LAB MANUAL-4

CONFIGURATION OF HUB AND SWITCHES ON CISCO PACKET TRACER

Packet Tracer is a cross-platform simulation program designed by Cisco Systems that allows users to create network topologies, software allows users to simulate the configuration of Cisco routers and switches using a command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit.

AIM: 1) BASIC LAN CONFIGURATION USING HUBS AND SWITCHES:

1. Open terminal window and type packet tracer (By using this command, packet tracer will be opened which is already installed in PC)

   In Packet tracer window, different symbols of PC, Routers, Hubs and Switches are displayed on bottom left side. To implement the scenario of Hub,

2. Select Hub > Generic Hub (Drag and drop it on window, you can select any hub. Each type of hubs support various number of ports.)

3. Select End devices > Generic (Drag and drop it on window)

4. Pick necessary components to implement the scenario of figure 1

5. Select Connections > Copper Straight Through

   Left click on hub (Port0, Port1 .... Port n will be displayed, select any one port option) and then left click on any unconnected end device (RS232 and FastEthernet0,

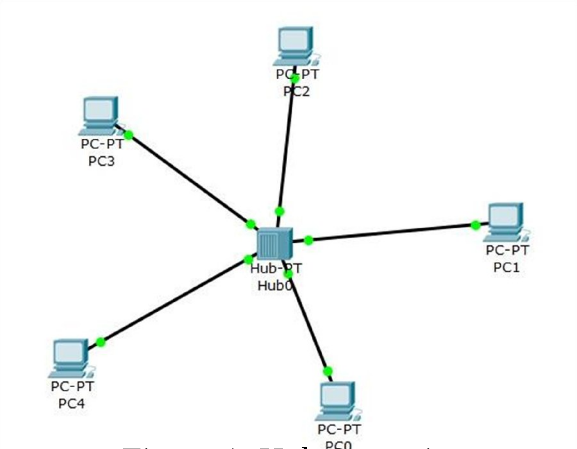
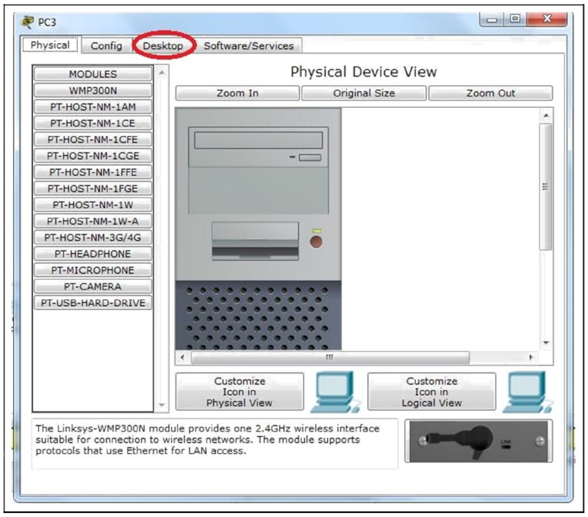


Figure 1: Hub Scenario



The Linksys-WMP300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The module supports protocols that use Ethernet for LAN access.

Figure 2: Display Window of End Device

FastEthernet1 ... Fast Ethernet n option will be displayed, select any fast Ethernet option.)

6. Left click on End Device, windows shown in figure 2 is displayed.
7. In display window select Desktop > IP Configuration
8. Select Static > IP Address > enter IP Address > Click on subnet Mask
9. Close the current assignment window and configure the remaining end devices in a same way with different IP address.

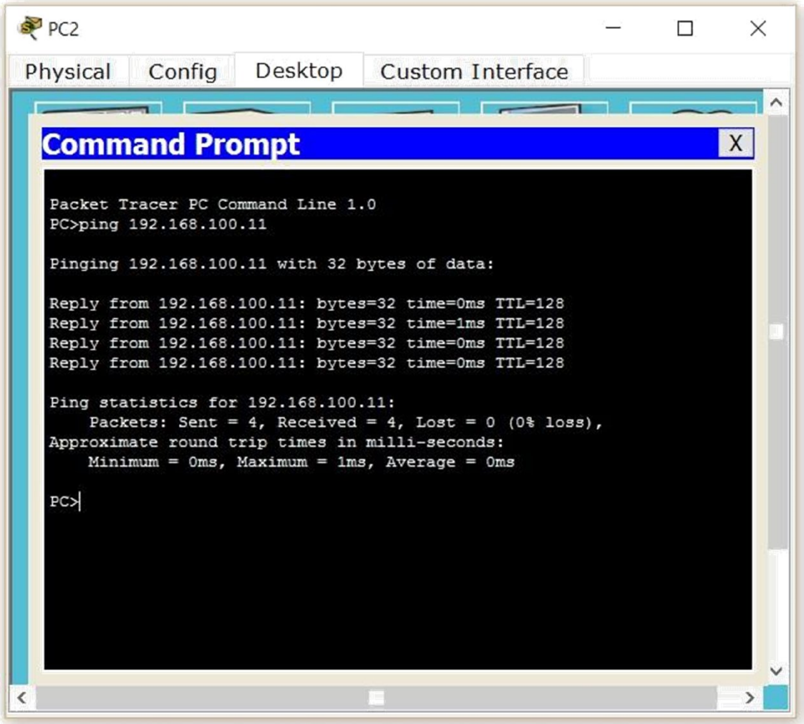
   Assign IP address e.g. 192.168.1.100, 192.168.1.101, 192.168.1.102, 192.168.1.103 and 192.168.1.104.
10. To check the network connectivity, left click on end device > Desktop > Command Prompt
11. Type the following command on command prompt ping IP Address of other end device. When connection is successfully established, following output can be seen (shown in figure 3).

    For failed connection following output can be seen (shown in figure 4)
12. Save your workspace by using File > Save As > Hub

Repeat the above procedure. Instead of hub, use switch and implement the scenario shown in figure 5

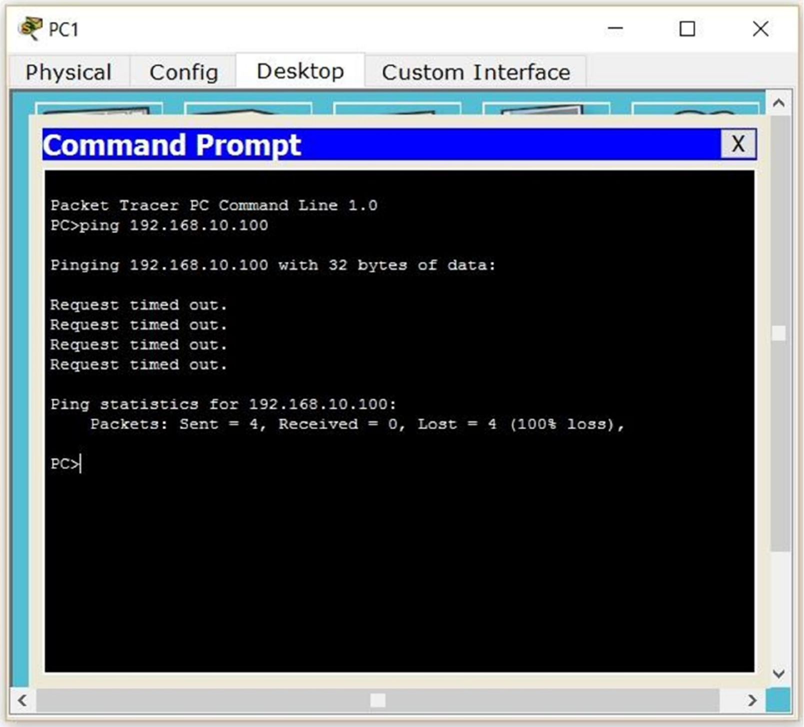
By left click on the switches (FastEthernet0/1, FastEthernet0/2 ... FastEthernet0/n) will be displayed. Repeat step 5 to 11.

Save your workspace by using File > Save As > Switch



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.100.11

Pinging 192.168.100.11 with 32 bytes of data:

Reply from 192.168.100.11: bytes=32 time=0ms TTL=128
Reply from 192.168.100.11: bytes=32 time=1ms TTL=128
Reply from 192.168.100.11: bytes=32 time=0ms TTL=128
Reply from 192.168.100.11: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.100.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

Figure 3: Ping Successful



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Figure 4: Ping Timeout

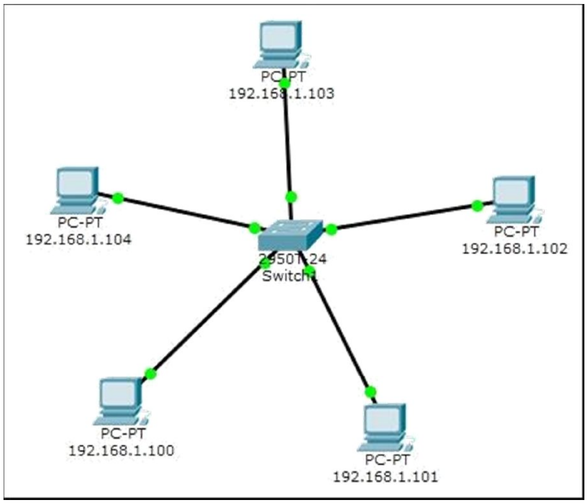


Figure 5: Switch Scenario

AIM 2) Brodcast and Collision domain in Hub and switch

Till now, we were working in real time domain. Now, we will be switching to Simulation domain Filters have the options of different protocols e.g. ICMP, ARP, OSPF, DNS etc.

1. Choose any two end devices (one should act as a source and other one as a destination)
2. Click on Message icon (Simple PDU), displayed in right side of the window.
3. Click on Source end device
4. Click on Destination end device

You may see two packets appearing at souce end device. Out of which, one corresponds to ARP (Address Resolution Protocol) and another corresponds to ICMP (Internet Control Message Protocol).

1. Click on Capture=Forward in simulation panel.
2. Broadcast nature of hub can be observed.
3. Click on Reset Simulation in simulation panel.
4. Click on delete option shown in bottom of window.

To observe collision domain,

1. Choose two pairs of source and destination end points.
2. Repeat the above procedure for both pairs simultaneously.
3. Two packets will be leaving the source at the same time.
4. Hence, collision can be observed at hub.

Brodcast and Collision domain in Switch

Repeat the above procedure (broadcast and collision domain in hub) and observe the broadcast and collision domain in switch.

Note down your observations from this exercise.

VLAN Configuration

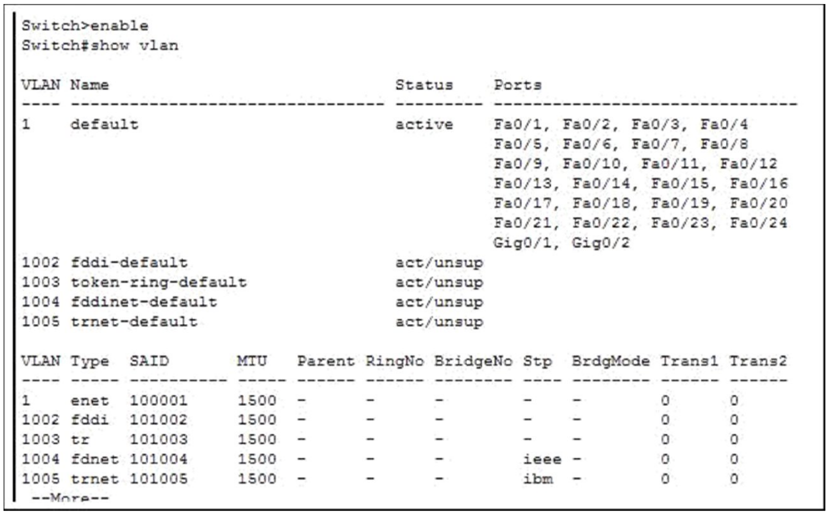
Consider the same scenario as shown in figure 5. Follow the below mentioned steps:

Click on switch

Click on CLI

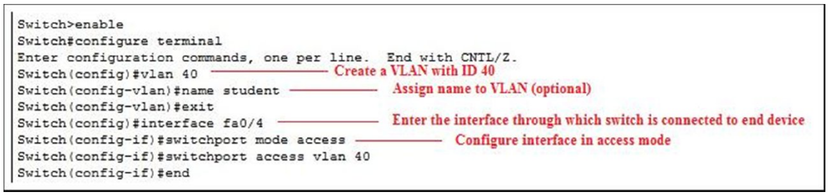
Type enable to go from user execution mode privileged execution mode

Type show vlan and you will get to see the output as shown in figure 6



```
Switch>enable
Switch#show vlan

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
                                                Gig0/1, Gig0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
 --More--
```

Figure 6: "show vlan" Command Output



```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 40
Switch(config-vlan)#name student
Switch(config-vlan)#exit
Switch(config)#interface fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config-if)#end
```

Create a VLAN with ID 40

Assign name to VLAN (optional)

Enter the interface through which switch is connected to end device

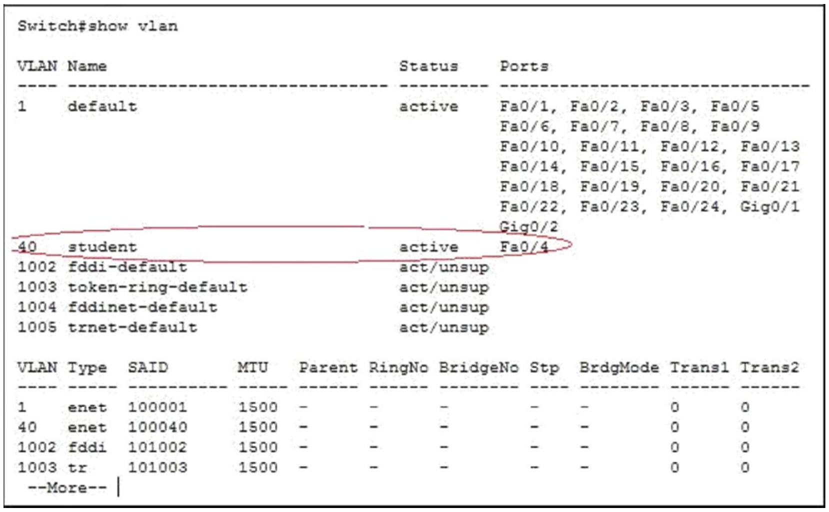
Configure interface in access mode

Figure 7: STEP 1 : VLAN Configuration on switch

Choose one end device (PC) to which you want to put in different VLAN. Note down the interface through which our switch is connected to end device. In our case we consider end device named 192.168.1.104 in different vlan network. (named vlan 40).

Follow the commands shown in figure 7 and figure 8.

ping the end device which you recently configured on different vlan. Observe the output. As it is shifted to different network, it becomes unreachable.



```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, 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, Gig0/1
                                                Gig0/2
40   student                          active    Fa0/4
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
 --More-- |
```

Figure 8: STEP 2 : Addition of VLAN

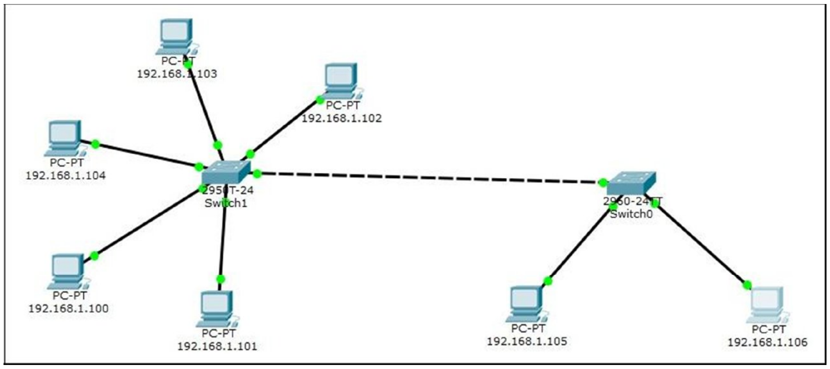
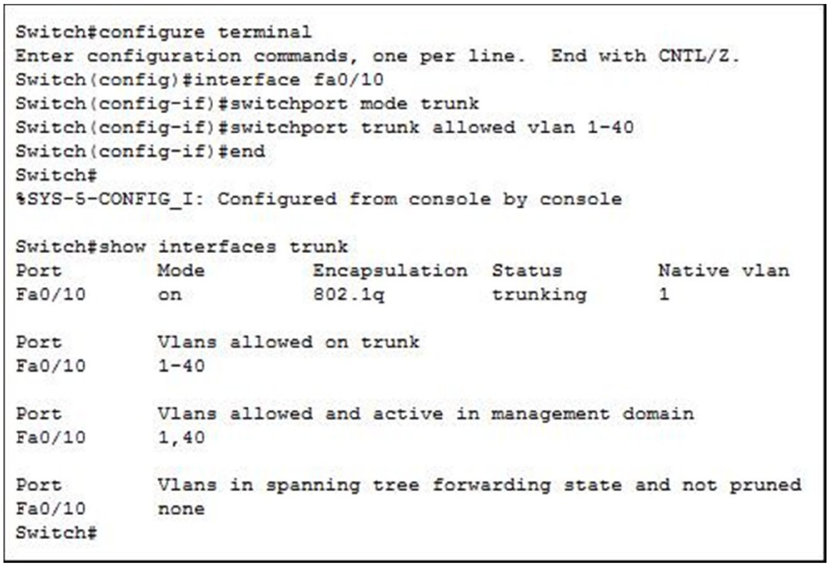


Figure 9: VLAN Trunking scenario

Now configure the scenario shown in figure 9.

1. Both newly added PCs should be assign IP of same network as the earlier one.
2. Configure any one PC in vlan network created earlier.
3. Follow the same steps mentioned in figure 7
4. Interface between two switched should be configured as a trunk, so that it can carry tracs of multiple VLANs.
5. Follow the steps shown in figure 10



```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa0/10
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 1-40
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/10      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/10      1-40

Port        Vlans allowed and active in management domain
Fa0/10      1,40

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/10      none
Switch#
```

Figure 10: Trunk Configuration

.