



NETWORK DESIGN AND IMPLEMENTATION OF LUMINA UNIVERSITY

A dissertation submitted for the
Higher National Diploma in
Network Engineering

COHNDNE232F-018 – V.S Liyanage

COHNDNE232F-045 – G.N.M De Zoysa

COHNDNE232F-049 – D.M.D.J.B Dissanayake

COHNDNE232F-050 – S.N.W.M.S.S Sandaruwan

**National Institute of Business Management
School of Computing
2025**

Declaration

We, hereby affirm that the network project titled Lumina University Network Project is solely my original work and has not been previously submitted for a degree at Lumina University or any other academic institution.

I further declare that to the best of my knowledge, this project does not incorporate any material that has been published or written by another person, except for the explicit acknowledgments made within the document.

I take full responsibility for the content, research, and findings presented in this Lumina University Network Project. This work represents my own efforts and contributions in the field of network engineering.

Date: 10/24/2025

Signatures:

- | | |
|---------------------------|-------|
| 1. V.S Liyanage | |
| 2. G.N.M De Zoysa | |
| 3. D.M.D.J.B Dissanayake | |
| 4. S.N.W.M.S.S Sandaruwan | |

Certified by:

Supervisor Name: Mr. Niranga , Mr. Ilham

Signature:

Date:

ABSTRACT

The "Lumina University Network Project" is a comprehensive initiative aimed at enhancing the efficiency, security, and scalability of the university's network infrastructure. In response to the evolving demands of modern academia, this project focuses on the design, implementation, and optimization of critical network components.

The primary objectives include the evaluation and improvement of network security measures, the integration of advanced technologies to boost performance, and the documentation of a robust network architecture. Through the collaboration of a dedicated team of network engineers, architects, and security analysts, the project seeks to elevate the overall reliability and functionality of the university's network.

Key deliverables encompass detailed documentation of the network architecture, configuration files for all network devices, and comprehensive test reports showcasing the achieved improvements in performance and security. The project timeline, carefully structured to meet milestones and deadlines, reflects a strategic approach to its execution.

As a testament to academic integrity, this thesis adheres to a stringent originality declaration, ensuring that all content is the result of the author's independent work. The findings presented herein contribute to the field of network engineering, providing insights into the successful implementation of network optimization strategies in an academic setting.

The "Lumina University Network Project" not only addresses current challenges but also positions the university's network infrastructure for future advancements, fostering a harmonious environment conducive to academic excellence.

ACKNOWLEDGMENT

I extend my heartfelt gratitude to all those who have contributed to the successful completion of the "Lumina University Network Project." This endeavour has been a collaborative effort, and I am deeply appreciative of the support and guidance received throughout its development.

I express my sincere thanks to Mr. Ilham and Mr. Niranga, whose mentorship and expertise played a pivotal role in shaping the project's direction. Their insights, encouragement, and constructive feedback were invaluable, contributing significantly to the refinement of the network infrastructure.

I extend my appreciation to the entire team involved in the project, including the network engineers, architects, and security analysts. Each team member brought a unique set of skills and dedication, fostering a collaborative environment that enabled the seamless execution of project tasks.

CONTENT

Chapter 1	6
1.1 INTRODUCTION	6
1.2 Importance and Objectives.....	6
1.2.2 Project Implementation and Technologies Used.....	7
Chapter 2: Network Design.....	8
2.1 Network Diagram	8
2.2 Port Table	9
2.3 Heat Map.....	12
2.4 Server Cabinets	15
2.5 Other Tables	18
2.5.1 IP Table	18
2.5.2 Budget Table	20
2.5.3 Bandwidth Allocation	22
Chapter 3: Implementation.....	23
3.1 Our Implementation	23
3.2 Network Devices and services	24
3.2.1 Device Configuration	24
3.2.2 L3 Switch Configuration.....	25
3.2.3 Firewall Configuration (PFSense).....	27
3.2.4 Server Configuration.....	32
3.2.5 Virtualization Configuration	37
3.2.6 Zabbix Configuration	42
3.2.7 NAS Configurations.....	45
3.2.8 Cloud Configuration.....	47
Chapter 4: Predicted problems and Solution.....	50
Chapter 5: Future Implementation	51
CONCLUSION.....	51
Chapter 6: References	52
Annexure 1: Floor plans and Network wiring.....	53
Annexure 2: Devices.....	58

LIST OF FIGURES

Number	Name	Page Number
1	Network diagram	08
2-6	Heat map	12-14
7-11	Server rack	15-17
12	Our Implementation	23
13	Packet tracer Diagram	24
14-17	L3 Main Switch Configuration	25
18-19	L3 Backup Switch Configurations	26
21-31	Firewall Configurations	27-31
32-34	OpenVPN Configuration	32
35-47	Server Configuration	32-36
48-60	Virtualization Configuration	37-41
61-67	Zabbix Configuration	42-44
68-72	NAS Configuration	45-46
73-78	Cloud Configuration	47-49
79-83	Floor plans	53-57
84-89	Devices	58-63

LIST OF TABLES

Table Number	Table Name	Page Number
1-4	Port table	10-12
5	IP table	18-19
6	Budget table	20-21
7	Bandwidth table	22

Chapter 1

1.1 INTRODUCTION

The Lumina University network design mainly focuses on specific needs, like the computer, science, and engineering departments and spans 5 floors. Balancing educational and other complex activities, the facility incorporates modern design, features redundancy for uninterrupted access, and contains advanced security technology. The design is also flexible and allows for additional future construction as Lumina University continues to grow.

1.2 Importance and Objectives

The computer, science, and engineering departments require specifically tailored infrastructure. This design focuses on reliability, security, and adaptability. This design also incorporates redundant connectivity, enhanced security, and focuses on sustainable, adaptable design construction. The end goal is to provide Lumina University students and faculty with a world-class educational experience. The primary purpose is to balance educational activities with Lumina University activities.

- Enhanced Academic Experience
- Efficient Collaboration
- Secure Information Environment
- Scalability for Growth
- High Availability and Reliability
- Competitive Edge

1.2.2 Project Implementation and Technologies Used

Core Network – PFsense Firewall

Handles routing, VLAN creation, DHCP service, setting firewall rules and OpenVPN configurations. All VLANs and sub-interfaces were created in PFsense, followed by each VLAN getting separate DHCP scope assignment. OpenVPN is configured to allow admins to securely connect to the DMZ for remote access to the servers.

Distribution Layer – Redundant MLS Switches

The Distribution Layer is in two MLS that have been configured for redundancy. Trunk links were created to carry all VLANs from the firewall, and access ports were used to distribute VLANs to different departments. In order to increase reliability, EtherChannels were used for link aggregation and used STP to prevent loops. All security hardening included encrypted passwords, SSH access, MOTD banners, and shutting down unused ports.

Access Layer – L2 Switches

In the Access Layer, Layer 2 switches are deployed to provide departmental VLANs to end users. The same security measures are used on the MLS (Secure Shell, encrypted passwords, Message of the Day, disabling unused ports) for this as well. This allows users to retrieve information in a streamlined manner.

Virtualization Environment

For the virtualization, we used two servers running VMware ESXi and one additional ESXi host for the Disaster Recovery (DR) site. In the DMZ, we provisioned several virtual machines, particularly the AD/DNS Server, the Zabbix Monitoring Server, the Veeam Backup Server, and other necessary services. An vCenter Appliance was used to manage all ESXi hosts in a datacenter cluster. Veeam was set up to perform virtual machine replication to the Disaster Recovery site, allowing for quick failover and continuous business operations.

Storing Data – Synology NAS

To provide shared storage, we deployed a Synology NAS. The LUNs were made and attached to the ESXi hosts through iSCSI protocol, enabling better centralization of stored VMs and higher performance. The NAS served to us, in our case, as shared SaaS storage.

Cloud Deployment – Integration of AWS

Deployment to the cloud was done using AWS, where we launched an EC2 instance to host the Lumina University LMS webpage. This serves as cloud elasticity and availability for the learning platform of the university.

Chapter 2: Network Design

2.1 Network Diagram

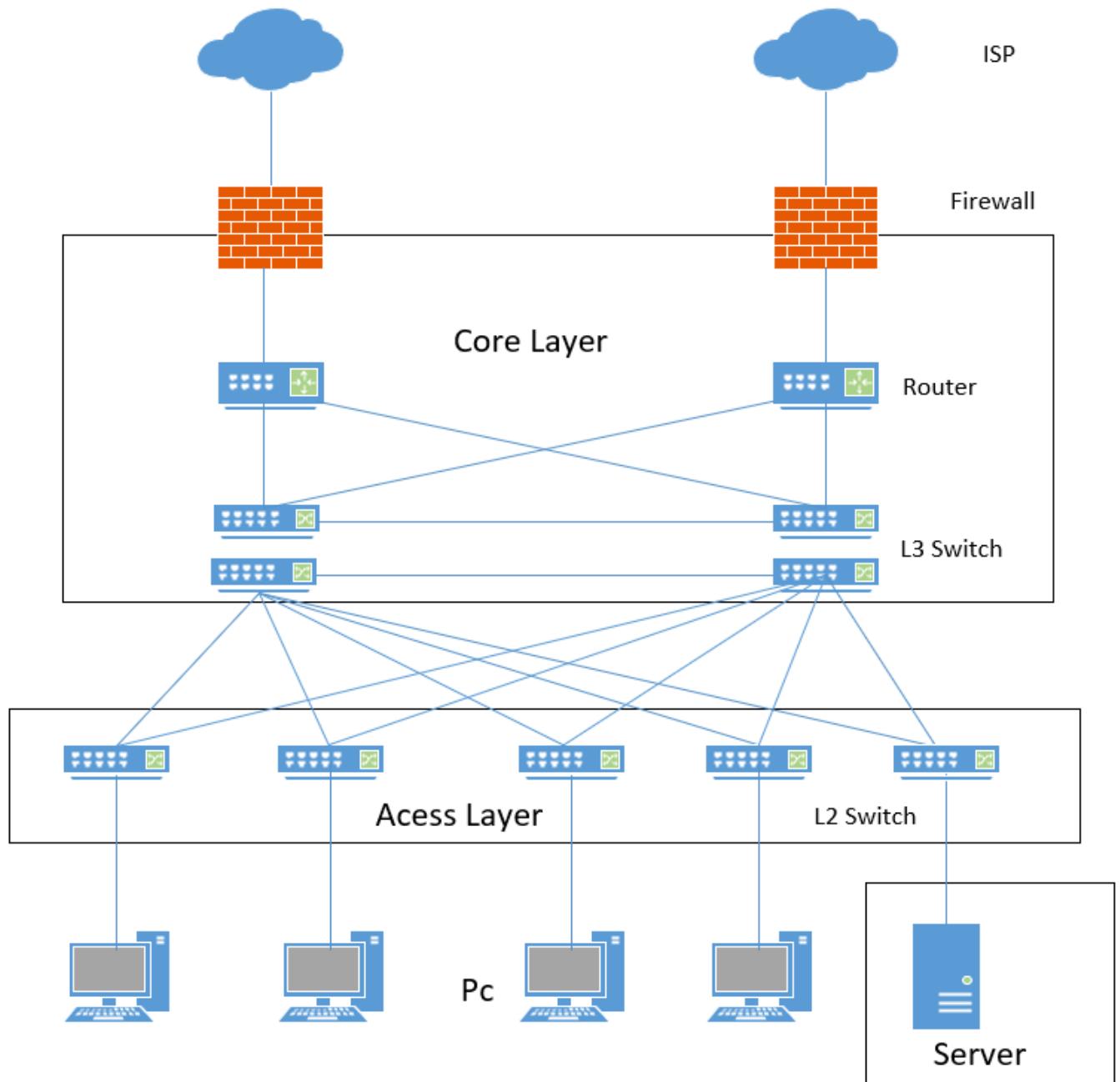


Figure 1

2.2 Port Table

Device	Interface	VLAN	Ip Address	Subnet Mask	Port status
L3 switch 1	G1/0/2	10	192.168.10.78	255.255.255.0	No shutdown
			192.168.10.94	255.255.255.0	No shutdown
			192.168.10.122	255.255.255.0	No shutdown
	G1/0/3	20	192.168.20.126	255.255.255.0	No shutdown
	G1/0/4	40	192.168.40.2	255.255.255.0	No shutdown
		20	192.168.20.190	255.255.255.0	No shutdown
	G1/0/5	20	192.168.20.222	255.255.255.0	No shutdown
			192.168.20.254	255.255.255.0	No shutdown
		10	192.168.10.94	255.255.255.0	No shutdown
	G1/0/6	10	192.168.10.30	255.255.255.0	No shutdown
			192.168.10.46	255.255.255.0	No shutdown
			192.168.10.62	255.255.255.0	No shutdown
			192.168.10.102	255.255.255.0	No shutdown
			192.168.10.110	255.255.255.0	No shutdown
			192.168.10.118	255.255.255.0	No shutdown
	G1/0/7		192.168.10.126	255.255.255.0	No shutdown
			192.168.10.134	255.255.255.0	No shutdown
	G1/0/8				Ether channel
	G1/0/9				
	G1/0/2	10	192.168.10.78	255.255.255.0	No shutdown
			192.168.10.94	255.255.255.0	No shutdown
			192.168.10.122	255.255.255.0	No shutdown
	G1/0/3	20	192.168.20.126	255.255.255.0	No shutdown
	G1/0/4	40	192.168.40.3	255.255.255.0	No shutdown

L3 switch (Backup)		20	192.168.20.190	255.255.255.0	No shutdown
	G1/0/5	20	192.168.20.222	255.255.255.0	No shutdown
			192.168.20.254	255.255.255.0	No shutdown
		10	192.168.10.94	255.255.255.0	No shutdown
	G1/0/6	10	192.168.10.30	255.255.255.0	No shutdown
			192.168.10.46	255.255.255.0	No shutdown
			192.168.10.62	255.255.255.0	No shutdown
			192.168.10.102	255.255.255.0	No shutdown
			192.168.10.110	255.255.255.0	No shutdown
			192.168.10.118	255.255.255.0	No shutdown
	G1/0/7	50	192.168.50.126	255.255.255.0	No shutdown
		50	192.168.50.134	255.255.255.0	No shutdown
	G1/0/8				Ether channel
	G1/0/9				

Table 1

Network type	L3 port	Ip address	Subnet mask	Firewall port	Ip address	Subnet mask	Port status
LAN 1 (Main)	G1/0/1	192.168.1.2	255.255.255.252	G0/1	192.168.1.3	255.255.255.252	
LAN 2	G1/0/1	192.168.2.2	255.255.255.0	G0/1	192.168.2.3	255.255.255.252	

Table 2

Network type	Firewall port	Ip address	Subnet mask	Isp router port	Ip address	Subnet mask	Port status
WAN 1 (Main)	G0/0	192.168.18.11	255.255.255.0	G0/0	192.168.18.12	255.255.255.0	
WAN 2	G0/0	203.143.38.1	255.255.255.0	G0/0	203.143.38.2	255.255.255.0	
	G0/2						shutdown

Table 3

Floor	Device	Vlan	Usable port range	Port Status
Ground	GS1	10	F0/1-10	
			F0/11-14	
			F0/15-16	
			F0/24-48	Shutdown
First Floor	F1S1	20	F1/0/1-48	
	F1S2		F2/0/1-37	
	F1S3		F2/0/38-48	Shutdown
			F3/0/8-24	Shutdown
Second Floor	F2S1	30	F1/0/1-48	
	F2S2		F2/0/1-48	
	F2S3		F3/0/1-48	
	F2S4		F4/0/1-48	
	F2S5		F5/0/1-33	
		20	F5/0/34-48	
			F6/0/1-25	
			F6/0/26-48	Shutdown
	F2S6		F7/0/8-24	Shutdown
	F2S7			
Third Floor	F3S1	20	F1/0/1-15	
			F1/0/16-35	
			F1/0/36-39	
			F1/0/40-48	Shutdown
	F3S2	10	F2/0/8-24	Shutdown
Fourth Floor	F4S1	20	F1/0/1-21	
			F1/0/22-31	
			F1/0/32-41	
			F1/0/42-46	
			F1/0/47-48	
		F4S2	F2/0/1-3	
			F2/0/4-8	
			F2/0/16-48	
				Shutdown
CCTV	CS1	40	F1/0/1-48	
	CS2		F2/0/1-43	
			F2/0/44-48	Shutdown
	CS3		F3/0/1-24	Shutdown
			F0/5-8	Shutdown
Access Point	GS1	50	F0/17-23	
	F1S3		F1/0/1-7	
	F2S7		F7/0/1-7	
	F3S2		F2/0/1-7	
	F4S2		F2/0/9-15	

Table 4

2.3 Heat Map

- 2.4 GHz band used
- Blue -Least Coverage Area
- Red -High Coverage Area

Ground floor

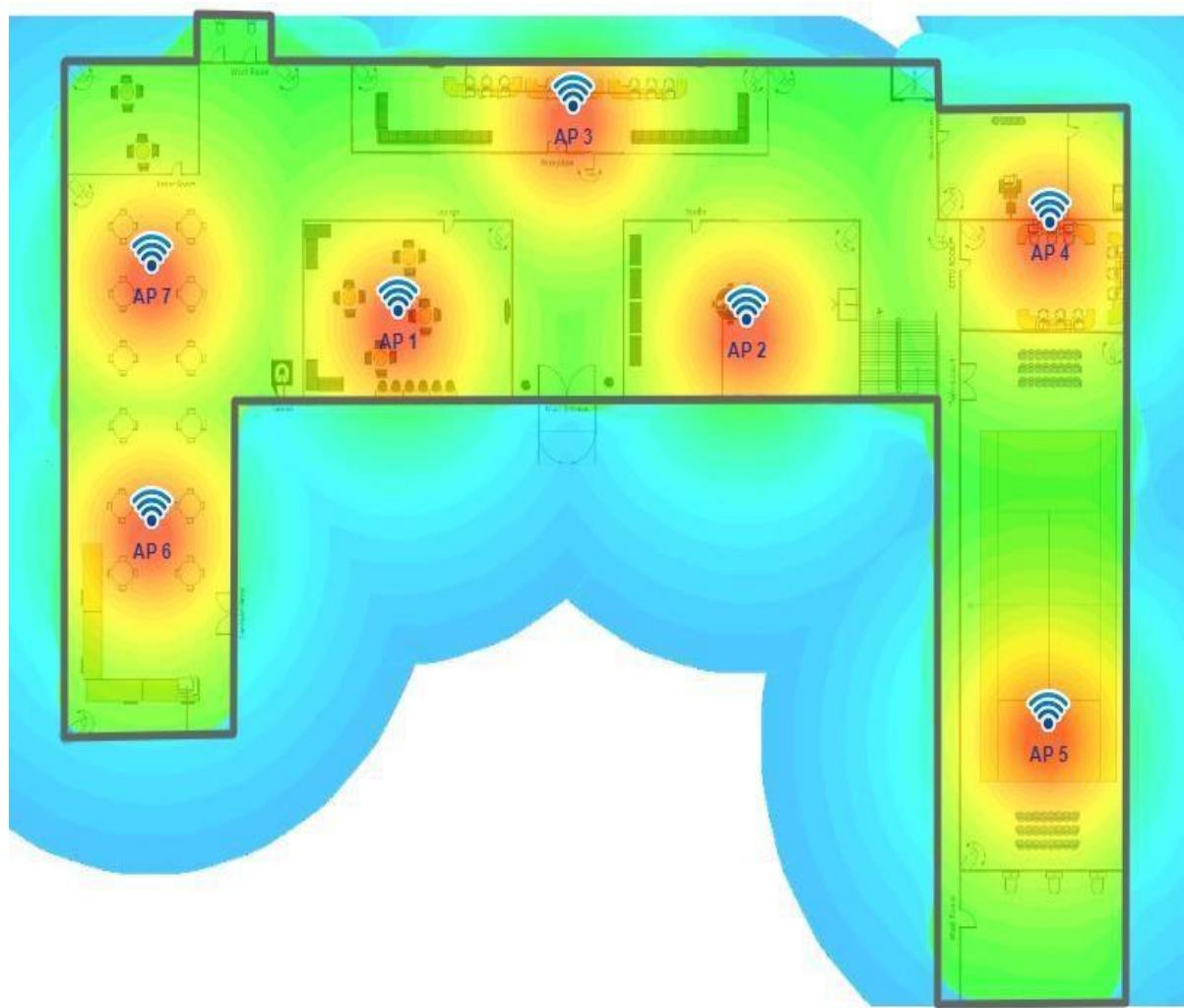


Figure 2

1st Floor

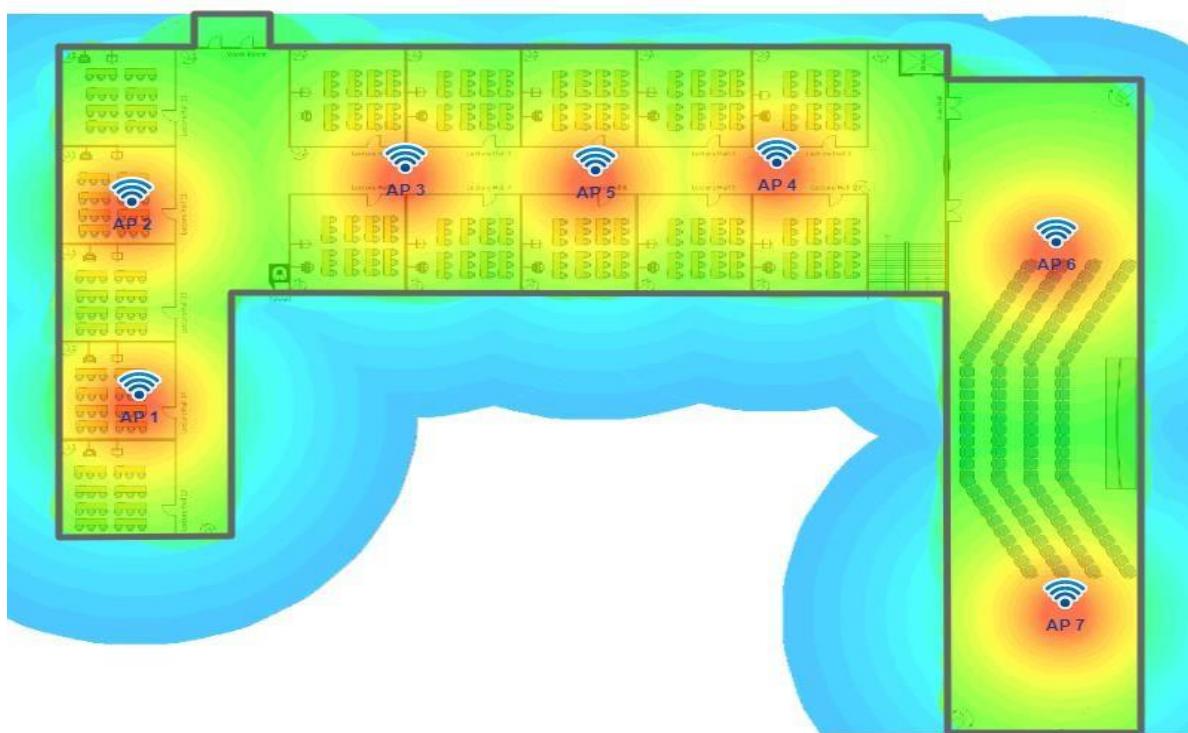


Figure 3

2nd Floor

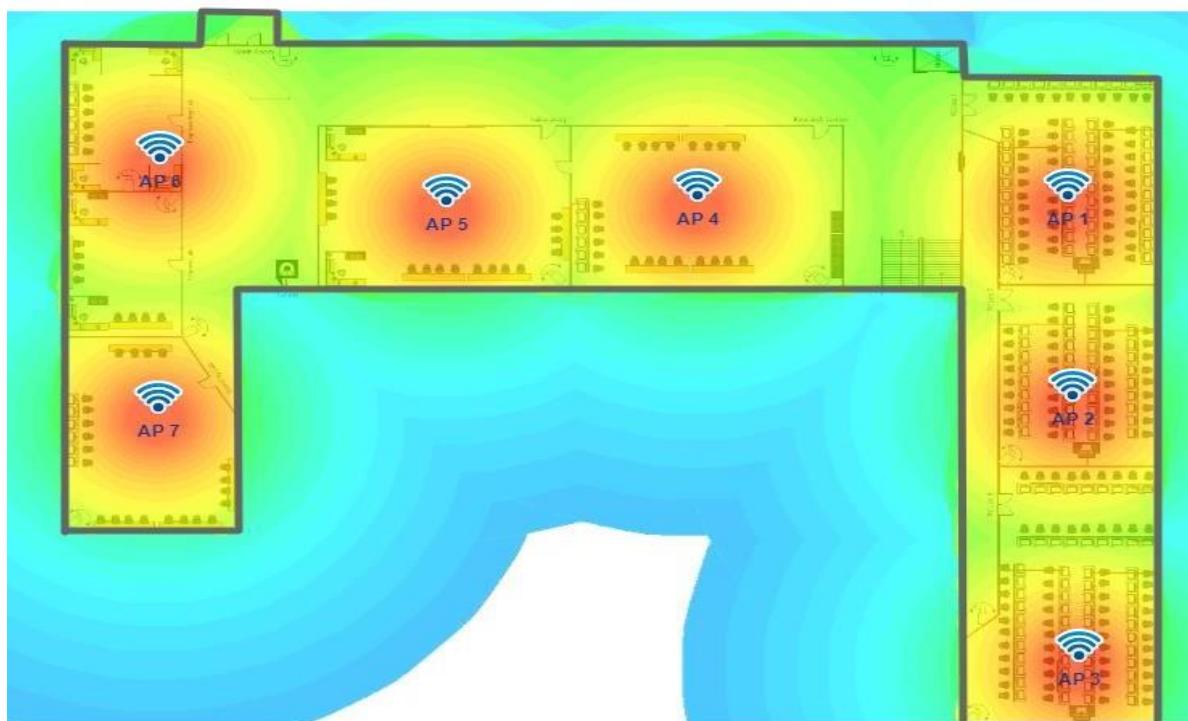


Figure 4

3rd Floor

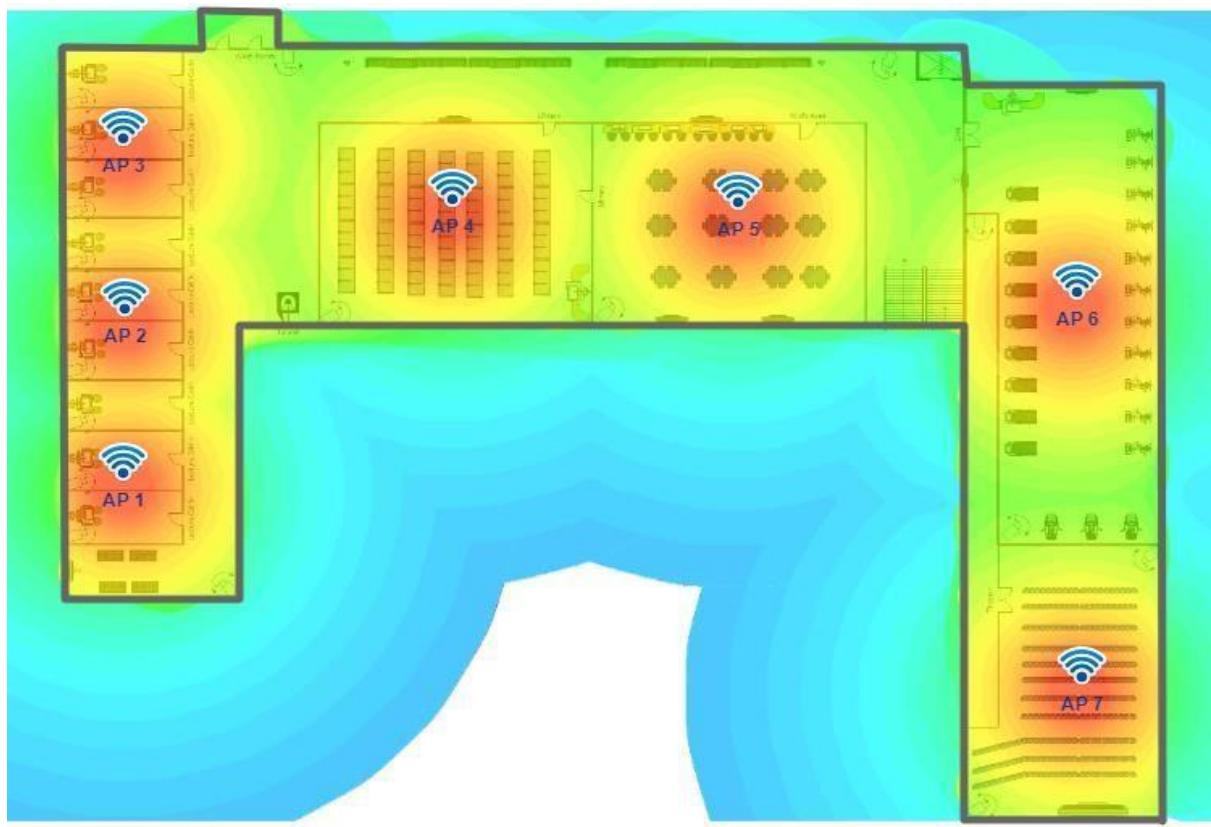


Figure 5

4th Floor

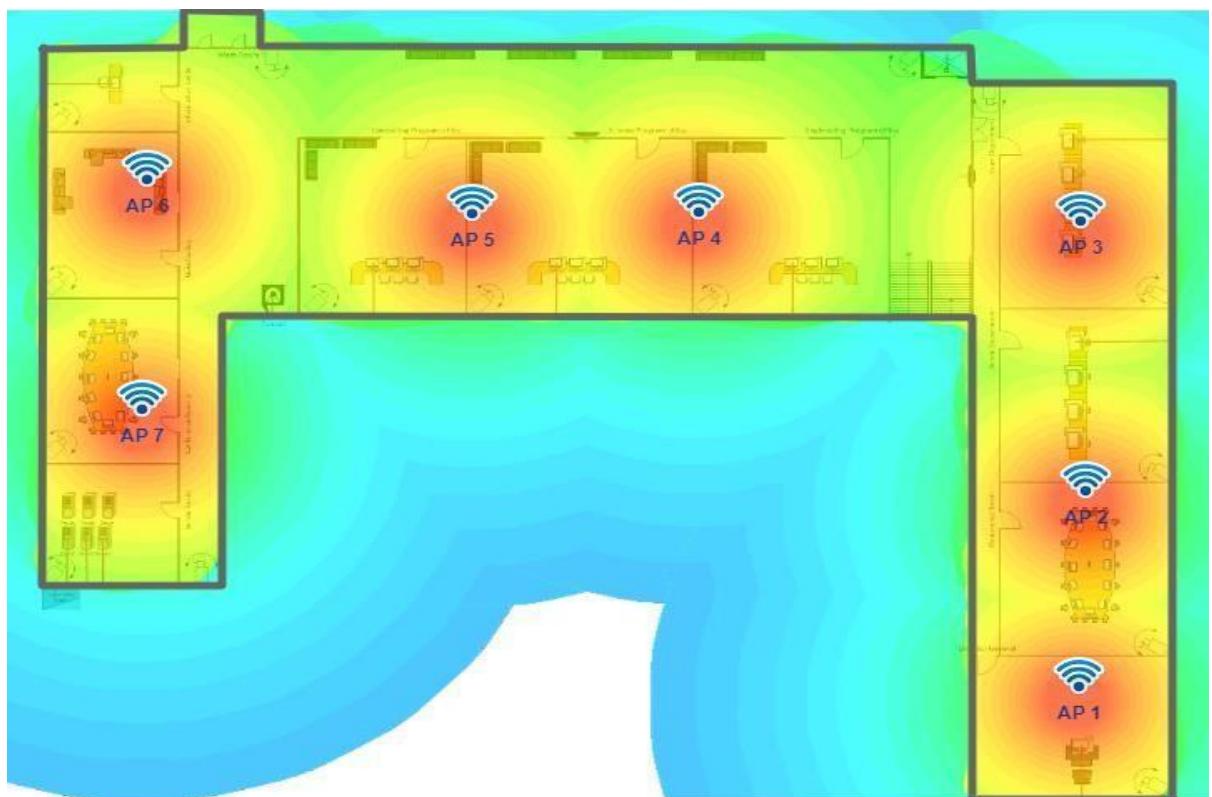


Figure 6

2.4 Server Cabinets

Main Server Rack

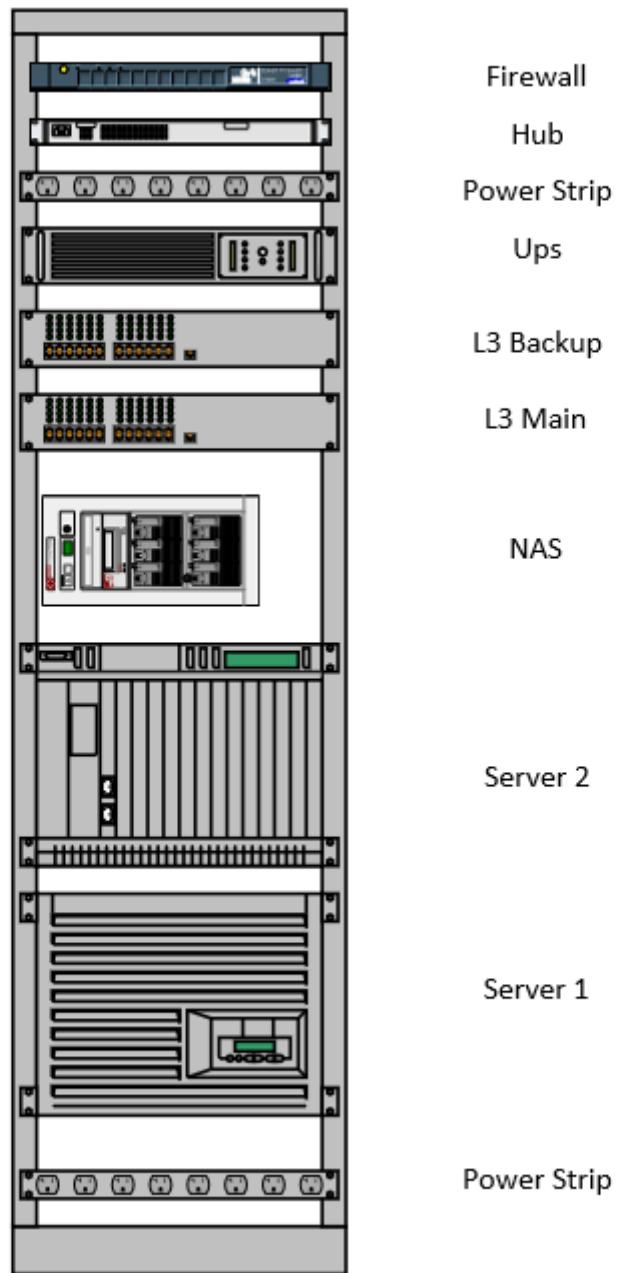
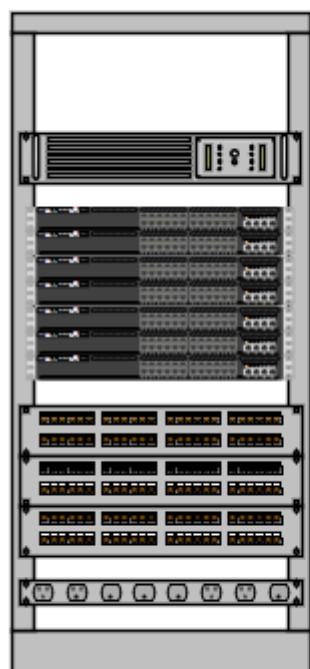


Figure 7

Ground Floor Server Rack



Ups

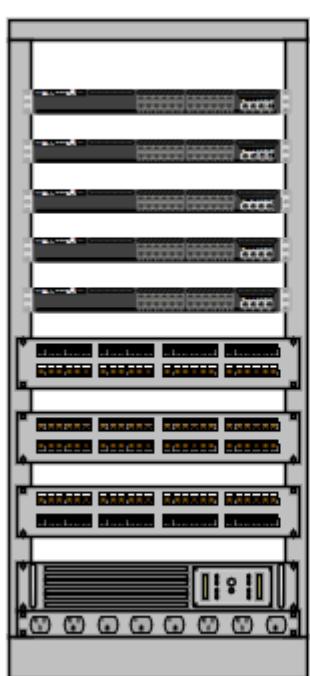
L2 Switch X 7

Patch panel

Power Strip

Figure 8

1st Floor Server Rack



L2 Switch

L2 Switch

L2 Switch

L2 Switch

L2 Switch

Patch panel

Patch panel

Patch panel

Ups

Power Strip

Figure 9

2nd Floor Server Rack

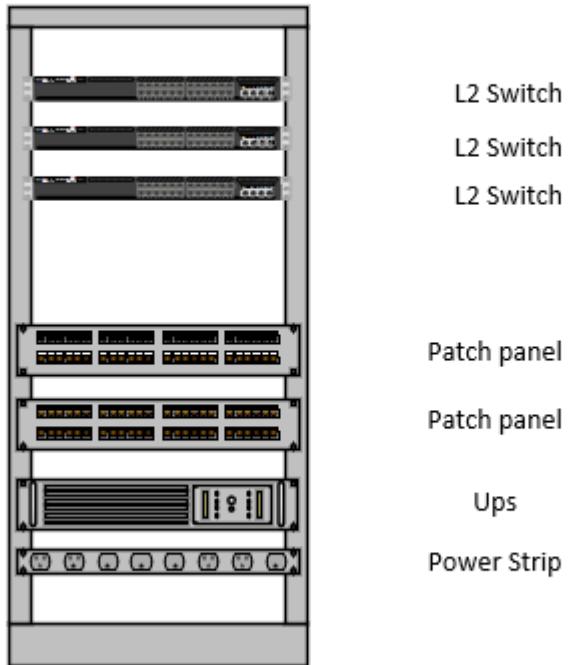


Figure 10

3rd Floor Server Rack

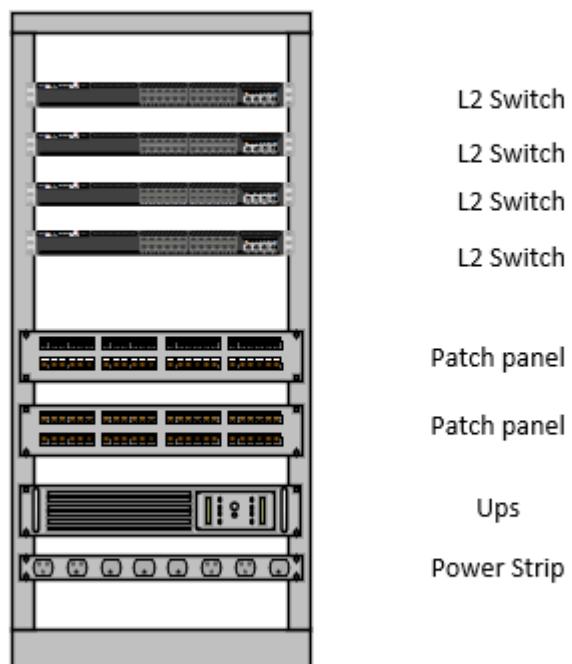


Figure 11

2.5 Other Tables

2.5.1 IP Table

Floor	Department Name	VLA N	Host Needed	Host Available	Network Address	Subnet mask	Usable Ip Range
Ground Floor	Studio	10	10	4	192.168.10.0	255.255.255.0	192.168.10.65-192.168.10.74
	Reception + Information center		4	2			192.168.10.89-192.168.10.92
	Sick room		2	0			192.168.10.121-192.168.10.122
1 st floor	Classroom	20	30	35	192.168.2.0	255.255.255.0	192.168.20.1-192.168.20.85
	Pc classroom		50				
	Auditorium		5				
2 nd floor	Pc Lab	30	225	27	192.168.30.0	255.255.255.0	192.168.30.1-192.168.30.225
	laboratory	20	10	20	192.168.20.0	255.255.255.0	192.168.20.129-192.168.20.168
	Science Lab		10				
	Engineering Lab		10				
	Standby Lab		10				
3 rd floor	Lectures	20	15	15	192.168.20.0	255.255.255.0	192.168.20.193-192.168.20.207
	Library		20	10	192.168.20.0	255.255.255.0	192.168.20.225-192.168.20.244
	Theater	10	4	2	192.168.10.0	255.255.255.0	192.168.10.89-192.168.10.92
	Gym						
4 th floor	Administrator	20	20	9	192.168.20.0	255.255.255.0	192.168.20.1-192.168.20.21
	Director		1				
	Conference Room		10	4			192.168.20.33-192.168.20.42
	Exam Department		10	4			192.168.20.49-192.168.20.58
	Computing program office		5	1			192.168.20.97-192.168.20.101
	Science program office		5	1			192.168.20.105-192.168.20.209-
	Engineer program office		5	1			192.168.20.113-192.168.20.117

	CCTV room	40	120(CCT V) 10(pc)	115	192.168. 40.0	255.255. 255.0	192.168.40.11- 192.168.40.140
	Wireless users	50	254	-	192.168. 50.0	255.255. 255.0	192.168.50.1- 192.168.50.254
	DNS sever	40	1	6	192.168. 40.0	255.255. 255.0	192.168.40.241- 192.168.40.242
	Web server		1				
	Email server		1				

Table 5

2.5.2 Budget Table

Device	Equipment	Model	Qty	Unit Price	Total Price
Firewall	Netgate	Netgate 8200	1	\$1,549	\$1,549
Cloud Hosting	AWS	EC2 t2 small instance (2GB RAM)	1	\$15.30	\$15.30
Layer 3 switch	Cisco catalyst 9300	C9300-24T-A	2	\$5,900	\$11,800
	Power Supply	PWR-C1-350WAC-P/2	2	\$769	\$1,538
	Redundant Power Supply	PWR-C1-350WAC-P/2	2	\$769	\$1,538
	IP Services Electronic RTU License	C9300-DNA-A-24-3Y	2	\$1,248	\$2,496
	Redundant cooling Fans	Fan-T2	6	\$518	\$3,108
	Console Cable	USB Console Cable USB to RJ45	2	\$15	\$30
Layer 2 switch	CISCO SYSTEMS	Switch (SF110D08NA)	1	\$109	\$109
	Cisco catalyst 2960 PoE	WS-C2960+24PC-S	4	\$2,800	\$11,200
	Cisco catalyst 9200 PoE	C9200L-24P-4X-E	14	\$5,660	\$79,240
	Console cable	USB Console Cable USB to RJ45	10	\$15	\$150
	Patch panel	ICC CAT6 Patch Panel with 48 Ports and 2 RMS	14	\$169	\$2,366
		Wallmount 24-Port Cat6 Patch Panel RJ45	3	\$46	\$138
CCTV Equipment	Ip camera	DS-2CD2143G0-I	88	\$95	\$8,360
	NVR	DAHUA DHI-NVR2104HS-4KS2	1	\$106	\$106
	Power Distribution Unit	Hardy Rack Power Strip, Surge Protector 4 Socket	1	\$20	\$20
	HDD for NVR	8TB Internal Hard Drive HDD	3	\$170	\$510
Access point	WLAN controller	AIR-CT3504-K9	1	\$5,816	\$5,816
	Cisco 9100 access point	C9115AXE-H	35	\$844	\$29,540
Cable	Copper straight Through	CAT6E1M	100	\$2	\$200
		CAT6E10M	50	\$5	\$250
		CAT6E20M	100	\$8	\$800

server	Cable Managers-vertical	32611-E02	1	\$1,500	\$1,500
	Power Distribution unit	Rackmount PDU with 8 Outlets and Surge Protection	2	\$100	\$200
	Cable Ties	500 Pack Cable Tie	1	\$15	\$15
	Fan Kit	3U Triple Fan Kit, 3x 115 CFM	3	\$150	\$450
	UPS	AWP APO3000RT 3KVA RACK	1	\$500	\$500
	Servers	Cisco UCS C220 M6	3	\$6,830	\$20,420
	KVM switch with a monitor	17-inch LCD KVM Switch	1	\$1,800	\$1,800
	Power Cords	6ft premium universal power code	8	\$12	\$96
	WLAN Controllers cisco	Cisco Catalyst 9800-L	1	\$11,830	\$11,830
	Server Rack enclosure	9u AcoustiQuiet Desktop Server Rack	1	\$1,900	\$1,900
Cabinets	Wall Mount Rack	6U Wall Mount Network Rack	5	\$30	\$150
	Power Distribution Unit	MASS RACK Power Strip 6 Socket	6	\$10	\$60
PC	Hp desktop pc	EliteOne 800 G3 AIO	370	\$200	\$73,400
laptop	Hp laptop	Elitebook 840 G5	75	\$310	\$23,250
TV	VIZIO TV	40-inch D-Series Full HD 1080p Smart TV	12	\$168	\$2,016
Projector		GP - 12 LED Projector Support 1080P	20	\$59	\$1,180
		GP90 Portable LED Projector 3200LMS HD projector LCD	1	\$121	\$121
Smart Whiteboard	FITOUCHE Interactive Whiteboard	FIT-TBI94D	15	\$274	\$4,110

Table 6

Total budget = \$303877.2

2.5.3 Bandwidth Allocation

Department	Users	Bandwidth (MBps)	Total Band. (MBps)	Backup Bandwidth (MBps)	Total Backup (MBps)
CCTV	88	3	264	.5	44
Wi-fi	1024	3	3072	.5	512
Labs	265	70	18480	5	1325
Staff Cabins	15	50	750	1	15
Library	20	10	200	1	20
Lecture halls	30	40	1200	2	60
Program office	10	10	100	1	10
Administrator and Director	21	40	840	2	42
Reception	3	10	30	1	3
Server and CCTV rooms	8	70	560	5	40
Auditorium	5	5	25	0.5	3
Programming office	15	10	150	1	15
Studio	10	10	100	1	10

Table 7

- Bandwidth measures using Mbps
- We Recommended 25800 Mbps as main ISP bandwidth.
- And Secondary ISP Bandwidth as 25000 Mbps.

Chapter 3: Implementation

3.1 Our Implementation



Figure 12- Our WorkSpace

3.2 Network Devices and services

3.2.1 Device Configuration

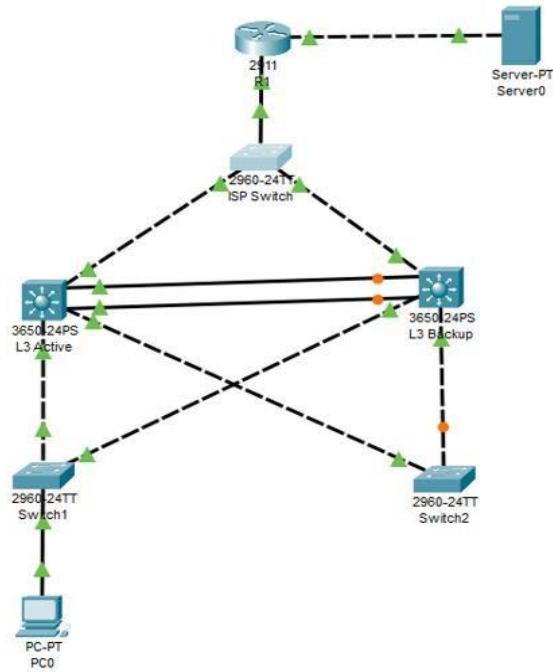


Figure 13

Figure 13 (The PacketTracer Diagram We Implement on Lab)

Our Implementation has been Configured with real time and by troubleshooting.

As stated, the Campus uses two lease lines from different ISPs as primary and backup Also, its Domain base authentication and high security. Therefore, Wireless access for all users by our DHCP server.

3.2.2 L3 Switch Configuration

The Below screenshots shows Main L3 switch Configurations

```
interface Vlan10
description Student
ip address 192.168.10.1 255.255.255.0
ip helper-address 192.168.1.3
!
interface Vlan20
description Staff
ip address 192.168.20.1 255.255.255.0
ip helper-address 192.168.1.3
!
interface Vlan30
description IT
ip address 192.168.30.1 255.255.255.0
ip helper-address 192.168.1.3
!
interface Vlan40
description DMZ
ip address 192.168.40.1 255.255.255.0
ip helper-address 192.168.1.3
!
interface Vlan50
description management
ip address 192.168.50.1 255.255.255.0
!
interface Vlan60
description DR
ip address 192.168.60.1 255.255.255.0
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip ssh version 2
```

Figure 17- Vlans Interface

```
crypto pki trustpoint TP-self-signed-2658623008
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-2658623008
revocation-check none
rsakeypair TP-self-signed-2658623008
!
!
crypto pki certificate chain TP-self-signed-2658623008
!
license boot level ipservicesk9
diagnostic bootup level minimal
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
username pearlwave password 7 0014160716571C071924
username admin secret 5 $1$a7iB$u8zwzFZvicEJP/JC49RfJ.
!
redundancy
mode sso
!
!
```

Figure 16- Passwords and Crypto Key

```
!
interface Port-channel1
switchport mode trunk
!
interface GigabitEthernet0/0
vrf forwarding Mgmt-vrf
no ip address
negotiation auto
!
interface GigabitEthernet1/0/1
switchport mode trunk
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/0/3
switchport access vlan 40
switchport mode access
!
interface GigabitEthernet1/0/4
switchport access vlan 40
switchport mode access
!
interface GigabitEthernet1/0/5
switchport access vlan 40
switchport mode access
!
interface GigabitEthernet1/0/6
switchport access vlan 40
switchport mode access
!
interface GigabitEthernet1/0/7
switchport access vlan 50
switchport mode access
!
interface GigabitEthernet1/0/8
switchport access vlan 50
switchport mode access
!
interface GigabitEthernet1/0/9
switchport access vlan 40
switchport mode access
!
interface GigabitEthernet1/0/10
switchport access vlan 50
switchport mode access
!
interface GigabitEthernet1/0/11
switchport access vlan 10
switchport mode access
!
```

Figure 15-Port Channel and Access Vlan

```
line con 0
password 7 0723344147071825464058
login
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
```

Figure 14- SSH

The Below screenshots shows Backup L3 switch Configurations

```
!
banner motd ^C=====
    W E L C O M E   T O   L U M I N A   U N I V E R S I T Y
=====
        Authorized Access Only!

    This system is the property of Lumina University
    Access is restricted to authorized users and personnel.

    Unauthorized access or use is strictly prohibited and may result
    in disciplinary action and/or legal prosecution.

        All activities are monitored and logged.
=====
^C
!
line con 0
password 7 0723344147071825464058
login
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  login local
  transport input ssh
line vty 5 15
  login local
  transport input ssh
!
!
wsma agent exec
!
wsma agent config
!
wsma agent filesys
!
wsma agent notify
!
!
```

Figure 19- Banner and SSH

VLAN	Name	Status	Ports
1	default	active	Gi1/0/1, Gi1/0/2, Gi1/1/1 Gi1/1/2, Gi1/1/3, Gi1/1/4
10	student	active	Gi1/0/11, Gi1/0/12, Gi1/0/13 Gi1/0/14
20	staff	active	Gi1/0/15, Gi1/0/16, Gi1/0/17 Gi1/0/18
30	IT	active	Gi1/0/21, Gi1/0/22, Gi1/0/23
40	DMZ	active	Gi1/0/3, Gi1/0/4, Gi1/0/5 Gi1/0/6, Gi1/0/9
50	manage	active	Gi1/0/7, Gi1/0/8, Gi1/0/10
60	DR	active	
1002	fdmi-default	act/unsup	
1003	token-ring-default	act/unsup	

Figure 18- Vlan Brief

3.2.3 Firewall Configuration (PFSense)

The Below screenshots shows Firewall DHCP Configurations

This screenshot shows the 'General DHCP Options' configuration for the 'STUDENT' interface. The 'Enable' checkbox is checked, and the 'Subnet' is set to 192.168.10.0/24. The 'Address Pool Range' is defined from 192.168.10.10 to 192.168.10.254.

General DHCP Options	
DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on STUDENT interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<input type="button" value="Allow all clients"/>
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to All interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address with	
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address server behavior violates the official DHCP specification.
Primary Address Pool	
Subnet	192.168.10.0/24
Subnet Range	192.168.10.1 - 192.168.10.254
Address Pool Range	From 192.168.10.10 To 192.168.10.200

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Figure 21- Student DHCP Pool

This screenshot shows the 'General DHCP Options' configuration for the 'STAFF' interface. The 'Enable' checkbox is checked, and the 'Subnet' is set to 192.168.20.0/24. The 'Address Pool Range' is defined from 192.168.20.10 to 192.168.20.254.

General DHCP Options	
DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on STAFF interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<input type="button" value="Allow all clients"/>
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to All interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address with	
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address server behavior violates the official DHCP specification.
Primary Address Pool	
Subnet	192.168.20.0/24
Subnet Range	192.168.20.1 - 192.168.20.254
Address Pool Range	From 192.168.20.10 To 192.168.20.200

Figure 20- Staff DHCP Pool

DNS Servers	8.8.8
	192.168.40.10
	DNS Server 3
	DNS Server 4
MAPI	
OMAPI Port	OMAPI Port
Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable. Only the first OMAPI configuration is used.	
OMAPI Key	OMAPI Key
Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.	
<input type="checkbox"/> Generate New Key	
Generate a new key based on the selected algorithm.	
Key Algorithm	HMAC-SHA256 (current bind9 default)
Set the algorithm that OMAPI key will use.	
Other DHCP Options	
Gateway	192.168.10.3
The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct network. Enter "none" for no gateway assignment.	
Domain Name	lumina.local
The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.	

Figure 24-DNS and DHCP Configuration

Interfaces / Interface Assignments	
Interface	Network port
WAN	re1 (30:5a:3a:0e:27:52)
LAN	re0 (18:d6:c7:06:88:06)
Student	VLAN 10 on re0 - lan (Student)
Staff	VLAN 20 on re0 - lan (Staff)
IT	VLAN 30 on re0 - lan (IT)
DMZ	VLAN 40 on re0 - lan (DMZ)
MANGEMENT	VLAN 50 on re0 - lan (MANGEMENT)
OPT6	ovpn1 (OpenVPN_Client_To_Site)
DR	VLAN 60 on re0 - lan (DR)

Figure 23- Interfaces

CPU Type	Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz Current: 3104 MHz, Max: 3400 MHz 8 CPUs: 1 package(s) x 4 core(s) x 2 hardware threads AES-NI CPU Crypto: Yes (Inactive) QAT Crypto: No	<ul style="list-style-type: none"> Netgate Global Support FAQ Official pfSense Training by Netgate Netgate Professional Services Visit Netgate.com <p>If you decide to purchase a Netgate Global TAC Support subscription, you MUST have your Netgate Device ID (NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports here.</p>
Hardware crypto	Inactive	
Kernel PTI	Enabled	
MDS Mitigation	Inactive	
Uptime	3 Days 01 Hour 16 Minutes 37 Seconds	
Current date/time	Mon Oct 27 16:27:16 +0530 2025	
DNS server(s)	<ul style="list-style-type: none"> 192.168.2.5 8.8.8 8.8.4.4 192.168.40.10 	
Last config change	Mon Oct 27 16:25:49 +0530 2025	
State table size	0% (321/801000) Show states	
MBUF Usage	2% (21590/1000000)	
Temperature	27.9°C	
Load average	0.30, 0.16, 0.11	
CPU usage	0%	
Memory usage	10% of 8016 MiB	
SWAP usage	0% of 1024 MiB	

Interfaces

WAN	100baseT <full-duplex>	192.168.18.11
LAN	100baseTX <full-duplex>	192.168.1.3
STUDENT	100baseTX <full-duplex>	192.168.10.3
STAFF	100baseTX <full-duplex>	192.168.20.3
IT	100baseTX <full-duplex>	192.168.30.3
DMZ	100baseTX <full-duplex>	192.168.40.3
MANGEMENT	100baseTX <full-duplex>	192.168.50.3
DR	100baseTX <full-duplex>	192.168.60.3

OpenVPN

OpenVPN_Client_To_Site UDP4:1194 (1)	
Name/Time	Real/Virtual IP
sysadmin	172.16.101.69:34343
2025-10-27 15:55:58	10.8.0.3

Figure 22- PfSense Dashboard

The Below screenshots shows Firewall Rules Configurations (PFSense)

Floating	WAN	LAN	STUDENT	STAFF	IT	DMZ	MANGEMENT	DR	OpenVPN		
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
<input type="checkbox"/>	✓ 0/47.96 MiB	IPv4 *	*	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	192.168.18.11	1194 (OpenVPN)	*	none		Allow OpenVPN incoming's	
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	WAN address	*	*	*	*	none		Default allow LAN to any rule	

Figure 25- WAN Rules

Floating	WAN	LAN	STUDENT	STAFF	IT	DMZ	MANGEMENT	DR	OpenVPN		
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/4.41 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 0/278.95 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Figure 26- LAN Rules

Floating	WAN	LAN	STUDENT	STAFF	IT	DMZ	MANGEMENT	DR	OpenVPN		
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	STAFF subnets	*	This Firewall (self)	80 (HTTP)	*	none		Firewall block For Staff	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	STAFF subnets	*	DMZ subnets	*	*	none		Firewall block for Staff	
<input checked="" type="checkbox"/>	✓ 0/786 B	IPv4 *	STAFF subnets	*	*	*	*	none		ANY	

Figure 27- Staff Rules

Floating	WAN	LAN	STUDENT	STAFF	IT	DMZ	MANGEMENT	DR	OpenVPN		
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 6/3.26 GiB	IPv4 *	DMZ subnets	*	MANGEMENT subnets	*	*	none		Default allow LAN IPv6 to any rule	
<input type="checkbox"/>	✓ 16/7.75 GiB	IPv4 *	DMZ subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Figure 28- DMZ Rules

Floating	WAN	LAN	STUDENT	STAFF	IT	DMZ	MANGEMENT	DR	OpenVPN		
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/32 KiB	IPv4 *	STUDENT subnets	*	DMZ subnets	*	*	none		block DMZ server	
<input type="checkbox"/>	✗ 0/780 B	IPv4 TCP	STUDENT subnets	*	This Firewall (self)	80 (HTTP)	*	none		Firewall block For Students	
<input type="checkbox"/>	✓ 0/189.30 MiB	IPv4 *	STUDENT subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Figure 29- Student Rules

Floating	WAN	LAN	STUDENT	STAFF	IT	DMZ	MANGEMENT	DR	OpenVPN		
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 25/3.34 GiB	IPv4 *	DR subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	DR subnets	*	DMZ subnets	*	*	none		Default allow LAN IPv4 to any rule	

Figure 30- DR Rules

Floating	WAN	LAN	STUDENT	STAFF	IT	DMZ	MANGEMENT	DR	OpenVPN		
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/20.13 MiB	IPv4 *	10.8.0.0/24	*	DMZ subnets	*	*	none		DMZ access	
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	10.8.0.0/24	*	*	*	*	none		Allow all VPN client traffic	
		Add	Add	Delete	Toggle	Copy	Save	Separator			

Figure 31- OpenVPN Rules

The Below screenshots shows VPN Configurations (PFSense)

Installed Packages	Available Packages		
Installed Packages			
Name	Category		
✓ freeradius3	net		
		0.15.10_1	A free implementation of the RADIUS protocol. Supports MySQL, PostgreSQL, LDAP, Kerberos.
			Package Dependencies:
			bash-5.2.15 freeradius3-3.2.3 python311-3.11.6
✓ openvpn-client-export	security		
		1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.
			Package Dependencies:
			openvpn-client-export-2.6.7 openvpn-2.6.8_1 zip-3.0_1 7-zip-23.01

Figure 32- OpenVPN Installed Packages

Enter a search string or *nix regular expression to search certificate names and distinguished names.					
Certificate Authorities					
Name	Internal	Issuer	Certificates	Distinguished Name	In Use
OpenVPN-CA	✓	self-signed	3	CN=pfSense-ca, C=LK	
				Valid From: Sun, 26 Oct 2025 10:05:30 +0530	
				Valid Until: Wed, 24 Oct 2035 10:05:30 +0530	

Figure 33- Certificate Authorities

Users	Groups	Settings	Authentication Servers
Users			
Username	Full name	Status	Groups
<input type="checkbox"/> admin	System Administrator	✓	admins
<input type="checkbox"/> navod		✓	
<input type="checkbox"/> sysadmin		✓	

Figure 34- VPN Users

3.2.4 Server Configuration

The Below screenshots shows DNS AD Configurations

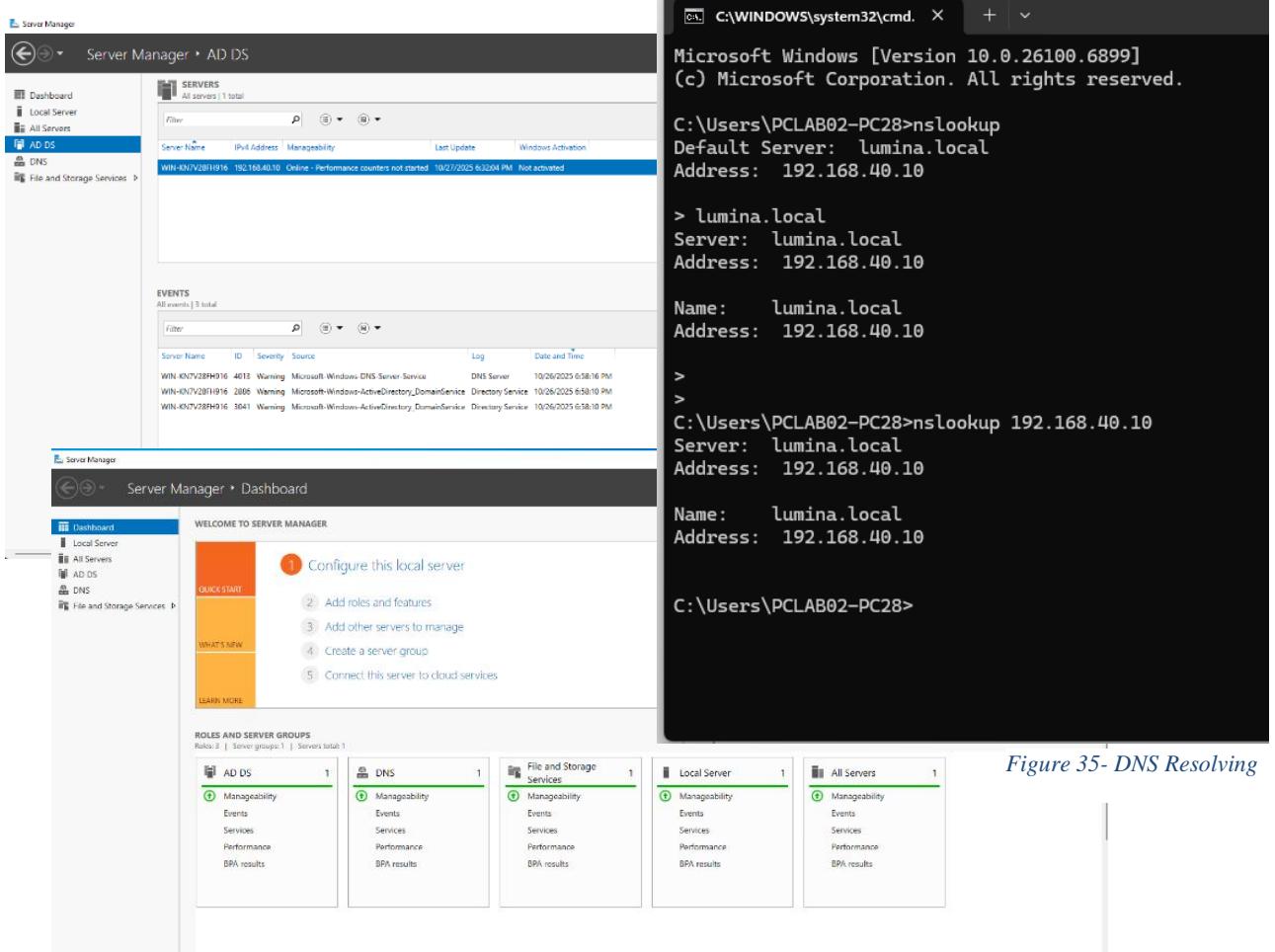


Figure 35- DNS Resolving

Figure 36- Server Manage Dashboard

The Below screenshots shows VCenter Server 1 Configurations

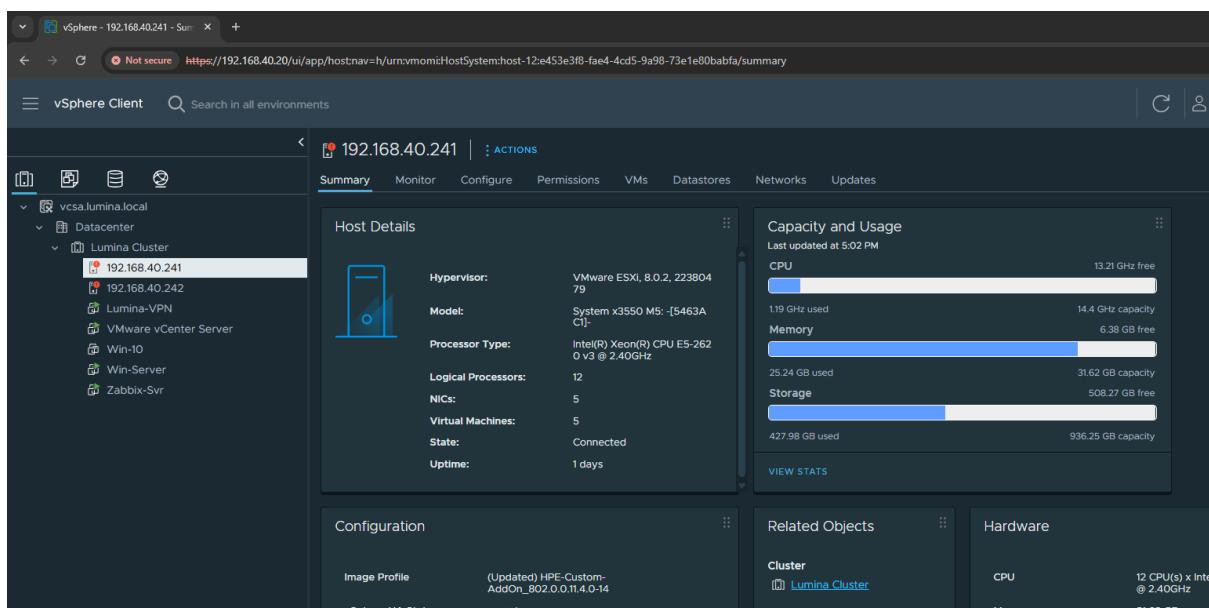


Figure 37- Server Summary

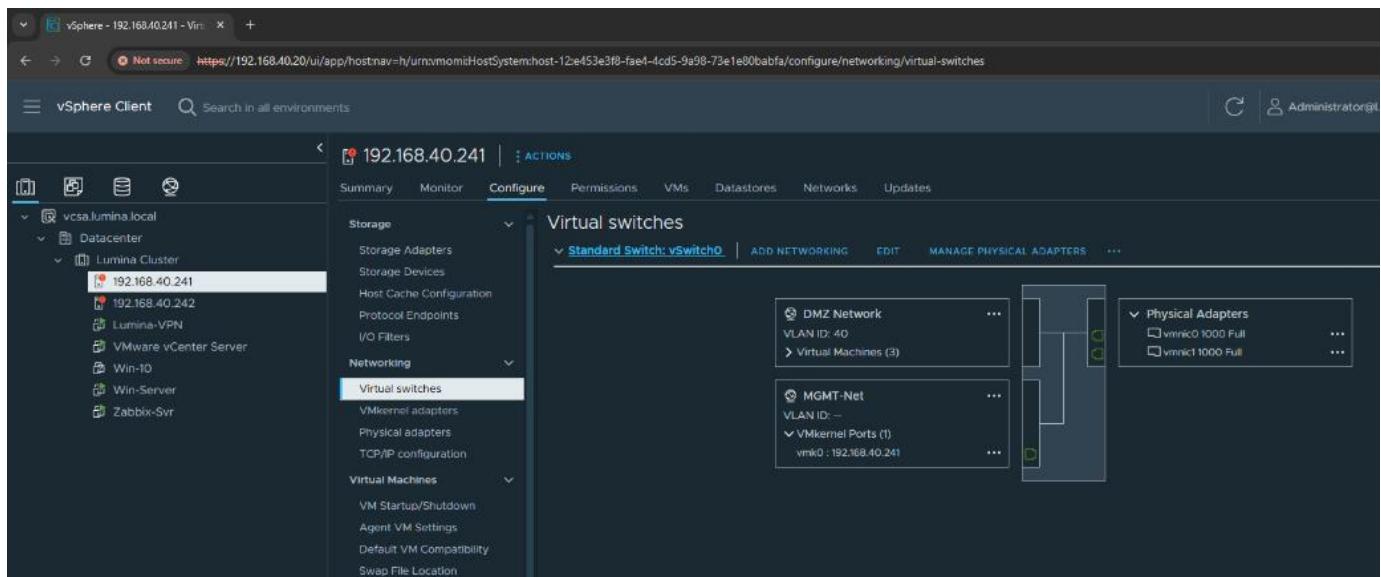


Figure 38- Virtual Switches

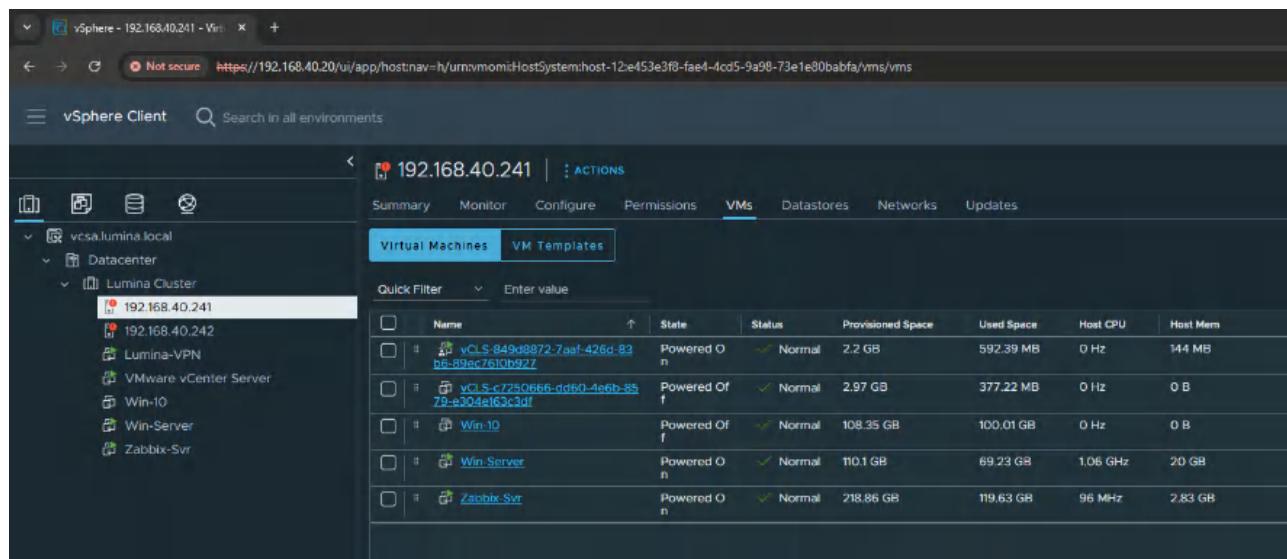


Figure 39- Virtual Machines

The Below screenshots shows Vcenter Server 2 Configurations

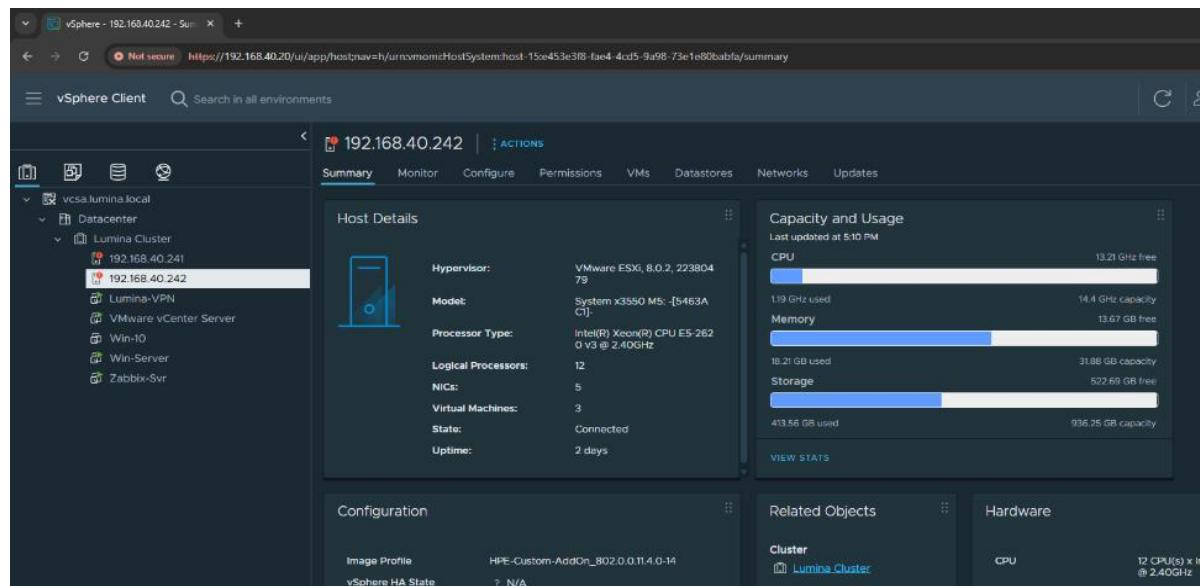


Figure 40- Server Summary

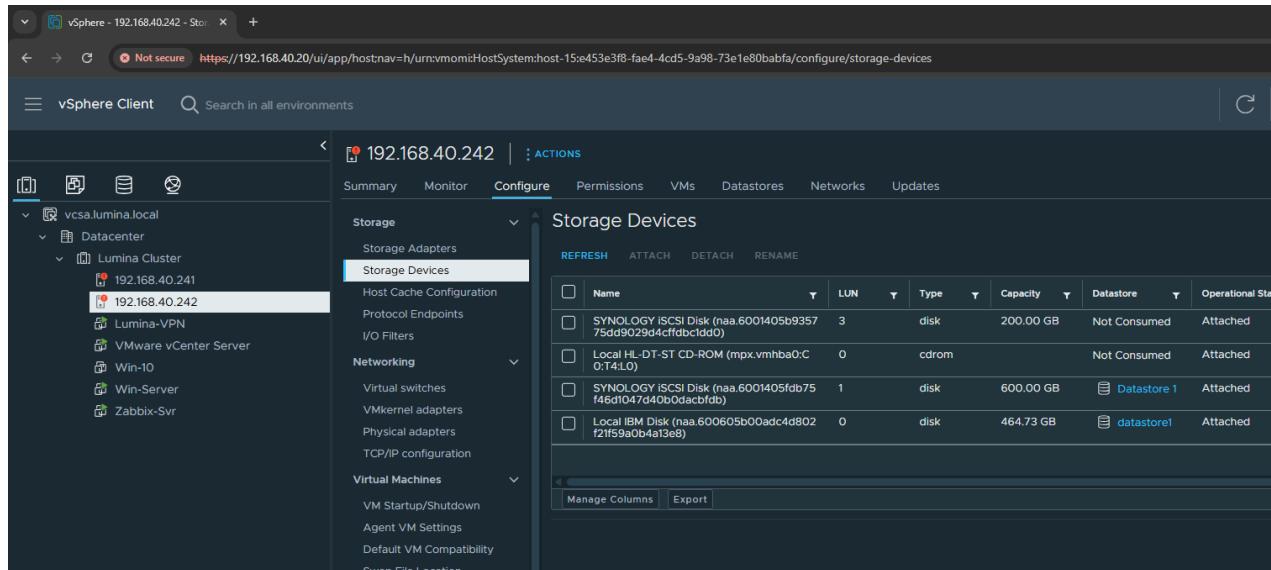


Figure 41- Storages Device

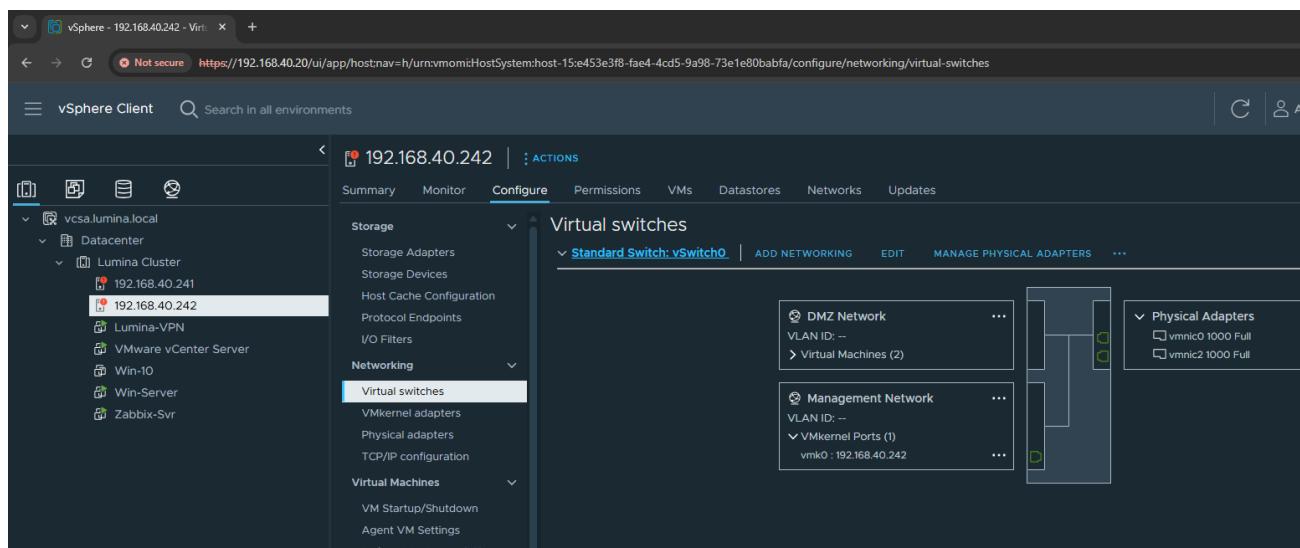


Figure 42- Virtual Switches

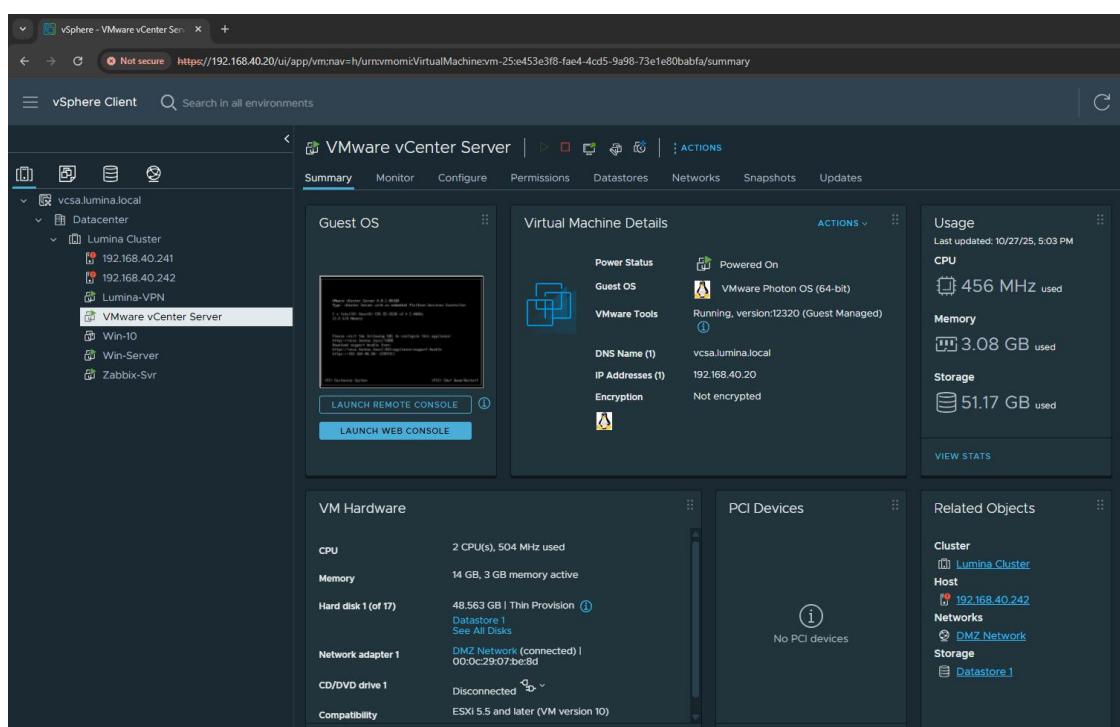


Figure 43- vCenter-Server Summary

The Below screenshots shows Veeam Backup Replication and Failover Configurations

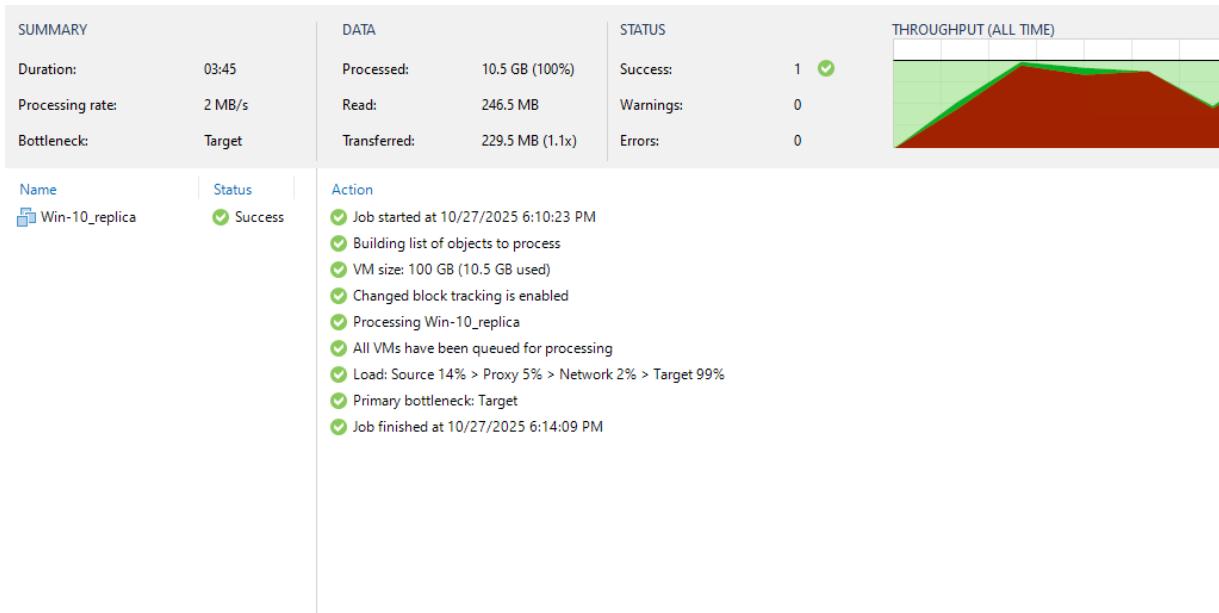


Figure 44-Replication Job Summary

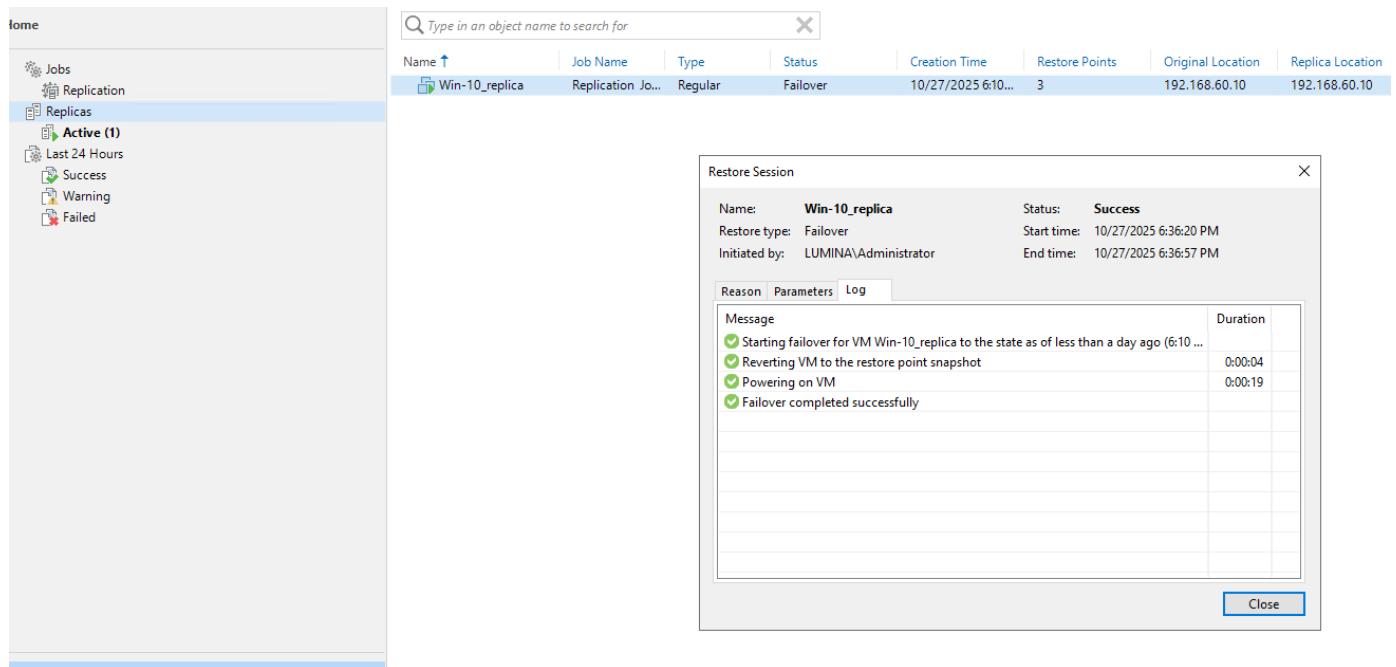
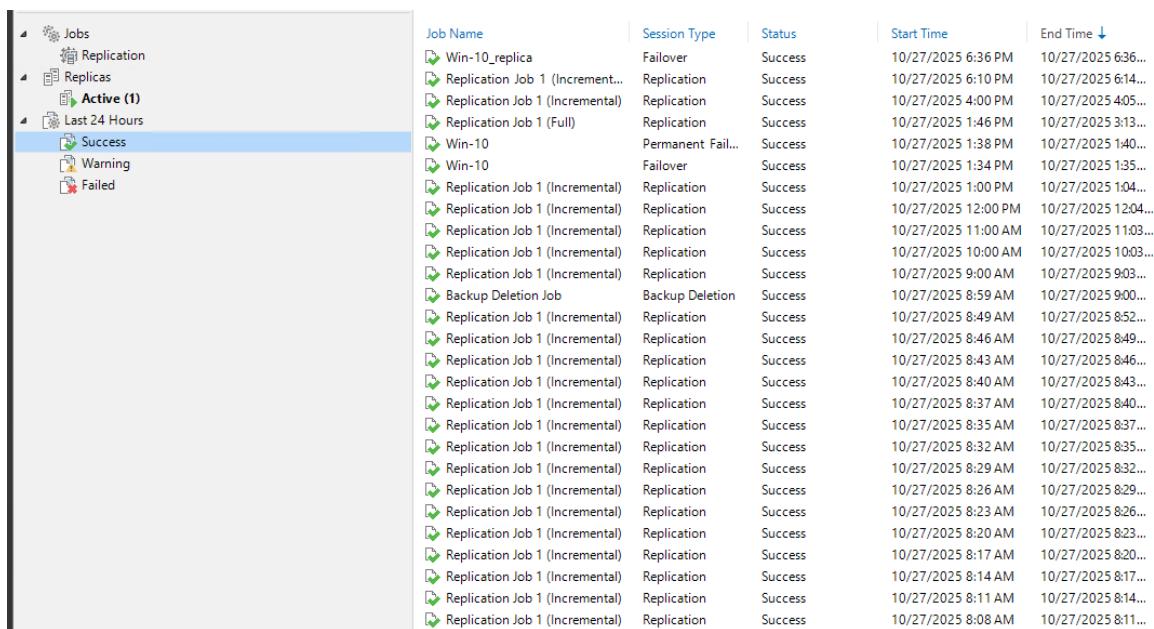


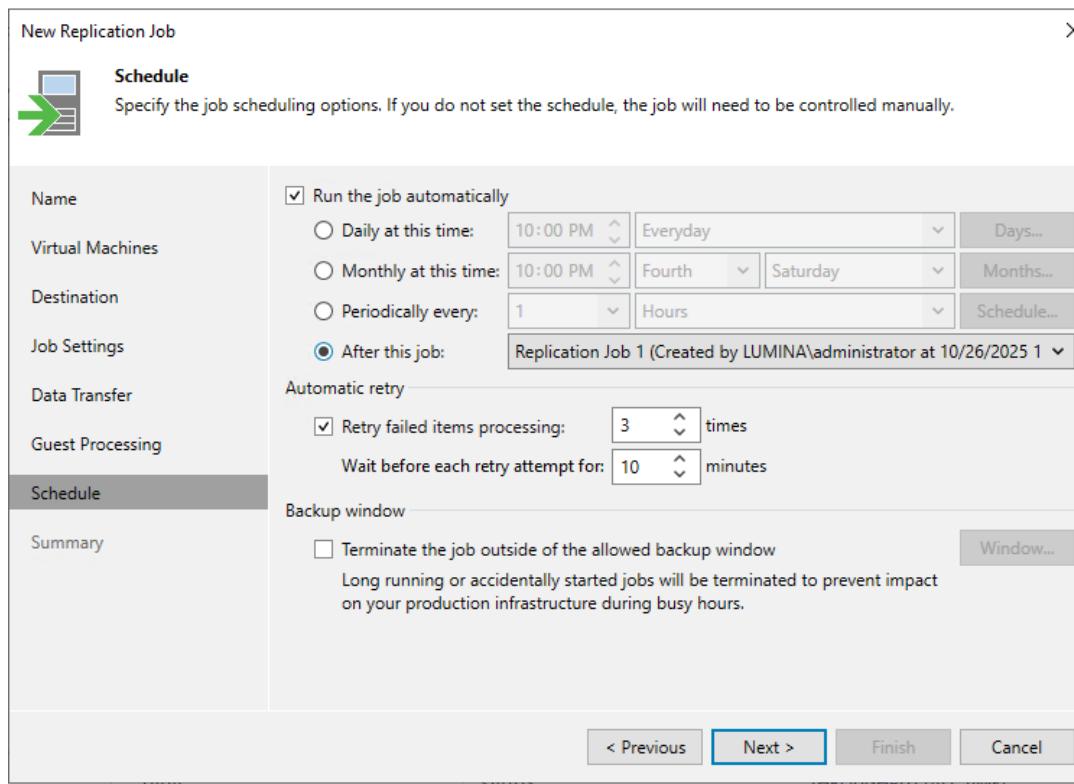
Figure 45- Failover Success



The screenshot shows a table titled "Success" under the "Last 24 Hours" section of the navigation pane. The table has columns for "Job Name", "Session Type", "Status", "Start Time", and "End Time". The data in the table is as follows:

Job Name	Session Type	Status	Start Time	End Time ↓
Win-10.replica	Failover	Success	10/27/2025 6:36 PM	10/27/2025 6:36...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 6:10 PM	10/27/2025 6:14...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 4:00 PM	10/27/2025 4:05...
Replication Job 1 (Full)	Replication	Success	10/27/2025 1:46 PM	10/27/2025 3:13...
Win-10	Permanent Fail...	Success	10/27/2025 1:38 PM	10/27/2025 1:40...
Win-10	Failover	Success	10/27/2025 1:34 PM	10/27/2025 1:35...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 1:00 PM	10/27/2025 1:04...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 12:00 PM	10/27/2025 12:04...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 11:00 AM	10/27/2025 11:03...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 10:00 AM	10/27/2025 10:03...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 9:00 AM	10/27/2025 9:03...
Backup Deletion Job	Backup Deletion	Success	10/27/2025 8:59 AM	10/27/2025 9:00...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 8:49 AM	10/27/2025 8:52...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 8:46 AM	10/27/2025 8:49...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 8:43 AM	10/27/2025 8:46...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 8:40 AM	10/27/2025 8:43...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 8:37 AM	10/27/2025 8:40...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 8:35 AM	10/27/2025 8:37...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 8:32 AM	10/27/2025 8:35...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 8:29 AM	10/27/2025 8:32...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 8:26 AM	10/27/2025 8:29...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 8:23 AM	10/27/2025 8:26...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 8:20 AM	10/27/2025 8:23...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 8:17 AM	10/27/2025 8:20...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 8:14 AM	10/27/2025 8:17...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 8:11 AM	10/27/2025 8:14...
Replication Job 1 (Incremental)	Replication	Success	10/27/2025 8:08 AM	10/27/2025 8:11...

Figure 46- Success Status History



The screenshot shows the "New Replication Job" dialog box, specifically the "Schedule" tab. The left sidebar lists other tabs: "Name", "Virtual Machines", "Destination", "Job Settings", "Data Transfer", "Guest Processing", "Schedule" (which is selected), and "Summary". The "Schedule" tab contains the following configuration:

- Name:** Run the job automatically (checkbox checked).
- Virtual Machines:** Daily at this time: 10:00 PM, Everyday, Days... button.
- Destination:** Monthly at this time: 10:00 PM, Fourth Saturday, Months... button.
- Job Settings:** Periodically every: 1 Hours, Schedule... button.
- Data Transfer:** After this job: Replication Job 1 (Created by LUMINA\administrator at 10/26/2025 1).
- Automatic retry:** Retry failed items processing: 3 times, Wait before each retry attempt for: 10 minutes.
- Backup window:** Terminate the job outside of the allowed backup window (checkbox unchecked). A note below states: "Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours." A "Window..." button is also present.

At the bottom, there are buttons for "< Previous", "Next >" (highlighted in blue), "Finish", and "Cancel".

Figure 47- Replication Scheduling

3.2.5 Virtualization Configuration

The Below screenshots shows VMSEsxi-1 Configurations

This screenshot shows the 'Host' section of the ESXi Host Client interface. The main panel displays the host details for 'Lumina', which is connected to vCenter Server at 192.168.40.20. The hardware section lists the manufacturer (LENOVO), model (System x3550 M5 - [D463AC]), 6 CPUs, 31.62 GB of memory, and networking details including IP addresses (192.168.40.241, fe80::a94:effff:fe14:a3d7) and DNS servers (1.192.168.1.3, 2.192.168.40.20). The configuration section includes options for image profile, vSphere HA state, and vMotion. The system information section provides details like date/time, install date, asset tag, serial number, BIOS version, and BIOS release date. A performance summary for the last hour is also present.

Figure 48- Host System information (192.168.40.241)

This screenshot shows the 'Adapters' tab for the 'Storage' section of the ESXi Host Client. It is configuring the iSCSI adapter 'vmhba64'. The 'Configure iSCSI' tab is selected. The 'Name' field is set to 'Configure iSCSI - vmhba64'. The 'iSCSI enabled' option is set to 'Enabled'. Under 'Static targets', there is a table with one entry: Target (iqn.2000-01.com.synology:NAS-WonderLand.default-target) and Address (192.168.40.5). Under 'Dynamic targets', there is a table with one entry: Address (192.168.40.5) and Port (3260). At the bottom right, there are 'CANCEL' and 'SAVE CONFIGURATION' buttons, with the latter being blue and indicating success ('Completed successfully').

Figure 49- NAS Connected with ISCSI to ESXI

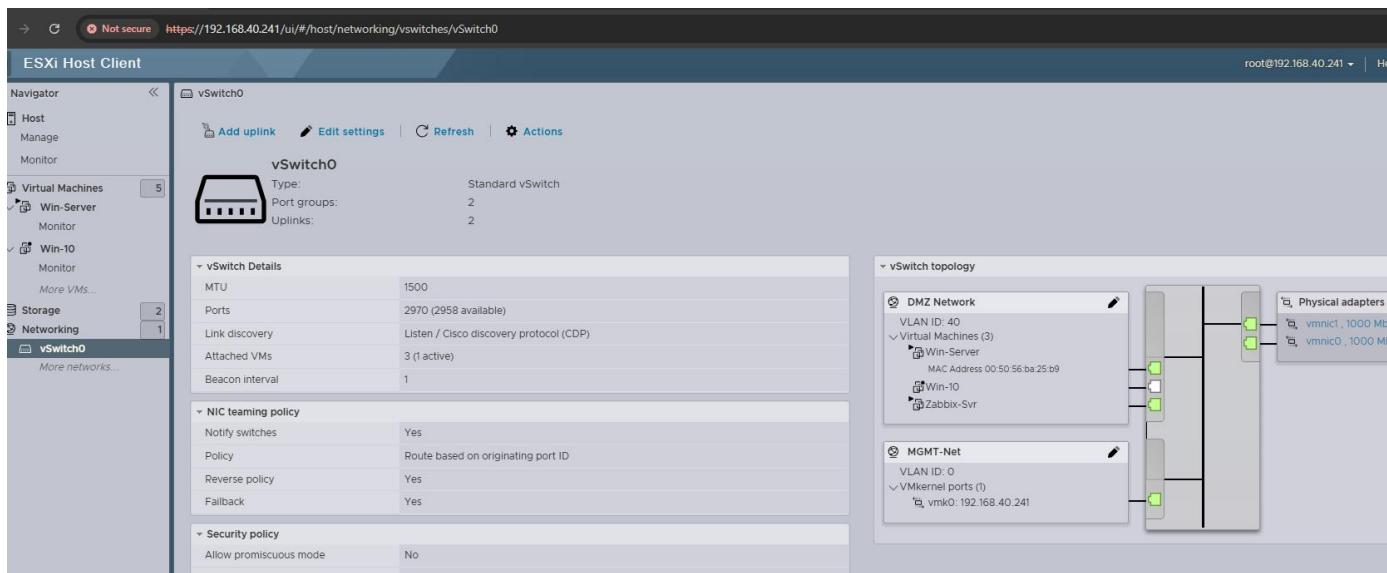


Figure 50- Virtual Switch Configuration and Topology

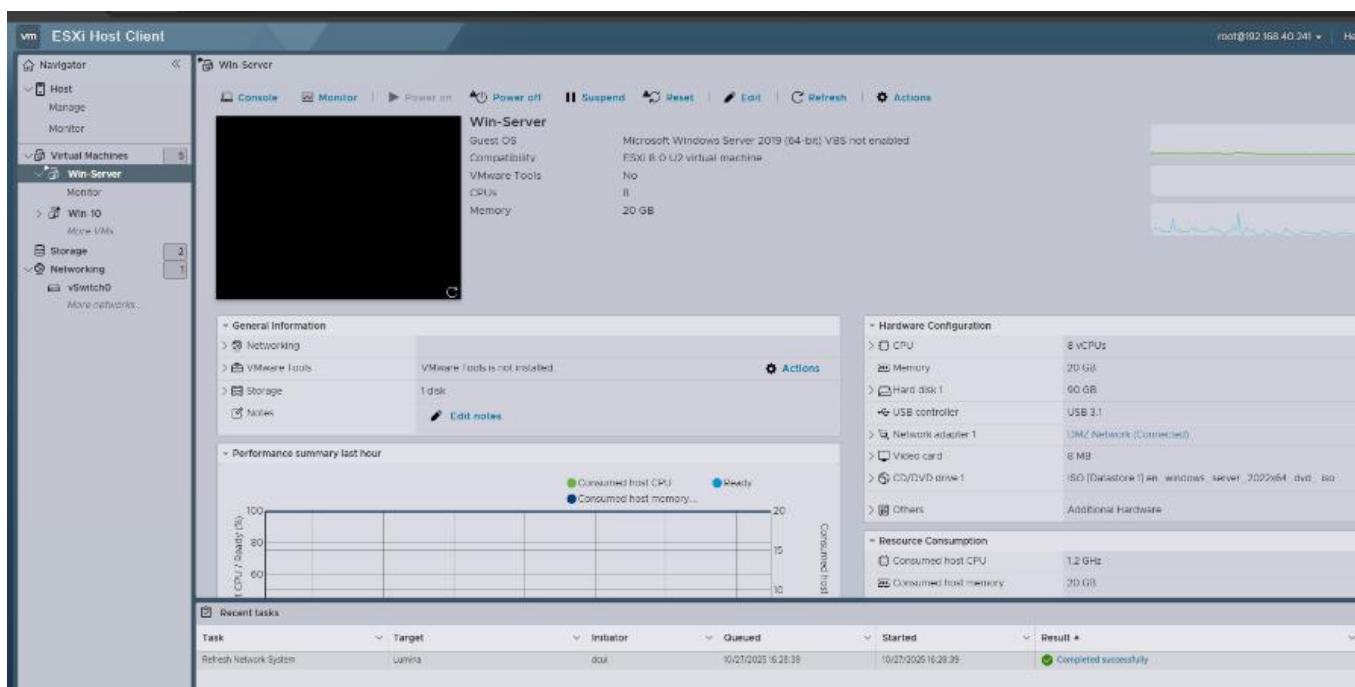


Figure 51- Win-Server Overview

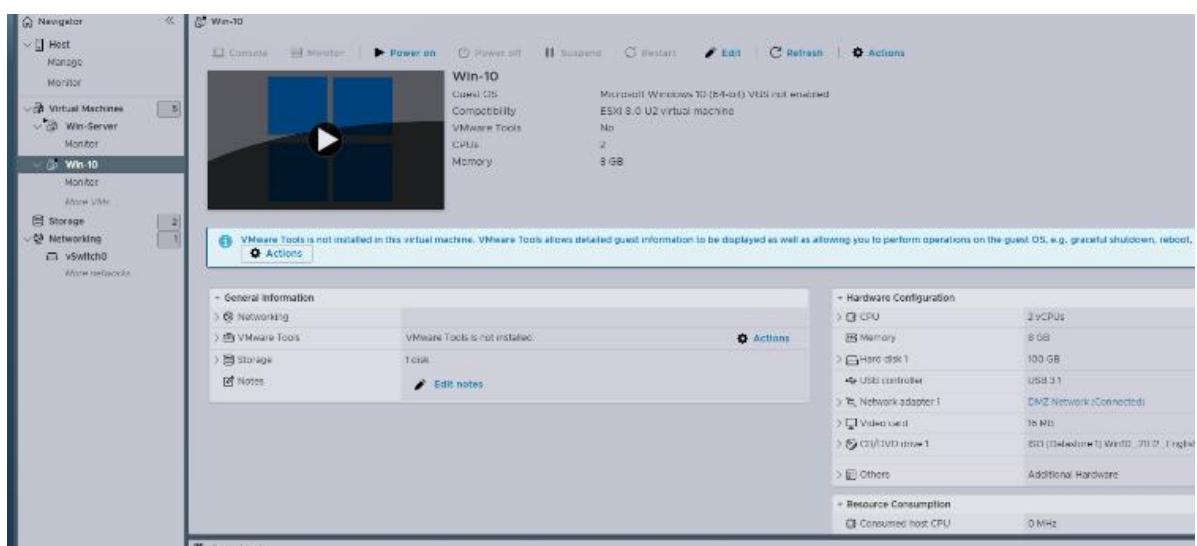


Figure 52- Win 10 VM Overview

The Below screenshots shows VMESxi 2 Configurations

This screenshot shows the ESXi Host Client interface. The left sidebar navigation includes Host, Virtual Machines, Storage, and Networking. The main content area displays the host configuration for 'localhost.localdomain'. Key details shown include:

- Host Information:** Version: 8.0 Update 2, State: Normal (connected to vCenter Server at 192.168.40.20), Uptime: 2.05 days.
- Hardware:** Manufacturer: LENOVO, Model: System x3550 M5 - [5463AC1], CPU: 6 CPUs x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz, Memory: 31.88 GB, Virtual flash: 0 B used, 0 B capacity.
- Networking:** Hostname: localhost.localdomain, IP addresses: 1. vmk0: 192.168.40.242, 2. vmk0: fe80::42f2:e9ff:febd:c070, DNS servers: 1. 192.168.1.3, Default gateway: 192.168.40.3, IPv6 enabled: Yes, Host adapters: 5.
- Configuration:** Image profile: HPE-Custom-AddOn, vSphere HA state: Supported, vMotion: Supported.
- System Information:** Date/time on host: Monday, October 27, 2023, Install date: Friday, October 24, 2023, Asset tag: (none), Serial number: 06HEDDB, BIOS version: -[TBEG06MUS-1.1]-, BIOS release date: Tuesday, August 04, 2023.
- Performance summary last hour:** A chart showing performance metrics over the last hour, with values ranging from 0 to 100.

Figure 55- Host System Information (192.168.40.242)

This screenshot shows the configuration and topology of the vSwitch0. The left sidebar navigation includes Host, Virtual Machines, Storage, and Networking. The main content area shows the vSwitch0 settings and its connection to physical adapters and virtual machines.

vSwitch0 Details:

- Type: Standard vSwitch
- Port groups: 2
- Uplinks: 2

vSwitch topology:

- DMZ Network:** VLAN ID: 0, Virtual Machines (2): VMware vCenter Server (MAC Address 00:0c:29:07:be:8d) and Lumina-VPN (MAC Address 00:0c:29:88:38:bb).
- Management Network:** VLAN ID: 0, VMkernel ports (1): vmk0: 192.168.40.242.
- Physical adapters:** vmnic2, vmnic0.

Figure 54- Virtual Switch Configuration and Topology

This screenshot shows the Datastore browser interface. The left sidebar navigation includes Host, Virtual Machines, Storage, and Networking. The main content area displays the datastores available on the host.

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin provision
Datastore 1	SSD	599.75 GB	408.65 GB	191.1 GB	VMFS6	Supported
datastore1	Non-SSD	336.5 GB	4.92 GB	331.58 GB	VMFS6	Supported

Figure 53- Data Store Capacity and Browser Interface

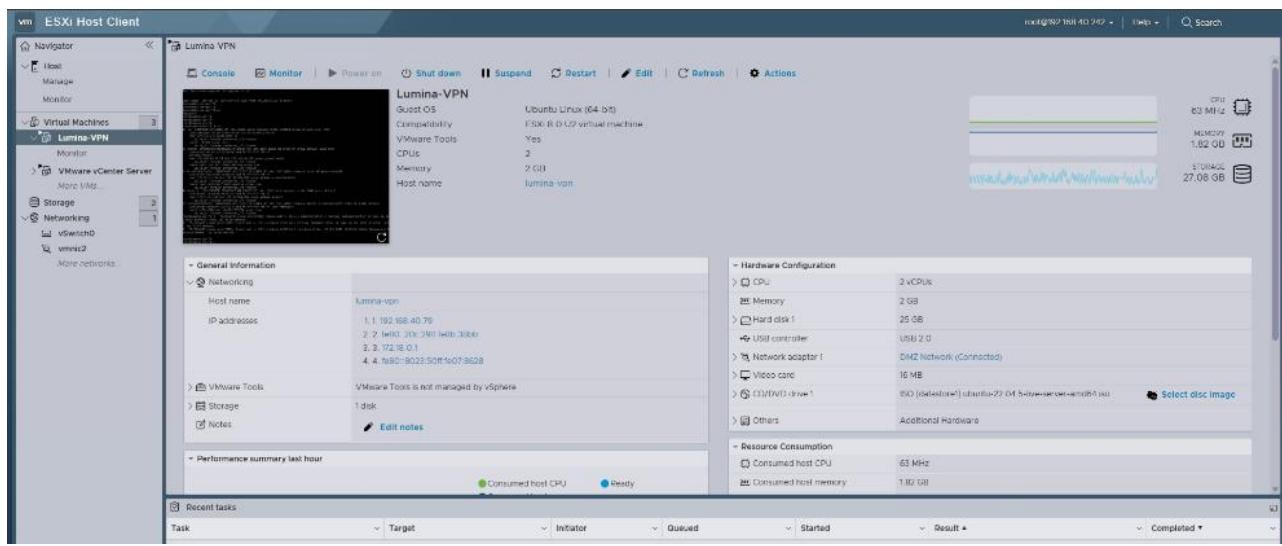


Figure 56- Lumina VPN Machine Details

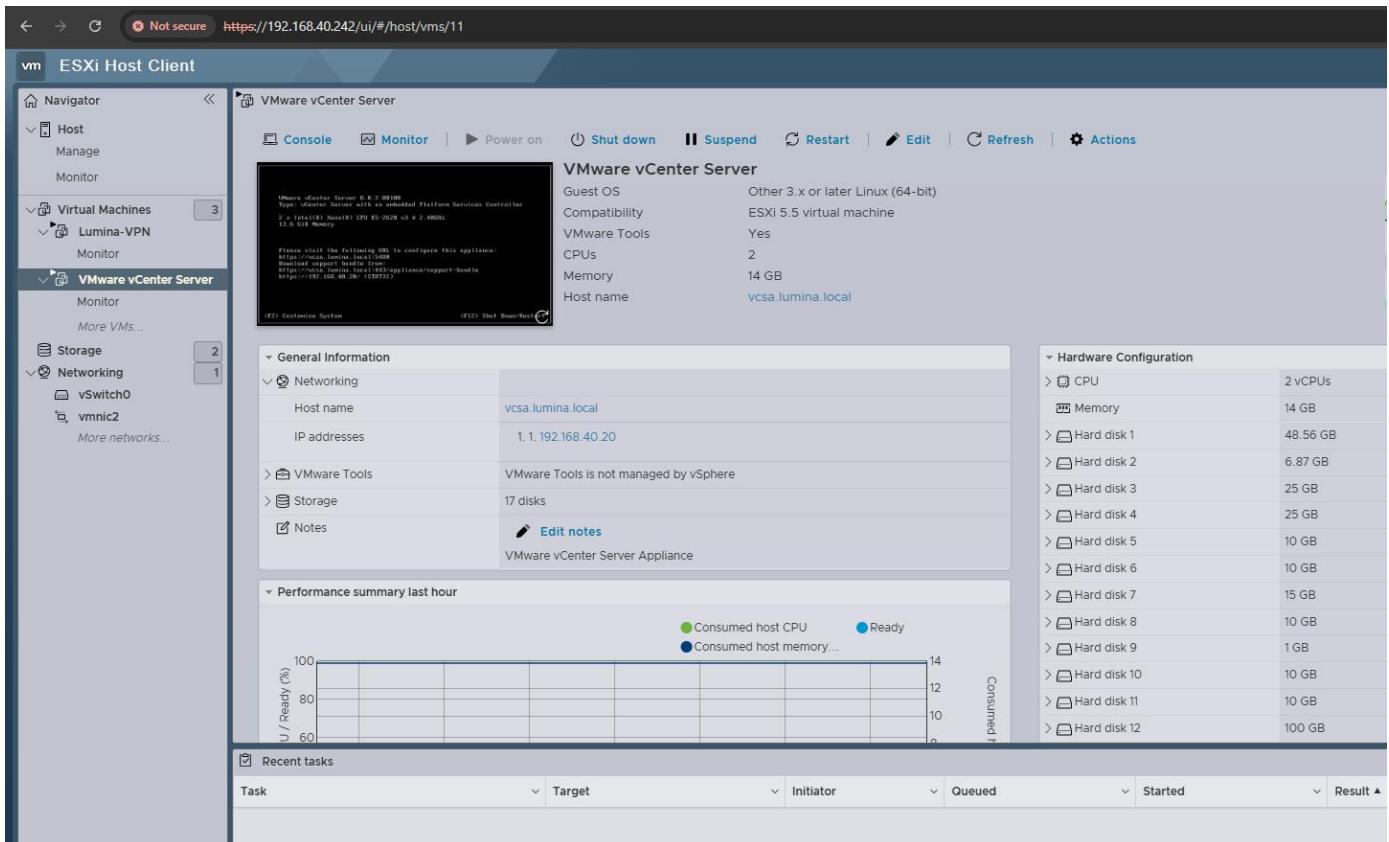


Figure 57- vCenter Server Application VM Details

The Below screenshots shows VMESxi-DR Site Configurations

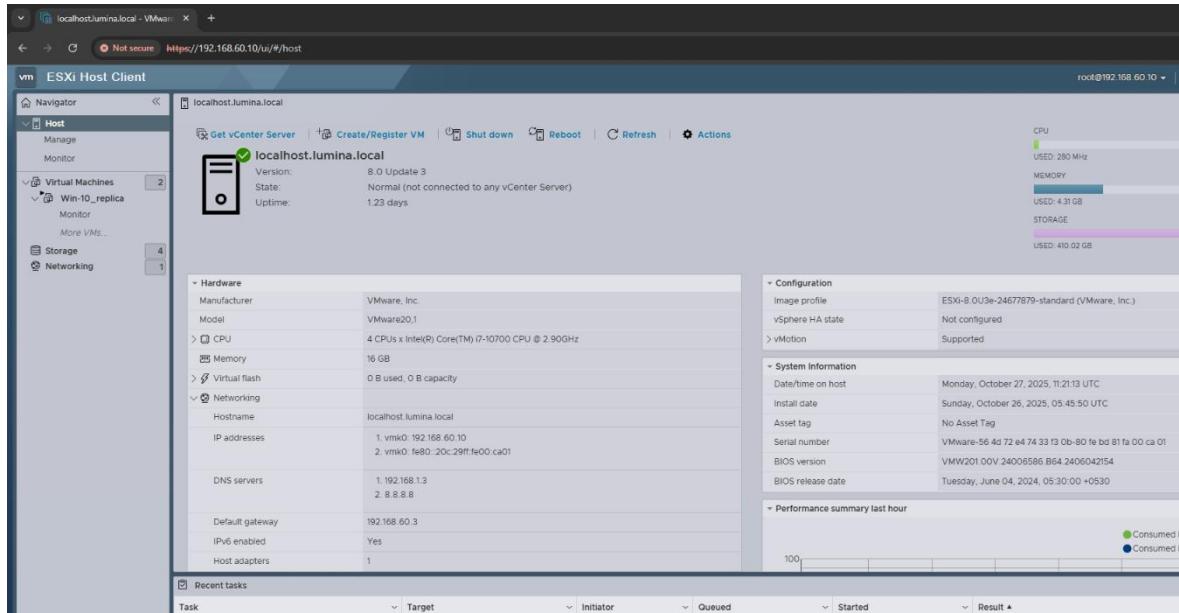


Figure 59- Host System Information (192.168.60.10)

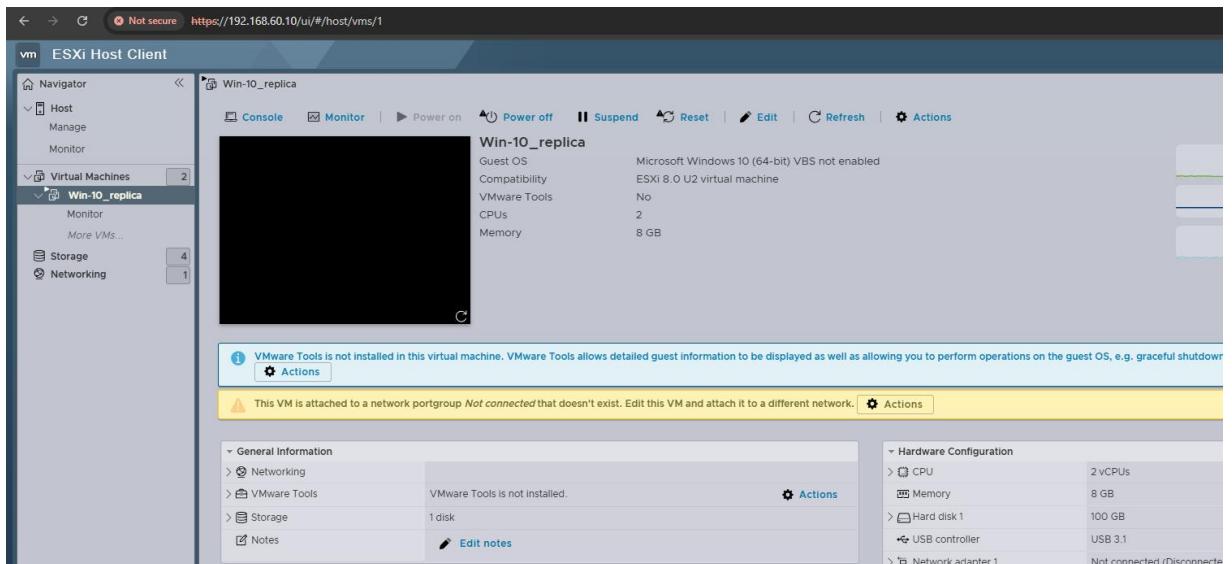


Figure 60- Win 10 Replica VM Details

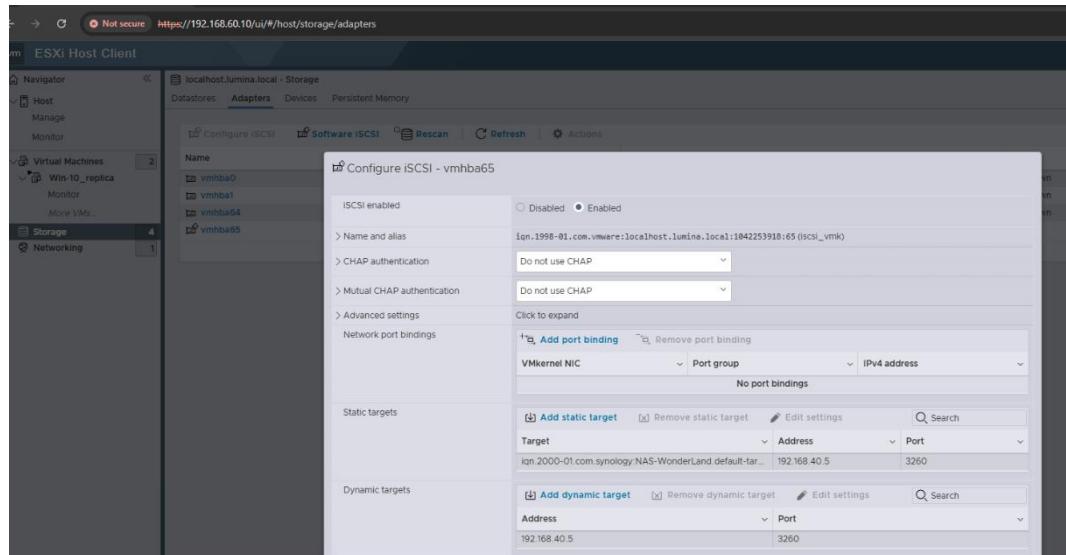


Figure 58- NAS Connectivity with DR Site

3.2.6 Zabbix Configuration

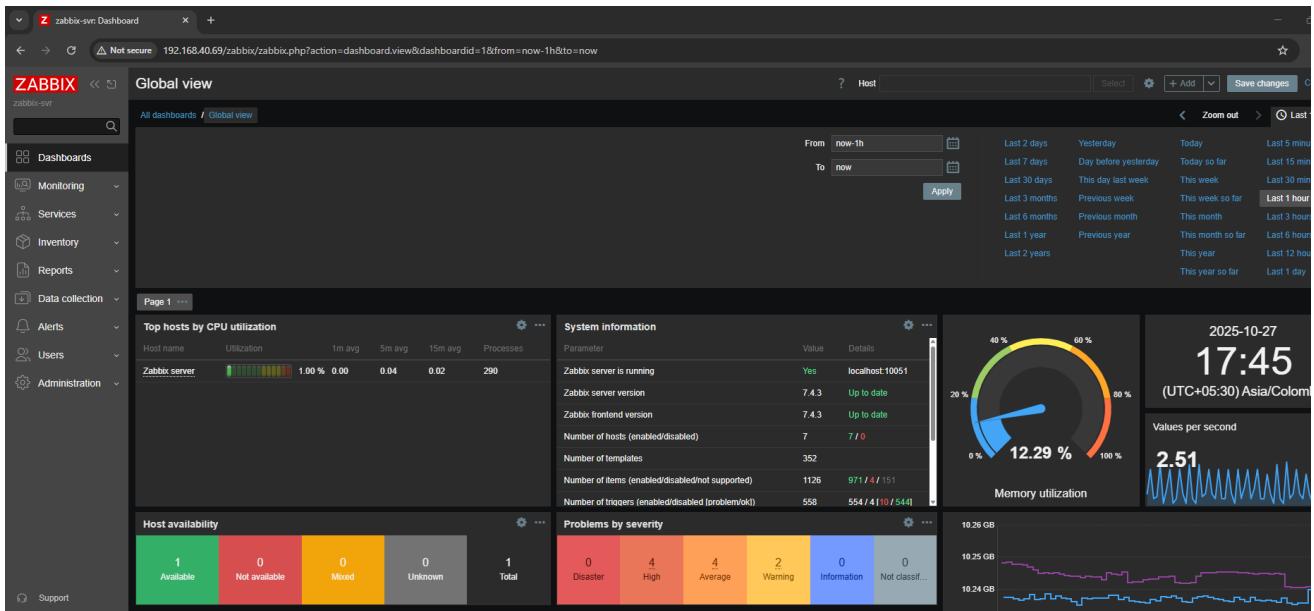


Figure 61- Global View

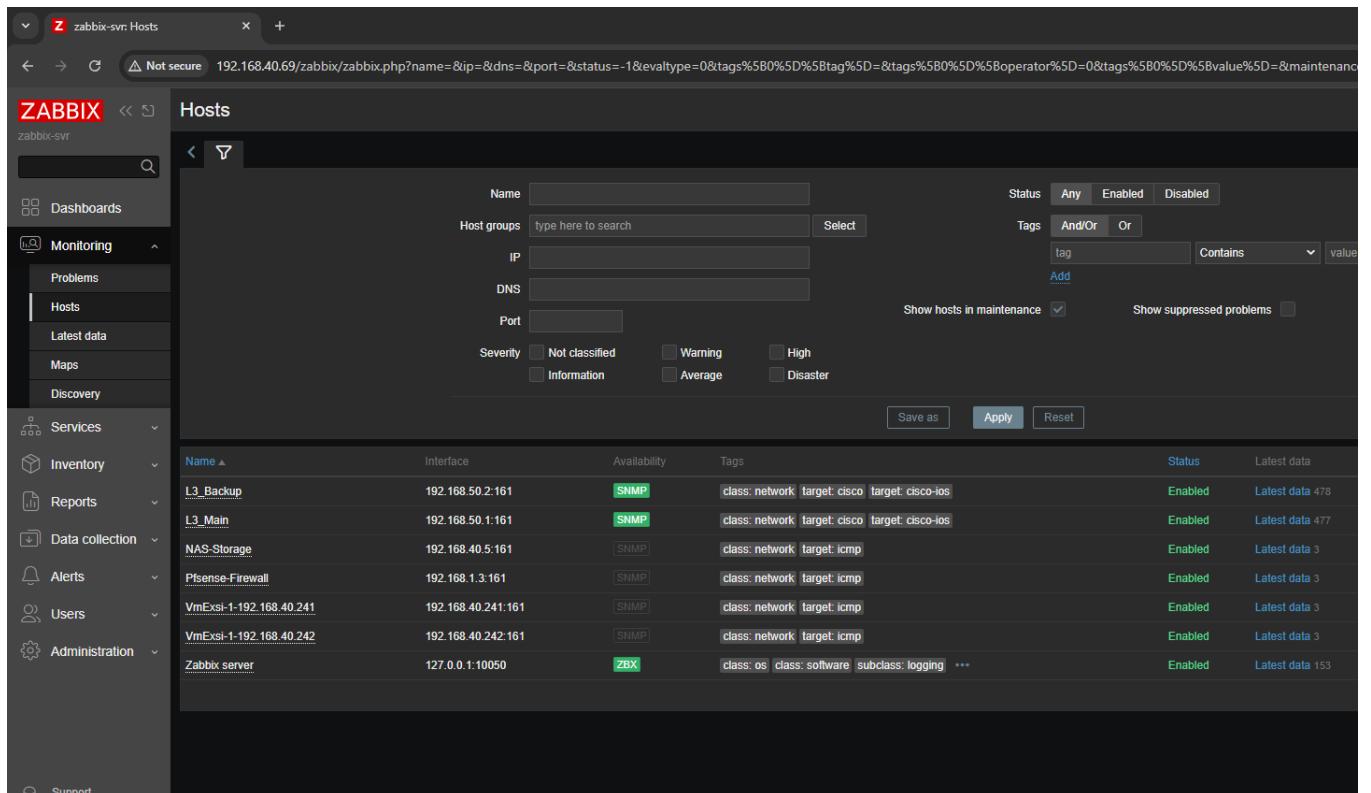


Figure 62- Host List

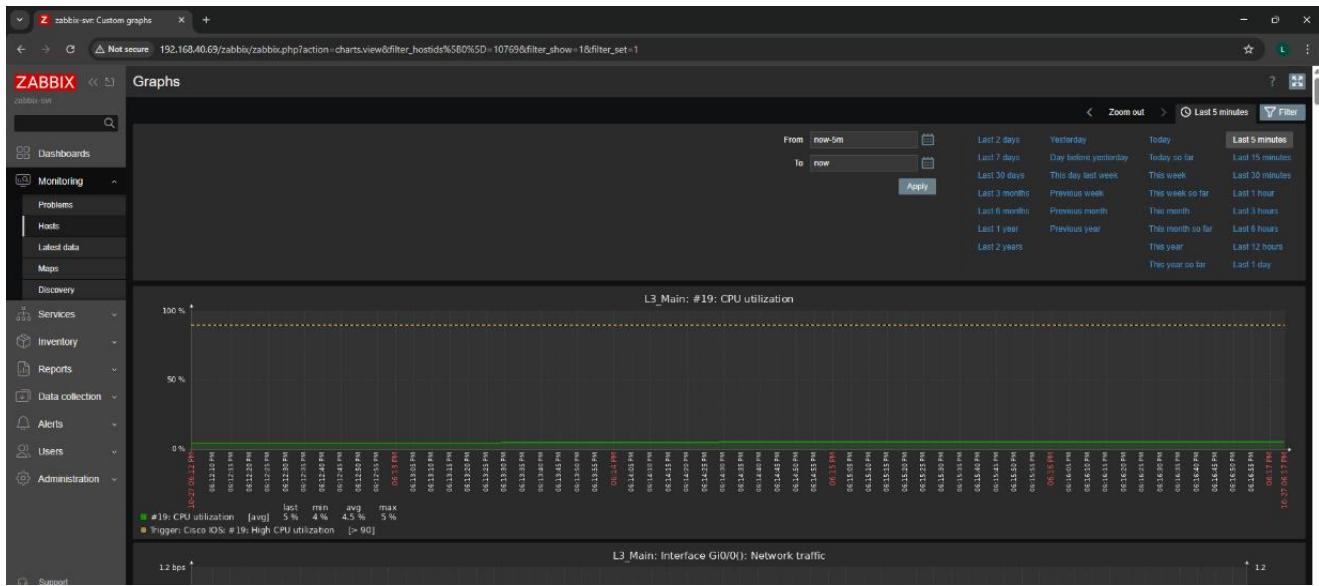


Figure 63- L3 main Switch-CPU Utilization

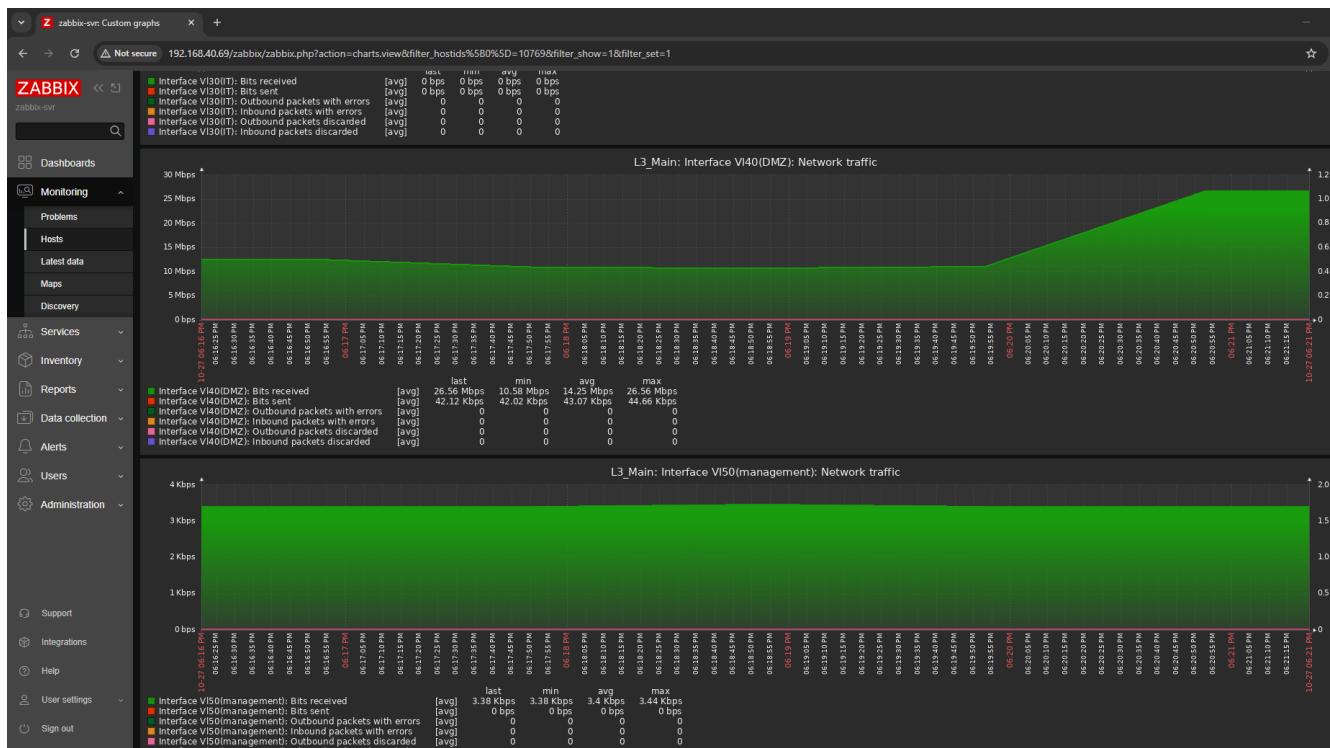


Figure 64- L3 main Switch-Vlan Utilization

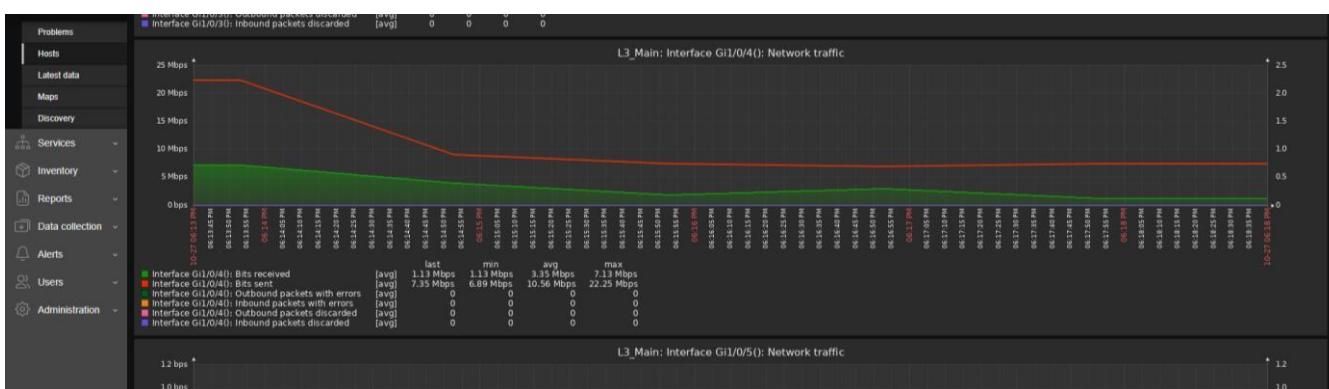


Figure 65-L3 Main Swtich-Monitoring

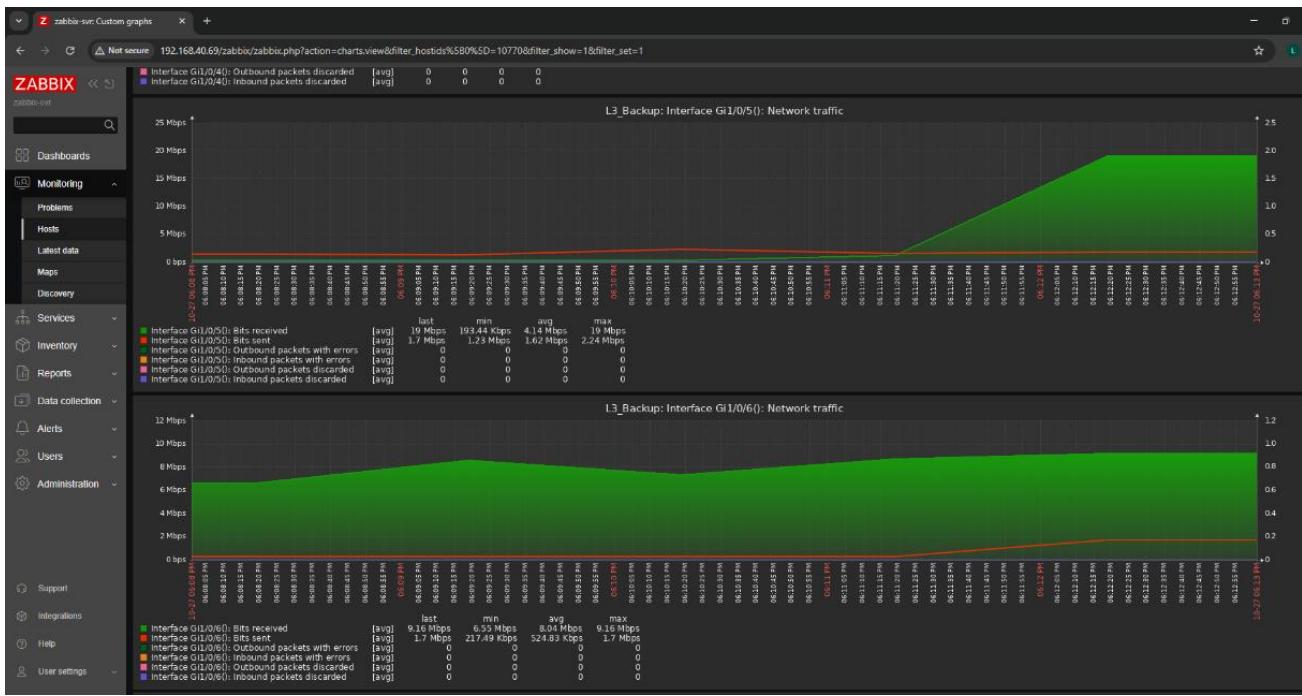


Figure 66- L3 Backup Switch-Graph

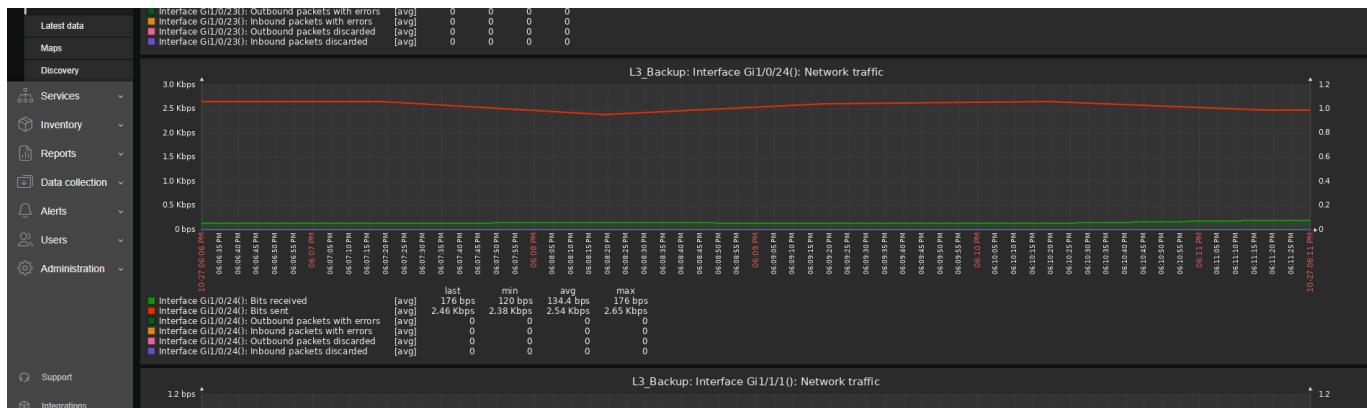


Figure 67- L3 Backup Switch-Uplink

3.2.7 NAS Configurations

The screenshot shows the Synology Storage Manager Dashboard. The left sidebar has tabs for Overview, Storage, Storage Pool 1, Volume 1, and HDD/SSD. The main area displays:

- System Status:** Healthy. System is healthy.
- Volume Usage:** Volume 1 (Storage Pool 1) - 368.1 GB used, 975.9 GB free.
- Drive Information:** NAS_WonderLand (RAID 5 array with 4 drives labeled 1-4).
- Task Schedule:** No task schedule.

Figure 68- Storage Manager Dashboard

The screenshot shows the Storage Manager interface for Storage Pool 1. The left sidebar shows Storage Pool 1 selected. The main area displays:

- Storage Pool 1:** Healthy. 1.4 TB allocated | 0 Bytes free.
- Data Scrubbing:** Status: Ready. Run Now button.
- Completed on:** 10/26/2025 20:35.
- Drive Info:** A table showing four drives (NAS_WonderLand) as SSDs, each with 476.9 GB capacity, assigned to Storage Pool 1, and all marked as Healthy.
- Volume 1:** Healthy. 368.1 GB used, 975.9 GB free. File system: Btrfs. Total capacity: 1.3 TB.

Figure 69- Storage Pool 1 Details

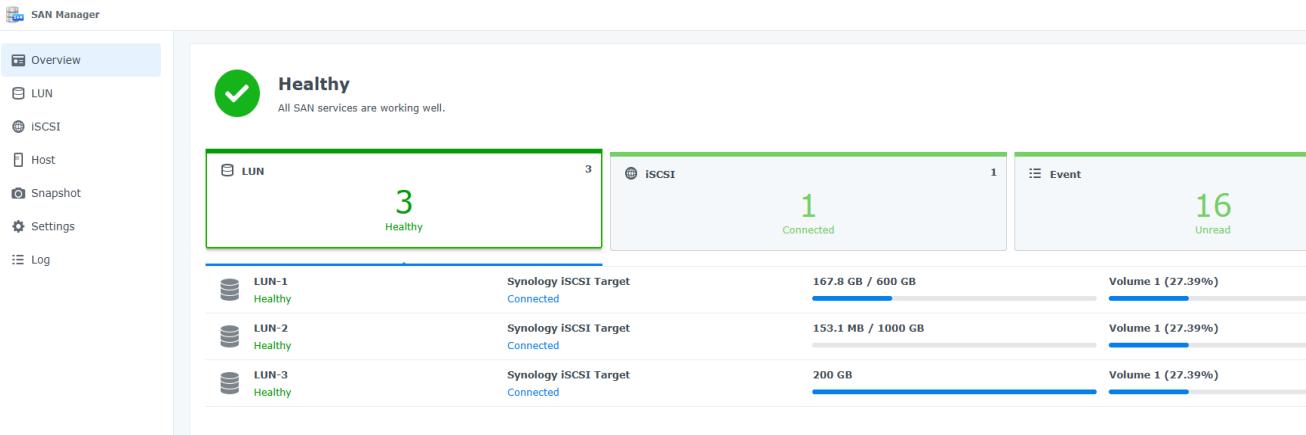


Figure 70- LUNs and iSCSI Overview

Synology iSCSI Target - Connected

Name: iqn.2000-01.com.synology:NAS-WonderLand.default-target.c60e556b9a5

Synology iSCSI Target
iqn.2000-01.com.synology:NAS-WonderLand.default-target.c60e556b9a5 ([Copy IQN](#))
EsX12 (192.168.40.242)
DREsx1 (192.168.60.10)
iqn.1991-05.com.microsoft:desktop-e39iq9d (192.168.60.5) ([Create Host](#))
EsX11 (192.168.40.241)

Authentication: None
Multiple Sessions: Enable
Header digest: Disable
Data digest: Disable
Maximum receive segment bytes: 262144 Bytes
Maximum send segment bytes: 262144 Bytes

Mapped LUNs

Name	Used / Total	Status
LUN-1	167.8 GB / 600 GB	Healthy
LUN-2	153.1 MB / 1000 GB	Healthy
LUN-3	200 GB / 200 GB	Healthy

Figure 71- iSCSI Target Configuration and Mapped LUNs

General

Enter the server name, DNS server and default gateway information.

Server name: NAS_WonderLand

Default gateway: 192.168.40.3 (Bond 1)

IPv6 default gateway: --

Manually configure DNS server:

Preferred DNS server: 192.168.40.10

Alternative DNS server:

Proxy

Connect via a proxy server:

Address:

Port: 80

Bypass proxy server for local addresses:

Figure 72- Network General Setting

3.2.8 Cloud Configuration

The screenshot shows the AWS Management Console EC2 Instances dashboard. The left sidebar navigation includes EC2, Dashboard, AWS Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Capacity Manager, Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, Elastic IPs selected), and Network & Security (Security Groups). The main content area displays 'Instances (3) Info' with a table showing three instances: i-0dd7d865e436debae (Stopped, t2.small, -), i-04d916ff373b6297c (Stopped, t2.micro, -), and i-04f25af372700b6f6 (Running, t2.micro, 2/2 checks passed). A 'Select an instance' dropdown is open below the table.

Figure 73- AWS EC2 Instances Dashboard

The screenshot shows the AWS Management Console Instance details page for instance i-04f25af372700b6f6 (Lumina). The left sidebar navigation is identical to Figure 73. The main content area displays the 'Instance summary for i-04f25af372700b6f6 (Lumina)' with various details: Instance ID (i-04f25af372700b6f6), Public IPv4 address (13.250.34.190), Instance state (Running), Private IP DNS name (ip-172-31-31-114.ap-southeast-1.compute.internal), Instance type (t2.micro), VPC ID (vpc-08119f82f15836191), Subnet ID (subnet-0d36fed06be2cdc6c), Instance ARN (arn:aws:ec2:ap-southeast-1:311141529020:instance/i-04f25af372700b6f6), and other fields like IMDSv2 (Required), Operator (-), and AWS Compute Optimizer finding (Opt-in to AWS Compute Optimizer for recommendations). The bottom navigation bar includes Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags.

Figure 74- Instance Summary of Deployed Web Server

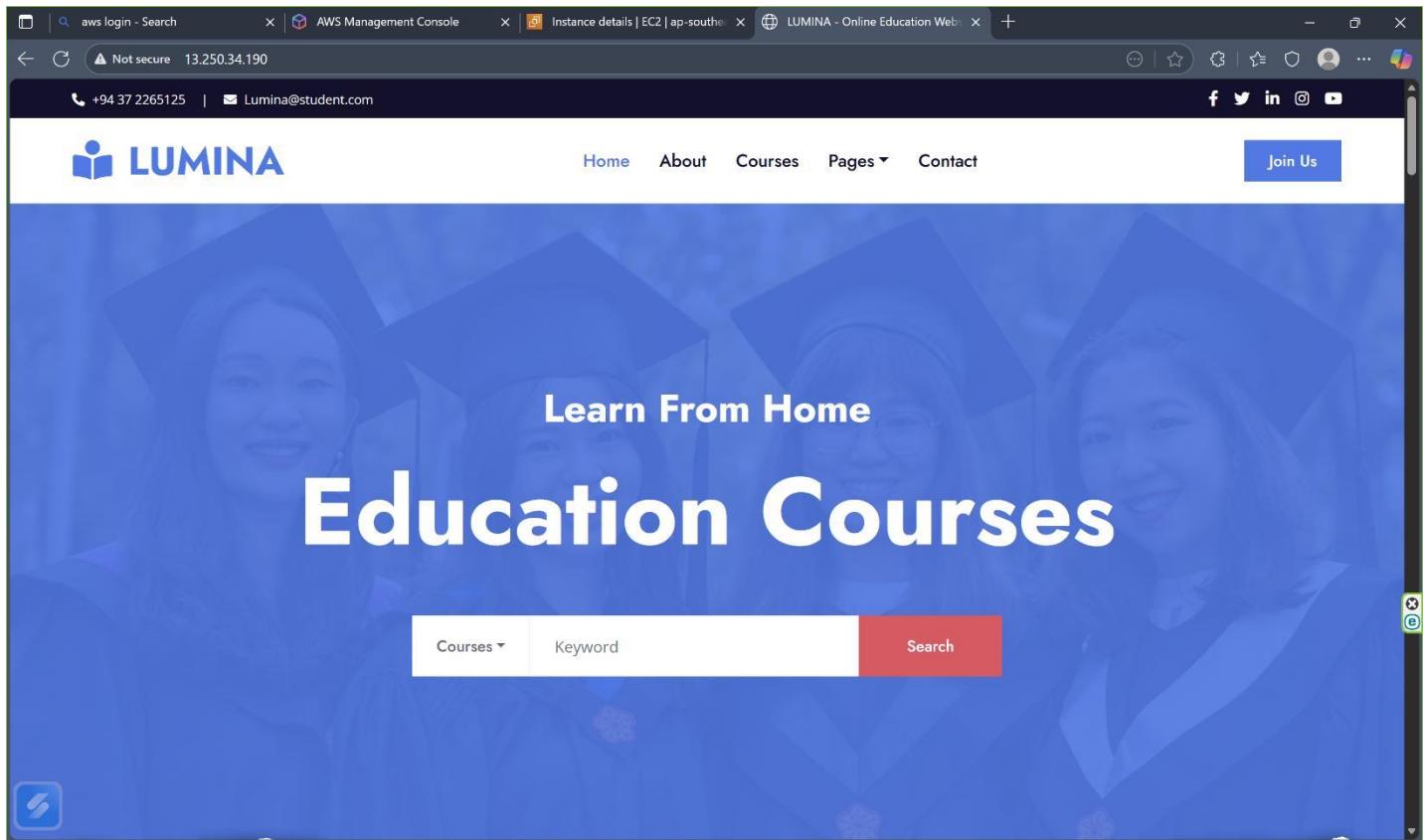


Figure 75- Home Page of the Web Page Hosted on AWS EC2

A screenshot of the 'About' page from the LUMINA website. The top navigation bar shows the same structure as the home page. The main content features a large photo of a smiling graduate in a cap and gown. To the right, the heading 'ABOUT US' is followed by the text 'First Choice For Online Education Anywhere'. Below this is a paragraph of placeholder text (lorem ipsum). At the bottom, there are four colored boxes with statistics: a green box for 'AVAILABLE SUBJECTS' (123), a blue box for 'ONLINE COURSES' (1234), a red box for 'SKILLED INSTRUCTORS' (123), and a yellow box for 'HAPPY STUDENTS' (1234).

Figure 76- About Page of the Web Page Hosted on AWS EC2

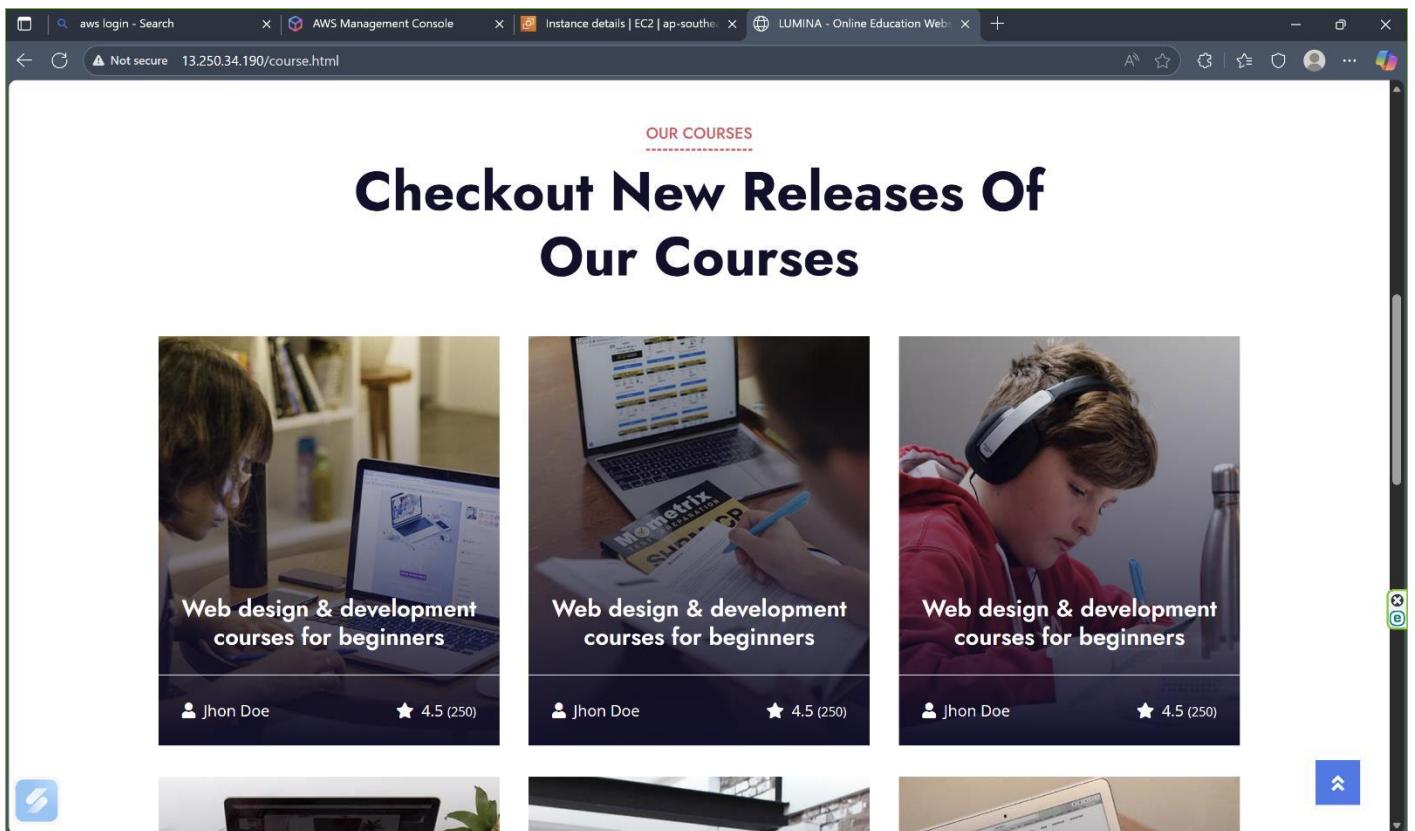


Figure 77- Our Courses Page of the Web Page Hosted on AWS EC2

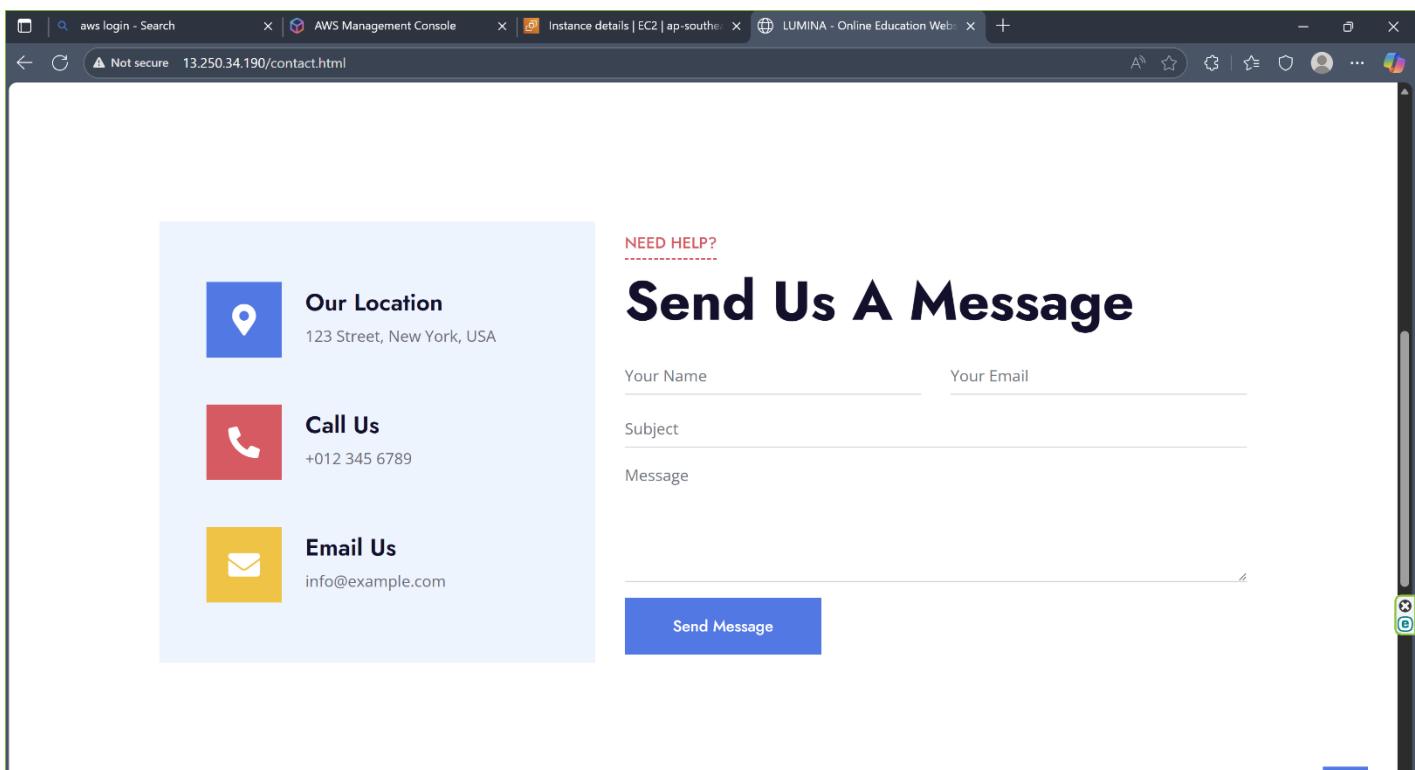


Figure 78- Contact Page of the Web Page Hosted on AWS EC2

Chapter 4: Predicted problems and Solution

We anticipate that there might be issues that may arise in the future so in-order to deal with these issues we implemented solutions to mitigate these issues. By doing so we can avoid complex issues and make the network infrastructure more reliable and efficient. This approach is designed to help us solve and avoid issues.

Problems and Solutions

- Using CCTVs may cause some issues in relation to power supply in the future. To solve this issue, we have decided to use switches that have Power over Ethernet(PoE). This way, we do not have to use external power sources, allowing us to use a more optimal and clean power structure when we use the CCTVs.
- As some users grow, changes in the network structure will be needed. The use of modular switches with extra ports will allow the network to grow with users, without the network structure having to be changed. This will allow us to stay ahead of the network structure changes and changes in users.
- In the implementation of wireless infrastructure, if not executed strategically, cover gaps and interferences may arise. with a proper installation of enterprise access points and VLANs will mitigate issues of reliable and secured Wi - Fi connectivity.
- There will be cases the core and distribution link may be congested due to the increase of users and services, and performance of the network will decline. The problem may be solved by upgrading the backbone to 10G uplinks.

Chapter 5: Future Implementation

Having an HA(High Availability) setup for pfSense firewalls would allow for uninterrupted workings, this would further solidify our network infrastructure. Upgrading the backbone links to 10G would be beneficial to our university network. More separate VLANs can be created for staff, students, and guests for more secure wireless infrastructures. More advanced security can be added like IDS, IPS, SIEM, endpoint security. The disaster recovery site can be extended with automated failover for quicker recovery from outages. Furthermore, more workloads can be transitioned to the cloud (AWS) to bolster hybrid cloud frameworks, and access security can be improved with multi-factor authentication and role-based access. To increase the service LMS and DNS, Load balancers could be put in place. More workloads can be migrated to AWS to bolster hybrid cloud frameworks, and access security can be improved with multi-factor authentication and role-based access to improve the flow of the system.

CONCLUSION

The Lumina University Network project delivered a broad of technologies to secure, scalable, and fully functional system that incorporates on-premise networking, virtualization, and monitoring, storage, and cloud technologies. Achieving a stable and efficient environment suitable for a true university deployment, we utilized PFsense as the core router and firewall, along with redundant multilayer switches, secure access switches, and a complete ESXi-based server farm. AWS cloud hosting, Veeam replication, and centralized vCenter management enhanced monitoring, continuity, and availability. The project overall achieved all relevant primary design goals, resulting in a strong platform for additional future development.

Chapter 6: References

<https://netacad.com/> Cisco netacad.

<https://router-switch.com> Get Device prices.

<https://docs.netgate.com/> PfSense Documentation

<https://docs.vmware.com/> Vmware vSphere documentation

https://www.zabbix.com/download?os_distribution=ubuntu Zabbix Documentation

<https://aws.amazon.com/ec2> AWS EC2

Annexure 1: Floor plans and Network wiring

The Floor plans

Ground floor



Figure 79

Ground Floor Includes

- | | |
|---------------|---------------|
| -Reception | -CCTV room |
| -Lounge | -Wash rooms |
| -Labour room | -Studio |
| -Canteen area | -Tennis court |

1st Floor

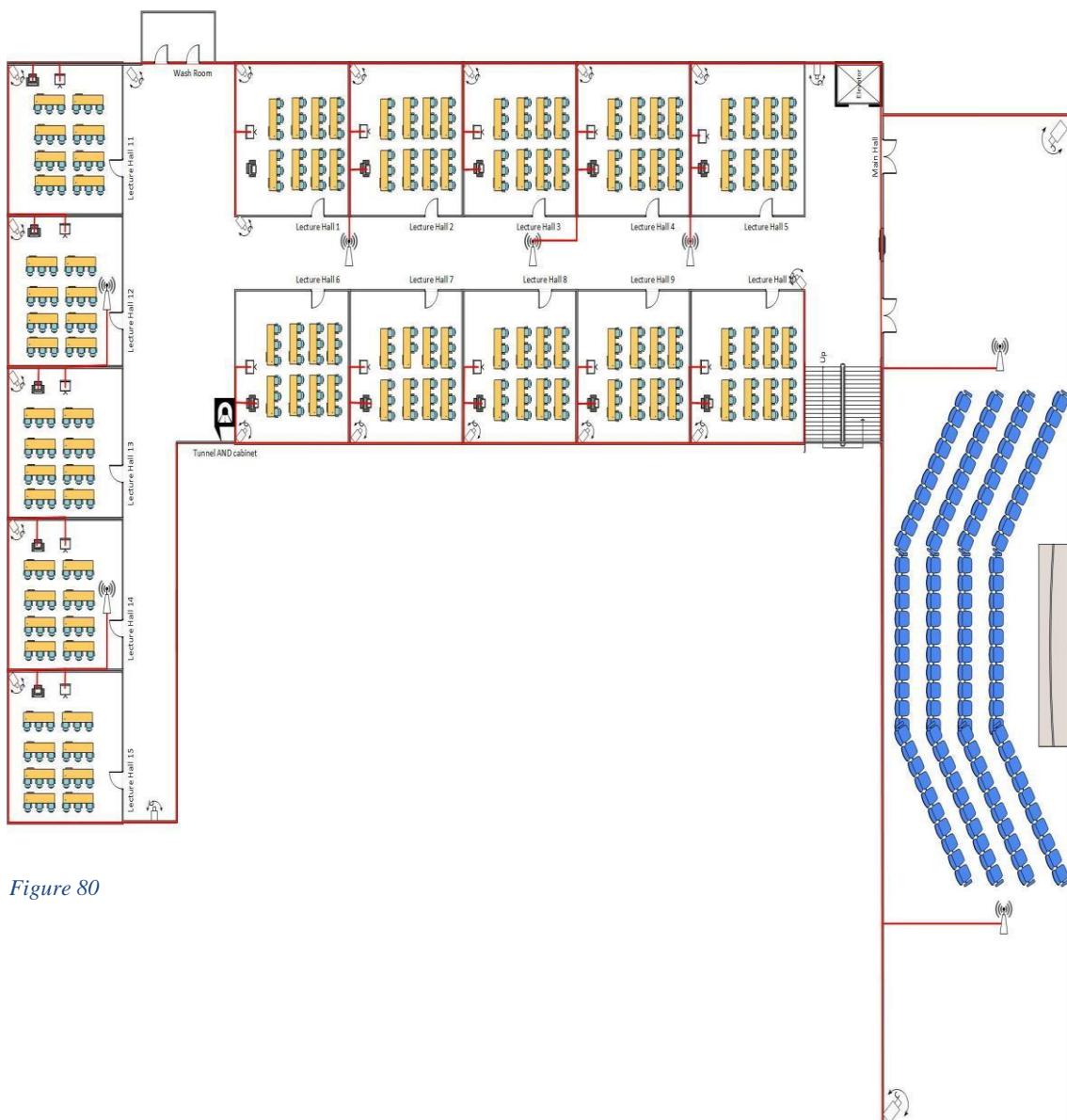


Figure 80

1st Floor Includes

- Lecture Halls
- Main hall
- Wash room

2nd Floor

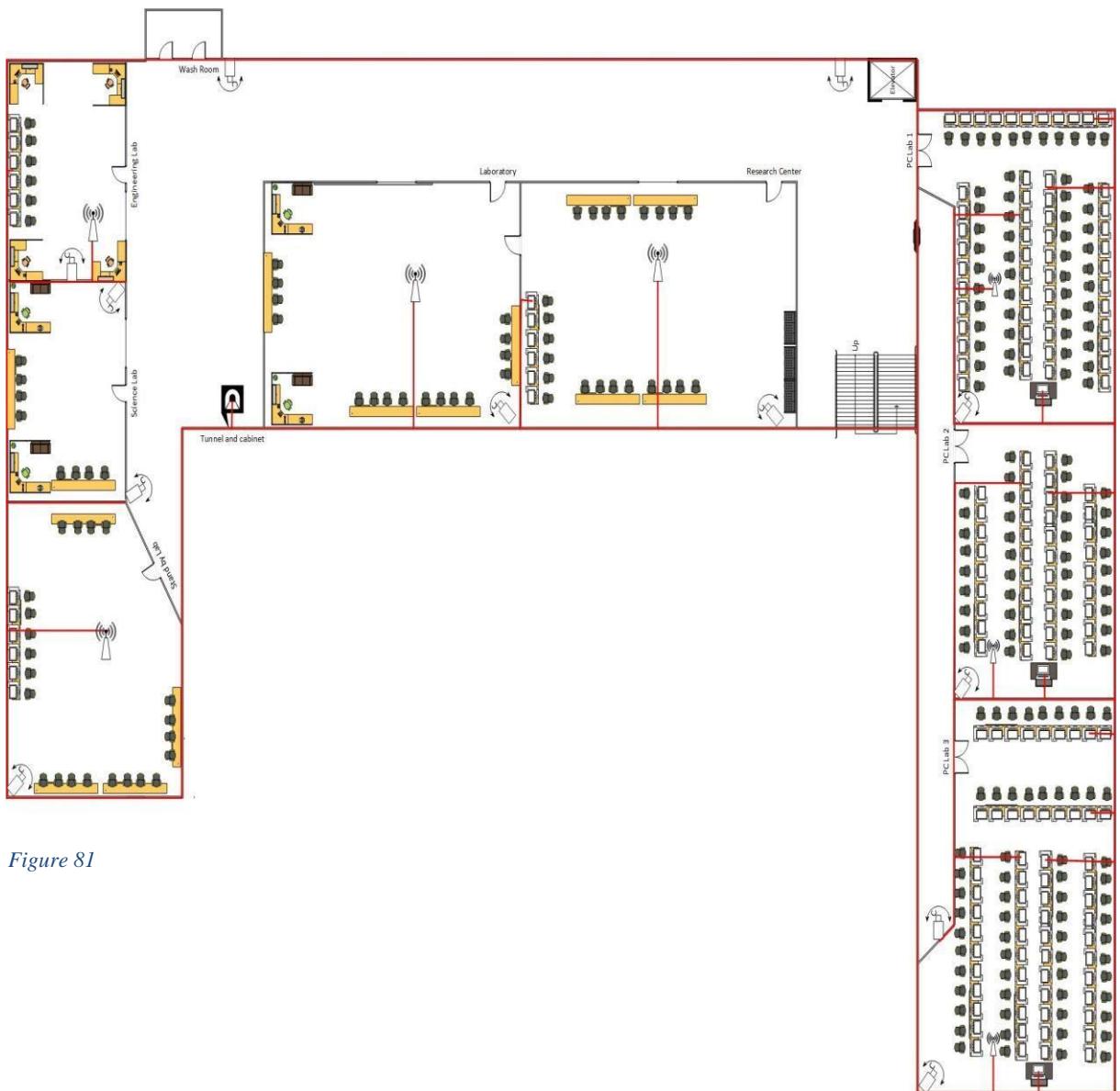


Figure 81

2nd Floor Includes

- Engineering Lab
- Science Lab
- Standby Lab
- Laboratory
- Research Centre
- Computer Labs
- Wash rooms

3rd Floor

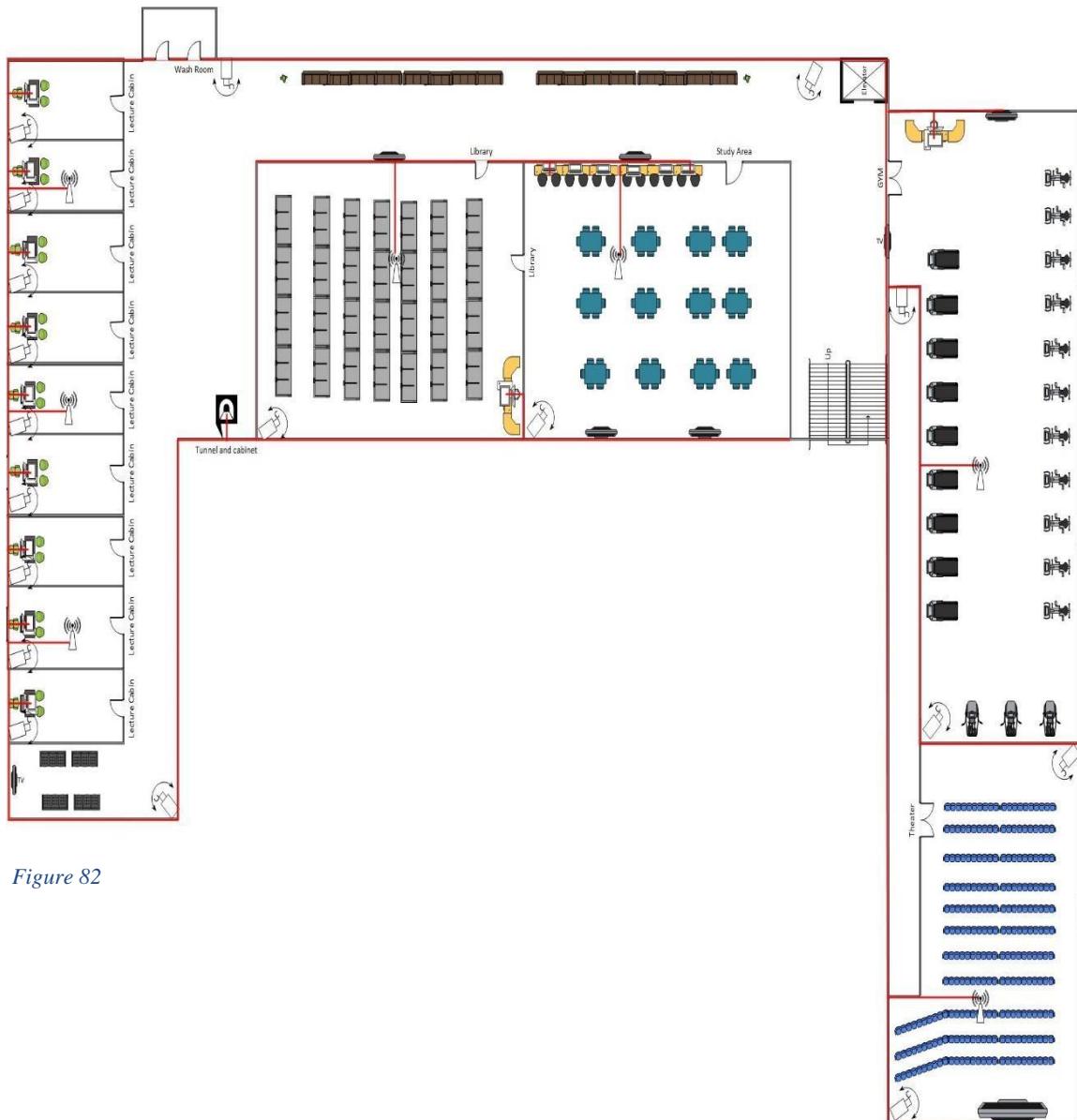


Figure 82

3rd Floor Includes

- Lecture Cabins
- Theatre
- GYM
- Library
- Study Area
- Wash Rooms

4th Floor

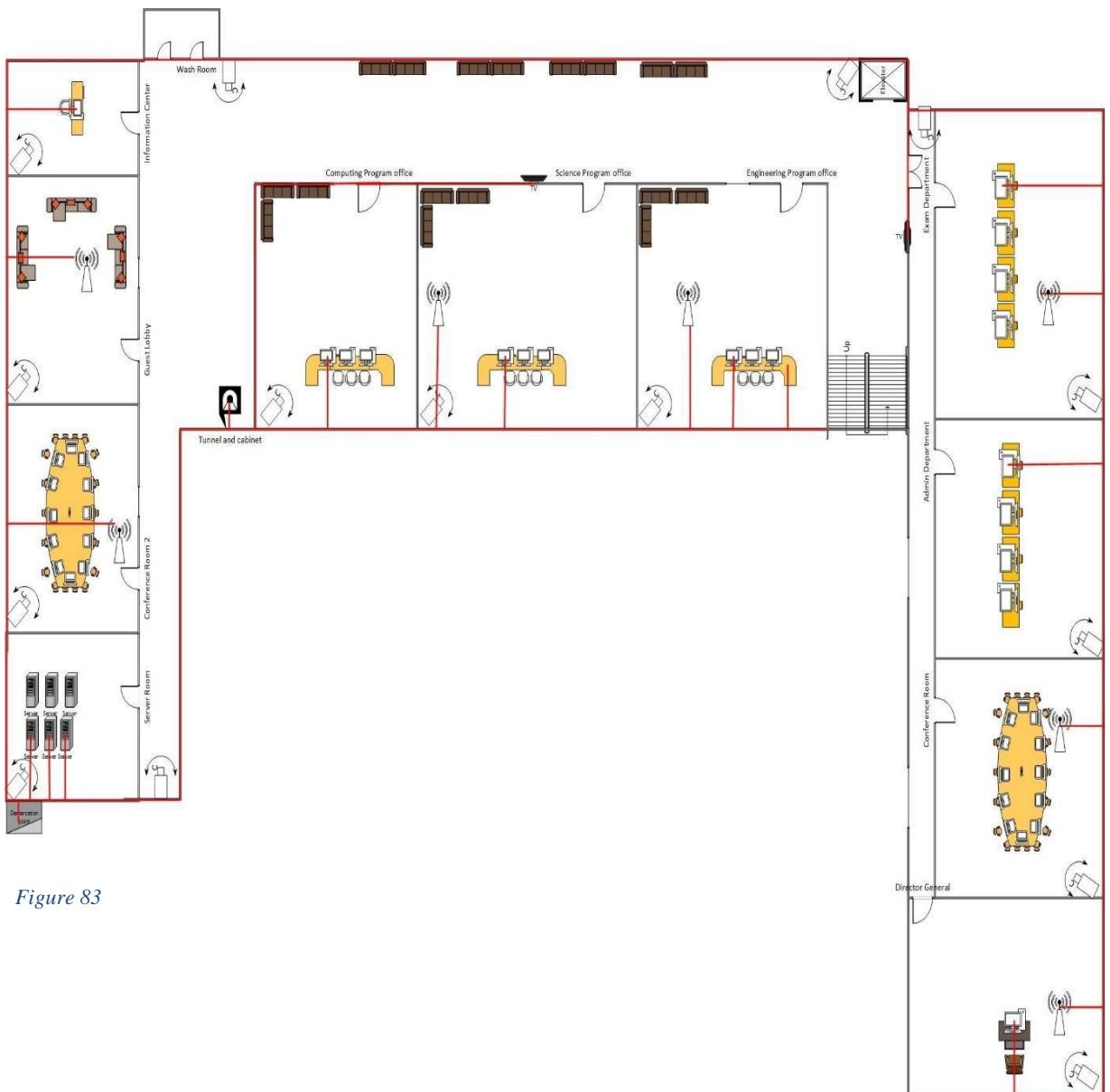


Figure 83

4th Floor Includes

- Server Room
- Engineering Program Office
- Conference Rooms
- Wash Rooms
- Director General Room
- Admin Department
- Exam Department
- Science Program office
- Computing Program Office

Annexure 2: Devices

Firewall Netgate 8200



Figure 84

- pfSense software is a leading open source firewall and router distribution based on FreeBSD that is functionally competitive with expensive, proprietary commercial firewalls. pfSense software-based appliances can be configured as a stateful packet filtering firewall, a LAN or WAN router, VPN Appliance, DHCP Server, DNS Server, or can be configured for other applications and special purpose appliances.
 - Intel® Atom® C3758R with QAT, 8-core @ 2.4 GHz
 - Storage :- 128GB NVMe M.2 SSD
 - Memory :- 16 GB DDR4
 - Consol Port :- x auto-detect console port: "Cisco pinout" RJ45 + micro-USB
 - USB Port :- 2 x USB 3.0 jacks (USB-A female) (located on Right Side Rear)
 - Enclosure :- 10 x 7.88 x 1.88 inches
 - Cooling :- Active - integrated quiet chassis fan with onboard control , External ITE P/S AC/DC 100-240V, 50-60 Hz, 12V 5.0A (60W), threaded (locking) barrel connector.
 - Power :- AC Inlet: IEC320-C7 (2 PIN) - Power Cord: One US, UK, EU or ANZ power cord included
 - Environmental :- 0°C (32°F) to 40°C (104°F) - ambient

- Certifications :- FCC (Class B), IEC / CE, CB, UL, RoHS, RCM

Cisco UCS C220 M6



Figure 85

- C220 M6 servers can be deployed as standalone servers, part of a Cisco UCS managed environment, or via Cisco Intersight. When used in combination with Cisco Intersight, the C220 M6 brings the power and automation of unified computing to enterprise applications, including Cisco SingleConnect technology, drastically reducing switching and cabling requirements.
- Supports the third-generation Intel Xeon Scalable CPU, with up to 40 cores per socket
- Up to 32 DDR4 DIMMs for improved performance including higher density DDR4 DIMMs (16 DIMMs per socket)
- 16x DDR4 DIMMs + 16x Intel Optane persistent memory modules for up to 10 TB of memory
- Up to 3 PCIe 4.0 slots plus a modular LAN on Motherboard (mLOM) slot
- Support for Cisco UCS VIC 1400 Series adapters as well as third-party options
- Up to 10 SAS/SATA or NVMe disk drives
- M.2 boot options
- Up to three GPUs supportedModular LAN-On-Motherboard (mLOM) slot that can be used to install a Cisco UCS Virtual Interface Card (VIC) without consuming a PCIe slot, supporting quad port 10/40 Gbps or dual port 40/100 Gbps network connectivity

- Dual embedded Intel x550 10GBASE-T LAN-On-Motherboard (LOM) ports
- Modular M.2 SATA SSDs for boot

Cisco Catalyst 9300 Model(C9300-24T-A)



Figure 86

- Cisco Catalyst C9300-24T-A. Switch type: Managed, Switch layer: L2/L3. Basic switching RJ-45 Ethernet ports type: Gigabit Ethernet (10/100/1000), Basic switching RJ-45 Ethernet ports quantity: 24. Full duplex. MAC address table: 32000 entries, Switching capacity: 208 Gbit/s. Networking standards: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3ad, IEEE.... Power over Ethernet (PoE). Rack mounting, Form factor: 1U

Cisco Catalyst 2960 PoE



Figure 87

Product Highlights

Cisco Catalyst 2960-Plus switches feature:

- 24 or 48 Fast Ethernet ports
- Small Form-Factor Pluggable (SFP) and 1000BASE-T Gigabit Ethernet uplinks
- IEEE 802.3af-compliant Power over Ethernet (PoE)
- LAN Base or LAN Lite Cisco IOS® Software feature set

Applications and Benefits

The Cisco Catalyst 2960-Plus Series provides cost-effective, enterprise class Ethernet switching for:

- Branch offices, remote sites, and retail locations
- Conventional desktop workspaces

Benefits of the 2960-Plus include:

- Robust quality of service (QoS) that prioritizes voice and critical business applications
- Flexible security features that can limit access to the network and mitigate threats. Tools that reduce total cost of ownership through simplified operations and automation

Cisco 9100 Access Point



Figure 88

- Cisco Catalyst 9100 Access Points are wireless access points designed for providing integrated security for IoT devices and mobile clients¹. They are the follow-ups to the Cisco Aironet 1800 Series Access Points, specifically the Cisco Aironet 1830 and 1850 Series². The Cisco Catalyst 9100 Access Points come equipped with Wi-Fi 6 capabilities, better industrial design, and improved RF performance, and deliver reliability, security, and intelligence at scale².

Hikvision DS-2CD1043G0-I



Figure 89

- **Image Sensor**-1/3" Progressive Scan CMOS
- **Min. Illumination**-Color: 0.01 Lux @ (F1.2, AGC ON), 0.018 Lux @ (F1.6, AGC ON), 0 Lux with IR
- **Shutter Speed**-1/3 s to 1/100,000 s
- **Wide Dynamic Range**-120dB
- **Day & Night**-IR Cut Filter
- **Angle -Adjustment**Pan: 0° to 355°, tilt: 0° to 75°, rotate: 0° to 355°

Lens

- **Focus**-Fixed
- **Lens Type**-2.8/4/6/8 mm
- **FOV**-2.8 mm, horizontal FOV: 103°, vertical FOV: 58°, diagonal FOV: 123°, 4 mm, horizontal FOV: 83°, vertical FOV: 45°, diagonal FOV: 99°, 6 mm, horizontal FOV: 51°, vertical FOV: 29°, diagonal FOV: 58°, 8 mm, horizontal FOV: 39°, vertical FOV: 22°, diagonal FOV: 45°
- **Aperture**-F1.6
- **Lens Mount**-M12
- **Aperture Type**-Fixed