

Khoa Khoa học và Kỹ Thuật Máy Tính

Đại Học Bách Khoa Thành Phố Hồ Chí Minh

BÀI TẬP LỚN 2: MẠNG MÁY TÍNH-NETWORK DESIGN



Môn: Mạng máy tính TN - Chương trình KSTN
Mã môn: CO3094

GVHD: Nguyễn Lê Duy Lai
GV Lý Thuyết: Nguyễn Lê Duy Lai

Họ và Tên sinh viên	MSSV
Đặng Hoàng Khang	2211422
Đinh Xuân Quyết	2212854
Lê Phúc Hoàng	2211081

Ngày 28.11.2024 - Thành Phố Hồ Chí Minh

MỤC LỤC

MỤC LỤC	2
• Tổng quát:	3
• Phân tích nội dung tư vấn:	4
• Phân tích hiện trạng và đề nghị giải pháp:	5
• Các sơ đồ thiết kế:	7
• Giải quyết yêu cầu bài toán:	10
LAN trụ sở chính:	10
LAN chi nhánh	15
Kết nối ra Internet	16
Cấu hình và các công nghệ sử dụng	17
Mạng dạng hình sao - Star Topology	17
VLAN (Virtual Local Area Network)	18
DHCP (Dynamic Host Configuration Protocol)	18
DNS (Domain Name System)	19
WAN	19
Giao thức OSPF (Open Shortest Path First)	19
Firewall	20
VPN	21
IPsec	21
NAT	22
Những cải tiến sau khi thuyết trình:	23
IPS/IDS	23
CCTV	24
CORE SWITCH	24
Kiểm thử: xem video trong demo	25
Kết luận:	25

● Tổng quát:

Case Study:

Công ty Tư vấn và Dịch vụ mạng CCC được yêu cầu thiết kế dự án mạng máy tính trong bệnh viện Chuyên Khoa Nhi chuẩn bị xây mới với cơ sở chính tại TP.HCM và 2 cơ sở phụ ở đường DBP và đường BHTQ.

Các thông số tổng quát:

- 2 tòa building A và B, với mỗi tòa là 5 tầng, và mỗi tầng được phân bố 10 phòng kết nối với các máy tính và các thiết bị y tế.
- Trung tâm dữ liệu, phòng kỹ thuật mạng (IT) và phòng đầu nối (phòng tập trung dây mạng và patch panel) được đặt tập trung tại một phòng cách 2 tòa building A và B 50m.
- CCC dạng SMB Enterprise: 600 workstations, 10 Servers, 12 Network Equipments.
- Mạng wireless được phủ sóng toàn khu vực.
- Dùng công nghệ mới (new technology) về hạ tầng mạng: cáp quang (GPON), và Giga Ethernet 1GbE/10GbE/40GbE, Wired và Wireless.
- Tổ chức hệ thống mạng theo VLAN.
- Dùng kết hợp giữa Licensed và Open source Softwares.
- Kết nối với bên ngoài nhờ 2 Leased Line và 2 ADSL, load balancing.
- Ứng dụng văn phòng, client-server, đa phương tiện, database và hospital software (HIS, RIS - PACS, LIS, CRM, etc.).
- Bảo mật cao, an toàn khi xảy ra sự cố và dễ dàng nâng cấp hệ thống.
- Cung cấp VPN configuration cho kết nối site-to-site và cho làm việc từ xa kết nối với Company LAN.
- Cung cấp hệ thống camera giám sát an ninh cho bệnh viện.

Các yêu cầu về chi nhánh:

Bệnh viện có nhu cầu kết nối đến 2 chi nhánh khác ở 2 đường DBP và BHTQ. Mỗi chi nhánh cũng được thiết kế tương tự như trụ sở nhưng quy mô nhỏ hơn:

- Tòa nhà cao khoảng 2 tầng, tầng 1 được trang bị 1 phòng kỹ thuật mạng (IT) và phòng đầu nối (phòng tập trung dây mạng và patch panel), tầng 2 dành cho các Workstation.
- CCC Chi nhánh: 60 workstations, 2 Servers, 5 Network Equipments.

Các thông số hệ thống:

Việc thực hiện kết nối giữa cơ sở chính và chi nhánh thông qua đường links WAN, chúng ta có thể chọn một trong các công nghệ dùng cho đường links này theo tính kinh tế của giải pháp phân tích ưu nhược điểm của giải pháp được chọn.

Các thông số về lưu lượng và tải của hệ thống (tập trung khoảng 80% vào giờ cao điểm 9g-11g và 15g-16g có thể dùng chung cho Cơ sở chính và Chi nhánh như sau:

- Máy chủ để cập nhật phần mềm, truy cập web và truy cập cơ sở dữ liệu,
Tổng dung lượng tải xuống ước tính khoảng 1000 MB/ngày và dung lượng tải lên ước tính là 2000MB/ngày.
- Mỗi máy trạm được sử dụng để duyệt web, tải xuống tài liệu và giao dịch với khách hàng, ... Tổng dung lượng tải xuống ước tính khoảng 500 MB/ngày và dung lượng tải lên ước tính là 100MB/ngày.
- Các thiết bị được kết nối WiFi từ quyền truy cập của khách hàng để tải xuống ước tính khoảng 500MB/ngày.

Hệ thống Mạng máy tính của Công ty được dự toán cho mức độ phát triển 20% trong 5 năm (về số lượng người sử dụng, tải trọng mạng, mở rộng nhiều chi nhánh...)

● Phân tích nội dung tư vấn:



Mỗi tòa nhà gồm 5 tầng, mỗi tầng 10 phòng, mỗi phòng được trang bị 6 máy tính. Mỗi tầng được lắp đặt 3 switch và 1 camera.

Tòa A gồm 5 tầng:

- Tầng 1: 4 phòng khoa KHTH - ĐT - CDT, 3 phòng tổ chức - hành chính, 3 phòng QLCL - CTXH - CSKH
- Tầng 2: 5 phòng chẩn đoán, 5 phòng dược
- Tầng 3: 5 phòng khám bệnh, 5 phòng cấp cứu tổng hợp
- Tầng 4: 5 phòng sanh, 5 phòng khoa phụ
- Tầng 5: 3 phòng hiếm muộn, 3 phòng hậu phẫu, hậu sản, 4 phòng HSTC và CD nhi

Tòa B gồm 5 tầng:

- Tầng 1: 3 phòng điều dưỡng, 3 phòng tài chính kế toán, 4 phòng công nghệ thông tin.
- Tầng 2: 5 phòng kiểm soát nhiễm khuẩn, 5 phòng xét nghiệm.
- Tầng 3: 5 phòng sơ sinh, 5 phòng nhi.
- Tầng 4: 5 phòng nhiễm nhi, 5 ngoại nhi.
- Tầng 5: 3 phòng liên chuyên khoa, 3 phòng gây mê hồi sức, 4 phòng dinh dưỡng.

● Phân tích hiện trạng và đề nghị giải pháp:

Đối với yêu cầu được đưa ra, nhóm đưa ra các mục tiêu chung, quy định chung cho hệ thống mạng như sau:

- Phải đảm bảo tính ổn định của hệ thống mạng LAN.
- Đảm bảo tính bảo mật và tính độc lập giữa các tầng trong cơ sở chính, nhóm áp dụng chia VLAN, chia subnet cho từng tầng...
- Dễ dàng nâng cấp hệ thống .
- Tiết kiệm tối đa các vật tư mạng cũng như chi phí cần thiết.

Tính toán throughput:

Ta tính throughput cho **2 tòa nhà A và B** vào lúc sử dụng đường truyền cao nhất (9h-11h và 15h16h, tổng cộng là 3h)

- Server: tính tổng tất cả các server mà công ty sử dụng, tổng dung lượng là 3000MB/ngày, tập trung 80% vào các giờ cao điểm:
$$3000*0.8/(3*3600) = 0.22 \text{ MB/s} = 1.78 \text{ Mbps}$$
- Mỗi tầng của tòa nhà có 60 máy, sử dụng cho duyệt WEB, tải tài liệu, tác vụ y tế, khám chữa bệnh... với tổng dung lượng mỗi máy 600MB/ngày, tập trung 80% vào giờ cao điểm:
$$60*600*0.8/(3*3600) = 2.67 \text{ MB/s} = 21.33 \text{ Mbps}$$

→ 5 tầng của 1 tòa nhà: $13.33 \text{ MB/s} = 106.67 \text{ Mbps}$
→ Tổng 2 tòa A và B: $26.67 \text{ MB/s} = 213.33 \text{ Mbps}$
- Hệ thống wireless của mỗi tòa nhà bao gồm 7 access point (tầng trệt 3 AP, các tầng khác 1AP , mỗi laptop sử dụng wireless dùng 500M/ngày, tập trung 80% vào giờ cao điểm, giả sử mỗi AP cho phép tối đa 30 người truy cập cùng lúc:
$$7*30*500*0.8/(3*3600) = 7.78 \text{ MB/s} = 62.22 \text{ Mbps}$$

→ Tổng 2 tòa A và B: $15.56 \text{ MB/s} = 124.44 \text{ Mbps}$
→ Toàn bộ tòa nhà A và B với throughput cao nhất có thể đạt được là: 339.55 Mbps

Các chi nhánh: mỗi chi nhánh có 60 máy, mỗi máy sử dụng 600MB/ngày, tập trung 80% vào giờ cao điểm:

$$60*600*0.8/(3*3600) = 2.67 \text{ MB/s} = 21.33 \text{ Mbps}$$

- Giả sử mỗi chi nhánh sử dụng 3 access point, mỗi access point có thể phục vụ cho 30 laptop cùng lúc, mỗi laptop kết nối wireless sử dụng 500MB/ngày, tập trung 80% giờ cao điểm:

$$3*30*500*0.8/(3*3600) = 3.33 \text{ MB/s} = 26.67 \text{ Mbps}$$

→ Mỗi chi nhánh sử dụng throughput cao nhất có thể là: 48Mbps

Cấu hình firewall:

Nhóm đề xuất sử dụng firewall Cisco ASA 5506.

Cấu hình thiết bị để thực hiện các chức năng sau:

- Ngăn chặn các ứng dụng được cho là “không cần thiết” như Yahoo Messenger, MSN...
- Ngăn chặn chia sẻ mạng ngang hàng P2P nhằm tiết kiệm băng thông
- Lọc nội dung các trang web theo chủ đề, từ khóa
- Chống tấn công từ chối dịch vụ Dos/DDoS.

Bảng tổng quan các vật tư mạng:

		Workstation	Server	Network Equipment
Trụ sở chính	Phòng IT	3	10	1 switch tổng 2960 - 24TT 24 cổng, 1 wireless router, 1 router DSL
	Mỗi tầng	60	0	3 switch 2960 - 24TT 24 cổng, 1 wireless router
Chi nhánh DBP	Tầng 1	0	2	1 switch tổng 2960 - 24TT 24 cổng, 1 wireless router, 1 router DSL
	Tầng 2	60	0	2 switch 2960 - 24TT, 1 wireless router
Chi nhánh BHTQ	Tầng 1	0	2	1 switch tổng 2960 - 24TT 24 cổng, 1

				wireless router, 1 router DSL
	Tầng 2	60	0	2 switch 2960 - 24TT, 1 wireless router

● Các sơ đồ thiết kế:

Sơ đồ tòa nhà

Mỗi tòa nhà gồm 5 tầng, mỗi tầng 10 phòng, mỗi phòng được trang bị 6 máy tính. Mỗi tầng được lắp đặt 3 switch và 1 camera.

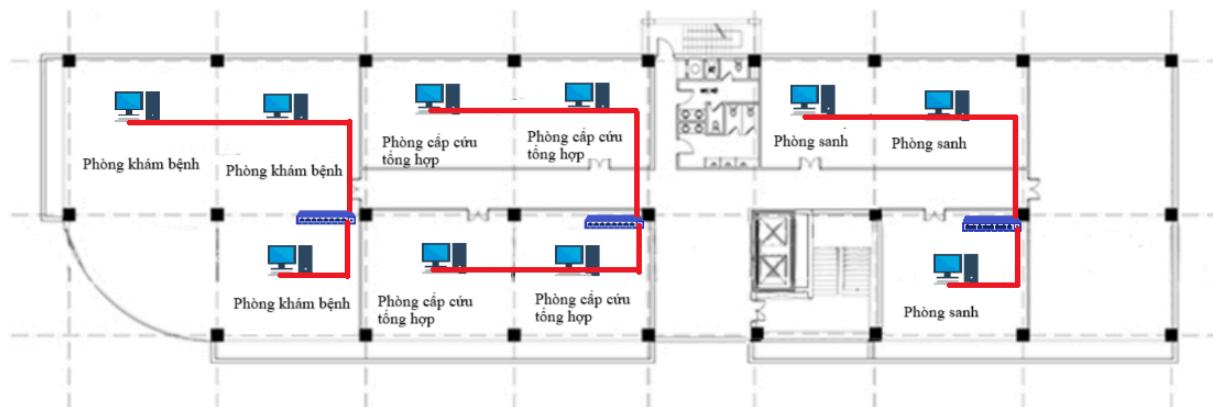
Tòa A gồm 5 tầng:

- Tầng 1: 4 phòng khoa KHTH - ĐT - CDT, 3 phòng tổ chức - hành chính, 3 phòng QLCL - CTXH - CSKH
- Tầng 2: 5 phòng chẩn đoán, 5 phòng dược
- Tầng 3: 5 phòng khám bệnh, 5 phòng cấp cứu tổng hợp
- Tầng 4: 5 phòng sanh, 5 phòng khoa phụ
- Tầng 5: 3 phòng hiếm muộn, 3 phòng hậu phẫu, hậu sản, 4 phòng HSTC và CD nhi

Tòa B gồm 5 tầng:

- Tầng 1: 3 phòng điều dưỡng, 3 phòng tài chính kế toán, 4 phòng công nghệ thông tin.
- Tầng 2: 5 phòng kiểm soát nhiễm khuẩn, 5 phòng xét nghiệm.
- Tầng 3: 5 phòng sơ sinh, 5 phòng nhi.
- Tầng 4: 5 phòng nhiễm nhi, 5 ngoại nhi.
- Tầng 5: 3 phòng liên chuyên khoa, 3 phòng gây mê hồi sức, 4 phòng dinh dưỡng.

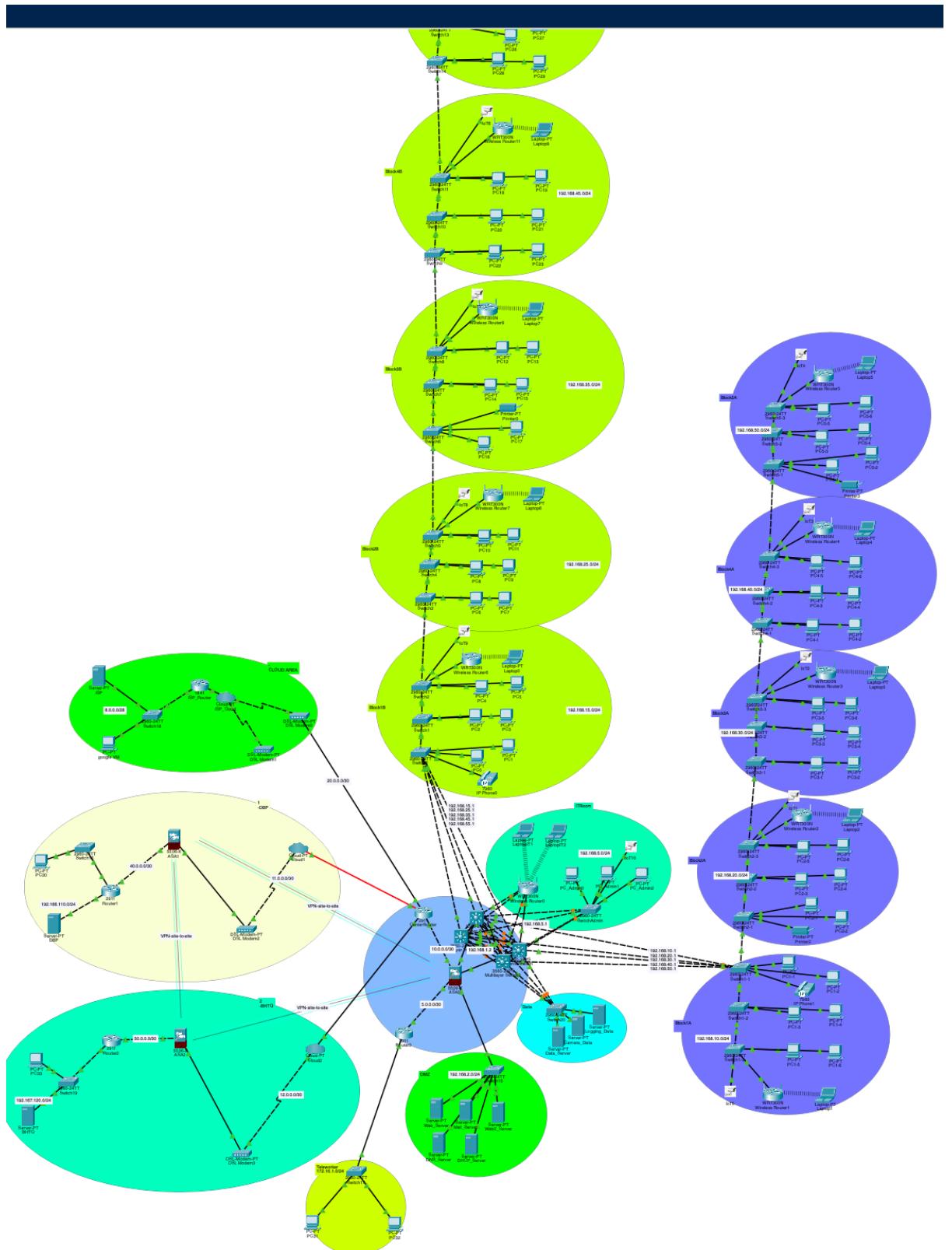
Sơ đồ đi dây và sơ đồ thiết bị



Soi dò IP

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WIC Address
serverPool	192.168.1.1	192.168.2.20	192.168.2.0	255.255.255.0	205	0.0.0	0.0.0
PhongIT	192.168.5.1	192.168.2.20	192.168.5.10	255.255.255.0	50	0.0.0	0.0.0
TangA2	192.168.20.1	192.168.2.20	192.168.20.10	255.255.255.0	205	0.0.0	0.0.0
TangA1	192.168.10.1	192.168.2.20	192.168.10.10	255.255.255.0	205	0.0.0	0.0.0
TangA4	192.168.40.1	192.168.2.20	192.168.40.10	255.255.255.0	205	0.0.0	0.0.0
TangA5	192.168.50.1	192.168.2.20	192.168.50.10	255.255.255.0	205	0.0.0	0.0.0
TangA3	192.168.30.1	192.168.2.20	192.168.30.10	255.255.255.0	205	0.0.0	0.0.0
TangB1	192.168.15.1	192.168.2.20	192.168.15.10	255.255.255.0	205	0.0.0	0.0.0
TangB2	192.168.25.1	192.168.2.20	192.168.25.10	255.255.255.0	205	0.0.0	0.0.0
TangB3	192.168.35.1	192.168.2.20	192.168.35.10	255.255.255.0	205	0.0.0	0.0.0
TangB4	192.168.45.1	192.168.2.20	192.168.45.10	255.255.255.0	205	0.0.0	0.0.0
TangB5	192.168.55.1	192.168.2.20	192.168.55.10	255.255.255.0	205	0.0.0	0.0.0

SƠ ĐỒ LUẬN LÝ



- Giải quyết yêu cầu bài toán:

LAN trung tâm:

Trung tâm được thiết kế các tầng có số lượng vật tư mạng là như nhau (trừ phòng kỹ thuật). Cụ thể như sau: mỗi tầng bao gồm 60 máy workstations, 3 switch 24, 1 wireless router và 1 dây đi ra tầng khác. Lý do đi dây như vậy là vì trong các giải pháp về dây cũng như thiết bị mạng, nhóm đã kiểm tra tất cả các trường hợp khả thi và đưa ra giải pháp đi dây tối ưu nhất, tiết kiệm nhất và vẫn không làm giảm tốc độ đường truyền.

Bảng giá các vật tư được liệt kê như sau:

Tên thiết bị	Hình ảnh	Số lượng	Giá
Linksys WRT300N wireless router		1 (cái)	1,499,791.67 VND
2960 – 24TT Switch		3 (cái)	2,291,458.33 VND x 3
Dây UTP CAT 5e 100BASE-TX (cuộn 300m)		300 (m)	1,350,000 VND
Tổng (1 tầng)			9,724,165 VND

(Theo www.ebay.com)



470.000
VND

$$470.000 \times 11 = 5.170.000 \text{ VND}$$

Do diện tích toàn nhà theo bản thiết kế là 14x20 m nên lượng dây ước tính trung bình cho mỗi tầng khoảng 200m dự trữ khoảng 100m dây 3 switch 24 nên có thể dùng tối đa $3 * 24 - 3 = 72$ máy, dự trữ khoảng 12 máy Như vậy, để tiết kiệm tối đa nhưng vẫn đạt hiệu suất cao, số lượng dự trữ đã được tối ưu hóa đến 1 con số chấp nhận được như trên.

Chi phí trên là chi phí cho riêng từng tầng (trừ phòng kỹ thuật) , ngoài ra còn có thêm các chi phí cho các vật tư sau:



Firewall ASA 5506

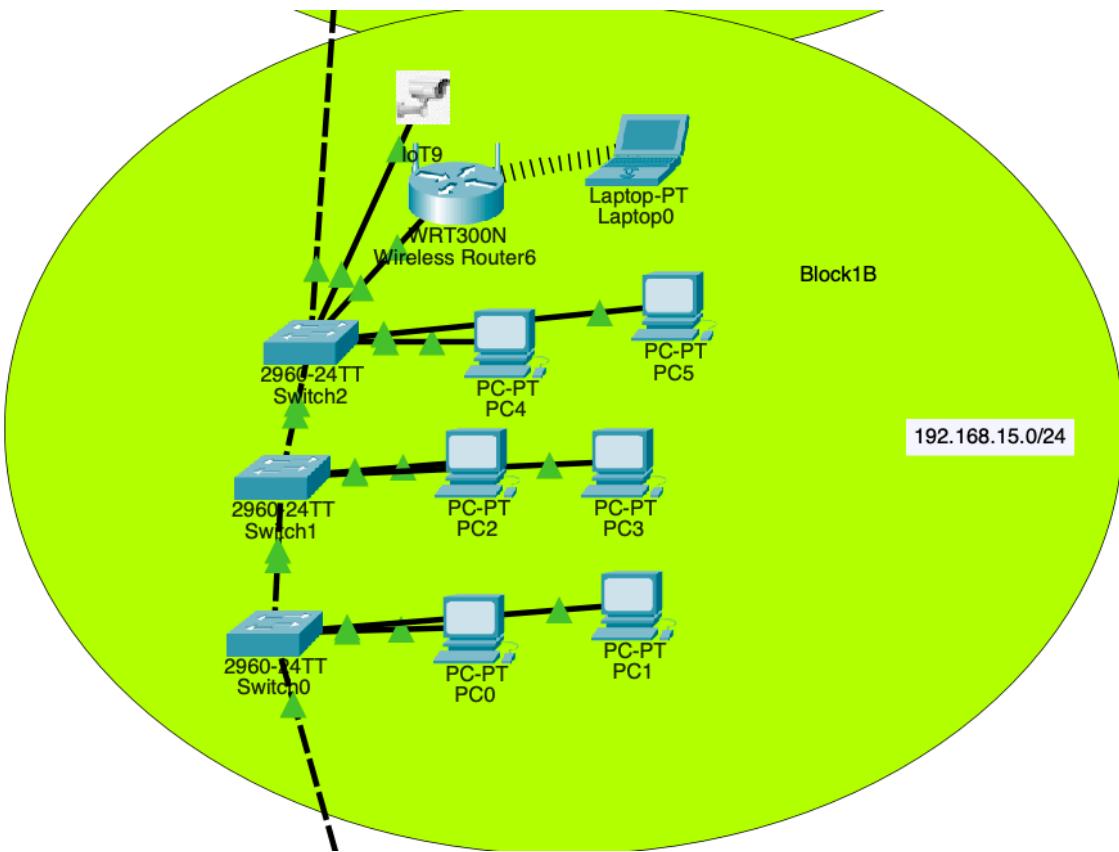
18.450.000VND

$$3 \text{ ASA } 5506 = 18.450.000 \times 3 = 55.350.000 \text{ VND}$$

Tên thiết bị	Hình ảnh	Số lượng	Giá
2960 – 24TT Switch		1 (cái)	2,291,458.33 VND <i>(theo ebay.com)</i>
Cisco 2621XM router		1 (cái)	1,145,833.33 VND <i>(theo ebay.com)</i>
Dây UTP CAT 5e 100BASE-TX (cuộn 300m)		300 (m)	1,350,000 VND <i>(theo vatgia.com)</i>
Cáp quang 100 BASE-SX		1000 (m)	9,500 VND x 1000 <i>(theo vatgia.com)</i>
Linksys WRT300N wireless router		1 (cái)	1,499,791.67 VND <i>(theo ebay.com)</i>
Tổng			15,787,082VND

Cấu hình cho các workstations, router:

Cấu hình các tầng:



Hệ thống 60 máy, 24 máy được nối vào switch 1, sau đó, 24 máy tiếp theo được nối vào switch 2, còn lại 12 máy và 1 Wireless router và 1 camera được nối vào switch còn lại, 1 dây đi ra ngoài, dây này có tốc độ đường truyền cao hơn nhiều lần so với các đường truyền khác. Các dây không sử dụng thì shutdown để tránh người xâm nhập vào hệ thống.

Cấu hình từng máy cụ thể như sau:

IP Configuration	
Interface	FastEthernet0
IP Configuration	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IPv4 Address	192.168.15.11
Subnet Mask	255.255.255.0
Default Gateway	192.168.15.1
DNS Server	192.168.2.20

Cấu hình wireless router:

LAN Settings

IP Configuration		
IPv4 Address	192.168.15.254	
Subnet Mask	255.255.255.0	

SSID	TangB1	
2.4 GHz Channel	1 - 2.412GHz	
Coverage Range (meters)	250,00	
Authentication		
<input type="radio"/> Disabled	<input type="radio"/> WEP	WEP Key
<input type="radio"/> WPA-PSK	<input checked="" type="radio"/> WPA2-PSK	PSK Pass Phrase
<input type="radio"/> WPA	<input type="radio"/> WPA2	12345678
RADIUS Server Settings		
IP Address		
Shared Secret		
Encryption Type	AES	

Cấu hình vLan cho Switch:

Switch0

Physical **Config** CLI Attributes

GLOBAL	
Settings	
Algorithm Settings	
SWITCHING	
VLAN Database	
INTERFACE	
FastEthernet0/1	
FastEthernet0/2	
FastEthernet0/3	
FastEthernet0/4	
FastEthernet0/5	
FastEthernet0/6	
FastEthernet0/7	
FastEthernet0/8	

VLAN Configuration

VLAN Number	
VLAN Name	
Add	Remove
VLAN No	VLAN Name
1	default
5	PhongIT
10	TangA1
15	TangB1
20	TangA2
25	TangB2
30	TangA3
35	TangB3
40	TangA4
45	TangB4

FastEthernet0/1		
Port Status	<input checked="" type="checkbox"/> On	
Bandwidth	<input type="radio"/> 100 Mbps	<input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex	<input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
Trunk	VLAN	1-1005
Tx Ring Limit	10	
FastEthernet0/2		
Port Status	<input checked="" type="checkbox"/> On	
Bandwidth	<input type="radio"/> 100 Mbps	<input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex	<input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
Access	VLAN	15
Tx Ring Limit	10	

Cấu hình tương tự cho switch 2 và 3 của cùng tầng B1.

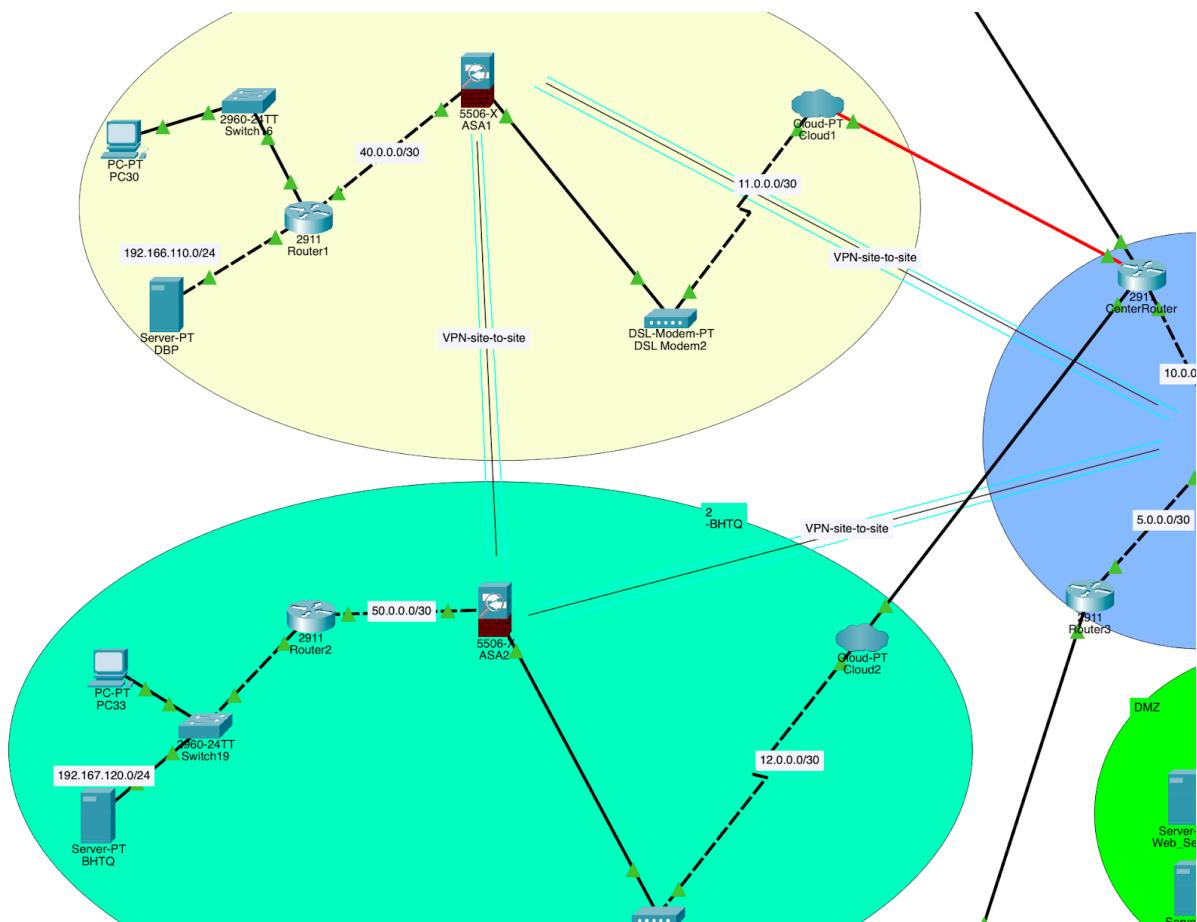
Cấu hình dải IP ở tầng này cho các workstations: từ 192.168.15.10 đến 192.168.15.254, subnet mask 255.255.255.0.

LAN chi nhánh

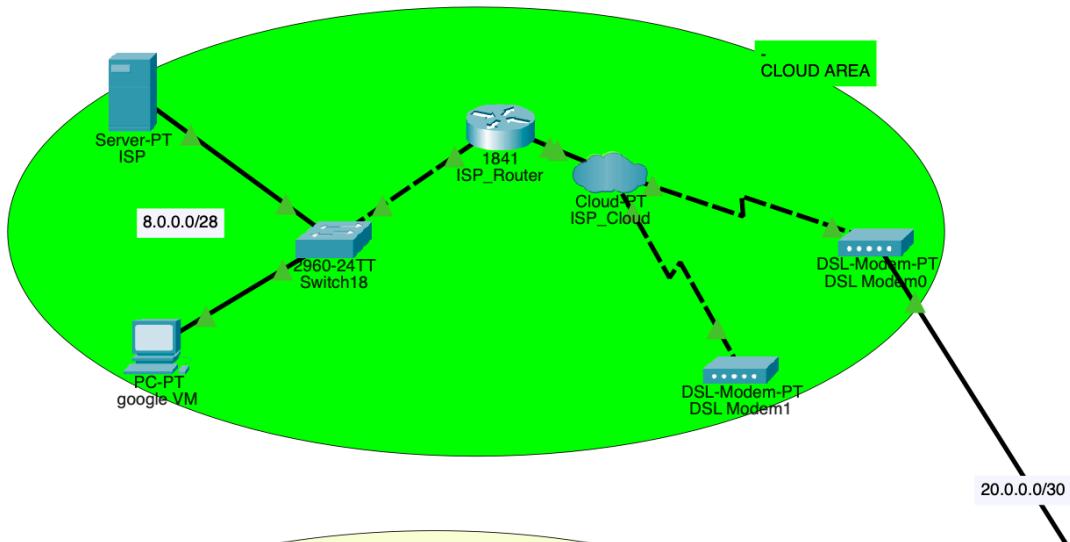
Chi nhánh được thiết kế lại theo bản vẽ tầng 2 trụ sở chính là tầng 1 cabling của chi nhánh, Tầng 2 lấy lại bản vẽ tầng 3 của trụ sở chính Sơ đồ luận lý, đi dây và sơ đồ bố trí máy đều hoàn toàn tương tự đối với phòng kỹ thuật và tầng kinh doanh của trụ sở chính công ty.

Kết nối ra Internet

Sơ đồ luận lý kết nối của chi nhánh:



Sơ đồ luận lý kết nối của trung tâm:



Cấu hình và các công nghệ sử dụng

Mạng dạng hình sao - Star Topology

Mạng dạng hình sao gồm có một trung tâm và các nút thông tin. Trong đó, các nút thông tin sẽ là các trạm đầu cuối, đôi khi cũng có thể là hệ thống máy tính và các thiết bị khác của mạng.

Trung tâm của mạng dạng hình sao sẽ có nhiệm vụ điều phối tất cả các hoạt động trong hệ thống. Do đó sẽ thực hiện các chức năng cơ bản như sau:

- Xác định các cặp địa chỉ gửi, nhận có quyền chiếm tuyến thông tin và thực hiện liên lạc với nhau
- Phê duyệt theo dõi và xử lý trong quá trình các thiết bị trao đổi thông tin với nhau
- Gửi thông báo về các trạng thái của mạng

Ưu điểm

- Có tốc độ nhanh nhất
- Đảm bảo hệ thống vẫn hoạt động bình thường, dù cáp mạng bị đứt gây mất kết nối của một máy
- Cấu trúc mạng đơn giản, giúp điều khiển thuật toán ổn định hơn
- Cho phép mở rộng mạng tùy theo nhu cầu của người dùng

Nhược điểm

- Khả năng mở rộng mạng phụ thuộc vào khả năng hoạt động của trung tâm. Nếu trung tâm gặp sự cố thì hệ thống mạng sẽ bị ngừng hoạt động.
- Yêu cầu kết nối độc lập với từng thiết bị ở các nút thông tin đến trung tâm. Khoảng cách kết nối giữa thiết bị và trung tâm cũng rất hạn chế, chỉ khoảng 100 m.
- Tốn kém chi phí cho dây mạng và thiết bị trung gian

Mạng dạng hình sao cho phép kết nối các máy tính với một bộ tập trung (HUB) thông qua cáp xoắn. Từ đó cho phép kết nối trực tiếp máy tính với HUB mà không cần thông qua trực BUS, giúp giảm thiểu các yếu tố gây ngưng trệ mạng

VLAN (Virtual Local Area Network)

Là cụm từ viết tắt của **Virtual Local Area Network** hay còn gọi là **mạng LAN ảo**, được hiểu là mạng tùy chỉnh được hình thành từ một hoặc nhiều mạng LAN khác nhau, giúp các nhóm thiết bị có thể kết nối với một mạng dùng không đặt cùng nhau.

Nếu Router đảm nhận vai trò chính là miền quảng cáo thì trong mạng VLAN thiết bị chuyển mạch Switch sẽ đảm nhận chức năng tương để tạo miền quảng bá. Do đó, nếu xét về kỹ thuật thì mạng LAN được xem như một miền quảng bá được tạo ra bởi Switch.

Hiểu đơn giản, VLAN là một kỹ thuật giúp quản trị viên thiết lập hệ thống nhiều mạng trên cùng một hạ tầng hệ thống. Mạng VLAN được sử dụng trong trường hợp mạng máy tính người dùng quá lớn với dung lượng truy cập quá nhiều. Đôi khi có những trường hợp người dùng VLAN chỉ đơn giản là vì máy tính của họ cũng đang dùng mạng VLAN.

Ưu điểm

- Hỗ trợ giải quyết các vấn đề thường gặp của broadcast như giảm kích thước của **broadcast domain**, tăng hiệu suất mạng.
- Dễ dàng thiết lập lớp bảo mật bổ sung, giúp đơn giản hóa việc quản lý thiết bị, quá trình này trở nên đơn giản, dễ dàng hơn.
- Tạo ra các nhóm thiết bị, hỗ trợ phân loại theo chức năng.
- Tổ chức mạng theo vị trí địa lý, giúp nâng cao hiệu suất và giảm độ trễ (**latency**).
- Bảo vệ thông tin nhạy cảm của người dùng, loại bỏ rào cản vật lý.
- Giúp cung cấp bảo mật mạng, tách biệt các máy chủ.
- Tiết kiệm chi phí nhờ không cần thêm phần cứng hoặc cáp.
- Dễ dàng thay đổi IP subnet của người dùng thông qua phần mềm.
- Giảm số lượng thiết bị cần thiết cho cấu trúc kết nối mạng, đồng thời hỗ trợ đơn giản hóa quá trình quản lý các thiết bị vật lý.

DHCP (Dynamic Host Configuration Protocol)

DHCP là một cơ chế tự động hóa việc gán địa chỉ IP cho các máy chủ cố định và máy chủ di động được kết nối có dây hoặc không dây.

Khi một thiết bị muốn truy cập vào mạng đang sử dụng DHCP, thiết bị đó sẽ yêu cầu địa chỉ IP từ máy chủ DHCP. Sau đó máy chủ DHCP sẽ phân phối địa chỉ IP đến thiết bị, giám sát việc sử dụng địa chỉ IP. Địa chỉ IP sau đó được sẽ được thu hồi và trả về nhóm địa chỉ do máy chủ DHCP quản lý để gán lại cho một thiết bị khác khi nó yêu cầu quyền truy cập vào mạng.

DHCP cũng chỉ định nhiều tham số mạng liên quan bao gồm subnet mask, địa chỉ gateway mặc định và domain name server (DNS).

Những lợi ích của giao thức DHCP:

DHCP được sử dụng để phân phối địa chỉ IP trong mạng và để định cấu hình mặt nạ mạng con (subnet mask), gateway và thông tin máy chủ DNS trên thiết bị. DHCP có thể mang đến những lợi ích đáng kể như:

- Giúp cấu hình địa chỉ IP đáng tin cậy khi DHCP có thể loại bỏ các lỗi để giảm thiểu xung đột, trùng địa chỉ IP, lỗi cấu hình hoặc lỗi chính tả đơn giản.
- Cung cấp cấu hình TCP/IP tập trung và tự động. Bằng cách triển khai DHCP relay agent, máy chủ DHCP không cần thiết phải có trên mọi mạng con.
- DHCP có thể xử lý hiệu quả các thay đổi địa chỉ IP cho người dùng trên các thiết bị di động di chuyển đến các vị trí khác nhau trên mạng có dây hoặc không dây.
- Tối ưu hóa địa chỉ IP. Giao thức DHCP không chỉ chỉ định các địa chỉ IP mà nó còn tự động lấy lại và đưa chúng trở lại nhóm địa chỉ IP khi chúng không còn được sử dụng nữa.
- Giúp các doanh nghiệp dễ dàng thay đổi lược đồ địa chỉ IP từ dải địa chỉ này sang dải địa chỉ khác. DHCP cho phép quản trị viên mạng thực hiện những thay đổi đó mà không làm gián đoạn cho người dùng cuối.

DNS (Domain Name System)

DNS là hệ thống phân giải tên miền cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền trên internet. Khi người dùng nhập địa chỉ trang web trên trình duyệt, DNS sẽ tìm địa chỉ IP của máy chủ chứa trang web và trả về kết quả hiển thị tương ứng của trang web cần tìm. Do đó, thay vì phải ghi nhớ địa chỉ IP phức tạp, người dùng có thể dễ dàng truy cập các trang web thông qua tên miền. Ngoài ra, DNS cũng giúp tăng tính linh hoạt và quản lý hiệu quả hơn cho hệ thống mạng, cung cấp tính bảo mật và tăng tốc độ truy cập internet.

WAN

Mạng diện rộng (WAN) là công nghệ kết nối các văn phòng, trung tâm dữ liệu, ứng dụng đám mây và bộ nhớ đám mây của bạn với nhau. Nó được gọi là mạng diện rộng vì không chỉ nằm trong phạm vi một tòa nhà hoặc khuôn viên rộng lớn mà còn mở rộng ra nhiều vị trí trải dài trên một khu vực địa lý cụ thể, hoặc thậm chí trên khắp thế giới. Ví dụ: các doanh nghiệp có nhiều văn phòng chi nhánh quốc tế sử dụng mạng WAN để kết nối các mạng văn phòng với nhau. Mạng WAN lớn nhất thế giới là Internet vì nó là tập hợp của nhiều mạng quốc tế kết nối với nhau.

Giao thức OSPF (Open Shortest Path First)

Giao thức OSPF hoạt động dựa vào thuật toán link state routing. Theo đó, mỗi bộ định tuyến sẽ chứa các thông tin của tất cả tên miền. Dựa vào những thông tin này, OSPF sẽ xác định quãng đường ngắn nhất. Điều này có nghĩa, mục tiêu chính của định tuyến là tìm hiểu về tuyến đường.

OSPF tìm hiểu toàn bộ bộ định tuyến cùng các mạng con có trong hệ thống mạng. Các bộ định tuyến sẽ chứa thông tin về mạng giống nhau. Chúng tiến hành tìm hiểu thông tin thông qua hoạt động gửi Link State Advertisements (LSA). Các LSA chứa thông tin về tất cả bộ định tuyến, mạng con, kể cả hệ thống mạng khác. Khi LSA bị đầy, giao thức OSPF sẽ thực hiện lưu trữ thông tin vào cơ sở dữ liệu có trạng thái liên kết (LSDB), với mục đích là chứa thông tin các bộ định tuyến một cách đồng nhất trong từng LSDB.

Firewall

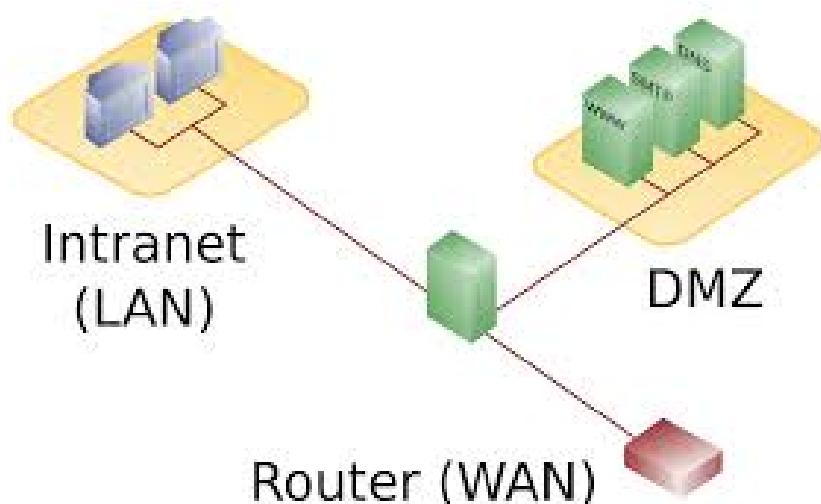
Firewall (Tường lửa) là phần mềm hoặc phần cứng được cài đặt và tích hợp vào mạng nhằm mục đích bảo mật, ngăn chặn sự xâm nhập trái phép vào hệ thống mạng. Tường lửa hoạt động như một bức tường phân chia giữa mạng trong nội bộ được bảo vệ và mạng bên ngoài tiềm ẩn nguy cơ mất an toàn thông tin.

Firewall kiểm soát tất cả lưu lượng truy cập vào và ra khỏi mạng, chặn tất cả các nỗ lực xâm nhập trái phép và cảnh báo các hoạt động đáng ngờ để đảm bảo an toàn. Để hiểu đơn giản, có thể hình dung nó giống như người canh gác ở cổng. Người canh sẽ quản lý và kiểm tra xem ai được phép vào ra, giữ an toàn cho các không gian bên trong.

Cấu hình các vùng inside, dmz và outside với security-level lần lượt là 100, 70 và 0

Các gói tin được phép đi ra từ vùng có security-level cao hơn sang vùng có security-level thấp hơn và ngược lại thì không được

Cấu hình các Access List để giải quyết vấn đề đó.



VPN

VPN (viết tắt của Virtual Private Network) là mạng riêng ảo. Chúng cho phép các thiết bị kết nối mạng một cách riêng tư thông qua Internet.

Chưa dừng lại ở đó, VPN còn tạo ra một kết nối an toàn giữa người dùng và Internet, giúp mã hóa dữ liệu và ngăn chặn theo dõi các hoạt động trực tuyến của người sử dụng nhờ vào việc ẩn địa chỉ IP.

VPN giúp nâng cao tính bảo mật dữ liệu cá nhân cho người dùng, chẳng hạn như: thông tin cá nhân, mật khẩu ngân hàng,... Điều này có thể làm ảnh hưởng trực tiếp đến bạn, chúng sẽ rao bán thông tin cho bên thứ ba.

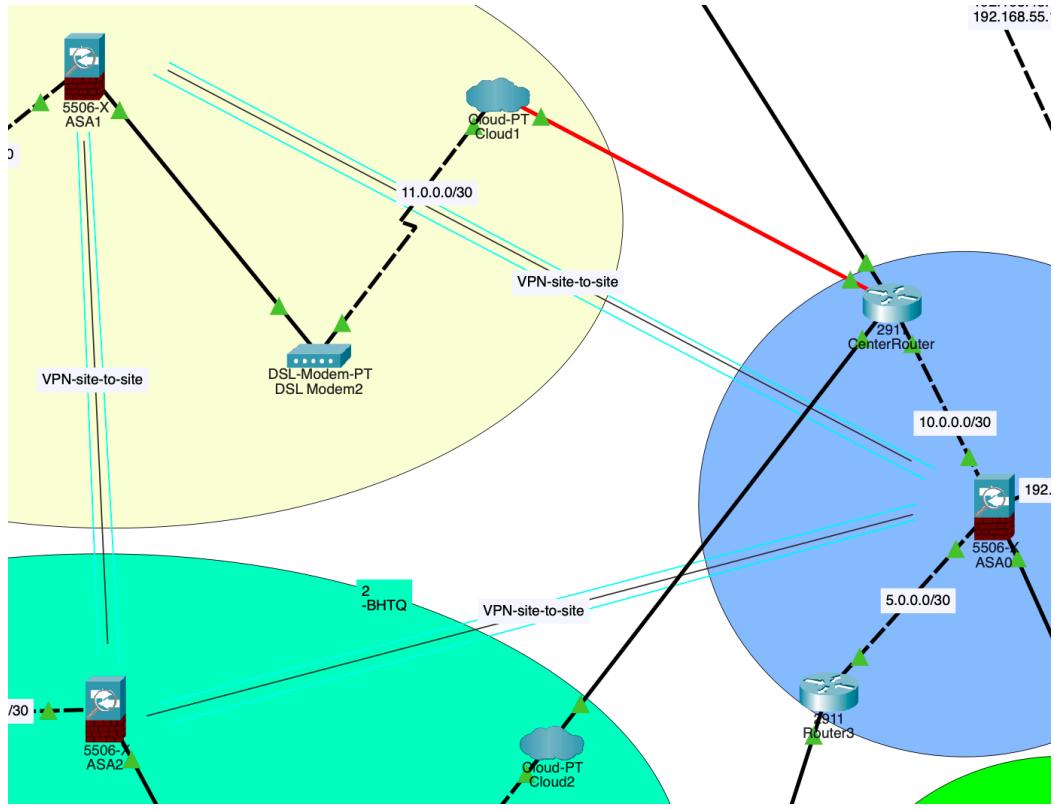
Trường hợp này rất dễ xảy ra nếu như bạn thường xuyên sử dụng Wi-Fi công cộng. Nguyên nhân chính là do quyền riêng tư của chúng thấp, hacker dễ dàng xâm nhập.

IPsec

IPSec, viết tắt của Internet Protocol Security, là một bộ giao thức mật mã bảo vệ lưu lượng dữ liệu qua mạng Internet Protocol (IP). Mạng IP – bao gồm cả World Wide Web – thiếu khả năng mã hóa và bảo vệ quyền riêng tư. VPN IPSec giải quyết điểm yếu này, bằng cách cung cấp một framework cho việc giao tiếp được mã hóa và riêng tư trên web.

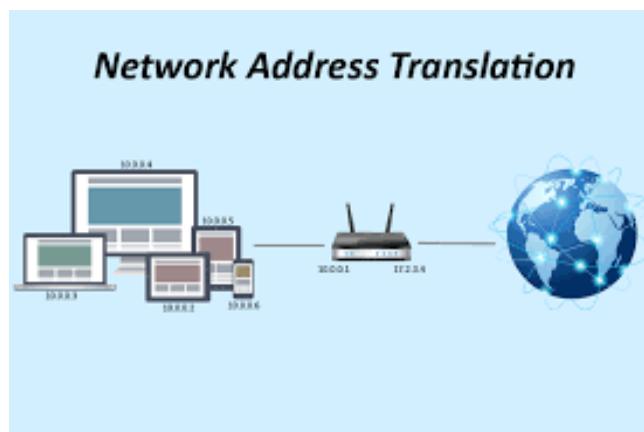
IPsec là một nhóm giao thức được sử dụng cùng nhau để thiết lập các kết nối được mã hóa giữa các thiết bị. Nó giúp bảo mật dữ liệu được gửi qua public network. Nhóm giao thức này thường được sử dụng để thiết lập VPN. Nó hoạt động bằng

cách mã hóa IP packet cùng với việc xác thực nguồn của các packet. Được ví như một đường hầm giữa các cơ sở.



NAT

NAT (Network Address Translation) là một kỹ thuật cho phép chuyển đổi từ một địa chỉ IP này thành một địa chỉ IP khác. Thông thường NAT được sử dụng phổ biến trong mạng sử dụng địa chỉ cục bộ, cần truy cập đến mạng công cộng (Internet).



Những cải tiến sau khi thuyết trình:

IPS/IDS

IPS là một trong những thành phần quan trọng trong các giải pháp bảo vệ hệ thống, hỗ trợ bảo mật dữ liệu. Tại sao mọi doanh nghiệp cần triển khai IPS? Đơn giản bởi:

- IPS mang đến khả năng giám sát, theo dõi các hoạt động bất thường trong lưu lượng truy cập hệ thống.
- Xác định đối tượng đang xâm nhập vào hệ thống với cách thức ra sao. Phát hiện vị trí trong cấu trúc mạng đang bị xâm nhập, khai thác.
- Cài đặt, thiết lập với hệ thống tường lửa để ngăn chặn kịp thời các hoạt động thâm nhập, phá hoại hệ thống hay ăn cắp dữ liệu.

Trong bài, nhóm quyết định đặt IPS ở center router trước firewall có thể bảo vệ được toàn bộ hệ thống bên trong kẽ cả firewall, **vùng DMZ**. Từ đó, có thể giảm thiểu các nguy cơ tấn công từ chối dịch vụ đối với firewall.

The screenshot shows a software interface for managing network services. At the top, there is a navigation bar with tabs: Physical, Config, Services, Desktop, and Software/Services. The Services tab is selected, and a sidebar on the left lists various services: HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, and FTP. The main panel is titled "Syslog" and contains a sub-section titled "Syslog". It features a table with columns: Service, Time, HostName, and Message. There are two radio buttons at the top right: "On" (selected) and "Off". The table data is as follows:

Service	Time	HostName	Message
1	1 00:06:03.786	192.168.1.1	%IPS-4-
2	1 00:06:09.815	192.168.1.1	%IPS-4-
3	1 00:06:15.825	192.168.1.1	%IPS-4-

CCTV

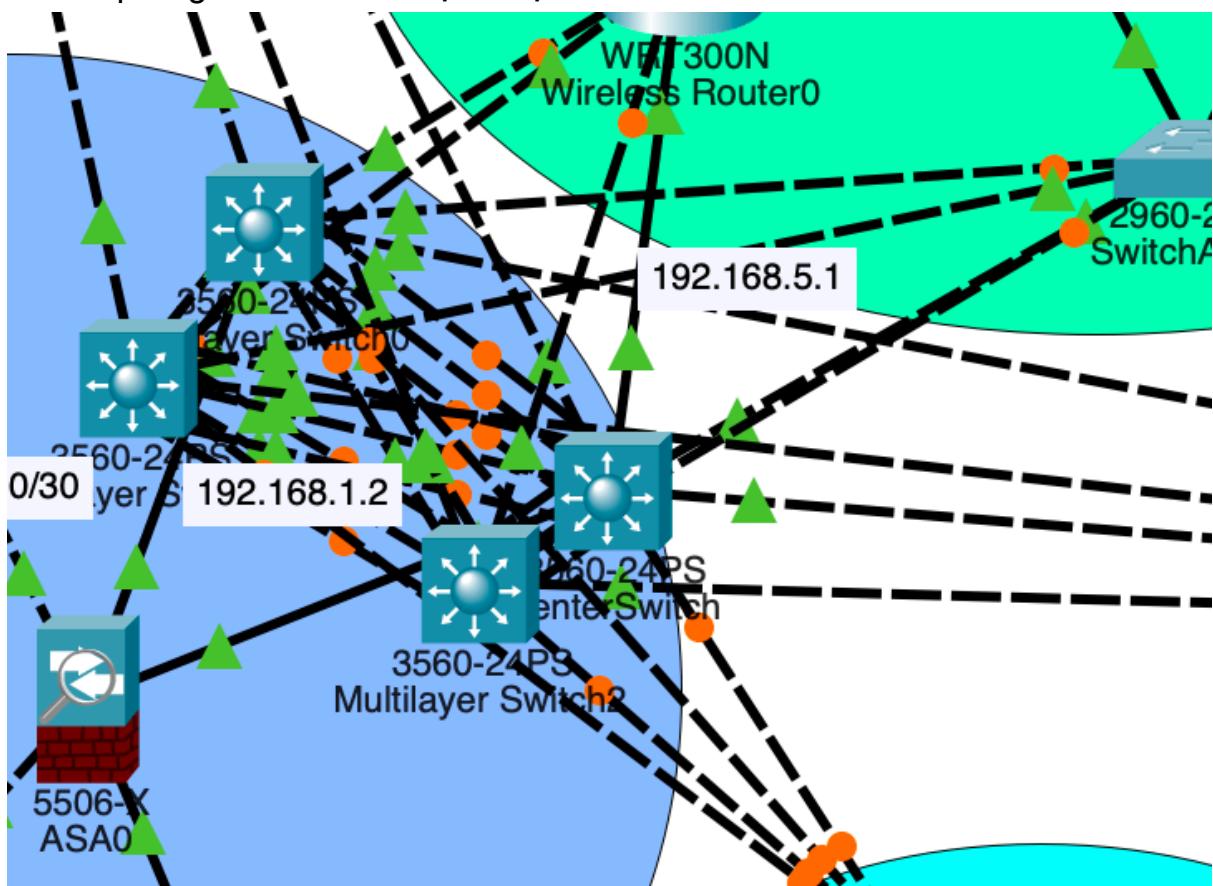
Hệ thống camera giám sát CCTV được cung cấp DHCP bởi VLAN riêng biệt ngăn chặn các kết nối từ các VLAN khác của 2 tòa nhà A và B ngoại trừ **Camera Data server (Host 192.168.1.20)** được quyền truy cập và xem nội dung camera CCTV bằng tài khoản và mật khẩu SSH cùng với đó khi một máy tính trong phòng IT kết nối với Host này cũng sẽ được cung cấp quyền truy cập vào camera CCTV thông qua việc sử dụng **default gateway 192.168.1.20**.



CORE SWITCH

Core switch ở hệ thống cấp phát ở 2 tòa nhà A và B được nâng cấp thành 4 cục để đảm bảo khi có sự cố xảy ra hoặc dừng hoạt động để sửa chữa bảo trì với một hoặc nhiều hơn một cục multi switch thì những cục còn lại vẫn không gặp vấn đề và hoạt động tốt đáp ứng nhu cầu kết nối sẽ không bị ảnh hưởng diện rộng trên toàn bộ 2 tòa nhà. Đồng thời, việc sử dụng đồng thời nhiều cục multi switch như vậy sẽ đáp bảo tốc độ truyền tải băng thông

luôn đáp ứng nhu cầu của bệnh viện.



Kiểm thử: xem video trong demo

Kết luận:

Kết luận dự án mạng máy tính bằng Packet Tracer

Sau khi hoàn thành dự án thiết kế và mô phỏng mạng máy tính bằng Cisco Packet Tracer, chúng em đã đạt được những mục tiêu đề ra và rút ra được nhiều bài học quan trọng:

1. Hoàn thành mục tiêu thiết kế mạng:

- Đã triển khai thành công các thành phần chính của mạng như định tuyến (Routing), chuyển mạch (Switching), cấu hình VLAN, và kết nối các thiết bị đầu cuối.
- Hệ thống mạng mô phỏng đáp ứng được các yêu cầu về hiệu năng, an toàn và khả năng mở rộng.

2. Tích lũy kinh nghiệm thực tiễn:

- Làm quen với các thiết bị mạng, giao thức và kỹ thuật cấu hình như RIP, OSPF, EIGRP, ACLs, NAT.
- Hiểu rõ cách thức các giao thức vận hành và phối hợp để đảm bảo truyền tải dữ liệu hiệu quả.

3. Thủ nghiệm và xử lý sự cố:

- Đã tiến hành kiểm tra hoạt động của hệ thống bằng cách sử dụng các công cụ kiểm tra gói tin và công cụ giám sát.
- Kỹ năng khắc phục sự cố được cải thiện nhờ việc phát hiện và sửa lỗi trong cấu hình.

4. Ý nghĩa thực tiễn:

- Mô hình mạng được xây dựng trong Packet Tracer có thể áp dụng như một bước thử nghiệm trước khi triển khai thực tế.
- Dự án giúp hiểu rõ hơn về tầm quan trọng của việc lập kế hoạch mạng, tính toán tài nguyên và dự đoán rủi ro.

Tóm lại, thông qua dự án này, nhóm chúng em đã có thêm kiến thức và kinh nghiệm quý báu trong lĩnh vực mạng máy tính. Đây là nền tảng để tiếp tục nghiên cứu và phát triển các hệ thống mạng phức tạp hơn trong tương lai.