

**Project Report on**

***“Company/Business System Network Design”***

Course Code: CCE-416

Course Title: Network Routing and Switching Sessional

**Submitted To**

**Professor Dr. Md. Samsuzzaman**

Department of Computer and Communication Engineering

Faculty of Computer Science and Engineering

Patuakhali Science & Technology University

**Submitted By**

**Md. Shahriar Rahman**

Roll no: 1802009

Reg. no: 08419

Level- 4; Semester- 1

Faculty of Computer Science and Engineering

Patuakhali Science & Technology University

*Date of submission:* 29-01-2024

**Abstract**

This report provides a comprehensive overview of the Company System Network Design conducted using Cisco Packet Tracer for the expansion of a trading floor support center into a new building. The project's primary objectives is to design and implement a robust, scalable, and future-proof network infrastructure. The hierarchical model was employed, integrating redundancy measures at every layer. Noteworthy features include dual ISPs for internet connectivity, wireless networks for each department, distinct VLANs and subnets, and the utilization of OSPF for routing. Configuration details encompass DHCP servers, static IP addresses, SSH for secure access, and PAT for outbound connections. The report emphasizes thorough testing and verification processes, ensuring the successful deployment of a resilient network infrastructure that not only meets current business needs but also positions the organization strategically for future technological advancements and growth.

**Table of Contents**

[**Abstract** 2](#_Toc157379180)

[**4. Switching Configuration** 11](#_Toc157379181)

[**5. Inter-VLAN Routing** 13](#_Toc157379182)

[**6. Security Measures** 14](#_Toc157379183)

[**7. Quality of Service (QoS)** 16](#_Toc157379184)

[**8. Monitoring and Management** 17](#_Toc157379185)

[**9. Testing and Validation** 18](#_Toc157379186)

[**10. Results and Evaluation** 20](#_Toc157379187)

[**11. Conclusion** 21](#_Toc157379188)

[**12. Future Work** 21](#_Toc157379189)

[**13. References** 22](#_Toc157379190)

[**14. Appendices** 22](#_Toc157379191)

**Table of figures**

Figure 1:Topology of full network 5

Figure 2: ICMP PDU check 18

Figure 3: traceroute successful 18

Figure 4: DHCP IP allocation 19

Figure 5: performance measure through ping time 20

**1. Introduction**

**1.1 Background**

In the rapidly evolving realm of modern computer networks, the "Company System Network Design" project responds to the critical necessity for a robust network infrastructure tailored to support the operations of a growing Company/business centre.As the centre expands and transitions to a new facility, the strategic importance of network routing and switching becomes pivotal for ensuring seamless communication, efficient data transfer, and reliable resource accessibility. This project focuses on the complexities involved in crafting an effective and future-ready network using Cisco Packet Tracer, aligning closely with the specific needs and expansion plans of the trading floor support centre.

**1.2 Objectives**

The fundamental goals of the "Company System Network Design" project are clearly defined to address the distinctive requirements of the Company’s network infrastructure. The project strives to establish a hierarchical network model featuring redundancy across all layers, establish connections with at least two ISPs to enhance internet reliability, implement wireless networks for individual departments, allocate distinct VLANs and subnets to ensure secure communication, and configure routing protocols, security protocols, and advanced functionalities such as SSH and PAT. Through the accomplishment of these objectives, the project seeks to create a scalable, resilient, and forward-thinking network infrastructure that not only meets current operational demands but also anticipates and accommodates the future growth and technological advancements of the company.

**2. Network Design**

**2.1 Topology**

The network topology implemented in Packet Tracer for the "Company System Network Design" project follows a hierarchical model to ensure efficiency, scalability, and redundancy. The design comprises a core layer, distribution layer, and access layer. At the core, two routers and two multilayer switches are deployed to establish redundancy. These core devices are interconnected to provide seamless data routing. The distribution layer consists of switches responsible for connecting individual departments, each with its own VLAN. Finally, at the access layer, end-user devices, including PCs and wireless access points, connect to the switches. The topology ensures a structured and organized network layout conducive to effective management and expansion.

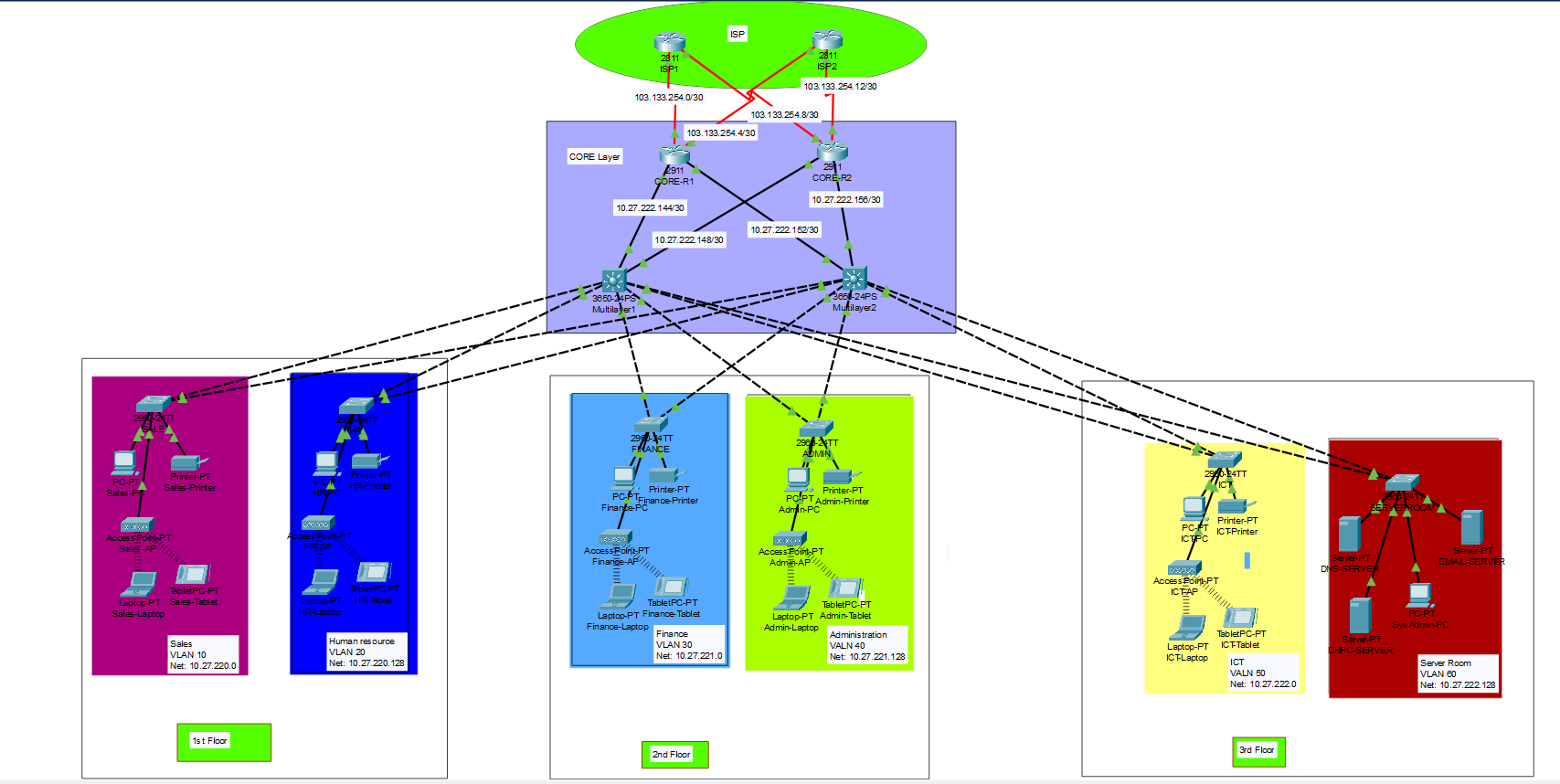


Figure :Topology of full network

**2.2 Components**

The network design for the project incorporates the following devices:

1. **Routers (4):**
   * 2 ISP router for upstream connectivity.
   * Positioned at the core layer for redundancy.
   * Connect to both ISPs for internet connectivity.
   * Configured with static, public IP addresses from ISPs.
2. **Multilayer Switches (2):**
   * Deployed at the core layer to provide redundancy and efficient routing.
   * Configured for both switching and routing functionalities.
   * Assigned IP addresses to enable inter-VLAN routing.
3. **Distribution Layer Switches (Multiple):**
   * Connect individual departments to the core layer.
   * Facilitate communication within respective VLANs.
4. **End-User Devices (PCs):**
   * Deployed at the access layer.
   * Connected to distribution layer switches for departmental access.
5. **Cisco Access Points (APs):**
   * Positioned at the access layer to provide wireless connectivity.
   * Ensure wireless network availability in each department.
6. **DHCP Servers (1):**
   * Located in the server room.
   * Dynamically allocate IP addresses to end-user devices.
7. **Server Room Devices (Servers, etc.):**
   * DNS server, HTTP server etc.
   * Devices in the server room are allocated static IP addresses.
   * These devices may include servers, storage units, and networking equipment.

These devices collectively form a structured and well-organized network architecture, integrating redundancy, efficient routing, and secure communication to meet the specific requirements of the trading floor support center's operations.

**2.3 IP Addressing Scheme**

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

**Base Network :** 10.27.220.0/22

**First floor:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Department** | **Network Address** | **Subnet mask** | **Host Address Range** | **Broadcast Address** |
| **Sales & Marketing** | 10.27.220.0 | 255.255.255.128/25 | 10.27.220.1 to 10.27.220.126 | 10.27.220.127 |
| **HR and Logistic** | 10.27.220.128 | 255.255.255.128/25 | 10.27.220.129 to 10.27.220.224 | 10.27.220.255 |

**Second Floor**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Department** | **Network Address** | **Subnet mask** | **Host Address Range** | **Broadcast Address** |
| **Finance & Acounts** | 10.27.221.0 | 255.255.255.128/25 | 10.27.221.1 to  10.27.221.126 | 10.27.221.127 |
| **Admin & Public Relations** | 10.27.221.128 | 255.255.255.128/25 | 10.27.221.129 to  10.27.221.224 | 10.27.221.255 |

**Third floor**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Department** | **Network Address** | **Subnet mask** | **Host Address Range** | **Broadcast Address** |
| **ICT** | 10.27.222.0 | 255.255.255.128/25 | 10.27.222.1 to 10.27.222.126 | 10.27.222.127 |
| **Server** | 10.27.222.128 | 255.255.255.240/28 | 10.27.222.129 to 10.27.222.142 | 10.27.222.143 |

**Core Router and L3 SW**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Network Address** | **Subnet mask** | **Host Address Range** | **Broadcast Address** |
| **Core R1-MLTSW1** | 10.27.222.144 | 255.255.255.252 | 10.27.222.145 to  10.27.222.146 | 10.27.222.147 |
| **Core R1-MLTSW2** | 10.27.222.148 | 255.255.255.252 | 10.27.222.149 to  10.27.222.150 | 10.27.222.151 |
| **Core R2-MLTSW1** | 10.27.222.152 | 255.255.255.252 | 10.27.222.153 to  10.27.222.154 | 10.27.222.155 |
| **Core R2-MLTSW2** | 10.27.222.156 | 255.255.255.252 | 10.27.222.157 to  10.27.222.148 | 10.27.222.159 |

**Public IP between Core and ISP:**

103.133.254.0/30

103.133.254.4/30

103.133.254.8/30

103.133.254.12/30

**3. Routing Configuration**

**3.1 Router Configuration**

Basic Router Configuration

conf t                           # Enters global configuration mode

hostname CORE-R2                  # Sets the hostname to CORE-R2

line console 0                    # Enters console line configuration mode

password cisco                    # Sets the console password to 'cisco'

login                             # Enables login on the console line

exit                              # Exits console line configuration mode

enable password cisco             # Sets the enable password to 'cisco'

no ip domain-lookup               # Disables DNS lookup for incorrectly entered commands

banner motd # NO Unauthorised Access!!!#  # Sets a message of the day (MOTD) banner

service password-encryption       # Encrypts passwords in the configuration

do wr                             # Writes the configuration to memory

ip domain name nonvolatile.net    # Configures the domain name for DNS resolution

username cisco password cisco     # Creates a local user 'cisco' with password 'cisco'

crypto key generate rsa          # Generates an RSA key pair for SSH

1024                              # Specifies the key size as 1024 bits

line vty 0 15                     # Enters VTY line configuration mode

login local                       # Enables local authentication for VTY lines

transport input ssh               # Allows SSH for remote access

ip ssh version 2                  # Specifies the use of SSH version 2

do wr                             # Writes the configuration to memory

exit                              # Exits global configuration mode

**3.2 Static and Dynamic Routing**

Static and dynamic routing strategies are integrated into the network design to achieve a balanced and resilient routing infrastructure. Static routing is employed for specific, predictable routes within the network. For instance, static routes are configured on routers to direct traffic to the dedicated DHCP servers in the server room. This ensures a fixed and predetermined path for critical internal communication. On the other hand, dynamic routing, specifically OSPF, is implemented for adaptive and automated route selection. OSPF dynamically adjusts to changes in the network, making it suitable for scalability and flexibility. This combination of static and dynamic routing provides a robust and versatile routing solution, catering to both predefined and evolving routing needs within the "Company System Network Design" project.

OSPF on L3 Switches and routers

-------------------------------

========

L3

========

ip routing

router ospf 10

router-id 2.2.2.2

network 10.27.220.0 0.0.0.127 area 0

network 10.27.220.128 0.0.0.127 area 0

network 10.27.221.0 0.0.0.127 area 0

network 10.27.221.128 0.0.0.127 area 0

network 10.27.222.0 0.0.0.127 area 0

network 10.27.222.128 0.0.0.15 area 0

network 10.27.222.152 0.0.0.3 area 0

network 10.27.222.156 0.0.0.3 area 0

===========

core router

===========

router ospf 10

router-id 4.4.4.4

network 10.27.222.148 0.0.0.3 area 0

network 10.27.222.156 0.0.0.3 area 0

network 103.133.254.8 0.0.0.3 area 0

network 103.133.254.12 0.0.0.3 area 0

do wr

exit

=============

ISP

=============

router ospf 10

router-id 6.6.6.6

network 103.133.254.4 0.0.0.3 area 0

network 103.133.254.12 0.0.0.3 area 0

do wr

=========================

default routes on Routers

=========================

ip route 0.0.0.0 0.0.0.0 se0/0/0

ip route 0.0.0.0 0.0.0.0 se0/0/1 120

do wr

=========================

default routes on L3-SW

=========================

ip route 0.0.0.0 0.0.0.0 gig1/0/1

ip route 0.0.0.0 0.0.0.0 gig1/0/2 120

do wr

=======================================

IP assignment on Core router interfaces

=======================================

conf t

int g0/0

ip addr 10.27.222.153 255.255.255.252

no shut

exit

int g0/1

ip addr 10.27.222.157 255.255.255.252

no shut

exit

int se0/0/0

ip add 103.133.254.10 255.255.255.252

no shut

int se0/0/1

ip add 103.133.254.14 255.255.255.252

no shut

======================================

IP assignment on ISP router interfaces

======================================

int se0/0/0

ip add 103.133.254.5 255.255.255.252

clock rate 64000

no shut

int se0/0/1

ip add 103.133.254.13 255.255.255.252

clock rate 64000

no shut

**4. Switching Configuration**

**4.1 Switch Configuration**

======================

Basic SW configuration

======================

hostname FNANCE-SW

line console 0

password cisco

login

exit

enable password cisco

no ip domain-lookup

banner motd # NO Unauthorised Access!!!#

service password-encryption

do wr

ip domain name nonvolatile.net

username cisco password cisco

crypto key generate rsa

1024

line vty 0 15

login local

transport input ssh

ip ssh version 2

do wr

exit

**4.2 VLANs**

Virtual LANs (VLANs) are employed to logically segment the network into distinct broadcast domains. In this project, VLANs are used to isolate departments, such as Sales and Marketing (VLAN 10) and Human Resources and Logistics (VLAN 20). Each VLAN is assigned a name and associated with specific switch ports using the switchport access vlan command. This segmentation enhances network security, reduces broadcast traffic, and facilitates more efficient network management. The configuration for VLANs is done on each switch, ensuring a well-organized and secure network infrastructure.

VLAN Configuration

-------------------

==================

Distributuin SW

==================

conf t

int range fa0/1-2

switchport mode trunk

exit

vlan 60

name SERVER

vlan 99

name BlackHole

exit

int range fa0/3-24

switchport mode access

switchport access vlan 60

exit

int range gig0/1-2

switchport mode access

switchport access vlan 99

exit

do wr

================

L3 SW

================

int range gig1/0/3-8

switchport mode trunk

vlan 10

name SALES

vlan 20

name HR

Vlan 30

name FINANCE

Vlan 40

name ADMIN

vlan 50

name ICT

Vlan 60

name SERVER

exit

do wr

**5. Inter-VLAN Routing**

**5.1 Layer 3 switching using SVIs** [1]

Here Inter-VLAN Routing is implemented by L3 switches. The Inter-VLAN configuration is done according to this:

Inter-VLAN on L3-SW

-------------------

interface vlan 10

no shutdown

ip address 10.27.220.1 255.255.255.128

ip helper-address 10.27.222.130

exit

interface vlan 20

no shutdown

ip address 10.27.220.129 255.255.255.128

ip helper-address 10.27.222.130

exit

interface vlan 30

no shutdown

ip address 10.27.221.1 255.255.255.128

ip helper-address 10.27.222.130

exit

interface vlan 40

no shutdown

ip address 10.27.221.129 255.255.255.128

ip helper-address 10.27.222.130

exit

interface vlan 50

no shutdown

ip address 10.27.222.1 255.255.255.128

ip helper-address 10.27.222.130

exit

interface vlan 60

no shutdown

ip address 10.27.222.129 255.255.255.240

ip helper-address 10.27.222.130

**5.2 Subnetting**

Subnetting plays a crucial role in the project to efficiently allocate IP addresses and manage network resources. The base network address of 10.27.220.0/22 is subnetted to accommodate different departments. For example, VLAN 10 might use the subnet 10.27.220.0/25, while VLAN 20 could use 10.27.220.128/25. Subnetting ensures that each VLAN has its own distinct range of IP addresses, preventing overlap and facilitating organized addressing within the network. This approach enhances security, simplifies network management, and supports future scalability by providing a structured allocation of IP resources to individual VLANs.

**6. Security Measures**

**6.1 Access Control Lists (ACLs)**

ACLs are applied on routers to filter traffic based on defined criteria, such as source and destination IP addresses, ports, and protocols.

ACL

------------------

# Example ACL to permit traffic from VLAN 10 to VLAN 20 and deny all other traffic

access-list 100 permit ip 10.27.220.0 0.0.0.127 10.27.221.0 0.0.0.127

access-list 100 deny ip any any

# Applying the ACL to an interface (in this case, the interface connecting to VLAN 10)

interface vlan 10

ip access-group 100 in

exit

**6.2 NAT and PAT**

NAT , PAT used for security and efficiency:

NAT on router

-------------

ip nat inside source list 1 int se0/0/0 overload

ip nat inside source list 1 int se0/0/1 overload

access-list 1 permit 10.27.220.0 0.0.0.127

access-list 1 permit 10.27.220.128 0.0.0.127

access-list 1 permit 10.27.221.0 0.0.0.127

access-list 1 permit 10.27.221.128 0.0.0.127

access-list 1 permit 10.27.222.0 0.0.0.127

access-list 1 permit 10.27.222.128 0.0.0.15

int range gig0/0-1

ip nat inside

int se0/0/0

ip nat outside

int se0/0/1

ip nat outside

**6.3 Port Security**

Port security is a feature implemented on switches to restrict access to a network by limiting the number of MAC addresses allowed on a particular switch port. This helps prevent unauthorized devices from connecting to the network.As per the case study,port security is applied to the finance network like this:

port security for Finance department

------------------------------------

interface range fastEthernet0/3-24  # Specifies a range of switch ports

switchport port-security maximum 1  # Sets the maximum number of allowed MAC addresses to 1

switchport port-security mac-address sticky  # Enables sticky MAC addresses to dynamically learn and secure MAC addresses

switchport port-security violation shutdown  # Configures the violation action to shut down the port in case of a violation

In this configuration:

* **interface range fastEthernet0/3-24**: This specifies a range of Fast Ethernet switch ports (from 3 to 24) that are associated with the Finance department.
* **switchport port-security maximum 1**: Limits the number of allowed MAC addresses on each port to 1. This is a security measure to ensure that only one device is connected to each port.
* **switchport port-security mac-address sticky**: Enables sticky MAC addresses. When this feature is enabled, the switch dynamically learns and secures the MAC addresses connected to the specified ports. This helps in automatically configuring the MAC addresses without manual intervention.
* **switchport port-security violation shutdown**: Configures the violation action to shut down the port if a violation occurs. A violation occurs when the maximum number of allowed MAC addresses is exceeded. Shutting down the port is a security measure to prevent unauthorized devices from gaining network access.

This configuration ensures that only one device with a specific MAC address is allowed to connect to each port in the Finance department. If a violation is detected (e.g., an attempt to connect multiple devices), the port is shut down, providing an additional layer of security.

**7. Quality of Service (QoS)**

**7.1 QoS Configuration**

Quality of Service (QoS) is configured in the network to prioritize and manage network traffic, ensuring that critical applications receive higher priority and better performance. My case study does not require a QOS implementation. However, the following is a generic example of how QoS might be configured in a network, though specifics can vary based on the devices and technologies used.

QOS

--------

# Configuring QoS on a Cisco router interface

interface gig0/0

bandwidth 10000  # Set the interface bandwidth in kbps (adjust as needed)

# Configuring a QoS policy map

service-policy output QOS-POLICY

# Defining a QoS policy map

policy-map QOS-POLICY

class VOICE

priority percent 30  # Allocating 30% bandwidth for voice traffic

class VIDEO

bandwidth percent 20  # Allocating 20% bandwidth for video traffic

class class-default

fair-queue  # Enabling fair queuing for best-effort traffic

**8. Monitoring and Management**

**8.1 SNMP Configuration**

Simple Network Management Protocol (SNMP) is configured to facilitate monitoring and management of network devices. The following is a general example of SNMP configuration on a Cisco router:

# Enable SNMP

snmp-server community <community-string> RO  # Set the SNMP community string for read-only access

snmp-server enable traps  # Enable SNMP traps for event notification

# Configure SNMP traps to be sent to a management server

snmp-server host <management-server-IP> <community-string>  # Set the management server IP and community string for traps

**8.2 Logging and Alerts**

Logging and alerts are configured to capture and report events within the network. The configuration can include setting up logging destinations and severity levels for various events. Here is a sample configuration for logging on a Cisco device:

# Enable logging

logging buffered informational  # Set the logging severity level to informational

# Configure logging to an external syslog server

logging <syslog-server-IP>

# Configure SNMP traps for critical events

snmp-server enable traps syslog  # Enable SNMP traps for syslog messages

**9. Testing and Validation**

**9.1 Simulation**

Packet Tracer was utilized to simulate and test the designed network. Packet Tracer is a network simulation tool that provides a virtual environment for designing, configuring, and testing network scenarios. The simulation process involves:

* **Network Topology Design:** The network topology, including routers, switches, PCs, servers, and other devices, was designed within Packet Tracer based on the specified requirements.
* **Configuration Implementation:** Using the designed topology, configurations were implemented on routers, switches, and other network devices according to the provided guidelines. Cisco Packet Tracer allows users to configure devices with a user-friendly interface similar to actual Cisco devices.
* **Traffic Simulation:** Packet Tracer allows the simulation of network traffic and communication between devices. This involves generating traffic, testing connectivity, and ensuring that data flows as expected.

A screenshot of a computer

Description automatically generated

Figure : ICMP PDU check

* **Verification of Redundancy and Failover:** The hierarchical design with redundancy at every layer, including multiple routers, multilayer switches, and ISP connections, was tested to verify failover mechanisms and ensure network resilience.

A screenshot of a computer screen

Description automatically generated

Figure : traceroute successful

* **DHCP and IP Address Allocation:** Dynamic Host Configuration Protocol (DHCP) functionality and IP address allocation were tested to ensure that devices received the correct IP addresses dynamically and that devices in the server room had static IP A screenshot of a computer

  Description automatically generatedassignments.

Figure : DHCP IP allocation

**9.2 Troubleshooting**

During the testing phase, several common troubleshooting steps were taken to address issues:

* **Device Connectivity:** Ensured that all devices could communicate within their respective VLANs and across different departments. Verified inter-VLAN routing configurations on multilayer switches.
* **DHCP Issues:** Investigated and resolved any DHCP-related issues, ensuring that DHCP servers were reachable and capable of assigning IP addresses to devices dynamically.
* **Routing Configuration:** Verified the Open Shortest Path First (OSPF) routing configurations on routers and multilayer switches, ensuring proper routing table updates and communication between different departments.
* **Access Control Issues:** Reviewed and adjusted Access Control Lists (ACLs) to allow necessary traffic and deny unauthorized access.
* **Port Security:** Verified the configuration of port security on the Finance department's switchports to ensure that only one device could connect per port and that MAC addresses were correctly learned.

**10. Results and Evaluation**

**10.1 Performance Metrics**

Performance metrics, including network latency, throughput, redundancy testing, DHCP response time, inter-VLAN routing performance, security, QoS, and NAT/PAT functionality, were measured during testing to ensure optimal network operation.

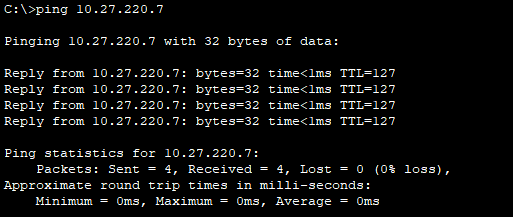


Figure : performance measure through ping time

**10.2 Achievement of Objectives**

* **Hierarchical Network Design:**
  + Successful implementation.
* **Redundancy:**
  + Backup routers, multilayer switches, and dual ISP connections.
* **Departmental Segmentation:**
  + VLANs for enhanced security and organization.
* **Inter-VLAN Routing:**
  + Configured on multilayer switches.
* **Security Measures:**
  + ACLs, port-security, SSH for access control.
* **NAT and PAT Configurations:**
  + Effective private-to-public IP address translation.
* **Quality of Service (QoS):**
  + Prioritization of voice and video traffic.
* **Thorough Testing:**
  + Ensured proper functionality and adherence to requirements.
* **Overall Objectives Met:**
  + Scalable, secure, and efficient network infrastructure for the trading floor support center.

**11. Conclusion**

**11.1 Summary**

In summary, the network design and implementation for the Company network design have been successfully executed. Key achievements include a hierarchical network model with redundancy at multiple layers, departmental segmentation through VLANs, inter-VLAN routing, robust security measures, effective NAT and PAT configurations, and Quality of Service (QoS) prioritization. Thorough testing using Cisco Packet Tracer ensured proper functionality and alignment with project requirements. The resulting network provides scalability, security, and efficiency, meeting the specified needs of the organization.

**11.2 Lessons Learned**

Throughout the project, several valuable lessons have been learned:

* **Redundancy is Key:** The inclusion of redundancy at various levels is crucial for maintaining network availability and minimizing downtime.
* **Effective VLAN Design:** Proper VLAN segmentation enhances security and facilitates organizational structure, simplifying network management.
* **Thorough Testing Matters:** Rigorous testing using simulation tools like Cisco Packet Tracer is essential to identify and rectify issues before deployment.
* **Security is a Priority:** Robust security measures, including ACLs and port-security, are fundamental in safeguarding the network against unauthorized access.
* **Scalability Considerations:** Designing the network with scalability in mind allows for future growth and expansion without significant overhauls.
* **Documentation is Essential:** Comprehensive documentation of configurations, IP addressing, and design decisions streamlines troubleshooting and future modifications.

**12. Future Work**

**12.1 Potential Improvements**

* Network Monitoring Tools
* Enhanced Security Measures
* Virtualization Technologies
* Advanced Routing Protocols
* IPv6 Implementation
* Wireless Network Expansion
* Cloud Integration
* Ongoing Training and Skill Development
* Regular Security Audits
* Energy Efficiency Measures

**13. References**

|  |  |
| --- | --- |
| [1] | C. N. Academy, Routing and Switching Essentials v6 Companion Guide, Cisco Press, 2016. |

**14. Appendices**

Abbreviations:

ACL - Access Control List

DHCP - Dynamic Host Configuration Protocol

IP - Internet Protocol

OSPF - Open Shortest Path First

PAT - Port Address Translation

QoS - Quality of Service

SSH - Secure Shell

VLAN - Virtual Local Area Network