ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

MẠNG MÁY TÍNH (THÍ NGHIỆM) (CO3094)

Báo cáo Bài tập lớn

Bài tập lớn 2

NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE COMPANY

Giảng viên hướng dẫn: Lê Bảo Khánh
Nhóm: Baby Panther
Sinh viên thực hiện: Nguyễn Thanh Hiền (2111203)
Nguyễn Nhật Khải (2111506)
Phạm Văn Nhật Vũ (2110676)
Nguyễn Ngọc Phú (2114417)

THÀNH PHỐ HỒ CHÍ MINH, THÁNG 10 2023

Mục lục

1 XÁC ĐỊNH KIẾN TRÚC MẠNG **3**
1.1 Phân tích yêu cầu hệ thống mạng . . . 3
1.1.1 Yêu cầu kết nối . . . 3
1.1.2 Yêu cầu kiến trúc tòa nhà . . . 3
1.1.3 Yêu cầu về lưu lượng và tải . . . 3
1.1.4 Yêu cầu phi tính năng . . . 4
1.2 Phân tích kiến trúc tòa nhà . . . 5
1.2.1 Sơ đồ công ty . . . 5
1.2.2 Trụ sở chính . . . 6
1.2.3 Chi nhánh . . . 6
1.3 Khảo sát địa điểm lắp đặt . . . 7
1.4 Các tiêu chuẩn bảo mật mạng và phân vùng mạng . . . 8
1.4.1 Các tiêu chuẩn bảo mật . . . 8
1.4.2 Các phân vùng mạng . . . 8
1.5 Lựa chọn kiến trúc mạng . . . 9
1.5.1 Kết nối tại mỗi địa điểm . . . 9
1.5.2 Kết nối giữa chi nhánh và trụ sở . . . 10
1.5.3 Truy cập Internet . . . 10

2 ĐẶC TẢ KỸ THUẬT & TRANG THIẾT BỊ **11**
2.1 Danh sách thiết bị . . . 11
2.1.1 Router . . . 11
2.1.2 Multilevel Switch . . . 12
2.1.3 Switch . . . 13
2.1.4 Access Point . . . 14
2.2 IP Plan . . . 14
2.3 Label Plan . . . 15
2.4 Wiring Diagram . . . 16

3 XÁC ĐỊNH CẤU HÌNH HỆ THỐNG **17**
3.1 Tính toán thông lượng . . . 17
3.1.1 Tính toán chung . . . 17
3.1.2 Trụ sở chính . . . 17
3.1.3 Chi nhánh . . . 17
3.2 Dự kiến băng thông . . . 18
3.2.1 Yêu cầu chung . . . 18
3.2.2 Kết quả tính toán . . . 18
3.3 Lựa chọn thiết bị . . . 18

3.3.1 Router: 2911 18
3.3.2 Multilayer switch: 3560-24PS 19
3.3.3 Switch: 2950T-24 20
3.3.4 Access Point: AccessPoint-PT-N 20
3.3.5 ASA: 5506-X 20

4 THIẾT KẾ SƠ ĐỒ MẠNG 21
4.1 Sơ đồ kết nối luận lý 21
4.2 Sơ đồ kết nối vật lý 26

5 KIỂM THỬ HỆ THỐNG 30
5.1 Kịch bản kiểm thử 30
5.1.1 Thiết bị trong cùng VLAN 30
5.1.2 Thiết bị giữa các VLAN 30
5.1.3 Các thiết bị giữa trụ sở và chi nhánh 31
5.1.4 Các server trong DMZ 31
5.1.5 Hệ thống camera giám sát 32
5.1.6 Kết nối từ Internet 33
5.2 Kết quả kiểm thử 34
5.2.1 Kết nối giữa các thiết bị trong cùng VLAN tại mỗi trụ sở, chi nhánh công ty 34
5.2.2 Kết nối giữa các thiết bị khác VLAN tại mỗi trụ sở, chi nhánh công ty 37
5.2.3 Kết nối các thiết bị giữa trụ sở và chi nhánh 40
5.2.4 Kết nối của các server trong DMZ 43
5.2.5 Hệ thống camera giám sát 45
5.2.6 Kết nối từ Internet 46

6 ĐÁNH GIÁ HỆ THỐNG 54
6.1 Kết quả đạt được 54
6.1.1 Mức độ tin cậy và khả năng đáp ứng yêu cầu hệ thống . . . 54
6.1.2 Khả năng mở rộng, nâng cấp của hệ thống 54
6.1.3 Tính an toàn, bảo mật của hệ thống 54
6.2 Hạn chế còn tồn tại 55
6.3 Định hướng phát triển 55

7 TÀI LIỆU THAM KHẢO 56

Danh sách hình vẽ

1 Sơ đồ công ty 5
2 Mô hình sao ở mạng cục bộ 9
3 Các địa điểm kết nối với Internet 10
4 Wiring Diagram 16
5 Router 2911 18
6 Các module mạng sử dụng 19
7 Multilayer switch 3560-24PS 19
8 Switch 2950T-24 20
9 AccessPoint-PT-N 20
10 ASA 5506-X 20
11 Toàn bộ hệ thống mạng 21
12 Trụ sở chính 22
13 Tầng 1 - Trụ sở chính 23
14 Tầng 2-7 - Trụ sở chính 23
15 Các chi nhánh 24
16 Tầng 1 - Chi nhánh 25
17 Tầng 2 - Chi nhánh 25
18 Toàn bộ hệ thống mạng 26
19 Trụ sở chính 27
20 Chi nhánh 27
21 Tầng 1 - Trụ sở chính 28
22 Tầng 1 - Chi nhánh 28
23 Tầng 2-7 - Trụ sở chính 29
24 Tầng 2 - Chi nhánh 29
25 Trụ sở chính: 2 PC bất kỳ tầng 2 có thể ping lẫn nhau 34
26 Chi nhánh: 2 PC bất kỳ tầng 1 có thể ping lẫn nhau 34
27 Trụ sở chính: Laptop tầng 2 có thể ping webcam IoT2 35
28 Chi nhánh: Laptop tầng 1 có thể ping webcam IoT10 35
29 Trụ sở chính : Laptop tầng 1 có thể ping Laptop tầng 2 35
30 Chi nhánh : Laptop tầng 1 có thể ping Smartphone tầng 2 36
31 Trụ sở chính : Smartphone tầng 3 có thể ping Webcam tầng 4 . . . 36
32 Chi nhánh : Smartphone tầng 2 có thể ping Webcam tầng 1 36
33 Trụ sở chính: PC tầng 2 có thể ping PC tầng 3 37
34 Chi nhánh : PC tầng 1 có thể ping PC tầng 2 37
35 Trụ sở chính: PC tầng 7 có thể ping Smartphone tầng 7 37
36 Chi nhánh : PC tầng 1 có thể ping Laptop tầng 1 38
37 Trụ sở chính: PC tầng 5 có thể ping Webcam tầng 5 38
38 Chi nhánh : PC tầng 2 có thể ping Webcam tầng 2 38

39 Trụ sở chính: PC tầng 2 có thể truy cập Web Server trong vùng DMZ 39
40 Chi nhánh : PC tầng 2 có thể truy cập Web Server trong vùng DMZ ở trụ sở chính 39
41 Trụ sở chính: PC tầng 2 có thể truy cập Camera Server trong vùng Private Server ở tầng 1 39
42 Chi nhánh : PC tầng 1 có thể truy cập Camera Server trong vùng Private Server ở tầng 1 40
43 PC tầng 2 trụ sở chính có thể ping PC tầng 2 chi nhánh (cùng VLAN 40) 40
44 PC tầng 1 chi nhánh (VLAN 30) có thể ping PC tầng 5 trụ sở (VLAN 70) 41
45 Smartphone tầng 2 chi nhánh (VLAN 20) có thể ping PC tầng 7 trụ sở (VLAN 90) 41
46 Smartphone tầng 4 trụ sở (VLAN 60) có thể ping Smartphone tầng 2 chi nhánh (VLAN 20) 41
47 PC tầng 3 trụ sở (VLAN 50) có thể ping Webcam tầng 1 chi nhánh (VLAN 20) 42
48 Laptop tầng 1 chi nhánh (VLAN 20) có thể ping Webcam tầng 2 trụ sở (VLAN 20) 42
49 PC tầng 2 chi nhánh (VLAN 40) có thể truy cập Web Server trong vùng Private Server của trụ sở (VLAN 10) 43
50 2 server trong vùng DMZ có thể ping lẫn nhau 43
51 PC nội bộ bất kỳ của trụ sở có thể truy cập vào Web Server vùng DMZ 44
52 PC nội bộ bất kỳ của chi nhánh có thể truy cập vào Web Server vùng DMZ 44
53 Các thiết bị kết nối không dây tới access point của trụ sở có thể truy cập vào Web Server vùng DMZ 44
54 Các thiết bị của khách hàng khác có thể truy cập vào Web Server vùng DMZ 45
55 PC tại tầng 3 của trụ sở có thể truy cập vào địa chỉ của Camera Server tại trụ sở (192.168.10.2) và đăng nhập với tài khoản ***admin*** để quan sát camera tại các tầng 45
56 Smartphone tại tầng 2 của chi nhánh Hà Nội có thể truy cập vào địa chỉ của Camera Server tại chi nhánh (192.166.10.2) và đăng nhập với tài khoản ***admin*** để quan sát camera tại các tầng 46
57 Thiết bị điện tử của khách hàng (kết nối với access point tại trụ sở) không thể kết nối tới PC nội bộ bất kỳ của trụ sở 46
58 Thiết bị điện tử của khách hàng khác cũng không thể kết nối tới PC nội bộ bất kỳ của trụ sở 47

59 Thiết bị điện tử của khách hàng (kết nối với access point tại chi nhánh Đà Nẵng) không thể kết nối tới PC nội bộ bất kỳ của chi nhánh này . . . 47
60 Thiết bị điện tử của khách hàng khác cũng không thể kết nối tới PC nội bộ bất kỳ của chi nhánh Đà Nẵng . . . 48
61 Thiết bị điện tử của khách hàng (kết nối với access point tại trụ sở) không thể truy cập vào web server nội bộ của trụ sở (địa chỉ 192.168.10.6) . . . 48
62 Thiết bị điện tử của khách hàng khác cũng không thể truy cập vào web server nội bộ của trụ sở . . . 49
63 Thông tin đăng nhập VPN của nhân viên làm việc từ xa . . . 49
64 Nhân viên làm việc từ xa có thể ping tới PC bất kỳ tại trụ sở sau khi đã đăng nhập VPN . . . 50
65 Nhân viên làm việc từ xa có thể ping tới PC bất kỳ tại chi nhánh sau khi đã đăng nhập VPN . . . 50
66 Thông tin đăng nhập VPN của một nhân viên tại chi nhánh Hà Nội 51
67 Nhân viên tại chi nhánh Hà Nội có thể ping tới PC bất kỳ tại chi nhánh Đà Nẵng thông qua VPN . . . 51
68 Gói tin ICMP gửi từ chi nhánh Hà Nội tới chi nhánh Đà Nẵng . . . 52
69 Các thiết bị bất kỳ trong nội bộ công ty có thể truy cập một trang Web trên Internet . . . 52
70 Cơ chế cân bằng tải được áp dụng, các gói tin gửi từ thiết bị bất kỳ trong nội bộ công ty ra Internet sẽ được truyền luân phiên qua 2 Interface 20.0.1.1 và 20.0.2.1 của ISP . . . 53

Danh sách bảng

1 Yêu cầu kiến trúc tòa nhà . . . 3
2 Danh sách thiết bị mạng tại trụ sở chính (mỗi tầng) . . . 6
3 Danh sách thiết bị mạng tại chi nhánh . . . 6
4 Checklist khảo sát địa điểm . . . 7
5 Danh sách thiết bị: Module . . . 11
6 Danh sách thiết bị: Router . . . 12
7 Danh sách thiết bị: Multilevel Switch . . . 13
8 Danh sách thiết bị: Switch . . . 13
9 Danh sách thiết bị: Access Point . . . 14
10 IP Plan: Trụ sở chính . . . 14
11 IP Plan: Chi nhánh Đà Nẵng . . . 15
12 IP Plan: Chi nhánh Hà Nội . . . 15
13 Kịch bản kiểm thử: Thiết bị trong cùng VLAN . . . 30

14 Kịch bản kiểm thử: Thiết bị giữa các VLAN 30
15 Kịch bản kiểm thử: Các thiết bị giữa trụ sở và chi nhánh 31
16 Kịch bản kiểm thử: Các server trong DMZ 31
17 Kịch bản kiểm thử: Hệ thống camera giám sát 32
18 Kịch bản kiểm thử: Kết nối từ Internet 33

TỔNG QUAN

Phần 1 tập trung vào việc phân tích hệ thống mạng theo yêu cầu của đề bài và phân tích kiến trúc của công ty dựa trên mô hình nhóm tự đề xuất. Cùng với đó, nhóm thực hiện khảo sát vị trí lắp đặt các thiết bị mạng, thiết bị sử dụng mạng trong công ty. Mục tiêu cuối cùng của phần 1 là dựa vào những phân tích trên nhằm lựa chọn kiến trúc mạng phù hợp cho công ty.

Dựa trên kiến trúc mạng đã lựa chọn, phần 2 tiến hành thống kê các thiết bị tối thiểu có thể đáp ứng yêu cầu của hệ thống mạng; đưa ra sơ đồ địa chỉ IP và sơ đồ nối dây tổng quát giữa các thiết bị. Đồng thời, nhóm đánh giá và lựa chọn mô hình mạng diện rộng WAN phù hợp. Kết quả của phần 2 là mô hình mạng ở mức trừu tượng cao.

Phần 3 thực hiện tính toán thông lượng trên phạm vi toàn bộ hệ thống mạng và ước tính băng thông tối đa của hệ thống. Từ kết quả đó, lựa chọn thiết bị mạng đáp ứng được yêu cầu với chi phí tối ưu. Kết thúc phần 3, mô hình mạng hoàn chỉnh của toàn bộ công ty sẽ được hoàn chỉnh một cách chi tiết.

Phần 4 tiến hành mô phỏng hệ thống mạng trên phần mềm Packet Tracer (Cisco). Thực hiện các bước cấu hình trên router, switch, định tuyến tại các router, thiết lập bảo mật bằng tường lửa.

Phần 5 thực hiện kiểm thử dựa trên kịch bản đã được soạn sẵn, bao gồm kiểm tra kết nối giữa các thiết bị trong cùng VLAN hoặc khác VLAN, các thiết bị giữa trụ sở và chi nhánh, các thiết bị trong hệ thống mạng nội bộ của công ty với các thiết bị ngoài Internet.

Dựa vào kết quả kiểm thử, phần 6 thực hiện việc đánh giá hệ thống mạng đã thiết kế dựa trên các tiêu chí về độ tin cậy, tính dễ dàng nâng cấp và mở rộng, độ an toàn và bảo mật. Đồng thời, nêu ra những hạn chế còn vướng mắc trong dự án và các định hướng cải thiện, bảo trì hệ thống trong tương lai.

1 XÁC ĐỊNH KIẾN TRÚC MẠNG

1.1 Phân tích yêu cầu hệ thống mạng

1.1.1 Yêu cầu kết nối

- **Phương tiện kết nối:** không dây và có dây, cáp quang (GPON), và Gigabit Ethernet 1GbE/10GbE.
- **Kết nối tại mỗi địa điểm:** Hệ thống mạng được cấu trúc theo VLAN của mỗi phòng ban khác nhau.
- **Kết nối giữa các địa điểm:** Trụ sở chính kết nối tới hai chi nhánh thông qua hai đường WAN thuê riêng (có thể sử dụng SD-WAN, MPLS), và 2 xDSL với cơ chế cân bằng tải để truy cập Internet. Đặc biệt, toàn bộ hệ thống (bao gồm cả chi nhánh) muốn kết nối với Internet đều phải thông qua trụ sở chính.
- **Cấu hình VPN:** Hệ thống mạng được hỗ trợ cấu hình VPN giữa các trụ sở/chi nhánh (site-to-site) và cho nhân viên làm việc từ xa kết nối với mạng LAN của công ty (remote acccess).

1.1.2 Yêu cầu kiến trúc tòa nhà

Nội dung	**Trụ sở**	**Chi nhánh**
Tầng	7 tầng	2 tầng
Phòng kỹ thuật	Tầng 1, với Cable Central Location	Tầng 1, với Cable Central Location
Thiết bị mạng	Tối thiểu 12 thiết bị	Tối thiểu 5 thiết bị
Workstation	Khoảng 120 thiết bị	Khoảng 30 thiết bị
Máy chủ	5 máy chủ	3 máy chủ
Camera giám sát	Có	Có
Kết nối không dây	Có	Có

Bảng 1: Yêu cầu kiến trúc tòa nhà

1.1.3 Yêu cầu về lưu lượng và tải

Thời gian hoạt động: Hoạt động 80% trong các khung giờ cao điểm (9h00 - 11h00 và 15h00 - 16h00) được chia cho trụ sở và chi nhánh. Cụ thể:

- **Server:** để cập nhật phần mềm, truy cập trang, cơ sở dữ liệu,... với tốc độ: khoảng 100 MB/ngày (tải xuống) và khoảng 2000 MB/ngày (tải lên)

- **Mỗi workstation:** để truy cập trang web, tài tài liệu, giao dịch khách hàng,... với tốc độ: khoảng 500 MB/ngày (tải xuống) và khoảng 100 MB/ngày (tải lên)
- **Thiết bị kết nối WiFi:** của người dùng để truy xuất với tốc độ 500 MB/ngày

1.1.4 Yêu cầu phi tính năng

- **Tính nâng cấp:** Dễ dàng nâng cấp hệ thống, tích hợp công nghệ mới.
- **Tính tin cậy:** Có tính sẵn sàng cao, xử lý khi có vấn đề phát sinh.
- **Tính bảo mật:** Có tính bảo mật cao (có thể sử dụng Firewall, IPS, IDS, phising detection).
- **Tính tương thích:** Tương thích với các ứng dụng được công ty sử dụng: phần mềm được cấp phép và phần mềm mã nguồn mở, ứng dụng văn phòng, ứng dụng client-server, đa phương tiện và cơ sở dữ liệu.
- **Tính mở rộng:** Các chi nhánh BB Bank dự tính tăng trưởng 20% trong 5 năm (về số lượng người dùng, tải kết nối, mở rộng chi nhánh,...)

1.2 Phân tích kiến trúc tòa nhà

1.2.1 Sơ đồ công ty

Sử dụng sơ đồ sau làm sơ đồ chung cho các tầng của toàn bộ công ty.

Hình 1: Sơ đồ công ty

Sơ đồ của mỗi tầng làm việc được quy định như sau:

- Phòng số 1 được chọn là phòng kỹ thuật mạng (đối với tầng 1), với các thiết bị mạng quan trọng, toàn bộ server. Đường dây mạng chính, xuyên giữa các tầng cũng được bố trí tại đây. Tại các tầng khác, phòng này được thay đổi tùy mục đích sử dụng của các phòng ban.
- Phòng số 2 được chọn là phòng quản lý, giám sát bằng camera (đối với tầng 1). Tại các tầng khác, phòng này trở thành phòng họp không được trang bị máy làm việc cố định (PC).
- Khu vực 3 là khu vực làm việc chung. Nhân viên làm việc tại khu vực này được trang bị máy làm việc cố định (PC).
- Khu vực 4 là khu vực làm việc cá nhân. Nhân viên làm việc tại khu vực này được trang bị máy làm việc cố định (PC).
- Khu vực 5 được sử dụng vào mục đích khác.

1.2.2 Trụ sở chính

Mục đích và cách bố trí thiết bị sử dụng mạng *(số lượng thiết bị kết nối được tính trên mỗi tầng)*:

- Tầng 1 được bố trí: 1 phòng kỹ thuật của với những thiết bị mạng quan trọng, toàn bộ server được lắp đặt tại phòng kỹ thuật này; 1 phòng quản lý dữ liệu từ các camera trong tòa nhà và là địa điểm tiếp đón khách đến tham quan (cho phép thiết bị của khách kết nối với Internet).
- Các tầng còn lại là khu vực làm việc của các phòng ban khác. Mỗi tầng đều có một số workstation, số PC không vượt quá số lượng tối đa được thể hiện ở Bảng 2.
- Mỗi tầng đều lắp đặt 2 camera giám sát không dây được lắp đặt tại khu làm việc chung, truyền dữ liệu tới phòng giám sát tập trung dưới tầng 1.

Tầng	Server	Workstation	Thiết bị không dây
1	5	20	*
2-7	0	20	*

Bảng 2: Danh sách thiết bị mạng tại trụ sở chính (mỗi tầng)

1.2.3 Chi nhánh

Mục đích và cách bố trí thiết bị sử dụng mạng *(số lượng thiết bị kết nối được tính trên mỗi tầng)*:

- Tầng 1 được bố trí: 1 phòng kỹ thuật của với những thiết bị mạng quan trọng, toàn bộ server được lắp đặt tại phòng kỹ thuật này; 1 phòng quản lý dữ liệu từ các camera trong tòa nhà.
- Vì quy mô của chi nhánh tương đối nhỏ, cả hai tầng đều là khu vực làm việc của các phòng ban trong công ty.
- Tương tự trụ sở chính, mỗi tầng đều có một số workstation, số PC không vượt quá số lượng tối đa được thể hiện ở Bảng 3.
- Mỗi tầng đều được lắp đặt 2 camera giám sát, bố trí tương tự trụ sở chính.

Tầng	Server	Workstation	Thiết bị không dây
1	3	20	*
2	0	20	*

Bảng 3: Danh sách thiết bị mạng tại chi nhánh

1.3 Khảo sát địa điểm lắp đặt

Để tiến hành thiết kế, lắp đặt hệ thống mạng cho ngân hàng, phía công ty cần dữ liệu khảo sát từ cơ sở hạ tầng, kiến trúc sẵn có tại địa điểm lắp đặt. Danh sách được xây dựng tham khảo từ: Cisco [1] [2]

Giả sử, hệ thống đang được thiết kế, lắp đặt cho cơ sở mới, công ty sẽ thực hiện dạng khảo sát dự đoán (**Predictive Survey**) tại trụ sở và từng chi nhánh.

Check	Nội dung	Chi tiết thông số
❑	Đánh giá tổng quan	- Đánh giá kiến trúc tòa nhà, cơ sở hạ tầng mạng sẵn có - Dự đoán các vùng gây khó khăn: lắp đặt, kết nối - Lựa chọn mô hình khảo sát phù hợp: Data, Voice, Location
❑	Đặc điểm triển khai	- Mức độ dày đặc, phủ sóng kết nối các thiết bị - Tính di động trang thiết bị kết nối - Đặc điểm khí hậu, môi trường lắp đặt - Khoảng cách giữa các chi nhánh với trụ sở - Vị trí cần giám sát đặc biệt, góc quay và lắp đặt cho camera
❑	Công cụ khảo sát	- Xây dựng bản đồ khảo sát: tòa nhà, các phòng, lối di chuyển - Công cụ: phân tích tầm phủ sóng, đo đạc diện tích, khoảng cách - Vị trí các thiết bị kiểm thử
❑	Số lượng thiết bị	- Số lượng, vị trí các phòng ban, thiết bị kết nối - Số lượng các nhân viên làm việc từ xa - Mục đích sử dụng, lưu lượng các server hệ thống
❑	Yêu cầu vật lý	- Điện năng tiêu thụ - Vị trí các đường dẫn kết nối điện, mạng - Cân nhắc loại giá đỡ, dây buộc, đường nối dây

Bảng 4: Checklist khảo sát địa điểm

[1] Cisco (2022). *"Understand Site Survey Guidelines for WLAN Deployment"*. Truy cập từ: https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html (ngày 11/11/2023)

[2] Cisco. *"Performing a Site Survey"*. Truy cập từ: https://www.cisco.com/c/en/us/td/docs/wireless/wlan_adapter/350_cb20a/user/win_ce/2-3/configuration/guide/hig/CE_appE.pdf (ngày 11/11/2023)

1.4 Các tiêu chuẩn bảo mật mạng và phân vùng mạng

1.4.1 Các tiêu chuẩn bảo mật

- **Firewall**: sử dụng các **access list** để kiểm soát quyền truy cập hệ thống mạng cục bộ của nhân viên trong công ty.
- **Camera server**: chỉ có nhân viên truy cập được (phải có password).
- **VPN**: Mã hóa thông tin người gửi/nhận và nội dung gói tin trong lúc truyền dữ liệu.

1.4.2 Các phân vùng mạng

Cấu trúc mạng dự kiến xây dựng sẽ bao gồm các phần chính sau:

- **Vùng mạng Internet**: Phần này được trang bị các thiết bị kết nối Gateway Cisco Router riêng kết nối với mạng Internet, cho phép mở rộng và nâng cấp tốc độ cổng kết nối Internet tuỳ theo nhu cầu phát triển. Người dùng truy cập vào mạng được xác thực tuỳ theo quyền truy cập để vào mạng nội bộ hoặc Internet và CSDL dùng để xác thực được quản lý tập trung trên máy chủ đặt ở vùng quản trị hệ thống.
- **Vùng mạng DMZ**: Gồm hệ thống máy chủ Web, E-mail công cộng. DMZ network giúp bảo vệ các máy chủ trong mạng nội bộ. Nếu các máy chủ công cộng bị tấn công, tin tặc vẫn không thể dựa vào chúng để tấn công các máy chủ đặt bên trong có chứa thông tin quan trọng.
- **Vùng mạng nội bộ**: Bao gồm các workstations và server đặt trên các tầng của tòa nhà, phục vụ cho các nhân viên làm việc, duyệt web, gửi mail,...

Ngoài ra cách phân chia vùng như trên, ta có thể kết hợp thêm những cách sau:

- **Vùng Wireless LAN**: Hỗ trợ kết nối internet không dây cho nhân viên.
- **Vùng kết nối với các chi nhánh khác của công ty**: Trụ sở công ty kết nối với hai chi nhánh của nó thông qua hai đường WAN thuê riêng.

1.5 Lựa chọn kiến trúc mạng

1.5.1 Kết nối tại mỗi địa điểm

Mỗi địa điểm sẽ được cấu trúc theo mô hình **Extended Star Topology** với nơi tập trung kết nối sẽ là Router tại địa điểm đó, còn lại các node sẽ mang đặc điểm của **Star Topology**. Cụ thể, mỗi node trong hệ thống mạng tại mỗi địa điểm sẽ bao gồm:

Mạng cục bộ nội bộ công ty

Multilayer Switch Layer 3 liên kết tới các node khác là Switch Layer 2 của tầng. Mỗi tầng sẽ có các workstation kết nối với VLAN tương ứng với phòng ban tại tầng đó, đồng thời, cho phép các thiết bị không dây của nhân viên và camera giám sát kết nối với mạng LAN chung của công ty. Ngoài ra, các server private cũng sẽ được kết nối riêng để phục vụ cho các tác vụ nội bộ của địa điểm.

Trước Multilayer switch sẽ được thiết lập tường lửa để gia tăng cơ chế bảo vệ cho mạng nội bộ công ty.

Hình 2: Mô hình sao ở mạng cục bộ

Mạng không dây cho khách

Tầng 1 là được ấn định cho phòng chăm sóc khách hàng, các phòng hội nghị để tiếp đón quan khách. Vì vậy, hệ thống cung cấp một access point tại đây để các thiết bị không dây của khách có thể truy cập và sử dụng Internet.

Demilitarized zone (DMZ)

Node này chỉ áp dụng tại trụ sở, được ấn định là nơi tập trung các server public cho phép người dùng bên ngoài công ty có thể truy cập với 2 server là: Web server và Email server.

1.5.2 Kết nối giữa chi nhánh và trụ sở

Với 2 đường truyền chuyên biệt (leased line) được cung cấp, hệ thống sẽ sử dụng **Star topology** với Router của trụ sở là trung tâm:

1. Đường thứ nhất: Từ trụ sở ở Hồ Chí Minh đến chi nhánh Hà Nội.
2. Đường thứ hai: Từ trụ sở ở Hồ Chí Minh đến chi nhánh ở Đà Nẵng.

1.5.3 Truy cập Internet

Sau khi đã kết nối các chi nhánh tập trung tại trụ sở, ta có thể thực hiện kết nối từ router của trụ sở tới 2 modem DSL để truy cập Internet. Tất cả dữ liệu đều phải đi qua subnet của trụ sở tại Hồ Chí Minh trước khi đến được Internet và ngược lại. Vì vậy, router của trụ sở là thiết bị mạng cần phải chịu nhiều tải nhất, cơ chế cân bằng tải được áp dụng ở đây để phân bổ các gói tin truyền nhận với Internet qua 2 modem DSL một cách hợp lý.

Hình 3: Các địa điểm kết nối với Internet

2 ĐẶC TẢ KỸ THUẬT & TRANG THIẾT BỊ

2.1 Danh sách thiết bị

2.1.1 Router

Yêu cầu tối thiểu của router bao gồm:

- Khả dụng đối với phần mềm Cisco Packet Tracer phiên bản 8.2.1.
- Hỗ trợ ít nhất 1 cổng kết nối WAN (2 cổng đối với router ở trụ sở chính) với tốc độ tối thiểu 1Gbps, kết nối thông qua cáp quang trên đường dây riêng (Fiber WAN Port).
- Ngoài ra, router ở trụ sở chính còn phải đảm bảo hỗ trợ ít nhất 2 cổng Gigabit Ethernet với tốc độ tối thiểu 1Gbps, sử dụng cho kết nối với Internet.

Ghi chú:

- Trong Bảng 6, cột "Loại module" chỉ tập trung đề cập đến các module giúp mở rộng số cổng Gigabit Etherner, Fast Ethernet và cổng Fiber WAN.
- Trên thực tế, một số router có thể hỗ trợ nhiều module hơn, một số module cũng có thể hỗ trợ nhiều kết nối hơn, Bảng 6 và Bảng 5 chỉ thu thập dữ liệu từ phần mềm mô phỏng.

Module	Số cổng Gigabit Ethernet	Số cổng Fast Ethernet	Số cổng Fiber WAN
HWIC-1GE-SFP	0	0	1
HWIC-4ESW	0	4	0
NIM-ES2-4	4	0	0
NM-1FE2W	0	1	2
NM-2FE2W	0	2	2
NM-2W	0	0	2
NM-ESW-161	0	16	0

Bảng 5: Danh sách thiết bị: Module

Router	Số cổng Gigabit Ethernet	Số cổng Fast Ethernet	Số cổng Fiber WAN	Số module mạng	Loại module
ISR4331	3	0	2	2	NIM-ES2-4
ISR4321	2	0	1	2	NIM-ES2-4
1941	2	0	0	2	HWIC-1GE-SFP, HWIC-4ESW
2901	2	0	0	4	HWIC-1GE-SFP, HWIC-4ESW
2911	3	0	0	4	HWIC-1GE-SFP, HWIC-4ESW
819IOX	1	4	0	0	
819HGW	1	4	0	0	
829	6	0	0	0	
CGR1240	3	4	0	0	
1841	0	2	0	2	HWIC-1GE-SFP, HWIC-4ESW
2620XM	0	1	0	3	NM-1FE2W, NM-2FE2W, NM-2W
2621XM	0	2	0	3	NM-1FE2W, NM-2FE2W, NM-2W
2811	0	2	0	5	HWIC-1GE-SFP, HWIC-4ESW, NM-1FE2W, NM-2FE2W, NM-2W, NM-ESW-161

Bảng 6: Danh sách thiết bị: Router

Từ kết quả Bảng 6 và Bảng 5, các router thỏa mãn điều kiện của trụ sở chính gồm ISR4331, 1941, 2901 và 2911; các router thỏa mãn điều kiện của chi nhánh bao gồm ISR4331, ISR4321, 1941, 2901, 2911, 1841 và 2811.

2.1.2 Multilevel Switch

Yêu cầu tối thiểu của multilevel switch bao gồm:

- Khả dụng đối với phần mềm Cisco Packet Tracer phiên bản 8.2.1.

- Hỗ trợ tối thiểu 14 cổng Ethernet đối với trụ sở chính và 4 cổng Ethernet đối với chi nhánh, tương đương với 2 cổng / tầng nhằm kết nối Switch và Access Point của từng tầng.
- Có khả năng hỗ trợ cấu hình và VLAN.

Multilevel Switch	Số cổng FastEthernet	Số cổng Gigabit Ethernet	Hỗ trợ cấu hình VLAN
3560-24PS	24	2	✓
3650-24PS	0	28	✓

Bảng 7: Danh sách thiết bị: Multilevel Switch

Từ kết quả Bảng 7, các multilevel switch thỏa mãn điều kiện bao gồm 3560-24PS và 3650-24PS.

2.1.3 Switch

Yêu cầu tối thiểu của switch bao gồm:

- Khả dụng đối với phần mềm Cisco Packet Tracer phiên bản 8.2.1.
- Hỗ trợ tối thiểu 20 cổng Ethernet, tương ứng với số lượng thiết bị của các tầng [2] [3].
- Có khả năng hỗ trợ cấu hình và VLAN.

Switch	Số cổng FastEthernet	Số cổng Gigabit Ethernet	Hỗ trợ cấu hình VLAN
2960	24	2	✓
2950-24	24	0	✓
2950T-24	24	2	✓
IE-2000	8	2	✓

Bảng 8: Danh sách thiết bị: Switch

Từ kết quả Bảng 8, các switch thỏa mãn điều kiện bao gồm 2960, 2950-24 và 2950T-24.

2.1.4 Access Point

Yêu cầu tối thiểu của access point bao gồm:

- Khả dụng đối với phần mềm Cisco Packet Tracer phiên bản 8.2.1.
- Tương thích với các thiết bị sử dụng mạng trong hệ thống, phải bao gồm 2.4GHz và 5GHz.

Access Point	Hỗ trợ FastEthernet	2.4GHz	5.0GHz
AP-PT	✓	✓	✗
AP-PT-A	✓	✗	✓
AP-PT-AC	✓	✗	✓
AP-PT-N	✓	✓	✓

Bảng 9: Danh sách thiết bị: Access Point

Từ kết quả Bảng 9, access point thỏa mãn điều kiện là AP-PT-N.

2.2 IP Plan

VLAN	Mục đích sử dụng	Subnet	Tầng	WS
2	Guest Wireless	193.168.0.0/24	1	Không
3	Teleworker	194.168.0.0/24	Không	Không
4	Public Server	195.168.0.0/24	1	Không
10	Phòng IT & Private server	192.168.10.0/24	1	Không
20	Wireless LAN	192.168.20.0/24	1-7	Không
30	Lễ tân	192.168.30.0/24	1	10
40	Phòng Tài chính - Kế toán	192.168.40.0/24	2	20
50	Phòng Kinh doanh Đầu tư	192.168.50.0/24	3	20
60	Phòng Marketing Sales	192.168.60.0/24	4	20
70	Phòng Nghiên cứu Phát triển	192.168.70.0/24	5	20
80	Phòng Thi công - Vận hành	192.168.80.0/24	6	20
90	Phòng Nhân sự	192.168.90.0/24	7	20

Bảng 10: IP Plan: Trụ sở chính

VLAN	Mục đích sử dụng	Subnet	Tầng	WS
2	Guest Wireless	193.167.0.0/24	1	Không
10	Phòng kỹ thuật - Server	192.167.10.0/24	1	10
20	Wireless LAN	192.167.20.0/24	1-2	Không
30	Chăm sóc khách hàng	192.167.30.0/24	1	10
40	Phòng Tài chính - Kế toán	192.167.40.0/24	2	20

Bảng 11: IP Plan: Chi nhánh Đà Nẵng

VLAN	Mục đích sử dụng	Subnet	Tầng	WS
2	Guest Wireless	193.166.0.0/24	1	Không
10	Phòng kỹ thuật - Server	192.166.10.0/24	1	10
20	Wireless LAN	192.166.20.0/24	1-2	Không
30	Chăm sóc khách hàng	192.166.30.0/24	1	10
40	Phòng Tài chính - Kế toán	192.166.40.0/24	2	20

Bảng 12: IP Plan: Chi nhánh Hà Nội

2.3 Label Plan

Cú pháp đặt tên của các thiết bị: Router, Multilayer Switch, Switch, Access Point sẽ được chuẩn hóa thành:

[Địa điểm[3]]_[Loại thiết bị[4]][STT thiết bị[5]]_Flr[STT tầng]

Ví dụ: tên của một switch trong tại tầng 6 của trụ sở chính sẽ là: *SG_Switch0_Flr6*

Cú pháp đặt tên của các Server sẽ được chuẩn hóa thành:

[Địa điểm]_[Quyền truy cập[6]]_[Mục đích sử dụng[7]]Server[STT[8]]

Ví dụ: tên của một Camera Server (trong vùng private) tại chi nhánh Hà Nội sẽ là: *HN_Pri_CameraServer0*

[3]Địa điểm: Trụ sở chính (`SG`), Chi nhánh Đà Nẵng (`DN`), Chi nhánh Hà Nội (`HN`), bên ngoài công ty (`Ext`)

[4]Loại thiết bị: Switch (`Switch`), Multilayer Switch (`MulSwitch`), Access point (`AcsPoint`), Router (`Router`), ASA (`ASA`)

[5]STT thiết bị: Đánh số lại đối với mỗi địa điểm

[6]Quyền truy cập: Private (`Pri`), Public (`Pub`)

[7]Mục đích sử dụng: `Web/Email/Data/Video/Camera`

[8]STT: Đánh số lại đối với mỗi địa điểm và mỗi chức năng sử dụng

2.4 Wiring Diagram

Hình 4: Wiring Diagram

3 XÁC ĐỊNH CẤU HÌNH HỆ THỐNG

3.1 Tính toán thông lượng

3.1.1 Tính toán chung

Quy ước:

- Giả sử mỗi ngày công ty làm việc 8 giờ.
- Các kết quả tính toán được làm tròn lên ở chữ số thập phân thứ 3.

Đối với mỗi server:

- Tổng dung lượng download và upload: $1000 + 2000 = 3000$(MB).
- Thông lượng: $3000/(8 * 3600) \approx 0.105$(MB/s) $=$ **0.840(Mbps)**.

Đối với mỗi máy làm việc:

- Tổng dung lượng download và upload: $500 + 100 = 600$(MB).
- Thông lượng: $600/(8 * 3600) \approx 0.021$(MB/s) $=$ **0.168(Mbps)**.

Đối với kết nối từ khách hàng:

- Thông lượng: $500/(8 * 3600) \approx 0.018$(MB/s) $=$ **0.144(Mbps)**.

3.1.2 Trụ sở chính

- Tổng thông lượng của các server: $5 \times 0.840 = 4.200$(Mbps).
- Tổng thông lượng của các máy làm việc: $120 \times 0.168 = 20.160$(Mbps).
- Tổng thông lượng của khách hàng: 0.144(Mbps).
- Tổng thông lượng: $4.200 + 20.160 + 0.144 =$ **24.504(Mbps)**.

3.1.3 Chi nhánh

- Tổng thông lượng của các server: $3 \times 0.840 = 2.520$(Mbps).
- Tổng thông lượng của các máy làm việc: $30 \times 0.168 = 5.040$(Mbps).
- Tổng thông lượng của khách hàng: 0.144(Mbps).
- Tổng thông lượng: $2.520 + 5.040 + 0.144 =$ **7.704(Mbps)**.

3.2 Dự kiến băng thông

3.2.1 Yêu cầu chung

- Khoảng thời gian cao điểm trong một ngày kéo dài 3 giờ: gồm hai khoảng 9g-11g và 15g-16g.
- Dung lượng download/upload trong khoảng thời gian cao điểm, chiếm 80% tổng số dung lượng.
- Ngoài ra, mô hình mạng của công ty có tốc độ tăng trưởng ước tính vào khoảng 20% trong vòng 5 năm.
- Từ một số kết quả, các thiết bị mạng có tuổi thọ lên đến 10 năm. Cùng với nhu cầu thực tiễn, nhóm chọn mốc 10 năm làm thời gian hoạt động của mô hình mạng. Băng thông của thiết bị được chọn phải đáp ứng nhu cầu của công ty trong khoảng thời gian này.

3.2.2 Kết quả tính toán

- Băng thông hiện tại của trụ sở chính: $24.504 \times 0.8 \times (8/3) \approx 52.276$(Mbps).
- Băng thông trụ sở chính cần đảm bảo: $52.276 \times 1.2^2 \approx$ **75.278(Mbps)**.
- Băng thông hiện tại của mỗi chi nhánh: $7.704 \times 0.8 \times (8/3) \approx 16.436$(Mbps).
- Băng thông mỗi chi nhánh cần đảm bảo: $16.436 \times 1.2^2 \approx$ **23.668(Mbps)**.

3.3 Lựa chọn thiết bị

3.3.1 Router: 2911

Hình 5: Router 2911

Các thông số chính của Router gồm:

- 3 cổng Giga Ethernet hỗ trợ tốc độ tối đa 1Gbps.
- 4 khe cắm module mở rộng, mỗi module có thể cung cấp thêm 4 cổng Fast Ethernet với tốc độ lên đến 100Mbps hoặc 1 cổng Fiber WAN hỗ trợ tốc độ tối đa 1Gbps.
- Định tuyến: OSPF, MPLS.

(a) HWIC-1GE-SFP

(b) GLC-LH-SMD

(c) HWIC-4ESW

(d) WIC-Cover

Hình 6: Các module mạng sử dụng

Các module mạng sử dụng gồm:

- Module **HWIC-1GE-SFP**: Module đơn khe cắm Small Form-Factor Pluggable (SFP) cung cấp 1 cổng kết nối Gigabit Ethernet.
- **GLC-LH-SMD**: 1000BASE-LX/LH SFP cung cấp khả năng kết nối cáp quang cho các cổng kết nối Gigabit Ethernet.
- Module **HWIC-4ESW**: Module cung cấp 4 cổng chuyển mạch.
- **WIC-Cover**: Bảo vệ các khe cắm module mạng chưa sử dụng, bảo vệ các linh kiện điện tử bên trong, duy trì khả năng làm mát đầy đủ bằng cách bình thường hóa luồng không khí.

3.3.2 Multilayer switch: 3560-24PS

Hình 7: Multilayer switch 3560-24PS

- Switching Fabric: 160Gbps.
- Forwarding Rate: 65.5Mpps.

3.3.3 Switch: 2950T-24

Hình 8: Switch 2950T-24

- Switching Fabric: 8.8Gbps.
- Forwarding Rate: 8.8Gbps.

3.3.4 Access Point: AccessPoint-PT-N

Hình 9: AccessPoint-PT-N

3.3.5 ASA: 5506-X

Hình 10: ASA 5506-X

4 THIẾT KẾ SƠ ĐỒ MẠNG

4.1 Sơ đồ kết nối luận lý

Hình 11: Toàn bộ hệ thống mạng

Hệ thống chia ra gồm Trụ sở (Ho Chi Minh City), 2 Chi nhánh (Ha Noi, Da Nang) và vùng DSL kết nối lên Internet. Các router trụ sở và chi nhánh kết nối với nhau thông qua 2 đường dây Leased line và được định tuyến bằng OSPF protocol.
Trụ sở chính kết nối với Internet thông qua 2 đường dây DSL với cơ chế cân bằng tải theo gói tin (**per-packet load balacing**, các gói tin sẽ được gửi luân phiên qua 2 đường dây), là cơ chế mặc định được cung cấp sẵn của router 2911 mà nhóm lựa chọn. Các PCs từ các tầng và các chi nhánh đều có thể kết nối đến Internet thông qua router của trụ sở chính.

Hình 12: Trụ sở chính

Trụ sở chính gồm 3 phân vùng:

1. **Vùng DMZ**: nằm ở tầng 1, gồm các server đều được cấu hình IP tĩnh:
   - Mail Server: máy chủ chuyển/nhận mail.
   - Web Server: máy chủ cài đặt các ứng dụng web.
2. **Vùng Access Point**: nằm ở tầng 1, là địa điểm tiếp đón khách đến tham quan, cung cấp kết nối không dây cho các thiết bị di động truy cập vào mạng LAN của trụ sở.
3. **Vùng nội bộ**: 7 tầng của trụ sở được kết nối với nhau thông qua một multilayer switch. Vùng này có thiết lập tường lửa hạn chế lưu lượng truy cập vào và ra giữa mạng nội bộ các tầng và bên ngoài trụ sở. Tầng 1 bao gồm một phòng chứa các private servers (bao gồm cả Camera Server quản lý các camera được lắp đặt tại mỗi tầng), các thiết bị mạng (switch, access point) kết nối các thiết bị nội bộ của nhân viên và một phòng tập trung các đường dây mạng chính. Tầng 2-7 đều bao gồm 1 switch kết nối có dây các workstations và 1 access point kết nối không dây các thiết bị di động (Laptop, Smartphone) và các thiết bị IOT (Webcam) của hệ thống camera giám sát.

(a) Vùng Private Server

(b) Vùng kết nối các thiết bị sử dụng mạng

(c) Vùng DMZ Server

(d) Vùng access point

Hình 13: Tầng 1 - Trụ sở chính

Hình 14: Tầng 2-7 - Trụ sở chính

Hình 15: Các chi nhánh

Các chi nhánh đều có cấu trúc mạng như nhau. Mỗi chi nhánh bao gồm 2 phân vùng:

1. **Vùng Access Point**: nằm ở tầng 1, là địa điểm tiếp đón khách đến tham quan, cung cấp kết nối không dây cho các thiết bị di động truy cập vào mạng LAN của chi nhánh.

2. **Vùng nội bộ**: 2 tầng của chi nhánh được kết nối với nhau thông qua một multilayer switch. Vùng này có thiết lập tường lửa hạn chế lưu lượng truy cập vào và ra giữa mạng nội bộ các tầng và bên ngoài chi nhánh.

   - Tầng 1: được bố trí tương tự trụ sở chính bao gồm 1 phòng kỹ thuật mạng, 1 phòng tập trung các đường dây mạng chính, các thiết bị mạng (switch, access point) kết nối các thiết bị nội bộ của nhân viên.
   - Tầng 2: cũng được bố trí tương tự các tầng từ 2-7 trụ sở chính, bao gồm 1 switch và 1 access point.

(a) Vùng server

(b) Vùng access point

(c) Vùng kết nối các thiết bị sử dụng mạng

Hình 16: Tầng 1 - Chi nhánh

Hình 17: Tầng 2 - Chi nhánh

4.2 Sơ đồ kết nối vật lý

Hình 18: Toàn bộ hệ thống mạng

Hai chi nhánh Hà Nội và Đà Nẵng kết nối với trụ sở chính TP Hồ Chí Minh bằng 2 đường dây thuê riêng (Hình 18- Đường màu vàng).
Sơ đồ kết nối vật lý giữa các tầng của trụ sở và chi nhánh có cấu trúc giống nhau. Tuy nhiên, chỉ có trụ sở mới có đường kết nối ra Internet (Hình 19 - Tầng 1 trụ sở có đường dây kết nối Internet), các thiết bị trong các chi nhánh muốn kết nối Internet đều phải đi qua router của trụ sở.

Hình 19: Trụ sở chính

Hình 20: Chi nhánh

Tầng 1 của trụ sở chính và chi nhánh có thiết kế vật lý giống nhau, đều bao gồm 1 phòng kỹ thuật mạng, 1 phòng tập trung các đường dây mạng chính, các thiết bị mạng

(switch, access point) kết nối các thiết bị nội bộ của nhân viên và một access point cung cấp Internet cho khách hàng.

Hình 21: Tầng 1 - Trụ sở chính

Hình 22: Tầng 1 - Chi nhánh

Các tầng từ 2-7 của trụ sở chính và tầng 2 của chi nhánh cũng có cấu trúc vật lý

tương tự, mỗi phòng đều có 1 switch và 1 access point cung cấp các kết nối mạng nội bộ có dây và không dây.

Hình 23: Tầng 2-7 - Trụ sở chính

Hình 24: Tầng 2 - Chi nhánh

5 KIỂM THỬ HỆ THỐNG

5.1 Kịch bản kiểm thử

Ghi chú: Thiết bị trong cùng địa điểm nghĩa là cùng thuộc Trụ sở hoặc chi nhánh. Ngược lại, khác địa điểm là giữa trụ sở, chi nhánh hoặc các trường hợp khác.

5.1.1 Thiết bị trong cùng VLAN

Mục đích	#	Nội dung kiểm thử	Kỳ vọng	Kết quả
Kiểm tra kết nối thành công các thiết bị trong cùng VLAN tại mỗi trụ sở, chi nhánh công ty	SV-01	- PCs cùng phòng ban, cùng tầng	Thành công	Thành công
	SV-02	- Camera với thiết bị di động cùng tầng	Thành công	Thành công
	SV-03	- Giữa các thiết bị di động	Thành công	Thành công
	SV-04	- Thiết bị di động với camera khác tầng	Thành công	Thành công

Bảng 13: Kịch bản kiểm thử: Thiết bị trong cùng VLAN

5.1.2 Thiết bị giữa các VLAN

Mục đích	#	Nội dung kiểm thử	Kỳ vọng	Kết quả
Kiểm tra kết nối thành công các thiết bị khác VLAN tại mỗi trụ sở, chi nhánh công ty	DV-01	- PCs khác phòng ban, khác tầng	Thành công	Thành công
	DV-02	- PCs với các thiết bị di động	Thành công	Thành công
	DV-03	- PCs với các camera	Thành công	Thành công
	DV-04	- PCs với public server	Thành công	Thành công
	DV-05	- PCs với private server	Thành công	Thành công

Bảng 14: Kịch bản kiểm thử: Thiết bị giữa các VLAN

5.1.3 Các thiết bị giữa trụ sở và chi nhánh

Mục đích	#	Nội dung kiểm thử	Kỳ vọng	Kết quả
Kiểm tra kết nối thành công các thiết bị khác mạng nội bộ mỗi trụ sở, chi nhánh công ty	SS-01	- PCs cùng VLAN, khác địa điểm	Thành công	Thành công
	SS-02	- PCs khác VLAN, khác địa điểm	Thành công	Thành công
	SS-03	- PC với thiết bị di động khác địa điểm	Thành công	Thành công
	SS-04	- Giữa các thiết bị di động khác địa điểm	Thành công	Thành công
	SS-05	- PC với camera khác địa điểm	Thành công	Thành công
	SS-06	- Thiết bị di động với camera khác địa điểm	Thành công	Thành công
	SS-07	- PCs với các private server khác địa điểm	Thành công	Thành công

Bảng 15: Kịch bản kiểm thử: Các thiết bị giữa trụ sở và chi nhánh

5.1.4 Các server trong DMZ

Mục đích	#	Nội dung kiểm thử	Kỳ vọng	Kết quả
Kiểm tra kết nối của các server trong DMZ	SD-01	- Giữa các server trong DMZ	Thành công	Thành công
	SD-02	- Server trong DMZ với PCs cùng địa điểm	Thành công	Thành công
	SD-03	- Server trong DMZ với PCs khác địa điểm	Thành công	Thành công
	SD-04	- Server trong DMZ với các thiết bị của khách hàng (kết nối tới access point tại trụ sở)	Thành công	Thành công
	SD-05	- Server trong DMZ với các thiết bị của khách hàng khác	Thành công	Thành công

Bảng 16: Kịch bản kiểm thử: Các server trong DMZ

5.1.5 Hệ thống camera giám sát

Mục đích	#	Nội dung kiểm thử	Kỳ vọng	Kết quả
Kiểm tra hoạt động của hệ thống camera giám sát tại trụ sở	CM-01	Các thiết bị truy cập vào camera server tại trụ sở, tiến hành đăng nhập vào tài khoản ***admin***	Quan sát được trạng thái của các camera tại trụ sở.	Quan sát được
Kiểm tra hoạt động của hệ thống camera giám sát tại chi nhánh	CM-02	Các thiết bị truy cập vào camera server tại chi nhánh, tiến hành đăng nhập vào tài khoản ***admin***	Quan sát được trạng thái của các camera tại chi nhánh.	Quan sát được

Bảng 17: Kịch bản kiểm thử: Hệ thống camera giám sát

5.1.6 Kết nối từ Internet

Mục đích	#	Nội dung kiểm thử	Kỳ vọng	Kết quả
Kiểm tra tính cách ly mạng nội bộ với Internet	IN-01	- Thiết bị điện tử của khách hàng (kết nối với access point tại trụ sở) tới PCs trụ sở	Thất bại	Thất bại
	IN-02	- Thiết bị điện tử của khách hàng khác tới PCs trụ sở	Thất bại	Thất bại
	IN-03	- Thiết bị điện tử của khách hàng (kết nối với access point tại chi nhánh) tới PCs chi nhánh	Thất bại	Thất bại
	IN-04	- Thiết bị điện tử khách hàng khác tới PCs chi nhánh	Thất bại	Thất bại
	IN-05	- Thiết bị điện tử khách hàng (kết nối với access point tại trụ sở) tới private server	Thất bại	Thất bại
	IN-06	- Thiết bị điện tử khách hàng khác tới private server	Thất bại	Thất bại
Kiểm tra VPN cho kết nối truy cập từ xa	IN-07	- Nhân viên làm việc từ xa với PCs trụ sở	Thành công	Thành công
	IN-08	- Nhân viên làm việc từ xa với PCs chi nhánh	Thành công	Thành công
	IN-09	- Kết nối giữa PCs tại 2 chi nhánh thông qua VPN	Thành công (được mã hóa)	Thành công (được mã hóa)
Kiểm tra khả năng truy cập Web Server	IN-10	Kết nối giữa máy tính trong công ty với một Web Server	Thành công	Thành công
Kiểm tra cơ chế cân bằng tải	IN-11	Các gói tin gửi đi được phân bổ qua 2 modem DSL theo cơ chế **per-packet load balacing**	Có cân bằng tải	Có cân bằng tải

Bảng 18: Kịch bản kiểm thử: Kết nối từ Internet

5.2 Kết quả kiểm thử

5.2.1 Kết nối giữa các thiết bị trong cùng VLAN tại mỗi trụ sở, chi nhánh công ty

Hình 25: Trụ sở chính: 2 PC bất kỳ tầng 2 có thể ping lẫn nhau

Hình 26: Chi nhánh: 2 PC bất kỳ tầng 1 có thể ping lẫn nhau

Hình 27: Trụ sở chính: Laptop tầng 2 có thể ping webcam IoT2

Hình 28: Chi nhánh: Laptop tầng 1 có thể ping webcam IoT10

Hình 29: Trụ sở chính : Laptop tầng 1 có thể ping Laptop tầng 2

Hình 30: Chi nhánh : Laptop tầng 1 có thể ping Smartphone tầng 2

Hình 31: Trụ sở chính : Smartphone tầng 3 có thể ping Webcam tầng 4

Hình 32: Chi nhánh : Smartphone tầng 2 có thể ping Webcam tầng 1

5.2.2 Kết nối giữa các thiết bị khác VLAN tại mỗi trụ sở, chi nhánh công ty

Hình 33: Trụ sở chính: PC tầng 2 có thể ping PC tầng 3

Hình 34: Chi nhánh : PC tầng 1 có thể ping PC tầng 2

Hình 35: Trụ sở chính: PC tầng 7 có thể ping Smartphone tầng 7

Hình 36: Chi nhánh : PC tầng 1 có thể ping Laptop tầng 1

Hình 37: Trụ sở chính: PC tầng 5 có thể ping Webcam tầng 5

Hình 38: Chi nhánh : PC tầng 2 có thể ping Webcam tầng 2

Hình 39: Trụ sở chính: PC tầng 2 có thể truy cập Web Server trong vùng DMZ

Hình 40: Chi nhánh : PC tầng 2 có thể truy cập Web Server trong vùng DMZ ở trụ sở chính

Hình 41: Trụ sở chính: PC tầng 2 có thể truy cập Camera Server trong vùng Private Server ở tầng 1

Hình 42: Chi nhánh : PC tầng 1 có thể truy cập Camera Server trong vùng Private Server ở tầng 1

5.2.3 Kết nối các thiết bị giữa trụ sở và chi nhánh

Hình 43: PC tầng 2 trụ sở chính có thể ping PC tầng 2 chi nhánh (cùng VLAN 40)

Hình 44: PC tầng 1 chi nhánh (VLAN 30) có thể ping PC tầng 5 trụ sở (VLAN 70)

Hình 45: Smartphone tầng 2 chi nhánh (VLAN 20) có thể ping PC tầng 7 trụ sở (VLAN 90)

Hình 46: Smartphone tầng 4 trụ sở (VLAN 60) có thể ping Smartphone tầng 2 chi nhánh (VLAN 20)

Hình 47: PC tầng 3 trụ sở (VLAN 50) có thể ping Webcam tầng 1 chi nhánh (VLAN 20)

Hình 48: Laptop tầng 1 chi nhánh (VLAN 20) có thể ping Webcam tầng 2 trụ sở (VLAN 20)

Hình 49: PC tầng 2 chi nhánh (VLAN 40) có thể truy cập Web Server trong vùng Private Server của trụ sở (VLAN 10)

5.2.4 Kết nối của các server trong DMZ

Hình 50: 2 server trong vùng DMZ có thể ping lẫn nhau

Hình 51: PC nội bộ bất kỳ của trụ sở có thể truy cập vào Web Server vùng DMZ

Hình 52: PC nội bộ bất kỳ của chi nhánh có thể truy cập vào Web Server vùng DMZ

Hình 53: Các thiết bị kết nối không dây tới access point của trụ sở có thể truy cập vào Web Server vùng DMZ

Hình 54: Các thiết bị của khách hàng khác có thể truy cập vào Web Server vùng DMZ

5.2.5 Hệ thống camera giám sát

Hình 55: PC tại tầng 3 của trụ sở có thể truy cập vào địa chỉ của Camera Server tại trụ sở (192.168.10.2) và đăng nhập với tài khoản ***admin*** để quan sát camera tại các tầng

Hình 56: Smartphone tại tầng 2 của chi nhánh Hà Nội có thể truy cập vào địa chỉ của Camera Server tại chi nhánh (192.166.10.2) và đăng nhập với tài khoản ***admin*** để quan sát camera tại các tầng

5.2.6 Kết nối từ Internet

Hình 57: Thiết bị điện tử của khách hàng (kết nối với access point tại trụ sở) không thể kết nối tới PC nội bộ bất kỳ của trụ sở

Hình 58: Thiết bị điện tử của khách hàng khác cũng không thể kết nối tới PC nội bộ bất kỳ của trụ sở

Hình 59: Thiết bị điện tử của khách hàng (kết nối với access point tại chi nhánh Đà Nẵng) không thể kết nối tới PC nội bộ bất kỳ của chi nhánh này

Hình 60: Thiết bị điện tử của khách hàng khác cũng không thể kết nối tới PC nội bộ bất kỳ của chi nhánh Đà Nẵng

Hình 61: Thiết bị điện tử của khách hàng (kết nối với access point tại trụ sở) không thể truy cập vào web server nội bộ của trụ sở (địa chỉ 192.168.10.6)

Hình 62: Thiết bị điện tử của khách hàng khác cũng không thể truy cập vào web server nội bộ của trụ sở

Để kết nối tới các thiết bị nội bộ của công ty, nhân viên làm việc từ xa tiến hành đăng nhập VPN theo các thông tin như sau:

Hình 63: Thông tin đăng nhập VPN của nhân viên làm việc từ xa

Hình 64: Nhân viên làm việc từ xa có thể ping tới PC bất kỳ tại trụ sở sau khi đã đăng nhập VPN

Hình 65: Nhân viên làm việc từ xa có thể ping tới PC bất kỳ tại chi nhánh sau khi đã đăng nhập VPN

Để kết nối tới các thiết bị nội bộ tại các địa điểm khác qua VPN, nhân viên tại chi nhánh Hà Nội tiến hành đăng nhập theo các thông tin như sau:

Hình 66: Thông tin đăng nhập VPN của một nhân viên tại chi nhánh Hà Nội

Hình 67: Nhân viên tại chi nhánh Hà Nội có thể ping tới PC bất kỳ tại chi nhánh Đà Nẵng thông qua VPN

Sử dụng chế độ *Simulation* trong Cisco Packet Tracer, có thể thấy địa chỉ đích của gói tin ICMP gửi từ chi nhánh Hà Nội tới chi nhánh Đà Nẵng đã được bảo mật và nội dung của gói tin đó đã được mã hóa.

Hình 68: Gói tin ICMP gửi từ chi nhánh Hà Nội tới chi nhánh Đà Nẵng

Hình 69: Các thiết bị bất kỳ trong nội bộ công ty có thể truy cập một trang Web trên Internet

Hình 70: Cơ chế cân bằng tải được áp dụng, các gói tin gửi từ thiết bị bất kỳ trong nội bộ công ty ra Internet sẽ được truyền luân phiên qua 2 Interface 20.0.1.1 và 20.0.2.1 của ISP

6 ĐÁNH GIÁ HỆ THỐNG

6.1 Kết quả đạt được

6.1.1 Mức độ tin cậy và khả năng đáp ứng yêu cầu hệ thống

Với kết quả khảo sát yêu cầu hệ thống mạng và sơ đồ công ty, việc lựa chọn kiến trúc mạng Extended Star Topology cho từng tòa nhà và Star Topology cho kết nối WAN là phù hợp cả về kiến trúc và yêu cầu thẩm mỹ.

Từ kết quả tính toán thông lượng và dự kiến băng thông, các thiết bị được chọn hoàn toàn đáp ứng đầy đủ yêu cầu về tốc độ của hệ thống mạng cho toàn bộ công ty trong ít nhất 10 năm tiếp theo.

Bằng cách cấu hình thích hợp, mức độ tin cậy của hệ thống được đảm bảo, mọi tiêu chí kiểm thử đều đạt kỳ vọng đặt ra.

6.1.2 Khả năng mở rộng, nâng cấp của hệ thống

Các thiết bị mạng được chọn đều có khả năng mở rộng mạnh mẽ, cụ thể:

- Router 2911 ở trụ sở chính vẫn còn một khe cắm module chưa sử dụng, có khả năng mở rộng thêm 4 cổng chuyển mạch hoặc 1 kết nối Fiber WAN. Yếu tố trên là vô cùng cần thiết đặc biệt trong trường hợp công ty có thêm chi nhánh.
- Multilevel switch đang sử dụng 14 trên tổng số 26 cổng Ethernet khả dụng (đối với trụ sở chính). Do đó khả năng mở rộng vẫn còn rất lớn, sẵn sàng đáp ứng nếu công ty cần mở rộng quy mô thiết bị ở các tầng hoặc sử dụng đến các tầng khác của tòa nhà.
- Các switch ở mỗi tầng gần như đã đạt mức sử dụng tối đa, tuy nhiên như đề cập ở trên, mỗi tầng đều có khả năng sử dụng thêm switch nếu cần thiết.

Ngoài ra, bằng cách sử dụng module mạng thay vì các phần tử cố định, việc nâng cấp, thay thế là hoàn toàn khả thi và không tốn nhiều công sức.

6.1.3 Tính an toàn, bảo mật của hệ thống

Các thiết bị Firewall ASA được kết nối với các Multilayer Switch tại trụ sở chính và 2 chi nhánh nhằm kiểm soát được quyền truy cập tới các thiết bị trong mạng nội bộ của công ty, từ đó tăng tính bảo mật cho hệ thống.

Hệ thống camera giám sát được trang bị cũng góp phần đảm bảo tốt hơn an ninh tại công ty. Mặt khác, để có thể quan sát được trạng thái của các camera, cần phải kết nối vào một server nội bộ của công ty và thực hiện xác thực tài khoản. Điều này giới hạn được quyền truy xuất thông tin của các camera, chỉ có có những người có thẩm quyền (như tổ bảo vệ, an ninh của công ty) mới có thể thực hiện tác vụ này.

Ngoài ra, mạng riêng ảo (VPN) được sử dụng để giúp các nhân viên làm việc từ xa có thể kết nối tới hệ thống mạng nội bộ của công ty một cách bảo mật, dữ liệu trên

đường truyền từ máy tính của nhân viên qua Internet tới công ty được mã hóa. Nhân viên tại các chi nhánh và trụ sở cũng có thể sử dụng VPN để tăng tính bảo mật cho các thông tin mà họ truyền nhận với nhau.

6.2 Hạn chế còn tồn tại

Đối với các thiết bị đang sử dụng, đặc biệt là các thiết bị ở chi nhánh, các thiết bị mạng sử dụng hoàn toàn vượt xa yêu cầu của hệ thống mạng cả về khả năng kết nối, băng thông yêu cầu,... Tuy nhiên, phần mềm mô phỏng nhóm chọn sử dụng không cung cấp các thiết bị phù hợp.

Trong bài tập lớn, nhóm không sử dụng Patch Panel để tập trung các dây. Nguyên nhân do Patch Panel làm cho việc yêu cầu địa chỉ IP thông qua DHCP thất bại và nhóm không tìm được cách khắc phục.

Bên cạnh đó, đối với khả năng kết nối ra Internet của các thiết bị nội bộ trong công ty, nhóm chỉ mới hiện thực được các kết nối qua các giao thức DNS, FTP, H323, HTTP, ICMP và TFTP. Nguyên nhân là do nhóm hiện thực các kết nối này bằng kỹ thuật *Application Layer Protocol Inspection*, đối với thiết bị ASA 5506-X mà nhóm sử dụng thì kỹ thuật này chỉ áp dụng được cho các giao thức nêu trên và nhóm chưa tìm được giải pháp thay thế.

6.3 Định hướng phát triển

Từ các kết quả đã đạt được, nhóm đề xuất các định hướng sau để tiếp tục hoàn thiện đề tài:

- Tiếp tục tìm cách khắc phục những hạn chế được nêu ở phần trên.
- Tìm hiểu thêm về cách hiện thực những giao thức mới, phù hợp với yêu cầu thực tiễn hiện nay.
- Tìm kiếm cơ hội hiện thực trên phần cứng, ứng với các loại thiết bị mới hiện nay nhằm nâng cao kinh nghiệm cho toàn bộ thành viên nhóm.

7 TÀI LIỆU THAM KHẢO

1. Cisco. *IP Addressing Guide*. Truy cập từ: https://www.cisco.com/c/dam/global/en_ca/solutions/strategy/docs/sbaBN_IPv4addrG.pdf (ngày 17/11/2023)

2. Cisco. *"Performing a Site Survey"*. Truy cập từ: https://www.cisco.com/c/en/us/td/docs/wireless/wlan_adapter/350_cb20a/user/win_ce/2-3/configuration/guide/hig/CE_appE.pdf (ngày 11/11/2023)

   Cisco (2022). *"Understand Site Survey Guidelines for WLAN Deployment"*. Truy cập từ:https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html (ngày 11/11/2023)

3. HOW TO NETWORK. *Network Design – Designing Advanced IP Addressing*. Truy cập từ: https://www.howtonetwork.com/technical/network-management/network-design/ (ngày 15/11/2023)

4. Kurose, J.F. & Ross, K.W. *Computer Networks, A Top-down Approach*. (2020). 8th ed.