Faculty of Computer Science & Engineering

Project Report on

Company/Business System Network Design using Packet-Tracer

Course Code: CCE 416

Course Title: Network Routing and Switching Sessional

Submitted by

Md. Babul Hasan
ID: 1802027
Reg: 08437
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 revolves around the design and implementation of a Voice over Internet Protocol (VoIP) network for Turtle Consultancy Limited, a company specializing in IT infrastructure solutions for medium-sized organizations. The objective is to establish a scalable and available network infrastructure that integrates voice and data services efficiently.

Using Cisco Packet Tracer, the network engineer constructs a comprehensive system that encompasses routers, switches, servers, and telephony devices. Each department within the organization is interconnected via routers equipped with VoIP capabilities, facilitating seamless communication across the network.

Key components of the network design include the utilization of VLANs to segregate voice and data traffic, router-on-a-stick configuration for inter-VLAN routing, and implementation of OSPF as the routing protocol for dynamic route advertisement. DHCP services are tailored to assign IP addresses dynamically, with dedicated servers for data and routers serving as DHCP servers for voice.

Security measures are implemented through SSH configuration for remote access, ensuring secure management of network devices. Telephony services are provisioned with dial-peering configurations, enabling IP phones to communicate across different routers.

The project concludes with rigorous testing to verify the functionality and performance of the configured network components, ensuring that all requirements and specifications outlined by the IT Manager are met satisfactorily. Through the adoption of hierarchical network design principles and adherence to industry-standard protocols, Turtle Consultancy Limited is poised to achieve enhanced communication capabilities and operational efficiency across its organizational infrastructure.

1. Introduction:

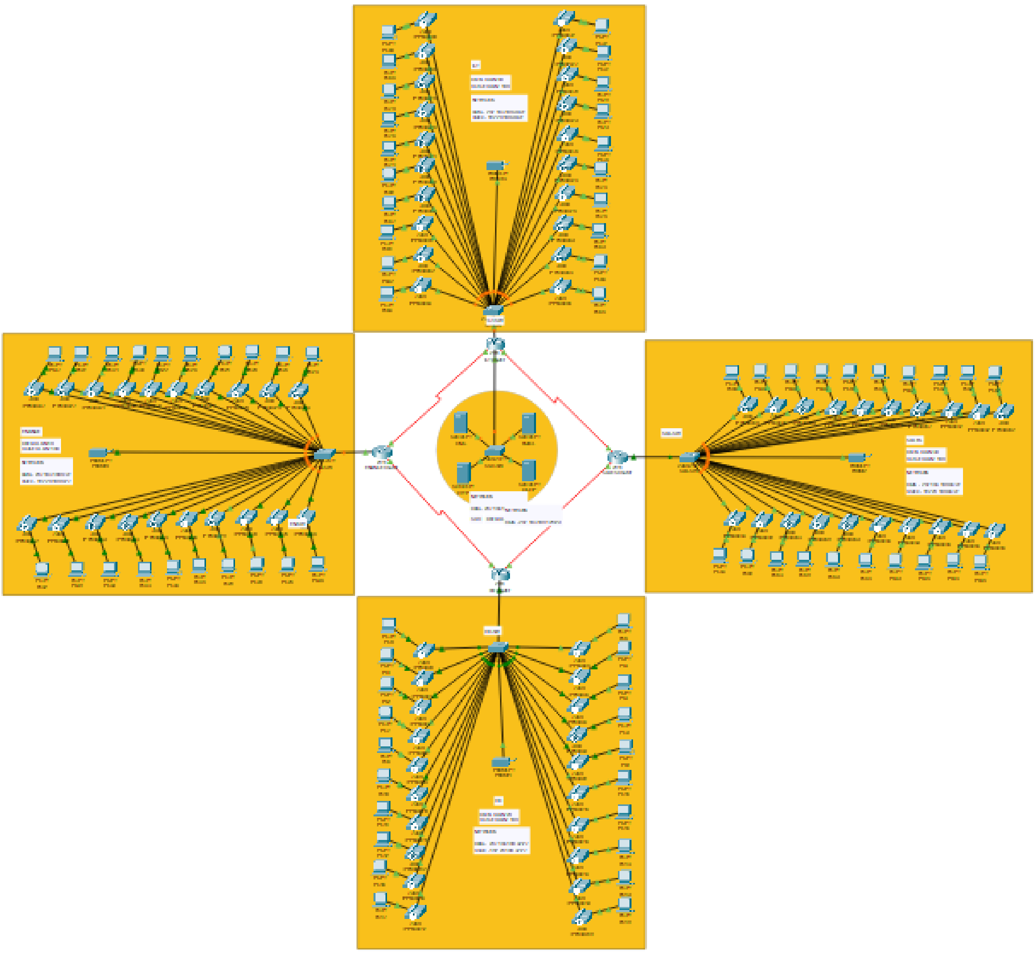
1.1 Objectives:

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

- Design a scalable and available VoIP network infrastructure for Turtle Consultancy Limited to meet the communication needs of its newly acquired branch.
- Integrate voice and data services seamlessly within the network to facilitate efficient communication and collaboration among employees.
- Implement VLANs to segregate voice and data traffic, ensuring optimal performance and security throughout the network.
- Configure routers with VoIP capabilities to enable inter-departmental communication and support dial-peering for IP phone connectivity across routers.
- Establish router-on-a-stick configuration for efficient inter-VLAN routing, allowing for communication between different VLANs within the network.
- Implement DHCP services to dynamically allocate IP addresses to devices, with dedicated servers for data and routers serving as DHCP servers for voice.
- Configure OSPF as the routing protocol to advertise routes dynamically and ensure efficient routing and network convergence.
- Enhance network security by configuring SSH for secure remote access to network devices, safeguarding against unauthorized access.
- Allocate dial numbers for telephony services in each department, adhering to a standardized format for easy identification and communication.
- Conduct thorough testing and validation of the configured network components to ensure adherence to requirements and specifications outlined by the IT Manager.
- Provide documentation and training materials to facilitate the understanding and management of the implemented network infrastructure by relevant stakeholders.
- Ensure compliance with industry best practices and standards throughout the design and implementation phases of the VoIP network.

2. Network Design:

2.1 Topology:



2.2 Components:

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: Cisco 2811 routers are deployed in each department, equipped with VoIP capabilities and serving as the backbone of the network infrastructure. These routers facilitate inter-departmental communication and routing of voice and data traffic.

- Switches: Cisco 2960 switches are deployed as access layer switches in each department, providing connectivity to desktops, phones, and other network devices. These switches enable efficient data transmission within local networks and VLAN segmentation.

- Servers: Four servers (DHCP, EMAIL, DNS, HTTP) are located at the server-side site, serving the entire organization. These servers handle essential network services such as dynamic IP address allocation, email hosting, domain name resolution, and web hosting.

- Telephony Devices: Each desktop is equipped with an associated telephone set, forming an integral part of the VoIP network. These devices enable users to make and receive phone calls over the IP network seamlessly.

- Cabling: Serial connections are utilized between routers for interconnection, while straight-through cables are used to connect routers to switches and switches to hosts. This ensures proper data transmission and connectivity across the network infrastructure.

- VLANs: Virtual LANs are implemented to segregate voice and data traffic within the network. Each department is assigned two VLANs—one for data and another for voice—to optimize network performance and security.

- DHCP Servers: Dedicated DHCP servers are configured to allocate IP addresses dynamically to devices within the data VLANs, ensuring efficient IP address management and network scalability.

- OSPF Routing Protocol: OSPF is implemented as the routing protocol to facilitate dynamic route advertisement and efficient routing within the network infrastructure, ensuring optimal traffic flow and network convergence.

- SSH Configuration: Secure Shell (SSH) is configured on all routers to provide secure remote access for network management and administration, enhancing network security and access control.

- Dial Peering Configuration: Dial peering is configured on routers to enable IP phones from different departments to communicate effectively, facilitating seamless voice communication across the organization.

- Testing and Validation: Rigorous testing and validation procedures are conducted to ensure the proper functionality and performance of all configured network components, adhering to requirements and specifications outlined by the IT Manager.

- Documentation and Training: Comprehensive documentation and training materials are provided to relevant stakeholders to facilitate understanding and management of the implemented network infrastructure, ensuring smooth operations and support.

2.3 IP Addressing Scheme

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

For Data:

Dept	Network Add	Subnet mask	Host add range
Finance	192.168.100.0	255.255.255.224/27	192.168.100.1 192.168.100.30
HR	192.168.100.32	255.255.255.224/27	192.168.100.33 192.168.100.62
Sales	192.168.100.64	255.255.255.224/27	192.168.100.65 192.168.100.94
ICT	192.168.100.96	255.255.255.224/27	192.168.100.97 192.168.100.126
Server	192.168.100.128	255.255.255.224/27	192.168.100.129 192.168.100.134

For VOICE:

Dept	Network Add	Subnet mask	Host add range
Finance	172.16.100.0	255.255.255.224/27	172.16.100.1 172.16.100.30
HR	172.16.100.32	255.255.255.224/27	172.16.100.33 172.16.100.62
Sales	172.16.100.64	255.255.255.224/27	172.16.100.65 172.16.100.94
ICT	172.16.100.96	255.255.255.224/27	172.16.100.97 172.16.100.126

3. Routing Configuration:

3.1 Router Configuration:

Basic Config:

```
hostname Router_Name
enable password cisco
line con 0
password cisco
login
exit
banner motd #NO UNAUTHORIZE ACCESS, THIS IS PUNISHABLE BY LAW!!!#
service password-encryption
no ip domain-lookup

do wr

username cisco password cisco
ip domain name cisco.net
crypto key generate rsa general-keys modulus 1024

ip ssh version 2
line vty 0 15
login local
transport input ssh
exit

do wr
```

3.2 DHCP Configuration:

For Voice :

```
ip dhcp excluded-address default_gateway_ip
ip dhcp pool ICTVOICE
network network_address network_mask
default-router default_gateway_ip
option 150 ip default_gateway_ip
exit

do wr
```

4. Switching Configuration:

4.1 Switch Configuration:

For All Access Layer Switch =

```
hostname Switch_name
enable password cisco
line con 0
password cisco
login
exit
banner motd #NO UNAUTHORIZE ACCESS, THIS IS PUNISHABLE BY LAW!!!#
service password-encryption
no ip domain-lookup
```

4.2 VLANs:

Basic VLAN Setup:

```
vlan 10
name DATA

vlan 100
name VOICE
exit


int fa0/1
switchport mode trunk
exit

int range fa0/2-24
switchport mode access
switchport access vlan 10
switchport voice vlan 100

do wr
```

5. Telephony Configuration:

5.1 Dial Peering:

```
dial-peer voice 1 voip
destination-pattern 2..
session target ipv4:20.30.25.2
exit


dial-peer voice 2 voip
destination-pattern 4..
session target ipv4:20.30.25.9
exit


dial-peer voice 3 voip
destination-pattern 3..
session target ipv4:20.30.25.10
exit


do wr
```

5.2 Telephony Service:

```
telephony-service
max-dn 20
max-ephones 20
ip source-address 10.10.1.1 port 2000
auto assign 1 to 20
exit


ephone-dn 1
number 101
ephone-dn 2
number 102
```

```
ephone-dn 3
number 103
ephone-dn 4
number 104
ephone-dn 5
number 105
ephone-dn 6
number 106
ephone-dn 7
number 107
ephone-dn 8
number 108
ephone-dn 9
number 109
ephone-dn 10
number 110
ephone-dn 11
number 111
ephone-dn 12
number 112
ephone-dn 13
number 113
ephone-dn 14
number 114
ephone-dn 15
number 115
ephone-dn 16
number 116
ephone-dn 17
```

```
number 117
ephone-dn 18
number 118
ephone-dn 19
number 119
ephone-dn 20
number 120
```

6. Inter-VLAN routing:

6.1 Configuring Command:

Example Command:

```
int fa0/0.10
encapsulation dot1Q 10
ip address 207.103.100.1 255.255.255.224
ip helper-address 207.103.100.130
exit

int fa0/0.100
encapsulation dot1Q 100
ip address 182.20.100.1 255.255.255.224
exit

do wr
```

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:

- Scalable and Available VoIP Network Infrastructure: The designed network architecture ensures scalability and availability to meet the communication demands of Turtle Consultancy Limited's newly acquired branch.

- Integration of Voice and Data Services: Voice and data services are seamlessly integrated within the network infrastructure, enabling efficient communication and collaboration among employees.

- VLAN Segregation for Traffic Optimization: VLANs are implemented to segregate voice and data traffic, optimizing network performance and enhancing security.

- Inter-Departmental Communication via Routers: Cisco 2811 routers with VoIP capabilities facilitate inter-departmental communication, supporting dial peering for IP phone connectivity across routers.

- Efficient Inter-VLAN Routing: Router-on-a-stick configuration enables efficient inter-VLAN routing, allowing communication between different VLANs within the network.

- Dynamic IP Address Allocation with DHCP: DHCP services are configured to dynamically allocate IP addresses to devices, enhancing IP address management and network scalability.

- Dynamic Route Advertisement with OSPF: OSPF is implemented as the routing protocol, enabling dynamic route advertisement and efficient routing throughout the network infrastructure.

- Secure Remote Access with SSH: Secure Shell (SSH) is configured on all routers, ensuring secure remote access for network management and administration.

- Telephony Service Provisioning: Dial numbers are allocated for telephony services in each department, facilitating easy identification and communication.

- Dial Peering Configuration for VoIP Routing: Dial peering is configured on routers to facilitate effective VoIP routing, enabling IP phones from different departments to communicate seamlessly.

- Thorough Testing and Validation: Rigorous testing and validation procedures are conducted to ensure proper functionality and performance of all network components, meeting requirements and specifications outlined by the IT Manager.

- Documentation and Training: Comprehensive documentation and training materials are provided to relevant stakeholders, facilitating understanding and management of the network infrastructure.

11. Conclusion:

In conclusion, the design and implementation of the VoIP network infrastructure for Turtle Consultancy Limited's newly acquired branch represent a significant advancement in communication technology and network efficiency. Through meticulous planning, configuration, and testing, the network engineer has successfully addressed the requirements and challenges outlined by the IT Manager.

The hierarchical network design, incorporating Cisco routers, switches, servers, and telephony devices, ensures scalability, availability, and optimized traffic flow within the organization. By segregating voice and data traffic using VLANs, implementing dynamic IP address allocation with

DHCP, and enabling efficient routing with OSPF, the network infrastructure is robust and adaptable to the company's evolving needs.

Security measures, including SSH configuration for secure remote access, add an additional layer of protection to the network, safeguarding against unauthorized access and potential threats.

The successful provisioning of telephony services, coupled with dial peering configuration for VoIP routing, enhances inter-departmental communication and collaboration, fostering productivity and efficiency across the organization.

Overall, the designed VoIP network infrastructure aligns closely with industry best practices and standards, laying a solid foundation for Turtle Consultancy Limited's continued growth and success in delivering IT infrastructure solutions to medium-sized organizations worldwide. With comprehensive documentation and training materials provided, stakeholders are well-equipped to manage and maintain the network infrastructure effectively.

As technology evolves and business requirements change, ongoing monitoring, evaluation, and adaptation of the network infrastructure will be essential to ensure continued performance, security, and alignment with organizational objectives. Through proactive management and strategic investment in technology, Turtle Consultancy Limited is well-positioned to leverage its network infrastructure as a competitive advantage in the dynamic landscape of IT solutions delivery.

12. Future Work:

12.1 Potential Improvements:

- Enhanced Security Measures: Continuously assess and improve security measures within the network infrastructure to mitigate emerging threats and vulnerabilities. Consider implementing advanced security protocols, intrusion detection systems, and regular security audits to ensure robust protection of sensitive data and network resources.

- Integration of Advanced Technologies: Explore opportunities to integrate emerging technologies such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Internet of Things (IoT) devices to enhance network agility, scalability, and functionality. Evaluate the potential benefits and challenges of adopting these technologies within the existing network architecture.

- Quality of Service (QoS) Optimization: Implement Quality of Service (QoS) mechanisms to prioritize voice traffic over data traffic, ensuring optimal voice quality and reliability for VoIP communications. Fine-tune QoS parameters based on traffic patterns and network requirements to optimize network performance and user experience.

- Disaster Recovery and Business Continuity Planning: Develop comprehensive disaster recovery and business continuity plans to minimize downtime and data loss in the event of network outages, natural disasters, or cyber-attacks. Establish redundant network infrastructure, backup systems, and contingency measures to ensure uninterrupted operation and data integrity.

- Capacity Planning and Performance Optimization: Conduct regular capacity planning exercises to anticipate future growth and scalability requirements of the network infrastructure. Monitor network performance metrics, analyze traffic patterns, and optimize resource allocation to maintain optimal network performance and user satisfaction.

- End-User Training and Education: Provide ongoing training and education programs for end-users to promote awareness of network security best practices, efficient use of network resources, and troubleshooting techniques. Empower users to leverage network capabilities effectively while minimizing security risks and operational challenges.

- Adoption of Cloud Services and Hybrid Networking: Explore opportunities to leverage cloud services and hybrid networking models to augment existing network infrastructure capabilities, enhance scalability, and streamline resource provisioning. Evaluate the suitability of cloud-based solutions for specific workloads and applications within the organization's IT environment.

- Compliance and Regulatory Requirements: Stay abreast of evolving regulatory requirements, industry standards, and compliance frameworks relevant to network operations and data security. Ensure adherence to data protection regulations, privacy laws, and industry-specific compliance mandates to mitigate legal and regulatory risks.

- Collaboration and Vendor Partnerships: Foster collaboration with technology vendors, industry peers, and strategic partners to leverage expertise, share best practices, and stay informed about emerging trends and innovations in network technology. Cultivate strong vendor relationships to access technical support, training resources, and product roadmaps for informed decision-making.

- Continuous Improvement and Innovation: Foster a culture of continuous improvement and innovation within the organization's IT department, encouraging cross-functional collaboration, knowledge sharing, and experimentation with new technologies and methodologies. Embrace feedback, lessons learned, and industry insights to drive continuous enhancement of the network infrastructure and IT service delivery capabilities.

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.