

ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH  
TRƯỜNG ĐẠI HỌC BÁCH KHOA  
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH



BÁO CÁO BÀI TẬP LỚN 2  
MẠNG MÁY TÍNH (CO3093)

---

COMPUTER NETWORK DESIGN  
FOR A CRITICAL LARGE COMPANY

---

GV hướng dẫn: TS. Nguyễn Lê Duy Lai  
ThS. Bùi Xuân Giang

Lớp thực hành: TN01

SV thực hiện: Võ Nguyễn Doan Thảo 2110546  
Nguyễn Trần Bảo Ngọc 2111860  
Lê Duy Anh 2112762

Ho Chi Minh City, December, 2023



## Mục lục

<b>1</b>	<b>Giới thiệu đề tài</b>	<b>3</b>
<b>2</b>	<b>Yêu cầu hệ thống</b>	<b>3</b>
2.1	Yêu cầu hệ thống mạng . . . . .	3
2.1.1	Hệ thống mạng tại trụ sở . . . . .	3
2.1.2	Hệ thống mạng tại chi nhánh . . . . .	3
2.1.3	Thông lượng và tải truyền của hệ thống . . . . .	4
2.2	Khảo sát vị trí lắp đặt . . . . .	4
2.3	Xác định các vùng có tải lớn trong hệ thống . . . . .	5
2.4	Thiết kế cấu trúc mạng . . . . .	5
<b>3</b>	<b>Thiết kế hệ thống</b>	<b>6</b>
3.1	Danh sách các thiết bị mạng . . . . .	6
3.1.1	Router . . . . .	6
3.1.2	Switch . . . . .	7
3.1.3	Access-point . . . . .	9
3.1.4	Firewall . . . . .	9
3.1.5	Dự trù kinh phí . . . . .	10
3.2	Sơ đồ IP . . . . .	10
3.2.1	Sơ đồ IP trụ sở chính . . . . .	10
3.2.2	Sơ đồ IP chi nhánh Đà Nẵng . . . . .	10
3.2.3	Sơ đồ IP chi nhánh Hà Nội . . . . .	11
3.3	Sơ đồ đi dây . . . . .	11
<b>4</b>	<b>Công nghệ sử dụng</b>	<b>12</b>
4.1	VLAN - Virtual Local Area Network . . . . .	12
4.2	VTP - VLAN Trunking Protocol . . . . .	12
4.3	OSPF - Open Shortest Path First . . . . .	13
4.4	DHCP - Dynamic Host Configuration Protocol . . . . .	13
4.5	Site-to-Site IPsec VPN . . . . .	14
<b>5</b>	<b>Tính toán các thông số cho mạng máy tính</b>	<b>14</b>
5.1	Một số khái niệm liên quan đến hiệu suất mạng . . . . .	14
5.1.1	Băng thông - Bandwidth . . . . .	14
5.1.2	Thông lượng - Throughput . . . . .	14
5.2	Trụ sở chính . . . . .	15
5.3	Chi nhánh . . . . .	15
<b>6</b>	<b>Thiết kế hệ thống mạng sử dụng Cisco Packet Tracer</b>	<b>15</b>
<b>7</b>	<b>Kiểm thử kết quả</b>	<b>17</b>
7.1	Trong cùng VLAN . . . . .	17
7.2	Giữa các VLAN . . . . .	18
7.3	Giữa chi nhánh và trụ sở chính . . . . .	19
7.4	Kết nối với server trong vùng DMZ . . . . .	20
7.5	Kết nối giữa mạng Customer và LAN . . . . .	21
7.6	Kết nối tới một Web server ở ngoài Internet . . . . .	22
7.7	Hệ thống Camera giám sát . . . . .	23



---

<b>8 Bảo mật hệ thống</b>	<b>23</b>
8.1 Sử dụng WiFi Protected Access (WPA-2) . . . . .	23
8.2 Sử dụng Hardware-based Firewall . . . . .	24
<b>9 Đánh giá hệ thống</b>	<b>24</b>
9.1 Những điều đạt được . . . . .	24
9.2 Những hạn chế . . . . .	25
9.3 Định hướng phát triển trong tương lai . . . . .	25
<b>10 Tài liệu tham khảo</b>	<b>26</b>



## 1 Giới thiệu đề tài

Bài tập lớn này liên quan đến việc thiết kế một cấu trúc mạng cho một công ty lớn, trong đó mỗi phòng ban có một số máy tính ở các tòa nhà khác nhau và thiết lập mạng để họ có thể tương tác và giao tiếp với nhau bằng cách trao đổi dữ liệu.

Mạng được thiết kế và mô phỏng bằng phần mềm mô phỏng mạng Cisco Packet Tracer. Cisco Packet Tracer (CPT) là một phần mềm mô phỏng mạng đa nhiệm có thể được sử dụng để thực hiện và phân tích các hoạt động mạng khác nhau như triển khai các cấu trúc mạng khác nhau, chọn lựa các đường đi tối ưu dựa trên các bộ định tuyến khác nhau và phân tích các cấu hình mạng khác nhau.

## 2 Yêu cầu hệ thống

### 2.1 Yêu cầu hệ thống mạng

CCC (Computer & Construction Concept) được yêu cầu để thiết kế một mạng máy tính triển khai tại Trụ sở chính (tại Thành phố Hồ Chí Minh) và hai Chi nhánh (tại Đà Nẵng và Hà Nội) của một Ngân hàng BB đang được xây dựng. Các đặc điểm chính của việc sử dụng Công nghệ Thông tin trong Công ty này như sau.

#### 2.1.1 Hệ thống mạng tại trụ sở

- Toàn bộ tòa nhà trụ sở chính bao gồm 7 tầng, tầng đầu tiên được trang bị một phòng IT và Trung tâm Cáp Quang Cục Bộ (sử dụng các bảng kết nối dây).
- Quy mô trung bình: 120 máy trạm, 5 máy chủ, 12 thiết bị mạng (hoặc có thể nhiều hơn với các thiết bị đặc biệt về bảo mật).
- Sử dụng **công nghệ mới** cho cơ sở hạ tầng mạng bao gồm kết nối có dây và không dây, cáp quang (GPON), và GigaEthernet 1GbE/10GbE. Mạng được tổ chức theo cấu trúc VLAN cho các bộ phận khác nhau.
- Mạng con Trụ sở kết nối với mạng con của hai Chi nhánh thông qua **2 đường leased lines cho kết nối WAN** (có thể áp dụng SD-WAN, MPLS) và 2 xDSL để truy cập Internet với cơ chế cân bằng tải. Tất cả lưu lượng truy cập Internet đi qua mạng con Trụ sở chính.
- Yêu cầu về an ninh cao (ví dụ: tường lửa, IPS/IDS, phát hiện lừa đảo), khả năng sẵn có cao (HA), độ bền khi xảy ra vấn đề, dễ dàng nâng cấp hệ thống.
- **Đề xuất cấu hình VPN** cho kết nối site-to-site và cho người làm việc từ xa kết nối vào Mạng LAN của Công ty.
- **Đề xuất hệ thống camera giám sát** cho Công ty

#### 2.1.2 Hệ thống mạng tại chi nhánh

- Toàn bộ tòa nhà có 2 tầng, tầng đầu tiên được trang bị 1 phòng IT và 1 Trung tâm Cáp Quang Cục Bộ.
- Quy mô nhỏ của Chi nhánh BB: 30 máy trạm, 3 máy chủ, 5 hoặc nhiều thiết bị mạng hơn.



### 2.1.3 Thông lượng và tải truyền của hệ thống

Thực hiện kết nối giữa Trụ sở và Chi nhánh thông qua các liên kết WAN, bạn có thể chọn một trong các công nghệ như SD-WAN, MPLS, vv. được sử dụng cho liên kết này tùy thuộc vào chi phí của giải pháp. Liệt kê tất cả các lựa chọn có sẵn.

- Đề xuất các tùy chọn với chi phí.
- Phân tích ưu và nhược điểm của giải pháp đã chọn.

Luồng dữ liệu và công việc của hệ thống (khoảng 80% vào giờ cao điểm từ 9g-11g và 15g-16g) có thể được chia sẻ cho Trụ sở chính và Chi nhánh như sau:

- Máy chủ cho cập nhật phần mềm, truy cập web và truy cập cơ sở dữ liệu,... Ước tính tổng dung lượng tải là khoảng 1000 MB/ngày và dung lượng tải lên ước tính là 2000 MB/ngày.
- Mỗi máy trạm được sử dụng để duyệt web, tải văn bản và giao dịch của khách hàng,... Ước tính tổng dung lượng tải là khoảng 500 MB/ngày và dung lượng tải lên ước tính là 100 MB/ngày.
- Thiết bị kết nối WiFi từ quy trình tải của khách hàng là khoảng 500 MB/ngày.

Mạng của Ngân hàng BB được ước tính có tốc độ tăng trưởng 20% trong 5 năm (về số lượng người dùng, tải mạng, mở rộng chi nhánh,...).

## 2.2 Khảo sát vị trí lắp đặt

Trụ sở gồm 120 máy trạm, 5 máy chủ và 12 thiết bị mạng (hoặc hơn) được bố trí trong một tòa nhà 7 tầng theo cấu trúc sau:

Tầng	Phòng ban	Thiết bị
1	Giao dịch	20 máy trạm
	Công cộng	1 Access Point
	IT	5 Server, 1 Multilayer Switch và 1 switch
2	Hỗ trợ khách hàng	20 máy trạm
3	Tài chính	15 máy trạm
4	Tài chính	15 máy trạm
5	Truyền thông	20 máy trạm
6	Kinh doanh	20 máy trạm
7	Quản lý	10 máy trạm
Chung	Thiết bị mạng	1 Router, 1 Multilayer Switch, 7 Switch cho 7 tầng, 1 Firewall
	Camera	3-4 Camera cho mỗi tầng

Mỗi chi nhánh gồm 30 máy trạm, 3 máy chủ và 5 (hoặc nhiều hơn) thiết bị mạng được bố trí trong tòa nhà 2 tầng.

Tầng	Phòng ban	Thiết bị
1	Giao dịch	20 máy trạm
	IT	3 máy chủ, 1 Multilayer Switch và 1 Switch
	Công cộng	1 Access Point
	Quản lý	10 máy trạm
Chung	Thiết bị mạng	1 Router, 1 Multilayer Switch, 2 Switch cho 2 tầng, 1 Firewall
	Camera	2-3 Camera cho mỗi tầng

## 2.3 Xác định các vùng có tải lớn trong hệ thống

Network Load Balancing:

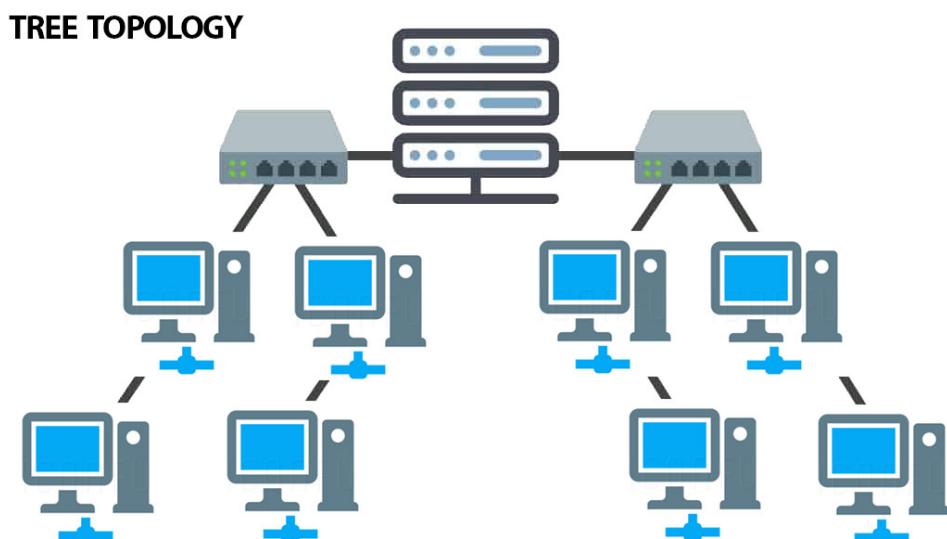
- Giải pháp cân bằng tải (Network Load Balancing) là một trong những tính năng rất quan trọng với những nhà phát triển, lập trình mạng. Là việc phân bổ đồng đều lưu lượng truy cập giữa hai hay nhiều các server có cùng chức năng trong cùng một hệ thống.
- Bằng việc sử dụng Network Load Balancing, hệ thống sẽ giảm thiểu tối đa tình trạng một server bị quá tải và ngưng hoạt động. Hoặc khi một server gặp sự cố, cân bằng tải sẽ chỉ đạo phân phối công việc của server đó cho các server còn lại, đẩy thời gian uptime của hệ thống lên cao nhất và cải thiện năng suất hoạt động tổng thể. Điều này đảm bảo tính khả dụng và độ tin cậy của hệ thống và có thể dễ dàng thêm vào hoặc loại bỏ các server theo yêu cầu nâng cấp trong tương lai một cách linh hoạt.

Về kỹ thuật, hệ thống web server: Cho phép tất cả người dùng Internet đều có thể tìm kiếm thông tin, trao đổi thông tin với website công ty. Do vậy, cần phải đảm bảo về tốc độ truy cập, tính ổn định.

Ta nhận thấy, tại tầng 1 và tầng 2 ở trụ sở chính có lượng truy cập từ nhiều khách hàng, lượng thông tin ở đây là rất lớn. Do đó cần chú trọng tới cân bằng tải ở nơi đây. Ngoài ra, cả tòa nhà sẽ cần một cân bằng tải ngay sau WAN connection để cân bằng giữa máy trạm và server do đây là kết nối bị bottleneck.

## 2.4 Thiết kế cấu trúc mạng

Ta thiết kế mạng theo mô hình Server-Client và topo cây, gồm các switch 100/1000 Mbps nhằm giảm thiểu các ảnh hưởng của mạng con với nhau, đồng thời đảm bảo chúng có thể giao tiếp hiệu quả. Trong mô hình này, nút gốc sẽ là router kết nối với các chi nhánh và Internet, tiếp theo đến tầng switch và cuối cùng là nút lá các máy trạm và thiết bị mạng.



Hình 1: Topo hình cây trong cấu trúc mạng



Hệ thống máy chủ được đặt tại phòng kỹ thuật gồm:

- Máy chủ web (Web Server) là máy chủ mà trên đó cài đặt phần mềm phục vụ web cho khách hàng,...
- Máy chủ Mail: để gửi-nhận thư điện tử.
- Máy chủ FTP (FTP server): FTP (File Transfer Protocol) được dùng để trao đổi tập tin qua mạng lưới truyền thông dùng giao thức TCP/IP (chẳng hạn như Internet - mạng ngoại bộ - hoặc intranet - mạng nội bộ)
- Máy chủ DNS (DNS Server) là máy chủ phân giải tên miền. Hệ thống tên miền DNS (Domain Name System) được sử dụng để ánh xạ tên miền thành địa chỉ IP.
- Máy chủ IoT (IoT Server): quản lý các thiết bị IoT được sử dụng, mà cụ thể là hệ thống camera giám sát.

Trong mạng sử dụng Switch Layer 3 để kết nối với hệ thống Server và workstation thông qua các switch layer 2. 7 Switch Layer 2 ở trụ sở chính hay 2 Switch Layer 2 ở chi nhánh kết nối vào Switch Layer 3. Đường kết nối từ Switch Layer 2 và Access Point đến Switch Layer 3 bằng Cáp quang để đảm bảo chất lượng và tốc độ đường truyền.

Kết nối từ chi nhánh khác đi vào hệ thống mạng công ty thông qua đường leased line do ISP cung cấp.

### 3 Thiết kế hệ thống

#### 3.1 Danh sách các thiết bị mạng

##### 3.1.1 Router

Sử dụng 2 loại router: Cisco ISR4321/K9 tại trụ sở chính và MikroTik RB3011 tại 2 chi nhánh.

##### Cisco ISR4321/K9:

- Nhà sản xuất: Cisco Systems, Inc.
- Số hiệu sản phẩm: ISR4321/K9.
- Giá cả tham khảo: 2,370\$
- Đặc tính kỹ thuật:
  - Thông lượng: 50 - 100 Mbps.
  - Tổng số cổng WAN hoặc LAN 10/100/1000 trên bo mạch: 2.
  - Cổng trên RJ-45: 2.
  - Cổng trên SFP: 1.
  - Khe cắm NIM: 2.
  - Khe cắm ISC: 1.
  - Bộ nhớ DRAM: 4 GB (đã cài đặt) / 8 GB (tối đa).
  - Bộ nhớ Flash: 4 GB (đã cài đặt) / 8 GB (tối đa).



- Cổng Serial Console: 1.
- Cổng phụ trợ Serial: 1.
- Tùy chọn nguồn điện: AC, PoE.
- Giao thức hỗ trợ: IPv4, IPv6, static routes, RIP, OSPF, DHCP, IP sec, EIGRP, BGP, IS-IS, IGMPv3, Ethernet, 802.1q VLAN,...
- Tiêu chuẩn: IEEE802.1ag, and IEEE802.3ah.
- Nguồn: AC 100/240 V ( 47-63 Hz)
- Kích thước (WxDxH): 44.55 x 369.57 x 294.64 mm
- Trọng lượng: 3.5 kg

#### MikroTik RB3011:

- Nhà sản xuất: MikroTik, Inc.
- Số hiệu sản phẩm: RB3011UiAS-RM.
- Giá cả tham khảo: 179\$
- Đặc tính kỹ thuật:
  - Thông lượng: 40 - 700 Mbps.
  - Tổng số cổng WAN hoặc LAN 10/100/1000 trên bo mạch: 10.
  - Cổng trên RJ-45: 1.
  - Cổng trên SFP: 1.
  - Bộ nhớ DRAM: 1 GB.
  - Cổng Serial Console: 1.
  - Tùy chọn nguồn điện: PoE.
- Giao thức hỗ trợ: RIP, OSPF, BGP, Dynamic routing, VPN,...
- Nguồn: DC 10-30 V
- Kích thước (WxDxH): 228 x 120 x 30 mm

#### 3.1.2 Switch

##### Switch Layer 3: HPE OfficeConnect 1920S 24G 2SFP Switch

- Nhà sản xuất: Hewlett Packard Enterprise (HPE).
- Số hiệu sản phẩm: JL381A.
- Giá cả tham khảo: 495\$
- Đặc tính kỹ thuật:
  - Tổng số cổng Ethernet 10/100/1000 trên bo mạch: 24.
  - Cổng SFP 100/1000 Mbps: 2.



- 100 Mb Latency < 7.0  $\mu$ s
- 1000 Mb Latency < 2.0  $\mu$ s
- Thông lượng: 38.6 Mpps
- Switching capacity: 52 Gbps
- MAC address table size: 8,000 entries
- Bộ nhớ DRAM: 256 MB.
- Bộ nhớ Flash: 64 MB.
- Packet Buffer: 1.5 MB.
- Tùy chọn nguồn điện: AC.
- Dịch vụ hỗ trợ: IPv4, IPv6, DHCP, NTP, FTP and TFTP, Quality of Service (QoS), IEEE 802.3X Flow Control, PoE+, Access Control Lists (ACLs), RADIUS, Secure Sockets Layer (SSL), IGMP snooping, Spanning Tree Protocol (STP), Address Resolution Protocol (ARP), Static IPv4 routing,...
- Tiêu chuẩn: IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.3ab.
- Nguồn: AC 100/240 V (50/60 Hz)
- Kích thước (WxDxH): 44.25 x 24.61 x 4.39 cm
- Trọng lượng: 2.72 kg

### Switch Layer 2:

- Nhà sản xuất: TP-Link Technologies Co.
- Số hiệu sản phẩm: TL-SG2428P V2.
- Giá cả tham khảo: 247\$
- Đặc tính kỹ thuật:
  - Tổng số cổng Ethernet 10/100/1000 trên bo mạch: 24.
  - Cổng SFP Gigabit: 4.
  - 100 Mb Latency < 7.0  $\mu$ s
  - 1000 Mb Latency < 2.0  $\mu$ s
  - Thông lượng: 41.7 Mpps
  - Switching capacity: 56 Gbps
  - MAC address table size: 8,000 entries
  - Packet Buffer: 4.1 MB.
  - Tùy chọn nguồn điện: AC.
- Dịch vụ hỗ trợ: IPv4, IPv6, DHCP, NTP, FTP and TFTP, Quality of Service (QoS), IEEE 802.3X Flow Control, PoE+, Access Control Lists (ACLs),...
- Tiêu chuẩn: IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3ad, IEEE 802.3x, IEEE 802.3az, IEEE 802.1d, IEEE 802.1s, IEEE 802.1w, IEEE 802.1q, IEEE 802.1p, IEEE 802.1x.
- Nguồn: AC 100/240 V (50/60 Hz)
- Kích thước (WxDxH): 440 × 220 × 44 mm



### 3.1.3 Access-point

- Nhà sản xuất: TP-Link Technologies Co.
- Số hiệu sản phẩm: EAP660 HD.
- Giá cả tham khảo: 220\$
- Đặc tính kỹ thuật:
  - 1 cổng Ethernet 2.5 Gbps (hỗ trợ IEEE802.3at PoE)
  - Khả năng kết nối: 1,000+.
  - Băng tần: 2.4 GHz và 5 GHz
  - Tốc độ tín hiệu: 5 GHz: Up to 2402 Mbps, 2.4 GHz: Up to 1148 Mbps.
- Dịch vụ hỗ trợ: 1024-QAM, 4× Longer OFDM Symbol, OFDMA, Multiple SSIDs (Up to 16 SSIDs, 8 for each band), Enable/Disable Wireless Radio, Automatic Channel Assignment, Transmit Power Control (Adjust Transmit Power on dBm), QoS(WMM), MU-MIMO, Seamless Roaming, Band Steering, Load Balance, Wireless Schedule, Wireless Statistics based on SSID/AP/Client,...
- Chứng chỉ: CE, FCC, RoHS.
- Nguồn: 12V DC.
- Kích thước (WxDxH): 243 × 243 × 64 mm
- Trọng lượng: 2.72 kg

### 3.1.4 Firewall

- Nhà sản xuất: FORTINET.
- Số hiệu sản phẩm: FG-60F.
- Giá cả tham khảo: 1,400\$
- Đặc tính kỹ thuật:
  - GE RJ45 WAN / DMZ Ports: 2/1.
  - GE RJ45 Internal Ports: 5.
  - GE RJ45 FortiLink Ports (Default): 1.
  - USB Ports: 1.
  - Console (RJ45): 1.
  - IPS Throughput: 1.4 Gbps.
  - NGFW Throughput: 1 Gbps.
  - Threat Protection Throughput: 700 Mbps
  - Firewall Latency: 3.3 s.
  - Firewall Throughput: 9 Mpps.



- Dịch vụ hỗ trợ: FortiGuard Security Services (IPS Service, Anti-Malware Protection (AMP), URL, DNS, Video Filtering Service, Anti-Spam, AI-based Inline Malware Prevention Service,...), SD-WAN and SASE Services, NOC and SOC Services, Hardware and Software Support, Base Services.
- Chứng chỉ: FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB.
- Nguồn: 12V DC.
- Kích thước (WxDxH): 38.5 x 216 x 160 mm
- Trọng lượng: 1.01 kg

### 3.1.5 Dự trù kinh phí

STT	Tên sản phẩm	Danh mục	Số lượng	Đơn giá	Thành tiền
1	Cisco ISR4321/K9	Router	1	2,370\$	2,370\$
2	MikroTik RB3011	Router	2	179\$	358\$
3	HPE JL381A	Switch Layer 3	6	495\$	2,970\$
4	TP-Link TL-SG2428P V2	Switch Layer 2	14	247\$	3,458\$
5	TP-Link EAP660 HD	Access-point	3	220\$	660\$
6	Fortinet FortiGate 60F	Firewall	3	1,400\$	4,200\$
	Tổng cộng				14,016\$

## 3.2 Sơ đồ IP

### 3.2.1 Sơ đồ IP trụ sở chính

VLAN	Tầng	Địa chỉ IP định danh	Chi tiết - Miền cung cấp IP
VLAN10	Tầng 1 - Giao dịch	192.168.10.0/24	192.168.10.1->192.168.10.255
VLAN20	Tầng 2 - Chăm sóc khách hàng	192.168.20.0/24	192.168.20.1->192.168.20.255
VLAN30	Tầng 3 - Tài chính	192.168.30.0/24	192.168.30.1->192.168.30.255
VLAN40	Tầng 4 - Tài chính	192.168.40.0/24	192.168.40.1->192.168.40.255
VLAN50	Tầng 5 - Truyền thông	192.168.50.0/24	192.168.50.1->192.168.50.255
VLAN60	Tầng 6 - Kinh doanh	192.168.60.0/24	192.168.60.1->192.168.60.255
VLAN70	Tầng 7 - Quản lý	192.168.70.0/24	192.168.70.1->192.168.70.255
	Wireless	1.1.1.0/24	1.1.1.1->1.1.1.255
	Server	10.10.1.0/24	10.10.1.1->10.10.1.255

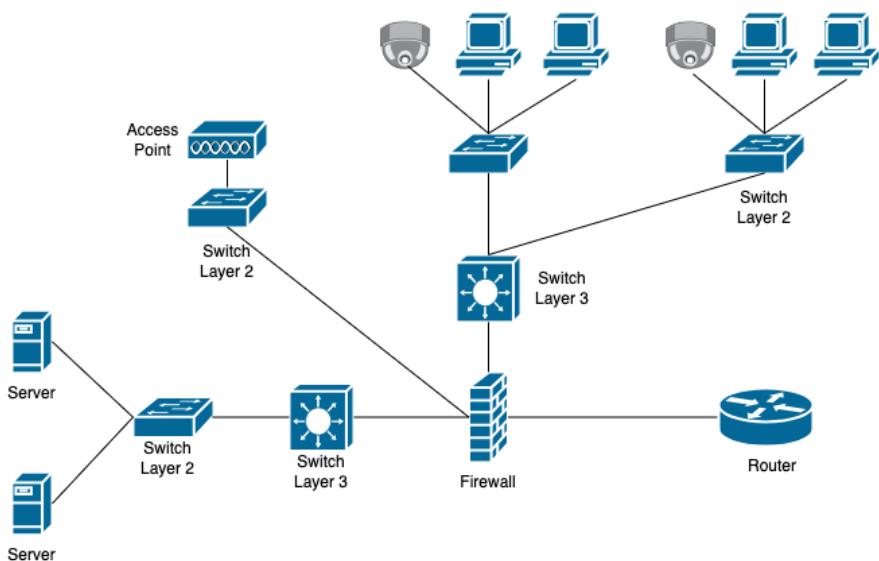
### 3.2.2 Sơ đồ IP chi nhánh Đà Nẵng

VLAN	Tầng - Phòng ban	Địa chỉ IP định danh	Chi tiết - Miền cung cấp IP
VLAN10	Tầng 1 - Giao dịch	182.18.10.0/24	182.18.10.1->182.18.10.255
VLAN20	Tầng 2 - Quản lý	182.18.20.0/24	182.18.20.1->182.18.20.255
	Wireless	2.2.2.0/24	2.2.2.1->2.2.2.255
	Server	20.20.1.0/24	20.20.1.1->20.20.1.255

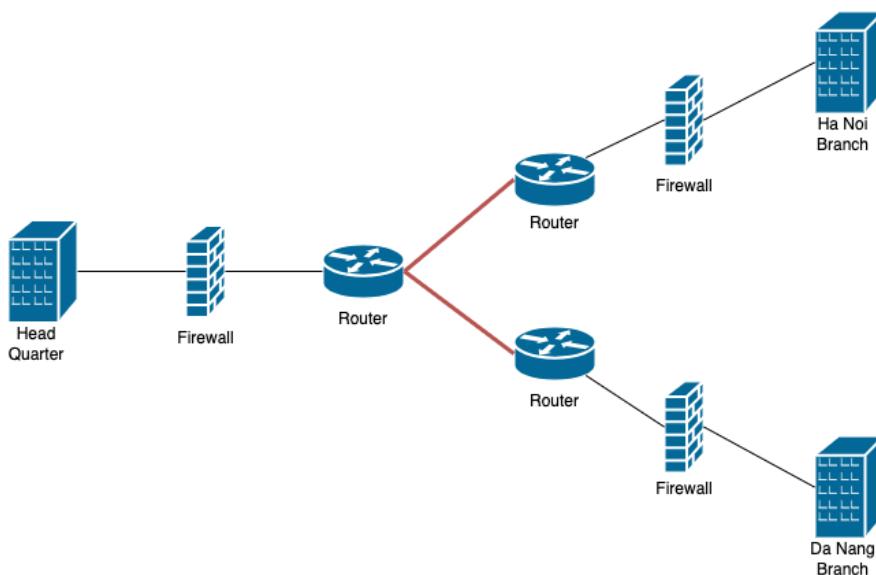
### 3.2.3 Sơ đồ IP chi nhánh Hà Nội

VLAN	Tầng - Phòng ban	Địa chỉ IP định danh	Chi tiết - Miền cung cấp IP
VLAN10	Tầng 1 - Giao dịch	172.17.10.0/24	172.17.10.1->172.17.10.255
VLAN20	Tầng 2 - Quản lý	172.17.20.0/24	172.17.20.1->172.17.20.255
	Wireless	3.3.3.0/24	3.3.3.1->3.3.3.255
	Server	30.30.1.0/24	30.30.1.1->30.30.1.255

### 3.3 Sơ đồ đi dây



Hình 2: Sơ đồ đi dây ở 1 tòa nhà



Hình 3: Sơ đồ đi dây giữa các chi nhánh

## 4 Công nghệ sử dụng

### 4.1 VLAN - Virtual Local Area Network

VLAN hay mạng LAN ảo, là một mạng tuỳ chỉnh, được hình thành từ một hoặc nhiều mạng LAN, cho phép các nhóm thiết bị khả dụng kết nối cùng với một mạng dù không đặt cạnh nhau. VLAN là một kỹ thuật cho phép tạo lập các mạng LAN độc lập một cách logic trên cùng một kiến trúc hạ tầng vật lý.

Ưu điểm của VLAN:

- Tiết kiệm băng thông của mạng: Do VLAN có thể chia nhỏ LAN thành các vùng (vùng quảng bá – broadcast domain). Khi một gói tin quảng bá, nó sẽ lan truyền trong một mạng Vlan duy nhất, không truyền sang các Vlan khác nên tiết kiệm được băng thông đường truyền.
- Tăng khả năng bảo mật: Các VLAN khác nhau không truy cập vào nhau được (ngoại trừ có việc khai báo định tuyến).
- Dễ dàng thêm hay bớt các máy tính vào VLAN nên mạng có tính linh động cao.

### 4.2 VTP - VLAN Trunking Protocol

Giao thức VTP có vai trò duy trì cấu hình của VLAN và đồng nhất trên toàn mạng. VTP là giao thức sử dụng đường trunk để quản lý sự thêm, xóa, sửa các VLAN trên toàn mạng từ switch trung tâm được đặt trong Server mode. VTP hoạt động ở 3 cơ chế:

- Switch ở chế độ VTP Server có thể tạo, chỉnh sửa và xóa VLAN. VTP server lưu cấu hình VLAN trong NVRAM của nó. VTP Server gửi thông điệp ra tất cả các cổng” trunk”.



- Switch ở chế độ VTP client không tạo, sửa và xóa thông tin VLAN. VTP Client có chức năng đáp ứng theo mọi sự thay đổi của VLAN từ Server và gửi thông điệp ra tất cả các cổng “trunk” của nó. VTP Client đồng bộ cấu hình VLAN trong hệ thống.
- Switch ở chế độ transparent sẽ nhận và chuyển tiếp các thông điệp quảng bá VTP do các switch khác gửi đến mà không quan tâm đến nội dung của các thông điệp này. Nếu “transparent switch” nhận thông tin cập nhật VTP nó cũng không cập nhật vào cơ sở dữ liệu của nó; đồng thời nếu cấu hình VLAN của nó có gì thay đổi, nó cũng không gửi thông tin cập nhật cho các switch khác. Trên “transparent switch” chỉ có một việc duy nhất là chuyển tiếp thông điệp VTP. Switch hoạt động ở “transparent-mode” chỉ có thể tạo ra các VLAN cục bộ. Các VLAN này sẽ không được quảng bá đến các switch khác.

Ưu điểm của VTP:

- Tiết kiệm thời gian cài đặt, quản lý các switch.
- Dễ dàng thêm, bớt hay chỉnh sửa các VLAN trên mạng.

### 4.3 OSPF - Open Shortest Path First

Giao thức Open Shortest Path First (OSPF) được định nghĩa trong RFC 2328, là một giao thức định tuyến trong (IGP) được sử dụng để phân phối thông tin định tuyến trong một AS (Autonomous System). OSPF là một giao thức định tuyến link – state điển hình. Mỗi router khi chạy giao thức sẽ gửi các trạng thái đường link của nó cho tất cả các router trong vùng (area). Sau một thời gian trao đổi, các router sẽ đồng nhất được bảng cơ sở dữ liệu trạng thái đường link (Link State Database – LSDB) với nhau, mỗi router đều có được bản đồ mạng của cả vùng. Từ đó mỗi router sẽ chạy giải thuật Dijkstra tính toán ra một cây đường đi ngắn nhất (Shortest Path Tree) và dựa vào cây này để xây dựng nên bảng định tuyến.

Ưu điểm của OSPF:

- OSPF sử dụng gói tin multicast để gửi cập nhật trạng thái đường link. Cập nhật chỉ được gửi trong trường hợp có thay đổi định tuyến xảy ra thay vì cập nhật định kỳ. Điều này đảm bảo sử dụng băng thông tốt hơn.
- Mỗi router đều có một sơ đồ đầy đủ và đồng bộ về toàn bộ cấu trúc hệ thống mạng. Do đó chúng rất khó để lặp vòng.
- Mọi router sử dụng sơ đồ cấu trúc mạng của riêng nó để chọn đường. Đặc tính này sẽ giúp chúng ta khi cần xử lý sự cố.
- Giao thức định tuyến theo trạng thái đường liên kết hỗ trợ VLSM và CIDR.

### 4.4 DHCP - Dynamic Host Configuration Protocol

DHCP có nhiệm vụ giúp quản lý nhanh, tự động và tập trung việc phân phối địa chỉ IP bên trong một mạng. Ngoài ra DHCP còn giúp đưa thông tin đến các thiết bị hợp lý hơn cũng như việc cấu hình subnet mask hay cổng mặc định. Giao thức này được thiết kế để giảm thời gian chỉnh cấu hình cho mạng TCP/IP bằng cách tự động gán các địa chỉ IP cho các máy tính khi chúng vào mạng. Ta nên sử dụng DHCP cho mô hình mạng có nhiều máy không cố định (Wifi) hoặc với số lượng máy lớn mà việc chia IP bằng tay là rất khó khăn, phức tạp.

Ưu điểm:



- DHCP tự động quản lý các địa chỉ IP và loại bỏ được các lối trùng lặp.
- Dễ dàng theo dõi và quản lý mạng.
- Người quản lý có thể thay đổi cấu hình và thông số của các địa chỉ IP giúp việc nâng cấp cơ sở hạ tầng được dễ dàng hơn.

Nhược điểm:

- DHCP cho thuê địa chỉ trong một khoảng thời gian, nên các địa chỉ này sẽ còn được dùng cho hệ thống khác.

## 4.5 Site-to-Site IPsec VPN

VPN Site-to-Site là công cụ thường được sử dụng bởi các công ty có nhiều văn phòng ở các vị trí địa lý khác nhau cần truy cập và sử dụng mạng công ty liên tục. Với VPN site-to-site, một công ty có thể kết nối an toàn mạng công ty của mình với các văn phòng từ xa để giao tiếp và chia sẻ tài nguyên như một mạng duy nhất. Một cách hiểu khá đơn giản, 1 kết nối VPN kết nối 2 mạng nội bộ (mạng LAN - Local Area Network) với nhau thì được gọi là 1 kết nối VPN site to site.

Bộ giao thức IPsec là 1 trong những bộ giao thức chuẩn được sử dụng chủ yếu trong các kết nối VPN site to site. IPsec (Internet Protocol Security) là một bộ giao thức dùng để xác thực và mã hóa các gói dữ liệu truyền trên internet. IPsec bao gồm các giao thức để 2 đầu VPN gateway xác thực lẫn nhau lúc khởi tạo kết nối và đảm phán việc sử dụng khóa mã hóa trong suốt quá trình truyền dữ liệu sau đó. Dữ liệu truyền trên đường truyền sẽ đảm bảo an toàn và bảo mật bằng các thuật toán mã hóa và xác thực khác nhau.

# 5 Tính toán các thông số cho mạng máy tính

## 5.1 Một số khái niệm liên quan đến hiệu suất mạng

### 5.1.1 Băng thông - Bandwidth

Băng thông (bandwidth) là độ rộng của kênh truyền tải dữ liệu mà mạng có thể chứa được trong một khoảng thời gian nhất định. Đơn vị đo của bandwidth thường là bit trên giây (bps), byte trên giây (Bps), kilobit trên giây (Kbps), megabit trên giây (Mbps), gigabit trên giây (Gbps) và terabit trên giây (Tbps). Băng thông càng lớn thì khả năng truyền tải dữ liệu càng nhanh, do đó, việc có một băng thông lớn sẽ đảm bảo rằng người dùng có thể truyền tải dữ liệu với tốc độ cao hơn.

Công thức tính băng thông:

$$\text{bandwidth} = \frac{\text{số bit được truyền tải trong một giây}}{\text{thời gian truyền tải}}$$

### 5.1.2 Thông lượng - Throughput

Thông lượng (throughput) là số lượng dữ liệu thực sự được truyền tải qua mạng trong một đơn vị thời gian cụ thể, thường là giây. Đơn vị đo của throughput thường là bit trên giây (bps), byte trên giây (Bps), kilobit trên giây (Kbps), megabit trên giây (Mbps), gigabit trên giây (Gbps) và terabit trên giây (Tbps). Nó thể hiện tốc độ thực tế của truyền tải dữ liệu mà mạng có thể đảm bảo.

Công thức tính băng thông:

$\text{throughput} = (\text{số bit được truyền tải thành công trong một đơn vị thời gian}) / (\text{thời gian truyền tải} + \text{thời gian xử lý})$

## 5.2 Trụ sở chính

Tổng thời gian vào giờ cao điểm là 3 giờ (9-11h, 15-16h).

Tổng dung lượng cho các server:  $1000 * 5 = 5000 \text{ MB/ngày}$ .

Tổng dung lượng cho các workstation:  $500 * 200 = 100000 \text{ MB/ngày}$ .

Tổng dung lượng cho các thiết bị không dây khoảng:  $1000\text{MB/ngày}$ .

$$\text{Bandwidth} = \frac{(5000 + 100000 + 1000) \times 0.8}{3 \times 3600} \times 8 = 62.814(\text{Mbps})$$

$$\text{Throughput} = \frac{(5000 + 100000 + 1000)}{24 \times 3600} \times 8 = 9.814(\text{Mbps})$$

## 5.3 Chi nhánh

Tổng thời gian vào giờ cao điểm là 3 giờ (9-11h, 15-16h).

Tổng dung lượng cho các server:  $1000 * 3 = 3000 \text{ MB/ngày}$ .

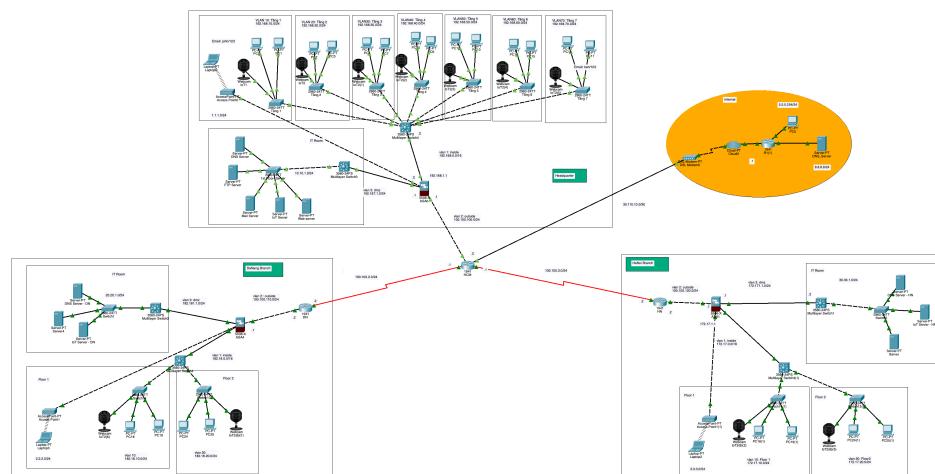
Tổng dung lượng cho các workstation:  $500 * 30 = 15000 \text{ MB/ngày}$ .

Tổng dung lượng cho các thiết bị không dây khoảng:  $1000\text{MB/ngày}$ .

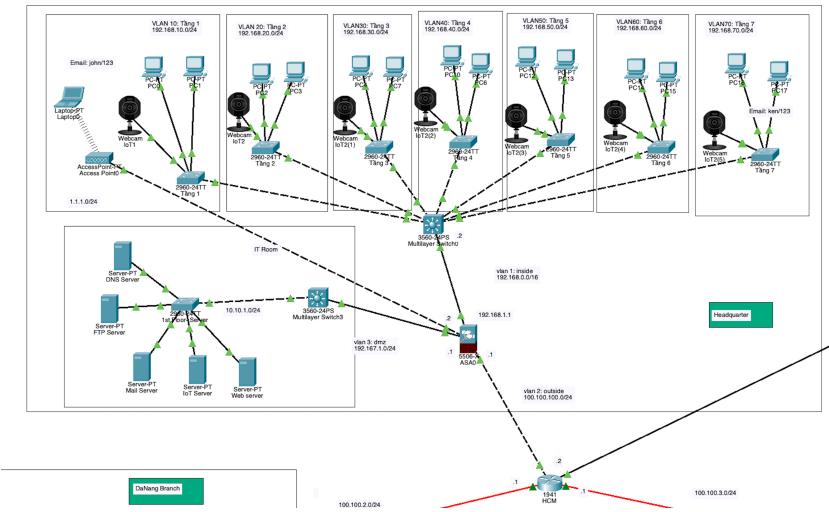
$$\text{Bandwidth} = \frac{(3000 + 15000 + 1000) \times 0.8}{3 \times 3600} \times 8 = 11.259(\text{Mbps})$$

$$\text{Throughput} = \frac{(3000 + 15000 + 1000)}{24 \times 3600} \times 8 = 1.759(\text{Mbps})$$

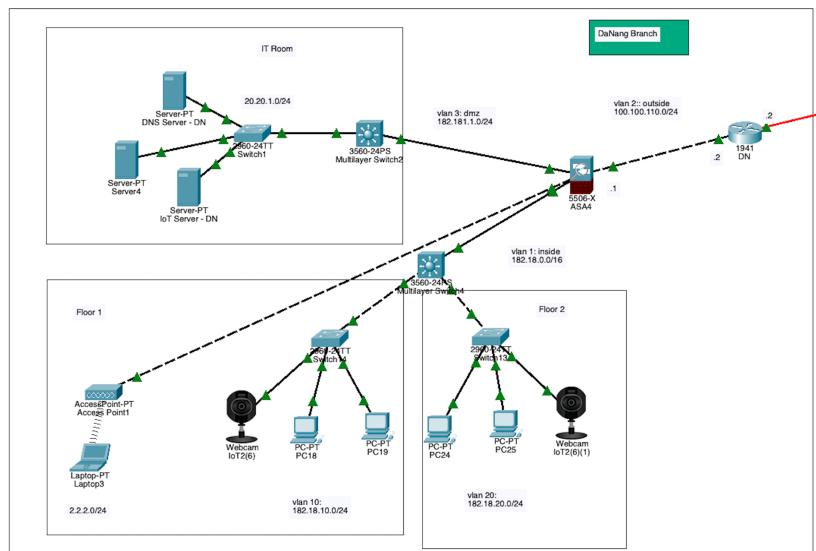
# 6 Thiết kế hệ thống mạng sử dụng Cisco Packet Tracer



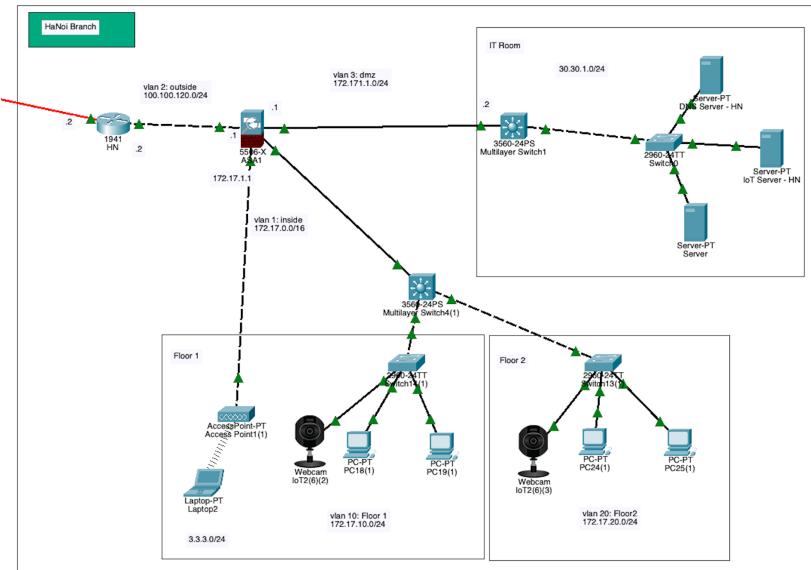
Hình 4: Thiết kế mạng



Hình 5: Thiết kế mạng ở trụ sở chính



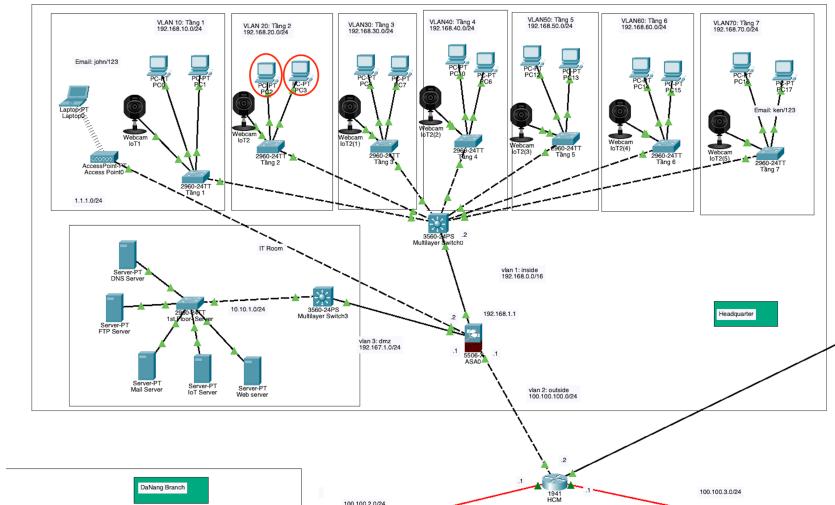
Hình 6: Thiết kế mạng ở chi nhánh Đà Nẵng



Hình 7: Thiết kế mạng ở chi nhánh Hà Nội

## 7 Kiểm thử kết quả

### 7.1 Trong cùng VLAN



Hình 8: Ping trong cùng VLAN

```
C:\>ping 192.168.20.3

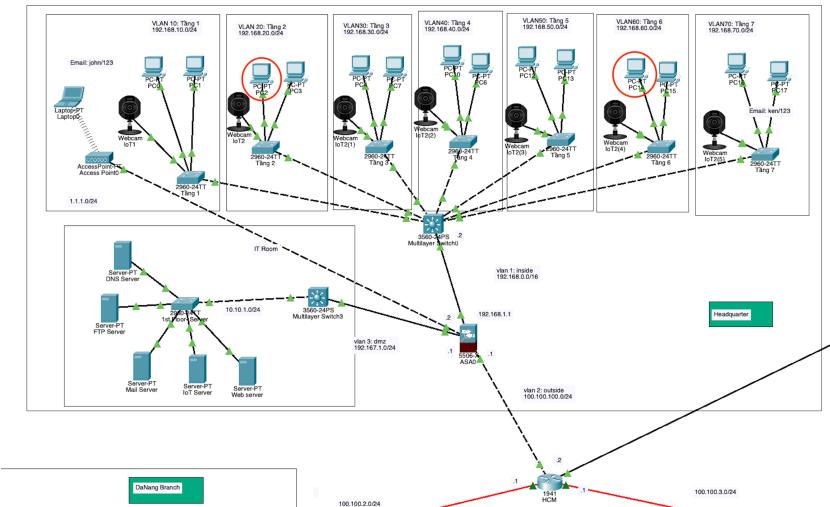
Pinging 192.168.20.3 with 32 bytes of data:

Reply from 192.168.20.3: bytes=32 time=3ms TTL=128
Reply from 192.168.20.3: bytes=32 time=19ms TTL=128
Reply from 192.168.20.3: bytes=32 time<1ms TTL=128
Reply from 192.168.20.3: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 19ms, Average = 6ms
```

Hình 9: Kết quả ping trong cùng VLAN

## 7.2 Giữa các VLAN



Hình 10: Ping giữa các VLAN

```
C:\>ping 192.168.60.3

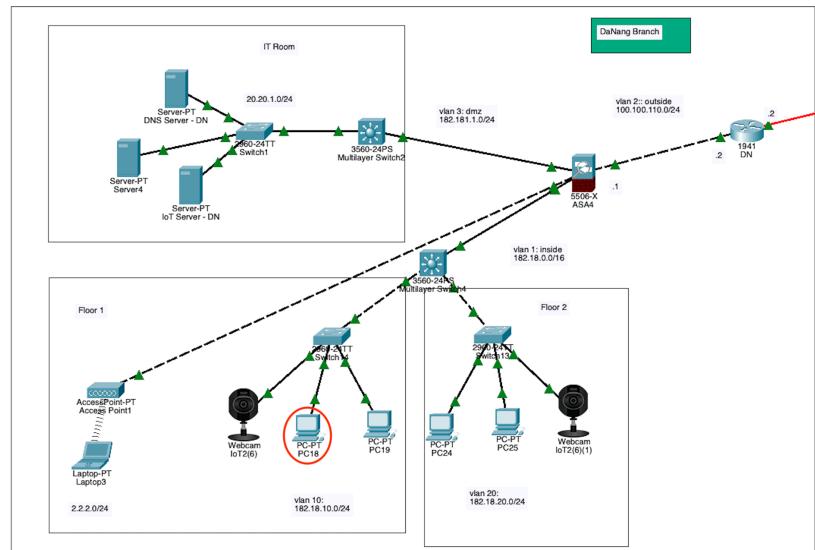
Pinging 192.168.60.3 with 32 bytes of data:

Reply from 192.168.60.3: bytes=32 time=36ms TTL=127
Reply from 192.168.60.3: bytes=32 time<1ms TTL=127
Reply from 192.168.60.3: bytes=32 time<1ms TTL=127
Reply from 192.168.60.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.60.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 36ms, Average = 9ms
```

Hình 11: Kết quả ping giữa các VLAN

### 7.3 Giữa chi nhánh và trụ sở chính



Hình 12: Ping giữa chi nhánh và trụ sở chính



```
C:\>ping 182.18.10.3

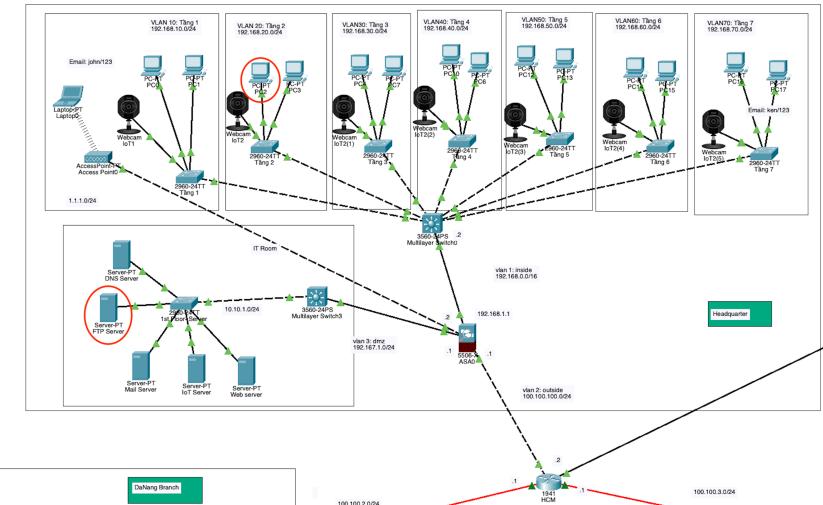
Pinging 182.18.10.3 with 32 bytes of data:

Reply from 182.18.10.3: bytes=32 time=3ms TTL=122
Reply from 182.18.10.3: bytes=32 time=2ms TTL=122
Reply from 182.18.10.3: bytes=32 time=1ms TTL=122
Reply from 182.18.10.3: bytes=32 time=2ms TTL=122

Ping statistics for 182.18.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

Hình 13: Kết quả ping giữa chi nhánh và trụ sở chính

#### 7.4 Kết nối với server trong vùng DMZ



Hình 14: Kết nối với server trong vùng DMZ

```
C:\>ping 10.10.1.2

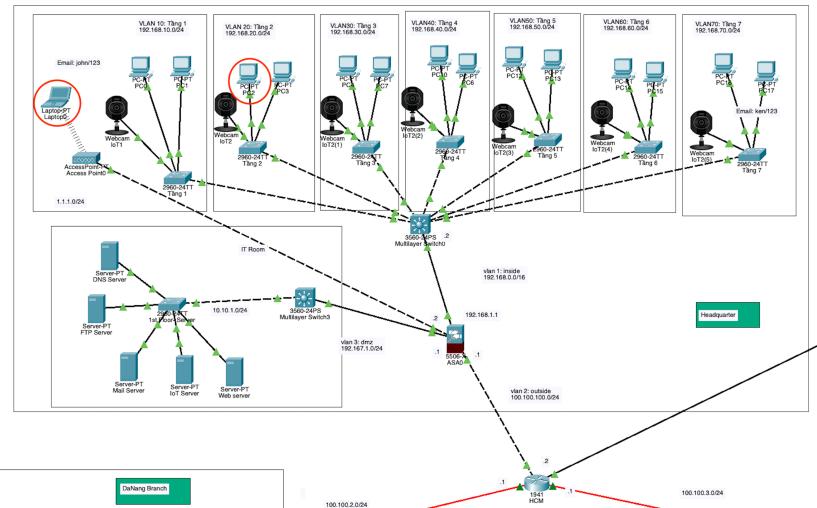
Pinging 10.10.1.2 with 32 bytes of data:

Reply from 10.10.1.2: bytes=32 time<1ms TTL=125

Ping statistics for 10.10.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Hình 15: Kết nối với server trong vùng DMZ

## 7.5 Kết nối giữa mạng Customer và LAN



Hình 16: Kết nối giữa mạng Customer và LAN



```
C:\>ping 192.168.20.2

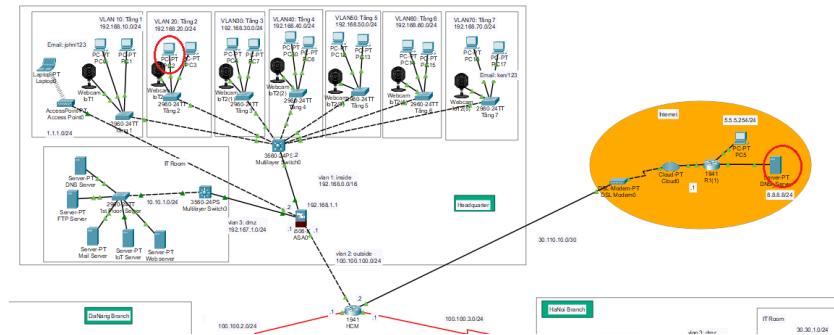
Pinging 192.168.20.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

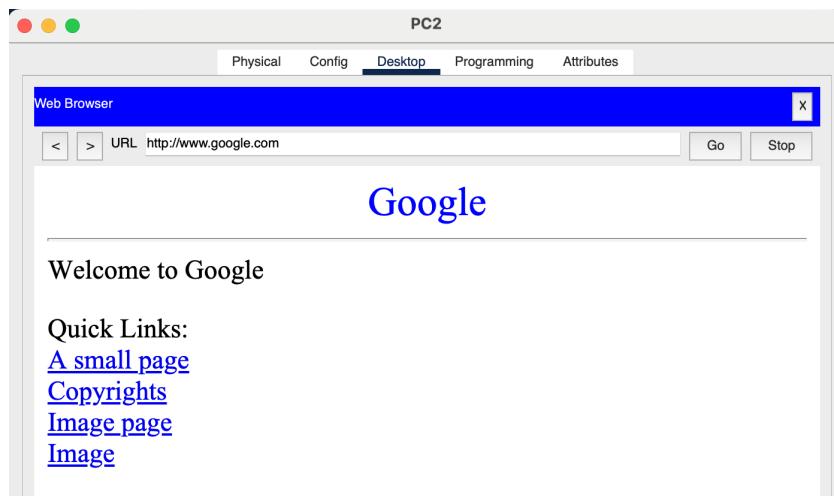
Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Hình 17: Kết nối giữa mạng Customer và LAN3

## 7.6 Kết nối tới một Web server ở ngoài Internet

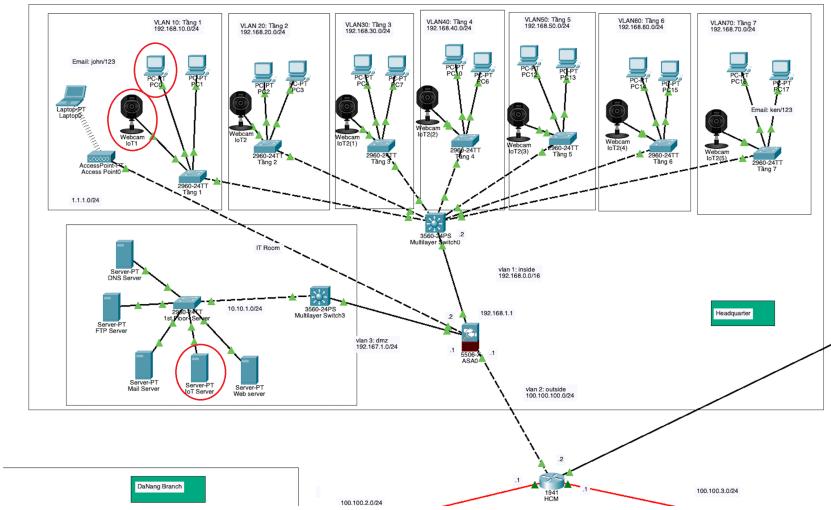


Hình 18: Kết nối tới một Web server ở ngoài Internet

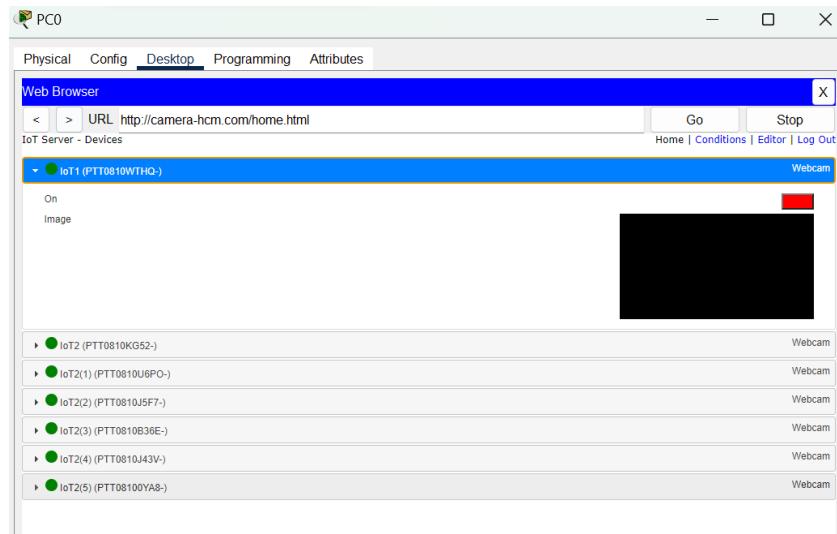


Hình 19: Kết nối tới một Web server ở ngoài Internet

## 7.7 Hệ thống Camera giám sát



Hình 20: Hệ thống Camera giám sát



Hình 21: Hệ thống Camera giám sát

## 8 Bảo mật hệ thống

### 8.1 Sử dụng WiFi Protected Access (WPA-2)

WiFi Protected Access (WPA) là một chuẩn bảo mật được sử dụng trong mạng WiFi. WPA được sử dụng để tránh khỏi sự dòm ngó của các hacker và nhằm đảm bảo chỉ những người được



chỉ định mới có thể truy cập vào WiFi.

Một chuẩn bảo mật đầu tiên trước WPA đó là WEP, tuy nhiên WEP được cho là không an toàn vì khóa bí mật dùng để mã hóa chỉ có độ dài là 40 bit, các hacker đã sử dụng thuật toán vét cạn để tìm ra khóa bí mật trong thời gian không quá dài.

WPA có những tính chất sau:

- Dynamic: WPA sử dụng mật khẩu động để mã hóa, tức khóa bí mật sẽ thay đổi sau mỗi phiên đăng nhập.
- Authenticity: WPA có cơ chế xác thực danh tính người dùng để đảm bảo chỉ những người được chỉ định mới có thể truy cập vào WiFi.
- Maximum encryption: WPA sử dụng cơ chế mã hóa AES (Advanced Encryption Standard) là một hệ mật mã sử dụng 1 khóa duy nhất để mã hóa và giải mã (chi phí cao và độ bảo mật cao).

Hiện thì WPA cũng đã không còn an toàn trước công nghệ của hacker, nên WPA-2 ra đời. WPA-2 sử dụng mã hóa đối xứng AES (Advanced Encryption Standard) (sử dụng duy nhất một khóa cho việc mã hóa và giải mã). Cho đến hiện tại, hacker không thể tìm ra key trong thời gian hợp lý được, vì mã hóa đối xứng có độ bảo mật hiệu quả đối với các loại tấn công vét cạn.

## 8.2 Sử dụng Hardware-based Firewall

Firewall nhìn chung sẽ bao gồm 2 loại:

- Hardware-based firewall: Căn bản là một thiết bị riêng biệt, được lắp đặt để kiểm soát các gói tin ra vào khi đi qua firewall. Có tác dụng bảo vệ cho toàn bộ một network.
- Host-based firewall: là một phần mềm được cài đặt trên máy tính (PC, Laptop, ...) có tác dụng chỉ để bảo vệ một máy tính khỏi các luồng gói tin trái phép xâm nhập vào

Ưu điểm của Hardware-based firewall:

- Tốc độ: Tường lửa phần cứng được thiết kế cho thời gian phản hồi nhanh hơn, do đó, nó có thể xử lý nhiều lưu lượng truy cập hơn.
- Bảo mật: Tường lửa có hệ điều hành riêng ít bị tấn công hơn. Điều này lần lượt làm giảm nguy cơ bảo mật và ngoài ra, tường lửa phần cứng có các điều khiển bảo mật nâng cao.
- Không có nhiễu: Vì tường lửa phần cứng là một thành phần mạng bị cô lập, nó có thể được quản lý tốt hơn và không tái hoặc làm chậm các ứng dụng khác. Tường lửa có thể được di chuyển, tắt máy hoặc cấu hình lại với sự can thiệp tối thiểu vào mạng.

# 9 Đánh giá hệ thống

## 9.1 Những điều đạt được

- Làm quen với phần mềm Cisco Packet Tracer, đồng thời tìm hiểu được các giải pháp thiết kế về phần cứng, cũng như cách cấu hình cho thiết bị mạng. Nhóm đã có khả năng thiết kế được một hệ thống mạng có quy mô vừa hoặc nhỏ. Thiết kế mô hình mạng cho công ty bao gồm mô hình IP và mô hình đi dây.



- Hệ thống mạng đáp ứng tương đối phù hợp với yêu cầu đưa ra, có khả năng nâng cấp phù hợp với sự phát triển sau này.
- Các trang thiết bị được lựa chọn phù hợp với nhu cầu và kinh phí. Sử dụng những trang thiết bị chính hãng, trong thời hạn hỗ trợ.
- Băng thông lớn, đáp ứng đầy đủ nhu cầu của nhân viên làm việc trong công ty.
- Mô hình mạng mô hình Server-Client và Topo cây nhằm giảm thiểu các ảnh hưởng của mạng con với nhau, đồng thời đảm bảo chúng có thể giao tiếp hiệu quả.
- Chia VLAN cho các phòng ban của trụ sở chính và chi nhánh.
- Thực hiện kết nối ra Internet, kết nối giữa trụ sở và chi nhánh.
- Định tuyến cho các router.
- Cấu trúc mạng đơn giản. Giúp cho thuật toán được điều khiển một cách ổn định hơn (ví dụ như thuật toán Dijkstra trong Cấu hình định tuyến động OSPF).
- Đã làm được một số tính năng về bảo mật.
- Sử dụng OSPF để kết nối các router.

## 9.2 Những hạn chế

- Chưa có kiến thức về một mạng ngân hàng/doanh nghiệp cụ thể, khi thiết kế gấp khó khăn về việc quyết định các mô hình, công nghệ, thiết bị nên được sử dụng.
- Chưa có nhiều kiến thức về vấn đề bảo mật và sự cố.
- Mặc dù có khả năng mở rộng mạng, nhưng điều này hoàn toàn phụ thuộc vào khả năng hoạt động của bộ phận trung tâm. Một khi trung tâm gặp phải sự cố (switch tổng hoặc router tổng), toàn bộ hệ thống mạng sẽ không thể hoạt động.
- Chưa thực hiện cấu hình cân bằng tải tại các bottleneck, dễ gây tắc nghẽn nếu lượng truy cập tăng đột biến.
- Việc phân chia các subnet còn nhiều bất cập, chưa phù hợp với điều kiện thực tế.

## 9.3 Định hướng phát triển trong tương lai

Trong tương lai, công ty sẽ phát triển và mở rộng phạm vi hoạt động ra nhiều địa điểm khác. Do đó, việc tính đến sự mở rộng của hệ thống mạng giữa trụ sở và các chi nhánh với nhau là rất quan trọng.

Đối với vấn đề băng thông, khi cần nâng cấp thì chỉ cần đăng ký thay đổi gói cước với nhà cung cấp dịch vụ. Hơn nữa, trong hệ thống mạng thiết kế chưa có giải pháp cân bằng tải (Network Load Balancing) - vậy nên trong tương lai thì mô hình có thể thiết kế thêm hệ thống cân bằng tải, nhằm giúp cho việc phân bổ đồng đều lưu lượng truy cập giữa các máy chủ có cùng chức năng.

Đối với vấn đề bảo mật của mô hình trong tương lai, mô hình có thể phát triển thêm về hệ thống tường lửa cục bộ cho cả trụ sở và các chi nhánh. Đồng thời thiết kế 1 hệ thống ngăn chặn việc khách hàng sử dụng wifi truy cập vào hệ thống mạng LAN hiệu quả hơn việc ngăn chặn trên Firewall.



## 10 Tài liệu tham khảo

1. <https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-router-data-sheet-c78-732542.html>
2. [https://i.mt.lv/cdn/product\\_files/RB3011-RM\\_210522.pdf](https://i.mt.lv/cdn/product_files/RB3011-RM_210522.pdf)
3. [https://www.hpe.com/psnow/doc/a00001630enw?jumpid=in\\_lit-psnow-red](https://www.hpe.com/psnow/doc/a00001630enw?jumpid=in_lit-psnow-red)
4. <https://www.tp-link.com/vn/business-networking/smart-switch/tl-sg2428p/v2/#specifications>
5. <https://www.tp-link.com/vn/business-networking/omada-wifi-ceiling-mount/eap620-hd/#specifications>