NED UNIVERSITY OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND IT

TSDS (with Specialization in Data Science)

CT-376 COMPUTER COMMUNICATION NETWORKS

CCP REPORT

COMPLEX NETWORK TOPOLOGY

SUBMITTED BY:

Ebaad Khan	**DT-22045**
Ezaan Khan	**DT-22046**
Syed Ahmed Ali	**DT-22301**
Muhammad Khuzaima Hassan	**DT-22302**

Submitted to: Dr. Abdul Karim Kazi

Contents

1. PROBLEM STATEMENT

The objective of this project is to design and implement a **complex network topology** to demonstrate the integration of various networking concepts and protocols. The topology must showcase **network segmentation, secure management access, dynamic and static routing, redundancy, and scalability**, while being centrally manageable and highly secure. This will be achieved through the implementation of technologies such as **VLANs, Telnet, DHCP, FTP, RIP, Eth-Trunk (LACP), STP, static routing, and subnetting**.

2. PROBLEM DESCRIPTION

This project involves the simulation of a network consisting of several routers and switches interconnected to emulate a realistic enterprise-like infrastructure. The network will be logically divided into departments or zones through **VLANs and subnetting**, and each segment will be assigned its own routing and addressing scheme.

The topology must integrate:

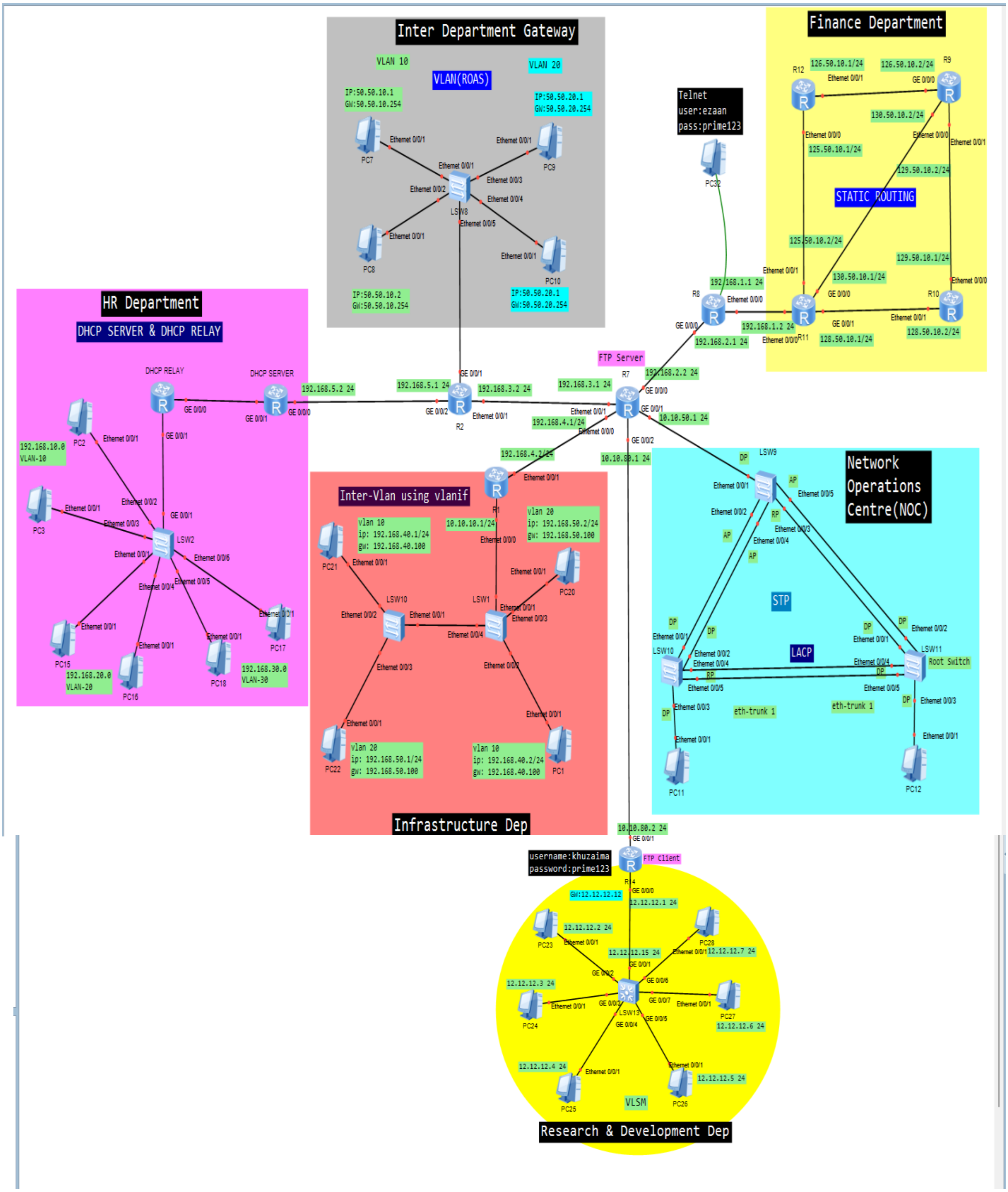
- **Console and Telnet security** on all routers and switches
- **Static and dynamic (RIP) routing** for inter-network communication
- **STP** for Layer 2 loop prevention and redundancy
- **Eth-Trunk using LACP** to demonstrate link aggregation
- **DHCP** to automate IP assignment
- **FTP** for backup and file transfer simulations

3. INTRODUCTION

In modern networking, the deployment of reliable and secure infrastructures is crucial for operational success. This project simulates such a complex environment using **virtual routers, switches, and hosts** to understand the real-time behavior of integrated networking features. The use of subnetting, VLANs, dynamic routing protocols, and remote access tools like Telnet helps build a topology that mimics the challenges and solutions of enterprise networks.

Through this project, learners will gain hands-on experience with advanced features such as **STP convergence, ROAS (Router-on-a-Stick), DHCP automation,** and **FTP file sharing**, all of which are vital in configuring a robust and scalable network.

4. NETWORK TOPOLOGY



5. TERMINOLOGIES USED IN TOPOLOGY

- **Subnetting**
  Subnetting is the process of dividing a larger IP network into smaller, more manageable sub-networks (subnets). In this topology, subnetting is used to allocate IP ranges to different departments or VLANs (e.g., HR, Finance, IT). This improves IP address utilization, reduces broadcast domains, and enhances network efficiency. Each subnet is associated with a specific VLAN or physical segment to logically separate traffic.

- **Telnet**
  Telnet is enabled on all routers and switches to allow remote configuration and monitoring from a central management device. For security, a login password and VTY (Virtual Terminal Lines) configurations are applied to each device. A designated PC (or router) acts as the administrative terminal that can access every network device using Telnet. This setup enables centralized control, remote troubleshooting, and configuration without direct physical access.

- **Eth-Trunk (LACP)**
  Eth-Trunk, using **Link Aggregation Control Protocol (LACP)**, is configured between switches and between routers and switches to form **logical aggregated links**. These links combine multiple physical interfaces into one logical channel, increasing bandwidth and providing redundancy. If one link in the trunk fails, the traffic automatically reroutes over the remaining links, ensuring high availability and load balancing.

- **Static Routes**
  Static routing is used to manually define specific paths for traffic between routers that are not part of the same dynamic routing domain. This gives the network administrator **greater control** over how traffic flows and can be useful for default routing, backup links, or secure point-to-point connections. In this topology, static routes are configured alongside RIP to demonstrate hybrid routing configurations.

- **RIP (Routing Information Protocol)**
  RIP is used to enable dynamic route exchange between routers. By periodically broadcasting the routing table, RIP helps routers learn paths to remote networks automatically. RIP version 2 (RIPv2), which supports subnet masks and authentication, is used to ensure compatibility with sub netted networks and provide a level of route security. It is ideal for the medium-sized topology in this simulation.

- **Spanning Tree Protocol (STP)**
  STP is enabled on all switches to **prevent Layer 2 loops** in the network. STP ensures that only one active path exists between any two switches at a time by placing extra links in a blocking state. When a link fails, STP reconverges and reactivates one of the backup paths, thus maintaining network stability and redundancy.

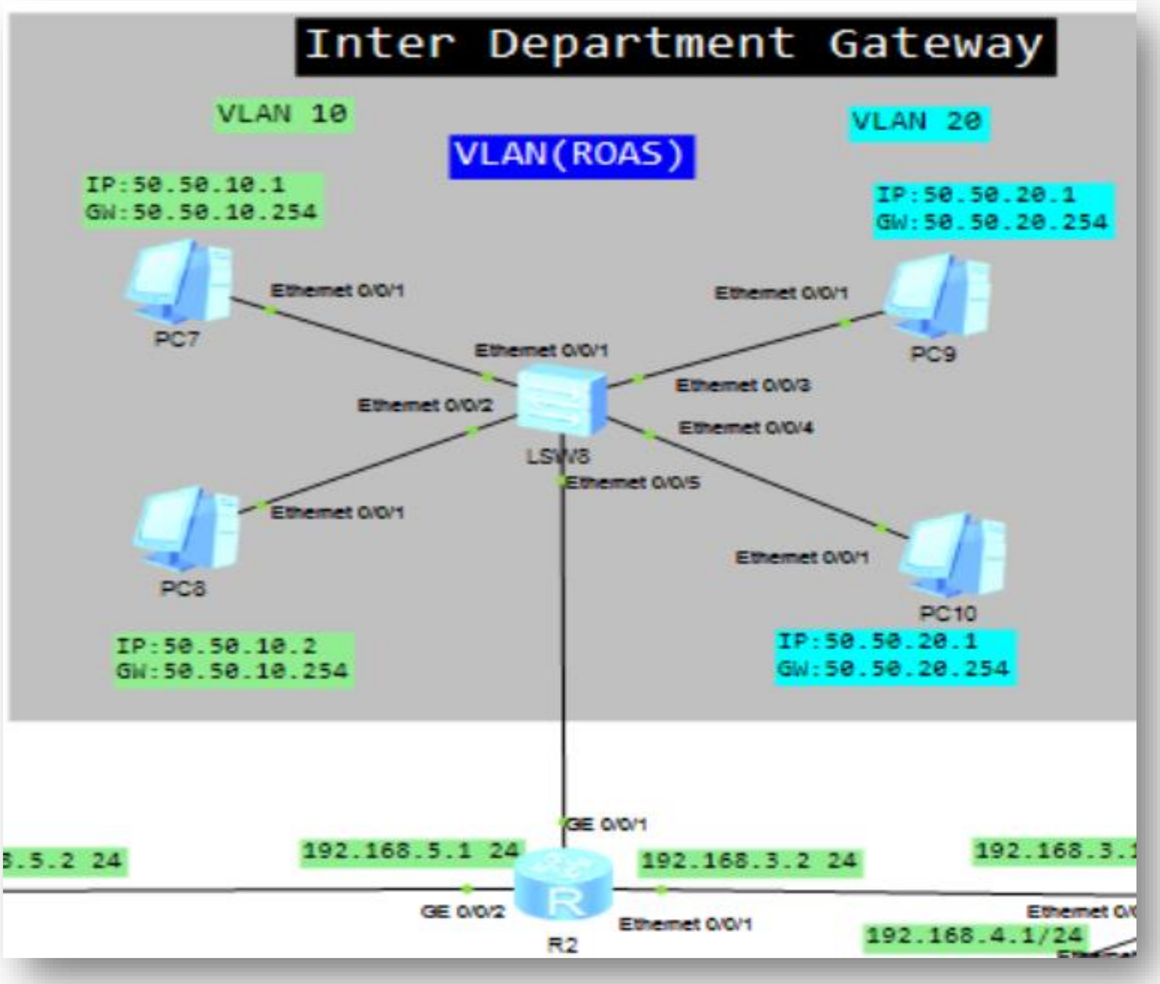
- **VLANs with ROAS (Router-on-a-Stick)**
  VLANs (Virtual Local Area Networks) are used to logically separate different departments or service groups within the network. A single router interface is configured with multiple sub-interfaces, each corresponding to a VLAN, enabling **inter-VLAN routing**. This is known as Router-on-a-Stick (ROAS). It helps reduce broadcast traffic, enforces policy-based routing, and maintains scalability.

- **DHCP (Dynamic Host Configuration Protocol)**
  DHCP is configured on one or more routers to **dynamically assign IP addresses** to client PCs within each VLAN or subnet. It reduces the need for manual IP configuration and ensures consistency. Each VLAN or subnet has its own DHCP pool, including settings for default gateway, DNS, and lease time.

- **FTP (File Transfer Protocol)**
  An FTP server is included in the topology to **simulate file-sharing and backup operations**. Routers and switches can upload/download configuration files to/from the server. This also helps demonstrate how FTP access can be controlled through ACLs and secured using login credentials. The FTP client (PC or router) tests connectivity and successful file transfer to validate network functionality.

6. CONFIGURATION & JUSTIFICATION ON SUBSYSTEMS

6.1 Inter Department Gateway (ROAS)



CONFIGURATION ON R2:

```
<R2>display saved-configuration
#
sysname R2
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher ;j.vTe-U0H939O4.`(ZGD>'#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
 ip address 192.168.3.2 255.255.255.0
```

```
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/1.10
 dot1q termination vid 10
 ip address 50.50.10.254 255.255.255.0
 arp broadcast enable
#
interface GigabitEthernet0/0/1.20
 dot1q termination vid 20
 ip address 50.50.20.254 255.255.255.0
 arp broadcast enable
#
interface GigabitEthernet0/0/2
 ip address 192.168.5.1 255.255.255.0
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
rip 1
 version 2
 network 192.168.3.0
 network 192.168.5.0
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

CONFIGURATION ON LSW8:

```
<LSW8>display saved-configuration
#
sysname LSW8
#
vlan batch 10 20
#
cluster enable
ntdp enable
```

```
ndp enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
interface Vlanif1
#
interface MEth0/0/1
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 10
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 10
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 20
#
interface Ethernet0/0/4
 port link-type access
 port default vlan 20
#
interface Ethernet0/0/5
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
```

JUSTIFICATION:

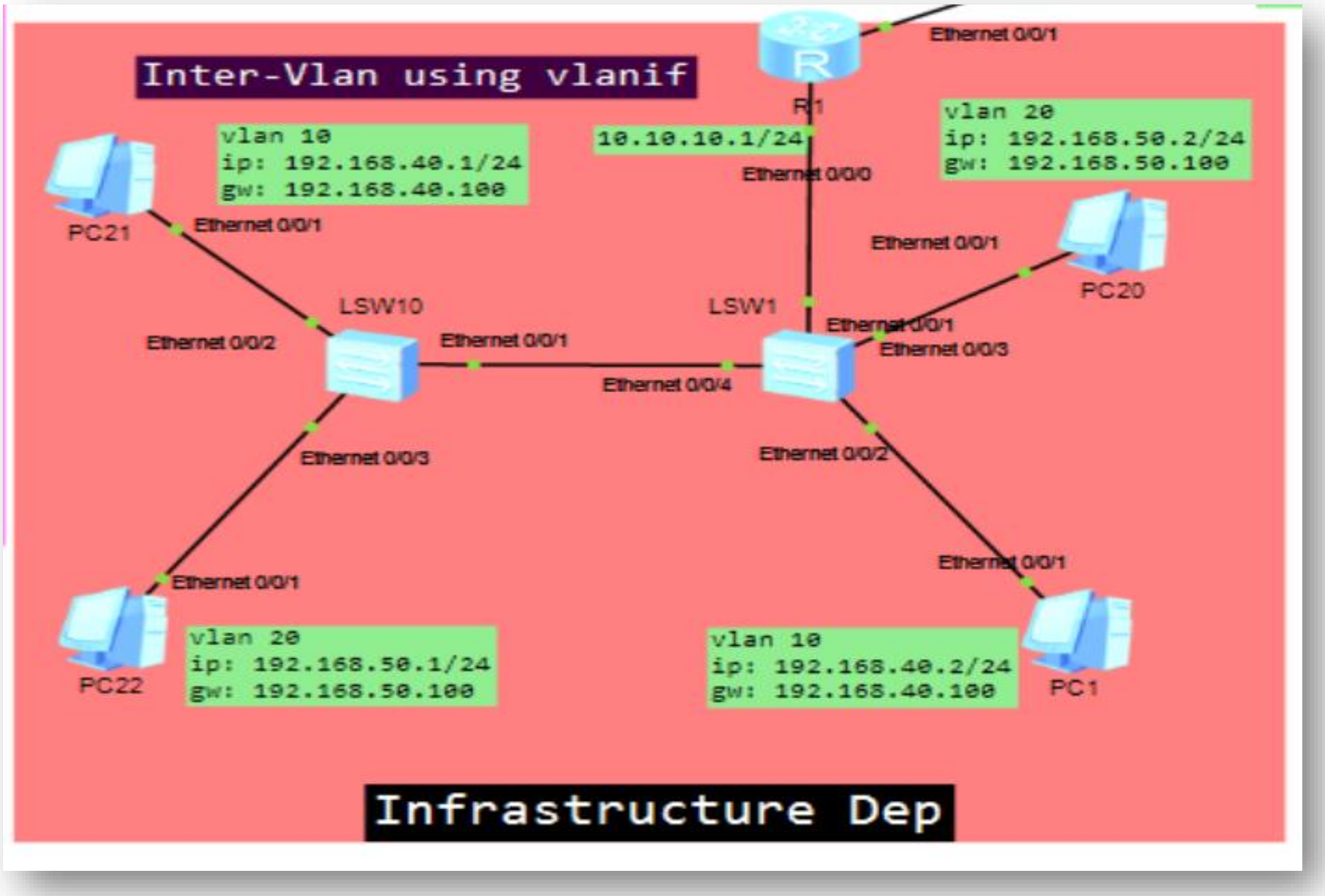
R2:

- The router hostname was set to R2 for identification.
- The Ethernet0/0/1 interface was assigned the IP address 192.168.3.2 with a /24 subnet mask.
- Subinterfaces GigabitEthernet0/0/1.10 and .20 were created for VLAN routing using dot1q encapsulation.
- IP addresses were assigned to the subinterfaces for inter-VLAN routing (ROAS).
- ARP broadcast was enabled on both subinterfaces to allow IP-to-MAC resolution in VLANs.
- RIP version 2 was configured for dynamic routing on networks 192.168.3.0 and 192.168.5.0.

LSW8:

- The switch hostname was set to LSW8 for easy identification.
- VLANs 10 and 20 were created to segment the network.
- Ethernet0/0/1 and Ethernet0/0/2 were configured as access ports for VLAN 10.
- Ethernet0/0/3 and Ethernet0/0/4 were configured as access ports for VLAN 20.
- Ethernet0/0/5 was set as a trunk port allowing VLANs 10 and 20 to pass through for inter-VLAN communication.

6.2 Infrastructure Department (Inter-Vlan using Vlanif)



CONFIGURATION:

LSW10:

```
#
vlan batch 10 20
#
cluster enable
ntdp enable
ndp enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
```

```
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
interface Vlanif1
#
interface Vlanif10
 ip address 192.168.40.100 255.255.255.0
#
interface Vlanif20
 ip address 192.168.50.100 255.255.255.0
#
interface MEth0/0/1
#
interface Ethernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 10
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 20
#
```

LSW1:

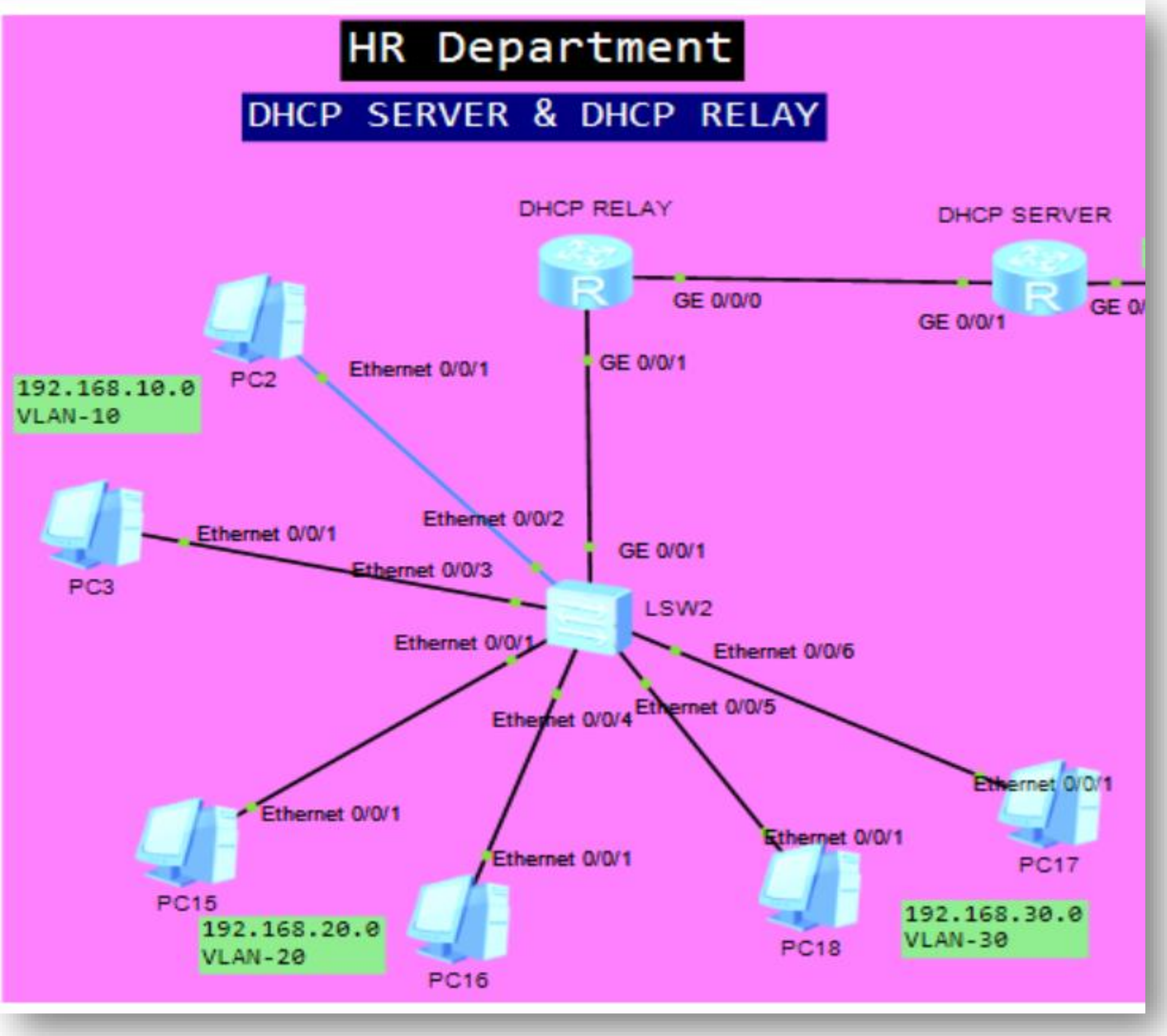
```
#
vlan batch 10 20
#
cluster enable
ntdp enable
ndp enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
```

```
#
interface Vlanif1
#
interface Vlanif10
 ip address 192.168.40.100 255.255.255.0
#
interface Vlanif20
 ip address 192.168.50.100 255.255.255.0
#
interface MEth0/0/1
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 10
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 20
#
interface Ethernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
```

JUSTIFICATION:

- **Use of VLAN 10 and VLAN 20**
  VLAN 10 (192.168.40.0/24) and VLAN 20 (192.168.50.0/24) are used to segment the network for security, traffic isolation, and broadcast control.
- PCs like **PC1 and PC21** are in **VLAN 10** with gateway 192.168.40.100.
- PCs like **PC20 and PC22** are in **VLAN 20** with gateway 192.168.50.100.
- All PCs have been assigned their VLAN-specific **default gateway IP**, which matches the IP of the corresponding **VLANIF interfaces** on both of the switches, allowing for inter-VLAN communication.
- This enables **Inter-VLAN routing**.
- **Switch Access Port Configurations:** Access ports like Ethernet 0/0/1 on LSW10 and LSW1 are set to VLAN 10 or 20 based on which PC they connect to.
- This ensures **correct VLAN tagging** for end device traffic.
- **Trunk Link Between LSW1 and LSW10**
  Port Ethernet 0/0/4 is a **trunk port** between LSW1 and LSW10, allowing **multiple VLANs (10 and 20)** to pass between switches.

6.3 HR Department (DHCP Server and Relay)



CONFIGURATION:

DHCP Server:

```
<DHCP-SERVER>display saved-configuration
#
sysname DHCP-SERVER
#
dhcp enable
#
ip pool LAN-10
 gateway-list 192.168.10.1
 network 192.168.10.0 mask 255.255.255.0
 dns-list 8.8.8.8
#
ip pool LAN-20
 gateway-list 192.168.20.1
 network 192.168.20.0 mask 255.255.255.0
 dns-list 8.8.8.8
#
ip pool LAN-30
 gateway-list 192.168.30.1
 network 192.168.30.0 mask 255.255.255.0
 dns-list 8.8.8.8
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher "I.HG>~xuEjKUGU-KkpB6>o#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 192.168.5.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 1.1.1.2 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
rip 1
 version 2
 network 192.168.5.0
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.1
#
user-interface con 0
```

```
user-interface vty 0 4
user-interface vty 16 20
#
return
```

DHCP Relay:

```
<DHCP-RELAY>display saved-configuration
#
sysname DHCP-RELAY
#
dhcp enable
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher OOCM4m($F4ajUn1vMEIBNUw#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/1.10
 dot1q termination vid 10
 ip address 192.168.10.1 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 1.1.1.2
#
interface GigabitEthernet0/0/1.20
 dot1q termination vid 20
 ip address 192.168.20.1 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 1.1.1.2
#
interface GigabitEthernet0/0/1.30
 dot1q termination vid 30
 ip address 192.168.30.1 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 1.1.1.2
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

LSW2:

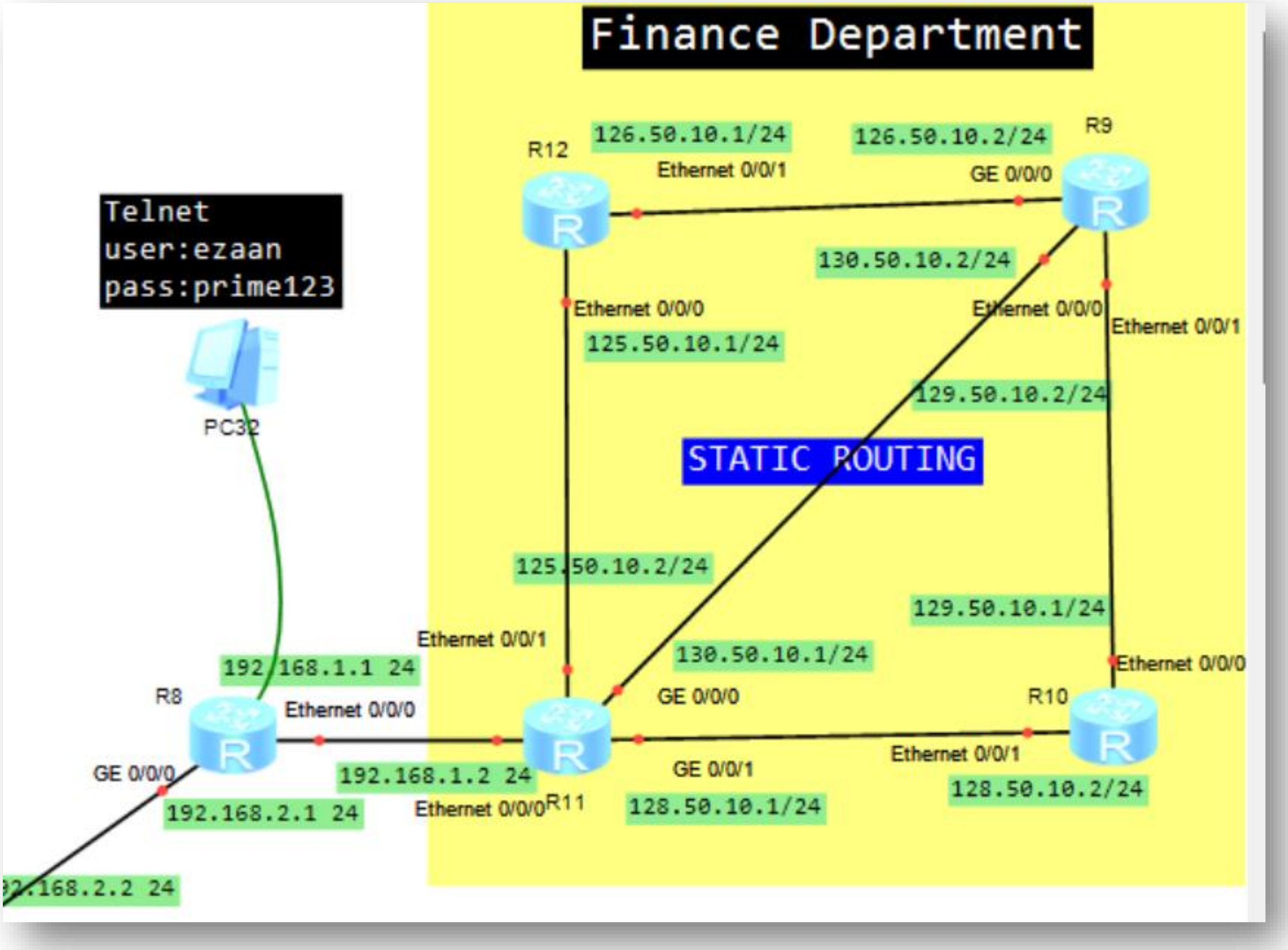
```
sysname LSW2
#
vlan batch 10 20 30
#
cluster enable
ntdp enable
ndp enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
interface Vlanif1
#
interface MEth0/0/1
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 20
#
```

```
interface Ethernet0/0/2
 port link-type access
 port default vlan 10
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 10
#
interface Ethernet0/0/4
 port link-type access
 port default vlan 20
#
interface Ethernet0/0/5
 port link-type access
 port default vlan 30
#
interface Ethernet0/0/6
 port link-type access
 port default vlan 30
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20 30
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
user-interface con 0
user-interface vty 0 4
#
return
```

JUSTIFICATION:

- **Centralized DHCP Management:** The presence of a dedicated "DHCP SERVER" simplifies IP address management. Instead of manually configuring IP addresses on each PC, the server dynamically assigns them, reducing administrative overhead and the risk of IP address conflicts.
- **Network Segmentation with VLANs:** The use of VLANs (VLAN-10, VLAN-20, VLAN-30) logically divides the network into separate broadcast domains. This enhances security by isolating traffic between different departments or user groups. For instance, traffic in VLAN-10 (192.168.10.0) is isolated from traffic in VLAN-20 (192.168.20.0) and VLAN-30 (192.168.30.0).
- **DHCP Relay for Inter-VLAN DHCP:** Since the DHCP server is likely on a different VLAN than some of the PCs (e.g., PC2 in VLAN-10, PCs 15 & 16 in VLAN-20, PCs 17 & 18 in VLAN-30), a "DHCP RELAY" is necessary. The DHCP relay agent receives DHCP requests from clients in different VLANs and forwards them to the DHCP server. The server then sends the DHCP responses back to the relay agent, which in turn forwards them to the requesting clients. This allows a single DHCP server to serve multiple VLANs.
- **Layer-2 Switching (LSW2):** The Layer-2 switch (LSW2) provides connectivity for multiple devices within the same VLAN. It forwards traffic based on MAC addresses, allowing efficient communication between PCs within VLAN-10, VLAN-20, and VLAN-30.

6.4 Finance Department (Telnet & Static Routing)



CONFIGURATION:

R8:

```
sysname R8
#
undo nap slave enable
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher I@qZ>s3UmQ+/Y@:Y>Lw(D=c#
 local-user admin service-type http
 local-user ezaan password cipher cero<ZqY\F:z9:%F`[a=pMR#
 local-user ezaan privilege level 3
 local-user ezaan service-type terminal
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/0
 ip address 192.168.2.1 255.255.255.0
#
wlan
#
interface NULL0
#
rip 1
 version 2
 network 192.168.1.0
 network 192.168.2.0
#
user-interface con 0
user-interface vty 0 4
 set authentication password cipher *Z5"7k-^)Y;BH^68NhwOWX-#
user-interface vty 16 20
#
return
```

R9:

```
interface Ethernet0/0/0
 ip address 130.50.10.2 255.255.255.0
#
interface Ethernet0/0/1
 ip address 129.50.10.2 255.255.255.0
#
interface GigabitEthernet0/0/0
 ip address 126.50.10.2 255.255.255.0
#
wlan
#
interface NULL0
#
ip route-static 125.50.10.0 255.255.255.0 126.50.10.1
ip route-static 125.50.10.0 255.255.255.0 130.50.10.1
ip route-static 128.50.10.0 255.255.255.0 129.50.10.1
ip route-static 128.50.10.0 255.255.255.0 130.50.10.1
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

R10:

```
interface Ethernet0/0/0
 ip address 129.50.10.1 255.255.255.0
#
interface Ethernet0/0/1
 ip address 128.50.10.2 255.255.255.0
```

```
#
wlan
#
interface NULL0
#
ip route-static 125.50.10.0 255.255.255.0 128.50.10.1
ip route-static 126.50.10.0 255.255.255.0 129.50.10.2
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

R11:

```
interface Ethernet0/0/0
 ip address 192.168.1.2 255.255.255.0
#
interface Ethernet0/0/1
 ip address 125.50.10.2 255.255.255.0
#
interface GigabitEthernet0/0/0
 ip address 130.50.10.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 128.50.10.1 255.255.255.0
#
wlan
#
interface NULL0
#
rip 1
 version 2
 network 192.168.1.0
#
ip route-static 126.50.10.0 255.255.255.0 125.50.10.1
ip route-static 126.50.10.0 255.255.255.0 130.50.10.2
ip route-static 129.50.10.0 255.255.255.0 128.50.10.2
ip route-static 129.50.10.0 255.255.255.0 130.50.10.2
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

R12:

```
interface Ethernet0/0/0
 ip address 125.50.10.1 255.255.255.0
#
interface Ethernet0/0/1
 ip address 126.50.10.1 255.255.255.0
#
wlan
#
```

```
interface NULL0
#
ip route-static 128.50.10.0 255.255.255.0 125.50.10.2
ip route-static 129.50.10.0 255.255.255.0 126.50.10.2
ip route-static 130.50.10.0 255.255.255.0 126.50.10.2
ip route-static 130.50.10.0 255.255.255.0 125.50.10.2
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

JUSTIFICATION:

- **Static Routing:** The explicit label "STATIC ROUTING" indicates that the routing tables on the routers (R9, R10, R11, R12) are manually configured. This approach is suitable for smaller, relatively stable networks where the network topology doesn't change frequently. It offers more control over routing paths.

- **Inter-Router Connectivity:** The routers are interconnected via various Ethernet interfaces and IP subnets. This allows network traffic to be forwarded between different parts of the "Finance Department" network. The specific IP addresses and subnet masks (e.g., 126.50.10.1/24, 130.50.10.2/24) define the network segments and the interfaces used for communication.

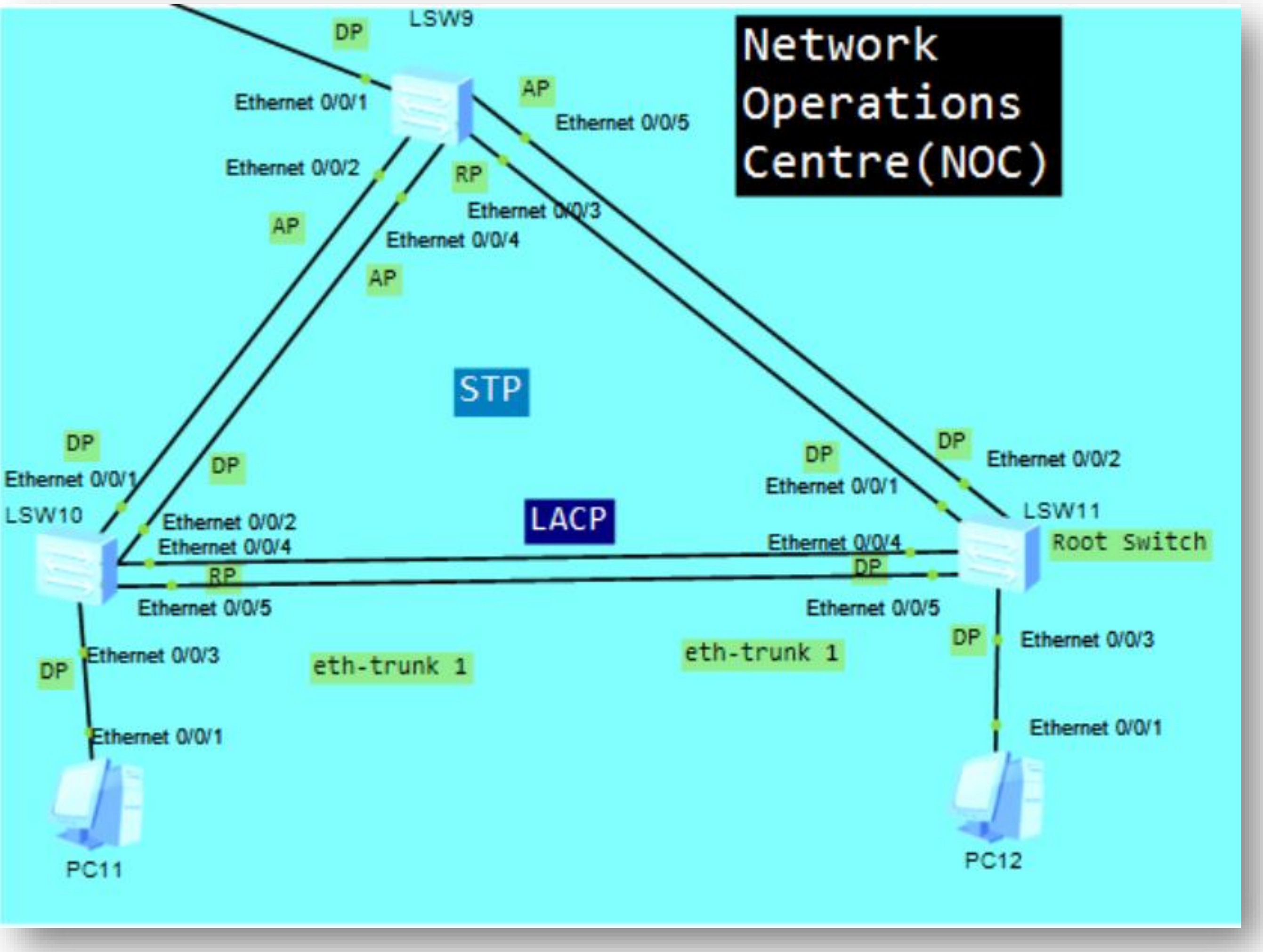
- **Multiple Paths for Redundancy (Potential):** Although configured for static routing, the topology shows multiple potential paths between some routers (e.g., between R9 and R11). While static routing dictates a specific path, the physical links could offer a degree of redundancy if the static routes were configured to take advantage of them in case of a link failure.

- **Network Segmentation:** The use of different IP subnets (e.g., 126.50.10.0/24, 130.50.10.0/24, 125.50.10.0/24, 129.50.10.0/24, 128.50.10.0/24) suggests network segmentation. This can be done for organizational purposes, security, or to manage broadcast domains. Different teams or functions within the finance department could potentially be on different subnets.

- **Connectivity to a Local Network (R8 and PC32):** Router R8 connects to a local network segment (192.168.1.0/24 and 192.168.2.0/24) where PC32 resides. This indicates that PC32 is part of a separate local area network that needs to communicate with the "Finance Department" network.

- **Telnet Access (PC32):** The "Telnet user: ezaan pass: prime123" information near PC32 suggests that remote access to a network device (likely R8 or another router) is configured using Telnet. This allows administrators to manage network devices from PC32.

6.5 Network Operations Centre (STP & LACP)



CONFIGURATION:

LSW10:

```
sysname LSW10
#
cluster enable
ntdp enable
ndp enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
interface Vlanif1
#
interface MEth0/0/1
#
interface Eth-Trunk1
 mode lacp-static
#
interface Ethernet0/0/4
 eth-trunk 1
#
interface Ethernet0/0/5
 eth-trunk 1
#
user-interface con 0
user-interface vty 0 4
#
return
```

LSW11:

```
sysname LSW11
#
cluster enable
ntdp enable
ndp enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
interface Vlanif1
#
interface MEth0/0/1
#
interface Eth-Trunk1
 mode lacp-static
#
interface Ethernet0/0/4
 eth-trunk 1
#
interface Ethernet0/0/5
```

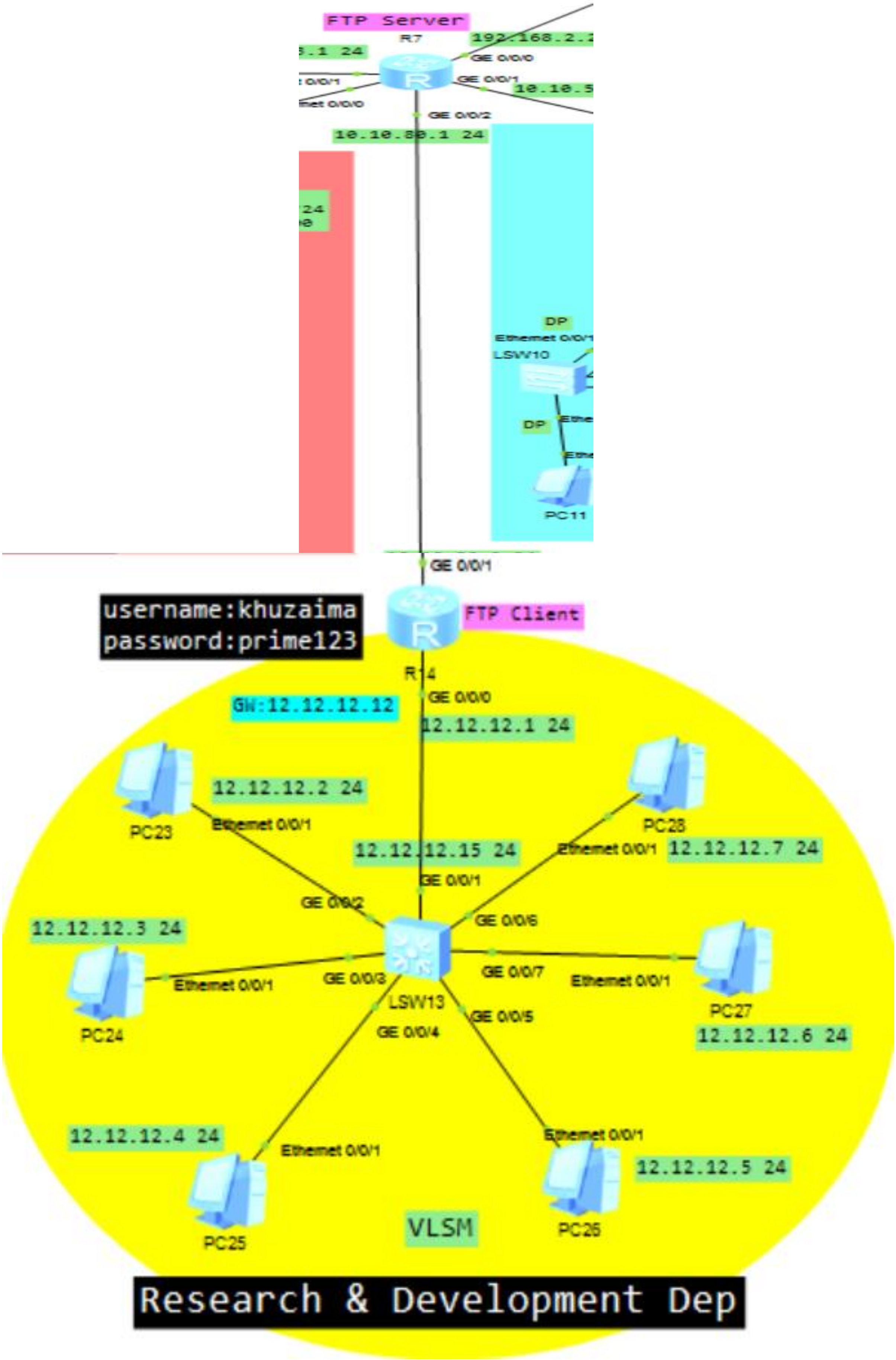
```
 eth-trunk 1
#
interface NULL0
#
user-interface con 0
user-interface vty 0 4
#
return
```

JUSTIFICATION:

- **Redundancy and High Availability with STP:** The presence of the Spanning Tree Protocol (STP) indicates a design focused on preventing Layer-2 loops within the network. This is crucial for maintaining network stability and preventing broadcast storms, especially in a topology with multiple interconnected switches. STP ensures that only one active path exists between any two broadcast domains, while still providing redundant paths that can become active if the primary path fails. This enhances the overall availability of the NOC network.

- **Increased Bandwidth and Resilience with LACP (Etherchannel):** The configuration of "eth-trunk 1" utilizing Link Aggregation Control Protocol (LACP) between LSW10 and LSW11 is a key design element for increasing bandwidth capacity and link resilience. By bundling multiple physical Ethernet links into a single logical link, you've effectively multiplied the available bandwidth between these critical switches. Furthermore, LACP provides link redundancy; if one or more physical links within the EtherChannel fail, traffic can continue to flow over the remaining active links, ensuring connectivity.

6.6 Research & Development Department (FTP)



CONFIGURATION:

FTP SERVER:

```
#
FTP server enable
set default ftp-directory flash/
#
undo info-center enable
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher iaBOGI,N$53IF$':[285"=I#
 local-user admin privilege level 3
 local-user admin service-type ftp
 local-user khuzaima password cipher ctJB$3$m\V3IF$':[285"=I#
 local-user khuzaima privilege level 3
 local-user khuzaima service-type ftp
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 192.168.4.1 255.255.255.0
#
interface Ethernet0/0/1
 ip address 192.168.3.1 255.255.255.0
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 10.10.50.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.10.80.1 255.255.255.0
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
rip 1
 version 2
 network 10.0.0.0
 network 192.168.2.0
 network 192.168.3.0
 network 192.168.4.0
#
user-interface con 0
user-interface vty 0 4
 user privilege level 3
 set authentication password cipher f$SBG9._k<pe}@HMNPn@=DV#
user-interface vty 16 20
#
return
```

FTP CLIENT:

```
sysname R14
#
undo info-center enable
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher vKw%T{>b<2ajUn1vMEIB4=P#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 12.12.12.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 10.10.80.2 255.255.255.0
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
rip 1
 version 2
 network 10.0.0.0
 network 12.0.0.0
#
user-interface con 0
user-interface vty 0 4
 user privilege level 3
 set authentication password cipher &H^,.5s*+5pe}@HMNPn@_Hf#
user-interface vty 16 20
#
return
```

JUSTIFICATION:

- **Routed Network Infrastructure:** The configuration establishes a routed network where Router R14 acts as the **gateway** for the R&D department's **local area network (LAN)** segment (12.12.12.0/24). It facilitates **inter-network routing** using the **RIP routing protocol** to communicate with other network segments.

- **Dynamic Routing with RIP:** The use of **RIP version 2** enables both R14 and the FTP server to dynamically exchange **routing information**, allowing them to learn and adapt to network topology changes. This ensures reachability between the R&D network and the network where the FTP server resides.

- **Separate Network Segments:** The R&D department's PCs are on the `12.12.12.0/24` **subnet**, while the FTP server primarily resides on the `192.168.2.0/24` **subnet**. This necessitates **Layer-3 routing** for communication between these segments, which is handled by R14 and the FTP server via RIP.

- **FTP Service Provision:** The FTP server is explicitly configured to provide **File Transfer Protocol (FTP)** services. It defines local users (`admin`, `khuzaima`) with specific **privilege levels** and restricts their **service type** to FTP for controlled access. A **default FTP directory** is set.

- **Potential Direct Interconnection:** The configuration of interfaces on both R14 and the FTP server within the `10.10.80.0/24` subnet suggests a potential direct Layer-2 connection or a shared segment. This could offer a more direct communication path between the R&D network's router and the FTP server.

- **Basic Security Measures:** Both devices implement basic security through **local user authentication** with **ciphertext passwords** for management and FTP access.

- **Remote Management Capabilities:** Both R14 and the FTP server are configured for **remote management** via **Virtual Terminal (VTY) lines**, secured with password authentication.

7. CONCLUSION

This project demonstrates the implementation of a complex and well-structured enterprise network topology by integrating various network technologies and protocols across multiple departments. Each department's unique networking requirements were addressed through specific configurations, ensuring both functionality and scalability.

The **Inter Department Gateway** was configured using **Router-on-a-Stick (ROAS)** to enable inter-VLAN communication. The **Infrastructure Department** utilized **VLANIF** for efficient inter-VLAN routing within switches, while the **HR Department** was dynamically managed using a **DHCP Server and DHCP Relay** configuration to automate IP addressing.

In the **Finance Department**, **Static Routing** ensured deterministic path selection and simplified troubleshooting, while **Telnet access** facilitated remote management. The **Network Operations Centre (NOC)** leveraged **Spanning Tree Protocol (STP)** to eliminate switching loops and **Link Aggregation Control Protocol (LACP)** to increase bandwidth and provide redundancy. The **Research & Development Department** implemented an **FTP server** for secure file transfer operations and utilized **VLSM** to optimize IP address allocation.

To support communication between most routers and departments, **RIP (Routing Information Protocol)** was deployed, enabling dynamic routing updates and simplifying route management across the network.

This topology showcases how combining static and dynamic routing protocols with advanced switching technologies can build a resilient, secure, and high-performance enterprise network. The modular design also supports future scalability, making it a robust foundation for expanding business needs.