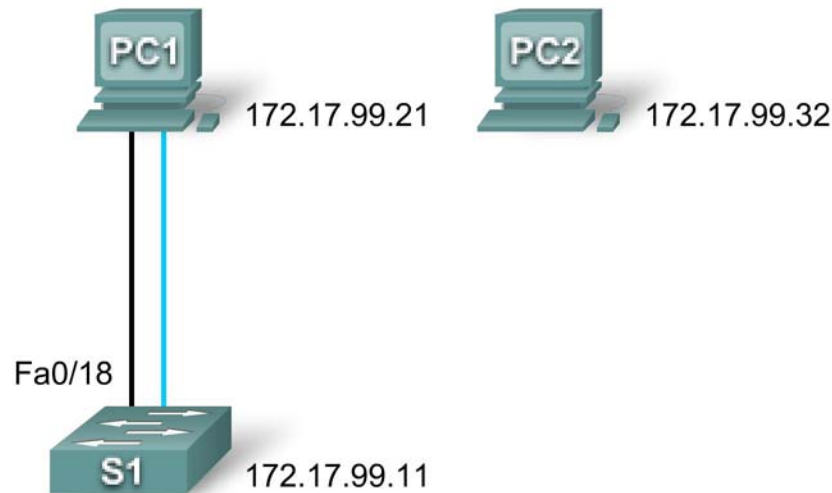# PT Activity 2.5.1: Basic Switch Configuration

Topology

NOTE TO USER: This activity is a variation of Lab 2.5.1. Packet Tracer may not support all the tasks specified in the hands-on lab. This activity should not be considered equivalent to completing the hands-on lab. Packet Tracer is not a substitute for a hands-on lab experience with real equipment.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC1	NIC	172.17.99.21	255.255.255.0	172.17.99.1
PC2	NIC	172.17.99.22	255.255.255.0	172.17.99.1
S1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1

Learning Objectives

- Clear an existing configuration on a switch.
- Verify the default switch configuration.
- Create a basic switch configuration.
- Manage the MAC address table.
- Configure port security.

Introduction

In this activity, you will examine and configure a standalone LAN switch. Although a switch performs basic functions in its default out-of-the-box condition, there are a number of parameters that a network

administrator should modify to ensure a secure and optimized LAN. This activity introduces you to the basics of switch configuration.

Task 1: Clear an Existing Configuration on a Switch

Step 1. Enter privileged EXEC mode by typing the enable command.

Click S1 and then the **CLI** tab. Issue the **enable** command to enter the privileged EXEC mode.

```
Switch>enable
Switch#
```

Step 2. Remove the VLAN database information file.

VLAN database information is stored separately from the configuration files in vlan.dat in flash. To remove the VLAN file, issue the **delete flash:vlan.dat** command.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]? [Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

Step 3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm] [Enter]
[OK]
Erase of nvram: complete
```

Step 4. Verify the VLAN information was deleted.

Verify that the VLAN configuration was deleted using the **show vlan** command.

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   VLAN10                           active
30   VLAN30                           active
1002 fddi-default                     active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

The VLAN information is still on the switch. Follow the next step to clear it.

Step 5. Reload the switch.

At the privileged EXEC mode prompt, enter the **reload** command to begin the process.

```
Switch#reload
Proceed with reload? [confirm] [Enter]
```

```
%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.

<output omitted>

Press RETURN to get started! [Enter]

Switch>
```

Task 2: Verify the Default Switch Configuration

Step 1. Enter privileged mode.

You can access all the switch commands in privileged mode. However, because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use. The privileged command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes are gained.

```
Switch>enable
Switch#
```

Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

Step 2. Examine the current switch configuration.

   a. Examine the current running configuration by issuing the **show running-config** command.

       1. How many Fast Ethernet interfaces does the switch have? _____

       2. How many Gigabit Ethernet interfaces does the switch have? _____

       3. What is the range of values shown for the vty lines? _____

   b. Examine the current contents of NVRAM by issuing the **show startup-config** command.

       1. Why does the switch give this response?

           _____

   c. Examine the characteristics of the virtual interface VLAN1 by issuing the command **show interface vlan1**.

       1. Is there an IP address set on the switch? _____

       2. What is the MAC address of this virtual switch interface? _____

       3. Is this interface up? _____

   d. Now view the IP properties of the interface using the **show ip interface vlan1**.

       1. What output do you see?

           _____

Step 3. Display Cisco IOS information.

   a. Display Cisco IOS information using the **show version** command.

       1. What is the Cisco IOS version that the switch is running? _____

       2. What is the system image filename? _____

       3. What is the base MAC address of this switch? _____

Step 4. Examine the Fast Ethernet interfaces.

   a.   Examine the default properties of the Fast Ethernet interface used by PC1 using the **show interface fastethernet 0/18** command.

```
Switch#show interface fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
   Hardware is Lance, address is 0060.5c36.4412 (bia 0060.5c36.4412)
   MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
        reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation ARPA, loopback not set
   Keepalive set (10 sec)
   Full-duplex, 100Mb/s

   <Output Omitted>
```

       1.   Is the interface up or down? _____

       2.   What event would make an interface go up? _____

       3.   What is the MAC address of the interface? _____

       4.   What is the speed and duplex setting of the interface? _____

Step 5. Examine VLAN information.

   a.   Examine the default VLAN settings of the switch using the **show vlan** command.

       1.   What is the name of VLAN 1? _____

       2.   Which ports are in this VLAN? _____

       3.   Is VLAN 1 active? _____

       4.   What type of VLAN is the default VLAN? _____

Step 6. Examine flash memory.

   a.   There are two commands to examine flash memory, **dir flash:** or **show flash**. Issue either one of the commands to examine the contents of the flash directory.

       1.   Which files or directories are found?

       _____

Step 7. Examine and save the startup configuration file.

Earlier in step 2 you saw that the startup configuration file did not exist. Make one configuration change to the switch and then save it. Type the following commands:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
```

To save the contents of the running configuration file to non-volatile RAM (NVRAM), issue the the **copy running-config startup-config** command.

```
Switch#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
```

Now display the contents of NVRAM. The current configuration has been written to NVRAM.

Task 3: Create a Basic Switch Configuration

Step 1. Assign a name to the switch.

Enter global configuration mode. Configuration mode allows you to manage the switch. Enter the configuration commands, one on each line. Notice that the command line prompt changes to reflect the current prompt and switch name. In the last step of the previous task, you configured the hostname. Here's a review of the commands used.

```
S1#configure terminal
S1(config)#hostname S1
S1(config)#exit
```

Step 2. Set the access passwords.

Enter **config-line** mode for the console. Set the login password to **cisco**. Also configure the vty lines 0 to 15 with the password **cisco**.

```
S1#configure terminal
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

Why is the **login** command required? _____

Step 3. Set the command mode passwords.

Set the enable secret password to class.

```
S1(config)#enable secret class
```

Step 4. Configure the Layer 3 address of the switch.

Set the IP address of the switch to 172.17.99.11 with a subnet mask of 255.255.255.0 on the internal virtual interface VLAN 99. The VLAN must first be created on the switch before the address can be assigned.

```
S1(config)#vlan 99
S1(config-vlan)#exit
S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
```

Step 5. Assign ports to the switch VLAN.

Assign Fastethernet 0/1, 0/8, and 0/18 to ports to VLAN 99.

```
S1(config)#interface fa0/1
S1(config-if)#switchport access vlan 99
S1(config-if)#interface fa0/8
S1(config-if)#switchport access vlan 99
S1(config-if)#interface fa0/18
```

```
S1(config-if)#switchport access vlan 99
S1(config-if)#exit
```

Step 6. Set the switch default gateway.

S1 is a layer 2 switch, so it makes forwarding decisions based on the Layer 2 header. If multiple networks are connected to a switch, you need to specify how the switch forwards the internetwork frames, because the path must be determined at Layer three. This is done by specifying a default gateway address that points to a router or Layer 3 switch. Although this activity does not include an external IP gateway, assume that you will eventually connect the LAN to a router for external access. Assuming that the LAN interface on the router is 172.17.99.1, set the default gateway for the switch.

```
S1(config)#ip default-gateway 172.17.99.1
S1(config)#exit
```

Step 7. Verify the management LANs settings.

Verify the interface settings on VLAN 99 with the **show interface vlan 99** command.

```
S1#show interface vlan 99
Vlan99 is up, line protocol is up
  Hardware is CPU Interface, address is 0060.47ac.1eb8 (bia 0060.47ac.1eb8)
  Internet address is 172.17.99.11/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, 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 Omitted>
```

What is the bandwidth on this interface? _____

What is the queuing strategy? _____

Step 8. Configure the IP address and default gateway for PC1.

Set the IP address of PC1 to 172.17.99.21, with a subnet mask of 255.255.255.0. Configure a default gateway of 172.17.99.11. Click PC1 and its **Desktop** tab then IP configuration to input the addressing parameters.

Step 9. Verify connectivity.

To verify the host and switch are correctly configured, ping the switch from PC1.

If the ping is not successful, troubleshoot the switch and host configuration. Note that this may take a couple of tries for the pings to succeed.

Step 10. Configure the port speed and duplex settings for a Fast Ethernet interface.

Configure the duplex and speed settings on Fast Ethernet 0/18. Use the **end** command to return to privileged EXEC mode when finished.

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#speed 100
S1(config-if)#duplex full
S1(config-if)#end
```

The default on the Ethernet interface of the switch is auto-sensing, so it automatically negotiates optimal settings. You should set duplex and speed manually only if a port must operate at a certain speed and duplex mode. Manually configuring ports can lead to duplex mismatches, which can significantly degrade performance.

Notice how the link between PC1 and S1 went down. Remove the **speed 100** and **duplex full** commands. Now verify the settings on the Fast Ethernet interface with the **show interface fa0/18** command.

```
S1#show interface fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Lance, address is 0060.5c36.4412 (bia 0060.5c36.4412)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
<Output omitted>
```

Step 11. Save the configuration.

You have completed the basic configuration of the switch. Now back up the running configuration file to NVRAM to ensure that the changes made will not be lost if the system is rebooted or loses power.

```
S1#copy running-config startup-config

Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
S1#
```

Step 12. Examine the startup configuration file.

To see the configuration that is stored in NVRAM, issue the **show startup-config** command from privileged EXEC (enable mode).

Are all the changes that were entered recorded in the file?

Task 4: Managing the MAC Address Table

Step 1. Record the MAC addresses of the hosts.

Determine and record the Layer 2 (physical) addresses of the PC network interface cards using the following steps:

- Click the PC.
- Select the **Desktop** tab.
- Click **Command Prompt**.
- Type the **ipconfig /all** command.

Step 2. Determine the MAC addresses that the switch has learned.

Display the MAC addresses using the **show mac-address-table** command in privileged EXEC mode. If there are no MAC addresses, ping from PC1 to S1 then check again.

```
S1#show mac-address-table
```

Step 3. Clear the MAC address table.

To remove the existing MAC addresses, use the **clear mac-address-table dynamic** command from privileged EXEC mode.

```
S1#clear mac-address-table dynamic
```

Step 4. Verify the results.

Verify that the MAC address table was cleared.

```
S1#show mac-address-table
```

Step 5. Examine the MAC table again.

Look at the MAC address table again in privileged EXEC mode. The table has not changed, ping S1 from PC1 and check again.

Step 6. Set up a static MAC address.

To specify which ports a host can connect to, one option is to create a static mapping of the host MAC address to a port.

Set up a static MAC address on Fast Ethernet interface 0/18 using the address that was recorded for PC1 in Step 1 of this task, 0002.16E8.C285.

```
S1(config)#mac-address-table static 0002.16E8.C285 vlan 99 interface
fastethernet 0/18
S1(config)#end
```

Step 7. Verify the results.

Verify the MAC address table entries.

```
S1#show mac-address-table
```

Step 8. Remove the static MAC entry.

Enter configuration mode and remove the static MAC by putting a **no** in front of the command string.

```
S1(config)#no mac-address-table static 0002.16E8.C285 vlan 99 interface
fastethernet 0/18
S1(config)#end
```

Step 9. Verify the results.

Verify that the static MAC address has been cleared with the **show mac-address-table static** command.

Task 5: Configuring Port Security

Step 1. Configure a second host.

A second host is needed for this task. Set the IP address of PC2 to 172.17.99.22, with a subnet mask of 255.255.255.0 and a default gateway of 172.17.99.11. Do not connect this PC to the switch yet.

Step 2. Verify connectivity.

Verify that PC1 and the switch are still correctly configured by pinging the VLAN 99 IP address of the switch from the host. If the pings were not successful, troubleshoot the host and switch configurations.

Step 3. Determine which MAC addresses that the switch has learned.

Display the learned MAC addresses using the **show mac-address-table** command in privileged EXEC mode.

Step 4. List the port security options.

Explore the options for setting port security on interface Fast Ethernet 0/18.

```
S1# configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#switchport port-security ?
  mac-address  Secure mac address
  maximum      Max secure addresses
  violation    Security violation mode
  <cr>
```

Step 5. Configure port security on an access port.

Configure switch port Fast Ethernet 0/18 to accept only two devices, to learn the MAC addresses of those devices dynamically, and to shutdown the port if a violation occurs.

```
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 2
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security violation shutdown
S1(config-if)#exit
```

Step 6. Verify the results.

Show the port security settings with the **show port-security interface fa0/18** command.

How many secure addresses are allowed on Fast Ethernet 0/18?
What is the security action for this port?

Step 7. Examine the running configuration file.

```
S1#show running-config
```
Are there statements listed that directly reflect the security implementation of the running configuration?

Step 8. Modify the port security settings on a port.

On interface Fast Ethernet 0/18, change the port security maximum MAC address count to 1.

```
S1(config-if)#switchport port-security maximum 1
```

Step 9. Verify the results.

Show the port security settings with the **show port-security interface fa0/18** command.

Have the port security settings changed to reflect the modifications in Step 8?

Ping the VLAN 99 address of the switch from PC1 to verify connectivity and to refresh the MAC address table.

Step 10. Introduce a rogue host.

Disconnect the PC attached to Fast Ethernet 0/18 from the switch. Connect PC2, which has been given the IP address 172.17.99.22 to port Fast Ethernet 0/18. Ping the VLAN 99 address 172.17.99.11 from the new host.

What happened when you tried to ping S1?

Note: Convergence may take up to a minute. Switch between **Simulation** and **Realtime** mode to accelerate convergence.

Step 11. Reactivate the port.

As long as the rogue host is attached to Fast Ethernet 0/18, no traffic can pass between the host and switch. Reconnect PC1 to Fast Ethernet 0/18, and enter the following commands on the switch to reactivate the port:

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#no shutdown
S1(config-if)#end
```

Step 12. Verify connectivity.

After convergence, PC1 should be able to again ping S1.

Step 13. Check results.

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