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

Báo cáo bài tập lớn 2

Chủ đề: Thiết kế mạng máy tính

Tên thành viên	MSSV
Nguyễn Đinh Bằng	2210298
Trần Thanh Bình	2210335

TP Hồ Chí Minh, Tháng 12 Năm 2024

Mục lục

1 Phân tích yêu cầu và thiết kế kiến trúc mạng phù hợp

1.1 Phân tích yêu cầu hệ thống mạng của Headquarters và Branches

1.1.1 Headquarters

- Quy mô: Tòa nhà 7 tầng.
- Các thiết bị:
  - 120 máy trạm được phân bố trong các phòng ban khác nhau.
  - 5 server phục vụ các ứng dụng doanh nghiệp (Web, Database, File Sharing,...).
  - 12 thiết bị mạng trở lên, bao gồm Switch, Router, Firewall, Access Point.
  - Hỗ trợ cả kết nối có dây và không dây.
  - Công nghệ: GPON, GigaEthernet (1GbE/10GbE), Wi-Fi chuẩn mới (Wi-Fi 6).
  - VLAN: Phân chia VLAN theo phòng ban và loại người dùng.
  - Yêu cầu tích hợp các giải pháp bảo mật như DMZ, Firewall, IPS/IDS.
  - Đề xuất cấu hình VPN cho kết nối site-to-site và hệ thống camera giám sát cho công ty.

1.1.2 Branches

- Quy mô: Tòa nhà 2 tầng.
- Các thiết bị:
  - 30 máy trạm tại mỗi chi nhánh.
  - 3 server tại mỗi chi nhánh để xử lý dữ liệu nội bộ.
  - 5 thiết bị mạng trở lên.
  - Hỗ trợ kết nối Wi-Fi cho khách hàng và nhân viên.
  - Kết nối với Headquarters thông qua SD-WAN hoặc MPLS...

1.2 Checklist khảo sát tại các vị trí cài đặt

Table 1: Checklist khảo sát tại các vị trí cài đặt

Tiêu chí khảo sát	**Headquarters**	**Branches**
Diện tích và sơ đồ tòa nhà	Xác định vị trí phòng IT, cabling central, các tầng.	Xác định IT room và hệ thống cáp.
Số lượng người dùng	120 máy trạm, chia theo các phòng ban.	30 máy trạm, chia theo khu vực làm việc.
Camera	1 Camera cho mỗi tầng, tầng 1 được bố trí 2 camera.	1 Camera cho mỗi tầng, tầng 1 được bố trí 2 camera.
Vị trí cài đặt thiết bị mạng	Switch Layer 2 ở từng tầng, Core Switch tại IT room.	Core Switch tại tầng IT room.
Khả năng mở rộng tương lai	Dự trù mở rộng 20% trong 5 năm.	Dự trù mở rộng 20% trong 5 năm.
Tải mạng dự kiến	Cao nhất vào 9-11h và 15-16h (80% tải).	Mức tải thấp hơn HQ, chủ yếu là giao dịch nội bộ.
Cấu trúc dây mạng (Cabling)	Hỗ trợ cáp quang (GPON) và Ethernet (Cat6A).	Hỗ trợ Ethernet (Cat6A).
Bảo mật	Yêu cầu Firewall, IPS/IDS, DMZ.	Firewall cơ bản và VPN kết nối HQ.
Kết nối không dây (Wi-Fi)	Yêu cầu AP Wi-Fi chuẩn Wi-Fi 6 cho khách và nhân viên.	Yêu cầu AP Wi-Fi cho khách và nhân viên.

1.3 Xác định các khu vực có tải cao và thiết bị phù hợp

Headquarters

- **Khu vực tải cao:**
  - Phòng IT: Chứa các server, thiết bị mạng chính (Core Switch, Router, Firewall).
  - Phòng ban kinh doanh và tài chính: Tải giao dịch cao trong giờ làm việc (9-11h và 15-16h).
- **Thiết bị phù hợp:**
  - Load Balancer: Đặt tại IT room, quản lý tải giữa các server nội bộ.
  - Core Switch Layer 3: Quản lý định tuyến và phân luồng mạng.
  - Access Points (APs): Đặt tại mỗi tầng, hỗ trợ nhiều thiết bị kết nối không dây.
  - Router: Kết nối WAN đến các branch.

Branches

- **Khu vực tải cao:**
  - IT room (nơi đặt server).
  - Khu vực giao dịch khách hàng.
- **Thiết bị phù hợp:**
  - Switch Layer 3 để kết nối máy trạm.
  - Router kết nối WAN và VPN tới Headquarters.

1.4 Lựa chọn cấu trúc mạng phù hợp với kiến trúc tòa nhà

Headquarters

- **Mạng có dây:**
  - Sử dụng cấu trúc Star Topology:
    - Một Core Switch Layer 3 đặt tại IT room.
    - Switch Layer 2 đặt tại mỗi tầng, kết nối với Core Switch qua cáp quang (GPON).
  - Kết nối máy trạm bằng cáp Ethernet Cat6A.

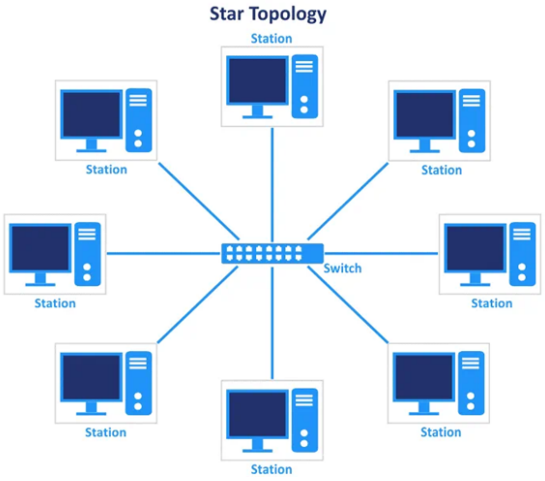


Figure 1: Cấu trúc Star Topology

- **Mạng không dây:**
  - Sử dụng các Access Points Wi-Fi chuẩn Wi-Fi 6.
  - Các AP được kết nối về Core Switch bằng cáp Ethernet hỗ trợ PoE.
- **Kiến trúc:**
  - Dây cáp và thiết bị được đặt trong cable management rack để đảm bảo tính thẩm mỹ và dễ bảo trì.

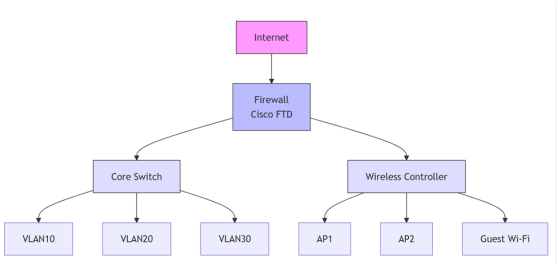
Branches

- **Mạng có dây:**
  - Sử dụng cấu trúc tương tự Headquarters nhưng đơn giản hơn:
    - Một Switch Layer 3 tại IT room.
    - Các máy trạm kết nối trực tiếp tới Switch qua Ethernet Cat6A.
- **Mạng không dây:**
  - Access Points Wi-Fi được đặt tại khu vực giao dịch khách hàng và phòng làm việc.

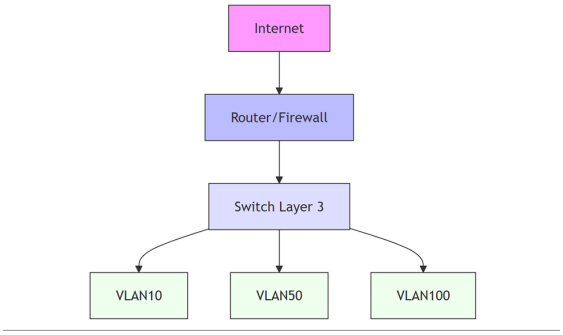
1.5 Thiết kế mạng trong môi trường không dây và bảo mật

1.5.1 Phân chia VLAN và phân vùng mạng

- **Headquarters VLAN:**
  - VLAN 10: IT Department (Quản trị mạng và server farm).
  - VLAN 20: Finance Department.
  - VLAN 30: HR Department.
  - VLAN 40: Marketing Department.
  - VLAN 50: Server Farm.
  - VLAN 60: DMZ (dành cho server cung cấp dịch vụ công khai như Web Server).
  - VLAN 100: Guest Wi-Fi (cách ly với mạng nội bộ).



- **Branches VLAN:**
  - VLAN 10: IT Department, gồm các máy trạm, access point và server.
  - VLAN 50: Tầng 2, bao gồm các máy trạm, access point.
  - VLAN 100: Guess wifi.



1.5.2 Thiết lập DMZ và Firewall

- **DMZ:**
  - Đặt các server công khai (Web Server, Mail Server) trong VLAN DMZ, tách biệt với mạng nội bộ.
- **Firewall:**

  - Triển khai Cisco Firepower Firewall:
    * Chặn các truy cập trái phép từ Internet.
    * Cấu hình NAT để cấp quyền truy cập tới DMZ.

- **IPS/IDS:**
  - Phát hiện và ngăn chặn các tấn công mạng.

1.5.3 Cấu hình Wi-Fi an toàn

- **SSID riêng biệt:**
  - SSID cho nhân viên (mã hóa WPA3).
  - SSID cho khách hàng (với VLAN Guest, cách ly hoàn toàn với mạng nội bộ).
- **AP Management:**
  - Sử dụng controller để quản lý các Access Points (Cisco Wireless Controller).

2 Danh sách thiết bị tối thiểu, IP Plan, và Wiring Diagram

2.1 Danh sách thiết bị tối thiểu và thông số kỹ thuật

2.1.1 Headquarters

Thiết bị	Số lượng	Mô tả/Thông số kỹ thuật đề xuất
Core Switch Layer 3	1	Cisco Catalyst 9500: Hỗ trợ 1GbE/10GbE, 48 port uplink, hỗ trợ routing OSPF, VLAN.
Switch Layer 2	7	Cisco Catalyst 9200: Hỗ trợ 1GbE, PoE (Power over Ethernet) để cấp nguồn cho Access Points.
Router	1	Cisco ISR 4451-X: Hỗ trợ SD-WAN, VPN IPSec, băng thông WAN tối thiểu 500 Mbps.
Firewall	1	Cisco Firepower 1010 hoặc Fortinet FG-100F: Hỗ trợ NGFW, IPS/IDS, VPN, High Availability.
Access Point (AP)	7	Cisco Aironet 2800: Hỗ trợ Wi-Fi 6, dual-band, roaming, VLAN tagging.
Load Balancer	1	F5 BIG-IP hoặc tương đương: Quản lý tải giữa các server nội bộ.
Server	5	Dell PowerEdge R740: Hỗ trợ 2 CPU, 256GB RAM, RAID 5, card mạng 10GbE.
Patch Panel	2	Patch Panel 24 port Cat6A để tổ chức dây cáp mạng trong IT room.
UPS	1	APC Smart-UPS 5000VA: Đảm bảo nguồn dự phòng cho thiết bị mạng và server.
Cable (Ethernet Cat6A)	500m+	Dây cáp mạng Cat6A hỗ trợ tốc độ 10GbE, chiều dài tùy thuộc vào khoảng cách giữa các tầng.
Fiber Optic Cable (GPON)	300m+	Cáp quang multi-mode (MMF), hỗ trợ tốc độ 10Gbps, kết nối Core Switch với Switch tầng.
Camera	8	Mỗi camera có độ phân giải Full HD (1080p) và nén H.265

2.1.2 Branches (mỗi chi nhánh)

Thiết bị	Số lượng	Mô tả/Thông số kỹ thuật đề xuất
Switch Layer 3	1	Cisco Catalyst 9300: Hỗ trợ VLAN, routing OSPF, uplink quang.
Access Point (AP)	2	Cisco Aironet 2800: Hỗ trợ Wi-Fi 6, dual-band, roaming, VLAN tagging.
Router	1	Cisco ISR 1100 Series: Hỗ trợ SD-WAN, VPN IPSec, băng thông WAN tối thiểu 100 Mbps.
Firewall nhỏ	1	Cisco Firepower 1010 hoặc Fortinet FG-60F.
Server	3	Dell PowerEdge R340: Hỗ trợ 1 CPU, 64GB RAM, RAID 5, card mạng 1GbE.
Patch Panel	1	Patch Panel 12 port Cat6A để tổ chức dây cáp mạng.
UPS	1	APC Smart-UPS 1500VA: Đảm bảo nguồn dự phòng.
Cable (Ethernet Cat6A)	100m+	Dây cáp mạng Cat6A hỗ trợ tốc độ 1GbE, cho máy trạm và AP.
Camera	3	Mỗi camera có độ phân giải Full HD (1080p) và nén H.265

2.2 IP Plan

2.2.1 Headquarters IP Plan

- Mạng nội bộ:
  - VLAN 10 (IT Department): 192.168.10.0/24 (120 máy trạm, subnet mask 255.255.255.0).
  - VLAN 20 (Finance Department): 192.168.20.0/24 (30 máy trạm).
  - VLAN 30 (HR Department): 192.168.30.0/24 (30 máy trạm).
  - VLAN 40 (Marketing Department): 192.168.40.0/24 (30 máy trạm).
  - VLAN 50 (Server Farm): 192.168.50.0/24 (5 server).
  - VLAN 60 (DMZ): 192.168.60.0/24 (Web Server, Mail Server...).
  - VLAN 70 (Management): 192.168.70.0/24 (Quản lý thiết bị mạng).
  - VLAN 100 (Guest Wi-Fi): 192.168.100.0/24 (khách hàng).
- Gateway của các VLAN: 192.168.X.1 (Core Switch Layer 3 làm default gateway cho mỗi VLAN).
- Địa chỉ WAN: 172.16.1.0/30
  - HQ Router WAN: 172.16.1.1.
  - Branch 1 Router WAN: 172.16.1.2.

2.2.2 Branches IP Plan

- Mạng nội bộ:
  - VLAN 10 (Nhân viên): 192.168.110.0/24.
  - VLAN 50 (Server Farm): 192.168.150.0/24.
  - VLAN 100 (Guest Wi-Fi): 192.168.200.0/24.

- Gateway của các VLAN: 192.168.X.1 (Switch Layer 3 tại chi nhánh làm default gateway).
- Địa chỉ WAN: Theo kế hoạch trên (ví dụ: 172.16.1.2 cho Branch 1).

2.3 Schematic Physical Setup - Sơ đồ vật lý và wiring diagram cho Headquarters và Branches

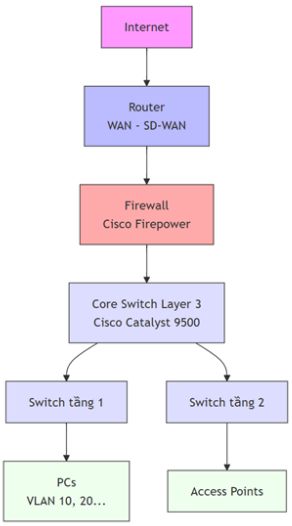
2.3.1 Wiring Diagram (Headquarters)

Tầng IT Room (tầng 1):

- Core Switch Layer 3 kết nối với:
  - Firewall.
  - Router (WAN SD-WAN).
  - Các Switch tầng bằng cáp quang GPON.

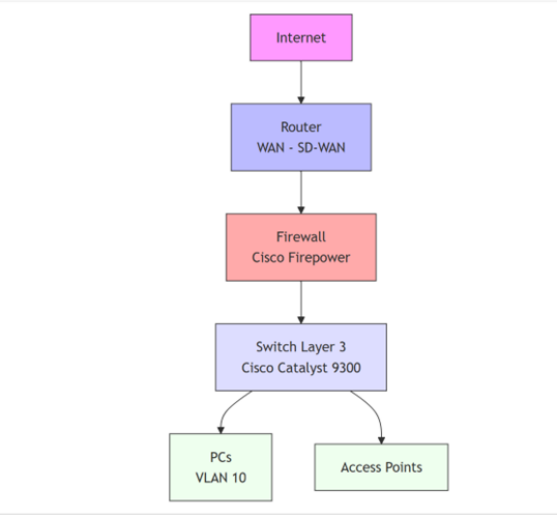
Các tầng khác:

- Mỗi tầng lắp 1 Switch Layer 2 để kết nối với các máy trạm qua Cat6A.
- Access Points tại các tầng kết nối với Switch tầng qua PoE.



2.3.2 Wiring Diagram (Branches)

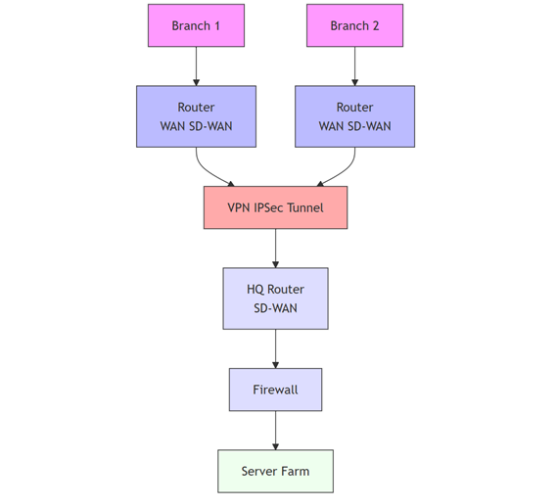
- Switch Layer 3 tại IT room kết nối với:
  - Router (WAN).
  - Các máy trạm qua cáp Ethernet.
  - Access Points qua cáp PoE.



2.4 WAN Connection Diagram

Sử dụng SD-WAN làm công nghệ kết nối chính giữa Headquarters và Branches, và định tuyến bằng giao thức OSPF.

- Cấu hình SD-WAN:
  - Mỗi site được định danh (HQ, Branch 1, Branch 2).
  - Kết nối VPN IPSec bảo mật giữa các site.
  - Các gói tin được tối ưu qua các đường truyền (load balancing giữa MPLS và xDSL).



- Routing (OSPF):
  - Các site được định cấu hình OSPF với các Area:
    - HQ (Area 0).

    * Branch 1 và Branch 2 (Area 1).
  - HQ là backbone (Area 0) quản lý định tuyến.

3 Tính toán thông lượng, băng thông cần thiết từ ISP và cấu hình mạng

3.1 Tính toán thông lượng yêu cầu

3.1.1 Tính toán thông lượng yêu cầu

Số lượng thiết bị và tải dự kiến:

- Máy trạm (120):
  - Mỗi máy trạm sử dụng 500 MB/ngày (download) và 100 MB/ngày (upload).
  - Giờ cao điểm: 80
  - Lưu lượng trong giờ cao điểm:
    * Download: 24,000 MB/giờ (47 Mbps).
    * Upload: 4,800 MB/giờ (9 Mbps).
- Server (5):
  - Download: 400 MB/giờ (0.8 Mbps).
  - Upload: 800 MB/giờ (1.6 Mbps).
- Wi-Fi Guest Devices:
  - Download: 200 MB/giờ (0.4 Mbps).
- Camera (8):
  - Tổng băng thông upload: 48 Mbps.

Tổng thông lượng yêu cầu tại Headquarters:

- Download: 48.2 Mbps.
- Upload: 58.6 Mbps.

3.1.2 Thông lượng tại mỗi Branch

Số lượng thiết bị và tải dự kiến:

- Máy trạm (30):
  - Download: 6,000 MB/giờ (11.7 Mbps).
  - Upload: 1,200 MB/giờ (2.3 Mbps).
- Server (3):
  - Download: 400 MB/giờ (0.8 Mbps).
  - Upload: 800 MB/giờ (1.6 Mbps).

- Wi-Fi Guest Devices:
  - Download: 200 MB/giờ (0.4 Mbps).
- Camera (3):
  - Tổng băng thông upload: 18 Mbps.

Tổng thông lượng yêu cầu tại mỗi Branch:

- Download: 12.9 Mbps.
- Upload: 21.9 Mbps.

3.1.3 Tổng thông lượng WAN cần thiết

Tổng thông lượng giữa Headquarters và các Branches:

- Tổng tải từ Branch 1 và Branch 2 đến Headquarters:
  - Download tại HQ: 25.8 Mbps.
  - Upload tại HQ: 43.8 Mbps.
- Kết nối Internet qua HQ (bao gồm truy cập từ Branches):
  - Download: 74 Mbps.
  - Upload: 80.5 Mbps.

Tổng băng thông yêu cầu:

- Headquarters:
  - Download: Ít nhất 50 Mbps.
  - Upload: Ít nhất 60 Mbps.
- Mỗi branch:
  - Download: Ít nhất 15 Mbps.
  - Upload: Ít nhất 25 Mbps.

3.2 Đề xuất băng thông từ ISP

3.2.1 Headquarters

- Download: Ít nhất 50 Mbps.
- Upload: Ít nhất 75 Mbps.

3.2.2 Branches

- Download: Ít nhất 20 Mbps.
- Upload: Ít nhất 30 Mbps.

3.3 Cấu hình đề xuất cho mạng của công ty

3.3.1 Cấu hình WAN (SD-WAN và MPLS)

Thiết bị:

- HQ Router: Cisco ISR 4451-X.
- Branch Router: Cisco ISR 1100 Series.
- SD-WAN Controller: Triển khai tại HQ để quản lý các site.

Cấu hình OSPF (trên SD-WAN hoặc MPLS):

- OSPF Area:
  - HQ là Area 0 (Backbone).
  - Branches là Area 1.
- Cấu hình OSPF để định tuyến động giữa các site, cho phép chia sẻ tải và failover nhanh.

VPN IPSec (kết nối giữa các site):

- HQ Router: Làm VPN Hub.
- Branch Routers: Làm VPN Spoke.
- Mã hóa AES-256, xác thực SHA-256.

3.3.2 Cấu hình LAN

Phân chia VLAN (Headquarters):

- Thiết lập các VLAN:
  - VLAN 10 (IT): 192.168.10.0/24.
  - VLAN 20 (Finance): 192.168.20.0/24.
  - VLAN 30 (HR): 192.168.30.0/24.
  - VLAN 40 (Marketing): 192.168.40.0/24.
  - VLAN 50 (Server Farm): 192.168.50.0/24.
  - VLAN 60 (DMZ): 192.168.60.0/24.
  - VLAN 100 (Guest Wi-Fi): 192.168.100.0/24.

Switch Layer 3 tại HQ:

- Thiết lập routing giữa các VLAN.
- Default Gateway: 192.168.X.1 cho từng VLAN.
- Static Route: Cấu hình đường tĩnh về router WAN.

Branches:

- Cấu hình tương tự HQ nhưng với subnet riêng.
- VLAN Management: VLAN 70 cho quản trị mạng.

3.3.3 Load Balancer

Load Balancer (HQ): Đặt giữa Firewall và Server Farm để cân bằng tải.

- Phân phối yêu cầu đến các server (Web, Database) dựa trên:
  - Round Robin hoặc Least Connection.

4 Thiết kế sơ đồ bằng Cisco Packet Tracer

4.1 Các công nghệ được áp dụng trong thiết kế

Trong thiết kế mạng cho BB Bank, các công nghệ và kỹ thuật sau đây đã được tích hợp để đảm bảo tính hiệu quả, bảo mật và khả năng mở rộng:

- Phân chia VLAN (Virtual Local Area Network): VLAN được sử dụng để tạo các nhóm mạng logic cho từng phòng ban tại Headquarters (HQ) và các chi nhánh (Branches). Điều này giúp quản lý lưu lượng mạng hiệu quả hơn và tăng cường bảo mật bằng cách:
  - Cách ly lưu lượng giữa các VLAN như IT, Tài chính, Marketing, và Wi-Fi khách.
  - Giảm tải broadcast, tối ưu hóa băng thông cho các khu vực có lưu lượng cao như phòng giao dịch hoặc phòng máy chủ.
  - Tạo điều kiện thuận lợi cho việc bổ sung hoặc thay đổi thiết bị mà không cần điều chỉnh cáp vật lý.

  Ví dụ: VLAN 10 tại HQ được dành riêng cho phòng IT, trong khi VLAN 100 phục vụ Wi-Fi khách hàng với chính sách cách ly khỏi mạng nội bộ.
- SD-WAN và VPN: Kết nối giữa HQ và các chi nhánh được thực hiện qua SD-WAN với các đường VPN IPSec bảo mật:
  - SD-WAN đảm bảo hiệu suất mạng cao với khả năng load balancing giữa các đường truyền.
  - VPN bảo vệ dữ liệu truyền tải qua Internet bằng cách mã hóa toàn bộ luồng dữ liệu giữa HQ và Branches.
- Access Control List (ACL): ACL được cấu hình trên router và firewall tại các vị trí quan trọng, giúp kiểm soát quyền truy cập và ngăn chặn các mối đe dọa:
  - Hạn chế truy cập từ các IP hoặc thiết bị không xác thực.
  - Đảm bảo chỉ những gói tin hợp lệ được phép truyền qua các VLAN hoặc ra Internet.
  - Tăng cường bảo mật mạng nội bộ, bảo vệ dữ liệu nhạy cảm khỏi truy cập trái phép.
- DHCP: Dịch vụ DHCP được triển khai tại HQ và các chi nhánh để tự động cấp phát địa chỉ IP cho thiết bị. Điều này giúp:
  - Đơn giản hóa cấu hình mạng cho hơn 150 máy trạm và các thiết bị di động.
  - Quản lý tập trung, giảm nguy cơ xung đột địa chỉ IP.
- Công nghệ Wi-Fi hiện đại (Wi-Fi 6): Hệ thống mạng không dây được thiết kế với các Access Points chuẩn Wi-Fi 6, hỗ trợ hiệu suất cao và khả năng kết nối nhiều thiết bị đồng thời:

  - SSID riêng biệt cho nhân viên và khách hàng.
  - Hỗ trợ VLAN tagging, giúp lưu lượng Wi-Fi tuân theo các quy tắc bảo mật của mạng LAN.
  - Sử dụng controller tập trung để quản lý toàn bộ hệ thống không dây.
- Định tuyến động (OSPF): Giao thức OSPF được áp dụng để định tuyến dữ liệu giữa HQ và các chi nhánh:
  - Tự động tính toán và chọn đường truyền tối ưu, giảm thiểu độ trễ.
  - Duy trì kết nối ổn định ngay cả khi một tuyến đường bị lỗi.

4.2 Tổng thể toàn bộ hệ thống

4.2.1 Headquarters

Trụ sở chính của BB Bank được thiết kế với một hệ thống mạng hiện đại, tối ưu cho hiệu năng cao, bảo mật và khả năng mở rộng trong tương lai. Toàn bộ hệ thống bao gồm các thành phần chính:

- Mỗi tầng được kết nối với một Switch Layer 2, tập trung vào Core Switch đặt tại phòng IT tầng 1.
- Sử dụng cấu trúc Star Topology, đảm bảo mỗi tầng kết nối độc lập với Core Switch qua cáp quang GPON, tối ưu tốc độ và giảm thiểu điểm lỗi.
- Mỗi phòng ban (IT, Tài chính, Nhân sự, Marketing) được gán vào một VLAN riêng biệt, đảm bảo bảo mật và giảm tải broadcast.

Các thiết bị mạng:

- Core Switch Layer 3: Chịu trách nhiệm định tuyến giữa các VLAN và kết nối ra Router WAN.
- Switch Layer 2: Được đặt tại mỗi tầng, hỗ trợ kết nối máy trạm và Access Points.
- Router WAN: Đảm bảo kết nối với các chi nhánh thông qua SD-WAN và VPN IPSec.
- Access Points (Wi-Fi): Hỗ trợ chuẩn Wi-Fi 6, đặt tại mỗi tầng để cung cấp kết nối không dây cho nhân viên và khách hàng.
- Camera: Hệ thống camera giám sát, một camera mỗi tầng, riêng tầng IT có 2 camera giám sát.

Dịch vụ hệ thống:

- Server farm (cụm máy chủ): 5 server được đặt trong phòng IT, phục vụ các ứng dụng doanh nghiệp như Web Server, Database Server, File Sharing Server...
- DHCP Server: Cấu hình tự động cấp phát IP cho hơn 120 máy trạm và các thiết bị không dây.

- DMZ (De-Militarized Zone): Tách biệt các server công khai như Web Server và Mail Server khỏi mạng nội bộ để giảm thiểu nguy cơ tấn công.

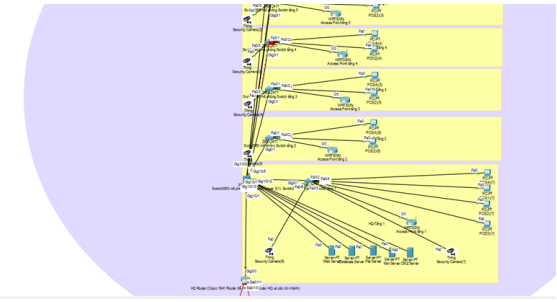


Figure 2: Sơ đồ thiết kế ở Headquater trong Cisco Packet Tracer

4.2.2 Branch

Các chi nhánh của BB Bank được thiết kế với hệ thống mạng đơn giản hơn so với trụ sở chính, nhưng vẫn đảm bảo đáp ứng yêu cầu về hiệu năng, bảo mật và tính ổn định. Mỗi chi nhánh bao gồm các đặc điểm chính:

Kiến trúc mạng:

- Tòa nhà 2 tầng:
  - Sử dụng Switch Layer 3 tại phòng IT tầng 1, đóng vai trò làm trung tâm kết nối cho toàn bộ chi nhánh.
  - Các máy trạm trên từng tầng được kết nối trực tiếp qua cáp Ethernet Cat6A đến Switch Layer 3.
- Phân chia VLAN:
  - VLAN được áp dụng để phân tách lưu lượng mạng cho các bộ phận và dịch vụ. Ví dụ:
    - VLAN 10: Máy trạm và các thiết bị của phòng IT.
    - VLAN 50: Các máy trạm tại tầng 2.
    - VLAN 100: Guest Wi-Fi, cách ly hoàn toàn khỏi mạng nội bộ.

Các thiết bị mạng:

- Switch Layer 3: Chịu trách nhiệm định tuyến nội bộ và làm gateway cho các VLAN tại chi nhánh.
- Router WAN: Đảm bảo kết nối chi nhánh với trụ sở chính thông qua SD-WAN và VPN IPSec.
- Access Points (Wi-Fi): Cisco Aironet 2800, hỗ trợ Wi-Fi chuẩn 6, cung cấp kết nối không dây cho nhân viên và khách hàng tại chi nhánh.
- Camera: Tương tự như headquarter, tầng IT gồm các cụm máy chủ có 2 camera, tầng còn lại có 1 camera.

Dịch vụ hệ thống:

- Server farm:
  - Mỗi chi nhánh có 3 server, đảm nhận các chức năng như xử lý dữ liệu nội bộ, lưu trữ tài liệu và quản lý giao dịch.
- DHCP: Được cấu hình trên Switch Layer 3 để tự động cấp phát IP cho các thiết bị mạng tại chi nhánh.

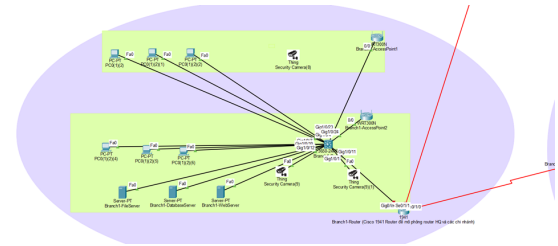


Figure 3: Sơ đồ thiết kế ở chi nhánh 1 trong Cisco Packet Tracer