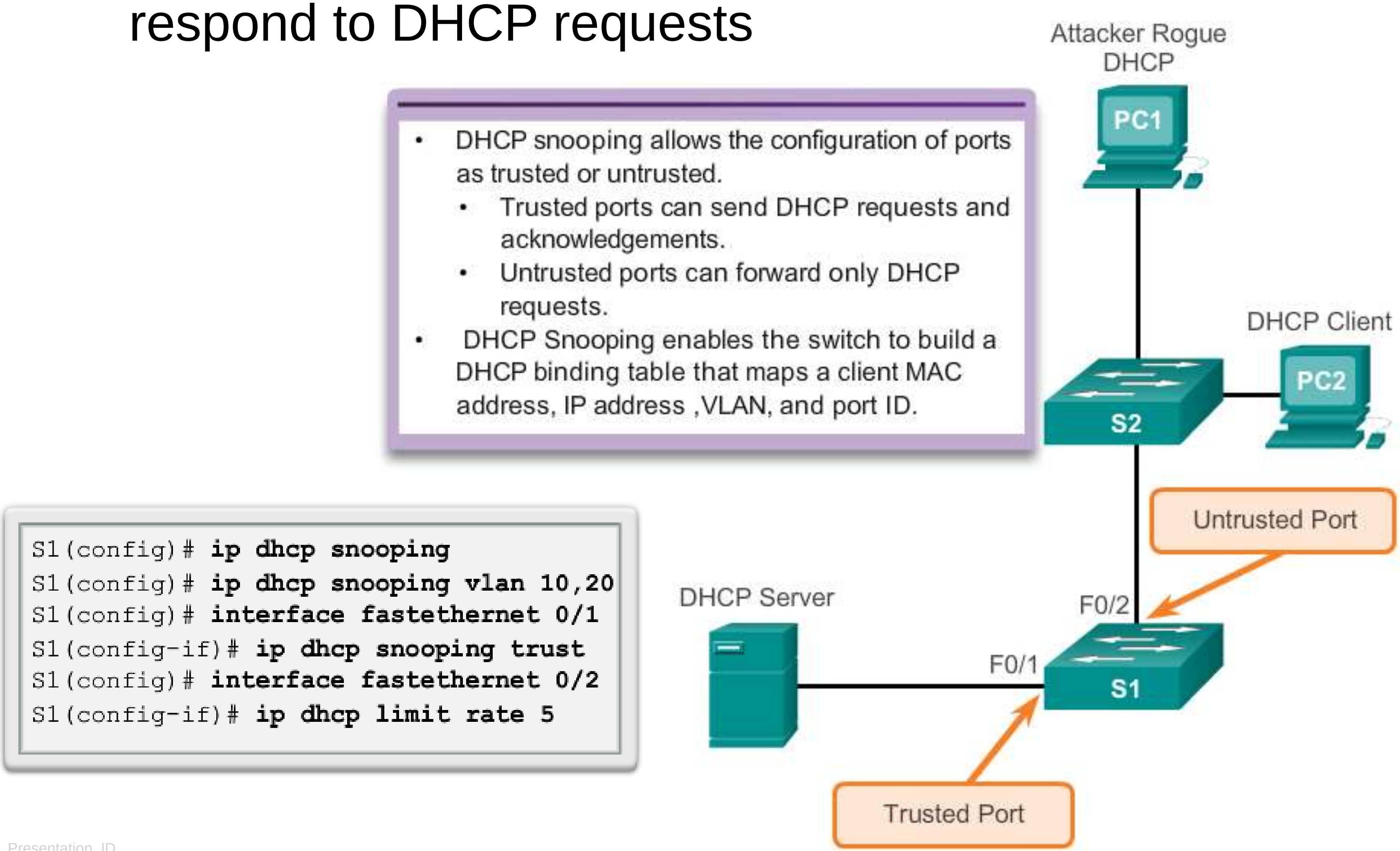
1) An attacker activates a DHCP server on a network segment.
2) The client broadcasts a request for DHCP configuration information.
3) The rogue DHCP server responds before the legitimate DHCP server can respond, assigning attacker-defined IP configuration information.
4) Host packets are redirected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



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 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
```

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 will 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

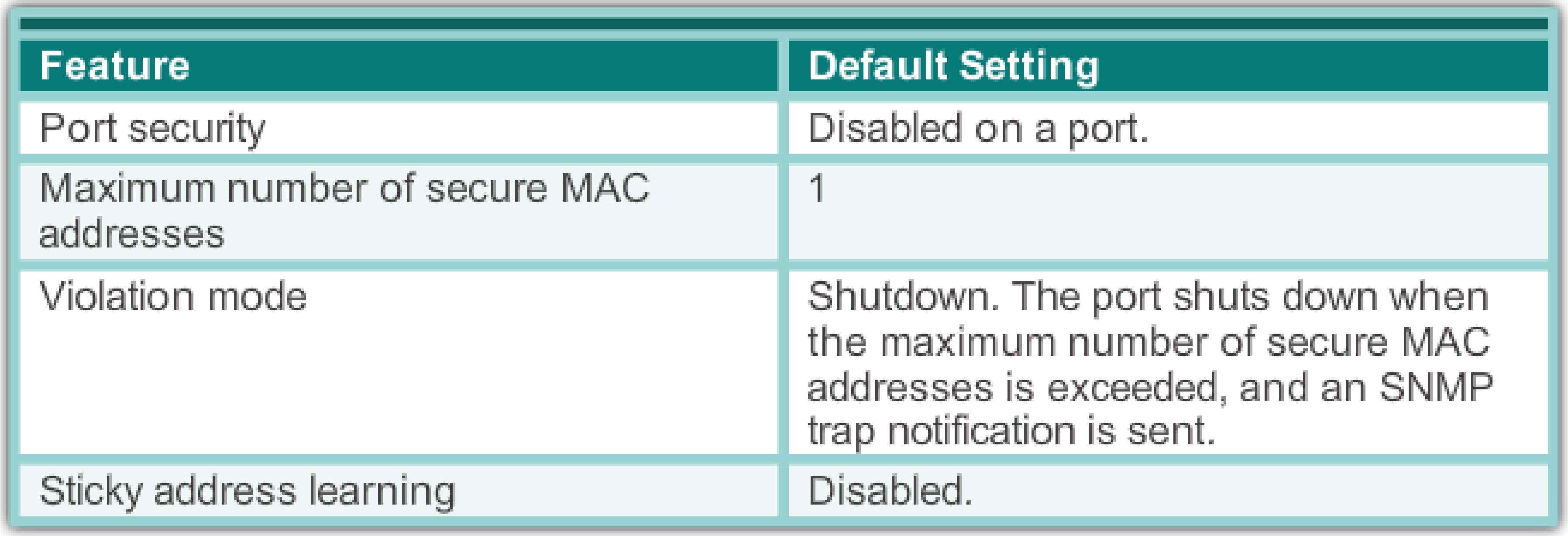
Port Security: Violation Modes

- 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 action to be taken when a violation is detected:
  - Protect
  - Restrict
  - Shutdown

Switch Port Security

Port Security: Configuring

- Dynamic Port Security Defaults

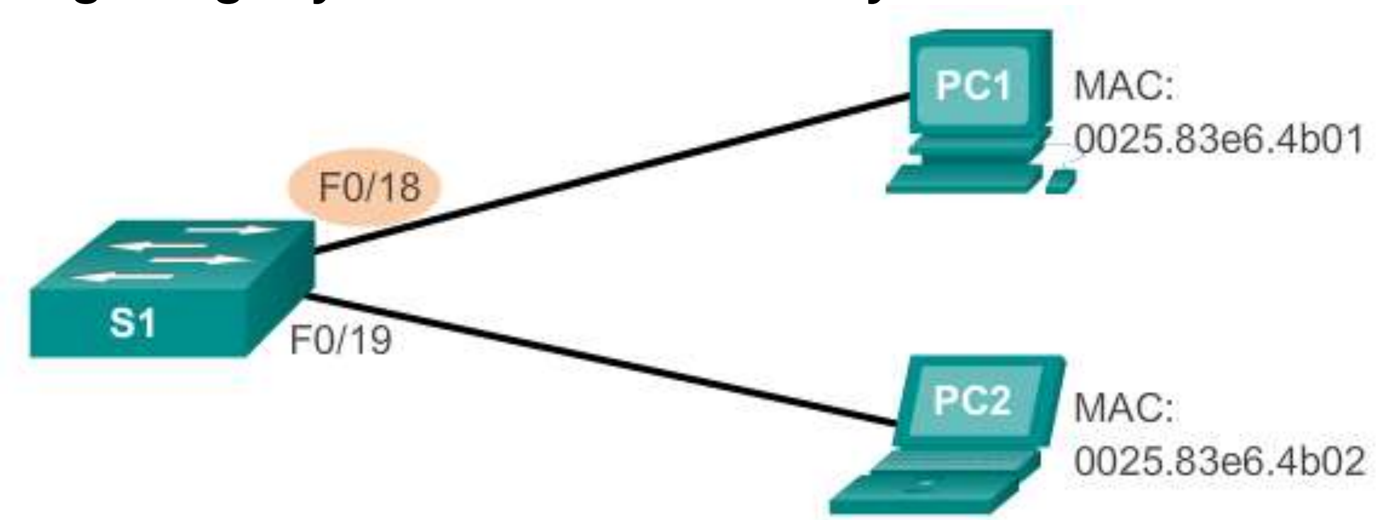


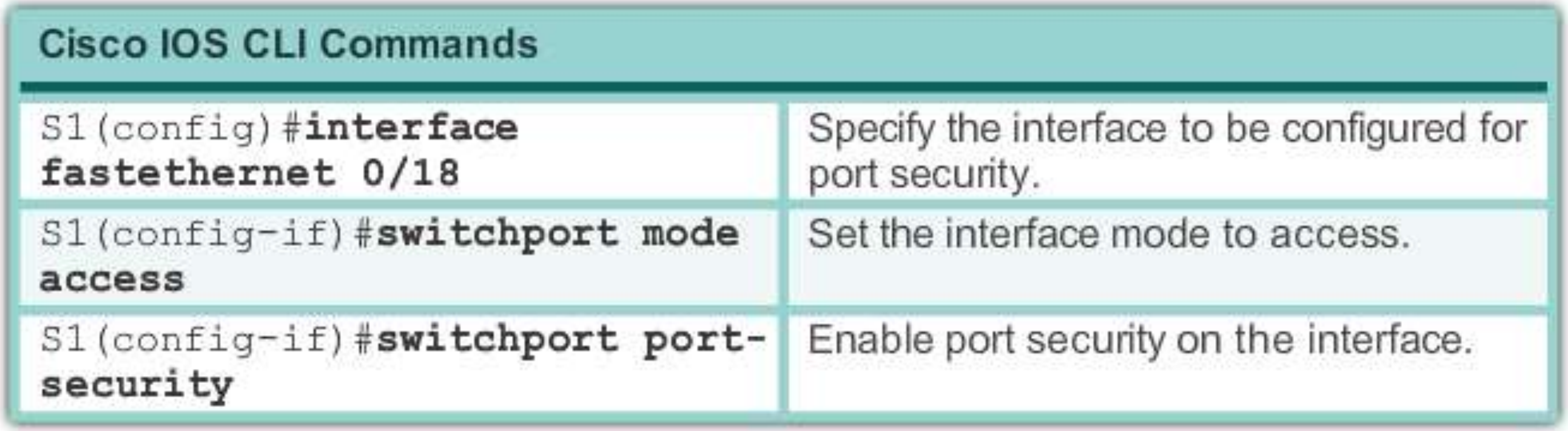
Feature	Default Setting
Port security	Disabled on a port.
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.
Sticky address learning	Disabled.

Switch Port Security

Port Security: Configuring

- Configuring Dynamic Port Security



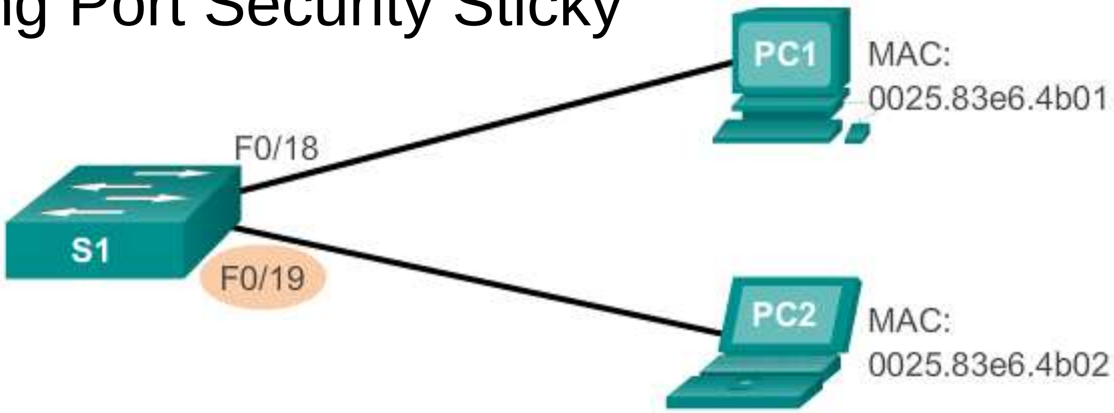


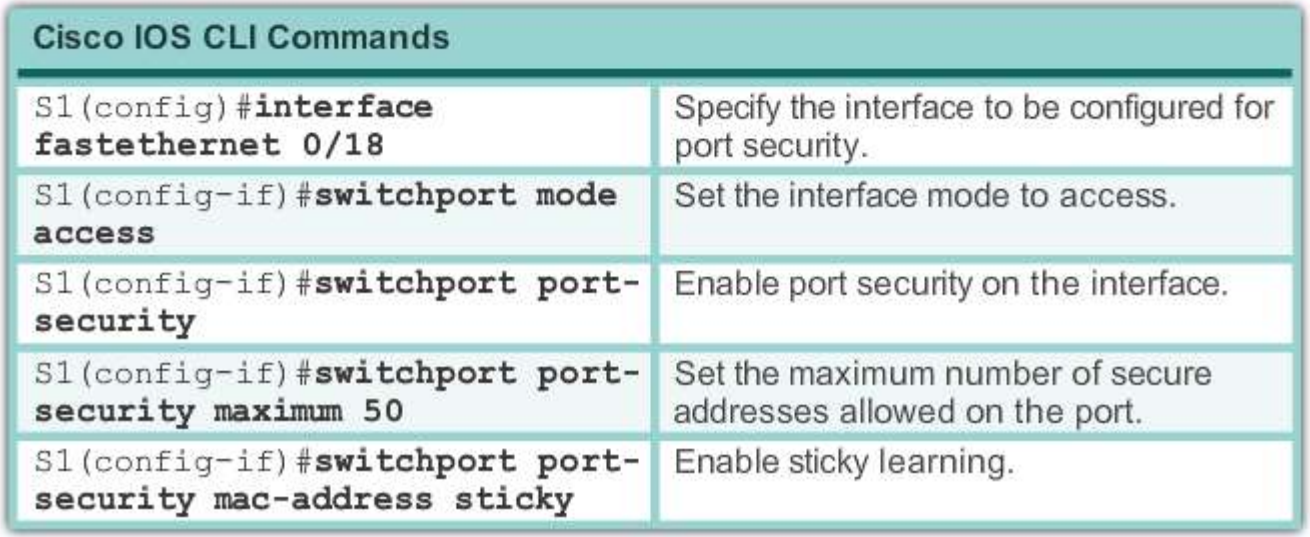
Cisco IOS CLI Commands	
`S1(config)#`**`interface fastethernet 0/18`**	Specify the interface to be configured for port security.
`S1(config-if)#`**`switchport mode access`**	Set the interface mode to access.
`S1(config-if)#`**`switchport port-security`**	Enable port security on the interface.

Switch Port Security

Port Security: Configuring

- Configuring Port Security Sticky





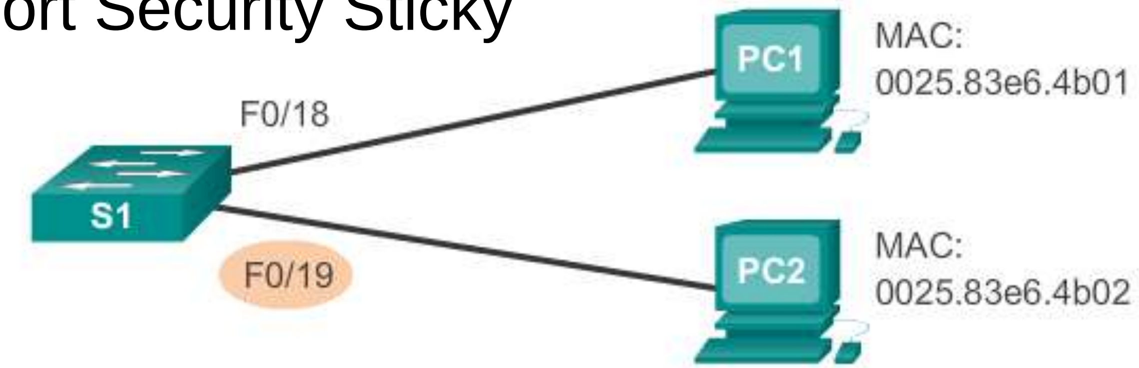
Cisco IOS CLI Commands

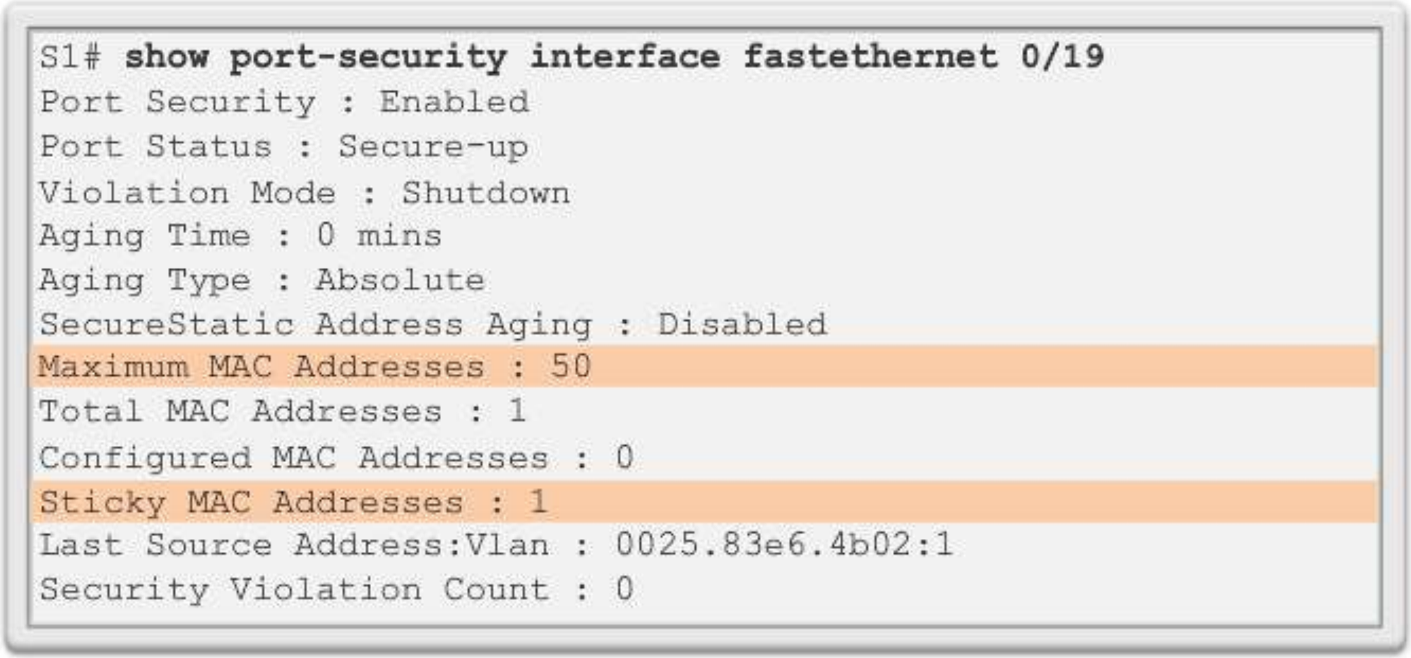
`S1(config)#`**`interface fastethernet 0/18`**	Specify the interface to be configured for port security.
`S1(config-if)#`**`switchport mode access`**	Set the interface mode to access.
`S1(config-if)#`**`switchport port-security`**	Enable port security on the interface.
`S1(config-if)#`**`switchport port-security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

Port Security: Verifying

- Verifying Port Security Sticky



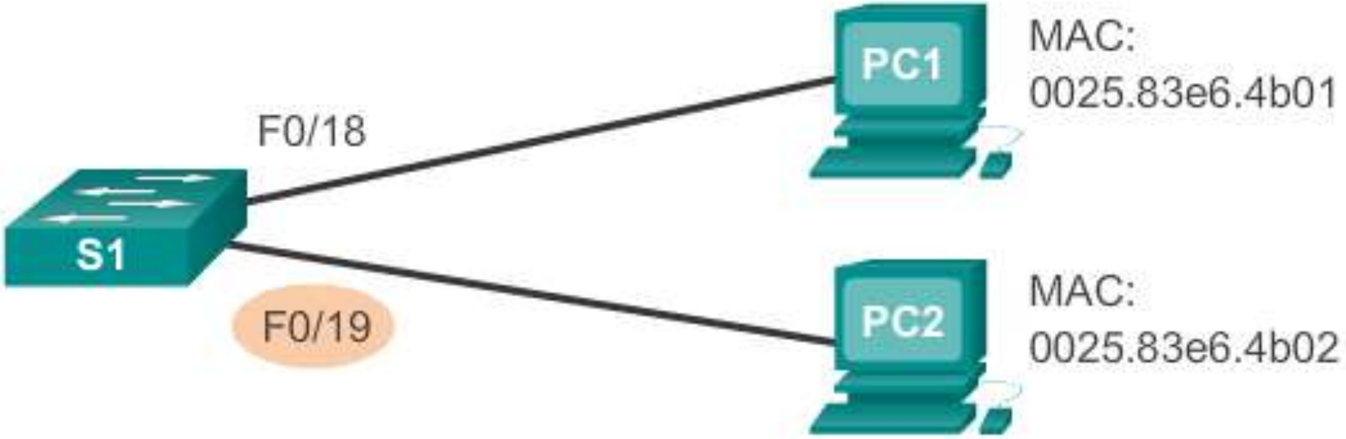


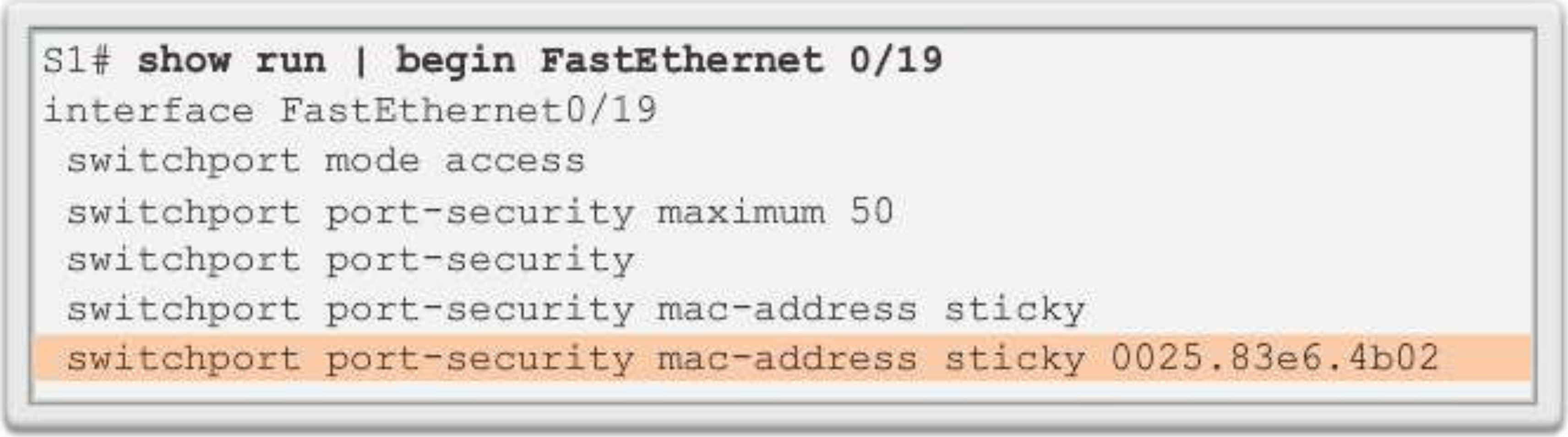
```
S1# show port-security interface fastethernet 0/19
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 50
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses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

Switch Port Security

Port Security: Verifying

- Verifying Port Security Sticky – Running Config

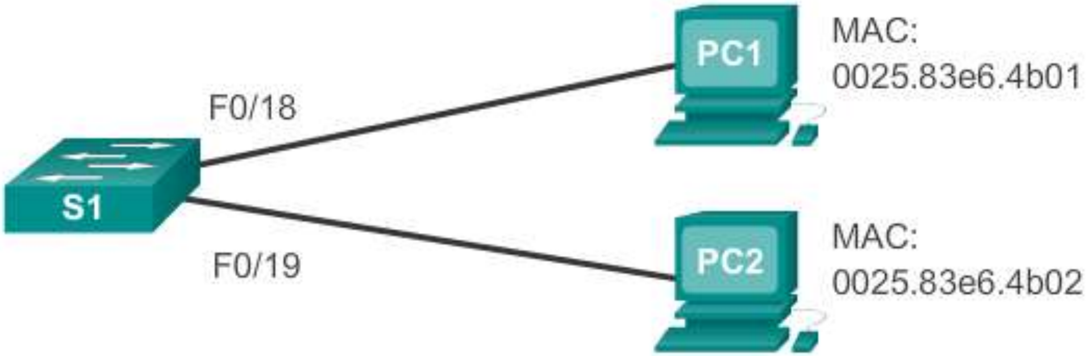


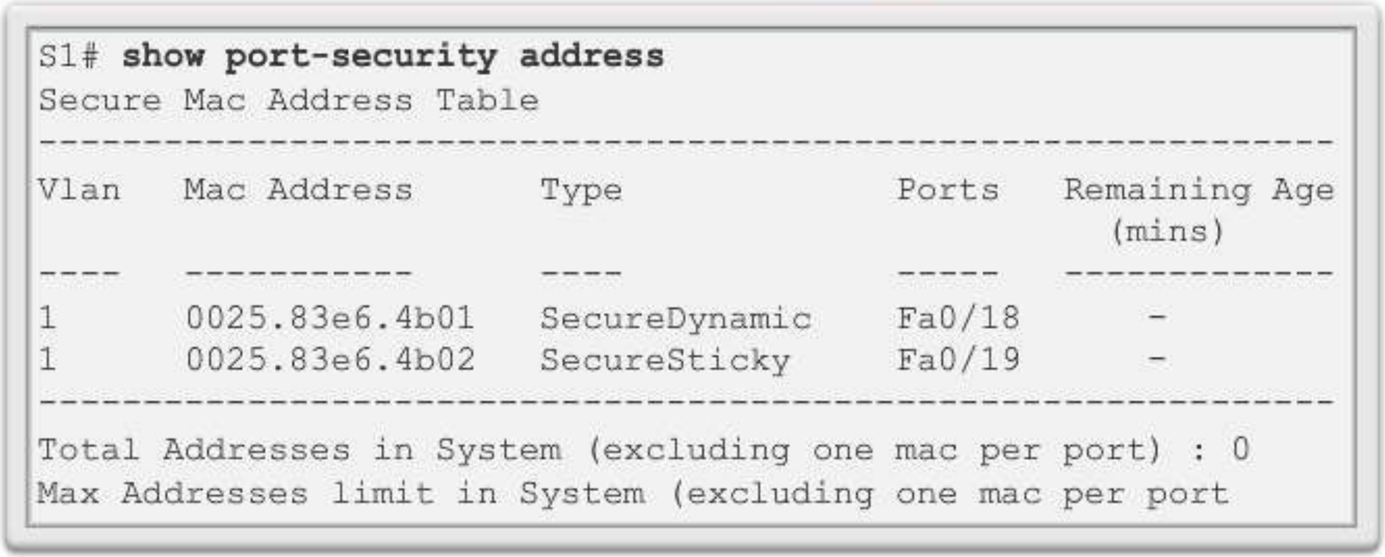


```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 50
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

Port Security: Verifying

- Verifying Port Security Secure MAC Addresses



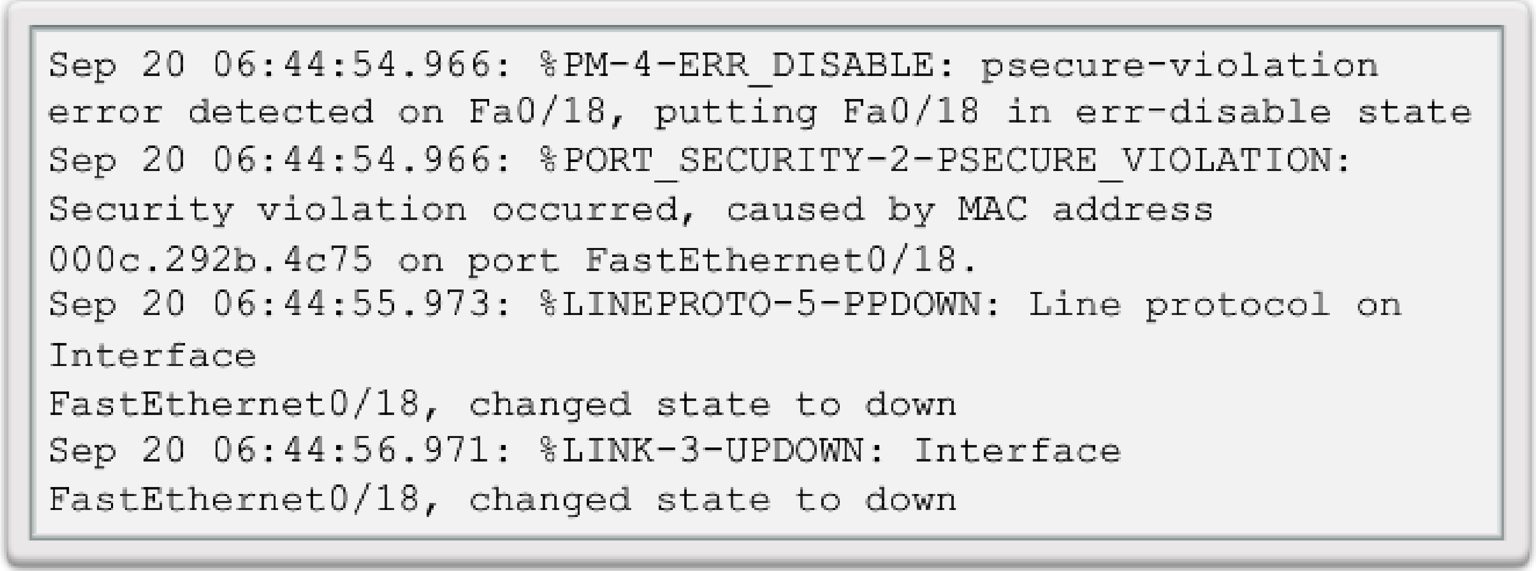


```
S1# show port-security address
Secure Mac Address Table
-------------------------------------------------------------
Vlan    Mac Address       Type                Ports    Remaining Age
                                                           (mins)
----    -----------       ----                -----    -------------
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 shut down
- The switch will communicate these events through console messages

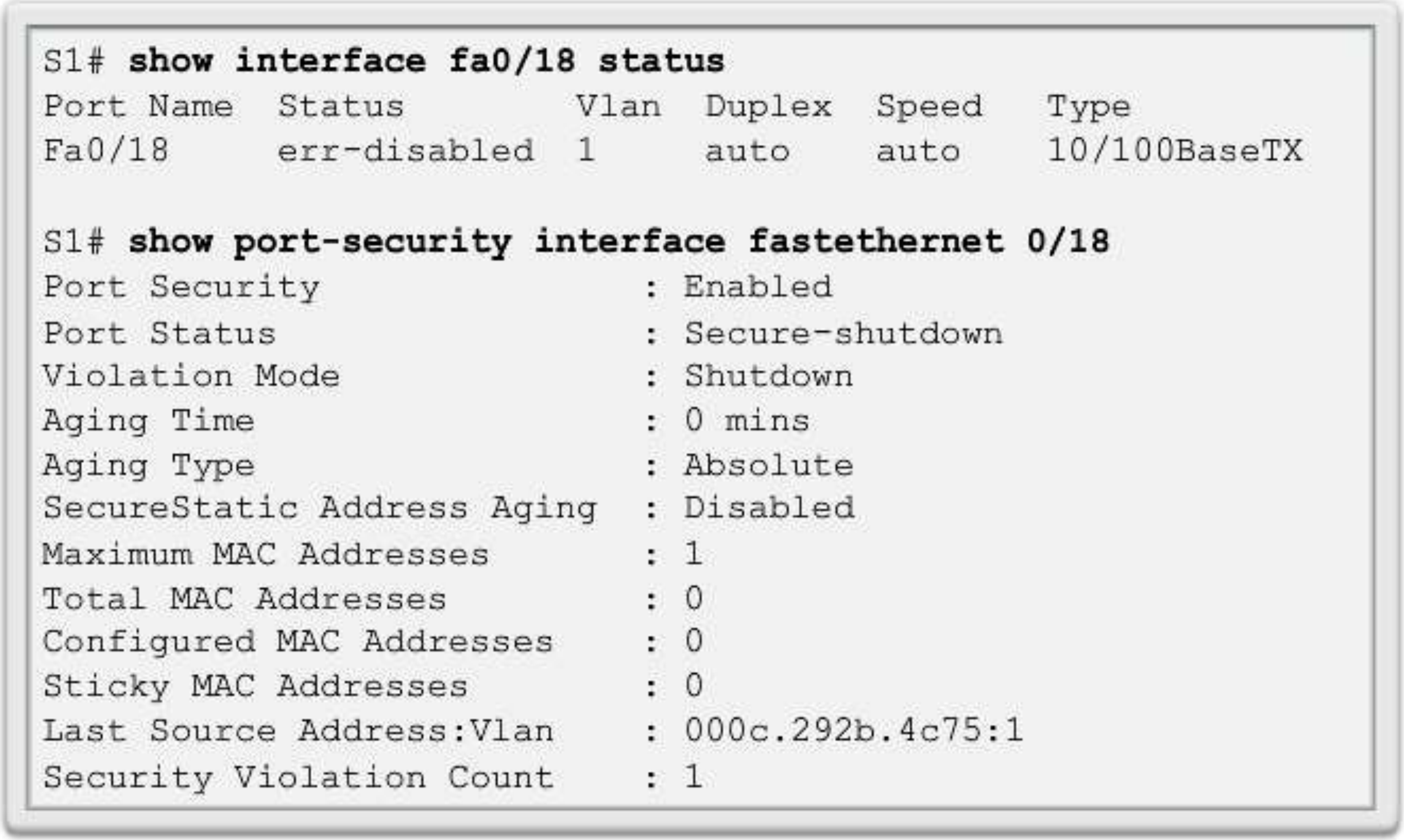


```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: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

- The show interface command also reveals a switch port on error disabled state



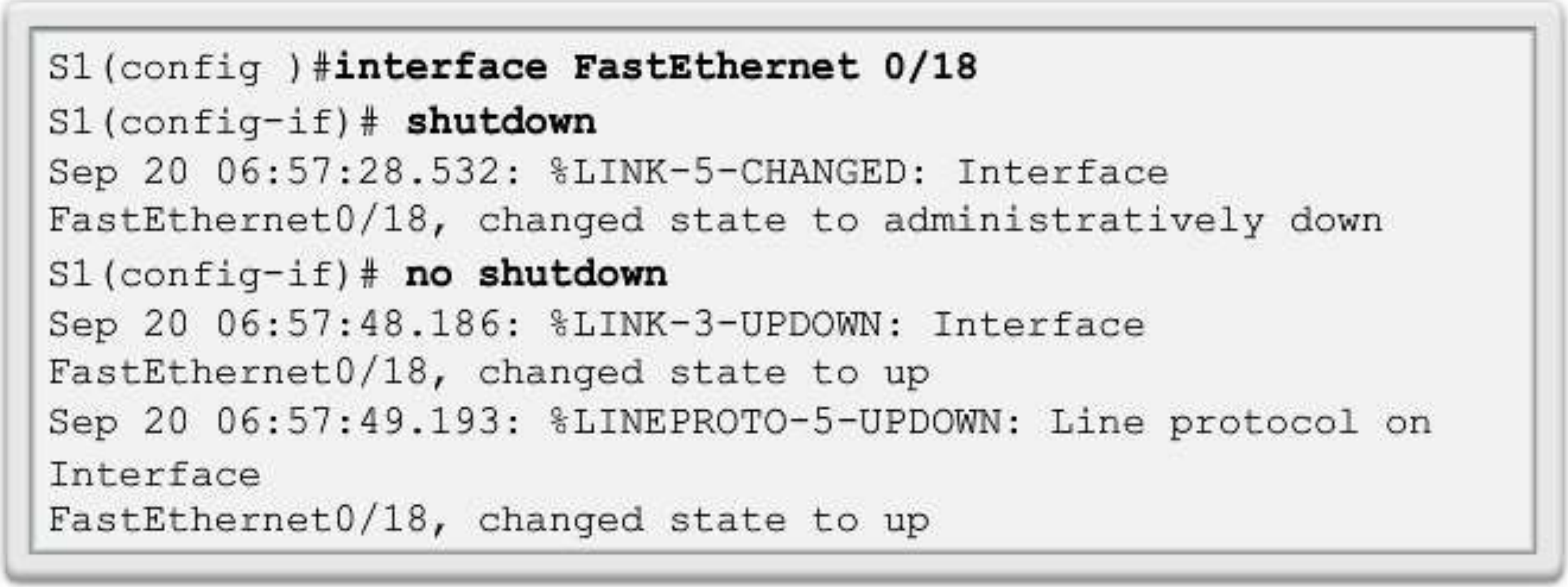
```
S1# show interface fa0/18 status
Port Name   Status         Vlan  Duplex  Speed   Type
Fa0/18      err-disabled   1     auto    auto    10/100BaseTX

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

- A shutdown/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
```

Cisco | Networking Academy®

Mind Wide Open™