

VIETNAM NATIONAL UNIVERSITY, HO CHI MINH CITY
UNIVERSITY OF TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND ENGINEERING



Mạng máy tính

Assignment Report

THIẾT KẾ HỆ THỐNG MẠNG CHO TÒA H6

Instructor: Bùi Xuân Giang
Students: Lê Anh Huy - 2013293
Thái Tăng Huy - 2013329
Trà Trung Tín - 2010702
Lê Nguyễn Ngọc Hân - 2011169

HO CHI MINH CITY, NOV 2022



Contents

1	Kiến trúc mạng	2
1.1	Phân tích yêu cầu hệ thống	2
1.2	Tính dung lượng lưu trữ, lưu lượng mạng	2
1.2.1	Phòng hành chính tòa H6	2
1.2.2	Phòng học thực hành tòa H6	2
1.2.3	Các thiết bị kết nối mạng WIFI (các cảm biến)	2
1.2.4	Các camera	3
1.3	Các thiết bị sử dụng	3
1.4	Tính toán chi phí	4
1.5	Kiến trúc mạng vật lý	5
1.6	Kỹ thuật sử dụng trong Kiến trúc mạng	5
1.6.1	VLAN với VTP	5
1.6.2	Subnet Mask	5
2	Sơ đồ IP và sơ đồ đường dây	6
2.1	Sơ đồ IP	6
2.2	Sơ đồ đường dây bên trong	6
3	Kiểm thử mô hình hệ thống	8
4	Thiết kế mô hình bằng Packet Tracer	9
5	Đánh giá mô hình	9
5.1	Tính tin cậy và bảo mật	9
5.1.1	Yêu cầu về tính tin cậy	9
5.1.2	Giải pháp đối với yêu cầu về bảo mật	10
5.2	Phần mềm sử dụng trong hệ thống	10
5.3	Sửa chữa, bảo trì và nâng cấp hệ thống	10
5.4	Định hướng phát triển trong tương lai	10

1 Kiến trúc mạng

1.1 Phân tích yêu cầu hệ thống

Để phục vụ cho công tác giám sát, nhà trường sẽ đầu tư cho mỗi phòng học trong tòa nhà H6 các thiết bị IoT:

- Các phòng lý thuyết:
 - Diện tích lớn hơn 60m²: 6 cảm biến nhiệt độ, 6 cảm biến ánh sáng, các thiết bị điều khiển ánh sáng
 - Diện tích nhỏ hơn 60m²: 3 cảm biến nhiệt độ, 3 cảm biến ánh sáng
- Tại mỗi dãy điều hành ở mỗi tầng sẽ được lắp 4 camera giám sát
- Các phòng thực hành:
 - Được trang bị máy tính để bàn
 - Được lắp thiết bị điều hòa không khí

Thiết bị đo sẽ thu thập dữ liệu liên tục 1 phút 1 lần theo thời gian thực và gửi về cho máy chủ xử lý 5 phút 1 lần.

Một cảm biến sẽ đo một chỉ số khác nhưng kích thước định dạng dữ liệu của chúng là 32 Kb. Các cảm biến sẽ thu thập dữ liệu 1 phút 1 lần và sau 5 phút, chúng sẽ gửi dữ liệu này đến máy chủ trong tâm qua mạng WIFI

Hệ thống camera giám sát hoạt động 24/7 sẽ lưu trữ dữ liệu trực tiếp về máy chủ trung tâm với tốc độ truyền dữ liệu 100Mbps

Máy tính tại các phòng học mỗi ngày tải khoảng 200MB (giờ cao điểm từ 7h đến 17h30)

Mỗi thiết bị khi kết nối với mạng WIFI được sử dụng với tốc độ tối đa là 256 Kbps trong khoảng thời gian từ 7h đến 17h30

Tòa nhà H6 có phòng hành chính với 10 máy tính. Các máy tính này mỗi ngày tải khoảng 200 MB (giờ cao điểm là 8h-11h40, 13h-16h30) và gửi 10 email mỗi ngày, dung lượng tối đa là 10 MB/email. Mỗi tầng là VLAN config và hệ thống có thể kết nối với H6

1.2 Tính dung lượng lưu trữ, lưu lượng mạng

(Tính theo tháng, một tháng có 30 ngày)

1.2.1 Phòng hành chính tòa H6

$$[10 \text{ (máy tính)} \times 200 \text{ (MB/máy tính} \times \text{ngày)} + 10 \text{ (email/ngày)} \times 10 \text{ (MB/email)}] \times 30 = 6300 \text{ (MB)}$$

1.2.2 Phòng học thực hành tòa H6

Giả sử tòa H6 có 2 tầng dùng để thực hành (tầng 6, tầng 7), mỗi tầng có 5 phòng học thực hành, mỗi phòng học thực hành có 20 máy tính

$$\bullet 200 \text{ (MB/máy tính)} \times 20 \text{ (máy tính/phòng)} \times 5 \text{ (phòng/tầng)} \times 2 \text{ tầng} \times 30 = 120\,000 \text{ (MB)}$$

1.2.3 Các thiết bị kết nối mạng WIFI (các cảm biến)

Giả sử tòa H6 có 6 tầng dùng để học lý thuyết, mỗi tầng có 5 phòng lý thuyết diện tích lớn hơn 60m² và có 5 phòng lý thuyết diện tích nhỏ hơn 60m²

Theo đề, mỗi phòng lý thuyết diện tích lớn hơn 60m² có 6 cảm biến nhiệt độ + 6 cảm biến ánh sáng = 12 cảm biến. Mỗi phòng lý thuyết diện tích nhỏ hơn 60m² có 3 cảm biến nhiệt độ + 3 cảm biến ánh sáng = 6 cảm biến

$$- \text{Số cảm biến trong một tầng} = 12 \times 5 + 6 \times 5 = 90 \text{ (cảm biến)}$$

- Tổng số cảm biến của H6 = $90 \times 6 = 540$ (cảm biến)
- Lưu lượng mạng trong 1 giờ = $540 \times 256 \times 12 = 1\,658\,880$ (Kb)
- Lưu lượng mạng = $1\,658\,880 \times 10.5 \times 30 = 522\,547\,200$ (Kb)

1.2.4 Các camera

Giả sử tòa H6 có 8 tầng

- Lưu lượng mạng = $8 \times 4 \times 100 \times 30 \times 24 \times 3600 = 8\,294\,400\,000$ (MB)

1.3 Các thiết bị sử dụng

- Cisco WS-C3560V2-48PS-S Catalyst 3560V2 Layer 3 : switch layer 3 dùng làm switch tổng



- WS-C3850-24P-L Cisco Catalyst 3850: switch later 2 dùng làm switch của mỗi tầng



- Sever Dell PowerEdge T550 42SVRDT550-714 (xeon 4310/16GB/2TB/1100W/4yr): dùng làm server



- Cisco WAP361-E-K9: điểm truy cập không dây



- Ngoài ra còn các cảm biến, dây cáp

1.4 Tính toán chi phí

- Tổng số cảm biến = $(6 + 6) \times 5 + (3 + 3) \times 5 = 90$ (cảm biến), giá mỗi cảm biến là 6.500.000 VND.
- Tổng số switch thường = 8 (switch), giá mỗi switch thường là 20.000.000 VND (VND)
- Tổng số switch tổng = 1 (switch), giá của 1 switch tổng là 200.000.000 (VND)
- Tổng số camera = $4 \times 8 = 32$ (camera), giá của mỗi camera là 1.000.000 (VND)
- Tổng số server = 4 (server) , giá mỗi server là 86.990.000 VND $\Rightarrow 4 \times 86.990.000 = 374.960.000$ (VND)

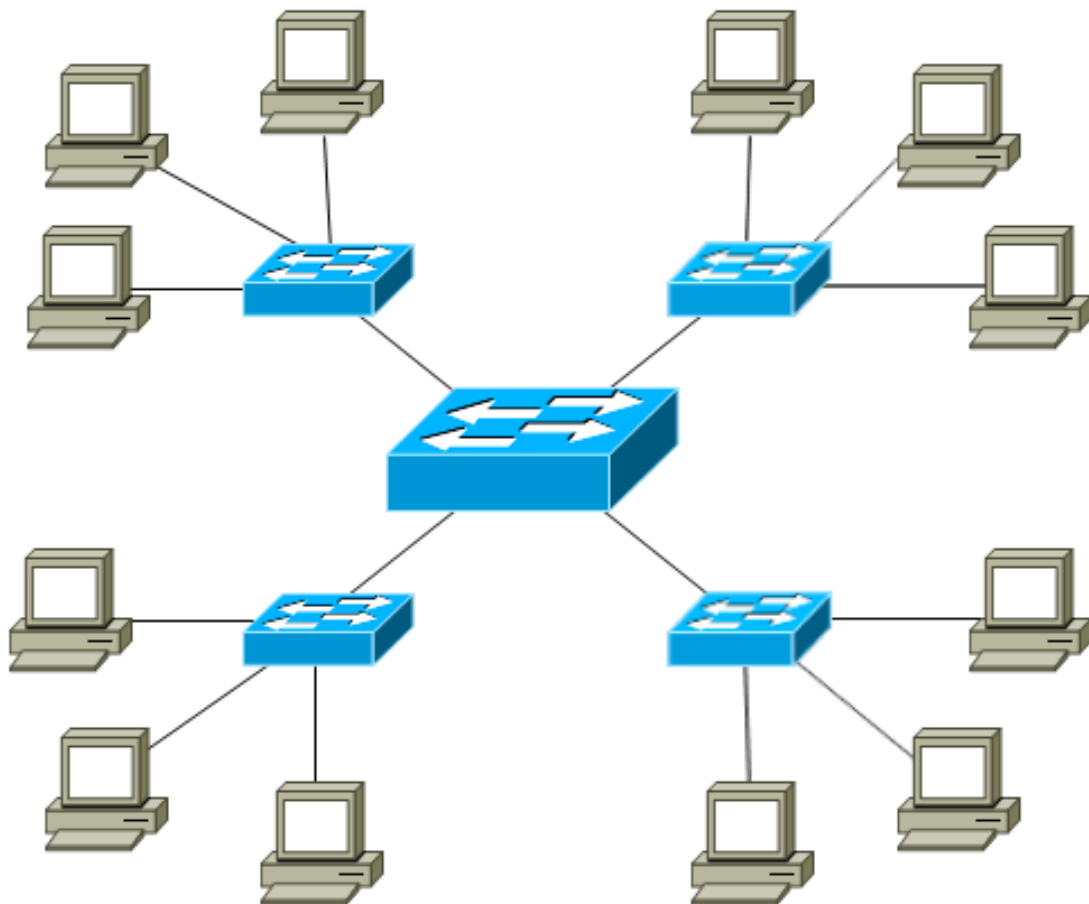
Tổng chi phí = 1.351.960.000 (VNĐ)

1.5 Kiến trúc mạng vật lý

Trong thiết kế này, chúng ta sử dụng cấu trúc liên kết hình sao mở rộng cho tòa. Trong đó có 1 switch layer 3 ở phòng kĩ thuật kết nối với các switch layer 2 ở mỗi tầng. Lựa chọn thiết kế trên bởi vì.

- Tối ưu hóa thiết bị, tiết kiệm ngân sách.
- Thiết kế trên cho phép quản lý và khắc phục sự cố mạng dễ dàng hơn, việc mở rộng mạng bằng cách thêm các thiết bị bổ sung sẽ nhanh hơn và dễ dàng hơn nhiều.
- Trong mô hình mạng sao thì một thiết bị gặp sự cố sẽ không ảnh hưởng đến các thiết bị còn lại.

Cấu trúc chung của hệ thống:



1.6 Kỹ thuật sử dụng trong Kiến trúc mạng

1.6.1 VLAN với VTP

Với mỗi bộ phận, chúng ta sẽ tạo một VLAN riêng cho bộ phận đó. Điều này đáp ứng nhu cầu chia sẻ riêng tư giữa các phòng ban và tăng hiệu suất hệ thống bằng cách giảm chi phí phát sóng, giúp dễ dàng phát hiện lỗi. Một kỹ thuật khác được sử dụng là VLAN Trunking Protocol (VTP). Công nghệ này giúp cho việc quản lý VLAN (thêm / xóa / sửa) đồng bộ và dễ dàng hơn vì chỉ cần thực hiện thay đổi trên Server Switch, mọi thay đổi sẽ được cập nhật vào Client Switch.

1.6.2 Subnet Mask

Chúng ta sẽ sử dụng kỹ thuật subnet mask cho IP riêng tư bắt đầu từ 192.168.0.0. Mỗi VLAN sẽ có dải IP khác nhau. Sử dụng công nghệ này, chúng ta sẽ có những ưu điểm sau:

- Lưu và tối ưu hóa việc phân bổ địa chỉ IP
- Tối ưu hóa lưu lượng mạng và cải thiện hiệu suất mạng.

2 Sơ đồ IP và sơ đồ đường dây

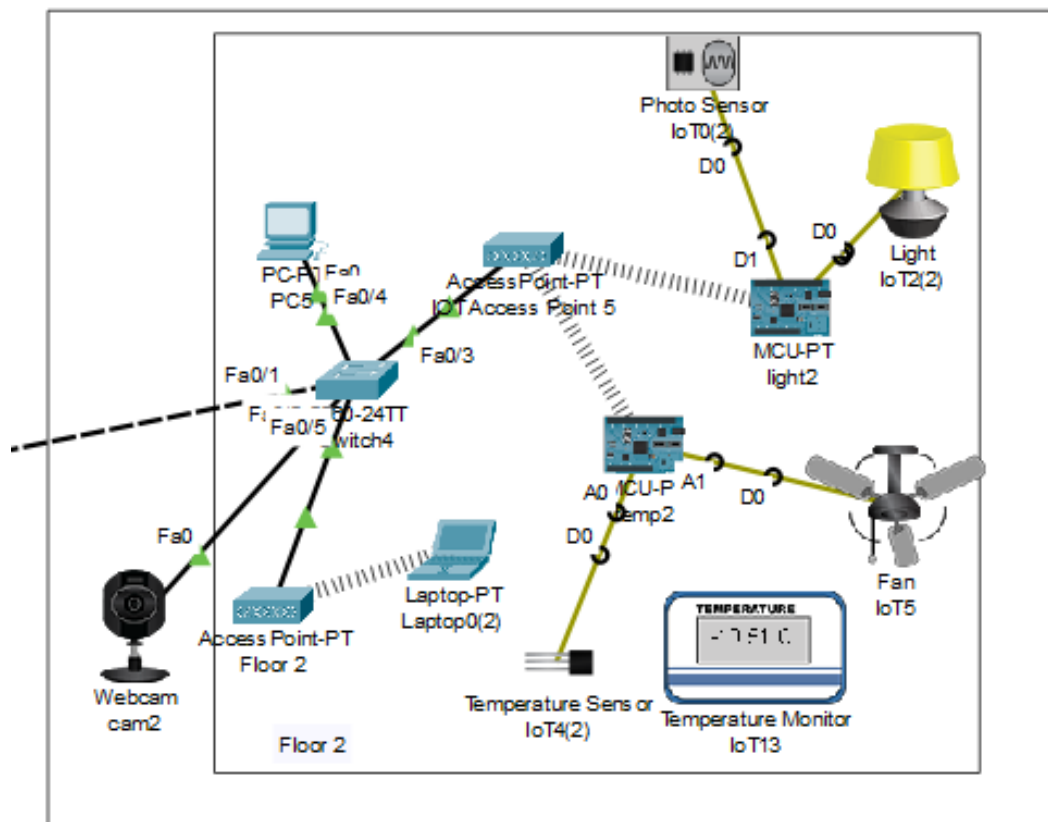
2.1 Sơ đồ IP

Vlan	Phòng ban	Mạng	Phạm vi địa chỉ IP
10	Tầng 1	192.168.10.1	192.168.10.1 -> 192.168.10.255
20	Tầng 2	192.168.20.1	192.168.20.1 -> 192.168.20.255
30	Tầng 3	192.168.30.1	192.168.30.1 -> 192.168.30.255
40	Tầng 4	192.168.40.1	192.168.40.1 -> 192.168.40.255
50	Tầng 5	192.168.50.1	192.168.50.1 -> 192.168.50.255
60	Tầng 6	192.168.60.1	192.168.60.1 -> 192.168.60.255
70	Tầng 17	192.168.70.1	192.168.70.1 -> 192.168.70.255
80	Thiết bị IoT và phòng Server	192.168.80.1	192.168.80.1 -> 192.168.80.255
90	Khách	192.168.90.1	192.168.90.1 -> 192.168.90.255

2.2 Sơ đồ đường dây bên trong

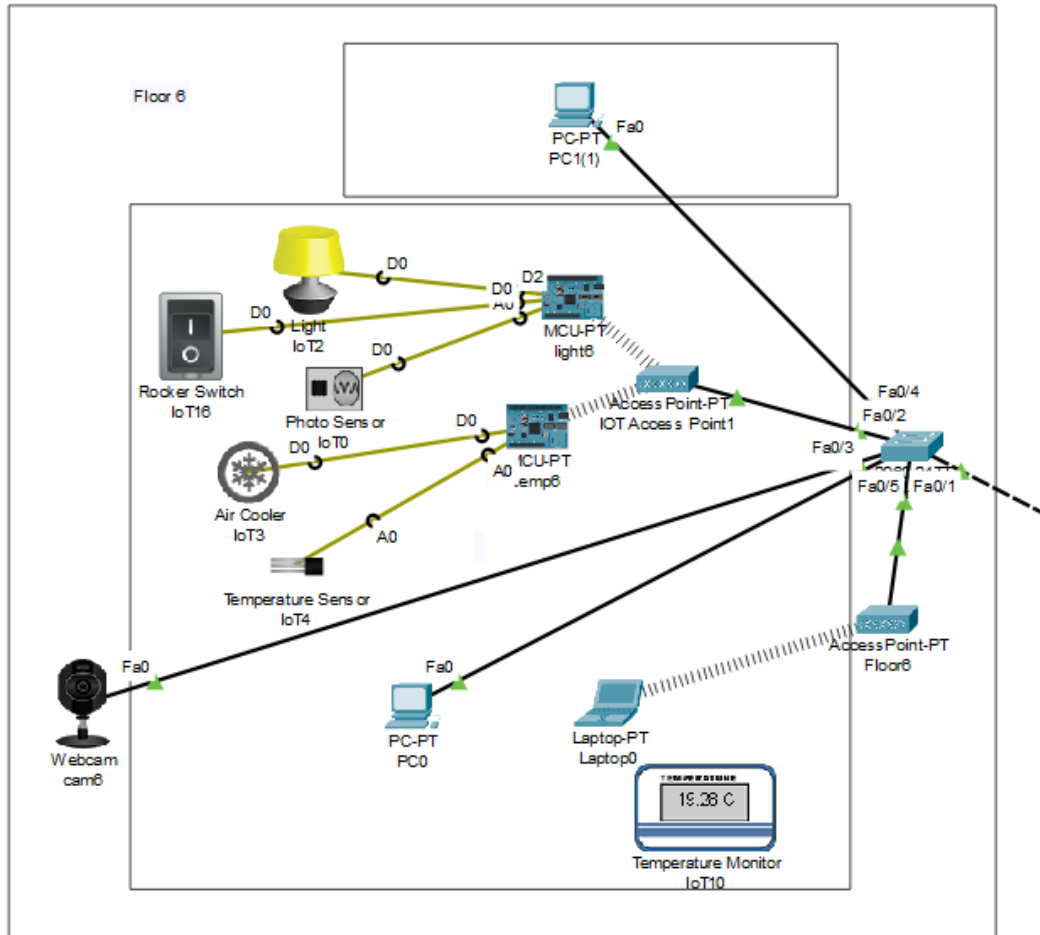
1. Tầng 2-5

- 1 switch chung của tầng kết nối với các máy tính, camera, access point và MCU



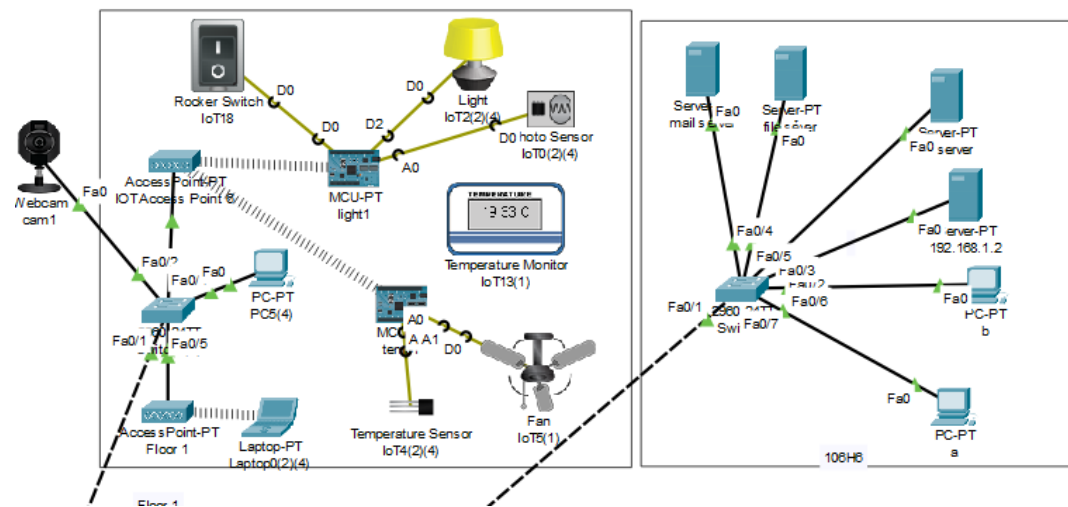
2. Tầng 6-7

- 1 switch chung của tầng kết nối với các máy tính, camera, access point và MCU, switch này được dùng chung cho cả phòng máy tính và phòng lí thuyết.



3. Phòng admin và server ở tầng 1

- 1 switch dùng để kết nối tới 10 máy chủ và các server.
- Ở phòng học thường sẽ có 1 switch khác nối tới các thiết bị, máy tính và camera

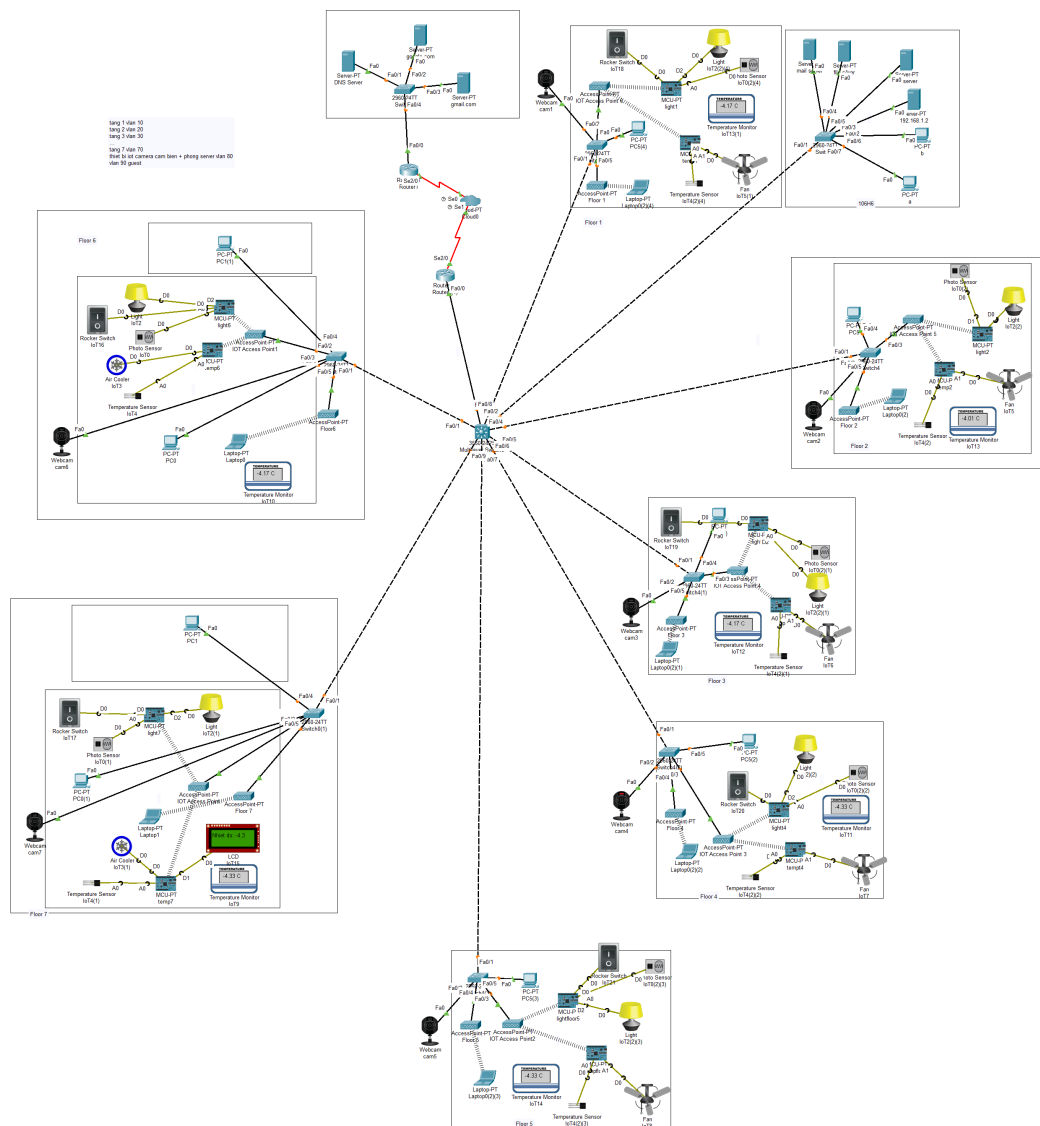


- Các Switch của từng bộ phần trên được nối với switch layer 3.

3 Kiểm thử mô hình hệ thống

- Các thiết bị trong cùng vlan có thể ping lẫn nhau ngoại trừ các thiết bị Iot và Camera không thể ping được bởi các máy tính thường.
- Các máy tính ở phòng admin có thể ping được tới các thiết bị Iot và Camera, có thể kết nối tới server để truy xuất các thiết bị hay bật tắt chúng.
- Các thiết bị có thể truy cập tới mạng bên ngoài
- Kết nối không dây hoạt động bình thường
- Các thiết bị khác vlan không thể ping lẫn nhau

4 Thiết kế mô hình bằng Packet Tracer



Hình 1: Thiết kế của mô hình bằng Packet Tracer

5 Đánh giá mô hình

5.1 Tính tin cậy và bảo mật

5.1.1 Yêu cầu về tính tin cậy

Yêu cầu về tính bảo mật dữ liệu của hệ thống

- Bảo vệ dữ liệu của người dùng không bị lộ ra ngoài một cách trái phép, kiểm soát quyền truy cập dữ liệu trong nội bộ hệ thống.
- Đảm bảo dữ liệu luôn sẵn sàng khi những người dùng hoặc ứng dụng được uỷ quyền yêu cầu.
- Việc thay đổi hệ thống mạng phải có sự cho phép của những người có uỷ quyền, các hành vi không có sự cho phép đều bị cấm

- Hệ thống có khả năng ngăn chặn và phát hiện tấn công mạng, có thông báo cho bộ phận quản lý để có thể xử lý kịp thời.
- Hệ thống phải có khả năng phục hồi sau khi bị tấn công để đảm bảo hiệu suất hoạt động không bị ảnh hưởng

5.1.2 Giải pháp đối với yêu cầu về bảo mật

- Tăng cường đầu tư vào hệ thống tường lửa để ngăn chặn truy cập bất hợp pháp và các cuộc tấn công, cung cấp cho người quản trị một giải pháp toàn diện về đảm bảo an ninh và quản lý hệ thống
- Sử dụng các phần mềm chống mã độc để phòng chống và xử lý khi hệ thống máy trạm/máy chủ bị nhiễm mã độc
- Mã hoá dữ liệu khi trao đổi giữa các thiết bị nhằm tránh bị rò rỉ thông tin
- Đảm bảo hệ thống luôn được cập nhật và có khả năng phục hồi nhanh chóng khi bị tấn công mạng.
- Xác minh nguồn gốc dữ liệu

5.2 Phần mềm sử dụng trong hệ thống

- Hệ điều hành máy trạm: Windows 10 Enterprise 21H1
- Hệ điều hành máy chủ: Ubuntu Server 20.04 LTS.
- Ứng dụng văn phòng: Microsoft 365 Business Premium.
- Phần mềm bảo mật máy chủ và máy trạm: GravityZone Business Security Premium.

5.3 Sửa chữa, bảo trì và nâng cấp hệ thống

- Với thiết kế hệ thống hình sao, khi một thiết bị gặp vấn đề sẽ không ảnh hưởng đến quá trình hoạt động của các thiết bị khác trong hệ thống.
- Các thiết bị chủ yếu mua từ Cisco nên sẽ gặp ít khó khăn hơn trong quá trình bảo hành và sửa chữa thiết bị mạng trong hệ thống.
- Các switch trong hệ thống đều sử dụng công nghệ VLAN Trunk Protocol của Cisco cho phép giảm bớt khối lượng công việc trong trường hợp cần bổ sung thêm switch khi mở rộng hệ thống, đồng thời đảm bảo tính nhất quán và đồng bộ trong hệ thống
- Với khả năng tương thích ngược tốt, các thiết bị trong hệ thống có thể dễ dàng nâng cấp lên phiên bản phần mềm cao hơn hay thay thế bằng thiết bị đời mới.

5.4 Định hướng phát triển trong tương lai

- Cần kiểm tra và bảo dưỡng các switch thường xuyên để giảm các sự cố nghiêm trọng trong hệ thống.
- Cần kiểm tra và bảo dưỡng các switch thường xuyên để giảm các sự cố nghiêm trọng trong hệ thống.
- Cần điều chỉnh hệ thống sát với thực tế thông qua chạy thử nghiệm.
- Có thể cấu hình thêm các phương pháp bảo mật khác để tăng tính bảo mật của hệ thống.