# Submitted By

Aqsa

**Submitted To**

Mr.Saqib Haleem,GM Tech,IT.

**Registration No**.

CAAD-HR/INT-1167/IT

**DESIGINATION**

Information Technology(Networking Internee)

[**Introduction 2**](#_Toc170922403)

[**Overview 3**](#_Toc170922404)

[**Internship objective 3**](#_Toc170922405)

[**Internship Activities 4**](#_Toc170922406)

[**Learning and achivements 5**](#_Toc170922407)

[**Conclusion 6**](#_Toc170922408)

[**Recommendations 7**](#_Toc170922409)

[**References 8**](#_Toc170922410)

[**Appendices 8**](#_Toc170922411)

# 

In the rapidly evolving world of information technology, the backbone of efficient communication and data exchange lies in the understanding and implementation of network infrastructures. This report delves into the foundational elements of networking, offering a comprehensive exploration of network devices, IP protocols, switching, VLANs (Virtual Local Area Networks), routing, routing protocols, and Linux basics. The study begins with an overview of network devices, which are the critical components that facilitate data transfer and communication between different systems. From routers and switches to firewalls and access points, understanding these devices is essential for building and maintaining robust networks.

This report provides an in-depth exploration of essential networking concepts and technologies, developed through hands-on learning and guided instruction at (), an institute known for its supportive and cooperative staff. The report covers a range of topics critical for anyone looking to build a strong foundation in networking.

At (), the learning environment is one where students are encouraged to grow without the burden of steep learning curves. The staff’s dedication to providing clear, practical instruction has allowed me to master the fundamentals of network devices, IP addressing , IP protocols, switching, VLANs (Virtual Local Area Networks), routing, routing protocols, and Linux basics.

The journey begins with an examination of network devices, the hardware that forms the backbone of any network. Understanding these devices, including routers, switches, is crucial for managing and securing network traffic.

Next, the report delves into IP protocols, the rules and standards that govern how data is transmitted across networks. Mastery of these protocols ensures that data flows smoothly and securely between different systems.

The topics of switching and VLANs are also explored, highlighting how data is managed and directed within a network. The use of VLANs for segmenting network traffic is particularly important for optimizing both performance and security.

Routing, and the protocols that govern it, are critical to understanding how data finds its way across complex networks. This section of the report explains how routing decisions are made to ensure efficient and reliable data transmission.

Finally, the basics of Linux are introduced.

The combination of ()’s excellent instructional support and these key topics ensures that this report is not just a summary of technical knowledge but also a testament to the effective, accessible learning environment provided by the institute.

The objective of this internship is to gain practical, hands-on experience in the field of networking by applying theoretical knowledge to real-world scenarios. Through this internship, I aim to deepen my understanding of network.

I seek to develop the technical proficiency required to design, implement, and manage network infrastructures effectively. Additionally, I aim to strengthen my problem-solving abilities and adapt to the dynamic challenges of the IT industry. This internship will also provide an opportunity to work alongside industry professionals, allowing me to learn from their expertise and grow both professionally and personally.

#### 

During the course of this internship, I will be engaged in a variety of activities designed to provide comprehensive exposure to networking concepts and practical experience in the field. These activities include:

1. **Network Device Configuration and Management**:
   * Setting up and configuring routers, switches, and other networking devices.
   * Learning how to manage network devices through command-line interfaces and web-based management tools.
   * Troubleshooting hardware and software issues related to network devices.
2. **IP Protocol Implementation**:
   * Understanding and configuring IP addressing schemes, including IPv4.
   * Implementing subnetting and supernetting techniques to optimize network performance.
   * Exploring and configuring IP protocols like TCP/IP, DHCP, and DNS.
3. **Switching and VLAN Configuration**:
   * Configuring network switches and learning about Layer 2 switching.
   * Creating and managing Virtual Local Area Networks (VLANs) to segment network traffic.
   * Implementing VLAN tagging and trunking for effective traffic management.
4. **Routing and Routing Protocols**:
   * Configuring static and dynamic routing on routers.
   * Exploring and implementing various routing protocols such as RIP, and EIGRP.
   * Analyzing routing tables and understanding the path selection process.
5. **Linux System Administration**:
   * Gaining hands-on experience with Linux operating systems, focusing on networking aspects.
6. **Documentation and Reporting**:
   * Documenting network configurations, changes, and troubleshooting steps.
   * Creating detailed reports on the progress of network projects and tasks completed.
   * Presenting findings and recommendations based on hands-on experiences.

Throughout the duration of this internship, I have gained significant insights and developed key skills that have enhanced my understanding of networking and IT. These are some of the most important learnings and achievements:

1. **In-Depth Knowledge of Networking Fundamentals**:
   * Gained a solid understanding of core networking concepts, including the OSI model, IP addressing, and subnetting.
   * Developed the ability to configure and manage network devices such as routers and switches, essential for maintaining network infrastructure.
2. **Mastery of IP Protocols and Networking Standards**:
   * Learned how to implement and troubleshoot various IP protocols like TCP/IP, DHCP, and DNS.
   * Acquired the skills to optimize network performance through effective IP addressing and routing strategies.
3. **Proficiency in Switching and VLAN Configuration**:
   * Successfully configured and managed VLANs, improving network segmentation and traffic management.
   * Learned how to set up and manage switches, ensuring efficient data flow within local networks.
4. **Advanced Routing Techniques**:
   * Gained experience in configuring both static and dynamic routing protocols, including RIP, EIGRP.
   * Enhanced my understanding of how routers select the best paths for data transmission, which is crucial for optimizing network efficiency.
5. **Effective Documentation and Reporting**:
   * Developed the ability to document network configurations, changes, and troubleshooting procedures clearly and concisely.
   * Gained experience in creating detailed reports and presentations to communicate technical findings and recommendations.

#### ****Achievements:****

1. **Successful Configuration of a Multi-Layer Network**:
   * Completed the configuration of a multi-layer network involving routers, switches, and VLANs, demonstrating a deep understanding of both Layer 2 and Layer 3 networking.
2. **Implementation of Dynamic Routing Protocols**:
   * Successfully implemented and tested dynamic routing protocols such as RIP in a simulated network environment, optimizing data flow and improving network resilience.
3. **Collaboration on Network Projects**:
   * Contributed to team projects that involved network design and troubleshooting, demonstrating the ability to work effectively in a collaborative environment and providing valuable input to achieve project goals.
4. **Recognition for Problem-Solving Skills**:
   * Received positive feedback from mentors and colleagues for my ability to quickly diagnose and resolve complex network issues, reflecting a strong problem-solving aptitude.

This internship has been an invaluable experience, providing me with a deep understanding of networking and IT fundamentals, as well as practical, hands-on skills that are essential for success in this field. The combination of learning about network devices, IP addressing, IP protocols, switching, VLANs, routing, routing protocols, and Linux Virtual Machine.

The supportive and cooperative environment at () played a crucial role in my learning journey, allowing me to overcome challenges without overwhelming difficulties. The mentorship and guidance provided by the staff have not only helped me grasp complex concepts but also instilled confidence in my ability to apply this knowledge in real-world scenarios.

Through the various activities and projects I engaged in, I have achieved significant milestones, from successfully configuring multi-layer networks to implementing advanced routing protocols and enhancing network security. These accomplishments have equipped me with the skills and knowledge necessary to contribute effectively to any networking environment.

Overall, this internship has been a critical step in my professional development, preparing me for future challenges and opportunities in the IT and networking industry. I am now better equipped to tackle complex networking tasks and continue advancing my career in this dynamic and ever-evolving field.

Based on my experiences and the skills I have developed during this internship, I offer the following recommendations for anyone looking to pursue a career in networking or similar fields:

1. **Embrace Hands-On Learning**:
   * Theory is important, but practical experience is essential for mastering networking concepts. Engage in hands-on activities such as configuring devices, setting up networks, and troubleshooting issues to solidify your understanding.
2. **Build a Strong Foundation in Networking Fundamentals**:
   * Ensure a thorough understanding of core networking principles, including the OSI model, IP addressing, subnetting, and routing. These basics are critical for advancing in more complex areas of networking.
3. **Stay Current with Technology and Industry Trends**:
   * The field of networking is constantly evolving. Keep yourself updated on the latest technologies, tools.
4. **Develop Proficiency in Linux**:
   * Linux is widely used in networking and IT.
5. **Document Your Work**:
   * Develop the habit of documenting your configurations, troubleshooting steps, and project progress. Clear documentation not only helps in understanding and replicating solutions but also serves as a valuable reference in the future.
6. **Seek Out Mentorship and Guidance**:
   * Take advantage of opportunities to learn from experienced professionals. Their insights and advice can help you navigate complex topics and provide guidance on career development.
7. **Engage in Continuous Learning**:
   * Networking and IT fields are dynamic, requiring ongoing learning. Pursue certifications, online courses, and other educational opportunities to stay ahead and enhance your skill set.
8. **Take Initiative and Challenge Yourself**:
   * Don’t hesitate to take on challenging projects or tasks that push your limits. This is where significant learning occurs, and it will prepare you for the complexities of a professional networking environment.

**Cisco Systems, Inc.**  
"Networking Basics: What You Need to Know."  
Cisco Networking Academy.

**NCP (Networking and Computer Professionals)**  
Internal training materials and practical sessions provided by NCP instructors during the internship.

**Router:** A networking device that forwards data packets between computer networks, directing traffic based on IP addresses.

**Switch:** A device that connects multiple devices within the same network and uses MAC addresses to forward data to the correct destination.

### ****Hub:**** A basic device that connects multiple devices on a network but does not manage traffic as efficiently as a switch. Mostly obsolete, replaced by more intelligent devices like switches.

**IP protocol:** An Internet Protocol (IP) address is the unique identifying number assigned to every device connected to the internet. An IP address definition is a numeric label assigned to devices that use the internet to communicate.

**TCP/UDP:** TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are two fundamental communication protocols that play a crucial role in how data is transmitted across networks. TCP is connection-oriented, meaning it establishes a reliable connection between sender and receiver before transmitting data. It ensures that data is delivered accurately and in the correct order, making it ideal for applications where reliability is essential, such as web browsing, email, and file transfers. TCP’s error-checking mechanisms and flow control further contribute to its reliability, although this also makes it slower and more complex compared to UDP. On the other hand, UDP is a connectionless protocol that sends data without establishing a connection or ensuring its delivery. This makes UDP faster and more efficient for applications where speed is critical and some data loss is acceptable, such as live streaming, online gaming, and video conferencing. Unlike TCP, UDP does not guarantee the order of data or provide error correction, making it less reliable but more suitable for real-time applications where latency is a key concern. Both protocols are widely used, each serving different purposes based on the specific needs of the application.

**Repeater:** is a device that regenerates and amplifies signals in a network, enabling the extension of the signal over longer distances without degradation, which is crucial in ensuring reliable communication over large areas. On the other hand.

**Bridge:** is used to connect and filter traffic between two different network segments, working at the data link layer (Layer 2) of the OSI model. It helps reduce traffic by dividing networks into smaller, manageable sections and only forwarding necessary data, effectively improving network efficiency.

**Modem:** (short for modulator-demodulator) is another key device that allows digital data from a computer to be transmitted over analog communication lines, such as telephone lines or cable systems. It modulates digital signals into analog signals for transmission and then demodulates incoming analog signals back into digital form for processing by the computer.

**Physical topology:**  It refers to the physical arrangement of network devices, cables, and other infrastructure within a network. Common types include star, bus, ring, and mesh topologies, each with its strengths and weaknesses depending on factors like scalability, fault tolerance, and ease of installation. For instance, in a star topology, all devices are connected to a central hub or switch, which can make the network easy to manage and troubleshoot but also introduces a single point of failure. Understanding these devices and topologies is essential for designing and maintaining efficient, reliable networks.

**Transmission media:** are the physical pathways through which data is transmitted from one device to another in a network. These media can be broadly categorized into two types:

* **guided (wired)**
* **unguided (wireless)**

**Guided media:**

Includes twisted pair cables, coaxial cables, and fiber optic cables. Twisted pair cables, commonly used in Ethernet networks, consist of pairs of wires twisted together to reduce electromagnetic interference, making them suitable for short to medium distances.

Coaxial cables, used in cable television and early networking, have a single conductor surrounded by insulation and shielding, offering better resistance to interference over longer distances.

Fiber optic cables: use light signals to transmit data, offering high-speed transmission over very long distances with minimal signal loss, making them ideal for backbone networks and long-distance communication.

**Unguided media:** encompasses wireless transmission methods like radio waves, microwaves, and infrared. These allow data to be transmitted through the air, providing flexibility and mobility, which is crucial for applications like Wi-Fi, mobile networks, and satellite communication. Each type of transmission media has its advantages and is chosen based on factors like distance, bandwidth requirements, cost, and the specific needs of the network environment.

**IP Protocol (Internet Protocol):** A set of rules governing the format of data sent over the internet or local network.

**OSI (Open Systems Interconnection)** model is a framework used to understand and standardize the functions of a networking system. It divides the process of communication into seven distinct layers:

1. **Physical Layer**: Deals with the physical connection between devices, including cables, switches, and the actual hardware.
2. **Data Link Layer**: Handles error detection and correction from the Physical Layer. It is responsible for the node-to-node delivery of data.
3. **Network Layer**: Manages the routing of data across networks, determining the best path for data to travel from source to destination.
4. **Transport Layer**: Ensures reliable data transfer between devices, handling error recovery and flow control.
5. **Session Layer**: Manages sessions or connections between applications, including opening, closing, and managing sessions.
6. **Presentation Layer**: Translates data between the application layer and the network. It handles data encoding, encryption, and compression.
7. **Application Layer**: Provides network services directly to applications. It is where end-user software interacts with the network, such as web browsers or email clients.

**VLAN (Virtual Local Area Network):** A subnetwork that groups together a collection of devices from different physical LANs, enhancing security and reducing broadcast traffic. A vlan is a logical divition of a physical network into multiple virtual network it allows multiple virtual networks to store the same physical network infrastructure , improving network organization , security and management.

**STP ( Spanning Tree protocol ):**

Spanning tree protocol is a network protocol that insure a loop-free topology in a layer 2 network loop and broadcast strome by creating a tree like stucture , hance the name:

1. Root bridge: The external switch that acts as the reference point for the spaning tree.
2. Bridge ID: A unique identifier for each switch consisting of the switch MAC address and priority.
3. Port state: A port can be in one of three state forwarding, blocking, Disable.
4. Path cost: The cost of a path from a switch to the root bridge.

**How STP works**

**1. Root bridge:** switch exchnage BPDU( Bridge protocol Data unit ) message to select the Root bridge. The switch with the lowest BID become the root bridge.

**2.The construction :** Each Switch calculated its path cost to the RB and designates its port as post port (RP) Designated port (DP) or Blocking port (BP).

**3.port rules:**

- Root port: The port that connects to the RB

-Designated port: The port that connects to the RB or another switch RP.

-Blocking Port: A port that is not forwarding traffic to prevent loop.

**4.Topology changes:**When a switch detect a topology change it sends BPDU message to update the tree structure.

**5. Conversion**: The process of updating the tree structure and port states to ensure a loop free topology.

**DHCP:** Is a network protocol that automatically assigns IP addresses and other network configuration parameters to devices on a network, such as computers and smartphones, allowing them to communicate effectively. This eliminates the need for manual IP address configuration and ensures that each device receives a unique IP address.

**DNS:** Is a system that translates human-friendly domain names (like www.example.com) into IP addresses that computers use to identify each other on the network. By converting domain names into IP addresses, DNS makes it easier for users to access websites and services without having to remember complex numerical addresses.

**SNMP:** Stands for Simple Network Management Protocol. It's a protocol used for managing and monitoring network devices such as routers, switches, servers, and printers. Here's a breakdown of its work and benefits:

**Tool:** Solarwind, Grafana.

……………………………………………………….

**Routing Protocol:** Protocols used by routers to communicate with each other to determine the best path for data to travel across a network. Examples include RIP, OSPF, and EIGRP.

**Linux:** An open-source operating system widely used in servers, networking, and IT environments.

**Virtual Machine:** Basic commands and how to create aVirtual Machine on VM ware.

**…………………………………………………………….**

**IP addressing:**

IPv4 (Internet Protocol version 4) is the fourth version of the Internet Protocol, widely used to identify devices on a network through an addressing system. Here’s an in-depth look at IPv4 addressing:

**1. IPv4 Address Format**

- Address Length: IPv4 uses 32-bit addresses.

- Notation**:** Typically written as four decimal numbers each ranging from 0 to 255 separated by dots.

- Example: `192.168.1.1`

- Binary Representation: Each of the four decimal numbers is the binary equivalent of an 8-bit number (octet).

- Example: `192.168.1.1` in binary is `11000000.10101000.00000001.00000001`

**2. Types of IPv4 Addresses**

- Public IP Address: Globally routable on the internet and unique across the entire web. Assigned by Internet Service Providers (ISPs).

- Private IP Address: Used within local networks, not routable on the public internet. Commonly used for internal devices like computers, printers, and phones within a private network.

4. **Subnetting:**

- **Subnetting:** The process of dividing a large network into smaller, more manageable subnetworks (subnets). This is done by extending the network portion of the address and reducing the host portion.

- **Subnet Mask:** A 32-bit number that divides the IP address into the network and host portions. Commonly used subnet masks:

- Class A: 255.0.0.0

- Class B: 255.255.0.0

- Class C: 255.255.255.0

**6. Dynamic vs. Static IP Addresses**

- Dynamic IP Address: Assigned automatically by a DHCP (Dynamic Host Configuration Protocol) server and may change periodically.

- Static IP Address: Manually configured and remains constant over time, typically used for servers, routers, and other critical network devices.

**7. NAT (Network Address Translation)**

- **NAT:** A technique used by routers to translate private IP addresses within a local network to a public IP address for Internet access. It allows multiple devices on a local network to share a single public IP address.

- **Purpose:** Conserves public IP addresses and adds a layer of security by masking internal IP addresses from the outside world.

**8. Broadcast, Multicast, and Unicast**

- Unicast: One-to-one communication between a single sender and a single receiver.

- Broadcast: One-to-all communication, where a message is sent to all devices in the network. The broadcast address for IPv4 is typically `255.255.255.255`.

- Multicast: One-to-many communication, where a message is sent to a specific group of devices. Uses Class D addresses.

**Subnetting**

**/21**

**= 224-21**

**= 23**

**= 256-8**

**=248**

**255.255.248.0**

**/27**

**= 232-27**

**= 25**

**= 256-32**

**=224**

**255.255.255.224**

**/22**

**= 224-22**

**= 22**

**= 256-4**

**=252**

**255.255.252.0**

**/18**

**= 224-18**

**= 26**

**= 256-64**

**=192**

**255.255.192.0**

**/30**

**= 232-30**

**= 22**

**= 256-4**

**=252**

**255.255.255.252**

**/14**

**= 216-14**

**= 22**

**= 256-4**

**=252**

**255.252.0.0**

**/4**

**= 28-4**

**= 24**

**= 256-16**

**=240**

**240.0.0.0**

**Subnet Mask**

192.168.10.102/28

Subnet mask is 255.255.255.240/28

**Range**

192.168.10.32

.

.

.

192.168.10.47

192.168.10.0

.

.

.

192.168.10.15

192.168.10.16

.

.

.

192.168.10.31

192.168.10.96

.

.

.

192.18.10.111

192.168.10.64

.

.

.

192.168.10.95

192.168.10.48

.

.

.

192.168.10.63

**Network I.D**

192.168.10.96

192.168.10.97

**First usable I.D**

**Broadcast ID**

192.168.10.110

192.168.10.111

**Last usable I.D**

**Network Device Configuration Examples**

1**. Router Configuration Example:**

- Basic IP address and subnet mask setup.

**- Example:**

Router(config)# interface gigabitethernet0/0

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# no shutdown

**2. Switch Configuration Example:**

VLAN creation and assignment.

**- Example:**

Switch(config)# vlan 10

Switch(config)# interface fastethernet0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

**Appendix A: Routing Protocol Configuration Examples**

**1. RIP (Routing Information Protocol):**

- Example:

Router(config)# router rip

Router(config-router)# version 2

Router(config-router)# network 192.168.1.0

**Appendix B:** Internship Logbook

- **Introduction to networking devices, OSI layers, IP addressing, and subnetting.**

**- Configuring and managing switches, VLAN setup, and network segmentation.**

**- Routing protocols (RIP, HSRP), hands-on router configuration, and troubleshooting.**

**Appendix C: Feedback and Evaluation**

- **Instructor Feedback:**

- Demonstrated strong problem-solving skills and a solid understanding of routing protocols.

-Showed great initiative in learning Linux system administration and applying it to networking tasks.

**- Self-Evaluation:**

- I have greatly improved my practical networking skills, particularly in VLAN configuration and routing. I also…

This appendix section provides additional details and resources that support the main content of the report, offering a deeper insight into the learning and practical experience gained during the internship.

**-Switching( Inter vlan routing)**

Inter-VLAN routing is a process used in computer networking that allows different Virtual Local Area Networks (VLANs) to communicate with each other. VLANs are used to segment a network into smaller, isolated subnetworks, each with its own broadcast domain. By default, devices in one VLAN cannot communicate with devices in another VLAN. Inter-VLAN routing is used to enable this communication.

**Assign name to Vlan**

**Step-by-Step Guide:**

2. **Enter Global Configuration Mode:**

* Switch> enable
* Switch# configure terminal

3. **Enter VLAN Configuration Mode:**

* Switch(config)# vlan [VLAN\_ID]

4. **Assign a Name to the VLAN:**

* Switch(config-vlan)# name [VLAN\_NAME]

5. **Exit Configuration Mode**:

* Switch(config-vlan)# exit

**Example**

Switch> enable

Switch# configure terminal

Switch(config)# vlan 10

Switch(config-vlan)# exit

Point to point route:

Router(config)# interface gigabitethernet0/0

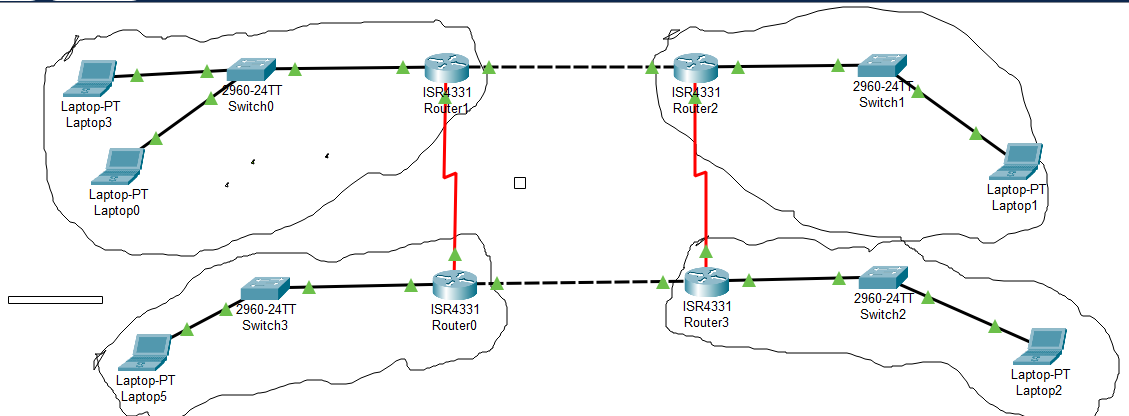
Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# no shutdown

**Methods of Inter-VLAN Routing**

**Layer 3 Switch (Multilayer Switch):**

A Layer 3 switch can perform both switching Layer 2 and routing Layer 3. VLANs are created on the switch, and then virtual interfaces called SVI Switched Virtual Interfaces are configured for each VLAN. The Layer 3 switch routes traffic between VLANs directly without the need for a separate router.

**Objective:** Connect four Network with two different VLAN’S using four router and four switches and ensure communication beteen devices.

1. **Create VLANs on the switch:**

Switch(config)# vlan 10

Exit

Switch(config)# vlan 20

Exit

**2. Assign switch ports to VLANs:**

Switch(config)# interface fastEthernet 0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

Switch(config)# interface fastEthernet 0/2

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 2

Same as like with 2 other switch.

**3. Configure the trunk port:**

Switch(config)# interface fastEthernet 0/5

Switch(config-if)# switchport mode trunk

**4. Configure subinterfaces on the router:**

Router(config)# interface gigabitEthernet 0/0.10

Router(config-subif)# encapsulation dot1Q 10

Router(config-subif)# ip address 192.168.10.1 255.255.255.0

Router(config)# interface gigabitEthernet 0/0.20

Router(config-subif)# encapsulation dot1Q 20

Router(config-subif)# ip address 192.168.20.1 255.255.255.0

Same as like with 2 other switch.

5**. Enable IP routing on the router:**

Router(config)# ip routing

With this setup, the router will route traffic between VLAN 10 and VLAN 20, allowing devices in these VLANs to communicate with each other.

**Dynamic Routing:**

Configure RIP routing on three routers to enable communication between three networks and a PC.

Task:

1. Enable RIP routing on all routers.

2. Configure network statements for each network.

3. Verify RIP routing tables.

4. Test connectivity from PC1 to Router3.

**Dynamic route rip**

1**. Access the Router's Command Line Interface (CLI)**

Select Router

Router> enable

2. **Enter Global Configuration Mode**

Router# configure terminal

**3. Enable RIP Routing Protocol**

Router(config)# router rip

**Network 1:**

192.168.1.0/24

PC1 (192.168.1.2)

Router1 (10.1.1.1)

**Network 2:**

192.168.2.0/24

Router2 (10.2.2.1)

Router1 (10.2.2.2)

**Network 3:**

192.168.3.0/24

Router3 (10.3.3.1)

Router2 (10.3.3.2)

**Configuration:**

**Router1:**

ip routing

router rip

network 192.168.2.0

network 192.168.3.0

**Router2:**

ip routing

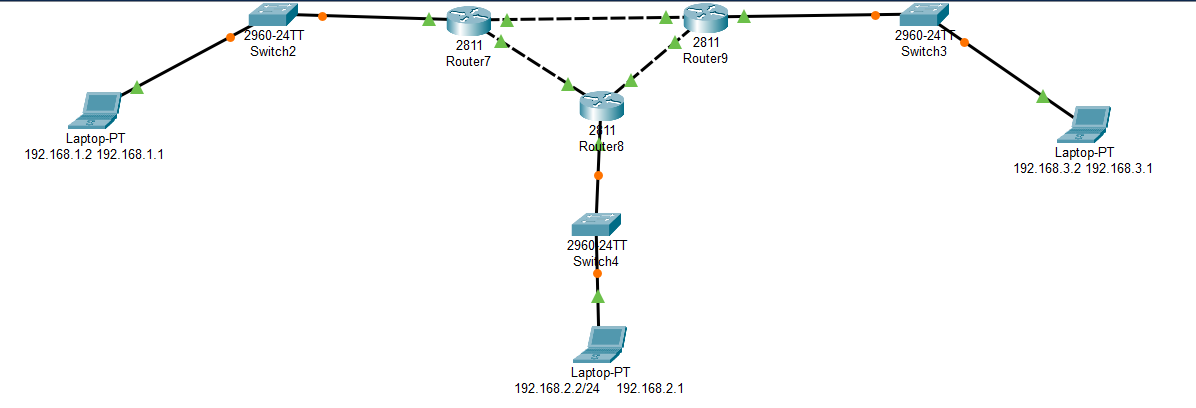
router rip

network 192.168.1.0

network 192.168.3.0

**Router3:**

ip routing

router rip

network 192.168.3.0

**Addresses:**

Laptop: 192.168.1.1

**Router1:**

gigabitEthernet0: 10.1.1.1

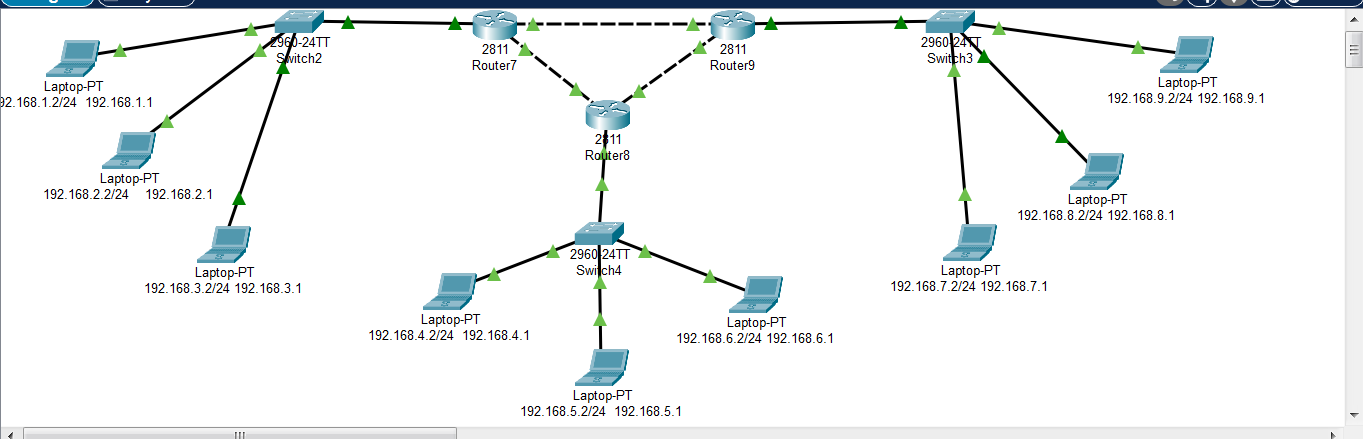
gigabitEthernet1: 10.2.2.2

**Router2:**

gigabitEthernet0: 10.2.2.1

gigabitEthernet1: 10.3.3.2

**Router3:**

gigabitEthernet0: 10.3.3.1

**HSRP (VRRP)Protocol:**

**Objective:**

**Configure two distributed switches (DS1 and DS2) connected to three other switches (S1, S2, and S3), each with three different networks and PCs.**

1. **Access the Router's Command Line Interface (CLI)**

Router> enable

**2.Enter Global Configuration Mode**

Router# configure terminal

**3. Enter Interface Configuration Mode**

Router(config)# interface [interface\_id]

**- Example:**

Router(config)# interface GigabitEthernet0/1

**4. Assign the HSRP Group Number and Virtual IP Address**

Router(config-if)# standby [group\_number] ip [virtual\_ip\_address]

- **Example:**

Router(config-if)# standby 1 ip 172.16.16.19

**5. (Optional) Set HSRP Priority**

Router(config-if)# standby [group\_number] priority [priority\_value]

- **Example:**

Router(config-if)# standby 1 priority 150

**6. (Optional) Configure Preemption**

- Preemption: allows a router with a higher priority to take over as the active router if it comes online after another router has already taken the active role. Enable preemption:

Router(config-if)# standby [group\_number] preempt

**7. Exit and Save Configuration**

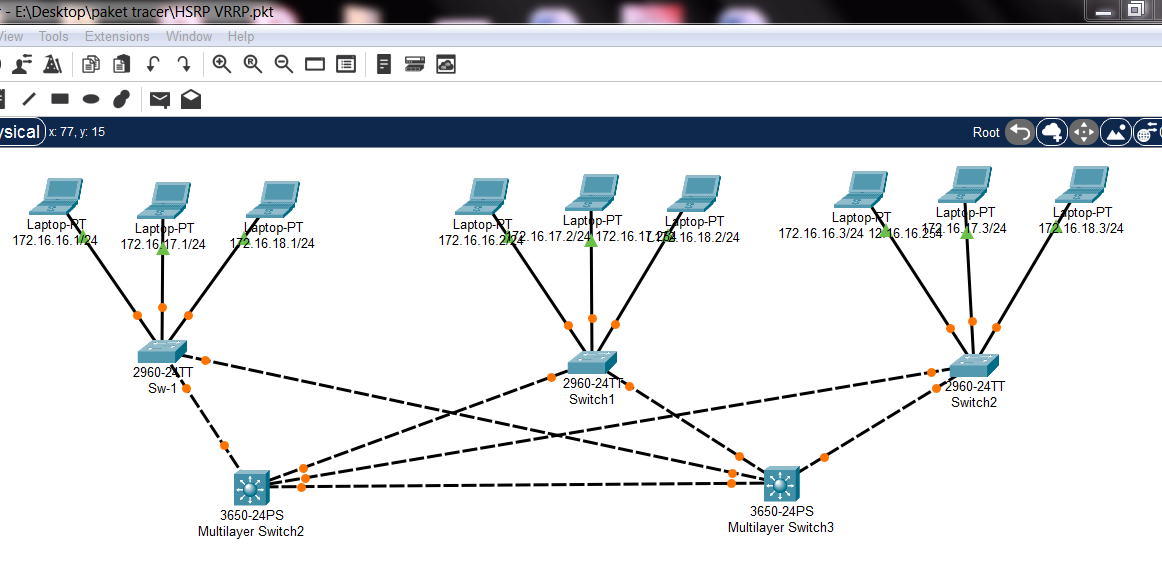
Router(config-if)# exit

- **Save the configuration** to ensure it persists after a reboot:

Router# write memory

Router# copy running-config startup-config

**8. Verification**

 Router# show standby