



UNIVERSITY  
of  
TECHNOLOGY,  
MAURITIUS

Module Weight: **25%**

Deadline: **31<sup>st</sup> December  
2018 @ 00:00Hours**  
Cohort: **PDITN18BFT**

## Lan Switching & Wireless LAN Assignment

This assignment is an individual assignment and consists of two parts: a Lab and an STP analysis situation. The lab will introduce some security concepts in Task 5 that were not covered during the lectures or practicals.

### Tasks

#### Lab:

1. You simply need to follow the instructions in the lab and note down your answers to the questions.  
*Note: I have adapted the steps to Packet Tracer simulation software as the original lab was intended on real physical hardware.*
2. You will have to compile your lab answers as part 1 of a word-processed report.
3. You will have also to save your final Packet Tracer simulation as **lab.pkt**.

[60 marks]

#### STP Analysis:

1. You simply have to analyze the topology given and determine the Root Bridge (RB), the Root Port for each switch, the Designated Port/s (DP) for each switch and finally the Blocking Port/s (BP) for each switch.
2. If you are short of time, you can print the topology and label the above with a pen and take a picture of same. You can then paste the picture in part 2 of your report. Otherwise, you can redraw the topology in any graphical or drawing software and include in Part 2 of your report.

[40 marks]

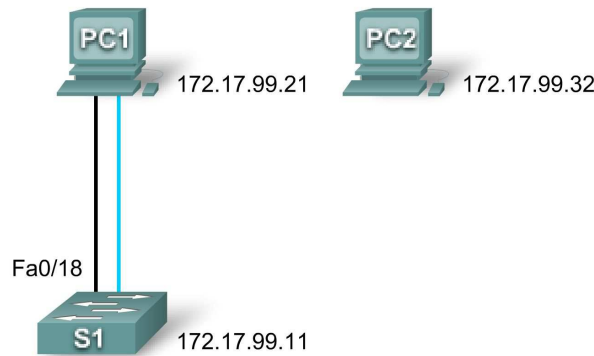
### Deliverables

You will have to submit your report containing answers to both part 1 (Lab) and part 2 (STP analysis topology).

You should also attach your lab.pkt file and zipped both files with filename as **your\_index\_number.zip** and email me at [pditn18b@rishiheerasing.net](mailto:pditn18b@rishiheerasing.net) before the deadline.

# Basic Switch Configuration Lab

## Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC1	NIC	172.17.99.21	255.255.255.0	172.17.99.11
PC2	NIC	172.17.99.32	255.255.255.0	172.17.99.11
SW1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1

## Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Clear an existing configuration on a switch
- Examine and verify the default configuration
- Create a basic switch configuration, including a name and an IP address
- Configure passwords to ensure that access to the CLI is secured
- Configure switch port speed and duplex properties for an interface
- Configure basic switch port security
- Manage the MAC address table
- Assign static MAC addresses
- Add and move hosts on a switch

## Scenario

In this lab, 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 lab introduces you to the basics of switch configuration. **Note: You will be using Packet Tracer Simulator and not real hardware so some physical steps might not be necessary and can be omitted.**

---

## Task 1: Cable, Erase, and Reload the Switch

### Step 1: Cable a network. (if you are working on an actual switch)

Cable a network that is similar to the one in the topology diagram. Create only a console connection (pale blue colour) with the switch for now. (Console port for PCs is RS-232; for Switch, it is Console)

You can use any current switch in this lab as long as it has the required interfaces shown in the topology. The output shown in this lab is from a **2960** switch. If you use other switches, the switch outputs and interface descriptions may appear different.

Note: PC2 is not initially connected to the switch. It is only used in Task 5.

### Step 2: Clear the configuration on the Switch.

Clear the configuration on the switch using the procedure in Appendix 1.

## 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. You will set passwords in Task 3.

The privileged EXEC 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. Enter privileged EXEC mode by entering the **enable** command.

```
Switch>enable
Switch#
```

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

### Step 2: Examine the current switch configuration.

Examine the current running configuration file.

```
Switch#show running-config
```

How many Fast Ethernet interfaces does the switch have? \_\_\_\_\_

How many Gigabit Ethernet interfaces does the switch have? \_\_\_\_\_

What is the range of values shown for the vty lines? \_\_\_\_\_

Examine the current contents of NVRAM:

```
Switch#show startup-config
startup-config is not present
```

Why does the switch give this response?

---

Examine the characteristics of the virtual interface VLAN1:

```
Switch#show interface vlan1
```

---

Is there an IP address set on the switch? \_\_\_\_\_

What is the MAC address of this virtual switch interface? \_\_\_\_\_

Is this interface up? \_\_\_\_\_

Now view the IP properties of the interface:

```
Switch#show ip interface vlan1
```

What output do you see? \_\_\_\_\_

### Step 3: Display Cisco IOS information.

Examine the following version information that the switch reports.

```
Switch#show version
```

What is the Cisco IOS simulated software version that the switch is running? \_\_\_\_\_

What is the base MAC address of this switch? \_\_\_\_\_

### Step 4: Examine the Fast Ethernet interfaces.

Examine the default properties of the Fast Ethernet interface 0/18 to be to be connected to PC1 later.

```
Switch#show interface fastethernet 0/18
```

Is the interface up or down? \_\_\_\_\_

What event would make an interface go up? \_\_\_\_\_

What is the MAC address of the interface? \_\_\_\_\_

What is the speed and duplex setting of the interface? \_\_\_\_\_

### Step 5: Examine VLAN information.

Examine the default VLAN settings of the switch.

```
Switch#show vlan
```

What is the name of VLAN 1? \_\_\_\_\_

Which ports are in this VLAN? \_\_\_\_\_

Is VLAN 1 active? \_\_\_\_\_

What type of VLAN is the default VLAN? \_\_\_\_\_

### Step 6 Examine flash memory.

Issue one of the following commands to examine the contents of the flash directory.

```
Switch#dir flash:
```

or

```
Switch#show flash
```

Which files or directories are found?

---

---

The output should look similar to this:

Directory of flash:

```
618  -rwx  4671175      <no date>          c2960-lanbase-mz.122-25.SEE3.bin
```

```
32514048 bytes total (24804864 bytes free)
```

What is the name of the Cisco IOS image file? \_\_\_\_\_

### Step 7: Examine the startup configuration file.

To view the contents of the startup configuration file, issue the **show startup-config** command in privileged EXEC mode.

```
Switch#show startup-config
startup-config is not present
```

Why does this message appear? \_\_\_\_\_

Let's 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 SW1
SW1(config)#exit
SW1#
```

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

```
SW1#copy running-config startup-config
Destination filename [startup-config]?  (enter)
Building configuration...
[OK]
```

Note: This command is easier to enter by using the **copy run start** abbreviation.

Now display the contents of NVRAM using the **show startup-config** command.

```
SW1#show startup-config
Using 1170 out of 65536 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname S1
!
<output omitted>
```

---

The current configuration has been written to NVRAM.

### Task 3: Create a Basic Switch Configuration

#### Step 1: Assign a name to the switch.

In the last step of the previous task, you configured the hostname. Here's a review of the commands used.

```
Switch# configure terminal
Switch(config)#hostname SW1
SW1(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**.

```
SW1#configure terminal
Enter the configuration commands, one for each line. When you are finished,
return to global configuration mode by entering the exit command or pressing
Ctrl-Z.
```

```
SW1(config)#line console 0
SW1(config-line)#password cisco
SW1(config-line)#login
SW1(config-line)#line vty 0 15
SW1(config-line)#password cisco
SW1(config-line)#login
SW1(config-line)#exit
```

Why is the **login** command required? \_\_\_\_\_

#### Step 3. Set the command mode passwords.

Set the enable secret password to **pditn4104**. This password protects access to privileged EXEC mode.

```
SW1(config)#enable secret pditn4104
```

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

Before you can manage SW1 remotely from PC1, you need to assign the switch an IP address. The default configuration on the switch is to have the management of the switch controlled through VLAN 1. However, a best practice for basic switch configuration is to change the management VLAN to a VLAN other than VLAN 1.

For management purposes, we will use VLAN 99. The selection of VLAN 99 is arbitrary and in no way implies you should always use VLAN 99.

First, you will create the new VLAN 99 on the switch. Then you will 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.

```
SW1(config)#vlan 99
SW1(config-vlan)#exit
SW1(config)#interface vlan99
%LINK-5-CHANGED: Interface VLAN 99, changed state to up

SW1(config-if)#ip address 172.17.99.11 255.255.255.0
SW1(config-if)#no shutdown
```

---

```
SW1(config-if)#exit
SW1(config)#
```

Notice that the VLAN 99 interface protocol is in the down state even though you entered the command **no shutdown**. The protocol interface is currently down because no switchports are assigned to VLAN 99.

Assign all user ports to VLAN 99.

```
SW1#configure terminal
SW1(config)#interface range fa0/1 - 24
SW1(config-if-range)#switchport access vlan 99
SW1(config-if-range)#exit
SW1(config)#
```

Now, connect PC1 to interface fa0/18 on SW1 using a straight-through cable. Examine the CLI window output, there should be lines similar to those:

```
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

#### **Step 5: Set the switch default gateway.**

SW1 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 an external IP gateway is not needed, 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.

```
SW1(config)#ip default-gateway 172.17.99.1
SW1(config)#exit
```

#### **Step 6: Verify the management LANs settings.**

Verify the interface settings on VLAN 99.

```
SW1#show interface vlan 99
```

What is the bandwidth on this interface? \_\_\_\_\_

What are the VLAN states? VLAN 99 is \_\_\_\_\_ Line protocol is \_\_\_\_\_

What is the queuing strategy? \_\_\_\_\_

#### **Step 7: 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.

#### **Step 8: Verify connectivity.**

To verify the host and switch are correctly configured, ping the IP address of the switch (172.17.99.11) from PC1.

Was the ping successful? \_\_\_\_\_

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

---

### Step 9: 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.

```
SW1#configure terminal
SW1(config)#interface fastethernet 0/18
SW1(config-if)#speed 100
SW1(config-if)#duplex full
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state
to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
SW1(config-if)#end
```

The line protocol for both interface FastEthernet 0/18 and interface VLAN 99 will go down.

Both line protocol and interface VLAN 99 go down because of the mismatch in duplex mode (full-duplex) on the switch port 18 compared to the interface on PC1 (half-duplex in Auto mode).

To correct this problem, manually uncheck the Auto checkbox in the PC 1 FastEthernet0 interface. Select Full-duplex instead of default half-duplex mode. Both line protocol and VLAN99 interface should go back up in the CLI window,

Verify the new duplex and speed settings on the Fast Ethernet interface.

```
SW1#show interface fastethernet 0/18
```

### Step 10: 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.

```
SW1#copy running-config startup-config
Destination filename [startup-config]?[Enter] Building configuration...
[OK]
SW1#
```

### Step 11: Examine the startup configuration file.

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

```
SW1#show startup-config
```

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:

**You can go in Destop > Command Prompt and enter**

```
PC> ipconfig /all
```

PC1: \_\_\_\_\_

PC2: \_\_\_\_\_

---

Ping the VLAN 99 IP address (172.17.99.11) of the switch from PC1

**Step 2: Determine the MAC addresses that the switch has just learned.**

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

```
SW1#show mac-address-table
```

How many dynamic addresses are there? \_\_\_\_\_

How many MAC addresses are there in total? \_\_\_\_\_

Do the dynamic MAC addresses match the host MAC addresses? \_\_\_\_\_

**Step 3: List the show mac-address-table options.**

```
SW1#show mac-address-table ?
```

How many options are available for the **show mac-address-table** command? \_\_\_\_\_

Note: MAC Address learned by switch have a timeout typically of 120 seconds. This is why we had to ping VLAN 99 interface again. If we didn't ping again, you will not have seen any entries. However, in a real PC, there would always be applications or services running that will continuously ping and hence maintain the MAC address table.

**Step 4: Clear the MAC address table.**

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

```
SW1#clear mac-address-table dynamic
```

**Step 5: Verify the results.**

Verify that the MAC address table was cleared.

```
SW1#show mac-address-table
```

How many static MAC addresses are there? \_\_\_\_\_

How many dynamic addresses are there? \_\_\_\_\_

**Step 6: Examine the MAC table again.**

Ping the VLAN 99 IP address of the switch from PC1

```
SW1#show mac-address-table
```

How many dynamic addresses are there? \_\_\_\_\_

---

### Step 7: 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. The MAC address **00e0.2917.1884** is used as an example only. You must use the MAC address of your PC1, which is different than the one given here as an example.

```
SW1(config)#mac-address-table static 00e0.2917.1884 vlan 99 interface
fastethernet 0/18
```

### Step 8: Verify the results.

Verify the MAC address table entries.

```
SW1#show mac-address-table
```

How many total MAC addresses are there? \_\_\_\_\_  
How many static addresses are there? \_\_\_\_\_

### Step 10: Remove the static MAC entry.

To complete the next task, it will be necessary to remove the static MAC address table entry. Enter configuration mode and remove the command by putting a **no** in front of the command string.

Note: The MAC address 00e0.2917.1884 is used in the example only. Use the MAC address for your PC1.

```
SW1(config)#no mac-address-table static 00e0.2917.1884 vlan 99 interface
fastethernet 0/18
```

### Step 10: Verify the results.

Verify that the static MAC address has been cleared.

```
SW1#show mac-address-table
```

How many total static MAC addresses are there? \_\_\_\_\_

## 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 172.17.99.32, 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.

Were the pings successful? \_\_\_\_\_

If the answer is no, troubleshoot the host and switch configurations.

### Step 3: Copy the host MAC addresses.

Write down the MAC addresses from Task 4, Step 1.

---

PC1\_\_\_\_\_

PC2\_\_\_\_\_

**Step 4: 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.

```
SW1#show mac-address-table
```

How many dynamic addresses are there? \_\_\_\_\_

Do the MAC addresses match the host MAC addresses? \_\_\_\_\_

**Step 5: List the port security options.**

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

```
SW1# configure terminal
SW1(config)#interface fastethernet 0/18
SW1(config-if)#switchport port-security ?
```

```
mac-address   Secure mac address
maximum       Max secure addresses
violation     Security violation mode
<cr>
```

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

**Step 6: 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 block traffic from invalid hosts if a violation occurs.

```
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security maximum 2
SW1(config-if)#switchport port-security mac-address sticky
SW1(config-if)#switchport port-security violation protect
SW1(config-if)#exit
```

**Step 7: Verify the results.**

Show the port security settings.

```
SW1#show port-security
```

How many secure addresses are allowed on Fast Ethernet 0/18? \_\_\_\_\_

What is the security action for this port? \_\_\_\_\_

**Step 8: Examine the running configuration file.**

```
SW1#show running-config
```

Are there statements listed that directly reflect the security implementation of the running configuration?

\_\_\_\_\_

---

### Step 9: Modify the port security settings on a port.

On interface Fast Ethernet 0/18, change the port security maximum MAC address count to 1 and to shut down if a violation occurs.

```
SW1(config-if)#switchport port-security maximum 1
SW1(config-if)#switchport port-security violation shutdown
```

### Step 10: Verify the results.

Show the port security settings.

```
SW1#show port-security
```

Have the port security settings changed to reflect the modifications in Step 9? \_\_\_\_\_

Ping the VLAN 99 address of the switch from PC1 to verify connectivity and to refresh the MAC address table. You should now see the MAC address for PC1 “stuck” to the running configuration.

```
S1#show run
```

```
Building configuration...
```

```
<output omitted>
```

```
!
```

```
interface FastEthernet0/18
```

```
switchport access vlan 99
```

```
switchport mode access
```

```
switchport port-security
```

```
switchport port-security mac-address sticky
```

```
switchport port-security mac-address sticky 00e0.2917.1884
```

```
speed 100
```

```
duplex full
```

```
!
```

```
<output omitted>
```

### Step 11: Introduce a rogue host.

Disconnect PC1 and connect PC2 to port Fast Ethernet 0/18. Ping the VLAN 99 address 172.17.99.11 from the new host. Wait for the amber link light to turn green. Once it turns green, it should almost immediately turn off. {If you are fast enough that is :) }

Record any observations: \_\_\_\_\_

---

### Step 12: Show port configuration information.

To see the configuration information for just Fast Ethernet port 0/18, issue the following command in privileged EXEC mode:

```
SW1#show interface fastethernet 0/18
```

What is the state of this interface?

Fast Ethernet0/18 is \_\_\_\_\_ Line protocol is \_\_\_\_\_

### Step 13: Reactivate the port.

If a security violation occurs and the port is shut down, you can use the **no shutdown** command to reactivate it. However, as long as the rogue host is attached to Fast Ethernet 0/18, any traffic from the

---

host disables the port. Reconnect PC1 to Fast Ethernet 0/18, and enter the following commands on the switch: (Note: These might not be needed if using a simulator like Packet Tracer)

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

You should see that both VLAN interface and line protocol should be up and running in CLI window.

#### **Step 14: Cleanup**

Unless directed otherwise, clear the configuration on the switches, turn off the power to the host computer and switches, and remove and store the cables. (If you are working on real switches).

## **Appendix 1**

### **Erasing and Reloading either a simulated or real Switch**

For the majority of labs, it is necessary to start with an unconfigured switch. Using a switch with an existing configuration may produce unpredictable results. These instructions show you how to prepare the switch prior to starting the lab. These instructions are for the 2960 switch; however, the procedure for the 2900 and 2950 switches is the same.

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

If prompted for a password, enter **pditn4104**. If that does not work, ask the instructor.

```
Switch>enable
```

#### **Step 2: Remove the VLAN database information file.**

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

If there is no VLAN file, this message is displayed:

```
%Error deleting flash:vlan.dat (No such file or directory)
```

#### **Step 3: Remove the switch startup configuration file from NVRAM.**

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press Enter to confirm.

The response should be:

```
Erase of nvram: complete
```

#### **Step 4: Check that the VLAN information was deleted.**

Verify that the VLAN configuration was deleted in Step 2 using the **show vlan** command.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the **reload** command.

---

If previous VLAN configuration information is still present (other than the default management VLAN 1), you must power-cycle the switch (hardware restart ) instead of issuing the **reload** command. To power-cycle the switch, remove the power cord from the back of the switch or unplug it, and then plug it back in.

**Step 5: Restart the software.**

Note: This step is not necessary if the switch was restarted using the power-cycle method (on physical switch.)

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

```
Switch(config)#reload
```

The responding line prompt will be:

```
System configuration has been modified. Save? [yes/no]:
```

Type **n** and then press **Enter**.

The responding line prompt will be:

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

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

```
Would you like to enter the initial configuration dialog? [yes/no]: Type n and then press Enter.
```

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

# STP Analysis Topology

