HealthyLife Hospital Capstone Project – Full Network Documentation

---

Part 1 – Introduction

We completed the NSA630 Capstone Project for HealthyLife Hospital, which required us to design, configure, and deploy a fully functional IT infrastructure.

Our design incorporated a complex and realistic hospital IT environment involving both physical and virtual components. We used four Cisco routers, four switches, a firewall, and multiple virtualized servers to build the infrastructure. We structured our network around seven VLANs to support different hospital departments: Outpatient, Inpatient, Research, Administration, Guest and IT. Each VLAN was assigned its own subnet, and we implemented Layer 3 routing and segmentation across the network.

To simulate enterprise-level operations, we deployed core services such as Active Directory Domain Services (AD DS), DNS and DHCP. A secondary server was set up as a backup and a RADIUS Server to ensure data redundancy and business continuity. Additionally, we integrated Microsoft 365 for cloud-based email services, allowing us to simulate external email communication using our custom domain.

We implemented security hardening measures across all network devices and endpoints. This included access control lists (ACLs), router and switch security best practices, and end-user device protections. We also introduced high availability protocols like HSRP and EtherChannel to prevent downtime in the event of equipment failure.

Moreover, we developed a front-end web page using pure HTML, CSS, and JavaScript and deployed it on GitHub Pages. This page was linked to a backend Python (Flask) application to simulate appointment scheduling, making our infrastructure interactive and user-friendly. The website is publicly accessible via: https://walidasakor.github.io/Capstone/

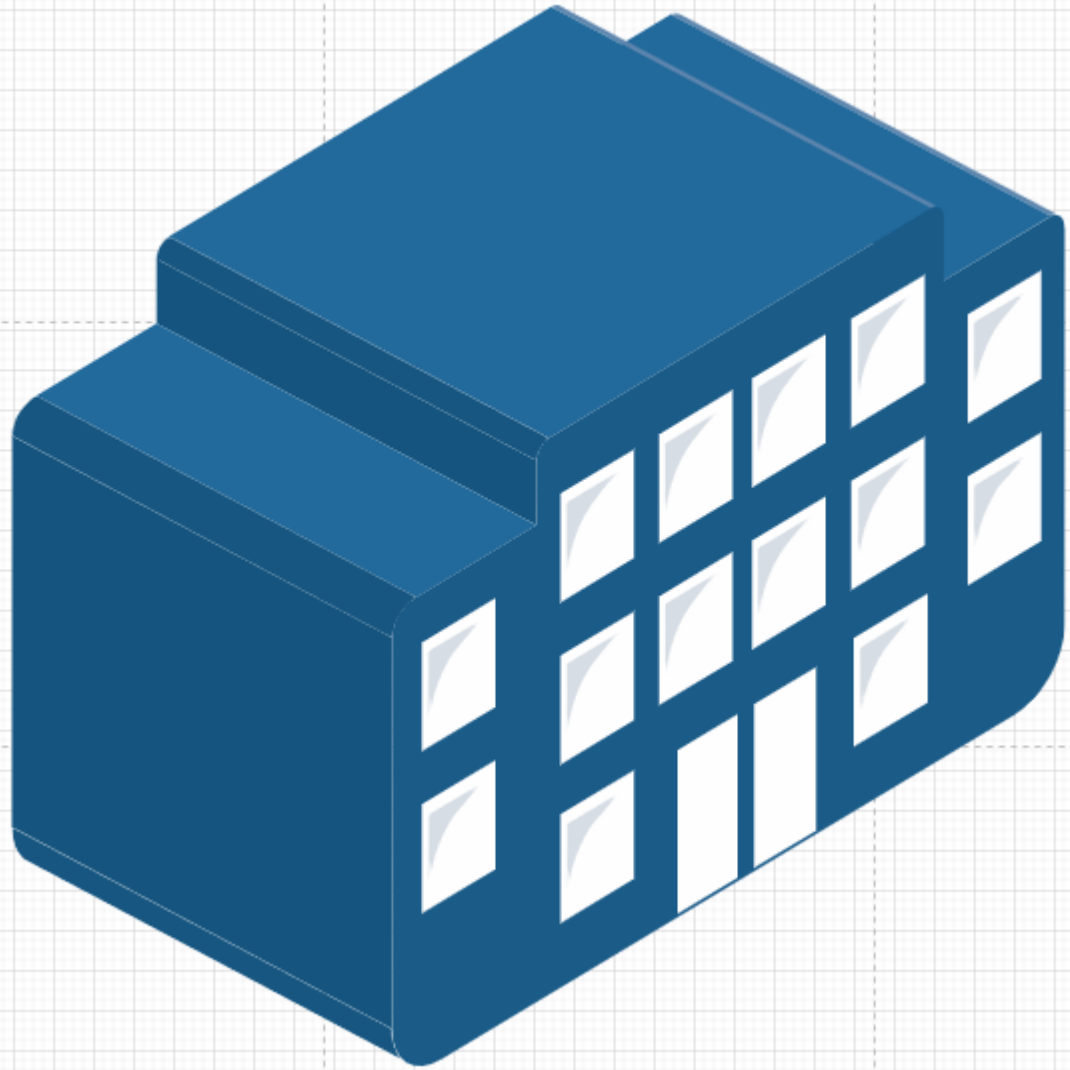
All components of the project were rigorously tested, documented, and demonstrated. Through this capstone, we demonstrated our ability to apply theoretical knowledge to a real-world scenario while meeting technical, organizational, and security requirements.

Part 2 – Physical and Logical Topology

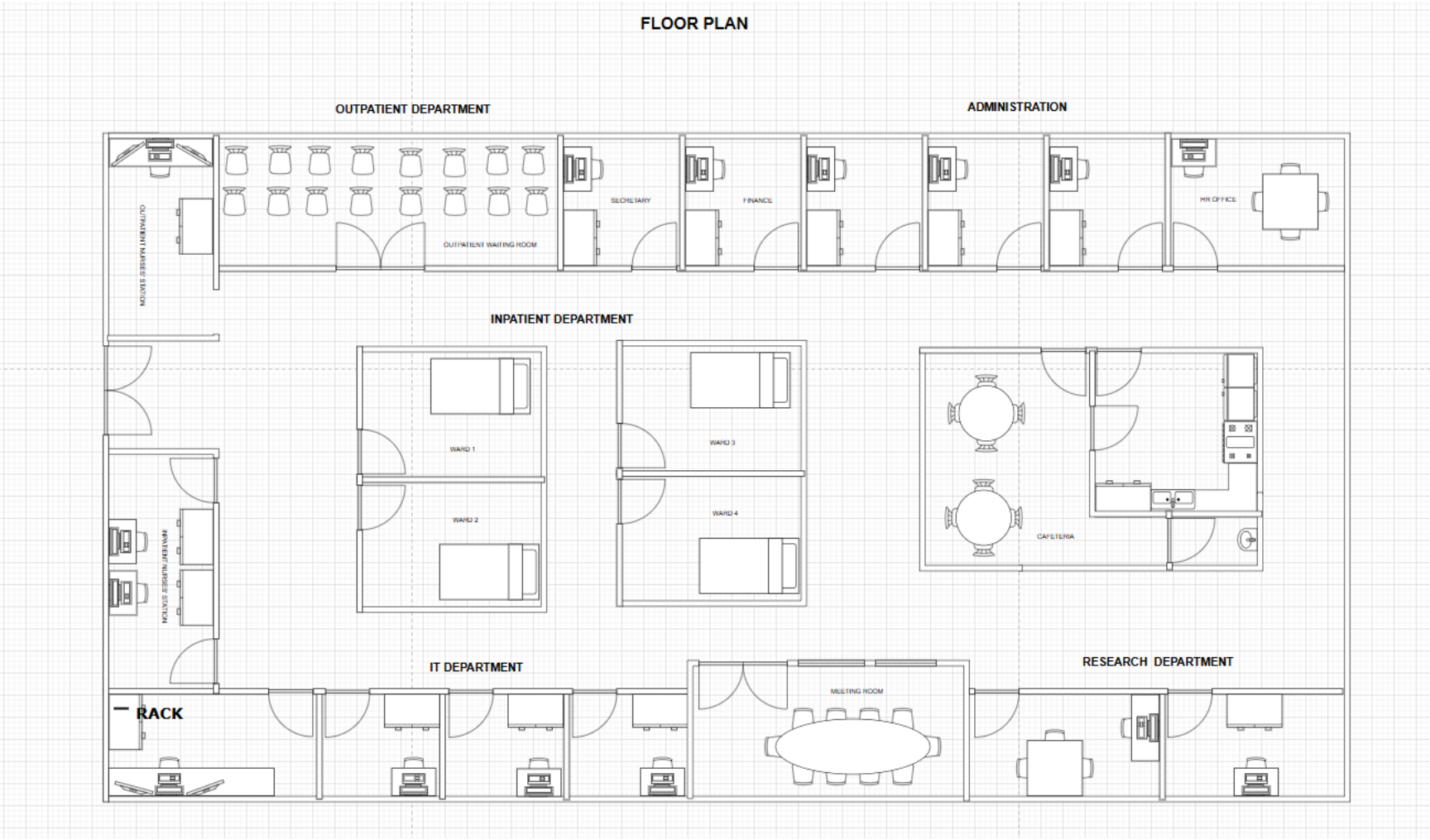
1. Physical Topology Design:

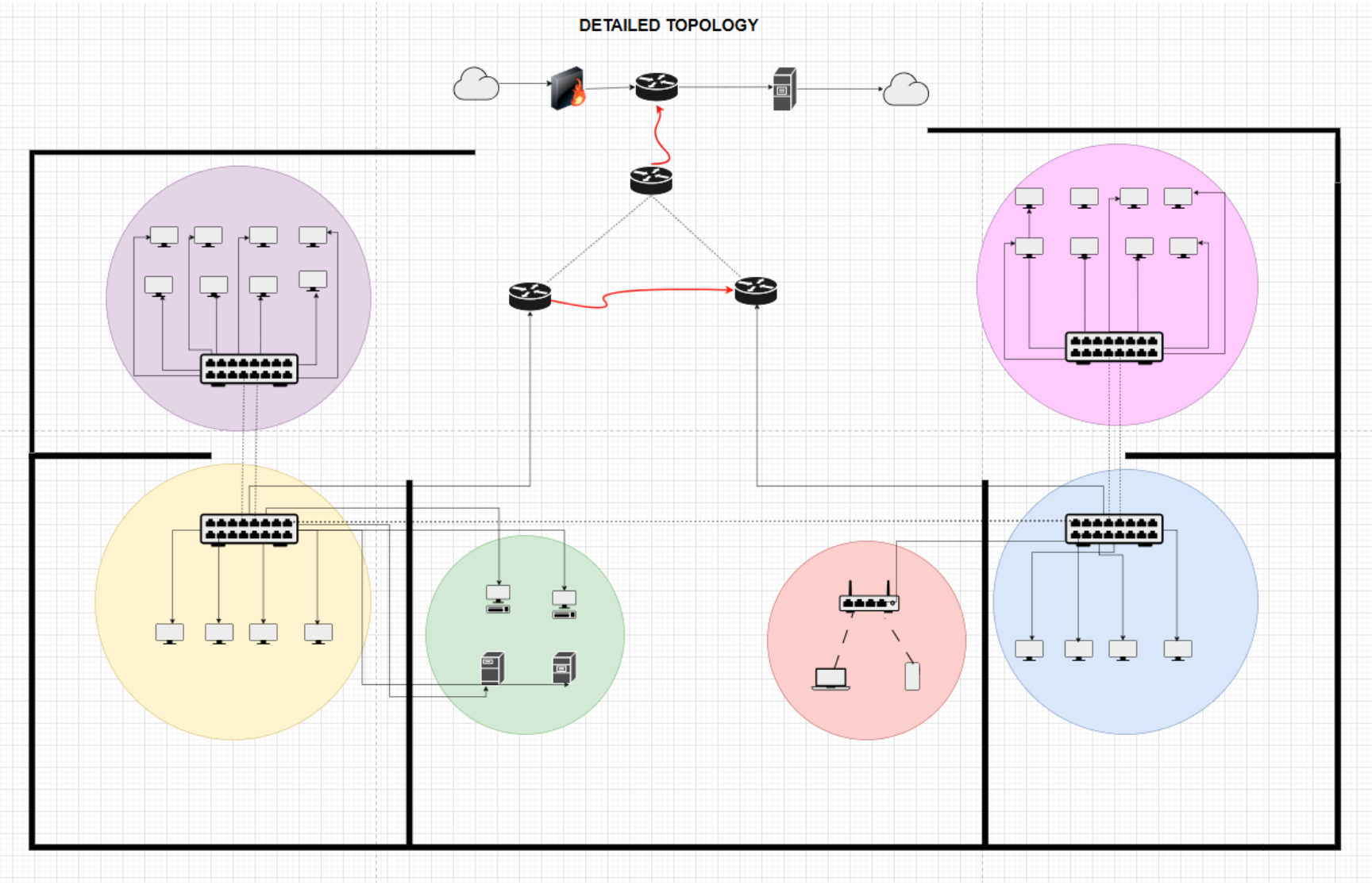
- We placed four Cisco routers (HealthyLife_RG, RH, RE and Edgerouter_RF) and four switches (HealthyLife_SG, SH, SE and SF) on the rack.
- We connected router HealthyLife_RG to Switch HealthyLife_SF, R2 to SW2, R3 to SW3, and R4 to SW4.
- We used straight-through cables from PCs and servers to the respective switches.
- We used crossover cables to interconnect switches where needed.
- We connected the firewall between the Edgerouter and the ISP to secure the edge of our network.

HEALTHYLIFE HOSPITAL BUILDING

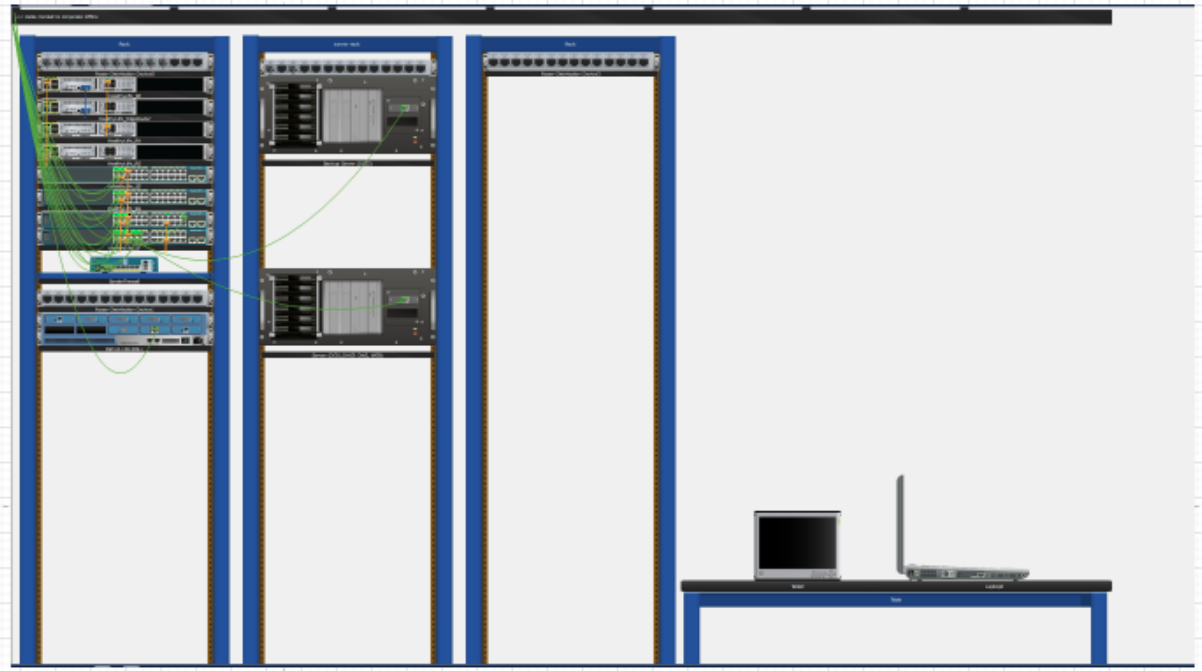


FLOOR PLAN


OUTPATIENT DEPARTMENT
ADMINISTRATION
OUTPATIENT NURSES STATION
OUTPATIENT WAITING ROOM
SECRETARY
FINANCE
HR OFFICE
INPATIENT DEPARTMENT
WARD 1
WARD 2
WARD 3
WARD 4
CAFETERIA
INPATIENT NURSES STATION
IT DEPARTMENT
RESEARCH DEPARTMENT
MEETING ROOM
RACK


DETAILED TOPOLOGY

WIRING CLOSET

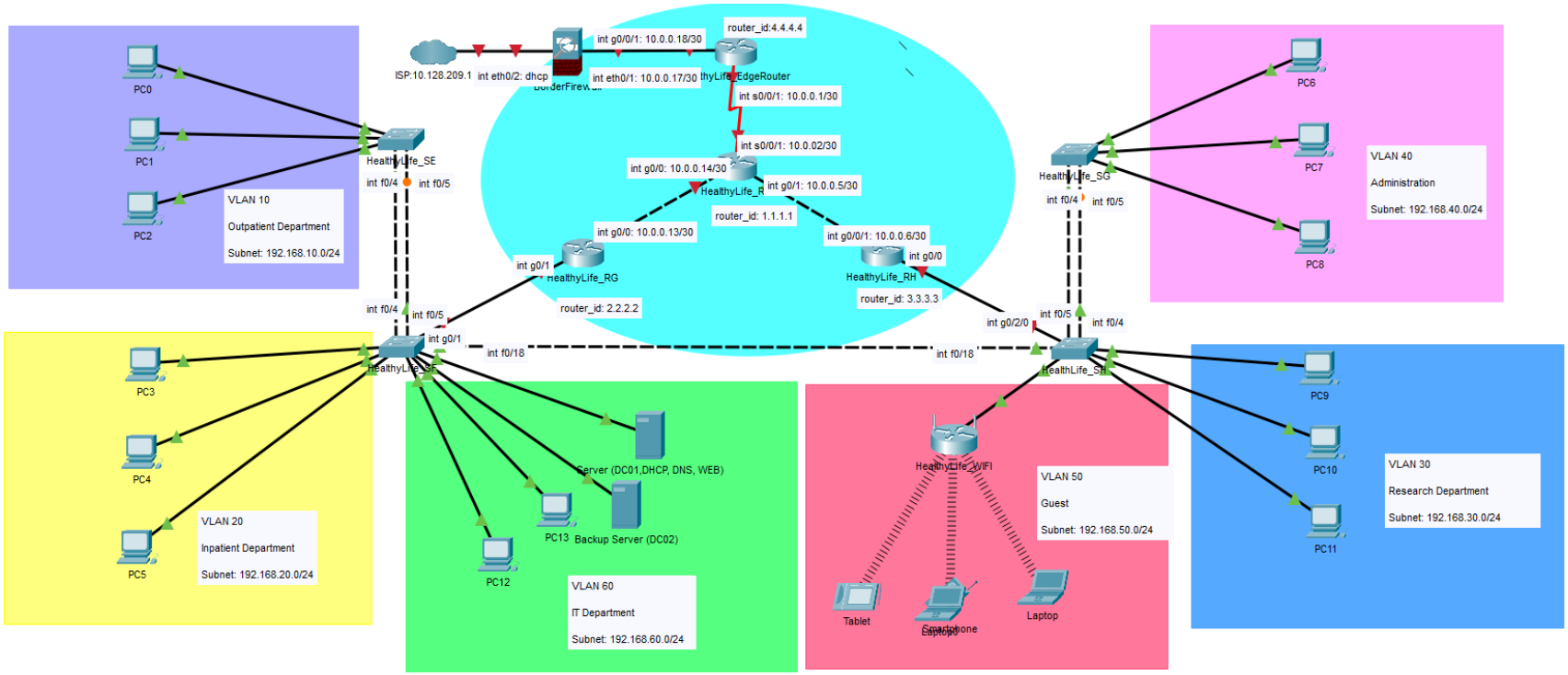


2. Logical Topology Design:

- We created the following VLANs and associated IP address subnets:

VLAN	VLAN Name	Subnet / CIDR	Gateway IP	DHCP Range	Reserved IP's
10	Outpatients	192.168.10.0/ 24	192.168.10.1	192.168.10.11-192.168.10.252	192.168.10.1-192.168.10.10
20	Inpatients	192.168.20.0/ 24	192.168.20.1	192.168.20.11-192.168.20.252	192.168.20.1-192.168.20.10
30	Research	192.168.30.0/ 24	192.168.30.1	192.168.30.11-192.168.30.252	192.168.30.1-192.168.30.10
40	Administration	192.168.40.0/ 24	192.168.40.1	192.168.40.11-192.168.40.252	192.168.40.1-192.168.40.10
50	Guest	192.162.50.0/ 24	192.168.50.1	192.168.50.11-192.168.50.252	192.168.50.1-192.168.50.10
60	IT	192.162.60.0/ 24	192.168.60.1	192.168.60.11-192.168.60.252	192.168.60.1-192.168.60.10

- We configured trunk ports on switch-to-router and switch-to-switch connections to allow VLAN traffic to flow.


PC0
PC1
PC2
VLAN 10
Outpatient Department
Subnet: 192.168.10.0/24
HealthyLife_SE
int f0/4
int f0/5
ISP:10.128.209.1
int eth0/2: dhcp
int g0/0/1: 10.0.0.18/30
int eth0/1: 10.0.0.17/30
router_id:4.4.4.4
int s0/0/1: 10.0.0.1/30
int s0/0/1: 10.0.0.2/30
int g0/0: 10.0.0.14/30
int g0/1: 10.0.0.5/30
router_id: 1.1.1.1
int g0/0: 10.0.0.13/30
int g0/0/1: 10.0.0.6/30
int g0/1
HealthyLife_RG
router_id: 2.2.2.2
HealthyLife_RH
int g0/0
router_id: 3.3.3.3
PC6
PC7
PC8
VLAN 40
Administration
Subnet: 192.168.40.0/24
HealthyLife_SG
int f0/4
int f0/5
int f0/4
int f0/5
int g0/1
int f0/18
int f0/18
int g0/2/0
int f0/5
int f0/4
PC3
PC4
PC5
VLAN 20
Inpatient Department
Subnet: 192.168.20.0/24
Server (DC01,DHCP, DNS, WEB)
PC13
Backup Server (DC02)
PC12
VLAN 60
IT Department
Subnet: 192.168.60.0/24
HealthyLife_WIFI
VLAN 50
Guest
Subnet: 192.168.50.0/24
Tablet
Laptop
PC9
PC10
PC11
VLAN 30
Research Department
Subnet: 192.168.30.0/24

Addressing Table

Device Name	Interface	IP Address	Description	Subnet	Status
HealthyLife_RH	G0/0/0.10	192.168.10.2	VLAN 10 sub interface on the RH	255.255.255.0	UP
HealthyLife_RH	G0/0/0.20	192.168.20.2	VLAN 20 sub interface on the RH	255.255.255.0	UP
HealthyLife_RH	G0/0/0.30	192.168.30.1	VLAN 30 sub interface on the RH	255.255.255.0	UP
HealthyLife_RH	G0/0/0.40	192.168.40.1	VLAN 40 sub interface on the RH	255.255.255.0	UP
HealthyLife_RH	G0/0/0.50	192.168.50.1	VLAN 50 sub interface on the RH	255.255.255.0	UP
HealthyLife_RH	G0/0/0.60	192.168.60.2	VLAN 60 sub interface on the RH	255.255.255.0	UP
HealthyLife_RH	G0/0/0.99	N/A	NATIVE VLAN	N/A	UP
HealthyLife_RH	G0/0/0	N/A	N/A	N/A	UP
HealthyLife_RG	G0/0	10.0.0.13	Interface to ROUTER (RE)	255.255.255.0	UP
HealthyLife_RG	G0/1.10	192.168.10.1	VLAN 10 sub interface on the RG	255.255.255.0	UP
HealthyLife_RG	G0/1.20	192.168.20.1	VLAN 20 sub interface on the RG	255.255.255.0	UP
HealthyLife_RG	G0/1.30	192.168.30.2	VLAN 30 sub interface on the RG	255.255.255.0	UP
HealthyLife_RG	G0/1.40	192.168.40.2	VLAN 40 sub interface on the RG	255.255.255.0	UP
HealthyLife_RG	G0/1.50	192.168.50.2	VLAN 50 sub interface on the RG	255.255.255.0	UP
HealthyLife_RG	G0/1.60	192.168.60.1	VLAN 60 sub interface on the RG	255.255.255.0	UP
HealthyLife_RG	G0/1	N/A	NATIVE VLAN	N/A	UP
HealthyLife_RF	G0/0/0	N/A	N/A	N/A	DOWN
HealthyLife_RF	G0/0/1	10.0.0.18	Connection to the firewall interface	255.255.255.0	UP
HealthyLife_RF	S0/1/0	N/A	N/A	N/A	DOWN
HealthyLife_RF	S0/1/1	N/A	N/A	N/A	DOWN
HealthyLife_RE	G0/0	10.0.0.14	Connection to the ROUTER (RG) G0/0/0	255.255.255.0	UP
HealthyLife_RE	G0/1	10.0.0.5	Connection to the ROUTER (RH) G0/0/1	255.255.255.0	UP
HealthyLife_RE	S0/0/0	N/A	N/A	N/A	DOWN

HealthyLife_RE	S0/0/1	10.0.0.2	Connection to the ROUTER (RF) S0/0/1	255.255.255.0	UP
HealthyLife_SE	FastEthernet0/4	N/A	EtherChannel group LACP to SWITCH (SF)	N/A	UP
HealthyLife_SE	FastEthernet0/5	N/A	EtherChannel group LACP to SWITCH (SF)	N/A	UP
HealthyLife_SF	FastEthernet0/4	N/A	EtherChannel group LACP to SWITCH (SE)	N/A	UP
HealthyLife_SF	FastEthernet0/5	N/A	EtherChannel group LACP to SWITCH (SE)	N/A	UP
HealthyLife_SF	FastEthernet0/17	N/A	Connection to main server VLAN 60	N/A	UP
HealthyLife_SF	FastEthernet0/18	N/A	Connection to SWITCH (SH) f0/18	N/A	UP
HealthyLife_SF	FastEthernet0/22	N/A	Connected To PC VLAN 60	N/A	UP
HealthyLife_SG	FastEthernet0/4	N/A	EtherChannel group LACP to SWITCH (SH)	N/A	UP
HealthyLife_SG	FastEthernet0/5	N/A	EtherChannel group LACP to SWITCH (SH)	N/A	UP
HealthyLife_SG	FastEthernet0/16	N/A	Connected To PC VLAN 30	N/A	UP
HealthyLife_SH	FastEthernet0/4	N/A	EtherChannel group LACP to SWITCH (SG)	N/A	UP
HealthyLife_SH	FastEthernet0/5	N/A	EtherChannel group LACP to SWITCH (SG)	N/A	UP
HealthyLife_SH	FastEthernet0/18		Connection to SWITCH (SF) f0/18	N/A	UP
HealthyLife_SH	G0/2		Connection ROUTER (RH) G0/0/0	N/A	UP

Protocol	Device Name	Interface	Virtual IP Address	Default Gateway	Priority
VRRP	HealthyLife_RG	G0/1.10	192.168.10.254	192.168.10.1	110
		G0/1.20	192.168.20.254	192.168.20.1	110
		G0/1.30	192.168.30.254	192.168.30.1	110
		G0/1.40	192.168.40.254	192.168.40.1	110
		G0/1.50	192.168.50.254	192.168.50.1	110
		G0/1.60	192.168.60.254	192.168.60.1	110
VRRP	HealthyLife_RH	G0/0/0.10	192.168.10.254	192.168.10.2	100
		G0/0/0.20	192.168.20.254	192.168.20.2	100
		G0/0/0.30	192.168.30.254	192.168.30.2	100
		G0/0/0.40	192.168.40.254	192.168.40.2	100
		G0/0/0.50	192.168.50.254	192.168.50.2	100
		G0/0/0.60	192.168.60.254	192.168.60.2	100

Page 3 – Device Configuration Steps

1. Switch Configuration:

- We accessed each switch using a console cable connected to our PC.
- We assigned hostnames to each switch for clarity and documentation.

- We configured trunk ports.
- We created VLANs and named them.

2. Router Configuration (Router-on-a-Stick):

- We configured sub-interfaces on the router's trunk link:

```
interface g0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
```

- We repeated this for each VLAN with the corresponding encapsulation ID and IP address.

3. Routing Configuration:

- We enabled OSPF routing protocol to allow router communication.

```
router ospf 10
 network 10.0.0.0 0.0.0.255 area 0
```

- We verified OSPF adjacency using:

```
show ip ospf neighbor
```

Page 4 – High Availability & Redundancy

1. EtherChannel Configuration:

- We bundled switch interfaces for redundancy and load balancing:

```
interface range fa0/4 - 5
 channel-group 1 mode active
```

2. HSRP (FHRP):

- We implemented Hot Standby Router Protocol to ensure gateway redundancy:

```
interface g0/1.10
 standby 1 ip 192.168.10.254
 standby 1 priority 110
 standby 1 preempt
```

- We repeated this for each VLAN using a unique group number.

3. Redundant Uplinks:

- We connected each access switch to two routers.
- We tested failover scenarios by disabling primary router interfaces and observed automatic failover.

Page 5 – Server Deployment & Service Configuration

1. Active Directory:

- We installed Active Directory Domain Services on Windows Server.
- We promoted the server to a Domain Controller with domain: `healthylife.local`
- We created Organizational Units (OU) and populated them with user accounts.

2. DNS and DHCP:

- We installed the DNS Server role and configured forward and reverse lookup zones.
- We installed the DHCP Server role and defined scopes for each VLAN's subnet.

3. Backup Server:

- We installed Windows Server Backup.
- We scheduled full backups to a secondary hard disk every 24 hours.

Page 6 – Email Configuration & External Services

1. Microsoft 365 Configuration:

- We registered our hospital domain with Microsoft 365.
- We created user mailboxes and distribution lists.
- We configured DNS records to support mail flow.

2. Testing Mail Flow:

- We sent and received test emails between internal and external addresses.
- We verified connectivity using `HS-Mailflow` and `nslookup` tools.

Page 7 – Network Security & Hardening

1. Device Hardening:

- We disabled unused ports on switches and routers.
- We configured encrypted remote access (SSH) and disabled Telnet.
- We configured the servers to limit access to only users in VLAN 60 (IT Department VLAN)

2. Firewall Configuration:

- We configured basic firewall rules to allow HTTP, HTTPS, SMTP, and block all other unsolicited traffic.
- We tested rules by simulating port scans.

3. Endpoint Protection:

- We enabled Windows Defender on all virtual machines.
- We configured firewall rules on servers and user devices.

Page 8 – Monitoring & Troubleshooting

Monitoring Tools:

- We used `show`, `ping`, and `traceroute` commands for diagnostics.
- We reviewed logs on switches, routers, and servers for anomalies.

Page 9 – Documentation & Backups

1. Running Configs:

- We saved the final running-configs of each router and switch.
- We backed up configurations to a centralized repository.

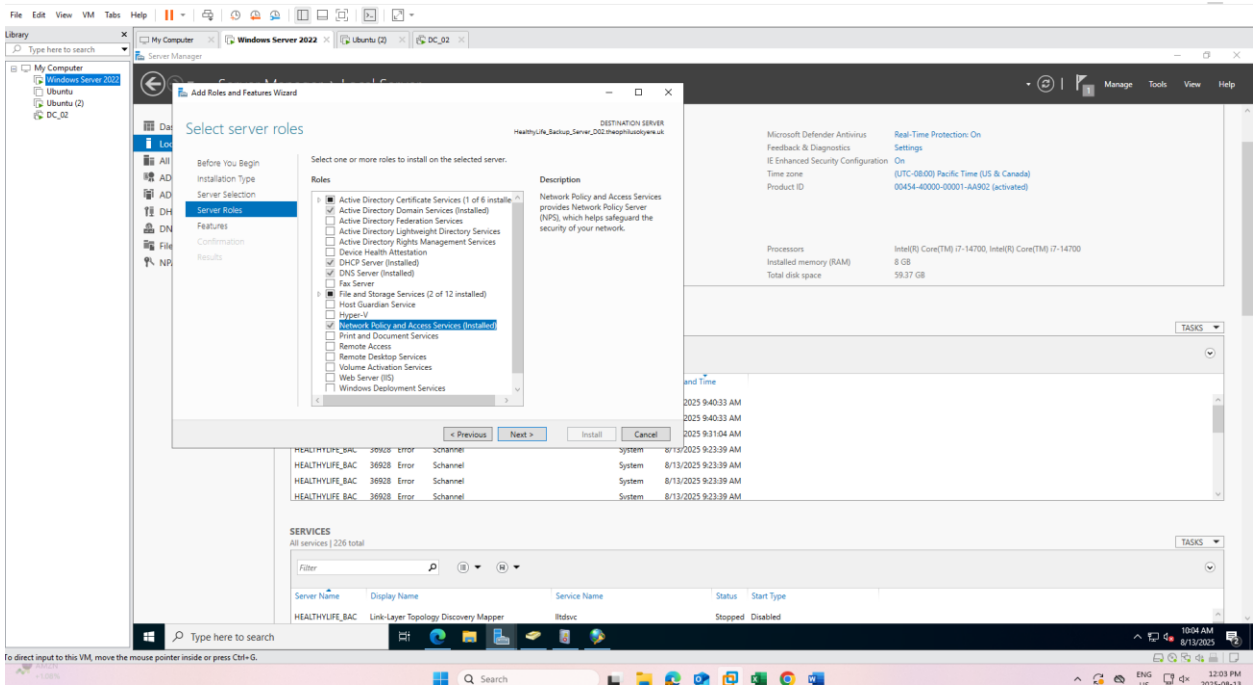
2. Diagrams & IP Tables:

- We documented physical and logical topologies.
- We maintained a master spreadsheet of IP assignments.

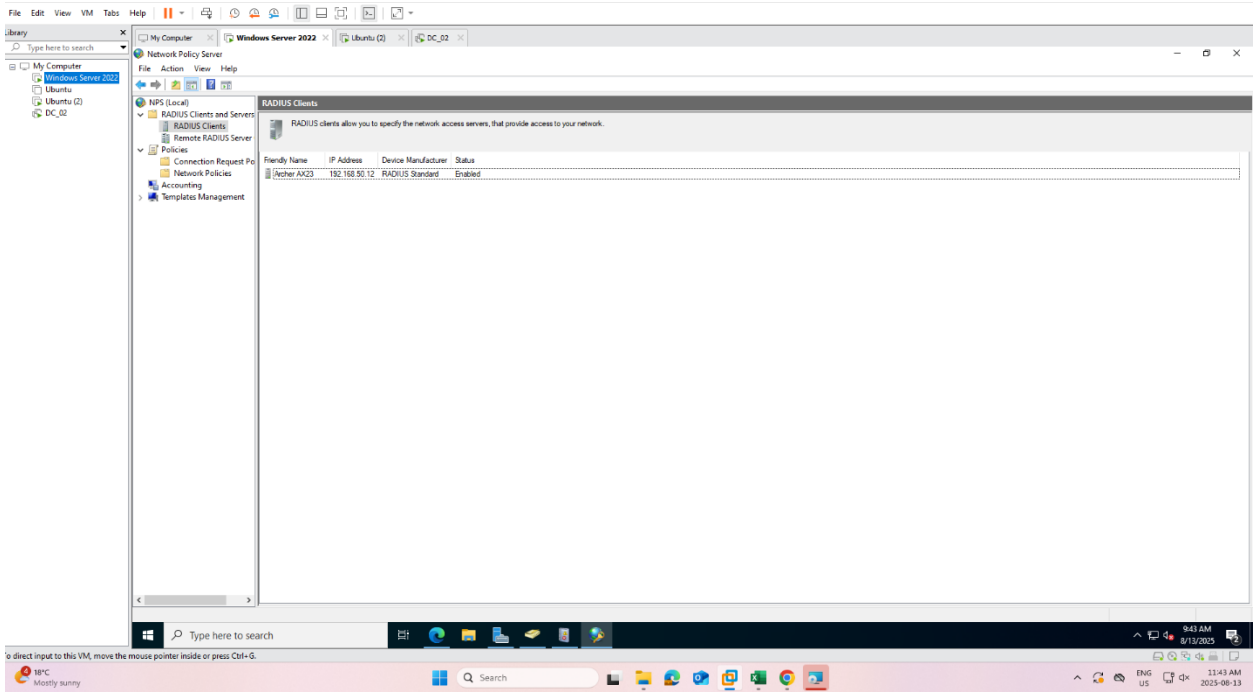
RADIUS SERVER

A RADIUS server has been implemented to manage user authentication for network access via the wireless router.

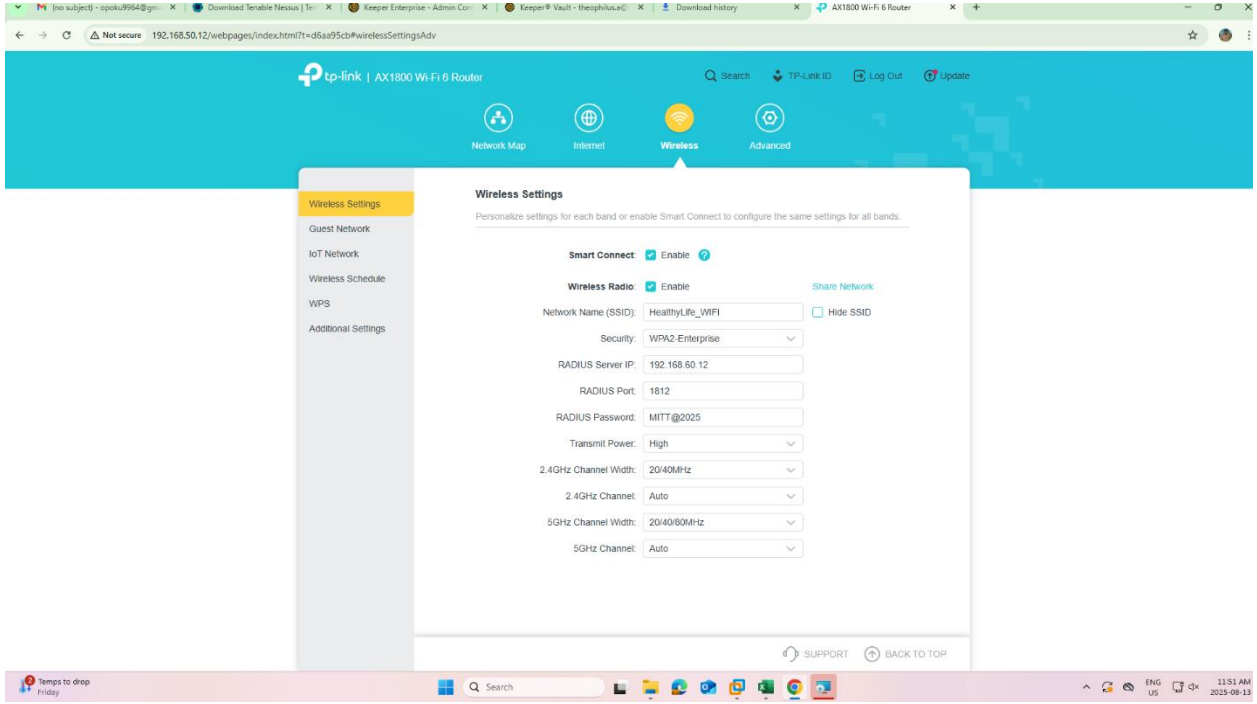
The implementation process begins with installing the Network Policy and Access Services (NPAS) role on the Windows Server.



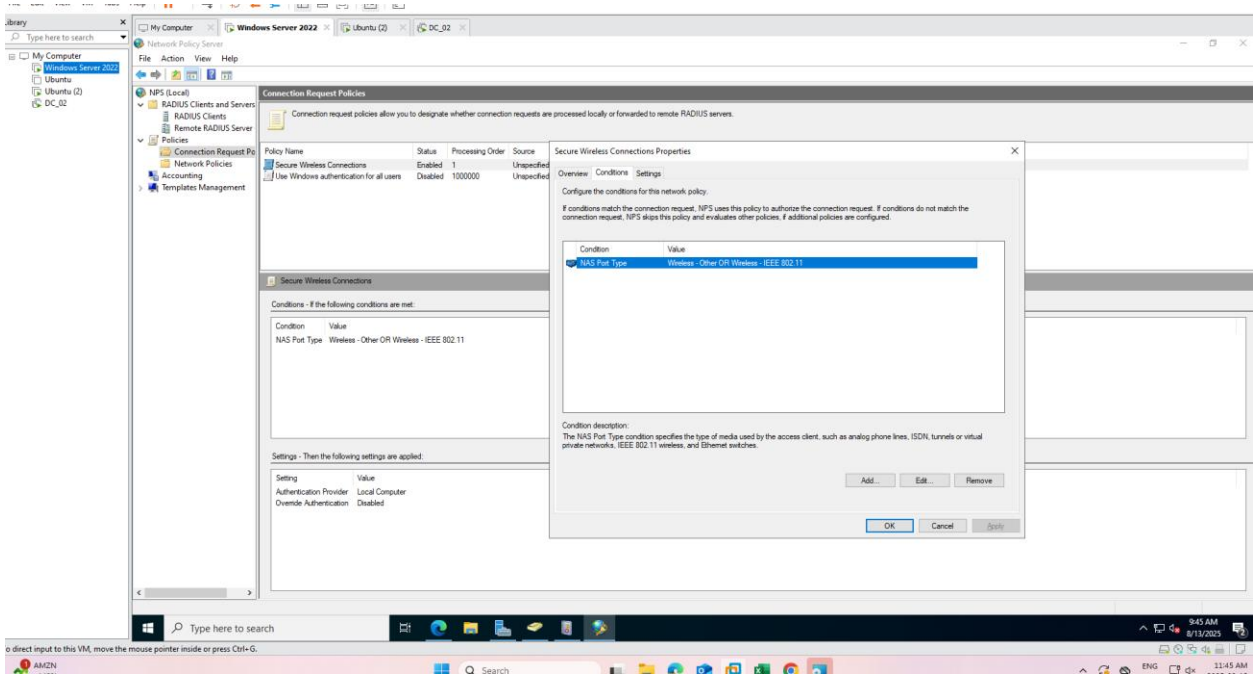
The next step involves configuring the Network Policy Server (NPS) on the Windows Server and setting up the RADIUS client

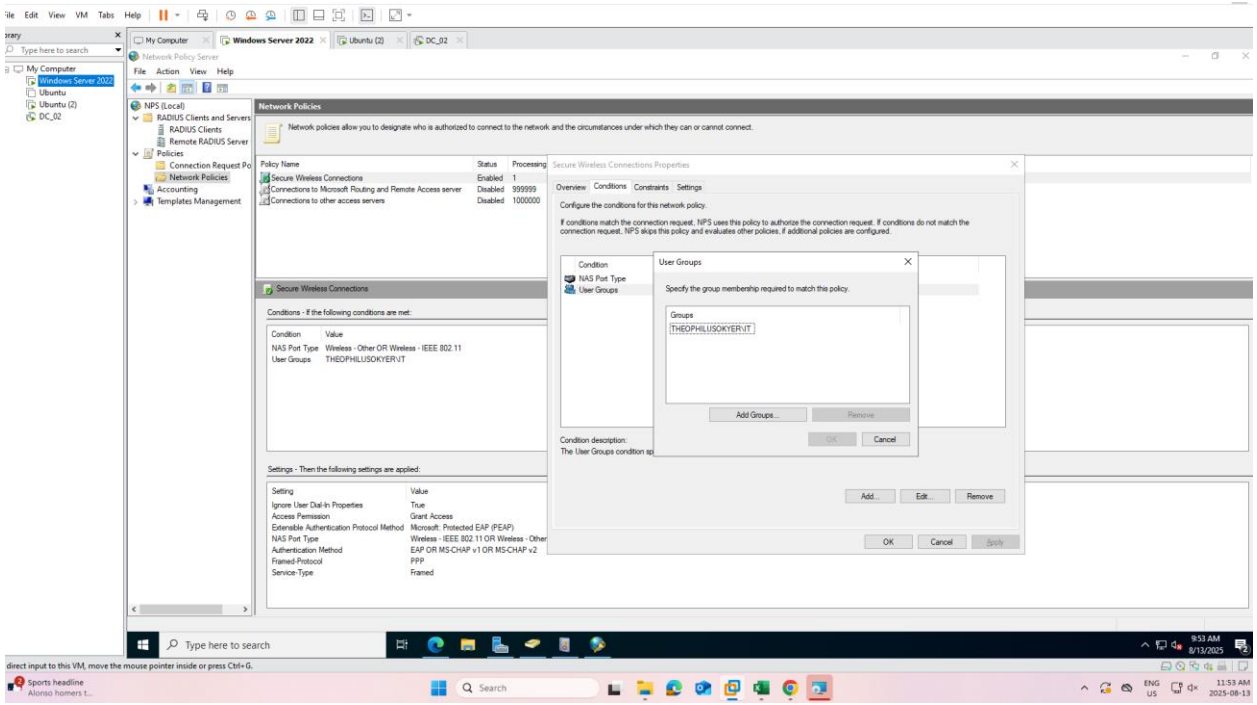


Configure the RADIUS server settings on the wireless router by specifying the IP address of the Windows Server hosting the NPS role.



Create a network policy that permits users from the Active Directory Domain Services (AD DS) to authenticate with their domain credentials when accessing the network via the wireless router.


Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server
Policies
Connection Request Po
Network Policies
Accounting
Templates Management
Connection Request Policies
Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.
Policy Name
Status
Processing Order
Source
Secure Wireless Connections
Enabled
1
Unspecified
Use Windows authentication for all users
Disabled
1000000
Unspecified
Secure Wireless Connections
Conditions - If the following conditions are met:
Condition
Value
NAS Port Type
Wireless - Other OR Wireless - IEEE 802.11
Settings - Then the following settings are applied:
Setting
Value
Authentication Provider
Local Computer
Override Authentication
Disabled
Secure Wireless Connections Properties
Overview
Conditions
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition description:
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.
Add...
Edit...
Remove
OK
Cancel
Apply
Type here to search
9:45 AM
8/13/2025
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
ENG
11:45 AM



Restrict network access based on Active Directory Domain Services (AD DS) group membership, allowing only users who are members of the **'IT Staff'** group.

Page 10 – Final Testing, Web Design & Conclusion

1. Final Testing:

We conducted an extensive and structured final testing phase to ensure the reliability, security, and functionality of the entire IT infrastructure.

- We began by testing basic end-to-end connectivity. We pinged default gateways from various end devices across all VLANs and confirmed successful communication across the subnets.
- We verified the accuracy of inter-VLAN routing by accessing services and resources located in different VLANs. For example, we connected a device in the Outpatient VLAN to the web server located in the IT VLAN and confirmed packet delivery.
- We confirmed the DHCP scope delivery and renewal by releasing and renewing IP addresses on different client machines. Each device received an IP address within the correct VLAN subnet.
- We validated HSRP (Hot Standby Router Protocol) failover by intentionally shutting down the active router interface. We monitored traffic continuity and confirmed that the standby router assumed the virtual IP address with no packet loss.
- We tested EtherChannel by disabling one of the physical interfaces forming the bundle between switches. Network traffic continued without interruption, proving that our Layer 2 redundancy was correctly configured.
- We performed DNS resolution tests by using the `nslookup` command to ensure internal and external domain names were resolved correctly.
- We logged in with test Active Directory accounts from machines in different VLANs to verify domain join status and GPO applications.
- We tested reverse DNS lookups to ensure the PTR records were appropriately configured in our internal DNS zone.
- We used the Microsoft 365 platform to send and receive emails with test accounts. We validated mail routing, domain resolution, and message delivery timing.
- We reviewed router and switch logs to ensure state changes and protocol events (e.g., HSRP transitions, interface changes) were correctly recorded and timestamped.

- We used tools like `traceroute`, `ipconfig`, `netstat`, and `ping` to check path reliability, address assignments, and port usage from the client-side perspective.
- We verified overall system stability by conducting these tests over extended periods and during simulated failures to evaluate resilience and uptime.

This comprehensive testing phase allowed us to validate every aspect of our hospital network infrastructure; from routing and switching to server operations, security protocols, and service availability. By the end of testing, we were confident that the environment was production-ready and met all critical operational and security requirements for a hospital setting.

2. Web Design Component:

- We developed and launched a hospital homepage using pure HTML, CSS, and JavaScript.
- We created a backend system using Python (Flask) to process appointment bookings.
- We hosted the front-end component on GitHub Pages.
- The website is accessible via: https://walidasakor.github.io/Capstone/

3. Web Development Steps:

- We wrote the base layout using HTML elements for structure and form fields.
- We applied custom styles using CSS to define layout responsiveness, spacing, and colors.
- We implemented dynamic form validation and animations with JavaScript.
- We built a simple Python Flask application to simulate data capture and form handling (executed in a local environment).
- We integrated both front-end and back-end and tested them locally before deployment.
- We committed the front-end files to GitHub and enabled GitHub Pages for live hosting.

- We validated the user interface for responsiveness on mobile and desktop devices.