CCT COLLEGE DUBLIN

PROGRAMME TITLE: HIGHER DIPLOMA IN SCIENCE IN COMPUTING

ASSIGNMENT TITLE:

GUIDED TECHNOLOGY PROJECT

AUTHOR : GONZALO MAURICIO VASQUEZ JALDIN

STUDENT ID : 2022500

Dublin – Ireland 2023

Table of contents

Contents

1.- ABSTRACT 8

1.2.- ACKNOLEDGMENTS 9

2.-INTRODUCTION 9

3.- BACKGROUND 10

3.1.- Requirements 10

3.2.-Objectives 11

3.2.1.- General Objectives 11

3.2.2.- Specific objectives 11

4.- Hierarchical Network Design 12

4.1.1.- Core Layer 13

4.1.2.- Distribution Layer 13

4.1.3 Access Layer 13

4.1.4 Collapse core 13

4.1.5.- VPN 15

4.1.6 Site to Site VPN 15

4.1.7 IPSEC 16

4.1.8.- L2TP 16

4.1.9.- STP 17

4.2.0.- SSH 19

4.3.- Routing 19

4.3.1.- Dynamic routing 19

4.3.2.- LACP 19

4.3.3.- Etherchannel (Bonding) 20

4.4.- Standard ANSI/TIA/EIA 606A 21

4.5.- Standard ANSI/TIA/EIA 607 21

4.6.- Fiber optic single-mode and multi-mode 22

4.7.- Fiber optic multi-mode 24

5.- Chapter ll . Project engineering 25

5.1.- Design methodology 25

5.2.- Network specifications 26

5.2.1.- EVE-NG 26

5.2.2.- Mikrotik RouterOS 27

4.3.- Logic design network topology 28

4.4.- IP address 29

4.5.- Subnetting table 29

4.6.- Equipment selection 30

4.7.- Implementation 30

4.7.1.- Security of information 30

4.8.- Address List 31

4.9.- DHCP 32

5.- Configure device security and encryption 33

6.- For security, hosts cannot change ports 34

7.- Price.. 34

8.- Conclusion and recommendations 35

8.1.- Recommendations 35

9.-Network Device configurations... 36

9.1.- Core Router 36

9.2.- Core Back-up 41

9.3.- Switch Core – 1... 45

9.4.- Switch core – 2 47

9.5.- Access Switches 1- 4 50

10.- References.. 52

Table of figures

Figure 1 Network Design 12

Figure 2 . 3 Layer Topology 14

Figure 3 . List of spanning tree protocols 18

Figure 4 . Single mode connection 23

Figure 5 . Multimode connection 24

Figure 6 . EVE-NG Simulator 26

Figure 7 . Mikrotik RouterOS 27

Figure 8 Logic design LAN 28

Figure 9 . Networking IP Address Class 29

Figure 10 . Subnetting table 29

Figure 11 . Networking Products 30

Figure 12 . Windows Server 30

Figure 13 . Address-List 31

Figure 14 . Firewall Rule 31

Figure 15 . Firewall Drop packets 32

Figure 16 . DHCP Server Table 32

Figure 17 . SSH 33

Figure 18 . ARP 34

Figure 19 . Price 34

1.- ABSTRACT

Haleon (PLC) are an expanding sales and research medical company, Haleon was established on 18 July 2022 as a corporate spin-off from GSK .

Due to its recent expansion, Haleon are moving to a new greenfield site in Waterford Co. Dungarvan. In addition to this, the business is going to establish a data collaborative partnership with another pharmaceutical company also based in Dublin.

The company currently has approx. 1000 employees located in its main office divided into three distinct divisions: research and development (R&D) – (300 employees), manufacturing (550) and Sales/Marketing(150). The R&D division, while located in the same premises, must be securely segregated from the other divisions. All divisions will require an external Internet connection. DPL R&D division require an intranet site accessible only to that division and the partner company.

1.2.- ACKNOLEDGMENTS

First of all, I would like to express my thanks to CCT College which gives me the opportunity to improve mi IT skills. Lectures have been supportive during the programme .Also, I would like to express my sincere gratitude to all those who have supported and guided me through this journey. I am so grateful for the unwavering love and encouragement my family gives me. Their constant belief in me has been a driving force to get things done. I would also like to express my sincere appreciation to my mentors and teachers for their valuable guidance and wisdom that shaped my intellectual development. In addition, I would like to thank my friends and colleagues for their friendship, inspiration and collaborative efforts. Finally, I acknowledge the many scholars and individuals whose work and research have paved my own path. My own efforts would not have been possible without their contributions. Thank you all for your unwavering support and belief in me.

2.-INTRODUCTION

The purpose of this project is to solve the needs of Haleon’s Company with the available technology, to generate a system that maximizes success. The network design is a discipline that grew from the success of structured software programming and structured systems analysis, concentrating on applications, sessions, and data transport prior to the selection of routers, switches, and media that work in the lower layers.

The following presents how various techniques and models can be used to characterize the existing system, new user requirements and a framework for the future system.

3.- BACKGROUND

The company Haleon requires engineers to design its new networking enterprise.

User distribution:

- Manufacturing: 550 users.
- Research and development : 330 users.
- Sales/Marketing: 150 users.

3.1.- Requirements

- You must have redundancy in the field.
- Secure inter-communications within internal divisions.
- Communication between partner sites.
- Segregated Wireless LAN solution for guest access.
- VOIP solution.
- Automated IPv4 address allocation.
- Logical network subdivisions.
- Access Control.
- Name resolution services.
- Secure local and remote management of networking devices.
- Device Security best practices.

3.2.-Objectives

3.2.1.- General Objectives

Design the Network for the pharmaceutical company including solutions for all the requirements raised by making a safe, available, redundant and scalable design.

3.2.2.- Specific objectives

- Analyze the needs of the company.
- Propose solutions to the company's requirements.
- Determine which applications will run and how those applications behave on a network.

4.- Hierarchical Network Design

Hierarchical network design involves dividing the network into independent layers. Each layer fulfills specific functions that define its role within the general network.

The separation of the different existing functions in a network makes the network design modular and this facilitates scalability and performance. The typical hierarchical design model is separated into three layers: access layer, distribution layer, and core layer. An example of a three-layer hierarchical network design is shown in the figure.

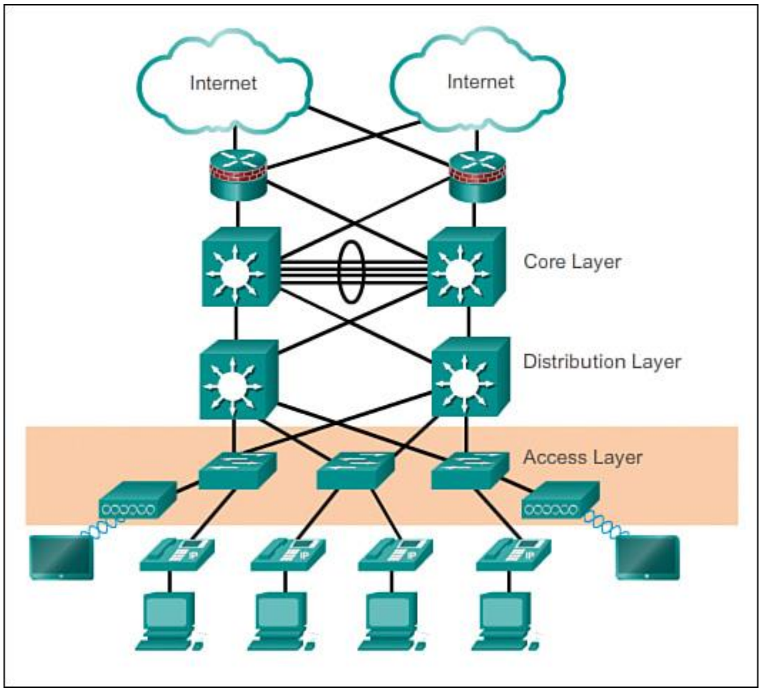


Figure 1 Network Design

4.1.1.- Core Layer

The core layer of the hierarchical design is the high-speed backbone of the network. The distribution layer devices are interconnected through the core. It must be highly available and redundant, since, in the event of a failure, the entire network will be affected.

4.1.2.- Distribution Layer

La capa de distribución controla el flujo de tráfico de la red, separándolo, filtrándolo y priorizándolo, para garantizar un servicio adecuado a cada subred. Se trata de switches fiables y redundantes para garantizar en la medida de lo posible que no se interrumpe el servicio.

4.1.3 Access Layer

The access layer services the end devices. Any device to which a PC, printer, telephone, etc., can be connected can be included. Therefore, access points, switches or routers can be found. The main purpose of the access layer is to provide a means of connecting devices to the network and to control which devices can communicate on the network.

4.1.4 Collapse core

As we know, in a derivative of the 3-layer model in which we have Core, distribution or aggregation and Access, in which the function of the kernel is to forward the packets as fast as possible. At the distribution layer we comply with the policies, security, filtering and quality of service, working as a backbone and access to which all end devices connect.

In the Collapsed Core model, we merge the Core and distribution layers into a single one, in which the “largest” equipment with more features and better throughput are placed, and it is directly connected to the access layer.

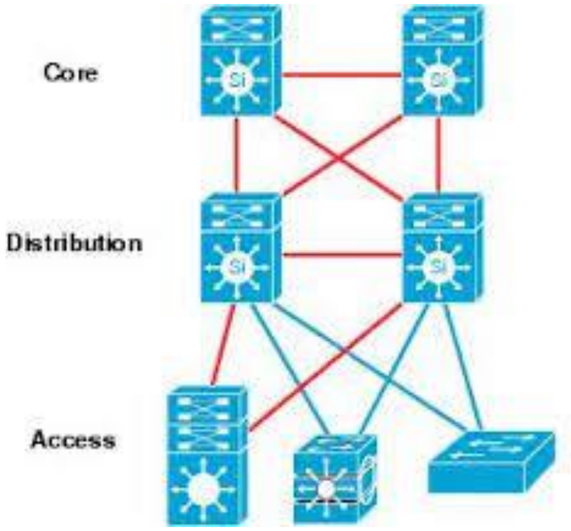


Figure 2 . 3 Layer Topology

Features:

- Connecting a physical port to many virtual machines.
- More than one path possible for both east-west and north-south traffic, with varying number of hops.
- Use of protocols such as Spanning-tree that “deactivate” a path to avoid loops.
- Limited bandwidth with possible oversubscription.

4.1.5.- VPN

VPN (Virtual Private Network) is a network technology that allows a secure extension of the local network (LAN) over a public or uncontrolled network such as the Internet, through an encapsulation and encryption process, of data packets to different points through the use of public transport infrastructures.

VPN offers a low-cost solution to implement a long-distance network by being based on the Internet, in addition to offering user or device authentication through encryption, digital signatures or access codes for unequivocal identification; it also offers integrity, guaranteeing that the data sent by the issuer is exact to the data received, confidentiality and encryption.

4.1.6 Site to Site VPN

This scheme is used to connect remote offices with the organization headquarters. The central VPN team, which has a permanent Internet link, accepts Internet connections from the sites and establishes the VPN "tunnel." Branch office servers connect to the Internet using the services of your local Internet provider, typically through broadband connections. This allows costly traditional point-to-point links to be eliminated, especially in international communications.

4.1.7 IPSEC

Ipsec (short for Internet Protocol security) is a suite of protocols whose function is to secure communications over the Internet Protocol (IP) by authenticating and/or encrypting each IP packet in a data stream. Ipsec also includes protocols for establishing encryption keys.

The Ipsec protocols operate at the network layer, layer 3 of the OSI model. Other widely used Internet security protocols, such as SSL, TLS, and SSH, operate at the application layer (layer 7 of the OSI model). This makes Ipsec more flexible, as it can be used to protect Layer 4 protocols, including TCP and UDP.

4.1.8.- L2TP

L2TP (Layer 2 Tunneling Protocol) is a protocol used by virtual private networks that was designed by an IETF working group as the heir apparent to the PPTP and L2F protocols, created to correct the deficiencies of these protocols and establish itself as an approved standard. By the IETF (RFC 2661).12 L2TP uses PPP to provide dial-up access that can be tunneled through the Internet to a point. L2TP defines its own tunneling protocol, based on L2F. The L2TP transport is defined for a wide variety of data packet types, including X.25, Frame Relay, and ATM.

By using PPP for telephony trunk establishment, L2TP includes the authentication mechanisms of PPP, PAP, and CHAP. Similar to PPTP, it supports the use of these authentication protocols, such as RADIUS.

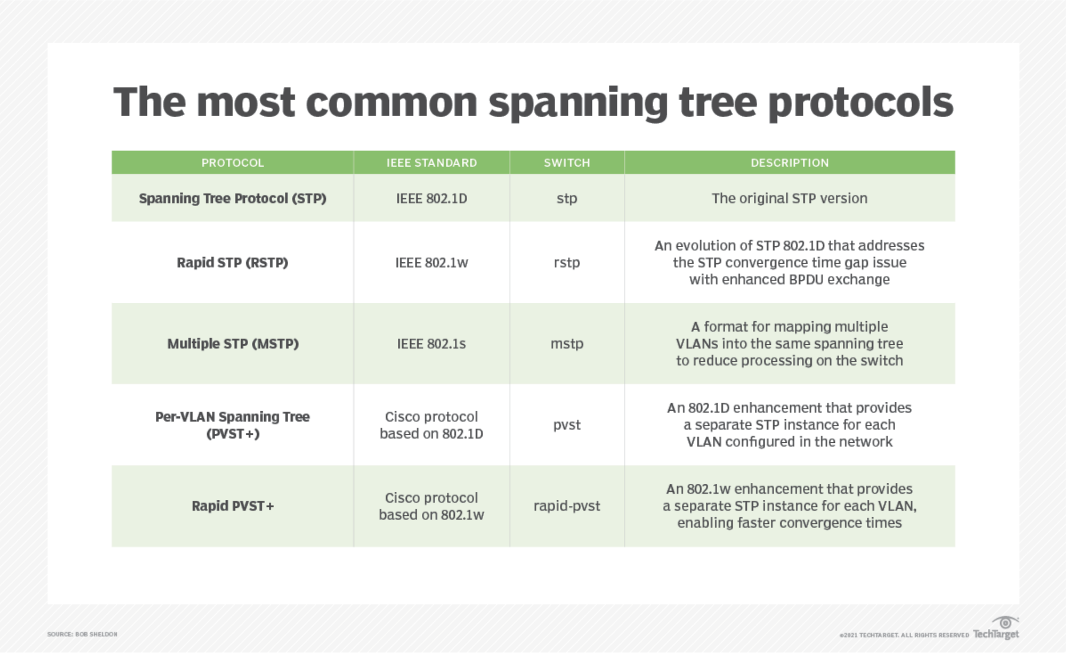
L2TP is actually a variation of an IP encapsulation protocol. An L2TP tunnel is created by encapsulating an L2TP frame in a UDP packet, which is encapsulated in turn into an IP packet, whose source and destination addresses define the ends of the tunnel. Being the outermost IP encapsulation protocol, IPSec protocols can be used over this packet, thus protecting the information that is transported through the tunnel.

4.1.9.- STP

Varieties of spanning tree protocols include the following:

- STP – This is the original version of IEEE 802.1D (802.1D-1998 and earlier), which provides a loop-free topology on a network with redundant links. Common Spanning Tree (CTS) assumes one spanning tree instance for the entire bonded network, regardless of the number of VLANs.
- PVST+ – This is a Cisco enhancement of STP that provides one 802.1D Spanning Tree instance for each VLAN configured on the network. The separate instance supports PortFast, UplinkFast, BackboneFast, BPDU Guard, BPDU Filter, Root Guard, and Loop Guard.
- 802.1D-2004 – This is an updated version of the STP standard that incorporates IEEE 802.1w.

- Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1w: This is an evolution of STP that provides faster convergence than STP.
- Fast PVST+ – This is a Cisco enhancement of RSTP that uses PVST+. Fast PVST+ provides a separate 802.1w instance per VLAN. The separate instance supports PortFast, BPDU guard, BPDU filter, root guard, and loop guard.
- Multiple Spanning Tree Protocol (MSTP) – An IEEE standard inspired by the earlier Cisco-only implementation of Multi-Instance STP (MISTP). MSTP assigns multiple VLANs on the same spanning tree instance. MST is Cisco's implementation of MSTP, providing up to 16 RSTP instances and combining multiple VLANs with the same physical and logical topology into a common RSTP instance. Each instance supports PortFast, BPDU Guard, BPDU Filter, Root Guard, and Loop Guard.



The most common spanning tree protocols

PROTOCOL	IEEE STANDARD	SWITCH	DESCRIPTION
Spanning Tree Protocol (STP)	IEEE 802.1D	stp	The original STP version
Rapid STP (RSTP)	IEEE 802.1w	rstp	An evolution of STP 802.1D that addresses the STP convergence time gap issue with enhanced BPDU exchange
Multiple STP (MSTP)	IEEE 802.1s	mstp	A format for mapping multiple VLANs into the same spanning tree to reduce processing on the switch
Per-VLAN Spanning Tree (PVST+)	Cisco protocol based on 802.1D	pvst	An 802.1D enhancement that provides a separate STP instance for each VLAN configured in the network
Rapid PVST+	Cisco protocol based on 802.1w	rapid-pvst	An 802.1w enhancement that provides a separate STP instance for each VLAN, enabling faster convergence times

SOURCE: BOB SHELDON

©2021 TECHTARGET. ALL RIGHTS RESERVED TechTarget

Figure 3 . List of spanning tree protocols

4.2.0.- SSH

SSH, or Secure Shell, is a remote administration protocol that allows users to control and modify their remote servers over the Internet. The service was created as a secure replacement for unencrypted Telnet and uses cryptographic techniques to ensure that all communication to and from the remote server happens encrypted. It provides a mechanism to authenticate a remote user, transfer input from the client to the host, and relay the output back to the client.

4.3.- Routing

4.3.1.- Dynamic routing

Dynamic routing is known as a technique of finding the best path for the data to travel over a network in this process a router can transmit data through various different routes and reach its destination on the basis of conditions at that time of communication circuits.

4.3.2.- LACP

In computer networking, the term link aggregation applies to various methods of combining (aggregating) multiple network connections in parallel to increase performance beyond what a single connection could support, and to provide redundancy in the event that one of the links fail. A link aggregation group (LAG) combines a number of physical ports to create a single high-bandwidth data path, in order to implement traffic load sharing among member ports in the group and improve connection reliability.

4.3.3.- Etherchannel (Bonding)

EtherChannel is a Cisco technology built according to the 802.3 full-duplex Fast Ethernet standards. It allows the logical grouping of several Ethernet physical links, this grouping is treated as a single link and allows the nominal speed of each used Ethernet physical port to be added and so on. get a high-speed trunk link.

EtherChannel technology is an extension of a technology offered by Kalpana in its switches in the 1990s.

A maximum of 8 Fast Ethernet, Giga Ethernet or 10Gigabit Ethernet ports can be grouped together to form an EtherChannel. With this last grouping it is possible to achieve a maximum of 80 Gbps of bandwidth. EtherChannel connections can interconnect switches, routers, servers, or clients.

4.4.- Standard ANSI/TIA/EIA 606A

- Standardizes management and labeling practices for Structured Cabling elements.
- Provides guidelines for the coding, identification and documentation of a Structured Cabling system in classes
- Facilitates fault detection and speeds up the solution of eventual problems.
- Unique, to avoid being confused with other similar components. Legible and permanent enough to last the life of the component.
- Identifiers for Class 1 systems. Telecommunications Room Identifier
- Identifier for Horizontal Link

4.5.- Standard ANSI/TIA/EIA 607

The grounding system is very important in the design of a network since it helps to maximize the life time of the equipment, in addition to protecting the life of the personnel despite the fact that it is a system that handles low voltages. Approximately 70% of anomalies and problems associated with power distribution systems are directly or indirectly related to connection and grounding issues. Despite this, the grounding system is one of the most overlooked structured cabling components in the installation.

The standard that describes the grounding system for telecommunication networks is ANSI/TIA/EIA-607. The main purpose is to create an adequate path and with sufficient capacity to direct the electric currents and passing voltages towards the earth. These paths to ground are shorter, lower impedance than those to the building.

The following will explain basic terms to understand a grounding system in general:

- Grounding: It is the connection between an electrical equipment or circuit and the earth.
- Equipotential grounding (bonding): It is the permanent connection of metal parts to form an electrical conductive path that ensures electrical continuity and the ability to safely conduct any current imposed on it.

4.6.- Fiber optic single-mode and multi-mode

Single-mode connection cable: It has the peculiarity that, within its core, the data travels without bouncing off its walls, which allows it to maintain higher transfer speeds.

Data is transferred by tracing a line, so not many light beams can travel at the same time through the small proportions of your conduit.

This type of fiber is used to cover long distances and is built with cores that can measure 9 micrometers with a 125 micrometer cladding.

There are two types of single mode cable:

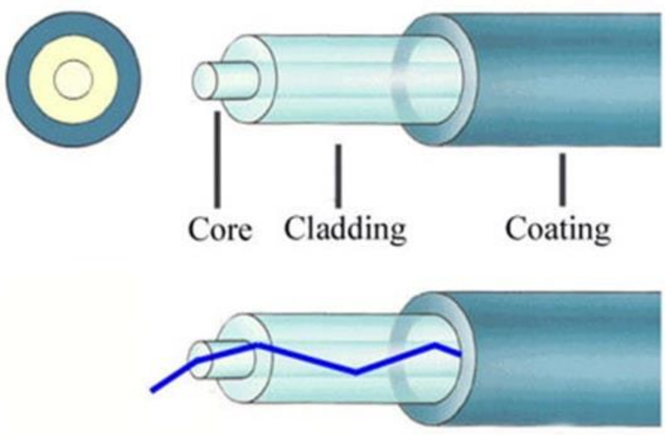
- Single-mode OS1: It can be used indoors and the distance in which it can be deployed is a maximum of 2,000 meters.
- OS2 single mode: It is designed for all uses, making it more than suitable for outdoors.

The distance in which it can be deployed varies between 5,000 to 10,000 meters. This allows from 1 to 10 gigabits of Ethernet.

OS1 and OS2 are long distance cables due to their low bendability.

Single-mode fiber is quite useful for transmitting data over long distances, making it perfect for college campuses and cable TV networks.

Single mode installations are a vital part of broadband networks.



The optical fiber carries the light in its core, whose refractive index greater than the cladding.

Figure 4 . Single mode connection

4.7.- Fiber optic multi-mode

This is “home” fiber and in contrast to single mode fiber, allows light beams to bounce off the walls of the cadding or siding.

A greater number of light beams traveling at the same time through the nucleus. Compared to single-mode fiber, the multimode core measures from 50 to 62.5 micrometers, allowing more space for data to travel.

The 125 micron cladding allows light to travel through the fiber. Multimode fiber is used for local patch networks, building-to-building data centers, and for Fiber To The Home.

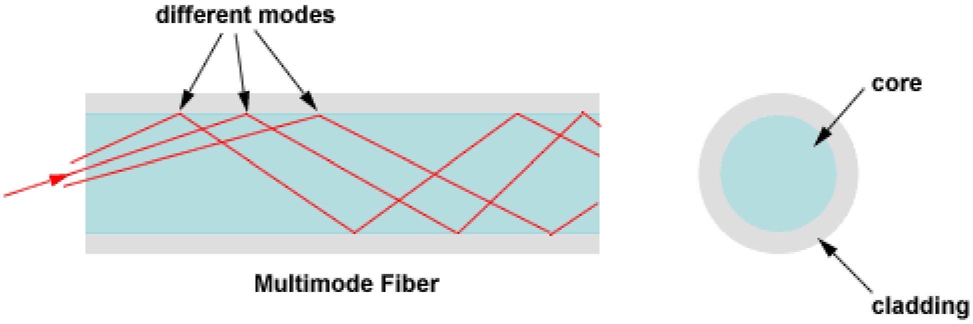


Figure 5 . Multimode connection

5.- Chapter ll . Project engineering

5.1.- Design methodology

The development methodology for the realization presented in the document will be:

Top Down Network Design Top Down is used because it allows designing a network based on modularization starting from the top down.

Each module must have a hierarchy among themselves, since each module is designed separately, even in relation to other modules, it also focuses first on what the business is looking for and then on the technical details.

- Analyze requirements.
- Develop logical design.
- Develop physical design.
- Test, optimize and document the design.
- Implement and test the network.
- Monitor and optimize performance.

5.2.- Network specifications

5.2.1.- EVE-NG

Figure 6 . EVE-NG Simulator

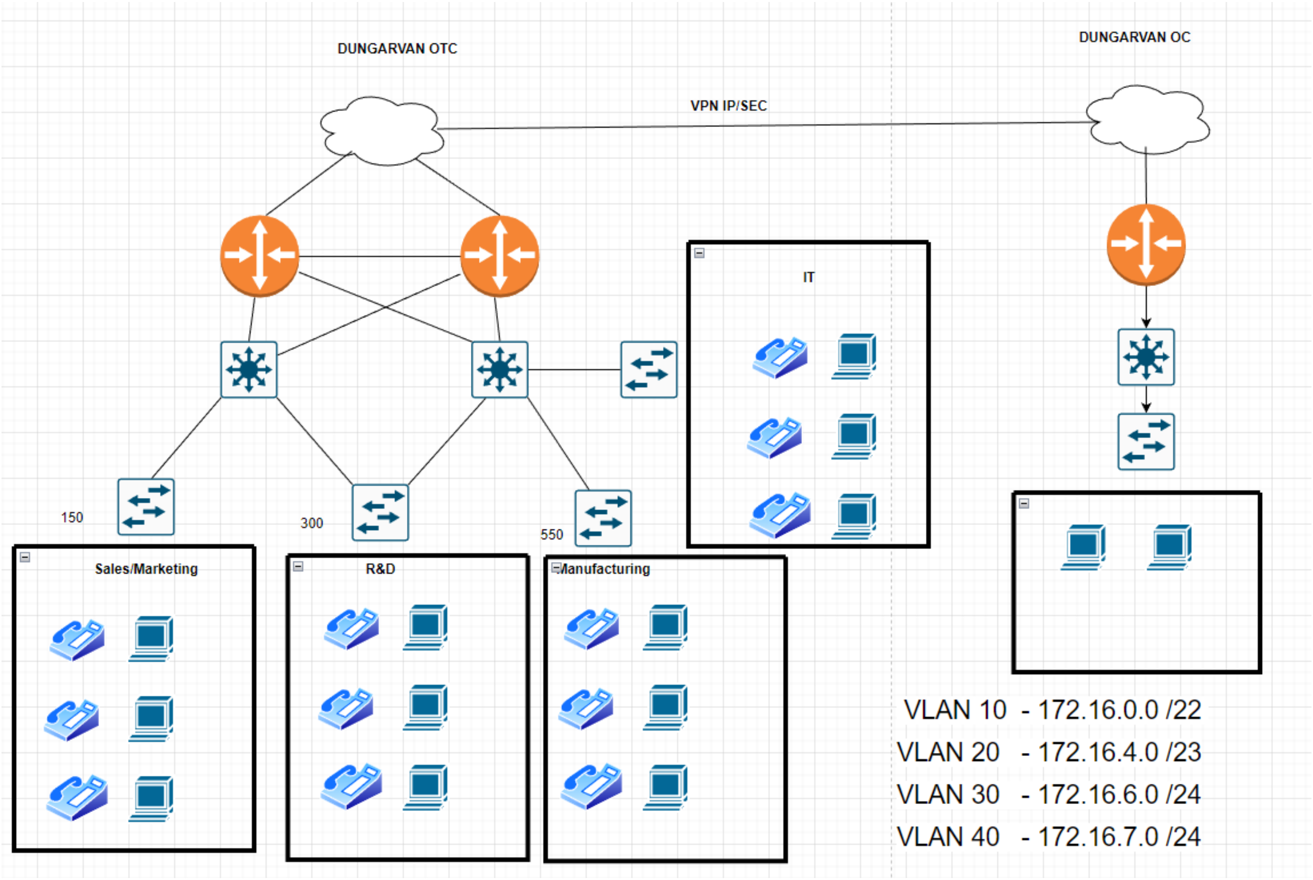
EVE- NG is an Emulated Virtual Environment for Network, Security, and DevOps Professionals. EVE-NG is a clientless multivendor network emulation software that empowers network and security professionals with huge opportunities in the networking world. With EVE-NG, you can build your own virtual labs and train yourself with Cisco, Juniper, Checkpoint, Palo Alto, F5, and many other vendors. You can also construct the network and plan the design to validate solutions. EVE-NG platform is ready for today's IT-world requirements. It allows enterprises, e-learning providers, individuals, and group collaborators to create virtual proof of concepts, solutions, and training environments.

5.2.2.- Mikrotik RouterOS

Figure 7 . Mikrotik RouterOS

Mikrotik RouterOS is the operating system of Mikrotik RouterBOARD hardware. It can also be installed on a PC and will turn it into a router with all the necessary features – routing, firewall, bandwidth management, wireless access point, backhaul link, hotspot gateway, VPN server and more. RouterOS is a stand-alone operating system based on the Linux v2.6 kernel, and our goal here at Mikrotik is to provide all these features with a quick and simple installation and an easy-to-use interface.

4.3.- Logic design network topology



VLAN 10	- 172.16.0.0 /22
VLAN 20	- 172.16.4.0 /23
VLAN 30	- 172.16.6.0 /24
VLAN 40	- 172.16.7.0 /24

Figure 8 Logic design LAN

4.4.- IP address

Class B will be used for IP addressing since growth is being considered in the coming years at the user level.

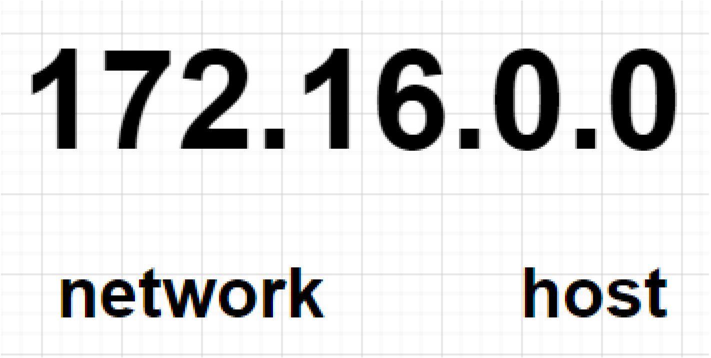
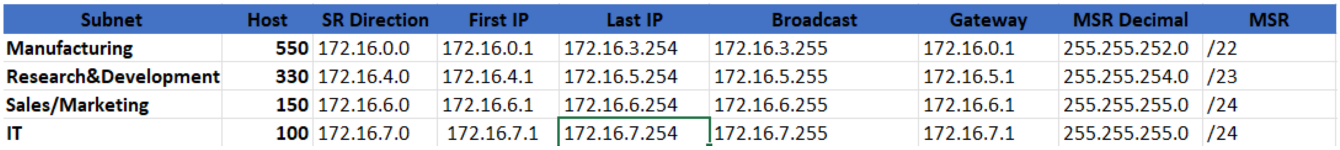


Figure 9 . Networking IP Address Class

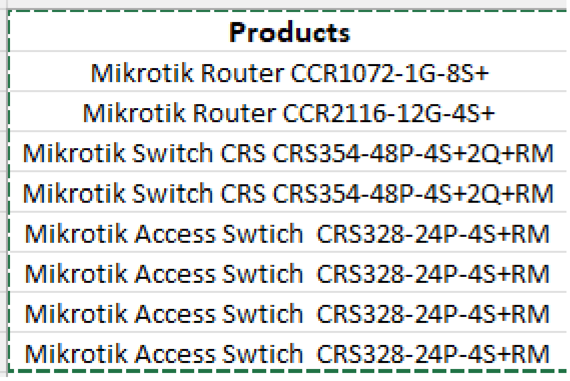
4.5.- Subnetting table



Subnet	Host	SR Direction	First IP	Last IP	Broadcast	Gateway	MSR Decimal	MSR
Manufacturing	**550**	172.16.0.0	172.16.0.1	172.16.3.254	172.16.3.255	172.16.0.1	255.255.252.0	/22
Research&Development	**330**	172.16.4.0	172.16.4.1	172.16.5.254	172.16.5.255	172.16.5.1	255.255.254.0	/23
Sales/Marketing	**150**	172.16.6.0	172.16.6.1	172.16.6.254	172.16.6.255	172.16.6.1	255.255.255.0	/24
IT	**100**	172.16.7.0	172.16.7.1	172.16.7.254	172.16.7.255	172.16.7.1	255.255.255.0	/24

Figure 10 . Subnetting table

4.6.- Equipment selection



Products
Mikrotik Router CCR1072-1G-8S+
Mikrotik Router CCR2116-12G-4S+
Mikrotik Switch CRS CRS354-48P-4S+2Q+RM
Mikrotik Switch CRS CRS354-48P-4S+2Q+RM
Mikrotik Access Swtich CRS328-24P-4S+RM
Mikrotik Access Swtich CRS328-24P-4S+RM
Mikrotik Access Swtich CRS328-24P-4S+RM
Mikrotik Access Swtich CRS328-24P-4S+RM

Figure 11 . Networking Products

4.7.- Implementation

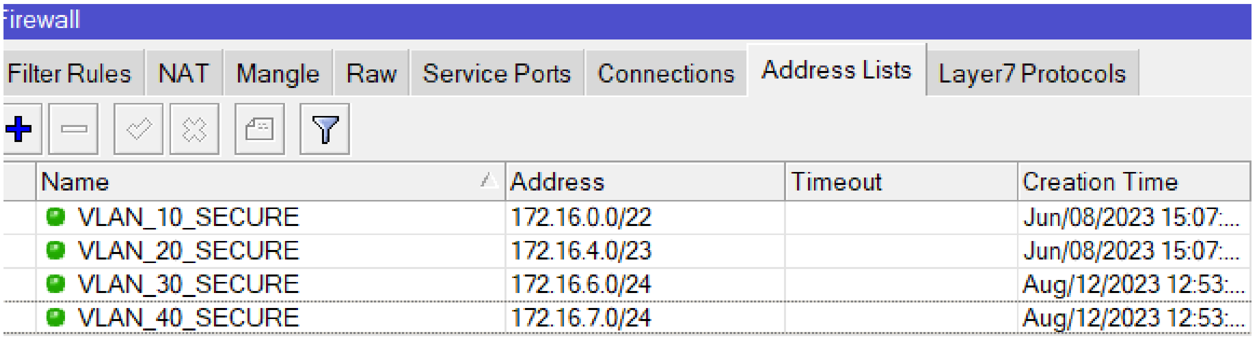
4.7.1.- Security of information

- We will work with the Screened Subnet Firewall Architecture to be able to protect the datacenter, likewise we segment access to resources through Firewall filters.
- The firewall contributes to your IDS/IPS system.
- Use of Active Directory / Windows Server (GPO, Domain, DNS).

Figure 12 . Windows Server

4.8.- Address List

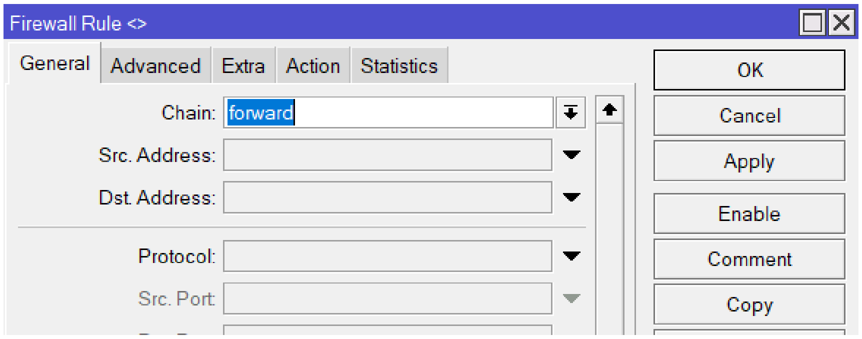
The Mirotik address-list allows for the grouping of two or more users, using the source or destination address as the factor. This allows rules to be applied to a group instead of individual IPs, thereby reducing the number of rules that an administrator can configure for each user in the group. Address-lists can be used in the firewall rule, etc. An address-list can be created manually of dynamically.



Name	Address	Timeout	Creation Time
● VLAN_10_SECURE	172.16.0.0/22		Jun/08/2023 15:07:...
● VLAN_20_SECURE	172.16.4.0/23		Jun/08/2023 15:07:...
● VLAN_30_SECURE	172.16.6.0/24		Aug/12/2023 12:53:...
● VLAN_40_SECURE	172.16.7.0/24		Aug/12/2023 12:53:...

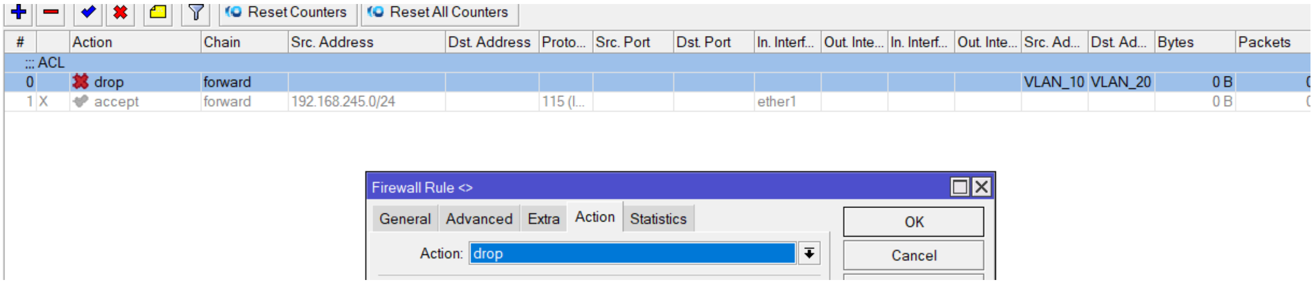
Figure 13 . Address-List

The chain: forward Used to process data packets through routers, connections that occur from the public to local.



Chain: forward

Figure 14 . Firewall Rule



#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Interf...	Out. Inte...	In. Interf...	Out. Inte...	Src. Ad...	Dst. Ad...	Bytes	Packets
::: ACL																
0		drop	forward										VLAN_10	VLAN_20	0 B	
1	X	accept	forward	192.168.245.0/24		115 (l...			ether1						0 B	

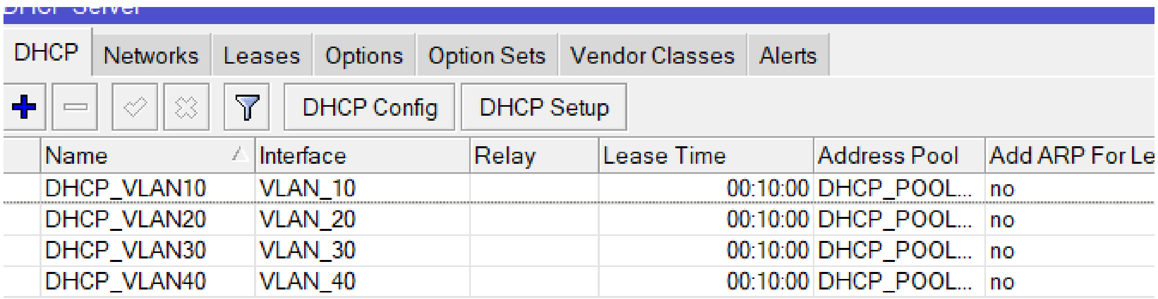
Action: drop

Figure 15 . Firewall Drop packets

The logic says the following: any host other than the Access List "SECURE" will have the DROP action.

4.9.- DHCP

DHCP has been configured for the VLANS.

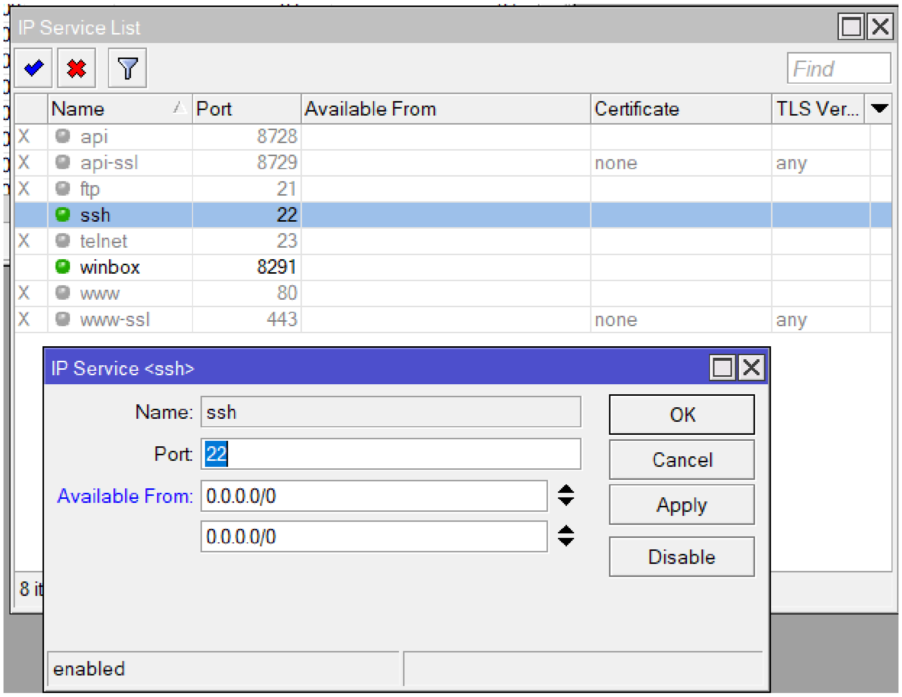


Name	Interface	Relay	Lease Time	Address Pool	Add ARP For Le
DHCP_VLAN10	VLAN_10		00:10:00	DHCP_POOL...	no
DHCP_VLAN20	VLAN_20		00:10:00	DHCP_POOL...	no
DHCP_VLAN30	VLAN_30		00:10:00	DHCP_POOL...	no
DHCP_VLAN40	VLAN_40		00:10:00	DHCP_POOL...	no

Figure 16 . DHCP Server Table

5.- Configure device security and encryption

We can encrypt the access keys to Mikrotik equipment, through the encryption service of this brand and also apply RSA, which is an encryption algorithm. In the case of border routers using IPSEC, SHA, MD5 can be applied.



	Name	Port	Available From	Certificate	TLS Ver...
X	api	8728			
X	api-ssl	8729		none	any
X	ftp	21			
	ssh	22			
X	telnet	23			
	winbox	8291			
X	www	80			
X	www-ssl	443		none	any

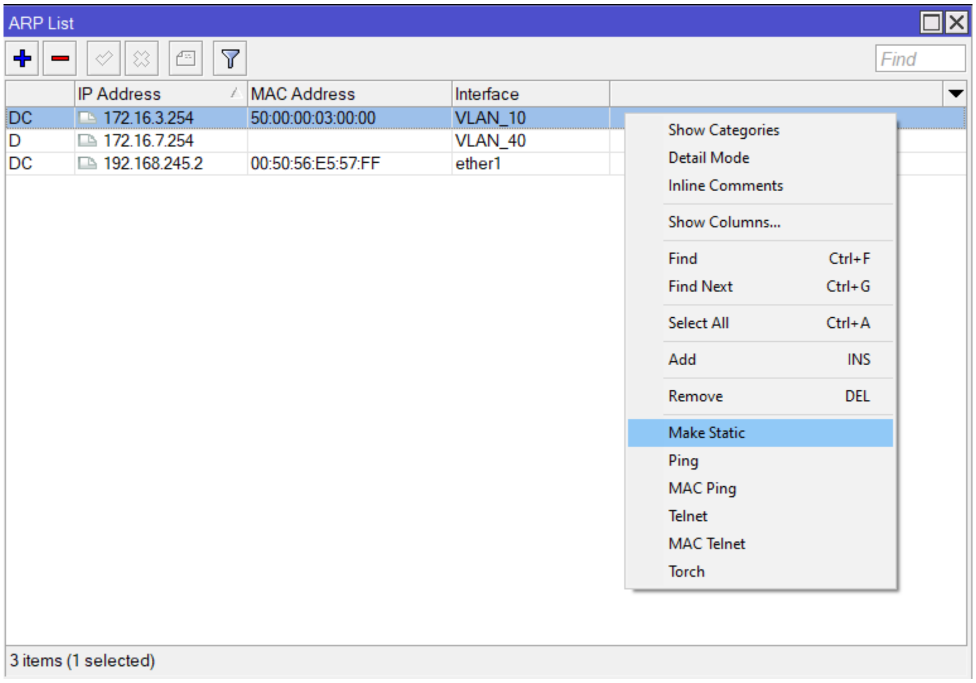
Name: ssh
Port: 22
Available From: 0.0.0.0/0
0.0.0.0/0

enabled

Figure 17 . SSH

6.- For security, hosts cannot change ports

All unused ports are disabled, and MACs are also matched to an IP via ARP.



ARP List

	IP Address	MAC Address	Interface
DC	172.16.3.254	50:00:00:03:00:00	VLAN_10
D	172.16.7.254		VLAN_40
DC	192.168.245.2	00:50:56:E5:57:FF	ether1

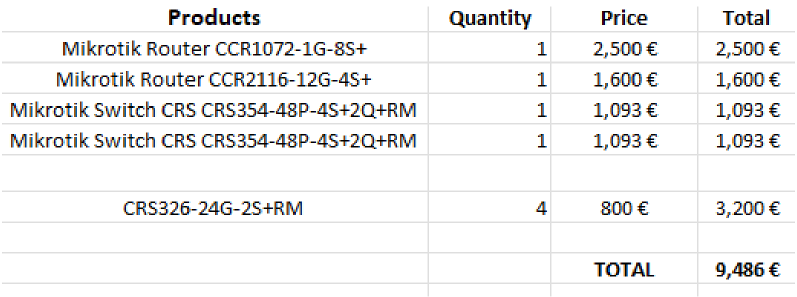
3 items (1 selected)

Figure 18 . ARP

7.- Price

The following quote is not 100% defined because there are too many necessary parameters such as infrastructure map, real distance from the fields, height of the buildings, etc.

The initial price of equipment is as follows:



Products	Quantity	Price	Total
Mikrotik Router CCR1072-1G-8S+	1	2,500 €	2,500 €
Mikrotik Router CCR2116-12G-4S+	1	1,600 €	1,600 €
Mikrotik Switch CRS CRS354-48P-4S+2Q+RM	1	1,093 €	1,093 €
Mikrotik Switch CRS CRS354-48P-4S+2Q+RM	1	1,093 €	1,093 €
CRS326-24G-2S+RM	4	800 €	3,200 €
		TOTAL	9,486 €

Figure 19 . Price

8.- Conclusion and recommendations

It was possible to develop a network design proposal for the pharmaceutical company. An efficient IP addressing was developed that allows it to be scalable in case they are going to grow both at the level of users and network devices. The logical design for their entire network was also drawn up.

8.1.- Recommendations

Se recomienda cumplir el plan de mantenimiento establecido para poder evitar que los equipos sufran daños y a su vez llegue afectar el funcionamiento de toda la red.

9.-Network Device configurations

9.1.- Core Router

```
# aug/12/2023 15:58:52 by RouterOS 6.48.1

# software id =

#

#

#

/interface ethernet

set [ find default-name=ether1 ] comment=WAN

/interface vrrp

add interface=ether2 name=VRRP priority=200 vrid=50

/interface vlan

add interface=ether3 name=VLAN_10 vlan-id=10

add interface=ether3 name=VLAN_20 vlan-id=20

add interface=ether4 name=VLAN_30 vlan-id=30

add interface=ether4 name=VLAN_40 vlan-id=40

add interface=ether10 name=VLAN_99 vlan-id=99

/interface wireless security-profiles
```

```
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=DHCP_POOL_VLAN10 ranges=172.16.0.2-172.16.3.254
add name=DHCP_POOL_VLAN20 ranges=172.16.4.2-172.16.5.254
add name=DHCP_POOL_VLAN30 ranges=172.16.6.2-172.16.6.254
add name=DHCP_POOL_VLAN40 ranges=172.16.7.2-172.16.7.254
add name=dhcp_pool8 ranges=192.168.1.2
add name=VPN_POOL ranges=172.16.8.2-172.16.8.254
/ip dhcp-server
add address-pool=DHCP_POOL_VLAN10 disabled=no interface=VLAN_10 name=\
    DHCP_VLAN10
add address-pool=DHCP_POOL_VLAN20 disabled=no interface=VLAN_20 name=\
    DHCP_VLAN20
add address-pool=DHCP_POOL_VLAN30 disabled=no interface=VLAN_30 name=\
    DHCP_VLAN30
add address-pool=DHCP_POOL_VLAN40 disabled=no interface=VLAN_40 name=\
    DHCP_VLAN40
```

```
/ppp profile
set *0 local-address=172.16.4.1 remote-address=VPN_POOL
/interface l2tp-server server
set authentication=mschap2 default-profile=default enabled=yes ipsec-secret=\
    123456 keepalive-timeout=disabled use-ipsec=required
/ip address
add address=172.16.0.1/22 comment=MANUFACTURING interface=VLAN_10 network=\
    172.16.0.0
add address=172.16.4.1/23 comment=RESEARCH&DEVELOPMENT interface=VLAN_20 \
    network=172.16.4.0
add address=10.0.0.1 comment="High Aviability" interface=VRRP network=\
    10.0.0.1
add address=10.0.0.3/24 interface=ether2 network=10.0.0.0
add address=172.16.6.1/24 comment=SALES/MARKETING interface=VLAN_30 network=\
    172.16.6.0
add address=172.16.7.1/24 comment=IT interface=VLAN_40 network=172.16.7.0
add address=192.168.1.1/30 comment=MGMT interface=VLAN_99 network=192.168.1.0
```

```
/ip dhcp-client

add disabled=no interface=ether1

/ip dhcp-server network

add address=172.16.0.0/22 dns-server=172.16.7.254,8.8.8.8 gateway=172.16.0.1

add address=172.16.4.0/23 dns-server=172.16.7.254,8.8.8.8 gateway=172.16.4.1

add address=172.16.6.0/24 dns-server=172.16.7.254,8.8.8.8 gateway=172.16.6.1

add address=172.16.7.0/24 dns-server=172.16.7.254,8.8.8.8 gateway=172.16.7.1

/ip dns

set servers=1.1.1.1

/ip firewall address-list

add address=172.16.0.0/22 list=VLAN_10_SECURE

add address=172.16.4.0/23 list=VLAN_20_SECURE

add address=172.16.6.0/24 list=VLAN_30_SECURE

add address=172.16.7.0/24 list=VLAN_40_SECURE

/ip firewall filter

add action=drop chain=forward comment=ACL disabled=yes dst-address-list=\

    VLAN_20 src-address-list=VLAN_10
```

```
add action=accept chain=forward disabled=yes in-interface=ether1 protocol=\
    l2tp src-address=192.168.245.0/24
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set api disabled=yes
set api-ssl disabled=yes
/ppp secret
add local-address=172.16.4.1 name=haleon password=123456 remote-address=\
    172.16.8.3 service=l2tp
/system identity
set name=Dungarvan-OTC-Core-R
/tool romon
set enabled=yes
```

9.2.- Core Back-up

```
# aug/12/2023 16:02:10 by RouterOS 6.48.6
# software id =
#
#
#
/interface ethernet
set [ find default-name=ether1 ] comment=WAN
set [ find default-name=ether2 ] comment=LAN
/interface vrrp
add interface=ether2 name=VRRP preemption-mode=no vrid=50
/interface vlan
add interface=ether4 name=VLAN_10 vlan-id=10
add interface=ether4 name=VLAN_20 vlan-id=20
add interface=ether3 name=VLAN_30 vlan-id=30
add interface=ether3 name=VLAN_40 vlan-id=40
add interface=ether10 name=VLAN_99 vlan-id=99
/interface wireless security-profiles
```

```
set [ find default=yes ] supplicant-identity=MikroTik

/ip pool

add name=DHCP_POOL_VLAN10 ranges=172.16.0.2-172.16.3.254

add name=DHCP_POOL_VLAN20 ranges=172.16.4.2-172.16.5.254

add name=DHCP_POOL_VLAN30 ranges=172.16.6.2-172.16.6.254

add name=DHCP_POOL_VLAN40 ranges=172.16.7.2-172.16.7.254

add name=dhcp_pool8 ranges=192.168.1.2

/ip dhcp-server

add address-pool=DHCP_POOL_VLAN10 disabled=no interface=VLAN_10 name=\

    DHCP_VLAN10

add address-pool=DHCP_POOL_VLAN20 disabled=no interface=VLAN_20 name=\

    DHCP_VLAN20

add address-pool=DHCP_POOL_VLAN30 disabled=no interface=VLAN_30 name=\

    DHCP_VLAN30

add address-pool=DHCP_POOL_VLAN40 disabled=no interface=VLAN_40 name=\

    DHCP_VLAN40

/ip address
```

```
add address=10.0.0.1 interface=VRRP network=10.0.0.1

add address=10.0.0.2/24 interface=ether2 network=10.0.0.0

add address=172.16.0.1/22 comment=MANUFACTURING interface=VLAN_10 network=\

   172.16.0.0

add address=172.16.4.1/23 comment=RESEARCH&DEVELOPMENT interface=VLAN_20 \

   network=172.16.4.0

add address=10.0.0.3/24 interface=ether2 network=10.0.0.0

add address=172.16.6.1/24 comment=SALES/MARKETING interface=VLAN_30 network=\

   172.16.6.0

add address=172.16.7.1/24 comment=IT interface=VLAN_40 network=172.16.7.0

add address=192.168.1.1/30 comment=MGMT interface=VLAN_99 network=192.168.1.0

/ip arp

add address=192.168.40.254 interface=VLAN_40 mac-address=50:00:00:06:00:00

/ip dhcp-client

add disabled=no interface=ether1

/ip dhcp-server network

add address=172.16.0.0/22 dns-server=172.16.7.254,8.8.8.8 gateway=172.16.0.1
add address=172.16.4.0/23 gateway=172.16.4.1
add address=172.16.6.0/24 gateway=172.16.6.1
add address=172.16.7.0/24 gateway=172.16.7.1
/ip firewall address-list
add address=172.16.0.0/22 disabled=yes list=VLAN_10
add address=172.16.4.0/23 disabled=yes list=VLAN_20
/ip firewall nat
add action=masquerade chain=srcnat
/system identity
set name=Core-B
/tool romon
set enabled=yes
```

9.3.- Switch Core – 1

```
# aug/12/2023 16:03:32 by RouterOS 6.48.6
# software id =
#
#
#
/interface bridge
add name=bridge1 vlan-filtering=yes
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge port
add bridge=bridge1 interface=ether1 pvid=10
add bridge=bridge1 interface=ether2
add bridge=bridge1 interface=ether3 pvid=20
add bridge=bridge1 interface=ether4
add bridge=bridge1 interface=ether5
add bridge=bridge1 interface=ether6
add bridge=bridge1 interface=ether7
add bridge=bridge1 interface=ether8
add bridge=bridge1 interface=ether9
add bridge=bridge1 interface=ether10
/interface bridge vlan
add bridge=bridge1 tagged=ether2,ether4,ether3 vlan-ids=20
add bridge=bridge1 tagged=ether2,ether4,ether1 vlan-ids=10
/ip dhcp-client
add interface=ether1
/system identity
set name=CORE-SW
/tool romon
set enabled=yes
```

9.4.- Switch core – 2

```
# aug/12/2023 16:05:04 by RouterOS 6.48.6
# software id =
#
#
#
/interface bridge
add name=SW-BR vlan-filtering=yes
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=dhcp_pool0 ranges=10.0.0.2-10.0.0.254
add name=dhcp_pool1 ranges=192.168.10.2-192.168.10.62
add name=dhcp_pool2 ranges=192.168.20.2-192.168.20.62
add name=dhcp_pool3 ranges=192.168.99.2-192.168.99.254
add name=dhcp_pool4 ranges=192.168.99.2-192.168.99.254
/caps-man manager
set enabled=yes
```

```
/interface bridge port
add bridge=SW-BR interface=ether1
add bridge=SW-BR interface=ether2 pvid=10
add bridge=SW-BR interface=ether3 pvid=30
add bridge=SW-BR edge=yes interface=ether4 point-to-point=no
add bridge=SW-BR interface=ether5 pvid=40
add bridge=SW-BR interface=ether6
add bridge=SW-BR interface=ether7
add bridge=SW-BR interface=ether8
add bridge=SW-BR interface=ether9
add bridge=SW-BR interface=ether10
/interface bridge vlan
add bridge=SW-BR tagged=ether1,ether4,ether3 vlan-ids=30
add bridge=SW-BR disabled=yes tagged=ether1,ether2 vlan-ids=10
add bridge=SW-BR disabled=yes tagged=ether1,ether4 vlan-ids=20
add bridge=SW-BR tagged=ether1,ether4,ether5 vlan-ids=40
/ip dhcp-client
```

```
add interface=SW-BR
/ip dns
set allow-remote-requests=yes servers=1.1.1.1
/ip route
add distance=1 gateway=172.16.1.1
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set ssh disabled=yes
set api disabled=yes
set winbox disabled=yes
set api-ssl disabled=yes
/system identity
set name=SW-Core-2
/tool romon
set enabled=yes
```

9.5.- Access Switches 1- 4

```
# aug/12/2023 16:06:25 by RouterOS 6.48.6
# software id =
#
#
#
/interface bridge
add name=SW-BR vlan-filtering=yes
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge port
add bridge=SW-BR interface=ether1 pvid=10
add bridge=SW-BR interface=ether4 pvid=10
add bridge=SW-BR disabled=yes interface=ether2
add bridge=SW-BR disabled=yes interface=ether2 pvid=10
add bridge=SW-BR disabled=yes interface=ether3 pvid=10
/interface bridge vlan
add bridge=SW-BR tagged=ether1 untagged=ether4,ether2,ether3 vlan-ids=10
```

```
/ip dhcp-client

add interface=ether2

/system identity

set name=SW-A1

/tool romon

set enabled=yes
```

10.- References

help.mikrotik.com. (n.d.). VLAN - RouterOS - MikroTik Documentation. [online] Available at: https://help.mikrotik.com/docs/display/ROS/VLAN.

wiki.mikrotik.com. (n.d.). Manual:IP/DHCP Server - MikroTik Wiki. [online] Available at: https://wiki.mikrotik.com/wiki/Manual:IP/DHCP_Server.

Timigate (2022). Mikrotik trunk and access port configuration. [online] Timigate. Available at: https://timigate.com/2022/11/mikrotik-trunk-and-access-port-configuration.html#:~:text=The%20two%20major%20port%20types.

Cloud Brigade. (n.d.). MikroTik L2TP VPN Setup. [online] Available at: https://www.cloudbrigade.com/mikrotik-l2tp-vpn-setup/.

Search WindowsServer. (n.d.). What is Active Directory (AD)? [online] Available at: https://www.techtarget.com/searchwindowsserver/definition/Active-Directory.

help.mikrotik.com. (n.d.). Building Your First Firewall - RouterOS - MikroTik Documentation. [online] Available at: https://help.mikrotik.com/docs/display/ROS/Building+Your+First+Firewall.