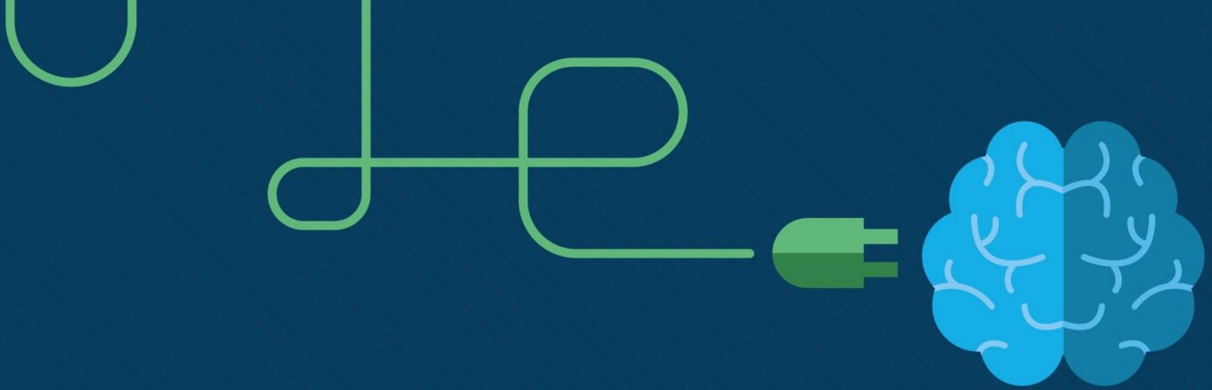


Chapter 5: Switch Configuration

CCNA Routing and Switching

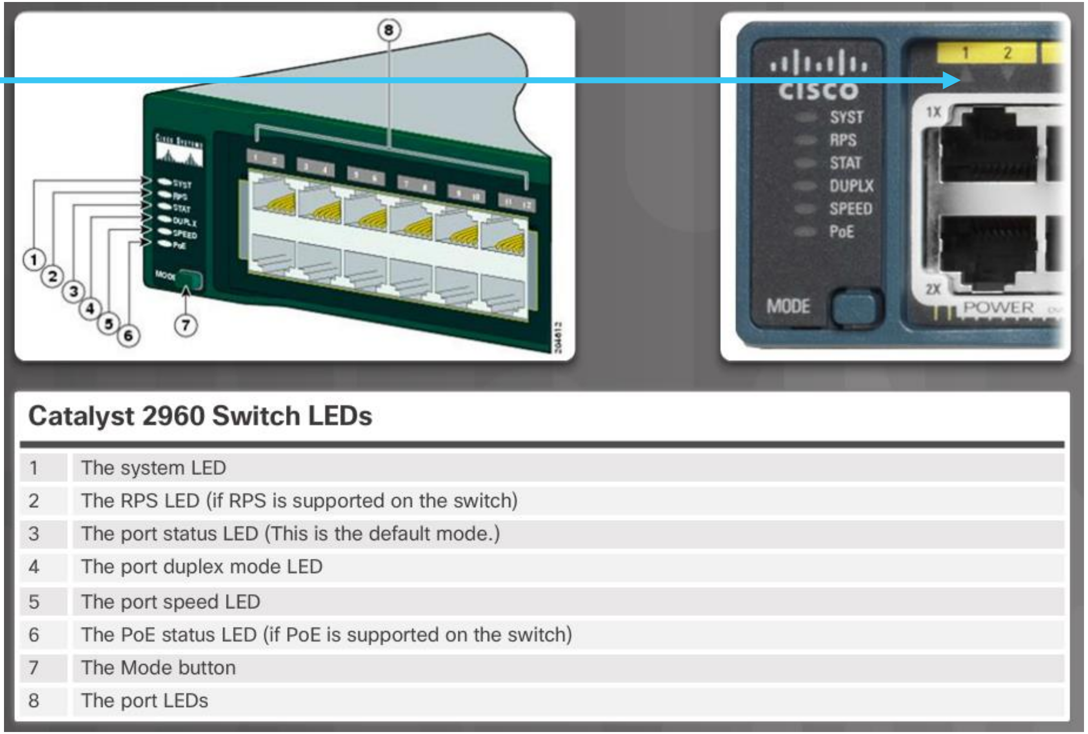
Routing and Switching
Essentials v6.0

5.1 Configure a Switch with Initial Settings

Configure a Switch with Initial Settings

Switch LED Indicators

- System LED shows if the switch has power applied.
- Port LED states:
  - Off – no link or shut down
  - Green – link is present ▲
  - Blinking green – data activity
  - Alternating green and amber – link fault ▲→▲→▲→▲
  - Amber – port is not sending data; common for first 30 seconds of connectivity or activation ▲
  - Blinking amber – port is blocking to prevent a switch loop



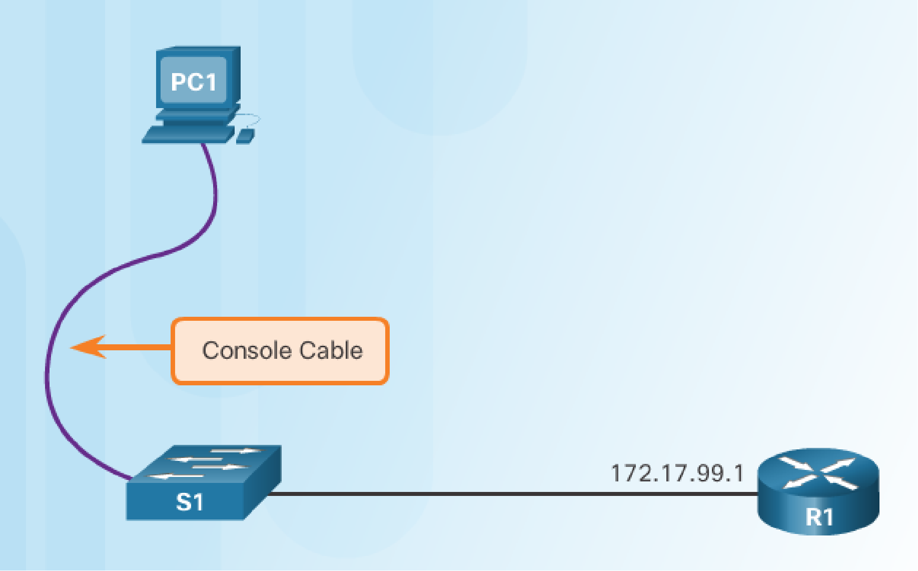
Catalyst 2960 Switch LEDs

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

Configure a Switch with Initial Settings

Preparing for Basic Switch Management

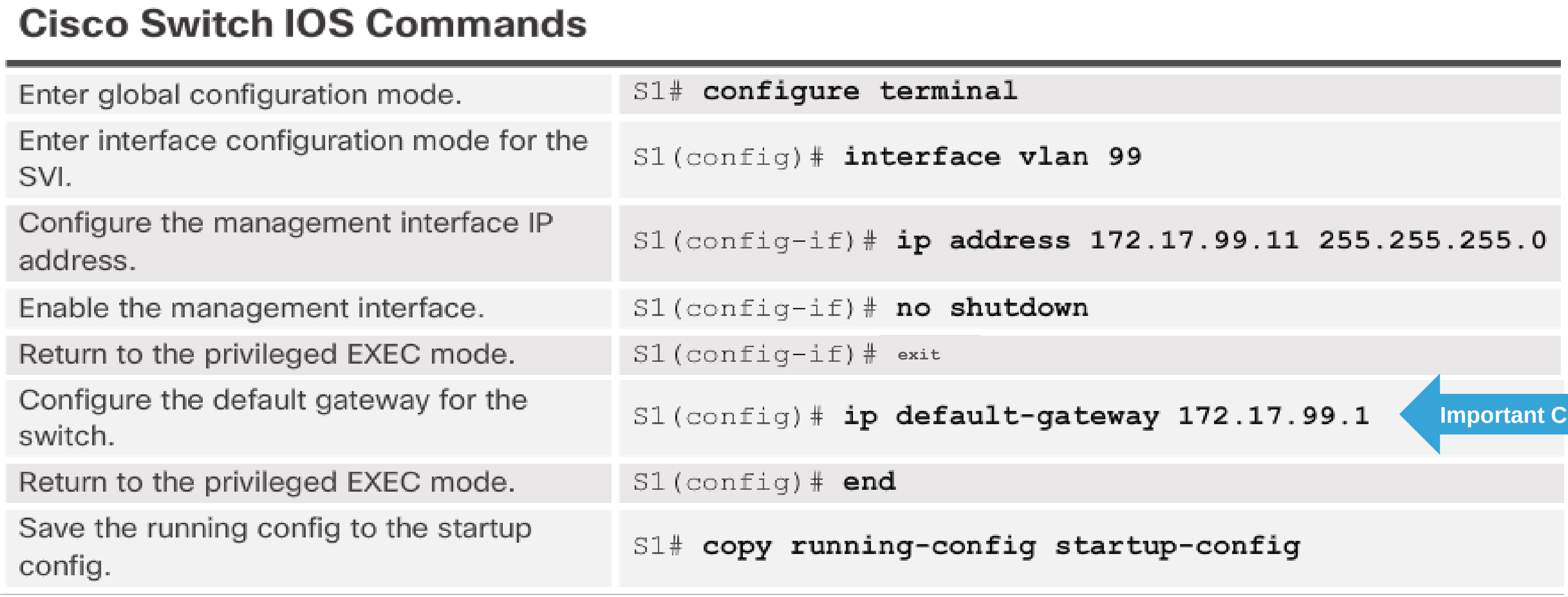
- To configure a switch for remote access, the switch must be configured with an IP address, subnet mask, and default gateway.
- One particular switch virtual interface (SVI) is used to manage the switch:
  - A switch IP address is assigned to an SVI.
  - By default the management SVI is controlled and configured through VLAN 1.
  - The management SVI is commonly called the management VLAN.
- For security reasons, it is best practice to use a VLAN other than VLAN 1 for the management VLAN.



Remember that the switch console port is on the back of the switch.

Configure a Switch with Initial Settings

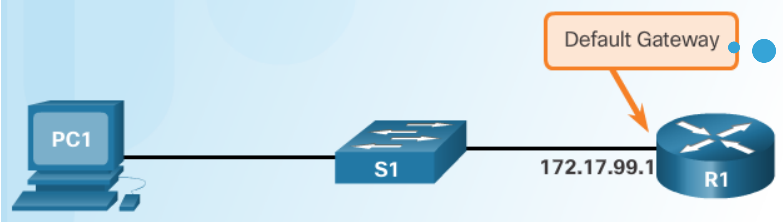
Configuring Basic Switch Management Access with IPv4



Cisco Switch IOS Commands

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 172.17.99.11 255.255.255.0**
Enable the management interface.	S1(config-if)# **no shutdown**
Return to the privileged EXEC mode.	S1(config-if)# exit
Configure the default gateway for the switch.	S1(config)# **ip default-gateway 172.17.99.1**
Return to the privileged EXEC mode.	S1(config)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

Important Concept



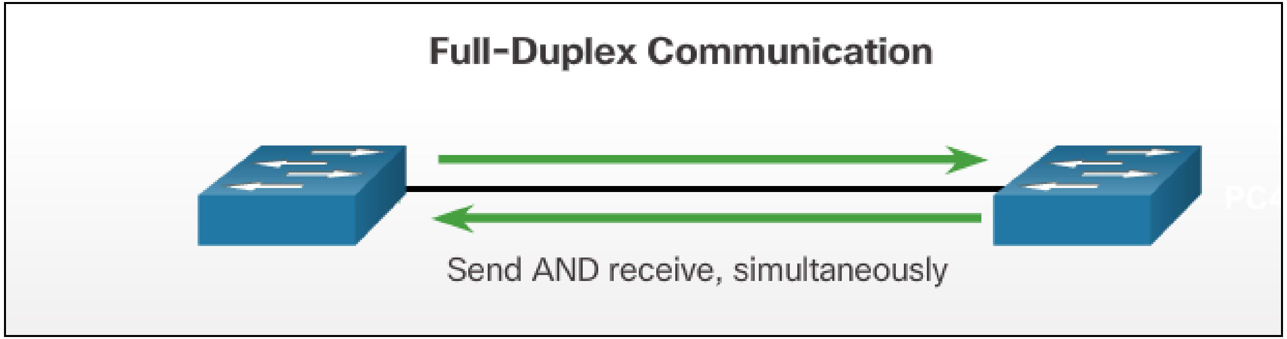
The default gateway is the router address and is used by the switch to communicate with other networks.

Configure Switch Ports

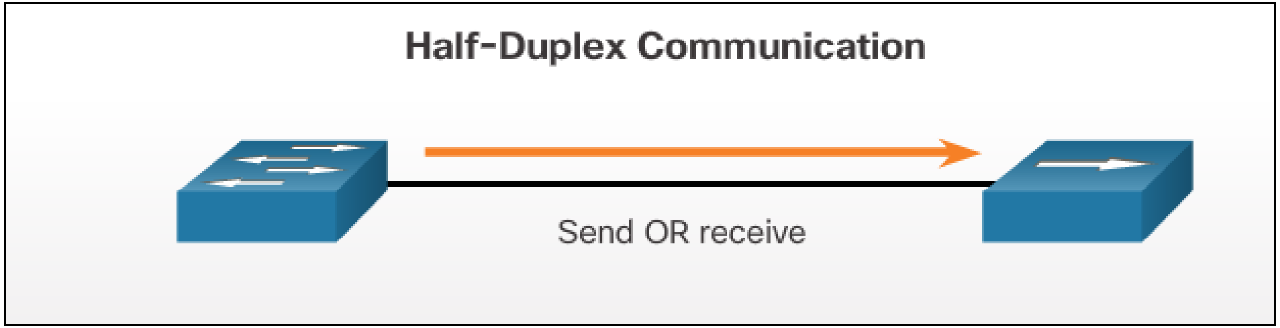
Duplex Communication

- Gigabit Ethernet and 10Gb Ethernet NICs require full-duplex connections to operate.

Bidirectional communication

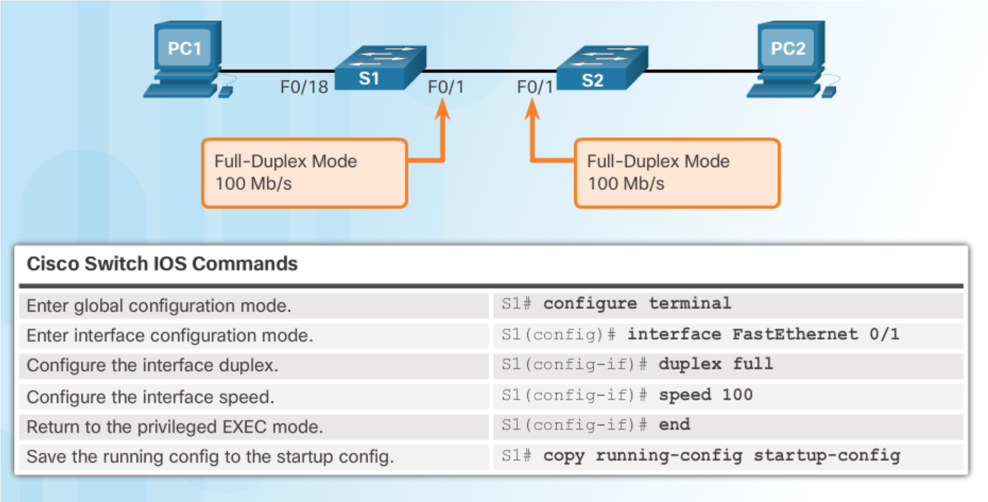


Unidirectional communication



Configure Switch Ports at the Physical Layer

- Some switches have the default setting of auto for both duplex and speed.
- Mismatched duplex and/or speed settings can cause connectivity issues.
- Always check duplex and speed settings using the **show interface** *interface_id* command.
- All fiber ports operate at one speed and are always full-duplex.



Full-Duplex Mode
100 Mb/s

Full-Duplex Mode
100 Mb/s

Cisco Switch IOS Commands

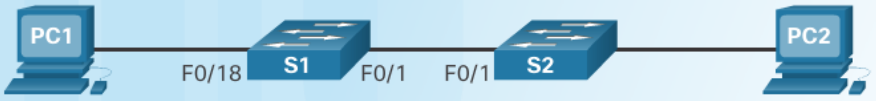
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface FastEthernet 0/1`
Configure the interface duplex.	`S1(config-if)# duplex full`
Configure the interface speed.	`S1(config-if)# speed 100`
Return to the privileged EXEC mode.	`S1(config-if)#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

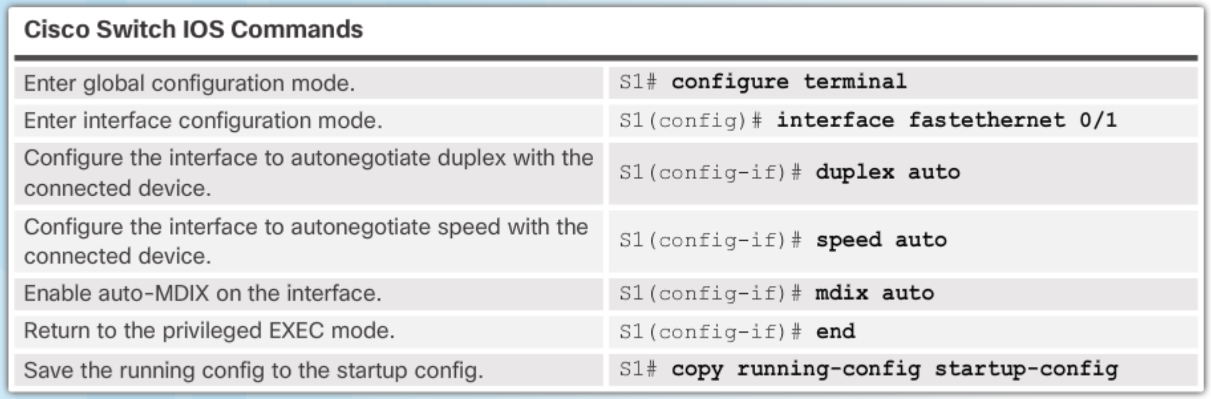
Configure Switch Ports

Auto-MDIX

- Some switches have the automatic medium-dependent interface crossover (auto-MDIX) feature that allows an interface to detect the required cable connection type (straight-through or crossover) and configure the connection appropriately.

Configure auto-MDIX



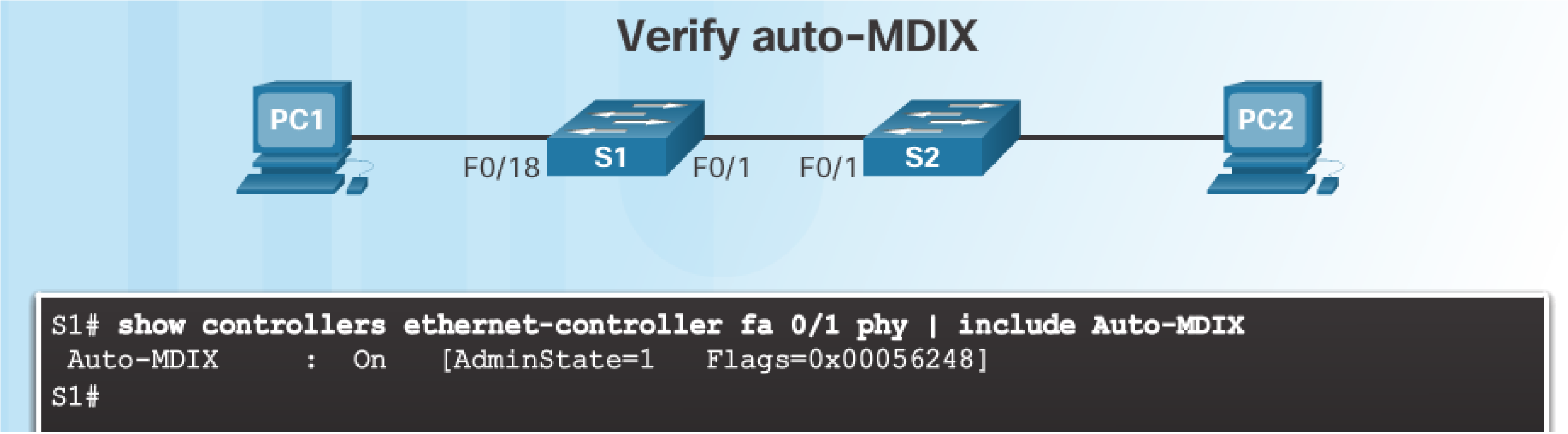


Cisco Switch IOS Commands

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`

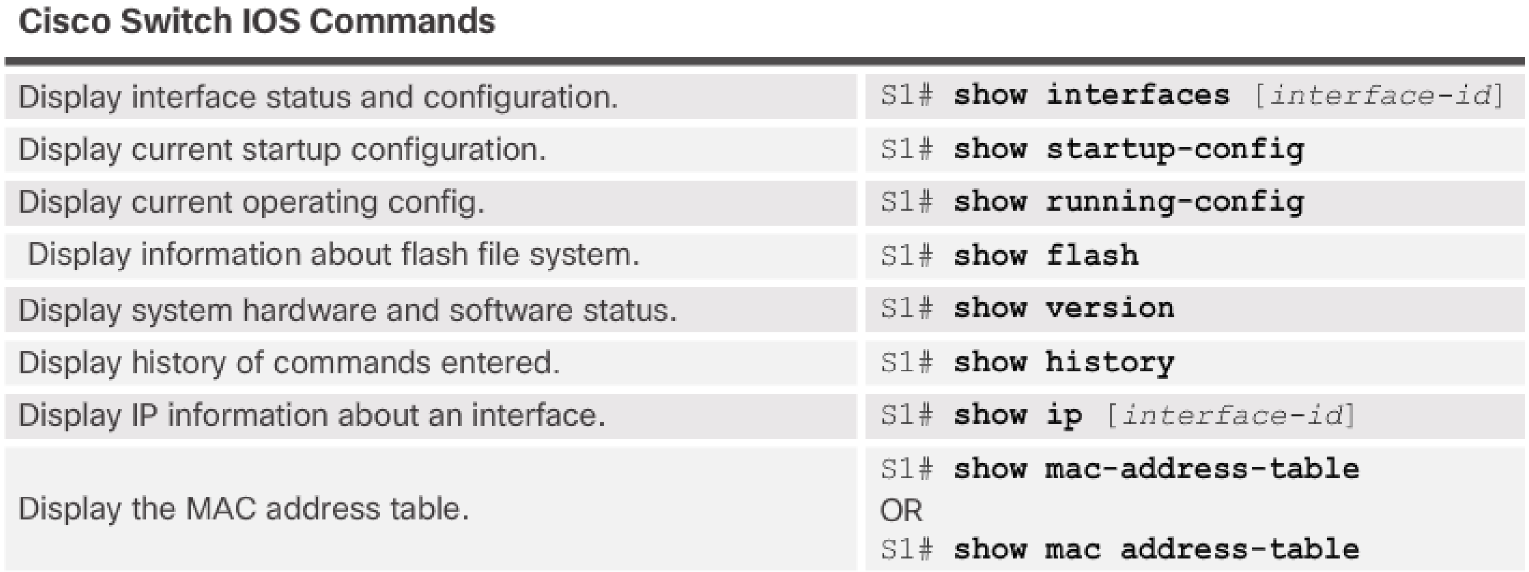
Auto-MDIX (Cont.)

- Use the **show controllers Ethernet-controller** command to verify auto-MDIX settings.



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

Verifying Switch Port Configuration



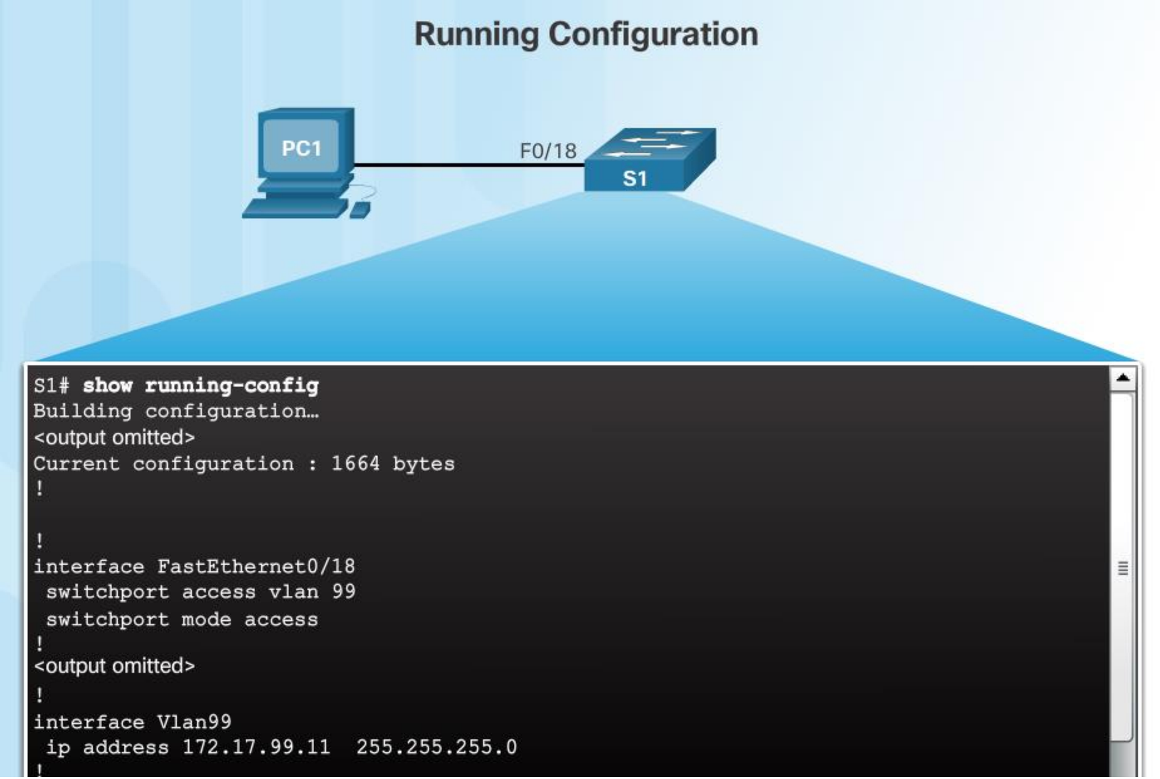
Cisco Switch IOS Commands

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`**

Configure Switch Ports

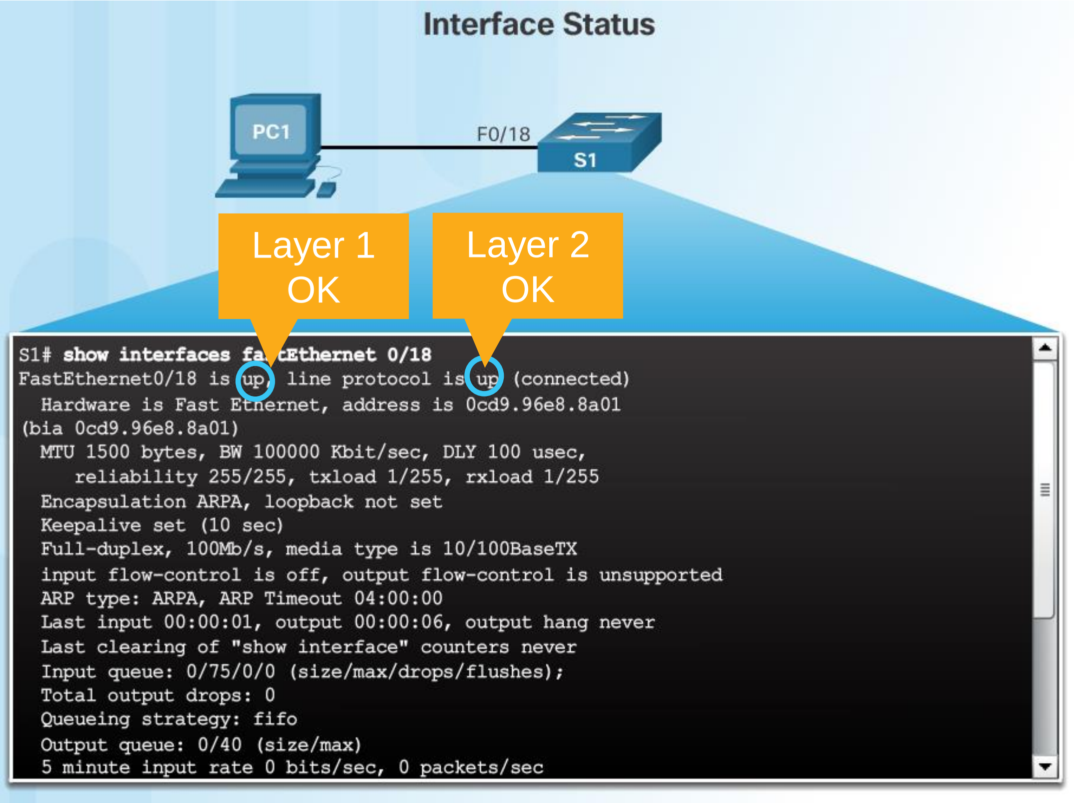
Verifying Switch Port Configuration (Cont.)



Running Configuration

```
S1# show running-config
Building configuration…
<output omitted>
Current configuration : 1664 bytes
!

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

Verifying Switch Port Configuration (Cont.)

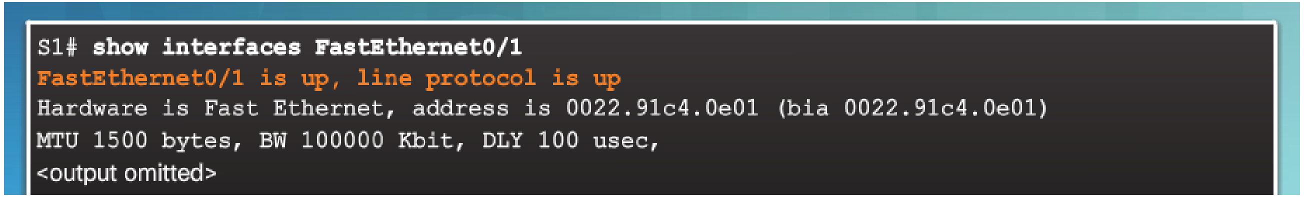


```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96e8.8a01
(bia 0cd9.96e8.8a01)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes);
  Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
```

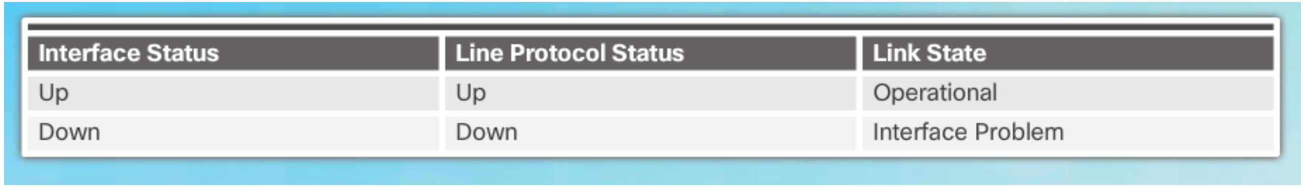
Configure Switch Ports

Network Access Layer Issues

- Use the **show interfaces** command to detect common media issues.
- The first parameter refers to Layer 1, the physical layer, and indicates if the interface is receiving a carrier detect signal.
- The second parameter (protocol status) refers to the data link layer and indicates whether the data link layer protocol has been configured correctly and keepalives are being received.



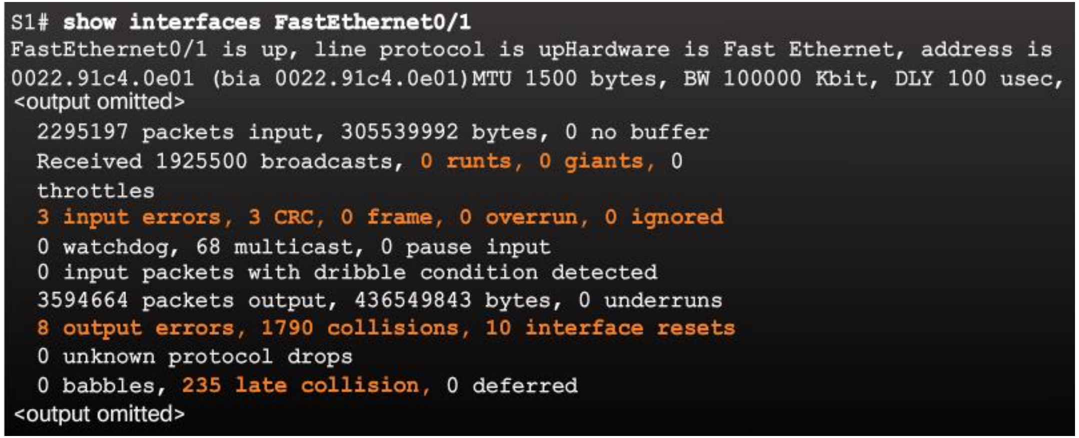
```
S1# show interfaces FastEthernet0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<output omitted>
```



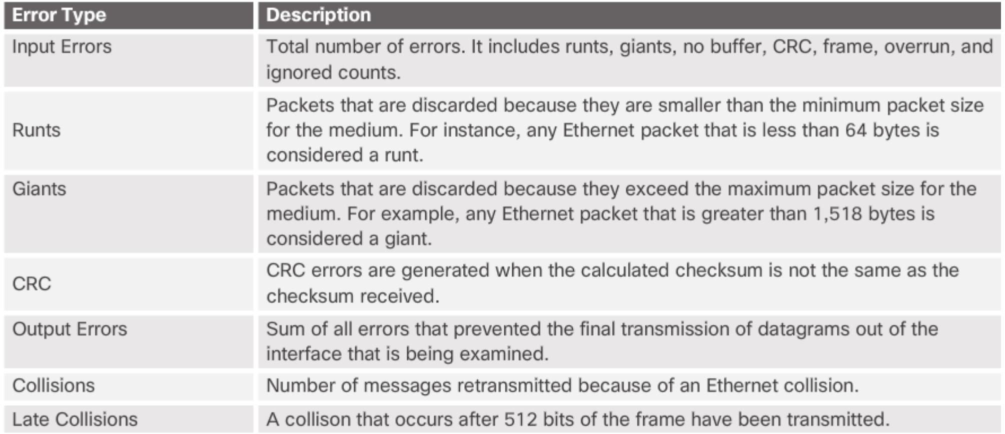
Interface Status	Line Protocol Status	Link State
Up	Up	Operational
Down	Down	Interface Problem

Configure Switch Ports

Network Access Layer Issues (Cont.)



```
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>
```



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

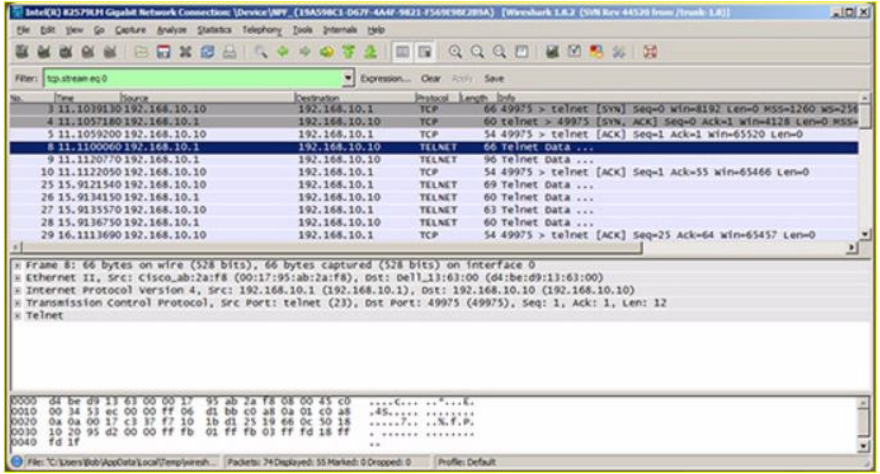
5.2 Switch Security

Secure Remote Access

SSH Operation

- Secure Shell (SSH)
  - An alternative protocol to Telnet. Telnet uses unsecure plaintext of the username and password as well as the data transmitted.
  - SSH is more secure because it provides an encrypted management connection.

Wireshark Capture of Telnet



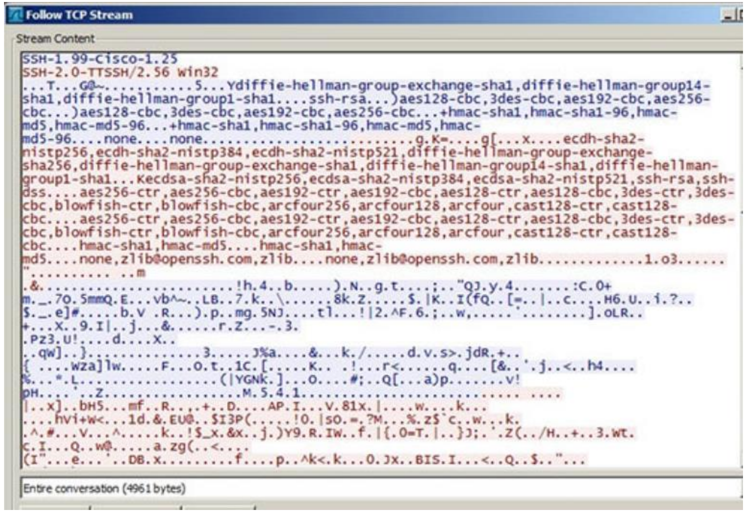
Intel(R) 82579LM Gigabit Network Connection: \Device\NPF_{19A598C1-D67F-4A4F-9821-F569E98E2B9A} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]

Filter: tcp.stream eq 0

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

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

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

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

Wireshark Capture of SSH



Follow TCP Stream

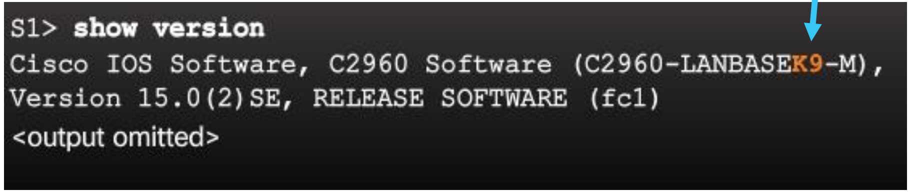
Stream Content

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

Entire conversation (4961 bytes)

SSH Operation (Cont.)

- A switch must have an IOS version (k9 at the end of the IOS file name) that includes cryptographic capabilities in order to configure and use SSH.
  - Use the **show version** command to see the IOS version.



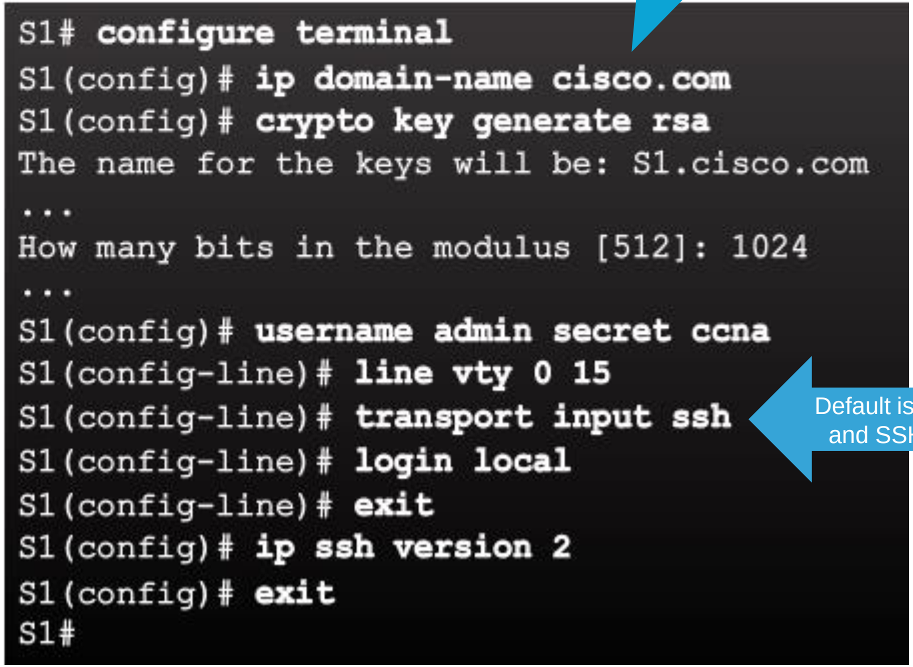
```
S1> show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M),
Version 15.0(2)SE, RELEASE SOFTWARE (fc1)
<output omitted>
```

Secure Remote Access

Configuring SSH

1. Verify SSH support.
2. Configure the IP domain name.
3. Generate RSA key pairs.
4. Configure user authentication.
5. Configure the vty lines.
6. Enable SSH version 2.

Commonly forgotten command that is used in key generation



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

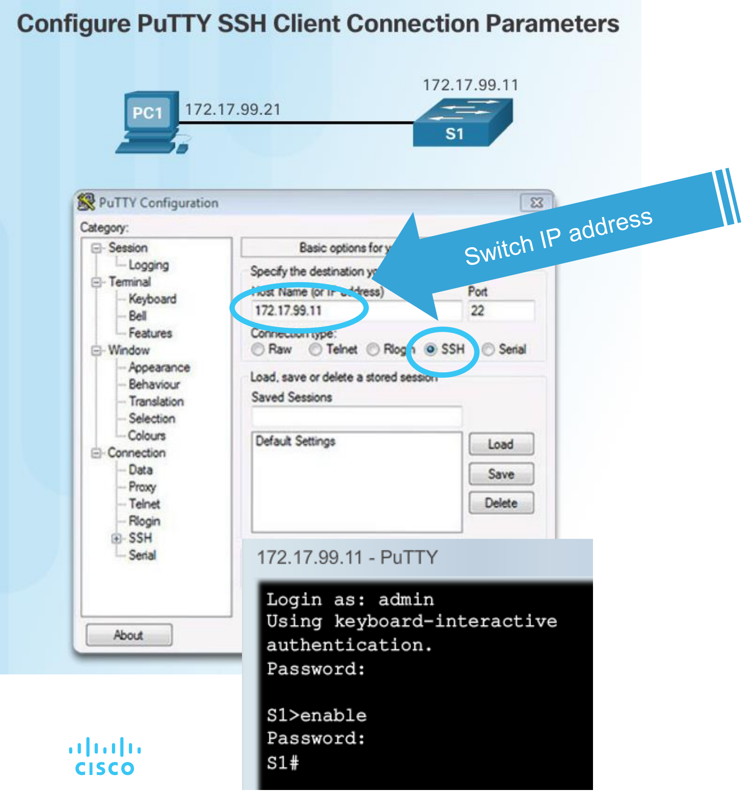
Default is to accept both Telnet and SSH (transport input all)

The `login local` command forces the use of the local database for username/ password.

Secure Remote Access

Verifying SSH

- On the PC, connect to the switch using SSH.



Configure PuTTY SSH Client Connection Parameters

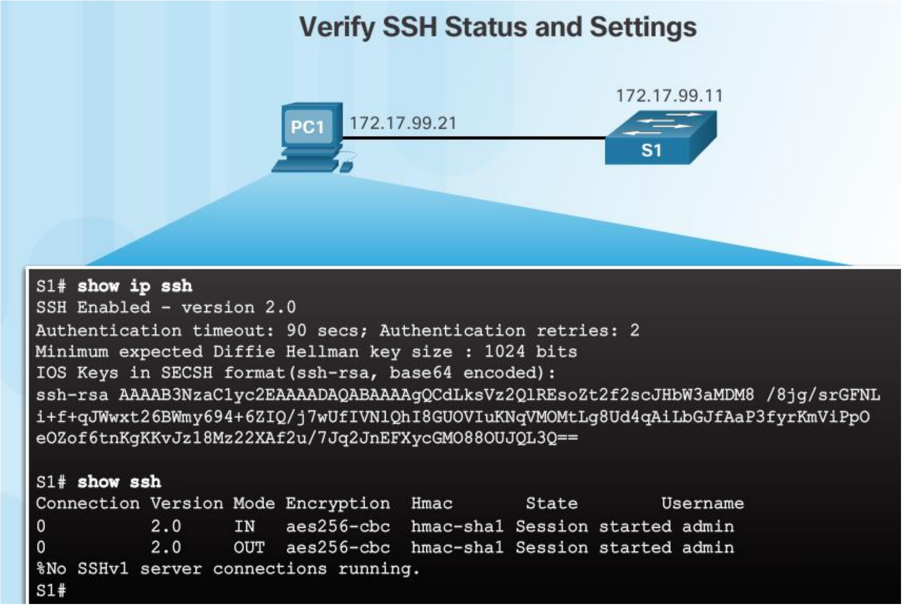
Specify the destination y

Host Name (or IP address): 172.17.99.11 Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

172.17.99.11 - PuTTY

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

S1>enable
Password:
S1#
```



Verify SSH Status and Settings

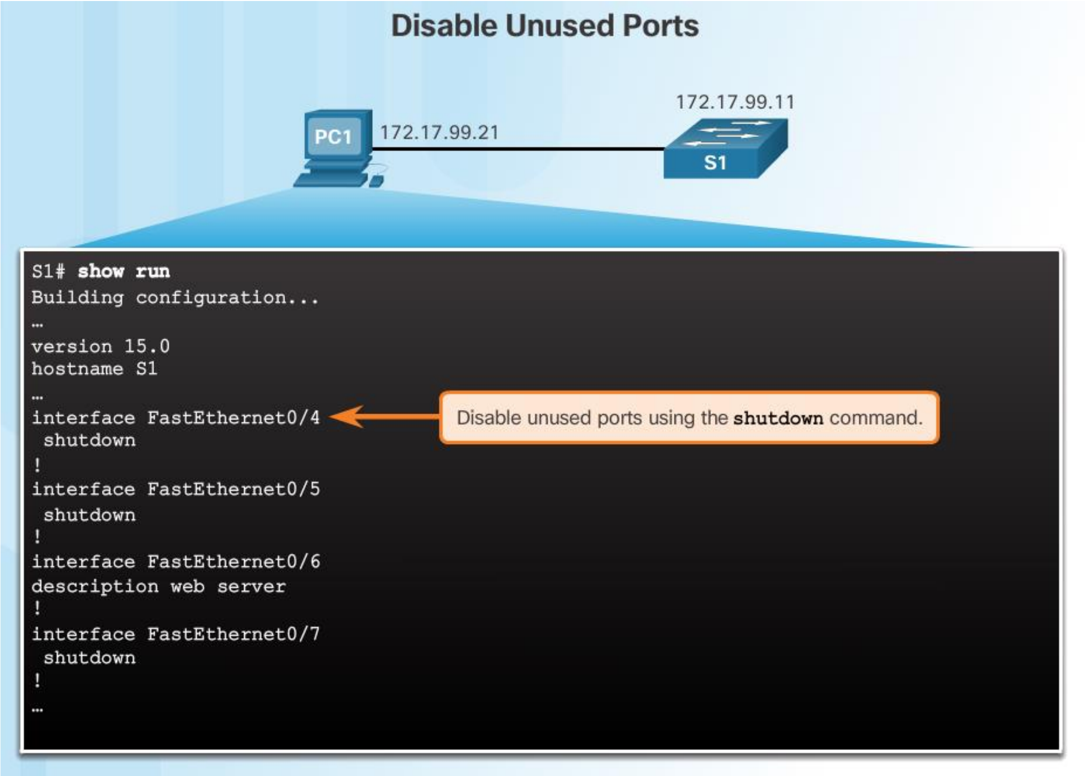
```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8 /8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAaP3fyrKmViPpO
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#
```

The PC is using SSH to communicate and issue commands on the switch.

Switch Port Security

Secure Unused Ports

The `interface range` command can be used to apply a configuration to several switch ports at one time.



Disable Unused Ports

```
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
!
…
```

Disable unused ports using the `shutdown` command.

Port Security: Operation

- Port security limits the number of valid MAC addresses allowed to transmit data through a switch port.
  - If a port has port security enabled and an unknown MAC address sends data, the switch presents a security violation.
  - Default number of secure MAC addresses allowed is 1.
- Methods use to configure MAC addresses within port security:
  - Static secure MAC addresses – manually configure

    switchport port-security mac-address *mac-address*
  - Dynamic secure MAC addresses – dynamically learned and removed if the switch restarts
  - Sticky secure MAC addresses – dynamically learned and added to the running configuration (which can later be saved to the startup-config to permanently retain the MAC addresses)

    switchport port-security mac-address sticky *mac-address*

Note: Disabling sticky learning converts sticky MAC addresses to dynamic secure addresses and removes them from the running-config.

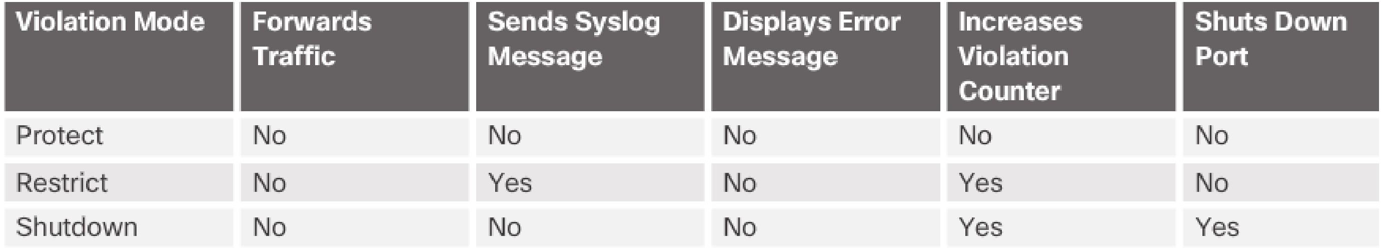
Switch Port Security

Port Security: Violation Modes

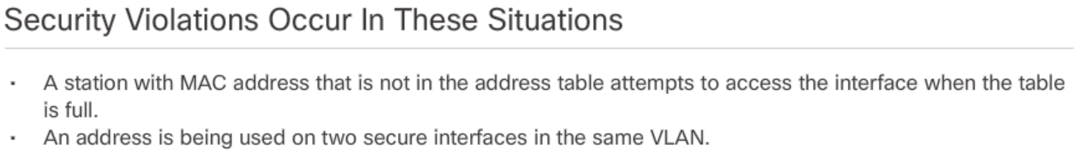
- Protect – data from unknown source MAC addresses are dropped; a security notification **IS NOT** presented by the switch

- Restrict - data from unknown source MAC addresses are dropped; a security notification **IS** presented by the switch and the violation counter increments.

- Shutdown – (default mode) interface becomes error-disabled and port LED turns off. The violation counter increments. Issues the shutdown and then the no shutdown command on the interface to bring it out of the error-disabled state.



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

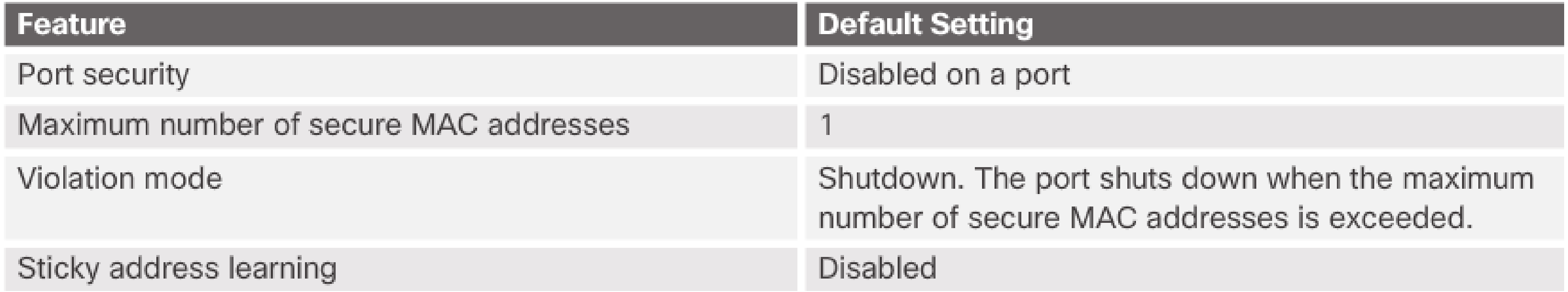


Security Violations Occur In These Situations

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

Switch Port Security

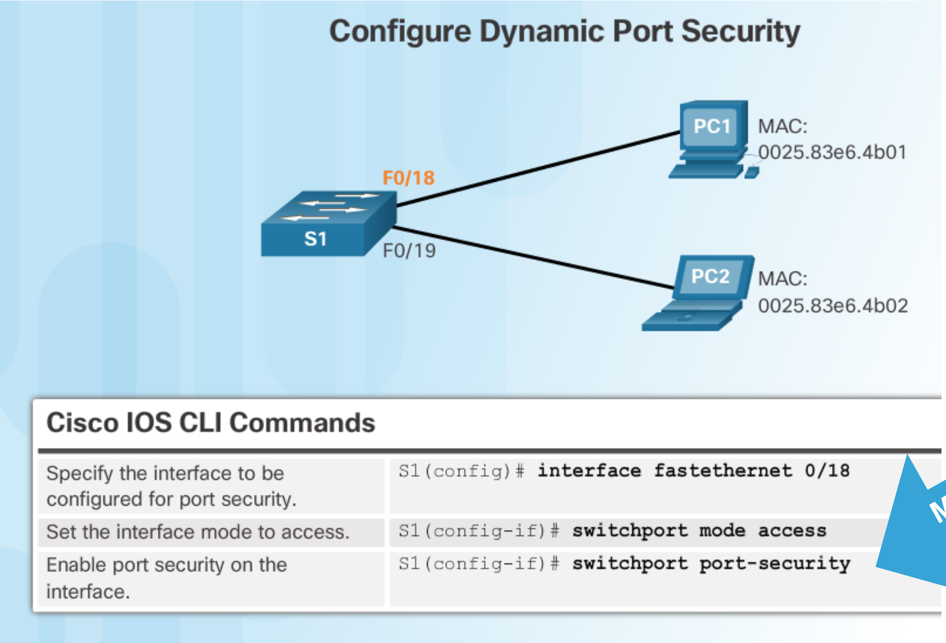
Port Security: Configuring



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

Port Security: Configuring (Cont.)

- Before configuring port-security features, place the port in access mode and use the **switchport port-security** interface configuration command to enable port security on an interface.



Configure Dynamic Port Security

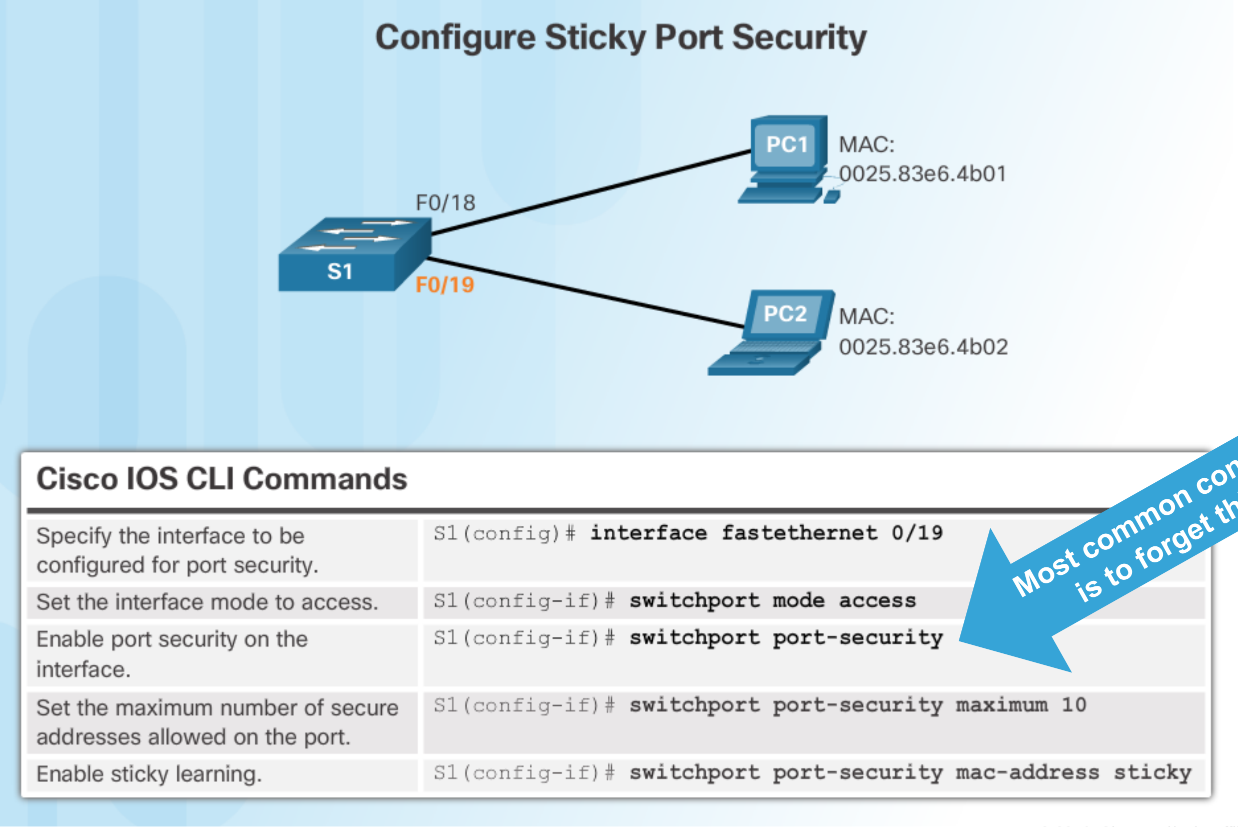
Cisco IOS CLI Commands

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

Most common configuration error is to forget this command!

Switch Port Security

Port Security: Configuring (Cont.)



Configure Sticky Port Security

Cisco IOS CLI Commands

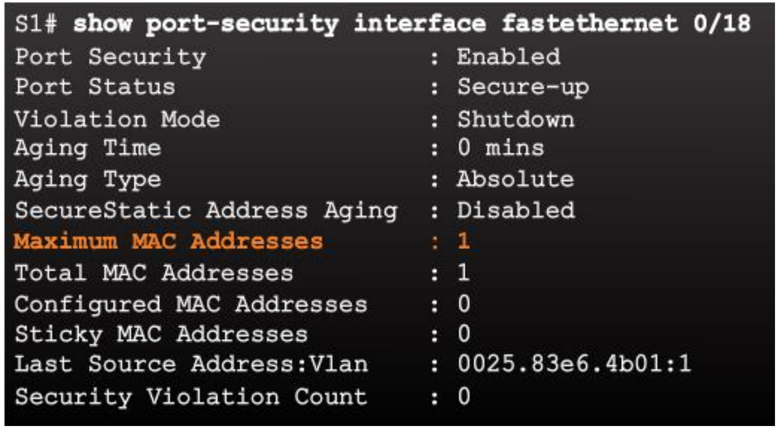
Specify the interface to be configured for port security.	`S1(config)# interface fastethernet 0/19`
Set the interface mode to access.	`S1(config-if)# switchport mode access`
Enable port security on the interface.	`S1(config-if)# switchport port-security`
Set the maximum number of secure addresses allowed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

Most common configuration error is to forget this command!

Port Security: Verifying

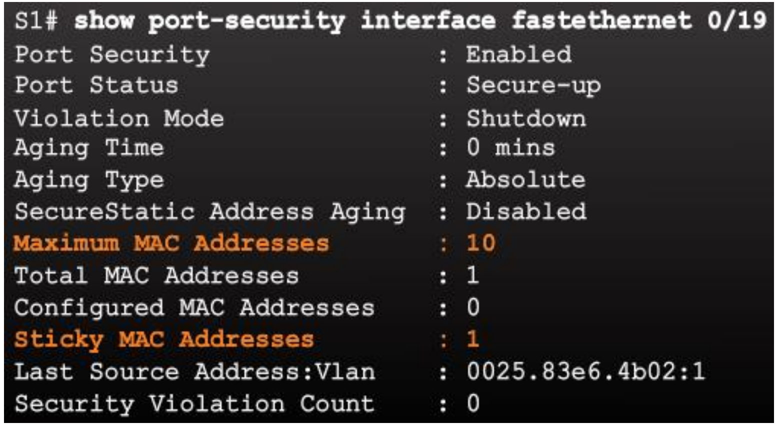
- Use the **show port-security interface** command to verify the maximum number of MAC addresses allowed on a particular port and how many of those addresses were learned dynamically using sticky.

Dynamic



```
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
```

Sticky

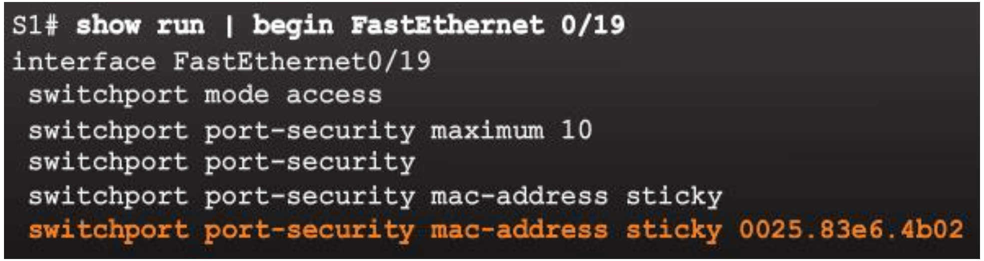


```
S1# show port-security interface fastethernet 0/19
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 10
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

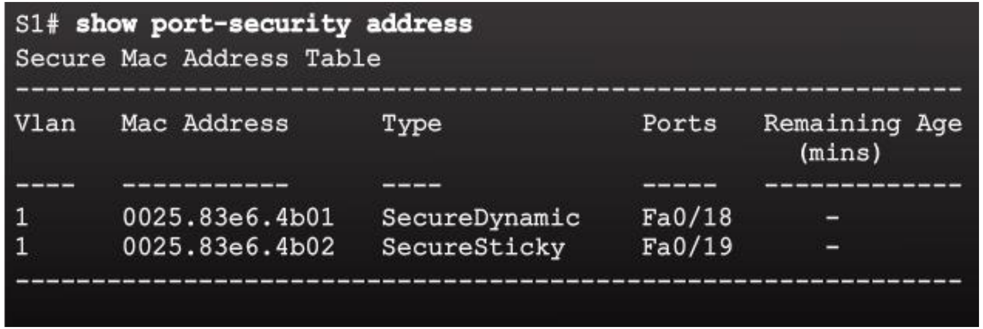
Port Security: Verifying (Cont.)

- Use the **show running-config** command to see learned MAC addresses added to the configuration.



```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 10
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

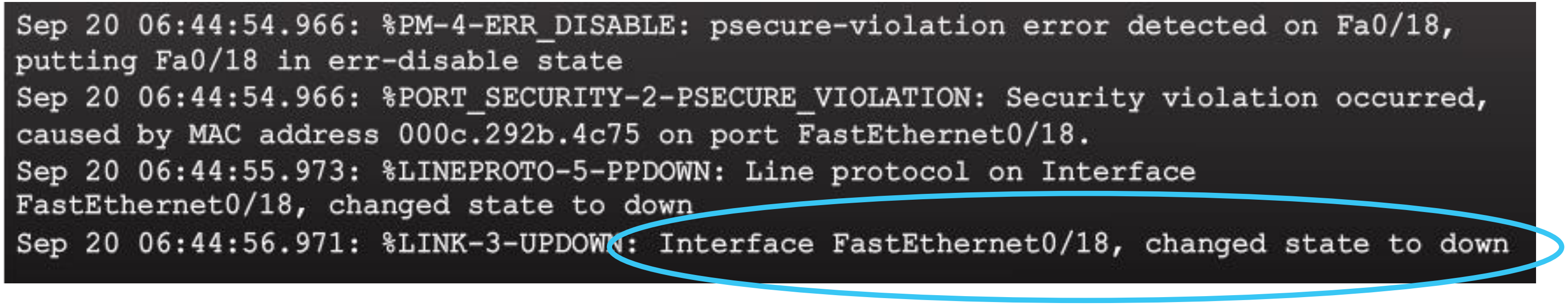
- The **show port-security address** command shows how MAC addresses were learned on a particular port.



```
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

- Switch console messages display when a port security violation occurs. Notice the port link status changes to down.

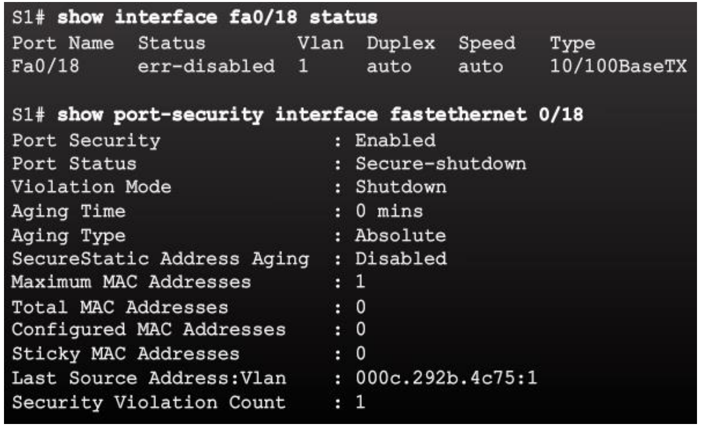


```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18,
putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: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

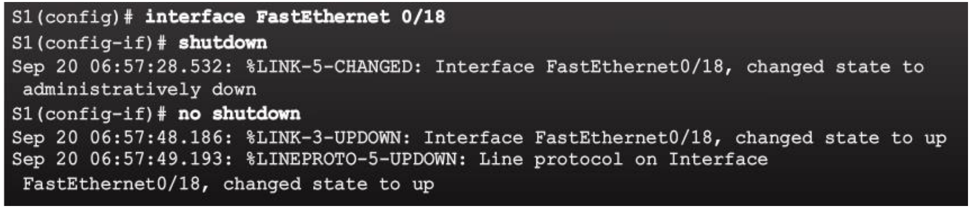
Ports in Error Disabled State (Cont.)

- Check the port status and the port security settings.



```
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
```

- Do not re-enable a port until the security threat is investigated and eliminated.
- Notice that you must first shut the port down and then issue the **no shutdown** command in order to use the particular port again after a security violation has occurred.



```
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