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

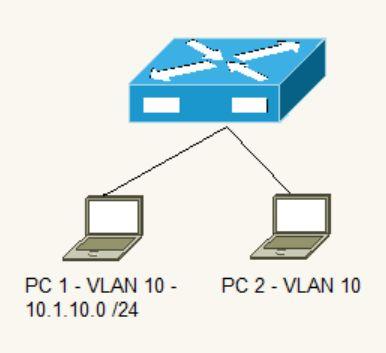
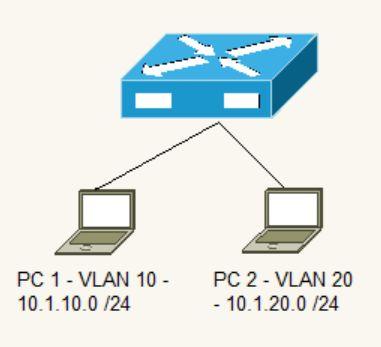


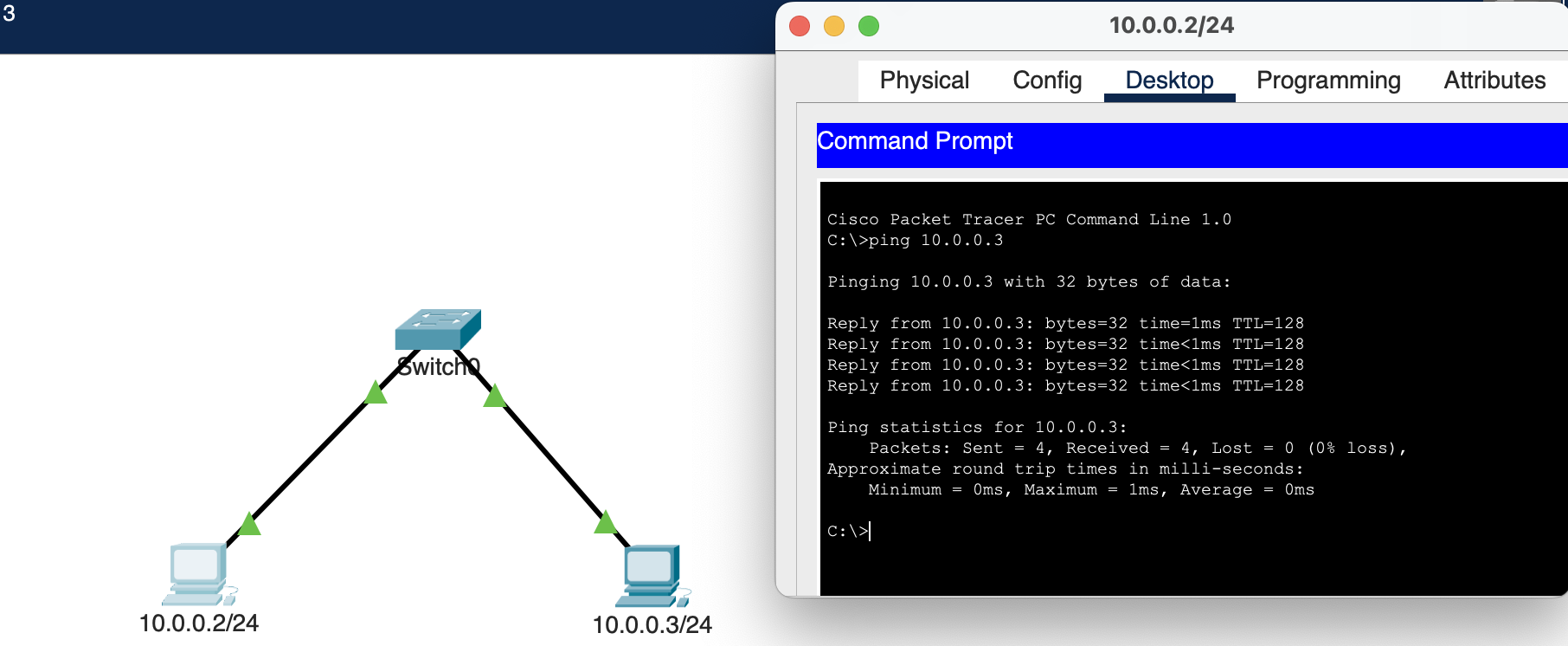
Diagram 2



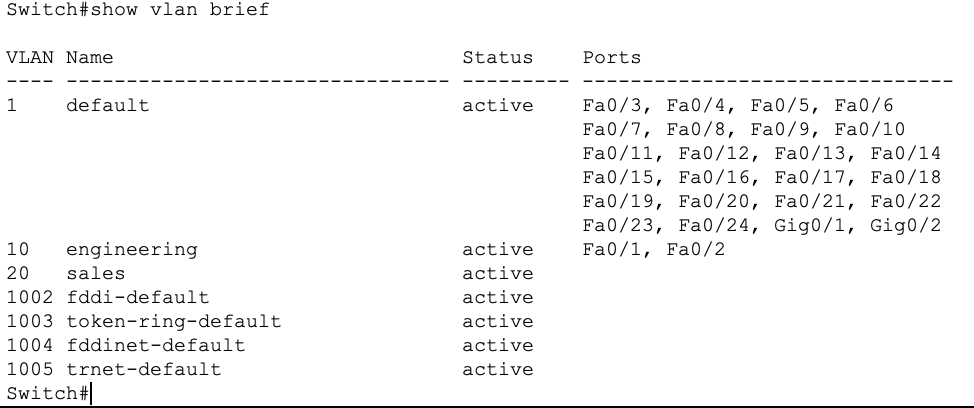
1. Use diagram 1 to verify connectivity within same VLAN (VLAN 10)
2. Assign IP addresses to the PCs
   1. Make sure the PCs are in the same subnet
   2. What are the IPs you assigned to both PCs? Why do these IP subnets have to be in the same subnet? **[5 points]**

I assigned 10.0.0.2/24 and 10.0.0.3/24 IP addresses to the PCs. Since they are in the same VLAN, they should be in the same broadcast domain. Also, devices within the same VLAN communicate with each other directly at Layer 2 using MAC addresses. However, when they need to communicate at Layer 3, they use IP addresses. If two devices in the same VLAN have IP addresses from different subnets, they won't be able to communicate at the network layer because their IP addresses won't be considered part of the same network.

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



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

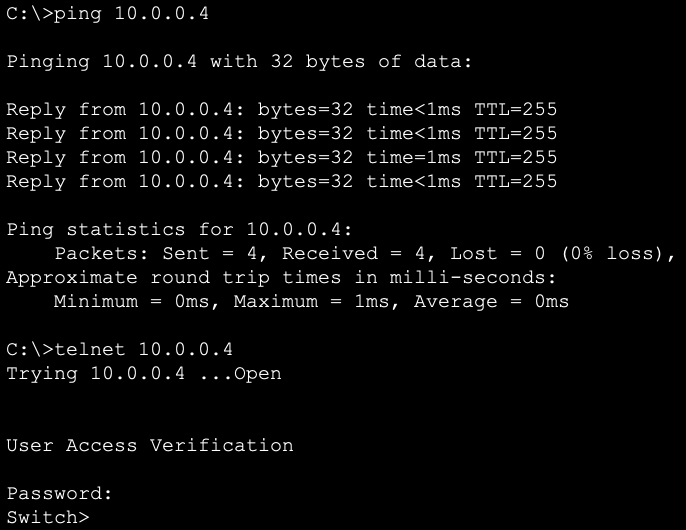
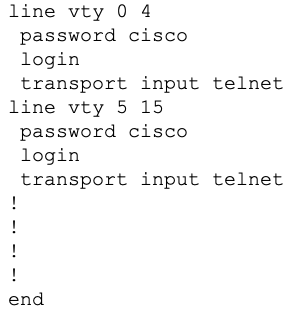
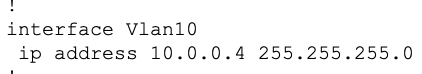


1. Assign PC1 to Engineering
2. Assign PC2 to Sales
   1. Assume no MAC entries exist in the switch. Explain step by step everything that happens in the network as soon as ping is initiated from PC1 towards PC2. Can PC1 ping PC2? Why or why not? [**10 points**]

* PC1 is unable to ping PC2 due to the following sequence of events: When PC1 initiates a ping to PC2, it first checks if PC2's IP address is within the same subnet as PC1. Since they share the same subnet, PC1 proceeds to look for the associated MAC address of PC2 within that subnet. Subsequently, PC1 generates a broadcast frame with the source IP set to **10.0.0.2/24**, the destination IP as **10.0.0.3/24**, the source MAC address as PC1's MAC address, and the destination MAC address as **ff:ff:ff:ff:ff:ff**. This frame is then sent to the switch. The switch records the interface, and MAC address of PC1 in its MAC table and attempts to flood the frame to all interfaces, excluding the one from which it received the frame (as it has already learned this interface and MAC address). However, it refrains from broadcasting to other broadcast domains (i.e., VLANs). It knows that the interface that PC1 is connected to is in **VLAN 10**, so it will attempt to flood the frame to all interfaces that are on **VLAN 10**.
* In this specific case, there is only one other interface, which belongs to **VLAN 20**, and as a result, the frame cannot be sent to it. Consequently, the two PCs are unable to establish a successful ping connection.

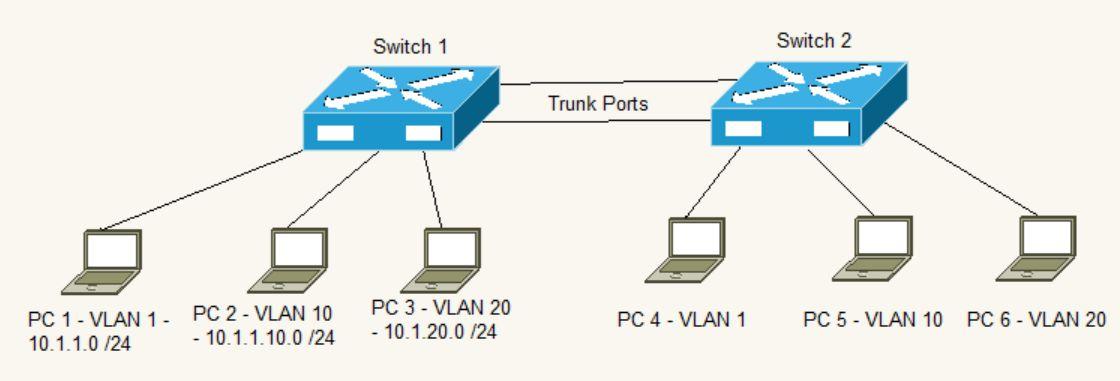
1. Enable Telnet on the switch
   1. What should be done so PC1 can Telnet to the switch? [**5 points]**

* Given that PC1 is in VLAN 10, it's imperative for it to exist in the same VLAN in order to establish connectivity with the switch. Thus, I established a Switched Virtual Interface (SVI) for VLAN 10 and assigned an IP address of 10.0.0.4/24 to it.
* I then configured the switch to facilitate telnet access by applying the necessary settings to all line vty 0 through 15, and I also implemented a password.
* I then verified the connectivity by attempting to ping 10.0.0.4/24 from PC1, and I successfully achieved a response.
* The telnet functionality operated smoothly without any issues.



# Objective 2 - Switch VLAN and Trunk Configuration

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



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]**

The IP address of PC5 is present in the 10.1.10.0/24 subnet.

When choosing this IP subnet, several design considerations were taken:

* The IP subnet choice aligns with the VLAN segmentation. Each VLAN corresponds to a unique subnet. In this case, VLAN 10 belongs to the 10.1.10.0/24 subnet.
* A logical and hierarchical IP addressing scheme is utilized, where the third octet of the IP address aligns with the VLAN number (*e.g., VLAN 10 corresponds to the 10.1.10.0/24 subnet and VLAN 20 belongs to 10.1.20.0/24*). This makes it easier to identify the VLAN associated with a particular IP address.
* The subnetting scheme allows for future scalability. /24 allows 256 IP addresses (254 usable IP addresses). It ensures that each VLAN has its own address space, preventing IP address conflicts. Also, it gives more room to expand the subnet, in case for any need for expansion.

1. Can PC1 and PC2 Ping each other? Why or why not? [**3 points**]

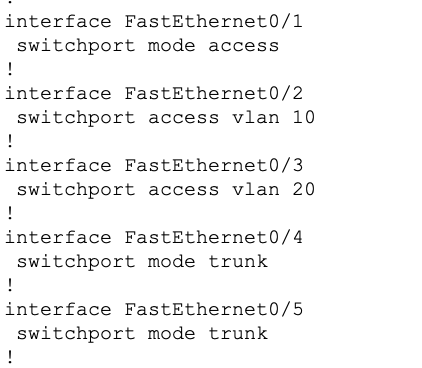
PC1 and PC2 are in different VLANs and different IP subnets. They cannot ping each other directly because VLANs segregate broadcast domains, and a router is required to enable communication between devices in different VLANs and/or different subnets.

1. Can PC2 and PC3 Ping each other? Why or why not? [**3 points**]

As the above, PC2 and PC3 cannot ping each other as they are in different VLANs and different IP subnets. They cannot ping each other directly because VLANs segregate broadcast domains, and a router is required to enable communication between devices in different VLANs and/or different subnets.

1. Configure the switches so PCs can ping within the same VLAN.
   1. Provide the relevant configuration from both switches [**5 points**]

I set up the link between both switches as trunk ports, permitting all VLANs across the trunk link. Additionally, I configured the interfaces for all PCs with access VLANs, placing them within their respective VLANs. The configuration on both switches is as follows:



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

* We would have to add a router here which would act as a gateway for all these PCs to communicate to each other.
* We divide the router’s interface into 3 sub-interfaces (*say, Gi0/1.1, Gi0/1.10, Gi0/1.20*) preferably with the Vlan numbers for easy identification and assign IP addresses.

Interface Gi0/1.1: IP address 10.1.1.1/24

Interface Gi0/1.10: IP address 10.1.10.1/24

Interface Gi0/1.20: IP address 10.1.20.1/24

* And configure all the PC’s gateways as follows:

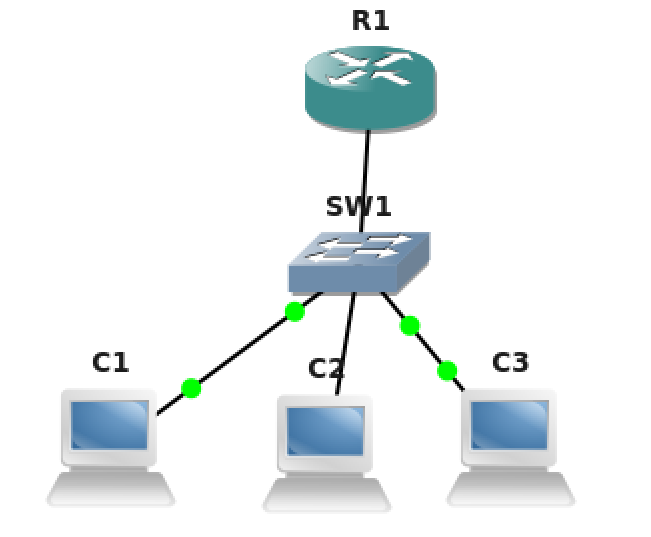
PC1 & PC4: 10.1.1.1/24

PC2 & PC5: 10.1.10.1/24

PC3 & PC6: 10.1.20.1/24

# 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”





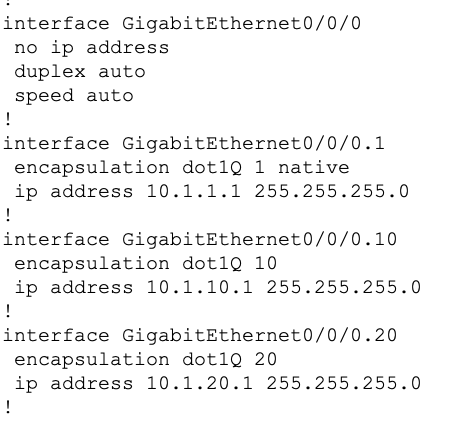
1. What are sub-interfaces on a router? What are its advantages? **[2 points]**

Sub-interfaces are virtual interfaces on a router. One of the advantages of having sub-interfaces is that it is cost-efficient. They eliminate the requirement for physical connections to create multiple physical links for numerous VLANs. When you need to add more VLANs or subnets to your network, you can simply create additional sub-interfaces without the need for physical hardware changes. Sub-interfaces provide a clear and logical separation of network segments, making it easier to troubleshoot network issues and manage network traffic.

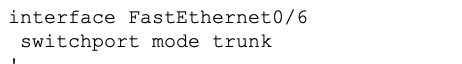
1. Configure VLAN sub-interfaces on the router (VLAN1 “native”, VLAN 10, and VLAN 20).
   1. Submit the router configuration that indicates the trunking setup.

[**10 points**]

**Router config:**

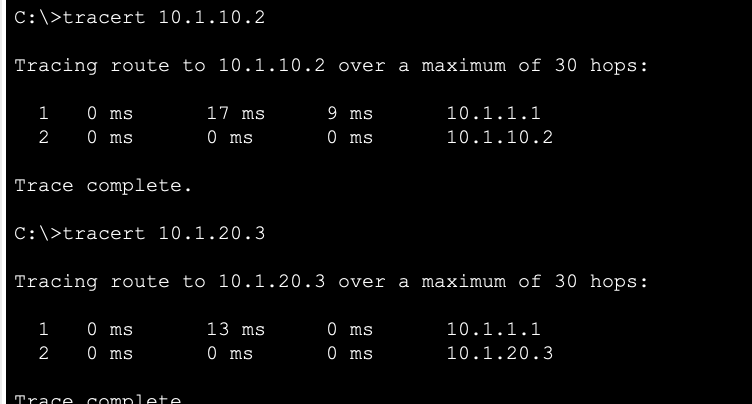


**Switch config:**

****

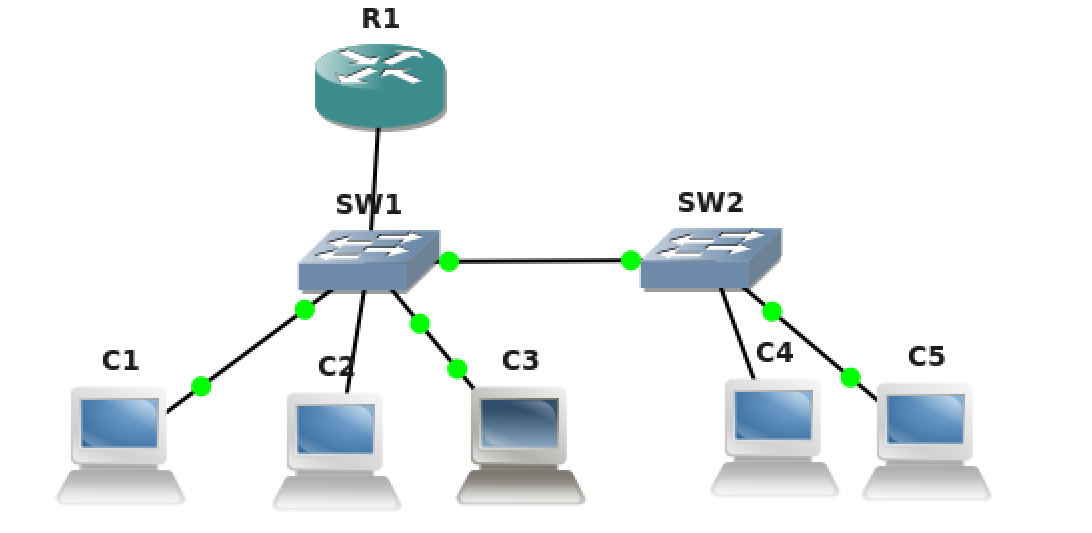
1. Verify all PCs can Ping each other.
   1. Paste screenshots of traceroute from the PC to indicate the packets are traversing through the router for inter-VLAN communication. [**5 points**]

**traceroute from PC1 with IP address 10.1.1.2/24 in Vlan 10:**



# 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.





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?)

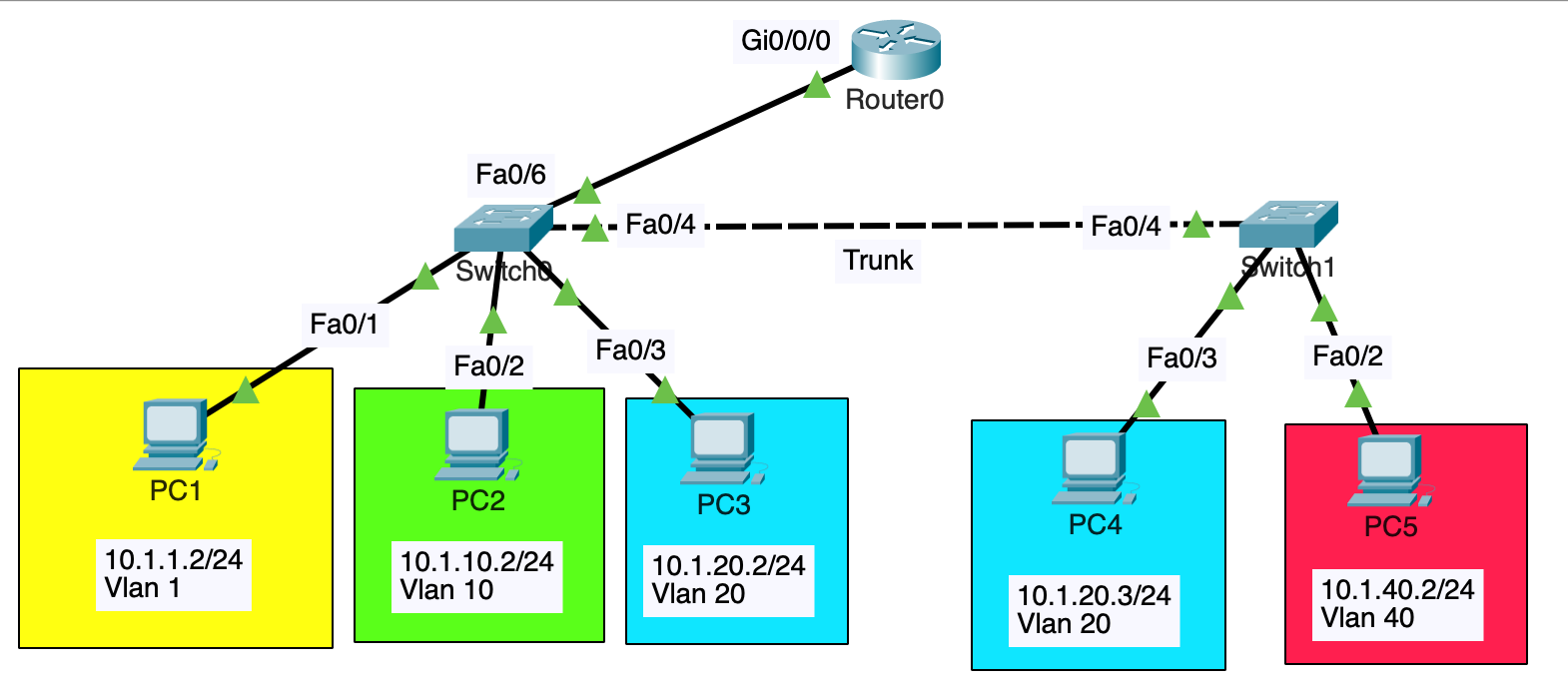
Why do you have to use this port type? Justify. **[3 points]**

Between the two switches, we would have to configure trunk ports. The reason why we would need to do that is so that machines across switches can talk to each other in the same VLAN. Trunk ports are designed to carry traffic for multiple VLANs simultaneously. Also, trunk ports use VLAN tagging to differentiate traffic from different VLANs. When a frame exits a trunk port, it is tagged with a VLAN identifier. This tagging allows the receiving switch to understand which VLAN the frame belongs to and ensures that it is placed in the correct VLAN on the receiving switch.

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]**

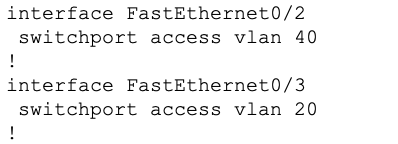
**Here’s the entire topology:**

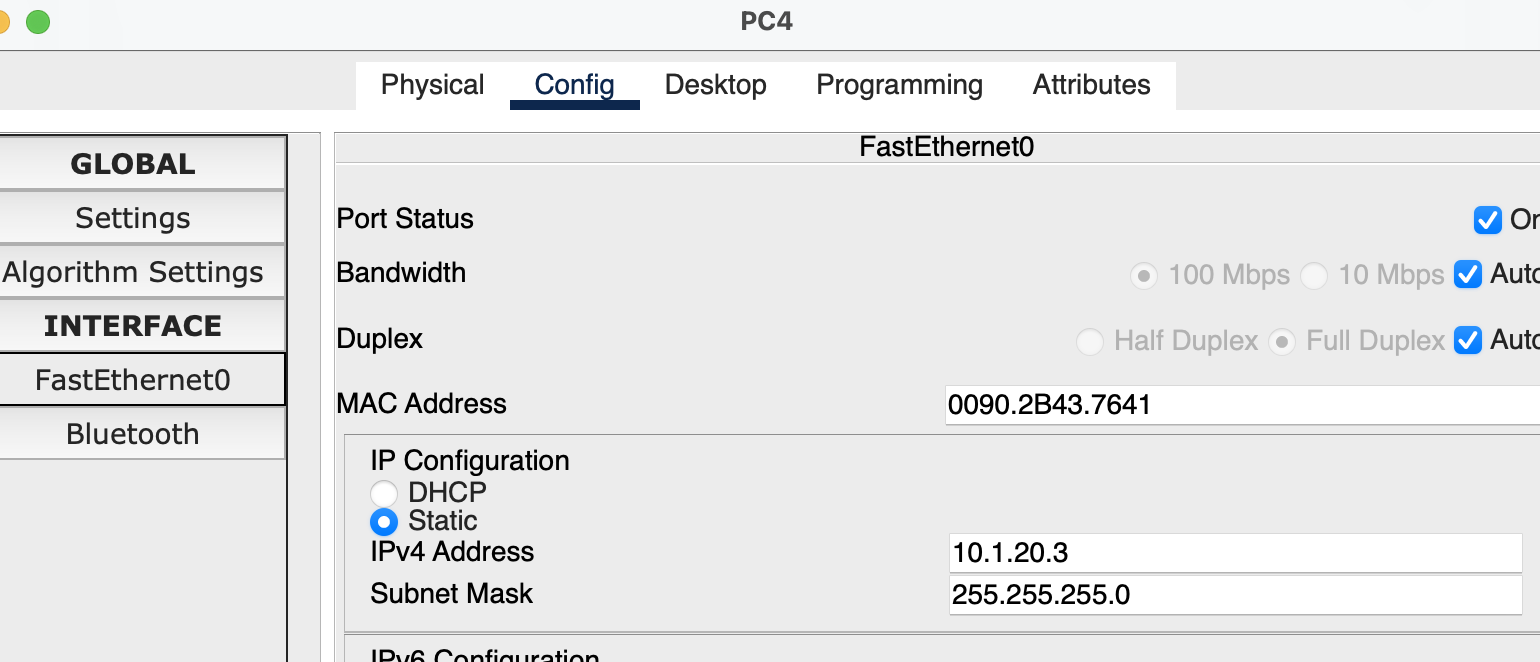


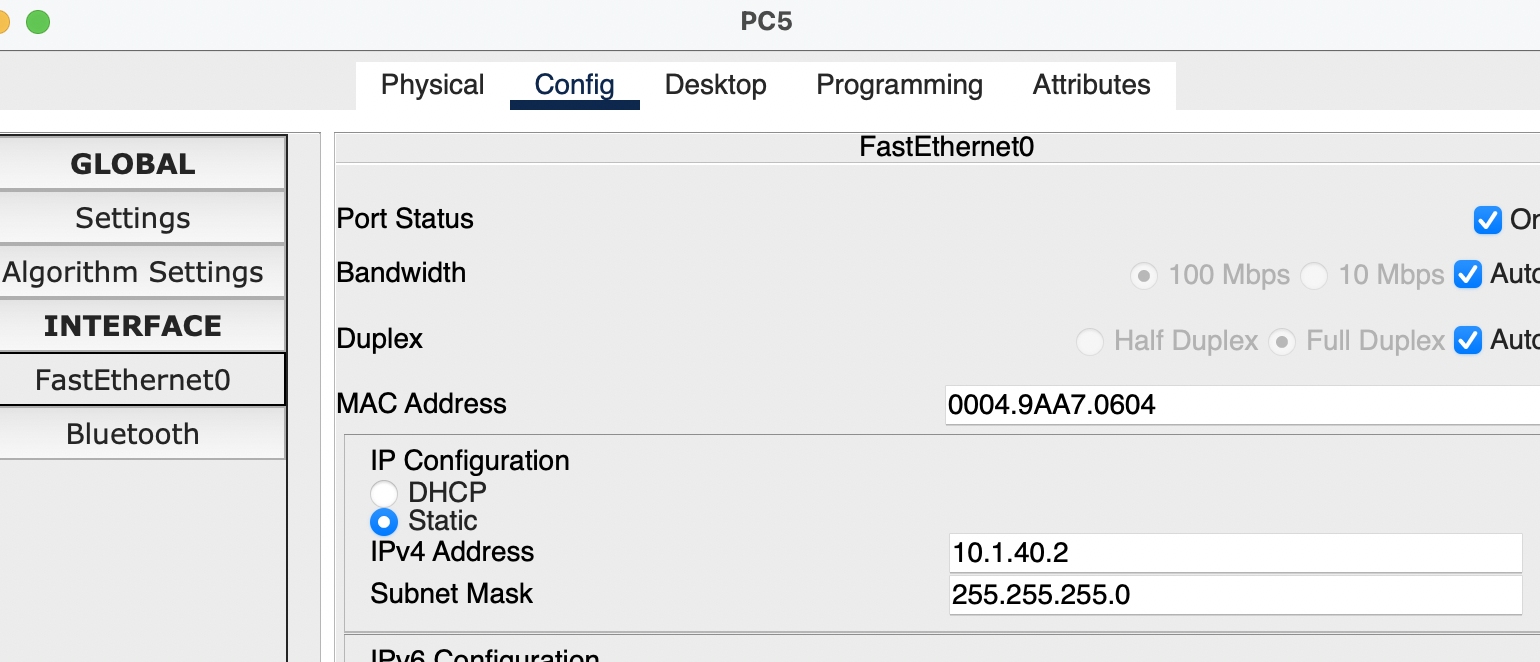
- I configured trunk ports between switch1 and switch2 to allow all VLAN traffic between the link.



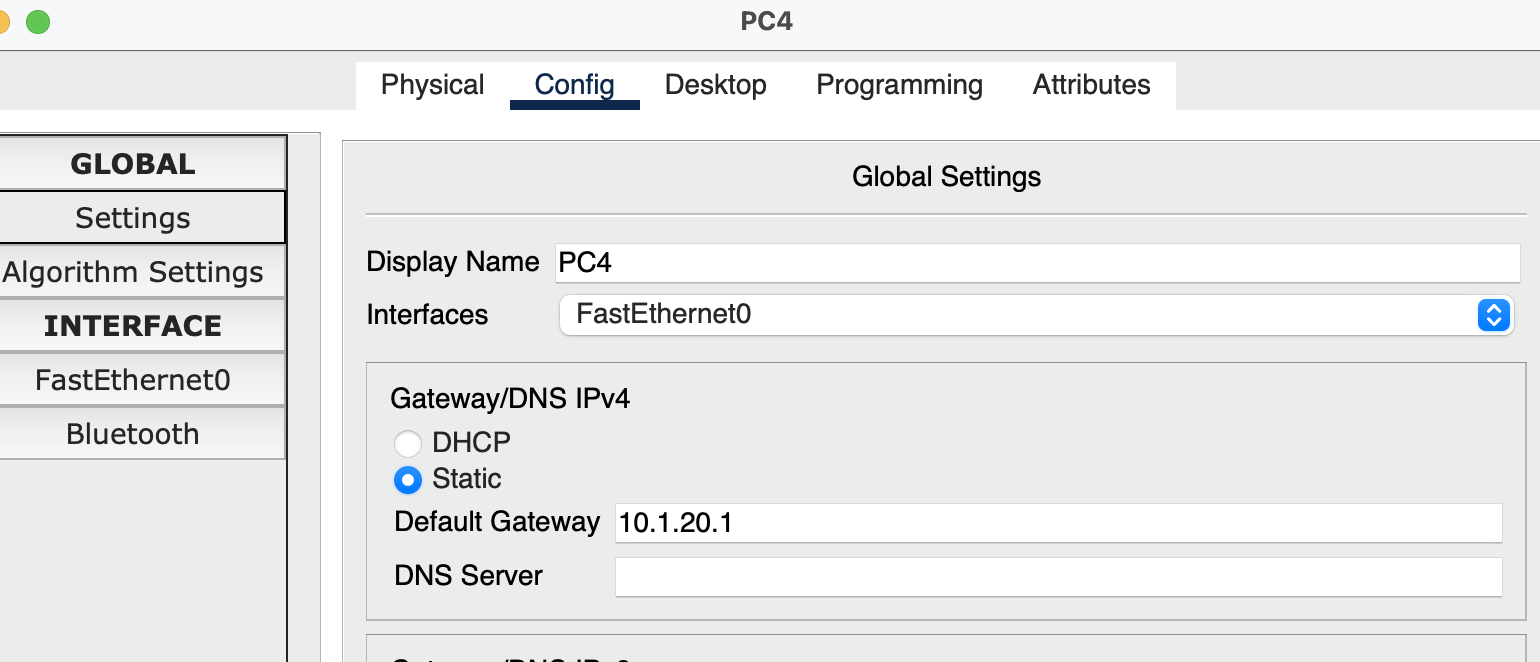
* I configured access VLANs for PC4 and PC5 putting PC4 in VLAN 20 and assigned IP address as 10.1.20.3/24; PC5 in VLAN 40 and assigning IP address as 10.1.40.2/24.

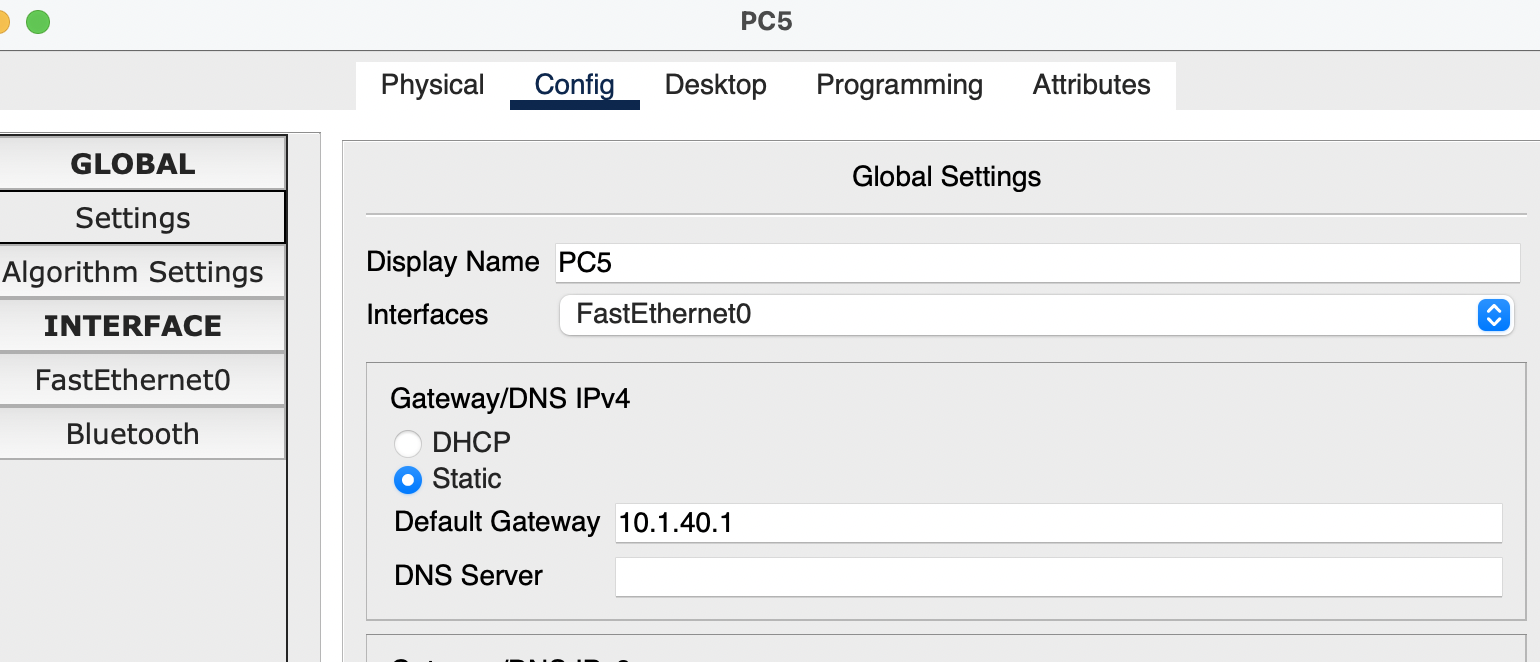




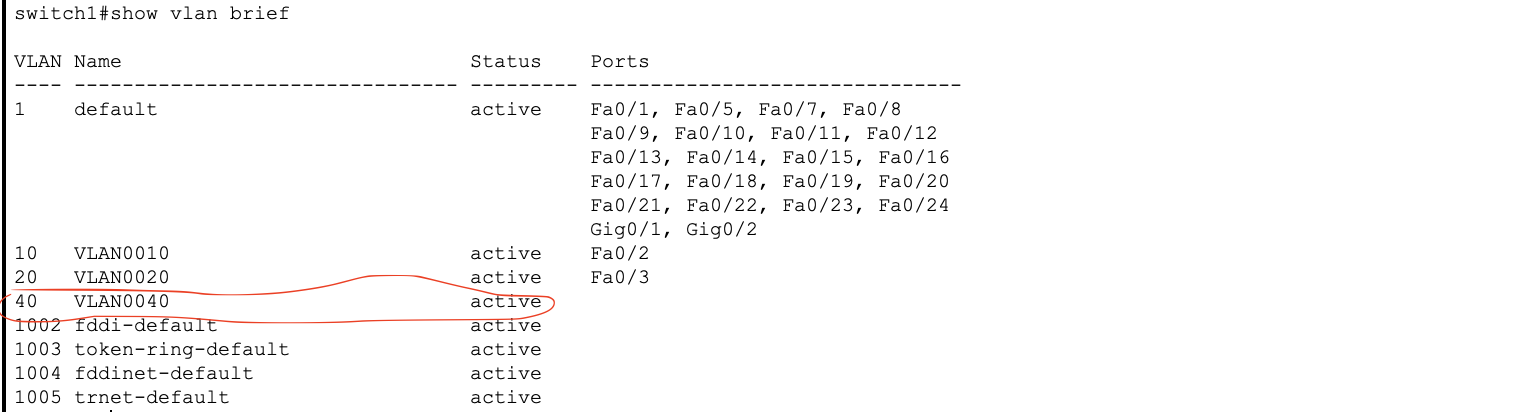


* I configured gateways for PC4 & PC5. PC4’s gateway: 10.1.20.1. PC5’s gateway: 10.1.40.1.

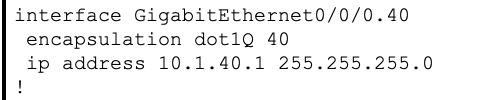




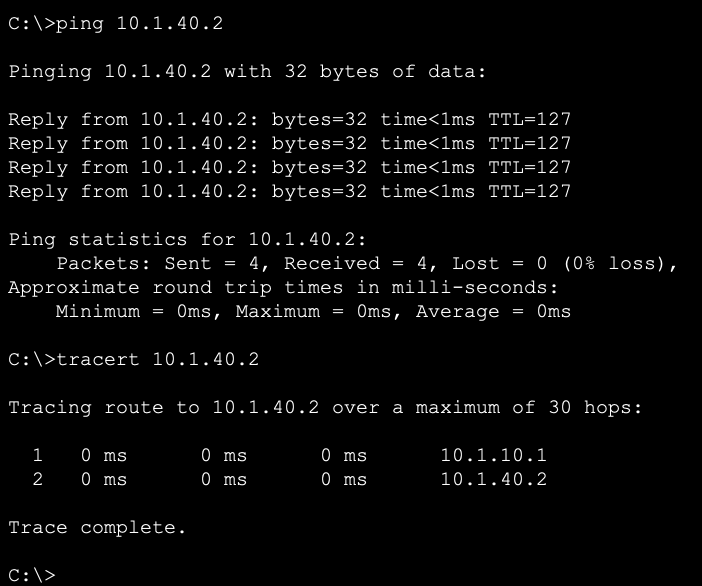
* I had to manually configure VLAN 40 on Switch1 because Switch2 tags the traffic for VLAN 40, and Switch1 needs to be aware of it to correctly handle the traffic. Similarly, I manually configured VLAN 10 on Switch2.



* On R1, I created another sub-interface, Gi0/0/0.40, and assigned the IP address as 10.1.40.1/24.



And voila! I was able to ping across PC2 and PC5.



Report Questions [23 pts]

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

* VLANs allow you to logically segment a physical network into multiple isolated virtual networks. This segmentation enhances network security by preventing broadcast traffic from crossing VLAN boundaries. It also enables better organization and management of network resources.
* VLANs enable in prioritizing and managing network traffic more effectively. You can assign different Quality of Service (QoS) settings to VLANs, ensuring that critical traffic receives higher priority over less important data.

1. 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**]

Without any specific routing config in place, a machine any VLAN would not be able to telnet to the switch as switches often have management interfaces or virtual interfaces (*like SVIs*) associated with specific VLANs for management purposes with their IP addresses. If the machine belongs to a different broadcast domain, it needs to have a Layer 3 protocol (routing) in place.

To make it work:

Assign a specific VLAN (*often a management VLAN*) to the switch's management interfaces or SVIs and assign an IP address to it.

Enable the telnet on the switch.

For machines in other VLANs, they need to have a route to the SVI configured in the previous step. This might either involve a router or an L3 switch can take care of routing as well.

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

Access ports are used to connect end-user devices like computers, printers, IP phones, or other devices to a network. Each access port is typically associated with a single VLAN, and it carries traffic only for that VLAN.

Trunk ports are used to interconnect switches, routers, or other network devices and are designed to carry traffic for multiple VLANs simultaneously. Trunk ports add VLAN tags to Ethernet frames, indicating the VLAN to which each frame belongs.

Access Ports are associated with a single VLAN and carry traffic for that VLAN only, making them suitable for connecting end-user devices to a specific network segment whereas Trunk Ports are configured to carry traffic for multiple VLANs simultaneously by adding VLAN tags to frames.

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

Trunk ports are scalable. As a network grows and more VLANs are added, you can continue using the same trunk ports without the need for additional physical connections or interfaces. Also, it is const-efficient. By consolidating multiple VLANs onto a single trunk link, you can reduce hardware costs associated with additional physical connections.

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

You need to add a router. One of the ways to achieve this is through “Router On a Stick”. You divide a router’s physical interface into multiple logical interfaces, each associated with the VLANs on the switch. Consequently, the PCs can establish communication with their respective default gateways, which are configured on the sub-virtual interfaces of the router and exist within the same subnet.

1. 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 ping to PC5. PC2 would first check if PC5 is in its subnet or not. PC5 is not in PC2’s subnet, thus, PC2 would not send an ARP request, but rather, send it to the default gateway.
* PC2 has a default gateway configured to 10.1.1.1. However, since the default gateway is in the same subnet as PC2, PC2 would now talk to the gateway via MAC address.
* Assuming this is the first time PC2 is talking to the default gateway, PC2 would send an ARP request with the headers as:

Source IP: 10.1.1.2

Destination IP: 10.1.1.1

Source MAC: *PC2’s source MAC*

Destination MAC: ff:ff:ff:ff:ff:ff

* On receiving the broadcast frame, Switch1 learns the MAC address of PC2, the interface on which the frame came in on and store it in its MAC table. Note here that Switch1 is already aware of the interface’s VLAN (*VLAN 10*) as that is configured by us.
* Switch 1 floods it to all of its ports except the interface that it came in on and all other VLANs. For example, Fa0/3 is on Vlan 20. Switch1 would check that the Fa0/3 is not in Vlan 10 and would not send this frame.
* In this scenario, Switch 1 floods to Fa0/4 (*the trunk link since the trunk link is configured to carry all VLAN traffic including VLAN 10*) and Fa0/6 (*link connecting to the router)*
  + **Case 1: Traffic going through the trunk link (Fa0/4):**
    - While sending the traffic across the trunk link, Switch1 “tags” the frame with “VLAN 10”.
    - Switch2 on receiving it, floods it to all interfaces configured with VLAN 10. In our scenario, none of the interfaces are configured on VLAN 10 hence Switch2 drops the packets there and does not flood it to its interfaces.
  + **Case 2: Traffic going through the switch1<->router link (Fa0/6):**
    - Since Fa0/6 is also a trunk link, Switch1 would tag the frame as “Vlan 10” while sending it across the Fa0/6 link.
    - Router, on receiving the frame, checks the destination IP address and immediately knows that the destination IP address is indeed configured on one of its sub-interfaces (Gi0/0/0.10).
    - Router then responds with an ARP response frame with source MAC address as Router’s MAC address, destination MAC address as PC2’s MAC address, source IP as 10.1.1.1, destination IP as 10.1.1.2. This frame would be a unicast frame.
    - Switch1 on receiving it, would learn the Router’s MAC address, the interface on which it came on and store it in its MAC table. It would then forward the ARP response directly to the recently learned interface to PC2.

- PC2, on learning the MAC address of the router (its default gateway), can now talk to its default gateway via MAC address directly without having to broadcast it now. PC2 now resumes the ping command with

* + - * destination IP address as 10.1.40.2/24
      * source IP as 10.1.1.2/24
      * source MAC as PC2’s MAC address
      * destination MAC as Default Gateway (Router’s) MAC address

- PC2 forwards this to Switch1. Switch1 now knows how to send it to the default gateway (router) from the previous ARP step. Switch1 sends it directly via the Fa0/6 interface to the router with the VLAN tag as “VLAN 10”.

- Router1, on seeing the packet, would then check its route table and immediately see that the destination IP address 10.1.40.2 is configured to one of its sub-interfaces (Gi0/0/0.40). Router does its router thingy and works through the headers. It decapsulates the packet, looking at the ethernet header first which contains the VLAN ID. Using that VLAN ID it knows which of its own subinterfaces the traffic belongs to (Gi0/0/0.10). Then it moves onto the IP header, does its layer-3 stuff like route lookups and finding egress interface. The ethernet header is rewritten with new source/destination MAC addresses, and the VLAN ID of the corresponding egress subinterface is added before sending the packet back out to the switch.

- Source MAC: Router’s MAC

Destination MAC Switch1’s MAC

Source IP and Destination IP would remain the same

VLAN as 40.

- Switch1 on receiving this, checks that the packet now has a VLAN tag of 40. None of its interfaces are configured to be VLAN 40, except the Fa0/4 trunk link which carries all VLAN traffic (including VLAN 40).

- Switch1 sends the packet across Fa0/4 link to Switch2.

- Switch2 on receiving this packet, checks the VLAN tag as 40. Since only Fa0/2 is configured to VLAN 40, it sends the packet to Fa0/2.

- PC5, on receiving the packet, decapsulates it and checks the IP address is indeed destined to it and responds. Now, source IP address becomes 10.1.40.2/24 and destination IP address becomes 10.1.1.2/24. Since the destination IP address is not in the same subnet as PC5, PC5 would have to communicate via the default gateway.

- Assuming this is also the first time PC5 is communicating to its default gateway, it would perform the whole ARP process as mentioned above to learnt he MAC address of the router.

- Once it learns the MAC address of the router, it sends the ICMP response to Switch2 with the following headers:

- Source IP: 10.1.40.2/24

- Destination IP: 10.1.1.2/24

- Source MAC: PC5’s MAC address

- Destination MAC: Router’s MAC address

- Switch2 on receiving this, forwards this packet to Switch1 through the trunk link tagging the packet as VLAN 40.

- Switch1 would then forward the same packet to the router since it’s destined there.

- Router, checks the headers, decapsulates it, knows which sub-interface it came on based on the VLAN tag, knows how to route the destination IP address since the subnet is configured on its other sub-interface which is tagged with a VLAN ID of 10, re-writes the headers, strips off the VLAN tag, re-writes the VLAN tag to VLAN 20, changes the source and destination mac address and forwards to Switch1.

- Switch1, seeing the destination MAC address and VLAN tag of 20, forwards it to PC2 and that’s how connection is established.

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 a computer network, where all devices within the domain can directly send broadcast messages to one another. Broadcast messages are data packets sent to all devices in a network segment, and they are typically used for functions like address resolution (ARP) and network discovery.

Each VLAN represents a separate broadcast domain. So VLAN 1, VLAN 10, VLAN 20, VLAN 40 are different broadcast domains. Hence, there are 4 broadcast domains.

# 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]**

This is the error message I get.

**%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (10), with switch2 FastEthernet0/4 (20).**

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

This error message indicates a mismatch in the native VLAN. Native VLAN is used for untagged frames on the trunk link (frames that do not have a VLAN tag). Both ends of a trunk link must have the same native VLAN to avoid issues in the case of an event when a frame isn’t tagged with a VLAN (*native broadcasts or ARP*).

**FastEthernet0/4 (10)**: This part of the error message indicates that the Fa0/4 on switch1 has VLAN 10 configured as the native VLAN.

**with switch2 FastEthernet0/4 (20):** This part of the error message indicates that switch2 on its interface FastEthernet0/4 has VLAN 20 configured as the native VLAN.

# Total Score = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/122