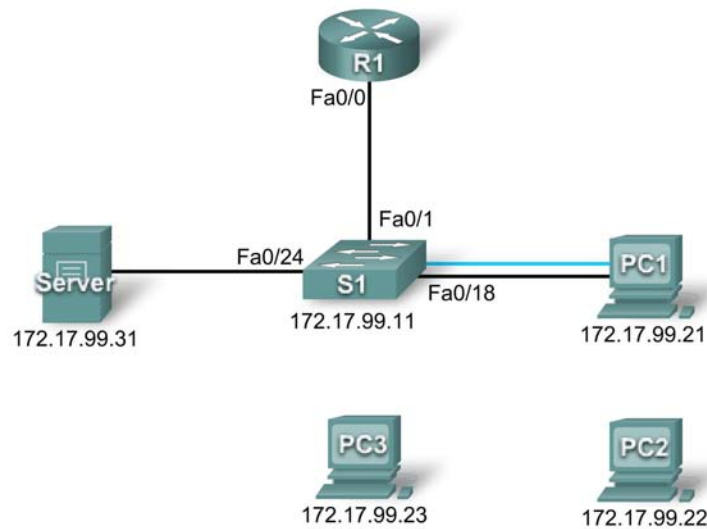


## PT Activity 2.6.1: Packet Tracer Skills Integration Challenge

### Topology Diagram



### Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	Fa0/0	172.17.99.1	255.255.255.0
S1	Fa0/1	172.17.99.11	255.255.255.0
PC1	NIC	172.17.99.21	255.255.255.0
PC2	NIC	172.17.99.22	255.255.255.0
Server	NIC	172.17.99.31	255.255.255.0

### Objectives

- Establish console connection to switch.
- Configure hostname and VLAN99.
- Configure the clock.
- Modify the history buffer.
- Configure passwords and console/Telnet access.
- Configure login banners.
- Configure the router.
- Configure the boot sequence.
- Solve duplex and speed mismatch.
- Manage the MAC address table.

- Configure port security.
- Secure unused ports.
- Manage the switch configuration file.

## Introduction

In this Packet Tracer Skills Integration Challenge activity, you will configure basic switch management, including general maintenance commands, passwords, and port security. This activity provides you an opportunity to review previously acquired skills.

### Task 1: Establish a Console Connection to a Switch

#### Step 1: Connect a console cable to S1.

For this activity, direct access to S1 **Config** and **CLI** tabs is disabled. You must establish a console session through PC1. Connect a console cable from PC1 to S1.

#### Step 2: Establish a terminal session.

From PC1, open a **Terminal** window and use the default **Terminal Configuration**. You should now have access to the **CLI** for S1.

#### Step 3: Check results.

Your completion percentage should be 6%. If not, click **Check Results** to see which required components are not yet completed.

### Task 2: Configure the Hostname and VLAN 99

#### Step 1: Configure the switch hostname as S1.

#### Step 2: Configure port Fa0/1 and interface VLAN 99.

Assign VLAN 99 to FastEthernet 0/1 and set the mode to access mode. These commands are discussed further in the next chapter.

```
S1(config)#interface fastethernet 0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 99
```

Configure IP connectivity on S1 using VLAN 99.

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
```

#### Step 3: Configure the default gateway for S1.

Configure the default gateway and then test connectivity. S1 should be able to ping R1.

#### Step 4: Check results.

Your completion percentage should be 26%. If not, click **Check Results** to see which required components are not yet completed. Also, make sure that interface VLAN 99 is active.

### Task 3: Configure the Clock Using Help

#### Step 1: Configure the clock to the current time.

At the privileged EXEC prompt, enter **clock ?**. Use Help to discover each additional step required to set the current time. Packet Tracer does not grade this command, so the completion percentage does not change.

#### Step 2: Verify that the clock is set to the current time.

Use the **show clock** command to verify that the clock is now set to the current time. Packet Tracer may not correctly simulate the time you entered.

### Task 4: Modify the History Buffer

#### Step 1: Set the history buffer to 50 for the console line.

#### Step 2: Set the history buffer to 50 for the vty lines.

#### Step 3: Check results.

Your completion percentage should be 32%. If not, click **Check Results** to see which required components are not yet completed.

### Task 5: Configure Passwords and Console/Telnet Access

#### Step 1: Configure the privileged EXEC password.

Use the encrypted form of the privileged EXEC mode password and set the password to **class**.

#### Step 2: Configure the passwords for console and Telnet.

Set the console and vty password to **cisco** and require users to log in.

#### Step 3: Encrypt passwords.

View the current configuration on S1. Notice that the line passwords are shown in clear text. Enter the command to encrypt these passwords.

#### Step 4: Check results.

Your completion percentage should be 41%. If not, click **Check Results** to see which required components are not yet completed.

### Task 6: Configure the Login Banner

If you do not enter the banner text exactly as specified, Packet Tracer does not grade your command correctly. These commands are case-sensitive. Also make sure that you do not include any spaces before or after the text.

#### Step 1: Configure the message-of-the-day banner on S1.

Configure the message-of-the-day as **Authorized Access Only**.

#### Step 2: Check results.

Your completion percentage should be 44%. If not, click **Check Results** to see which required components are not yet completed.

## Task 7: Configure the Router

### Step 1: Configure the router with the same basic commands you used on S1.

Routers and switches share many of the same commands. Access the **CLI** for R1 by clicking the device. Do the following on R1:

- Configure the hostname.
- Set the history buffer to 50 for both console and vty.
- Configure the encrypted form of the privileged EXEC mode password and set the password to **class**.
- Set the console and vty password to **cisco** and require users to log in.
- Encrypt the console and vty passwords.
- Configure the message-of-the-day as **Authorized Access Only**.
- Move the console cable to reconnect PC1 to S1.

### Step 2: Check results.

Your completion percentage should be 65%. If not, click **Check Results** to see which required components are not yet completed.

## Task 8: Configure the Boot Sequence

### Step 1: View current files stored in flash.

On S1, enter the command **show flash**. You should see the following files listed:

```
S1#show flash
```

```
Directory of flash:/
```

1	-rw-	4414921	<no date>	c2960-lanbase-mz.122-25.FX.bin
3	-rw-	4670455	<no date>	c2960-lanbase-mz.122-25.SEE1.bin
2	-rw-	616	<no date>	vlan.dat

```
32514048 bytes total (23428056 bytes free)
```

### Step 2: Configure S1 to boot using the second image listed.

Make sure your command includes the file system, which is **flash**.

**Note:** Packet Tracer does not show this command in the running configuration. In addition, if you reload the switch, Packet Tracer does not load the image you specified.

### Step 3: Check results.

Your completion percentage should be 68%. If not, click **Check Results** to see which required components are not yet completed.

## Task 9: Solve a Mismatch Between Duplex and Speed

### Step 1: Change the duplex and speed on S1.

PC1 and Server currently do not have access through S1 because of a mismatch between duplex and speed. Enter commands on S1 to solve this problem.

### Step 2: Verify connectivity.

Both PC1 and Server should now be able to ping S1, R1, and each other.

### Step 3: Check results.

Your completion percentage should be 74%. If not, click **Check Results** to see which required components are not yet completed.

## Task 10: Manage the MAC Address Table

### Step 1: View the current MAC address table.

What command would you use to display the MAC address table?

```
S1#  
      Mac Address Table  
-----  
  
Vlan    Mac Address      Type      Ports  
----    -  
99      0001.637b.b267    DYNAMIC   Fa0/24  
99      0004.9a32.8e01    DYNAMIC   Fa0/1  
99      0060.3ee6.1659    DYNAMIC   Fa0/18
```

The list of MAC address in your output may be different depending on how long it has been since you sent any packets across the switch.

### Step 2: Configure a static MAC address.

Network policy may dictate that all server addresses be statically configured. Enter the command to statically configure the MAC address of Server.

### Step 3: Check results.

Your completion percentage should be 76%. If not, click **Check Results** to see which required components are not yet completed.

## Task 11: Configure Port Security

### Step 1: Configure port security for PC1.

Use the following policy to establish port security on the port used by PC1:

- Enable port security
- Allow only one MAC address
- Configure the first learned MAC address to "stick" to the configuration
- Set the port to shut down if there is a security violation

**Note:** Only the enable port security step is graded by Packet Tracer and counted toward the completion percentage. However, all the port security tasks listed above are required to complete this activity successfully.

### Step 2: Verify port security.

Verify that port security is enabled for Fa0/18. Your output should look like the following output. Notice that S1 has not yet learned a MAC address for this interface.

What command generated the following output?

```
S1#  
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     : 0  
Configured MAC Addresses : 0  
Sticky MAC Addresses    : 0  
Last Source Address:Vlan : 0000.0000.0000:0  
Security Violation Count : 0
```

### Step 3: Force S1 to learn the MAC address for PC1.

Send a ping from PC1 to S1. Then verify that S1 has added the MAC address for PC1 to the running configuration.

```
!  
interface FastEthernet0/18  
  <output omitted>  
  switchport port-security mac-address sticky 0060.3EE6.1659  
  <output omitted>  
!
```

### Step 4: Test port security.

Remove the FastEthernet connection between S1 and PC1. Connect PC2 to Fa0/18. Wait for the link lights to turn green. If necessary, send a ping from PC2 to S1 to cause the port to shut down. Port security should show the following results:

```
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     : 1  
Configured MAC Addresses : 1  
Sticky MAC Addresses    : 0  
Last Source Address:Vlan : 00D0.BAD6.5193:99  
Security Violation Count : 1
```

Viewing the Fa0/18 interface shows that **line protocol is down (err-disabled)**, which also indicates a security violation.

```
S1#show interface fa0/18  
FastEthernet0/18 is down, line protocol is down (err-disabled)  
<output omitted>
```

### Step 5: Reconnect PC1 and re-enable the port.

To re-enable the port, disconnect PC2 from Fa0/18 and reconnect PC1. Interface Fa0/18 must be manually configured before returning to the active state.

### **Step 6: Check results.**

Your completion percentage should be 82%. If not, click **Check Results** to see which required components are not yet completed.

## **Task 12: Secure Unused Ports**

### **Step 1: Disable all unused ports on S1.**

Disable all ports that are currently not used on S1. Packet Tracer grades the status of the following ports: Fa0/2, Fa0/3, Fa0/4, Gig 1/1, and Gig 1/2.

### **Step 2: Check results.**

Your completion percentage should be 97%. If not, click **Check Results** to see which required components are not yet completed.

## **Task 13: Manage the Switch Configuration File**

### **Step 1: Save the current configuration to NVRAM for R1.**

### **Step 2: Back up the startup configuration files for S1 and R1 to Server.**

Back up the startup configuration file on S1 and R1 by uploading them to Server. Once complete, verify the server has the **R1-config** and **S1-config** files.

Move the console cable to reconnect PC1 to S1

### **Step 3: Check results.**

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.