Nhóm 2:

Đặng Trung Hậu - 21520833

Nguyễn Gia Quân – 21521327

Hồ Mạnh Đạt – 21520695

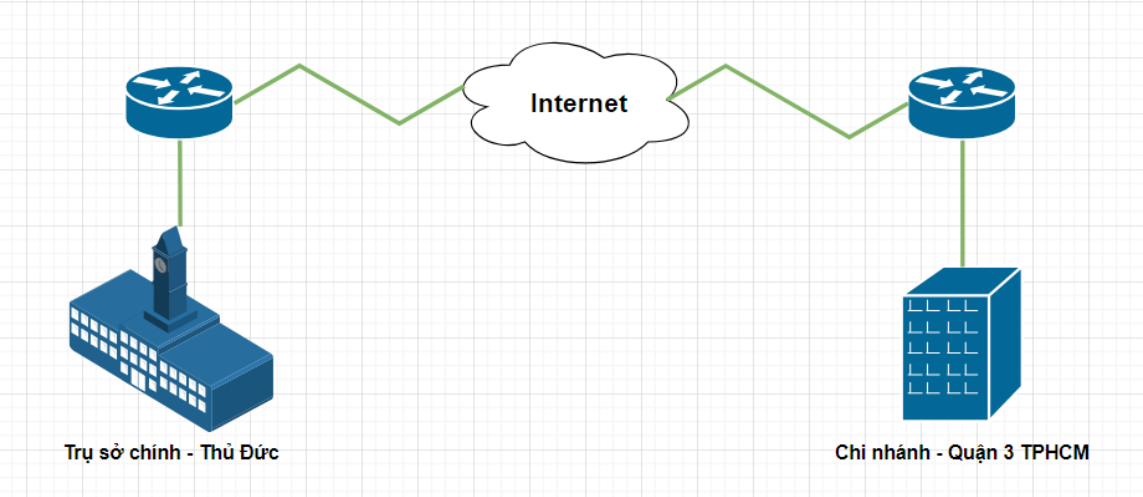
Note: Nhóm chưa thực hiện cấu hình trên các thiết bị, sẽ bổ sung ở báo cáo chính thức.

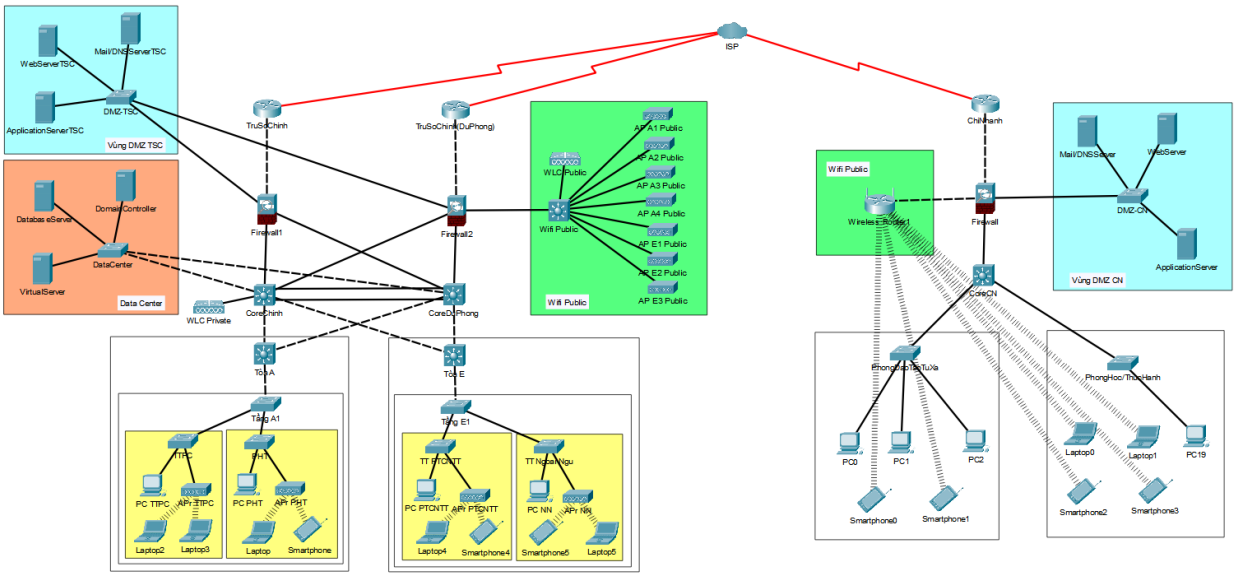
3. Thiết kế hệ thống mạng:

3.1. Thiết kế mô hình mạng logic

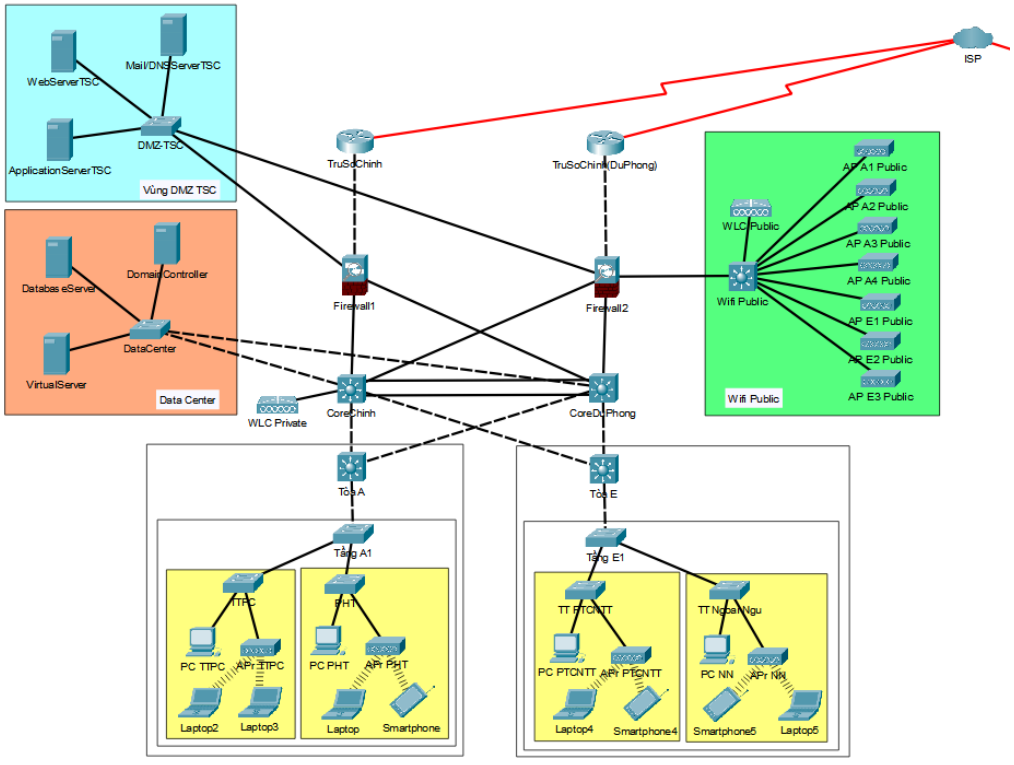
Sơ đồ logic, giải thích tóm tắt về mô hình, các giao thức, cấu hình cần có cho mô hình

Sơ đồ logic mạng tổng quan trường Đại học NT-UIT: **File thiết kế .pkt**

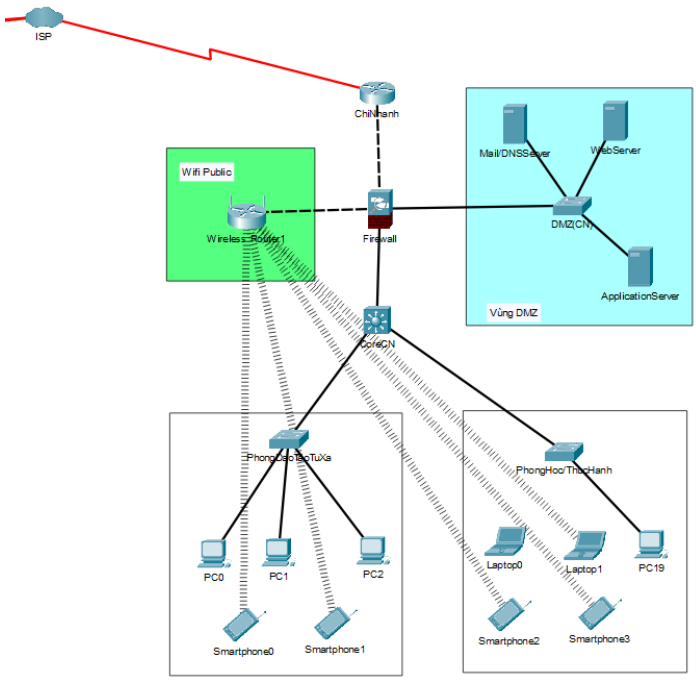




Trụ sở chính:



Chi nhánh Quận 3:



- **Giải thích tóm tắt về mô hình:**

  + Mô hình mạng trường Đại học NT-UIT xây dựng theo mô hình mạng 3 lớp đề xuất bởi Cisco.

  Lớp mạng Core dùng để kết nối giữa các tòa nhà được sử dụng các thiết bị core Switch có khả năng chịu tải lớn, hỗ trợ công nghệ hiện đại, đảm bảo traffic yêu cầu ở lớp core.

  + Lớp mạng Distribution sử dụng các thiết bị Switch layer 3, đóng vai trò phân phối tải, cấu hình chia mạng các phòng ban thành các VLAN để dễ quản lý, mở rộng thiết bị.

  + Lớp mạng Access sử dụng các thiết bị Switch layer 2, tối thiểu 24 port, kết nối trực tiếp với các thiết bị đầu cuối (end host).

  + Mô hình thiết kế Data Center ở tòa A sẽ đặt riêng ở một vùng gọi là DMZ. Dùng đảm bảo tính đáp ứng cho người dùng và tính bảo mật cho toàn bộ hệ thống mạng nội bộ.

  + Các Server vật lý được thiết kế kết hợp với dịch vụ Server ảo, tạo thành kiến trúc Hybrid, đáp ứng tốt nhu cầu mở rộng khi có traffic yêu cầu lớn.

+ Mô hình thiết kế các Wireless LAN Controller (WLC) để quản lý tập trung các Access Point, cung cấp dịch vụ WiFi chứng thực và WiFi Public theo kênh kết nối riêng.

- **Các giao thức, cấu hình cần có cho mô hình:**

+ Giao thức chuyển mạch:

- Sử dụng các Transparent Bridging và thuật toán Spanning Tree Protocol (STP) sử dụng giao thức kết nối các Switch có hỗ trợ chia VLAN như (Inter-Switch Link) ISL.
- STP chặn một số cổng trên các thiết bị chuyển mạch có liên kết dự phòng để ngăn chặn Broadcast và đảm bảo cấu trúc liên kết không bị Loop.

+ Mô hình sử dụng giao thức định tuyến EIGRP phát triển bởi Cisco:

- EIGRP là giao thức định tuyến riêng của Cisco nhằm khắc phục các nhược điểm của RIP/IGRP, ra đời vào năm 1994, được mở rộng từ giao thức IGRP(Gateway Routing Protocol).
- EIGRP là Classless Protocol, có hỗ trợ CIDR(Classless interdomain routing), cho phép tiết kiệm không gian địa chỉ bằng VLSM và vấn đề mạng không liên tục (discontiguous network). So với IGRP, EIGRP có thời gian hội tụ nhanh hơn nhưng vẫn chống được Loop trong mọi trường hợp, sử dụng băng thông hiệu quả hơn , có khả năng mở rộng tốt hơn, vì vậy EIGRP là một sự lựa chọn lý tưởng cho các mạng lớn, đa giao thức được xây dựng dựa trên các Router Cisco.

+ Cấu hình DHCP cấp phát địa chỉ IP động cho các thiết bị kết nối vào mạng.

+ Cấu hình VLAN dễ dàng mở rộng, quản lý host.

+ Cấu hình dịch vụ WiFi chứng thực sử dụng công nghệ Captive Portal:

- Đây là một kỹ thuật buộc người dùng phải chứng thực qua 1 giao diện web trước khi kết nối vào Internet. Kỹ thuât này thường áp dụng cho các điểm

truy cập WiFi, mạng có dây. Người dùng muốn truy cập vào, phải có một account chứng thực, ...

+ Cấu hình dịch vụ VPN Site to Site, VPN Client to Site phục vụ nhu cầu kết nối riêng tư cho giảng viên.

+ Cấu hình chính sách tường lửa bảo mật cho mạng nội bộ và Data Center.

3.2 Mô hình địa chỉ IP cho hệ thống mạng

- **Sơ đồ bố trí phòng:**

+ Trụ sở chính - Thủ Đức:

Sơ đồ bố trí phòng tòa A:

Tòa A:

Tầng 5					
Tầng 4	Vpk cnpm	Vpk toán - lý	Vp OEP		
Tầng 3	Vpk khmt	Vpk cntt	Vpk ktmt	Vpk mạng	Vpk httt
Tầng 2	ctsv	Đt đại học	Đt sau đh	Khtc	Tổ chức hc
Tầng 1	p.hiệu trưởng	Data center	Thanh tra pc	QT thiết bị	QH đối ngoại

Sơ đồ bố trí phòng tòa E:

Tòa E:

Tầng 6					
Tầng 5					
Tầng 4					
Tầng 3	PTN TT đa PT				
Tầng 2	PTN ATTT	PTN HTTT			
Tầng 1	TT ngoại ngữ	TT phát triển CNTT	TT CNSC		

- **Mô hình địa chỉ IP:**

VPN Site-to-Site:

Interfaces	IP Address	Subnet Mask

Tunnel ThuDuc	192.168.200.1	255.255.255.252
Tunnel Quan3	192.168.200.2	255.255.255.252
Tunnel source	ISP cung cấp	
Tunnel destination		

Giải thích: Sử dụng Interface Tunnel giúp cho việc truyền dữ liệu giữa các mạng con trở nên an toàn và hiệu quả hơn:

+ Tunnel source: Đây là địa chỉ IP công khai của Router, được cung cấp bởi ISP (Internet Service Provider). Địa chỉ này được sử dụng để khởi tạo kết nối VPN.

+ Tunnel destination: Đây là địa chỉ IP công khai của Router đích, nơi tunnel kết thúc.

Trong trường hợp này, Router tại Thủ Đức sẽ có địa chỉ IP công khai (tunnel source) và sẽ kết nối đến Router tại Quận 3 thông qua địa chỉ IP công khai của nó (tunnel destination), và ngược lại.

Trụ sở chính:

+ Tòa A:

Tên mạng con	**Số host (số lượng thiết bị cần gán địa chỉ IP)**	**Địa chỉ mạng con**	**Subnet Mask**	**Số lượng địa chỉ tối đa có thể dùng tại subnet này**
Data Center	5	192.168.60.0	255.255.255.240	10
P.Hiệu trưởng	2	192.168.10.0	255.255.255.252	4
P.TTPC	5	192.168.11.0	255.255.255.240	10
P.QTthiết bị	5	192.168.12.0	255.255.255.240	10

P.QHđối ngoại	5	192.168.13.0	255.255.255.240	10
CTSV	10	192.168.20.0	255.255.255.224	20
ĐTĐH	20	192.168.21.0	255.255.255.192	40
ĐTSĐH	20	192.168.22.0	255.255.255.192	40
KHTC	20	192.168.23.0	255.255.255.192	40
TCHC	20	192.168.24.0	255.255.255.192	40
VPK KHMT	50	192.168.30.0	255.255.255.128	100
VPK CNTT	50	192.168.31.0	255.255.255.128	100
VPK KTMT	50	192.168.32.0	255.255.255.128	100
VPK MMT	50	192.168.33.0	255.255.255.128	100
VPK HTTT	50	192.168.34.0	255.255.255.128	100
VPK CNPM	50	192.168.40.0	255.255.255.128	100
VPK toán lý	50	192.168.41.0	255.255.255.128	100
VP OEP	50	192.168.42.0	255.255.255.128	100
VP	50	192.168.50.0	255.255.255.128	100

+ Tòa E:

Tên mạng con	Số host (số lượng thiết bị cần gán địa chỉ IP)	Địa chỉ mạng con	Subnet Mask	Số lượng địa chỉ tối đa có thể dùng tại subnet này
TT PTCNTT	20	192.168.70.0	255.255.255.192	40
TT CNSC	20	192.168.71.0	255.255.255.192	40
TT NN	20	192.168.72.0	255.255.255.192	40
PTN ATTT	50	192.168.80.0	255.255.255.128	100
PTN HTTT	50	192.168.81.0	255.255.255.128	100
PTN TTDPT	50	192.168.90.0	255.255.255.128	100
Phòng học	50	192.168.100.0	255.255.255.128	100
Phòng thực hành	50	192.168.110.0	255.255.255.128	100

STT	Tên thiết bị	Interfaces	Địa chỉ	Subnet Mask	Default gateway
1	Router trụ sở chính	Cổng nối với Internet	10.20.30.2	255.255.255.252	N/A
		Cổng nối Firewall 1 vào LAN	192.168.0.1	255.255.255.252	
	Router trụ sở chính (DP)	Cổng nối với Internet	14.15.16.2	255.255.255.252	
		Cổng nối với Firewall 2 vào LAN	172.16.0.1	255.255.255.252	

2	Firewall 1	Cổng nối với Router trụ sở chính	192.168.0.2	255.255.255.252	
		Cổng nối với DMZ	192.168.1.1	255.255.255.252	
		Cổng nối với Core Switch	192.168.2.1	255.255.255.252	
		Cổng nối với Core DP	192.168.3.1	255.255.255.252	
	Firewall 2	Cổng nối với Router trụ sở chính (DP)	172.16.0.2	255.255.255.252	
		Cổng nối với DMZ	172.16.1.1	255.255.255.252	
		Cổng nối với Core Switch	172.16.2.1	255.255.255.252	
		Cổng nối với Core DP	172.16.3.1	255.255.255.252	
3	Core Switch Layer 3	Cổng nối với Firewall 1	192.168.2.2	255.255.255.252	
		Cổng nối với Firewall 2	172.16.2.2	255.255.255.252	
		Cổng nối với SwitchA1	VLAN10 192.168.10.1	255.255.255.252	
			VLAN11 192.168.11.1	255.255.255.240	
			VLAN12 192.168.12.1	255.255.255.240	
			VLAN13 192.168.13.1	255.255.255.240	
		Cổng nối với SwitchA2	VLAN20 192.168.20.1	255.255.255.224	
			VLAN21 192.168.21.1	255.255.255.192	
			VLAN22 192.168.22.1	255.255.255.192	
			VLAN23 192.168.23.1	255.255.255.192	
			VLAN24 192.168.24.1	255.255.255.192	
		Cổng nối với SwitchA3	VLAN30 192.168.30.1	255.255.255.128	
			VLAN31 192.168.31.1	255.255.255.128	
			VLAN32 192.168.32.1	255.255.255.128	

			VLAN33 192.168.33.1	255.255.255.128	
			VLAN34 192.168.34.1	255.255.255.128	
		Cổng nối với SwitchA4	VLAN40 192.168.40.1	255.255.255.128	
			VLAN41 192.168.41.1	255.255.255.128	
			VLAN42 192.168.42.1	255.255.255.128	
		Cổng nối với SwitchA5	VLAN50 192.168.50.1	255.255.255.128	
			VLAN51 192.168.51.1	255.255.255.128	
		Cổng nối với Data Center	192.168.60.1	255.255.255.240	
		Cổng nối với SwitchE1	VLAN70 192.168.70.1	255.255.255.192	
			VLAN71 192.168.71.1	255.255.255.192	
			VLAN72 192.168.72.1	255.255.255.192	
		Cổng nối với SwitchE2	VLAN80 192.168.80.1	255.255.255.128	
			VLAN81 192.168.81.1	255.255.255.128	
		Cổng nối với SwitchE3	VLAN90 192.168.90.1	255.255.255.128	
		Cổng nối với SwitchE4	VLAN100 192.168.100.1	255.255.255.128	
		Cổng nối với SwitchE5	VLLAN110 192.168.110.1	255.255.255.128	
4	WLC Private	Cổng nối với CoreSwitch	192.168.500.0	255.255.255.0	
5	Core Switch WiFi Public	Cổng nối với Firewall 1	192.168.3.2	255.255.255.252	
6	WLC Public	Cổng nối với CoreSwitch	192.168.600.0	255.255.255.0	

7	Web Server	NIC	192.168.1.2	255.255.255.252	
8	Mail Server		192.168.1.3	255.255.255.252	
9	Domain Controller		192.168.60.2	255.255.255.240	
10	Database Server		192.168.60.3	255.255.255.240	
11	Virtual Server		SP	SP	
12					

Chi nhánh Quận 3:

Tên mạng con	Số lượng thiết bị cần gán địa chỉ IP	Địa chỉ mạng con	Subnet Mask	Số lượng địa chỉ tối đa có thể dùng tại subnet này
PDTTX	20	192.168.120.0	255.255.255.192	40
PH/PTH	20	192.168.121.0	255.255.255.192	40

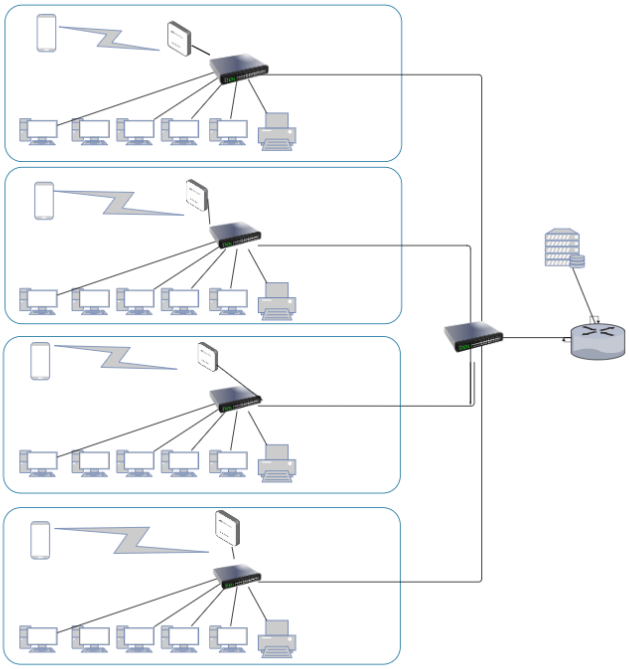
STT	Tên thiết bị	Interfaces	Địa chỉ	Subnet Mask	Default gateway
1	Router Chi Nhánh	Cổng nối với Internet	10.20.30.3	255.255.255.252	N/A
		Cổng nối với firewall	192.168.120.1	255.255.255.252	
2	Firewall	Cổng nối với Router Chi nhánh	192.168.120.2	255.255.255.252	
		Cổng nối với vùng DMZ	192.168.121.2	255.255.255.252	
		Cổng nối với Router wifi	192.168.122.1	255.255.255.252	
		Cổng nối với SwitchLayer3	192.168.123.1	255.255.255.252	
3	Router wifi	Cổng nối với firewall	192.168.122.2	255.255.255.252	
4	SwitchLayer3	Cổng nối với firewall	192.168.123.2	255.255.255.252	

		Cổng nối với switchPDTTX	VLAN150 192.168.150.1	255.255.255.192	
		Cổng nối với switchPH/TH	VLAN151 192.168.151.1	255.255.255.192	
5	WebServer	NIC	192.168.121.3	255.255.255.252	
6	MailServer	NIC	192.168.121.4	255.255.255.252	
7	ApplicationServer	NIC	192.168.121.5	255.255.255.252	

3.3 Thiết kế sơ đồ vật lý của hệ thống mạng

3.3.1 Sơ đồ vật lý

- Mỗi tầng sẽ bố trí 1 phòng thiết bị, đặt tập trung các thiết bị Switch Layer 2, Access Point và các thiết bị đầu cuối sẽ được đặt trong từng phòng. Kết nối tới Switch bằng cáp mạng.



- Data Center được bố trí ở tầng trệt tòa nhà A, đặt tập trung các Server vật lý.

- Các thiết bị mạng core sẽ được đặt trong phòng dữ liệu của mỗi tòa, đảm bảo an toàn tránh hư hỏng.

3.3.2 Các ứng dụng, thiết bị dùng trong hệ thống

- Lựa chọn hệ điều hành Linux, Windows.
- Lựa chọn các công cụ phát triển ứng dụng phần mềm như các phần mềm quản trị cơ sở dữ liệu (Oracle, Informix, SQL, Lotus Notes,…).
- Lựa chọn các server như Web Server, FTP server,…
- Lựa chọn các phần mềm quản lý, giám sát và quản trị mạng.

  + PRTG Network Monitoring :

    - Khả năng giám sát lưu lượng, gói, ứng dụng, băng thông, dịch vụ đám mây, cơ sở dữ liệu, môi trường ảo, thời gian hoạt động, cổng, IP, phần cứng, bảo mật, dịch vụ web, sử dụng đĩa, môi trường vật lý, thiết bị IoT
    - Khả năng hỗ trợ SNMP (tất cả các phiên bản), Flow technologies (i.e. NetFlow, jFlow, sFlow), SSH, WMI, Ping, và SQL. API mạnh mẽ (Python, EXE, DLL, PowerShell, VB, Batch Scripting, REST).

Ứng dụng	Giá thành
Paesseler PRTG Network Monitor (PRTG500)	1.899 USD

Các thiết bị được lựa chọn sử dụng trong hệ thống mạng là các thiết bị mạng của Cisco, đáp ứng được tính đồng nhất, khả năng tương thích cao, hỗ trợ các giao thức được phát triển riêng bởi Cisco.

Tên thiết bị	Số lượng	Thông tin chi tiết
Cisco C9300-24T-A (Switch layer 3) (core layer)		Gồm 24 cổng Ethernet, Khả năng chuyển mạng: 48 Gbps(hiệu suất cao), hỗ trợ vlan, các

		phương thức quản lí từ xa như(SSH, telnet…), các phương thức bảo mật(ACLs…)
Cisco CBS250-16T-2G-EU (Switch layer 3) (distribution layer)		Cung cấp 16 cổng 10/100/1000 và 2 cổng 1G SFP uplink, 36.0 Gbps, CPU 800 MHz ARM. Phù hợp cho mô hình mạng doanh nghiệp nhỏ.
Switch Cisco Catalyst 2960 WS-C2960-24TC-S (Switch layer 2)		Gồm 24 cổng Ethernet, tốc độ chuyển mạng 6.5 Mbps, hỗ trợ quản lí từ xa, bảo mật, giao diện CLI hoặc web, VLAN.
Cisco Firewall ASA5508-K9 with FirePOWER services, 8GE Data, 3DES/AES		Hỗ trợ VPN Site-to-site và remote access VPN, cung cấp khả năng truy cập hiệu suất cao. Khả năng hiển thị và kiểm soát ứng dụng chi tiết (AVC) hỗ trợ hơn 4.000 lớp ứng dụng.
Aruba Instant On AP11 (Access Point - AP)		Hỗ trợ trên cả 2 băng tần 2.4 Ghz tốc độ 300 Mbps và 5Ghz tốc độ 867 Mbps với công nghệ 2×2(2.4 Ghz) 2×2 (5.0Ghz) Mu-Mimo, kích thước nhỏ gọn(phù hợp đặt trong phòng), chuẩn 802.11 ac Wave 2
Dell PowerEdge T550 Tower Server		
Cisco Catalyst 9800-L (WLCs)		Hỗ trợ tối đa 500 Access Point, 10000 thiết bị, băng thông tối đa 10 Gbps, tối đa 4096 WLAN và VLAN, tương thích tốt với thiết bị Access Point lựa chọn ở trên.
Bộ Lưu Điện UPS PROLINK PRO902WS - 2KVA		Duy trì ổn định nguồn cung cấp điện cho hệ thống.

Dây cáp mạng CAT6		Tốc độ hoạt động của cáp mạng Cat6 là 10 Gigabit/giây ở băng thông 250Mhz với khoảng cách từ 70m-100m.
Hạt mạng Cat6 Dintek		

3.3.3 Các dịch vụ cần thuê

- ISP cung cấp Internet.

+ Lựa chọn các ISP cung cấp đường kết nối Leased Line.

- Leased Line là một dịch vụ Internet được cung cấp bởi các nhà cung cấp dịch vụ viễn thông để kết nối doanh nghiệp với Internet. Điều này được thực hiện bằng cách cung cấp một đường kết nối trực tiếp từ doanh nghiệp đến cơ sở dữ liệu của nhà cung cấp dịch vụ viễn thông, giúp tăng tốc độ và độ tin cậy của kết nối Internet cho doanh nghiệp.
- Khi bạn sử dụng Leased Line, bạn sẽ được cung cấp một đường truyền trực tiếp từ nhà cung cấp dịch vụ viễn thông. Dữ liệu của bạn sẽ được truyền qua đường truyền này mà không bị gián đoạn bởi các khách hàng khác. Kết nối này được cung cấp bằng cách sử dụng một đường truyền vật lý (cáp đồng trục, cáp quang,..) hoặc một kết nối ảo (Virtual Private Network - VPN, MultiProtocol Label Switching – MPLS).

+ Lợi ích của Leased Line :

- Tốc độ truyền tải nhanh: Internet Leased Line cung cấp tốc độ truyền tải rất cao, đảm bảo các hoạt động kinh doanh diễn ra một cách suôn sẻ và hiệu quả.
- Độ tin cậy cao: Với một đường truyền Internetđược cấp riêng, doanh nghiệp sẽ có độ tin cậy cao hơn so với việc sử dụng Internetcông cộng. Điều này đảm bảo rằng doanh nghiệp của bạn không bị gián đoạn hoạt động và có thể tiếp cận Internetmột cách liên tục.
- Khả năng mở rộng: InternetLeased Line cho phép doanh nghiệp mở rộng mạng lưới của họ một cách dễ dàng và linh hoạt hơn. Điều này đảm bảo rằng doanh nghiệp của bạn có thể mở rộng quy mô kinh doanh một cách nhanh chóng và hiệu quả hơn.

- Nhà cung cấp kênh truyền VPN.
- Nhà cung cấp dịch vụ server ảo.

  + Lựa chọn nhà cung cấp Amazon Web Service, có khả năng tùy chỉnh cấu hình máy chủ, chi phí cạnh tranh với các nhà cung cấp khác.

Nhà cung cấp dịch vụ	Gói dịch vụ	Giá thành
VNPT	FiberXtra Xtra300+	990.000 VNĐ/ tháng
Viettel	Pro1000	700.000 VNĐ/ tháng
SufShark	VPN SufShark One	2.69 USD/ tháng
Amazon Web Service	EC2, VPC	On demand