University of Mohamed Khider Biskra
Faculty of Science and Technology
Department of Electrical Engineering

MASTER THESIS

Science and Technology
Field: Telecommunication
Option: Network and Telecommunication
Ref:

Presented and submitted by:

BERRI Chaouki – AMRANE Mohammed Islam

On: Wednesday 04 June 2025

A Deep Dive into Campus Network Infrastructure: Configuration, Security, and Attacks Emulation

---

Jury:

M.	BOUKREDINE Salah eddine	MAA	University of Biskra	President
M.	ABDESSELAM Salim	MCB	University of Biskra	Examiner
M.	AMEID Sofiane	MAA	University of Biskra	Supervisor

Academic Year: 2024-2025

Université Mohamed Khider de Biskra
Faculty of Sciences and Technology
Department of Electrical Engineering

MASTER THESIS

Science and Technology
Field: Telecommunication
Option: Network and Telecommunication
Ref :

A Deep Dive into Campus Network Infrastructure: Configuration, Security, and Attacks Emulation

On : Wednesday 04 June 2025

Presented By :

BERRI Chaouki

AMRANE Mohammed Islam

Favorable opinion of the supervisor:

Mr. AMEID Sofiane

Positive opinion of the President of the Jury

Mr. BOUKREDINE Salah eddine

Stamp and Signature

Abstract:

This project aims to design and develop a comprehensive campus network infrastructure that combines high performance, flexibility, and security while preparing for future scalability. The current infrastructure was analyzed, needs were identified, and a network was designed to provide full coverage and service continuity. Advanced simulation was utilized to model and design the network prior to physical implementation, which helped reduce costs and streamline testing and evaluation processes, alongside implementing mechanisms to ensure service continuity. Multiple security measures were integrated, such as applying protection protocols, system updates, and preventive measures to counter cyber threats. The network was tested through simulated cyber-attacks to identify vulnerabilities and strengthen cyber defense mechanisms. An optimal balance between performance, security, and flexibility was achieved to ensure network sustainability and meet the university's future needs, while guaranteeing a high level of security and efficiency.

ملخص:

يهدف هذا المشروع إلى تصميم وتطوير بنية تحتية شاملة لشبكة الحرم الجامعي تجمع بين الأداء العالي، والمرونة، والأمان، مع الاستعداد للتوسع المستقبلي. تم تحليل الوضع الحالي للبنية التحتية، وتحديد الاحتياجات، وتصميم شبكة توفر تغطية كاملة واستمرارية في الخدمة. تم الاعتماد على محاكاة متقدمة لنمذجة وتصميم الشبكة قبل تنفيذها الفعلي، مما ساعد في تقليل التكاليف وتسهيل عمليات الاختبار والتقييم، بالإضافة إلى تطبيق آليات لضمان استمرارية الخدمة. وكما تم دمج إجراءات أمان متعددة مثل تطبيق بروتوكولات الحماية، وتحديثات الأنظمة، وتنفيذ التدابير الوقائية لمواجهة التهديدات السيبرانية. وتم اختبار الشبكة عبر محاكاة هجمات إلكترونية بهدف تحديد الثغرات وتعزيز آليات الدفاع السيبراني، تم تحقيق توازن مثالي بين الأداء، والأمان، والمرونة لضمان استدامة الشبكة وتلبية احتياجات الجامعة المستقبلية، مع ضمان مستوى عالٍ من الأمان والكفاءة.

Résumé :

Ce projet vise à concevoir et développer une infrastructure réseau complète pour un campus universitaire, alliant haute performance, flexibilité et sécurité, tout en préparant une extensibilité future. L'infrastructure actuelle a été analysée, les besoins identifiés, et un réseau a été conçu pour offrir une couverture complète et une continuité de service. Une simulation avancée a été utilisée pour modéliser et concevoir le réseau avant sa mise en œuvre physique, ce qui a permis de réduire les coûts, de simplifier les processus de test et d'évaluation, ainsi que de mettre en place des mécanismes assurant la continuité de service. Des mesures de sécurité multiples ont été intégrées, telles que l'application de protocoles de protection, des mises à jour systèmes et des mesures préventives pour contrer les menaces cybernétiques. Le réseau a été testé via des simulations d'attaques informatiques visant à identifier les vulnérabilités et à renforcer les mécanismes de défense cybernétique. Un équilibre optimal entre performance, sécurité et flexibilité a été atteint pour garantir la durabilité du réseau et répondre aux besoins futurs de l'université, tout en assurant un niveau élevé de sécurité et d'efficacité.

Dedication

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

إلى من جعل الجنة تحت أقدامها إلى من سهّلت لي الشّدائد بدعائِها إلى الإنسانة العظيمة التي لطالما تمنت أن تقِرّ عينها لرُؤيتي في يوم كهذا **أُمّي العزيزة**

إلى من كلّل العرق جبينه وعلّمني أنّ النجاح لا يأتي إلا بالصّبر والإصرار، إلى النّور الذي انار دربي والسِّراج الذي لا ينطفئ بقلبي أبدا إلى الذي استمديت منه قوتي بنفسي **والدي العزيز**

إلى ضلعي الثّابت وأمان أيامي، الى من شددت عضدي بهم وكانوا لي ينابيع أرتوي منها، إلى خيرة أيامي وصفوتها، إلى قرة عيني إخواني وأخواتي الغاليين

لكل من كان عوناً وسنداً في هذا الطريق للأصدقاء الاوفياء ورفقاء السنين لأصحاب الشّدائد والأزمات

إليكم عائلتي، أُهديكم هذا الإنجاز وثمرة نجاحي الذي لطالما تمنّيته ها أنا اليوم أكملت وأتممْت أوّل ثمراته بفضله سبحانه وتعالى

فالحمد لله شكراً وحباً وإمتناناً على البدء والختام

Acknowledgments

All praise and gratitude are due to Allah Almighty for His guidance and blessings in completing this work.

We extend our deepest thanks and appreciation to our beloved parents for their unconditional love, constant support, and sacrifices, which paved the way for this achievement.

Our heartfelt gratitude goes to Professor Ameid Sofiane for his supervision and unwavering support. His guidance and encouragement were a source of inspiration throughout this journey.

Finally, we express our sincere appreciation to our friends and colleagues for their support and companionship, which were a great source of strength during this time.

الحمد والشكر لله عز وجل على توفيقه وفضله في إتمام هذا العمل

نتوجه بأسمى آيات الامتنان والعرفان لوالدينا الأعزاء على حبهم ودعمهم الدائمين، وتضحياتهم التي مهدت لنا الطريق لتحقيق هذا الإنجاز

نشكر الأستاذ عميد سفيان على إشرافه ودعمه المتواصل، حيث كان مصدر إلهام وتشجيع لنا خلال هذه الرحلة

وأخيرًا، نعرب عن تقديرنا العميق لأصدقائنا وزملائنا على دعمهم ومساندتهم التي كانت مصدر قوة لنا طوال هذه الفترة

Table of Content

List of Figures

List of Commands

List of Tables

List of Abbreviations

- **AAA**: Authentication, Authorization, and Accounting
- **ACL**: Access Control List
- **AD-DC**: Active Directory Domain Controller
- **AD-DS**: Active Directory Domain Services
- **AH**: Authentication Header
- **AI**: Artificial Intelligence
- **ARP**: Address Resolution Protocol
- **ASA**: Adaptive Security Appliance
- **BPDU**: Bridge Protocol Data Unit
- **BR**: Branch
- **BYOD**: Bring Your Own Device
- **CAN**: Campus Area Network
- **Cat6**: Category 6
- **CLI**: Command Line Interface
- **CSMA/CD**: Carrier Sense Multiple Access with Collision Detection
- **DDOS**: Distributed Denial of Service
- **DHCP**: Dynamic Host Configuration Protocol
- **DNS**: Domain Name System
- **DOS**: Denial of Service
- **DDoS**: Distributed Denial of Service
- **ESP**: Encapsulating Security Payload
- **ESS**: Extended Service Set
- **EVPN**: Ethernet Virtual Private Network
- **FW**: Firewall
- **FTP**: File Transfer Protocol
- **HQ**: Headquarter
- **HSRP**: Hot Standby Router Protocol
- **HTTP**: Hypertext Transfer Protocol
- **HTTPS**: Hypertext Transfer Protocol Secure
- **IaaS**: Infrastructure as a Service
- **ICMP**: Internet Control Message Protocol
- **IEEE**: Institute of Electrical and Electronics Engineers
- **IETF**: Internet Engineering Task Force
- **IKE**: Internet Key Exchange
- **IoT**: Internet of Things
- **IP**: Internet Protocol
- **IPS**: Intrusion Prevention System
- **IPsec**: Internet Protocol Security
- **ISP**: Internet Service Provider
- **LACP**: Link Aggregation Control Protocol
- **LAN**: Local Area Network
- **MAC**: Media Access Control
- **MAN**: Metropolitan Area Network
- **MITM**: Man-in-the-Middle
- **MSTP**: Multiple Spanning Tree Protocol
- **NAT**: Network Address Translation
- **NFP**: Network Foundation Protection
- **NGFW**: Next-Generation Firewall
- **NIC**: Network Interface Card
- **NOS**: Network Operating System
- **OS**: Operating System
- **OSPF**: Open Shortest Path First
- **OU**: Organizational Unit
- **PAgP**: Port Aggregation Protocol
- **PoE**: Power over Ethernet
- **QoS**: Quality of Service
- **RBAC**: Role-Based Access Control
- **RFC**: Request for Comments
- **SaaS**: Software as a Service
- **SDN**: Software-Defined Networking
- **SSH**: Secure Shell
- **SSID**: Service Set Identifier
- **SSO**: Single Sign-On
- **STP**: Spanning Tree Protocol
- **SVI**: Switched Virtual Interface
- **TCP**: Transmission Control Protocol
- **TCP/IP**: Transmission Control
- Protocol/Internet Protocol
- **UDP**: User Datagram Protocol
- **UTM**: Unified Threat Management
- **VLAN**: Virtual Local Area Network
- **VM**: Virtual Machine
- **VoIP**: Voice over Internet Protocol
- **VPN**: Virtual Private Network
- **VTP**: VLAN Trunking Protocol
- **VXLAN**: Virtual Extensible LAN
- **WAN**: Wide Area Network
- **WLAN**: Wireless Local Area Network
- **WLC**: Wireless LAN Controller

GENERAL INTRODUCTION

Digital networks are essential to modern communication frameworks, allowing for the effective transfer of information among different devices and platforms. These networks constitute the foundation of the internet, supporting countless services and applications that enhance both personal and professional engagements in the digital era.

Eenterprise networks are customized digital networks designed to address the intricate requirements of large businesses. These networks are created to manage large data amounts, and guarantee secure, dependable communication across different sites. Enterprise networks integrate Local Area Networks (LANs), Wide Area Networks (WANs), and cloud services creating connectivity and collaboration. In enterprise networks, Essential aspects contain security, scalability, and performance, necessitating strong planning and advanced technologies.

Establishing an enterprise network entail more than just linking physical network infrastructure equipment. The most difficult and important part is the planning and design stages, where numerous technical factors and technologies need to be taken into account (OSI model, TCP/IP, ethernet). A properly designed network is vital for scalability. This dissertation will examine the technologies and design factors required for developing a scalable enterprise network.

This graduation thesis is divided into three chapters:

Chapter I: This chapter outlines the development of campus networks from centralized systems to contemporary, software-defined architectures. It emphasizes significant progress such as Ethernet, SDN, and wireless integration, concentrating on scalability, efficiency, and security. Future networks need to emphasize automation, flexibility, and robustness to accommodate developing technologies such as IoT and AI.

Chapter II: This chapter talks about network management and server tools in enterprise network, exploring different types and famous network attacks and network security measures, emphasizing the need for robust security policies to protect network integrity and ensure reliable communication.

Chapter III: This chapter focuses on designing and building the campus network infrastructure. It includes developing a practical plan for gathering and analyzing technical requirements, as well as designing the network's passive and active components. The chapter covers steps for emulating the network topology and testing it with appropriate tools to ensure reliable connectivity and high performance. It also addresses securing the network against cyberattacks by implementing best practices such as configuring security protocols and mitigating potential threats. The success of the design is evaluated through performance verification and connectivity testing within the organization and its external branches.

CHAPTER I:

AN OVERVIEW OF HISTORIC EVOLUTION AND TECHNOLOGY ENTERPRISE CAMPUS NETWORK

I.1 Introduction

Campus networks evolved from the mainframes in the centralized mainframes before 1990, to Ethernet and TCP/IP LANs in the 1990s, to hierarchical designs and VLANs in the 2000s, to current networks with wireless technology, IoT and cloud.

During 1990-2000, hub to Switched Ethernet and Fast Ethernet (100 Mbps) were installed on campuses to provide better performance and relieve congestion. Hierarchical designs (Core, Distribution, Access layers) simplified scalability, and virtual local area networks (VLANs), Layer 3 switching, and spanning tree protocol (STP) provided security and reliability. Collapsed core configurations were implemented on small campuses, whereas large enterprises employed three-tier models for segmentation and efficiency measures.

During 2000-2010 witnessed campus networks transform with Gigabit Ethernet, VoIP, and WLANs to support unified communications and flexible access with 802.11a/b/g/n standards. Network Access Control (NAC), Authentication, Authorization, and Accounting (AAA) (RADIUS/TACACS+), and wireless LAN controllers (WLCs) provided dynamic security and centralized management. Routing had moved from static to dynamic with OSPF optimizing path calculation and HSRP ensuring redundancy for uninterrupted network functionality.

Since 2010, campus networks evolved with SDN, cloud integration, and virtualization to offer scalable, automated, and secure infrastructures. Flexibility, multi-tenancy, and effective routing of traffic are enhanced with technologies like VXLAN/EVPN. Active/passive devices like routers, switches, firewalls, servers, and cables are employed in projects these days for robust and modern network configurations.

I.2 Historical Evolution of campus network and its importance

Prior to 1990, campus networks were centralized mainframe systems; in the 1990s, they changed to local area networks (LANs) using Ethernet and TCP/IP. In the 2000s, scalability and oversight were improved by the switch to hierarchical structures and VLANs. Demands for flexibility and security increased in the 2010s as a result of the expansion of wireless networks, cloud computing, and the Internet of Things. Campus networks are currently being impacted by rapid connectivity, AI-powered automation, and software-defined networking (SDN). Their importance comes from their ability to help modern organizations communicate effectively, stay safe, and be flexible. [1]

I.2.1 Definition of Campus Networks

Campus Network is a distinct type of Metropolitan Area Network that links several LANs within a confined geographical space, like a university campus, corporate office, or government

facility. Campus area networks(CANs) offer a unified network framework that enables users and devices on the campus to interact and exchange resources effectively. [2]

CANs generally contain a core layer, distribution layer, and access layer, where building access nodes link specific buildings or floors to the core network.

I.2.2 Key Drivers of Change: Wireless technologies, IoT, cloud computing

Wireless technologies like Wi-Fi 6 and 7 improve mobility and connectivity in campus networks, allowing seamless communication among devices. IoT integration supports applications in smart campuses such as security, environmental monitoring, and automatic access control. Cloud computing offers elastic resources for data storage, computation, and collaboration, reducing dependence on local infrastructure. Together, these technologies improve efficiency, agility, and security, aligning with modern educational and institutional requirements. As networks expand, they rely on AI-driven automation and edge computing to work better and at low latency.[3]

I.3 Early Beginnings: From Centralized Computing to Local Networks (Pre-1990)

Early campus networks centralized on hub-and-spoke or flat Ethernet topologies, utilizing for connectivity shared media Ethernet (10 Mbps), coaxial cables, and hubs. They primarily supported basic data sharing, email communication, and file servers within buildings, but lacked scalability and security. Due to no redundancy and weak security measures, these networks were prone to congestion, failures, and vulnerability to unauthorized access.

I.3.1 Centralized Computing and Mainframe Systems

Centralized computing indicates a configuration for a single, central device or system manages all processing and data storage. This main unit handles all requests and oversees all data, while every other device in the system is linked to it and depends on it for their computing requirements. A traditional mainframe system is an illustration of a centralized computing system, in which a primary mainframe computer manages all processing and data storage for the system. In this kind of system, users connect to the mainframe using terminals or other devices linked to it.[4]

I.3.2 The Emergence of LANs and Flat Networks

Flat networks refer to network structures where every device is linked to one network segment, lacking any hierarchy or centralized management. In a flat network, every device is linked to a single switch or hub within the same broadcast domain and interacts directly with one another without intermediaries. These linked devices are regarded as equals with identical access levels. While flat networks are inexpensive and simple to establish in any setting, there are multiple architectural disadvantages that must be acknowledged, such as their absence of redundancy, challenges in troubleshooting, and susceptibility to lateral attacks.

I.3.3 Challenges of Flat Networks

1) Problem in Troubleshooting

The simplicity design of a flat network can also make troubleshooting significantly more challenging. When a network issue arises, it may be present nearly anywhere within the network, making the identification of the underlying cause of the issue challenging and time-intensive. In contrast, within a segmented network, identifying the problem's location can be simpler, and even if significant infrastructure requires replacement, the issue can be confined to the network segment containing that infrastructure

2) Higher Lateral Risks

Employing a flat network makes you more susceptible to lateral attacks, enabling attackers to enter through one access point and then move across the breached network unimpeded. For instance, if your organization operates a flat network and malware manages to compromise one of your devices, it can swiftly spread laterally to infect other devices on the network until all devices are affected

3) Low Visibility Cyber Threats

When hackers manage to breach the network perimeter and enter a corporate network, they frequently try to stay hidden while conducting scans and other reconnaissance activities. This enables them to move through the network to locate the most valuable assets they can seize.[5]

I.3.4 Early Fundamental Components: Cables, hubs, servers

Initial campus networks depended on coaxial cables and twisted-pair wiring to create physical connections between devices. Hubs facilitated the distribution of network traffic, but their lack of intelligence led to collisions and decreased efficiency. Servers offered critical capabilities such as file sharing, email services, and centralized data storage for both academic and administrative purposes. These elements constituted the foundation of fundamental local area networks (LANs), facilitating communication within organizations. Nevertheless, because of constrained bandwidth, insufficient security, and a lack of redundancy, these networks had difficulty scaling efficiently.[6]

I.4 The Ethernet Era and Transition to Hierarchical Designs (1990–2000)

Campus networks evolved with Switched Ethernet and Fast Ethernet (100 Mbps), improving performance and reducing network congestion. The three-tier architecture (Core, Distribution, Access) enhanced scalability and efficiency. VLAN segmentation allowed logical separation of networks, while Layer 3 switching introduced routing capabilities within switches. Redundant links and Spanning Tree Protocol (STP) helped prevent network loops and ensured reliability. Basic firewalls and access control lists (ACLs) were integrated to strengthen security measures against unauthorized access.

I.4.1 Dominance of Ethernet and TCP/IP Protocol

IEEE published the IEEE 802.3 standard to specify the physical-layer connection, electrical signals, and Media Access Control (MAC) protocols. The introduction of this standard means the beginning of Ethernet technology. Ethernet was more affordable and simpler to deploy than earlier networking technologies due to the use of twisted pair connections. As a result, Ethernet rapidly emerged as the dominant technology for campus networks.[1]

The TCP/IP model is a simplified framework of the OSI model made up of four layers. It was created specifically for the internet and is commonly utilized in contemporary networking technologies. Like the OSI model, it addresses data transmission through the physical medium, logical addressing and routing, dependable end-to-end communication, and application services.

I.4.2 Transition from Hubs to Switches

Early campus networks relied on hubs at the physical layer, which limited concurrent access and caused performance issues due to expanded collision domains. LANs had to be divided into multiple interconnected segments using expensive, low-speed routers, restricting online access. In the end 1980s, Layer 2 Ethernet switches come in place of hubs, offering dedicated ports and improving scalability. However, broadcast storms in large LANs made a challenge, leading to the need for better management systems. This era marked the rise of network engineers, as campus networks remained expensive and inefficient, primarily supporting basic services like email.[1]

I.4.2.1 Benefits of Switching

A collision domain refers to a group of devices whose frames have the potential to collide. In any network that utilizes a hub, there is a risk of frame collisions, meaning all devices within these Ethernet network types are in the same collision domain and employ CSMA/CD to identify and manage collisions

LAN switches greatly decrease, or may completely remove, the collisions in a LAN. In contrast to hubs, switches do not form a unified shared bus, switches do the following:

- Switches analyze the bits in the incoming frame to send the frame through the specific port needed, instead of all the other ports.
- When a switch has to send several frames through the same port, it stores the frames in memory and transmits them one by one, thus preventing collisions.

In addition, switches that have just a single device connected to each port enable the implementation of full-duplex operation. Full-duplex indicates that the network interface card (NIC) can simultaneously send and receive data, essentially increasing the bandwidth of a 100 Mbps connection to 200 Mbps—100 Mbps for transmission and 100 Mbps for reception.[7]

I.4.3 Shift to Architectural Models

The enterprise network architecture employs a hierarchical design framework that segments the network into modular layers, each performing unique functions. This modular method enhances performance, streamlines design, boosts scalability, and minimizes troubleshooting duration. The hierarchical structure is made up of three primary layers which are:

Access Layer

The access layer, famous as the network edge, is the point at which end-user devices or endpoints link to the network. It offers high-bandwidth device connectivity; this layer can be divided (for instance, using VLANs) to allocate different devices into separate logical networks for improved performance, management, and security reasons.

The access layer serves as the link for endpoints, significantly contributing to the network's defense against harmful attacks. This safeguard involves ensuring that the end users and endpoints linking to the network are blocked from accessing services they are not permitted to use.[8]

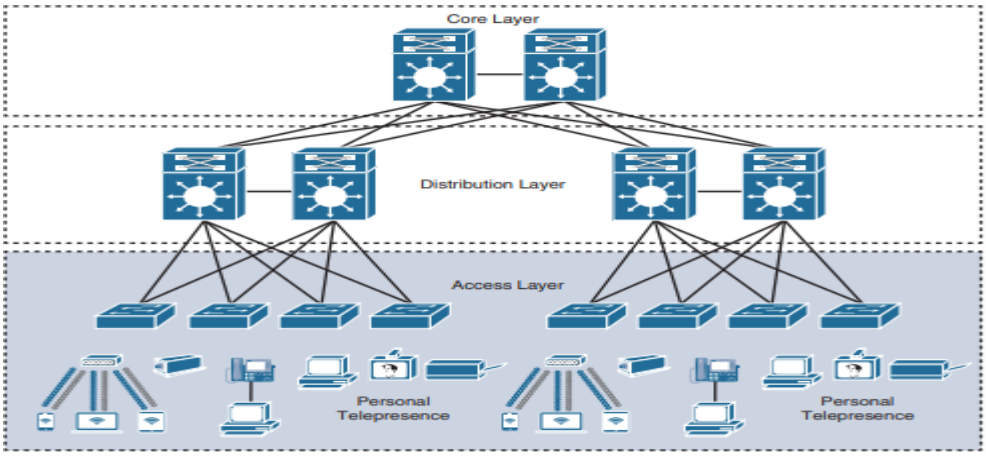


Figure I.1 Access Layer Connectivity [8]

Distribution Layer

The main role of the distribution layer is to aggregate access layer switches within a specific building or campus. The distribution layer acts as a border between the access layer's Layer 2 domain and the core's Layer 3 domain , this border serves two important roles for the LAN: On the Layer 2 side, the distribution layer creates a border for Spanning Tree Protocol (STP), which restricts the spread of Layer 2 issues, while on the Layer 3 side, the distribution layer offers a logical point to condense IP routing information as it enters the core of the network, The summarization decreases IP routing tables to simplify troubleshooting and minimizes protocol overhead for quicker recovery from failures.

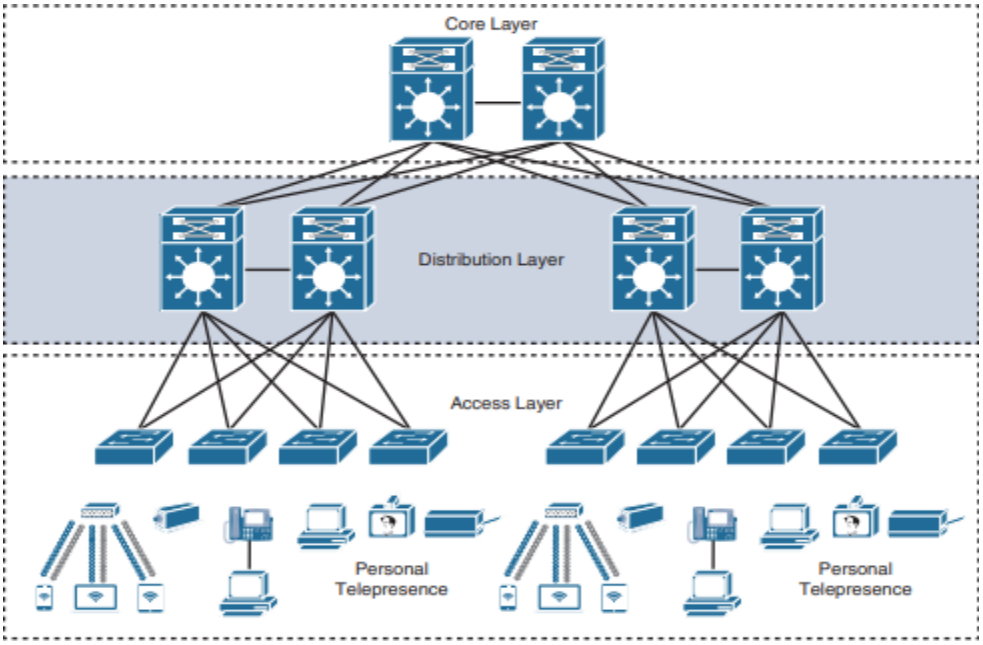


Figure I.2 Distribution Layer Connectivity [8]

Core Layer

The central layer serves as the foundation and aggregation hub for various networks, offering scalability, enhanced availability, and quick responsiveness approaching the network.

The core can deliver rapid connectivity for large businesses with several campuses' networks spread across the globe, and it can additionally offer connectivity among the end-user/endpoint campus entry layer and additional network segments, like the data center, the personal cloud, the shared cloud, the wide area network, the Internet perimeter, and network solutions.

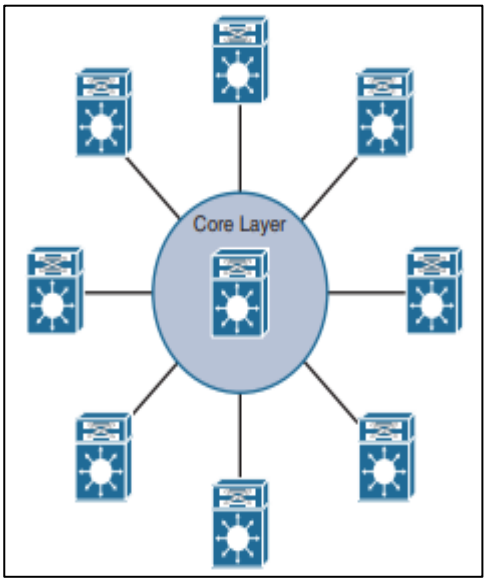


Figure I.3 Core Layer Connectivity

I.4.3.1 Two-Tier (Collapsed Core) Design Model

in smaller campus network, department might be spread across multiple floors of one building. The functions of collapsed core networks resemble those of their larger, three-layered equivalents. However, the collapsed core architecture is a better option for smaller campuses because of several unique benefits, and it can provide similar advantages with a more straightforward model and reduced costs compared to a three-tier design.

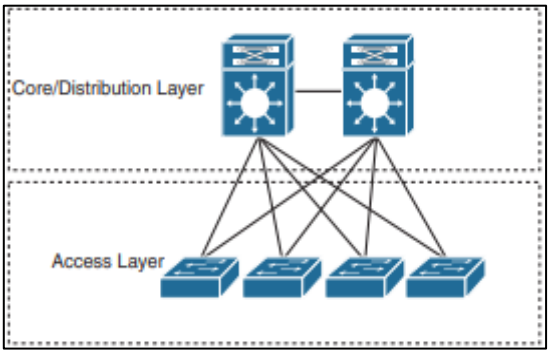


Figure I.4 Two-Tier Collapsed Core Design

I.4.3.2 Three-Tier Hierarchical Model

Enterprises work with the Three-Tier model as their network structure. A three-tier architecture distinguishes the core and distribution layers and is advised when more than two pairs of distribution switches are necessary. This establishes a core, distribution, and access layer within the network. The Core layer of the network's backbone offers a fast connectivity between devices. The Distribution layer collects traffic from the Access layer and authorizes access to the Core layer. [8]

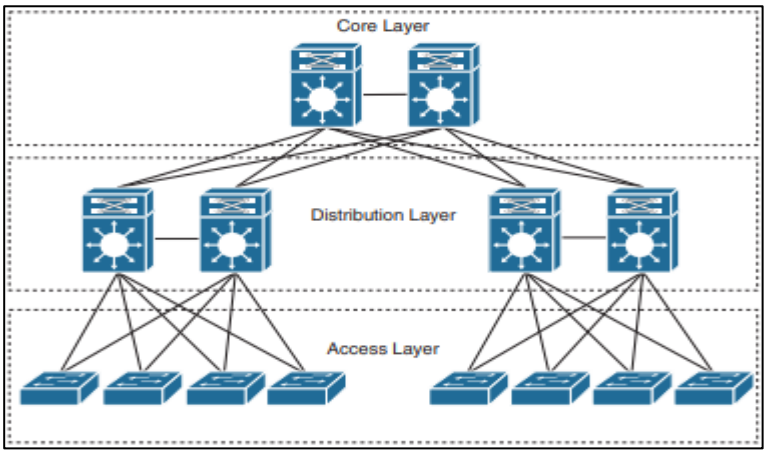


Figure I.5 Three-Tier Hierarchical Model [8]

I.4.4 Switching Protocols

I.4.4.1 Spanning Tree Protocol (STP)

STP is a layer 2 protocol that disable switching loops in redundant network configurations. Switching loops may lead to broadcast storms, making the network unusable. STP maintains a loop-free architecture by strategically blocking redundant connections and activating alternative routes when necessary. Due to a link failure. [9]

A. STP Operations:

Root Bridge Election: STP selects a root bridge according to set criteria, including bridge priority (a configurable parameter) and MAC address (used as a tiebreaker). The root bridge

acts as the framework for every other bridge in the network, and all routes are determined according to their distance from the root bridge

There are a steps to follow in the election of the root bridge

1. **Bridge Priority** Every bridge has a priority value, which is an adjustable parameter that ranges from 0 to 61440 (in increments of 4,096). Values with lower priority suggest an increased chance of becoming the root bridge. The standard priority value is 32768.
2. **Bridge MAC Address** the bridge with the lowest MAC address is designated as the root bridge if several bridges have the same priority value. This acts as a deciding factor when priorities are the same.
3. **Root Bridge Advertisement:** The chosen root bridge broadcasts Bridge Protocol Data Units (BPDUs) declaring itself as the root bridge. These BPDUs include the priority and MAC address of the root bridge.
4. **BPDU Propagation** Non-root bridges take the BPDUs and refresh their spanning tree data, identifying the root bridge and determining the shortest route to it.
5. **Root Path Cost Calculation:** Every non-root bridge determines the path cost to the root bridge by considering the port speed and the total cost of links along that path. The route with the least expense is selected as the primary path
6. **Root Port Selection:** On every non-root bridge, the port nearest to the root bridge (with the least root path cost) is designated as the root port, obligated with directing traffic towards the root bridge.
7. **Designated Port Election:** In every LAN segment, the port that has the lowest path cost to the root bridge is designated as the designated. Port, which is responsible for forwarding traffic on that segment.

The root bridge election procedure guarantees the existence of a single active root bridge in the network, avoiding switching loops and maintaining a stable spanning tree structure. When the root bridge fail, the election process will automatically choose a new root bridge according to the priorities and MAC addresses of the other bridges. [10].

B. **STP Port States and Roles**

a) **Port States:**

STP has five port states to control the flow of traffic and prevent loops:

Listening: The port gets ready to relay traffic by handling BPDUs but does not send data frames. It comprehends the network topology but does not engage in frame transmission.

Learning: The port fills the MAC address table by recognizing the source addresses of incoming frames, yet it does not transmit data frames. It will be ready to move into the forwarding state.

Forwarding: The port efficiently routes traffic and participate in the spanning tree structure, enabling the sending and receiving of data frames.

Blocking: In this condition, the port ignores all incoming traffic except from Bridge

Protocol Data Units (BPDUs) to avoid loops still being a part of the spanning tree topology. This utilized for redundant links and backup ports.

Disabled: The port has been administratively disabled and is not involved in the spanning tree topology or forwarding any traffic.

Ports shift through these states according to spanning tree computations and alterations in network topology, maintaining a loop-free setting while offering redundancy and failover options. [10].

b) Port Roles:

Root Port: The port obliged with directing traffic to the root bridge. Each non-root bridge possesses one root port, which is the port that has the lowest root path cost to the root bridge.

Designated Port: The port that transmit traffic for a single network segment or LAN. Every network segment has a single designated port, which is the port that has the lowest root path cost within that segment.

Backup Port: A backup port for the designated port. If the designated port down, the backup port with the next lowest root path cost on that segment assumes control and becomes the new designated port, avoiding loops.

Alternate Port: A backup port for the root port. if the root port down, the alternate port that has the next lowest root path cost accept control and becomes the new root port, providing the redundancy.

Disabled Port: A port that has been administratively down and doesn't be part of the spanning tree topology.

I.4.4.2 Virtual Local Area Networks (VLANs)

Virtual Local Area Networks (VLANs) are logical segments of one physical local area network (LAN) framework, allowing the establishment of distinct broadcast domains. VLANs offer a method to logically divide a network into several isolated virtual networks, promoting better security, increased network efficiency, and simplified network management [10].

I.4.4.3 Switched Virtual Interfaces (SVIs)

In a Layer 2 network that uses VLANs, transmission between devices in different VLANs usually needs a specific Layer 3 device which is a router. Nonetheless, Cisco switches provide a robust feature called Switched Virtual Interfaces (SVIs) that connects Layer 2 and Layer 3 capabilities. [11]

For example, SVI is a virtual link connecting your VLAN to the routing engine which is switch. This bridge enables devices located in a VLAN to communicate directly with devices in other VLANs or external networks, removing the necessity for a separate physical router for each VLAN.

A. Advantages of Using SVIs

- **Simplified Network Management:** SVIs simplify network management by allowing inter-VLAN routing directly on the switch. We can control VLAN routing setups from one device, minimizing complexity and possible configuration mistakes.
- **Reduced Hardware Costs:** SVIs remove the need for a separate router for every VLAN, resulting in considerable savings in hardware purchases and installation.
- **Improved Scalability:** when the network grows with more VLANs, SVIs easily adapt to these modifications without needing extra physical routing resources.

SVIs configuration needs:

A) Ip Addressing: Every SVI needs a distinct IP address, allowing it to operate as a Layer 3 endpoint for the associated VLAN.

B) Default Gateway: Devices in the VLAN use the SVI IP address as their default gateway to route traffic to different networks.

I.4.4.4 EtherChannel

EtherChannel, referred to as Port Channeling or Link Aggregation, is a method that combines several physical Ethernet connections into one logical link, offering enhanced bandwidth and redundancy.

1. EtherChannel Protocols

Link Aggregation Control Protocol (LACP): LACP is an IEEE protocol that dynamically invent and control bundles by exchanging control packets between the participating devices.

Port Aggregation Protocol (PAgP): PAgP is protocol owned by cisco for the automatic setup and management of EtherChannel groups on Cisco equipment. [12]

2. EtherChannel Benefits:

Redundancy: If one of the physical links in an EtherChannel down, the traffic is instantly rerouted through the remaining active links, ensuring reliability and reducing downtime.

Higher Bandwidth: EtherChannel combines multiple physical connections links into one, boosting bandwidth, allowing higher data transfer Speeds, and enhance the network performance.

Load Balancing: Traffic is shared across the grouped links, making the best use of available bandwidth and minimizing congestion on individual connections.

I.5 The Wireless Revolution and Growing Complexity (2000–2010)

Campus networking was transformed with the development of Gigabit Ethernet, VoIP, and wireless LANs, which allowed for integrated communication and quicker data transfer. By combining phone, video, and data over IP, unified communications increased efficiency and teamwork. Flexible access across campus contexts was made possible by the expansion of connection brought about by the deployment of 802.11a/b/g/n wireless standards. For large-scale installations, wireless LAN controllers (WLCs) optimize security and performance through centralized network management. Access to vital resources was secured through the enforcement of authentication and authorization policies using Network Access Control (NAC) and centralized AAA (RADIUS/TACACS+).

I.5.1 Spread of WLANs and the Impact of Wi-Fi

Setting up a WLAN goes beyond just choosing the preferred standard and a security method. The positioning of access points can influence throughput more than the standards do. It is essential to understand how elements such as topology, distance, and the positioning of access points affect the performance of a WLAN.

It exists two modes for the implementation of a WLAN:

- **Ad hoc mode**: Independent Basic Service Set (IBSS) serves as the topology mode for ad hoc networks. Mobile devices connect directly without needing an intermediary access point. Operating systems like Windows have simplified the setup process for this peer-to-peer network. This configuration can be utilized in a small office (or home office) to enable a laptop to connect with the main PC or for multiple individuals to easily exchange files. The reach is restricted. All individuals should be able to listen to one another. An access point is unnecessary. One disadvantage of peer-to-peer networks is that securing them is challenging

- **Infrastructure Mode**: In infrastructure mode, clients connect through an access point. There are two infrastructure modes:
    - **Basic Service Set (BSS):** The units that constitute a BSS are mobile clients using one access point to talk to one another or to hard-wired network resources. The Basic Service Set Identifier (BSSID) is the Layer 2 MAC address of the radio card of the access point of a BSS. Although the wireless topology and the BSS access point each consist of a single component in the BSS and are both identified by a BSSID, the wireless network itself is promoted by a SSID, announcing the existence of the wireless network to roaming clients. The SSID is a customizable wireless network name and may consist of up to 32 characters that are case-sensitive.

- **Extended Services Set (ESS):** The wireless topology is extended with two or more BSSs connected via a distribution system (DS) or a wired network. An ESS typically features a shared SSID, enabling seamless roaming between access points without needing client configuration.

In today's, in a connected world, Wi-Fi has emerged as the leading and most affordable method for offering connectivity to numerous devices. The quantity of devices linked to networks is constantly increasing, fostering innovation across different sectors. As we transition to a fully digital environment, we will increasingly depend on Wi-Fi for tasks beyond its traditional uses. Consequently, it is essential to reconsider our networking strategy, emphasizing smart solutions that value reliability and predictability.[13]

I.5.2 Network Routing: From Static to Dynamic

I.5.2.1 Static Routing

Static, default, and connected routes represent the most prevalent types of routes, as they are present on the majority of routers. Static and default routes are specifically set up and automatically incorporated into the local routing table when configured. Their administrative distance is 1 and the path metric is zero (0), the static routing has the lowest administrative distance in all routing protocols.[14]

I.5.2.2 Dynamic Routing

Is a collection of protocols and processes utilized by routers to share routing data and automatically modify their routing tables in response to changes in network topology. These protocols enable effective packet transmission both within and across autonomous systems.

I.5.3 Routing Protocols

I.5.3.1 OSPF (Open Shortest Path First)

OSPF is one of dynamic routing protocols used in computer networks, enabling routers to share routing information It works using link-state (Dijkstra) algorithms, where the exchange of information about network topology in routers is through Link-State Advertisements (LSAs). OSPF enables routers to autonomously identify the optimal path to destinations, improving network efficiency. It facilitates multiple functionalities, such as zones for structured network architecture, enabling scalability and effective routing in intricate networks.

- **Characteristic of OSPF**

Link-State Routing Protocol: OSPF is a link state protocol, which implies it keeps a map (link-state database) of the network containing all the potential routes and their statuses. Every router maintains a comprehensive view of the network structure.

Convergence: OSPF rapidly adjusts routes when changes happen in the network, guaranteeing minimal interruptions and effective network functionality. this swift convergence is accomplished by employing Dijkstra's algorithm.

Hierarchical Design: OSPF uses a hierarchical design with areas to enhance traffic flow and decrease the size of routing tables. The backbone area (Area 0) connects all other areas, enabling optimized route summarization and reducing routing overhead.

Cost-based Routing: OSPF directs packets according to cost, usually represented by bandwidth. The route with the smallest total cost (the total of all costs along the route) is selected as the optimal path.

Authentication: OSPF can be set up with basic password authentication or cryptographic authentication (utilizing MD5 or SHA) to protect routing exchanges and block unauthorized routing updates**.**

Neighbor Relationship: OSPF routers create neighbor connections by utilizing Hello packets. After establishing a neighbor relationship, routers exchange link-state advertisements (LSAs) to share routing data and construct the link-state database.

- **OSPF Tables**

The OSPF Neighbor Table: is an active database that keeps information about nearby routers with formed adjacencies, essential for the exchange of routing information. It logs crucial details like Neighbor Router ID, IP Address, State, and DR/BDR status. This table helps track OSPFneighbor connections, identify connectivity problems, and maintain optimal network performance.

Link State Data Base: identified as the topology table or database table, it contains the entire network topology, allowing routers to understand all network paths, names, and identities of routers. It retains this extensive network data to enable effective routing throughout the network. The topology table oversees the updating procedure, encompassing network additions, removals, or modifications. Each time a change happens, like adding, altering, or removing a network, the update procedure is initiated. These updates are subsequently shared with all adjacent routers to guarantee they obtain the most recent information, preserving uniformity throughout the network.

OSPF Routing Table: referred to as the OSPF forwarding database, is an essential part of OSPF routing. It retains details regarding the network topology encompassing routers, connections, and their related metrics. The OSPF routing table is updated in real-time using data obtained from adjacent routers via OSPF LSAs (Link-State Advertisements).[14]

We can find some information in the OSPF routing table:

- **Administrative Distance:** A value given to OSPF routes indicating their reliability or preference in comparison to routes from different routing protocols. OSPF routes usually possess an administrative distance of 110.
- **Path Metrics:** metrics employed by OSPF to determine the shortest route to every destination, generally founded on link expenses.
- **Router ID:** The identifier for every router involved in OSPF. It is utilized to recognize routers in the OSPF area**.**
- **Neighbor Router Information:** information concerning adjacent routers, containing their Router IDs and connection status. This information is crucial for creating and sustaining OSPF neighbor connections.
- **Link State Advertisement (LSAs)**: Details concerning the network connections and routers inside the OSPF area. LSAs contain information like router IDs, network IDs, link costs, and types of links.[9]

I.5.3.2 HSRP (Hot Standby Router Protocol)

Hot Standby Router Protocol (HSRP) is a Cisco-created proprietary protocol that guarantees redundancy for a local area network, HSRP allows the configuration of two or more routers to work as standby routers, while designating one router as the active router at any time. All routers that are in single HSRP group utilize a shared MAC address and IP address between them, working as the primary gateway for the local network. The Active router controls the transmission of the traffic. If it fails, the Standby router will work in the active router place and controls the traffic.[15]

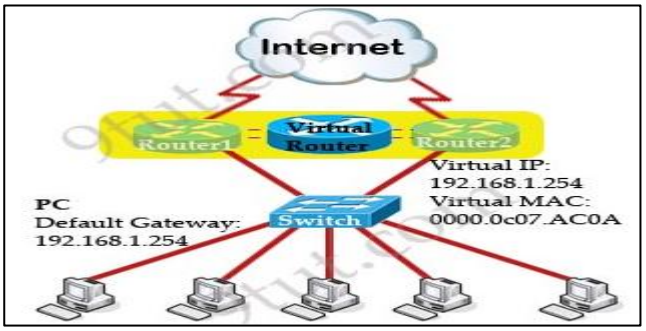


Figure I.6 Hot Standby Router Protocol (HSRP) [16]

I.6 The Era of Software-Defined Networking and Cloud Integration (2010–present)

The introduction of 10G Ethernet, SDN, and WLAN 802.11ac revolutionized campus networks by offering rapid connectivity and booted network management. The movement towards BYOD (Bring Your Own Device) enhanced mobility, necessitating strong security protocols. Cloud integration (SaaS, IaaS) facilitated scalable computing and storage options, lessening dependence on physical infrastructure. Management that is centralized via software platforms and controllers optimized operations, guaranteeing automation and efficiency. To improve security, identity-driven access and micro segmentation reduced risks, offering enhanced network protection

I.6.1 Emergence of SDN and VXLAN/EVPN:

Software-Defined Networking (SDN) arose as a revolutionary method for network management, distinguishing the control plane from the data plane to facilitate centralized, programmable network supervision. SDN started to gain popularity in the early 2010s, propelled by the demand for automation, scalability, and adaptability in enterprise and cloud settings

VXLAN (Virtual Extensible LAN) was developed to address the limitations of traditional VLANs by enabling scalable Layer 2 networks over Layer 3 infrastructure. It gained widespread acceptance in 2011, enabling improved multi-tenant segmentation and network virtualization

EVPN (Ethernet VPN) developed as a control-plane solution for VXLAN, offering effective Layer 2 and Layer 3 forwarding with improved redundancy and security. It was established as a standard in 2014, providing enhanced integration with SDN frameworks and boosting data center connectivity. [17]

I.6.2 Advantages of Virtual Architectures: Flexibility, Horizontal Scaling:

Virtual architectures offer flexibility, allowing networks to adapt dynamically to changing workloads, resource demands, and operational needs. They enable horizontal scalability, making it easy to expand infrastructure without disrupting existing systems, ensuring efficient scaling of applications and services. By separating control and data planes, technologies like SDN and VXLAN enhance automation, reduce hardware dependency, and simplify network management. Virtualized environments support multi-tenancy, improving cost efficiency by optimizing shared resources. Additionally, they strengthen security, enabling better isolation, segmentation, and traffic control for modern campus networks [18]

I.6.3 Integration with the Cloud and the Internet of Things:

Cloud and IoT integration in campus networks enhances connectivity, automation, and efficiency. Cloud-based solutions offer centralized management, scalability, and real-time data

processing, whereas IoT devices foster intelligent monitoring, security, and resource optimization. Huawei's Cloud Campus and Smart Campus architectures are some of the solutions that leverage AI, big data, and SDN to build intelligent, secure, and converged campus environments. IoT-enabled smart campuses also facilitate sustainability and operational efficiency.[19]

I.7 Practical Applications and Case Studies

In our campus network project, we are going to use some active/passive components and devices to configure and test our network connectivity such as

I.7.1 Passive Components

Passive components are crucial for creating connectivity, and they don't require power to work. Their essential function is to provide a pathway for data transmission without actively processing the signals. Here are some passive components that we are going to use**:**

A. **Cat6 Cable:** is network cable that is used for creating a functional network point.

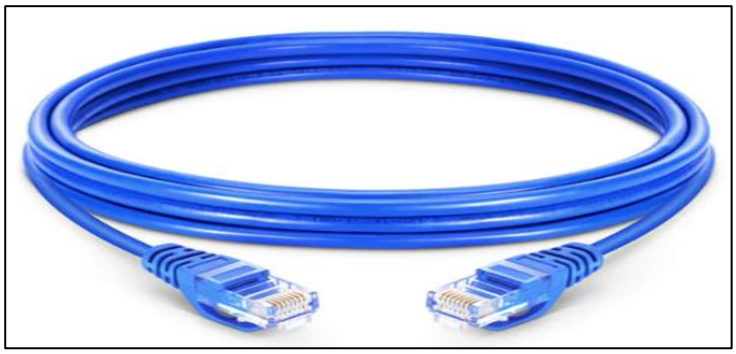


Figure I.7 Category 6 Cable (cat6) [20]

B. **Keystone Jack:** is a Cat6 module to connect both the end user side and the patch panel side.

Figure I.8 Keystone Jack (cat6) [21]

C. **Faceplate:** is the component where the keystone jack will be placed, and it comes in various types including: single, dual, and quad single face plate.

Figure I.9 Faceplate Keystone Jack (cat6) [22]

D. **Patch cord:** is a pre-made cat6 cable that can be found in the market in various lengths including: 1m, 2m, 3m, 5m, 10m, 15m, and 20m.it is used to extend the connection between the faceplate and the user's pc, as well as the patch panel to the network switch.

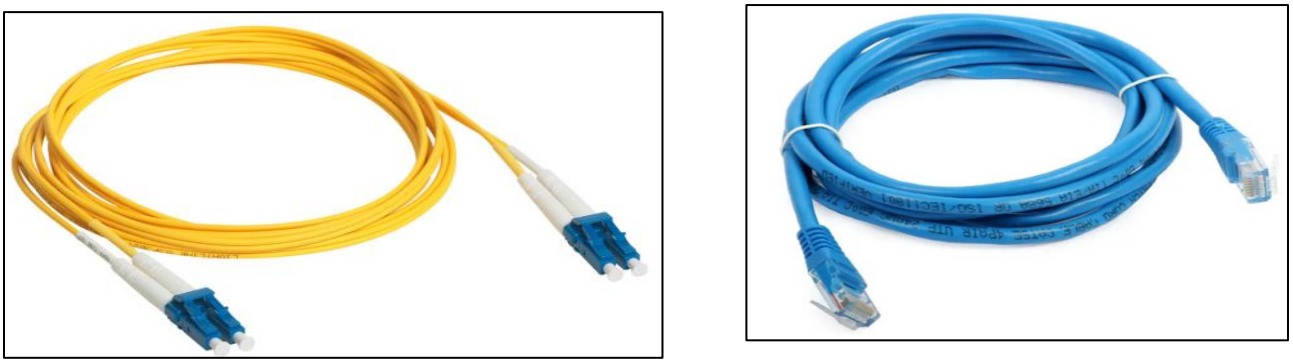


Figure I.10 Patch Cords [23][24]

E. **Patch panel:** It is the holder for keystone jacks from the server side or cabinet side, and it is disponible with 24 or 48 ports.

Figure I.11 Patch Panel with 48 Ports

Figure I.12 Patch Panel with 24 Ports [25]

F. **Rack:** system or framework to support and arrange different hardware elements like servers, networking equipment, and additional apparatus in a consistent way.

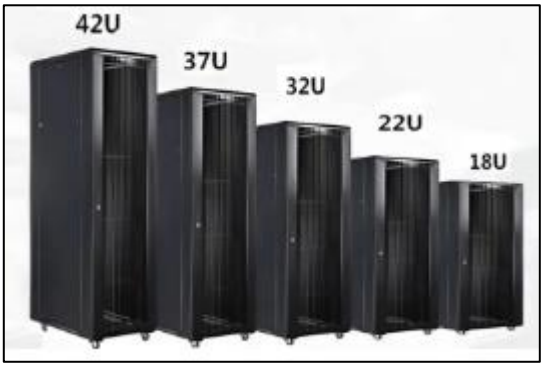


Figure I.13 Rack cabinet with Different Units [26]

I.7.2 Active Components

1. Routers

Devices that connect various networks and direct data packets among them, facilitating communication across multiple networks or the internet.

Cisco is one of the top and well-known firms in the networking industry. It provides big selection of routing devices that meet the requirements of its clients, from small to medium-sized businesses to large companies. Notable among its devices are the ISR and Catalyst series, offered in various versions.

Figure I.14 Cisco Router ISR 4331/K9[27]

Characteristics of Cisco Router ISR 4331/K9:

- **Ports**: Includes **3 onboard 10/100/1000 Ethernet ports**, with **2 RJ-45-based ports** and **2 SFP-based ports**.
- **Aggregate Throughput**: Supports **100 Mbps to 300 Mbps** depending on licensing and configuration.
- **Expansion Slots** :
    - **1 Enhanced Service-Module (SM-X) slot** for flexible deployment.

- **2 Network Interface Module (NIM) slots** for additional connectivity options.

- **Memory**: Comes with **4 GB default RAM**, expandable up to **16 GB**.
- **Flash Storage**: **4 GB default**, expandable up to **16 GB**.
- **Power Options**: Supports **AC and PoE** power supply.
- **Rack Height**: **1 RU**, making it compact for rack-mounted installations.[20]

2. **Switches**

Devices that enable communication among devices in a local area network (LAN). They function at the data link layer of the OSI model and utilize MAC addresses to direct data to the correct destination device.

with the routers, Cisco is also known for its range of switches, which are crucial to network infrastructure. The series of Cisco Catalyst, one of the famous switch series is the Catalyst 2960

Figure I.15 Catalyst WS-C2960X-24PS-L [28]

More than switch, we are going to use in our project the multi-layer switch. These switches match the characteristics of usual Layer 2 switches with the routing functions of Layer 3 devices. This integration allows them to make forwarding choices based on MAC addresses (Layer 2) and IP addresses (Layer 3), leading to enhance traffic routing and better network performance.

3. Firewalls

Firewalls are vital active network elements that function as security borders, overseeing and managing the incoming and the outgoing network traffic according to the security protocols. Cybersecurity companies such as Cisco and Fortinet give a variety of firewall solutions designed for various settings, ranging from small businesses to large enterprises and service providers to provide network protection.

In our project we will work with cisco ASA firewall to ensure the security of the network.

Figure I.16 Cisco ASA Firewalls [29]

4. Servers

Servers are obligated devices of today's network infrastructure, acting as the foundation for multiple services and applications. These robust computers are designed to manage significant workloads and offer centralized storage, processing, and management functionalities.

Top server manufacturers provide a vast array of server models designed to address the varied requirements of businesses. Servers are vital in contemporary network infrastructures, allowing organizations to provide essential services, handle data, and effectively and dependably support diverse business activities.

.

Figure I.17 Server Models [30]

I.8 Conclusion

This chapter has explored the historical evolution of campus networks, from centralized mainframe systems to today's software-defined, cloud-integrated architectures. We examined key technological advancements Ethernet, hierarchical designs, wireless integration, and SDN that have shaped modern network infrastructures. The transition from flat networks to segmented, secure architectures highlight the growing need for scalability, performance, and robust security in enterprise environments. Case studies on active and passive components demonstrate how these technologies are applied in real-world deployments. As networks continue evolving with IoT, AI, and cloud computing, future campus designs must prioritize automation, flexibility, and threat resilience. This foundation sets the stage for our practical implementation in subsequent chapters.

CHAPTER II:

Enterprise Network Administration: Threats, Vulnerabilities, and Countermeasures

II.1 Introduction

This chapter navigates the crucial intersections of network management, network attacks, and network security.

We begin by dissecting essential discipline of network management. This section explains the server technologies, tools, and protocols employed to maintain the operational integrity and optimal performance of complex network infrastructures. Efficient management ensures reliability and responsiveness.

Then, we delve into the anatomy of network attacks, exploring diverse definitions, types of attacks, and most confrontation attacks that menace the network security. Understanding these malicious endeavors is paramount for effective defense

Finally, the chapter explains the exploration of network security. We will examine a range of defensive mechanisms, including Network Foundation Protection (NFP) framework and its components, the role of IPsec vpn in securing data and layer 2 security protocol. we will go to one of security devices, such as firewalls, the objective is to provide a comprehensive understanding of building a resilient security posture capable of protecting networks and their valuable data against the threats previously discussed.

By investigating these three interconnected domains, this chapter aims to provide a foundational profound viewpoint on the challenges and solutions inherent in securing and managing the digital networks.

II.2 Network Management

Efficient network management is essential for guaranteeing the seamless functionality, performance, and security of enterprise networks. Network management contain a variety of tasks and Operations focused on monitoring, configuring, troubleshooting, and sustaining the different elements and services in the network infrastructure. These activities are usually Executed with the help of special network management tools, protocols, and technologies.

Servers are essential for managing networks as they host and deliver different network services, management systems, and monitoring tools. Server technologies facilitate centralized management, resource distribution, and policy implementation throughout the whole network framework. [31]

II.2.1 Servers tools in Enterprise Networks

In enterprise network environments, servers are vital for delivering different network services, managing resources, and guaranteeing the overall operation and security of the network infrastructure. Servers are robust computer systems created to manage high-demand processing operations, information storage, and connectivity services.[32]

II.2.1.1 Server Roles and Functions in Enterprise Networks

Servers can be classified according to their roles and functions in the network several typical types of servers contain:

Server roles	Functions
File Servers	specialized in storing and overseeing shared files and directories, facilitating centralized access and control of data throughout the network
Directory Services Servers	offers centralized authentication, authorization, and management of user accounts, computers, and other network resources.
Web Servers	host and deliver web content, web applications, and web services to clients over the internet or an intranet
Print Servers	manage network printers, allowing shared access to printing resources
Application Servers	control specific services and applications, such as email servers, database servers, or collaboration platforms
Monitoring and Management Servers	analyze network performance data, monitor system health, provide tools for centralized administration and management of network resources.
Virtualization Servers	host and manage multiple virtual machines (VMs) on a single physical server, enabling efficient resource utilization and server consolidation.
DHCP Servers	the server provides IP addresses to clients on the network. The DHCP feature configures settings automatically to prevent user configuration error and additional routing issues.
DNS Servers	the Domain Name System (DNS) keeps records that this service uses to convert domain names and computer addresses names converted to IP addresses
Security Servers	applying security measures such as firewalls, intrusion detection/prevention systems, and antivirus solutions for protecting the network from threats

Table II.1: Server Roles and Functions in Enterprise Networks

II.2.1.2 Active Directory Domain Services (AD DS) Functionalities

Within our enterprise network management, we have implemented Active Directory Domain Services (AD DS) for arranging network resources, facilitating centralized authentication, authorization, and administration of user profiles, devices, and various network components.[32]

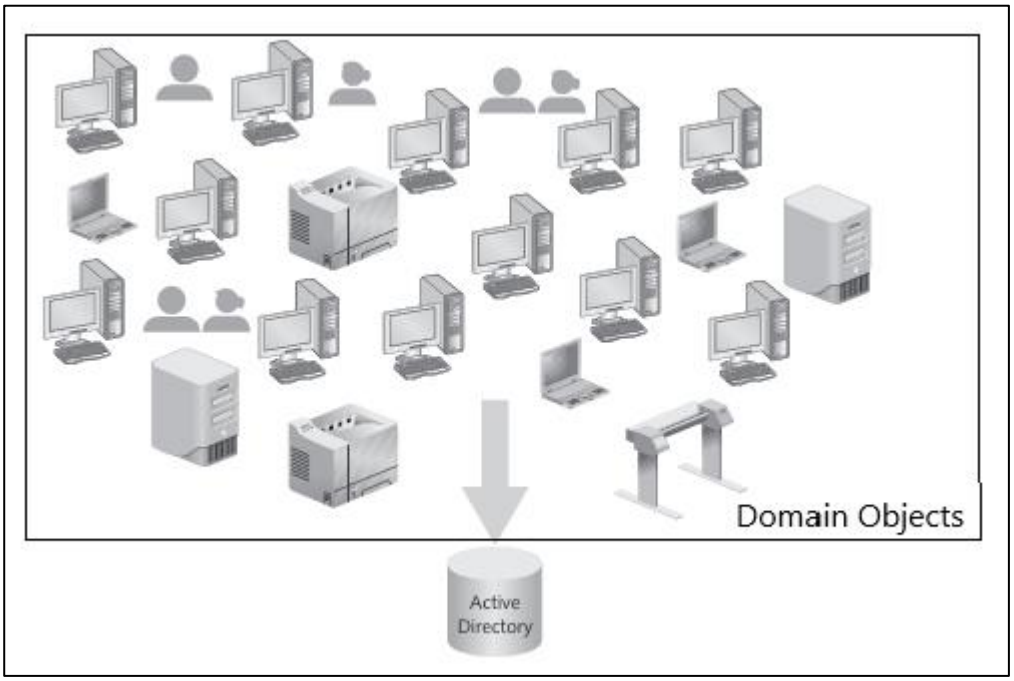


Figure II.1 Active Directory Domain Objects

With AD DS, the following benefits are guaranteed in our enterprise network framework environment as**:**

1. **Centralized User and Computer Management:** AD DS permit administrators to centrally create and manage user accounts, computer accounts, and groups. This simplifies the procedure for granting or retracting access to network resources, implementing security policies, and overseeing user permissions throughout the organization.

2. **Group Policy Management:** AD DS allows administrators to establish and enforce security protocols, desktop setups, and user preferences via Group Policy Objects (GPOs). GPOs can be utilized for users, computers, or organizational units, guaranteeing uniform and standardized configuration throughout the enterprise.

3. **Single Sign On (SSO):** users can log in a single time and access multiple network resources, including file shares printers, and applications, without needing to provide their credentials again. This improves user productivity and security by lessening the requirements for various passwords.

4. **Hierarchical Structure:** Active Directory arranges network resources into logical structure known as domains and organizational units (OUs). This hierarchical framework enables effective distribution of administrative duties and improved organization of resources according to geographic areas, departments, or various other factors.

5. **Integration with Microsoft Technologies:** Active Directory works with different Microsoft technologies, as Exchange Server for email, SharePoint for collaboration, and System Center for monitoring and management, Offering cohesive and uniform management experience.

6. **Availability and Redundancy:** Windows Server offers capabilities such as Active Directory Replication and Failover Clustering, which guarantee high availability and redundancy of Active Directory services, reducing downtime and enhancing fault tolerance.

II.3 Network Attacks

In this following paragraph we will introduce some original definitions in network attacks that it contained in IETF RFC 2828 which are**:**

- **Vulnerability:** A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Most systems possess some vulnerabilities, but this does not imply that the systems are overly defective to be used. Not every threat leads to an attack, and not every attack is successful. Achievement relies on the level of vulnerability, the intensity of attacks, and the efficiency of any defensive measures implemented.

- **Threat:** A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

  A threat refers to a potential risk that could take advantage of a weakness. A threat may be classified as "intentional" (deliberate; for instance, an individual hacker or a criminal organization) or "accidental" (for example, the possibility of a computer failing, or an "act of God" like an earthquake, wildfire, or tornado)
- **Risk:** An expectation of loss expressed as the probability that particular threat will exploit a particular vulnerability with particular harmful result.
- **Attack:** An assault on system security that derives from an intelligent threat., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system. [33]

II.3.1 Types of Attacks

We will define the most common types of attacks which derived into**:**

II.3.1.1 Passive Attacks

The passive attacks are defined as efforts to Understand information from the system without impacting system resources.[34]

in the passive attack, the system remains unharmed. The key point is that in a passive attack, the Victim does not be informed about the attack.

Figure II.2 Passive Attack

II.3.1.2 Active Attacks

The active attacks are defined as attempts to alter system resources or affect their operation. The attacker attempts to modify message content. As a result of the active attack, the system is continually compromised, and its resources may be modified [34]

Figure II.3 Active Attack

In the following table we summarize the main difference between the passive and active attacks

Passive attack	Active attack
Passive attacks are very difficult to detect because they do not involve any alteration of the data.	Hard to prevent (software, network, hardware, vulnerability)
Encryption prevent the success of the passive Attack	If the detection has a deterrent effect, it may also contribute to prevention.
the sender nor receiver are aware about the attack	detect the active attacks earlier and to recover from any disruption or delays caused by the attacks.
Passive Attack is a danger to Confidentiality.	Active Attack is a danger to Integrity and availability

Table II.2 Difference Between Passive and Active Attacks [35]

II.3.2 Most Confrontation Attacks

We have implemented these attacks for testing the security policies of our enterprise infrastructure

II.3.2.1 Man-in-the Middle Attacks(MITM)

A man-in-the-middle attack occurs when attackers insert themselves between two communicating devices to conduct surveillance or monitoring the data as it moves between them. This may occur at Layer 2 or Layer 3. The primary aim is eavesdropping, allowing an attacker to observe all the data flow.

If this occurs at Layer 2, the attacker fakes Layer 2 MAC addresses to convince the devices on a LAN that the attacker's Layer 2 address is that of its default gateway. This process is referred as ARP poisoning. Frames intended for the default gateway are redirected by the switch to the Layer 2 address of the attacker within the same network.

The attacker might also execute the attack by making a switch into the network and manipulating the Spanning Tree Protocol (STP) to establish itself as the root switch (have the capacity to view all traffic that must pass through the root switch).

A man-in-the-middle attack can happen at Layer 3 by introducing a malicious router into the network and deceiving the other routers into thinking this new router offers a better path. This might lead to network traffic passing through the unauthorized router, enabling the attacker to capture network data once more. You can reduce the impact of such attacks through several methods, including implementing routing authentication protocols and controlling the flow of information that is advertised or learned on designated interfaces. [36]

It exists different types of MITM attacks for example DHCP starvation and packet sniffing

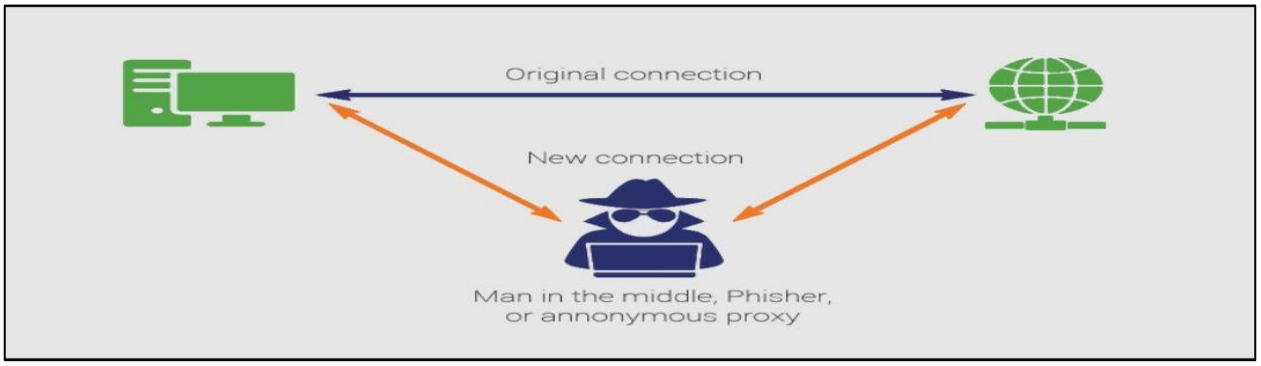


Figure II.4 Man-in-the Middle Attack [37]

II.3.2.2 Spoofing and Denial Of Service Attacks

In a spoofing attack, an attacker mimics a different device to carry out an assault. Here are some instances of spoofing attacks:

■ **IP Address Spoofing Attack**: The attacker transmits IP packets originating from a fraudulent

(or spoofed) source address to conceal their identity. DDoS attacks often employ IP spoofing to make the packets seem like they originate from valid source IP addresses.[36]

attackers executing a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack are attempting to refuse access to a certain service by depleting some limits or limited resource. DoS attacks can be initiated from several devices and aim to deplete certain system resources. DDoS attacks are carried out using hundreds or thousands of devices spread across the Internet and generally seek to deplete an outside resource, similar to utilizing the full capacity of a link or interface, an example for DOS attack is DHCP spoofing attack. [36]

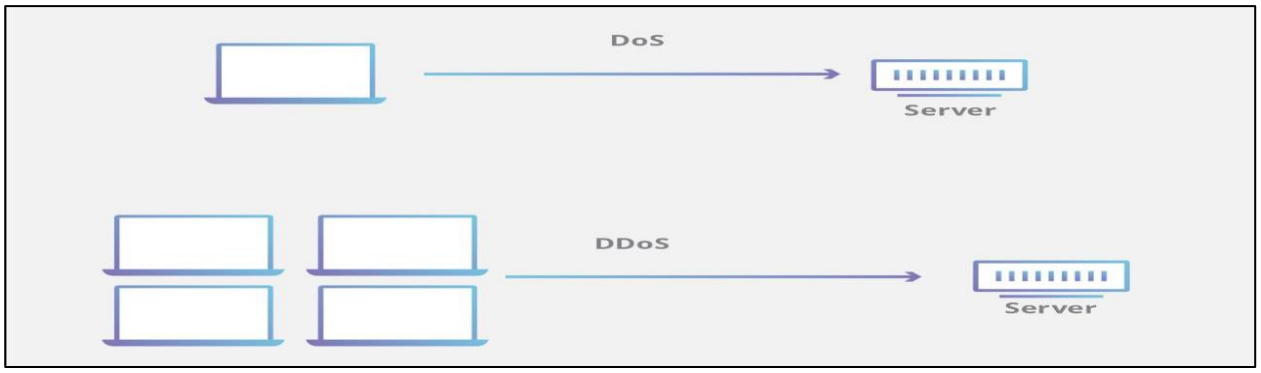


Figure II.5 DoS and DDoS Attacks

II.4 Network Security Measures

II.4.1 Network Foundation Protection (NFP) Framework

The Network Foundation Protection (NFP) framework offers a thorough method for securing enterprise networks. It offers an organized framework that includes multiple domains or elements to guarantee a strong and layered security stance. The NFP framework tackles security across various aspects of network operations, encompassing the data plane, control plane, management plane, and physical security issues.[38]

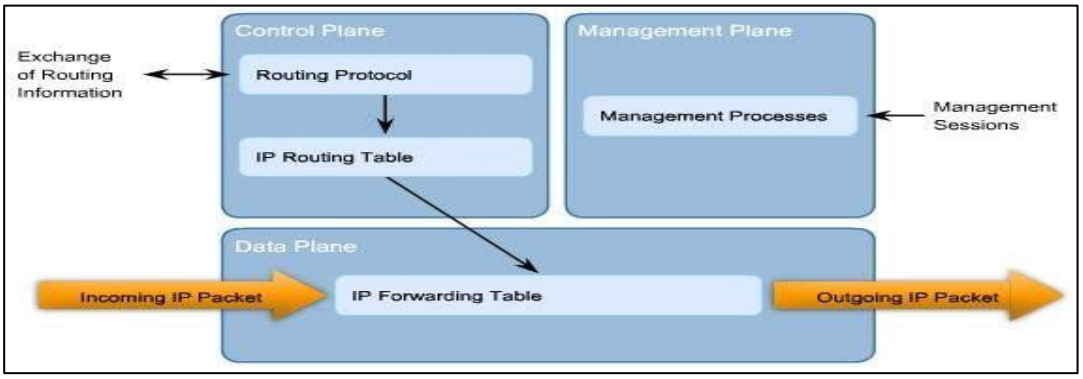


Figure II.6 NFP Planes [39]

II.4.1.1 Management Plane Security

The management plane is utilized for controlling, diagnosing, and Supervising network devices and services. Protecting the management plane is vital for maintaining the integrity and availability of network management operations. Essential security protocols in the

management plane consist of**:**

1. **Secure Management Protocols:** using secure protocols such as SSH and HTTPS for the remote management and monitoring of network devices and services
2. **Out-of-Band Management:** Establishing a distinct, independent management network or out-of-band management interfaces to separate management traffic from the data and control planes.
3. **Secure Log Management:** Guaranteeing the safe storage, transmission, and examination of log data from network equipment to facilitate efficient monitoring, incident handling, and forensic inquiries.

II.4.1.2 Control Plane Security

The control plane controls and configures network services and devices. Protecting the control plane is crucial to avoid unauthorized access, modifications in configuration, or interruptions that might Damage the network's functionality. essential security protocols in the control plane comprise:

1. **Access Control Lists (ACLs):** ACLs used to limit access to the control plane interfaces of network devices, permitting only approved IP addresses or networks to create management connections.
2. **Role-Based Access Control (RBAC):** RBAC guarantees that network administrators and staff possess suitable levels of access and privileges corresponding to their roles and duties.
3. **Secure Device Configurations:** make a strong network device configuration by turning off unneeded services, enforcing robust passwords, and applying security best practices to minimize the attack surface.

II.4.1.3 Data Plane Security

The data plane manages the transmission of real user or application data traffic through the network. Securing the data plane is essential in the aim of preventing illegal access, data leaks, and various security threats. Essential security protocols within the data plane comprise:

1. **Firewalls:** Firewalls serve as the initial barrier, monitoring and managing incoming and outgoing network traffic according to established security protocols. They can serve as perimeter firewalls, internal firewalls, or host-based firewalls to establish a multi-layered defense system.
2. **Secure Communication Protocols:** Utilizing secure communication protocols like IPsec, SSL/TLS, and SSH guarantees that information sent

across the network is Encoded and shielded against unauthorized interception or alteration.

3. **Intrusion Prevention Systems (IPS)**: IPS solutions oversee network traffic to detect harmful activities, policy violations, and recognized threats. They can identify and thwart attacks instantly, offering an extra level of security for the data plane.[38]

II.4.2 VPN IPSec

IPsec offers security functions at the IP layer by establishing a framework that selects necessary security protocols, identifies the algorithm needed for the service, and implements any cryptographic keys essential for delivering the requested services. IPsec can secure one or multiple routes between two hosts, between two security gateways (typically routers or firewalls), or between a security gateway and a host, it uses multiple protocols and mechanisms to achieve this, including:

a. **Authentication Header (AH):** This protocol ensures authentication, data integrity, and optional protection against replay attacks for IP packets.
b. **Encapsulating Security Payload (ESP)**: This protocol ensures authentication, data confidentiality, data integrity, and optional protection against replay attacks for IP packets.
c. **Internet Key Exchange (IKE)**: This protocol is utilized to create and manages Security Associations (SAs), which serve as secure communication links between the VPN endpoints. IKE manages the discussion of encryption algorithms, authentication techniques, and key exchange.

There are two modes for implementation of IPsec:

- ✓ **Transport mode:** This mode encrypts only the data portion (payload) of every packet and leaves the original IP packet header unchanged. Transport mode is applicable to both gateway and host implementations, and it provides protection for upper-layer protocols and selected IP header fields.
- ✓ **Tunnel mode:** This mode offers greater security compared to transport mode since it encrypts both the data payload and the initial IP header. IPsec in tunnel mode is typically employed when the final destination of a packet differs from the point of security termination. This mode is also applicable in situations where security is offered by a device that did not create packets, such as with VPNs. Tunnel mode is commonly utilized in networks that have unregistered IP addresses. the unregistered addresses can be

transmitted from one gateway encryption device to another by concealing them within the tunneled packet. [40]

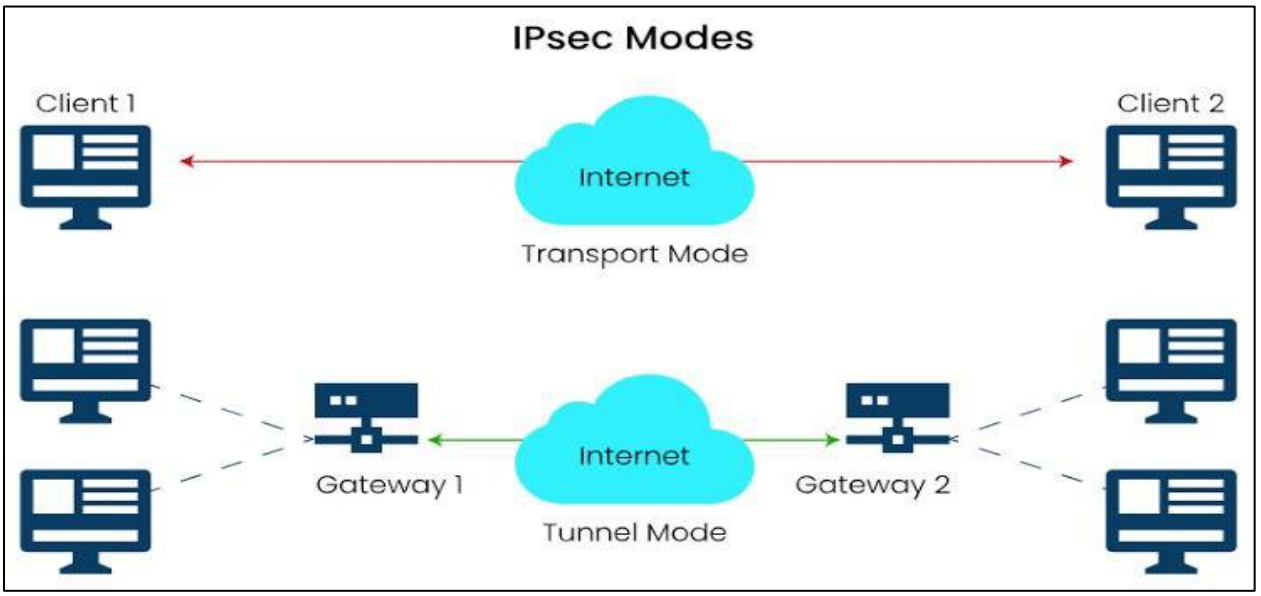


Figure II.7 VPN IPSEC Modes

Enterprises implement IPsec VPNs through focused VPN devices, as Cisco's Adaptive Security Appliance (ASA) or routers equipped with VPN features. These devices function as VPN gateways, initiating and concluding VPN connections with distant locations or clients. IPsec VPNs can be set up in different topologies, such as site-to-site (to link distant offices), remote access (for mobile users), and extranet (for secure connections with partners or customers).

IPsec VPN provides several advantages to enterprises:

1) **Confidentiality:** IPsec VPN secure the data across the network, blocking unauthorized access and interception.
2) **Data Integrity**: IPsec guarantees that the data Obtained isn't changed, securing against man-in-the-middle attacks and data tampering.
3) **Access Control:** IPsec VPNs can be set up to limit access according to user credentials, IP addresses, or additional parameters, offering detailed access control to company resources.
4) **Authentication:** IPsec authorizes the VPN endpoints, making certain that only permitted devices or users can create VPN connections.
5) **Scalability**: IPsec VPNs are capable of scaling to accommodate numerous remote users and sites, rendering them ideal for businesses with decentralized operations or a mobile workforce.

II.4.3 Layer 2 Security

Several Layer 2 securities can be used in the protection of the enterprise network:

- **Port Security**: This function restricts the maximum of MAC addresses that can be learned on access switch ports, it can be configured to take specific states as: protect, restrict, shutdown.
- **BPDU Guard:** when BPDUs appear in unexpected locations, the switch will secure itself.
- **Root Guard:** This function manages which ports are banned from becoming root ports to remote switches.
- **Access Control lists:** This future offers layer 2 and layer 3 ACLs for managing traffic and enforcing policies.
- **DHCP Snooping:** this future stops unauthorized DHCP servers from affecting the network.
- **IP Source Guard:** This future stop hosts from spoofing Layer 3 information.
- **802.1X:** This feature authorizes and authenticates users before enabling their communication with the rest of the network**.**
- **Storm Control:** This function restricts the volume of broadcast or multicast traffic passing through the switch [41]

II.4.4 Firewalls

Firewall is a network security system created for observing, filtering, and managing the incoming and outgoing network traffic according to specific security protocols. The main function of a firewall is to create a separation between a reliable internal network and potentially harmful external networks.

Firewalls must be the first front security device, but they shouldn't be the Single safeguard system or safety protocol on the network

firewall may be executed by one device or a collection of devices, or perhaps just software operating on a device like a router or a server.

All traffic between security domains must pass through the firewall to avoid Unauthorized access that might be exploited to ignore the firewall, violating the network access policy.

Firewalls typically manage the access between security zones by evaluating the source and destination IP address and port of packets.

Firewalls can be installed in different areas of a network; their threat management should be applied at minimum to the most vulnerable and essential sections of enterprise networks to ensure more protection.

Firewalls offer more services, as:

- NAT modifies the source or destination addresses of data packets when they traverse a firewall. This enables various devices to access the internet through a single IP address, which aids in securing the private network from direct risks posed by external threats.

  In a network environment, every employee utilizes their personal computer or mobile device to connect to the internet for web surfing, emailing, and using cloud services. Even though every device possesses its unique private IP address within the organization's internal network, all outgoing traffic shows to external networks as coming from the identical public IP address assigned to the organization. Consequently, it becomes more challenging for potential attackers to recognize and aim at specific devices.

- VPN acts as a shield between a computer or network and the internet, handling all web requests prior to passing them to the network.

  VPNs extend a private network over a public one, like the internet. This enables users to safely sending data though their devices were linked directly to the private network. The link creates an encrypted tunnel between distant devices and the corporate network, allowing secure access.

In a network, a firewall is designed to regulate what moves from one security zone to another. If a system is breached in one area, firewalls assist in limiting the attack to that specific zone [42]

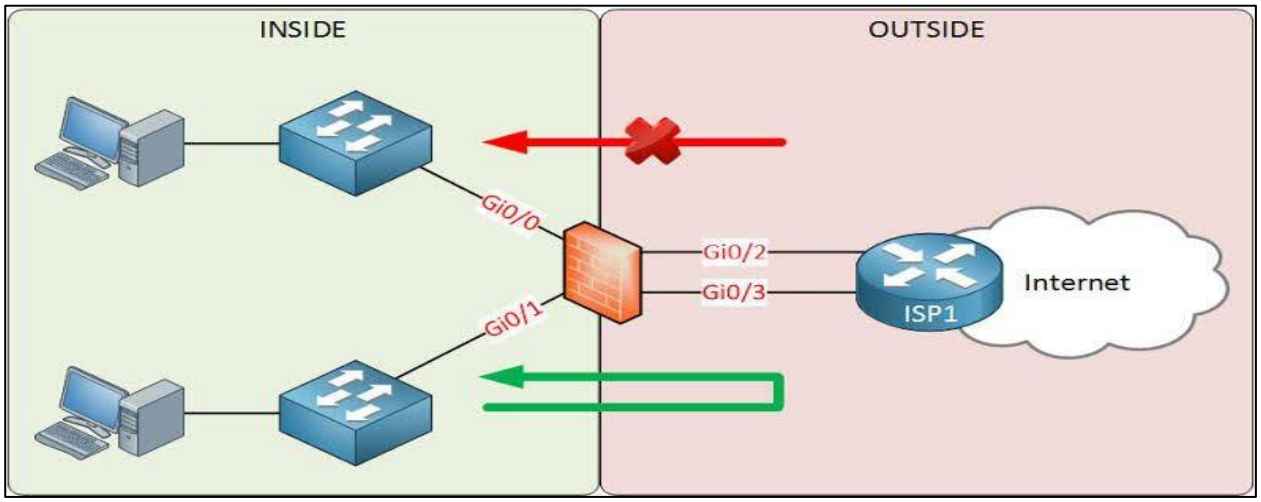


Figure II.8 Firewall Zones

The Inside Firewall Zone: refers to a trusted internal network where devices, systems, and data are protected from external threats, such as corporate networks or home-connected personal devices.

The Outside Firewall Zone: refers to an untrusted area, like the internet, where threats exist. Firewalls control and secure the traffic between this zone and the internal network.

II.4 Conclusion

In this chapter, we have talked about network management, examining the essential technologies and security protocols that support enterprise network functionality. The initial segment offered a comprehensive analysis of server solutions, bringing attention to the crucial importance of Windows Server in managing enterprise settings

Then, we initiated an extensive investigation into Network attacks which is unauthorized actions targeting network systems, categorized into passive and active attacks**.** these types include some famous attacks. Organizations need robust cybersecurity measures, to protect the network enterprise against these threats.

we explored network security that took a large section in our chapter, where we have talked about the implementation of Network Foundation Protection (NFP) and his planes.

We investigated the implementation of IPsec VPNs (Virtual Private Network), these protected communication pathways guarantee the privacy and authenticity of data transfers, allowing remote access to enterprise while guaranteeing a strong defense against eavesdropping. Layer 2 security and his robust advantages for securing the network devices and firewalls as barriers against unauthorized access and potential threats. Applying these security measures, enterprises can build a stable and protected network infrastructure.

CHAPTER III:

Enterprise Network Project: planning, designing, configuration and security implementation/testing

III.1 Introduction

This chapter details the implementation of a secure campus network designed for university requirements using PNETLab emulation. The project followed a complete lifecycle from planning to testing, beginning with stakeholder needs assessment. The architecture combines physical infrastructure (cabling, access points) with logical design (VLANs, HSRP redundancy, AD/DHCP management). Security measures included ASA firewalls, IPsec VPNs, and Layer 2 protections against DHCP attacks. Penetration testing validated resilience, while Active Directory enabled centralized authentication. Connectivity tests confirmed the network meets current and future needs, demonstrating how proper planning creates reliable, scalable infrastructure.

III.2 Project Framework (Work Plan)

The process of building the university network begins with a needs assessment phase, where a series of meetings are held with all relevant stakeholders. These meetings gather requirements from senior administration, colleges, and students, focusing on analyzing the expected number of users, types of devices, and required applications. This preliminary phase forms the cornerstone of the entire project.

We move to the detailed design phase, which consists of two main components. The first component involves designing the physical infrastructure, including planning the cabling system, determining network access point locations, and preparing main communication rooms. The second component focuses on the logical topology architecture, encompassing the hierarchical network structure, IP addressing scheme, VLAN segmentation, and security policies.

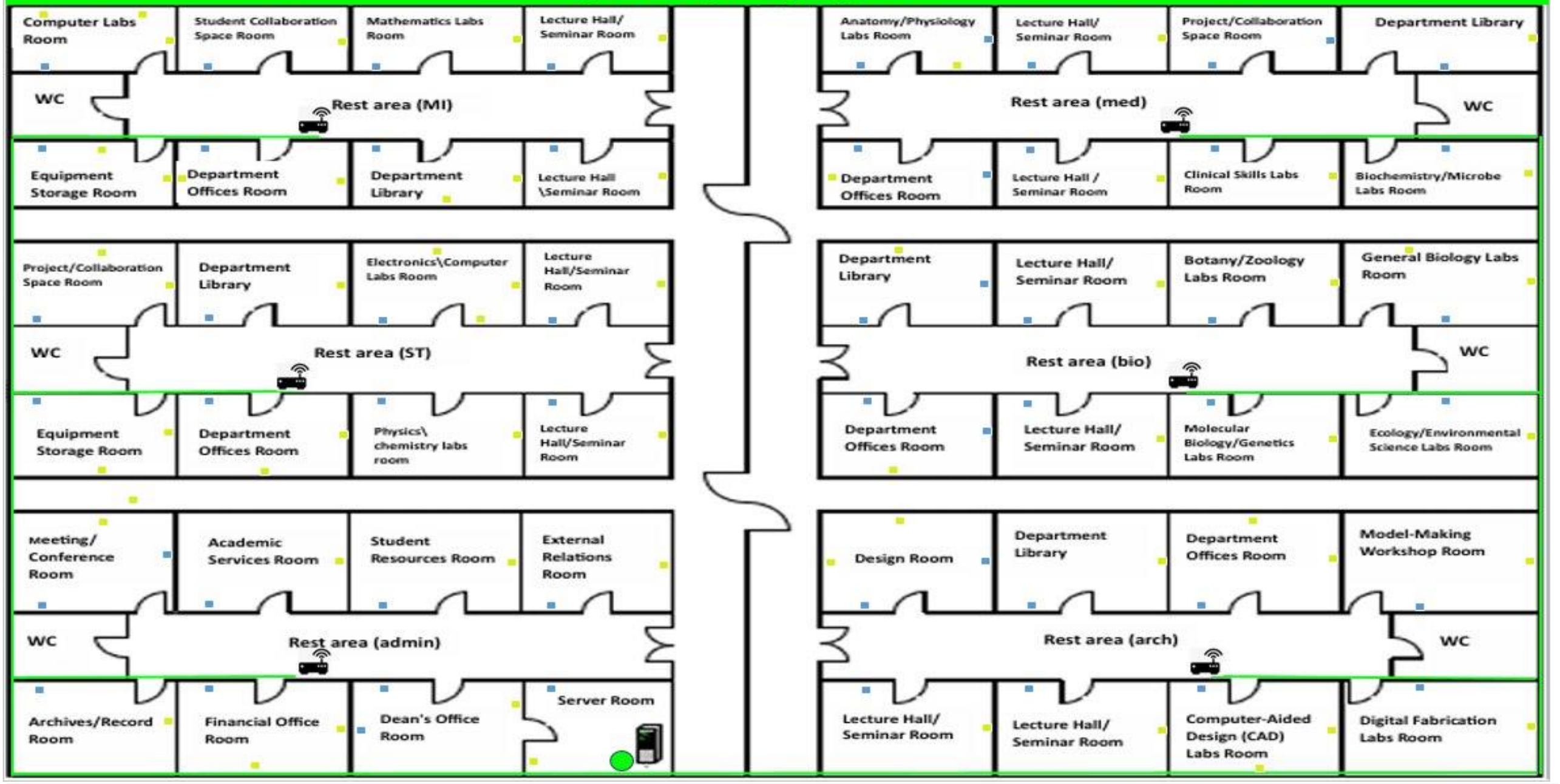
Next comes the implementation phase, starting with basic civil works such as cable installation and room preparation, followed by the installation of networking equipment including switches, routers, and security systems. This phase also includes configuring fundamental network settings, from routing protocols to authentication systems.

Prior to final handover, the network undergoes rigorous testing including performance tests, penetration tests, and compatibility tests. This stage also involves training the university's technical team on network management and delivering all necessary technical documentation.

The final outcome is an integrated network characterized by high performance and scalability, featuring multi-layered protection and centralized management. This network provides comprehensive support for various educational applications while adhering to the highest quality and security standards, ensuring sustainable service that meets both current and future university needs.

On the figure III-1, the physical topology plan of the university includes the passive component design and wireless access points.

Figure III-1 Physical Topology Plan



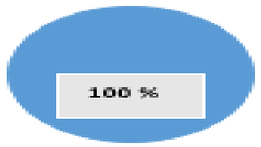
Access point cable FTP cat6 start point (server room)

Single Faceplate

68 sur 68

Dual Faceplate

56 sur 56



Cable FTP Cat6

III.2.1 Gathering Information

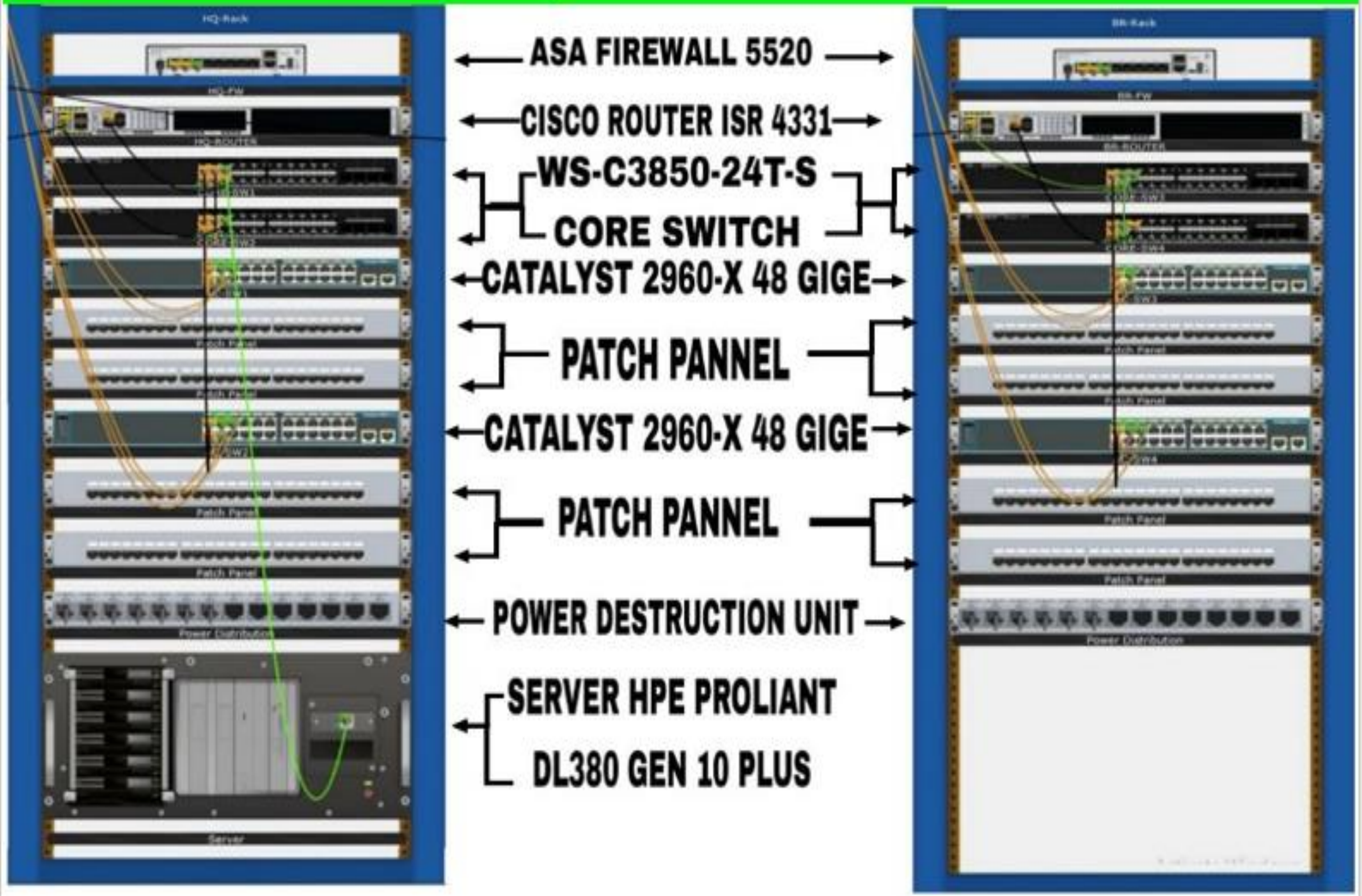
We designed a university campus network that perfectly balances performance and cost. After carefully analyzing the campus needs, we implemented a robust solution featuring optimal WIFI coverage in all buildings, a reliable server room with backup systems, and a hybrid fiber-copper cabling infrastructure. Working closely with university IT staff, we created an organized, easy-to-maintain system that currently supports thousands of daily users while being ready for future expansion. Based on university plan provided us, we build the following table that gathered information:

III.2.1.1 Passive Components Design

Description	Single Faceplate	Dual Faceplate	Wi-Fi
ADMINISTRATION	9	10	1
FACULTY OF SCIENCE TECHNOLOGY	13	8	1
FACULTY OF COMPUTER SCIENCE	13	8	1
FACULTY OF MEDICINE	7	11	1
FACULTY OF BIOLOGY	9	10	1
FACULTY OF ARCHITECTURE	11	9	1
Total	**62**	**56**	**6**
Total Points	**62+(56*2) +6=180 Points**		

Table III-1 End-User Access Points

Figure III-2 Rack Installation



III.2.1.2 Active Components Design

The racks devices that we have implemented can be grouped of :

Faculties	Access Switch	Core Switch	Router	Asa Firewall	server
ADMINISTRATION	*2*	*2*	*1*	*1*	*1*
FACULTY OF SCIENCE TECHNOLOGY					
FACULTY OF COMPUTER SCIENCE					
FACULTY OF MEDICINE	*2*	*2*	*1*	*1*	
FACULTY OF BIOLOGY					
FACULTY OF ARCHITECTURE					

Table III-2 Active Components Design

III.2.2 Purchases List

Passive components: are the physical connectivity and cabling infrastructure.

Description	Qty	Unit Price (DZD)
User Side Cat6 Keystone Jack	180	4000,00
Patch panel side Cat6 Keystone Jack	180	7000,00
Unloaded 24Ports Patch Panel	8	30000,00
Single Faceplate	62	150,00
Dual Faceplate	56	200,00
Patch Cord 3m User Side	180	330,00
Patch Cord 1m Patch Panel Side	180	180,00
Cat6 FTP cable Box Roll 305m	180	11900,00
RJ-45 50Pcs	8	1500,00
42U Rack 800mm*1000mm	2	400000,00
Power Distribution Unit 6Way	2	100000,00
Total Price	**5 486 300,00 DZD**	

Table III-3 Passive Components Purchase List

Active components: are devices that require power to operate and Perform functions

DESCRIPTION	QTY	Unit Price (DZD)
Catalyst 2960X-48LPS-L2 Switch	4	250000,00
WS-C3850-24T-S Core switch	4	270000,00
Cisco Router ISR 4331/K9	2	310000,00
ASA- 5520 Adaptive Security Appliance - 4 Gigabit Ethernet interfaces	2	400000,00
Server HPE ProLiant DL380 Gen10 Plus	1	800000,00
Total Price	**4 300000,00 DZD**	

Table III-4 Active Components Purchase List

The cost of this project is 9 786 300,00 DZD

III.2.3 Designing the Project- Logical Topology

III.2.3.1 Technical Requirements:

In order to perform this work, we need these following requirements:

- **A computer with at least 16 GB of RAM and 4 CPUs.**
- **VMware Workstation PRO 2017:** Virtual machine supervisor allocating 14 GB of RAM and 4 CPUs for the emulation platform.
- **PNETLab (Professional Network Emulation Platform):** PNETLab is an advanced network emulation platform that enables running virtual devices with real operating systems on a single computer, combining ease of use with powerful performance, delivering a professional network emulation experience with ease.
- **The operation system for all network devices:** IOSs for routers, switches and firewalls and the Windows server 2016 OS.

Using the PNETLab emulator we will build the well-designed infrastructure of the logical topology campus network that will be provided to as a full emulation designing and testing before his implementation in the real world

In the figure III.3 we proposed a full logical topology design of our project

ISP-AREA(ISP-1)

LANs :

ISP-1 & HQ-FW :10.10.10.0/30

ISP-1 & BR-FW :10.10.10.4/30

ISP-1 & NET :192.168.128.135/24(dhcp @)

OSPF & STATIC ROUTING

COLLAPSED CORE LAYER

HQ-FW(ASA Firwall)

LANs

HQ-FW & HQ-ROUTER :192.168.115.0/24 Inside Zone

HQ-FW & ISP-1 :10.10.10.0/30 Outside Zone

HQ-FW & ISP-2 :10.10.20.0/30 Outside Zone

OSPF & STATIC ROUTING & VPN IPsec Tunnel

HQ-ROUTER

LANs

HQ-ROUTER & CORE-SW1 :192.168.110.0/24

HQ-ROUTER & CORE-SW2 :192.168.120.0/24

HQ-ROUTER & HQ-FW : 192.168.115.0/24

OSPF & STATIC ROUTING

CORE SWITCHES

CORE-SW 1 & 2 :

L2 VLANs with SVI & HSRP

VTP mode server & EtherChannel

OSPF & STATIC ROUTING

ACCESS LAYER

ACCESS-SW 1 & 2 :

L2 VLANs & VTP mode client

LAYER 2 SECURITY

DHCP SPOOFING & DHCP STARVATION ATTACKS MITIGATION

VLANs Net IDs:

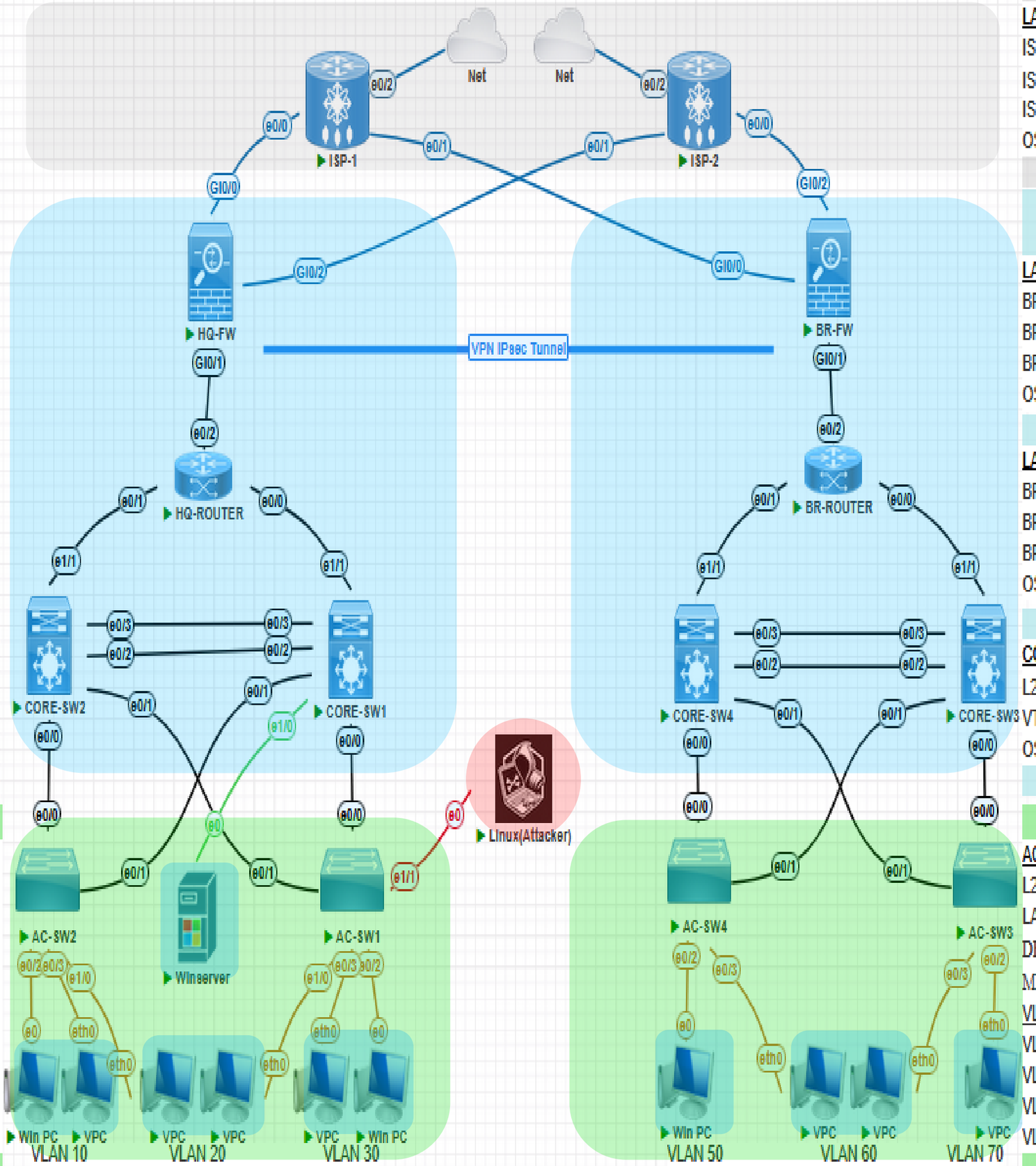
VLAN 10 **ADMIN** :192.168.10.0/24 GW: 192.168.10.100

VLAN 20 **MI** :192.168.20.0/24 GW: 192.168.20.100

VLAN 30 **ST** :192.168.30.0/24 GW: 192.168.30.100

VLAN 40 **VOICE** :192.168.40.0/24 GW: 192.168.40.100

Figure III-3 Network Topology & Configuration Overview



SERVER : IP Add 192.168.100.1/24 SERVICES Active Directory and Domain Controler , DHCP Server , DNS Server

ISP-AREA(ISP-2)

LANs :

ISP-2 & HQ-FW :10.10.20.0/30

ISP-2 & BR-FW :10.10.20.4/30

ISP-2 & NET :192.168.128.135/24(dhcp @)

OSPF & STATIC ROUTING

COLLAPSED CORE LAYER

BR-FW(ASA Firwall)

LANs

BR-FW & BR-ROUTER :192.168.125.0/24 Inside Zone

BR-FW & ISP-1 :10.10.10.4/30 Outside Zone

BR-FW & ISP-2 :10.10.20.4/30 Outside Zone

OSPF & STATIC ROUTING & VPN IPsec Tunnel

BR-ROUTER

LANs

BR-ROUTER & CORE-SW3 :192.168.90.0/24

BR-ROUTER & CORE-SW4 :192.168.95.0/24

BR-ROUTER & BR-FW : 192.168.125.0/24

OSPF & STATIC ROUTING

CORE SWITCHES

CORE-SW 3 & 4 :

L2 VLANs with SVI & HSRP

VTP mode server & EtherChannel

OSPF & STATIC ROUTING

ACCESS LAYER

ACCESS-SW 3 & 4 :

L2 VLANs & VTP mode client

LAYER 2 SECURITY

DHCP SPOOFING & DHCP STARVATION ATTACKS MITIGATION

VLANs Net IDs:

VLAN 50 **BIO** :192.168.50.0/24 GW: 192.168.50.100

VLAN 60 **MED** :192.168.60.0/24 GW: 192.168.60.100

VLAN 70 **ARC** :192.168.70.0/24 GW: 192.168.70.100

VLAN 40 **VOICE** :192.168.40.0/24 GW: 192.168.40.100

III.3 Management Part Setup

In this part we are going to configure our network services such as AD-DS and DHCP

III.3.1 Configuring the Server (Windows Server 2016)

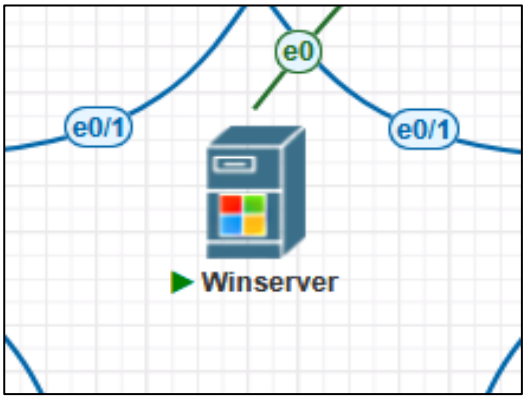


Figure III-4 Windows Server 2016

III.3.1.1 Installing AD-DC, DNS, DHCP and configuring AD-DC

First, we set up a static IP address (192.168.100.1/24) for the server. This is the network settings window where you manually assign an address to your server to join the network.

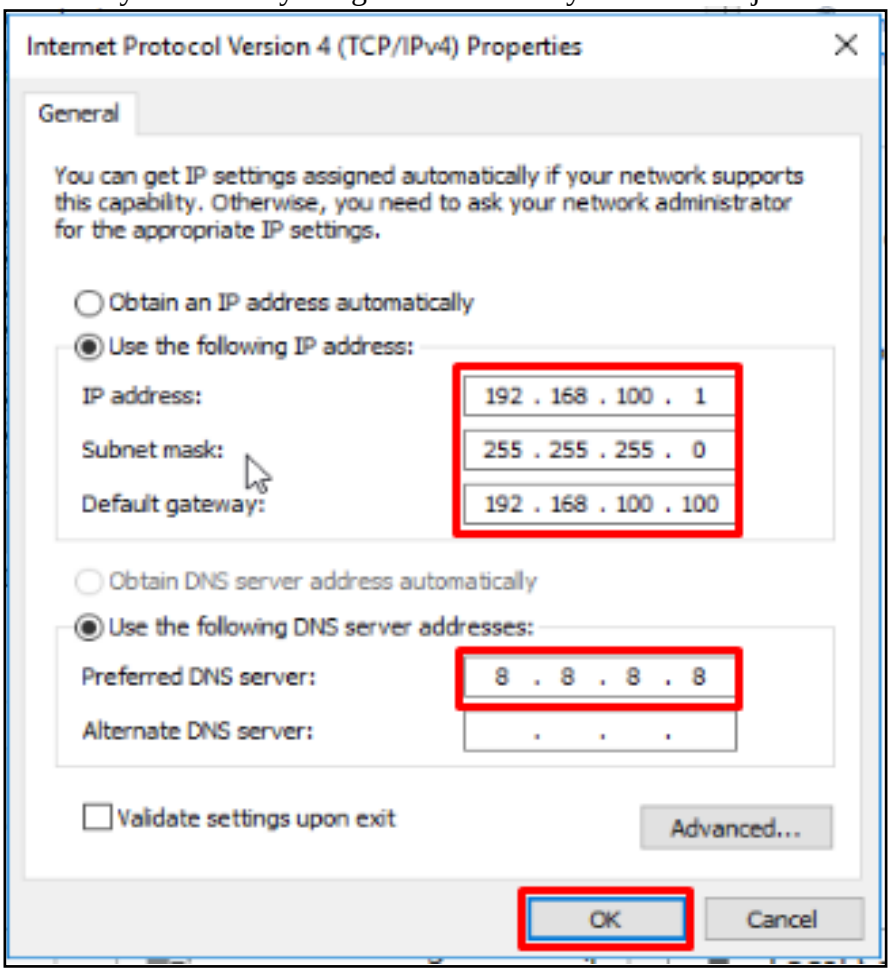


Figure III-5 Setting a Static IP Address for the Server

We'll now configure, install, and select the necessary network services

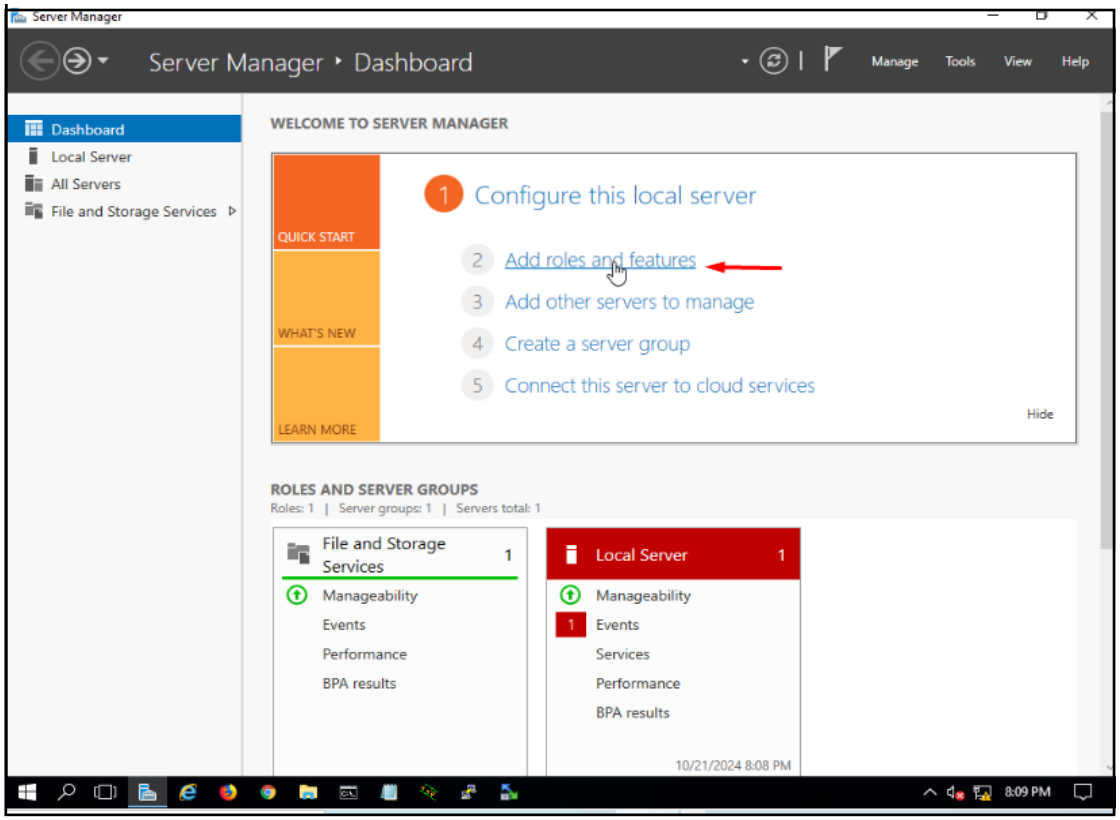


Figure III-6 Server Manager Dashboard

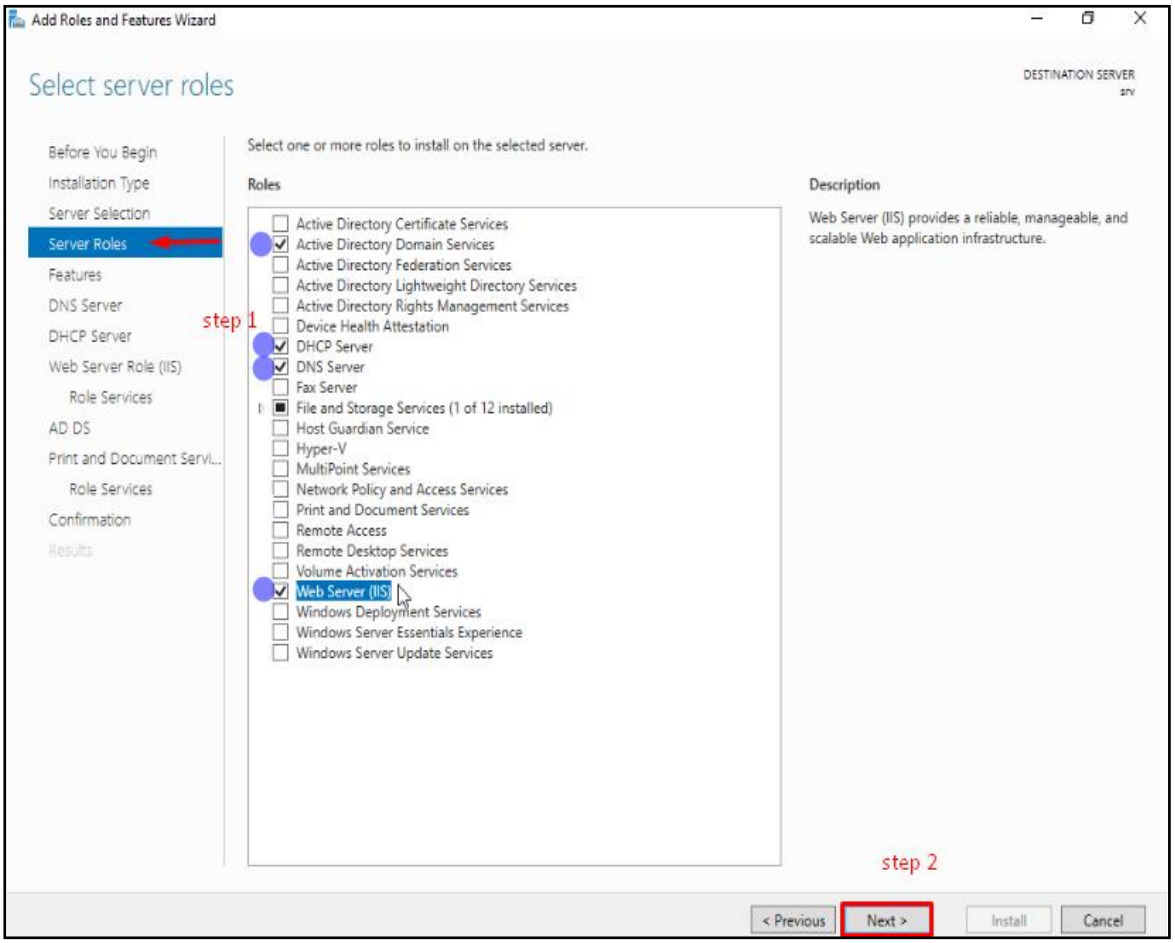


Figure III-7 Selecting AD DS, DHCP, and DNS Roles

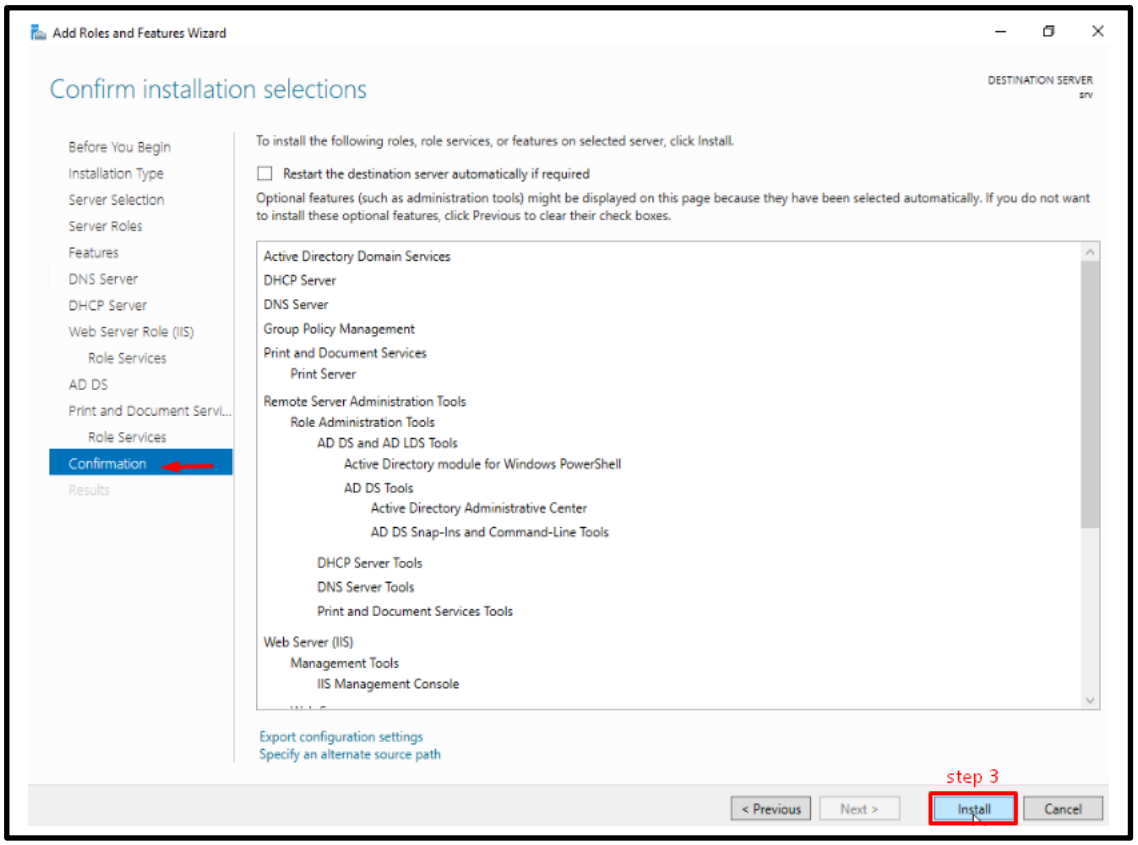


Figure III-8 Installing AD DS, DHCP, and DNS Roles

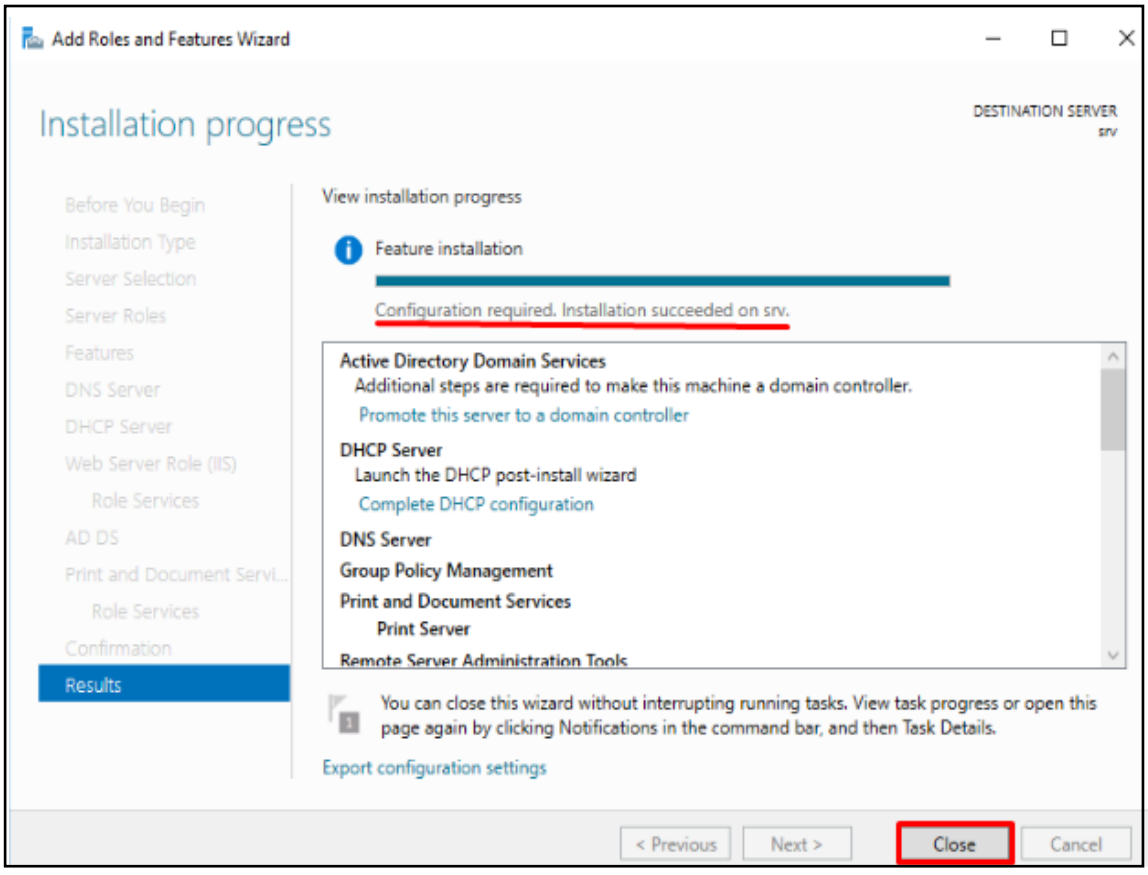


Figure III-9 Roles and Features Installation Completed Successfully

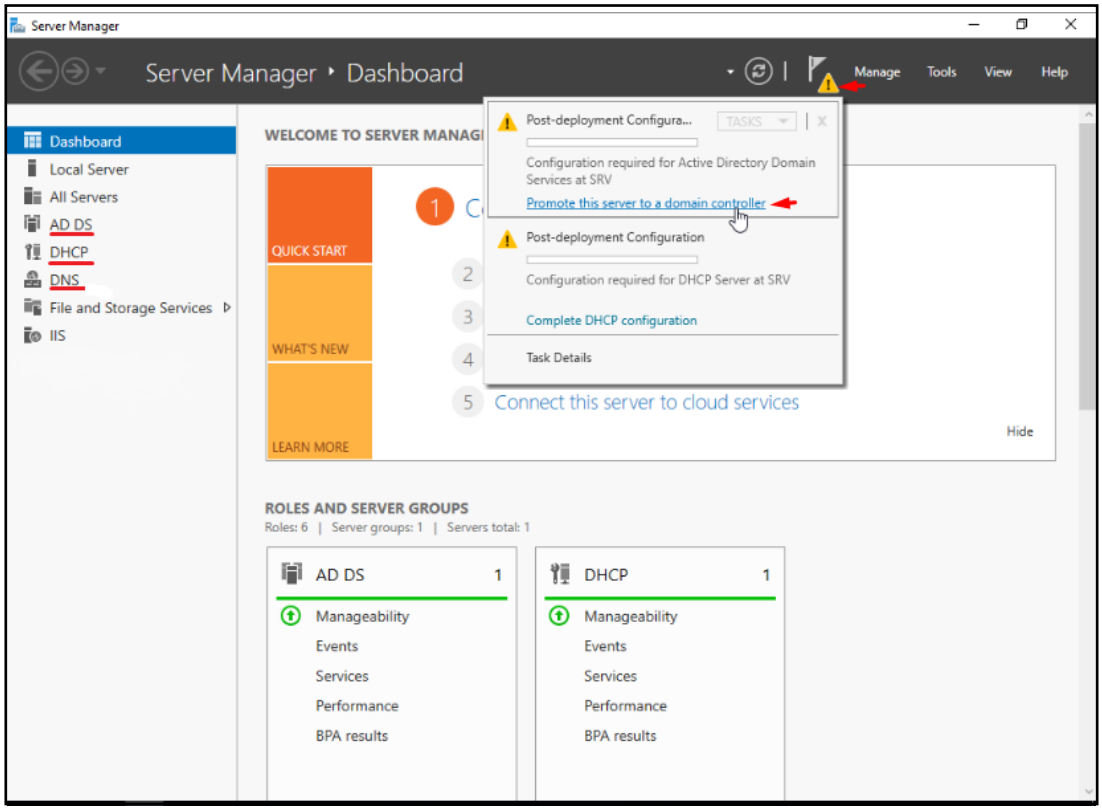


Figure III-10 Server Manager Dashboard After Installing AD DS, DHCP &DNS Roles

After completing the installation of the services, we move on to setting up the Active Directory Domain Controller.

III.3.1.2 Configuring Active Directory

Assign a name for the domain (UNIV.DZ).

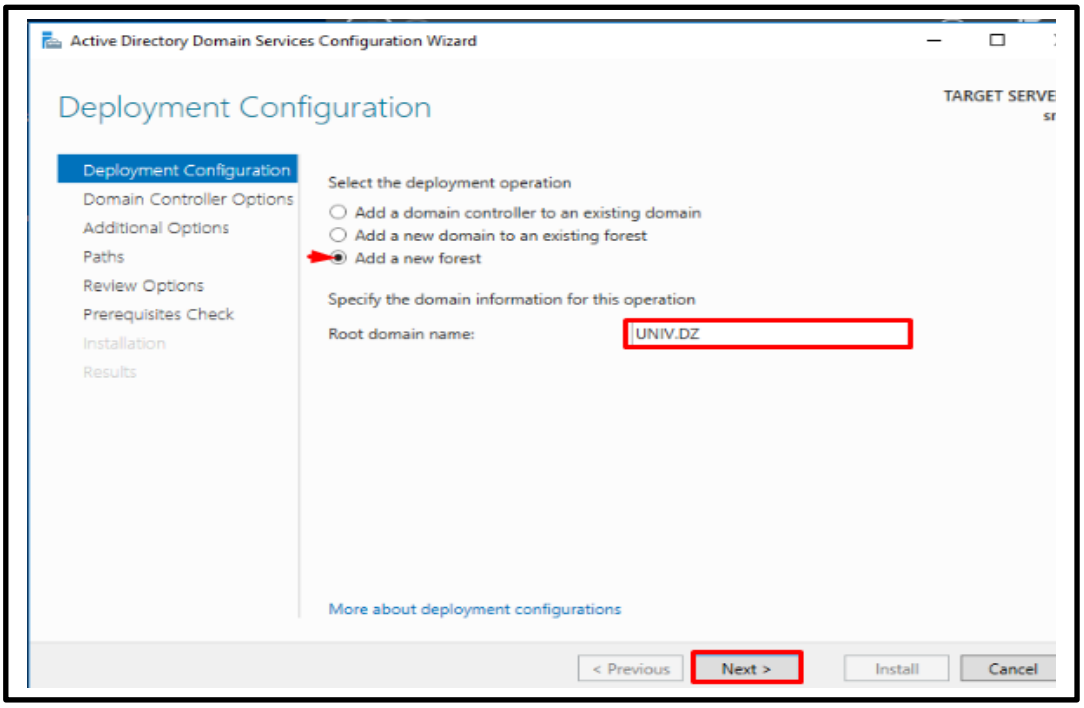


Figure III-11 Configuration of Active Directory

We set a password for the AD DC

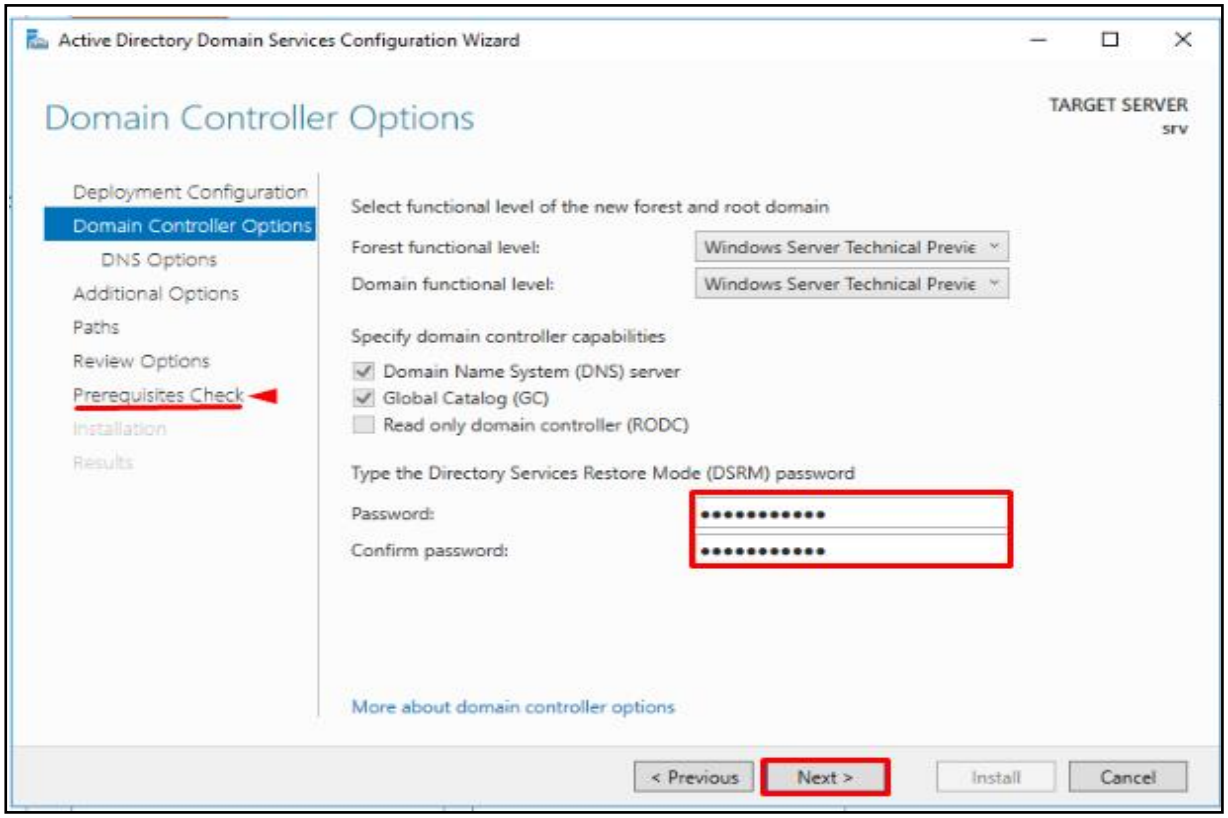


Figure III-12 Setting up the AD-DS Password

After setting up the AD DC service, the server reboots itself and checks the service status.

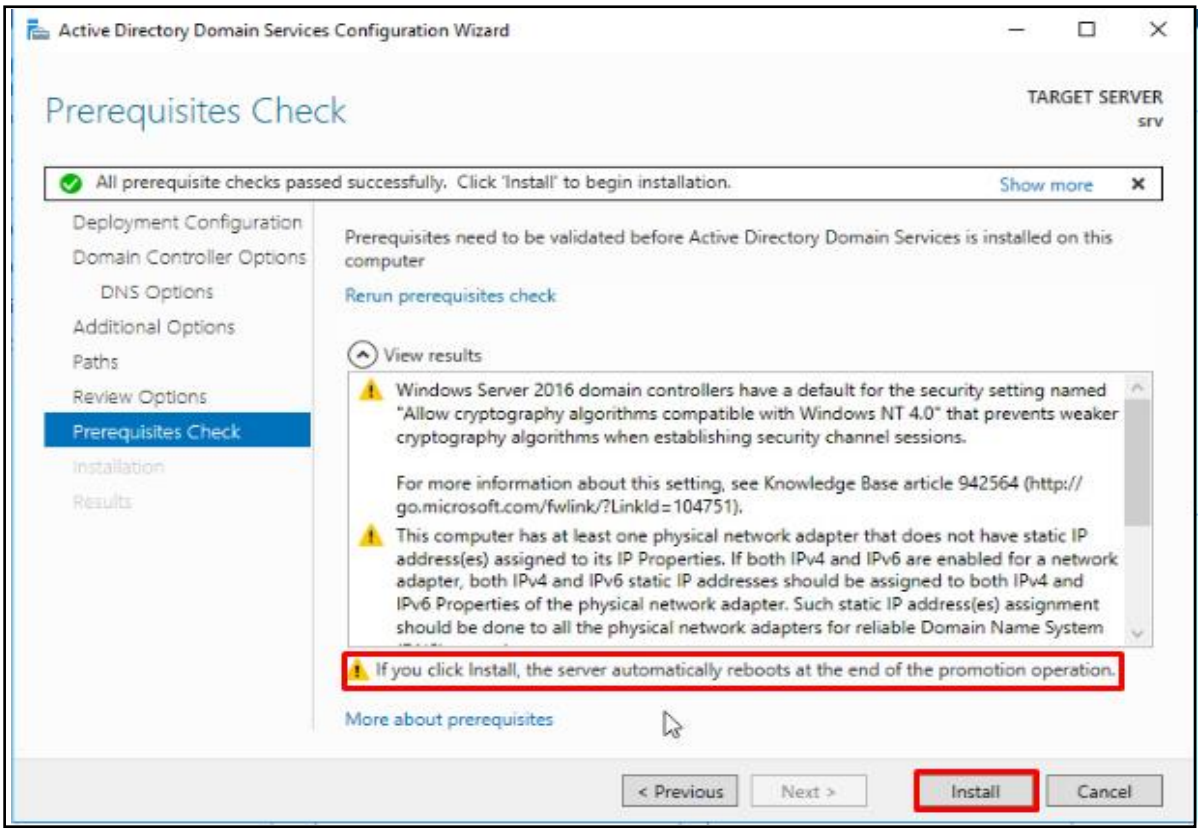


Figure III-13 Active Directory Prerequisites Check - Domain Controller Setup

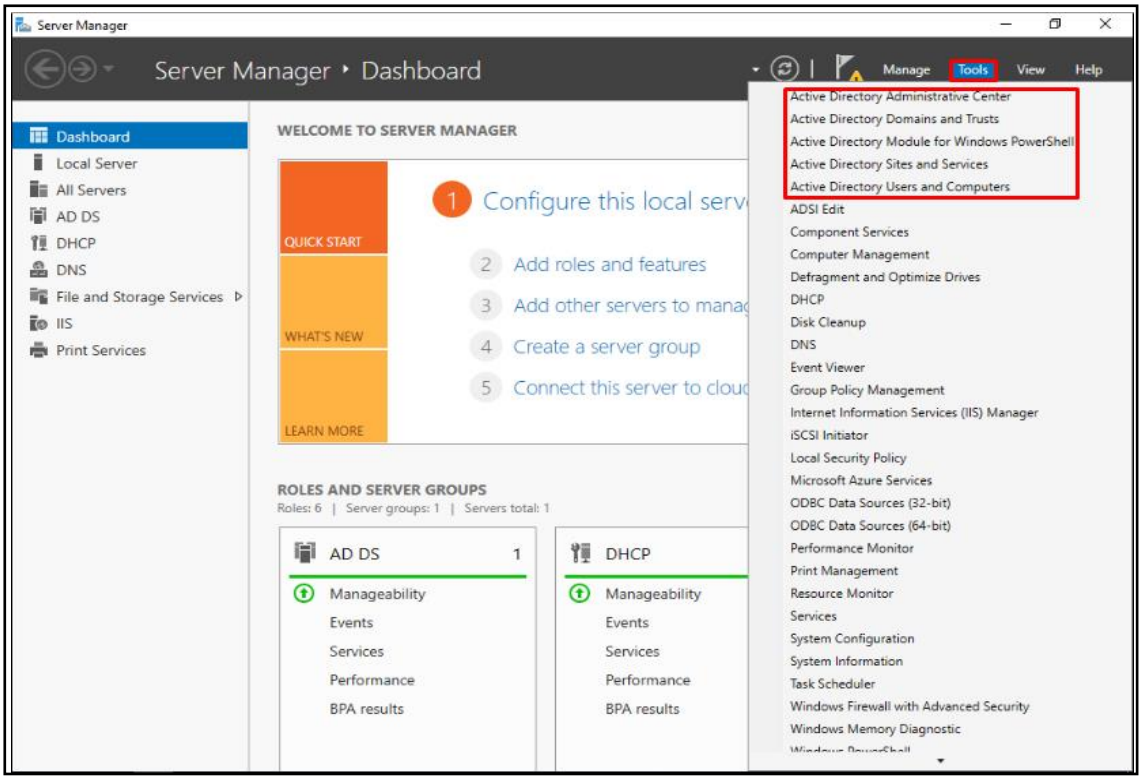


Figure III-14 Active Directory Services

After completing the AD DC setup, we proceed to configure the DHCP service.

III.3.1.3 Configuring DHCP

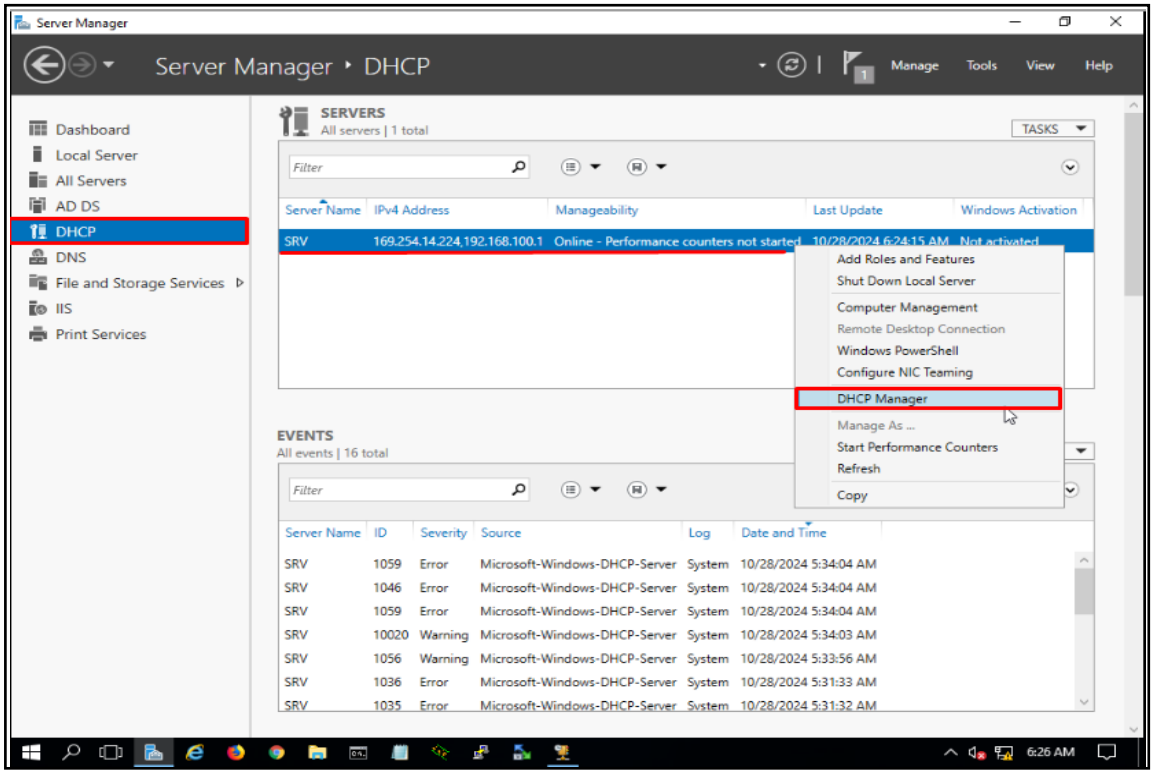


Figure III-15 DHCP Server Administration and Setup

Selecting IPv4 and New Scope.

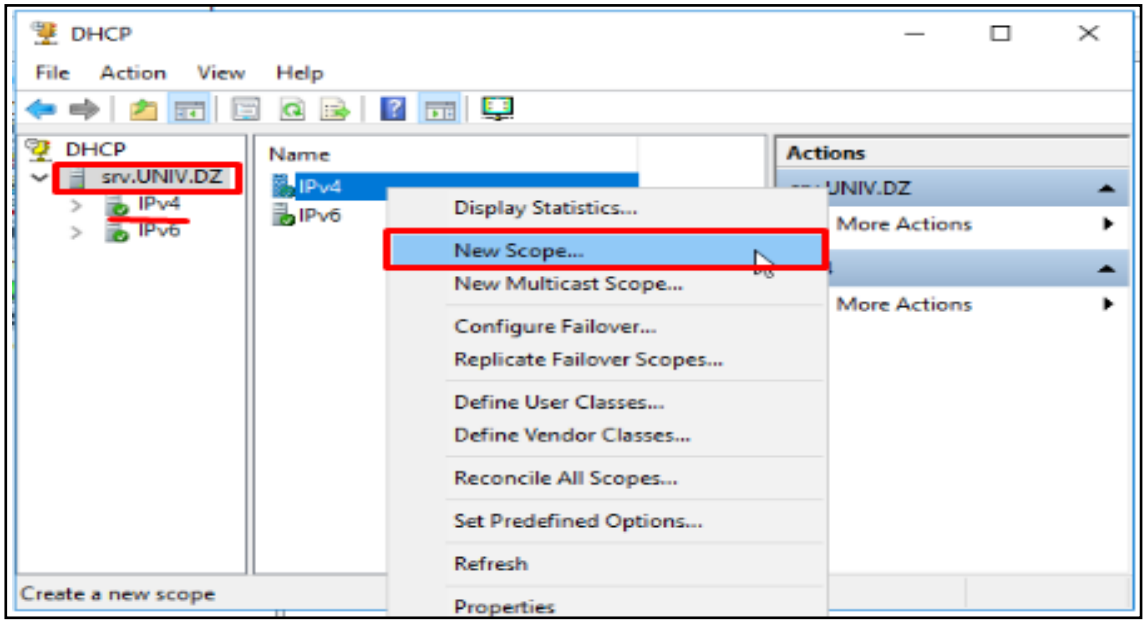


Figure III-16 DHCP Server Scope Management

Here is an example of how to add a DHCP Scope for VLAN 30 SCIENCE TECHNOLOGY (ST), and the same procedure applies to other VLANs.

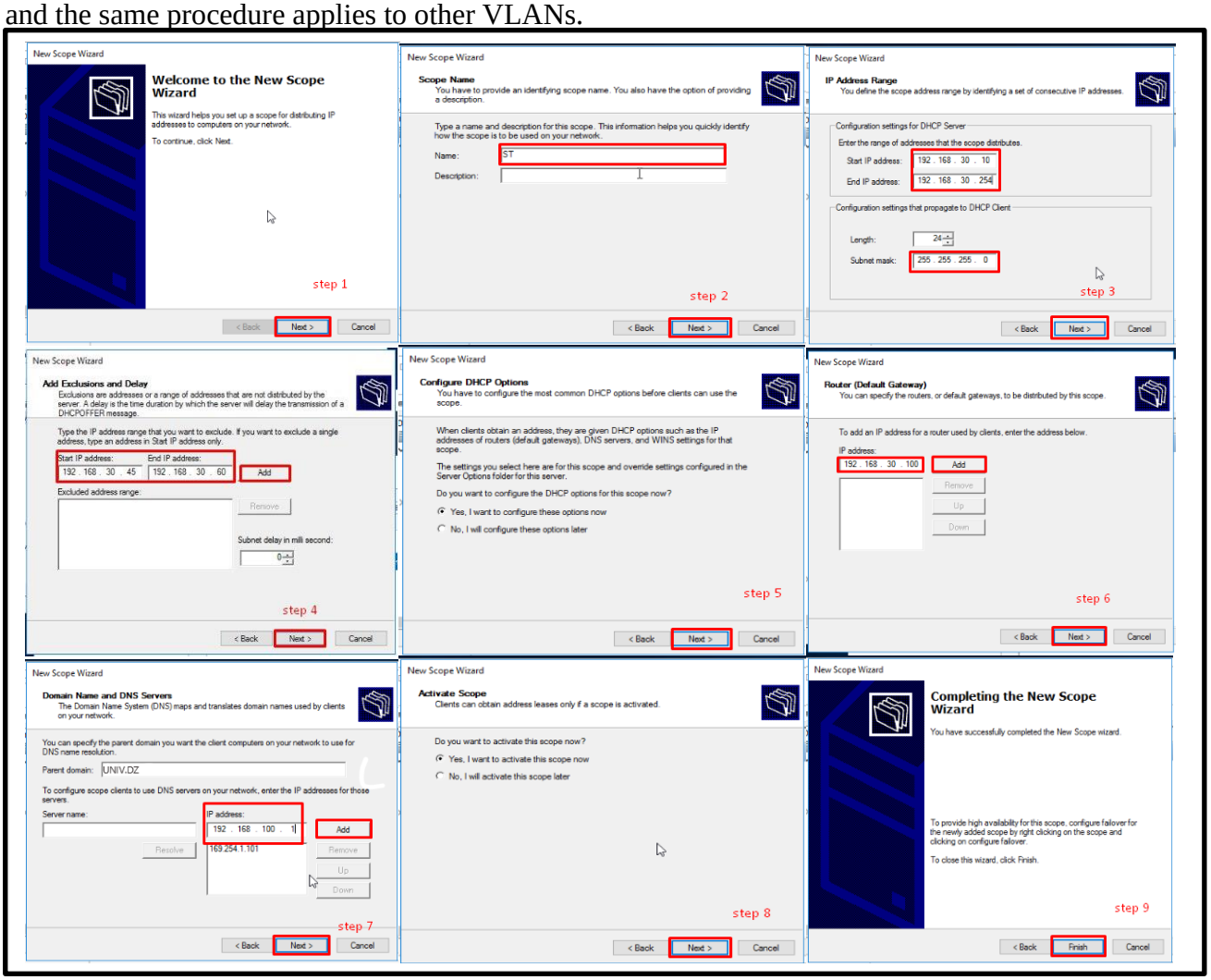


Figure III-17 Steps of Making a New DHCP Scope

III.3.1.3 Domain Management

In this part we are going to create organizational units to manage users, computers using active directory

- **Organizational Units Creation and Users Management**

Figure III-24 and III-25, Organizational Units (Ous) allow to organize and management users, computers within Active Directory.

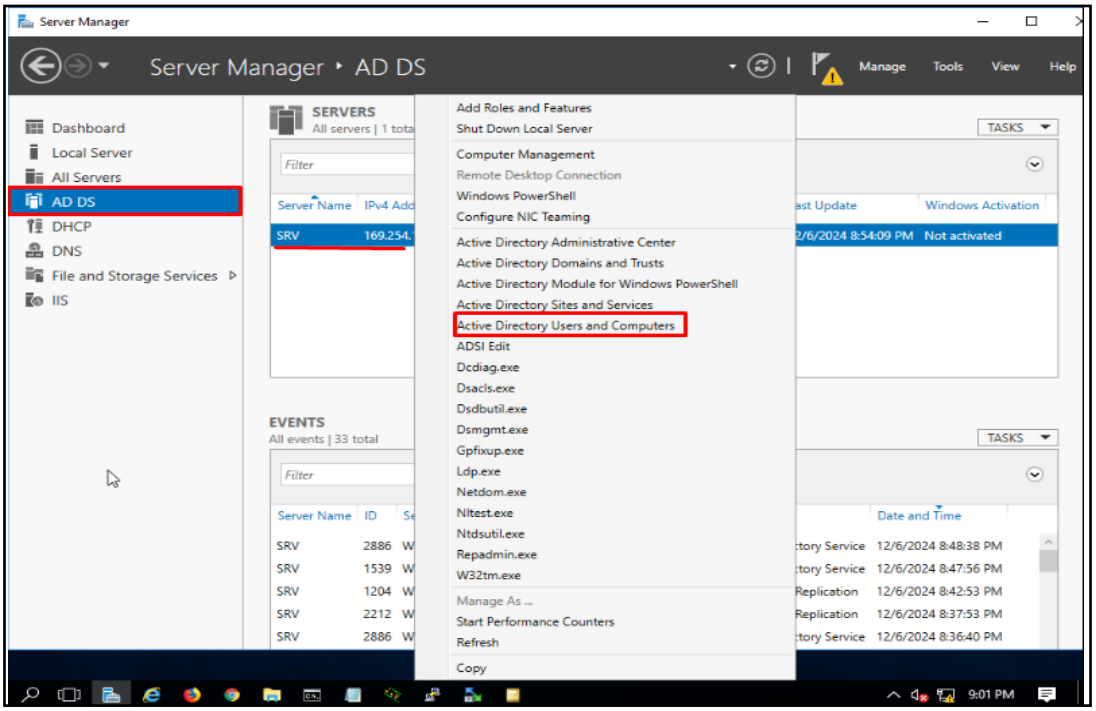


Figure III-18 AD-DS Server Administration and Setup

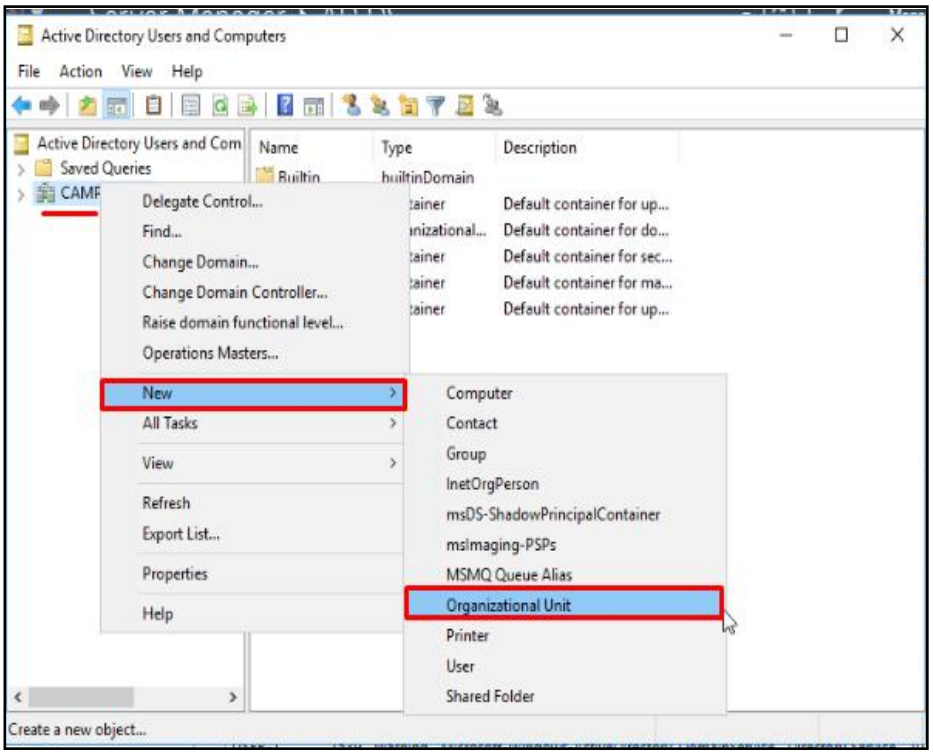


Figure III-19 Creating a New Organizational Unit

In the figure III-20 and III-21, we create a new object in our ous, and adding a new users to them

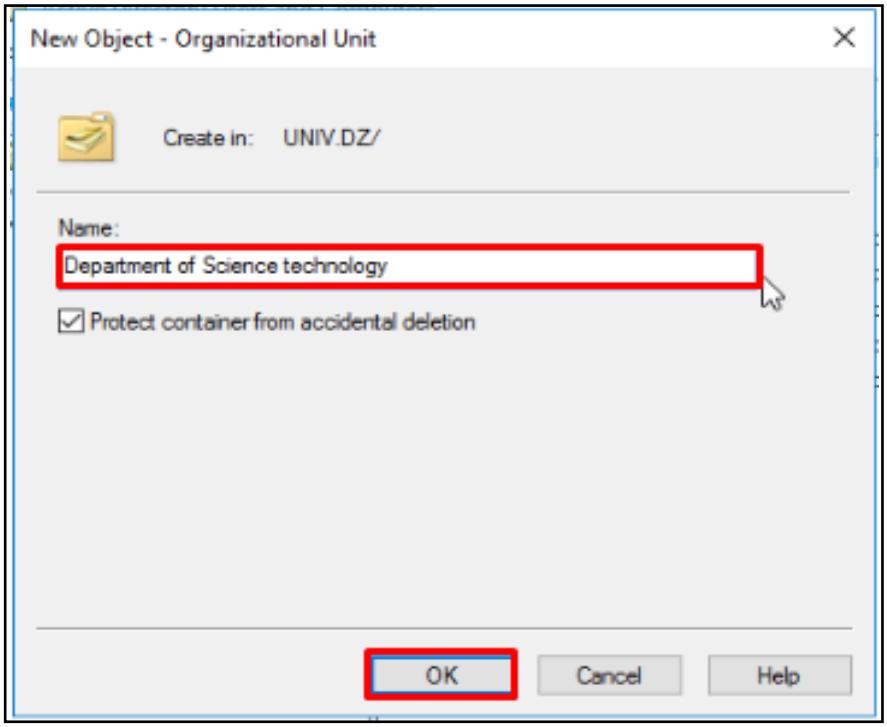


Figure III-20 Naming the Organizational Unit

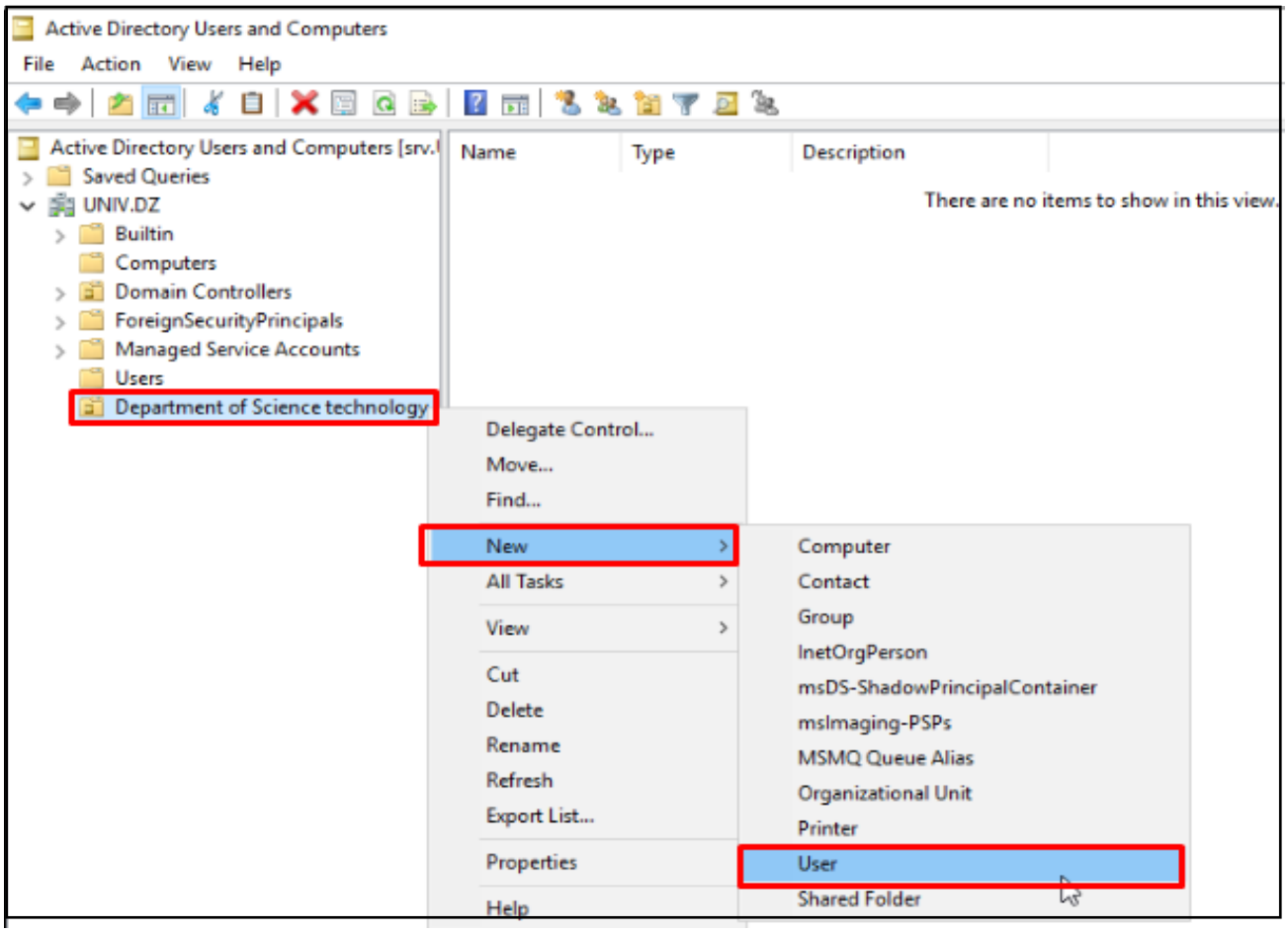


Figure III-21 Creating a New Users in the OU

Then, in the figure III-22 and III-23, we see the users creations steps and their appearance in the science & technology scope

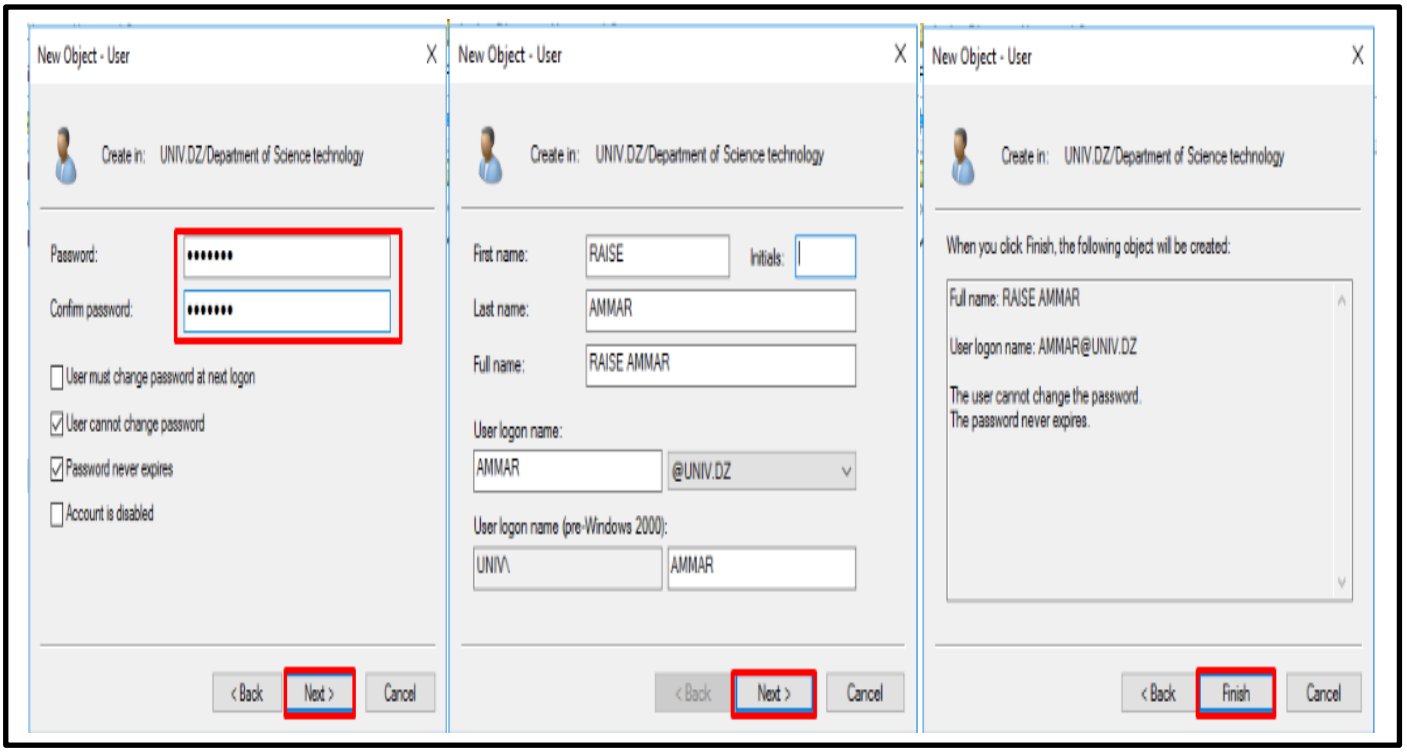


Figure III-22 User Creation and Account Settings

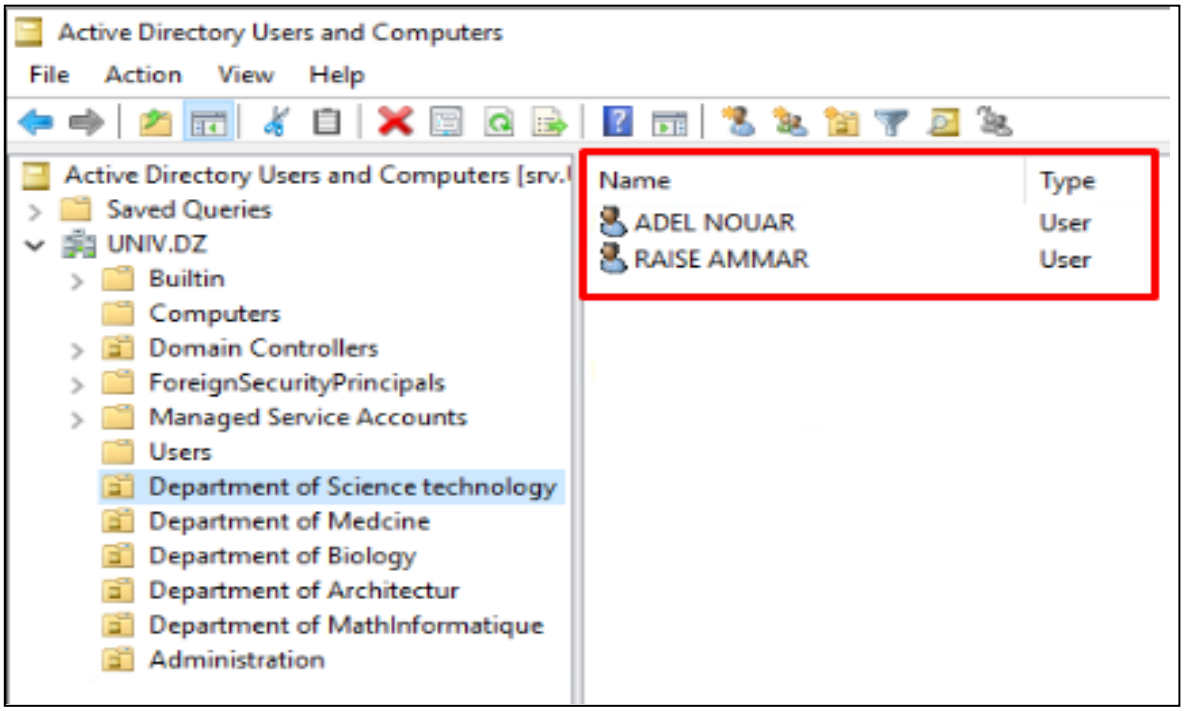


Figure III-23 The Appearance of the New Users and OUs

III.4 Network Part Configuration

In this part we will setup network devices such as switches routers firewalls

III.4.1 Configuring Access-Switches 1 & 2

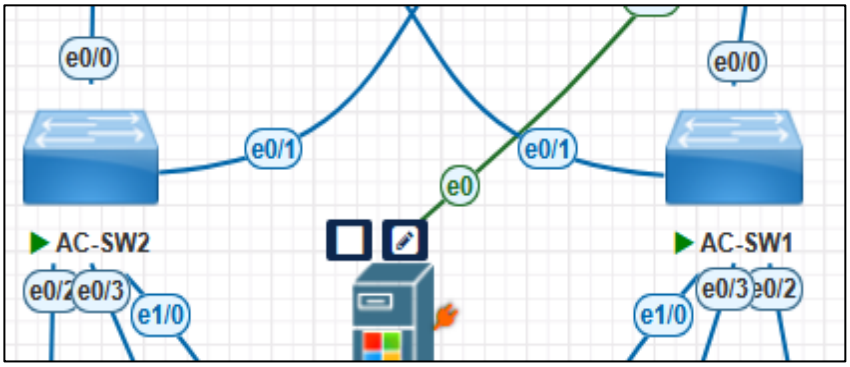


Figure III-24 Configuring Access Switches 1 & 2

III.4.1.1 VLANs Segmentation

We've configured 4 VLANs following university faculty naming conventions: Mathematics and Computer science (MI), Science technology (ST), Administration(Admin) plus a dedicated Voice VLAN.

```
AC-SW1>enable
AC-SW1#configure terminal
AC-SW1(config)#vlan 10
AC-SW1(config-vlan)#name ADMIN
AC-SW1(config-vlan)#exit
AC-SW1(config)#vlan 20
AC-SW1(config-vlan)#name MI
AC-SW1(config-vlan)#exit
AC-SW1(config)#vlan 30
AC-SW1(config-vlan)#name ST
AC-SW1(config-vlan)#exit
AC-SW1(config)#vlan 40
AC-SW1(config-vlan)#name VOICE
AC-SW1(config-vlan)#exit
```

Command list-1 VLANs Segmentation in AC-SW1

The same commands for ACCESS-SWITCH 2 (`AC-SW2`) .

Assign a designated interface to appropriate VLAN

```
AC-SW1(config)#interface range e0/0-1
AC-SW1(config-if-range)#switchport mode trunk
AC-SW1(config-if-range)#switchport trunk encapsulation dot1q
AC-SW1(config-if-range)#exit
AC-SW1(config)#interface range e0/2-3
AC-SW1(config-if-range)#switchport mode access
AC-SW1(config-if-range)#switchport voice vlan 40
AC-SW1(config-if-range)#switchport access vlan 30
AC-SW1(config-if-range)#exit
AC-SW1(config)#interface e1/0
AC-SW1(config-if-range)#switchport mode access
AC-SW1(config-if-range)#switchport voice vlan 40
AC-SW1(config-if-range)#switchport access vlan 20
```

Command list-2 AC-SW1 Interfaces *Settings*

The same commands for ACCESS-SWITCH 2 (`AC-SW2`) but VLAN 30 must be changed to VLAN 10 .

III.4.1.2 VTP Enabling

Setting device to VTP Client mode for VLANS.

```
AC-SW1(config)#vtp mode client
AC-SW1(config)#vtp domain RT
AC-SW1(config)#vtp version 3
AC-SW1(config)#vtp password rt
```

Command list-3 VTP Enabling

The same commands for ACCESS-SWITCH 2 (`AC-SW2`) .

III.4.2 Configuring Core-Switch 1 & 2

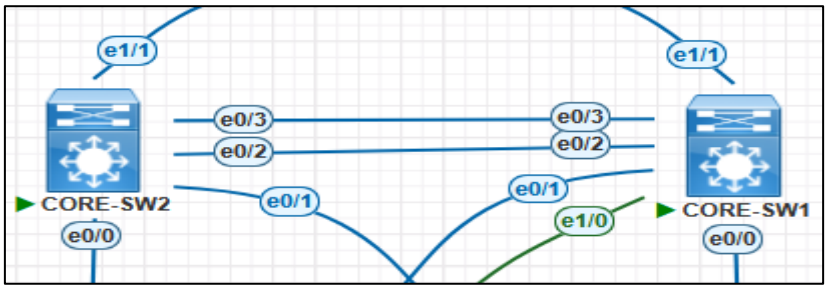


Figure III-25 Configuring Core Switch 1& 2

III.4.2.1 VLANs Segmentation

The same VLANs as configured in AC-SW1 (Command list 1: Configuring VLANs in AC-SW1)

```
CORE-SW1>enable
CORE-SW1#configure terminal
CORE-SW1(config)#vlan 10
CORE-SW1(config-vlan)#name ADMIN
CORE-SW1(config-vlan)#exit
CORE-SW1(config)#vlan 20
CORE-SW1(config-vlan)#name MI
CORE-SW1(config-vlan)#exit
CORE-SW1(config)#vlan 30
CORE-SW1(config-vlan)#name ST
CORE-SW1(config-vlan)#exit
CORE-SW1(config)#vlan 40
CORE-SW1(config-vlan)#name VOICE
CORE-SW1(config-vlan)#exit
```

Command list-4 Configuring VLANs in CORE-SW1

The same commands for CORE-SWITCH 2 (`CORE-SW2`) .

III.4.2.2 SVIs & HSRP Configuration

We've implemented HSRP across both core switches to keep all VLANs CORE-SW1 takes the active gateway (to configure priority 150), while CORE-SW2 waits on standby with the default priority 100. For IP addressing, CORE-SW1 uses .1 addresses, CORE-SW2 uses .2, and all devices point to the shared .100 virtual IP as their gateway. This way, if one switch has an issue, traffic fails over seamlessly. We also added DHCP relay to pass requests to our central server at 192.168.100.1, and enabled preempt so CORE-SW1 automatically takes back control when it's back connection.

```
--------------------------------CORE-SW1----------------------------------
CORE-SW1(config)#interface vlan 10
CORE-SW1(config-if)#ip add 192.168.10.1 255.255.255.0
CORE-SW1(config-if)#ip helper-address 192.168.100.1
CORE-SW1(config-if)#standby 10 ip 192.168.10.100
CORE-SW1(config-if)#standby 10 priority 150
CORE-SW1(config-if)#standby 10 preempt
CORE-SW1(config-if)#no shutdown
CORE-SW1(config-if)#interface vlan 20
CORE-SW1(config-if)#ip add 192.168.20.1 255.255.255.0
CORE-SW1(config-if)#ip helper-address 192.168.100.1
CORE-SW1(config-if)#standby 20 ip 192.168.20.100
CORE-SW1(config-if)#standby 20 priority 150
CORE-SW1(config-if)#standby 20 preempt
CORE-SW1(config-if)#no shutdown
CORE-SW1(config-if)#interface vlan 30
CORE-SW1(config-if)#ip add 192.168.30.1 255.255.255.0
CORE-SW1(config-if)#ip helper-address 192.168.100.1
CORE-SW1(config-if)#standby 30 ip 192.168.30.100
CORE-SW1(config-if)#standby 30 priority 150
CORE-SW1(config-if)#standby 30 preempt
CORE-SW1(config-if)#no shutdown
CORE-SW1(config-if)#interface vlan 40
CORE-SW1(config-if)#ip add 192.168.40.1 255.255.255.0
CORE-SW1(config-if)#ip helper-address 192.168.100.1
CORE-SW1(config-if)#standby 40 ip 192.168.40.100
CORE-SW1(config-if)#standby 40 priority 150
CORE-SW1(config-if)#standby 40 preempt
CORE-SW1(config-if)#no shutdown
```

Command list-5 SVIs & HSRP Configuration in CORE-SW1

```
-------------------------------CORE-SW2----------------------------------
CORE-SW2(config)#interface vlan 10
CORE-SW2(config-if)#ip add 192.168.10.2 255.255.255.0
CORE-SW2(config-if)#ip helper-address 192.168.100.1
CORE-SW2(config-if)#standby 10 ip 192.168.10.100
CORE-SW2(config-if)#standby 10 priority 100
CORE-SW2(config-if)#standby 10 preempt
CORE-SW2(config-if)#no shutdown
CORE-SW2(config-if)#interface vlan 20
CORE-SW2(config-if)#ip add 192.168.20.2 255.255.255.0
CORE-SW2(config-if)#ip helper-address 192.168.100.1
CORE-SW2(config-if)#standby 20 ip 192.168.20.100
CORE-SW2(config-if)#standby 20 priority 100
CORE-SW2(config-if)#standby 20 preempt
CORE-SW2(config-if)#no shutdown
CORE-SW2(config-if)#interface vlan 30
CORE-SW2(config-if)#ip add 192.168.30.2 255.255.255.0
CORE-SW2(config-if)#ip helper-address 192.168.100.1
CORE-SW2(config-if)#standby 30 ip 192.168.30.100
CORE-SW2(config-if)#standby 30 priority 100
CORE-SW2(config-if)#standby 30 preempt
CORE-SW2(config-if)#no shutdown
CORE-SW2(config-if)#interface vlan 40
CORE-SW2(config-if)#ip add 192.168.40.2 255.255.255.0
CORE-SW2(config-if)#ip helper-address 192.168.100.1
CORE-SW2(config-if)#standby 40 ip 192.168.40.100
CORE-SW2(config-if)#standby 40 priority 100
CORE-SW2(config-if)#standby 40 preempt
CORE-SW2(config-if)#no shutdown
```

Command list-6 SVIs & HSRP Configuration in CORE-SW2

III.4.2.3 Configuring Interfaces

Setting some ports to layer 3 for IP addresses and configuring others as trunk with Dot1Q encapsulation

```
-------------------------------CORE-SW1----------------------------------
CORE-SW1(config)#interface e1/0
CORE-SW1(config-if)#no switchport
CORE-SW1(config-if)#ip add 192.168.100.100 255.255.255.0
CORE-SW1(config-if)#interface e1/1
CORE-SW1(config-if)#no switchport
CORE-SW1(config-if)#ip add 192.168.110.1 255.255.255.0
CORE-SW1(config-if)#interface range e0/0-1
CORE-SW1(config-if-range)#switchport mode trunk
CORE-SW1(config-if-range)#switchport trunk encapsulation dot1q
CORE-SW1(config)# interface range e0/2-3
CORE-SW1(config-if-range)#switchport trunk encapsulation dot1q
CORE-SW1(config-if-range)#switchport mode trunk
```

Command list-7 Configuring Interfaces in CORE-SW1

```
-------------------------------CORE-SW2----------------------------------
CORE-SW2(config)#interface e1/1
CORE-SW2(config-if)#no switchport
CORE-SW2(config-if)#ip add 192.168.120.1 255.255.255.0
CORE-SW2(config-if)#exit
CORE-SW2(config-if)#interface range e0/0-1
CORE-SW2(config-if-range)#switchport mode trunk
CORE-SW2(config-if-range)#switchport trunk encapsulation dot1q
CORE-SW2(config-if-range)#exit
CORE-SW2(config)# interface range e0/2-3
CORE-SW2(config-if-range)#switchport trunk encapsulation dot1q
CORE-SW2(config-if-range)#switchport mode trunk
```

Command list-8 Configuring Interfaces in CORE-SW2

III.4.2.4 Configuring the EtherChannel Between Core-SW 1 and Core-SW 2

EtherChannel is configured to increase bandwidth, provide redundancy, simplify management and improve network performance

```
--------------------------------CORE-SW1---------------------------------
CORE-SW1(config)# interface range e0/2-3
CORE-SW1(config-if-range)# shutdown
CORE-SW1(config-if-range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1
CORE-SW1(config-if-range)#no shutdown
```

Command list-9 Configuring EtherChannel in CORE-SW1

```
--------------------------------CORE-SW2---------------------------------
CORE-SW2(config)# interface range e0/2-3
CORE-SW2(config-if-range)# shutdown
CORE-SW2(config-if-range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1
CORE-SW2(config-if-range)#no shutdown
```

Command list-10 Configuring EtherChannel in CORE-SW2

III.4.2.5 VTP Enabling

Setting device to VTP Server mode for VLANS

```
--------------------------------CORE-SW1---------------------------------
CORE-SW1(config)#vtp mode server
CORE-SW1(config)#vtp domain RT
CORE-SW1(config)#vtp version 3
CORE-SW1(config)#vtp password rt
```

Command list-11 Enabling VTP in CORE-SW1

The same commands for CORE-SWITCH 2 (`CORE-SW2`).

III.4.2.6 Routing Configuration

We configured a default routing for our internet connection while using OSPF as our internal routing protocol to connect all network segments.

```
--------------------------------CORE-SW1---------------------------------
CORE-SW1(config)#ip route 0.0.0.0 0.0.0.0 192.168.110.2
CORE-SW1(config)#router ospf 1
CORE-SW1(config-router)#network 192.168.10.0 0.0.0.255 area 0
CORE-SW1(config-router)#network 192.168.20.0 0.0.0.255 area 0
CORE-SW1(config-router)#network 192.168.30.0 0.0.0.255 area 0
CORE-SW1(config-router)#network 192.168.40.0 0.0.0.255 area 0
CORE-SW1(config-router)#network 192.168.100.0 0.0.0.255 area 0
CORE-SW1(config-router)#network 192.168.110.0 0.0.0.255 area 0
CORE-SW1(config-router)#network 192.168.120.0 0.0.0.255 area 0
```

Command list-12 Routing Configuration in CORE-SW1

```
-------------------------------CORE-SW2----------------------------------
CORE-SW2(config)#ip route 0.0.0.0 0.0.0.0 192.168.120.2
CORE-SW2(config)#router ospf 1
CORE-SW2(config-router)#network 192.168.10.0 0.0.0.255 area 0
CORE-SW2(config-router)#network 192.168.20.0 0.0.0.255 area 0
CORE-SW2(config-router)#network 192.168.30.0 0.0.0.255 area 0
CORE-SW2(config-router)#network 192.168.40.0 0.0.0.255 area 0
CORE-SW2(config-router)#network 192.168.110.0 0.0.0.255 area 0
CORE-SW2(config-router)#network 192.168.120.0 0.0.0.255 area 0
```

Command list-13 Routing Configuration in CORE-SW2

III.4.3 Configuring Head Quarter-Router

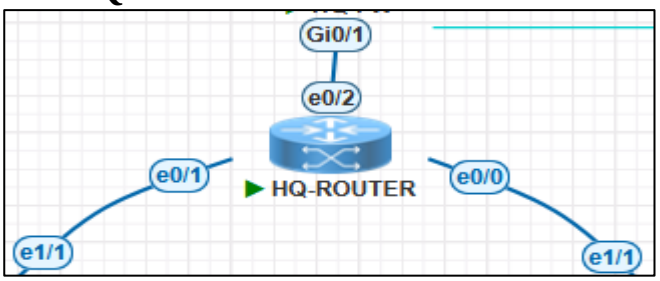


Figure III-26 Configuring the HQ-Router

We configure the interfaces and then set up routing

```
HQ-ROUTER(config)#int e0/0
HQ-ROUTER(config-if)#ip add 192.168.115.2 255.255.255.0
HQ-ROUTER(config-if)#no shutdown
HQ-ROUTER(config-if)#exit
HQ-ROUTER(config)#int e0/1
HQ-ROUTER(config-if)#ip add 192.168.110.2 255.255.255.0
HQ-ROUTER(config-if)#no shutdown
HQ-ROUTER(config-if)#exit
HQ-ROUTER(config)#int e0/2
HQ-ROUTER(config-if)#ip add 192.168.120.2 255.255.255.0
HQ-ROUTER(config-if)#no shutdown
HQ-ROUTER(config-if)#exit
HQ-ROUTER(config)#ip route 0.0.0.0 0.0.0.0 192.168.115.1
HQ-ROUTER(config)#router ospf 1
HQ-ROUTER(config-router)#network 192.168.110.0 0.0.0.255 area 0
HQ-ROUTER(config-router)#network 192.168.120.0 0.0.0.255 area 0
HQ-ROUTER(config-router)#network 192.168.115.0 0.0.0.255 area 0
```

Command list-14 Configuring the HQ- Router

III.4.4 Configuring ASA Firewall

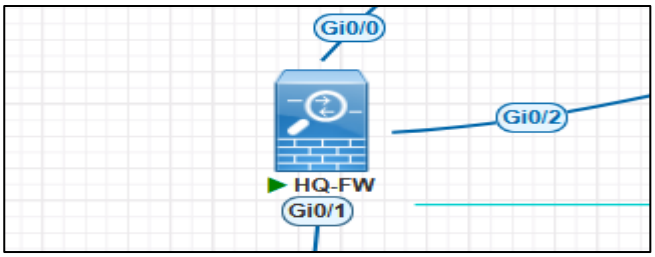


Figure III-27 Configuring the ASA Firewall (HQ-Firewall)

III.4.4.1 Configuring the INSIDE and The OUTSIDE Interfaces

In ASA firewall, interfaces are configured and named inside with security level 100 and outside with a security level of 0

```
HQ-FW(config)# int gigabitEthernet 0/0
HQ-FW(config-if)# ip add 10.10.10.1 255.255.255.252
HQ-FW(config-if)# nameif OUTSIDE
HQ-FW(config-if)# security-level 0
HQ-FW(config-if)# no sh
HQ-FW(config-if)# exit
HQ-FW(config)# int gigabitEthernet 0/1
HQ-FW(config-if)# ip add 192.168.115.1 255.255.255.0
HQ-FW(config-if)# nameif INSIDE
HQ-FW(config-if)# security-level 100
HQ-FW(config-if)# no sh
HQ-FW(config-if)# exit
HQ-FW(config)# int gigabitEthernet 0/2
HQ-FW(config-if)# ip add 10.10.20.1 255.255.255.252
HQ-FW(config-if)# nameif OUTSIDE
HQ-FW(config-if)# security-level 0
HQ-FW(config-if)# no sh
HQ-FW(config-if)# exit
```

Command list-15 Configuring Interfaces of HQ-FW

III.4.4.2 Routing Configuration

```
HQ-FW(config)# router ospf 1
HQ-FW(config-router)# network 192.168.115.0 255.255.255.0 area 0
HQ-FW(config-router)# network 10.10.10.0 255.255.255.252 area 0
HQ-FW(config-router)# network 10.10.20.0 255.255.255.252 area 0
HQ-FW(config-router)# exit
HQ-FW(config)# route outside 0.0.0.0 0.0.0.0 10.10.10.2
```

Command list-16 Routing Configuration in HQ-FW

III.4.4.3 Access List Permission

We've implemented access control lists to securely permit inbound traffic for essential services DHCP (using ports 67 and 68) to handle automatic IP, DNS and WEB (port 53), WEB (port 80) and FTP (ports 20 and 21) for file transfers. We've also enabled specific ICMP functions (unreachable icmp type 3) including echo and echo-reply for troubleshoot connectivity with ping tests when needed. These rules are applied to the outside interface.

```
HQ-FW(config)# access-list ACCESS permit icmp any any
HQ-FW(config)# access-list ACCESS permit icmp any any unreachable
HQ-FW(config)# access-list ACCESS permit icmp any any echo
HQ-FW(config)# access-list ACCESS permit icmp any any echo-reply
HQ-FW(config)# access-list ACCESS permit udp any any eq 67
HQ-FW(config)# access-list ACCESS permit udp any any eq 68
HQ-FW(config)# access-list ACCESS permit udp any any eq 53
HQ-FW(config)# access-list ACCESS permit tcp any any eq 53
HQ-FW(config)# access-list ACCESS permit tcp any any eq 20
HQ-FW(config)# access-list ACCESS permit tcp any any eq 21
HQ-FW(config)# access-group ACCESS in interface OUTSIDE
```

Command list-17 Configuring Access List in HQ-FW

III.4.4.4 NAT Overload

Configuring NAT Overload to translate internal network addresses into a shared external IP address via a single interface

```
HQ-FW(config)# object network LAN-INTERNET
HQ-FW(config-network-object)# subnet 0.0.0.0 0.0.0.0
HQ-FW(config-network-object)# nat (INSIDE,OUTSIDE) dynamic interface
HQ-FW(config-network-object)#exit
HQ-FW(config)# object network WAN-INTERNET
HQ-FW(config-network-object)# subnet 10.10.10.0 255.255.255.252
HQ-FW(config-network-object)# nat (INSIDE,OUTSIDE) dynamic interface
```

Command list-18 Configuring NAT overload in HQ-FW

III.4.5 ISP-ROUTER Configuration

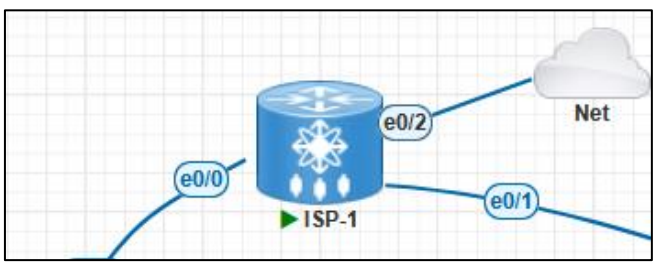


Figure III-28 Configuring the ISP-ROUTER

We configure the interfaces and then set up routing

```
ISP-1(config)#int e0/0
ISP-1(config-if)#ip add 10.10.10.2 255.255.255.252
ISP-1(config-if)#no shutdown
ISP-1(config-if)#int e0/1
ISP-1(config-if)#ip add 10.10.10.6 255.255.255.252
ISP-1(config-if)#no shutdown
ISP-1(config-if)#int e0/2
ISP-1(config-if)#ip add dhcp
ISP-1(config-if)#ip nat outside
ISP-1(config-if)#no shutdown
ISP-1(config-if)#exit
ISP-1(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.1
ISP-1(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.5
ISP-1(config)#router ospf 1
ISP-1(config-router)#network 10.10.10.0 0.0.0.3 area 0
ISP-1(config-router)#network 10.10.10.4 0.0.0.3 area 0
ISP-1(config-router)#network 192.168.128.0.0.0.255 area 0
```

Command list-19 ISP-ROUTER Configuration

III.4.6 Building the Branch Topology

The branch topology will have the same configuration as headquarter topology, with changes to the Ips and VLAN names.

VLAN 50 BIOLOGY, VLAN 60 MEDICINE and VLAN 70 ARCHITECTURE

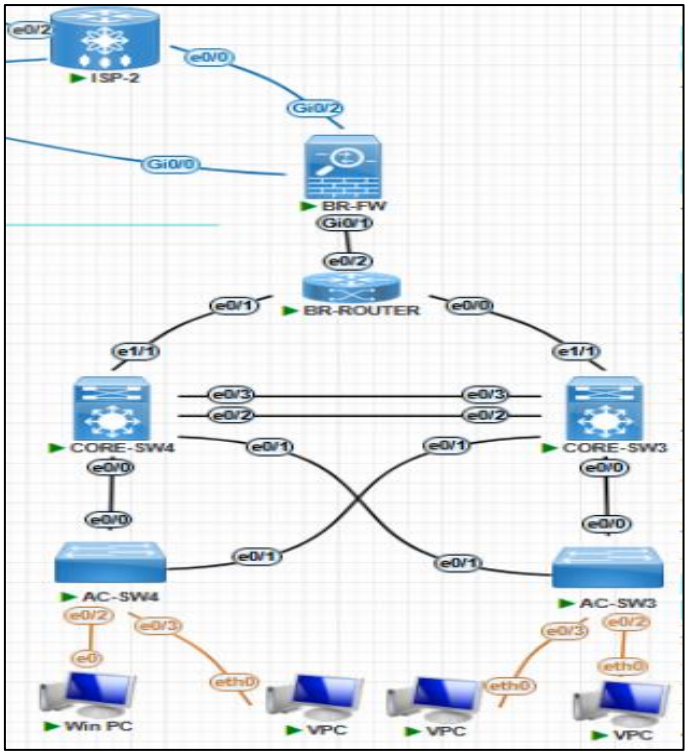


Figure III-29 Branch Topology

III.5 Security Part Implementation

We will secure our network using best security implementation

III.5.1 Layer 2 security best practice

Layer 2 security enhances network protection by preventing unauthorized access, mitigating attacks, and ensuring reliable data transmission.

```
AC-SW1 (config)#int range e0/2-3
AC-SW1 (config-if)#switchport port-security
AC-SW1 (config-if)#switchport port-security mac-address sticky
AC-SW1 (config-if)#switchport port-security maximum 1
AC-SW1 (config-if)#switchport port-security violation shutdown
AC-SW1 (config-if)#spanning-tree portfast
AC-SW1 (config-if)#spanning-tree bpduguard enable
AC-SW1 (config)#int range e0/0-1
AC-SW1 (config-if)# spanning-tree guard root
```

Command list-20 Configuration of Layer 2 Security

III.5.2 DHCP Spoofing & DHCP Starvation Attacks Mitigation

To prevent DHCP spoofing attacks, First, we enable DHCP snooping on all access and core switches to block rogue DHCP servers, then configure a strict rate limit of 3 DHCP packets per second per port to prevent flooding attacks. For centralized control, we designate authorized DHCP servers by configuring IP helper-addresses on each VLAN interface of our core switches

```
  ----------------For Access and Core Switches ---------------
AC-SW1 (config)#ip dhcp snooping
AC-SW1 (config)#ip dhcp snooping vlan 10
AC-SW1 (config)#ip dhcp snooping vlan 30
AC-SW1 (config)#ip dhcp snooping vlan 40
AC-SW1(config)#no ip dhcp snooping information option
------------------Access Switches Only----------------------
AC-SW1 (config)#interface range e0/0-3 , e1/0-1
AC-SW1 config-if-range)#ip dhcp snooping limit rate 10
```

Command list-21 Configuration of DHCP Snooping

III.5.3 Site-to-Site VPN configuration (IPsec VPN)

We've set up a VPN connection between local and remote networks (headquarter and branch networks) using AES-256 encryption and pre-shared key authentication. It works in two phases: the first phase for encryption and authentication, and the second phase for data transfer using an ESP with session duration.

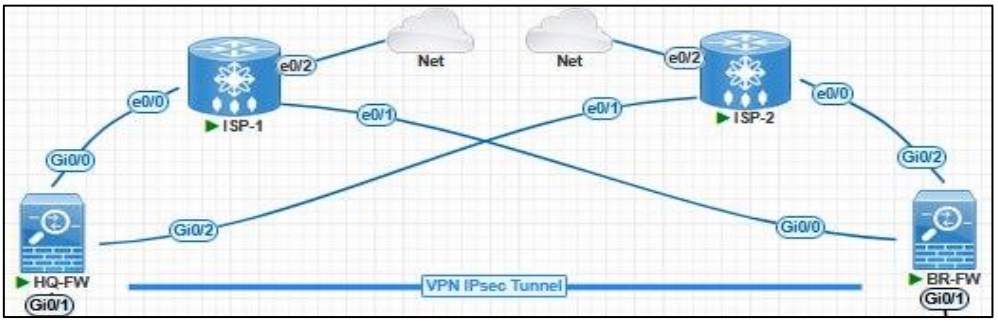


Figure III-30 IPsec VPN Configuration

```
----------------------------Object-group network ----------------------------
HQ-FW(config)# object-group network local-network
HQ-FW(config-network-object-group)# network-object 192.168.100.0 255.255.255.0
HQ-FW(config-network-object-group)# network-object 192.168.10.0 255.255.255.0
HQ-FW(config-network-object-group)# network-object 192.168.20.0 255.255.255.0
HQ-FW(config-network-object-group)# network-object 192.168.30.0 255.255.255.0
HQ-FW(config-network-object-group)# network-object 192.168.40.0 255.255.255.0
HQ-FW(config)# object-group network remote-network
HQ-FW(config-network-object-group)# network-object 192.168.50.0 255.255.255.0
HQ-FW(config-network-object-group)# network-object 192.168.60.0 255.255.255.0
HQ-FW(config-network-object-group)# network-object 192.168.70.0 255.255.255.0
--------------------------- Access-list ----------------------------------
HQ-FW(config)# access-list vpn extended permit ip object-group local-network $
object-group remote-network
--------------------------- Ike Phase 1 ipsec-vpn--------------------------
HQ-FW(config)# crypto ikev1 enable OUTSIDE
HQ-FW(config)# crypto isakmp identity address
HQ-FW(config)# crypto ikev1 policy 10
HQ-FW(config-ikev1-policy)# authentication pre-share
HQ-FW(config-ikev1-policy)# encryption aes-256
HQ-FW(config-ikev1-policy)# hash sha
HQ-FW(config-ikev1-policy)# group 5
HQ-FW(config-ikev1-policy)# lifetime 3600
--------------------------- Ike Phase 2 ipsec-vpn--------------------------
HQ-FW(config)# crypto ipsec ikev1 transform-set set esp-aes-256 esp-sha-hmac
HQ-FW(config)# crypto map map 10 match address vpn
HQ-FW(config)# crypto map map 10 set peer 10.10.10.5
HQ-FW(config)# crypto map map 10 set ikev1 transform-set set
HQ-FW(config)# crypto map map 10 set security-association lifetime seconds 28800
HQ-FW(config)# crypto map map interface OUTSIDE
HQ-FW(config)# tunnel-group 10.10.10.5 type ipsec-l2l
HQ-FW(config)# tunnel-group 10.10.10.5 ipsec-attributes
HQ-FW(config-tunnel-ipsec)# ikev1 pre-shared-key cisco
HQ-FW(config)# nat (inside,outside) source static local-network local-network
$destination static remote-network remote-network no-proxy-arp route-lookup
```

Command list-22 Site-to-Site VPN Configuration

III.6 Network Effectiveness Part Validation and Testing

After ending the configuration of the two sides, we are going to verify and test our network

III.6.1 Test1(Testing DHCP on End Devices)

On any PC of our campus network, the IP configuration was verified via Command Prompt to confirm automatic IP assignment from the DHCP server

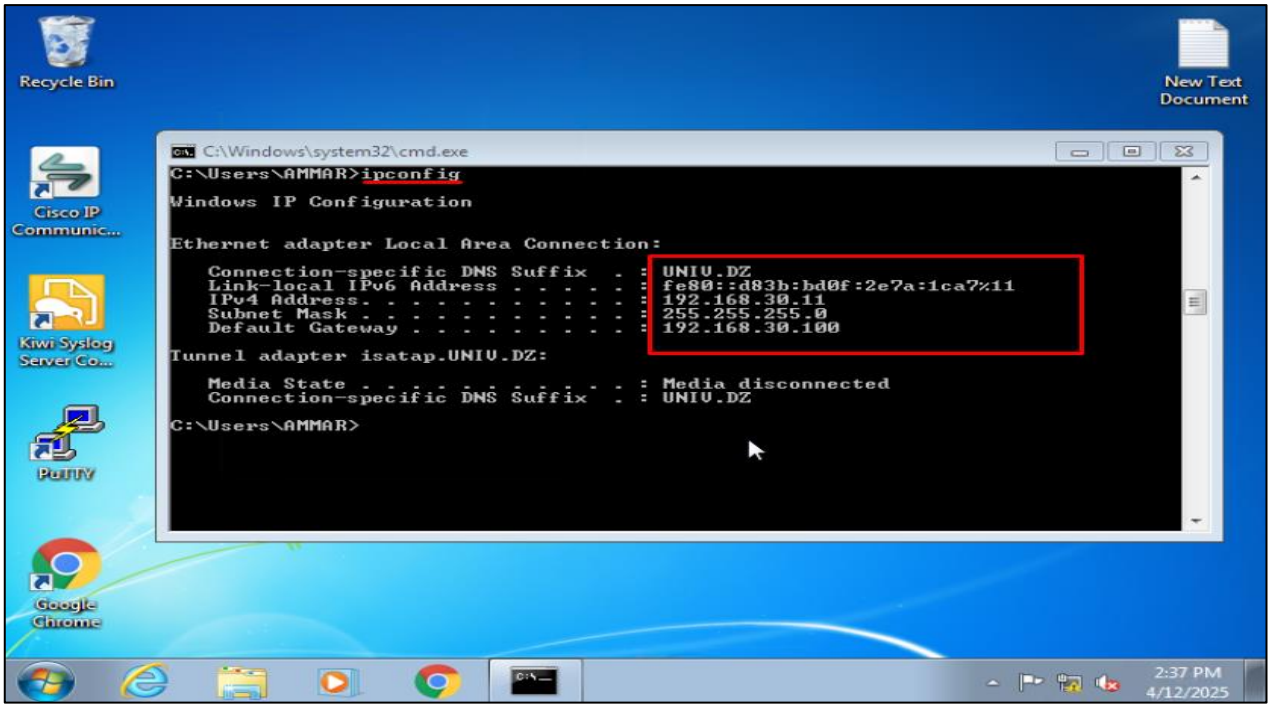


Figure III-31 Check IP Configuration in Windows (IP By DHCP) - Command Prompt

III.6.2 Test 2(Validating HSRP Protocol)

The show standby command displayed HSRP group settings (Vlan10 - Group 10) including virtual IP (192.168.10.100), router state (Active/Standby), and device priority (150). CORE-SW2 showed Standby state due to lower priority

```
------------------------------CORE-SW1----------------------------------
CORE-SW1#show standby
Vlan10 - Group 10
  State is Active
    2 state changes, last state change 00:45:51
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is 0000.0c07.ac0a (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.224 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.10.2, priority 100 (expires in 8.096 sec)
  Priority 150 (configured 150)
  Group name is "hsrp-Vl10-10" (default)
```

Command list-23 HSRP Protocol Validation in CORE-SW1

```
------------------------------CORE-SW2---------------------------------
CORE-SW2#show standby
Vlan10 - Group 10
  State is Standby
    1 state change, last state change 00:18:32
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is 0000.0c07.ac0a (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.208 secs
  Preemption enabled
  Active router is 192.168.10.1, priority 150 (expires in 7.408 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Vl10-10" (default)
```

Command list-24 HSRP Protocol Validation in CORE-SW2

III.6.3 Test 3 (Testing EtherChannel)

The show EtherChannel summary command revealed Port-channel 1 aggregation between Et0/2 and Et0/3 interfaces using PAgP protocol

```
------------------------------CORE-SW1---------------------------------
CORE-SW1#show etherchannel summary
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------------------------------------------------------------------------

1      Po1(SU)          PAgP      Et0/2(P)    Et0/3(P)
```

Command list-25 EtherChannel Validation in CORE-SW1

III.6.4 Test 4(Checking VTP Status)

CORE-SW1 operated in Server mode within "RT" domain with 9 VLANs and ACCESS-SW1 functioned as Client in same domain ensuring VLAN synchronization

```
------------------------------ACCESS-SW1---------------------------------
AC-SW1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : RT
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0a00
Feature VLAN:
VTP Operating Mode                : Client
Number of existing VLANs          : 9
```

Command list-26 VTP Status in AC-SW1

```
------------------------------CORE-SW1---------------------------------
CORE-SW1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : RT
VTP Pruning Mode                : Disabled
VTP Traps Generation         : Disabled
Device ID                 : aabb.cc80.0500
Feature VLAN:
--------------
VTP Operating Mode            : Server
Number of existing VLANs        : 9
```

Command list-27 VTP Status in CORE-SW1

III.6.5 Test 5(Checking Port-security)

Port Security Enabled on interface e1/1 with Shutdown violation mode, recording only permitted MAC address

```
AC-SW1#show port-security interface e1/1
Port Security               : Enabled
Port Status                 : Secure-shutdown
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses       : 1
Total MAC Addresses         : 1
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 1
Last Source Address:Vlan    : d2f8.ab43.2b74:30
Security Violation Count    : 1
```

Command list-28 Port-Security Validation

III.6.6 Test 6(Routing Table Verification)

HQ-FW displayed diverse routes (OSPF, connected, static) including default route and internal/external networks

```
HQ-FW# show route
Gateway of last resort is 10.10.10.2 to network 0.0.0.0
S*    0.0.0.0 0.0.0.0 [1/0] via 10.10.10.2, OUTSIDE
C     10.10.10.0 255.255.255.252 is directly connected, OUTSIDE
L     10.10.10.1 255.255.255.255 is directly connected, OUTSIDE
O     10.10.10.4 255.255.255.252 [110/20] via 10.10.10.2, 00:15:03, OUTSIDE
O     10.10.20.0 255.255.255.252 [110/30] via 10.10.10.2, 00:14:53, OUTSIDE
O     10.10.20.4 255.255.255.252 [110/30] via 10.10.10.2, 00:14:53, OUTSIDE
O     192.168.10.0 255.255.255.0
           [110/21] via 192.168.115.2, 00:16:01, INSIDE
O     192.168.20.0 255.255.255.0
           [110/21] via 192.168.115.2, 00:16:01, INSIDE
O     192.168.30.0 255.255.255.0
           [110/21] via 192.168.115.2, 00:16:01, INSIDE
O     192.168.40.0 255.255.255.0
           [110/21] via 192.168.115.2, 00:16:01, INSIDE
O     192.168.50.0 255.255.255.0 [110/41] via 10.10.10.2, 00:14:53, OUTSIDE
O     192.168.60.0 255.255.255.0 [110/41] via 10.10.10.2, 00:14:58, OUTSIDE
O     192.168.70.0 255.255.255.0 [110/41] via 10.10.10.2, 00:14:58, OUTSIDE
O     192.168.90.0 255.255.255.0 [110/40] via 10.10.10.2, 00:14:58, OUTSIDE
O     192.168.95.0 255.255.255.0 [110/40] via 10.10.10.2, 00:14:58, OUTSIDE
O     192.168.100.0 255.255.255.0
           [110/30] via 192.168.115.2, 00:16:06, INSIDE
O     192.168.110.0 255.255.255.0
           [110/20] via 192.168.115.2, 00:16:06, INSIDE
C     192.168.115.0 255.255.255.0 is directly connected, INSIDE
L     192.168.115.1 255.255.255.255 is directly connected, INSIDE
O     192.168.120.0 255.255.255.0
           [110/20] via 192.168.115.2, 00:16:07, INSIDE
O     192.168.125.0 255.255.255.0
           [110/30] via 10.10.10.2, 00:14:59, OUTSIDE
O     192.168.128.0 255.255.255.0
           [110/20] via 10.10.10.2, 00:14:59, OUTSIDE
```

Command list-29 Verifying Routing Table

III.6.7 Test 7 (Verifying IPsec VPN Tunnel)

The show crypto ipsec sa command detailed secure tunnel between HQ and branch with encryption statistics and algorithms used

```
BR-FW# show crypto ipsec sa
interface: OUTSIDE
    Crypto map tag: map, seq num: 10, local addr: 10.10.10.5

      access-list vpn extended permit ip 192.168.50.0 255.255.255.0
192.168.100.0 255.255.255.0
      local ident (addr/mask/prot/port):
(192.168.50.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port):
(192.168.100.0/255.255.255.0/0/0)
      current_peer: 10.10.10.1

      #pkts encaps: 153, #pkts encrypt: 153, #pkts digest: 153
      #pkts decaps: 85, #pkts decrypt: 85, #pkts verify: 85
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 153, #pkts comp failed: 0, #pkts decomp
failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments
created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.10.10.5/0, remote crypto endpt.:
10.10.10.1/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 833DE2BA
      current inbound spi : F99F1B0A
```

Command list-30 Verifying IPsec VPN

III.6.8 File Sharing Validation

The image depicts a secure file sharing among multiple computers in our campus network using Active Directory

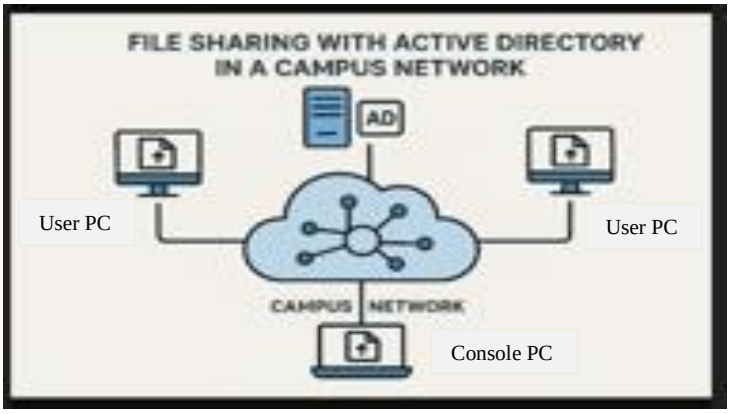


Figure III-32 File Sharing Purpose

Enabling file sharing can be summarized in these 2 steps

Step 1: Accessing the server and create a folder

We will create a file on our server and make it publicly accessible to everyone on our network. This turns the server into a file server as it mentioned in figure III.33 and III.34

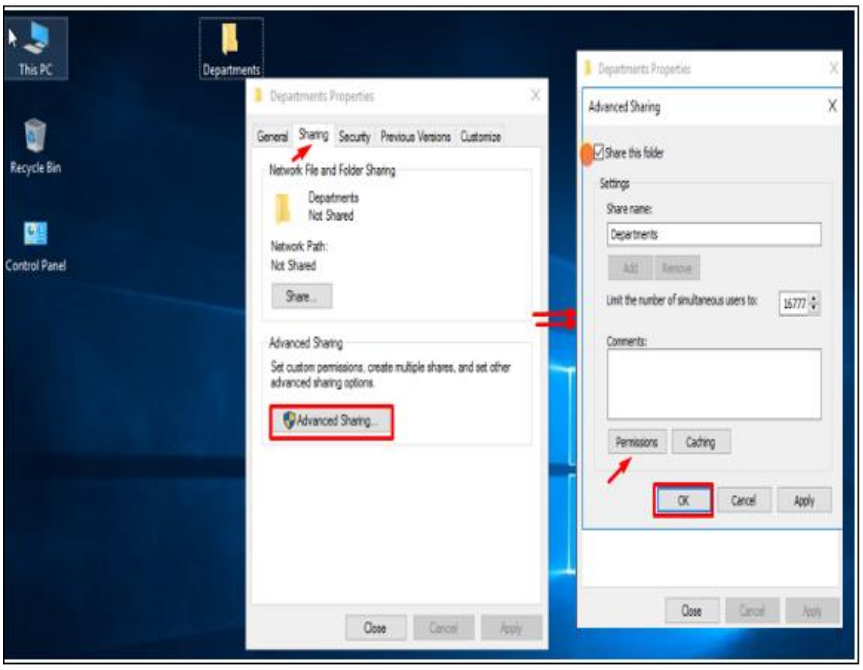


Figure III-33 Selecting Permissions for the Folder (For everyone)

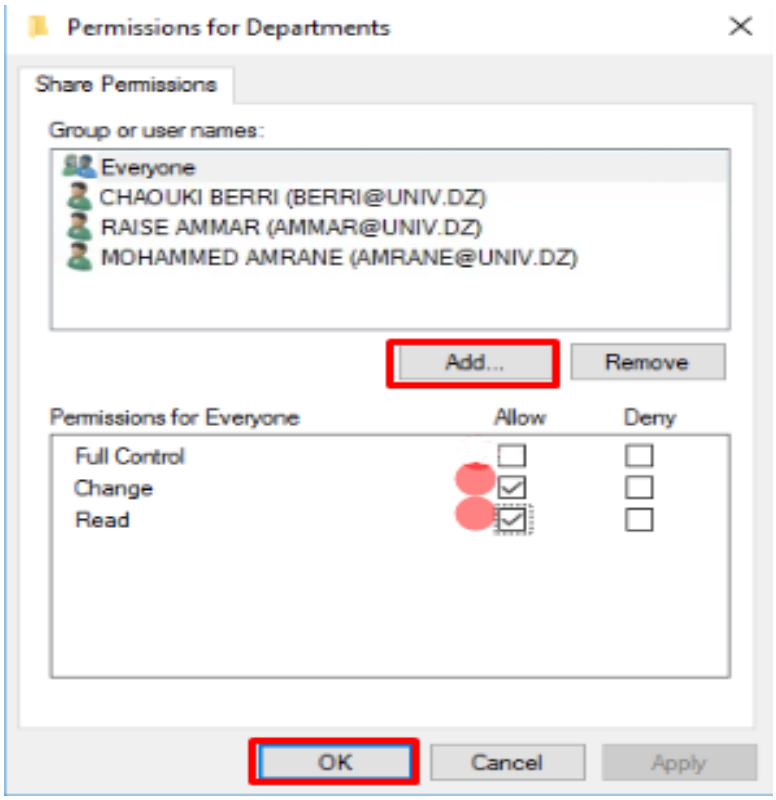


Figure III-34 Folder Sharing Properties in win -server

Step 02: Joining computers to the domain and file server setup

After creating a folder in the server, we will join the computers to the domain using steps explained in the list of figures (III.35 ➔ III. 39)

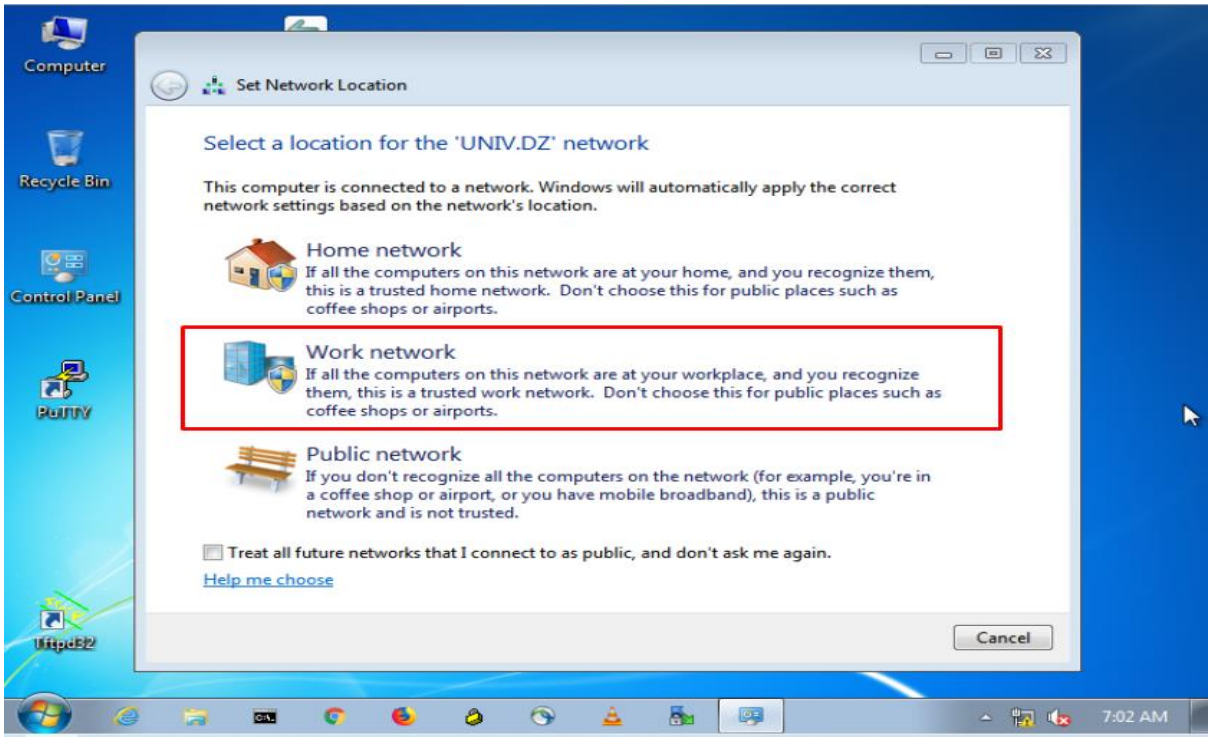


Figure III-35 Selecting Network Type for UNIV.DZ - Security Settings

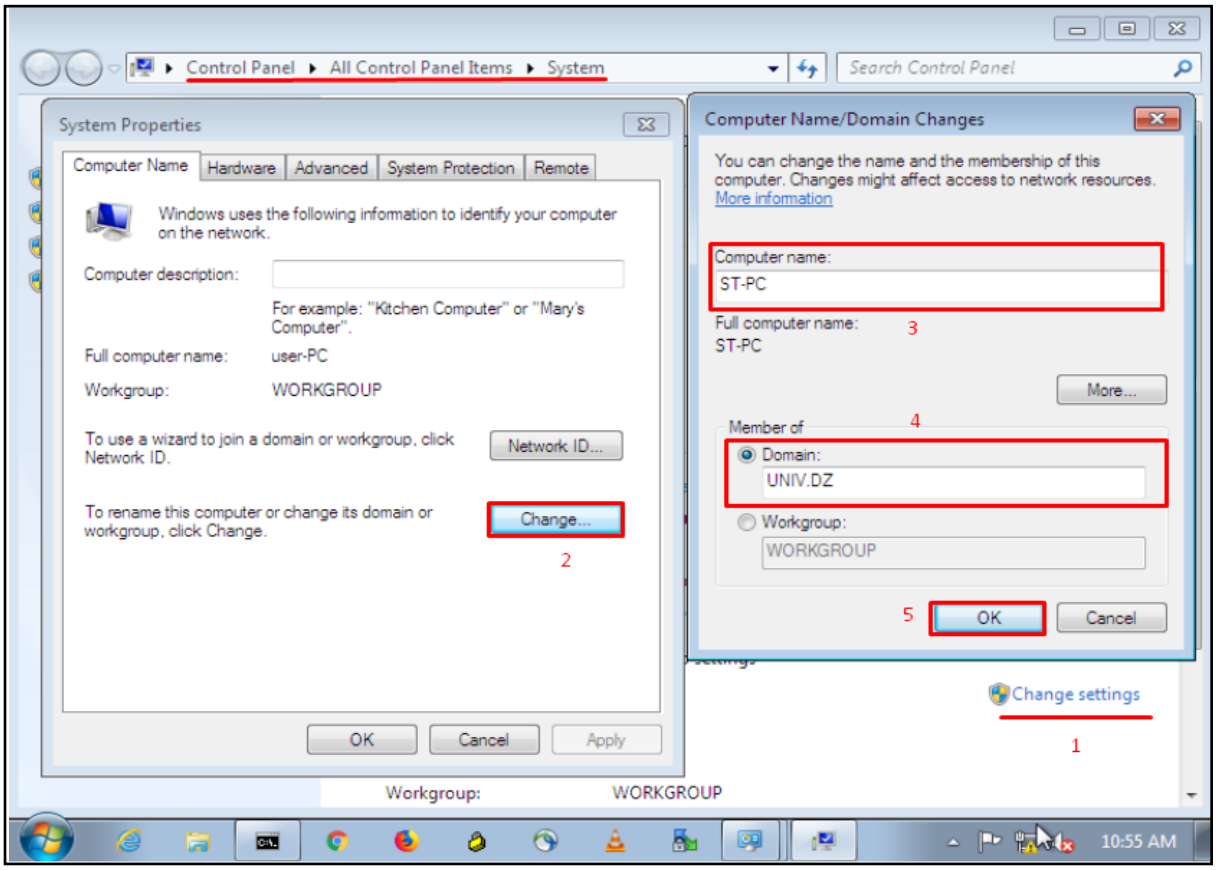


Figure III-36 Computer Name and Domain Configuration (UNIV.DZ) - System Properties

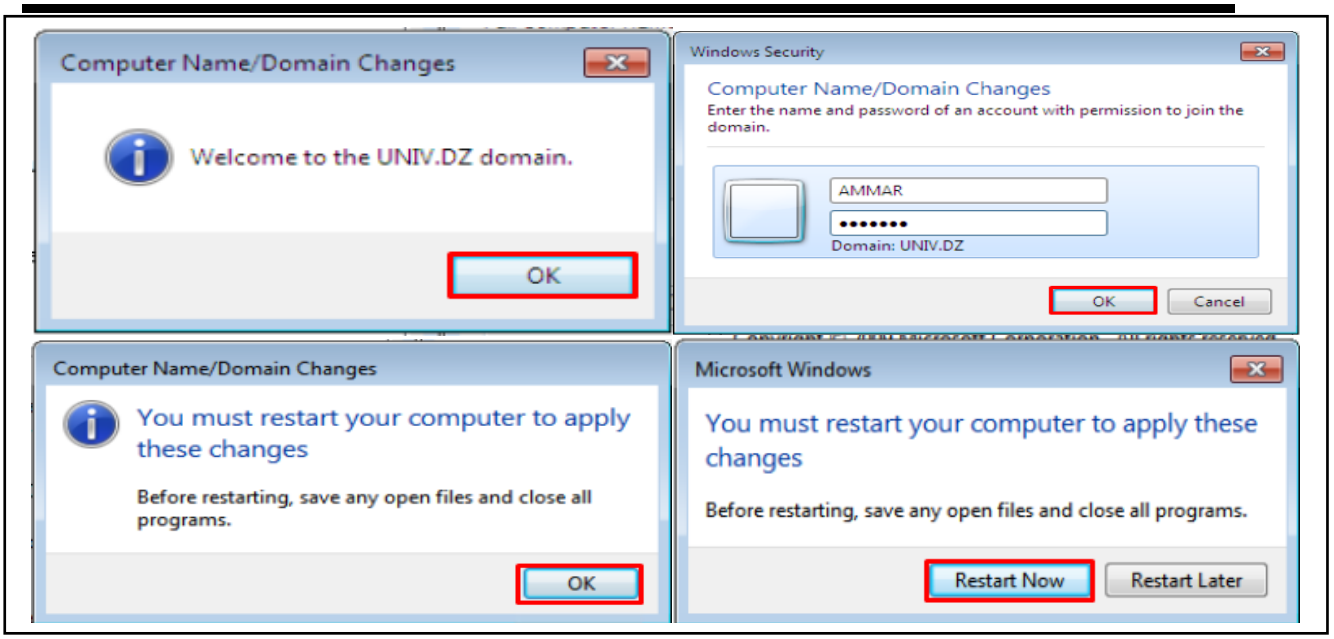


Figure III-37 Steps of Logging into the Domain (UNIV.DZ)

After restarting the computer, we will joined the university domain due the users that we have created before

Figure III-38 Windows 7 Login Screen

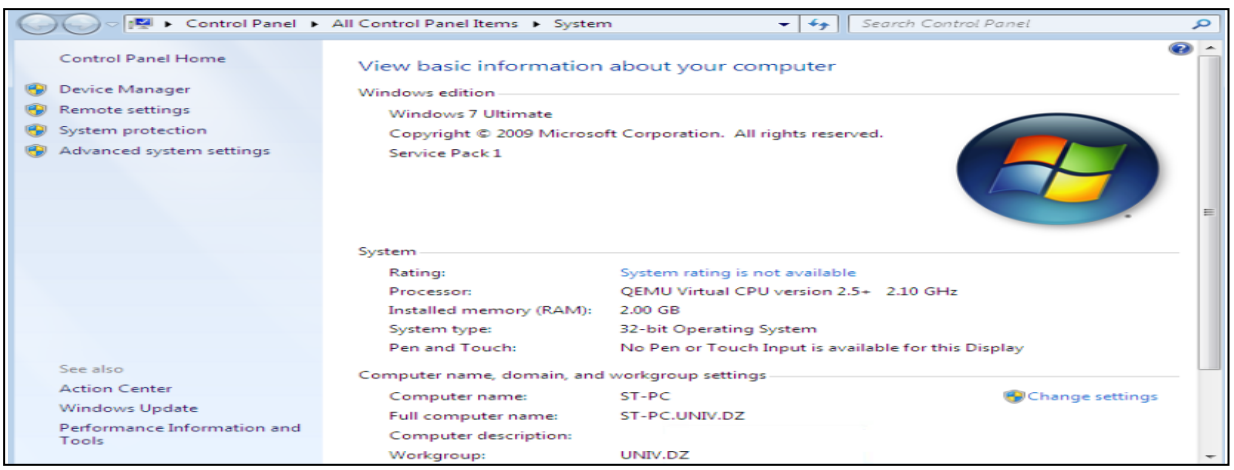


Figure III-39 Computer System window

After joining the computers to the domain, we will map the network folder in PCs

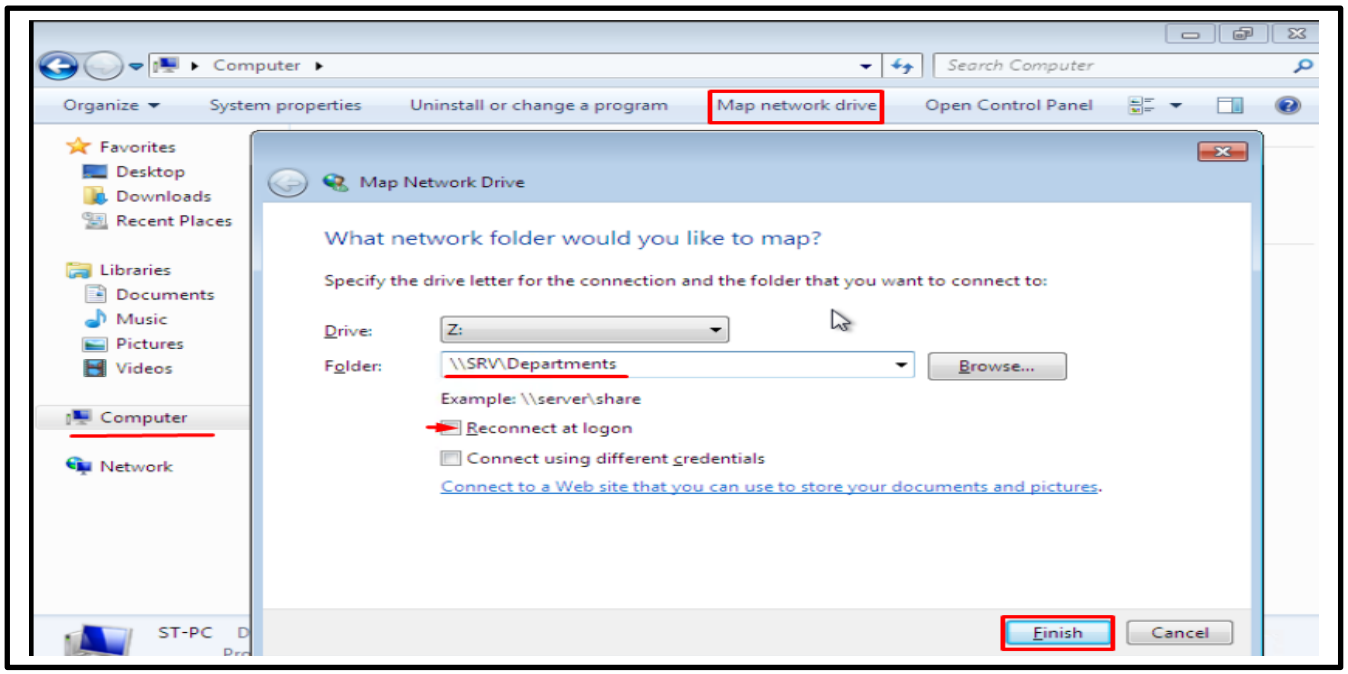


Figure III-40 Mapping the Network Folder in PCs

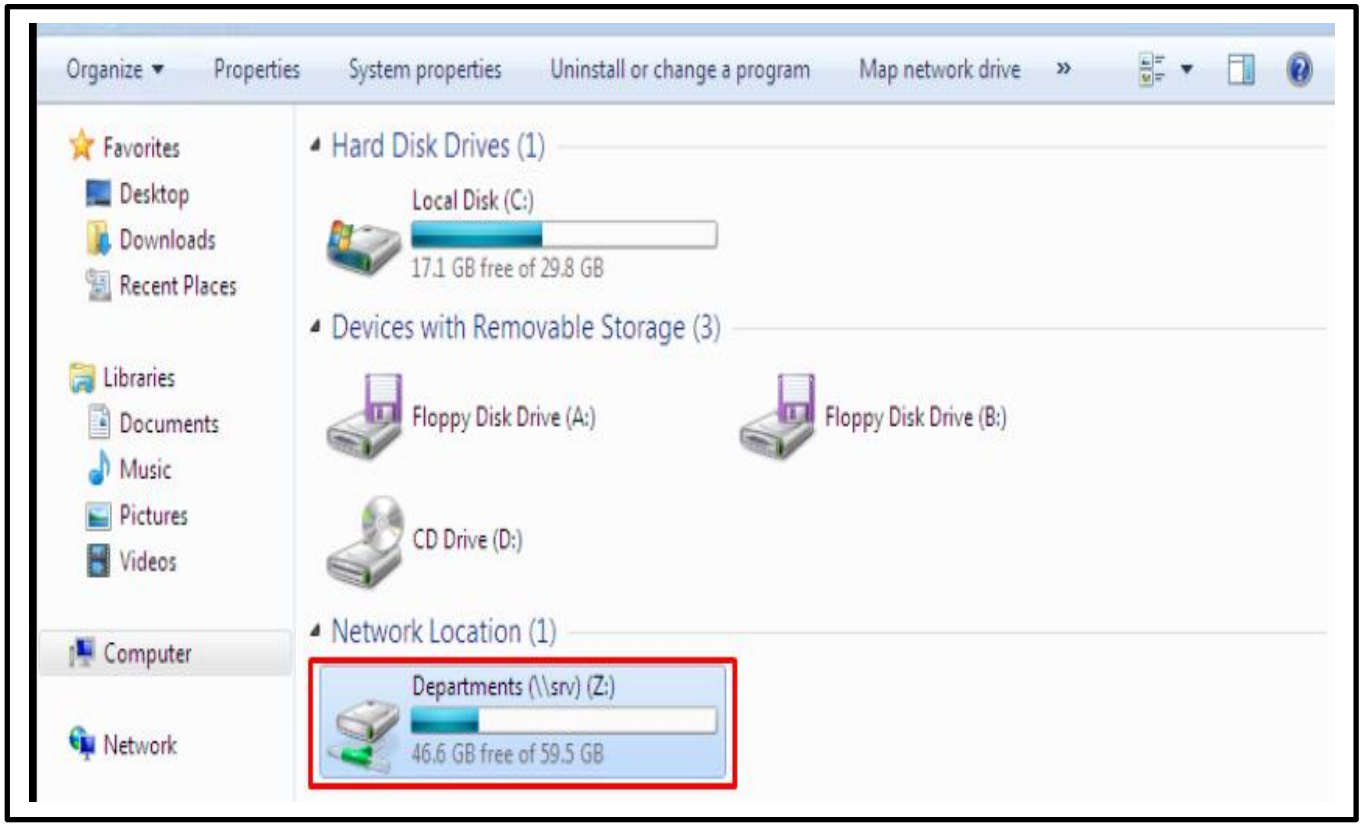


Figure III-41 Folder Sharing is Successful

Finally, we see the appearance of the folder created in our PC'S network, so we can say it's Successful file sharing creating.

III.6.9 Connectivity Testing

III.6.9.1 Testing Connectivity Between HQ and BR

Figure III-42 represent the CMD of AMMAR'S PC located in the HQ and Figure III-43 represent the CMD of ATTAFI'S PC located in the BR, we are going to ping between devices to test the connectivity of our campus network

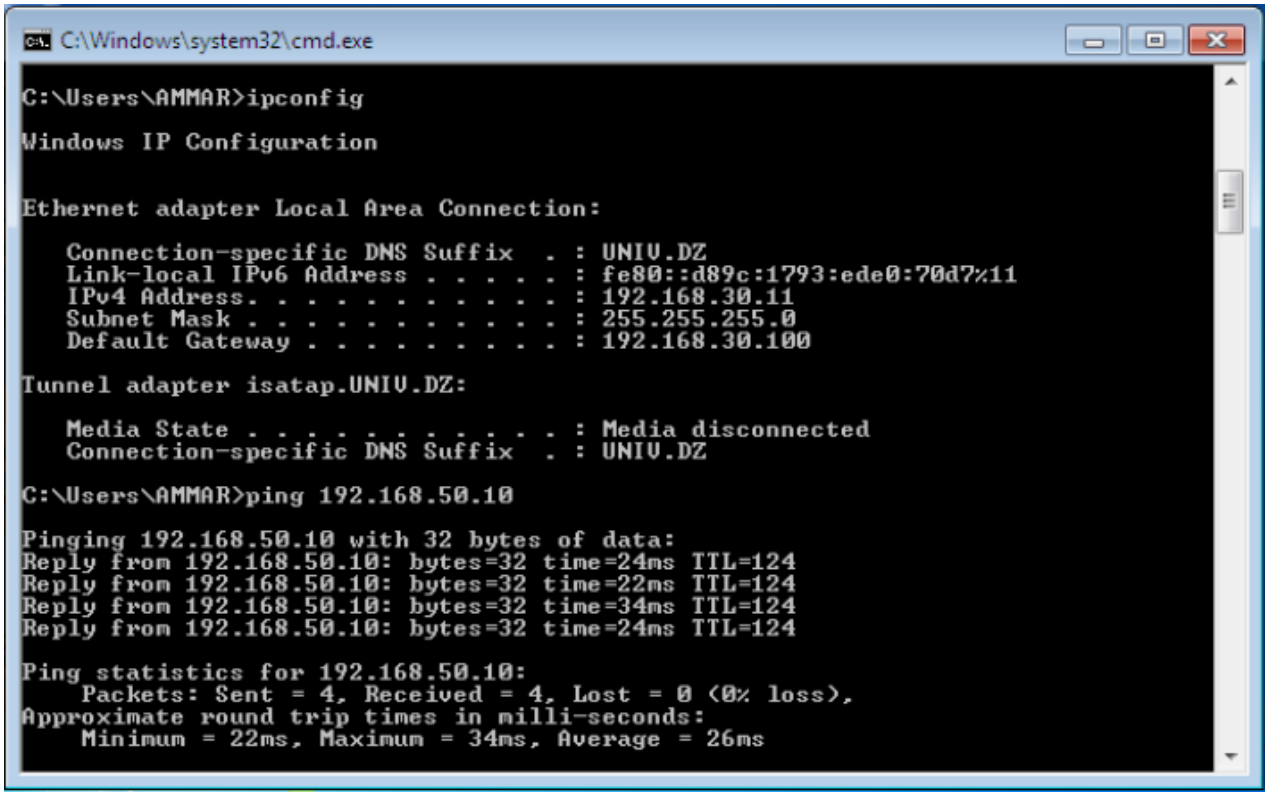


Figure III-42 Pinging the BR-PC From the HQ-PC

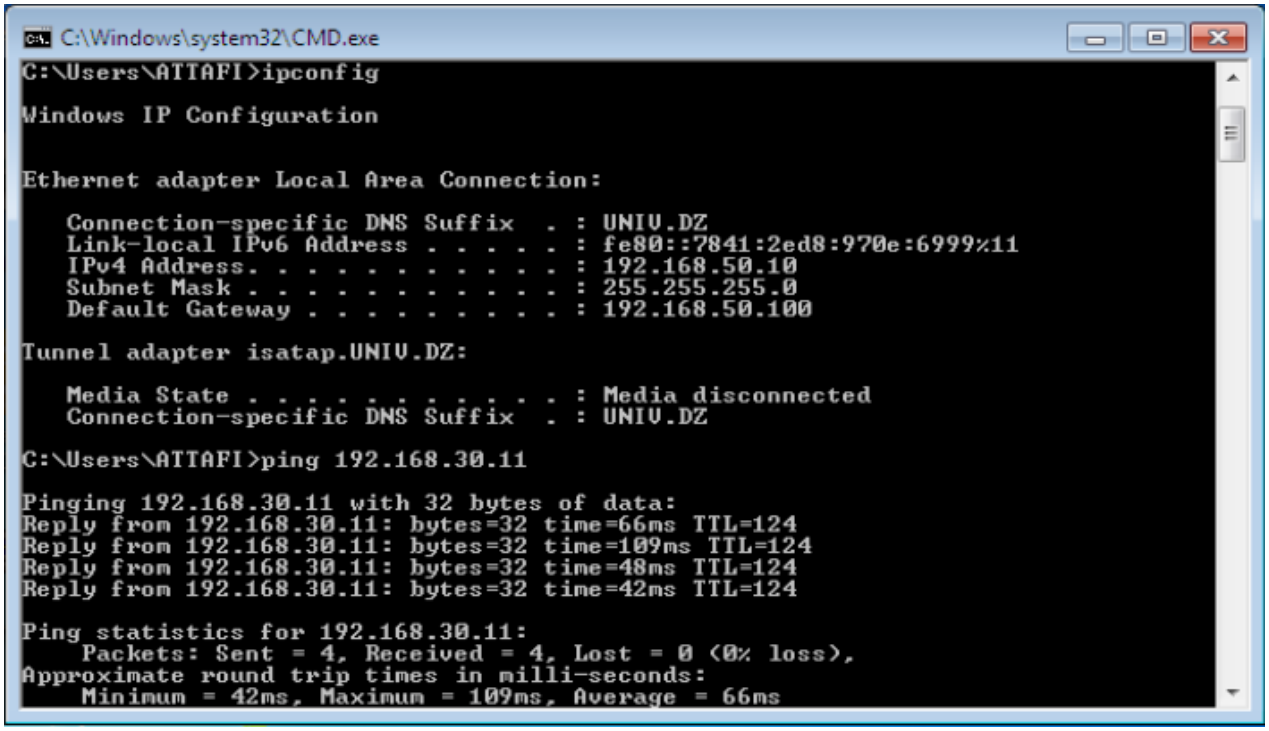


Figure III-43 Pinging the HQ-PC From the BR-PC

We remark that the ping between the two PC'S was successful with zero packet loss

III.6.9.2 Validating Internet Connectivity

On any PC of our network, we open CMD and ping 8.8.8.8 (Google's DNS) to verify internet connectivity

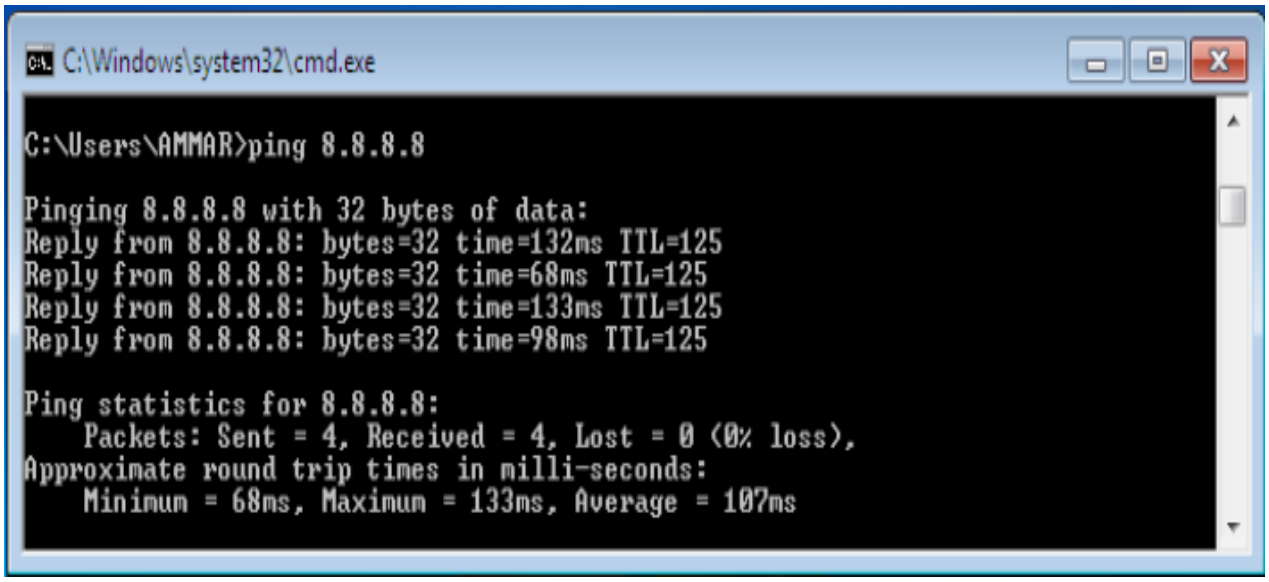


Figure III-44 Internet Connectivity in HQ PC -CMD

We will access any search engine on the server and use it to search for anything to verify internet connectivity

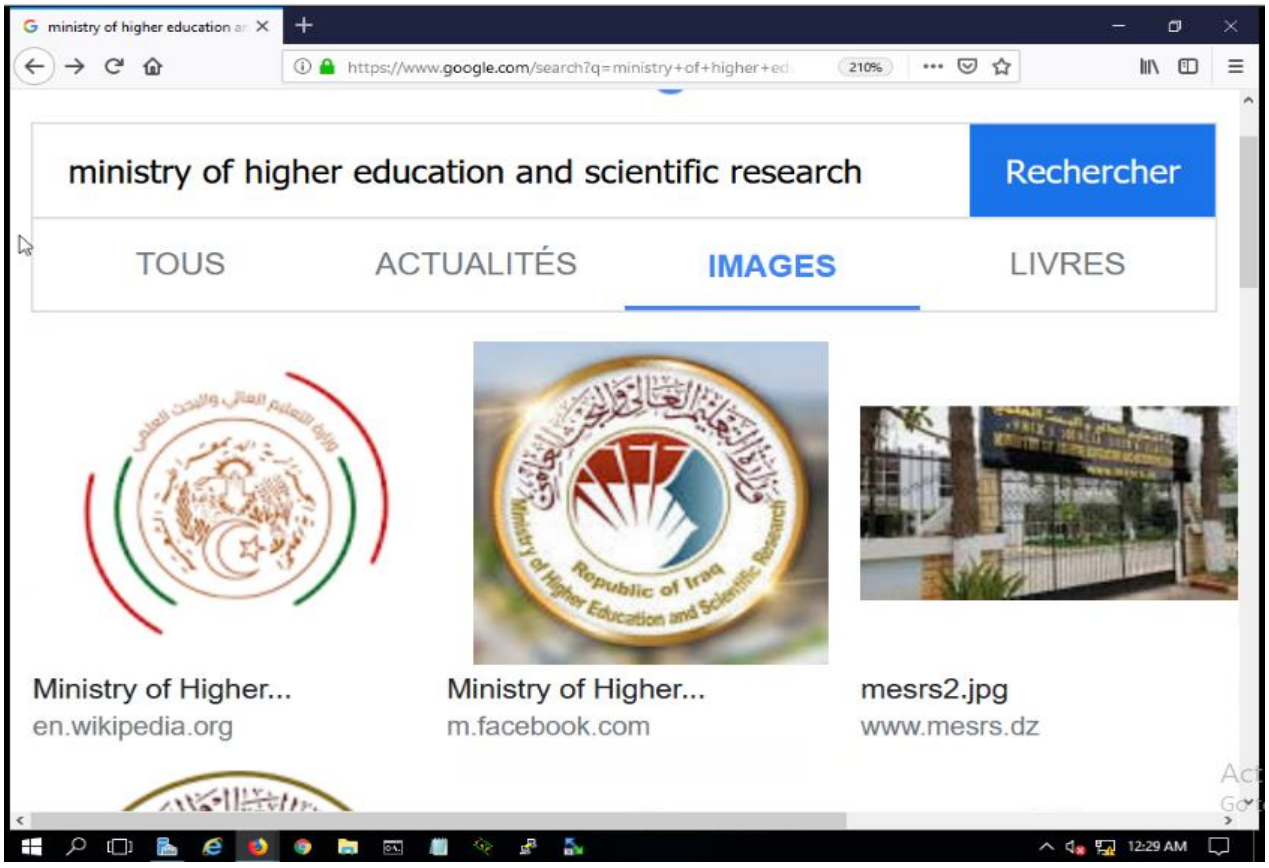


Figure III-45 Internet Connectivity in Server

III.7 Vulnerability Part Testing and Solutions

We test our security policies by emulating cyber-attacks using tools such as Kali Linux. Four key scenarios demonstrate how these protections safeguard network infrastructure.

III.7.1 Tools Used

We use Kali Linux ® (VERSION=”2019.2”) as our primary attack software platform, along with supporting tools such as Yersinia (for Layer 2 attacks, including DHCP spoofing) and Wireshark (for network traffic analysis and vulnerability detection).

III.7.2 General Scenario

In each test we say that the attacker must have a switch access. We assume that the attacker has an access to the interface e1\1 in AC-SW1

```
AC-SW1(config)#interface e1/1
AC-SW1(config-if)#no shutdown
AC-SW1(config-if)#switchport mode access
AC-SW1(config-if)#switchport access vlan 30
```

Command list-31 Network Commands for Attacker Accessing

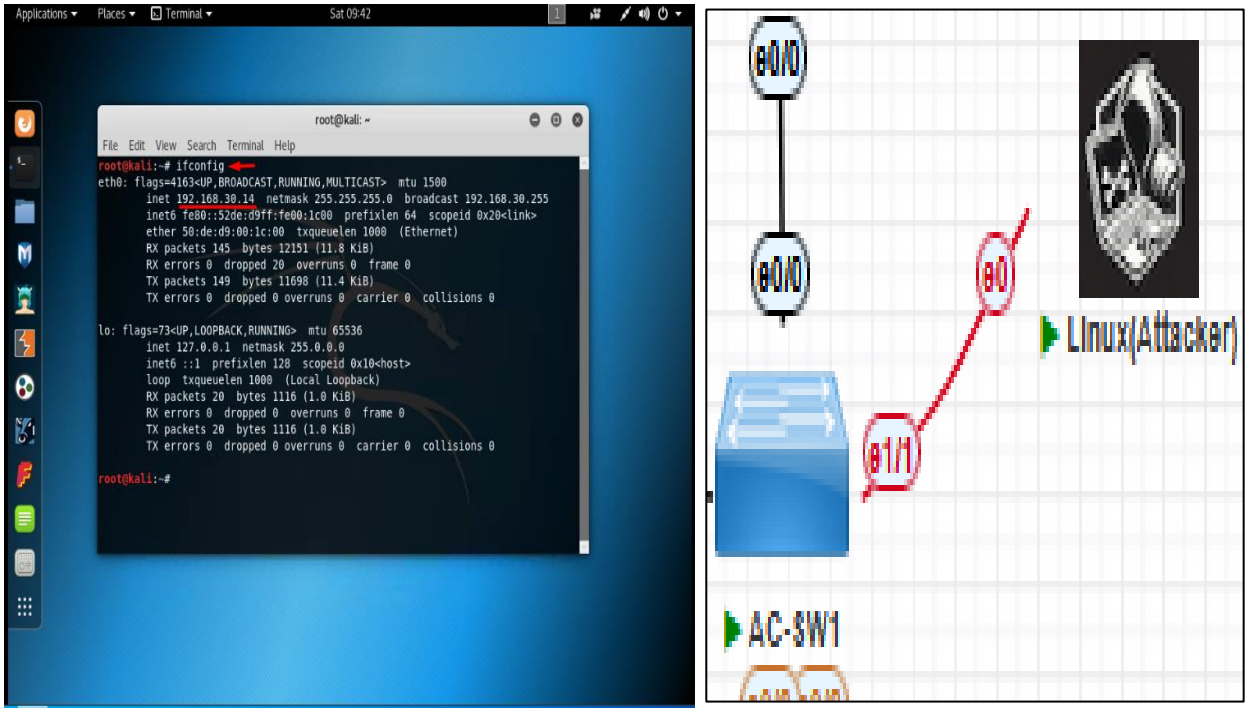


Figure III-46 Attacker’s Network Configuration Overview

III.7.3 Attacks Scenarios

In this scenario we proposed 3 Scenarios to emulate 3 types of attacks, then we compare the status of our network based on two conditions:

Firstly, before security policies implementation and after, the first is:

Secondly, after security policies implementation

III.7.3.1 DHCP Starvation Attack

This attack floods a DHCP server with fake IP requests to exhaust all available addresses and disrupt service for legitimate users.

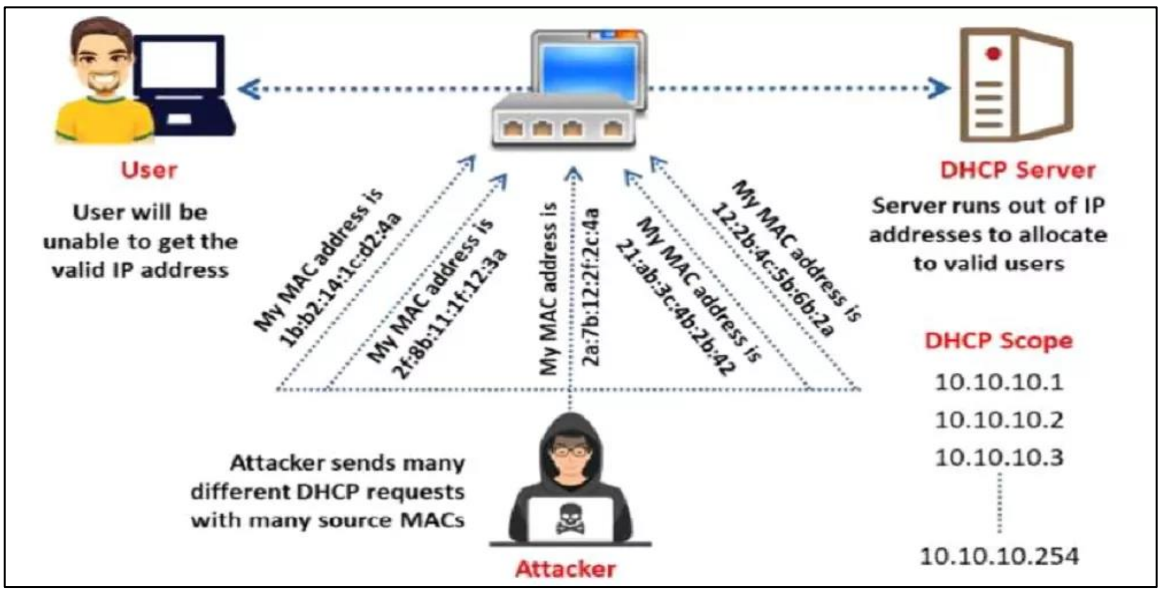


Figure III-47 DHCP Starvation Attack (Active DoS Attack) [43]

a) Before Security Policies

To access the Yersinia tool, we use the Terminal command: **root@kali: ~# yersinia -G**

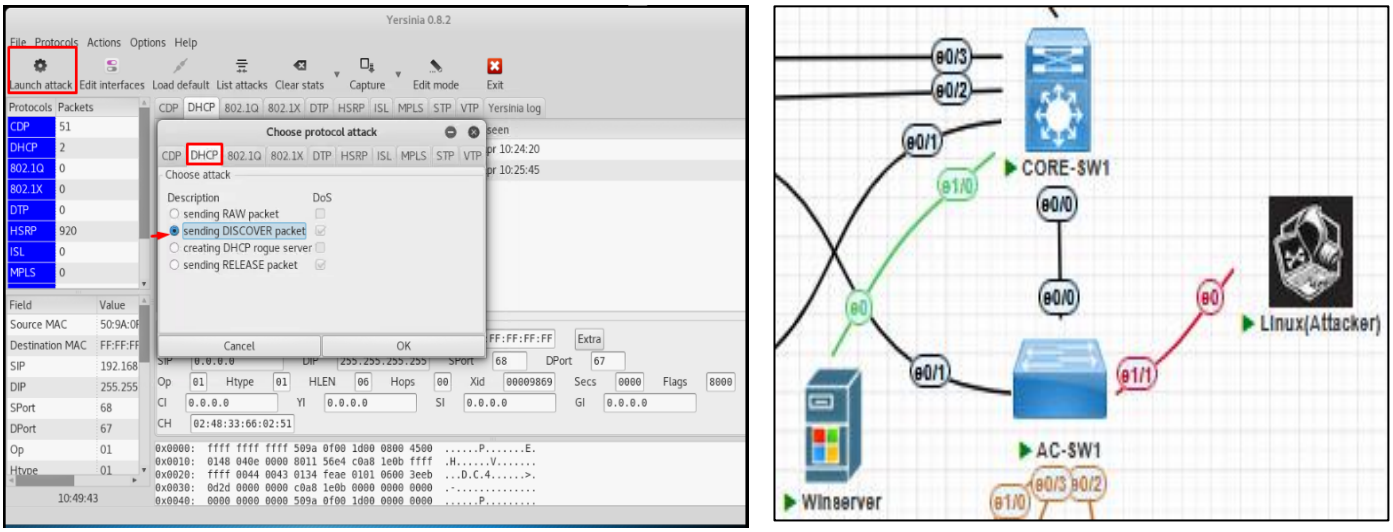


Figure III-48 DHCP Starvation Attack-DoS (Sending discover packet)

In the figure III-49 and III-50, after launching the attack, the attacker sends many DHCP discover packets to flood the server and we see that the ST scope detect the server flooding by the appearance of the blue exclamation marc in the scope

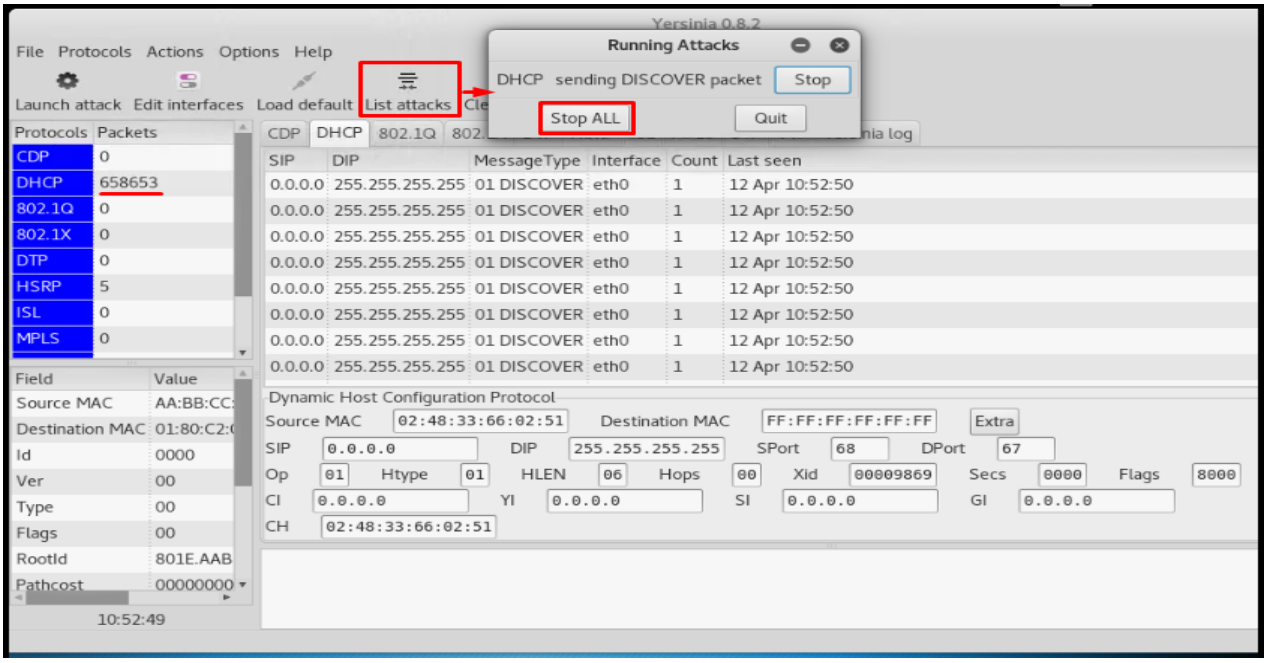


Figure III-49 Sending many DHCP Discover Packets to Flood the Server

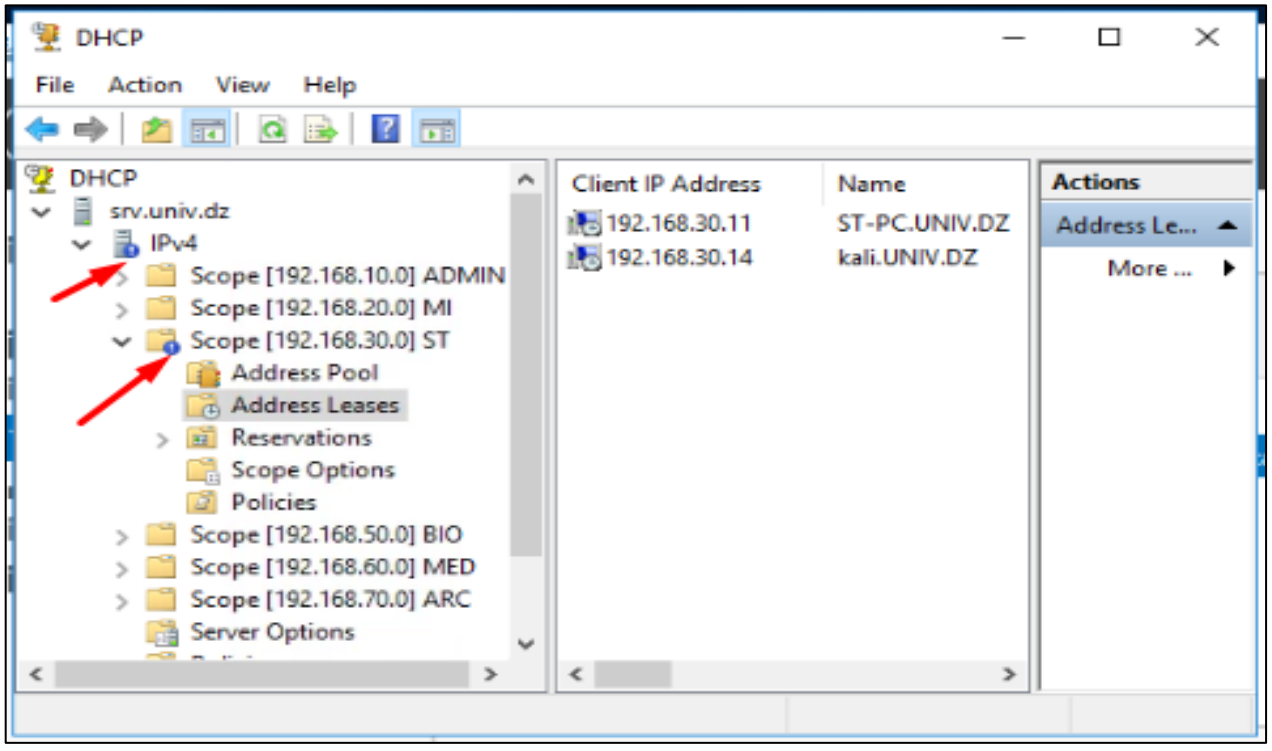


Figure III-50 Within Win Server Detecting a Server Flooding in Vlan 30 (ST)

Results:

As a result of this attack all DHCP IP addresses get exhausted, legitimate users cannot obtain their IP addresses and partial or complete network service is disabled.

b) After applying Security measures in AC-SW1 as mentioned in command List-20 we can show how this vulnerability is blocked

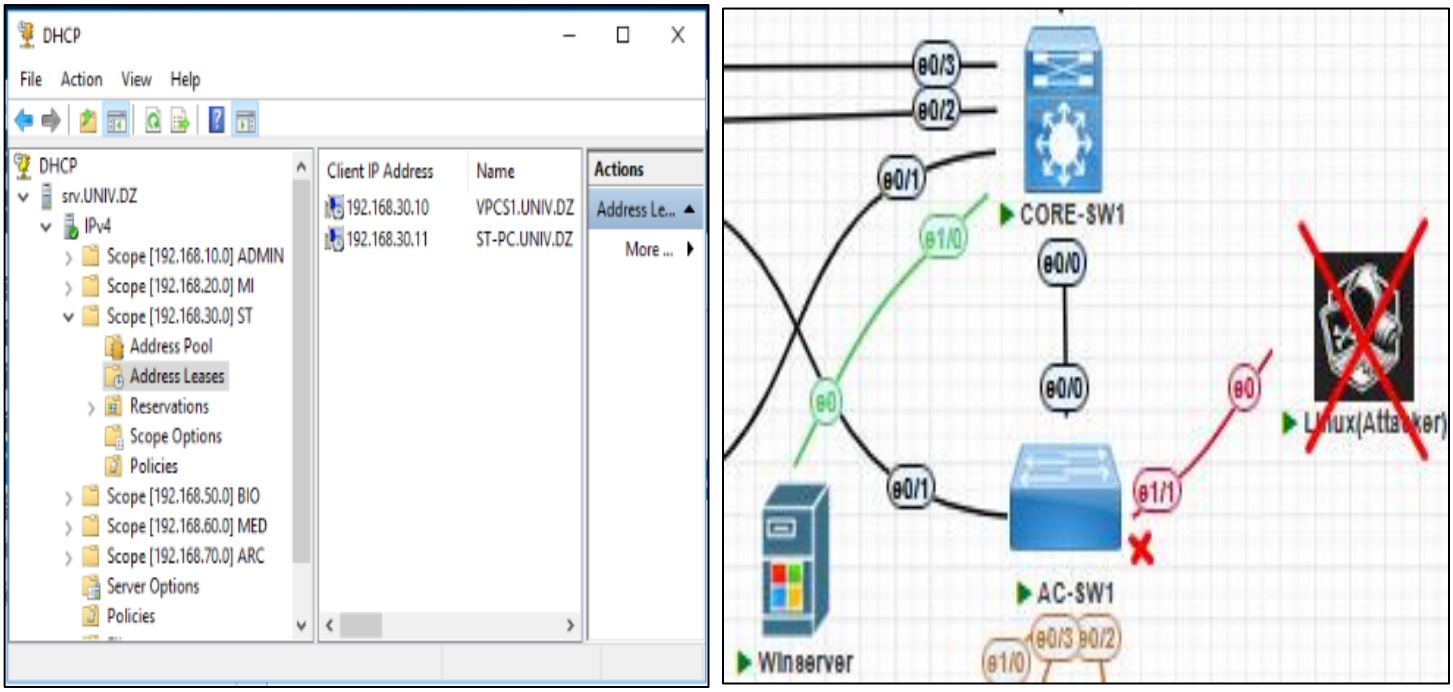


Figure III-51 Server Recovery to Normal State

Results:

After applying Security measures fake requests are blocked, only legitimate users can receive service, this security measures offered an effective protection against starvation attacks.

III.7.3.2 DHCP Spoofing Attack

Is an attempt to impersonate the DHCP server to provide malicious IP configurations to network clients.as the same condition to the first attack but in this attack the attacker try to play the role of rogue server

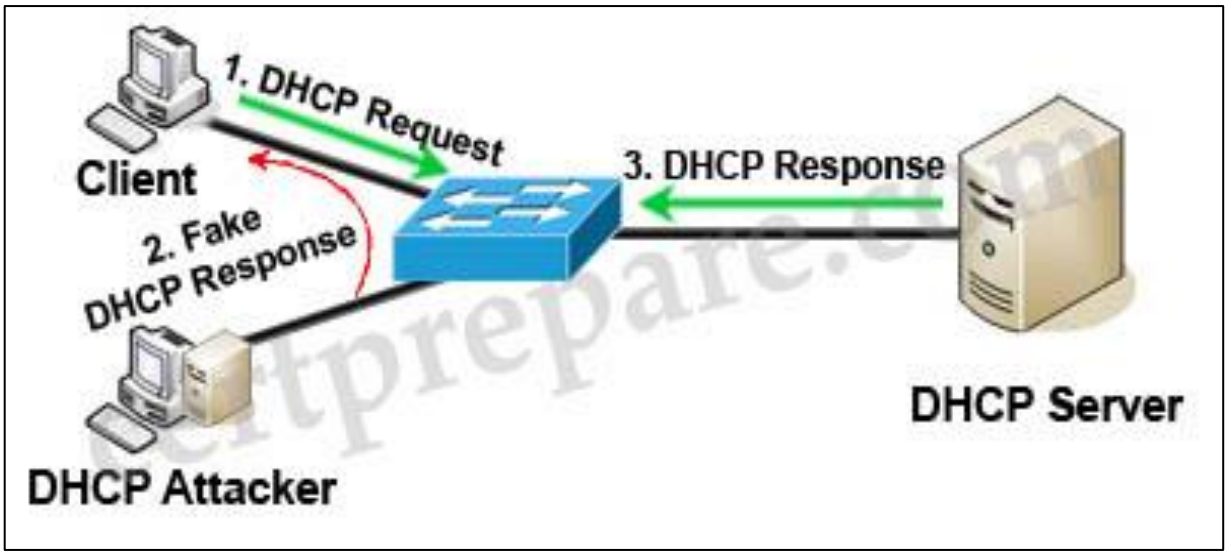


Figure III-52 DHCP Spoofing Attack [44]

a) Before Security Policies

When we launch the attack as shown in Figure III-53 and III-54, the attacker tries to create a

DHCP rogue server to monitor the distribution of the DHCP IP addressees

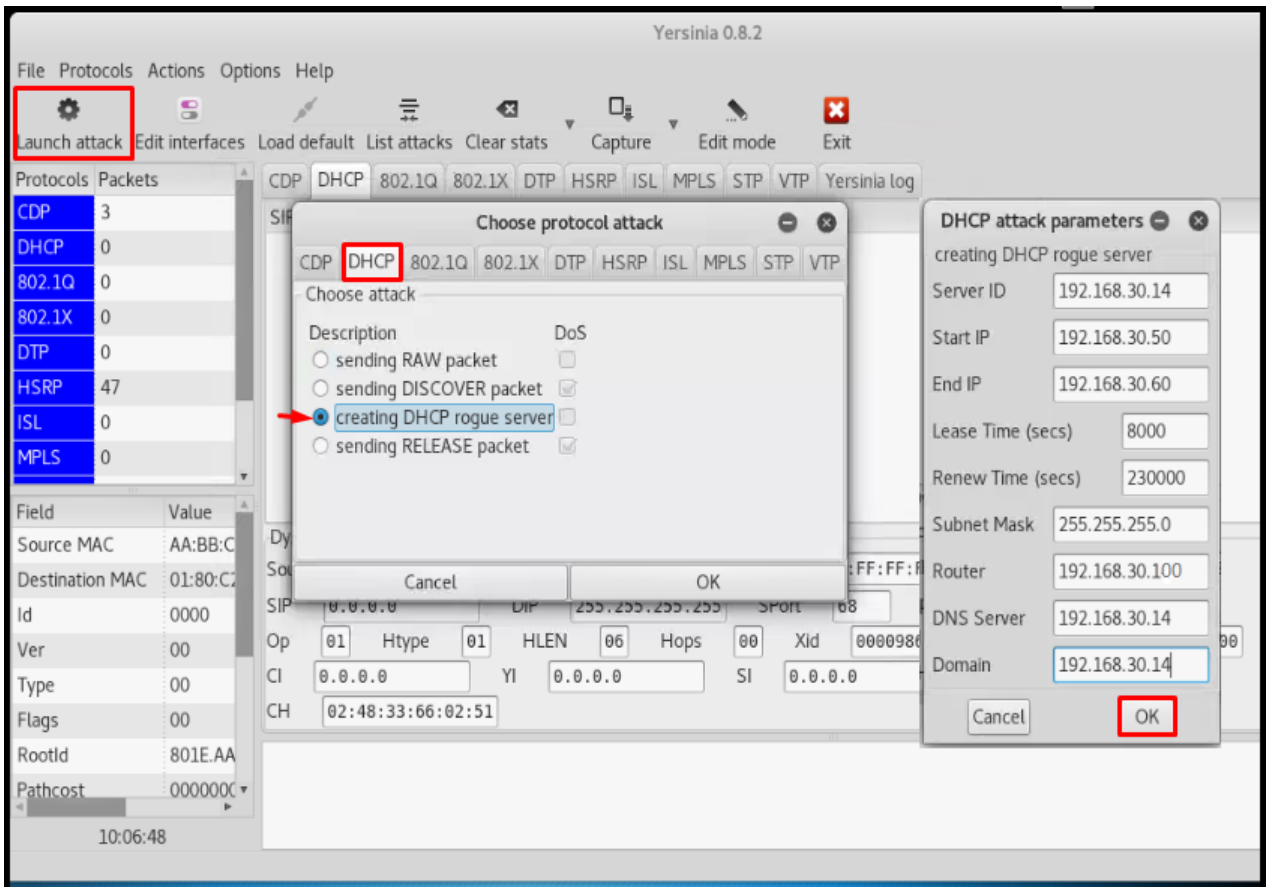


Figure III-53 DHCP Spoofing Attack (Active MITM Attack)

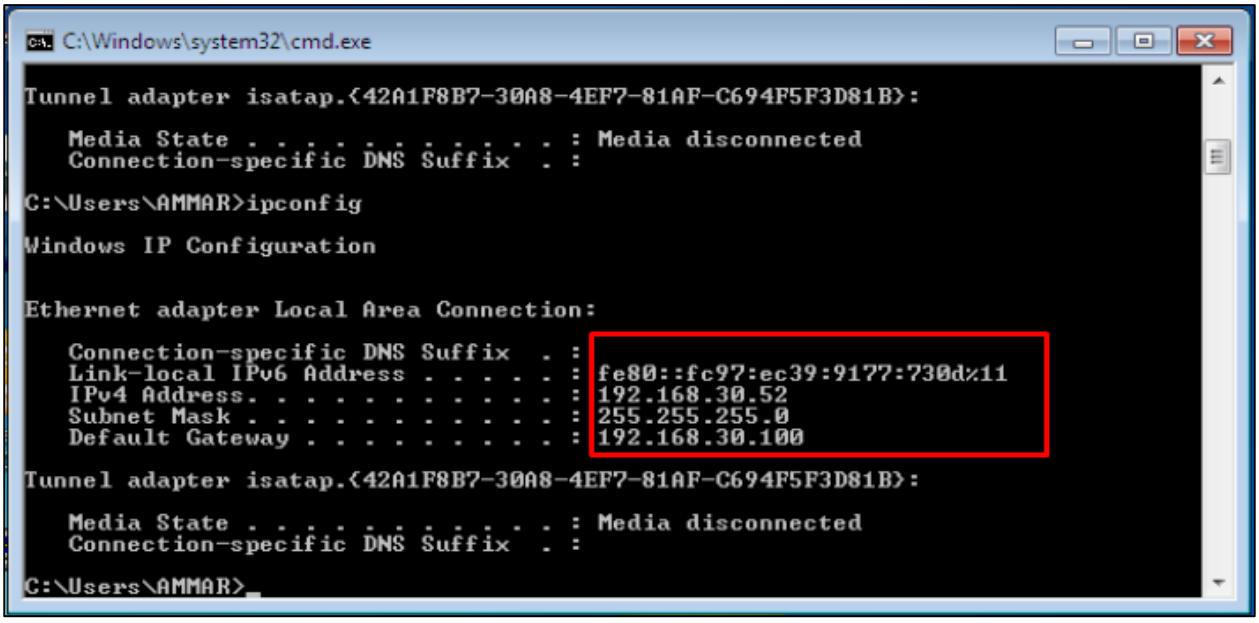


Figure III-54 Ip Taking from the Hacker

Result:

As a result of this weakness in the network, it was disrupted that can drive it to malicious sites

b) After applying Security measures in AC-SW1 as mentioned in command List-20 our campus network returns to work normally

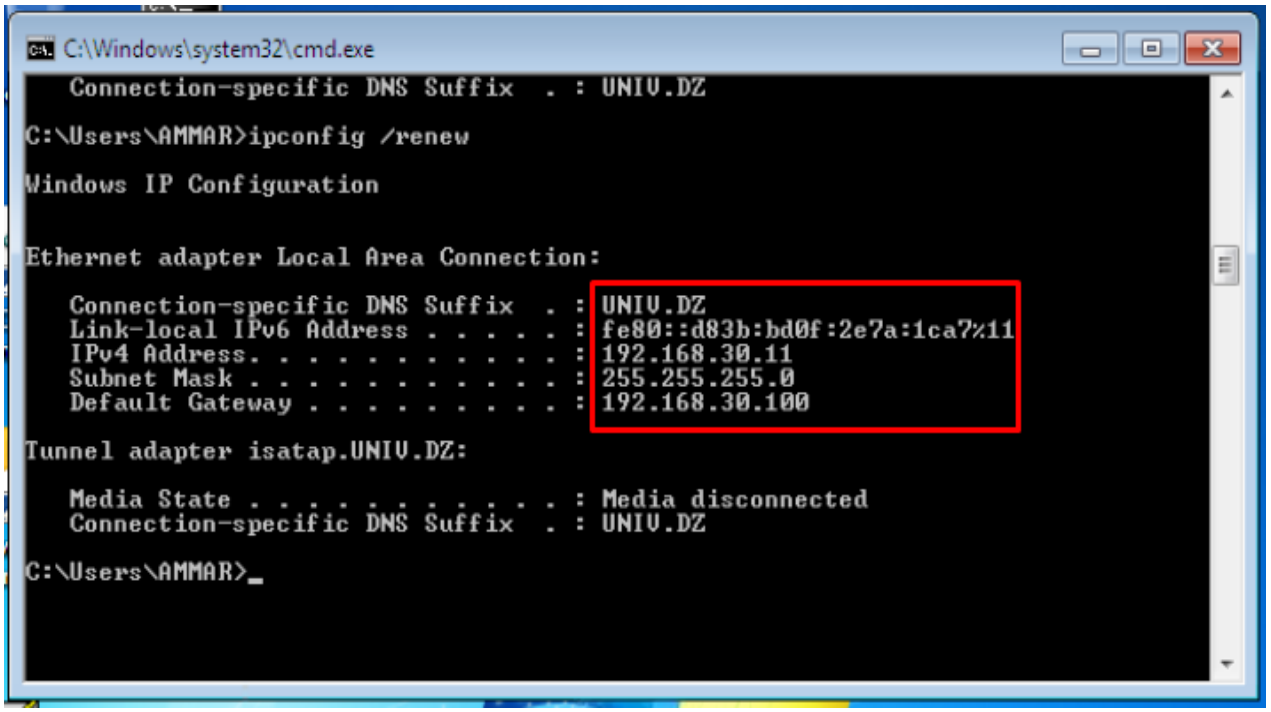


Figure III-55 Return the Same Ip from the Server to PC

Result:

The security measures applied drive our network to an effective protection against DHCP spoofing and MITM attacks.

III.7.3.3 Packet Sniffing Attack

An attempt to intercept and analyze network traffic to capture sensitive data, such as usernames, passwords, and other confidential information.

In this attack we are going to use another powerful Kali Linux tool which is **Wireshark**

Figure III-56 Packet Sniffing Attack [45]

a) Before Security Policies

after accessing the Wireshark tool using this command in the terminal: **root@kali: ~# Wireshark,** we remark that the attacker can capture all sensitive network data determined in Figure III-57 and III-58.

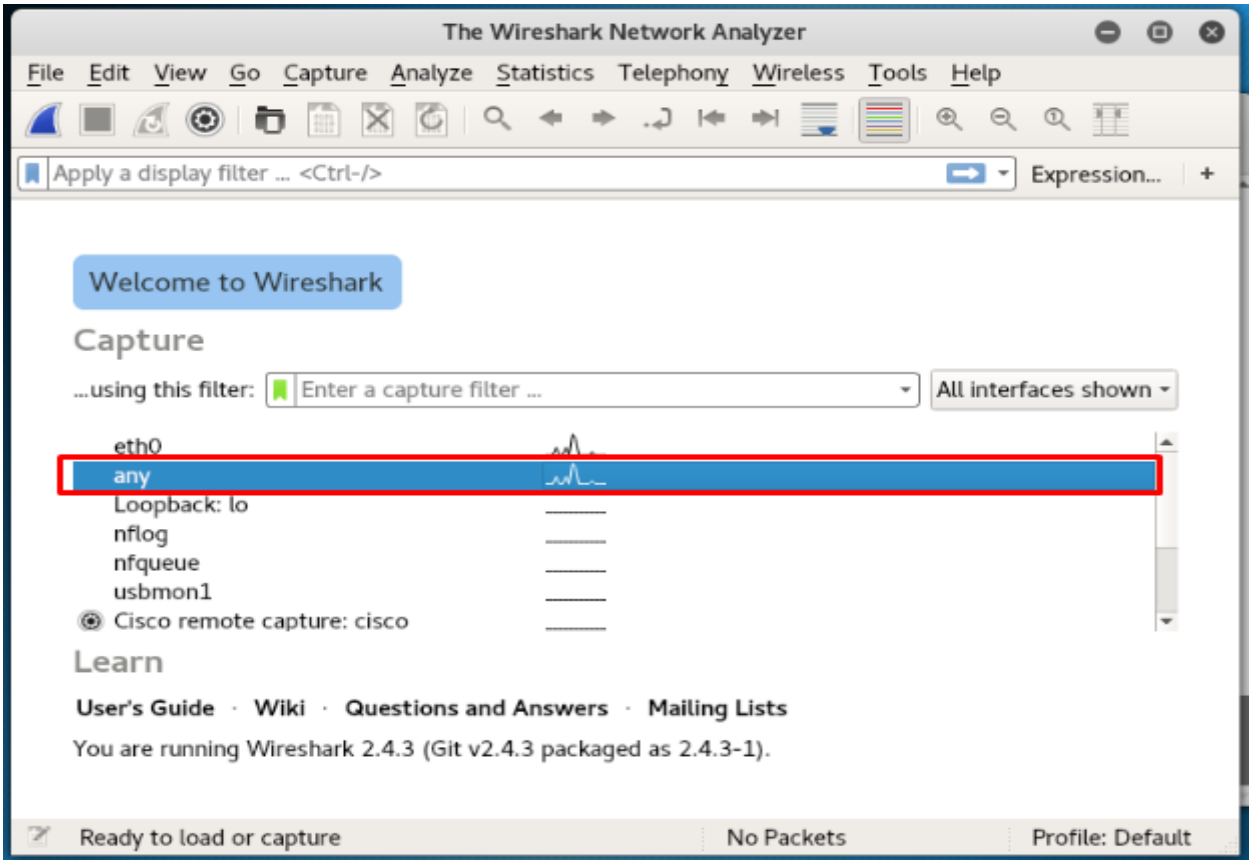


Figure III-57 Packet Sniffing Attack (Passive Attack)

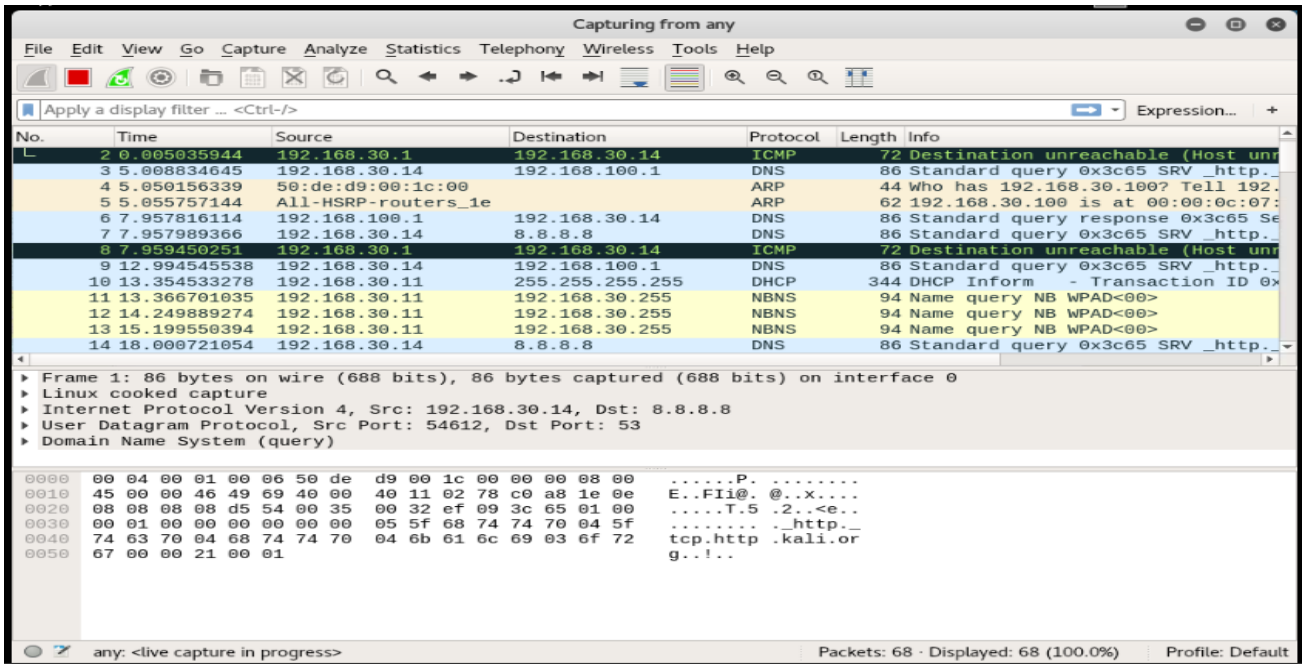


Figure III-58 Network Traffic Monitoring

Result:

In this attack captured sensitive data such as credentials and private communications and network IPs

b)After Security Policies

The attacker can't capture any traffic

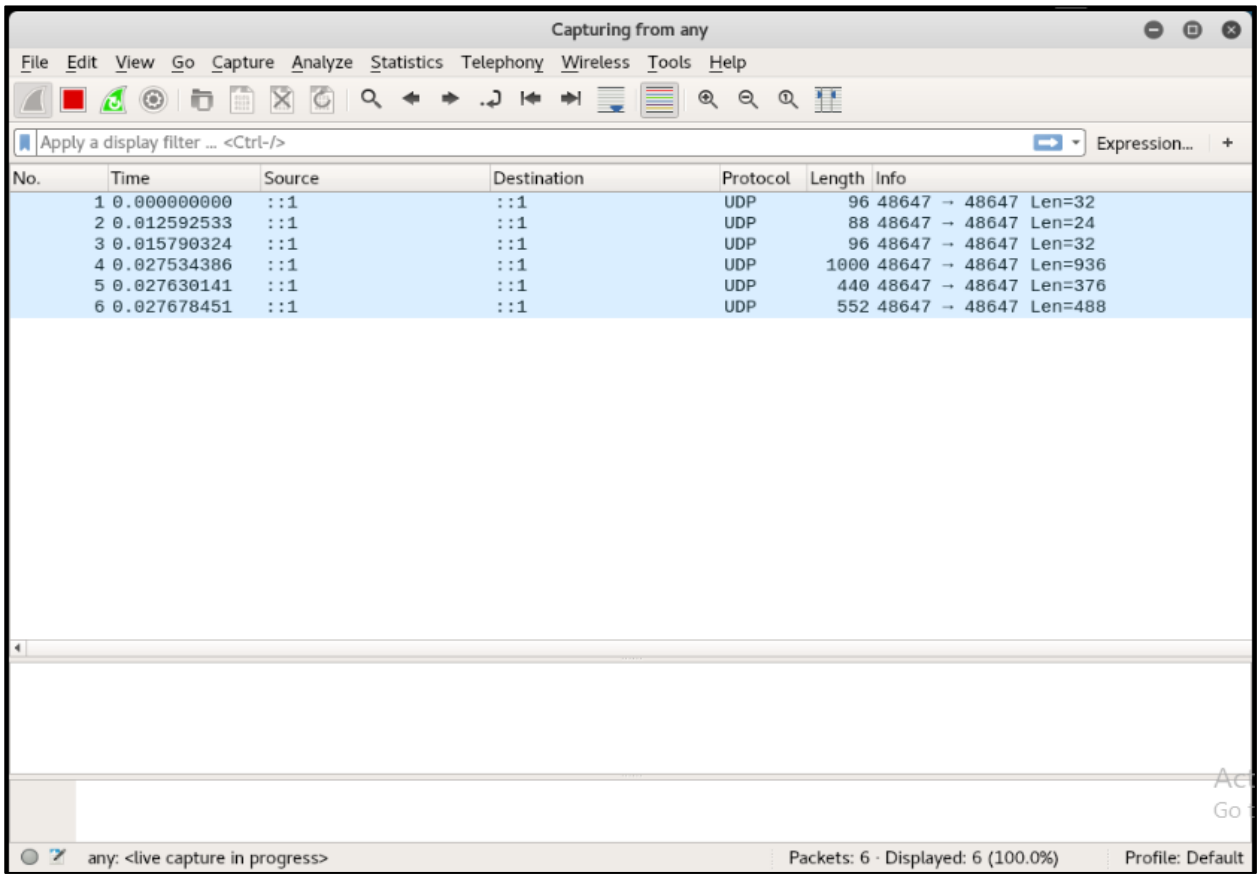


Figure III-59 No Packets were Captured

Results:

- Unauthorized traffic interception is blocked.
- Strong defense against packet sniffing attacks.

The same attack will be applied to the network from the service provider to capture packets with or without applying VPN IPsec

Without VPN IPsec tunnel:

If the attacker has compromised pc (Kali Linux®), within the service provider network he can capture all packets sended from the head quarter to the branch as mentioned in figure III.61 and configure its network access, and execute the attack.

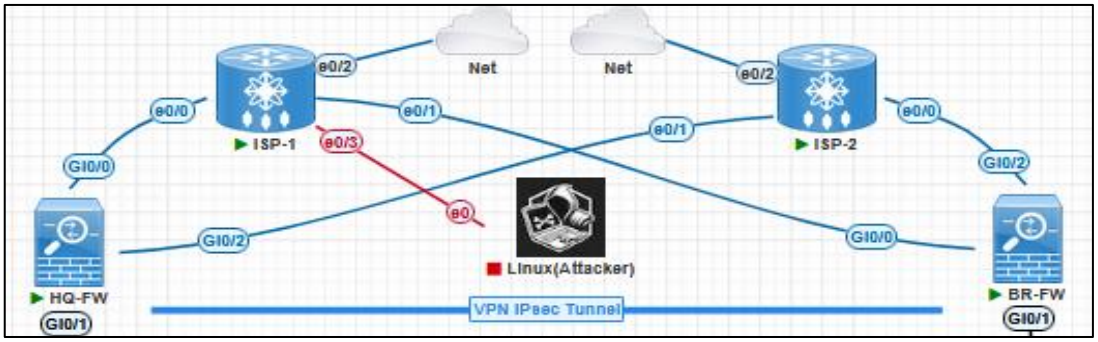


Figure III-60 Hacker's Position for Launching an Attack on VPN IPsec

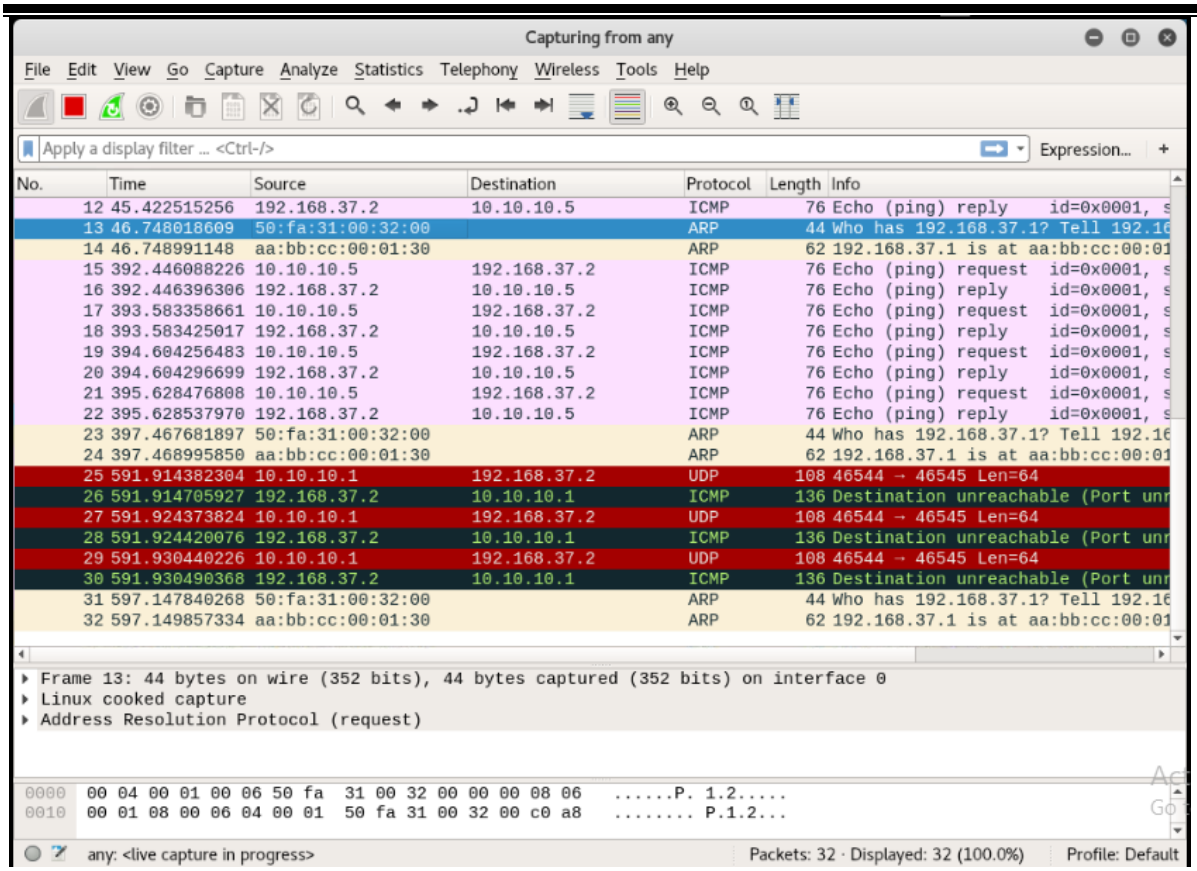


Figure III-61 Intercepting Unencrypted Packets

With VPN IPsec: we can show the captured packet in the attacker pc is all encrypted as shown in figure III-62

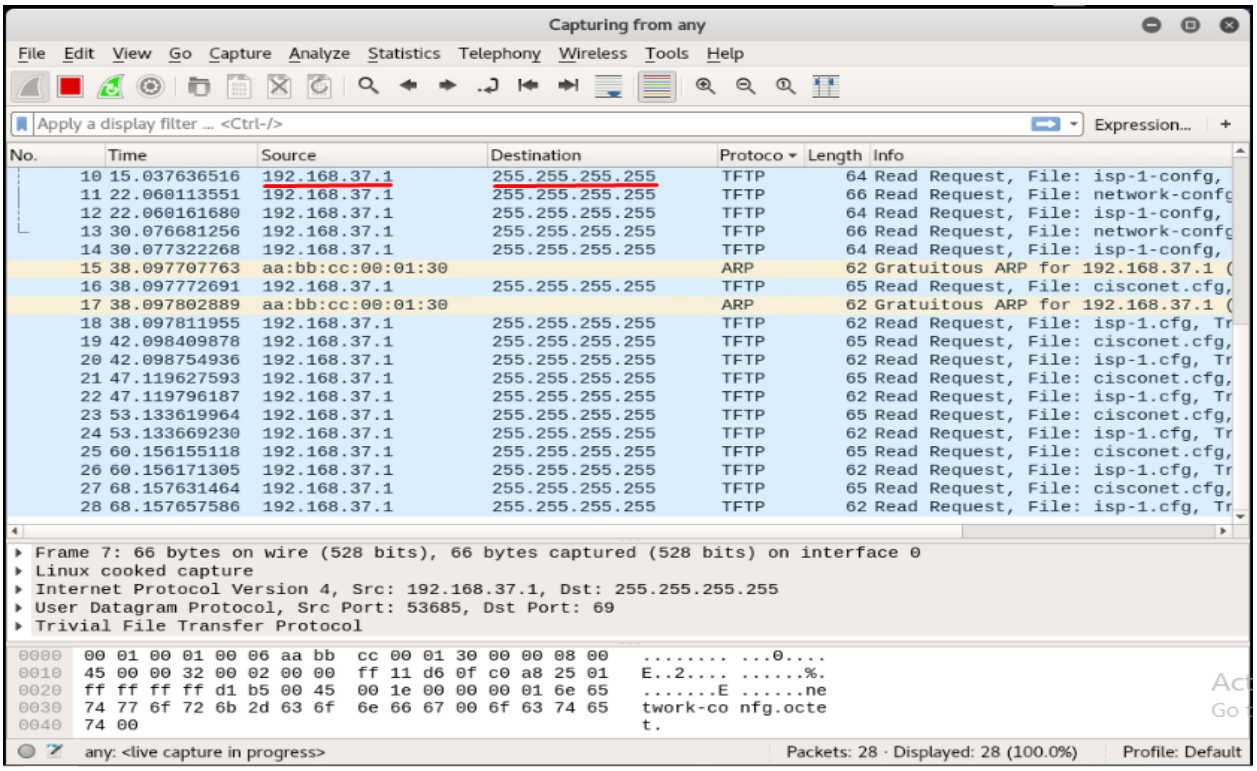


Figure III-62 Intercepting Encrypted Packets

III.8 Conclusion

This chapter walks through our step-by-step approach in constructing a high-performance campus network. We started by analyzing the organization's needs, selecting the right hardware, and designing an optimal network layout. To bring our design to life without physical hardware costs, we leveraged the PNETlab emulator—this virtual environment allowed us to experiment freely and refine our setup before real-world deployment.

To guarantee uninterrupted connectivity, we integrated HSRP and SVI redundancy protocols, ensuring automatic failover if any critical link went down. Security was a top priority, so we deployed Cisco ASA firewalls with advanced threat prevention to shield sensitive data from breaches.

At the heart of the network, a Windows Server 2016 system handled multiple roles: Active Directory authentication, DHCP management, and Domain Control. It also facilitated secure communication between the headquarters and a remote branch via an IPsec VPN tunnel, encrypting all cross-site traffic.

We didn’t just set up defenses we actively tested them. By simulating real-world attacks (e.g., packet sniffing, dhcp starvation), we identified vulnerabilities and fine-tuned security measures to block actual threats.

GENERAL CONCLUSION

This comprehensive project has demonstrated the critical interplay between theoretical networking principles and practical implementation in building a modern, secure campus network. By examining the historical evolution of campus networks move from centralized mainframes to software-defined, cloud-integrated architectures that exist today we established a firm foundation on how technology breakthroughs necessitate scalability, performance, and flexibility. The transition away from flat, exposed environments to hierarchical, partitioned ones served as the call for robust security models to offset the surging cyber threats.

The examination of network management, attacks, and security in Chapter II emphasized the significance of a multi-layered defense approach. Instruments such as Active Directory and IPsec VPNs developed as foundations for centralized management and secure communication, whereas Layer 2 protocols and firewalls demonstrated their necessity for reducing threats such as spoofing and DDoS assaults. The practical execution of the project in Chapter III confirmed these ideas, illustrating how VLAN segmentation, HSRP redundancy, and DHCP snooping can balance performance with security

Successful emulation of the network using PNETLab not only reduced expenses but also provided a risk-free environment to trial for resilience in real attack scenarios such as MITM and packet sniffing. The repeated cycle of processes showed the necessity for proactive security features, real-time monitoring, and adaptive design in securing sensitive data.

Ultimately, the project serves as a template for both educational establishments and companies, observing that modern networks must prioritize automation, scalability, and AI-driven threat detection to stay one step ahead of cyber-attacks. By infusing the insights obtained from older architectures with the newest technology, companies can build future-proofed infrastructures that deliver operational efficiency without compromising security. Transitioning from planning to penetration testing reinforces once again that a well-designed network is not just a technical asset but a strategic innovation and business growth facilitator in the Information Age.

REFRENCES

[1] Ebrary.net. PAST AND PRESENT OF CAMPUS NETWORKS
https://ebrary.net/180921/computer_science/campus_networks
[2] S. D. R. S. Lalita Kumari, Security Problems in Campus Network and Its Solutions, India: National Informatics Centre.
[3] Huawei Enterprise. Campus Network Solutions for Higher Education
https://e.huawei.com/ae/industries/education/higher-education/campus-network-higher-education
[4] GeeksforGeeks. What is Centralized Computing?. (2023, January 19)
https://www.geeksforgeeks.org/what-is-centralized-computing/
[5] Enterprise Networking Planet. What Is a Flat Network? Definition, Benefits & How It Works. (2023, February 21)
https://www.enterprisenetworkingplanet.com/management/the-risks-and-rewards-of-flat-networks/
[6] Cisco Systems. Networking Fundamentals
https://www.cisco.com/c/dam/global/fi_fi/assets/docs/SMB_University_120307_Networking_Fundamentals.pdf
[7] Cisco Press. CCNA Routing and Switching > 31 Days Before Your CCNA Exam: Connecting Switches and Ethernet Technology (2009, April 15)
https://www.ciscopress.com/articles/article.asp?p=1276662&seqNum=7
[8] B. E. &. R.G.Rios.&. D. Hucaby, J. Gooley, CCNP and CCIE Enterprise Core ENCOR 350 401 Official Cert Guide., Cisco Press,2020
[9] M. M. R. &. R. A. Dye, Network fundamentals, CCNA exploration companion guide., Cisco press, 2007.
[10] J. M. D. &. S. H. Cioara, CCNA, Pearson Education, Inc, 2008.
[11] W. Odom, CCNA 200-301 Official Cert Guide, Volume 1, 2019.
[12] cisco press. Implementing EtherChannel in a Switched Network. (2015, June 04) https://www.ciscopress.com/articles/article.asp?p=2348266&seqNum=3
[13] Cisco Press. Implementing a WLAN > Wireless LANs. (2008, June 17)
https://www.ciscopress.com/articles/article.asp?p=1156068&seqNum=4
[14] Cisco Community. Dynamic Routing Protocols: OSPF, EIGRP, RIPV2, IS-IS, BGP. (2021, December 04).
https://community.cisco.com/t5/networking-knowledge-base/dynamic-routing protocols-ospf-eigrp-ripv2- is- is-bgp/ta-p/4511577
[15] GeeksforGeeks. Hot Standby Router Protocol (HSRP). (2021, October 25) https://www.geeksforgeeks.org/hot-standby-router-protocol-hsrp/
[16] Website:9tut. Hot Standby Router Protocol HSRP Tutorial - CCNA Training. (n.d) https://www.9tut.com/hot-standby-router-protocol-hsrp-tutorial
[17] Proxmox PVE. Software-Defined Network.
https://pve.proxmox.com/pve-docs/chapter-pvesdn.html
[18] Hewlett Packard Enterprise. What is Cloud Scalability? | Scaling Computing | Glossary
https://www.hpe.com/emea_africa/en/what-is/cloud-scalability.html
[19] Huawei Technical Support. CloudCampus Solution V100R019C10 Deployment Guide for Large- and Medium-Sized Campus Networks (Non-virtualization Scenario). (2021, April 29)
https://support.huawei.com/enterprise/en/doc/EDOC1100141247
[20] cable applications. UTP Cat6 Flyleads Different Colours (n.d)
https://www.cables.co.za/products/utp-category-6-flyleads-different-colours?
[21] Ubuy Algeria. Achetez Borsuer 6 Pcs Cat6 Keystone Jack (n.d)
https://www.ubuy.dz/en/product/1AETH5JDC-borsuer-6-pcs-cat6-keystone-jack-cat6-rj45-90 coupler
[22] DCD Distribution Sdn Bhd . Keystone Jacks & Face Plates - Optic Digital Cable (n.d)
https://dcd.com.my/Optic-Digital/Keystone-Jacks-&-Face-Plates/105
[23] Ayoub Computers. 3m Cat6 Patch Cord Network Cable.
https://ayoubcomputers.com/3m-cat6-patch-cord-network-cable/

[24] Legrand Negiria . Patch cord fibre optic OS2 single-mode LC/LC Uniboot duplex reversible polarity 10m.
https://www.legrand.ng/fr/catalogue/patch-cord-fibre-optic-os2-single-mode-lclc uniboot-duplex-reversible-polarity-10m-032692
[25] CDW. Patch Panels.
https://www.cdw.com/category/cables/ethernet-cables/patch panels/?w=BD6
[26] Fibconet. What is a Server Rack? - Fibconet Communicate.
https://fibconet.com/pap/what is-a-server-rack/
[27] Router-Switch.com. isr4331-k9-datasheet.pdf.
[28] buyrouterswitch.com. Ws-C2960X-24Ps-L Prix Et Fiche Technique Pdf.
https://buyrouterswitch.com/fr/ws-c2960x-24ps-l-p-5265-price.html
[29] Cisco Systems. Cisco Adaptive Security Appliance (ASA) Software.
https://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa software/index.html
[30] Dell Technologies Info Hub. Form Factor Fun with Dell EMC vSAN Ready Nodes.
https://infohub.delltechnologies.com/fr-fr/p/form-factor-fun-with-dell-emc-vsan-ready-nodes/
[31] FS.com. Complete Guide to Understanding Network Server. (2024, mars 27).
https://www.fs.com/blog/complete-guide-to-understanding-network-server-6971.html
[32] M. J. Palmer, Hands-on Microsoft Windows Server 2016, Cengage Learning
[33] IETF | Internet Engineering Task Force. RFC 2828 Internet Security Glossary.
https://www.ietf.org/rfc/rfc2828.txt
[34] GeeksforGeeks. Active and Passive attacks in Information Security.
https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/
[35] GeeksforGeeks. Difference between Active Attack and Passive Attack. (2024,05 September)
https://www.geeksforgeeks.org/difference-between-active-attack-and-passive-attack/
[36] O. Santos, Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide., Cisco Press., 2021.
[37] tferdinand.net. non-le-cadenas-pres-de-votre-barre-dadresse-ne-veut-pas-dire-quun-site-est-fiable.
https://tferdinand.net/non-le-cadenas-pres-de-votre-barre-dadresse-ne-veut-pas-dire-quun-site-est-fiable/
[38] K. Barker &S. Morris, CCNA Security 640-554 Official Cert Guide., Pearson Education, Inc.,2013.
[39] Blogger.com. CCNA Security Chapter 1 - Modern Security Threats. (2012, 15 July)
https://sclabs.blogspot.com/2012/07/ccna-security-notes-chapter-1-modern.html
[40] GeeksforGeeks. What is IP Security (IPSec).(2025,03 February)
https://www.geeksforgeeks.org/ip-security-ipsec/
[41] R. White, Cisco Certified Support Technician CCST Networking 100-150 Official Cert Guide., Pearson Education, Inc.,2024
[42] Fortinet . What Is a Firewall? Definition and Types ... (n.d).
https://www.fortinet.com/resources/cyberglossary/firewall
[43] robodin.com. تكتيك الهجوم وطرق الحماية والدفاع – DHCP الهجمات على.
https://robodin.com/dhcp-attack/
[44] Certprepare. ENSDWI Training » DHCP Snooping. (2019,16 November)
https://www.certprepare.com/dhcp-snooping
[45] Studio Estrategia. Segurança da Informação - Conheça as 5 Dicas de Ouro.
https://studioestrategia.com.br/seguranca-da-informacao-dicas/