

TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI
KHOA CÔNG NGHỆ THÔNG TIN



ĐỒ ÁN TỐT NGHIỆP

ĐỀ TÀI
THIẾT KẾ HỆ THỐNG MẠNG MÁY TÍNH CHO
BỆNH VIỆN ĐA KHOA ANH QUẤT

Giảng viên hướng dẫn : ThS. Nguyễn Trần Hiếu
Sinh viên thực hiện : Nguyễn Văn Đức
Lớp : CNTT1
Mã sinh viên : 211211969
Khóa : 62

Hà Nội – 2025

TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI
KHOA CÔNG NGHỆ THÔNG TIN



ĐỒ ÁN TỐT NGHIỆP

ĐỀ TÀI

**THIẾT KẾ HỆ THỐNG MẠNG MÁY TÍNH CHO
BỆNH VIỆN ĐA KHOA ANH QUẤT**

Giảng viên hướng dẫn : ThS. Nguyễn Trần Hiếu
Sinh viên thực hiện : Nguyễn Văn Đức
Lớp : CNTT1
Mã sinh viên : 211211969
Khóa : 62

Hà Nội – 2025

LỜI CẢM ƠN

Trong suốt quá trình thực hiện đồ án tốt nghiệp, với đề tài “Thiết kế hệ thống mạng cho Bệnh viện Đa khoa Anh Quất”, em xin được bày tỏ lòng biết ơn chân thành và sâu sắc đến những người đã đồng hành, hỗ trợ và tạo điều kiện để em hoàn thành tốt công việc của mình.

Trước hết, em xin gửi lời cảm ơn đặc biệt đến ThS. Nguyễn Trần Hiếu, giảng viên Khoa Công nghệ thông tin, Trường Đại học Giao thông Vận tải đã tận tình hướng dẫn, chỉ bảo em trong suốt quá trình thực hiện đồ án.

Đồng thời em cũng xin cảm ơn tất cả các thầy cô công tác tại khoa Công nghệ thông tin – Trường Đại học Giao thông Vận tải đã dìu dắt, chỉ bảo cho em trong suốt quá trình học tập tại trường.

Bên cạnh đó, em xin gửi lời tri ân đến gia đình và bạn bè, những người luôn là nguồn động viên, cổ vũ tinh thần to lớn để em cố gắng trong thời gian thực hiện đồ án cũng như trong cuộc sống.

Mặc dù em đã cố gắng nhưng trong quá trình thực hiện đồ án sẽ không tránh khỏi những thiếu sót và hạn chế. Em mong sẽ nhận được sự thông cảm và đóng góp chân thành của thầy cô để bài đồ án tốt nghiệp được hoàn thiện hơn.

Em xin chân thành cảm ơn!

Hà Nội, ngày ... tháng ... năm 2025

Sinh viên thực hiện

Nguyễn Văn Đức

MỤC LỤC

LỜI CẢM ƠN.....	
MỤC LỤC.....	
DANH MỤC TỪ VIẾT TẮT.....	
DANH MỤC BẢNG BIỂU.....	
DANH MỤC HÌNH ẢNH.....	
LỜI MỞ ĐẦU	1
CHƯƠNG 1 - PHÂN TÍCH VÀ THU THẬP YÊU CẦU	2
1.1. Giới thiệu chung về Bệnh viện Đa khoa Anh Quát.....	2
1.2. Xác định bài toán.....	2
1.3. Xác định yêu cầu bài toán	3
1.3.1. Phương pháp khảo sát	3
1.3.2. Khảo sát thực tiễn cơ sở hạ tầng tại bệnh viện	6
1.3.3. Tìm hiểu về các mô hình hệ thống mạng bệnh viện đã có	7
1.4. Phát biểu bài toán.....	9
1.4.1. Nội dung bài toán	9
1.4.2. Yêu cầu chức năng đối với hệ thống mạng bệnh viện.....	9
1.4.3. Yêu cầu phi chức năng cho hệ thống mạng bệnh viện.....	10
1.4.4. Kiểm thử hoạt động hệ thống.....	11
CHƯƠNG 2 - PHÂN TÍCH VÀ THIẾT KẾ	12
2.1. Công nghệ - kỹ thuật xây dựng hệ thống.....	12
2.1.1. VLSM	12
2.1.2. Routing (Định tuyến)	12
2.1.3. SVI (Switch Virtual Interface).....	12
2.1.4. DHCP (Dynamic Host Configuration Protocol)	13
2.1.5. VPN	13
2.1.6. IPsec	14
2.1.7. Kỹ thuật dự phòng.....	14
2.1.8. NAT (Network Address Translation).....	15
2.1.9. ACL (Access Control List)	15
2.1.10. Phương pháp bảo mật hệ thống	15
2.2. Kiến trúc hệ thống.....	16
2.3. Thiết kế hệ thống.....	18
CHƯƠNG 3 - XÂY DỰNG VÀ KIỂM THỬ HOẠT ĐỘNG HỆ THỐNG	21
3.1. Triển khai hệ thống.....	21
3.2. Cấu hình mô phỏng hệ thống.....	26
3.2.1. Lớp Core	26
3.2.2. Lớp Distribution.....	26

3.2.3. Lớp Access	30
3.3. Kiểm thử hoạt động hệ thống theo kịch bản	32
3.3.1. Kịch bản 1: Kiểm tra dịch vụ DHCPv4 và DHCPv6.....	32
3.3.2. Kịch bản 2: Kiểm tra dịch vụ VPN site-to-site.....	33
3.3.3. Kịch bản 3: Kiểm tra dịch vụ DNS	34
3.3.5. Kịch bản 4: Kiểm tra dịch vụ Mail	35
3.3.6. Kịch bản 5: Kiểm tra dịch vụ Web.....	36
3.3.7. Kịch bản 6: Kiểm tra kết nối mạng trong trường hợp hệ thống vẫn hoạt động bình thường	37
3.3.8. Kịch bản 7: Kiểm tra kết nối mạng khi hệ thống có sự cố	39
KẾT LUẬN	
DANH MỤC TÀI LIỆU THAM KHẢO.....	

DANH MỤC TỪ VIẾT TẮT

Từ viết tắt	Định nghĩa
ACL	Access Control List
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
ISP	Internet Service Provider
NAT	Network Address Translation
OSPF	Open Shortest Path First
STP	Spanning Tree Protocol
SVI	Switched Virtual Interface
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Mask
VPN	Virtual Private Network

DANH MỤC BẢNG BIỂU

Bảng 1.1. Bảng thông tin bệnh viện tại cơ sở 1.....	6
Bảng 1.2. Bảng thông tin bệnh viện tại cơ sở 2.....	7
Bảng 2.1. Bảng các dải địa chỉ mạng ở tầng lõi.....	18
Bảng 2.2. Bảng các dải địa chỉ mạng ở tầng phân phối.....	18
Bảng 2.3. Bảng địa chỉ dải mạng và VLAN cơ sở 1.....	19
Bảng 2.4. Bảng địa chỉ dải mạng và VLAN cơ sở 2.....	20
Bảng 2.5. Bảng địa chỉ dải mạng các Router wifi	20
Bảng 3.1. Bảng kết nối thiết bị Firewall-1.....	21
Bảng 3.2. Bảng kết nối thiết bị Firewall-2.....	21
Bảng 3.3. Bảng kết nối thiết bị SW-L3-1	21
Bảng 3.4. Bảng địa chỉ IPv4 Interface Vlan cơ sở 1	22
Bảng 3.5. Bảng địa chỉ IPv6 Interface Vlan cơ sở 1	22
Bảng 3.6. Bảng địa chỉ IPv4 Interface Vlan cơ sở 2	23
Bảng 3.7. Bảng kết nối thiết bị SW-L3-2	23
Bảng 3.8. Bảng kết nối thiết bị SW-TANG 1.....	24
Bảng 3.9. Bảng kết nối thiết bị SW-TANG 2.....	24
Bảng 3.10. Bảng kết nối thiết bị SW-TANG 3.....	24
Bảng 3.11. Bảng kết nối thiết bị SW-TANG 4.....	24
Bảng 3.12. Bảng kết nối thiết bị SW-TANG 5.....	25
Bảng 3.13. Bảng kết nối thiết bị SW-TANG 6.....	25
Bảng 3.14. Bảng kết nối thiết bị SW-TANG 7.....	25
Bảng 3.15. Bảng kết nối thiết bị SW-TANG 8.....	25
Bảng 3.16. Bảng kết nối thiết bị SW-L3-1-2	25
Bảng 3.17. Bảng kết nối thiết bị Tang 1-2.....	26
Bảng 3.18. Bảng kết nối thiết bị Tang 2-2.....	26
Bảng 3.19. Bảng kết nối thiết bị của Tang 3-2	26
Bảng 3.20. Bảng Pool DHCPv4 của SW-L3-1.....	27
Bảng 3.21. Bảng Pool DHCPv4 của SW-L3-2.....	28
Bảng 3.22. Bảng Pool DHCPv4 của SW-L3-1-2.....	29

DANH MỤC HÌNH ẢNH

Hình 1.1. Kết quả khảo sát.....	3
Hình 1.2. Kết quả khảo sát (tiếp).....	3
Hình 1.3. Kết quả khảo sát (tiếp).....	4
Hình 1.4. Kết quả khảo sát (tiếp).....	4
Hình 1.5. Kết quả khảo sát (tiếp).....	4
Hình 1.6. Kết quả khảo sát (tiếp).....	5
Hình 1.7. Kết quả khảo sát (tiếp).....	5
Hình 1.8. Kết quả khảo sát (tiếp).....	5
Hình 1.9. Kết quả khảo sát (tiếp).....	6
Hình 1.10. Tài liệu thiết kế hệ thống mạng bệnh viện Ái Tâm.....	8
Hình 1.11. Tài liệu thiết kế hệ thống mạng bệnh viện Ái Tâm.....	8
Hình 2.1. Sơ đồ tổng quan về hệ thống mạng của bệnh viện.....	16
Hình 3.1. Sơ đồ hệ thống bệnh viện tổng quát.....	30
Hình 3.2. Sơ đồ bệnh viện của cơ sở 2.....	31
Hình 3.3. Sơ đồ bệnh viện của cơ sở 1.....	31
Hình 3.4. Kết quả dịch vụ DHCPv4 trên cơ sở 1.....	32
Hình 3.5. Kết quả dịch vụ DHCPv4 trên cơ sở 2.....	32
Hình 3.6. Kết quả dịch vụ DHCPv6 trên cơ sở 1.....	32
Hình 3.7. Kết quả kiểm tra 2 Firewall trước khi có kết nối giữa hai cơ sở.....	33
Hình 3.8. Kết quả kiểm tra sau khi có kết nối giữa hai cơ sở.....	33
Hình 3.9. Kết quả kiểm tra dịch vụ DNS tại cơ sở 1.....	34
Hình 3.10. Kết quả kiểm tra dịch vụ DNS tại cơ sở 2.....	34
Hình 3.11. Kết quả kiểm tra dịch vụ Mail tại cơ sở 1.....	35
Hình 3.12. Kiểm tra dịch vụ Mail tại cơ sở 2.....	35
Hình 3.13. Kết quả kiểm tra dịch vụ Mail giữa hai cơ sở.....	36
Hình 3.14. Kết quả kiểm tra dịch vụ Web cơ sở 1.....	36
Hình 3.15. Kết quả kiểm tra dịch vụ Web cơ sở 2.....	36
Hình 3.16. Kết quả kiểm tra dịch vụ Web từ bên ngoài.....	37
Hình 3.17. Kết quả kiểm tra kết nối giữa các máy trong cơ sở 1.....	37
Hình 3.18. Kết quả kiểm tra kết nối giữa các máy trong cơ sở 2.....	37
Hình 3.19. Kết quả kiểm tra kết nối giữa máy cơ sở 1 và Server.....	38
Hình 3.20. Kết quả kiểm tra kết nối qua IPv4 private của Server từ Outside.....	38
Hình 3.21. Kết quả kiểm tra kết nối đến địa chỉ đã NAT của Server từ Outside.....	38
Hình 3.22. Kết quả kịch bản 7 trước khi có sự cố.....	39
Hình 3.23. Kết quả kiểm tra kết nối sau khi có sự cố.....	39

LỜI MỞ ĐẦU

1. Lý do chọn đề tài

Trong thời đại công nghệ số phát triển mạnh mẽ, hạ tầng mạng máy tính đóng vai trò quan trọng trong mọi lĩnh vực, đặc biệt là trong môi trường y tế nơi yêu cầu sự ổn định, bảo mật và khả năng xử lý thông tin nhanh chóng. Việc thiết kế một hệ thống mạng hoàn chỉnh không chỉ giúp nâng cao hiệu quả làm việc, mà còn đảm bảo cho các dịch vụ y tế hoạt động liên tục, chính xác và an toàn. Việc thực hiện đề tài "Thiết kế hệ thống mạng máy tính cho Bệnh viện Đa khoa Anh Quất" là cơ hội để em củng cố, mở rộng và vận dụng kiến thức đã học về hạ tầng mạng. Đồng thời, đề tài cũng giúp em rèn luyện kỹ năng thực hành cấu hình, thiết kế mô hình mạng, từ đó làm nền tảng cho công việc sau này trong lĩnh vực công nghệ thông tin – đặc biệt là lĩnh vực quản trị và triển khai hệ thống mạng doanh nghiệp.

2. Phương pháp viết bài báo cáo

Bài báo cáo đồ án tốt nghiệp được thực hiện theo trình tự như sau:

- Xác định yêu cầu bài toán, phân tích các yêu cầu đặt ra từ thực tiễn tại bệnh viện Anh Quất. Nghiên cứu các kỹ thuật, công nghệ liên quan. Thực hiện các phương pháp thu thập yêu cầu và tổng hợp kết quả khảo sát thực tế.
- Lựa chọn công nghệ và kỹ thuật phù hợp để xây dựng hệ thống, đảm bảo khả năng mở rộng, an toàn và hiệu quả.
- Xây dựng kiến trúc tổng thể, mô hình hóa hệ thống mạng theo chuẩn ba lớp (Core – Distribution – Access) kết hợp VLAN, DHCP, NAT, VPN, Firewall, và các dịch vụ nội bộ.
- Cấu hình, mô phỏng hệ thống.
- Kiểm thử hệ thống.
- Hoàn thiện hệ thống và quyền báo cáo.

3. Cấu trúc và nội dung của quyển báo cáo

Quyển báo cáo gồm ba chương:

- Chương 1: Phân tích và thu thập yêu cầu.
- Chương 2: Phân tích và thiết kế hệ thống.
- Chương 3: Xây dựng và kiểm thử hoạt động hệ thống

CHƯƠNG 1 - PHÂN TÍCH VÀ THU THẬP YÊU CẦU

1.1. Giới thiệu chung về Bệnh viện Đa khoa Anh Quất

Bệnh viện Đa khoa Anh Quất trực thuộc Công ty TNHH Bệnh viện Đa khoa Anh Quất, là một trong những cơ sở y tế tư nhân hoạt động hiệu quả và uy tín trên địa bàn tỉnh Bắc Giang. Hiện nay, bệnh viện bao gồm hai cơ sở chính, phục vụ công tác khám chữa bệnh cho người dân tại nhiều địa phương trong tỉnh và các khu vực lân cận.

Bệnh viện Đa khoa Anh Quất được thành lập từ năm 2009 theo Giấy phép số 0244/GP-SYT do Sở Y tế tỉnh Bắc Giang cấp. Trụ sở đặt tại Khu Đồi Đỏ, thị trấn Cao Thượng, huyện Tân Yên, tỉnh Bắc Giang, kiến trúc gồm 8 tầng với tổng diện tích sử dụng lên đến 1.782 m².

Từ một cơ sở nhỏ ban đầu chỉ có 2 khoa, 3 bác sĩ và 5 cán bộ y tế khác, sau gần 15 năm phát triển, phòng khám hiện đã mở rộng lên 12 khoa, phòng chuyên môn, bao gồm: Nội, Ngoại, Sản, Nhi, Mắt, Da liễu, Răng hàm mặt, Tai mũi họng, Xét nghiệm, Chẩn đoán hình ảnh, Y học cổ truyền và Vật lý trị liệu – Phục hồi chức năng. Ngoài ra, còn có các bộ phận kỹ thuật thực hiện các thủ thuật hỗ trợ: tiêm, thay băng, đo huyết áp, đếm mạch... Các phòng khoa được chia ra các tầng khác nhau.

Bệnh viện Đa khoa Anh Quất (cơ sở 2) được phát triển từ chi nhánh Phòng khám tại Cụm công nghiệp Nội Hoàng, xã Nội Hoàng, huyện Yên Dũng, và chính thức được Bộ Y tế cấp phép hoạt động khám, chữa bệnh theo giấy phép số 374/BYT-GPHĐ ngày 21/6/2024. Bệnh viện có 11 khoa, phòng chuyên môn, thực hiện khám chữa bệnh bảo hiểm y tế thông tuyến và hoạt động tất cả các ngày trong tuần. Theo kế hoạch, bệnh viện có khả năng tiếp nhận khoảng 250 bệnh nhân mỗi ngày, gấp đôi năng lực hiện tại.

Hai cơ sở này cách nhau khoảng 30km, điều này đặt ra yêu cầu về một giải pháp kết nối mạng hiệu quả và bảo mật giữa chúng.

1.2. Xác định bài toán

Tên đề tài: Thiết kế hệ thống mạng máy tính cho bệnh viện Đa khoa Anh Quất.

Nơi dự kiến khảo sát: Bệnh viện Đa khoa Anh Quất.

Kế hoạch thu thập thông tin:

- Tạo phiếu câu hỏi lấy ý kiến từ các bộ phận.
- Khảo sát thực tế tại bệnh viện.
- Tìm và nghiên cứu hệ thống mạng máy tính tương tự.

Mục đích của việc thu thập thông tin:

- Xác định yêu cầu thiết kế mạng, phân tích số lượng thiết bị cần kết nối và nhu cầu sử dụng để xây dựng hệ thống phù hợp.
- Tìm hiểu các mô hình mạng tương tự nhằm để áp dụng những giải pháp hiệu quả và tối ưu hóa thiết kế.

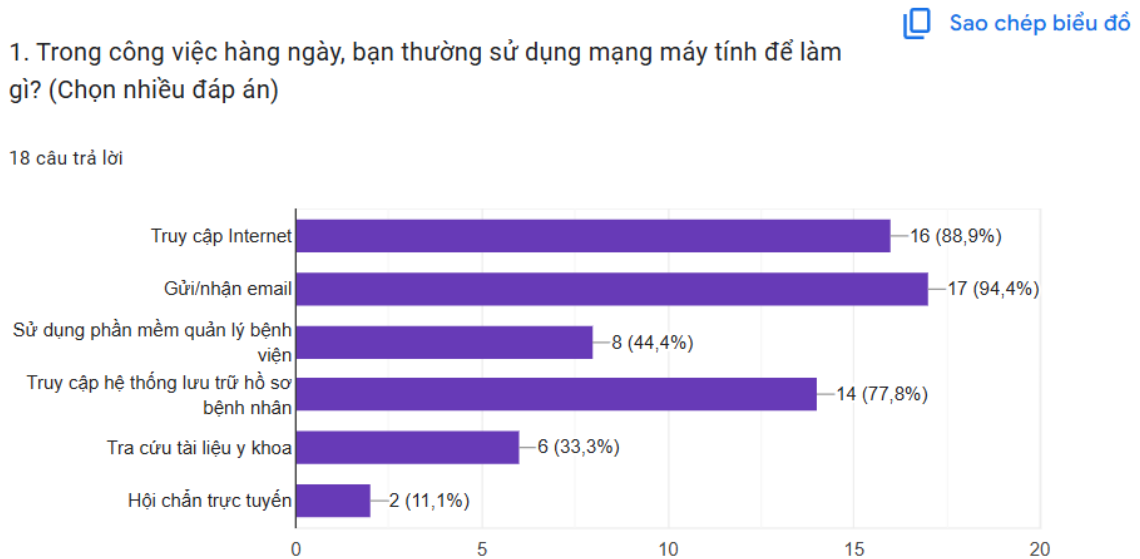
1.3. Xác định yêu cầu bài toán

1.3.1. Phương pháp khảo sát

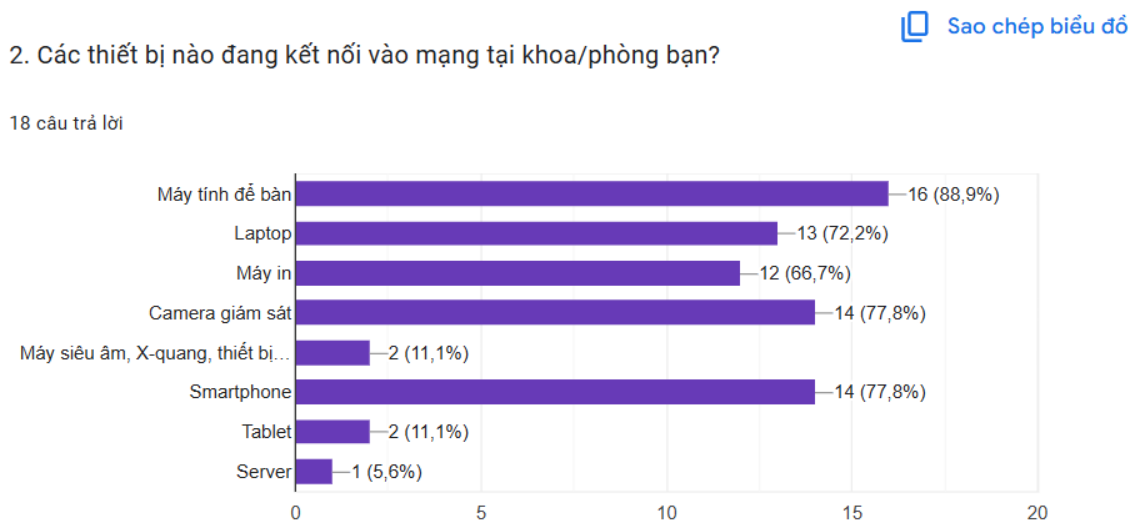
Cách thức khảo sát: Tạo phiếu hỏi lấy ý kiến các bộ phận.

Mục đích khảo sát: Thu thập nhu cầu sử dụng mạng của cán bộ nhân viên để xác định được những yêu cầu cần thiết cho hệ thống mạng.

Kết quả khảo sát:



Hình 1.1. Kết quả khảo sát

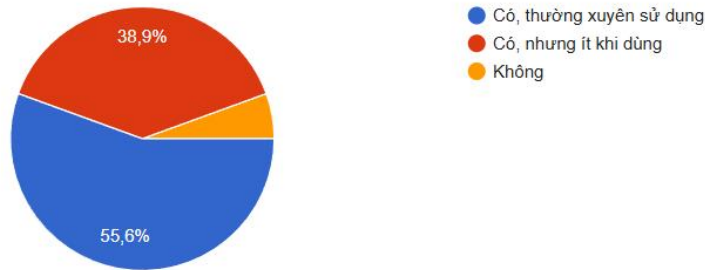


Hình 1.2. Kết quả khảo sát (tiếp)

3. Bạn có cần truy cập Wi-Fi không?

Sao chép biểu đồ

18 câu trả lời

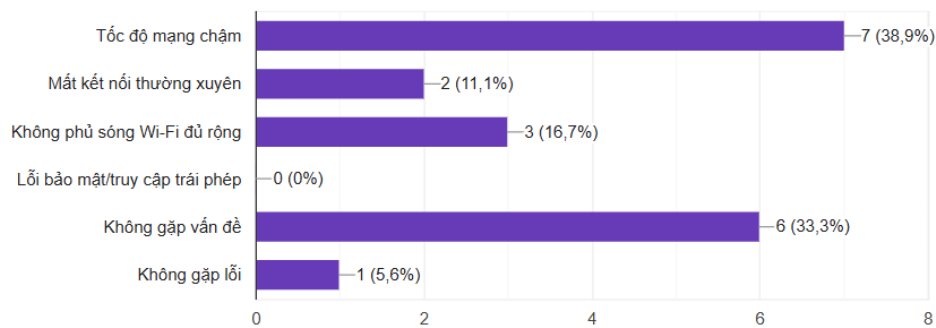


Hình 1.3. Kết quả khảo sát (tiếp)

4. Bạn có gặp vấn đề nào về mạng hiện tại không?

Sao chép biểu đồ

18 câu trả lời

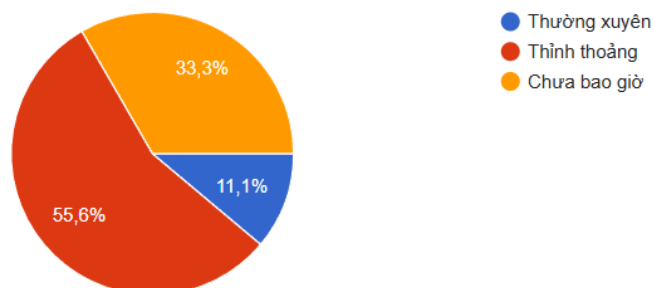


Hình 1.4. Kết quả khảo sát (tiếp)

5. Bạn có hay gặp các sự cố về mạng không?

Sao chép biểu đồ

18 câu trả lời

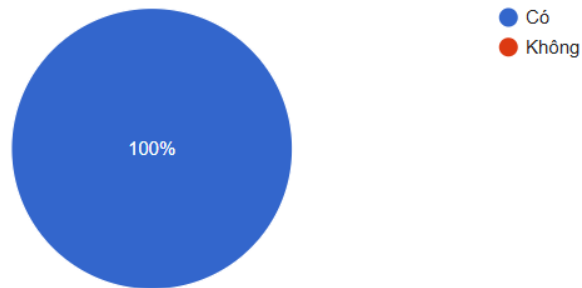


Hình 1.5. Kết quả khảo sát (tiếp)

6. Bạn có sử dụng Email nội bộ không?

18 câu trả lời

 Sao chép biểu đồ

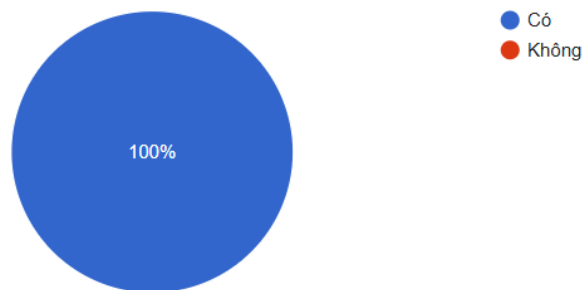


Hình 1.6. Kết quả khảo sát (tiếp)

7. Bạn có cần truy cập trang Web nội bộ của bệnh viện không? (Lịch làm việc, thông báo, kết quả xét nghiệm...)

18 câu trả lời

 Sao chép biểu đồ

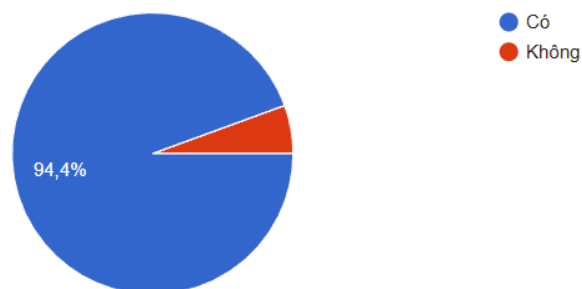


Hình 1.7. Kết quả khảo sát (tiếp)

8. Bạn có cần hệ thống lưu trữ hồ sơ/bệnh án trực tuyến không?

18 câu trả lời

 Sao chép biểu đồ

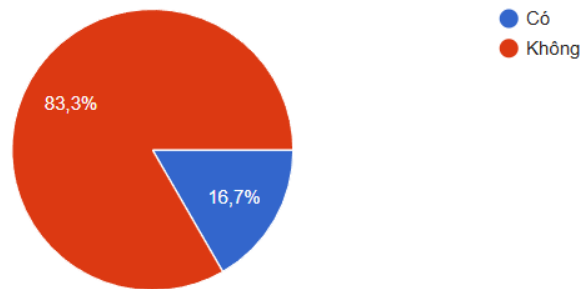


Hình 1.8. Kết quả khảo sát (tiếp)

9. Bạn có cần kết nối từ xa vào hệ thống bệnh viện không?

 Sao chép biểu đồ

18 câu trả lời



Hình 1.9. Kết quả khảo sát (tiếp)

1.3.2. Khảo sát thực tiễn cơ sở hạ tầng tại bệnh viện

Cách thức khảo sát: Thực hiện thông qua việc quan sát trực tiếp tại Bệnh viện Đa khoa Anh Quất, kết hợp với thu thập dữ liệu về cơ sở hạ tầng, trang thiết bị và hệ thống mạng.

Mục đích khảo sát: Thu thập thông tin chính xác về hệ thống hạ tầng mạng, số lượng và loại thiết bị tại từng phòng/khoa, đánh giá nhu cầu sử dụng để đảm bảo hệ thống mạng đáp ứng tốt hoạt động của bệnh viện.

Kết quả khảo sát:

Bảng 1.1. Bảng thông tin bệnh viện tại cơ sở 1

Tầng	Phòng/Khoa	Chức năng	Tổng số thiết bị
1	Khu cấp cứu	Tiếp nhận bệnh nhân cấp cứu	9
	Khu tiếp đón, thanh toán	Đón tiếp, hướng dẫn bệnh nhân Thu phí dịch vụ y tế	12
2	Khoa Nội	Khám và điều trị nội khoa	11
	Khoa Ngoại	Phẫu thuật và điều trị ngoại khoa	11
	Khoa Sản	Khám và điều trị sản phụ khoa	8
	Khoa Nhi	Khám và điều trị cho trẻ em	7
3	Khoa Mắt	Khám và điều trị bệnh về mắt	5
	Khoa Da liễu	Khám và điều trị bệnh da liễu	5
	Khoa Răng Hàm Mặt	Khám và điều trị nha khoa	5

	Khoa Tai Mũi Họng	Khám và điều trị TMH	5
4	Khoa Xét nghiệm	Thực hiện xét nghiệm y khoa	9
	Khoa Chẩn đoán hình ảnh	Chụp X-quang, CT, siêu âm	9
5	Khoa Vật lý trị liệu - Phục hồi chức năng	Điều trị bằng vật lý trị liệu	6
6	Khu nội trú	Giường bệnh cho bệnh nhân nội trú	6
7	Khu nội trú	Giường bệnh cho bệnh nhân nội trú	6
8	Phòng hội đồng	Phục vụ họp mặt, sự kiện	3
	Phòng hành chính	Xử lý công việc, giấy tờ hành chính	10
	Phòng máy chủ	Trung tâm điều hành hệ thống mạng	7
	Phòng kỹ thuật IT	Quản lý và hỗ trợ kỹ thuật	8

Bảng 1.2. Bảng thông tin bệnh viện tại cơ sở 2

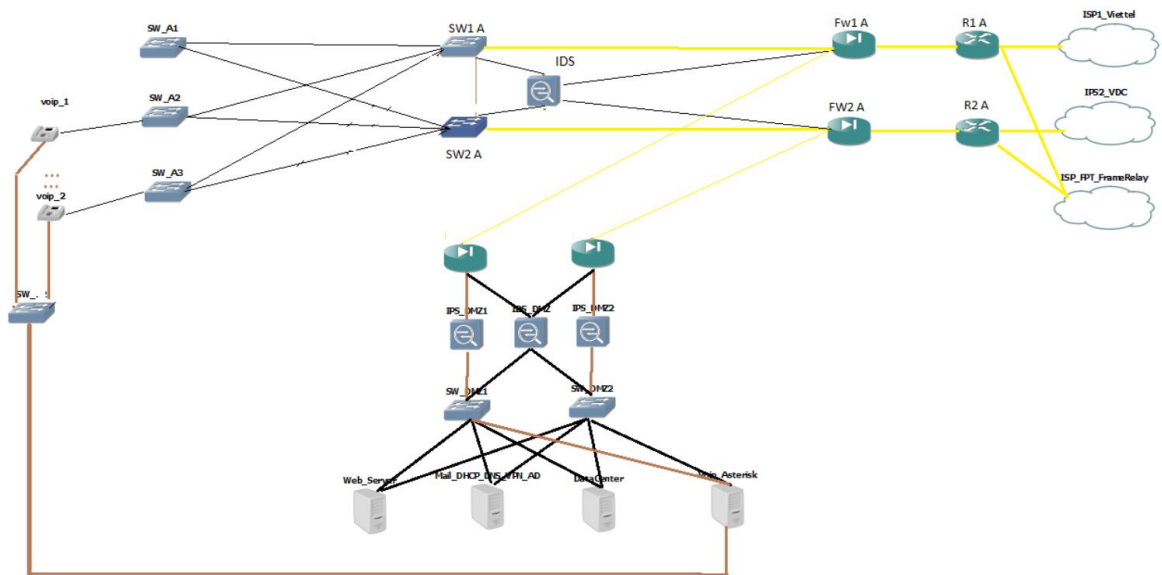
Tầng	Phòng/Khoa	Chức năng	Tổng số thiết bị
1	Phòng khám bệnh đa khoa	Khám bệnh thông thường	6
	Phòng tiếp đón bệnh nhân	Hướng dẫn, tiếp nhận bệnh nhân	3
	Phòng xét nghiệm	Thực hiện xét nghiệm cơ bản	5
2	Khoa Ngoại	Điều trị và tiểu phẫu	6
	Khoa Sản	Chăm sóc sức khỏe sinh sản	5
	Khoa Nhi	Điều trị nhi khoa	5
	Phòng tiêm chủng	Tiêm chủng Vaccine	3
3	Phòng hội đồng	Phục vụ họp mặt, sự kiện	3
	Phòng hành chính	Xử lý công việc, giấy tờ hành chính	6
	Phòng kỹ thuật	Hỗ trợ hệ thống mạng nội bộ	5

1.3.3. Tìm hiểu về các mô hình hệ thống mạng bệnh viện đã có

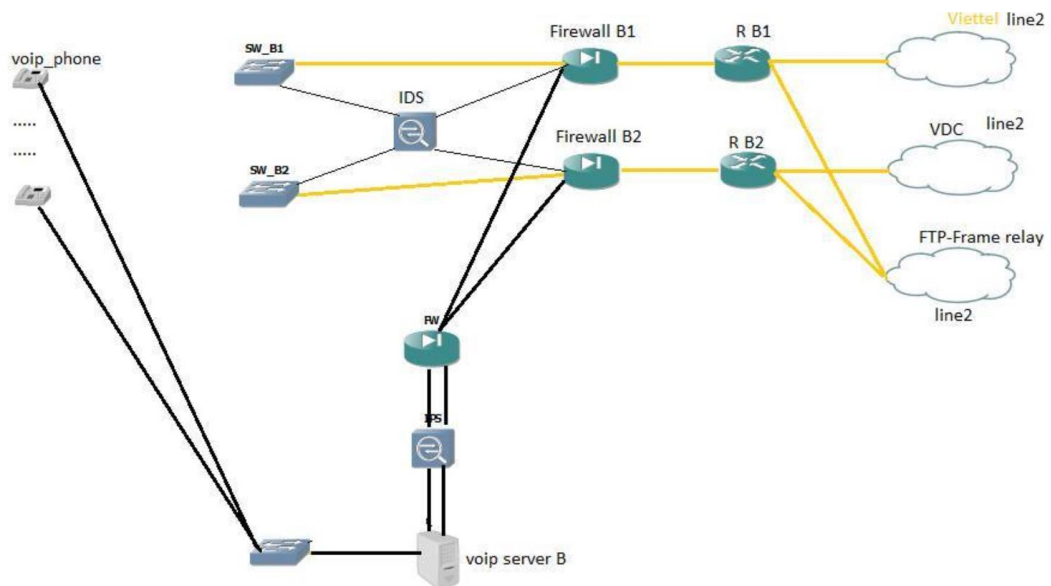
Cách thức: Nghiên cứu các tài liệu về hệ thống mạng.

Mục đích nghiên cứu: Tìm hiểu để xác định mô hình tổng quan bài toán và các dịch vụ cần thiết cho hệ thống mạng.

Kết quả nghiên cứu:



Hình 1.10. Tài liệu thiết kế hệ thống mạng bệnh viện Ái Tâm



Hình 1.11. Tài liệu thiết kế hệ thống mạng bệnh viện Ái Tâm

- Khu A gồm 3 tòa nhà: A1, A2, A3, có diện tích giống nhau. Nhà A2 và A3 gần đường Cống Quỳnh hơn so với nhà A1, và khoảng cách từ nhà A1 đến A3 gấp đôi khoảng cách từ A2 đến A3. Đặc biệt, tầng 7 của nhà A3 có diện tích trống nhiều nhất. Do đó, phòng Server (vùng DMZ) được đặt tại đây để thuận tiện cho việc quản lý và bảo trì.

- Khu B bao gồm hai tòa nhà: B1 và B2. Do không thể kéo dây mạng qua đường Cổng Quỳnh, khu A và khu B không thể kết nối trực tiếp với nhau mà phải sử dụng VPN để đảm bảo kết nối an toàn.
- Khu A sử dụng hai ISP riêng biệt (Viettel, VDC) để đảm bảo tính sẵn sàng cao. Mạng xương sống được thiết kế với hai Firewall bảo vệ, hai Switch hiệu suất cao kết nối đến các tòa nhà, và hệ thống IDS giúp phát hiện xâm nhập. Mỗi tòa nhà có Switch riêng kết nối trực tiếp đến mạng xương sống. Riêng vùng DMZ tại tầng 7 của nhà A3 được bảo vệ bởi hai Firewall chuyên dụng và có hệ thống VoIP Server riêng cho phòng mổ để đảm bảo kết nối ổn định.
- Tương tự khu A, khu B cũng có hai mạng xương sống với hai ISP riêng biệt, Firewall bảo vệ, IDS phát hiện xâm nhập, và Switch tổng kết nối toàn bộ hệ thống. Mỗi tòa nhà (B1, B2) có một Switch riêng kết nối đến mạng xương sống. Hệ thống VoIP tại khu B cũng có đường truyền riêng, đảm bảo chất lượng cuộc gọi. Kết nối giữa hai khu A và B được thực hiện thông qua VPN để đảm bảo bảo mật và ổn định.
- Nhờ hai ISP riêng biệt, hệ thống đảm bảo kết nối ổn định ngay cả khi một ISP gặp sự cố. Ngoài ra, hệ thống Firewall và IDS giúp tăng cường bảo mật, bảo vệ khỏi các mối đe dọa bên ngoài. Tuy nhiên, nhược điểm là việc triển khai hệ thống yêu cầu hạ tầng phức tạp, tốn kém chi phí đầu tư và bảo trì. Ngoài ra, VPN giúp kết nối giữa hai khu nhưng lại có thể trở thành điểm yếu nếu bị tấn công hoặc gặp sự cố, làm gián đoạn liên lạc nội bộ.

1.4. Phát biểu bài toán

1.4.1. Nội dung bài toán

Với sự phát triển không ngừng của công nghệ thông tin trong lĩnh vực y tế, nhu cầu thiết kế một hệ thống mạng ổn định, bảo mật và hiệu quả là vô cùng cần thiết. Đề tài "Thiết kế hệ thống mạng máy tính cho Bệnh viện Đa khoa Anh Quất" nhằm xây dựng một mô hình mạng hoàn chỉnh phục vụ cho việc quản lý, trao đổi thông tin và vận hành các dịch vụ y tế tại bệnh viện. Hệ thống mạng được thiết kế theo mô hình phân tầng (Core – Distribution – Access), áp dụng các công nghệ hiện đại như VLAN, DHCP, NAT, VPN, cùng với các dịch vụ cần thiết như Mail Server, Web Server, DNS Server. Ngoài ra, hệ thống còn đảm bảo bảo mật và tính sẵn sàng cao nhờ Firewall và ACL.

1.4.2. Yêu cầu chức năng đối với hệ thống mạng bệnh viện

Hệ thống mạng:

- Hỗ trợ giao thức IPv4, đảm bảo khả năng kết nối ổn định và mở rộng trong tương lai.
- Wi-Fi phủ sóng toàn bộ khu vực bệnh viện, đảm bảo truy cập không dây cho nhân viên và thiết bị.

- Phân chia VLAN hợp lý theo từng khoa, phòng ban để đảm bảo quản lý lưu lượng mạng, nâng cao hiệu suất và tính bảo mật.

Dịch vụ hệ thống:

- Mail Server: Hỗ trợ trao đổi thông tin nội bộ, thông báo, nhắc lịch làm việc và tư vấn từ xa.
- Web Server: Cung cấp thông tin bệnh viện, lịch khám, tra cứu kết quả xét nghiệm trực tuyến.
- DNS và DHCP Server: Tự động cấp phát địa chỉ IP và quản lý các tên miền của bệnh viện.

Bảo mật:

- Tăng cường bảo mật với các công nghệ: VPN, ACL, Firewall.
- NAT Overload (PAT): Hỗ trợ kết nối Internet cho toàn hệ thống với tính năng ẩn địa chỉ IP nội bộ, tối ưu và bảo vệ truy cập.
- Kết nối Internet ổn định thông qua nhà cung cấp ISP, đảm bảo tính sẵn sàng và độ tin cậy cho toàn bộ dịch vụ mạng bệnh viện.

1.4.3. Yêu cầu phi chức năng cho hệ thống mạng bệnh viện

Hệ thống mạng được thiết kế trong môi trường mô phỏng cần đảm bảo một số yêu cầu phi chức năng nhằm hướng đến một mô hình ổn định, có tính khả thi và mô phỏng được các yếu tố then chốt của một hệ thống mạng. Cụ thể như sau:

- Hiệu năng (Performance): Hệ thống phải đảm bảo tốc độ truyền tải dữ liệu ổn định và nhanh chóng giữa các thiết bị, đặc biệt trong các kịch bản mô phỏng có nhiều thiết bị truy cập đồng thời. Cấu trúc mạng cần tối ưu về mặt định tuyến, băng thông, phân bổ tải hợp lý nhằm giảm thiểu độ trễ và nghẽn mạng.
- Khả năng mở rộng (Scalability): Thiết kế mạng cần có khả năng mở rộng dễ dàng khi có nhu cầu tăng thêm số lượng máy tính, thiết bị y tế, hoặc các phân khu mới trong bệnh viện. Việc mở rộng không được làm gián đoạn hệ thống hiện tại và phải được tích hợp dễ dàng vào kiến trúc mạng tổng thể.
- Tính sẵn sàng (Availability): Mô hình cần thể hiện cấu trúc mạng có khả năng hoạt động liên tục với thời gian gián đoạn tối thiểu. Trong giới hạn mô phỏng, có thể áp dụng các kỹ thuật như định tuyến dự phòng, thiết bị mạng kép (redundant links/interfaces) hoặc mô phỏng cân bằng tải để đảm bảo tính khả dụng.
- Khả năng chịu lỗi (Fault Tolerance): Mạng cần có khả năng phục hồi hoạt động khi gặp sự cố. Điều này được thể hiện qua việc triển khai các đường truyền dự phòng, cấu hình định tuyến đa đường (multiple static routes), hoặc cơ chế chuyển đổi khi Router/Switch gặp trục trặc trong mô hình mô phỏng.
- Khả năng quản lý (Manageability): Hệ thống phải dễ dàng trong việc cấu hình, giám sát và vận hành. Việc quản lý tập trung cần thể hiện qua tên thiết bị rõ

ràng, phân tầng logic mạng (Core, Distribution, Access), và sử dụng các dịch vụ như DHCP, ACL để kiểm soát truy cập và tự động hóa cấu hình IP.

- Tính bảo mật (Security): Cần áp dụng các kỹ thuật mô phỏng bảo mật cơ bản để thể hiện ý thức thiết kế an toàn mạng. Các cấu hình như VLAN để cô lập lưu lượng giữa các khoa phòng hoặc ACL để giới hạn truy cập.
- Khả năng tương thích (Compatibility): Hệ thống phải hỗ trợ các giao thức và dịch vụ mạng phổ biến như IPv4, NAT, DHCP, DNS, đồng thời tương thích với các thiết bị và phần mềm trong mô hình mô phỏng. Việc tích hợp các dịch vụ như Web Server, Mail Server, VPN cũng cần được đảm bảo vận hành ổn định.
- Tính linh hoạt (Flexibility): Mạng cần linh hoạt để thích ứng với những thay đổi trong cơ cấu tổ chức hoặc nâng cấp công nghệ. Kiến trúc mạng nên được quy hoạch hợp lý để dễ dàng điều chỉnh địa chỉ IP, VLAN, cấu trúc định tuyến mà không gây ảnh hưởng đến toàn bộ hệ thống.
- Tính dễ sử dụng và trực quan (Usability & Visibility): Mô hình cần được trình bày trực quan, rõ ràng về sơ đồ kết nối, tên thiết bị, IP và các cấu hình.

1.4.4. Kiểm thử hoạt động hệ thống

- Kiểm tra dịch vụ DHCP: Xác minh khả năng cấp phát địa chỉ IPv4 và IPv6 tự động cho các thiết bị.
- Kiểm tra dịch vụ VPN site-to-site: Xác minh khả năng kết nối an toàn và ổn định giữa hai cơ sở qua đường hầm VPN.
- Kiểm tra dịch vụ DNS: Đảm bảo khả năng phân giải tên miền thành địa chỉ IP (IPv4 và IPv6) và ngược lại.
- Kiểm tra dịch vụ Mail Server: Xác minh khả năng gửi và nhận email nội bộ.
- Kiểm tra dịch vụ Web Server: Đảm bảo khả năng truy cập trang thông tin bệnh viện và các dịch vụ trực tuyến.
- Kiểm tra kết nối mạng tổng thể: Đánh giá kết nối mạng và tính sẵn sàng của toàn bộ hệ thống trong điều kiện bình thường.
- Kiểm tra khả năng dự phòng của hệ thống: Đánh giá xem nếu xảy ra sự cố thì hệ thống hoạt động có bình thường không.
- Kiểm tra khả năng bảo mật: Sử dụng Firewall, ACL để kiểm tra khả năng bảo mật.

CHƯƠNG 2 - PHÂN TÍCH VÀ THIẾT KẾ

2.1. Công nghệ - kỹ thuật xây dựng hệ thống

2.1.1. VLSM

VLSM (Variable Length Subnet Mask) cho phép phân chia một không gian địa chỉ IP thành một hệ thống các mạng con có kích thước khác nhau mà không làm lãng phí số lượng lớn địa chỉ IP. Nhờ VLSM, các subnet có thể có kích thước phù hợp với nhu cầu thực tế, thay vì phải tuân theo một subnet cố định. Trong bài toán, hệ thống mạng sẽ có dải mạng gốc là 172.16.0.0/24 cho cơ sở 1, 192.168.0.0/24 cho cơ sở 2 và sử dụng VLSM để chia ra thành các mạng con sao cho phù hợp với nhu cầu.

2.1.2. Routing (Định tuyến)

Routing (định tuyến) là quá trình tìm đường đi tốt nhất để chuyển tiếp gói tin từ nguồn đến đích trong một hệ thống mạng. Quá trình này được thực hiện bởi các thiết bị định tuyến như Router hoặc Layer 3 Switch. Router sử dụng bảng định tuyến (Routing Table) để lưu trữ các tuyến đường và quyết định gói tin sẽ được chuyển đến đâu dựa trên địa chỉ IP đích.

Có hai loại định tuyến chính: định tuyến tĩnh và định tuyến động. Định tuyến tĩnh yêu cầu quản trị viên mạng cấu hình thủ công các tuyến đường trên Router. Mặc dù phương pháp này đơn giản và bảo mật hơn, nhưng nó không linh hoạt khi mạng có sự thay đổi. Ngược lại, định tuyến động sử dụng các giao thức như RIP, OSPF, EIGRP hoặc BGP để tự động cập nhật bảng định tuyến và chọn đường đi tối ưu dựa trên các thuật toán khác nhau. Trong bài toán, hệ thống sử dụng giao thức định tuyến động OSPF để định tuyến giữa lớp Core, lớp Distribution và giữa các VLAN.

Cấu hình định tuyến động với OSPF:

```
# Router ospf [process-id]
# Router-id [x.x.x.x]
# network [mạng] [wildcard mask] area [số vùng]
```

2.1.3. SVI (Switch Virtual Interface)

Là một giao diện ảo trên Layer 3 Switch, cho phép thiết bị có địa chỉ IP và tham gia vào quá trình định tuyến giữa các VLAN (Inter-VLAN Routing).

Ứng dụng của SVI:

- Cung cấp IP cho Switch để quản lý từ xa (Telnet, SSH).
- Hỗ trợ Inter-VLAN Routing (định tuyến giữa các VLAN).
- Cải thiện hiệu suất bằng cách loại bỏ nhu cầu sử dụng Router-on-a-stick.

Cấu hình SVI cơ bản:

```
# ip routing
# interface vlan [VLAN ID]
# ip address [IP_ADDRESS] [SUBNET_MASK]
# no shutdown
# interface [INTERFACE]
# Switchport mode trunk
# Switchport trunk allowed vlan [VLAN LIST]
# interface [INTERFACE]
# Switchport mode access
# Switchport access vlan [VLAN ID]
```

2.1.4. DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) là một giao thức tự động cấp phát thông tin mạng như địa chỉ IP, Subnet Mask, Default Gateway và DNS cho các thiết bị trong mạng. Thay vì phải cấu hình thủ công từng thiết bị, DHCP giúp quản trị viên quản lý IP dễ dàng hơn, giảm thiểu lỗi và tránh xung đột địa chỉ IP.

Cấu hình DHCP cơ bản trên Router/Switch Layer 3:

```
# ip dhcp excluded-address [START_IP] [END_IP]
# ip dhcp pool [Pool_Name]
# network [dải địa chỉ IP của pool]
# default-router [địa chỉ IP Default Gateway]
# dns-server [địa chỉ IP DNS Server]
```

2.1.5. VPN

VPN (Virtual Private Network) là một công nghệ giúp tạo một kết nối an toàn giữa các mạng hoặc thiết bị thông qua một mạng công cộng như Internet. VPN mã hóa dữ liệu truyền tải, đảm bảo tính bảo mật và quyền riêng tư khi người dùng truy cập mạng từ xa.

Doanh nghiệp có thể sử dụng VPN để cho phép nhân viên truy cập hệ thống nội bộ từ xa một cách an toàn. Cá nhân có thể dùng VPN để bảo vệ quyền riêng tư, vượt qua hạn chế địa lý hoặc truy cập mạng Wi-Fi công cộng một cách an toàn. Ngoài ra, VPN cũng giúp kết nối các chi nhánh doanh nghiệp với nhau, tạo một hệ thống mạng thống nhất dù ở các địa điểm khác nhau.

VPN được chia thành hai loại chính là Site-to-Site VPN và Remote Access VPN:

- Site-to-Site VPN là loại VPN kết nối các mạng nội bộ (LAN) của doanh nghiệp lại với nhau thông qua Internet, giúp các chi nhánh có thể trao đổi dữ liệu an toàn mà không cần kết nối trực tiếp. VPN này thường được triển khai trên các

thiết bị mạng như Router hoặc Firewall và được sử dụng trong môi trường doanh nghiệp để tạo một hệ thống mạng thống nhất giữa các văn phòng từ xa.

- Remote Access VPN được thiết kế để cho phép người dùng từ xa kết nối vào hệ thống mạng nội bộ của doanh nghiệp. Nhân viên có thể sử dụng VPN Client để truy cập vào tài nguyên của công ty một cách an toàn từ bất kỳ đâu có Internet. Điều này đặc biệt hữu ích cho những người làm việc từ xa hoặc cần truy cập dữ liệu khi đi công tác. Remote Access VPN thường sử dụng giao thức bảo mật như SSL/TLS hoặc IPsec để đảm bảo an toàn cho dữ liệu truyền tải.

2.1.6. IPsec

IPsec là một bộ giao thức bảo mật được sử dụng để mã hóa và xác thực dữ liệu khi truyền qua mạng IP, đặc biệt là Internet. Nó giúp bảo vệ tính toàn vẹn, tính bảo mật và tính xác thực của dữ liệu, thường được sử dụng trong VPN để tạo các kết nối an toàn giữa các thiết bị hoặc mạng.

IPsec giúp thiết lập một kênh an toàn giữa các thiết bị hoặc mạng bằng cách mã hóa dữ liệu trước khi truyền đi. Khi kết nối VPN, IPsec được thiết lập, khi đó dữ liệu giữa hai điểm sẽ được bảo vệ khỏi nghe lén và tấn công trung gian, đảm bảo tính bảo mật và toàn vẹn thông tin.

2.1.7. Kỹ thuật dự phòng

Load Balancing là một kỹ thuật quan trọng trong quản lý hệ thống mạng và máy chủ, giúp phân phối lưu lượng truy cập hoặc cân bằng tải công việc giữa nhiều tài nguyên như máy chủ, đường truyền mạng hoặc các thiết bị khác. Mục tiêu chính của Load Balancing là tối ưu hóa hiệu suất, đảm bảo tính sẵn sàng và cải thiện trải nghiệm người dùng.

Công dụng của Load Balancing:

- Phân phối tải hiệu quả: Giúp chia đều lưu lượng truy cập giữa nhiều tài nguyên, tránh tình trạng quá tải cục bộ.
- Tăng cường hiệu suất: Hệ thống hoạt động ổn định, giảm thời gian phản hồi và cải thiện trải nghiệm người dùng.
- Đảm bảo tính sẵn sàng: Khi một máy chủ hoặc đường truyền gặp sự cố, hệ thống vẫn tiếp tục hoạt động bằng cách chuyển hướng lưu lượng sang tài nguyên khác.
- Hỗ trợ mở rộng linh hoạt: Dễ dàng thêm hoặc bớt tài nguyên mà không làm gián đoạn dịch vụ.
- Tối ưu hóa sử dụng tài nguyên: Tránh tình trạng một tài nguyên bị quá tải trong khi tài nguyên khác không được sử dụng hiệu quả.
- Cải thiện bảo mật: Một số hệ thống Load Balancing có khả năng phát hiện và giảm thiểu các cuộc tấn công DDoS bằng cách phân tán lưu lượng độc hại.

2.1.8. NAT (Network Address Translation)

NAT giúp chuyển đổi địa chỉ IP nội bộ (Private) thành IP công cộng (Public), phục vụ việc truy cập Internet từ mạng nội bộ. Ngoài ra, NAT Overload (PAT) còn cho phép nhiều thiết bị dùng chung một địa chỉ IP Public. Trong mô hình bệnh viện, NAT được triển khai tại ASA Firewall.

2.1.9. ACL (Access Control List)

ACL (Access Control List) là một công cụ quan trọng trong quản trị mạng, dùng để lọc và kiểm soát lưu lượng truy cập dựa trên các tiêu chí như địa chỉ IP nguồn, địa chỉ IP đích, giao thức và cổng. ACL có thể được áp dụng trên Router, Layer 3 Switch hoặc Firewall để thực hiện các chính sách kiểm soát truy cập.

2.1.10. Phương pháp bảo mật hệ thống

2.1.10.1. Bảo mật Layer 2

Bảo mật Layer 2 là các biện pháp bảo vệ liên quan đến lớp liên kết dữ liệu (Data Link Layer) trong mô hình OSI, giúp ngăn chặn các cuộc tấn công vào mạng LAN, bảo vệ Switch và đảm bảo an toàn cho lưu lượng nội bộ. Các phương pháp quan trọng gồm:

- Port Security: Hạn chế số lượng thiết bị có thể kết nối vào một cổng Switch để ngăn chặn giả mạo địa chỉ MAC.
- Dynamic ARP Inspection (DAI): Ngăn chặn tấn công ARP Spoofing bằng cách xác thực các gói ARP trước khi cho phép chúng truyền trong mạng.
- DHCP Snooping: Kiểm soát các máy chủ DHCP hợp lệ, ngăn chặn DHCP giả mạo cấp phát địa chỉ IP trái phép.
- STP (Spanning Tree Protocol) Protection: Bật BPDU Guard, Root Guard để ngăn chặn tấn công giả mạo BPDU, tránh loop mạng.
- VLAN Segmentation: Sử dụng VLAN để cô lập lưu lượng giữa các nhóm thiết bị, giảm nguy cơ lây lan tấn công trong mạng nội bộ.
- Private VLAN: Giúp kiểm soát giao tiếp giữa các thiết bị trong cùng VLAN, hạn chế các thiết bị không cần thiết liên lạc trực tiếp với nhau.
- IP Source Guard: Kiểm tra địa chỉ IP của thiết bị kết nối vào Switch, ngăn chặn giả mạo địa chỉ IP.

Các biện pháp này giúp bảo vệ hệ thống mạng nội bộ khỏi các cuộc tấn công phổ biến như giả mạo địa chỉ MAC, ARP Spoofing, DHCP Spoofing và các lỗi bảo mật trên Switch.

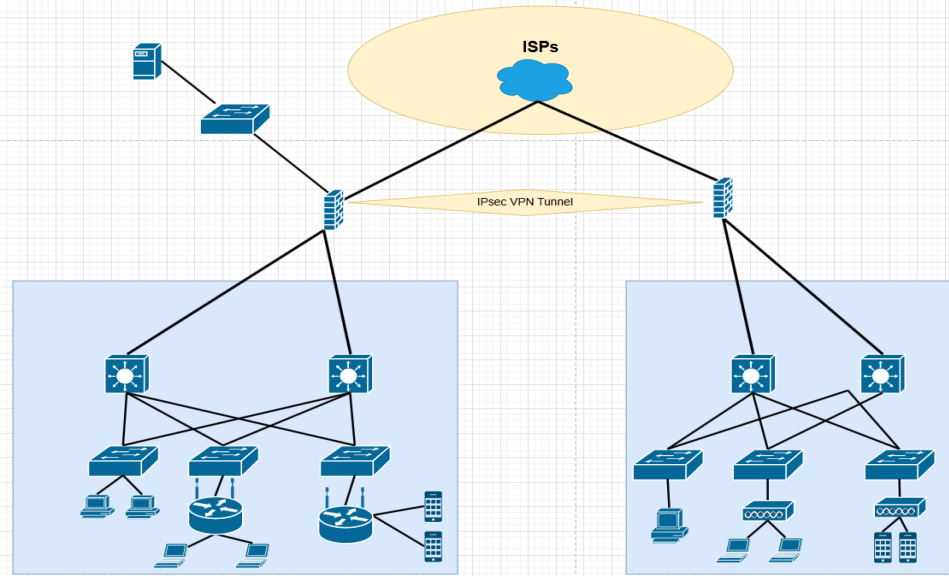
2.1.10.2. Bảo mật Layer 3

Bảo mật tại Layer 3 (Network Layer) giúp ngăn chặn các cuộc tấn công vào hệ thống định tuyến và kiểm soát lưu lượng IP. Một số phương pháp quan trọng bao gồm:

- Kiểm soát truy cập (ACLs): Sử dụng danh sách điều khiển truy cập trên Router hoặc Firewall để giới hạn lưu lượng dựa trên địa chỉ IP, giao thức hoặc cổng, ngăn chặn truy cập trái phép.
- Mã hóa và xác thực dữ liệu (IPSec): Bảo vệ tính toàn vẹn và bảo mật của dữ liệu bằng cách mã hóa các gói tin khi truyền qua mạng.
- Bảo vệ giao thức định tuyến: Áp dụng xác thực (MD5, SHA) cho các giao thức định tuyến như OSPF, EIGRP, BGP để ngăn chặn kẻ tấn công giả mạo thông tin định tuyến.
- Tường lửa (Firewall): Lọc và kiểm soát lưu lượng mạng nhằm ngăn chặn các mối đe dọa từ bên ngoài và giới hạn quyền truy cập vào hệ thống nội bộ.
- Ẩn địa chỉ IP nội bộ (NAT): Chuyển đổi địa chỉ IP riêng thành địa chỉ công cộng, giúp che giấu thông tin mạng nội bộ khỏi các cuộc tấn công từ Internet.
- Chuyển hướng lưu lượng độc hại (Blackhole Routing): Định tuyến dữ liệu không mong muốn vào giao diện null để loại bỏ lưu lượng độc hại, giảm tác động của các cuộc tấn công.
- Giới hạn băng thông (Rate Limiting): Kiểm soát tốc độ lưu lượng ICMP hoặc UDP để giảm nguy cơ bị tấn công từ chối dịch vụ (DoS/DDoS).
- Phân đoạn và cô lập mạng: Áp dụng VLAN và chia subnet để giới hạn phạm vi truy cập, giúp ngăn chặn sự lây lan của tấn công trong mạng nội bộ.

2.2. Kiến trúc hệ thống

Hệ thống mạng của bệnh viện được thiết kế theo mô hình kiến trúc mạng phân cấp ba tầng (Three-tier hierarchical network architecture) bao gồm ba tầng chính: Core layer (Tầng lõi), Distribution layer (Tầng phân phối), và Access layer (Tầng truy cập).



Hình 2.1. Sơ đồ tổng quan về hệ thống mạng của bệnh viện

Tầng lõi là trung tâm của toàn bộ hệ thống mạng, có vai trò kết nối giữa hệ thống mạng nội bộ của bệnh viện và mạng diện rộng (Internet/ISP), đồng thời chịu trách nhiệm định tuyến và quản lý truy cập cấp cao. Thành phần chính của tầng này bao gồm một Firewall ASA và kết nối đến ISP. Ngoài ra, tầng lõi cũng kết nối với vùng DMZ – nơi đặt các máy chủ công cộng như Web, Mail và DNS Server.

Firewall ASA bảo mật luồng dữ liệu giữa mạng nội bộ, vùng DMZ và mạng bên ngoài (Internet), đồng thời có các cơ chế NAT, VPN, và kiểm soát truy cập thông qua ACL.

Các chức năng chính:

- Kết nối hệ thống mạng nội bộ với nhà cung cấp dịch vụ Internet (ISP).
- Thực hiện định tuyến lưu lượng giữa các VLAN và các subnet trong toàn bộ hệ thống.
- Quản lý truy cập và bảo mật bằng cách triển khai các chính sách như ACL, NAT, VPN, và kiểm soát vùng DMZ.
- Đảm bảo khả năng dự phòng và phục hồi nhanh trong các tình huống lỗi.

Trong mô hình, tầng Distribution sẽ có hệ thống các dịch vụ Server và hai Layer 3 Switch sẽ được sử dụng để đảm nhiệm vai trò tầng phân phối, kết nối trực tiếp với tường lửa ASA và các Layer 2 Switch tại tầng Access. Các thiết bị ở tầng này có thể đảm nhiệm chức năng như định tuyến VLAN (Inter-VLAN Routing), thiết lập chính sách bảo mật, kiểm soát truy cập và giám sát hệ thống.

Các chức năng chính:

- Phân phối lưu lượng từ các Switch tầng truy cập lên tầng lõi.
- Thực hiện định tuyến giữa các VLAN.
- Dự phòng đường truyền và cân bằng tải trong hệ thống mạng.

Các dịch vụ tại tầng này:

- DNS: Cấu hình trên Server, dịch địa chỉ IPv4 99.0.0.9/28 thành hai tên miền “anhquat.com.vn” và “mail.anhquat.com.vn”.
- Web: Cấu hình trên Server, đặt tên miền của trang web là “anhquat.com.vn”.
- Mail: Cấu hình trên Server, định dạng của mail là “@anhquat.com.vn”, tên miền cho máy chủ gửi và nhận mail là “mail.anhquat.com.vn”.
- DHCP: Cấu hình trên các Layer 3 Switch, cấp phát tự động cho từng VLAN.

Mạng nội bộ được chia thành nhiều VLAN khác nhau phục vụ cho từng phòng/khoa riêng biệt dựa theo dải gốc là 172.16.0.0/24 cho cơ sở 1 và 192.168.0.0/24 cho cơ sở 2.

Mỗi phòng/khoa trong bệnh viện sẽ được bố trí một Layer 2 Switch đóng vai trò Switch truy cập. Các Switch này sẽ kết nối lên tầng phân phối qua Layer 3 Switch, đảm bảo việc phân vùng mạng theo VLAN, cấp phát IP, và cô lập lưu lượng giữa các phòng ban.

Các chức năng chính:

- Kết nối các thiết bị đầu cuối vào mạng.
- Quản lý truy cập thông qua VLAN, DHCP.
- Cung cấp kết nối Wi-Fi thông qua các Router Wifi gắn ở các tầng.
- Phân chia lưu lượng hợp lý và đảm bảo an toàn nội bộ cho từng khoa phòng.

Tại một số tầng sẽ trang bị Router Wifi cung cấp dịch vụ wifi cho bệnh viện.

2.3. Thiết kế hệ thống

Bảng 2.1. Bảng các dải địa chỉ mạng ở tầng lõi

Vùng Mạng	Dải IPv4 CIDR	Dải IPv6 CIDR	Chức năng
Firewall-1& SW-L3-1	10.0.0.0/30	10:1::/64	Dải IP kết nối giữa Firewall-1 và SW-L3-1
Firewall-1&ISP	10.0.1.0/30	10:2::/64	Dải IP kết nối ra Internet thông qua ISP cho cơ sở 1.
Firewall-1& SW-L3-2	172.16.255.4/30	10:3::/64	Dải IP cho kết nối giữa Firewall-1 và SW-L3-2
Firewall-2& SW-L3-1-2	11.0.0.0/30	11:1::/64	Dải IP cho kết nối giữa Firewall-2 và SW-L3-1-2
Firewall2&ISP	11.0.1.0/30	11:2::/64	Dải IP cho kết nối ra Internet thông qua ISP cho cơ sở 2.
Firewall-1& DMZ	99.0.0.0/28	99:1:1::/64	Dải IP kết nối giữa Firewall-1 và DMZ

Bảng 2.2. Bảng các dải địa chỉ mạng ở tầng phân phối

Vùng Mạng	Dải IPv4 CIDR	Dải IPv6 CIDR	Chức năng
Firewall-1& SW-L3-1	10.0.0.0/30	10:1::/64	Dải IP kết nối giữa Firewall-1 và SW-L3-1
Firewall-1& SW-L3-2	172.16.255.4/30	10:3::/64	Dải IP cho kết nối giữa Firewall-1 và SW-L3-2
Firewall-2& SW-L3-1-2	11.0.0.0/30	11:1::/64	Dải IP cho kết nối giữa Firewall-2 và SW-L3-1-2
SW-L3-1& SW-L3-2	172.16.100.0/30	100:100:100::/64	Dải IP kết nối giữa 2 Layer 3 Switch cơ sở 1
DMZ	99.0.0.0/28	99:1:1::/64	Dải IP của DMZ

Bảng 2.3. Bảng địa chỉ dải mạng và VLAN cơ sở 1

VLAN ID	Tên VLAN	IPv6 CIDR	IPv4 CIDR
101	VLAN_CAPCUU	1111:101::/64	172.16.0.0/28
102	VLAN_TIEPDON	1111:102::/64	172.16.0.16/28
103	VLAN_NOI	1111:103::/64	172.16.0.32/28
104	VLAN_NGOAI	1111:104::/64	172.16.0.48/28
105	VLAN_SAN	1111:105::/64	172.16.0.64/28
106	VLAN_NHI	1111:106::/64	172.16.0.80/28
107	VLAN_MAT	1111:107::/64	172.16.0.96/29
108	VLAN_DALIEU	1111:108::/64	172.16.0.104/29
109	VLAN_RHM	1111:109::/64	172.16.0.112/29
110	VLAN_TMH	1111:110::/64	172.16.0.120/29
111	VLAN_XETNGHIEM	1111:111::/64	172.16.0.128/28
112	VLAN_CDHA	1111:112::/64	172.16.0.144/28
113	VLAN_VLTL	1111:113::/64	172.16.0.160/29
114	VLAN_NOITRU6	1111:114::/64	172.16.0.168/29
115	VLAN_NOITRU7	1111:115::/64	172.16.0.176/29
116	VLAN_HOIDONG	1111:116::/64	172.16.0.184/29
117	VLAN_HANHCHINH	1111:117::/64	172.16.0.192/28
118	VLAN_SERVER	1111:118::/64	172.16.0.209/28
119	VLAN_IT	1111:119::/64	172.16.0.224/28

Bảng 2.4. Bảng địa chỉ dải mạng và VLAN cơ sở 2

VLAN ID	Tên VLAN	IPv6 CIDR	IPv4 CIDR
201	VLAN_PKDK	2222:201::/64	192.168.0.0/29
202	VLAN_TIEPDON2	2222:202::/64	192.168.0.8/29
203	VLAN_XETNGHIEM2	2222:203::/64	192.168.0.16/29
204	VLAN_NGOAI2	2222:204::/64	192.168.0.24/29
205	VLAN_SAN2	2222:205::/64	192.168.0.32/29
206	VLAN_NHI2	2222:206::/64	192.168.0.40/29
207	VLAN_TIEMCHUNG	2222:207::/64	192.168.0.48/29
208	VLAN_HOIDONG2	2222:208::/64	192.168.0.56/29
209	VLAN_HANHCHINH2	2222:209::/64	192.168.0.64/29
210	VLAN_IT2	2222:210::/64	192.168.0.72/29

Bảng 2.5. Bảng địa chỉ dải mạng các Router wifi

Tên thiết bị	LAN IP (CIDR)	Địa chỉ IP WAN	Ghi chú
Wifi Tang 1 (WRT300N)	30.0.0.0/24	172.16.0.4	Phủ Wi-Fi tầng 1 và 2, IP VLAN 101
Wifi Tang 3 (WRT300N)	40.0.0.0/24	172.16.0.106	Phủ Wi-Fi tầng 3 và 4, IP VLAN 108
Wifi Tang 5 (WRT300N)	50.0.0.0/24	172.16.0.162	Phủ Wi-Fi tầng 5 và 6, IP VLAN 113
Wifi Tang 7 (WRT300N)	70.0.0.0/24	172.16.0.177	Phủ Wi-Fi tầng 7 và 8, IP VLAN 115
Wifi Tang 2-2 (WRT300N)	22.0.0.0/24	192.168.0.26	Phủ Wi-Fi cơ sở 2, IP VLAN 204

CHƯƠNG 3 - XÂY DỰNG VÀ KIỂM THỬ HOẠT ĐỘNG HỆ THỐNG

3.1. Triển khai hệ thống

Bảng 3.1. Bảng kết nối thiết bị Firewall-1

Thiết bị	Giao diện	Tới giao diện của thiết bị	Địa chỉ IPv4	Địa chỉ IPv6
Firewall-1 (ASA5506X)	G1/1	Gi0/2 (SW-L3-1)	10.0.0.2	10:1::2
	G1/2	Gi0/0 (ISP-OUTSIDE)	10.0.1.2	10:2::2
	G1/3	Fa0/2 (SW-SERVER)	99.0.0.1	99:1:1::1
	Gi1/4	Gi1/0/20 (SW-L3-2)	172.16.255.5	10:3::2

Bảng 3.2. Bảng kết nối thiết bị Firewall-2

Thiết bị	Giao diện	Tới giao diện của thiết bị	Địa chỉ IPv4	Địa chỉ IPv6
Firewall-2 (ASA5506X)	G1/1	Gi0/0 (SW-L3-1-2)	11.0.0.2	11:1::2
	G1/2	Gi0/1 (ISP-OUTSIDE)	11.0.1.2	11:2::2

Bảng 3.3. Bảng kết nối thiết bị SW-L3-1

Thiết bị	Giao diện	Tới giao diện của thiết bị	Địa chỉ IPv4	Địa chỉ IPv6
SW-L3-1 (C3650-24PS)	Gi1/0/1	Gi0/1 (SW-TANG1)	Trunk	
	Gi1/0/2	Gi0/1 (SW-TANG2)		
	Gi1/0/3	Gi0/1 (SW-TANG3)		
	Gi1/0/4	Gi0/1 (SW-TANG4)		
	Gi1/0/5	Gi0/1 (SW-TANG5)		
	Gi1/0/6	Gi0/1 (SW-TANG6)		
	Gi1/0/7	Gi0/1 (SW-TANG7)		
	Gi1/0/8	Gi0/1 (SW-TANG8)		
	Gi1/0/9	SW-L3-2		
	Gi1/0/10	SW-L3-2	172.16.100.1	100:100:100::1
	Gi1/0/20	Gi0/1 (Firewall-1)	10.0.0.1	10:1::1

Bảng 3.4. Bảng địa chỉ IPv4 Interface Vlan cơ sở 1

VLAN	Mô tả	Địa chỉ Interface Vlan trên SW-L3-1	Địa chỉ Interface Vlan trên SW-L3-2
101	CAPCUU	172.16.0.1/28	172.16.0.2/28
102	TIEPDON	172.16.0.17/28	172.16.0.18/28
103	NOIKHOA	172.16.0.33/28	172.16.0.34/28
104	NGOAIKHOA	172.16.0.49/28	172.16.0.50/28
105	SANKHOA	172.16.0.65/28	172.16.0.66/28
106	NHIKHOA	172.16.0.81/28	172.16.0.82/28
107	KHAMMAT	172.16.0.97/29	172.16.0.98/29
108	DALIEU	172.16.0.105/29	172.16.0.106/29
109	RHM	172.16.0.113/29	172.16.0.114/29
110	TMH	172.16.0.121/29	172.16.0.122/29
111	XETNGHIEM	172.16.0.130/28	172.16.0.129/28
112	CDHA	172.16.0.146/28	172.16.0.145/28
113	VLTL	172.16.0.162/29	172.16.0.161/29
114	NOITRU6	172.16.0.170/29	172.16.0.169/29
115	NOITRU7	172.16.0.178/29	172.16.0.177/29
116	HOIDONG	172.16.0.186/29	172.16.0.185/29
117	HANHCHINH	172.16.0.194/28	172.16.0.193/28
119	PIT	172.16.0.226/28	172.16.0.225/28

Bảng 3.5. Bảng địa chỉ IPv6 Interface Vlan cơ sở 1

VLAN	Mô tả	Địa chỉ IPv6 Interface VLAN trên SW-L3-1	Địa chỉ IPv6 Interface VLAN trên SW-L3-2
101	CAPCUU	1111:101::1/64	1111:101::2/64
102	TIEPDON	1111:102::1/64	1111:102::2/64
103	NOIKHOA	1111:103::1/64	1111:103::2/64
104	NGOAIKHOA	1111:104::1/64	1111:104::2/64
105	SANKHOA	1111:105::1/64	1111:105::2/64
106	NHIKHOA	1111:106::1/64	1111:106::2/64
107	KHAMMAT	1111:107::1/64	1111:107::2/64
108	DALIEU	1111:108::1/64	1111:108::2/64
109	RHM	1111:109::1/64	1111:109::2/64
110	TMH	1111:110::1/64	1111:110::2/64

111	XETNGHIEM	1111:111::2/64	1111:111::1/64
112	CDHA	1111:112::2/64	1111:112::1/64
113	VLTL	1111:113::2/64	1111:113::1/64
114	NOITRU6	1111:114::2/64	1111:114::1/64
115	NOITRU7	1111:115::2/64	1111:115::1/64
116	HOIDONG	1111:116::2/64	1111:116::1/64
117	HANHCHINH	1111:117::2/64	1111:117::1/64
118	SERVER	1111:118::2/64	1111:118::1/64
119	PIT	1111:119::2/64	1111:119::1/64

Bảng 3.6. Bảng địa chỉ IPv4 Interface Vlan cơ sở 2

VLAN	Mô tả	Địa chỉ IPv4 Interface VLAN trên SW-L3-1-2	Địa chỉ IPv6 Interface VLAN trên SW-L3-1-2
201	PKDK	192.168.0.1/29	2222:201::1/64
202	TIEPDON2	192.168.0.9/29	2222:202::1/64
203	XETNGHIEM2	192.168.0.17/29	2222:203::1/64
204	NGOAI2	192.168.0.25/29	2222:204::1/64
205	SAN2	192.168.0.33/29	2222:205::1/64
206	NHI2	192.168.0.41/29	2222:206::1/64
207	TIEMCHUNG	192.168.0.49/29	2222:207::1/64
208	HOIDONG2	192.168.0.57/29	2222:208::1/64
209	HANHCHINH2	192.168.0.65/29	2222:209::1/64
210	IT2	192.168.0.73/29	2222:210::1/64

Bảng 3.7. Bảng kết nối thiết bị SW-L3-2

Thiết bị	Giao diện	Tối giao diện của thiết bị	Địa chỉ IPv4	Địa chỉ IPv6
SW-L3-2 (C3650-24PS)	Gi1/0/1	Gi0/2 (SW-TANG1)	Trunk	
	Gi1/0/2	Gi0/2 (SW-TANG2)		
	Gi1/0/3	Gi0/2 (SW-TANG3)		
	Gi1/0/4	Gi0/2 (SW-TANG4)		
	Gi1/0/5	Gi0/2 (SW-TANG5)		
	Gi1/0/6	Gi0/2 (SW-TANG6)		
	Gi1/0/7	Gi0/2 (SW-TANG7)		
	Gi1/0/8	Gi0/2 (SW-TANG8)		
	Gi1/0/9	SW-L3-1		
	Gi1/0/10	SW-L3-1	172.16.100.2	100:100:100::2
	Gi1/0/20	Gi0/0 (Firewall-1)	172.16.255.6	10:3::1

Bảng 3.8. Bảng kết nối thiết bị SW-TANG 1

Thiết bị	Giao diện	Tới giao diện của thiết bị	Ghi chú
SW-TANG 1 (C2960-24TT)	Fa0/1	Fa0(PHONGCAPCUU)	Khu cấp cứu
	Fa0/2	Fa0(PHONGTIEPDON)	Phòng tiếp nhận
	Fa0/3	HomeRouter Wifi Tang 1	Wifi tầng 1, 2
	Gi0/1	Gi1/0/1 (SW-L3-1)	Trunk
	Gi0/2	Gi1/0/1 (SW-L3-2)	

Bảng 3.9. Bảng kết nối thiết bị SW-TANG 2

Thiết bị	Giao diện	Tới giao diện của thiết bị	Ghi chú
SW-TANG 2 (C2960-24TT)	Fa0/1	Fa0(NOI KHOA)	Phòng khám nội
	Fa0/2	Fa0(NGOAI KHOA)	Phòng khám ngoại
	Fa0/3	Fa0(SAN KHOA)	Phòng khám sản
	Fa0/4	Fa0(NHI KHOA)	Phòng khám nhi
	Gi0/1	Gi1/0/2 (SW L3 -1)	Trunk
	gi0/2	Gi1/0/2 (SW L3 -2)	

Bảng 3.10. Bảng kết nối thiết bị SW-TANG 3

Thiết bị	Giao diện	Tới giao diện của thiết bị	Ghi chú
SW-TANG 3 (C2960-24TT)	Fa0/1	Fa0(KHOA MAT)	Phòng khám mắt
	Fa0/2	Fa0(KHOA DA LIEU)	Phòng khám da liễu
	Fa0/3	Fa0(KHOA RHM)	Phòng răng hàm mặt
	Fa0/4	Fa0(KHOA TMH)	Phòng tai mũi họng
	Fa0/5	HomeRouter Wifi Tang 3	Wifi tầng 3, 4
	Gi0/1	Gi1/0/3 (SW-L3-1)	Trunk
	Gi0/2	Gi1/0/3 (SW-L3-2)	

Bảng 3.11. Bảng kết nối thiết bị SW-TANG 4

Thiết bị	Giao diện	Tới giao diện của thiết bị	Ghi chú
SW-TANG 4 (C2960-24TT)	Fa0/1	Fa0(PHONGXNGHIEM)	Phòng xét nghiệm
	Fa0/2	Fa0(PHONGCDHA)	Phòng CDHA
	Gi0/1	Gi1/0/4 (SW L3 -1)	Trunk
	Gi0/2	Gi1/0/4 (SW L3 -2)	

Bảng 3.12. Bảng kết nối thiết bị SW-TANG 5

Thiết bị	Giao diện	Tối giao diện của thiết bị	Ghi chú
SW-TANG 5 (C2960-24TT)	Fa0/1	Fa0(PHONGVLTL)	Phòng vật lý trị liệu
	Fa0/2	HomeRouter Wifi Tang 5	Wifi tầng 5, 6
	Gi0/1	Gi1/0/5 (SW-L3-1)	Trunk
	Gi0/2	Gi1/0/5 (SW-L3-2)	

Bảng 3.13. Bảng kết nối thiết bị SW-TANG 6

Thiết bị	Giao diện	Tối giao diện của thiết bị	Ghi chú
SW-TANG 6 (C2960-24TT)	Fa0/1	Fa0(NOITRU6)	Khu nội trú tầng 6
	Gi0/1	Gi1/0/6 (SW-L3-1)	Trunk
	Gi0/2	Gi1/0/6 (SW-L3-2)	

Bảng 3.14. Bảng kết nối thiết bị SW-TANG 7

Thiết bị	Giao diện	Tối giao diện của thiết bị	Ghi chú
SW-TANG 7 (C2960-24TT)	Fa0/1	Fa0(NOITRU7)	Khu nội trú tầng 7
	Fa0/2	HomeRouter Wifi Tang 7	Wifi tầng 7, 8
	Gi0/1	Gi1/0/7 (SW-L3-1)	Trunk
	Gi0/2	Gi1/0/7 (SW-L3-2)	

Bảng 3.15. Bảng kết nối thiết bị SW-TANG 8

Thiết bị	Giao diện	Tối giao diện của thiết bị	Ghi chú
SW-TANG 8 (C2960-24TT)	Fa0/2	Fa0(PHONG HOI DONG)	Phòng họp hội đồng
	Fa0/3	Fa0(PHONG HANH CHINH)	Phòng hành chính
	Fa0/4	Fa0(PHONG IT)	Phòng kỹ thuật
	Gi0/1	Gi1/0/8 (SW-L3-1)	Trunk
	Gi0/2	Gi1/0/8 (SW-L3-2)	

Bảng 3.16. Bảng kết nối thiết bị SW-L3-1-2

Thiết bị	Giao diện	Tối giao diện của thiết bị	Địa chỉ IPv4	Địa chỉ IPv6
SW-L3-1-2 (C3650-24PS)	Gi1/0/1	Gi0/1 (SW-TANG1 - 2)	Trunk	
	Gi1/0/2	Gi0/1 (SW-TANG2 - 2)		
	Gi1/0/3	Gi0/1 (SW-TANG3 - 2)		
	Gi1/0/11	Gi0/1 (Firewall-2)	11.0.0.1	11::1

Bảng 3.17. Bảng kết nối thiết bị Tang 1-2

Thiết bị	Giao diện	Tới giao diện của thiết bị	Ghi chú
Tang 1-2 (C2960-24TT)	Fa0/1	Fa0 (PHONG KHAM)	Phòng khám bệnh
	Fa0/2	Fa0 (PHONG TIEP DON)	Khu tiếp đón
	Fa0/3	Fa0 (PHONGXET NGHIEM)	Phòng xét nghiệm
	Gi0/1	Gi1/0/1 (SW-L3-1 - 2)	Trunk

Bảng 3.18. Bảng kết nối thiết bị Tang 2-2

Thiết bị	Giao diện	Tới giao diện của thiết bị	Ghi chú
Tang 2-2 (C2960-24TT)	Fa0/1	Fa0 (NGOAI KHOA)	Phòng ngoại khoa
	Fa0/2	Fa0 (SAN KHOA)	Phòng sản khoa
	Fa0/3	Fa0 (NHI KHOA)	Phòng nhi khoa
	Fa0/4	Fa0 (TIEM CHUNG)	Phòng tiêm chủng
	Gi0/1	Gi1/0/2 (SW-L3-1 - 2)	Trunk

Bảng 3.19. Bảng kết nối thiết bị của Tang 3-2

Thiết bị	Giao diện	Tới giao diện của thiết bị	Ghi chú
Tang 3-2 (C2960-24TT)	Fa0/1	Fa0 (HOI DONG)	Phòng hội đồng
	Fa0/2	Fa0 (HANH CHINH)	Phòng hành chính
	Fa0/3	Fa0 (IT2)	Phòng kỹ thuật
	Gi0/1	Gi1/0/3 (SW-L3-1 - 2)	Trunk

3.2. Cấu hình mô phỏng hệ thống

3.2.1. Lớp Core

- Đặt tên, đặt mật khẩu cho thiết bị.
- Cấu hình các giao diện.
- Cấu hình OSPF tới DMZ và Insize. Định tuyến tĩnh ra Outside.
- Cấu hình ACL cho phép gói tin và dịch vụ.
- Cấu hình NAT dịch địa chỉ Private sang Public.
- Cấu hình VPN site-to-site IPsec.

3.2.2. Lớp Distribution

Trên các Layer 3 Switch:

- Đặt tên, đặt mật khẩu cho thiết bị.
- Tạo các VLAN phù hợp cho từng khoa/phòng.
- Tạo interface VLAN và gán địa chỉ IPv4 và IPv6 tương ứng từng VLAN.
- Cấu hình STP.
- Cấu hình dịch vụ DHCP IPv4 và IPv6

Bảng 3.20. Bảng Pool DHCPv4 của SW-L3-1

Pool Name	Network/Subnet	Excluded Address	Default Router (Int VLAN)	DNS Server
VLAN101	172.16.0.0/28	172.16.0.1 – 172.16.0.5	172.16.0.1	99.0.0.9
VLAN102	172.16.0.16/28	172.16.0.17 – 172.16.0.21	172.16.0.17	99.0.0.9
VLAN103	172.16.0.32/28	172.16.0.33 – 172.16.0.37	172.16.0.33	99.0.0.9
VLAN104	172.16.0.48/28	172.16.0.49 – 172.16.0.53	172.16.0.49	99.0.0.9
VLAN105	172.16.0.64/28	172.16.0.65 – 172.16.0.69	172.16.0.65	99.0.0.9
VLAN106	172.16.0.80/28	172.16.0.81 – 172.16.0.85	172.16.0.81	99.0.0.9
VLAN107	172.16.0.96/29	172.16.0.97 – 172.16.0.98	172.16.0.97	99.0.0.9
VLAN108	172.16.0.104/29	172.16.0.105 – 172.16.0.106	172.16.0.105	99.0.0.9
VLAN109	172.16.0.112/29	172.16.0.113 – 172.16.0.114	172.16.0.113	99.0.0.9
VLAN110	172.16.0.120/29	172.16.0.121 – 172.16.0.122	172.16.0.121	99.0.0.9
VLAN111-2	172.16.0.128/28	172.16.0.129 – 172.16.0.133	172.16.0.130	99.0.0.9
VLAN112-2	172.16.0.144/28	172.16.0.145 – 172.16.0.149	172.16.0.146	99.0.0.9
VLAN113-2	172.16.0.160/29	172.16.0.161 – 172.16.0.162	172.16.0.162	99.0.0.9
VLAN114-2	172.16.0.168/29	172.16.0.169 – 172.16.0.170	172.16.0.170	99.0.0.9
VLAN115-2	172.16.0.176/29	172.16.0.177 – 172.16.0.178	172.16.0.178	99.0.0.9
VLAN116-2	172.16.0.184/29	172.16.0.185 – 172.16.0.186	172.16.0.186	99.0.0.9
VLAN117-2	172.16.0.192/28	172.16.0.193 – 172.16.0.197	172.16.0.194	99.0.0.9
VLAN119-2	172.16.0.224/28	172.16.0.225 – 172.16.0.229	172.16.0.226	99.0.0.9

Bảng 3.21. Bảng Pool DHCPv4 của SW-L3-2

Pool Name	Excluded-Address	Network	Default-Router	DNS-Server
VLAN101-2	172.16.0.1 – 172.16.0.5	172.16.0.0/28	172.16.0.2	99.0.0.9
VLAN102-2	172.16.0.17 – 172.16.0.21	172.16.0.16/28	172.16.0.18	99.0.0.9
VLAN103-2	172.16.0.33 – 172.16.0.37	172.16.0.32/28	172.16.0.34	99.0.0.9
VLAN104-2	172.16.0.49 – 172.16.0.53	172.16.0.48/28	172.16.0.50	99.0.0.9
VLAN105-2	172.16.0.65 – 172.16.0.69	172.16.0.64/28	172.16.0.66	99.0.0.9
VLAN106-2	172.16.0.81 – 172.16.0.85	172.16.0.80/28	172.16.0.82	99.0.0.9
VLAN107-2	172.16.0.97 – 172.16.0.98	172.16.0.96/29	172.16.0.98	99.0.0.9
VLAN108-2	172.16.0.105 – 172.16.0.106	172.16.0.104/29	172.16.0.106	99.0.0.9
VLAN109-2	172.16.0.113 – 172.16.0.114	172.16.0.112/29	172.16.0.114	99.0.0.9
VLAN110-2	172.16.0.121 – 172.16.0.122	172.16.0.120/29	172.16.0.122	99.0.0.9
VLAN111	172.16.0.129 – 172.16.0.133	172.16.0.128/28	172.16.0.129	99.0.0.9
VLAN112	172.16.0.145 – 172.16.0.149	172.16.0.144/28	172.16.0.145	99.0.0.9
VLAN113	172.16.0.161 – 172.16.0.162	172.16.0.160/29	172.16.0.161	99.0.0.9
VLAN114	172.16.0.169 – 172.16.0.170	172.16.0.168/29	172.16.0.169	99.0.0.9
VLAN115	172.16.0.177 – 172.16.0.178	172.16.0.176/29	172.16.0.177	99.0.0.9
VLAN116	172.16.0.185 – 172.16.0.186	172.16.0.184/29	172.16.0.185	99.0.0.9

VLAN117	172.16.0.193– 172.16.0.197	172.16.0.192/28	172.16.0.193	99.0.0.9
VLAN119	172.16.0.225– 172.16.0.229	172.16.0.224/28	172.16.0.225	99.0.0.9

Bảng 3.22. Bảng Pool DHCPv4 của SW-L3-1-2

Pool Name	Excluded-Address	Network	Default-Router	DNS-Server
VLAN201_ POOL	192.168.0.1 - 192.168.0.2	192.168.0.0/29	192.168.0.1	10.0.1.3
VLAN202_ POOL	192.168.0.9 - 192.168.0.10	192.168.0.8/29	192.168.0.9	10.0.1.3
VLAN203_ POOL	192.168.0.17 - 192.168.0.18	192.168.0.16/29	192.168.0.17	10.0.1.3
VLAN204_ POOL	192.168.0.25 - 192.168.0.26	192.168.0.24/29	192.168.0.25	10.0.1.3
VLAN205_ POOL	192.168.0.33 - 192.168.0.34	192.168.0.32/29	192.168.0.33	10.0.1.3
VLAN206_ POOL	192.168.0.41 - 192.168.0.42	192.168.0.40/29	192.168.0.41	10.0.1.3
VLAN207_ POOL	192.168.0.49 - 192.168.0.50	192.168.0.48/29	192.168.0.49	10.0.1.3
VLAN208_ POOL	192.168.0.57 - 192.168.0.58	192.168.0.56/29	192.168.0.57	10.0.1.3
VLAN209_ POOL	192.168.0.65 - 192.168.0.66	192.168.0.64/29	192.168.0.65	10.0.1.3
VLAN210_ POOL	192.168.0.73 - 192.168.0.74	192.168.0.72/29	192.168.0.73	10.0.1.3

- Cấu hình định tuyến OSPF.
- Triển khai các kết nối đáp ứng:
 - + Kết nối với ASA qua dải ip riêng.
 - + Kết nối trunking với các Layer 2 Switch.

Trên Server:

- Đặt thông tin cho Server.
- Triển khai dịch vụ DNS dịch địa chỉ 99.0.0.9 thành tên hai tên miền “anhquaat.com.vn” và “mail.anhquaat.com.vn”.
- Triển khai dịch vụ Mail Server
- Mail Server:

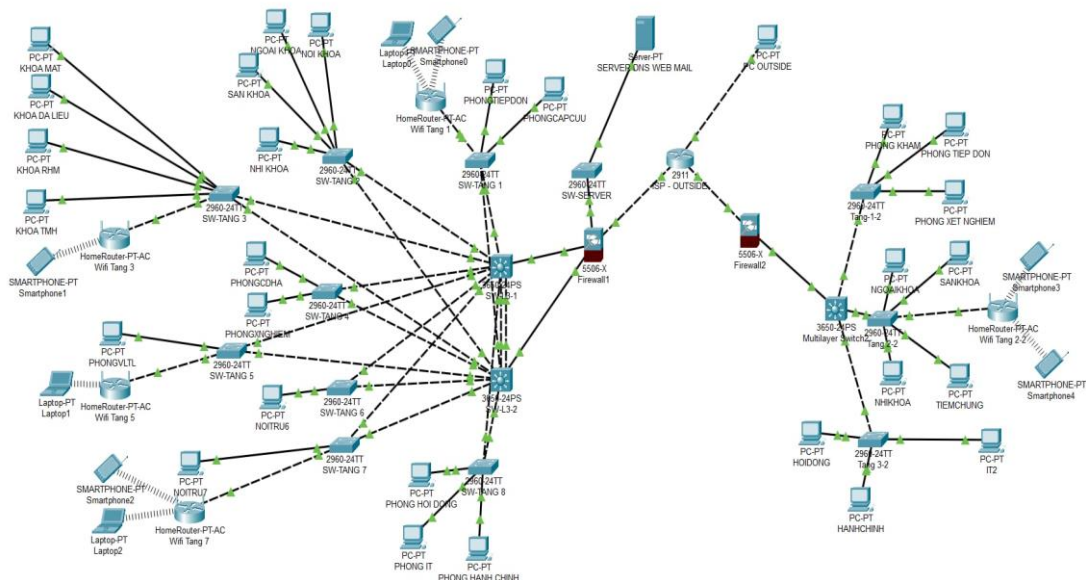
- + admin@anhquat.com.vn (admin/123456)
- + ptn@anhquat.com.vn (ptn/123456)
- + tchung@anhquat.com.vn (tchung/123456)
- + hchinh@anhquat.com.vn (hchinh/123456)
- + dtcs2@anhquat.com.vn (dtcs2/123456)
- DNS cho Mail Server:
 - + A Record (mail.anhquat.com.vn/IPv4).
 - + AAAA Record (v6.mail.anhquat.com.vn/IPv6).
- Các bản ghi trên Server:
 - + Bản ghi A: “anhquat.com.vn”(IPv4), “mail.anhquat.com.vn”.
 - + Bản ghi AAAA: ”www.anhquat.com.vn”(IPv6), “v6.mail.anhquat.com.vn”.
- Dịch vụ Web:
 - + Nội dung Web: Chào mừng đến với bệnh viện Đa khoa Anh Quất.
 - + Tên miền “anhquat.com.vn”, “www.anhquat.com.vn”.

3.2.3. Lớp Access

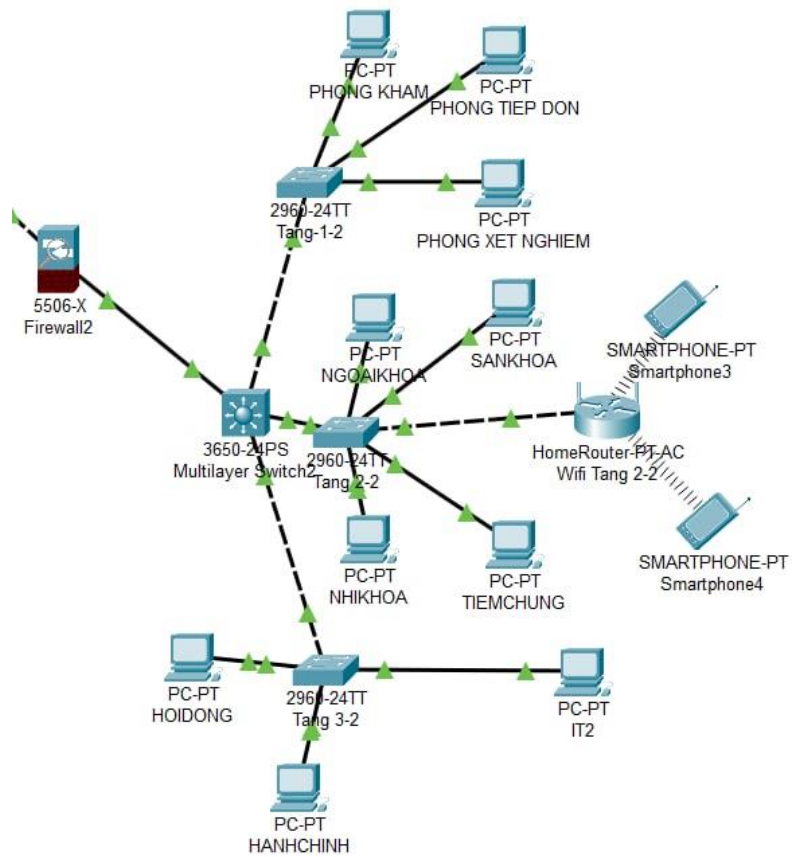
Trên các Layer 2 Switch:

- Đặt tên, đặt mật khẩu thiết bị.
- Đặt hostname phù hợp theo tầng (VD: SW-TANG1).
- Tạo các VLAN tương ứng trong mỗi tầng ứng với SW-TANGx.
- Triển khai các kết nối của Switch đáp ứng yêu cầu:
 - + Kết nối với PC, 1 PC tương ứng cho 1 VLAN.
 - + Gán các cổng tương ứng vào VLAN access.
 - + Có kết nối trunking lên các Layer 3 Switch .

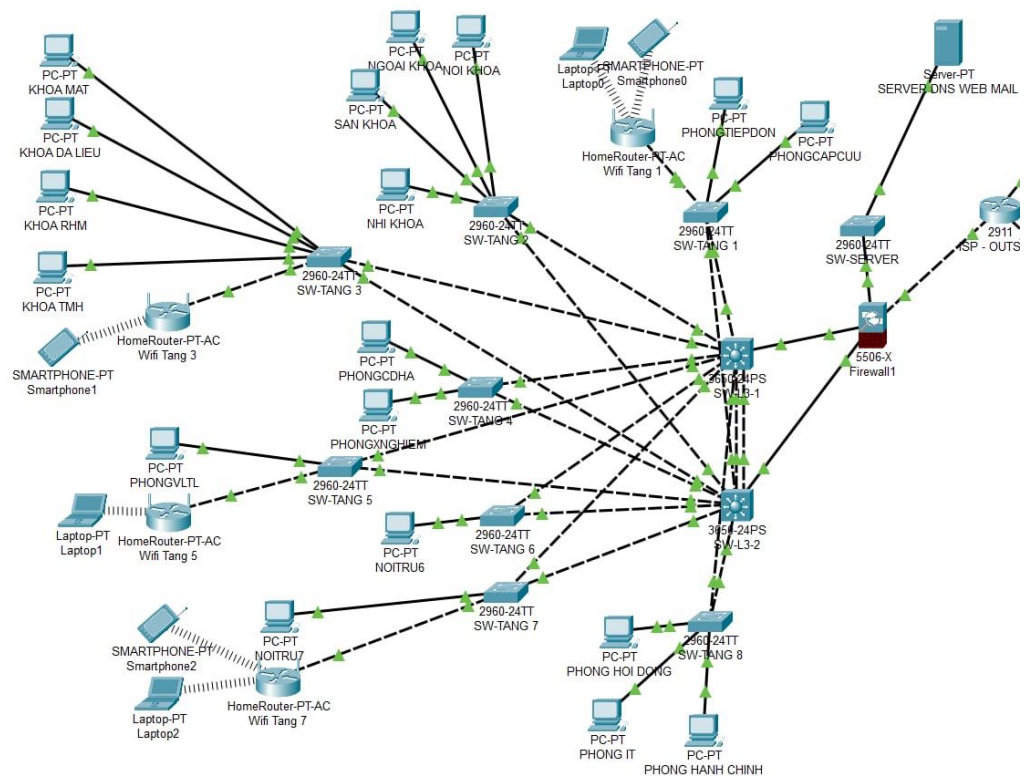
Trên các Router Wifi: Cài đặt các tham số trên Router Wifi.



Hình 3.1. Sơ đồ hệ thống bệnh viện tổng quát



Hình 3.2. Sơ đồ bệnh viện của cơ sở 2

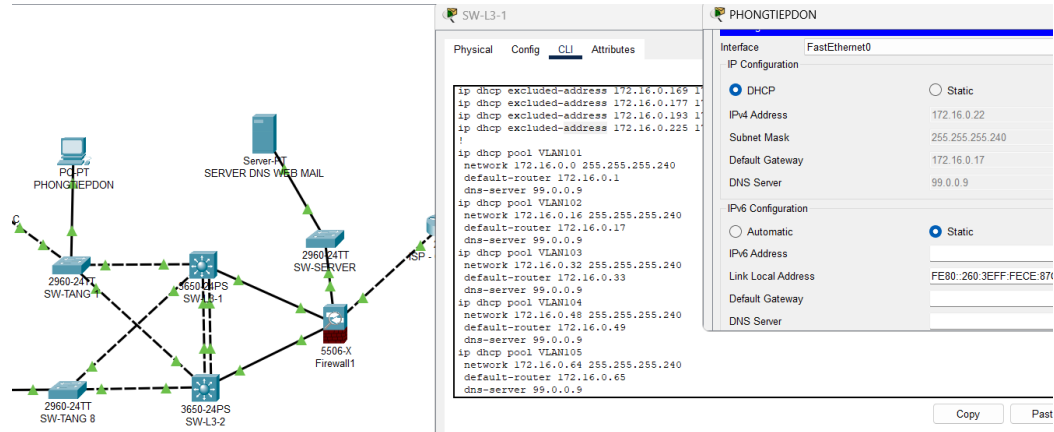


Hình 3.3. Sơ đồ bệnh viện của cơ sở 1

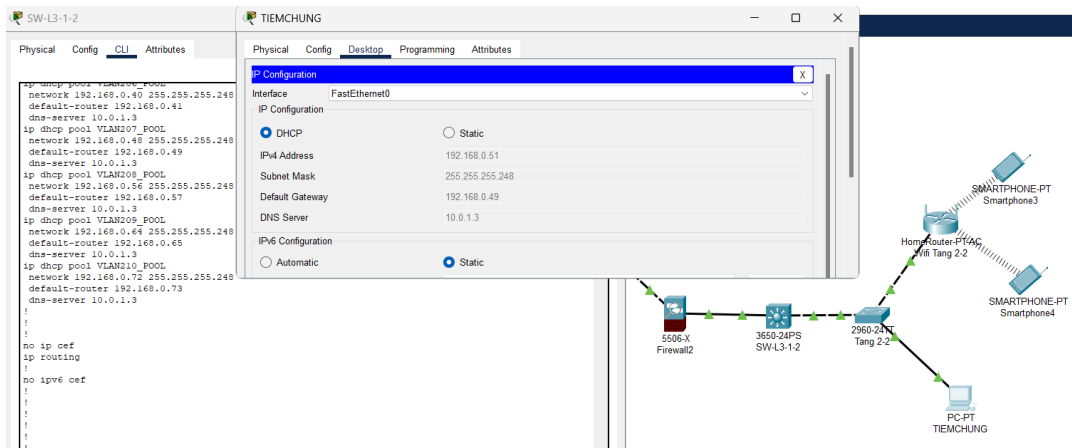
3.3. Kiểm thử hoạt động hệ thống theo kịch bản

3.3.1. Kịch bản 1: Kiểm tra dịch vụ DHCPv4 và DHCPv6

Thực hiện xin địa chỉ IPv4 tại cơ sở 1 và 2. Kết quả: Passed.

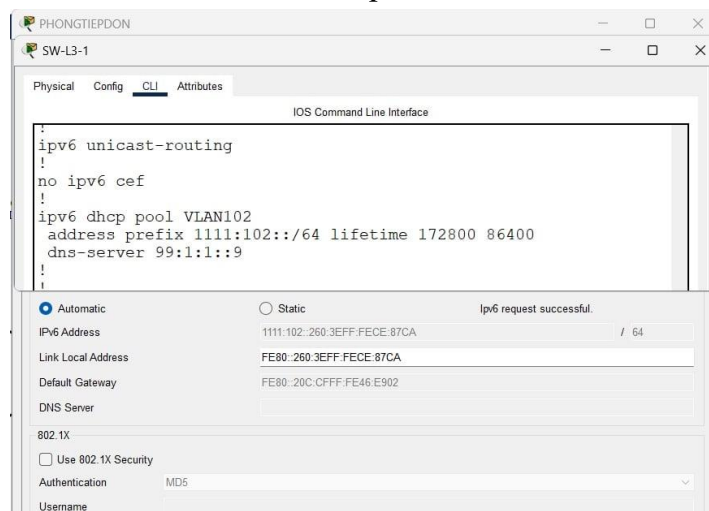


Hình 3.4. Kết quả dịch vụ DHCPv4 trên cơ sở 1



Hình 3.5. Kết quả dịch vụ DHCPv4 trên cơ sở 2

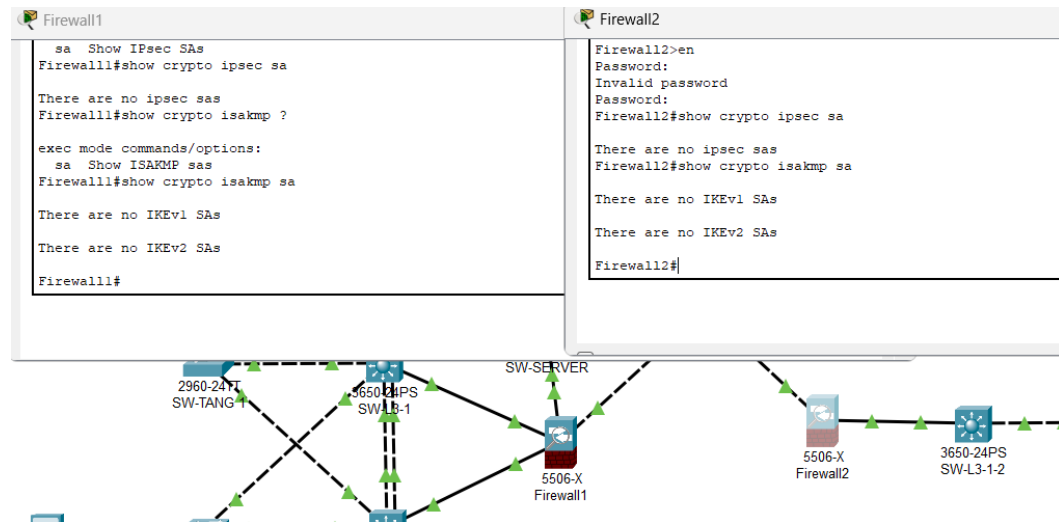
Thực hiện xin địa chỉ IPv6 tại cơ sở 1. Kết quả: Failed.



Hình 3.6. Kết quả dịch vụ DHCPv6 trên cơ sở 1

3.3.2. Kịch bản 2: Kiểm tra dịch vụ VPN site-to-site

Trước khi ping kiểm tra giữa 2 cơ sở



Hình 3.7. Kết quả kiểm tra 2 Firewall trước khi có kết nối giữa hai cơ sở
Sau khi ping kiểm tra kết nối giữa hai cơ sở

```

Firewall1
Physical Config CLI Attributes
IOS Command Line Interface

Firewall1#show crypto ipsec sa

interface: outside
Crypto map tag: CMAP, seq num: 10, local addr 10.0.1.2

permit ip 172.16.0.0 255.240.0.0 192.168.0.0 255.255.255.0
local ident (addr/mask/prot/port): (172.16.0.0/255.240.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
current_peer 11.0.1.2
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.0.1.2/0, remote crypto endpt.:11.0.1.2/0
path mtu 1500, ip mtu, ipsec overhead 78, media mtu 1500
current outbound spi: 0x63A3871F(1671661343)
current inbound spi: 0x6A728A6D(1671661343)

inbound esp sas:

Firewall1#show crypto isakmp sa

IKEv1 SAs:

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 1
1 IKE Peer: 11.0.1.2
Type : L2L Role : Initiator
Rekey : no State : QM_IDLE

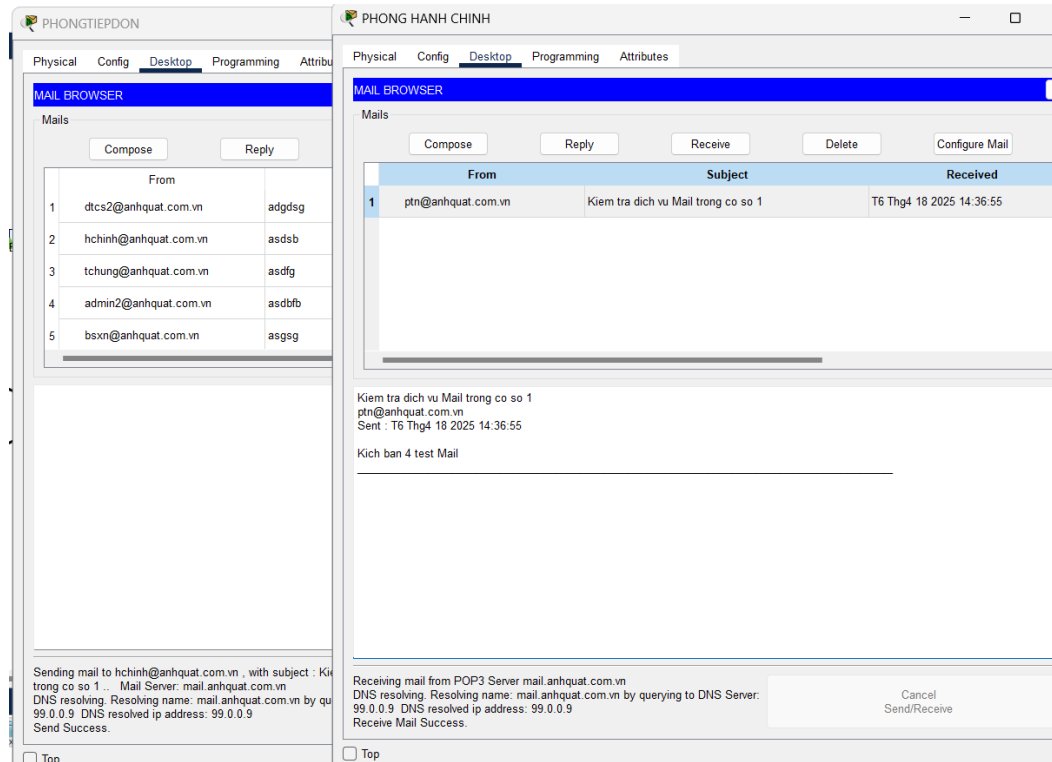
There are no IKEv2 SAs
  
```

Hình 3.8. Kết quả kiểm tra sau khi có kết nối giữa hai cơ sở

3.3.3. Kịch bản 3: Kiểm tra dịch vụ DNS

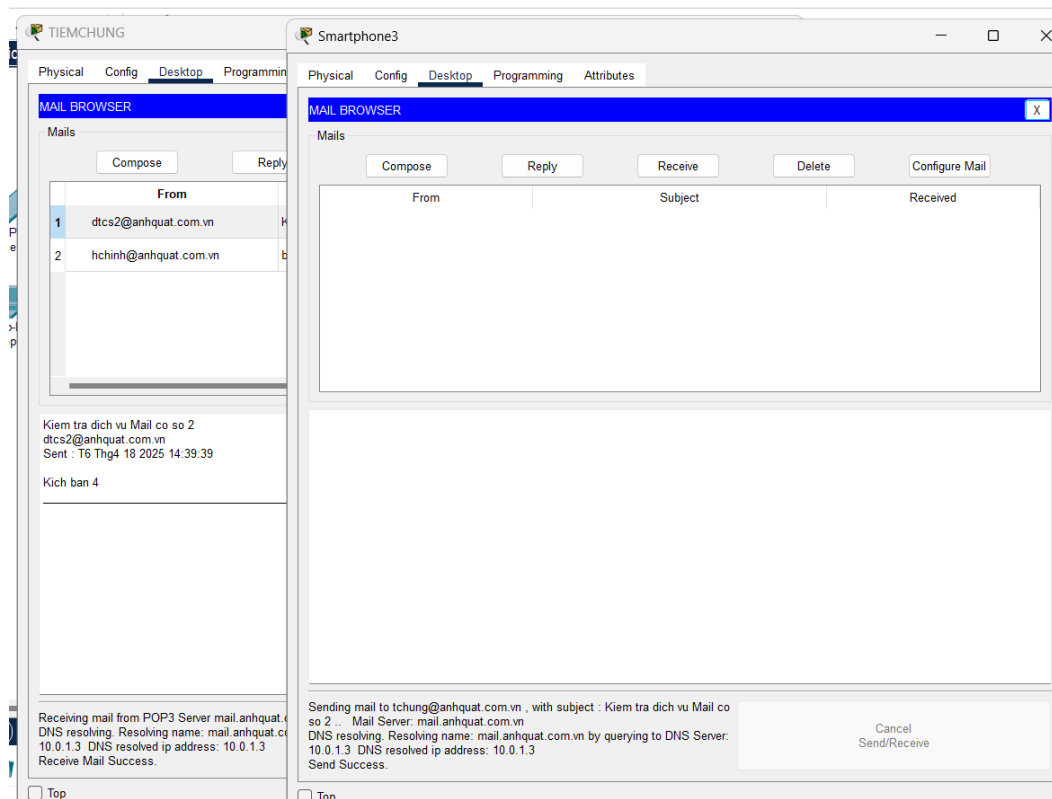
3.3.5. Kịch bản 4: Kiểm tra dịch vụ Mail

Kiểm tra dịch vụ Mail giữa các máy cơ sở 1



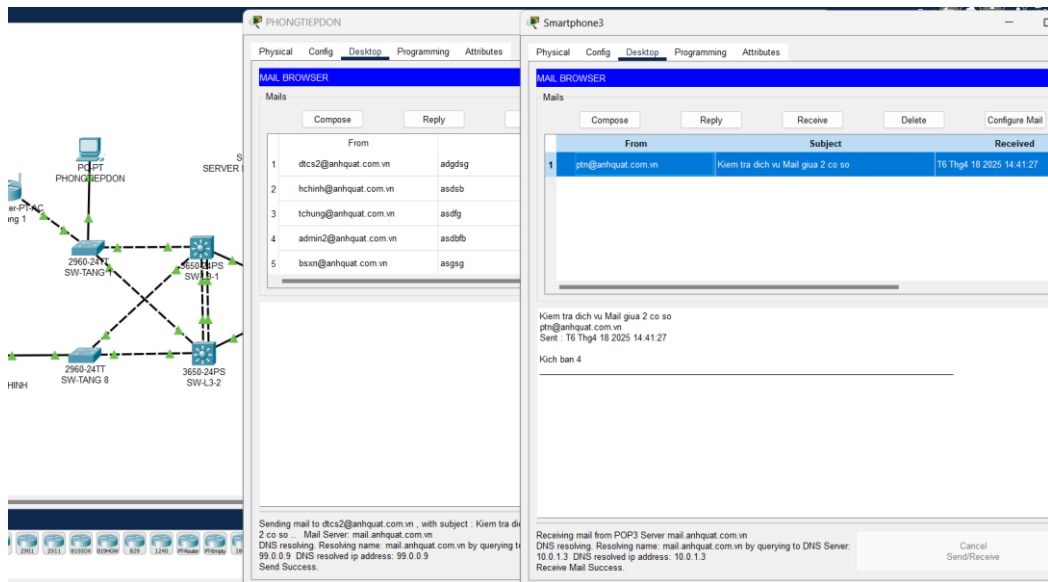
Hình 3.11. Kết quả kiểm tra dịch vụ Mail tại cơ sở 1

Kiểm tra dịch vụ Mail tại cơ sở 2



Hình 3.12. Kiểm tra dịch vụ Mail tại cơ sở 2

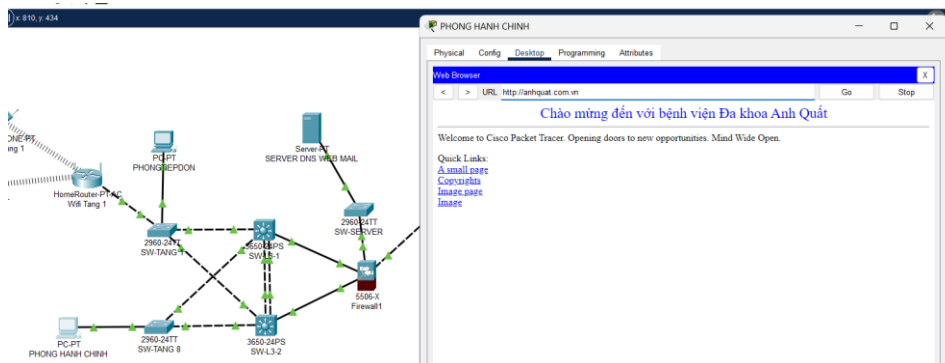
Kiểm tra dịch vụ Mail giữa hai cơ sở



Hình 3.13. Kết quả kiểm tra dịch vụ Mail giữa hai cơ sở

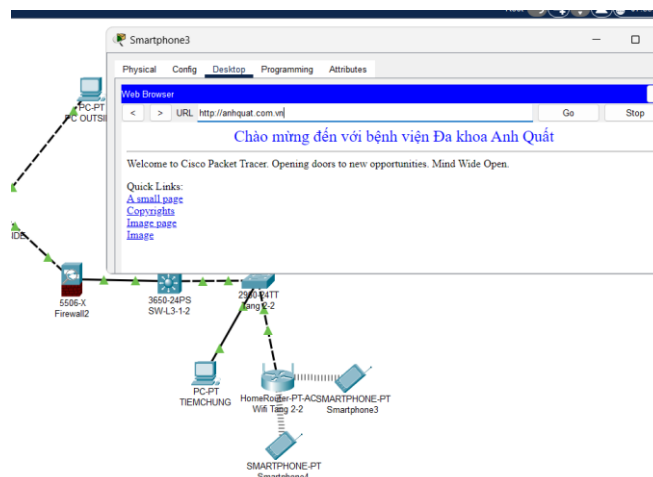
3.3.6. Kịch bản 5: Kiểm tra dịch vụ Web

Kiểm tra dịch vụ Web từ máy của cơ sở 1



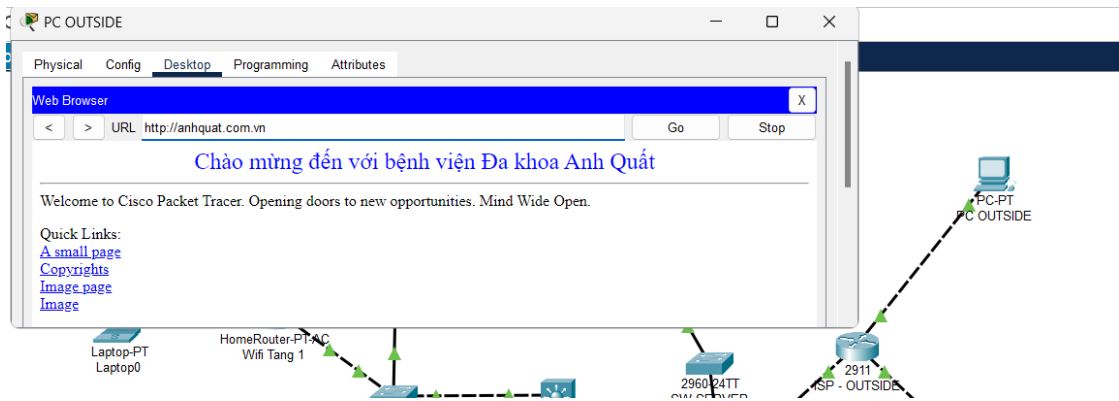
Hình 3.14. Kết quả kiểm tra dịch vụ Web cơ sở 1

Kiểm tra dịch vụ Web từ máy của cơ sở 2



Hình 3.15. Kết quả kiểm tra dịch vụ Web cơ sở 2

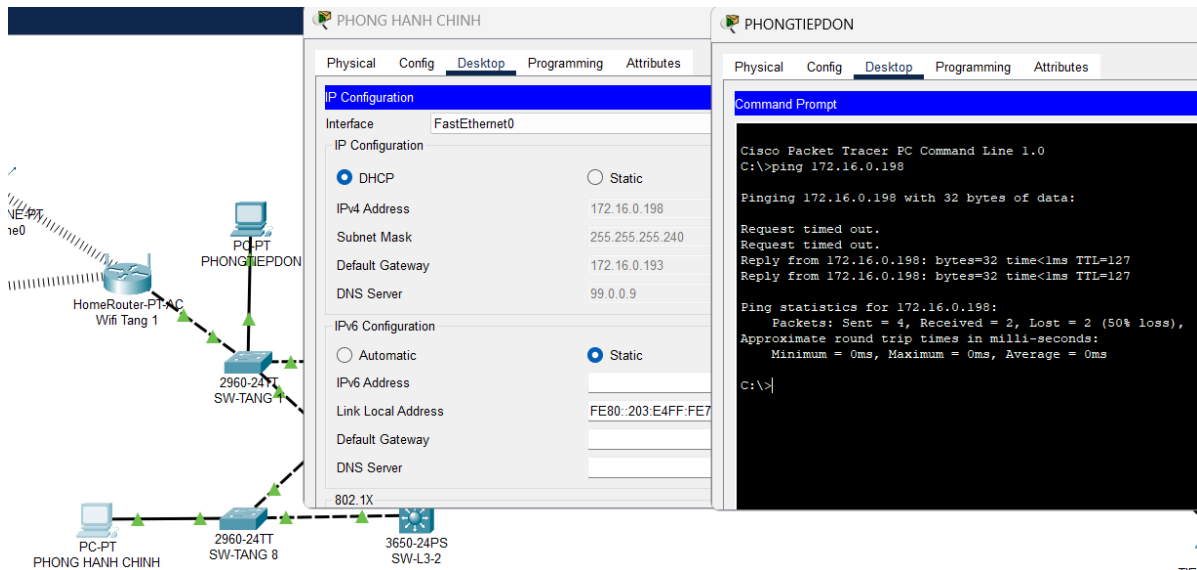
Kiểm tra dịch vụ Web từ máy bên ngoài



Hình 3.16. Kết quả kiểm tra dịch vụ Web từ bên ngoài

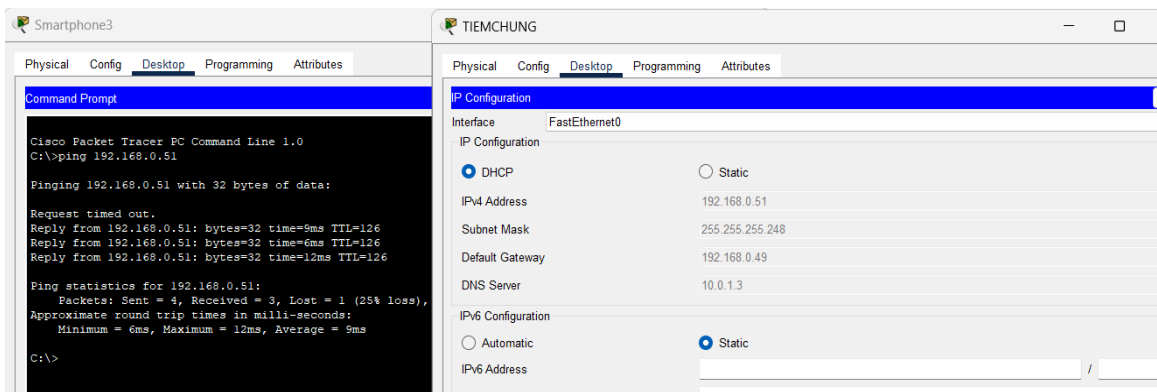
3.3.7. Kịch bản 6: Kiểm tra kết nối mạng trong trường hợp hệ thống vẫn hoạt động bình thường

Kiểm tra kết nối giữa các máy trong cơ sở 1.



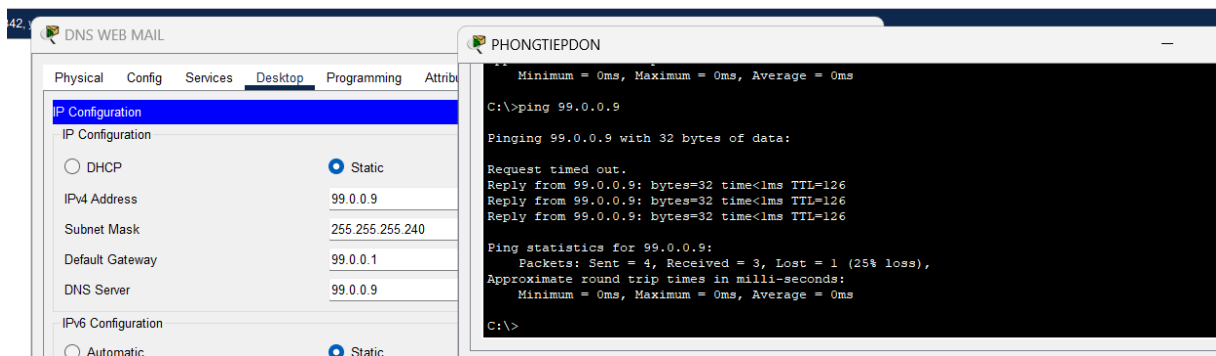
Hình 3.17. Kết quả kiểm tra kết nối giữa các máy trong cơ sở 1

Kiểm tra kết nối giữa các máy trong cơ sở 2.



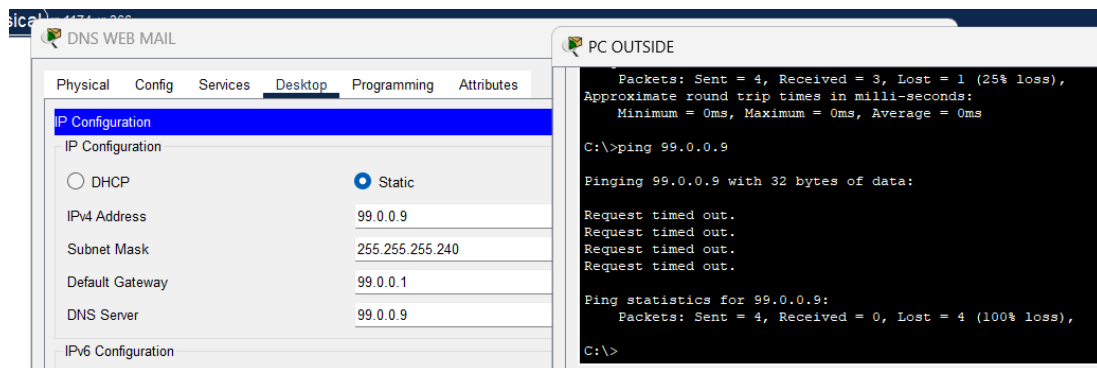
Hình 3.18. Kết quả kiểm tra kết nối giữa các máy trong cơ sở 2

Kiểm tra kết nối giữa các máy cơ sở 1 và Server “DNS WEB MAIL”.



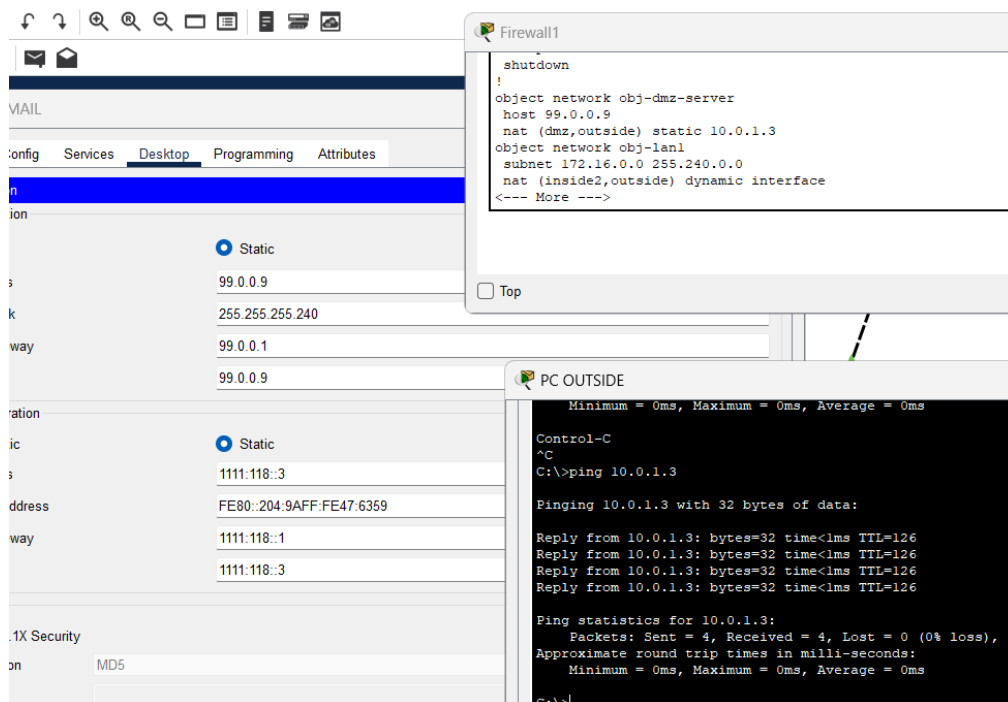
Hình 3.19. Kết quả kiểm tra kết nối giữa máy cơ sở 1 và Server

Kiểm tra kết nối giữa máy Outside đến Server “DNS WEB MAIL” qua IPv4 private của Server.



Hình 3.20. Kết quả kiểm tra kết nối qua IPv4 private của Server từ Outside

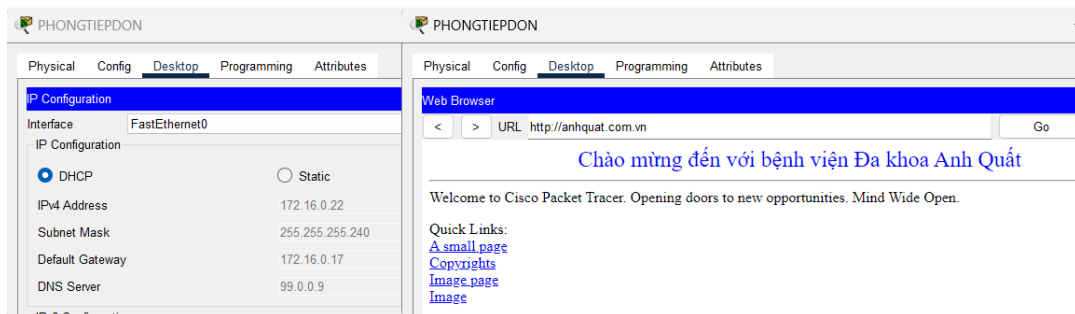
Kiểm tra kết nối giữa máy Outside đến địa chỉ đã NAT public của Server.



Hình 3.21. Kết quả kiểm tra kết nối đến địa chỉ đã NAT của Server từ Outside

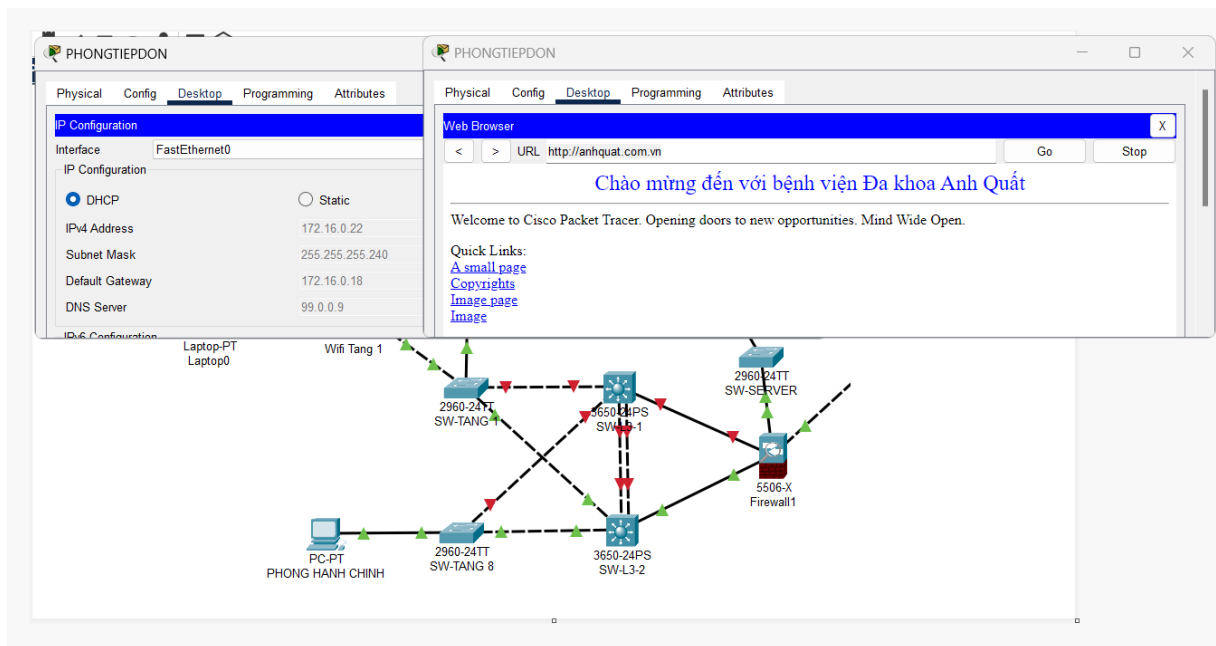
3.3.8. Kịch bản 7: Kiểm tra kết nối mạng khi hệ thống có sự cố

Kết quả truy cập dịch vụ khi hệ thống hoạt động bình thường.



Hình 3.22. Kết quả kịch bản 7 trước khi có sự cố

Kết quả truy cập dịch vụ khi hệ thống xảy ra sự cố.



Hình 3.23. Kết quả kiểm tra kết nối sau khi có sự cố

KẾT LUẬN

1. Kết quả đạt được

Trong quá trình thực hiện đồ án, phần lớn các nội dung theo kế hoạch đã được thực hiện. Em đã tiến hành đầy đủ các bước gồm khảo sát yêu cầu thực tế tại bệnh viện, phân tích hệ thống, thiết kế kiến trúc mạng theo mô hình ba lớp (Core – Distribution – Access), cấu hình các thiết bị mạng và mô phỏng hệ thống toàn diện. Các dịch vụ quan trọng như DHCP, DNS, Web, Mail, NAT, VPN, ACL và phân chia VLAN được cấu hình đúng chức năng và hoạt động ổn định. Đã thực hiện kiểm thử thông qua các test case để kiểm tra hệ thống đảm bảo yêu cầu về kết nối, hiệu suất, khả năng mở rộng và bảo mật mạng trong môi trường của bệnh viện.

2. Nhược điểm, hạn chế

Mặc dù đạt được nhiều kết quả tích cực, đồ án vẫn còn một số hạn chế nhất định. Do giới hạn của phần mềm Cisco Packet Tracer, một số chức năng nâng cao chưa thể triển khai, cụ thể là chưa thực hiện được cấu hình địa chỉ IPv6 như dự kiến và không sử dụng được các phần mềm giả lập chuyên sâu như GNS3 hoặc Kali Linux để kiểm thử bảo mật khiến cho mô phỏng một số tình huống tấn công để kiểm tra khả năng bảo mật của hệ thống chưa được thực hiện đầy đủ như kế hoạch ban đầu.

3. Định hướng phát triển trong tương lai

Trong tương lai, hệ thống sẽ được hoàn thiện và mở rộng thêm theo các hướng sau:

- Chuyển sang sử dụng phần mềm GNS3 hoặc EVE-NG để mô phỏng mạng thực tế với độ chính xác cao hơn.
- Tích hợp các công cụ kiểm thử bảo mật như Kali Linux để đánh giá và cải thiện khả năng phòng thủ mạng.
- Nâng cấp hệ thống để đáp ứng tốt hơn các nhu cầu thực tế khi số lượng người dùng và thiết bị trong bệnh viện tăng lên.

DANH MỤC TÀI LIỆU THAM KHẢO

- [1]. Cao Văn Lực - Phạm Nông - Nguyễn Lê Huy - Trịnh Minh Nhật (2015), *Thiết kế hệ thống mạng cho bệnh viện Ái Tâm*, Cử Nhân, Trường Đại học Công nghệ thông tin – Đại học Quốc gia TP. Hồ Chí Minh.
- [2]. Bộ môn Mạng và các hệ thống thông tin, *Giáo trình bộ môn Mạng máy tính*, Trường Đại học Giao thông Vận tải.
- [3]. Bộ môn Mạng và các hệ thống thông tin, *Giáo trình bộ môn Quản trị mạng*, Trường Đại học Giao thông Vận tải.
- [4]. Benard Otom (2023), *Cisco ASA Firewall Configuration*, <[youtube.com/watch?v=Lyc_EXEhJsk&list=PLvUOx2WG6R7NVLwLGB8ZU2qyCpxyqn8nd](https://www.youtube.com/watch?v=Lyc_EXEhJsk&list=PLvUOx2WG6R7NVLwLGB8ZU2qyCpxyqn8nd)>
- [5]. Đào Viết Phương (2024), *Tóm tắt CCNA*.