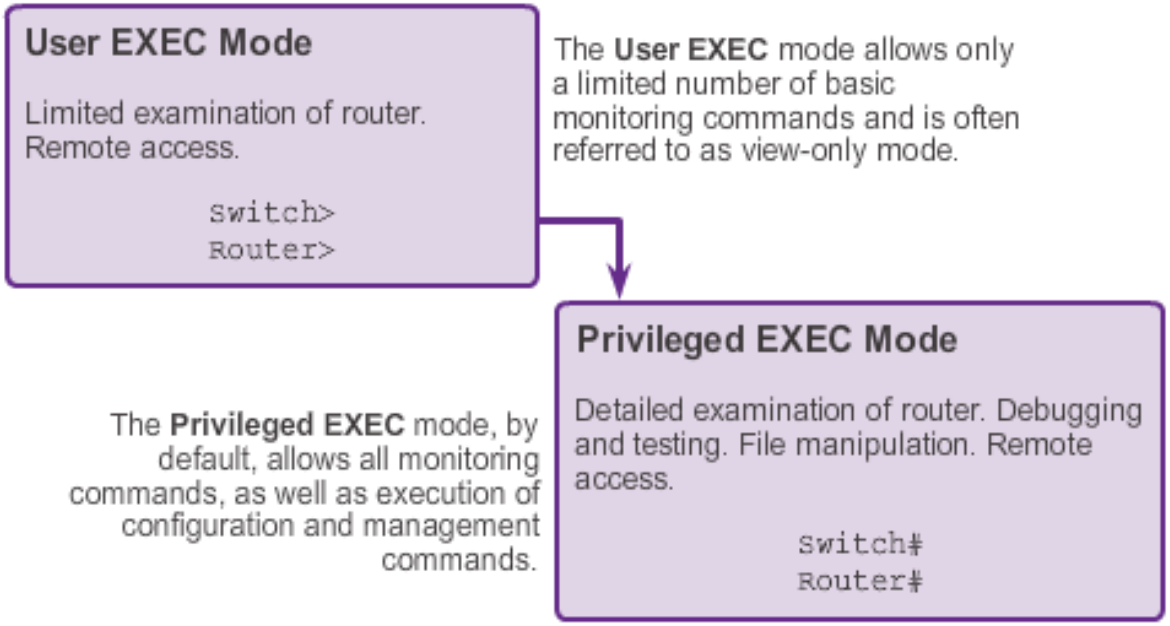
Switch

IOS

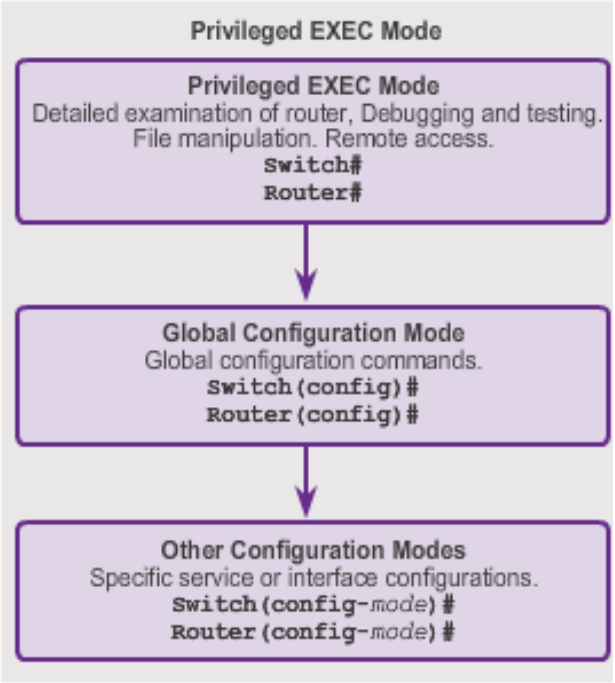
Feature the Cisco IOS

- The Cisco uses a **hierarchical structure**



Feature the Cisco IOS

- The Cisco uses a **hierarchical structure**



IOS Prompt Structure

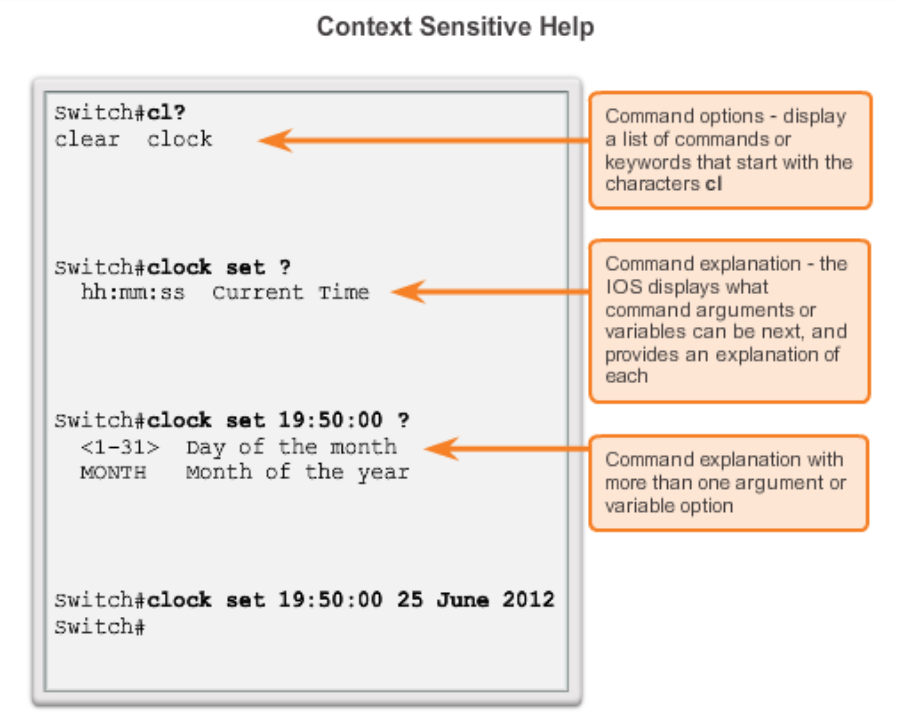
```
Router>ping 192.168.10.5

Router#show running-config

Router(config)#Interface FastEthernet 0/0

Router(config-if)#ip address 192.168.10.1 255.255.255.0
```

The prompt changes to denote the current CLI mode.

```
Switch>ping 192.168.10.9

Switch#show running-config

Switch(config)#Interface FastEthernet 0/1

Switch(config-if)#Description connection to WEST LAN4
```

Use the auto-completion feature

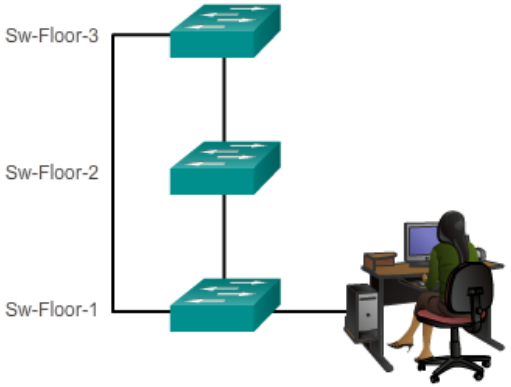
- Context-Sensitive Help



Device Names

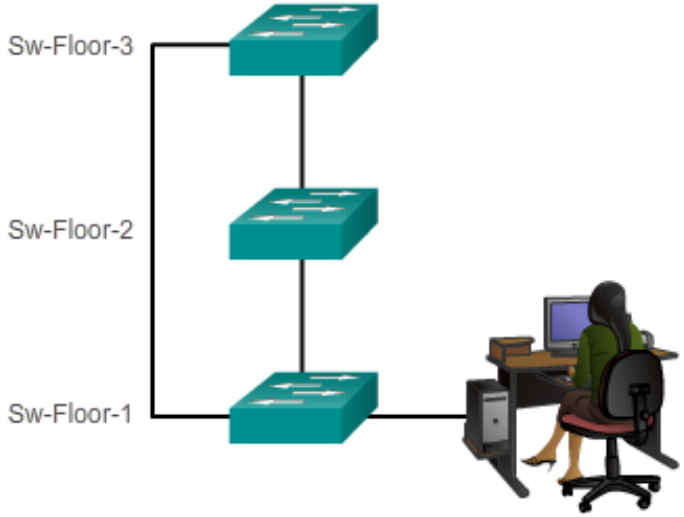
- The first step when configuring a switch is to assign it a unique **device name**, or hostname.
- **Hostnames** appear in **CLI prompts**, can be used in various authentication processes between devices, and should be used on topology diagrams.

  Without a hostname, network devices are **difficult to identify** for configuration purposes.



Configure Hostnames

- The **hostname** *name* global configuration command is used to assign a name.




```
Switch>
Switch> enable
Switch#
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

Feature the Cisco IOS

- Navigating **Between IOS Modes**

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# exit
Switch(config)# exit
Switch#
```

```
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# vlan 1
Switch(config-vlan)# end
Switch#
```

```
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# line vty 0 4
Switch(config-line)# interface fastethernet 0/1
Switch(config-if)# end
Switch#
```

Limiting Device Access

- **Step 1** - **Secure network devices** to physically limit access by placing them in wiring closets and locked racks
- **Step 2** - Enforce **secure passwords** as passwords are the primary defense against unauthorized access to network devices.

- Limit administrative access as follows.

Securing Administrative Access

- Secure privileged EXEC access with a password
- Secure user EXEC access with a password
- Secure remote Telnet access with a password

Other tasks

- Encrypt all passwords
- Provide legal notification

- Use strong password as suggested.

When Choosing Passwords

- Use passwords that are more than 8 characters in length.
- Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.
- Avoid using the same password for all devices.
- Don't use common words because these are easily guessed.

Configure Passwords

- **Enable Password**

```
Sw-Floor-1> enable
Sw-Floor-1#
Sw-Floor-1# conf terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
Sw-Floor-1# disable
Sw-Floor-1> enable
Password:
Sw-Floor-1#
```

Configure Passwords

- Secure privileged EXEC access using the **enable secret** *password* global config command.
- Secure user EXEC access by configuring the **line console** as follows:

Securing User EXEC Mode	Description
`Switch(config)#` **line console 0**	Command enters line console configuration mode.
`Switch(config-line)#` **password** *password*	Command specifies the line console password.
`Switch(config-line)#` **login**	Command makes the switch require the password.

- Secure remote Telnet or **SSH** access by configuring the Virtual terminal (VTY) lines as follows:

Securing Remote Access	Description
`Switch(config)#` **line vty 0 15**	Cisco switches typically support up to 16 incoming VTY lines numbered 0 to 15.
`Switch(config-line)#` **password** *password*	Command specifies the VTY line password.
`Switch(config-line)#` **login**	Command makes the switch require the password.

Configure Passwords

- **Password**

Secure Privileged EXEC	`Sw-Floor-1(config)# enable secret cisco`
	`Sw-Floor-1(config)# exit`
	`Sw-Floor-1#`
	`Sw-Floor-1# disable`
	`Sw-Floor-1> enable`
	`Password:`
	`Sw-Floor-1#`

Securing User EXEC	`Sw-Floor-1(config)# line console 0`
	`Sw-Floor-1(config-line)# password cisco`
	`Sw-Floor-1(config-line)# login`
	`Sw-Floor-1(config-line)# exit`
	`Sw-Floor-1(config)#`

Securing Remote Access	`Sw-Floor-1(config)# line vty 0 15`
	`Sw-Floor-1(config-line)# password cisco`
	`Sw-Floor-1(config-line)# login`
	`Sw-Floor-1(config-line)#`

Banner Messages

- Banners are **messages** that are displayed when someone attempts **to gain access to a device**. Banners are an important part of the legal process in the event that someone is prosecuted for breaking into a device
- Configured using the **banner motd** *delimiter message delimiter* command from global configuration mode. The delimiting character can be any character as long as it isunique and does not occur in the message (e.g., **#$%^&***)
- **banner motd** # *the message of the day* #

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) is to be assigned to a switch **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**

IP Addressing Overview

- **Each end device** on a network (e.g., PCs, laptops, servers, printers, VoIP phones, security cameras, …) require an IP configuration consisting of:

  IP address

  Subnet mask

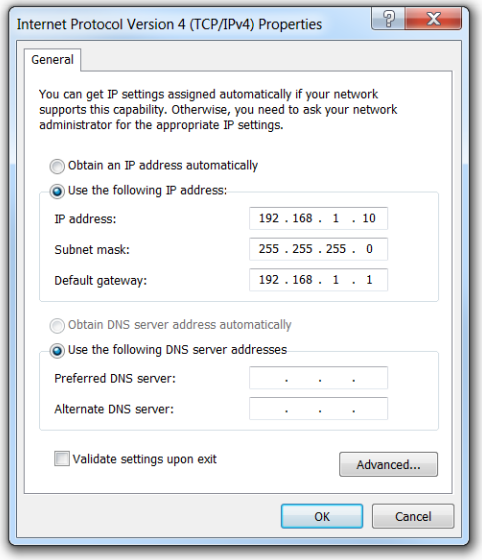
  Default gateway (optional for some devices)

- IPv4 addresses are displayed in dotted decimal format consisting of:

  4 decimal numbers **0 and 255**

  Separated by decimal points (dots)

  E.g., **192.168.1.10, 255.255.255.0, 192.168.1.1**



Interfaces and Ports

- Cisco IOS **Layer 2 switches** have physical ports for devices to connect. However, these ports **do not support** Layer 3 IP addresses
- To remotely connect to and manage a Layer 2 switch, it must be configured with one or more switch **virtual interfaces (SVIs)**
- Each switch has a **default VLAN 1 SVI**

Configure a Switch Virtual Interface

- **Enter interface configuration mode for VLAN 1.**
- **Configure the IPv4 address as 192.168.10.2 and the subnet mask as 255.255.255.0.**
- **Enable the interface.**

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.10.2 255.255.255.0
Switch(config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
Switch(config-if)#
```

You have successfully configured the switch virtual interface for VLAN 1.

Basic Switch Management

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

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**

Basic Switch Management

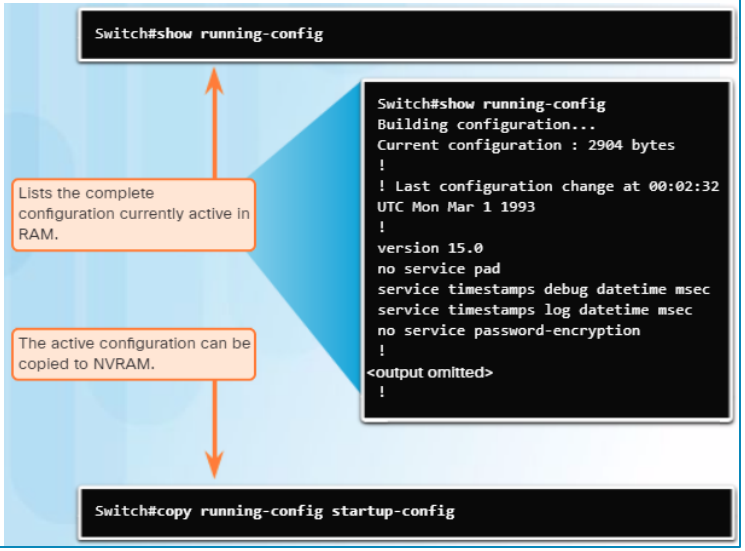
- Preparing for Basic Switch Management

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**

Save the Running Configuration File

- Cisco devices use a **running configuration** file and a **startup configuration** file
  - The running configuration file is stored in RAM and contains the current configuration on a Cisco IOS device.
    - Configuration changes are stored in this file.
    - If power is interrupted, the running config is lost.
    - Use the **show startup-config** command to display contents.
  - The startup config file is stored in NVRAM and contains the configuration that will be used by the device upon reboot.
    - Typically the running config is saved as the startup config.
    - If power is interrupted, it is not lost or erased.
    - Use the **show running-config** command to display contents

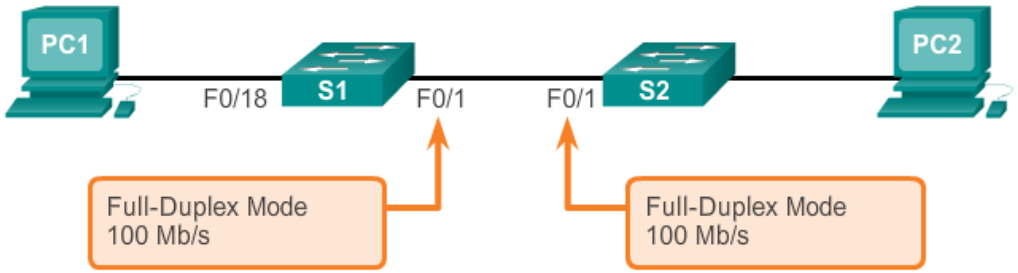
Use the **copy running-config startup-config command** to save the running configuration



Basic Switch Management

- Preparing for **Basic Switch Management**

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`**

Basic Switch Management

- **Auto-MDIX Feature**
- Certain cable types (**straight-through or crossover**) were required when connecting devices
- 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.**

Basic Switch Management

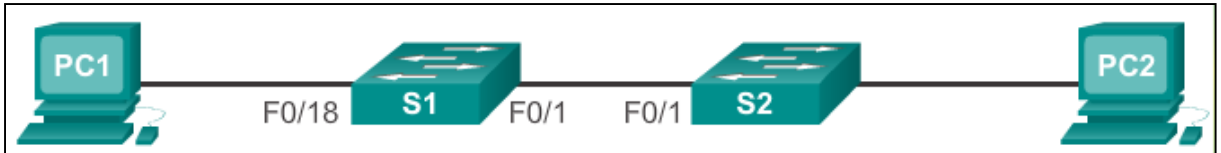
- Preparing for **Basic Switch Management**

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`

Basic Switch Management

- Preparing for **Basic Switch Management**




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

Basic Switch Management

- **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**

Basic Switch Management

- **Verifying Switch** Port Configuration

Display interface status and statistics.

```
S1# show interface 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>
```

Basic Switch Management

- **Verifying Switch** Port Configuration

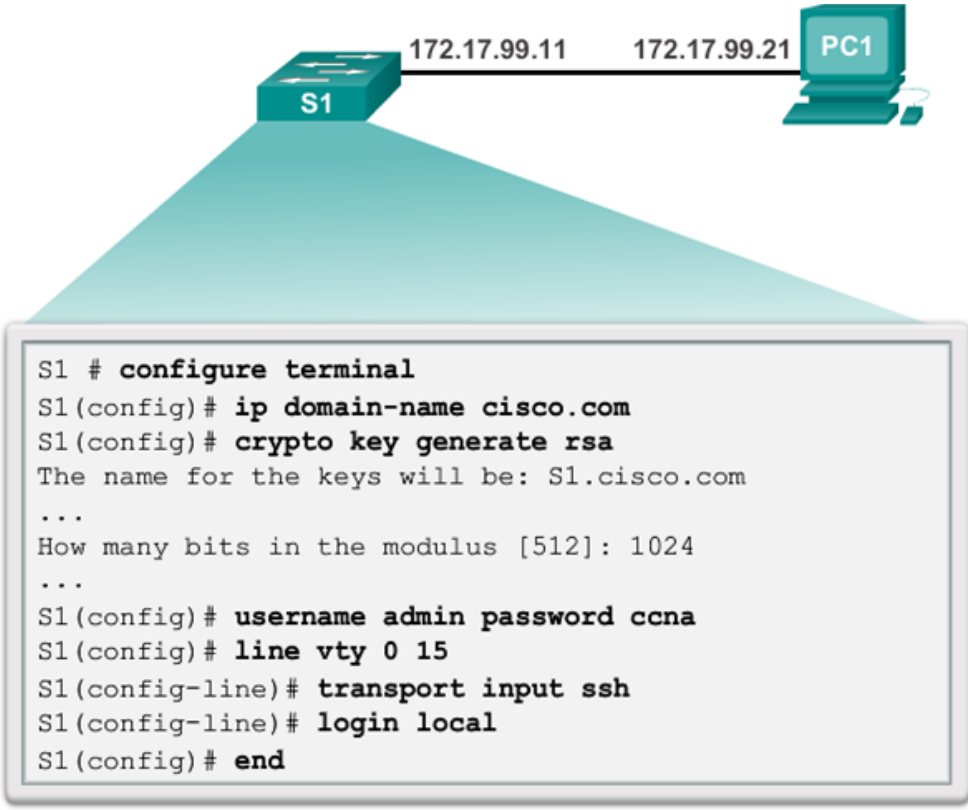
Parameter	Description
Runts	Packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
Giants	Packets that are discarded because they exceed the maximum packet size for the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
Input errors	Total number of errors. It includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
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	Jammed signal could not reach to ends.

SSH Operation

- **Secure Shell (SSH**) is a protocol that **provides a secure** (encrypted), command-line based connection to a remote device
- Because its strong encryption features, **SSH should replace Telnet** for management connections.
- SSH uses **TCP port 22**, by default. Telnet uses **TCP port 23**

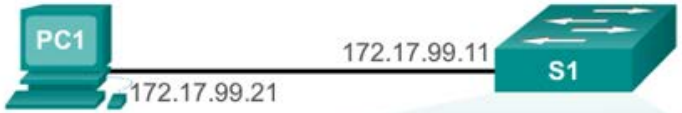
SSH Operation

- Configuring **SSH**



SSH Operation

- Configuring **SSH**



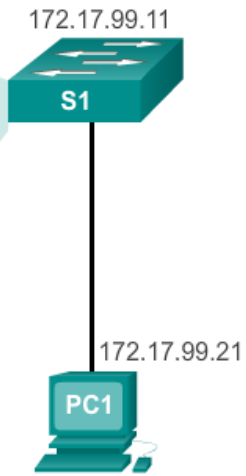

```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAa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

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

Switch

- Switch **Port Configuration**

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 Port Configuration

- 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.

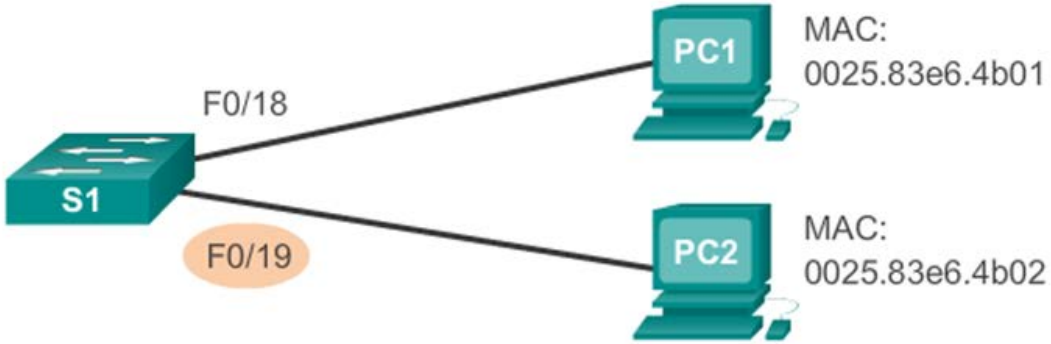
Switch Port Configuration

- 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.
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 Configuration

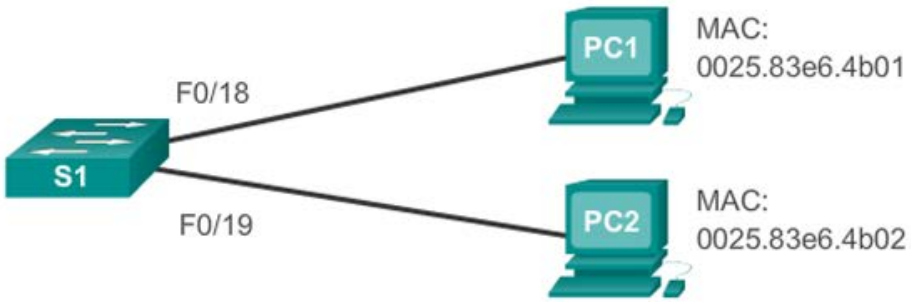
- Configuring **Dynamic Port Security**




```
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
```

Switch Port Configuration

- Configuring **Dynamic Port Security**




```
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 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

- The switch communicates these events through console messages.

```
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

- The switch communicates these events through console messages.

```
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
```

QA


Sister Cities
Eilat
Jakarta
Giza
Athens 6925 mi
Berlin 5759 mi
Lusaka 10,007 mi
Split 6386 mi
7406 mi Makati

Lab

Basic Switch Configuration

Lab