Branch Office Network

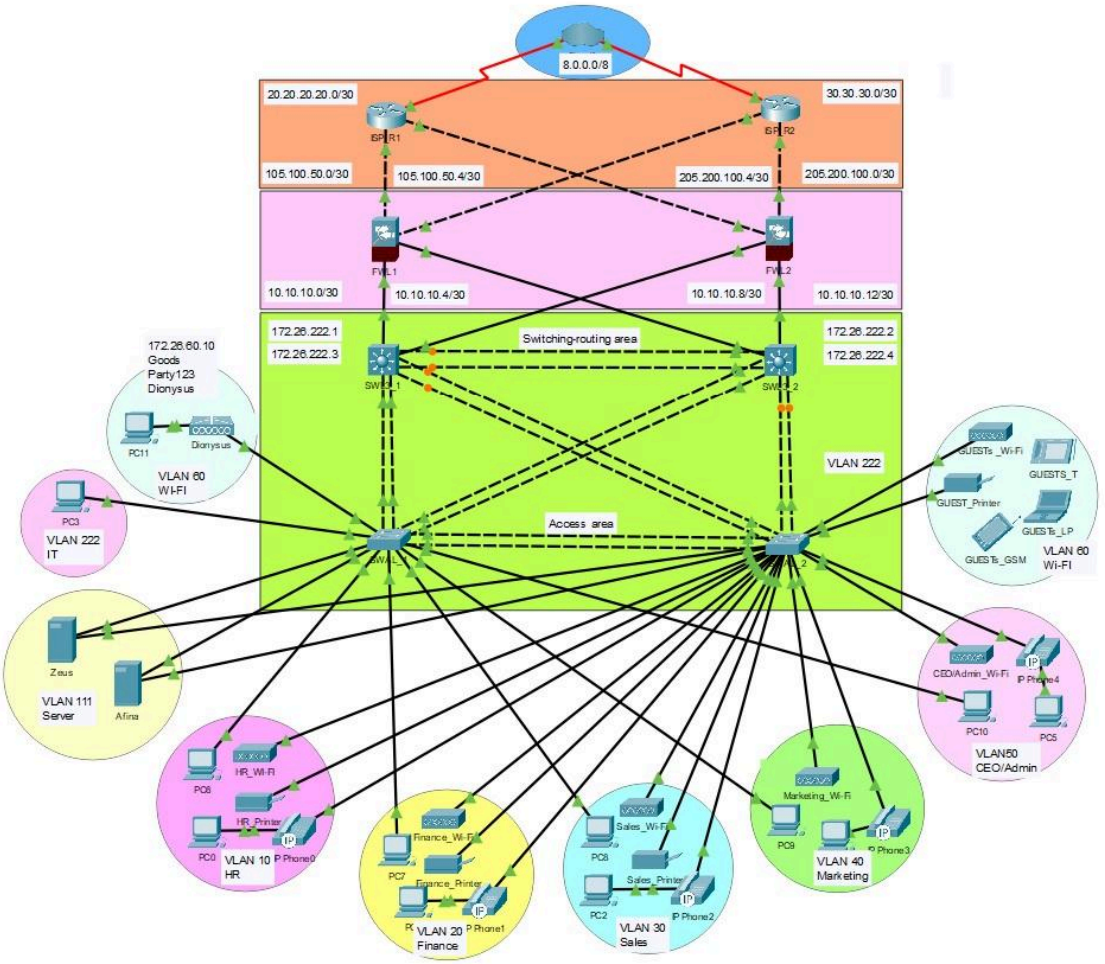
Branch Office Network Project Documentation
Project: Designing and Enhancing the Branch Office Network
Client: Proximus
Author: Lieniie Dzhelianchyk
Date: 17.12.2024
Version: 1.0

1. Introduction:

This document contains detailed documentation for the branch office network project. The goal of this project is to design and enhance the network infrastructure to ensure stable, secure, and efficient operation of the company's branch. This project will cover the phases of design, build, configuration, and improvement of network solutions, utilizing Cisco technologies,

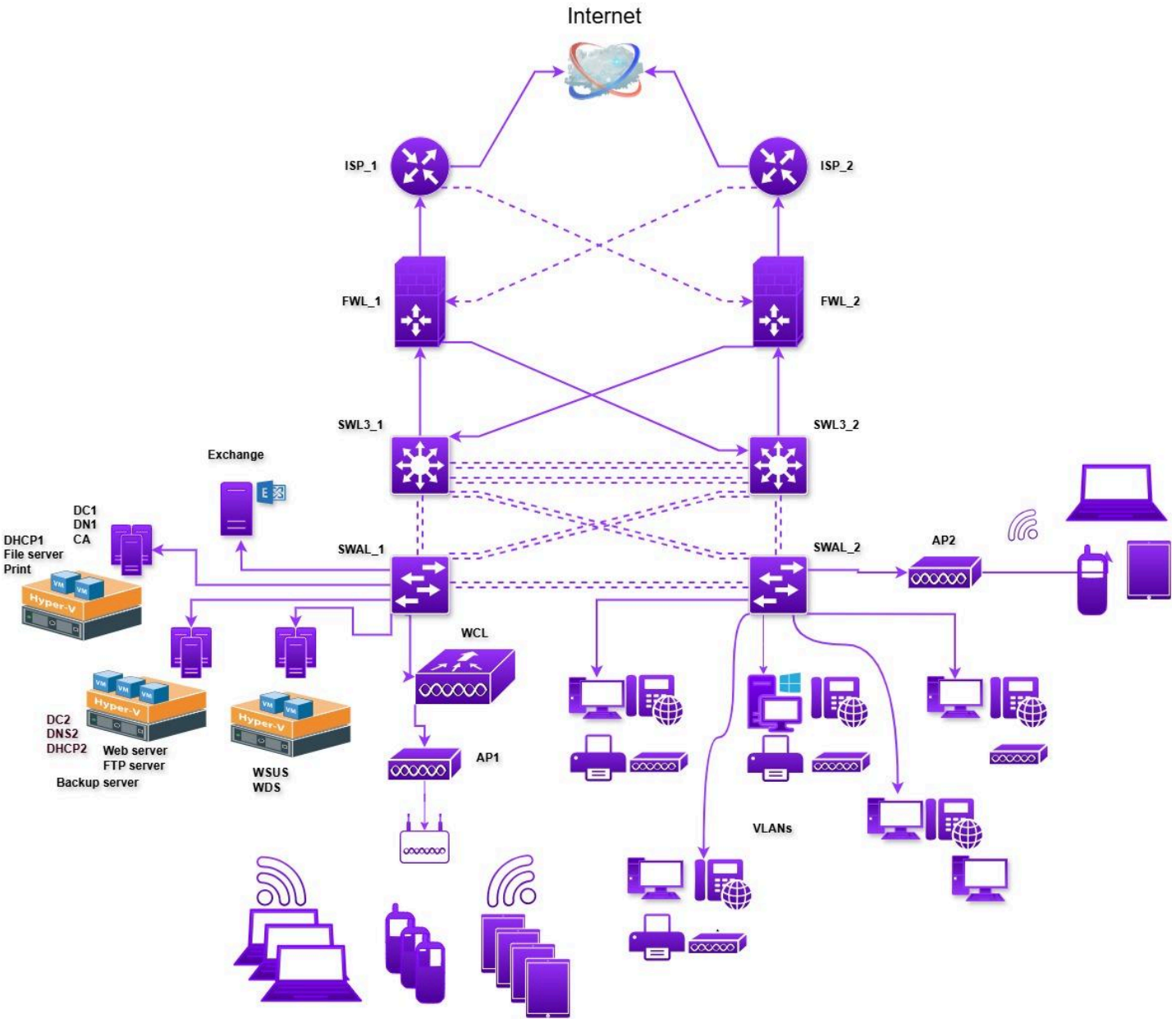
The project includes:
1. Network design, including needs analysis and technical requirements gathering.
2. Implementation of network solutions, including installation, configuration, and testing.
3. Solution enhancements including network redundancy, security, and network services improvements.
4. Solution presentation with an explanation of technology and configuration choices.
5. Add-ons such as automation and troubleshooting.

Below is a visual representation of the network diagram that will be implemented as part of this project.



2. Design Phase

This section will cover the main steps of the network design phase, including scenario analysis, technical solution proposal, and solution documentation.

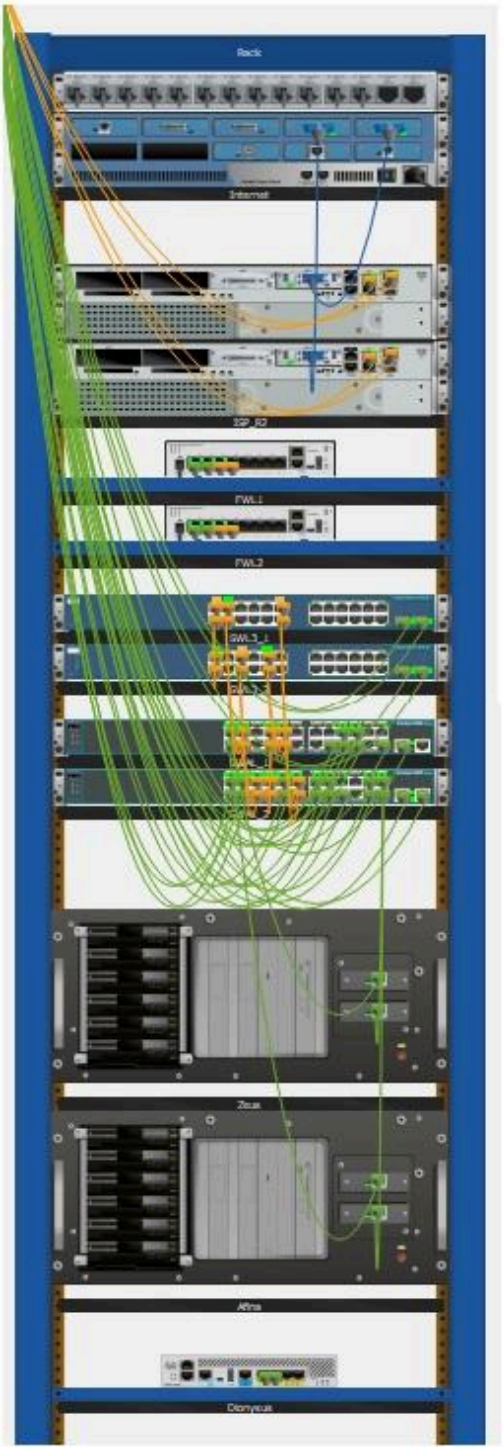


Logical Network Topology Diagrams

3. Scenario Analysis and Technical Requirements Gathering

Purpose of this Phase:

The goal of this phase is to understand the business requirements and gather the technical specifications needed for designing the network infrastructure. This step ensures that the network will meet both operational and performance needs before moving forward with the design and build phases.



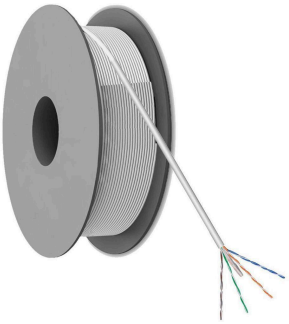
4. Network Topology Design:

- Topology: Hub-and-Spoke design with redundant paths.
- Spine and Leaf network architecture
- Enterprise branch module

Physical Network Topology Diagrams

Bill of Materials (BOM)

Device Type	Device	Model	Price (Budget)	Infra	Cost
Hardware					
Routers		Cisco ISR 1100 Series	~800–1.200	x2	~1800
Core Switchs		Cisco Catalyst 2960-X	~1.500–2.000	x2	~3000
Access Switches		Cisco Catalyst 9200L,48 - ports, +PoE	~1.000–1.500	x2	~2200
Firewall		Cisco Firepower 1010	~600–1.200	x2	~1600
KVM Switch (Keyboard, Video, and Mouse switch)		Basic KVM Switch, 8 ports,	€1000	x1	~1000

WLC		Cisco 3504 Wireless Controller	€550	x1	~550
Wireless AP		Cisco Aironet 1815i	€200–500	x10	~300
UPS power supply		1000W to 3000W	€500–700	x1	~600
Power supply cables		C14 -C15	€3.50	x30	~70
PoE Injectors		Multi-Port PoE Injector	€50 to €150	x5	~250
Cables		100m	€50	x2	~100

Rack		Digitus Netwerkkast 22U Unique 1164X800X800mm Zwart	€1500	x1	~1500
Plugs			€30-50	x2	~100
Software					
Servers		Windows Enterprise Linux	€800-5000 €350-5000		
OSPF BGP Inter-Vlan Routing NAT Qos IPSec VPN GRE Tunnels ACL FW DHCP Server DHCP Relay SNMP Syslog NetFlow IPv6 Routing	ISP FW SWL3 SWAL	IP Services	€500 to €1500	x8	~8000
Exchange		cloud server per client	€700 - €1000 per year €30-50 per client		
Azure		Vms ADC	€50 - €500 €6.50-9.50 per month per client		
Microsocf365		per client	€10.50 per month		

End devices					
Printer		Canon or Brother	€1200-2000	x4	6000
IP phone		Cisco	€150-300	x10	~2000
PCs		Dell, HP….	€600+	x10	~6000
		hp, lenovo….	€65+	x10	650
mouse keyboard		Totale:	35000-40000+		

5. IP Addressing and Subnetting:

Purpose: Plan how to allocate IP addresses to devices and segment the network using subnets.

1) Departments:

Number	Department	LAN
10	HR	172.26.10.0/24
20	Finance	172.26.20.0/24
30	Sales	172.26.30.0/24
40	Marketing	172.26.40.0/24
50	CEO/Administrative	172.26.50.0/24
60	Wi-Fi/Guests wi-fi	172.26.60.0/24
70	Printer	172.26.70.0/28
80	Native	172.26.80.0/24
90	VoIP	172.26.90.0/24
111	Server	172.26.111.0/27
222	IT	172.26.222.0/27
666	NoN	block ports

2) Between the Cloud, ISP, Firewall, Routers and Layer-3 Switch:

Area	Netwerk
CLOUD Area	8.0.0.0/8
ISP1_R1 - Internet	20.20.20.0/30
ISP2_R2 - Internet	30.30.30.0/30
ISP1_R1-FWL1	105.100.50.0/30
ISP1_R1-FWL2	105.100.50.4/30
ISP2_R2-FWL2	205.200.100.0/30
ISP2_R2-FWL1	205.200.100.4/30
FWL1 to -SWL3_1	10.10.10.0/30
FWL1 to -SWL3_2	10.10.10.4/30
FWL2 to -SWL3_1	10.10.10.8/30
FWL2 to -SWL3_2	10.10.10.12/30

3) Devices IP :

Devices	IP	MAC
SWL3_1	172.26.222.1	
SWL3_2	172.26.222.2	
SWAL_1	172.26.222.3	
SWAL_2	172.26.222.4	
Dionysus_WCL	172.26.60.10	
Zeus - server1	172.26.111.5	
Afina - server2	172.26.111.6	
HP_Printer	172.26.70.5	
Finance_Printer	172.26.70.6	
Sales_Printer	172.26.70.7	
GUESTs_Printer	172.26.70.10	
HR-Phone		00d0.97d6.b1b4
Finance_P		00e0.f90d.3803
Sales_P		0001.9641.370e
Marketing_P		00e0.f74d.3c20
CEO_P		0090.2150.50d4
PC_IT	172.26..222.5-10	

4) VLAN Design:

Purpose: Segment the network into virtual LANs (VLANs) to improve security and manage traffic efficiently

Network Addressing Table:
Starting address range is 172.26.0.0/16

Vlan*s	ID	Network address	SM	Subnet Mask	Subnet IP address	Virtual IP (DGW)	Usable Host IP Range:	Broadcast IP address	Wildcard
HR	10	172.26.10..0	/24	255.255.255.0	172.26.10.1	172.26.10.254	172.26.10.1 - 172.26.10..254	172.26.10.255	0.0.0.255
Finance	20	172.26.20.0	/24	255.255.255.0	172.26.20.1	172.26.20..254	172.26.20.1 - 172.26.20.254	172.26.20.255	0.0.0.255
Sales	30	172.26.30.0	/24	255.255.255.0	172.26.30.1	172.26.30.254	172.26.30.1 - 172.26.30.254	172.26.30.255	0.0.0.255
Marketing	40	172.26.40.0	/24	255.255.255.0	172.26.40.1	172.26.40.254	172.26.40.1 - 172.26.40.254	172.26.40.255	0.0.0.255
CEO/ Admin-istrative	50	172.26.50.0	/24	255.255.255.0	172.26.50.1	172.26.50.254	172.26.50.1 - 172.26.50.254	172.26.50.255	0.0.0.255
WI-FI	60	172.26.60.0	/24	255.255.255.0	172.26.60.1	172.26.60.254	172.26.60.1 - 172.26.60.254	172.26.60.254	0.0.0.255
Printer	70	172.26.70.0	/28	255.255.255.240	172.26.70.1	172.26.70.14	172.26.70.1- 172.26.70.14	172.26.70.15	0.0.0.15
Native	80	172.26.80.0	/24	255.255.255.0	172.26.80.1	172.26.80.254	172.26.80.1 - 172.26.80.254	172.26.80.254	0.0.0.255
VoIP	90	172.26.90.0	/24	255.255.255.0	172.26.90.1	172.26.90.254	172.26.90.1 - 172.26.90.254	172.26.90.254	0.0.0.24
Server	111	172.26.111.0	/27	255.255.255.224	172.26.111.1	172.26.111.30	172.26.111.1 - 172.26.111.30	172.26.111.31	0.0.0.31
IT	222	172.26.222.0	/27	255.255.255.224	172.26.222.1	172.26.222.30	172.26.222.1 - 172.26.222.30	172.26.222.31	0.0.0.31

5) Etherchannel groups:

1) group 1 - fa0/1-2
2) group 2 - fa0/3-4
3) group 3 - fa0/5-6
4) group 4 - fa0/7-8
5) group 5 - fa0/9-10
6) group 6 - fa0/11-12

8. Connection Ports:

Device	Connection	Ports	IP address	Device	Connection	Ports	IP address
ISP_1	>FWL_1	G0/0	105.100.50.1	**ISP_2**	>FWL_2	G0/0	205.200.100.1
	>FWL_2	G0/1	105.100.50.5		>FWL_1	G0/1	205.200.100.5
	>BGP	G0/2	20.20.20.1		>BGP	G0/2	30.30.30.1
	Internet	S0/0/0	8.0.0.1		Internet	S0/0/0	8.0.0.2
FWL_1	>ISP_1	G1/3	105.100.50.2 outside	**FWL_2**	>ISP_2	G1/3	205.200.100.2 outside
	>ISP_2	G1/4	205.200.100.6 outside		>ISP_1	G1/4	105.100.50.6 outside
	>SWL3_1	G1/1	10.10.10.2 inside		>SWL3_2	G1/1	10.10.10.13 inside
	>SWL3_2	G1/2	10.10.10.5 inside		>SWL3_1	G0/2	10.10.10.9 inside
SWL3_1	>FWL_1	G0/1	10.10.10.1	**SWL3_2**	>FWL_2	G0/1	10.10.10.14
	>FWL_2	G0/2	10.10.10.10		>FWL_1	G0/2	10.10.10.6
	>SWL3_2	Channel group 1 PortChannel 1 Fa0/1-2			>SWL3_1	Channel group 1 PortChannel 1 Fa0/1-2	
	>SWAL_1	Channel group 2 PortChannel 2 Fa0/3-4			>SWAL_1	Channel group 5 PortChannel 5 Fa0/9-10	
	>SWAL_2	Channel group 6 PortChannel 6 Fa0/11-12			>SWAL_2	Channel group 3 PortChannel 3 Fa0/5-6	
SWAL_1	>SWL3_1 VLAN IT	Channel group 2 PortChannel 2 Fa0/3-4		**SWAL_2**	>SWL3_1 VLAN IT	Channel group 6 PortChannel 6 Fa0/11-12	
	>SWAL_2 VLAN IT	Channel group 4 PortChannel 4 Fa0/7-8			>SWAL_1 VLAN IT	Channel group 4 PortChannel 4 Fa0/7-8	
	>SWL3_1 VLAN IT	Channel group 5 PortChannel 5 Fa0/9-10			>SWL3_2	Channel group 3 PortChannel 3 Fa0/5-6	
	>WCL VLAN 60	G0/1					
					AP-5 VLAN 60	Fa - 0/2, 0/4, 0/14, 0/16, 0/21, g0/1	
	Zeus - DC1 DHCP DNS Server VLAN	Fa0/1			Zeus - DC1 DHCP DNS Server VLAN	Fa0/23	
	Afina - DC2 Server VLAN	Fa0/2			Afina -DC2 Server VLAN	Fa0/24	
	IT VLAN	Fa0/23-24					
	HR VLAN	Fa0/20			HR VLAN	Fa0/1-3	
	Finance VLAN	Fa0/19			Finance VLAN	Fa0/9-10	
	Sales VLAN	Fa0/18			Sales VLAN	Fa0/13-15	

	Marketing VLAN	Fa0/17			Marketing VLAN	Fa0/16-18	
	CEO/Administrative	Fa0/16			CEO/Administrative VLAN	Fa0/19-22	
	PCs	Fa0/20 - HR 0/19 - FInance 0/18 - Sales 0/17 - Marketing 0/16 - CEO/Admin			Printer VLAN	Fa 0/3 - HR 0/9 -FInance 0/15 - Sales	
					VoIP VLAN	Fa 0/1 - HR 0/10 - FInance 0/13 - Sales 0/18 - Marketing 0/22 - CEO/Admin	

9. Routing and Switching Protocols:

Purpose: Choose the best routing protocols for network communication, and switching methods for traffic management.

Protocols:

1) Routing Protocols: OSPF, BGP, NAT, DHCP, HSRP, ISP
2) Switching Protocols: EtherChannel, VLAN, STP, Inter-VLAN Routing,, ACL
3) Basic: SSH, SNMPv2, DNS,

Done	Protocol	Explanation (English)	Пояснення (Українською)
✓	**OSPF**	Open Shortest Path First (OSPF) is a link-state routing protocol used to find the best path for data using a shortest path first (SPF) algorithm.	Open Shortest Path First (OSPF) — це протокол маршрутизації стану зв'язку, який використовується для знаходження найкращого маршруту за допомогою алгоритму найкоротшого шляху (SPF).
✓	**BGP**	Border Gateway Protocol (BGP) is a path-vector routing protocol used to exchange routing information between different networks (AS).	Border Gateway Protocol (BGP) — це протокол маршрутизації векторів шляхів, який використовується для обміну інформацією маршрутизації між різними мережами (AS).
✓	**NAT**	Network Address Translation (NAT) allows the translation of private IP addresses to public IP addresses, enabling private networks to communicate over the internet.	Network Address Translation (NAT) дозволяє перекладати приватні IP-адреси в публічні, що дає змогу приватним мережам спілкуватися через Інтернет.
✓	**DHCP**	Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses to devices on a network, reducing manual configuration.	Dynamic Host Configuration Protocol (DHCP) автоматично присвоює IP-адреси пристроям у мережі, зменшуючи потребу в ручній конфігурації.
✓	**HSRP**	Hot Standby Router Protocol (HSRP) provides redundancy for routers, ensuring a backup router is available if the primary router fails.	Hot Standby Router Protocol (HSRP) забезпечує резервування для маршрутизаторів, гарантуючи наявність резервного маршрутизатора у випадку виходу основного з ладу.

✓	**ISP**	Internet Service Provider (ISP) is an organization that provides services for accessing the Internet, including IP addresses and data transfer services.	Internet Service Provider (ISP) — це організація, яка надає послуги для доступу до Інтернету, включаючи IP-адреси та послуги з передачі даних.
✓	**EtherChannel**	EtherChannel is a technology used to combine multiple physical Ethernet links into a single logical link to increase bandwidth and redundancy.	EtherChannel — це технологія, що використовується для об'єднання кількох фізичних Ethernet-ліній в одну логічну лінію для збільшення пропускної здатності та резервування.
✓	**VLAN**	Virtual LAN (VLAN) is a network protocol that divides a physical network into multiple logical networks to improve security and traffic management.	Virtual LAN (VLAN) — це протокол мережі, який розділяє фізичну мережу на кілька логічних мереж для покращення безпеки та керування трафіком.
✓	**STP**	Spanning Tree Protocol (STP) prevents loops in Ethernet networks by designating one active path and blocking others if necessary.	Spanning Tree Protocol (STP) запобігає утворенню петель в Ethernet-мережах, призначаючи один активний шлях і блокуючи інші, якщо це необхідно.
✓	**Inter-VLAN Routing**	Inter-VLAN Routing allows communication between different VLANs, typically using a Layer 3 device like a router or Layer 3 switch.	Inter-VLAN Routing дозволяє зв'язок між різними VLAN, зазвичай за допомогою пристрою рівня 3, такого як маршрутизатор або комутатор рівня 3.
✓	**ACL**	Access Control Lists (ACL) are used to filter traffic in a network by permitting or denying specific packets based on predefined rules.	Access Control Lists (ACL) використовуються для фільтрації трафіку в мережі, дозволяючи або забороняючи певні пакети на основі попередньо визначених правил.
✓	**SSH**	Secure Shell (SSH) is a protocol used to securely access and manage network devices and servers remotely over a network.	Secure Shell (SSH) — це протокол, який використовується для безпечного віддаленого доступу та керування мережевими пристроями і серверами через мережу.
✓	**SNMPv2**	Simple Network Management Protocol (SNMPv2) is used to manage and monitor network devices and systems.	Simple Network Management Protocol (SNMPv2) використовується для керування та моніторингу мережевих пристроїв і систем.
✓	**DNS**	Domain Name System (DNS) translates human-readable domain names (e.g., www.example.com) into IP addresses that computers can understand.	Domain Name System (DNS) перетворює доменні імена, зрозумілі людині (наприклад, www.example.com), на IP-адреси, які можуть бути зрозумілі комп'ютерам.
✓	**NTP**	Network Time Protocol (NTP) is a protocol used to synchronize the clocks of computers over a network.	Network Time Protocol (NTP) — це протокол, який використовується для синхронізації годинників комп'ютерів через мережу.
✓	**HTTP**	Hypertext Transfer Protocol Secure (HTTPS) is an extension of HTTP that uses SSL/TLS to secure communication over a computer network.	Hypertext Transfer Protocol Secure (HTTPS) — це розширення HTTP, що використовує SSL/TLS для забезпечення безпечного зв'язку через комп'ютерну мережу.

Future implementation			
-	**OSPFv3**	Open Shortest Path First version 3 (OSPFv3) is an extension of OSPF used to support IPv6 routing.	Open Shortest Path First версії 3 (OSPFv3) — це розширення OSPF, яке підтримує маршрутизацію для IPv6.
-	**LACP**	Link Aggregation Control Protocol (LACP) is a protocol used to automatically combine multiple network links into a single logical link.	Link Aggregation Control Protocol (LACP) — це протокол, що використовується для автоматичного об'єднання кількох мережевих ліній в один логічний зв'язок.
-	**PAGP**	Port Aggregation Protocol (PAGP) is a Cisco proprietary protocol used to automatically create EtherChannel by aggregating multiple physical links into a single logical link.	Port Aggregation Protocol (PAGP) — це пропрієтарний протокол Cisco, що використовується для автоматичного створення EtherChannel шляхом об'єднання кількох фізичних ліній в одну логічну лінію.
-	**RADIUS**	Remote Authentication Dial-In User Service (RADIUS) is a protocol that provides centralized authentication, authorization, and accounting for network access.	Remote Authentication Dial-In User Service (RADIUS) — протокол, що забезпечує централізовану аутентифікацію, авторизацію та облік доступу до мережі.
-	**TACACS+**	Terminal Access Controller Access-Control System Plus (TACACS+) is a protocol used for network device administration, providing more granularity than RADIUS.	Terminal Access Controller Access-Control System Plus (TACACS+) — протокол для адміністрування мережевих пристроїв, який надає більшу деталізацію, ніж RADIUS.
-	**FTP**	File Transfer Protocol (FTP) is a standard network protocol used to transfer files between a client and a server.	File Transfer Protocol (FTP) — це стандартний мережевий протокол, що використовується для передачі файлів між клієнтом і сервером.
-	**HTTPS**	Hypertext Transfer Protocol Secure (HTTPS) is an extension of HTTP that uses SSL/TLS to secure communication over a computer network.	Hypertext Transfer Protocol Secure (HTTPS) — це розширення HTTP, що використовує SSL/TLS для забезпечення безпечного зв'язку через комп'ютерну мережу.
-	**SFTP**	Secure File Transfer Protocol (SFTP) is a secure version of FTP that uses SSH to encrypt data transfers.	Secure File Transfer Protocol (SFTP) — це безпечна версія FTP, яка використовує SSH для шифрування передачі даних.
-	**IPSec**	Internet Protocol Security (IPSec) is a suite of protocols used to secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a communication session.	Internet Protocol Security (IPSec) — набір протоколів, що використовується для забезпечення безпеки комунікацій Інтернет-протоколу (IP) шляхом аутентифікації та шифрування кожного IP-пакету в сесії зв'язку.
-	**FW**	pfSense, DMZ, PaloAlto, Metasploit	

	QoS		**Quality of Service (QoS)** у мережах — це набір технологій, які використовуються для управління трафіком, забезпечення пріоритету важливих даних і зниження затримок для критичних додатків, таких як голосові або відео-зв'язки.

10. Redundancy and Failover:

1. HSRP - Dual SW layer 3 ✓
2. EtherChannel ✓
3. Spanning Tree Protocol - Root Guard and BPDU Guard ✓
4. Inter-VLAN Routing ✓
5. OSPF ✓
6. DHCP Failover - DHCP server in DC1 and DC2 + in the SWs layer 3 ✓
7. VoIP Redundancy - SRST - ????
8. UPS (Uninterruptible Power Supply) - Power Redundancy ✓
9. Secondary Internet Link - ISP + BGP ✓
10. Access Point Failover configure to automatically reconnect tp WCL
11. Cloud-Based Failover and Backup
12. DC1 + DC2 + Backup server - Database Clustering ✓
13. SNMP ✓
14. DUAL ISP Failover ✓

11. Passwords:

Paswords now only - olimp1

plutus.expert - DNS

1) enable pasword - olimp10
2) enable secret - olimp@10
3) line console 0 - olimp1
4) line vrty 0 4 - olimp1
5) line aux 0 - olimp1
6) #username goods privilege 15 secret olimp10
7)SSH Modulus 2048
8)WI-Fi - Dionysus - Party123

12. Server Clusters