南通大學人工智能与计算机学院 （阿里云大数据学院）
School of Artificial Intelligence and Computer Science, Nantong University （人工智能研究院合署）

# 计算机网络课程设计

# Curriculum Design for Computer Networks

## LAB REPORT ON

## One-Armed Routing Experiment

***Supervisor***

**Dr. 万杰（Wan Jie）**

**Associate Professor**

School of Artificial Intelligence and Computer Science
Nantong University

**Submitted By**

Vaskar Chakma

2130130204

Class of 2021

2024 年 12 月 13 日

# 一、Relate Knowledge

## 1. Introduction of the Basic Knowledge Required

Communication across different VLANs (Virtual Local Area Networks) is an essential aspect of modern networking. VLANs allow network segmentation for improved performance, enhanced security, and better management of network resources. Traditionally, inter-VLAN communication required dedicated physical interfaces on a router, with each interface connected to a specific VLAN. However, one-armed routing, also referred to as router-on-a-stick, introduces an efficient alternative by enabling inter-VLAN communication through a single physical interface on the router. This technique utilizes logical sub-interfaces on the router, where each sub-interface is assigned a unique VLAN ID and IP address. These logical interfaces allow the router to process traffic from multiple VLANs over a single physical connection. The router connects to the switch through a trunk link, which supports VLAN tagging. Tagged frames traverse the trunk link, ensuring that VLAN-specific traffic can be identified and routed appropriately. When traffic reaches the router, it is de-encapsulated, processed, and re-encapsulated with the VLAN tag corresponding to the destination VLAN. This allows seamless communication between devices in different VLANs without requiring multiple physical connections.

One-armed routing demonstrates the practical application of concepts such as VLAN tagging, frame encapsulation, and routing protocols. It optimizes hardware usage, reduces costs, and simplifies network design, making it an ideal solution for small to medium-sized networks or environments with limited hardware resources.

## 2. Lab Principle

One-armed routing operates by leveraging a single physical router interface to handle traffic for multiple VLANs through logical sub-interfaces. This is achieved by configuring a trunk link between the switch and the router, allowing the router to process tagged frames from multiple VLANs. Each logical sub-interface is associated with a unique VLAN ID and IP address, enabling inter-VLAN communication. When a data frame arrives at the router, the VLAN tag is removed during the de-encapsulation process, and the packet is routed based on its destination. Subsequently, a new VLAN tag corresponding to the target VLAN is added to the packet during re-encapsulation. The tagged frame is then transmitted back through the trunk link to the switch, which forwards it to the appropriate VLAN devices.

This configuration demonstrates efficient traffic management, enhances network segmentation, and reduces hardware requirements by utilizing a single router interface. By implementing one-armed routing, networks can achieve seamless inter-VLAN communication while maintaining cost-effectiveness and simplifying infrastructure design.

## 3. Lab Steps

- Device and cable selection in Cisco Packet Tracer.
- VLAN creation and port assignment on the switch.
- Configuration of trunk mode for the switch port connected to the router.
- Sub-interface configuration on the router for VLANs.
- IP address assignment and testing connectivity between devices in different VLANs.

# 二、Lab Report

## 1. Lab Objective and Requirements

### Lab Objectives

The objectives of this lab are to configure router sub-interfaces to enable inter-VLAN communication and to implement one-armed routing, which allows efficient data exchange between devices in different VLANs. By achieving these objectives, the lab demonstrates the practical application of VLAN segmentation and logical routing to optimize network performance and resource utilization. This experiment aims to equip participants with essential networking skills for designing and implementing efficient network infrastructures.

### Lab Requirements

To carry out this lab, specific tools and equipment are essential. These include Cisco Packet Tracer software, which provides a virtual simulation environment for networking setups. Hardware requirements include a router, specifically the model 2811, which will facilitate routing functionalities, and a switch, the model 2950-24, for VLAN creation and management. Additionally, two PCs are required, each assigned to a separate VLAN, to simulate inter-VLAN communication scenarios. Together, these components create a foundational setup for exploring and understanding VLAN tagging, routing protocols, and network traffic management within a segmented network environment.

## 2. Lab Environment

The lab was conducted using Cisco Packet Tracer. The topology consists of a router, a switch, and two PCs in VLAN 10 and VLAN 20.

***Fig – 1:*** *Software → Cisco Packet Tracer*

## 3. Lab Design

The lab design centers on configuring and testing one-armed routing between two VLANs to enable inter-VLAN communication. The experiment begins by setting up a network topology with two VLANs (VLAN 10 and VLAN 20) on a switch, where ports 1 to 5 are assigned to VLAN 10 and ports 6 to 10 are assigned to VLAN 20. This segmentation ensures that devices in different VLANs cannot communicate directly with each other. In this setup, two PCs—PC1 and PC2—are placed in different VLANs. PC1, in VLAN 10, is assigned the IP address 192.168.1.2 with a default gateway of 192.168.1.1, while PC2, in VLAN 20, is assigned the IP address 192.168.2.2 with a default gateway of 192.168.2.1. These PCs cannot communicate directly due to their placement in separate VLANs, and so a router is required to enable inter-VLAN routing.

The router configuration involves creating sub-interfaces on a single physical Ethernet interface (Fa0/0). Each sub-interface corresponds to one VLAN—Fa0/0.1 for VLAN 10 and Fa0/0.2 for VLAN 20. The sub-interfaces are assigned IP addresses matching the default gateway addresses of the PCs in each VLAN: 192.168.1.1/24 for VLAN 10 and 192.168.2.1/24 for VLAN 20. The router is configured with 802.1Q encapsulation on the sub-interfaces to correctly process tagged frames from the switch, and the `no shutdown` command is applied to enable the interfaces.

Once the devices are configured, communication between PC1 and PC2 is tested. If the configuration is correct, the router will forward traffic from PC1 (VLAN 10) to PC2 (VLAN 20) and vice versa. The one-armed routing configuration, where the router uses a single physical interface and multiple sub-interfaces for different VLANs, minimizes the need for additional hardware interfaces and demonstrates an efficient way to manage inter-VLAN traffic in a network. The lab allows students to understand the process of VLAN segmentation, routing between VLANs, and the importance of trunking and encapsulation in managing VLAN traffic in real-world networks.

## 4. Lab Process and Recording

### Step 1: Device Selection and Cable Connection

The lab process begins by selecting the required devices in the network simulator, which includes a router (model 2811), a switch (e.g., Cisco 2950-24), and two PCs. The devices are connected using appropriate cables based on the topology diagram. In this case, the router's *FastEthernet* port (Fa0/0) is connected to the switch's trunk port (Fa0/24), and the PCs are connected to the switch ports designated for VLANs 10 and 20. It is essential to ensure the correct physical connections before proceeding with the configuration.

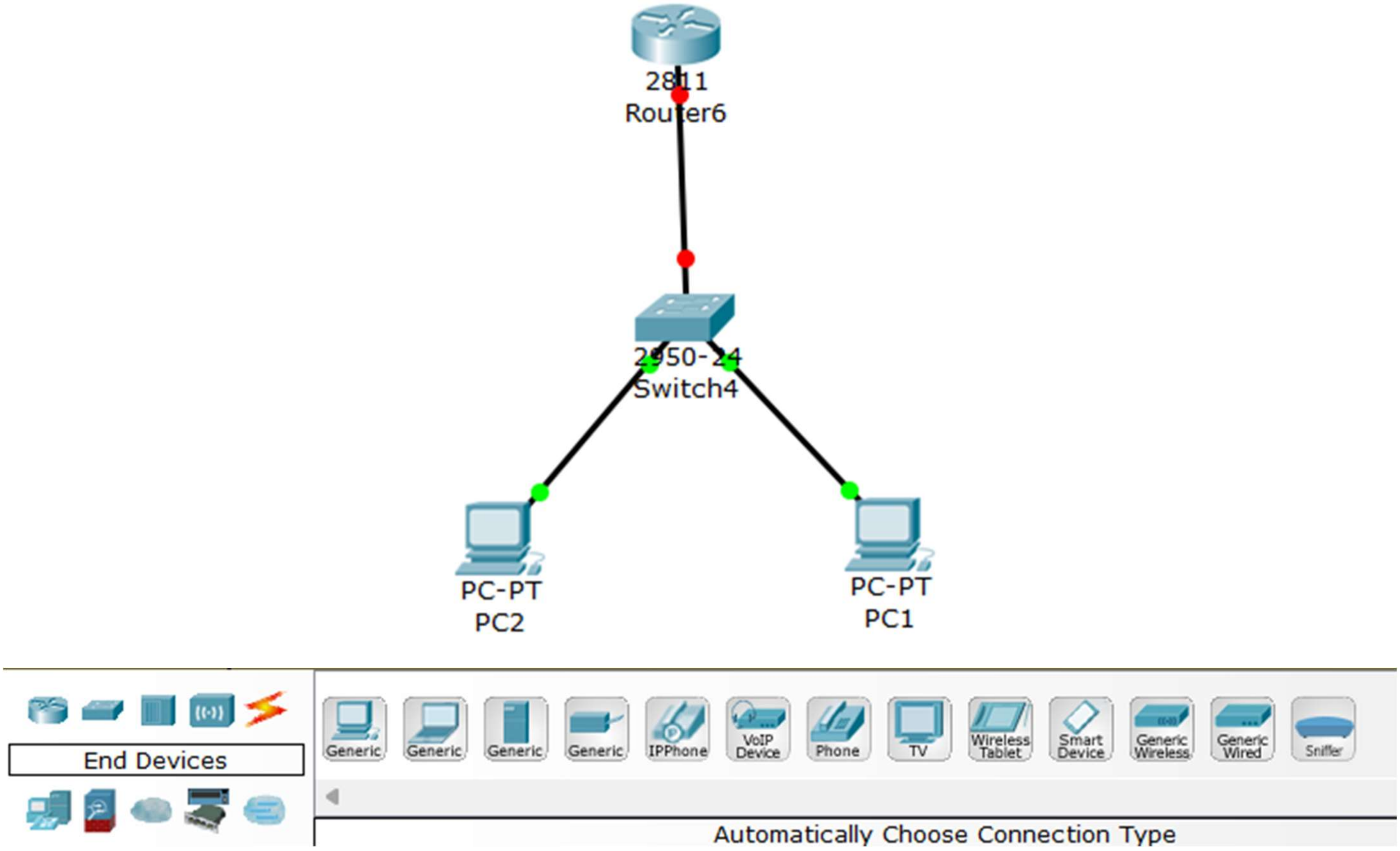
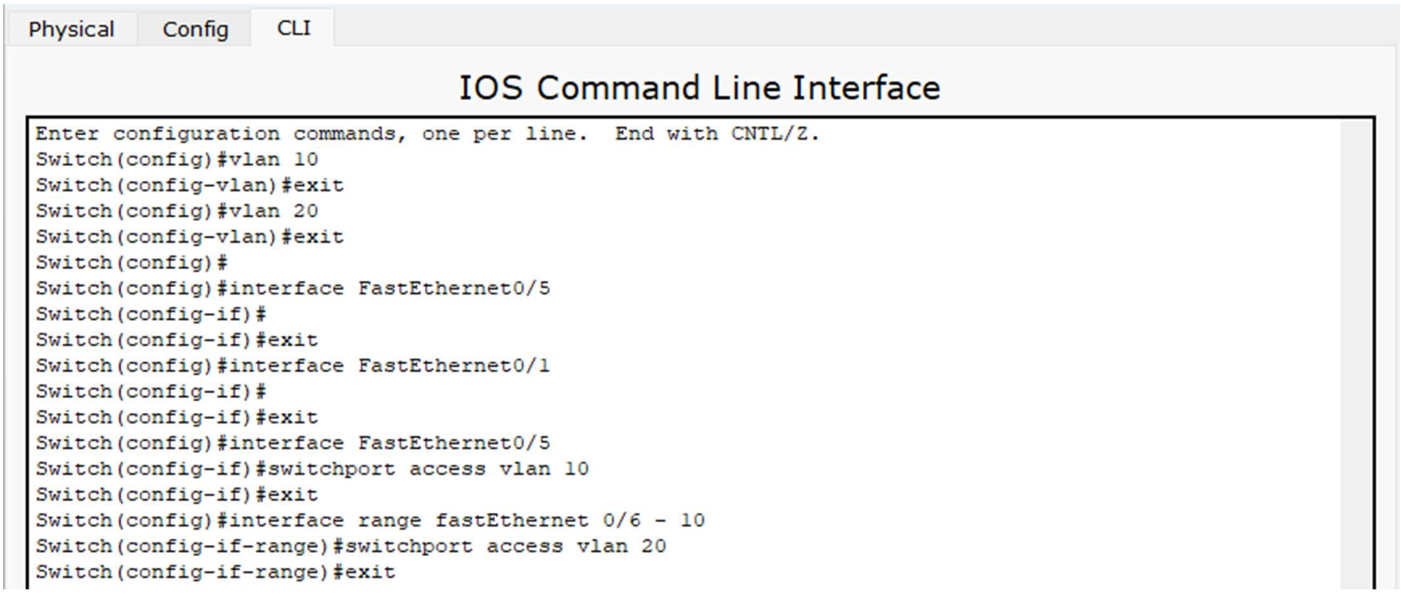


***Fig – 2:*** *Device Selection*

### Step 2: Configuring the Switch

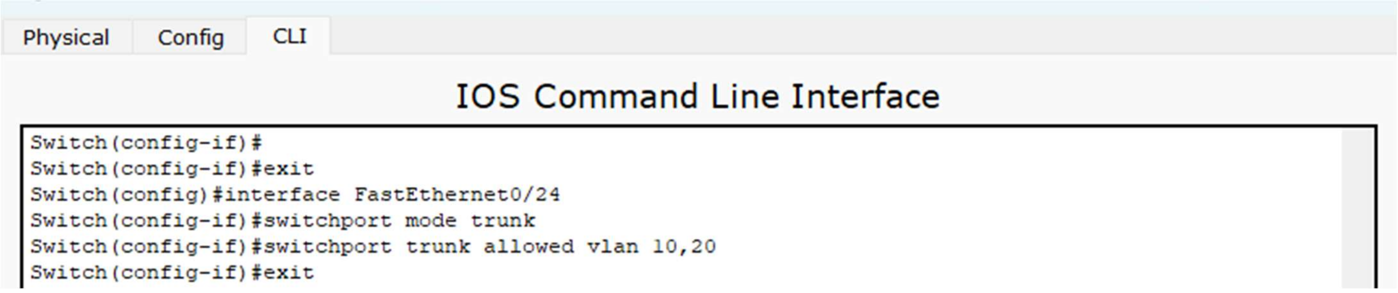
Once the devices are connected, the next step involves configuring the switch. The first task is to create VLAN 10 and VLAN 20 on the switch and assign the appropriate ports to each VLAN. VLAN 10 is assigned to ports 1 through 5, and VLAN 20 is assigned to ports 6 through 10. This is done through the following commands:



```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#interface FastEthernet0/5
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/5
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface range fastEthernet 0/6 - 10
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
```

***Fig – 3:*** *Switch Configuration*

After assigning VLANs to the appropriate ports, the next step is to configure the switch port connected to the router (Fa0/24) as a trunk. This allows the switch to carry traffic from both VLANs over a single link. The commands for configuring the trunk port are as follows:



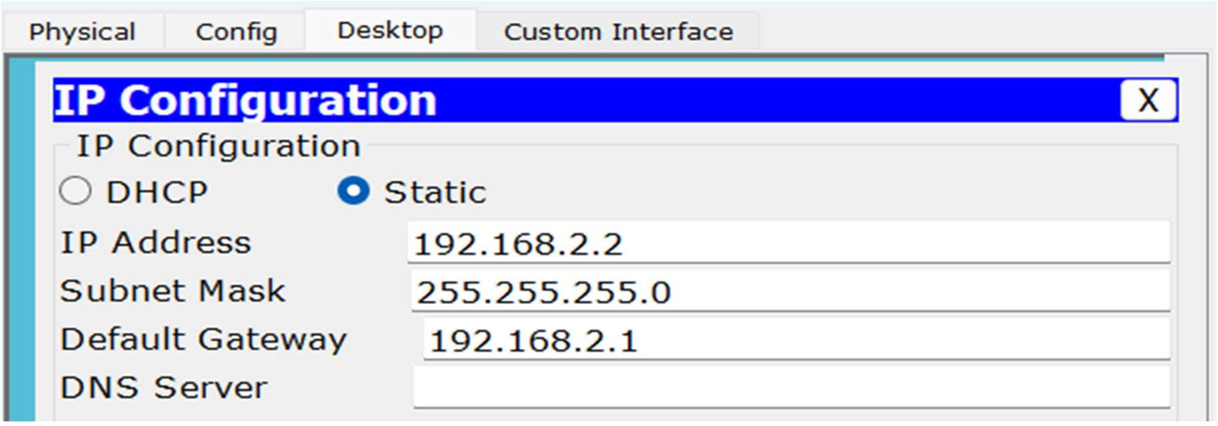
```
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20
Switch(config-if)#exit
```

***Fig – 4:*** *VLAN segmentation and trunking*

At this point, the switch is configured for VLAN segmentation and trunking, ensuring that the traffic from both VLANs can be sent to the router.

**Step 3: Configuring the PCs**

Next, the two PCs are configured with static IP addresses. PC1 in VLAN 10 is given the IP address 192.168.1.2 with the default gateway set to 192.168.1.1, while PC2 in VLAN 20 is configured with the IP address 192.168.2.2 and the default gateway 192.168.2.1. These IP configurations ensure that the PCs are in the correct subnets and can route traffic to their respective VLAN gateways.



IP Configuration

○ DHCP ● Static

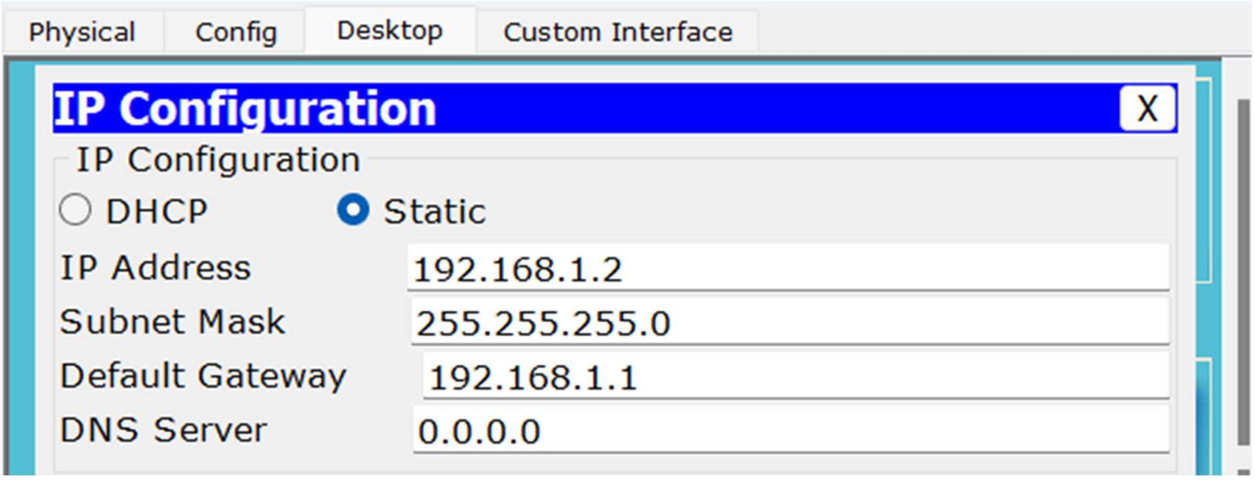
IP Address 192.168.2.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server

***Fig – 5:*** *PC1 Configuration*



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address 192.168.1.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

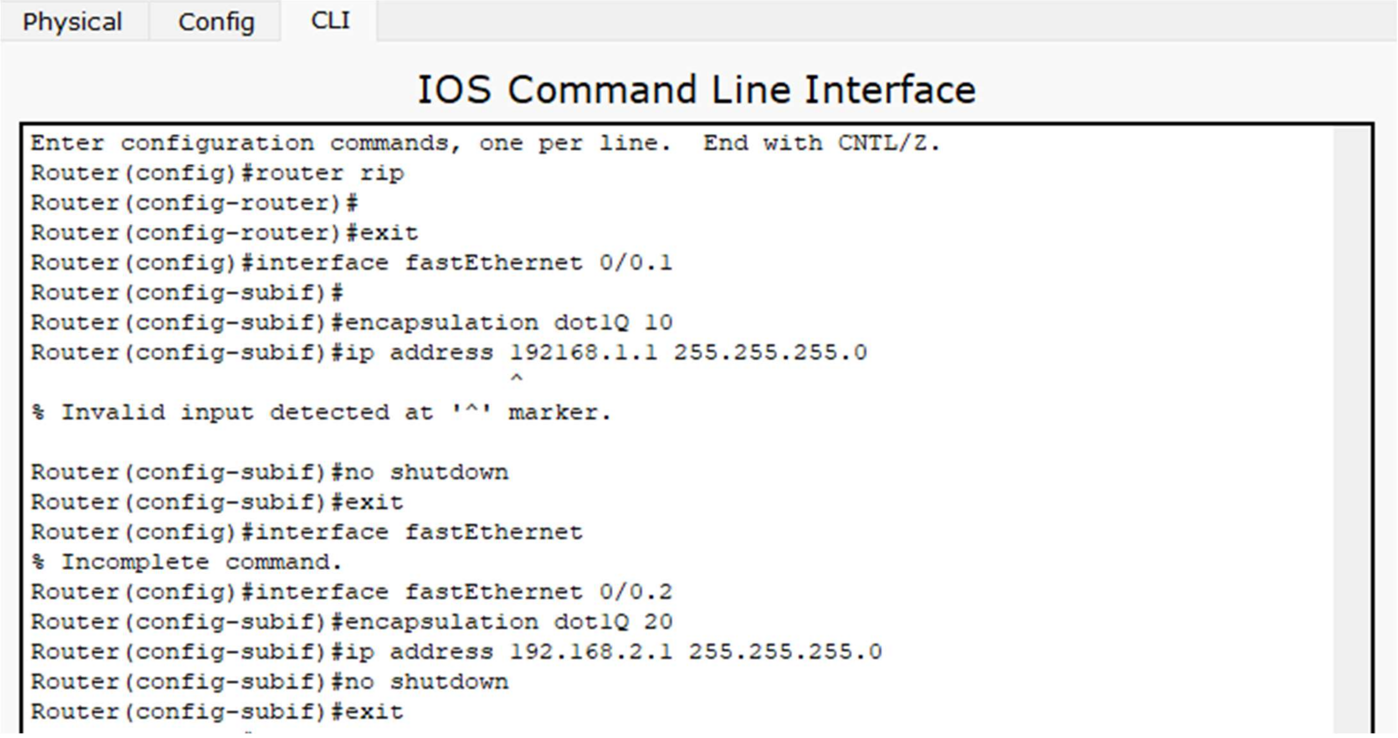
DNS Server 0.0.0.0

***Fig – 6:*** *PC2 Configuration*

The static IP configuration for PC1 and PC2 can be entered manually through the PC's desktop settings, as shown in the respective configuration windows for each PC.

### Step 4: Configuring the Router

The router is the key to enabling communication between VLANs, and it requires sub-interface configuration. The router’s Fa0/0 interface will be configured with two sub-interfaces: Fa0/0.1 for VLAN 10 and Fa0/0.2 for VLAN 20. The router sub-interfaces are configured with IP addresses that correspond to the default gateways of the PCs:



IOS Command Line Interface

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
Router(config-router)#exit
Router(config)#interface fastEthernet 0/0.1
Router(config-subif)#
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192168.1.1 255.255.255.0
                                  ^
% Invalid input detected at '^' marker.

Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#interface fastEthernet
% Incomplete command.
Router(config)#interface fastEthernet 0/0.2
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
```

***Fig – 7:*** *Router Configuration*

The dot1Q encapsulation ensures that the router can recognize the VLAN tags and process traffic accordingly. Once the sub-interfaces are configured, the router's physical interface (Fa0/0) is enabled using the no shutdown command.

### Step 5: Verifying and Testing Connectivity

After the configuration is completed, the final step is to verify the connectivity between the two PCs. Using the ping command, test the communication between PC1 (192.168.1.2) and PC2 (192.168.2.2). Since the router is responsible for forwarding traffic between the VLANs, the ping should successfully reach its destination if the configuration is correct. Any issues can be debugged by checking the VLAN assignments on the switch, the IP configurations on the PCs, and the sub-interface settings on the router.

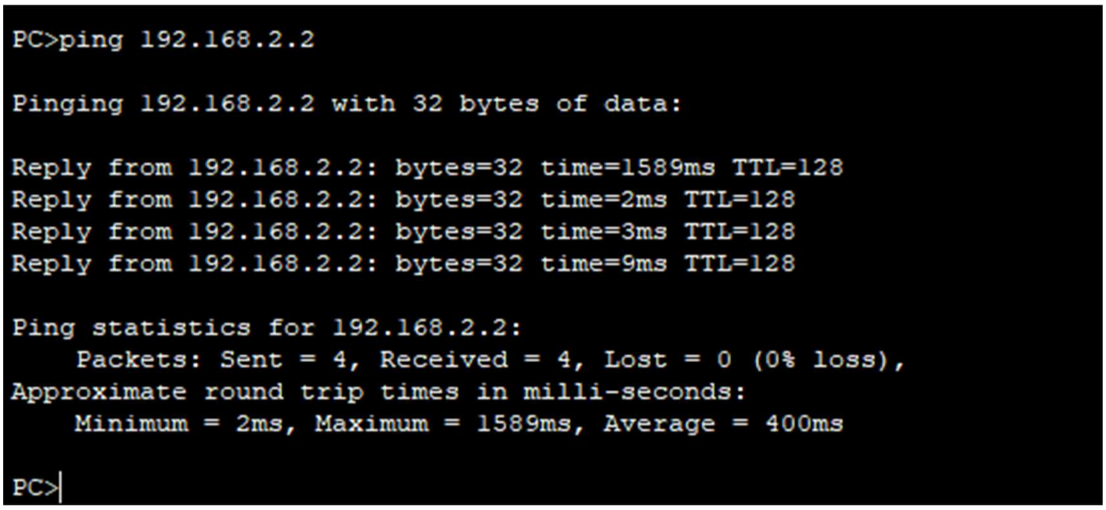
## 5. Lab Results and Analysis

After completing the configuration of the router, switch, and PCs, and verifying the network setup, the primary goal was to establish communication between the two PCs located in different VLANs (VLAN 10 and VLAN 20). The results were measured by performing a ping test from PC1 (192.168.1.2) in VLAN 10 to PC2 (192.168.2.2) in VLAN 20. The ping was successful, indicating that the one-armed routing configuration was properly set up and functional.

### Successful Ping Test

When the ping was initiated from PC1 (192.168.1.2) to PC2 (192.168.2.2), the following sequence of events occurred:

- PC1 sent the data frame with a VLAN 10 tag to the switch.
- The switch forwarded the frame to the router's trunk interface.
- The router identified the VLAN 10 tag, processed the data, and forwarded it to VLAN 20 through sub-interface Fa0/0.2.
- The switch then received the frame from the router with a VLAN 20 tag and forwarded it to PC2.
- PC2 successfully received the frame and responded to the ping, indicating that communication was established between the two PCs.



```
PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=1589ms TTL=128
Reply from 192.168.2.2: bytes=32 time=2ms TTL=128
Reply from 192.168.2.2: bytes=32 time=3ms TTL=128
Reply from 192.168.2.2: bytes=32 time=9ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 1589ms, Average = 400ms

PC>
```

***Fig – 8:*** *Ping Test*

### Analysis of Sub-Interface Configuration

The router's configuration of sub-interfaces for VLAN 10 and VLAN 20 was a critical component of the success. The use of dot1Q encapsulation on each sub-interface allowed the router to recognize the VLAN tags and properly route the traffic between the VLANs. The sub-interface IP addresses (192.168.1.1 for VLAN 10 and 192.168.2.2 for VLAN 20) acted as the default gateways for the PCs, ensuring proper routing of traffic between the two networks. The router's physical interface (Fa0/0) was configured to handle both VLANs, which reduced the need for multiple physical interfaces on the router, making the network setup more efficient. This one-armed routing approach simplified the configuration process and minimized hardware requirements.

## 三、Lab Summary

In this lab, the objective was to configure and test one-armed routing between two VLANs (VLAN 10 and VLAN 20) using a router and a switch. The one-armed routing technique involved setting up a router with sub-interfaces for each VLAN, connected to a switch through a trunk link. The lab configuration included creating VLANs, assigning switch ports to each VLAN, and configuring trunking on the switch port connected to the router. Additionally, IP addresses were assigned to the devices, and the router was set up to handle inter-VLAN communication through sub-interfaces with `dot1Q` encapsulation.

The experiment was successful, with the two PCs (one in each VLAN) successfully pinging each other, demonstrating that the router effectively routed traffic between the VLANs. The one-armed routing method was validated, showing that a single physical interface on the router, using multiple sub-interfaces, can manage traffic between multiple VLANs. This approach not only simplified the configuration but also minimized hardware requirements.

Overall, the lab reinforced key networking concepts such as VLAN configuration, trunking, sub-interface setup, and inter-VLAN routing, while demonstrating the practical application of one-armed routing in a network.