CCNA RS 2 – Routing and Switching Essentials

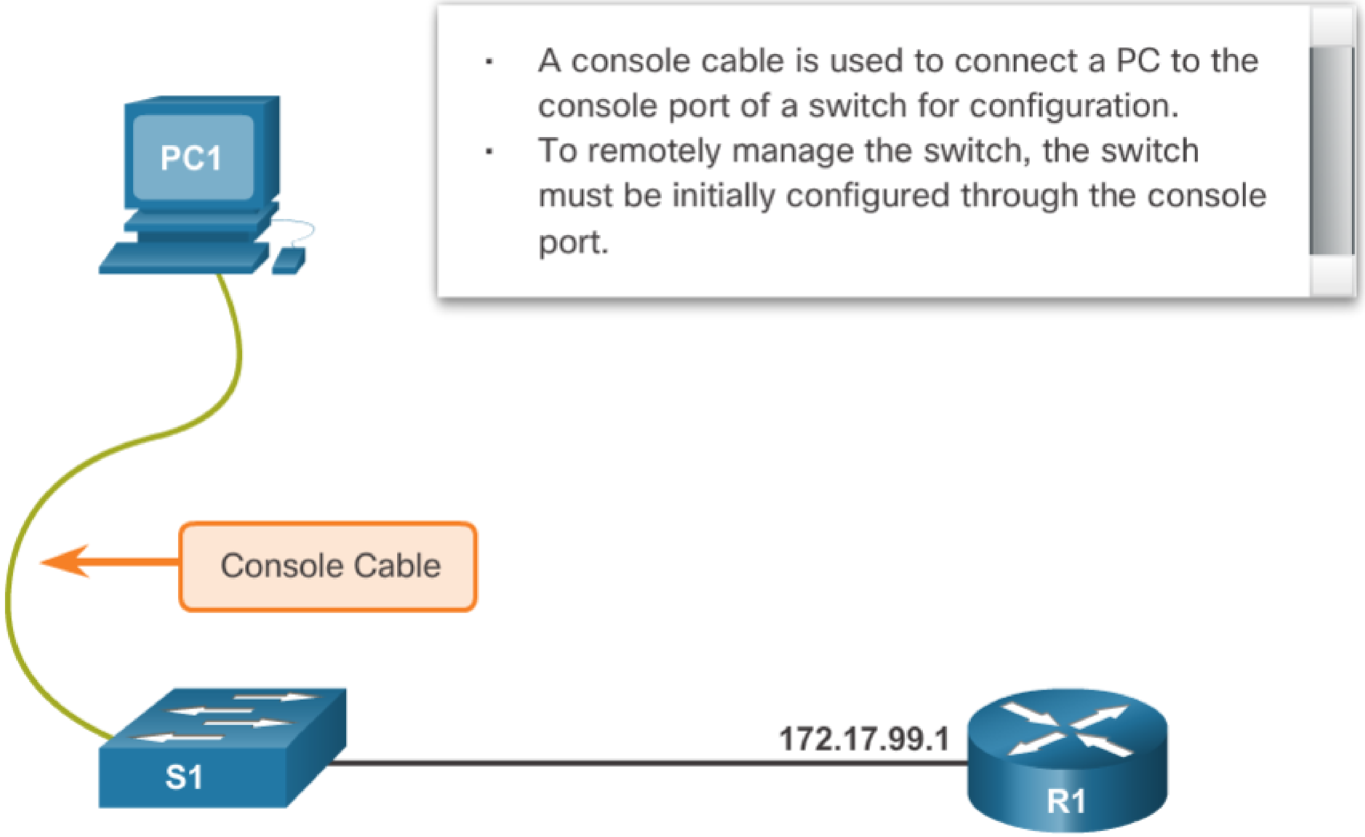
LESSON#5
SWITCH CONFIGURATIONS

BY AZAMAT ZHAMANOV

Switch Boot Sequence

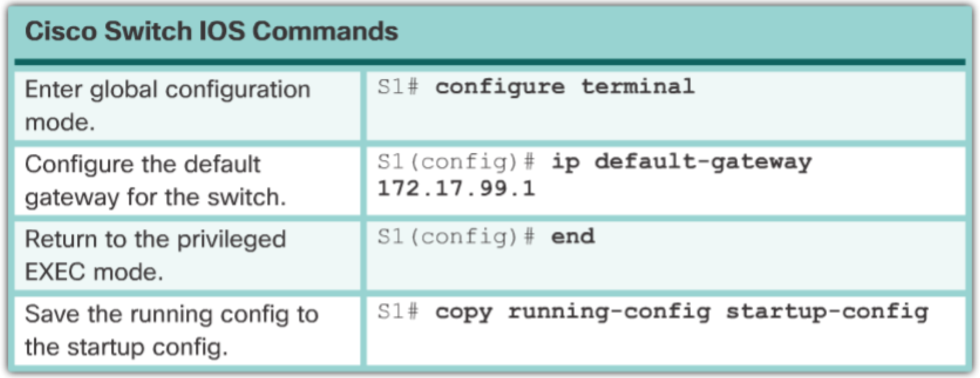
1. POST (Power-on-self-test).
2. Boot Loader (from ROM)
3. The boot loader performs low-level CPU initialization. It initializes the CPU registers, which control where physical memory is mapped, the quantity of memory, and its speed.
4. The boot loader initializes the flash file system on the system board.
5. Finally, the boot loader locates and loads a default IOS operating system software image into memory and gives control of the switch over to the IOS.

Managing Switch by Console cable

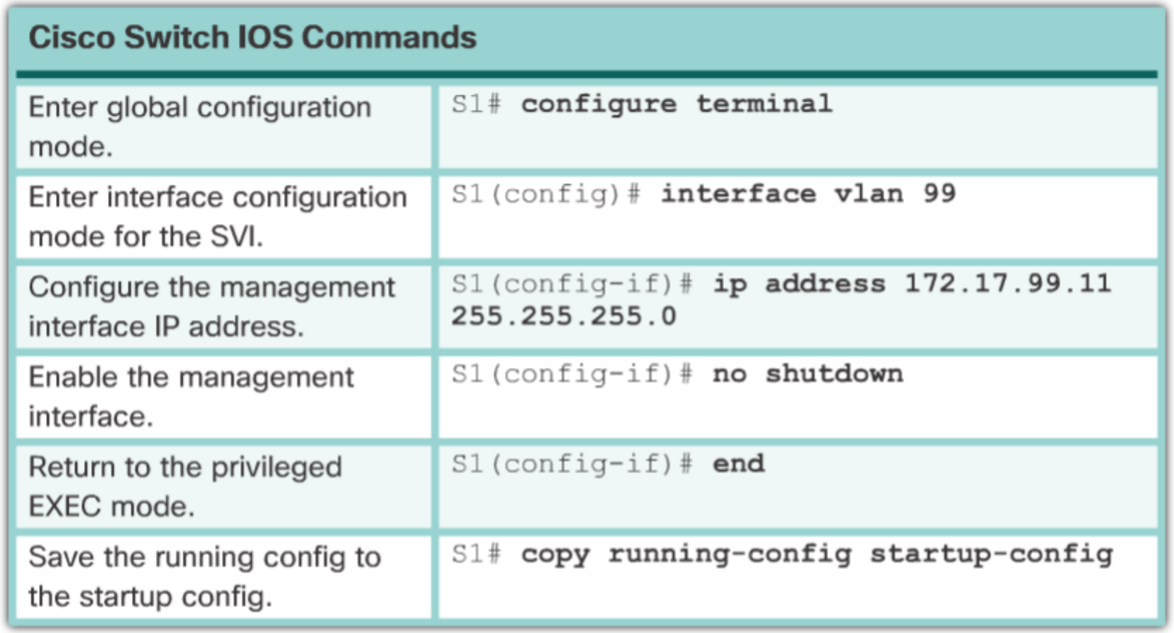


- A console cable is used to connect a PC to the console port of a switch for configuration.
- To remotely manage the switch, the switch must be initially configured through the console port.

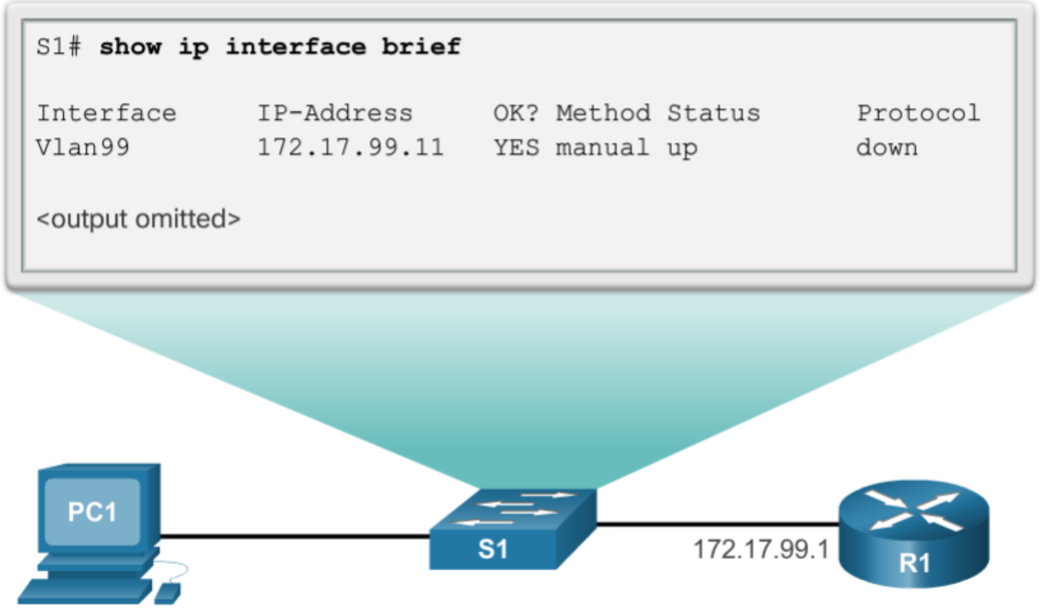
Managing Switch by SVI (Switch Virtual Interface)



Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Configure the default gateway for the switch.	`S1(config)# ip default-gateway 172.17.99.1`
Return to the privileged EXEC mode.	`S1(config)# 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`
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)# end`
Save the running config to the startup config.	`S1# copy running-config startup-config`

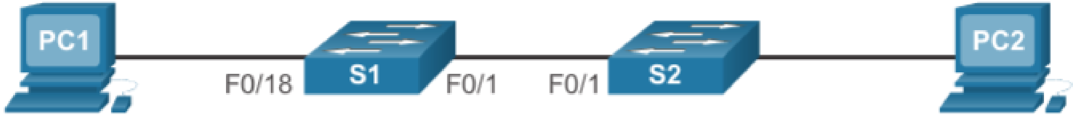


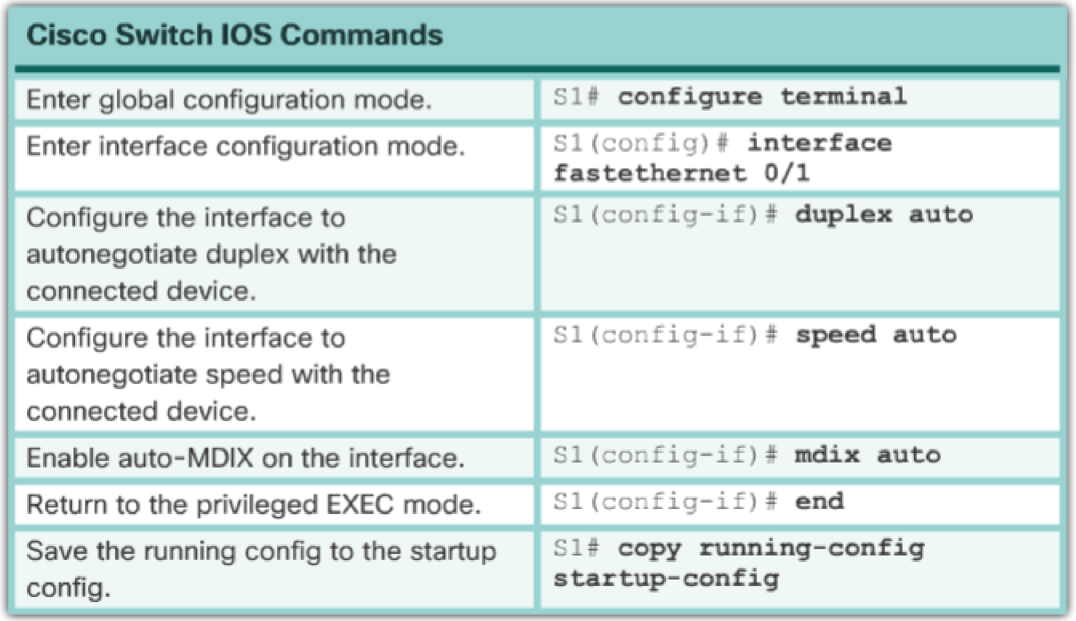
```
S1# show ip interface brief

Interface      IP-Address      OK? Method Status      Protocol
Vlan99         172.17.99.11    YES manual up          down

<output omitted>
```

Auto MDIX (automatic medium-dependent interface crossover)

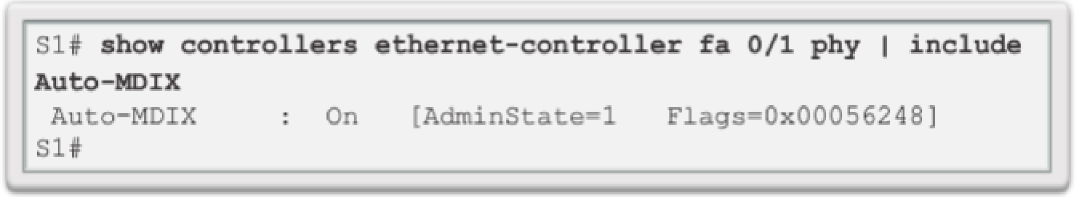




Cisco Switch IOS Commands

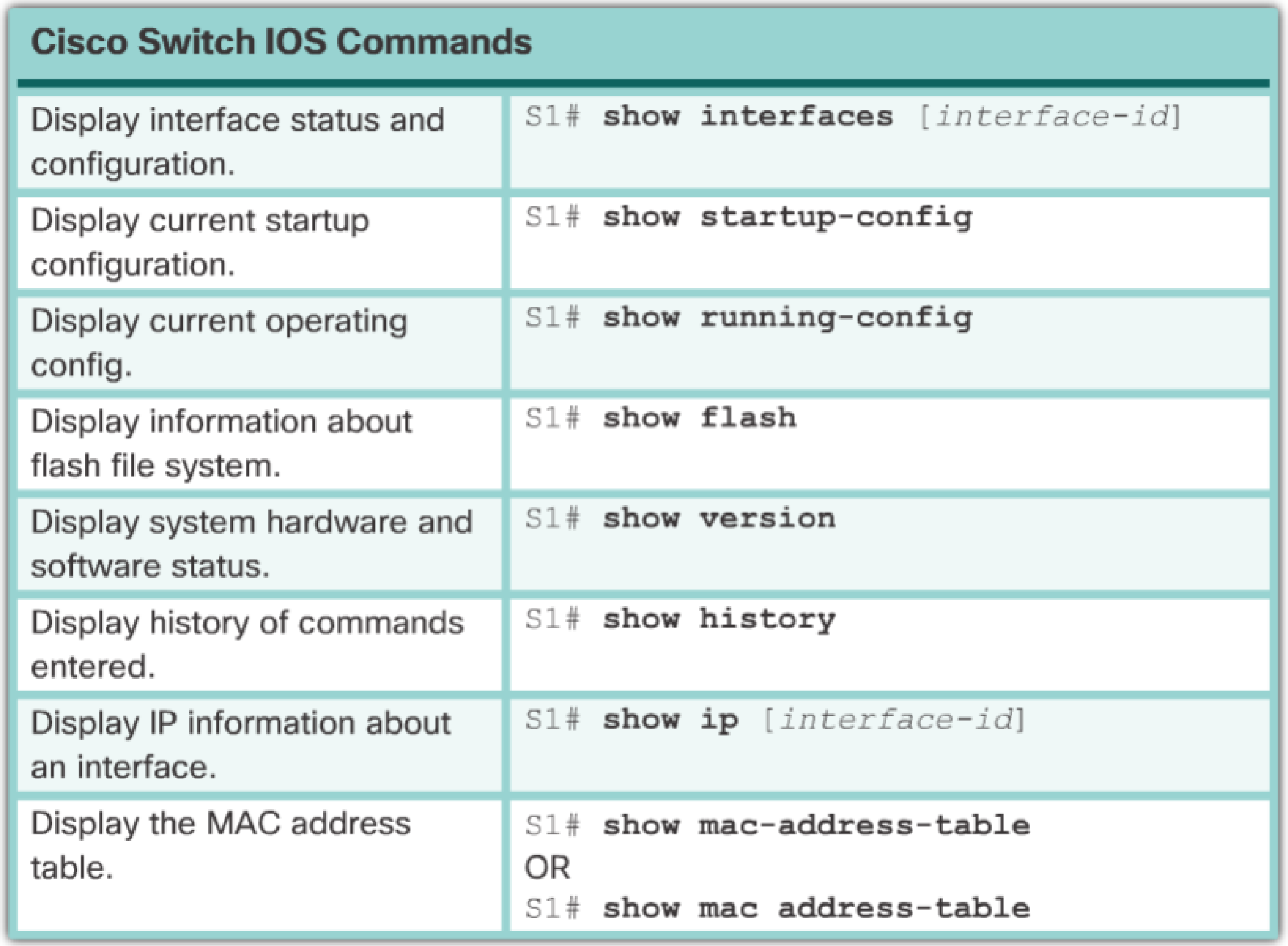
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface fastethernet 0/1`
Configure the interface to autonegotiate duplex with the connected device.	`S1(config-if)# duplex auto`
Configure the interface to autonegotiate speed with the connected 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`

The auto-MDIX feature is enabled by default on Catalyst 2960 and Catalyst 3560 switches, but is not available on the older Catalyst 2950 and Catalyst 3550 switches.



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

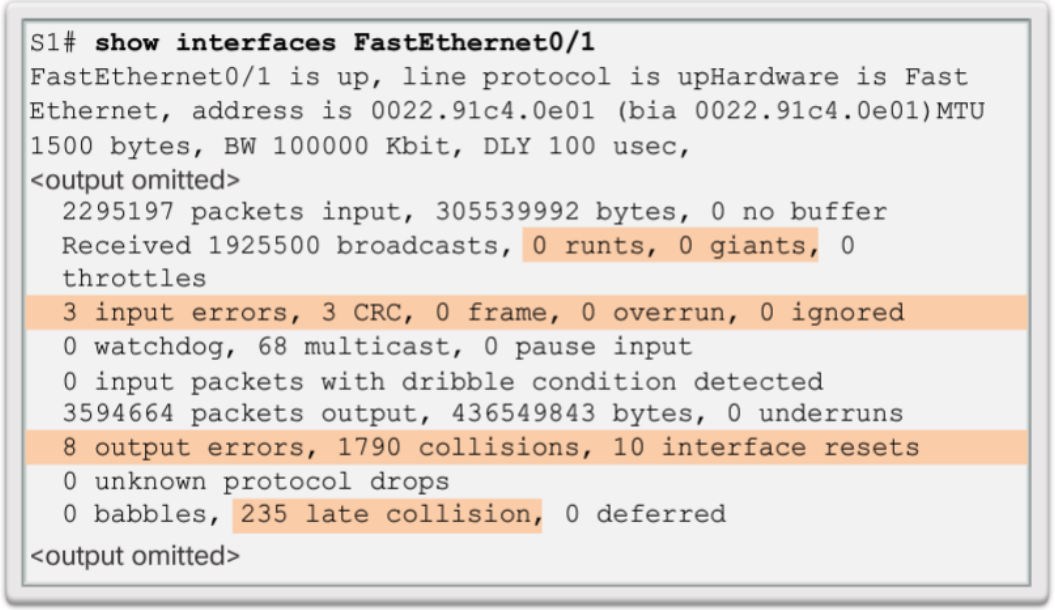
Verification of Configurations



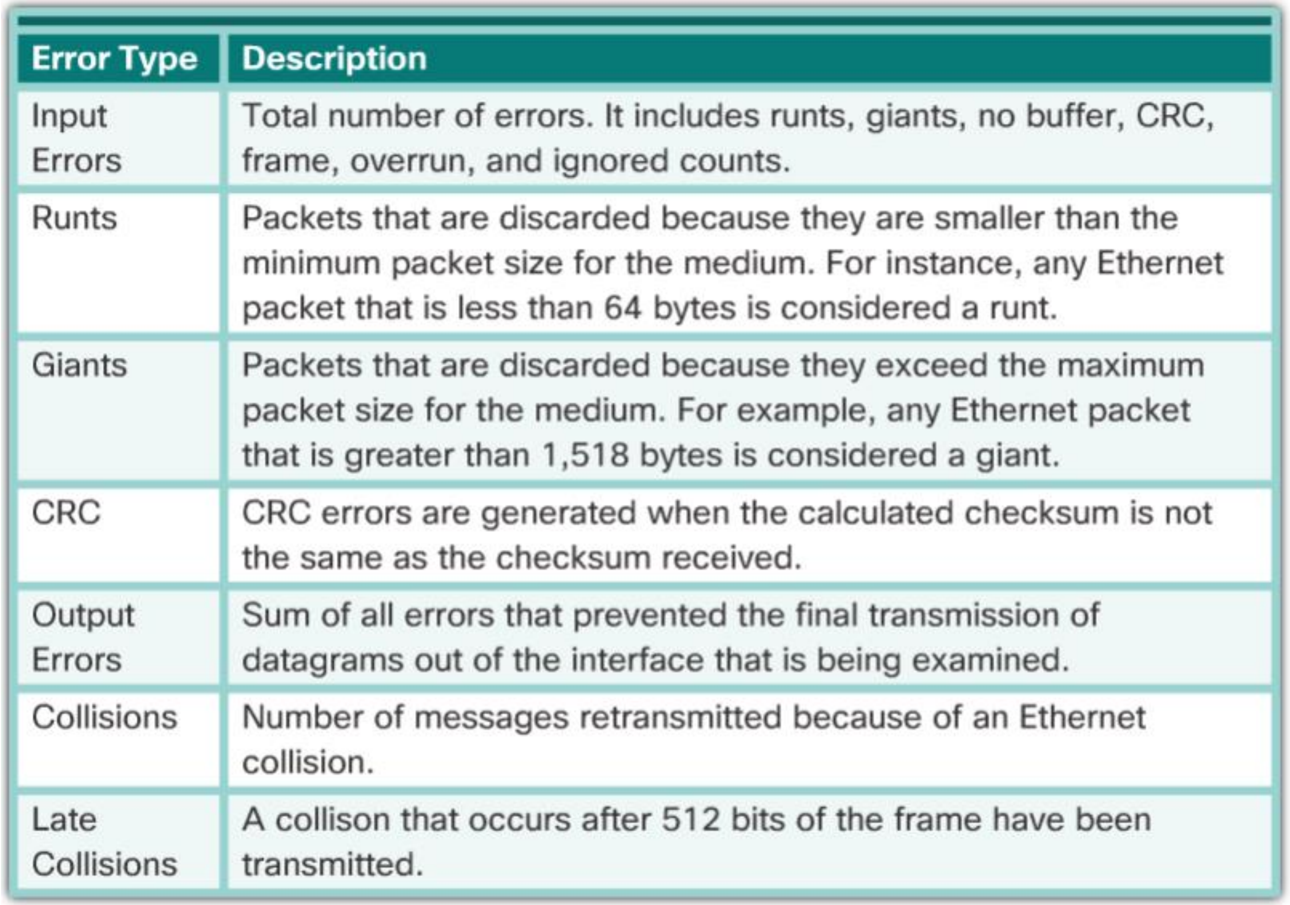
Cisco Switch IOS Commands	
Display interface status and configuration.	`S1# show interfaces [interface-id]`
Display current startup configuration.	`S1# show startup-config`
Display current operating config.	`S1# show running-config`
Display information about flash file system.	`S1# show flash`
Display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

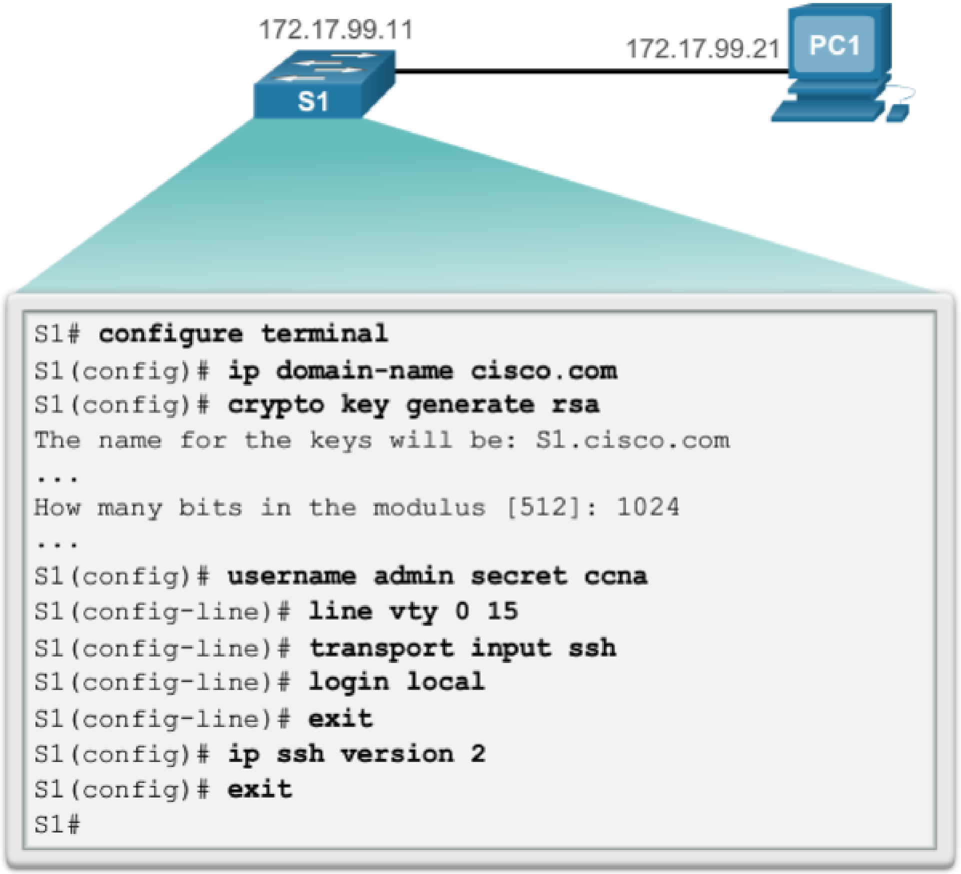


```
S1# show interfaces FastEthernet0/1
FastEthernet0/1 is up, line protocol is upHardware is Fast
Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)MTU
1500 bytes, BW 100000 Kbit, DLY 100 usec,
<output omitted>
  2295197 packets input, 305539992 bytes, 0 no buffer
  Received 1925500 broadcasts, 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.

SSH Configuration



```
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#
```

Step 1. Verify SSH support.
Use the **show ip ssh** command to verify that the switch supports SSH. If the switch is not running an IOS that supports cryptographic features, this command is unrecognized.

Step 2. Configure the IP domain.

Step 3. Generate RSA key pairs.

Note: To delete the RSA key pair, use the **crypto key zeroize rsa** global configuration mode command. After the RSA key pair is deleted, the SSH server is automatically disabled.

Step 4. Configure user authentication.

Step 5. Configure the vty lines.

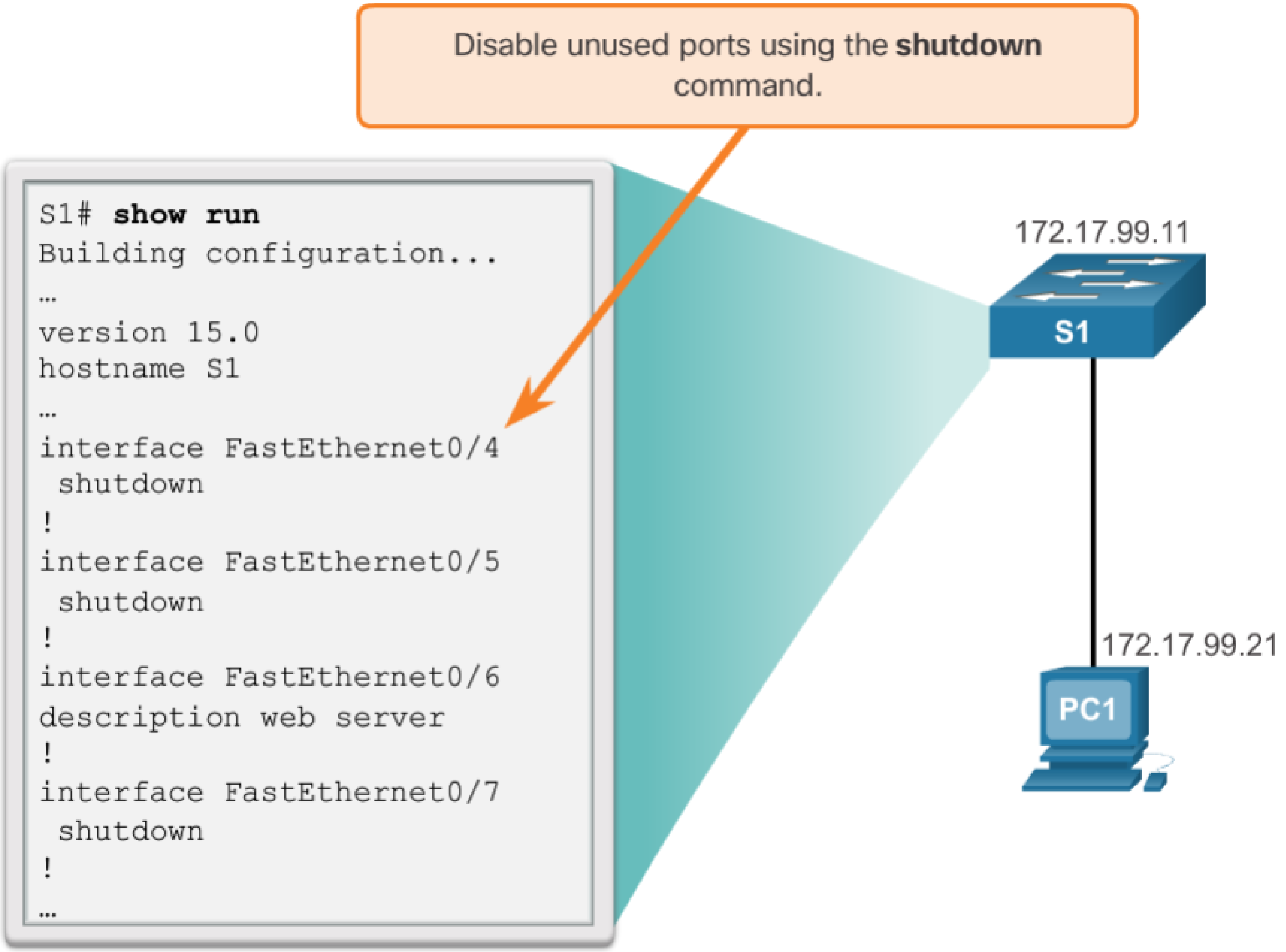
Step 6. Enable SSH version 2.

CCNA RS 2 – Routing and Switching Essentials

LESSON#5
SWITCH CONFIGURATIONS
PART 2

BY AZAMAT ZHAMANOV

Secure 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
!
…
```

```
Switch(config)# interface range type module/first-number – last-number
```

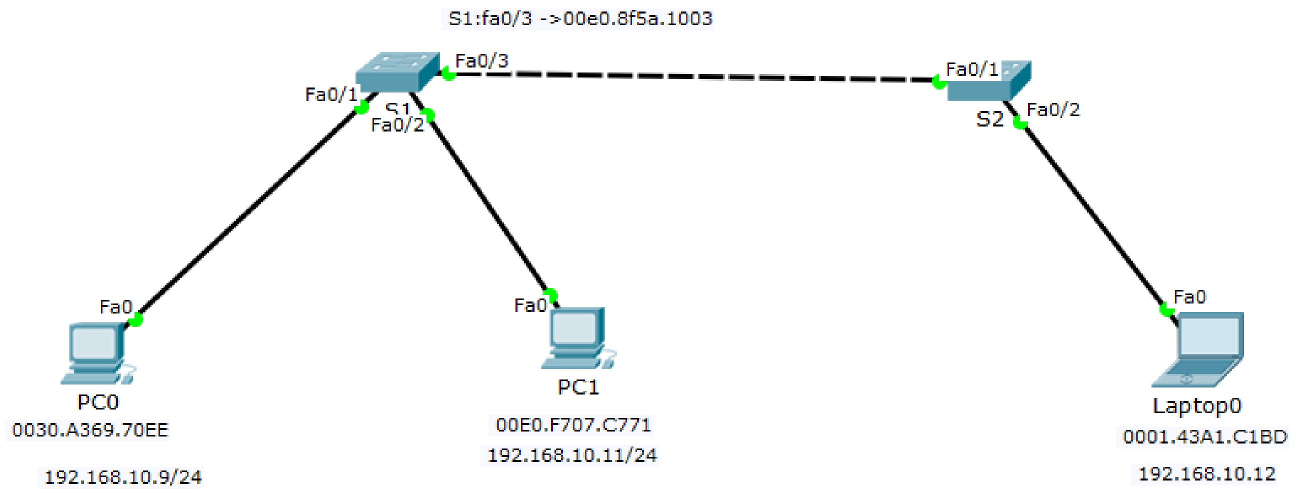
Port Security

Variants of Port Security usage:

- Static secure MAC addresses
- Dynamic secure MAC addresses
- Sticky secure MAC addresses

Types of Violations:

- Shutdown
- Protect
- Restrict



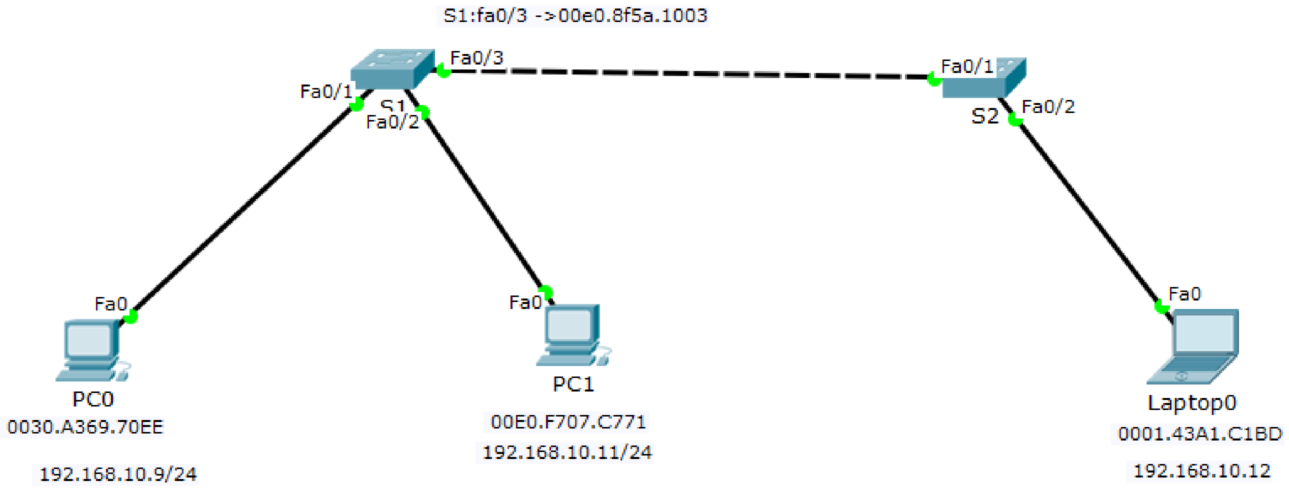
Port Security

Variants of Port Security usage:

- Static secure MAC addresses
- Dynamic secure MAC addresses
- Sticky secure MAC addresses

Types of Violations:

- Shutdown
- Protect
- Restrict



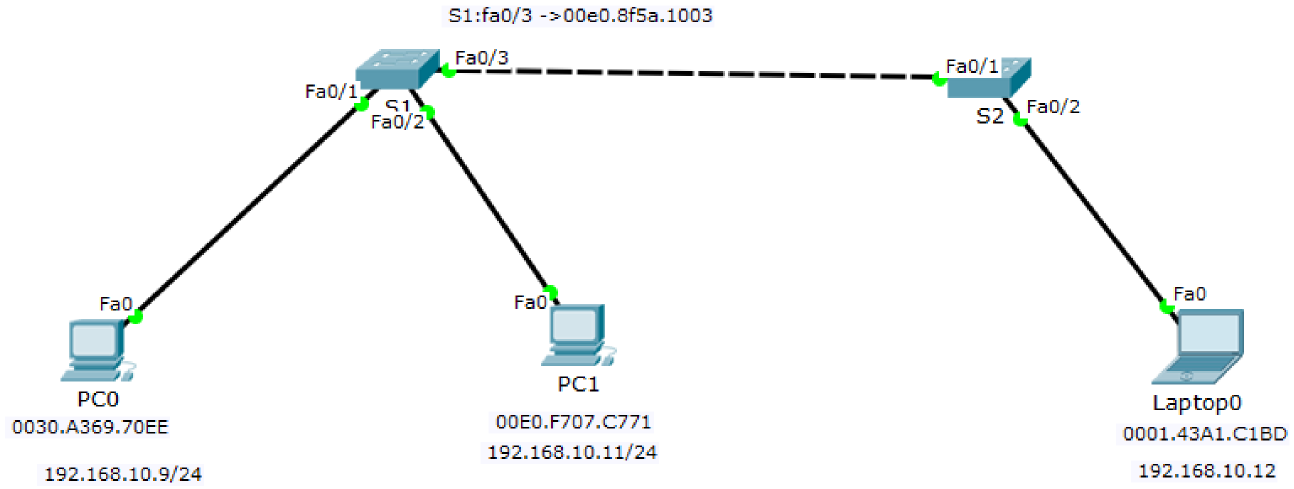
Port Security

Variants of Port Security usage:

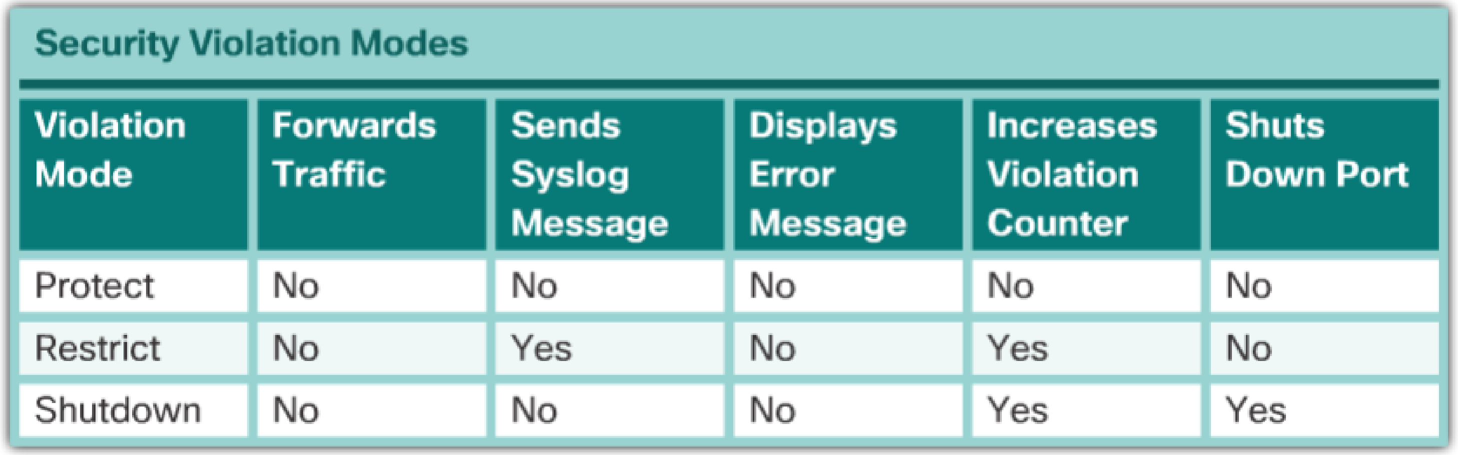
- Static secure MAC addresses
- Dynamic secure MAC addresses
- Sticky secure MAC addresses

Types of Violations:

- Shutdown
- Protect
- Restrict



Port Security Violation Modes



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

Q/A

zhamanov@gmail.com

azamat.zhamanov@sdu.eud.kz