



Chapter 5: Switch Configuration



Routing and Switching Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™



Configure a Switch with Initial Settings

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.



Configure a Switch with Initial Settings

Recovering From a System Crash

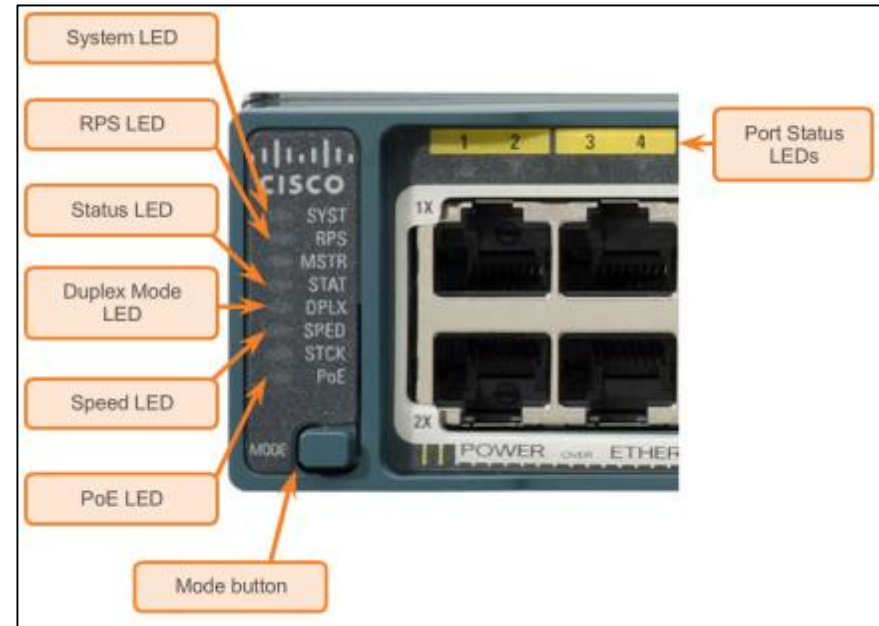
- The boot loader can also be used to manage the switch if the IOS cannot be loaded.
- The boot loader can be accessed through a console connection by:
 1. Connecting a PC by console cable to the switch console port. Unplug the switch power cord.
 2. Reconnecting the power cord to the switch and press 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.



Configure a Switch with Initial Settings

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





Configure a Switch with Initial Settings

Preparing for Basic Switch Management

To remotely manage a Cisco switch, it must be configured to access the network.

- A console cable is used to connect a PC to the console port of a switch for configuration.
- The IP information (address, subnet mask, gateway) is to be assigned to a switch virtual interface (SVI).
- If managing the switch from a remote network, a default gateway must also be configured.
- Although these IP settings allow remote management and remote access to the switch, they do not allow the switch to route Layer 3 packets.



Configure a Switch with Initial Settings

Configuring Switch Management Access

Configure Switch Management Interface

Cisco Switch IOS Commands

| | |
|---|---|
| Enter global configuration mode. | <code>S1# configure terminal</code> |
| Enter interface configuration mode for the SVI. | <code>S1(config)# interface vlan 1</code> |
| Configure the management interface IP address. | <code>S1(config-if)# ip address 172.17.99.11 255.255.255.0</code> |
| Enable the management interface. | <code>S1(config-if)# no shutdown</code> |
| Return to the privileged EXEC mode. | <code>S1(config-if)# end</code> |
| Save the running config to the startup config. | <code>S1# copy running-config startup-config</code> |



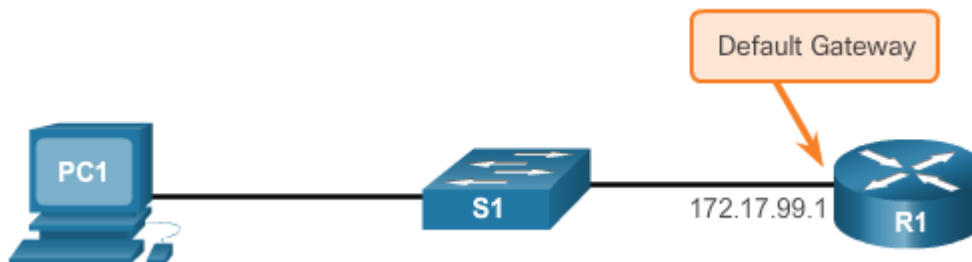
Configure a Switch with Initial Settings

Configuring Switch Management Access

Configure Switch Default Gateway

Cisco Switch IOS Commands

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

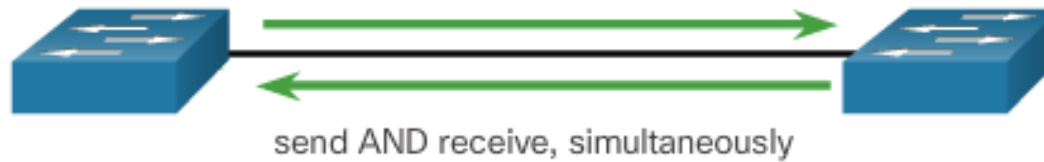




Configure Switch Ports

Duplex Communication

Full-Duplex Communication



Half-Duplex Communication

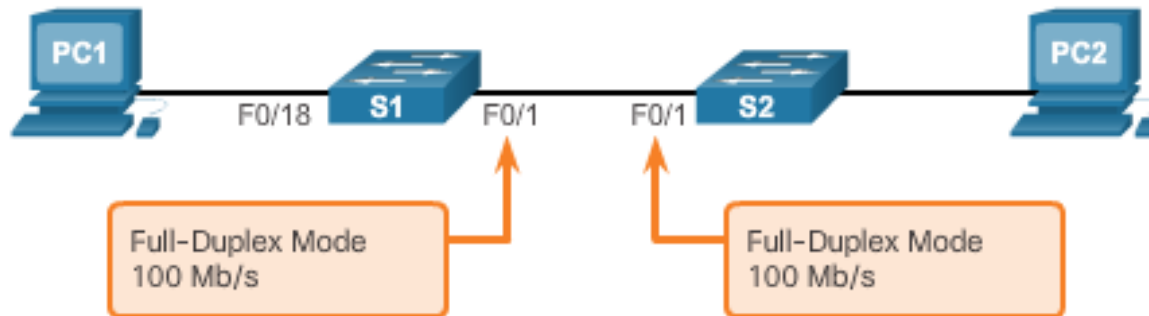




Configure Switch Ports

Configure Switch Ports at the Physical Layer

Configure Duplex and Speed



Cisco Switch IOS Commands

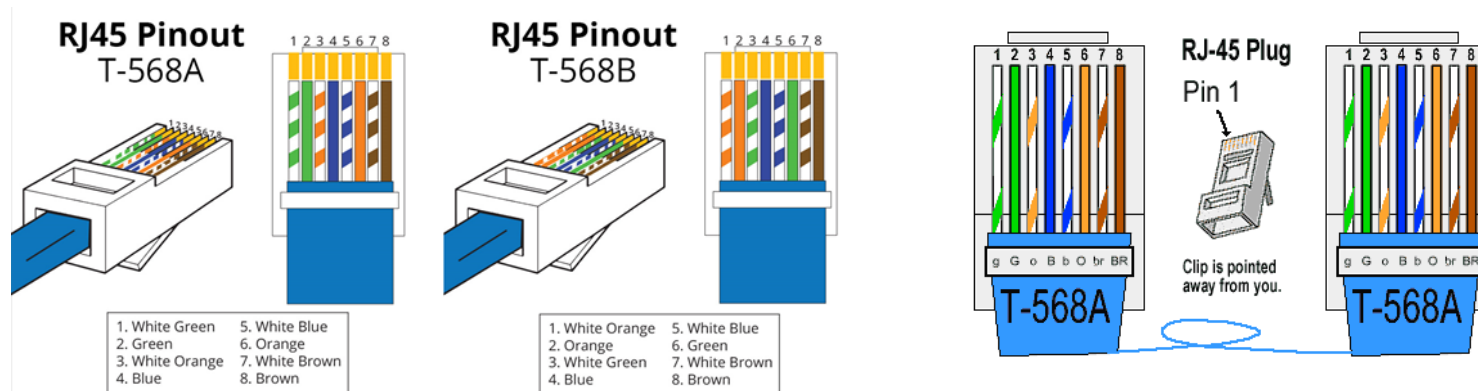
| | |
|--|---|
| Enter global configuration mode. | S1# configure terminal |
| Enter interface configuration mode. | S1(config)# interface FastEthernet 0/1 |
| Configure the interface duplex. | S1(config-if)# duplex full |
| Configure the interface speed. | S1(config-if)# speed 100 |
| Return to the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



Configure Switch Ports

Auto-MDIX

- 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.



Configure Switch Ports Auto-MDIX

Configure auto-MDIX



Cisco Switch IOS Commands

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



Configure Switch Ports

Verifying Switch Port Configuration

Verification Commands

| Cisco Switch IOS Commands | |
|--|--|
| Display interface status and configuration. | S1# show interfaces [<i>interface-id</i>] |
| 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 [<i>interface-id</i>] |
| Display the MAC address table. | S1# show mac-address-table OR S1# show mac address-table |



Configure Switch Ports

Network Access Layer Issue

```
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 runs, 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 runs, giants, no buffer, CRC, frame, overrun, and ignored counts. |
| Runs | 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 collision that occurs after 512 bits of the frame have been transmitted. |



5.2 Switch Security: Management and Implementation



Cisco | Networking Academy®
Mind Wide Open™



Secure Remote Access

SSH Operation

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



Secure Remote Access

Configuring SSH

Configure SSH for Remote Management

1. **Verify SSH Support –**
`show ip ssh`
2. **Configure the IP domain.**
3. **Generate RSA key pairs.**
4. **Configure user authentication.**
5. **Configure the vty lines.**
6. **Enable SSH version 2.**

172.17.99.11



172.17.99.21

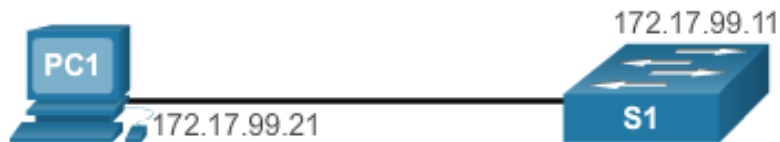


```
S1# configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin secret ccna
S1(config-line)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
S1(config)# ip ssh version 2
S1(config)# exit
S1#
```


Secure Remote Access

Verifying SSH

Remote Management SSH Connection



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

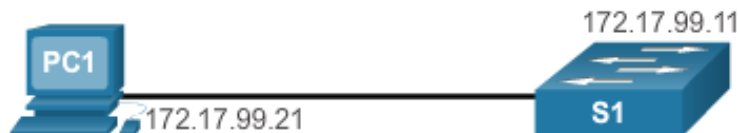
S1>enable
Password:
S1#
```



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
AAAAB3NzaC1yc2EAAAADAQABAAQGCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVN1QhI8GUOVluKNqVMOMtLg8Ud4qAilbGJfAa
P3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGM088OUJQL3Q==

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#
  
```



Switch Port Security

Secure Unused Ports

Disable Unused Ports

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
!
...
```

172.17.99.11

S1

172.17.99.21

PC1



Switch Port Security

Port Security: Operation

- 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 – manually configured and added to running configuration - **switchport port-security mac-address** *mac-address*
 - Dynamic secure MAC addresses – removed when switch restarts
 - Sticky secure MAC addresses – added to running configuration and learned dynamically – **switchport port-security mac-address sticky** interface configuration mode command



Switch Port Security

Port Security: Violation Modes

- IOS considers a security violation when:
 - 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.
- There are three possible actions to take when a violation is detected:
 - Protect – no notification received
 - Restrict – notification received of security violation
 - Shutdown
 - **switchport port-security violation {*protect* | *restrict* | *shutdown*}** interface
configuration mode command



Switch Port Security

Port Security: Violation Modes (cont.)

Security violation modes include: Protect, Restrict, and Shutdown.

| Security Violation Modes | | | | | |
|--------------------------|------------------|----------------------|------------------------|-----------------------------|-----------------|
| Violation Mode | Forwards Traffic | Sends Syslog Message | Displays Error Message | Increases Violation Counter | Shuts Down Port |
| Protect | No | No | No | No | No |
| Restrict | No | Yes | No | Yes | No |
| Shutdown | No | No | No | Yes | Yes |



Switch Port Security

Port Security: Configuring

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. |
| Sticky address learning | Disabled |

Configure Dynamic Port Security



Cisco IOS CLI Commands

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

Configure Sticky Port Security



Cisco IOS CLI Commands

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



Switch Port Security

Port Security: Verifying

Verify MAC Address - 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
```

Verify MAC Address - 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

Verify Sticky MAC - Running Config

```
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
```

Verify 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 | - |



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

Port Status

```
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
```

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

A **shutdown** and **no shutdown** interface configuration mode command must be issued to re-enable the port.

Re-Enabling an Error Disabled 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
```