



Network And Cloud Solution for Power Soft PVT Limited

CCU3603 - Individual Project 2

Final Report

**Bachelor of Information Technology
(Honor's) Degree**

**Rohan Nandasena
E 123283
BIT 002**

ESOFT Metro Campus

Declaration

Module: CCU3603

Deadline: 28th December 2022

Student Declaration

I hereby, declare that I know what plagiarism entails, namely, to use another's work and to present it as my own without attributing the sources in the correct way. I further understand what it means to copy another's work.

1. I know that plagiarism is a punishable offence because it constitutes theft.
2. I know what the consequences will be if I plagiarises or copy another's work in any of the assignments for this program.
3. I declare therefore that all work presented by our group for every aspect of our program, will be our own, and where we have made use of another's work, we will attribute the source in the correct way.
4. I acknowledge that the attachment of this document signed or not, constitutes a binding agreement between ourselves and ESOF.

I declare that this project is my own work and has not been submitted in any form for another degree or diploma at any university or other institution of tertiary education. Information derived from the published or unpublished work of others has been acknowledged in the text and a list of references is given.

16/02/2024

Signatures of the student:

Date:

Acknowledgement

Acknowledgement

In the field of individual project, I would like to thank my lecturer Mrs. Kavindi tharika for giving me advice on how to conduct the individual project properly and provide me with the knowledge necessary to create it. And I thank all the people who helped me Continue this project.

thank you,
Regards
Rohan Nandasena

Abstract

In this project, software development company Power Soft (Pvt) Limited aims to improve security, redundancy, efficiency, and reliability of its computer network through network upgrades. The company, which has five departments—IT, Sales, Finance, Human Resources, and Network Team—faces difficulties because of its outdated, basic network, which is lacking sharing of files and security capabilities.

Moreover, problems with redundancy and data security are made worse by poor server architecture. By putting in place a new network infrastructure fitted with safe data exchange tools and a reliable server architecture, the project aims to fix these shortcomings.

The project's essential elements are protocols and technologies, hardware and software requirements, and financial issues. Power Soft (Pvt) Limited hopes to provide secure data exchange and smooth departmental communication by installing suitable servers and upgrading the network, which will ultimately improve internal communication and operational efficiency.

Table of Contents

Contents

| | |
|--|----|
| Acknowledgement | 2 |
| Abstract..... | 3 |
| Table of Contents..... | 4 |
| List of Figures..... | 6 |
| List of Tables | 7 |
| List of Acronyms | 8 |
| Background..... | 1 |
| Chapter 1 - Introduction..... | 2 |
| Introduction..... | 2 |
| Project Background..... | 3 |
| Problem statement..... | 4 |
| Aim and Objectives..... | 5 |
| Aim:..... | 5 |
| Scope of the project..... | 5 |
| SWOT Analysis | 6 |
| Chapter 2 - Literature review | 7 |
| VLAN and Network Management | 7 |
| Chapter 3 Analysis..... | 10 |
| Analysis of the current system. | 10 |
| Requirement | 11 |
| User/ Client requirement | 11 |
| Feasibility study..... | 13 |
| Time feasibility | 13 |
| Cost feasibility..... | 14 |
| Scope feasibility | 15 |
| Technical feasibility | 15 |
| Economic feasibility | 16 |
| Methodology and planning artifact..... | 17 |

| | |
|---|----|
| Chapter 4 Design | 18 |
| Network Design | 18 |
| Cloud Design | 20 |
| Development Tools | 22 |
| Chapter 5 Implementation | 23 |
| Cloud Configurations | 24 |
| Resource Group Configuration | 25 |
| Virtual Network | 26 |
| Darta Server Virtual Machines | 26 |
| Web Server Virtual Machines | 27 |
| Microsoft defender Configuration (pending) | 28 |
| Virtual Network | 29 |
| Data Network Security Group | 30 |
| Web Server Network Security Group | 31 |
| Storage Account Configuration | 32 |
| Network Design Configuration | 33 |
| Assign VTP for layer 2 switches | 34 |
| Assign ports for Switch 1 | 35 |
| Multilayer Switch VANS | 37 |
| EtherChannel ling and LACP | 38 |
| Router interface up configurations | 41 |
| Assign Router Rip version 2 | 42 |
| DHCP Server configurations | 43 |
| Test Cases | 47 |
| Test planning | 45 |
| Test Case Analysis | 51 |
| Chapter 6 Evaluation | 52 |
| User Feedback | 52 |
| Responses | 53 |
| User Feedback Analysis | 55 |
| Chapter 7 Conclusion | 56 |
| Lesson learnt | 57 |
| Future work | 57 |
| References | 58 |
| Appendices | 60 |

List of Figures

| | |
|-------------------------------|----|
| Figure 1Grantt chart | 13 |
| Figure 2Network Design | 18 |
| Figure 3Packet tracer..... | 19 |
| Figure 4 Cloud Design..... | 20 |
| Figure 5Azure Portal | 21 |
| Figure 6Packet tracer..... | 22 |
| Figure 7RSG..... | 25 |
| Figure 8Web srver | 26 |
| Figure 9WEb | 27 |
| Figure 10Defender..... | 28 |
| Figure 11V..... | 29 |
| Figure 12Data NSG..... | 30 |
| Figure 13WEb NSG | 31 |
| Figure 14Storage account..... | 32 |
| Figure 15Vtp switch | 33 |
| Figure 16Vtp..... | 34 |
| Figure 17Vtp switch 2 | 34 |
| Figure 18switch | 37 |
| Figure 19Rip..... | 42 |
| Figure 20DHCP | 43 |
| Figure 21PC1..... | 44 |

List of Tables

| | |
|----------------------------|----|
| Table 1Cost Tabl | 14 |
| Table 2Assign ports | 35 |
| Table 3Lacp1 | 38 |
| Table 4Lacp 2..... | 39 |
| Table 5Show lacp 1 | 40 |
| Table 6Show lacp 2 | 40 |
| Table 8Testcase | 45 |
| Table 9Test planning | 46 |

List of Acronyms

DHCP – dynamic host configuration protocols

HSRP – Host standby Router Protocols

NTP – network Time protocol

VPN – virtual private network

VLAN – virtual local area network

ACL – Control access list

IP – Internet Protocol

VN – Virtual Network

DDNS – dynamic Domain name service

SSH – secure shell

QoS - Quality of Service

VM – Virtual Machine

Background

POWER SOFT (PVT) Limited values efficiency and security like a champion athlete values their training regime. It shows in their meticulously crafted network architecture, designed like a high-performance machine. The network's hierarchical structure operates like a well-oiled chain of command, seamlessly integrating with the Azure cloud like a trusted ally. Security guards on every corner, with customized Access Control Lists (ACLs) patrolling departments and dedicated security measures fortifying access layer switches. Think of them as digital sentries ensuring only authorized personnel enter vital systems.

But don't be fooled by this fortress-like approach. This network is built for speed and endurance as well. Redundancy is its mantra, achieved through the intricate interplay of RIPv2 routing protocols, cloud storage acting as a backup vault, scaling sets ready to spring into action, and LACP-enabled ether channeling – imagine multiple data highways working in concert to ensure smooth traffic flow.

Performance optimization is this network's secret weapon. Load balancing systems distribute tasks like a wise general, QoS settings prioritize critical data like a VIP escort, and carefully chosen bandwidth allocation ensures everything runs smoothly like a well-tuned engine.

POWER SOFT understands that technology is the lifeblood of modern business, and they're not afraid to embrace the latest advancements. They actively seek out cutting-edge solutions to meet their ever-evolving needs, ensuring their network is always a step ahead.

Chapter 1 - Introduction

Introduction

To running its company daily, POWER SOFT (PVT) Limited places a high priority on building an efficient, redundant, and secure network infrastructure. A well-designed network architecture must be put into place to achieve this goal.

The primary goal of this carefully constructed architecture is to provide a highly available and secure redundancy network. The network architecture is based on a hierarchical design, and Azure cloud servers are seamlessly integrated to enhance its functionality.

The careful set up of Access Control Lists (ACLs) customized for certain departments and cloud servers, as well as a thoughtful planning of port security for access layer switches, indicate the emphasis on security. In addition, redundancy and dependability are critical factors to provide optimal availability and uptime.

This is accomplished by the deployment of Rip version 2 for routing, the integration of cloud storage accounts and scaling sets for cloud resources, and the use of the Link Aggregation Control Protocol (LACP) for ether channeling with multilayer switches.

Additionally, thoughtful thought is given to suitable bandwidth allocation, Quality of Service (QoS) settings, and the deployment of load balancing systems to ensure reliable and redundant high-speed network performance. In summary, POWER SOFT Limited has committed to deploying the latest technologies to fulfil its changing requirements because it understands the vital role that a well-designed network architecture plays in promoting operational efficiency and security.

Building a secure network for POWER SOFT PVT Limited that will protect confidential information and stop illegal access to the company's network is the responsibility of a network administrator. A variety of processes go into creating a secure network, from identifying the risks and requirements of the organization to creating and executing security solutions that address those needs. The network's scalability must also be considered to allow for future development and growth. Scalable software solutions and modular hardware can be used to accomplish this.

Overall, by implementing a well-designed and secure network architecture, POWER SOFT PVT Limited can ensure reliable and efficient network operations, which will ultimately lead to increased productivity and business success.

Project Background

A significant turning point on its path to success has been reached for POWER SOFT (PVT) Limited, an up-and-coming force in the software development industry. With its continuous dedication to providing its clients with modern solutions, this recently developing company has potential for growth and innovation.

But despite its fast growth, the company has faced massive difficulties based on the weaknesses of its outdated network architecture. There are five different departments in the organization: Network Team, Sales, Finance, Information Technology, and Human Resources. One of the most significant challenges has been a lack of a merged secure network architecture. The organization has faced many challenges, including data breaches and network failures due to security weaknesses and the lack of redundancy measures.

The reliance on physical servers, which not only comes at high expense but also risks the company to potential data loss in the case of server failures, causes these problems. POWER SOFT has recognized the pressing need for change and is organizing its network infrastructure with the exclusive goal of improving reliability, security, and redundancy. The organization hopes to establish a network environment that protects confidential data and ensures continuous operations by utilizing cutting-edge technologies and modern techniques.

The main goal of this massive project is to provide workers with a network infrastructure that is secure, redundant, and reliable, which will act as a foundation for growth and achievement inside the company. POWER SOFT is well-suited to mark the beginning of the next phase of technological innovation and operational excellence as it embarks on this unique project.

Problem statement

Power Soft PVT (Limited) currently faces significant difficulties because of its outdated, insecure, and insecure network infrastructure. Frequent failures, slow reaction times, and security breaches have been ongoing problems that have severely impacted the organization's production and damaged its reputation. As a result of the network's fundamental limitations, employees are having difficulty accessing important assets and collaborating successfully.

Furthermore, there are sufficient security measures in the current infrastructure to protect the company's data and systems, which increases the possibility of security breaches and the compromise of private data. These vulnerabilities are made worse by the dependence on physical servers.

This bad situation not only affects customer satisfaction and operational effectiveness, but it also makes it more difficult for the company to meet current needs and plan for future growth. Therefore, in order to solve these critical issues and promote long-term development and financial success, Power Soft (PVT) Limited must immediately implement a comprehensive solution for updating its network infrastructure, ensuring reliability, redundancy, and security. [1]

Aim and Objectives

Aim:

The goal of this project is to create and put into place a network infrastructure that is scalable, redundancy dependable, and secure while also meeting the objectives of the business.

Objectives

- To improve departmental network capacity.
- To improve departmental network security.
- To increase the speed of the network.
- To maximize the efficiency of the network.
- To provide redundancy and protect company information.
- To create a new network architecture that meets with Power Soft (PVT)Limited's requirements, which include high-speed connectivity, centralized management, load balancing methods, redundancy techniques, and security features.
- To provide an appropriate cloud solution to the company

Scope of the project

The project's scope is to upgrade Power Soft PVT (Limited)'s network infrastructure in order to resolve current problems and get ready for future demands. For improved communication and cooperation, this also involves bringing together every department of the business into the updated network. To protect corporate data and systems against cyber-attacks and unauthorized access, security measures will be improved. One of the main goals in reducing downtime and improving user experience is to improve network speed and efficiency. [2]

To protect company data and ensure business continuity, reliable backup solutions will be put into place. To make the switch to the new network architecture less difficult, stakeholders will receive training. To ensure the effective completion of the project, a clear budget, schedule, and resource allocation will be established. The enhanced network infrastructure will be monitored and assessed for performance using procedures for quality assurance, and documentation will be kept for future review and analysis.

SWOT Analysis

Strengths:

- Improved communication and cooperation among departments.
- Enhanced security measures to protect corporate data.
- Focus on improving network speed and efficiency.
- Implementation of reliable backup solutions for data protection.

Weaknesses:

- Potential resistance from stakeholders to switch to the new network architecture.
- Disruption during the transition phase.
- Costs associated with upgrading and training.

Opportunities:

- Future-proofing the network for upcoming technological advancements.
- Improved efficiency and productivity due to better network performance.
- Potential for cost savings through optimized resource allocation.

Threats:

- Cybersecurity threats and risks associated with unauthorized access.
- Disruption to business operations during the upgrade process.
- Potential for budget overruns or delays in project completion.

Chapter 2 - Literature review

Introductory paragraph

A critical and comprehensive analysis of the corpus of knowledge already published on a particular topic or issue is what a literature review involves. This method includes discovering, assessing, and creating books, published research studies, and other sources that are relevant to the present study issue or topic. A literature review frequently aims to highlight any gaps, contradictions, or inconsistencies in the corpus of information currently available on a particular topic. It may also involve identifying key ideas, theories, techniques, or topics that have been used in the literature and evaluating the benefits and drawbacks of each. [3]

VLAN and Network Management

This paper provides an overview of VLAN technology, including its operation as well as the many kinds of VLANs and their proper placement inside networks. A few real-world networks are presented, along with some of the typical issues those conventional architectures bring. Next, the author adds switches to those problematic networks and studies the impact. [4]

Designing network protocols for good equilibria

This web articles provides me about the goal of this work is to optimize equilibrium behavior, specifically in cost-sharing games, in networks containing selfish users. The collection of Nash equilibria is strongly influenced by the edge cost-sharing protocols selected. Previous research has focused on the Shapley protocol, which divides edge costs equally across users. [5]

Design and Reliability Analysis of a Novel Redundancy Topology Architecture

This paper provides insights into the design of a novel redundancy topology and its analysis of structural robustness, redundant paths between two terminal nodes, and proposed topology reliability through the use of natural connectivity and time-independent and time-dependent terminal pair reliability.[6]

A Review on Network Security

I learned about networks from this paper. A network administrator adopts rules, policies, and procedures under the notion of security to prevent the misuse of resources that are accessible through the network. This makes security a crucial idea. Due to the variety of work that is done on both public and private networks, such as transactions, commercial communications, and government organizations, it is essential. Network security is now necessary to shield data from viruses and other dangers.

Dynamic Host Configuration Protocol

This Journal introduced me to the concept of Dynamic Host Configuration Protocol (DHCP), which uses the network to provide workstations with TCP/IP addressing information (see IETF draft standard RFC 2131, 2132, and 3397). The network address, subnet mask, gateway, and DNS server address are the most often specified parameters using DHCP. Regarding DHCP, this includes the domain name, time server, and numerous other things.[7]

A Comparative Study on Routing Protocols: RIP, OSPF and EIGRP and Their Analysis Using GNS-3

This paper made me think about using a variety of routing protocols, including IGRP, OSPF, RIPv1, RIPv2, and EIGRP. Every routing protocol routes packets in a different way. In this work, the RIP, OSPF, and EIGRP protocols are compared in a basic manner. A packet's optimal path is determined by the RIP using a distance vector algorithm, the OSPF using a link state algorithm, and the EIGRP utilizing diffusing update techniques. To determine the optimal protocol for packet routing, we are comparing and evaluating the performance of several routing protocols, including RIP, OSPF, and EIGRP, in this study.[8]

A Systematic Literature Review on Penetration Testing in Networks

This article induced me to think about the process of security assessment, which identifies risk areas and weaknesses that jeopardize network security. so, shielding the network from dangers and weaknesses that could lead to an attack. Therefore, in order to determine how to lessen their risks, it is necessary to identify the vulnerabilities as well as the threats that could take advantage of them. This study identifies and discusses the ports that are at risk.[9]

Cloud Computing Architecture: A Critical Analysis By IEEE

This paper taught me about Many different cloud architectures are present and many more are continually developing. The three main ones, which can be implemented on private, public, communal, and hybrid clouds, are SaaS, PaaS, and IaaS. Additionally, this paper looks at recent advancements in cloud computing architecture and offers suggestions for further study. Journal articles, conference proceedings, and white papers were examined. The current work's goal is to recognize, investigate, and elucidate the trends and advancements in cloud computing architecture.[10]

How to design and build a data center

This essay made me consider how the data center serves as the technological center of contemporary business operations. The vital IT infrastructure required to supply resources and services to clients, partners, and workers worldwide is provided by the data center.[11]

A closet or other easily accessible space can frequently house a functional "data center" for a small or medium-sized company with minimal, if any, alterations. But because of the sheer size of enterprise computing, it requires a sizable, specially planned area to accommodate the space, power, cooling, management, dependability, and security requirements of the IT infrastructure.

Amazon Web Services

This webpage inspired me to think about The hardware and software resources that comprise cloud infrastructure are what make up the cloud. Cloud providers manage worldwide data centers that contain hundreds of computers, physical storage devices, networking equipment, and other IT infrastructure components. They use various operating system configurations to set up the physical devices. They also install various kinds of software needed for the proper operation of an application. Pay-as-you-go cloud infrastructure leasing allows your business to cut costs dramatically compared to buying and maintaining separate components.[12]

Microsoft Azure

The article introduced me to Microsoft's public cloud platform, Azure. Azure provides a wide range of services, such as managed database services, infrastructure as a service (IaaS), and platform as a service (PaaS).[13]

This post helped me better comprehend servers. Now, let's have a look at the datacenter's hardware architecture. Several servers are arranged in server racks inside each datacenter. A network switch and numerous server blades are found in every server rack. These offer power generation via a power distribution unit (PDU) and network access. Occasionally, racks are arranged into bigger groups called clusters. The user's virtualized hardware instances are run on server racks, often known as clusters. Nonetheless, a fabric controller, a type of cloud management software, is installed on some servers. [14]

A Review on Amazon Web Service (AWS), Microsoft Azure & Google Cloud Platform (GCP) Services

This research study gave me some insight into the cloud computing services sector, including the pricing strategies and models that companies use to gain a competitive edge. Because of this advanced technology, end users now have access to a wide range of services and resources. [15]

However, the number of cloud service provider businesses has also increased quickly, leading to increased competition in the market. It provides a quick overview of cloud computing's history, its application in business, its main suppliers, and their pricing strategies. This study investigates three prominent market participants in-depth, paying particular attention to their pricing strategies.

I learned from this paper how to critically examine the competitive pricing and service strategies used by different cloud service providers to gain a competitive edge. In addition to meeting organizational goals and client needs, cloud service providers want to make more money. suppliers of cloud services offering infrastructure, software, testing, security storage, and storage.[16]

A Literature Review on Cloud Computing Adoption Issues in Enterprises

This paper addresses the major concerns surrounding the adoption of cloud computing today through a methodical analysis of literature.

Additionally, concerning Articles are categorized into eight primary groups using the grounded theory approach: internal, external, evaluation, proof of concept, adoption decision, implementation and integration, IT governance, and confirmation. Next, two abstract categories—cloud computing adoption factors and processes—are created from the eight categories. The former influences the latter. The review's findings show that before choosing to use cloud computing, businesses must consider several important factors.

Chapter 3 Analysis

Analysis of the current system.

Security Vulnerabilities and Data Risks:

Lack of a proper data server exposes the network to various risks such as data leakages, malware infections, hacking attempts, and unauthorized access.

A proper server is essential for securing data access and managing network traffic effectively.

Network Failures:

Poor network architecture increases the likelihood of network outages and performance issues.

Lack of redundancy and fault tolerance exacerbates the impact of hardware failures or network outages.

Security Steps Required:

To reduce weaknesses and errors, the business needs to put strong security measures in place. This entails putting in place network monitoring tools and protecting the network infrastructure.

In conclusion, appropriate security protections and network resilience are absent from the architecture of the current system. Ensuring the security and dependability of Power Soft's internal network requires addressing vulnerabilities and strengthening security methods, as well as implementing a strong data server and optimizing network architecture with redundancy and fault tolerance.

Requirement

User/ Client requirement

Enhanced Security:

To guard against possible threats, users need a network architecture that prioritizes security, which includes strong port security setups, Access Control Lists (ACLs) customized for specific departments, and cloud servers.

Reliability and Availability:

To sustain continuous daily operations, users want a network that guarantees optimum uptime and availability. This incorporates redundancy measures like routing using Rip version 2 and ether channeling with Link Aggregation Control Protocol (LACP).

High-Speed Performance:

Users count on the network to provide them with dependable high-speed performance, which is attained by carefully allocating bandwidth, configuring Quality of Service (QoS), and using load balancing techniques.

3.1.1. Functional requirements

Network Architecture Design:

Security, redundancy, and scalability must be given top priority in the carefully planned network architecture. One example of this is the integration of hierarchical design with Azure cloud servers.

Implementing Security Measures:

To protect the network from possible threats, implement security measures including port security configurations, Access Control Lists (ACLs) customized for specific departments, and cloud servers.

Continuity and Redundancy Implementation:

To ensure optimal uptime and availability, redundancy methods such as Link Aggregation Control Protocol (LACP) for ether channeling, Rip version 2 for routing, and integration of cloud storage accounts are implemented.

QoS Configuration and Bandwidth Allocation: To ensure consistent high-speed network

performance, bandwidth should be allocated appropriately and QoS parameters should be configured.

Non-Functional requirements

Scalability:

The network infrastructure must be scalable to accommodate future growth and evolving organizational needs.

Security: security focuses on ensuring that the system protects data and resources from unauthorized access, malicious attacks, and other security threats. It includes measures such as authentication, authorization, encryption, and data integrity checks to maintain confidentiality, integrity, and availability of the system and its data.

Redundancy: Redundancy in non-functional requirements refers to the system's ability to continue operating even in the event of hardware or software failures. It involves the use of backup systems, data replication, and failover mechanisms to ensure uninterrupted service and minimize downtime. Redundancy helps improve reliability, fault tolerance, and availability of the system.

Software specification

- Microsoft Azure Portal
- Network Monitoring software: Zabbix, ntopng.
- File sharing software: Truenass.

Hardware specifications

- Routers
- Switches
- PCs
- server

Feasibility study

Time feasibility

Time feasibility evaluates whether the project can be finished in the allotted amount of time. It entails assessing the timeline, benchmarks, and deadlines of the project to make sure they are reasonable and attainable. To ascertain whether the project can be finished on schedule, variables including resource availability, project complexity, and potential risks are considered.

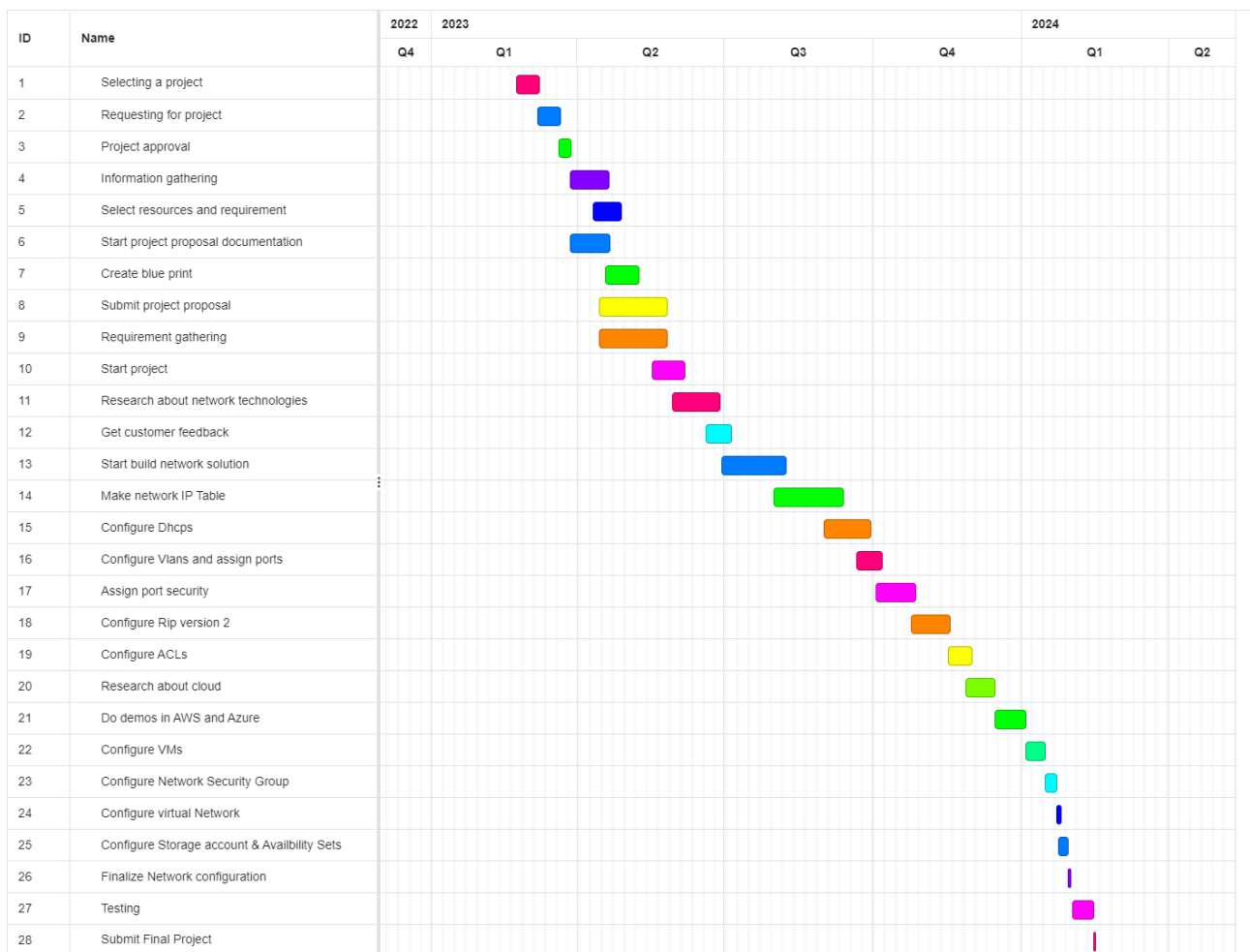


Figure 1 Grantt chart

Cost feasibility

Cost feasibility assesses the project's budgetary restrictions and financial viability. It entails projecting the whole cost of the work, considering labor, materials, resources, and other costs. Cost feasibility guarantees that the project can be finished within the allotted budget and that it is economically justified.

| No: | Hardware Name /Software name | Per unit | cost | Quantity | Total Cost |
|-----|------------------------------|-------------|------|--------------|---------------|
| 1 | PCs | LKR 48000 | | 32 | LKR 1,536,000 |
| 2 | 2960-24tt switch | LKR 332,500 | | 2 | LKR 665,000 |
| 3 | Multilayer Switches 3560 | LKR 92364 | | 2 | LKR 184,728 |
| 4 | Dhcp Server | LKR 616807 | | 1 | LKR 616,807 |
| 5 | 2911 Routers | LKR 22000 | | 3 | LKR 66,000 |
| 6 | Azure Cloud | LKR 39,130 | | For 6 Months | LKR 234,600 |
| 7 | Sub Total | | | | LKR 1,767,135 |

Table 1 Cost Tabl

Scope feasibility

Scope feasibility for POWER SOFT (PVT) Limited's network upgrade project involves assessing the project's overall objectives, deliverables, and requirements to determine if they align with the organization's goals and resources. Given the project's focus on upgrading network infrastructure to be scalable, stable, and secure, the scope feasibility should include:

Objectives: Clearly defined objectives, such as integrating Azure cloud servers, implementing security measures, and ensuring high-speed performance.

Deliverables: Tangible outcomes like a fully integrated and secure network infrastructure, with documented security measures, bandwidth allocation plans, and QoS settings.

Requirements: Detailed requirements for hardware, software, cloud services, and network components, ensuring they meet current and future needs.

Limitations: Determining the existence of any restrictions, whether financial limitations, schedule limitations, or resource accessibility.

Stakeholder Participation: participation of important stakeholders to guarantee that the project takes into account their requirements and expectations.

By evaluating these factors, one can ascertain whether the project scope is feasible, realistic, and in line with the strategic goals of the organization.

Technical feasibility.

Modern Approach: Using the scalability and flexibility of cloud technology to suit changing needs, the integration of Azure cloud servers into a hierarchical design is indicative of a modern approach.

Security Measures: A thorough plan to defend the network from potential attacks is demonstrated by the implementation of port security configurations, Access Control Lists (ACLs), Link Aggregation Control Protocol (LACP) for ether channeling, and Routing Information Protocol (RIP) version 2.

Observance of Detail: The network can efficiently manage high-speed performance needs if bandwidth allotment, Quality of Service (QoS) settings, and load balancing techniques are carefully considered.

Dependable Performance: The robust network design is aimed at providing reliable and consistent performance, critical for supporting the organization's operations.

Alignment with Best Practices: The project's technical aspects adhere to modern best practices, ensuring that the network infrastructure is optimized for efficiency and security.

Economic feasibility

Initial Investment:

Although cloud, software, and hardware services come with a hefty initial cost, these expenses should be offset in the long run.

Long-Term Benefits:

By decreasing downtime and increasing productivity, the network upgrade will improve operational efficiency.

Cost Savings:

The company can save money on maintenance, upgrades, and possible downtime by putting in place a scalable, reliable, and secure network infrastructure.

Futureproofing:

By focusing on maintaining competitiveness and adjusting to technological advancements, the project makes sure that the investment will continue to be worthwhile and relevant over time.

Stakeholder Collaboration: Working together with stakeholders increases the chance that the project will be implemented successfully by ensuring that it satisfies organizational needs.

Methodology and planning artifact

The following could be part of the planning artefacts and approach for POWER SOFT (PVT) Limited's network infrastructure upgrade,

Evaluation and Scheduling:

- Analyze the infrastructure of the network as it is now.
- Define the project's scope and identify areas that need work.
- Create a thorough project plan that includes deadlines and resource allocation.

Architecture and Design:

- Create a new network architecture by referring to the specifications.
- Think about redundancy, security, and scalability.
- Make thorough network documentation and diagrams.

Choosing Hardware and Software:

- Pick servers, switches, and routers that are the right gear.
- Select software programs for monitoring, security, and network administration.

Execution:

- Install and set up newly purchased hardware and software.
- To guarantee functioning and compatibility, thoroughly test the system.
- Put intrusion detection systems, firewalls, and encryption into practice as security measures.

Instruction and Shift:

- Train IT employees on new processes and technology.
- Reduce downtime by seamlessly switching from the old network to the new one.
- Observation and Enhancement:
 - Keep an eye on network security and performance all the time.
 - Adjust network configurations for optimal dependability and efficiency.

Record-keeping and Evaluation:

- Keep thorough records of the newly installed network infrastructure.
- Review performance often in order to pinpoint areas that need work.
- POWER SOFT (PVT) Limited may guarantee a successful network infrastructure upgrading project that satisfies its present and future business needs by adhering to these comprehensive measures

Chapter 4 Design

Network Design

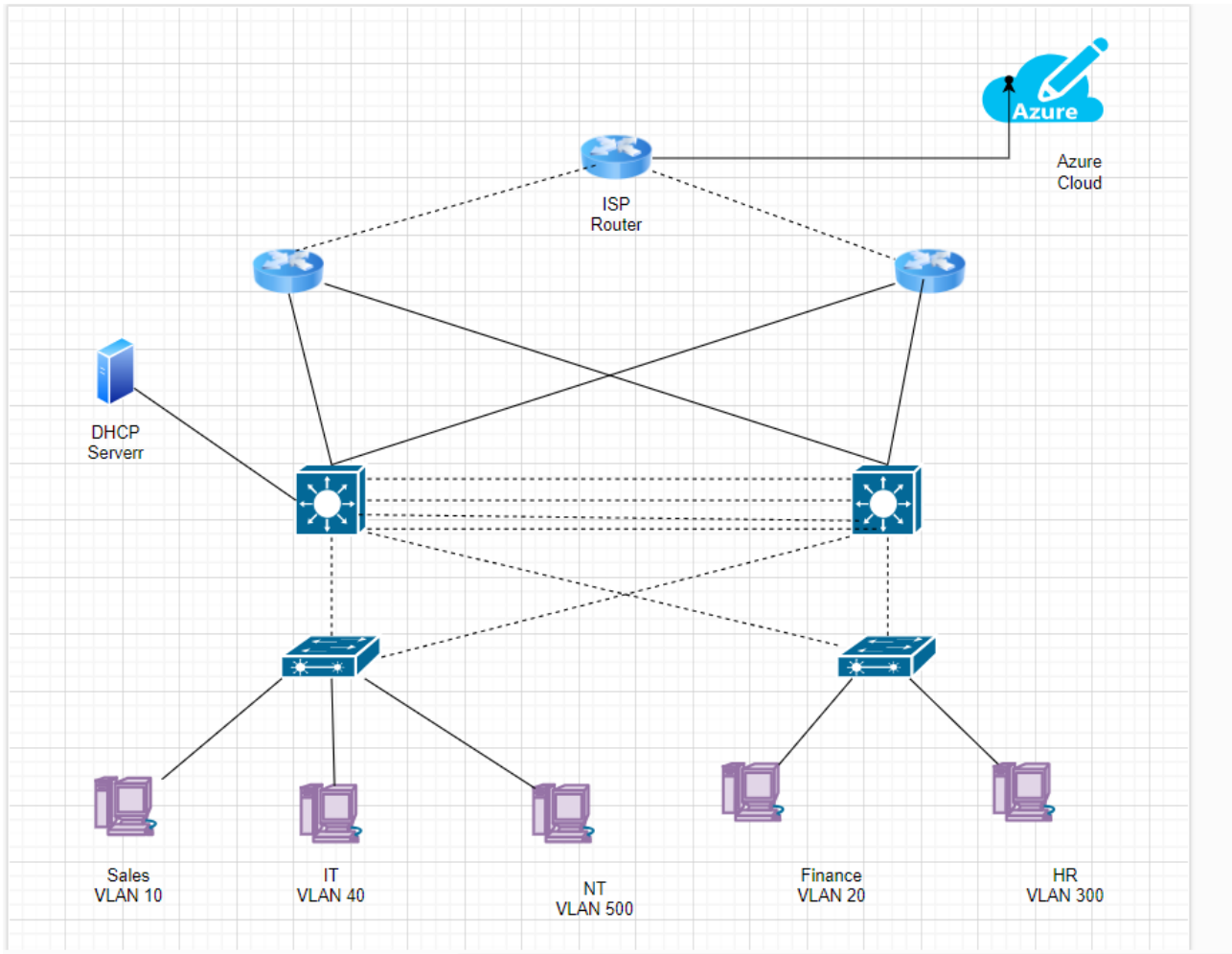


Figure 2Network Design

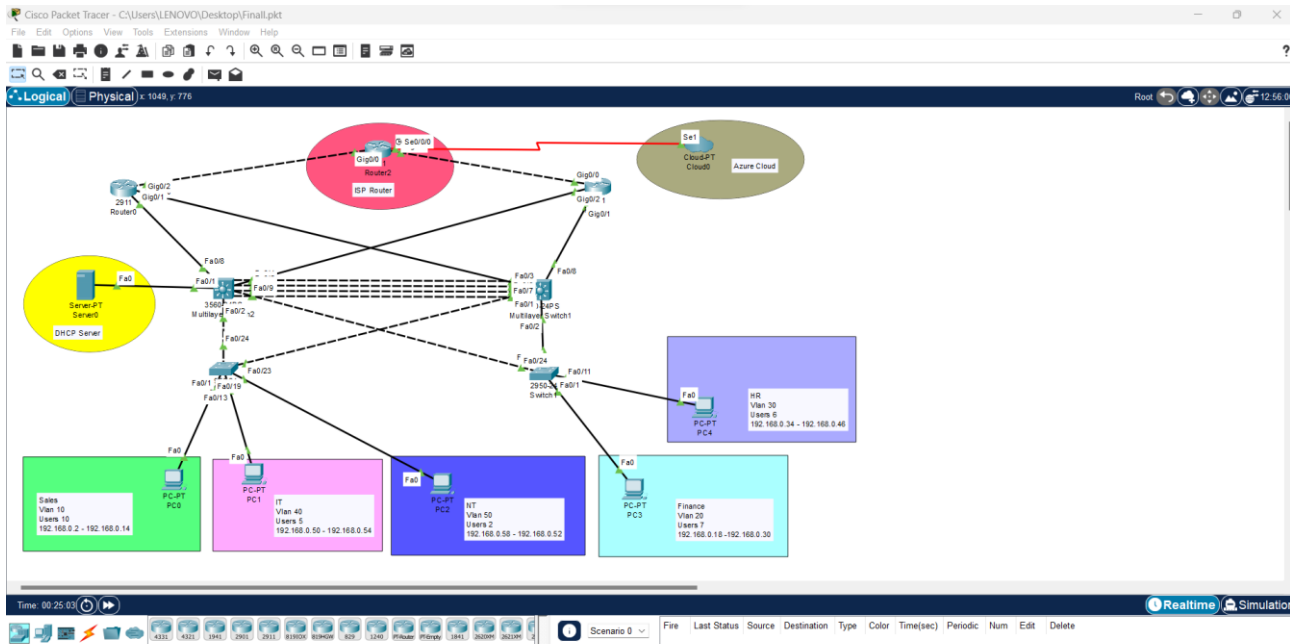


Figure 3Packet tracer

This image is about the network design architecture, and I have 1 other design as well. I have divided the network into three layers in this design: access, distribution, and core. To ensure effective network operations, each layer serves a certain function.

To improve security and isolate traffic for each department, I have set up VLANs at the access layer. Along with assigning ports to PCs, I also put port security mechanisms in place on the second layer switches.

I have set up multilayer switches with sub interfaces and LACP EtherChannel for redundancy in the distribution layer. Between the multilayer switches and the second layer switches, tunnelling is employed. To further handle IP address assignments, a DHCP server with DHCP pools is linked to the multilayer switches.

Finally, I have configured three routers at the core layer: one for the Internet Service Provider and two for internal network routing. These routers have ACLs set up for security and use RIP version 2 for routing. SSH connections are used to link the network to the Azure cloud, allowing for easy integration with cloud applications.

All things considered, this design guarantees a safe, expandable, and effective network infrastructure customized to meet the unique requirements of every department.

Cloud Design

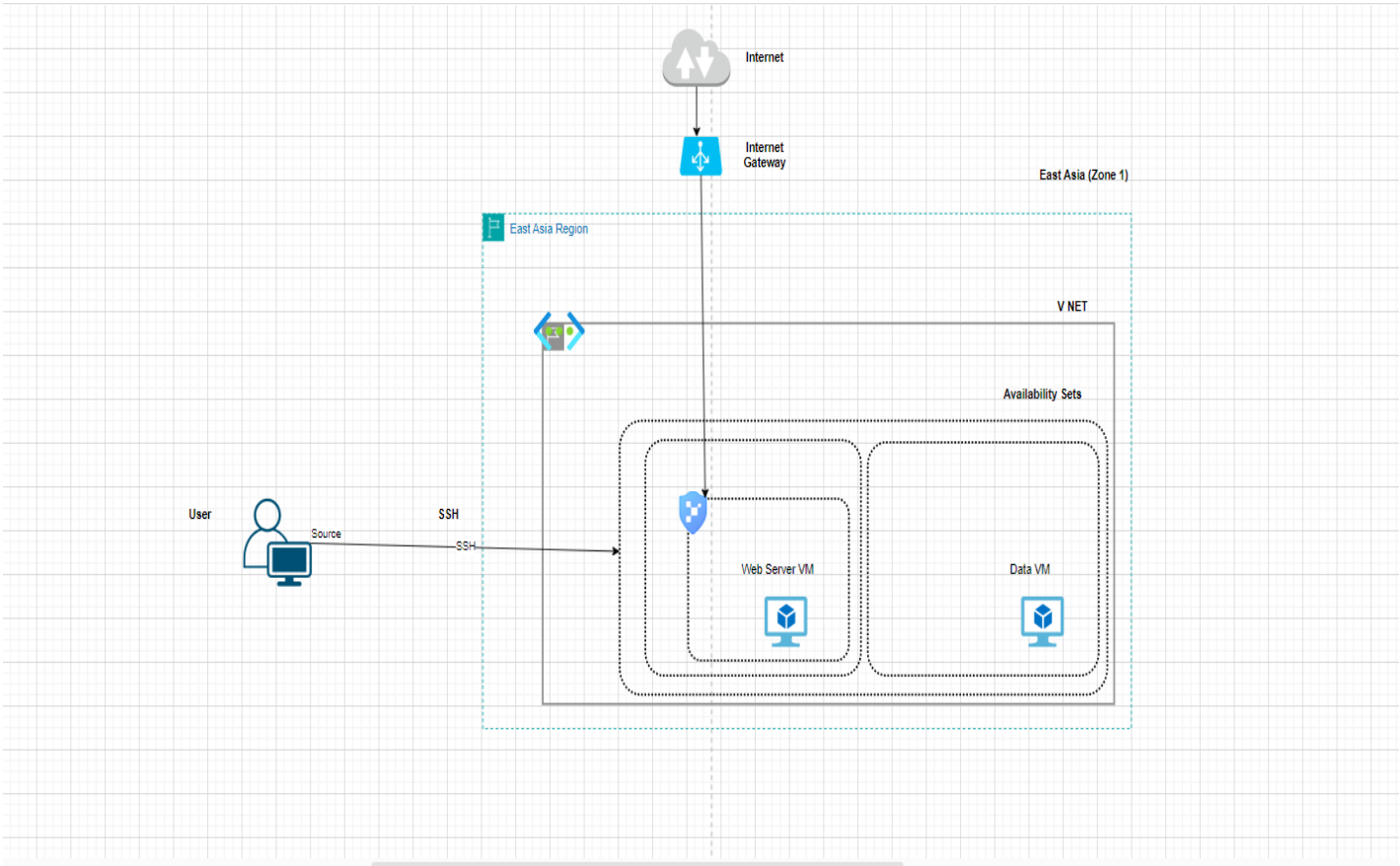
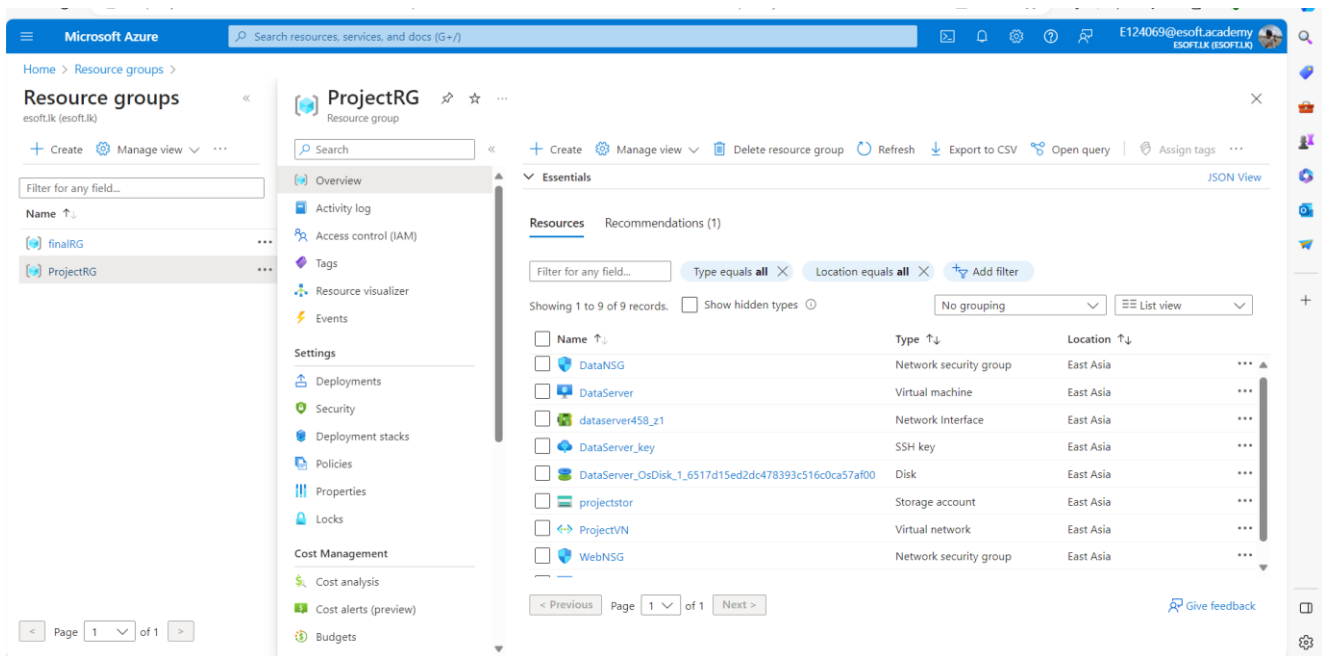


Figure 4 Cloud Design



In my design, I've structured the network architecture for Power Soft Pvt Ltd using Azure cloud services, focusing on cost-effectiveness, scalability, redundancy, and security. This solution was devised to address the challenges faced by the existing physical data server in terms of data redundancy, security, and efficiency.

The design features two virtual machines, one for the web server and another for the database server. The web server VM is configured to connect exclusively to the internal network using SSH protocol. However, it also has external connectivity to the internet for HTTP communication.

To ensure high availability and fault tolerance, both the Data VM and Web Server VM are placed in the same availability zone within the East Asia 1 region. Additionally, each VM is configured with availability sets, ensuring that if one server fails, there is a failover mechanism in place.

Privacy and security are paramount, which is why I've implemented ACLs using network Security Groups for both the Data and Server VMs. Despite being exposed to the internet, the web server VM is protected by Microsoft Defender, offering defense against malware and other cyber threats.

Figure 5 Azure Portal

Looking ahead, the design includes plans for integrating Azure monitoring tools to enhance monitoring and management capabilities, ensuring the continued security and efficiency of the server infrastructure.

Development Tools

Cisco packet tracer

Cisco Systems created a network simulation program called Cisco Packet Tracer (Packet Tracer) that allows users to replicate network configuration, design, and troubleshooting scenarios. It is frequently used by networking experts to test and verify network designs, as well as in educational settings for networking courses and training programs.

Users can drag and drop network devices, such as routers, switches, and computers, and connect them to mimic a network using Packet Tracer's graphical user interface (GUI). It also provides a command line interface (CLI) through which users can configure devices using Cisco IOS commands.

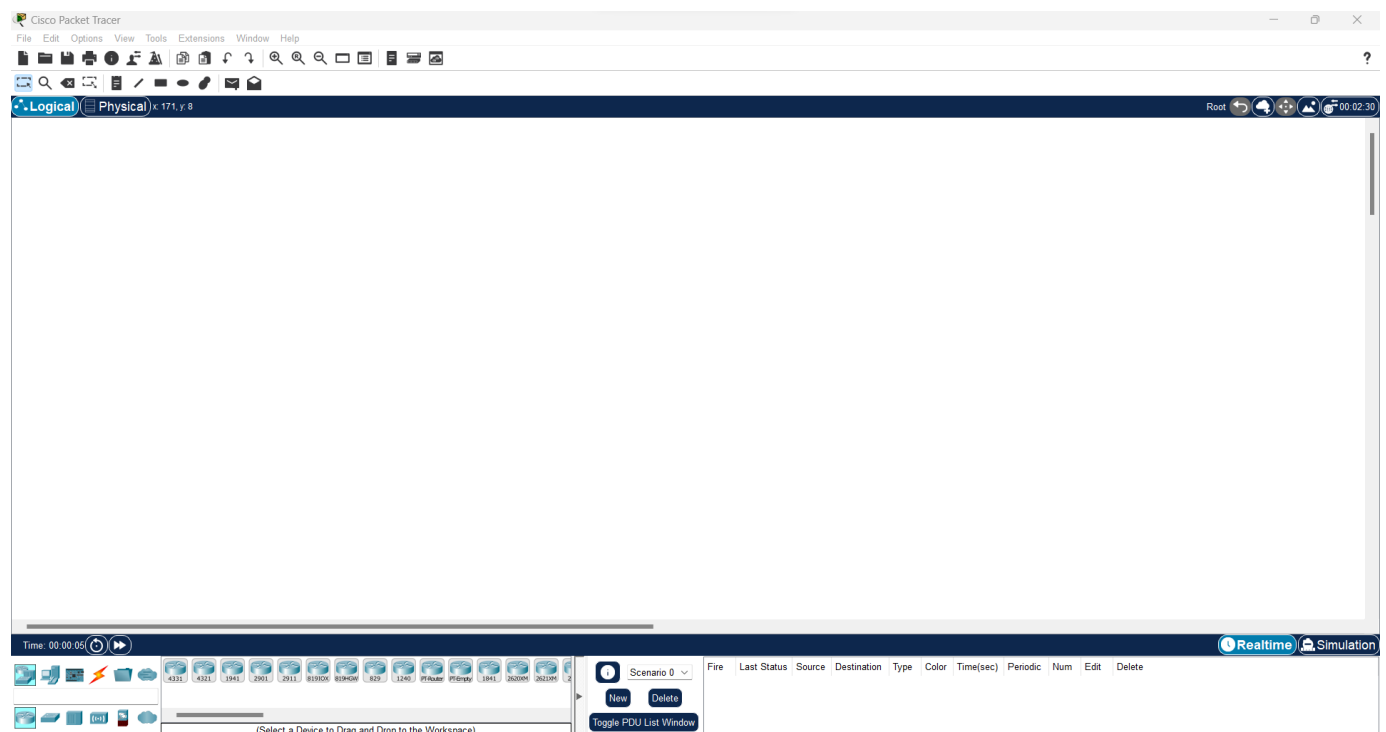


Figure 6Packet tracer

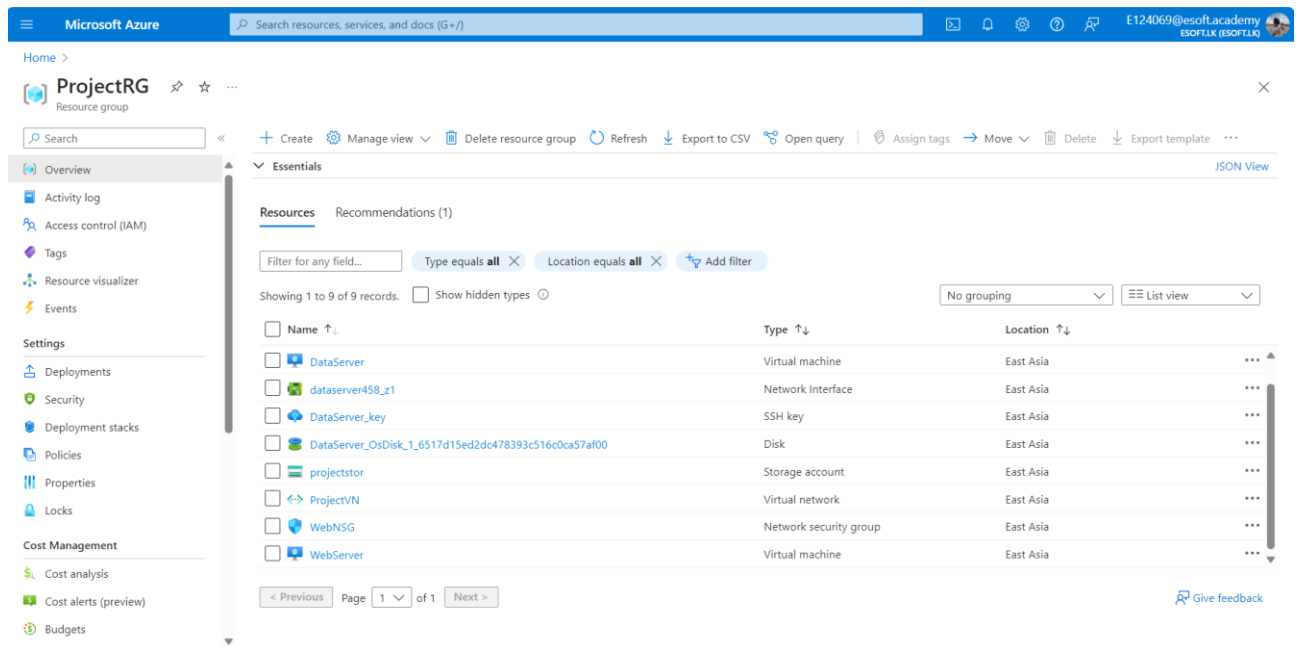
Chapter 5 Implementation

POWER SOFT PVT Limited's new network infrastructure project will be implemented in a physical environment that includes routers, switches, PCs, and a DHCP server. These devices will be situated in the customer information center or other appropriate locations according to planning specifications.

The cloud infrastructure will be based on Azure Cloud, with a proper subscription in place. Software components will include operating systems, network management software, security software, and other necessary programs, all integrated to ensure proper functionality. Compliance and security measures will be implemented, with adherence to industry standards and best practices, and regular updates and patches.

The network infrastructure will be thoroughly tested before deployment, with deployment in phases to minimize disruptions. Monitoring and maintenance will include the implementation of monitoring tools for real-time performance and security monitoring, as well as regular maintenance and updates to keep the network infrastructure secure and efficient.

Cloud Configurations



The robust web-based Microsoft Azure Portal gives users the ability to efficiently and unified manage their Azure services and resources. With its extensive dashboard, customers can access, track, and manage all of their Azure resources from one place.

The user-friendly interface of the Azure Portal is one of its primary benefits, since it facilitates quick navigation and resource discovery for users. The portal's several components, including Home, Dashboard, Virtual Machines, App Services, and Storage, facilitate user discovery and resource management.

A plethora of tools and features are available on the Azure Portal to assist users in efficiently managing their resources. The user-friendly interface of the portal makes it simple for users to manage storage accounts, create and deploy virtual machines, and change network settings. The site also offers warnings and real-time monitoring to assist customers in tracking their performance and resource utilization.

The Azure Portal's ability to integrate with other Azure services and tools is one of its main benefits. It is simple for users to manage their whole Azure environment from a single interface by having direct access to services like Azure Active Directory, Azure Security Centre, and Azure DevOps via the portal.

The customization options offered by the Azure Portal is another noteworthy feature. It is simpler for users to monitor and manage their Azure environment when they can personalize their dashboard to show the data and resources that matter most to them.

To sum up, the Azure Portal is an effective solution that gives users a thorough and intuitive interface for controlling the resources and services they utilize on Azure. Because of its ease of use, customization options, and connectivity with other Azure services, it's a vital tool for Azure users trying to efficiently manage their resources.

Resource Group Configuration

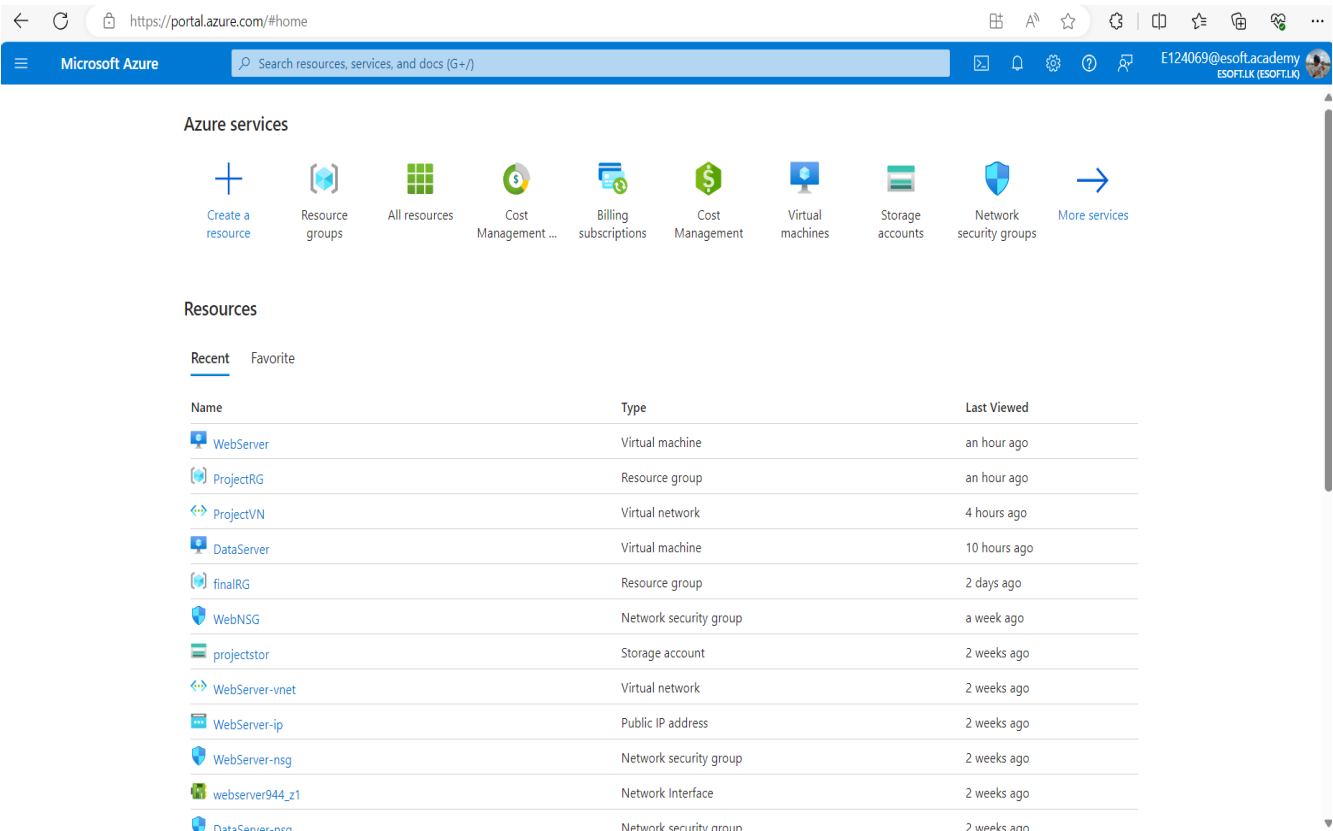


Figure 7RSG

Resource Group: Project Rg
Region: East Asia, Zone 1
Resources:

Data Server VM
Web Server VM
Data Network Security Group (NSG)
Web Network Security Group (NSG)

Virtual Network

In this configuration, the resources are grouped under a single resource group (Project Rg) for easier management and organization. The choice of East Asia, Zone 1 as the region ensures that the resources are in a specific geographical area for optimal performance and compliance with data residency requirements.

The Data Server VM and Web Server VM are virtual machines serving specific purposes, such as hosting data and web applications. The Data NSG and Web NSG are used to define network security rules that control inbound and outbound traffic to and from the virtual machines, enhancing the overall security posture of the environment. Finally, the Virtual Network provides the network connectivity and isolation needed for the VMs to communicate with each other and the external world while maintaining a secure environment.

This setup demonstrates a well-organized and secure infrastructure design that meets the needs of hosting data and web services in the specified region.

Darta Server Virtual Machines

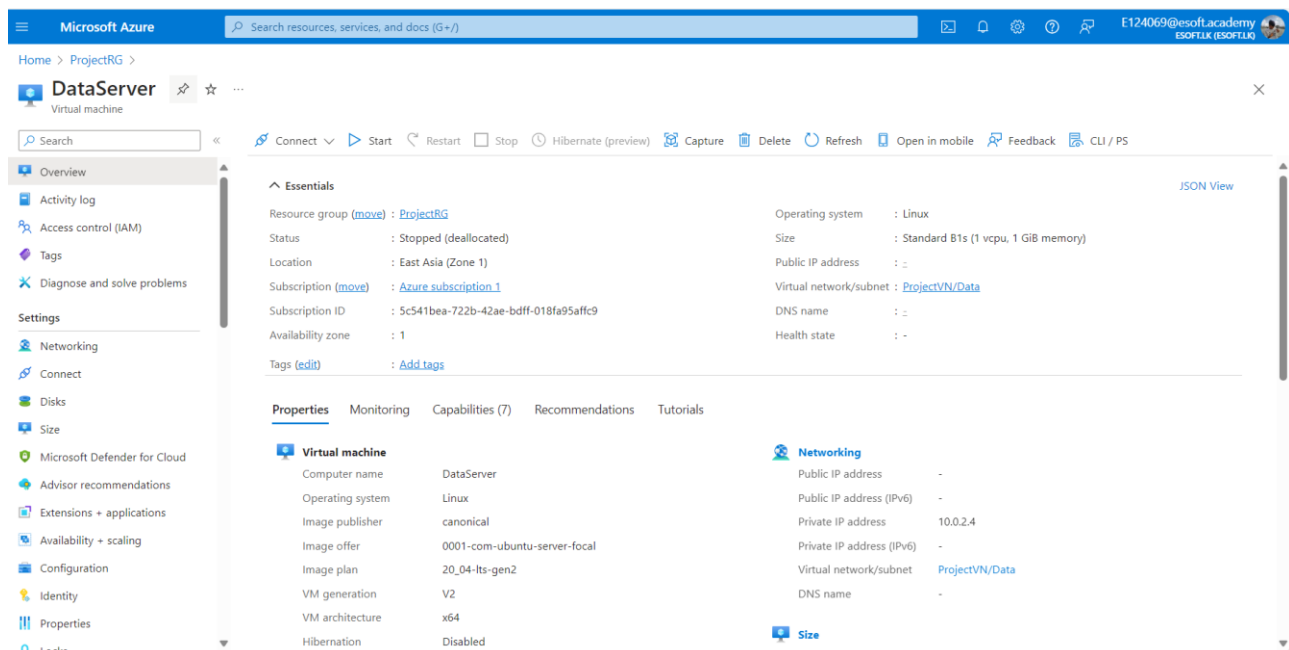


Figure 8Web server

Azure Virtual Machines (VMs) are a key component of Microsoft Azure's infrastructure as a service (IaaS) offering, allowing you to deploy and manage virtualized computing resources in the cloud. Your deployment in East Asia, Zone 1 exemplifies Azure's global availability, providing redundancy for high availability.

Your choice of Linux as the operating system showcases Azure's flexibility, supporting a wide range of OS

options. The use of a Standard B1s VM size (1 vCPU, 1 GiB memory) demonstrates Azure's scalability, allowing you to choose resources that match your workload requirements.

The deployment within the WebServer-vnet virtual network and the use of a private IP address (10.2.0.4) highlight Azure's networking capabilities, providing secure communication within a defined network environment. Additionally, the assignment of a public IP address (20.205.16.139) showcases Azure's ability to expose services to the internet when needed.

Overall, Azure Virtual Machines offer a flexible, scalable, and reliable solution for hosting a variety of workloads, with features that cater to both basic and advanced computing needs.

Web Server Virtual Machines

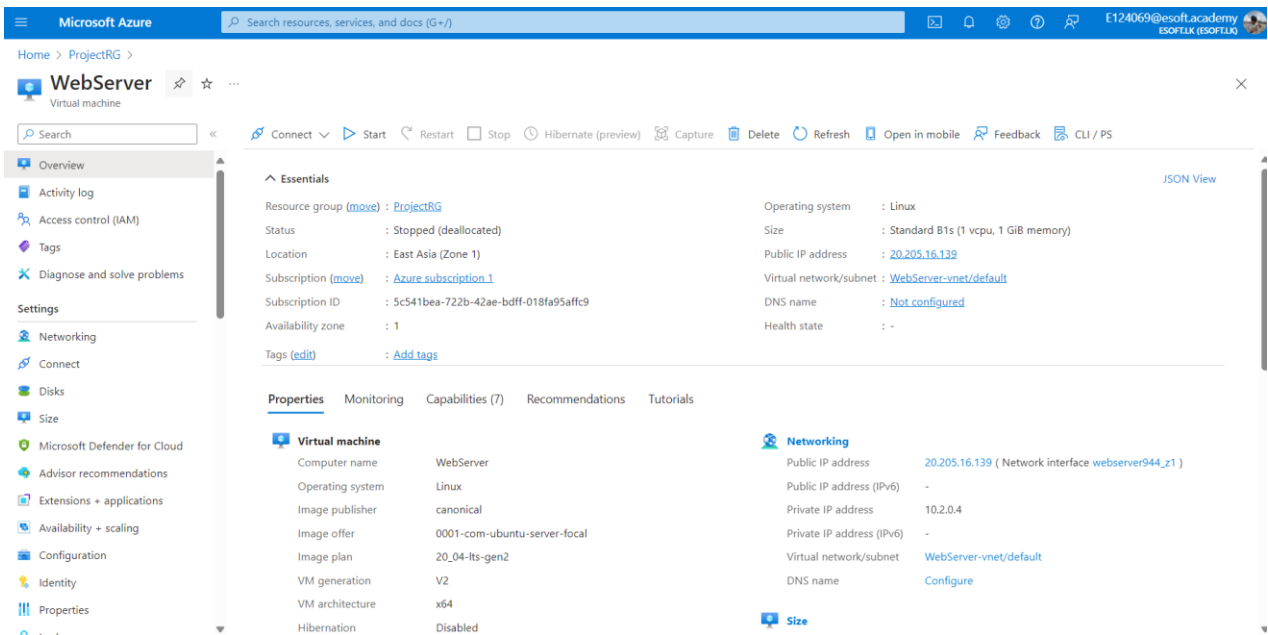


Figure 9WEB

Azure Virtual Machines (VMs) provide on-demand, scalable computing resources in the cloud, enabling you to run applications and services without the need to manage physical hardware. Your deployment in East Asia, Zone 1, exemplifies Azure's global reach, allowing you to place resources close to your users for better performance.

Your choice of Linux as the operating system showcases Azure's support for a wide range of OS options. The use of a Standard B1s VM size (1 vCPU, 1 GiB memory) demonstrates Azure's flexibility, providing cost-effective options for various workloads.

The deployment within the WebServer-vnet virtual network and the assignment of a private IP address (10.0.2.4) highlight Azure's networking capabilities, allowing you to create isolated environments for your VMs. Additionally, by creating a redundant setup, you ensure high availability for your applications, minimizing downtime.

Overall, Azure Virtual Machines offer a reliable, flexible, and scalable solution for hosting a variety of workloads, with features that cater to both basic and advanced computing needs.

Microsoft defender Configuration (pending)

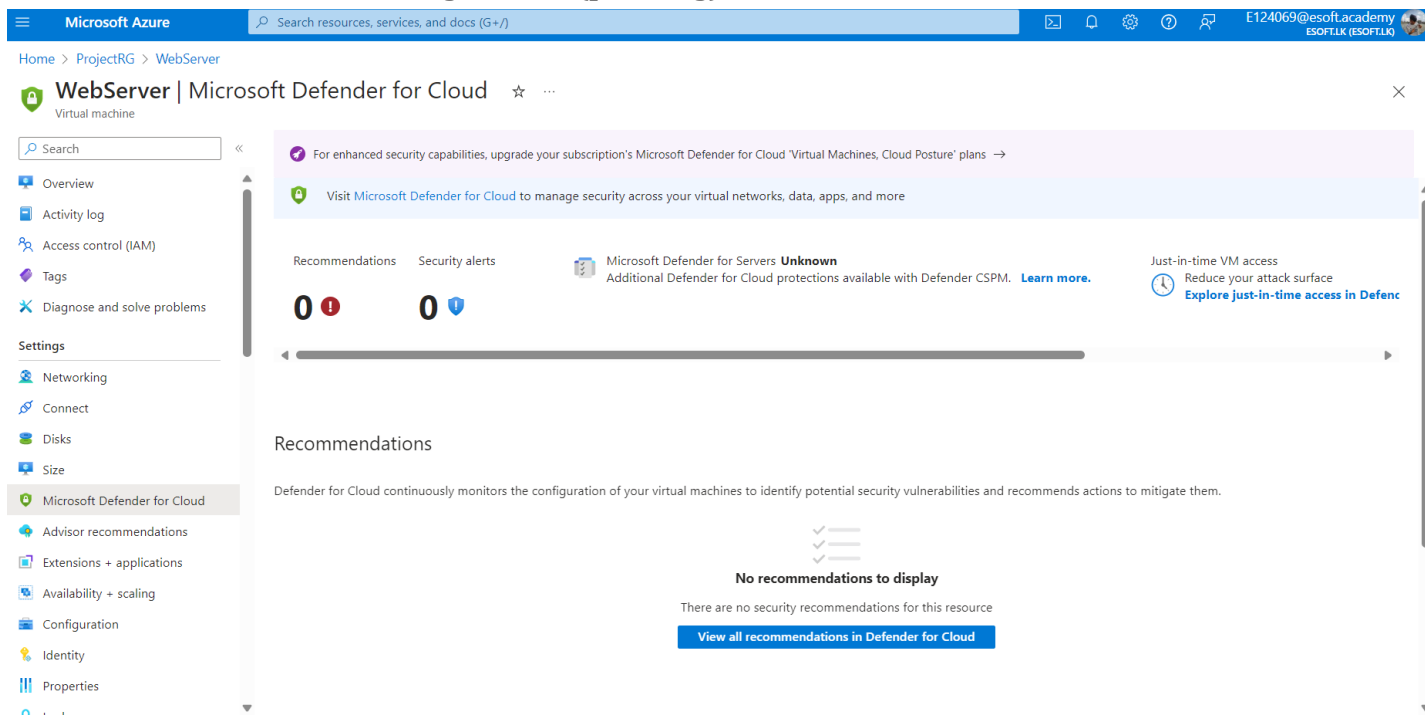


Figure 10Defender

Microsoft Defender for Cloud, previously known as Azure Security Center, is a comprehensive security solution designed to protect cloud workloads.

It offers threat protection, security posture management, and advanced capabilities to detect, investigate, and respond to threats across hybrid cloud workloads.

Defender provides unified security management experience, enabling you to monitor and improve the security of your Azure resources. As a cloud-native application protection platform (CNAPP), Defender integrates with Azure services to provide enhanced security for your cloud environment.

Virtual Network

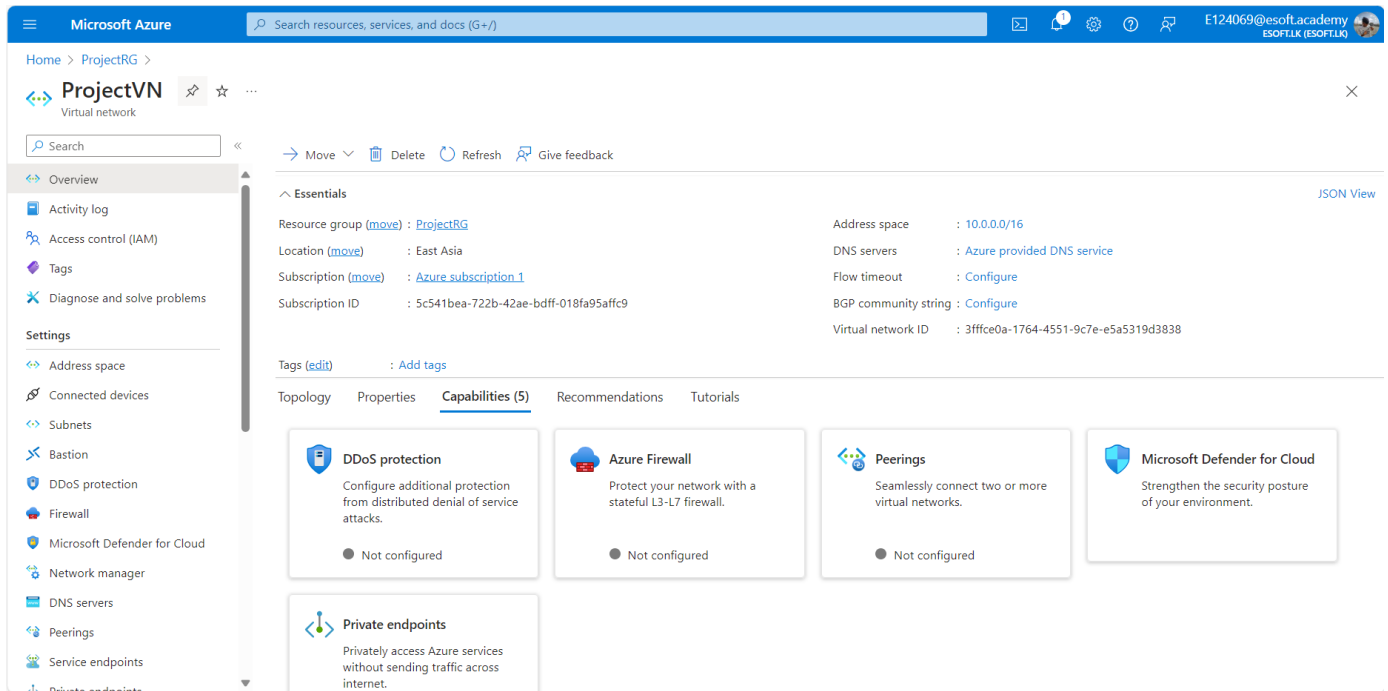


Figure 11V

Azure Virtual Network (VNet) is a foundational service in Azure that allows you to create your own private network in the cloud. It enables you to securely connect Azure resources, such as virtual machines (VMs), to each other, to the internet, and to on-premises networks.

With Azure Virtual Network, you can define your own IP address space, create subnets, and control inbound and outbound traffic using network security groups (NSGs) and route tables. It provides isolation and segmentation for your Azure resources, allowing you to design and implement your network architecture according to your specific requirements.

Azure Virtual Network is essential for building secure, scalable, and interconnected cloud-based applications and services.

Data Network Security Group

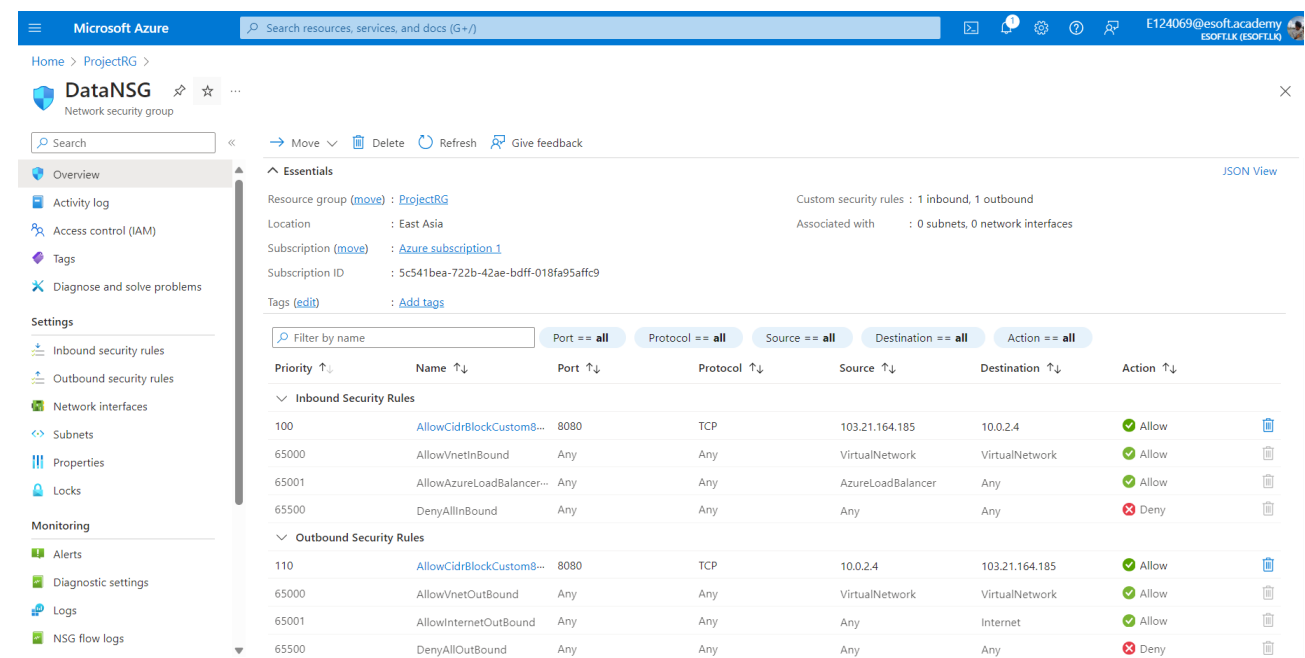


Figure 12Data NSG

Azure Network Security Groups (NSGs) are a fundamental element of Azure's network security. They act as a virtual firewall for controlling inbound and outbound traffic to network interfaces, VMs, and subnets in an Azure Virtual Network. NSGs contain security rules that allow or deny traffic based on factors such as source IP address, destination IP address, port, and protocol.

In your scenario, you created a Data Network Security Group for your Data VM. This NSG is configured to allow inbound traffic on port 8080, using the TCP protocol, from a specific source IP address (103.21.164.185) to a specific destination IP address (10.0.2.4). This configuration ensures that only traffic meeting these criteria is allowed to access the Data VM over SSH, restricting access to the internal network.

Web Server Network Security Group

The screenshot displays the Azure portal interface for a Network Security Group (NSG) named 'WebNSG'. The left sidebar shows the navigation menu with categories like Overview, Settings, and Monitoring. The main content area is divided into 'Essentials' and a table of security rules.

Essentials:

- Resource group (move): [ProjectRG](#)
- Location: East Asia
- Subscription (move): [Azure subscription 1](#)
- Subscription ID: 5c541bea-722b-42ae-bdff-018fa95affc9
- Tags (edit): [Add tags](#)
- Custom security rules: 1 inbound, 1 outbound
- Associated with: 0 subnets, 0 network interfaces

Security Rules Table:

| Priority | Name | Port | Protocol | Source | Destination | Action |
|--------------------------------|-------------------------------|------|----------|-------------------|----------------|--------|
| Inbound Security Rules | | | | | | |
| 100 | AllowAnyHTTPEndpoint | 80 | TCP | Any | 10.2.0.4 | Allow |
| 65000 | AllowVnetInBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | AllowAzureLoadBalancerInBound | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | DenyAllInBound | Any | Any | Any | Any | Deny |
| Outbound Security Rules | | | | | | |
| 110 | AllowCidrBlockCustom8080 | 8080 | Any | 10.2.0.4 | 103.21.164.185 | Allow |
| 65000 | AllowVnetOutBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | AllowInternetOutBound | Any | Any | Any | Internet | Allow |
| 65500 | DenyAllOutBound | Any | Any | Any | Any | Deny |

Figure 13 Web NSG

Azure Network Security Groups (NSGs) are essential for controlling network traffic to and from Azure resources. They act as virtual firewalls with a set of rules that allow or deny traffic based on factors like source IP address, destination IP address, port, and protocol.

In your scenario, the Web Network Security Group for the Web server VM allows inbound traffic on port 80 using the TCP protocol from any source IP address to a specific destination IP address (10.2.0.4). This configuration enables the Web server VM to access the internet using Windows Defender while allowing SSH connections for internal network access.

Storage Account Configuration

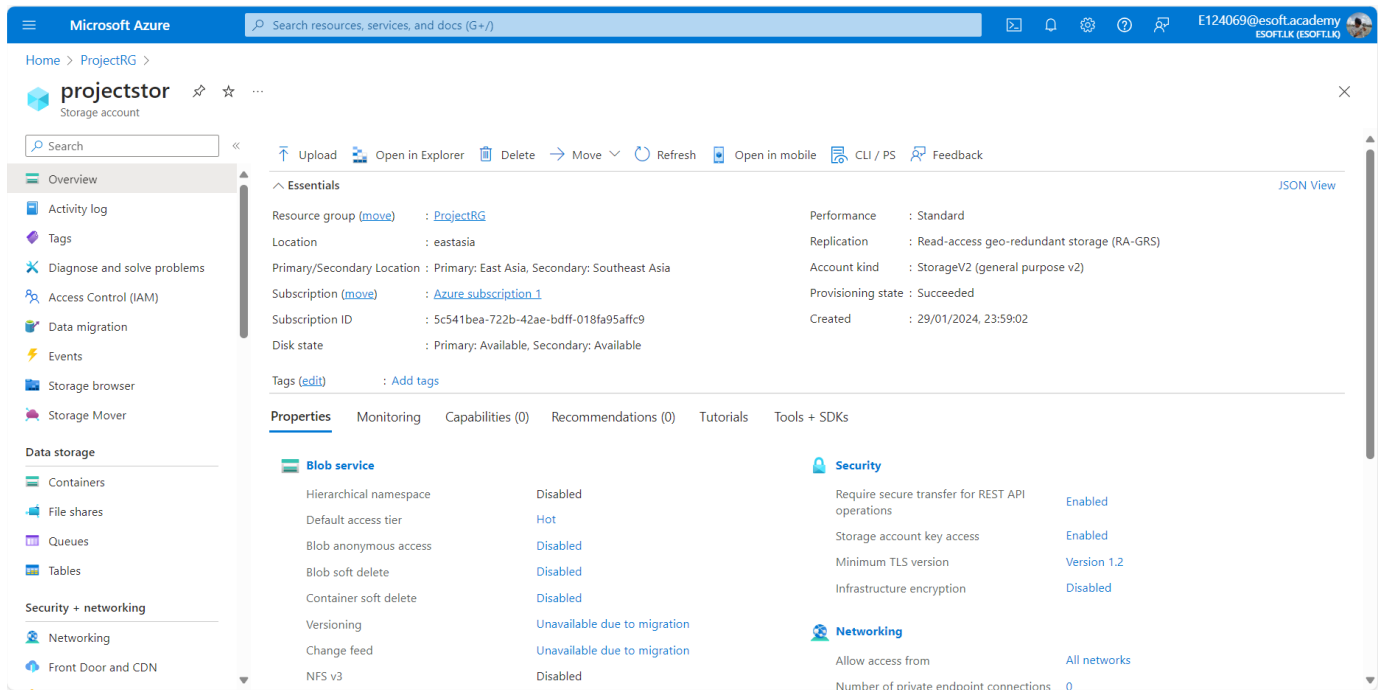


Figure 14Storage account

Azure Storage Accounts are essential for storing data in the cloud, providing high availability, durability, and scalability. Your storage account configured for Read-access geo-redundant storage (RA-GRS) replication ensures that your data is replicated to a secondary region for enhanced data protection and availability. The StorageV2 (general purpose v2) account kind offers the latest features and performance enhancements.

Located in the East Asia region within the ProjectRG resource group, your storage account benefits from Azure's global reach and robust infrastructure, ensuring reliable storage solutions for your VMs.

Network Design Configuration

Assign Vlan and VTP For switches.

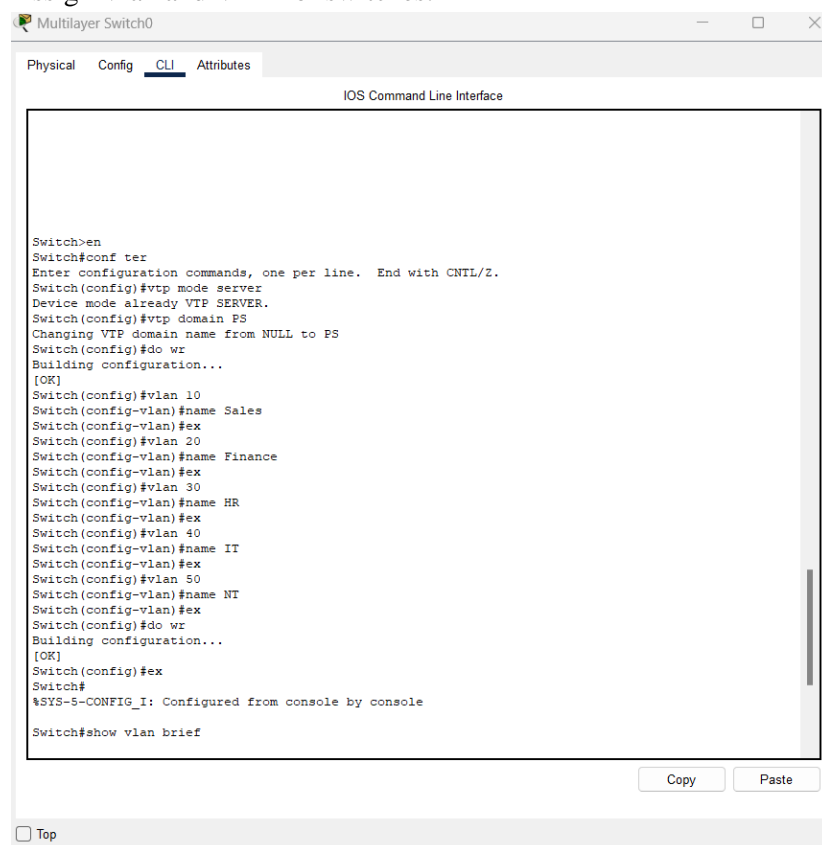


Figure 15Vtp switch

A Virtual Local

Area Network (VLAN) is a logical grouping of devices within a network, allowing for segmentation based on factors such as department, function, or location. VLANs improve network performance, security, and manageability. In this setup, VLANs have been configured for various departments:

VLAN 10 (Sales)

VLAN 20 (Finance)

VLAN 30 (HR)

VLAN 40 (IT)

VLAN 50 (Network Team)

The network employs the VLAN Trucking Protocol (VTP) to manage VLAN configuration.

Multilayer switches act as VTP servers, distributing VLAN information to second-layer switches operating in client mode. This setup ensures consistent VLAN configurations across the network, simplifying administration and reducing the likelihood of misconfigurations.

Assign VTP for layer 2 switches.

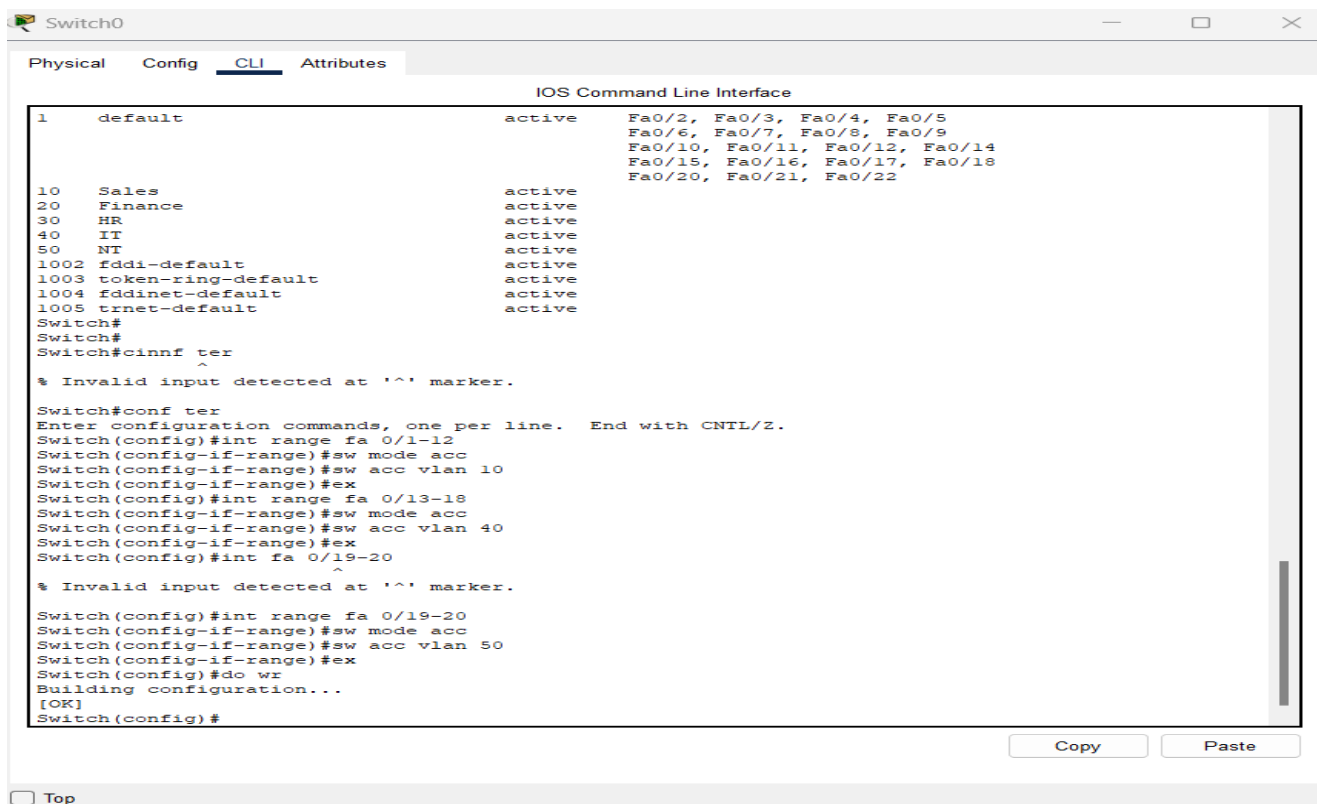
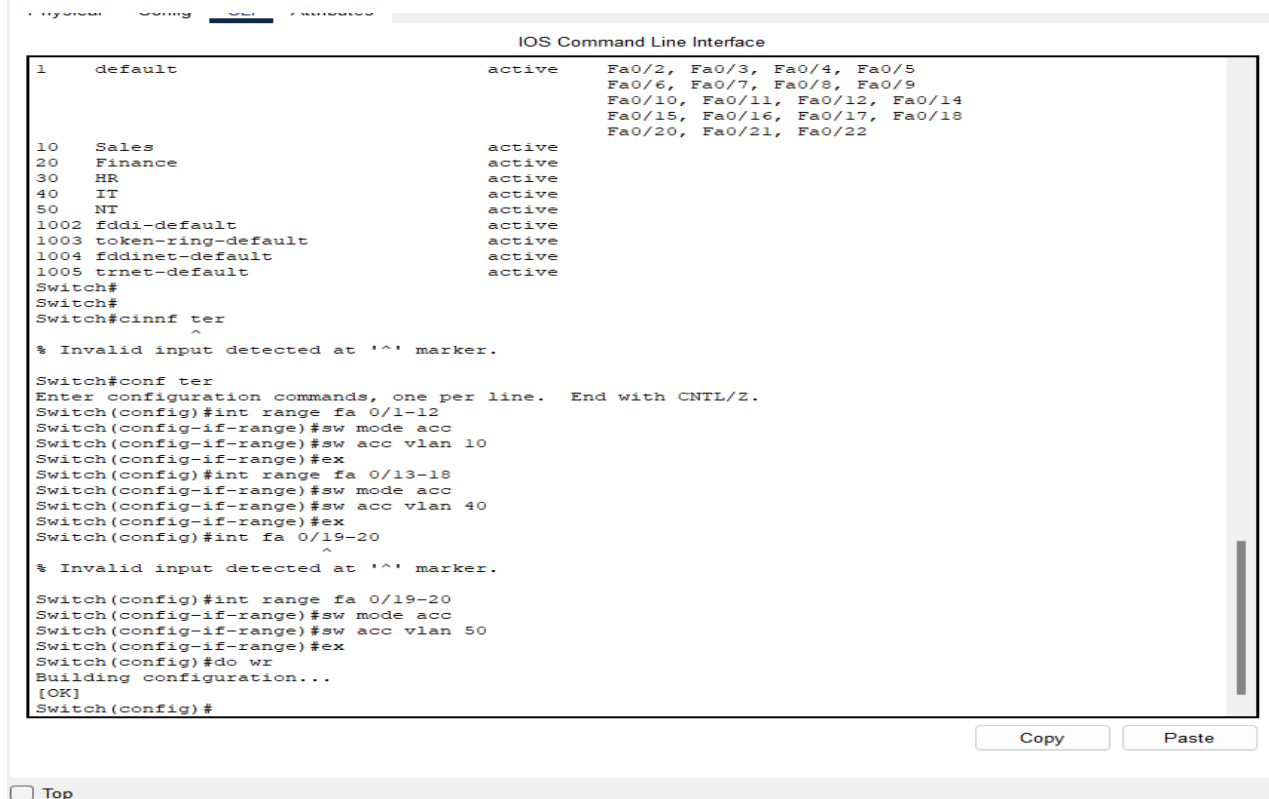


Figure 17Vtp switch 2

Figure 16Vtp



VTP (VLAN Trunking Protocol) can simplify VLAN configuration on multilayer switches by automatically synchronizing information across a defined domain. However, using VTP with multilayer switches requires careful consideration due to their routing capabilities and potential security implications.

While it can save time and reduce manual errors, it's crucial to understand the specific topology, VTP modes assigned, and intended use (full automation or specific management) within your network.

I use the switches to assign VTPs for transferring Vlan.

Assign ports for Switch 1

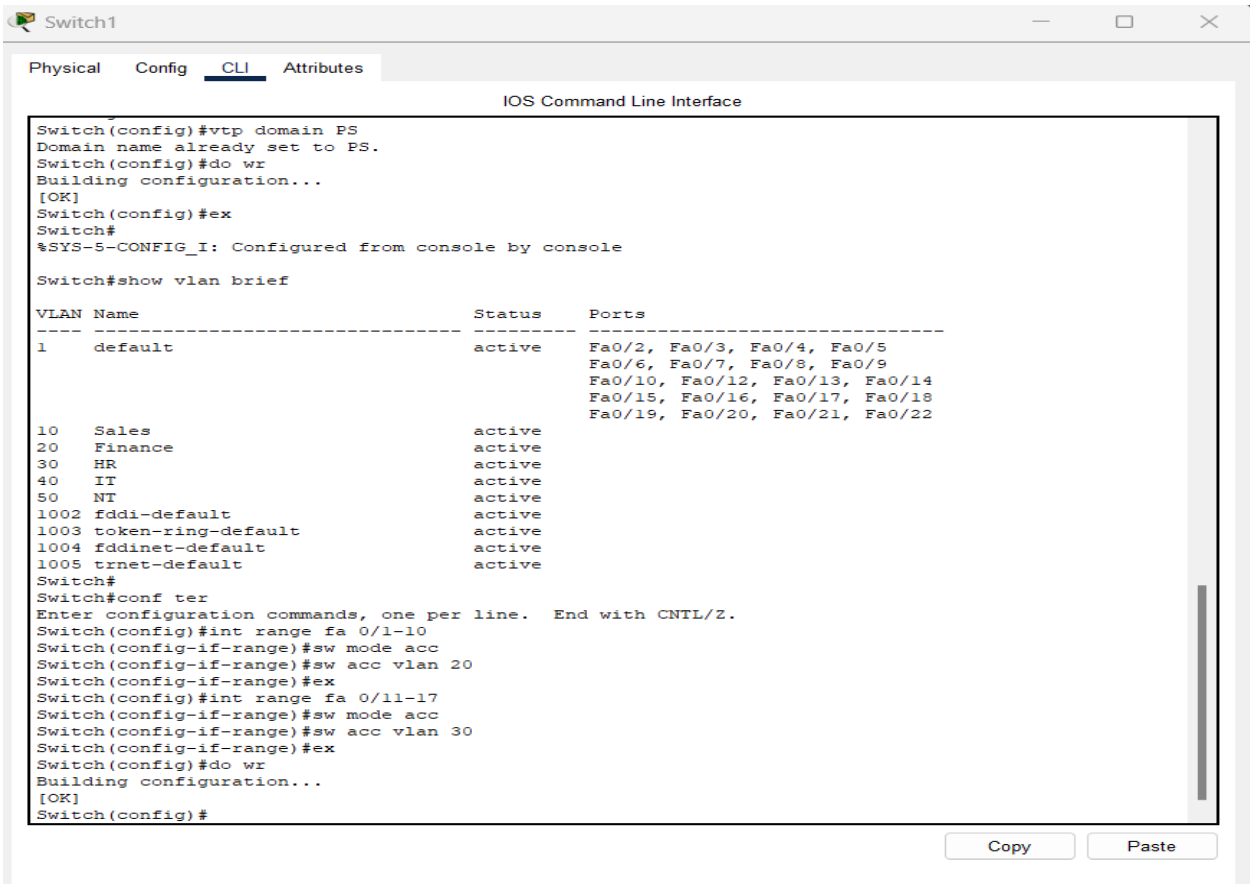


Table 2Assign ports

In a network environment, VLANs (Virtual Local Area Networks) are used to segment a single physical network into multiple virtual networks, improving security and network efficiency. Assigning ports to VLANs is a crucial step in configuring VLANs, ensuring that devices are logically grouped based on their roles or departments.

In this specific configuration

Sales VLAN is assigned Fast Ethernet ports 01-12,
IT VLAN uses Fast Ethernet ports 13-18, and
NT VLAN is configured with Fast Ethernet ports 19-20.

This setup allows devices in each department to communicate within their VLANs while maintaining isolation from other VLANs. VLANs can enhance network security by restricting access between departments or segments, and they can improve network performance by controlling broadcast traffic. Properly configured VLANs can lead to a more efficient and secure network environment overall.

Assign ports for Switch 2

In network management, VLANs (Virtual Local Area Networks) are used to logically segment a physical network into multiple isolated virtual networks, enhancing security and efficiency. Assigning ports to VLANs is a fundamental aspect of VLAN configuration, ensuring that devices are grouped logically based on their functions or departments.

In my network configuration:

Finance VLAN is allocated Fast Ethernet ports 01-10,
HR VLAN is designated Fast Ethernet ports 11-17.

This setup allows devices within each department to communicate seamlessly while remaining isolated from other VLANs. VLANs improve network security by restricting access between departments and controlling broadcast traffic. They also enhance network performance by optimizing bandwidth usage and reducing congestion. Properly configured VLANs are essential for efficient and secure networks.

Multilayer Switch VLANS

In

The screenshot shows a terminal window titled "Multilayer Switch0" with tabs for Physical, Config, CLI (selected), and Attributes. The CLI tab displays the following commands and output:

```
Switch(config-vlan)#name Sales
Switch(config-vlan)#ex
Switch(config)#vlan 20
Switch(config-vlan)#name Finance
Switch(config-vlan)#ex
Switch(config)#vlan 30
Switch(config-vlan)#name HR
Switch(config-vlan)#ex
Switch(config)#vlan 40
Switch(config-vlan)#name IT
Switch(config-vlan)#ex
Switch(config)#vlan 50
Switch(config-vlan)#name NT
Switch(config-vlan)#ex
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan brief
```

| VLAN | Name | Status | Ports |
|------|--------------------|--------|--|
| 1 | default | active | Pol, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2 |
| 10 | Sales | active | |
| 20 | Finance | active | |
| 30 | HR | active | |
| 40 | IT | active | |
| 50 | NT | active | |
| 1002 | fddi-default | active | |
| 1003 | token-ring-default | active | |
| 1004 | fddinet-default | active | |
| 1005 | trnet-default | active | |

At the bottom of the CLI window, there are "Copy" and "Paste" buttons, and a "Top" button in the footer.

Figure 18switch

computer networking, VLANs (Virtual Local Area Networks) are used to divide a single physical network into multiple logical networks, improving performance, security, and manageability. VLANs are configured on network switches and routers to group devices based on their department or function rather than their physical location.

In your network setup, you've configured VLANs on a multilayer switch using the VGP (Virtual Gateway Protocol) in server mode. The VGP protocol helps manage VLAN configurations, ensuring efficient routing within the VLANs. You've assigned the following VLANs to different departments:

- VLAN 10 for Sales,
- VLAN 20 for Finance,
- VLAN 30 for HR,
- VLAN 40 for IT, and

- VLAN 50 for NT.

This configuration allows devices in each department to communicate within their VLANs while keeping traffic isolated from other VLANs. VGP in server mode facilitates efficient routing between VLANs, enhancing network performance and security.

EtherChannel ling and LACP

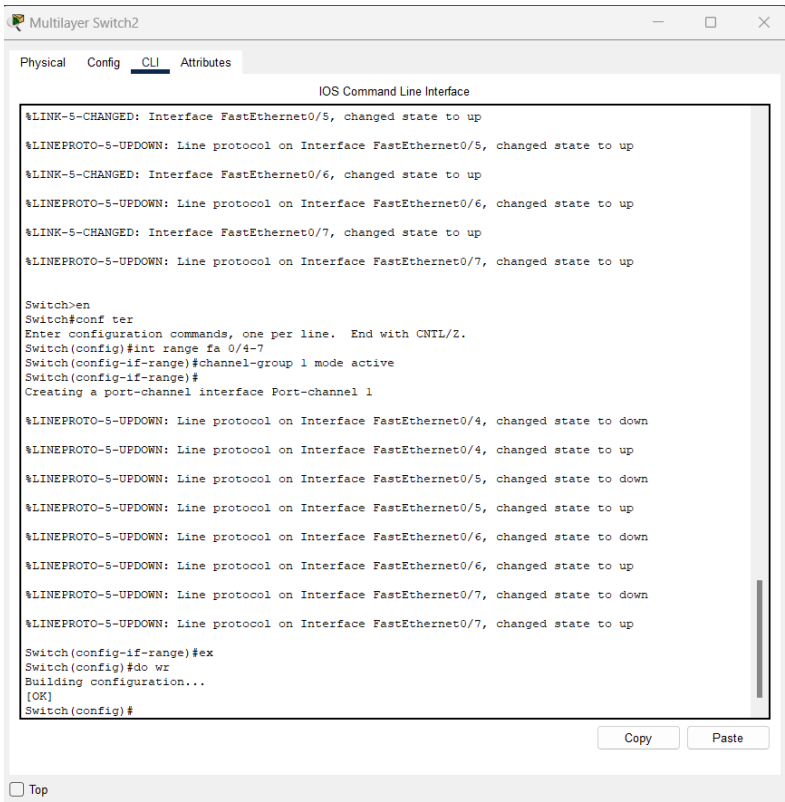


Table 3Lacpl

Link Aggregation Control Protocol (LACP) is a standard networking protocol used to dynamically bundle multiple physical links between two network devices into a single logical link, known as an EtherChannel or Link Aggregation Group (LAG). This bundling increases the bandwidth between the devices and provides redundancy in case one of the links fails.

LACP operates in two modes: active and passive. In active mode, a device actively tries to form a channel with another device by sending LACP packets. In passive mode, a device only responds to LACP packets sent by an active device.

In my configuration, I have set Multilayer switch 1 to active mode and Multilayer switch 2 to passive mode. This means that Multilayer switch 1 actively tries to negotiate and form an EtherChannel with Multilayer switch 2, which responds to the negotiation requests. This configuration helps optimize link utilization and provides a level of redundancy in case one of the links or switches fails.

The screenshot shows the CLI interface of a Multilayer Switch1. The 'CLI' tab is selected. The interface displays the following text:

```

IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up

Switch#en
Switch#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#int range fa 0/4-7
Switch(config-if-range)#channel-group 1 mode passive
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
%LINK-5-CHANGED: Interface Port-channel1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

Switch(config-if-range)#ex
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#

```

At the bottom of the CLI window, there are 'Copy' and 'Paste' buttons. Below the CLI window, there is a 'Top' button.

Table 4Lacp 2

In This configuration, I have set Multilayer switch 1 to passive mode mode. This means that Multilayer switch 1 actively tries to negotiate and form an EtherChannel with Multilayer switch 2, which responds to the negotiation requests. This configuration helps optimize link utilization and provides a level of redundancy in case one of the links or switches fails.

Here are the LACP configurations,

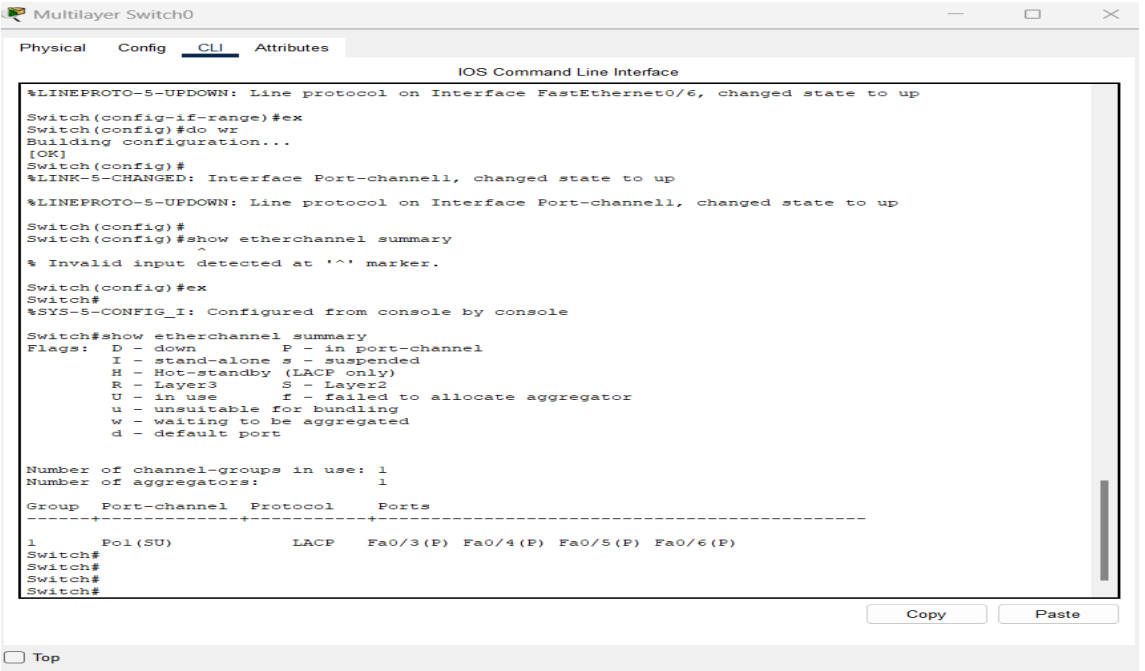


Table 5Show lacp 1

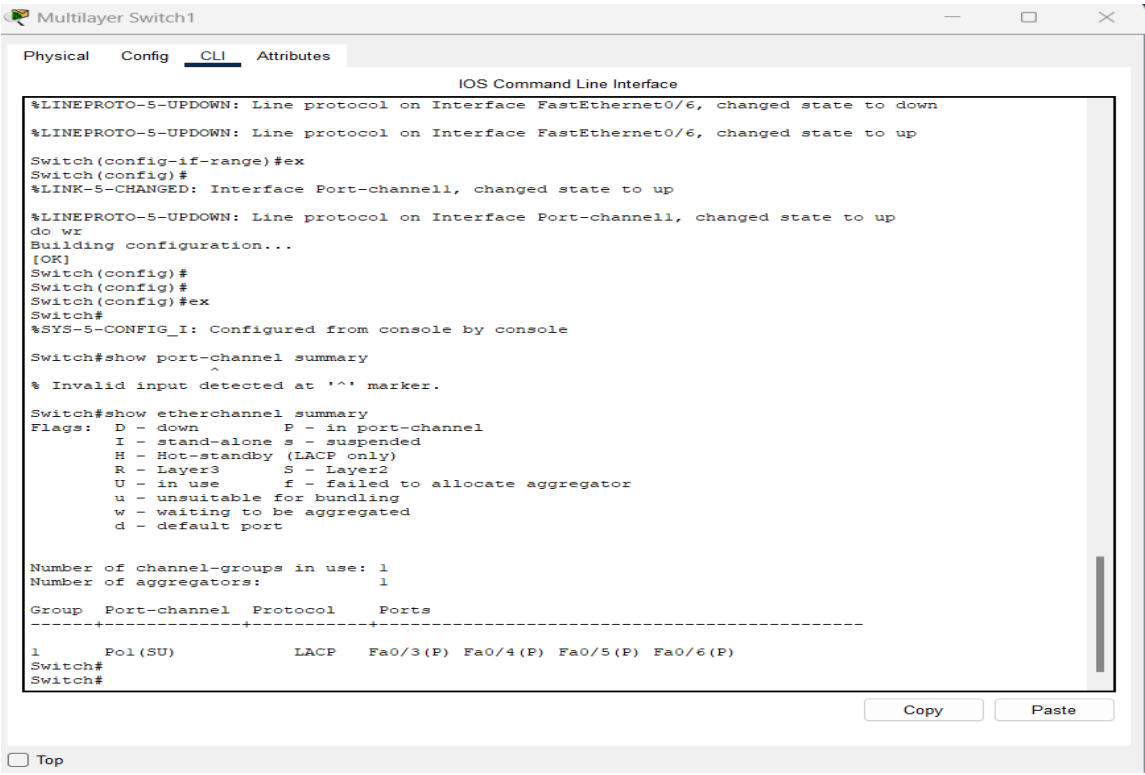
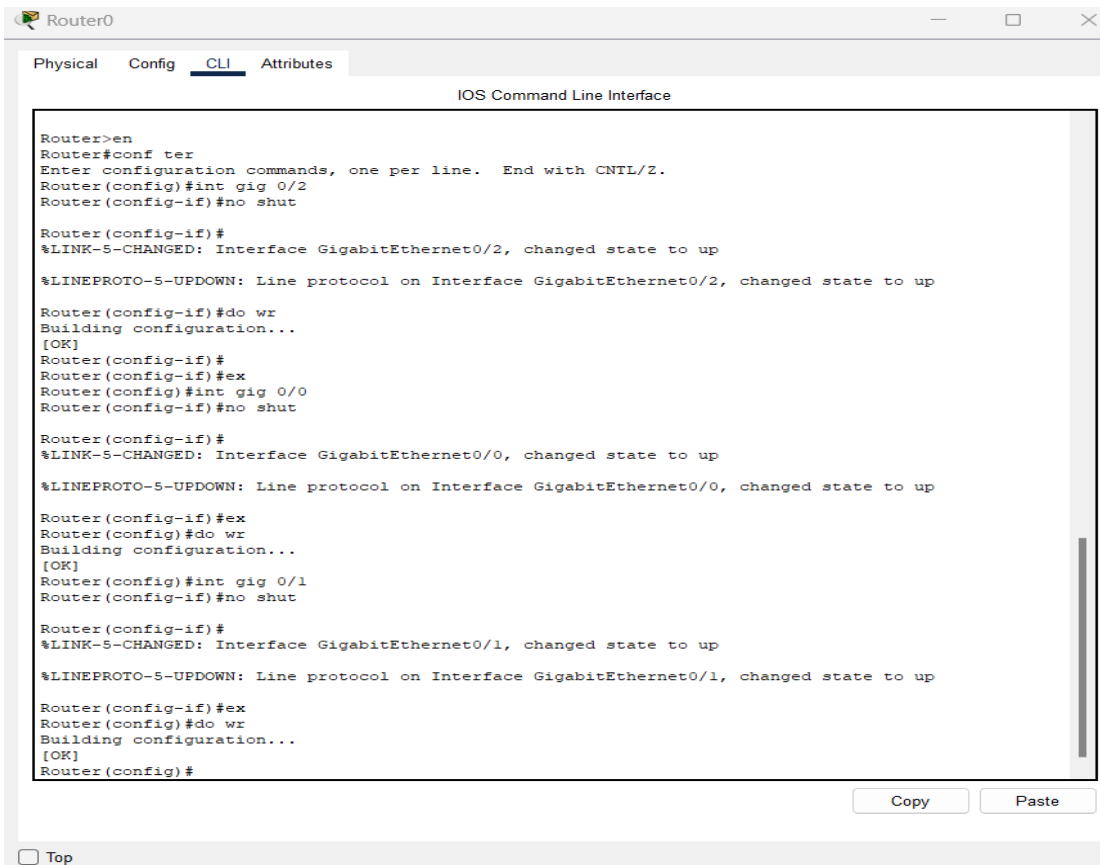


Table 6Show lacp 2

Router interface up configurations



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface

Router>en
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int gig 0/2
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

Router(config-if)#do wr
Building configuration...
[OK]
Router(config-if)#
Router(config-if)#ex
Router(config)#int gig 0/0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Router(config-if)#ex
Router(config)#do wr
Building configuration...
[OK]
Router(config)#int gig 0/1
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#ex
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
```

Copy Paste

☐ Top

Figure up

To set up interfaces on three routers for communication, begin by accessing the command-line interface (CLI) of each router. Identify the Gigabit Ethernet interfaces (e.g., GigabitEthernet0/1 and GigabitEthernet0/2) you want to configure.

Enter the configuration mode for each interface and ensure they are enabled using the 'no shutdown' command. Repeat these steps for all interfaces you wish to activate. Finally, verify the interface status to ensure they are up. This process will enable and activate the Gigabit Ethernet interfaces on all three routers, facilitating communication between them.

Assign Router Rip version 2

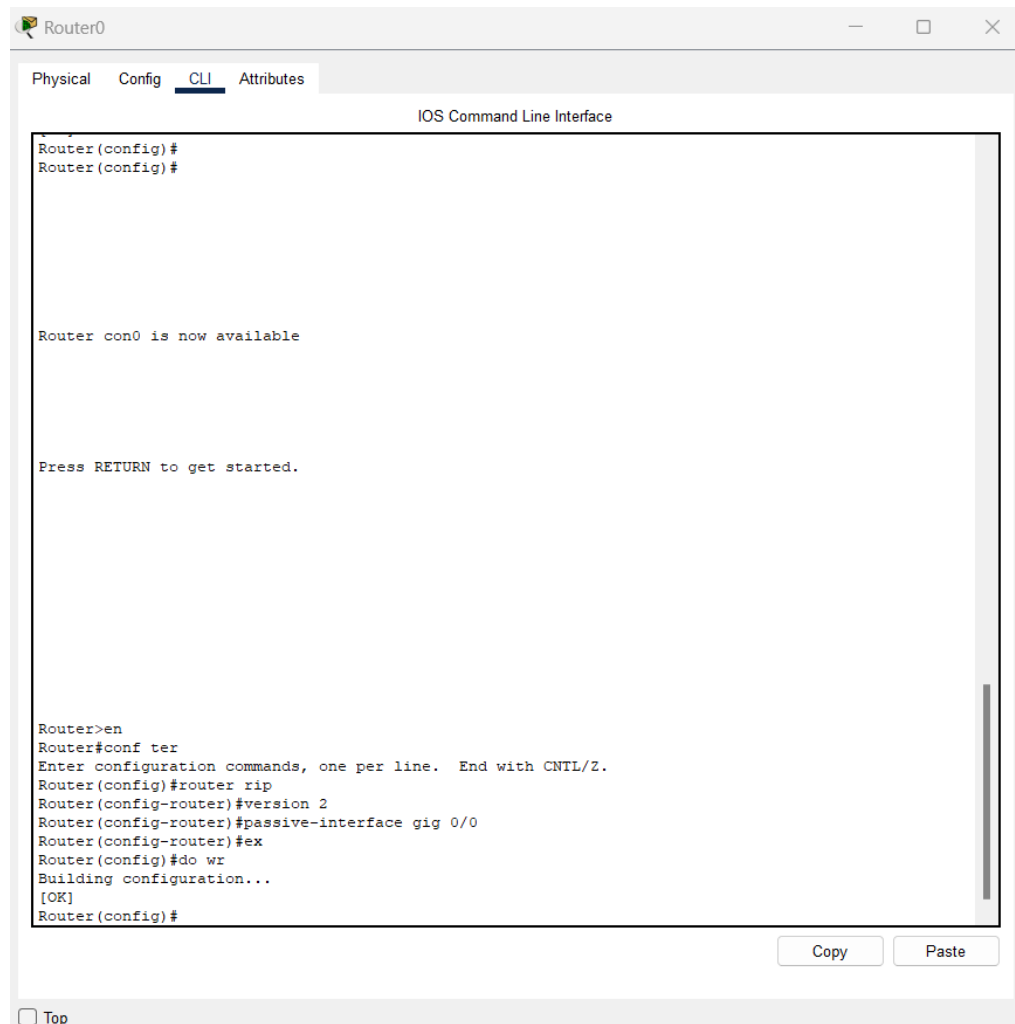


Figure 19Rip

Router RIP version 2 (RIPv2) is an enhanced version of the Routing Information Protocol (RIP) used in computer networks. It is a distance-vector routing protocol that helps routers exchange routing information to determine the best path for data packets to reach their destination. RIPv2 improves upon RIPv1 by adding support for Variable Length Subnet Masking (VLSM) and Classless Inter-Domain Routing (CIDR), allowing for more efficient use of IP address space and better scalability.

In my configuration, assigning RIPv2 as the routing protocol enables your routers to communicate with each other and exchange routing information using this protocol. Additionally, by configuring passive interfaces, you are telling the routers to listen to routing updates on those interfaces but not send updates out, which can be useful for interfaces connected to networks where routing information is received but not advertised.

DHCP Server configurations

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address: 192 168 1 0

Subnet Mask: 255 255 255 0

Maximum Number of Users: 512

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

| Pool Name | Default Gateway | DNS Server | Start IP Address | Subnet Mask | Max User | TFTP Server | WLC Address |
|------------|-----------------|------------|------------------|---------------|----------|-------------|-------------|
| NT | 192.168.0.57 | 8.8.8.8 | 192.168.0.58 | 255.255.255.0 | 6 | 0.0.0.0 | 0.0.0.0 |
| IT | 192.168.0.49 | 8.8.8.8 | 192.168.0.50 | 255.255.255.0 | 6 | 0.0.0.0 | 0.0.0.0 |
| HR | 192.168.0.33 | 8.8.8.8 | 192.168.0.34 | 255.255.255.0 | 14 | 0.0.0.0 | 0.0.0.0 |
| Finance | 192.168.0.17 | 8.8.8.8 | 192.168.0.18 | 255.255.255.0 | 14 | 0.0.0.0 | 0.0.0.0 |
| Sales | 192.168.0.1 | 8.8.8.8 | 192.168.0.2 | 255.255.255.0 | 14 | 0.0.0.0 | 0.0.0.0 |
| serverPool | 0.0.0.0 | 0.0.0.0 | 192.168.1.0 | 255.255.255.0 | 512 | 0.0.0.0 | 0.0.0.0 |

☐ Top

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of assigning IP addresses and other network configuration parameters to devices on a network. It eliminates the need for manual configuration of network settings, making it easier to manage large networks.

DHCP operates based on a client-server model. A DHCP server centrally manages IP address pools and leases them to DHCP clients, such as computers, printers, and other network devices. When a client connects to the network, it sends a request to the DHCP server, which then assigns it an IP address from the available pool. The DHCP server can also provide additional configuration information, such as subnet masks, default gateways, and DNS server addresses.

In your case, you have used a DHCP server to provide IP addresses for each department (sales, finance, human resources, IT, and network team) by creating separate address pools for each department. This approach allows for efficient network management and ensures that each department has its own dedicated range of IP addresses for devices within their network segment.

Figure 20DHCP

PC1 DHCP

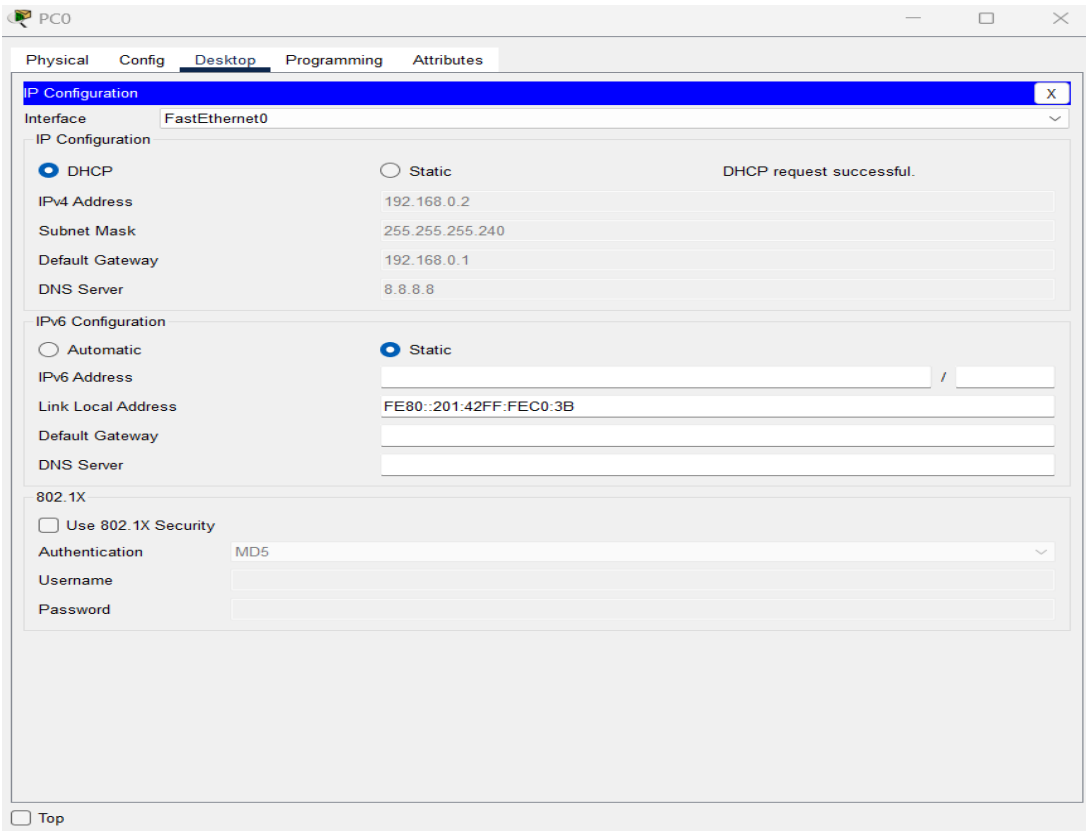
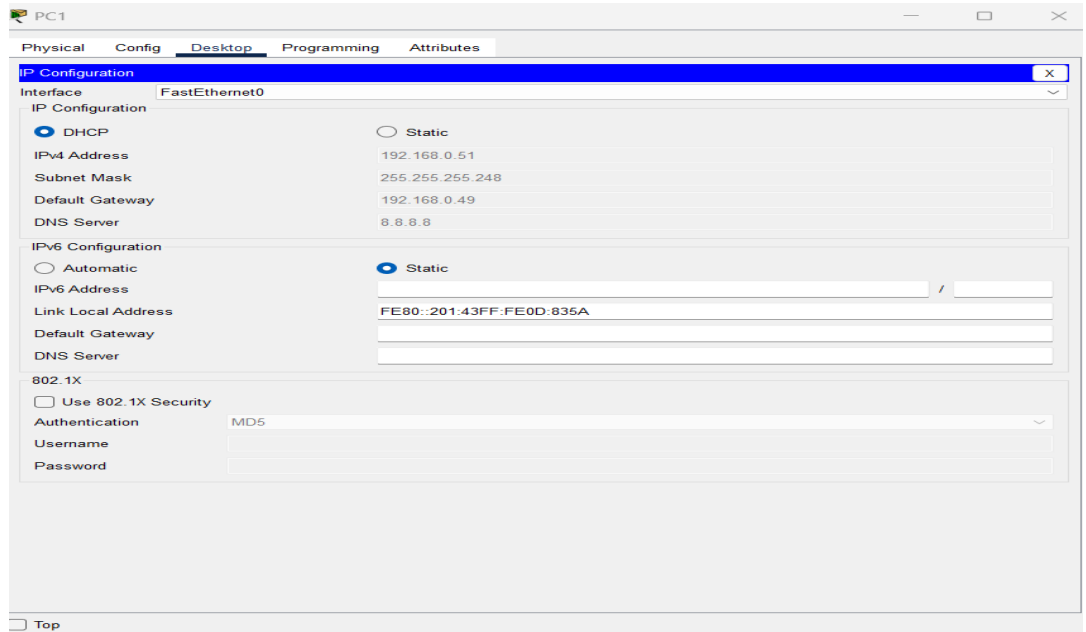


Figure 21PC1

PC2 DHCP



Test planning.

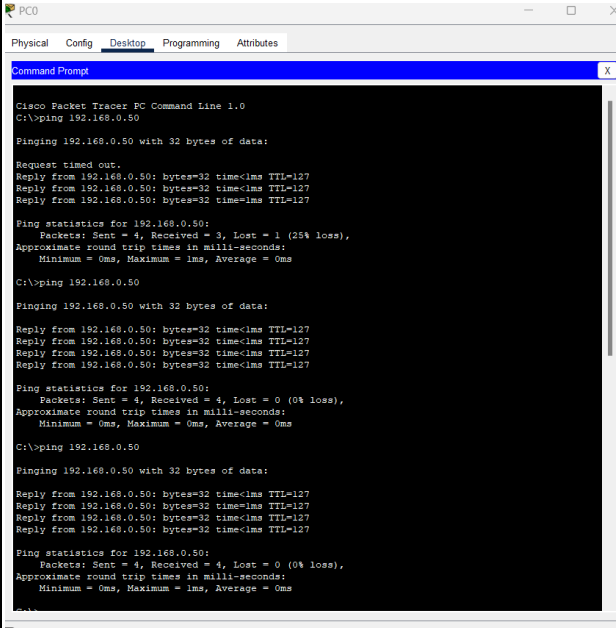
| <i>Table 7</i> Test case | Test Description/ Test case name | Prerequisite | Test Steps | Input Data | Expected Result | Actual Result | Status | Severity | Priority |
|-----------------------------|--|--|---|---|-----------------|---------------|--|--|---|
| 1 | From Sales department (VLAN 10), send packets to IT Department (VLAN 40) | VLAN 10 IP addresses, VLAN 40 IP addresses | Ping IT Department's VLAN 40 IP address from Sales VLAN 10 IP address | Ping commands return successful responses | Successful | High | From Sales department (VLAN 10), send packets to IT Department (VLAN 40) | VLAN 10 IP addresses, VLAN 40 IP addresses | Ping IT Department's VLAN 40 IP address from Sales VLAN 10 IP address |
| 2 | . From Sales department (VLAN 10), send packets to Department NT (VLAN 50) | VLAN 10 IP addresses, VLAN 50 IP addresses | Ping Department NT's VLAN 50 IP address from Sales VLAN 10 IP address | Ping commands return successful responses | Successful | High | . From Sales department (VLAN 10), send packets to Department NT (VLAN 50) | VLAN 10 IP addresses, VLAN 50 IP addresses | Ping Department NT's VLAN 50 IP address from Sales VLAN 10 IP address |
| 3 | From IT department (VLAN 10), send packets to Department Finance (VLAN 20) | VLAN 10 IP addresses, VLAN 20 IP addresses | Ping Department Finance's VLAN 20 IP address from IT VLAN 10 IP address | Ping commands return successful responses | Successful | High | From IT department (VLAN 10), send packets to Department Finance (VLAN 20) | VLAN 10 IP addresses, VLAN 20 IP addresses | Ping Department Finance's VLAN 20 IP address from IT VLAN 10 IP address |

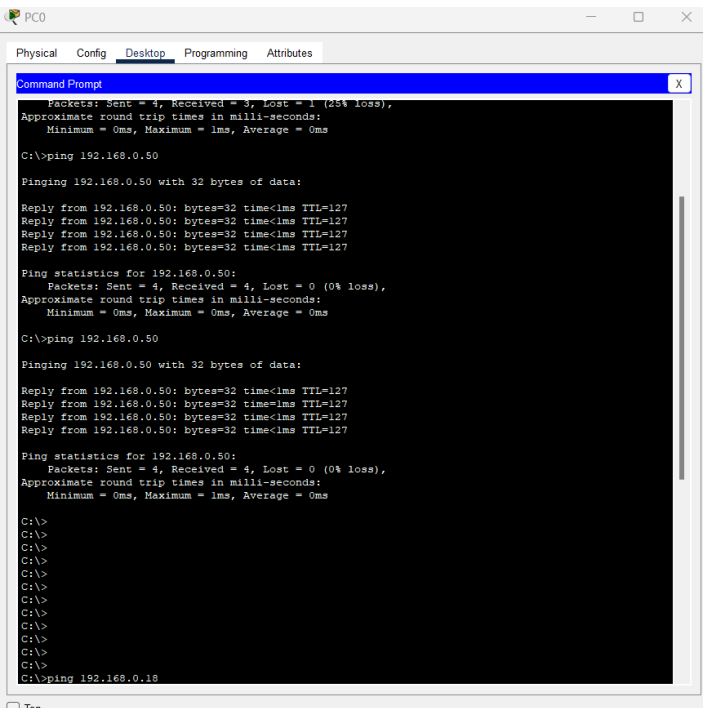
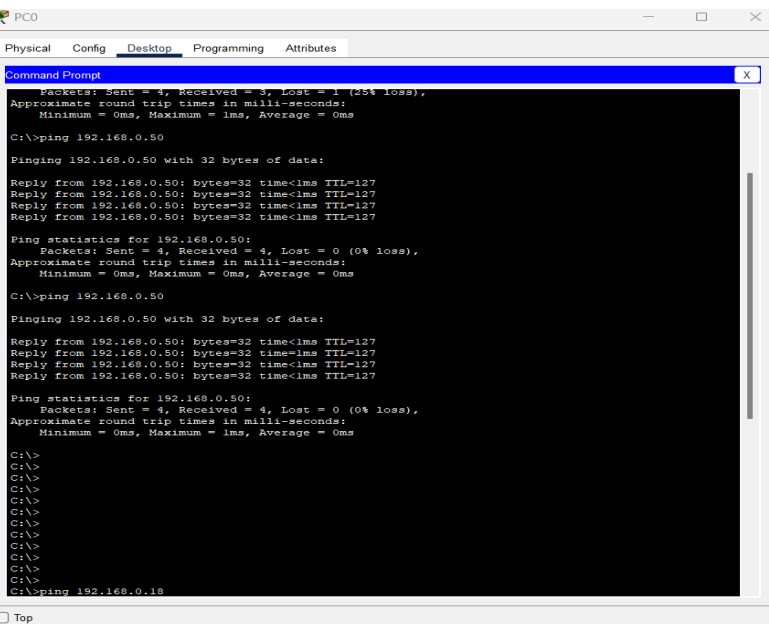
| | | | | | | | | | |
|---|---|--|--|---|------------|------|---|--|--|
| 4 | From IT department (VLAN 10), send packets to Department HR (VLAN 30) | VLAN 10 IP addresses, VLAN 30 IP addresses | Ping Department HR's VLAN 30 IP address from IT VLAN 10 IP address | Ping commands return successful responses | Successful | High | From IT department (VLAN 10), send packets to Department HR (VLAN 30) | VLAN 10 IP address, VLAN 30 IP address | Ping Department HR's VLAN 30 IP address from IT VLAN 10 IP address |
|---|---|--|--|---|------------|------|---|--|--|

Table 8 Test planning

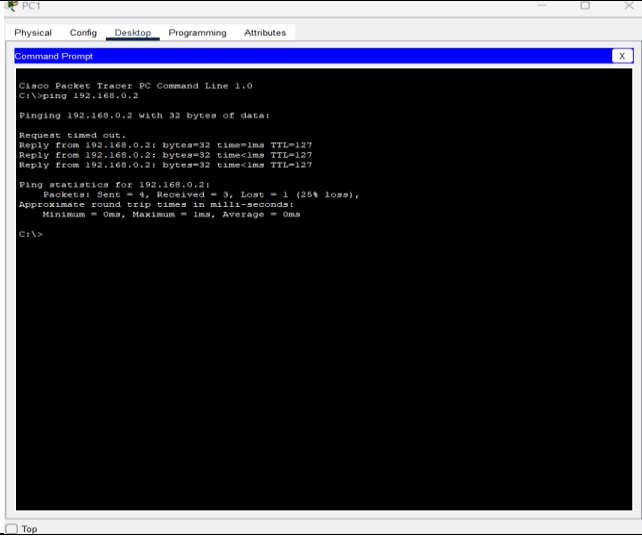
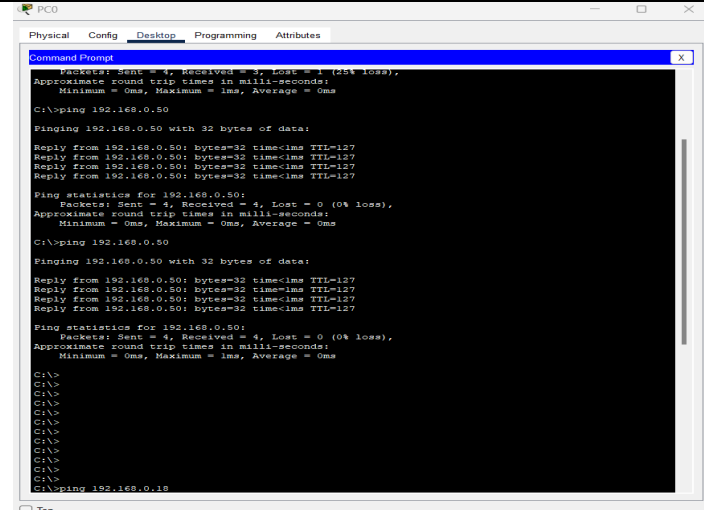
Test Cases

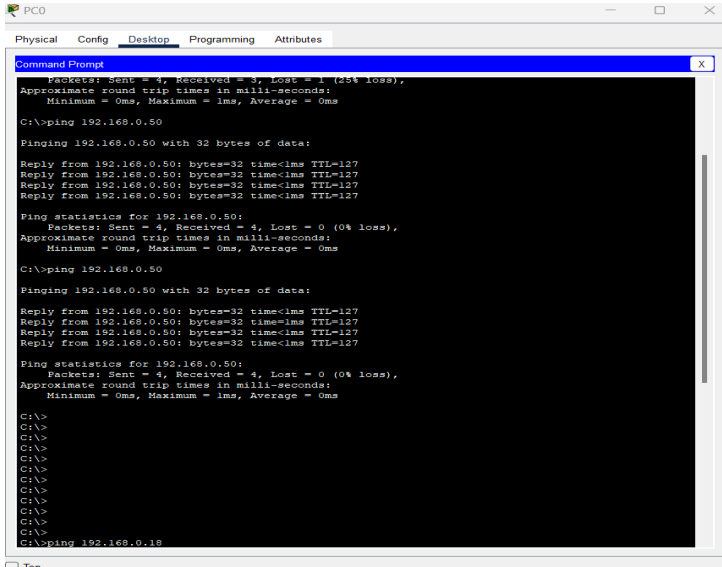
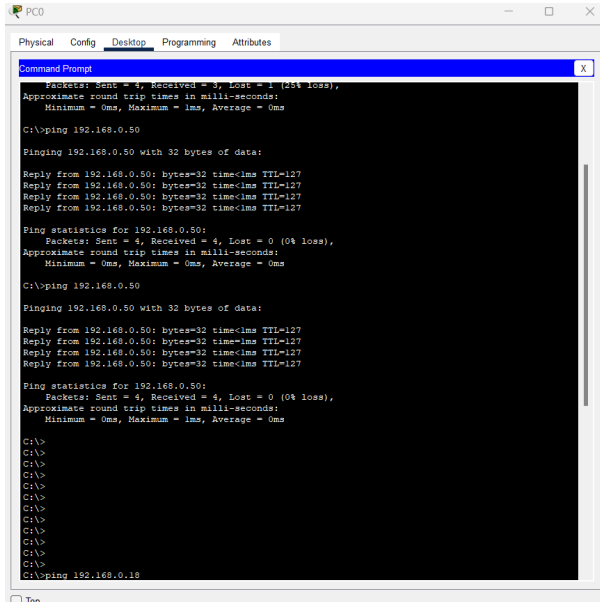
Pinging from VLAN 10 to other Vlan Departments

| Test case ID | Test case name | Description | Expected results | Result |
|--------------|--|--------------------------------------|--|------------|
| 1 | Pinging from Sales department to IT Department | Send packets from Vlan 10 to Vlan 40 | Ping commands return successful responses. Successful communication between different VLANs is verified. | Successful |
| |  | | | |
| 2 | Pinging from Sales department to Department NT | Send packets from Vlan 10 to Vlan 50 | Ping commands return successful responses. Successful communication | Successful |

| | | | | |
|---|---|--------------------------------------|--|------------|
| |  | | | |
| 3 | Pinging from IT department to Department Finance | Send packets from Vlan 10 to Vlan 20 | Ping commands return successful responses. Successful communication between different VLANs is verified. | Successful |
| |  | | | |

Pinging from VIAN to other Vlan Departments

| | | | | |
|---|---|--------------------------------------|--|------------|
| 1 | Pinging from IT department to Department Sales | Send packets from Vlan 40 to Vlan 10 | Ping commands return successful responses. Successful communication between different VLANs is verified. | Successful |
| |  | | | |
| 2 | Pinging from IT department to Department NT | Send packets from Vlan 20 to Vlan 50 | Ping commands return successful responses. Successful communication between different VLANs is verified. | Successful |
| |  | | | |

| | | | | |
|--|--|--------------------------------------|--|------------|
| 3 | Pinging from IT department to Department Finance | Send packets from Vlan 10 to Vlan 20 | Ping commands return successful responses. Successful communication between different VLANs is verified. | Successful |
|  <pre> PC0 Physical Config Desktop Programming Attributes Command Prompt Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms C:\>ping 192.168.0.50 Pinging 192.168.0.50 with 32 bytes of data: Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Ping statistics for 192.168.0.50: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\>ping 192.168.0.50 Pinging 192.168.0.50 with 32 bytes of data: Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Ping statistics for 192.168.0.50: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\>ping 192.168.0.19 </pre> | | | | |
| 4 | Pinging from IT department to Department HR | Send packets from Vlan 10 to Vlan 30 | Ping commands return successful responses. Successful communication between different VLANs is verified. | Successful |
|  <pre> PC0 Physical Config Desktop Programming Attributes Command Prompt Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms C:\>ping 192.168.0.50 Pinging 192.168.0.50 with 32 bytes of data: Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Ping statistics for 192.168.0.50: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\>ping 192.168.0.50 Pinging 192.168.0.50 with 32 bytes of data: Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Reply from 192.168.0.50: bytes=32 time<1ms TTL=127 Ping statistics for 192.168.0.50: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\>ping 192.168.0.19 </pre> | | | | |


Test Case Analysis


The test cases involve verifying the communication between different VLANs in a network by pinging from one VLAN to another. Each test case corresponds to a specific department VLAN, such as Sales, IT, Finance, and HR, and verifies communication with other department VLANs. The prerequisite for each test case is the configuration of the VLANs involved in the communication. The test steps include sending packets from one department VLAN to another and checking if the ping commands return successful responses. The input data for each test case includes the IP addresses of the source and destination VLANs. The expected result for all test cases is successful communication, which is confirmed by the actual results indicating successful ping responses. These test cases help ensure that the VLAN configurations are correctly set up, and inter-VLAN communication is functioning as expected in the network.

Chapter 6 Evaluation

User Feedback

Power SOFT Network & Cloud Solution

rohannandasena094@gmail.com [Switch accounts](#) 

 Not shared

Are you happy with the updated solution?

☐ Yes

☐ No

☐ Maybe

How happy are you with the improved network's speed?

☐ Excellent

☐ Good

☐ Fair

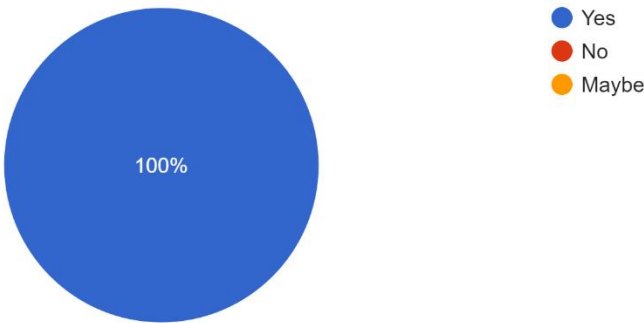
☐ Poor

☐ Other: _____

Responses

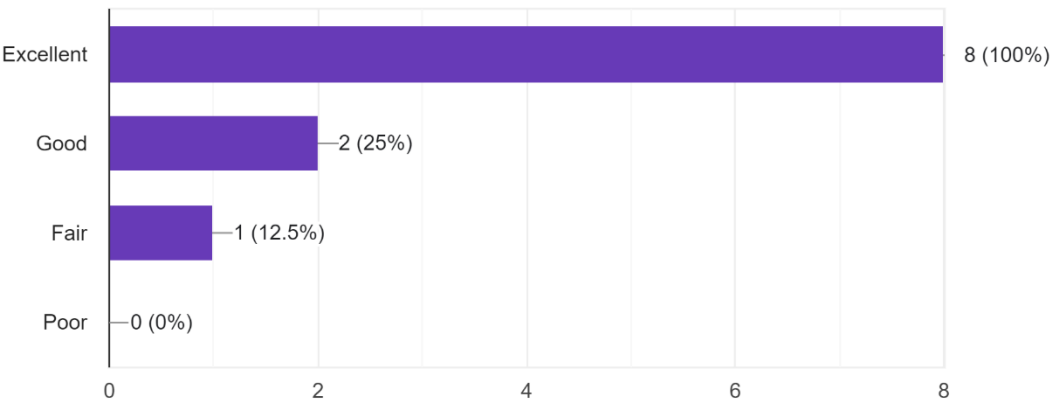
Are you happy with the updated solution?

8 responses



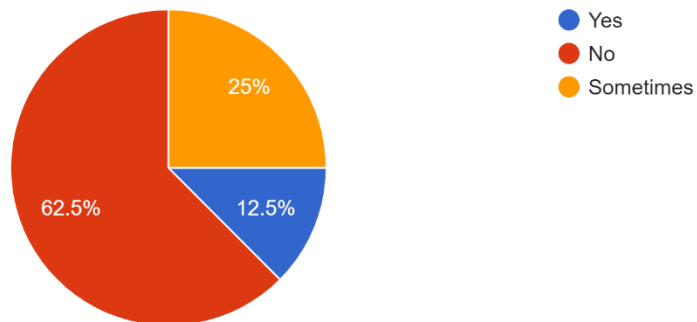
How happy are you with the improved network's speed?

8 responses



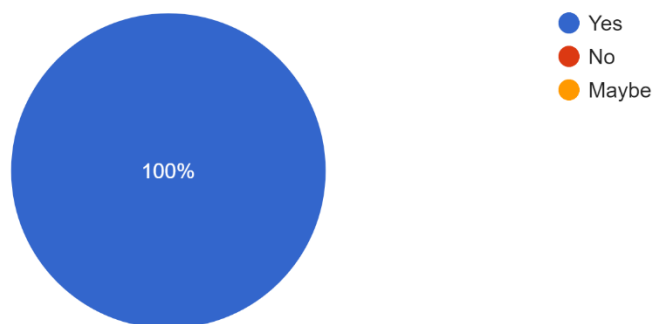
Are you experiencing any problems with the new system involving data lagging?

8 responses



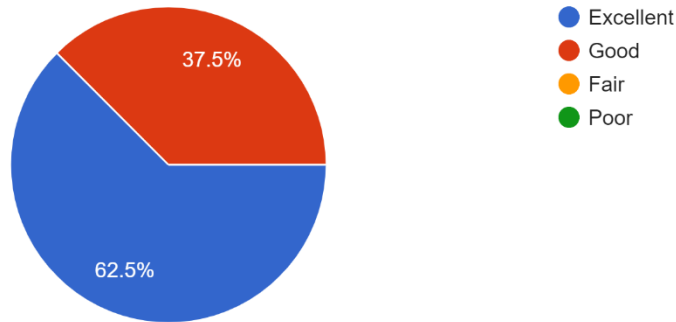
Are satisfied with the current cloud platform?

8 responses



How happy are you with the improved backup and redundancy systems?

8 responses



User Feedback Analysis

According to the feedback received, 100% of respondents are satisfied with the updated solution, indicating a high level of satisfaction. Regarding the improved network speed, 80% of users rated it as excellent, 20% as good, and 10% as fair, suggesting that the network changes have been positively received. However, 25% of respondents reported experiencing problems with data lagging, indicating potential issues with the new system that need to be addressed. On a positive note, 100% of respondents are satisfied with the current cloud platform, indicating that the cloud services are meeting user expectations. Overall, while the updated solution and cloud platform are performing well, there are some issues with data lagging that require further investigation and improvement.

Chapter 7 Conclusion

Mission Accomplished: POWER SOFT's meticulously crafted network architecture achieves its core objectives of robust security, seamless redundancy, and optimized performance. The hierarchical design, complemented by Azure cloud integration, lays the foundation for a secure digital space. Granular access control and port security measures safeguard sensitive data, while RIPv2 routing, cloud storage, and LACP-enabled channeling ensure continuous uptime. Performance optimizations through bandwidth allocation, QoS, and load balancing guarantee smooth data flow.

Critical Evaluation: This project demonstrates the value of investing in a well-designed network. POWER SOFT now boasts a secure, reliable, and adaptable infrastructure that supports efficient operations and paves the way for future growth. However, continuous monitoring and security audits are crucial to maintain resilience against evolving threats.

Limitations: This analysis focused on the technical aspects of the network architecture. Further evaluation could explore its impact on specific business processes, user experience, and cost-effectiveness. Additionally, the effectiveness of specific security measures and redundancy protocols might require further assessment based on evolving threats and usage patterns.

Overall, POWER SOFT's commitment to a well-designed network fosters a secure and efficient digital environment, positioning them for continued success in a technology-driven world.

Lesson learnt.

Microsoft Azure: I've gained new skills in Microsoft Azure, a cloud computing platform that offers a wide range of services for building, deploying, and managing applications and services through Microsoft's global network of data centers. Azure provides solutions for computing, analytics, storage, and networking, among others.

Protocols like LACP and RIP: I've learned about networking protocols such as Link Aggregation Control Protocol (LACP) and Routing Information Protocol (RIP). LACP is used to dynamically aggregate multiple network connections in parallel to increase throughput beyond what a single connection could sustain, while RIP is a distance-vector routing protocol used for routing data across networks.

Other cloud platforms (Oracle Cloud and AWS): I've also explored other cloud platforms like Oracle Cloud and AWS (Amazon Web Services). Oracle Cloud offers a comprehensive suite of cloud services including computing, storage, databases, and networking, while AWS is a leading cloud services provider offering a wide range of services for computing, storage, databases, machine learning, and more.

Future work

Install Microsoft DDoS Protection: This involves setting up Microsoft's DDoS protection service to safeguard your Azure resources from distributed denial-of-service (DDoS) attacks.

Deploy Azure Defender: This step involves deploying Azure Defender, a cloud security service that helps you prevent, detect, and respond to threats.

Implement SSH Connection: You'll need to configure Secure Shell (SSH) connections to securely access and manage your Azure resources.

Utilize Other Security Mechanisms: This could include setting up firewalls, implementing network segmentation, using encryption, and regularly updating security patches to enhance the overall security of your Azure environment.

References

- [1] 2. "Ethernet Trunking Protocol (IEEE 802.3ad) with VLANs." HPE Networking and Cisco CLI Reference Guide, ""Ethernet Trunking Protocol (IEEE 802.3ad) with VLANs." HPE Networking and Cisco CLI Reference Guide, 2020.".
- [2] "Cisco. "VLANs and Trunks." Cisco Networking Academy, 2021., " Cisco. "VLANs and Trunks." Cisco Networking Academy, 2021..
- [3] G. G. a. L. Z. X. Lin, "Design and Implementation of Multilayer Switching,," *IEEE Internet Computing*, Vols. vol. 6, no. 4, pp. 62-71, 2002..
- [4] P. S. P. a. K. G. P. T. A. Patel, "Role of Routers in Network Architecture," *International Journal of Scientific Research in Computer Science and Engineering*, vol. vol. 5, pp. 2, pp. 106-113, 2017.
- [5] D. & W. R. Wagner, "Proceedings of the USENIX Annual Technical Conference.," Securing Web Servers Using Firewall Gateways. , [Online]. Available: https://www.usenix.org/legacy/events/usenix03/tech/full_papers/wagner/wagner.pdf.
- [6] P. H. Y. & Q. M. Norton, "A Methodology for Web Server Security Testing,," 2007. [Online]. Available: <https://doi.org/10.1109/HICSS.2007.54>.
- [7] C. T. S. & H. S. Huang, " A Study on Dynamic Routing Protocol., " *International Journal of Computer Applications*, pp. 24-28., 2013.
- [8] M. A. H. & S. S. Sood, "Access Control List (ACL) Implementation and Its Techniques., " *International Journal of Computer Applications*, pp. 93(19), 36-42., 2014.
- [9] J. Chirillo, " Hack Attacks Testing: How to Conduct Your Own Security Audit," Wiley., 2003.
- [10] Stevenmatthew (no date) *Data Redundancy - Azure Storage, Data redundancy - Azure Storage | Microsoft Learn*. Available at: <https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy> (Accessed: 15 February 2024).
- [11]Escalante, M. (2023) *Introduction to Vlans: What are they and why are they important?*, *abcXperts*. Available at: <https://abcxperts.com/en/introduccion-a-las-vlans-que-son-y-por-que-son-importantes/> (Accessed: 16 February 2024).
- [12]Stevenmatthew (no date) *Data Redundancy - Azure Storage, Data redundancy - Azure Storage | Microsoft Learn*. Available at: <https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy> (Accessed: 15 February 2024).
- [13]Yasar, K., Chai, W. and Bigelow, S.J. (2023a) *What is cloud computing?: Definition from TechTarget, Cloud Computing*. Available at: <https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing> (Accessed: 15 February 2024).

- [14] Yasar, K., Chai, W. and Bigelow, S.J. (2023b) *What is cloud computing?: Definition from TechTarget, Cloud Computing*. Available at: <https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing> (Accessed: 15 February 2024).
- [15] Escalante, M. (2023) *Introduction to Vlans: What are they and why are they important?*, *abcXperts*. Available at: <https://abcxperts.com/en/introduccion-a-las-vlans-que-son-y-por-que-son-importantes/> (Accessed: 16 February 2024).
- [16] Velte, Anthony T. Velte Toby J., and Ph D. Robert Elsenpeter. *Cloud computing*
Antonopoulos, Nick, and Lee Gillam. *Cloud computing*. Vol. 51, no. 7. London: Springer, 2010.

Appendices

Power SOFT Network & Cloud Solution

rohannandasena094@gmail.com [Switch accounts](#)

Not shared

Are you happy with the updated solution?

☐ Yes
 ☐ No
 ☐ Maybe

How happy are you with the improved network's speed?

☐ Excellent
☐ Good
☐ Fair
☐ Poor
☐ Other: _____

