CSCI 5010 – Fundamentals of Data Communications

Lab 4 – VLANs, trunking and inter-VLAN routing

University of Colorado Boulder
Department of Computer Science
Network Engineering

Professor Levi Perigo, Ph.D.

Summary

The foundational layer to any network revolves around switching. This lab is intended to be an overview of VLANs, trunk links and inter-VLAN routing.

The questions in the lab are intentionally vague. The purpose of this is for you not only to research, investigate, and learn the technologies, but also become proficient at interpreting both non-technical and technical questions. Being able to research and discover answers on your own will be critical as you progress in your career.

- Learn how to create VLANs within a single switch
- Learn how to create VLANs across multiple switches
- Learn how to achieve Inter-VLAN communication using trunking (802.1q) and “routing on a stick”

Objective 1 - Switch VLAN Configuration

This objective will configure multiple VLANs on a single switch.

Diagram 1

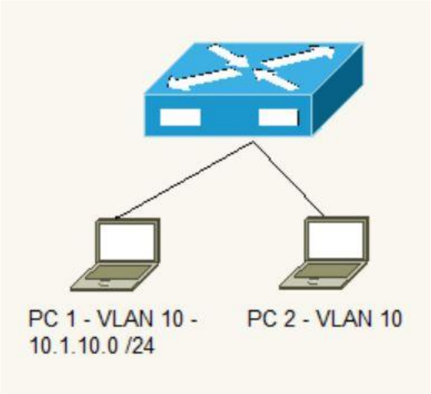
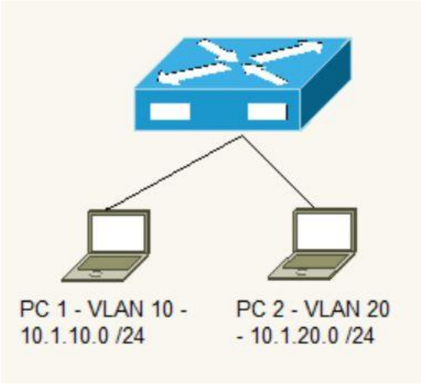


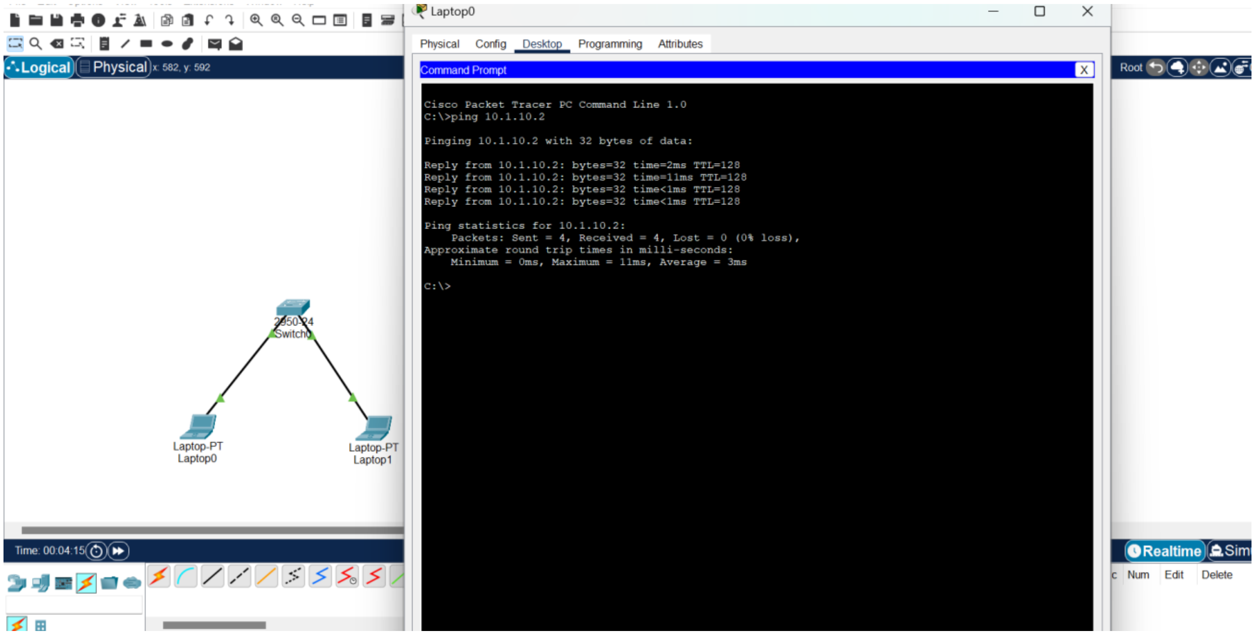
Diagram 2



1. Use diagram 1 to verify connectivity within same VLAN (VLAN 10)
2. Assign IP addresses to the PCs
    a. Make sure the PCs are in the same subnet
    b. What are the IPs you assigned to both PCs? Why do these IP subnets have to be in the same subnet? **[5 points]**

    I have assigned PC1 IP address as 10.1.10.1 and PC2 IP address as 10.1.20.2. PCs in the same VLAN need to have the same subnet to communicate directly and it works as a broadcast domain. When devices are in the same subnet, the switch can deliver packets directly by using VLAN and if it is in a different network, it would require routing.

c. Verify Ping connectivity between PCs. Paste screenshot **[2 points]**



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.1.10.2

Pinging 10.1.10.2 with 32 bytes of data:

Reply from 10.1.10.2: bytes=32 time=2ms TTL=128
Reply from 10.1.10.2: bytes=32 time=11ms TTL=128
Reply from 10.1.10.2: bytes=32 time<1ms TTL=128
Reply from 10.1.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms

C:\>
```

3. Now create two different VLANs (diagram 2)
    a. VLAN 10 should be named Engineering
    b. VLAN 20 should be named Sales
        i. Use the appropriate **show** commands on the switch to indicate this [**5 points**]

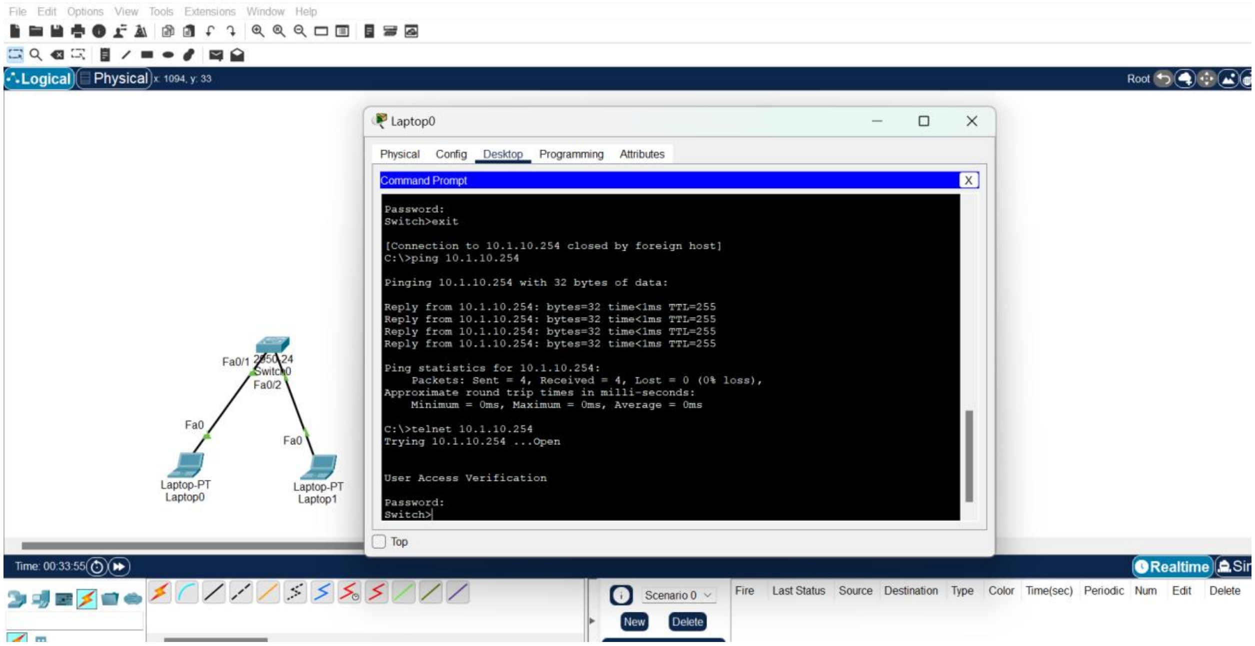
```
Switch#en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Engineering
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name sales
Switch(config-vlan)#exit
```

4. Assign PC1 to Engineering
5. Assign PC2 to Sales
    a. Assume no MAC entries exist in the switch. Explain step by step

everything that happens in the network as soon as ping is initiated from PC1 towards PC2. Can PC1 ping PC2? Why or why not? [**10 points**]

When a ping is sent from PC1 to PC2, since it does not know the MAC address it will send a ARP request to determine the MAC address. But, since PC2 is in a different VLAN (VLAN20) and whereas PC1 is VLAN 10 the ARP request won’t reach. No, PC1 and cannot ping PC2 because they are in different VLANs. Since both are in different networks it requires a router for communication. Hence it won’t ping.

6. Enable Telnet on the switch
    a. What should be done so PC1 can Telnet to the switch? [**5 points**]



```
Password:
Switch>exit

[Connection to 10.1.10.254 closed by foreign host]
C:\>ping 10.1.10.254

Pinging 10.1.10.254 with 32 bytes of data:

Reply from 10.1.10.254: bytes=32 time<1ms TTL=255
Reply from 10.1.10.254: bytes=32 time<1ms TTL=255
Reply from 10.1.10.254: bytes=32 time<1ms TTL=255
Reply from 10.1.10.254: bytes=32 time<1ms TTL=255

Ping statistics for 10.1.10.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>telnet 10.1.10.254
Trying 10.1.10.254 ...Open


User Access Verification

Password:
Switch>
```

By using commands:-

Switch#config t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#line vty 0 15

Switch(config-line)#password cisco

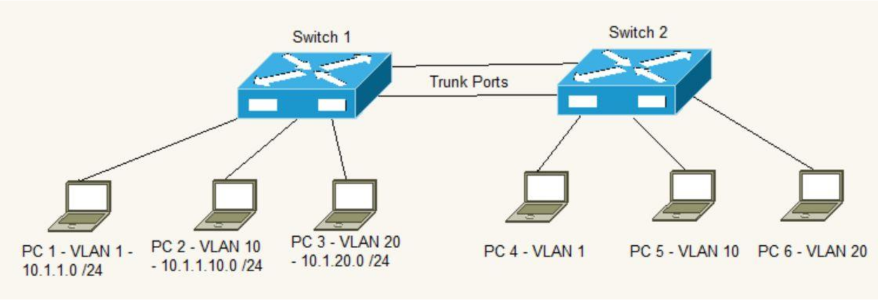
Switch(config-line)#login

Switch(config-line)#transport input telnet

```
Switch(config-line)#exit
Switch(config)#exit
```

Objective 2 - Switch VLAN and Trunk Configuration

This objective will configure multiple VLANs on multiple switches and connect the switches via trunk ports.


Switch 1
Switch 2
Trunk Ports
PC 1 - VLAN 1 - 10.1.1.0 /24
PC 2 - VLAN 10 - 10.1.1.10.0 /24
PC 3 - VLAN 20 - 10.1.20.0 /24
PC 4 - VLAN 1
PC 5 - VLAN 10
PC 6 - VLAN 20

1. Setup the network as indicated in the diagram (*hint: Switch2 configuration should be a duplicate of Switch1*)
2. In what IP subnet is IP address of PC5 present? What design considerations did you have to make when choosing this IP subnet? **[3 points]**

   PC5 is on VLAN 10 with an IP address of 10.1.1.2/24, the IP subnet is 10.1.1.0/24 and I can have host 254 usable addresses. Each VLAN is assigned to its own IP subnet so it means devices within VLANs are in the network and within VLAN devices can communicate. Using subnet mask /24 ensures enough host IPs for each VLAN.
3. Can PC1 and PC2 Ping each other? Why or why not? [**3 points**]

   No, Since PC1 and PC2 are from different VLAN so they cannot ping each other. VLANs prevent unnecessary traffic and there won't be any communication across VLANs without additional routing.
4. Can PC2 and PC3 Ping each other? Why or why not? [**3 points**]

   No, From the above case since PC2 and PC3 are from different VLAN it cannot communicate with each other. Devices from different VLANs cannot communicate without any additional routing.
5. Configure the switches so PCs can ping within the same VLAN.

a. Provide the relevant configuration from both switches [**5 points**]

Configuration for switch 1:-

```
Switch(config)#vlan 1
Switch(config-vlan)#exit
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#exit
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1
Switch(config-if)#exit
Switch(config)#interface FastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface FastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#
Switch(config)#interface FastEthernet 0/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 1,10,20
Switch(config-if)#exit
Switch(config)#exit
```

Configuration for switch 2:-

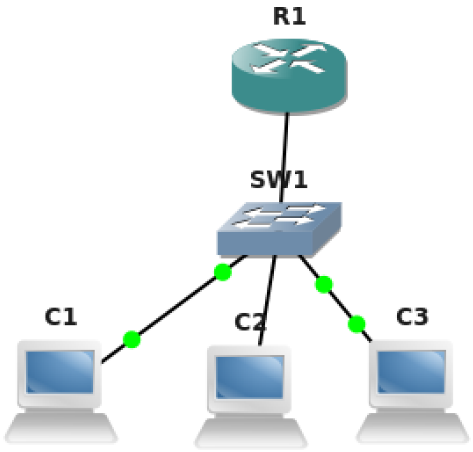
```
Switch(config)#vlan 1
Switch(config-vlan)#exit
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#exit
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1
Switch(config-if)#exit
Switch(config)#interface FastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface FastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#
Switch(config)#interface FastEthernet 0/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 1,10,20
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

6. Explain what must be done to allow all PCs to Ping each other [**10 points**]

To allow all PCs to ping each other we need to use inter-VLAN routing. VLAN allows devices within the network to communicate. Therefore, routing is needed for devices in separate VLANs to communicate. This can be done by using an external router or a layer 3 switch. By using Router-on-a-stick configuration, the router will act as the intermediate to route traffic between the VLANs. When a device in VLAN 1 wants to communicate with device in VLAN 10, the switch forwards the traffic to router and router checks the destination IP address and determines that the packet is destined for VLAN 10. So it routes the packet from the VLAN 1 sub-interface to the VLAN 10 sub- interface and sends back to the switch through the trunk port.

Objective 3 – Inter-VLAN Routing "Router on a Stick"

This objective will configure multiple VLANs on a switch, and uplink the switch to a router via a trunk port and we will use this router to route between VLANs. Since the router is using one physical port to route incoming and outgoing traffic, we call it "Router on a Stick"



PC1- VLAN**1** – 10.1.1.0/24	PC2- VLAN**10** – 10.1.10.0/24	PC3- VLAN**20** – 10.1.20.0/24

1. What are sub-interfaces on a router? What are its advantages? **[2 points]**

   Sub-interfaces on a router are virtual interfaces created under physical interface allowing Instead of needing separate physical cables for each network, I can use one cable and divide into multiple virtual pathways. Each pathway can handle traffic from a different network. They are used primarily in configuration involving VLANs. Advantages are it is cost effective such we can eliminate multiple physical routers or interfaces and use one physical interface to manage traffic for multiple VLANs. Segmentation of Network and simplified management such as managing multiple VLANs is simpler and since the configuration is made into one physical interface rather than multiple interface.

2. Configure VLAN sub-interfaces on the router (VLAN1 “native”, VLAN 10, and VLAN 20).
    a. Submit the router configuration that indicates the trunking setup. [**10 points**]

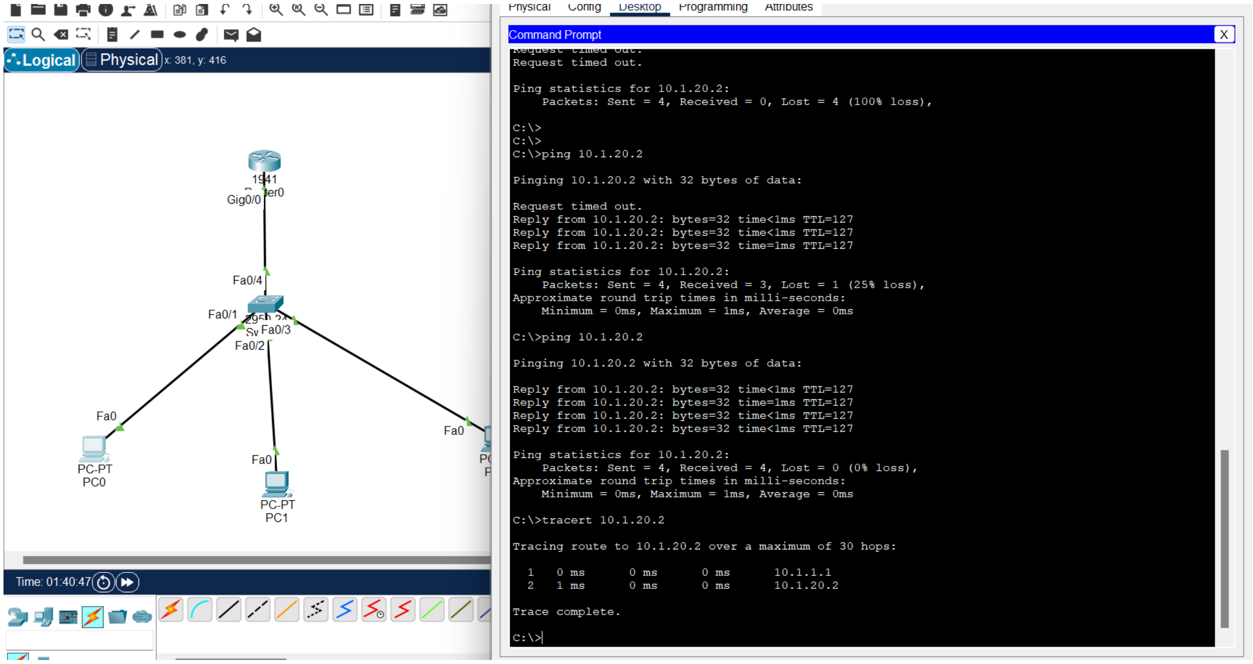
```
Router#show running-config
Building configuration...

Current configuration : 884 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
```

```
!
!
license udi pid CISCO1941/K9 sn FTX152447HY-
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/0.1
```

```
encapsulation dot1Q 1 native
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 10.1.10.1 255.255.255.0
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 10.1.20.1 255.255.255.0
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
```

```
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

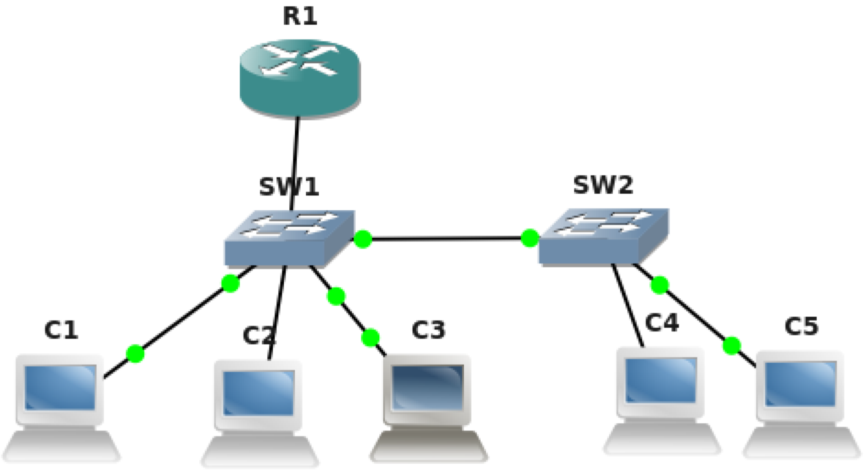
3. Verify all PCs can Ping each other.
   a. Paste screenshots of trace route from the PC to indicate the packets are traversing through the router for inter-VLAN communication. [**5 points**]



```
Request timed out.
Request timed out.

Ping statistics for 10.1.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>
C:\>ping 10.1.20.2

Pinging 10.1.20.2 with 32 bytes of data:

Request timed out.
Reply from 10.1.20.2: bytes=32 time<1ms TTL=127
Reply from 10.1.20.2: bytes=32 time<1ms TTL=127
Reply from 10.1.20.2: bytes=32 time=1ms TTL=127

Ping statistics for 10.1.20.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.1.20.2

Pinging 10.1.20.2 with 32 bytes of data:

Reply from 10.1.20.2: bytes=32 time<1ms TTL=127
Reply from 10.1.20.2: bytes=32 time=1ms TTL=127
Reply from 10.1.20.2: bytes=32 time<1ms TTL=127
Reply from 10.1.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.1.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>tracert 10.1.20.2

Tracing route to 10.1.20.2 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      10.1.1.1
  2   1 ms      0 ms      0 ms      10.1.20.2

Trace complete.

C:\>
```

Objective 4 – Inter-VLAN Routing 2: Multiple switches

This objective will configure multiple VLANs on multiple switches and use a router to route between VLANs.



PC1- VLAN**1** – 10.1.1.0/24	PC2- VLAN**10** – 10.1.10.0/24	PC3- VLAN**20** – 10.1.20.0/24	PC4- VLAN**20** – IP subnet-?	PC5- VLAN**40** – 10.1.40.0/24

1. Look at the above diagram. What is the type of port you should configure between

the two switches? (Eg: access port **or** trunk port **or** routed port **or** any other port?) Why do you have to use this port type? Justify. **[3 points]**

A trunk port is used to carry traffic for multiple VLANS across a single link. We are using VLAN1, VLAN10, VLAN20, VLAN40. Between switches we use trunk link to forward traffic. A trunk port uses 802.1Q encapsulation to tag VLAN traffic and ensures traffic from all the VLANs can pass between switches and get routed by the router correctly.

2. At the end of this lab objective all hosts must be able to ping each other. From your previous setup, you added Switch2 and hosts PC4 and PC5. What extra configurations did you have to add to this setup to establish connectivity between all hosts? Mention each device you had to configure or make changes to achieve this. Just mention snippets of extra configuration you had to add on each device you configured. Also attach screenshot of successful pings and traceroute from PC2 to PC5.
[15 points]

I have added switch 2 along with PC4 and PC5 and assigned them with IP addresses and default gateway, ensured they are assigned with the correct VLANs: -VLAN 20 and VLAN 40

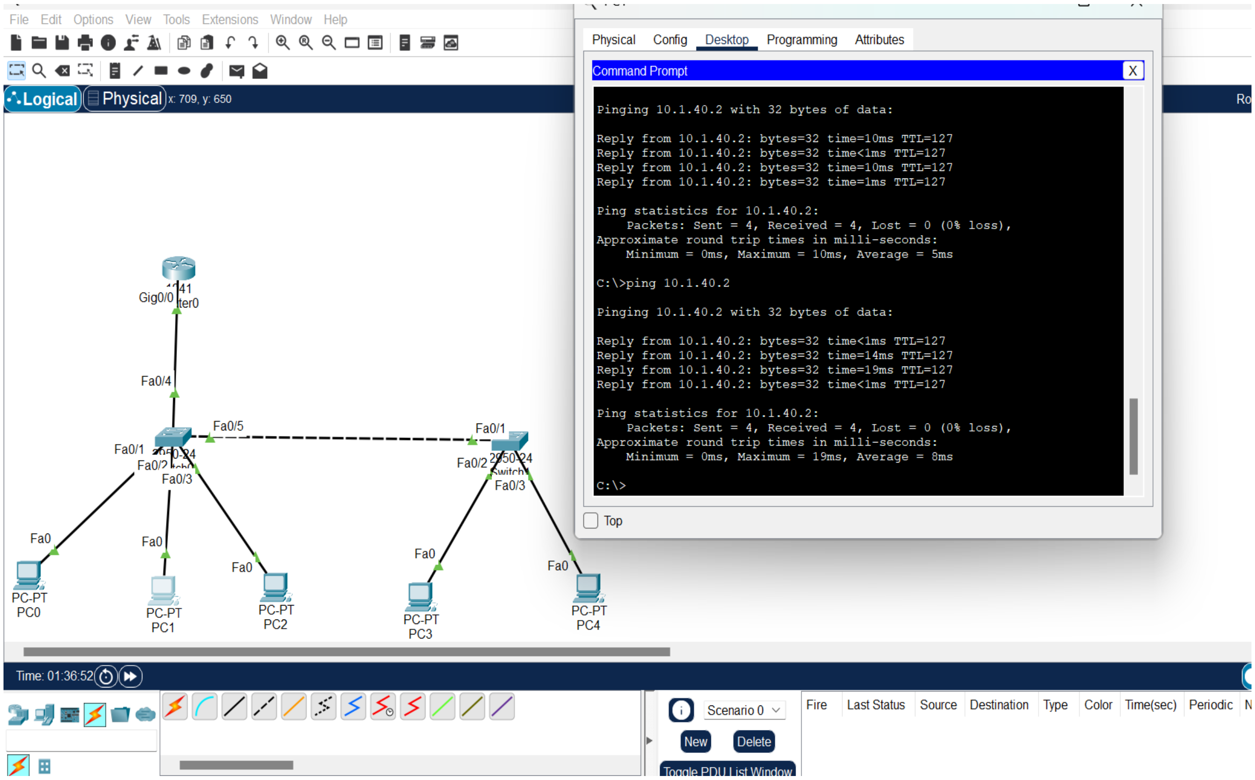
```
Switch(config)# interface fa 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit
Switch(config)# interface fa 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 40
Switch(config-if)# exit
```

Ensuring the trunk between the switches is allowing VLAN 1,10,20,40.

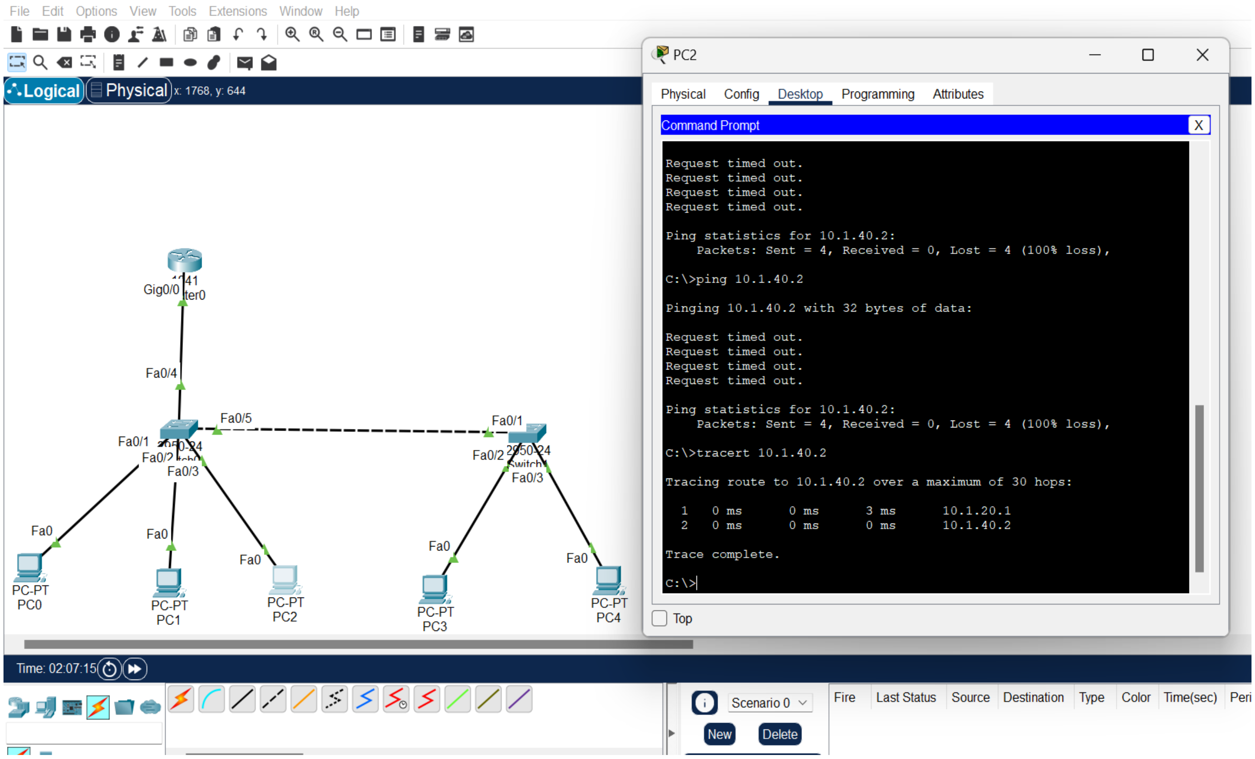
```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 1,10,20,40
Switch(config-if)#exit
Switch(config)#interface fa0/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 1,10,20,40
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

Also created a new sub-interface on the router to handle traffic for VLAN 40

```
Router(config)# interface gi0/0.40
Router(config-subif)# encapsulation dot1Q 40
Router(config-subif)# ip address 10.1.40.1 255.255.255.0
Router(config-subif)# exit
```



```
Pinging 10.1.40.2 with 32 bytes of data:

Reply from 10.1.40.2: bytes=32 time=10ms TTL=127
Reply from 10.1.40.2: bytes=32 time<1ms TTL=127
Reply from 10.1.40.2: bytes=32 time=10ms TTL=127
Reply from 10.1.40.2: bytes=32 time=1ms TTL=127

Ping statistics for 10.1.40.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 5ms

C:\>ping 10.1.40.2

Pinging 10.1.40.2 with 32 bytes of data:

Reply from 10.1.40.2: bytes=32 time<1ms TTL=127
Reply from 10.1.40.2: bytes=32 time=14ms TTL=127
Reply from 10.1.40.2: bytes=32 time=19ms TTL=127
Reply from 10.1.40.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.1.40.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 19ms, Average = 8ms

C:\>
```



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

Ping statistics for 10.1.40.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.1.40.2

Pinging 10.1.40.2 with 32 bytes of data:

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

Ping statistics for 10.1.40.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>tracert 10.1.40.2

Tracing route to 10.1.40.2 over a maximum of 30 hops:

  1   0 ms      0 ms      3 ms      10.1.20.1
  2   0 ms      0 ms      0 ms      10.1.40.2

Trace complete.

C:\>
```

Report Questions [23 pts]

1. What are two advantages of using VLANs? [**2 points**]

   VLANs can limit broadcasting to other networks rather than broadcasting just within the VLAN. So, devices within the network can communicate with each other without worrying about unnecessary traffic.

   Devices on different VLAN cannot communicate directly, minimizing the risk of unauthorized access and adding a layer of security.

2. Can a PC from any VLAN telnet into a switch? Why or why not? If not, what must be done to make it work? [**2 points**]

   No, a PC from one VLAN cannot telnet into a switch that is configured into a different VLAN. Either the PC and the switch should belong to the same VLAN in order to do telnet or else we have to configure router-on-a-stick.

3. What are access ports and what are trunk ports? Explain the difference **[3 points]**

   Access ports are assigned to a single VLAN and carry Traffic for that VLAN. Devices connected to access port can only communicate within the VLAN.

   Whereas Trunk ports are used to send traffic for multiple VLANs simultaneously and use tagging protocol to identify which VLAN each packet belongs to.

4. What is the benefit of using a trunk port? [**2 points**]

   Trunk ports help in reducing multiple links between switches and send traffic of multiple VLANs traffic in that single link. It reduces cost of installing multiple cables and the main benefit is bandwidth efficiency.

5. Describe what must be done to route between VLANs. [**2 points**]

   To send packet across VLAN, the router creates a sub-interfaces for each VLAN with its own IP address and ensures that router is connected to trunk port to send and receive traffic from multiple VLANs.

6. In Objective 4, let us say you issued a ping from PC2 to PC5. Explain how the ping packets flow through the network, paying attention to each step when switches forward the packet and routers route the packet. If necessary, mention any ARPs that may need to be issued to establish this communication.

   [12 points]

PC2 initiates a Request Packet to PC5 IP address which is 10.1.40.0/24 and checks is it is in different network. Since it is in a different network it forwards the packet to the default gateway. Since it does not know the MAC address it will send an ARP request to know the MAC address of the default gateway and once the ARP response is received which will contain the MAC address of the default gateway and then proceeds to send packet to the gateway. Once the router receives the packet it checks for the destination IP and checks how to reach the destination (VLAN 40, 10.1.20.0/24). The router knows that 10.1.40.0/24 is associated with VLAN 40 and forwards packet through its VLAN40 interface, since the router doesn’t know the PC5s MAC address, it will send an ARP request to know the MAC address of PC5 in VLAN 40. Once the router receives the MAC address of PC5 it will forward the packet to PC5. Once the PC5 receives the packet it will send reply packet back to PC2. The reply packet is sent to PC5s default gateway (10.1.40.1), the router receives the packet from its VLAN 40 interface and looks at the destination address and forwards the packet through its VLAN10 interface and if the router does not have the MAC address of PC2 it uses ARP to resolve PC2s MAC address and the reply packet is forwarded to PC2, therefore completing the ping process. Since PC2 and PC5 are in different VLANs, they need a layer 3 device to route the traffic and we used a router to route traffic.

Extra Credit [13 points]

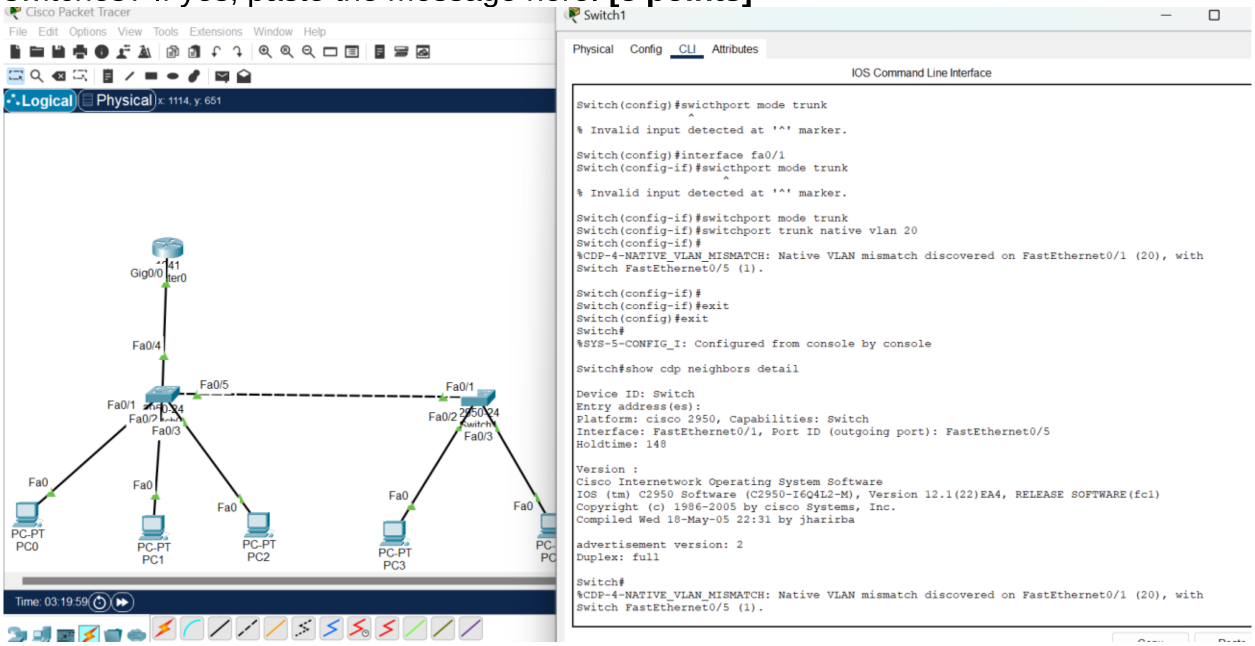
1. What is a broadcast domain? How many broadcast domains are there in the topology in Objective 4? **[3 points]**

A broadcast domain is a logical division of network in which all devices can reach other with broadcast frames. All devices in the same network can communicate with each other and can directly communicate using broadcasts (such as ARP request). In each VLAN network indicates one broadcast domain. There are four broadcast domains since ach VLAN represents a separate a broadcast domain.

2. From your setup in objective 4,

- On Switch-1 port (connected to Switch-2), configure VLAN 10 as native-vlan.
- On Switch-2 port (connected to Switch-1), configure VLAN 20 as native-vlan.

Give it a minute. Do you observe any debug/warning messages on either of your switches? If yes, paste the message here. **[8 points]**



```
Switch(config)#swicthport mode trunk
                ^
% Invalid input detected at '^' marker.

Switch(config)#interface fa0/1
Switch(config-if)#swicthport mode trunk
                      ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 20
Switch(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (20), with
Switch FastEthernet0/5 (1).

Switch(config-if)#
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show cdp neighbors detail

Device ID: Switch
Entry address(es):
Platform: cisco 2950, Capabilities: Switch
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/5
Holdtime: 148

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

advertisement version: 2
Duplex: full

Switch#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (20), with
Switch FastEthernet0/5 (1).
```

To your best knowledge, explain what you think it means **[2 points]**

When an untagged traffic passes through switch 1, native VLAN 10 makes traffic belong to VLAN 10 and therefore for VLAN 20 an untagged traffic passes through the trunk port it will make the traffic belong to VLAN 20. The traffic can go to some other devices and lead to broadcast storms. Because of this mismatch the switch will log in warning messages.

Total Score = ___________________/122