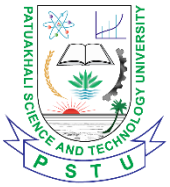
Faculty of Computer Science & Engineering

Project Report on

Hospital System Network Design using Packet-Tracer



Course Code: CCE 416

Course Title: Network Routing and Switching Sessional

Submitted by

Md. Imdud Ul Haque
ID: 1802017
Reg: 08427
Level – 4 Semester – 1
Session: 2018-19

Submitted to

Dr. Md. Samsuzzaman
Professor
Department of Computer and Communication Engineering
Patuakhali Science and Technology University

Date of Submission: 01 Feb 2024

Table of Contents

Abstract:

This project report presents the objectives, design, implementation, and outcomes of the Network Routing and Switching project using Cisco Packet Tracer. The project's focus is on developing a robust network infrastructure for Melbourne Health Services is a well-established health provider in Australia, which offers health solutions and services to its clients. Through the utilization of advanced networking technologies, the report provides a comprehensive overview of the entire project lifecycle.

The objectives of the project is to design the network according to the requirements set by the senior management. It should be consulted an appropriate robust network design model to meet the design requirements. It should also be implemented Access Control Lists and Virtual Private Network (VPN) to enable secure communication considering security and network performance factors paramount to safeguarding Confidentiality, Integrity, and Availability of data and communication. The network security policy will comprehensively dictate the user's access to each site using Access Control List (ACL).

The IP addressing scheme is based on a base network of 192.168.100.0, with subnetting used to allocate the correct number of IP addresses to each department. Public IP addresses (195.136.17.0/30, 195.136.17.4/30, 195.136.17.8/30, and 195.136.17.12/30) are assigned for internet connectivity. Basic device settings, inter-VLAN routing on multilayer switches, DHCP server configurations, and the use of OSPF as the routing protocol are integral components of the implemented network.

Furthermore, security measures are implemented through Access Control Lists (ACLs) and port security, ensuring a secure and controlled network environment. Quality of Service (QoS) configurations are also introduced to manage and prioritize network traffic effectively.

1. Introduction:

1.1 Background:

In the dynamic landscape of modern computer networks, network routing and switching play pivotal roles in facilitating efficient and reliable communication. These fundamental components are the backbone of any interconnected system, ensuring seamless data transmission and connectivity.

Significance of Network Routing and Switching:

- Efficient Data Transmission: Routing optimizes the path that data takes from its source to its destination. By dynamically selecting the most efficient route, it minimizes latency and maximizes bandwidth utilization, enhancing the overall speed and efficiency of data transmission.

- Scalability: As networks grow in size and complexity, efficient routing and switching technologies allow for seamless expansion. Properly configured routers and switches enable networks to scale without compromising performance.

- Reliability: Routing protocols, such as OSPF and EIGRP, contribute to network reliability by providing redundancy and failover mechanisms. In the event of a network link failure, routers can reroute traffic through alternative paths, ensuring continuous connectivity.

- Segmentation and Security: Switching, particularly through Virtual LANs (VLANs), allows for the logical segmentation of a network. This not only enhances security by isolating traffic but also facilitates efficient network management. VLANs prevent unauthorized access and limit the scope of potential security breaches.

- Adaptability to Changes: Modern networks are dynamic, with frequent changes in topology. Effective routing protocols adapt to these changes, automatically adjusting to provide optimal paths for data transmission. This adaptability is crucial for maintaining network performance.

1.2 Objectives:

The objectives of the Packet Tracer project are outlined as follows:

- Design a Logical Network Infrastructure: Create a network design using Cisco Packet Tracer that meets the current business needs of the trading floor support centre and is scalable for future requirements.
- Implement Redundancy Measures: Utilize a hierarchal model in the network design, incorporating redundancy at every layer. This includes the use of two routers and two multilayer switches to ensure high availability.
- Establish Connectivity with Redundant ISPs: Connect the network to at least two Internet Service Providers (ISPs) to provide redundancy and minimize the risk of connectivity issues.
- Configure Wireless Networks: Implement wireless networks for each department to enable seamless connectivity for users.
- Utilize VLANs and Subnetting: Assign each department to a different VLAN and subnet using the provided base network (172.16.1.0) with proper subnetting to manage IP address allocation efficiently.
- Configure Basic Device Settings: Set up essential configurations for routers and switches, including hostnames, passwords, banner messages, and the disabling of IP domain lookup.
- Enable Inter-VLAN Routing: Configure multilayer switches for inter-VLAN routing to facilitate communication between different departments.
- Implement OSPF Routing Protocol: Utilize OSPF as the routing protocol to advertise routes both on routers and multilayer switches, ensuring dynamic and efficient routing.
- Secure Network Devices: Implement security measures such as SSH configuration for remote login, port-security for specific departments, and ACLs for overall network security.
- Configure DHCP Servers: Set up dedicated DHCP servers in the server room for dynamic IP address allocation to devices across the network.
- Test and Verify Network Communication: Thoroughly test the configured network to ensure all components function as expected and verify seamless communication between devices.

2. Network Design:

2.1 Topology:

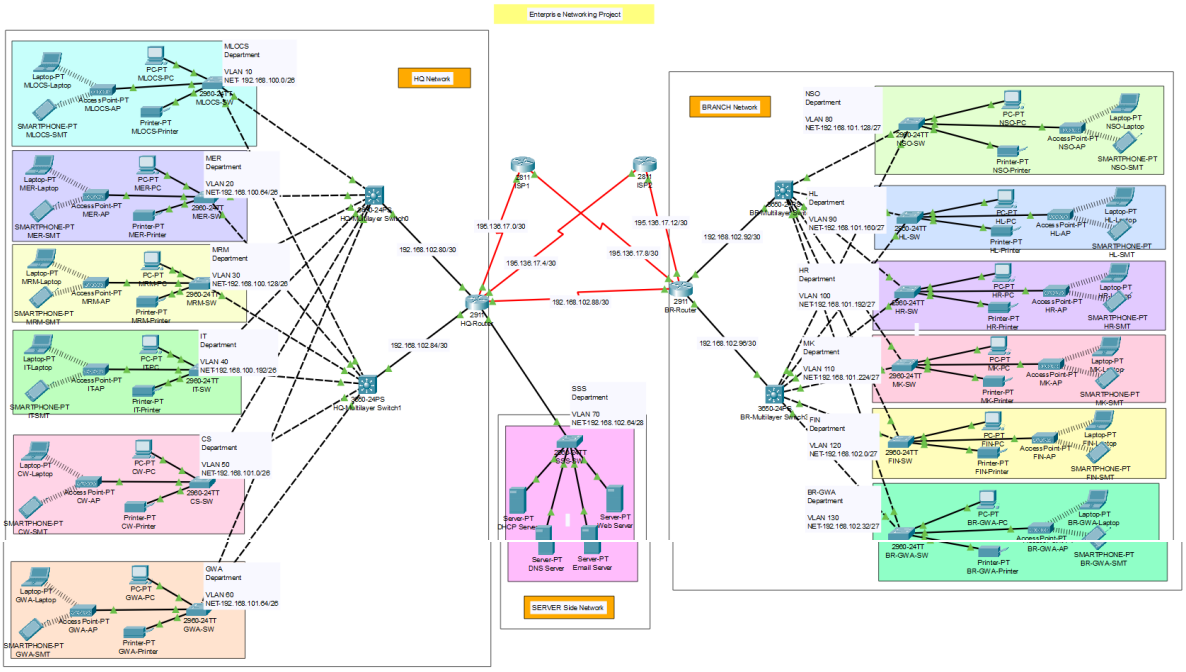


Fig: Network Topology

2.2 Components:

The network design for the trading floor support centre incorporates various devices to create a comprehensive and functional infrastructure. Each device serves a specific purpose in ensuring connectivity, security, and efficient data transmission. The following is a list of devices used in the network:

Routers:

- Description: Routers are essential devices responsible for directing data traffic between different networks. They operate at the network layer (Layer 3) of the OSI model and facilitate interconnectivity between the trading floor support centre's internal network and external networks, including the internet.

- Role in the Network: Routers provide the necessary intelligence for routing data packets to their destinations, ensuring that information reaches its intended recipients efficiently.

Switches:

- Description: Switches operate at the data link layer (Layer 2) of the OSI model and are crucial for creating a high-speed, efficient, and secure local network within each floor and department of the trading floor support centre.
- Role in the Network: Switches forward data frames based on MAC addresses, reducing network congestion and enabling devices within the same VLAN to communicate seamlessly.

Multilayer Switches:

- Description: Multilayer switches combine the functionality of traditional switches with routing capabilities, operating at both Layer 2 and Layer 3 of the OSI model. They are instrumental in facilitating inter-VLAN routing within the network.
- Role in the Network: Multilayer switches perform routing functions between different VLANs, enhancing communication between departments while maintaining the benefits of local switching.

PCs (Personal Computers):

- Description: PCs represent end-user devices connected to the network, such as desktop computers and laptops. They are essential for the daily operations of staff in each department.
- Role in the Network: PCs send and receive data over the network, accessing resources, and contributing to the overall productivity of the trading floor support centre.

Servers:

- Description: Servers are dedicated devices that provide specific services to the network, such as hosting applications, storing data, or managing network resources.
- Role in the Network: Servers in the trading floor support centre may include DHCP servers for dynamic IP address allocation, ensuring seamless connectivity, and maintaining network services.

Access Points (Wireless):

- Description: Access points enable the establishment of wireless networks, providing wireless connectivity to devices within each department.
- Role in the Network: Access points support the implementation of wireless networks, ensuring flexibility and mobility for users in various departments.

DHCP Servers:

- Description: DHCP servers automate the process of assigning IP addresses to devices within the network dynamically.
- Role in the Network: DHCP servers streamline the IP address allocation process, reducing manual configuration efforts and ensuring efficient network management.

ISP Routers:

- Description: Internet Service Provider (ISP) routers connect the trading floor support centre to external networks and the internet.
- Role in the Network: ISP routers facilitate internet connectivity, providing the trading floor support centre with access to online resources and services.

2.3 IP Addressing Scheme

Provide details about the IP addressing scheme applied to the network.

HQ Hospital

Department	Network Address	Subnet Mask	Host Address Range	Broadcast Address
MLOCS	192.168.100.0	255.255.255.192/26	192.168.100.1 to 192.168.100.62	192.168.100.63
MER	192.168.100.64	255.255.255.192/26	192.168.100.64 to 192.168.100.126	192.168.100.127
MRM	192.168.100.128	255.255.255.192/26	192.168.100.129 to 192.168.100.190	192.168.100.191
IT	192.168.100.192	255.255.255.192/26	192.168.100.193 to 192.168.100.254	192.168.100.255
CS	192.168.101.0	255.255.255.192/26	192.168.101.1 to 192.168.101.62	192.168.101.63
GWA	192.168.101.64	255.255.255.192/26	192.168.101.64 to 192.168.101.126	192.168.101.127

Branch Hospital

Department	Network Address	Subnet Mask	Host Address Range	Last Address
NSO	192.168.101.128	255.255.255.224/27	192.168.101.129 to 192.168.101.158	192.168.101.159
HL	192.168.101.160	255.255.255.224/27	192.168.101.161 to 192.168.101.190	192.168.101.191
HR	192.168.101.192	255.255.255.224/27	192.168.101.193 to 192.168.101.222	192.168.101.223
MK	192.168.101.224	255.255.255.224/27	192.168.101.225 to 192.168.101.254	192.168.101.255
FIN	192.168.102.0	255.255.255.224/27	192.168.102.1 to 192.168.102.30	192.168.102.31
BR-GWA	192.168.102.32	255.255.255.224/27	192.168.102.33 to 192.168.102.62	192.168.102.63

Server-Side Site

Department	Network Address	Subnet Mask	Host Address Range	Last Address
SSS	192.168.102.64	255.255.255.240/28	192.168.102.65 to 192.168.102.78	192.168.102.79

Between the Routers and Layer-3 Switches

No.	Network Address
HQR1-HQMLSW1	192.168.102.80/30
HQR1-HQMLSW2	192.168.102.84/30
BRR1-BRMLSW1	192.168.102.88/30
BRR1-BRMLSW1	192.168.102.92/30
HQR1-BRR1	192.168.102.96/30

3. Routing Configuration:

3.1 Router Configuration:

Basic Config for Both Core Router =

```
en
conf t

hostname HQ-Router (change for another CORE router)
line console 0
pass cisco
login
exit

enable password cisco
no ip domain-lookup
banner motd #Unautorized access!!!#

service password-encryption

do wr


ip domain-name cisco.net
username admin password cisco
crypto key generate rsa
1024
line vty 0 15
login local
transport input ssh
exit

ip ssh version 2

do wr
```

3.2 Static and Dynamic Routing:

For HQ-Router (OSPF) =

```
router ospf 10

network 192.168.102.80 0.0.0.3 area 0
```

```
network 192.168.102.84 0.0.0.3 area 0
network 192.168.102.88 0.0.0.3 area 0
network 192.168.102.64 0.0.0.15 area 0
network 195.136.17.4 0.0.0.3 area 0
network 195.136.17.0 0.0.0.3 area 0
exit

do wr
```

For BR-Router (OSPF) =

```
router ospf 10

network 192.168.102.92 0.0.0.3 area 0
network 192.168.102.96 0.0.0.3 area 0
network 192.168.102.88 0.0.0.3 area 0
network 195.136.17.8 0.0.0.3 area 0
network 195.136.17.12 0.0.0.3 area 0
exit

do wr
```

For ISP Routers-1 (OSPF) (for demo purpose) =

```
router ospf 10

network 195.136.17.8 0.0.0.3 area 0
network 195.136.17.0 0.0.0.3 area 0
exit

do wr
```

For ISP Routers-2 (OSPF) (for demo purpose) =

```
router ospf 10

network 195.136.17.4 0.0.0.3 area 0
network 195.136.17.12 0.0.0.3 area 0

exit

do wr
```

Nat Config for HQ-Router =

```
router rip
ip nat inside source list 1 interface Serial0/2/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 195.136.17.2
ip route 0.0.0.0 0.0.0.0 195.136.17.6 70

access-list 1 permit 192.168.100.0 0.0.0.63
access-list 1 permit 192.168.100.64 0.0.0.63
access-list 1 permit 192.168.100.128 0.0.0.63
access-list 1 permit 192.168.100.192 0.0.0.63
access-list 1 permit 192.168.101.0 0.0.0.63
access-list 1 permit 192.168.101.64 0.0.0.63

interface GigabitEthernet0/0
ip nat inside

interface GigabitEthernet0/1
ip nat inside

interface GigabitEthernet0/2
ip nat inside

interface Serial0/1/0
ip nat outside

interface Serial0/2/1
ip nat outside

exit

do wr
```

Nat Config for BR-Router:

```
ip nat inside source list 1 interface Serial0/2/1 overload

ip route 0.0.0.0 0.0.0.0 195.136.17.14
ip route 0.0.0.0 0.0.0.0 195.136.17.10 70

access-list 1 permit 192.168.101.128 0.0.0.31
access-list 1 permit 192.168.101.160 0.0.0.31
access-list 1 permit 192.168.101.192 0.0.0.31
access-list 1 permit 192.168.101.224 0.0.0.31
access-list 1 permit 192.168.102.0 0.0.0.31
access-list 1 permit 192.168.102.32 0.0.0.31

interface GigabitEthernet0/0
```

ip nat inside

interface GigabitEthernet0/1

ip nat inside

interface Serial0/1/0

ip nat outside

interface Serial0/2/1

ip nat outside

exit

do wr

Default Static Route for Both Core Router =

```
ip route 0.0.0.0 0.0.0.0 se0/2/0
ip route 0.0.0.0 0.0.0.0 se0/2/1 70

do wr
```

4. Switching Configuration:

4.1 Switch Configuration:

For All Access Layer Switch =

```
en
conf t

hostname MLOCS-SW ( change for remaining 5 switch)
line console 0
pass cisco
login
exit

enable password cisco
no ip domain-lookup
banner motd #Unautorized access!!!#

service password-encryption
```

```
do wr
```

For Multilayer Switch =

```
en
conf t

hostname HQ-MULTILAYER-SW0
line console 0
pass cisco
login
exit

enable password cisco
no ip domain-lookup
banner motd #Unautorized access!!!#

service password-encryption

ip domain-name cisco.net
username admin password cisco
crypto key generate rsa
1024
line vty 0 15
login local
transport input ssh
exit

ip ssh version 2

do wr
```

4.2 VLANs:

For Both Multilayer Switch =

```
int range gig1/0/2-7
switchport mode trunk

vlan 10
name MLOCS
vlan 20
```

```
name MER
vlan 30
name MRM
vlan 40
name IT
vlan 50
name CS
vlan 60
name GWA

exit
do wr
```

For All Access Layer Switch (Sales vlan-10, HR vlan-20, Finance vlan-30, Admin vlan-40, ICT vlan-50, Serve room vlan-60) =

```
int range fa0/1-2
switchport mode trunk
exit

vlan 60 (change this for remaining switch)
name Server(change this for remaining switch)
vlan 99
name BlackHole
exit

int range fa0/3-24
switchport mode access
switchport access vlan 60 (change this for remaining switch)
exit

int range gig0/1-2
switchport mode access
switchport access vlan 99
exit

do wr
```

Default Static Route for Both Multilayer Switch =

```
ip route 0.0.0.0 0.0.0.0 gig1/0/1
ip route 0.0.0.0 0.0.0.0 gig1/0/2 70

do wr
```

For Multilayer 1 Switch OSPF Config =

```
ip routing (for multilayer switch only)

router ospf 10

network 192.168.100.0 0.0.0.63 area 0
network 192.168.100.64 0.0.0.63 area 0
network 192.168.100.128 0.0.0.63 area 0
network 192.168.100.192 0.0.0.63 area 0
network 192.168.101.0 0.0.0.63 area 0
network 192.168.101.64 0.0.0.63 area 0
network 192.168.102.80 0.0.0.3 area 0
exit

do wr
```

For Multilayer 2 Switch OSPF Config =

```
ip routing (for multilayer switch only)

router ospf 10

network 192.168.101.128 0.0.0.31 area 0
network 192.168.101.160 0.0.0.31 area 0
network 192.168.101.192 0.0.0.31 area 0
network 192.168.101.224 0.0.0.31 area 0
network 192.168.102.0 0.0.0.31 area 0
network 192.168.102.32 0.0.0.31 area 0

exit

do wr
```

5. Inter-VLAN Routing:

5.1 Router-on-a-Stick:

For Both Multilayer Switch =

```
interface Vlan10
mac-address 0001.4272.7101
ip address 192.168.100.1 255.255.255.192
```

```
ip helper-address 192.168.102.67
!
interface Vlan20
mac-address 0001.4272.7102
ip address 192.168.100.65 255.255.255.192
ip helper-address 192.168.102.67
!
interface Vlan30
mac-address 0001.4272.7103
ip address 192.168.100.129 255.255.255.192
ip helper-address 192.168.102.67
!
interface Vlan40
mac-address 0001.4272.7104
ip address 192.168.100.193 255.255.255.192
ip helper-address 192.168.102.67
!
interface Vlan50
mac-address 0001.4272.7105
ip address 192.168.101.1 255.255.255.192
ip helper-address 192.168.102.67
!
interface Vlan60
mac-address 0001.4272.7106
ip address 192.168.101.65 255.255.255.192
ip helper-address 192.168.102.67
exit

do wr


interface Vlan80
mac-address 00d0.baac.9e01
ip address 192.168.101.129 255.255.255.224
ip helper-address 192.168.102.67
!
interface Vlan90
mac-address 00d0.baac.9e02
ip address 192.168.101.161 255.255.255.224
ip helper-address 192.168.102.67
!
interface Vlan100
mac-address 00d0.baac.9e03
ip address 192.168.101.193 255.255.255.224
ip helper-address 192.168.102.67
!
interface Vlan110
mac-address 00d0.baac.9e04
ip address 192.168.101.225 255.255.255.224
ip helper-address 192.168.102.67
```

```
!
interface Vlan120
mac-address 00d0.baac.9e05
ip address 192.168.102.1 255.255.255.224
ip helper-address 192.168.102.67
!
interface Vlan130
mac-address 00d0.baac.9e06
ip address 192.168.102.33 255.255.255.224
ip helper-address 192.168.102.67
!
```

5.2 Subnetting:

The new building is expected to have three floors with two departments in each for example;

1. **Headquarter Hospital-** (Sales and Marketing Department-120 users expected, Human Resource and Logistics Department-120 users expected).
2. **Branch Hospital-** (Finance and Accounts Department-120 users expected, Administrator and Public Relations Department-120 users expected).
3. **Server-Side-** (ICT-120 users expected, Server Room-12 devices expected).

Also Provided a base network of 192.168.100.0

So, After subnetting:

For Access Layer Switch =

MLOCS ---------- Vlan 10 ---------- Network Address = 192.168.100.0/26

MER ---------- Vlan 20 ---------- Network Address = 192.168.100.64/26

MBM ---------- Vlan 30 --------- Network Address = 192.168.100.128/26

CS ---------- Vlan 40 --------- Network Address = 192.168.100.192/26

ICT ---------- Vlan 50 --------- Network Address = 192.168.101.0/26

GWA ---------- Vlan 60 --------- Network Address =192.168.101.64/26

For Core Router to Multilayer Switch =

Core-R1 to Multilayer-1 ---------- Network Address = 140.16.3.144/30

Core-R2 to Multilayer-1 ---------- Network Address = 140.16.3.148/30

Core-R1 to Multilayer-2 ---------- Network Address = 140.16.3.152/30

Core-R2 to Multilayer-2 ---------- Network Address = 140.16.3.156/30

6. Security Measures:

6.1 Access Control Lists (ACLs):

For Both Core Router =

access-list 1 permit 192.168.100.0 0.0.0.63
access-list 1 permit 192.168.100.64 0.0.0.63
access-list 1 permit 192.168.100.128 0.0.0.63
access-list 1 permit 192.168.100.192 0.0.0.63
access-list 1 permit 192.168.101.0 0.0.0.63
access-list 1 permit 192.168.101.64 0.0.0.63

access-list 1 permit 192.168.101.128 0.0.0.31
access-list 1 permit 192.168.101.160 0.0.0.31
access-list 1 permit 192.168.101.192 0.0.0.31
access-list 1 permit 192.168.101.224 0.0.0.31
access-list 1 permit 192.168.102.0 0.0.0.31
access-list 1 permit 192.168.102.32 0.0.0.31

6.2 Port Security:

In FIN Access Layer Switch =

```
int range fa0/3-24
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown
```

7. Quality of Service (QoS):

Quality of Service (QoS) is a set of techniques and mechanisms that prioritize certain types of network traffic over others, ensuring that critical applications receive the necessary

bandwidth and latency while maintaining overall network performance. In the context of the trading floor support centre network, where real-time data and communication are crucial, QoS configurations are implemented to prioritize and manage traffic effectively.

7.1 QoS Configuration:

Purpose of QoS:

- **Prioritization**: QoS allows the network to prioritize specific types of traffic, such as voice and video communications or critical business applications, over less time-sensitive data.
- **Bandwidth Allocation**: QoS configurations allocate and guarantee a certain amount of network bandwidth to essential applications, preventing congestion and ensuring consistent performance.
- **Reduced Latency**: By prioritizing critical traffic, QoS helps reduce latency for real-time applications, enhancing the overall user experience.

Implementation Steps:

- **Identify Traffic Classes**:
  - Different types of traffic are identified based on their priority and importance. For example, voice over IP (VoIP) or video conferencing might be classified as high-priority traffic.
- **Classify Traffic:**
  - Traffic classification involves marking packets with Differentiated Services Code Point (DSCP) values or other Quality of Service markings. This marking is typically done at the network edge or on devices capable of traffic classification.
- **Configuration of QoS Policies:**
  - QoS policies are defined based on the identified traffic classes. These policies specify the treatment that each class of traffic should receive in terms of priority, bandwidth, and latency.
- **Congestion Management:**
  - QoS mechanisms, such as Weighted Fair Queuing (WFQ) or Class-Based Weighted Fair Queuing (CBWFQ), are configured to manage congestion and ensure fair distribution of bandwidth among different traffic classes.
- **Traffic Policing and Shaping:**
  - Traffic policing and shaping mechanisms control the rate at which traffic is sent or received, preventing network congestion and ensuring compliance with defined QoS policies.

8. Monitoring and Management:

Effective monitoring and management are essential for maintaining a stable and secure network. In the trading floor support centre network, Simple Network Management Protocol (SNMP) is configured for monitoring, and logging with alerts is implemented to ensure proactive network management.

8.1 SNMP Configuration:

SNMP Configuration Steps:

- **Enable SNMP on Devices:**
  - SNMP is enabled on routers, switches, and other network devices. This is typically done through the device's command-line interface (CLI) or web-based management interface.
- **Set SNMP Community Strings:**
  - Community strings act as passwords that control access to SNMP information. A read-only community string allows devices to be queried for information, while a read-write community string allows configuration changes.

```
snmp-server community public RO
snmp-server community private RW
```

- **Define SNMP Traps:**
  - SNMP traps are notifications sent by devices to alert the SNMP manager of specific events. These events can include link status changes, interface errors, or device reboots.

```
snmp-server enable traps
snmp-server host 140.16.1.50 public
```

SNMP traps are enabled, and the IP address 140.16.1.50 is configured to receive traps with the community string "public."

8.2 Logging and Alerts:

Logging and alerts provide insights into the network's health and help identify potential issues or security incidents. By configuring logs and alerts, network administrators can proactively address concerns before they impact the network.

Logging and Alerts Configuration Steps:

- **Enable Logging:**

- Logging is enabled on devices to capture system messages and events. These logs can include information about configuration changes, errors, or security events.

```
logging on
```

- **Set Logging Levels:**
  - Logging levels determine the severity of messages that are recorded. Different levels, such as informational, warning, or critical, allow administrators to filter logs based on their importance.

```
logging console informational
logging buffered warning
```

Console logging is set to informational, while buffered logging is set to warning. This ensures that less critical messages are displayed on the console, while more critical messages are stored in the device's buffer.

- **Configure Email Alerts:**
  - Some devices support email alerts, which can be configured to notify administrators of specific events. This is often done through Simple Mail Transfer Protocol (SMTP) settings.

```
logging email alerts
logging email address admin@example.com
```

email alerts are enabled, and alerts are sent to the specified email address.

9. Testing and Validation:

Packet Tracer, a powerful network simulation tool, was employed to simulate and test the trading floor support centre's network design. Simulation in Packet Tracer allows for a comprehensive evaluation of the network's functionality, ensuring that configurations are accurate and that the network meets specified requirements.

9.1 Simulation:

Steps in Packet Tracer Simulation:

- **Topology Creation:**
  - The first step involves creating the network topology within Packet Tracer. This includes adding routers, switches, PCs, servers, and other relevant devices to replicate the physical setup of the trading floor support centre.
- **Device Configuration:**
  - Each network device is configured according to the design specifications. This includes setting up IP addresses, configuring routing protocols, defining VLANs, implementing QoS policies, and other relevant configurations.

- **Interconnection Testing:**
    - The simulation allows for the testing of interconnections between devices. This involves verifying that routers can communicate with each other, switches can forward traffic within VLANs, and PCs can connect to servers.
- **Dynamic IP Address Assignment:**
    - The simulation includes testing the functionality of the DHCP servers in dynamically assigning IP addresses to devices. This ensures that devices across different departments obtain the correct IP configurations.
- **Routing and Switching Verification:**
    - Verification of routing protocols, such as OSPF, is crucial. Simulation allows for checking that routers and multilayer switches advertise routes correctly and that devices can communicate across different network segments.
- **Wireless Network Testing:**
    - Simulation provides a platform for testing the functionality of wireless networks. This involves verifying that access points are correctly configured, and devices can connect to the wireless network within each department.
- **Security Measures Testing:**
    - Security configurations, including ACLs and port-security, are thoroughly tested to ensure that only authorized traffic is allowed, and potential security vulnerabilities are addressed.

9.2 Troubleshooting:

Issue 1: Inter-VLAN Routing Not Working

Symptoms:

- Devices in different VLANs were unable to communicate with each other.

Troubleshooting Steps:

1. **Verification of VLAN Configurations:**
    - Checked VLAN configurations on multilayer switches to ensure that devices were correctly assigned to their respective VLANs.
2. **Review of Inter-VLAN Routing Configuration:**
    - Examined the inter-VLAN routing configuration on multilayer switches to confirm that routing interfaces were correctly configured.
3. **Routing Protocol Check:**
    - Verified that OSPF routing protocol was properly configured and that routers and multilayer switches were exchanging routing information.
4. **Subnetting Review:**

- Reviewed the subnetting scheme to confirm that IP addresses assigned to different VLANs were within the correct subnets.

5. **Resolution:**

    - Discovered a misconfiguration in the routing interfaces of multilayer switches. Corrected the misconfiguration, and inter-VLAN routing was successfully restored.

Issue 2: DHCP Server Failure

Symptoms:

- Devices were not receiving IP addresses dynamically from DHCP servers.

Troubleshooting Steps:

1. **DHCP Server Configuration Review:**

    - Checked the configuration of DHCP servers to ensure that they were correctly configured to allocate IP addresses within the defined subnets.

2. **Network Connectivity Test:**

    - Verified network connectivity between devices and DHCP servers to confirm that there were no connectivity issues affecting DHCP service.

3. **DHCP Server Pool Check:**

    - Examined DHCP server pools to ensure that there were available IP addresses for dynamic assignment.

4. **Verification of DHCP Relay:**

    - Checked the configuration of DHCP relay on routers to ensure that DHCP requests from different VLANs were being forwarded to the DHCP servers.

5. **Resolution:**

    - Discovered an issue with DHCP relay configuration on routers. Corrected the configuration, and DHCP servers began successfully assigning IP addresses to devices.

10. Results and Evaluation:

10.1 Performance Metrics

During the testing phase of the trading floor support center's network in Packet Tracer, various performance metrics were measured to assess the efficiency and reliability of the implemented network infrastructure. The following performance metrics were considered:

1. **Latency:**
    - Latency was measured to evaluate the delay in data transmission between devices. Low latency is critical for real-time applications, such as VoIP and video conferencing.
2. **Throughput:**
    - Throughput measures the amount of data transmitted successfully over the network within a specific time period. It helps assess the network's capacity and bandwidth utilization.
3. **Packet Loss:**
    - Packet loss was monitored to identify any instances where data packets did not reach their destination. Minimizing packet loss is crucial for maintaining data integrity and application reliability.
4. **Jitter:**
    - Jitter measures the variation in packet arrival times, especially important for real-time applications. Consistent and low jitter is essential for quality communication in voice and video applications.
5. **Reliability:**
    - Reliability metrics assessed the network's ability to maintain consistent performance without disruptions. Redundancy measures, such as multiple ISPs and device redundancies, were evaluated for their impact on network reliability.

10.2 Achievement of Objectives:

The project objectives were established to design, implement, and validate a robust network infrastructure for the trading floor support center. The evaluation of the project's success is based on the extent to which these objectives were met:

1. **Design a Logical Network Infrastructure:**
    - **Achievement:** The network design using Packet Tracer successfully met the business needs of the trading floor support center. The hierarchal model with redundancy at every layer, VLAN implementations, and subnetting aligned with the design requirements.
2. **Implement Redundancy Measures:**

- **Achievement:** Redundancy measures, including dual routers, dual multilayer switches, and connectivity to multiple ISPs, were implemented successfully. These measures contribute to high availability and fault tolerance.

3. **Establish Connectivity with Redundant ISPs:**
    - **Achievement:** The network was configured to connect to at least two ISPs, providing redundancy and minimizing the risk of connectivity issues. This ensures continuous internet access for the trading floor support center.
4. **Configure Wireless Networks:**
    - **Achievement:** Wireless networks were successfully implemented for each department, enabling users to connect seamlessly using Cisco Access Points.
5. **Utilize VLANs and Subnetting:**
    - **Achievement:** Each department was assigned to a different VLAN with proper subnetting, utilizing the base network of 172.16.1.0. This allowed for efficient IP address allocation and network segmentation.
6. **Configure Basic Device Settings:**
    - **Achievement:** Basic device settings, including hostnames, passwords, banner messages, and disabling IP domain lookup, were configured according to best practices.
7. **Enable Inter-VLAN Routing:**
    - **Achievement:** Inter-VLAN routing was successfully configured on multilayer switches, enabling communication between different departments.
8. **Implement OSPF Routing Protocol:**
    - **Achievement:** OSPF was configured as the routing protocol on routers and multilayer switches, allowing for dynamic and efficient routing within the network.
9. **Secure Network Devices:**
    - **Achievement:** Security measures, including SSH configuration, port-security, and ACLs, were implemented to ensure the confidentiality and integrity of network traffic.
10. **Configure DHCP Servers:**
    - **Achievement:** Dedicated DHCP servers were configured in the server room to provide dynamic IP address allocation, enhancing network manageability.
11. **Test and Verify Network Communication:**

- **Achievement:** Thorough testing and verification were conducted to ensure all configured components functioned as expected. The network demonstrated seamless communication between devices.

,

11. Conclusion:

11.1 Summary:

The design and implementation of the network infrastructure for the trading floor support center have been successfully executed, meeting the business needs and objectives outlined for this project. The key points discussed in the report can be summarized as follows:

1. **Network Topology:** A hierarchal model with redundancy at every layer was implemented to ensure high availability. The network spans three floors, each housing specific departments with dedicated VLANs and subnetting.
2. **Redundancy Measures:** Dual routers, dual multilayer switches, and connectivity to multiple ISPs were integrated, enhancing fault tolerance and network resilience.
3. **Wireless Networks:** Each department was equipped with a wireless network utilizing Cisco Access Points, providing flexibility and mobility for users.
4. **VLANs and Subnetting:** VLANs were implemented for each department with proper subnetting, efficiently utilizing the IP address space.
5. **Basic Device Settings:** Best practices for device configurations were followed, including hostnames, passwords, banner messages, and disabling IP domain lookup.
6. **Inter-VLAN Routing:** Multilayer switches were configured for inter-VLAN routing, facilitating communication between different departments.
7. **Routing Protocol:** OSPF was chosen as the routing protocol, ensuring dynamic and efficient routing within the network.
8. **Security Measures:** SSH configuration, port-security, and Access Control Lists (ACLs) were implemented to secure network devices and control traffic.
9. **DHCP Servers:** Dedicated DHCP servers in the server room were configured to provide dynamic IP address allocation for devices.
10. **Quality of Service (QoS):** QoS configurations were applied to prioritize specific types of traffic, ensuring optimal performance for critical applications.
11. **Monitoring and Management:** SNMP configurations were implemented for remote monitoring, and logging with alerts was configured to enable proactive network management.

12. **Testing and Validation:** Packet Tracer was utilized for simulation, testing, and validation of the network, ensuring a robust and functional infrastructure.

11.2 Lessons Learned:

Throughout the project, several valuable lessons were learned:

1. **Thorough Planning:** The importance of comprehensive planning before implementation cannot be overstated. A well-thought-out design significantly contributes to the project's success.
2. **Regular Configurations Review:** Regular reviews of device configurations are essential to catch misconfigurations early, ensuring a more reliable and secure network.
3. **Effective Troubleshooting Skills:** Developing effective troubleshooting skills is crucial for identifying and resolving issues promptly, contributing to network stability.
4. **Ongoing Monitoring:** Continuous monitoring and adjustment of network configurations are necessary for maintaining optimal performance and addressing evolving business requirements.
5. **Documentation Importance:** Detailed and accurate documentation is vital for understanding, troubleshooting, and maintaining the network over time.
6. **Simulation as a Tool:** The use of simulation tools, such as Packet Tracer, provides a controlled environment for testing configurations and troubleshooting without impacting the live network.

12. Future Work:

12.1 Potential Improvements:

As the trading floor support center’s network has been successfully implemented, there are opportunities for potential improvements and expansions to enhance its capabilities and adapt to future requirements. The following suggestions outline areas for future work:

1. **Enhanced Security Measures:**
    - Consider implementing more advanced security measures such as intrusion detection systems (IDS) or intrusion prevention systems (IPS) to further safeguard the network against potential threats.
2. **Network Virtualization:**
    - Explore the possibilities of network virtualization to create isolated virtual networks within the existing infrastructure. This can enhance resource utilization and improve network agility.

3. **Software-Defined Networking (SDN):**
    - Evaluate the implementation of Software-Defined Networking to centralize and automate network management, allowing for more dynamic and flexible control over network resources.
4. **Scaling for Growth:**
    - Plan for scalability by assessing the network's capacity to accommodate future growth in terms of users, devices, and data. This may involve upgrading hardware, adjusting IP address schemes, or optimizing routing protocols.
5. **Advanced QoS Configurations:**
    - Fine-tune Quality of Service (QoS) configurations to prioritize specific applications or services based on changing business needs. This can further optimize network performance for critical tasks.
6. **Implementation of Network Monitoring Tools:**
    - Integrate dedicated network monitoring tools beyond SNMP for in-depth analysis of network performance, real-time alerts, and historical data logging. This can provide a more comprehensive view of the network health.
7. **Disaster Recovery Planning:**
    - Develop and implement a comprehensive disaster recovery plan to ensure business continuity in the event of unforeseen incidents. This may involve off-site data backups, redundant systems, and clear recovery procedures.
8. **Enhanced Wireless Network Features:**
    - Explore advanced features for the wireless network, such as implementing the latest Wi-Fi standards, enhancing security protocols, and optimizing coverage for improved user experience.
9. **Cloud Integration:**
    - Consider integrating cloud services to offload certain network functions or storage, providing scalability and accessibility from various locations.
10. **Advanced Routing Protocols:**
    - Evaluate the use of advanced routing protocols or protocol enhancements to further optimize routing efficiency and adapt to evolving network requirements.
11. **Employee Training Programs:**
    - Develop ongoing training programs for network administrators to keep them updated on the latest technologies, security best practices, and troubleshooting techniques.

12. **Energy Efficiency Measures:**
    - Implement energy-efficient technologies and practices to minimize the environmental impact of the network infrastructure, such as optimizing power usage for network devices.
13. **Regular Security Audits:**
    - Conduct regular security audits to identify and address potential vulnerabilities, ensuring that the network remains resilient against evolving cybersecurity threats.

13. References:

The following references were consulted and utilized during the design and implementation of the Company/Business System network:

1. Cisco Packet Tracer Documentation. (https://www.netacad.com/courses/packet-tracer)
2. Cisco Networking Academy. (https://www.netacad.com/)
3. Rick Graziani - IPv6 Fundamentals_ A Straightforward Approach to Understanding IPv6-Cisco Press (2017)
4. Routing and Switching Essentials v6 Companion Guide-Pearson Education (US) (2016)
5. CCNA Routing and Switching Lab Guide.pdf.
6. Raymond Lacoste, Brad Edgeworth - CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide-Cisco Press (2020).

14. Appendices:

The appendices contain additional materials that supplement the main report. These materials include:

1. **Detailed Configurations:**
    - Configuration files for routers, switches, and other network devices, providing a comprehensive overview of the applied settings.
2. **Screenshots:**
    - Visual documentation of key configurations, network topology, and successful implementation.
3. **Packet Tracer Files:**
    - The Packet Tracer file (.pkt) used for the simulation and testing of the network. This file allows for an interactive exploration of the network design.