

MỤC LỤC

DANH MỤC HÌNH ẢNH.....	ii
LỜI NÓI ĐẦU.....	1
CHƯƠNG I. TỔNG QUAN VỀ ĐỀ TÀI.....	2
1.1. GIỚI THIỆU ĐỀ TÀI.....	2
1.1.1. Lý do chọn đề tài.....	2
1.1.2. Mục tiêu đề tài.....	2
1.1.3. Các giai đoạn thực hiện đề tài.....	3
1.2. ĐỐI TƯỢNG, PHẠM VI NGHIÊN CỨU CỦA ĐỀ TÀI.....	3
CHƯƠNG II. KHẢO SÁT VÀ THIẾT KẾ HỆ THỐNG MẠNG.....	4
2.1. YÊU CẦU.....	4
2.2. GIẢI PHÁP CHO HỆ THỐNG MẠNG CỦA DOANH NGHIỆP:.....	4
CHƯƠNG III. TRIỂN KHAI TRÊN PHẦN MỀM PACKET TRACER.....	5
3.1. MÔ PHỎNG TRÊN PHẦN MỀM PACKET TRACER.....	5
3.2. CẤU HÌNH ĐẶT ĐỊA CHỈ IP.....	5
3.3. CẤU HÌNH SWITCH.....	6
3.3.1. VLAN là gì?.....	6
3.3.2. Cấu hình trên các Switch:.....	8
3.4. CẤU HÌNH ĐỊNH TUYẾN VÀ DHCP TRÊN ROUTER DOANH NGHIỆP.....	11
3.5. CẤU HÌNH NAT (NETWORK ADDRESS TRANSLATION).....	12
3.5.1. Tổng quan về NAT.....	12
3.5.2. Các khái niệm cơ bản:.....	13
3.5.3. Các kỹ thuật NAT:.....	14
3.5.4. Cấu hình Access – list và NAT overloading (PAT) trên Router DOANH NGHIỆP:.....	17
3.6. CẤU HÌNH DNS – SERVER CHO WEB – SERVER VÀ MAIL – SERVER.....	18
CHƯƠNG IV. KẾT QUẢ MÔ PHỎNG.....	19
4.1. KIỂM TRA KẾT NỐI CÁC PC TRONG CÙNG 1 PHÒNG BAN.....	19
4.2. KIỂM TRA KẾT NỐI CÁC PC TRONG GIỮA CÁC PHÒNG BAN KHÁC NHAU.....	20
4.3. KIỂM TRA TRUY CẬP WEB.....	21
4.4. KIỂM TRA MAIL – SERVER:.....	22
CHƯƠNG V. KẾT LUẬN.....	23

DANH MỤC HÌNH ẢNH

Hình 2.1. Sơ đồ các phòng ban trong doanh nghiệp.....	4
Hình 3.1. Mô hình mạng doanh nghiệp.....	5
Hình 3.2. Các khái niệm về NAT.....	14
Hình 3.3. Kỹ thuật NAT tĩnh.....	15
Hình 3.4. Cấu hình DNS – Server	18
Hình 4.1. Kiểm tra kết nối từ PC – IT đến Laptop – IT.....	19
Hình 4.2. Ping từ PC – phòng kinh doanh đến Laptop – phòng kinh doanh.....	19
Hình 4.3. Ping từ PC – phòng kế toán đến Laptop – phòng kế toán	20
Hình 4.4. Ping từ PC – IT đến PC – PHÒNG KINH DOANH	20
Hình 4.5. Ping PC – PHÒNG KINH DOANH đến Laptop – PHÒNG KẾ TOÁN.....	20
Hình 4.6. Ping PC – PHÒNG KẾ TOÁN đến GIÁM ĐỐC.....	21
Hình 4.7. Truy cập Web với tên miền doanhnghiep.com	21
Hình 4.8. Truy cập Web google.com.vn	21
Hình 4.9. Gửi Email trong phòng IT	22
Hình 4.10. Gửi Email từ Phòng kế toán đến Phòng kinh doanh.....	22

LỜI NÓI ĐẦU

Trong thời gian nghiên cứu và học tập môn học ***Đồ án chuyên ngành kỹ thuật viễn thông 2***, cùng với nội dung bài tập lớn thiết kế xây dựng hệ thống mạng LAN cho doanh nghiệp đã nhận được sự giúp đỡ quý báu của các thầy giáo, cô giáo và các bạn, em đã hoàn thành chương trình và bài báo đồ án này với đề tài ***Xây dựng hệ thống mạng LAN cho doanh nghiệp***.

Cho phép em được bày tỏ lời cảm ơn các thầy cô giáo trong khoa đã giúp đỡ em hoàn thành chương trình và bài báo cáo này.

Đồng thời em gửi lời cảm ơn đặc biệt về sự hướng dẫn và chỉ bảo tận tình của thầy ***Hồ Đức Tâm Linh*** đã tận tình hướng dẫn giúp đỡ em trong suốt quá trình hoàn thành chương trình cũng như bài báo cáo này.

Do thời gian có hạn, cũng như kinh nghiệm còn thiếu nên trong chương trình cũng như báo cáo này sẽ không tránh khỏi những thiếu sót, hạn chế nhất định. Em rất mong nhận được nhận xét góp ý của thầy cô và các bạn.

Em xin chân thành cảm ơn !

CHƯƠNG I.

TỔNG QUAN VỀ ĐỀ TÀI

1.1. GIỚI THIỆU ĐỀ TÀI

1.1.1. Lý do chọn đề tài

- ✓ Ngày nay công nghệ thông tin trở thành một lĩnh vực mũi nhọn trong công cuộc phát triển kinh tế xã hội. Cùng với công nghệ sinh học và năng lượng mới, công nghệ thông tin (CNTT) vừa là công cụ, vừa là động lực thúc đẩy quá trình công nghiệp hóa, hiện đại hóa đất nước.
- ✓ Có thể nói trong khoa học máy tính không lĩnh vực nào có thể quan trọng hơn lĩnh vực nối mạng. Mạng máy tính là hai hay nhiều máy tính được kết nối với nhau theo một cách nào đó sao cho chúng có thể trao đổi thông tin qua lại với nhau, dùng chung hoặc chia sẻ dữ liệu thông qua việc in ấn hay sao chép qua đĩa mềm, CDroom....
- ✓ Do đó hạ tầng mạng máy tính là phần không thể thiếu trong các tổ chức hay các công ty, trường học. Trong điều kiện kinh tế hiện nay hầu hết đa số các tổ chức hay các công ty, trường học có phạm vi sử dụng bị giới hạn bởi diện tích và mặt bằng đều triển khai xây dựng mạng LAN để phục vụ cho việc quản lý dữ liệu nội bộ cơ quan mình được thuận lợi, đảm bảo tính an toàn dữ liệu cũng như tính bảo mật dữ liệu mặt khác mạng Lan còn giúp các nhân viên trong các tổ chức, nhà trường hay công ty truy nhập dữ liệu một cách thuận tiện với tốc độ cao, giúp việc.
- ✓ Vì thế đề tài ***“Xây dựng hệ thống mạng doanh nghiệp”*** được tiến hành nhằm góp phần giải quyết vấn đề bảo vệ an ninh, an toàn dữ liệu nội bộ, nhằm tăng hiệu suất làm việc của công ty.

1.1.2. Mục tiêu đề tài

- ✓ Phân loại mạng máy tính theo phạm vi địa lý (LAN, WAN, GAN, MAN), theo TOPO và theo từng chức năng.
- ✓ Mô hình tham chiếu hệ thống mở OSI và các bộ quản thúc mô hình TCP/IP.
- ✓ Các kiến thức cơ bản về LAN, các phương pháp điều khiển truy cập trong LAN, các công nghệ và các chuẩn cáp, các phương pháp đi cáp.
- ✓ Có thể thiết kế và xây dựng các mạng LAN, WAN và các dịch vụ khác trong mạng có thể phục vụ tốt được các yêu cầu thực tế của các tổ chức hay bất kỳ một công ty nào, mang lại hiệu quả kinh tế cao.

1.1.3. Các giai đoạn thực hiện đề tài

Quá trình nghiên cứu đề tài được tiến hành qua các bước như sau:

✓ **Giai đoạn 1 - Thu thập dữ liệu:**

- Khảo sát tình hình thực tiễn, thu thập dữ liệu (thu thập các yêu cầu từ phía người sử dụng, phân tích yêu cầu, tìm các bài viết, tài liệu liên quan...). Nghiên cứu tài liệu, tìm hiểu các phương pháp, tiếp cận đã biết, tham khảo các hệ thống mạng ở các công ty hiện tại đang được sử dụng. Phác họa bức tranh tổng thể, thiết kế giải pháp.

✓ **Giai đoạn 2 – Thiết kế giải pháp:** Từ yêu cầu của khách hàng ta bắt đầu:

- Thiết kế sơ đồ mạng ở mức luận lý: Thiết kế sơ đồ mạng ở mức luận lý liên quan đến việc chọn lựa mô hình mạng, giao thức mạng và thiết đặt các cấu hình cho các thành phần nhận dạng mạng. Những vấn đề chung nhất khi thiết đặt cấu hình cho mô hình mạng là:
 - Định vị các thành phần nhận dạng mạng, bao gồm việc đặt tên cho Domain, Workgroup, máy tính, định địa chỉ IP cho các máy, định cổng cho từng dịch vụ.
 - Phân chia mạng con, thực hiện vạch đường đi cho thông tin trên mạng.
- Xây dựng chiến lược khai thác và quản lý tài nguyên mạng.
- Thiết kế sơ đồ mạng ở mức vật lý, chọn hệ điều hành và các phần mềm ứng dụng.
- Cài đặt mạng, kiểm thử.
- Bảo trì hệ thống.

✓ **Giai đoạn 3 - Tổng kết:** Khái quát hóa và rút ra kết luận chung cho đề tài. Viết báo cáo, công bố kết quả nghiên cứu đề tài.

1.2. ĐỐI TƯỢNG, PHẠM VI NGHIÊN CỨU CỦA ĐỀ TÀI

Đề tài có thể được áp dụng sử dụng làm mô hình kết nối mạng cho doanh nghiệp.

➤ **Phương pháp nghiên cứu**

- Khảo sát thực tế việc ứng dụng các hệ thống mạng trong công ty.
- Thu thập các tài liệu liên quan đến việc thiết kế và xây dựng mô hình mạng cho công ty.
- Thực hiện các công việc như: thu thập các yêu cầu của khách hàng, phân tích yêu cầu, thiết kế giải pháp...

➤ **Ý nghĩa lý luận và thực tiễn của đề tài:**

- Ý nghĩa của đề tài đã được nêu rất rõ trong phần lí do lựa chọn đề tài là giúp cho các công ty có thể bảo vệ an ninh, an toàn dữ liệu nội bộ, giúp nhân viên trong công ty truy nhập dữ liệu một cách thuận tiện với tốc độ cao.

CHƯƠNG II.

KHẢO SÁT VÀ THIẾT KẾ HỆ THỐNG MẠNG

2.1. YÊU CẦU

- Một doanh nghiệp cần sử dụng một hệ thống mạng máy tính để phục vụ cho việc vận hành sản xuất và kinh doanh sản phẩm. Doanh nghiệp có Ban Giám đốc gồm 1 Giám đốc và 2 Phó Giám đốc, và có 4 phòng ban gồm Phòng vật tư, Phòng Hành chính, phòng kinh doanh và phòng kế toán. Các máy tính sử dụng hệ điều hành Windows 10 để nhân viên làm việc. Một máy chủ sử dụng hệ điều hành Windows Server 2016 để quản lý các máy tính khác trong mạng. Doanh nghiệp cũng sử dụng một máy in để in ấn tài liệu và máy in được chia sẻ để cho các nhân viên đều có thể sử dụng. Hệ thống mạng kết nối Internet bằng một đường truyền ADSL.
- Đối với máy chủ, yêu cầu chi tiết như sau:
 - Cài đặt dịch vụ Active Directory điều khiển vùng (domain controller), tạo tài khoản người dùng và phân quyền cho người dùng.
 - Cài đặt DHCP cấp IP động cho các máy trạm trong mạng.
 - Cấu hình File Server tạo các thư mục dùng chung và phân quyền truy cập vào các thư mục.
 - Cấu hình Printer Server, cài đặt và chia sẻ máy in trong mạng.

2.2. GIẢI PHÁP CHO HỆ THỐNG MẠNG CỦA DOANH NGHIỆP:

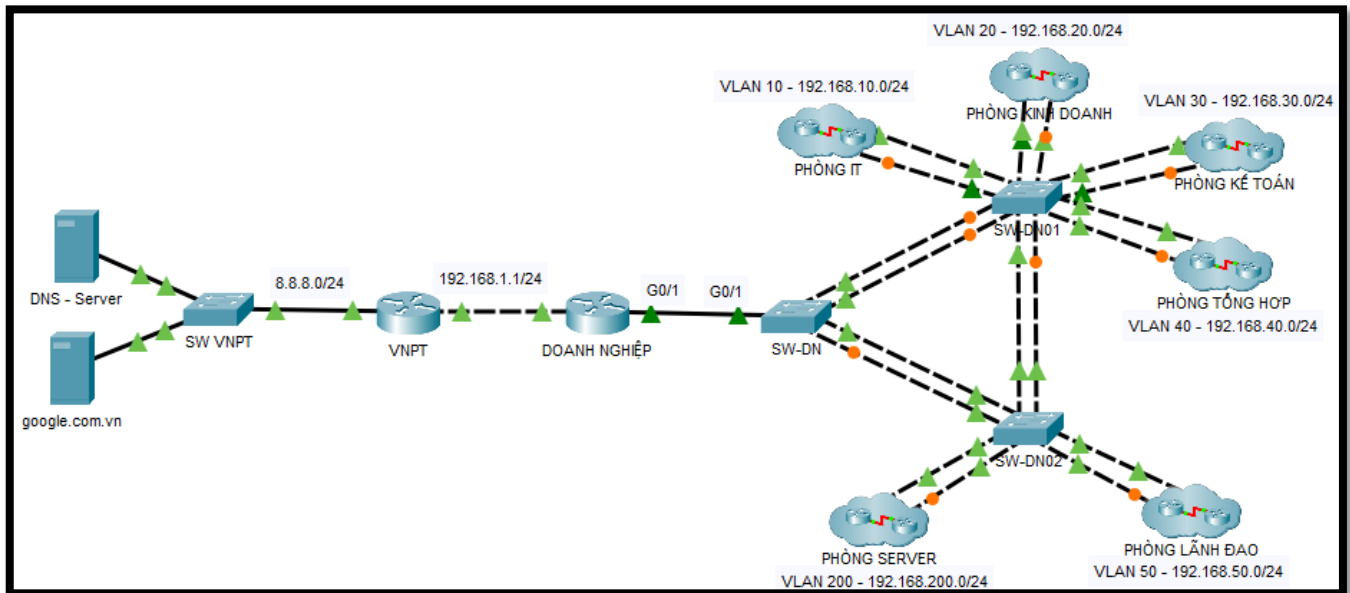
- Xây dựng hệ thống mạng Domain quản lý User và dữ liệu tập trung. Đảm bảo hệ thống mạng vận hành một cách trơn tru, đáp ứng tất cả yêu cầu của trung tâm. Hệ thống mạng còn phải có tính linh hoạt cao, có thể bổ sung thêm máy tính và các thành phần mạng nhanh chóng mà không mất nhiều thời gian và chi phí.
- Mô hình sử dụng máy tính của một doanh nghiệp nhỏ như sau:



Hình 2.1. Sơ đồ các phòng ban trong doanh nghiệp

CHƯƠNG III. TRIỂN KHAI TRÊN PHẦN MỀM PACKET TRACER

3.1. MÔ PHỎNG TRÊN PHẦN MỀM PACKET TRACER



Hình 3.1. Mô hình mạng doanh nghiệp

3.2. CẤU HÌNH ĐẶT ĐỊA CHỈ IP

Bảng địa chỉ:

Device	Interface	IP Address	Subnet Mask	Default – gateway
DOANH-NGHIEP	Fa0/0	113.114.115.1	255.255.255.0	N/A
	Fa0/1.10	192.168.10.1	255.255.255.0	N/A
	Fa0/1.20	192.168.20.1	255.255.255.0	N/A
	Fa0/1.30	192.168.30.1	255.255.255.0	N/A
	Fa0/1.100	192.168.100.1	255.255.255.0	N/A
VNPT	Fa0/1	115.114.113.1	255.255.255.0	N/A
	Fa0/0.10	172.16.10.1	255.255.255.0	N/A
	Fa0/0.20	172.16.20.1	255.255.255.0	N/A
	Fa0/0.30	172.16.30.1	255.255.255.0	N/A
	Fa0/0.100	172.16.100.1	255.255.255.0	N/A
Google.com	NIC	8.8.8.254	255.255.255.0	8.8.8.1
Doanhnghiep.com	NIC	192.168.200.254	255.255.255.0	192.168.200.1
DNS – SERVER	NIC	8.8.8.8	255.255.255.0	8.8.8.1
MAIL – SERVER	NIC	192.168.200.253	255.255.255.0	192.168.200.1

3.3. CẤU HÌNH SWITCH

3.3.1. VLAN là gì?

VLAN là viết tắt của Virtual Local Area Network hay còn gọi là mạng LAN ảo. Một VLAN được định nghĩa là một nhóm logic các thiết bị mạng và được thiết lập dựa trên các yếu tố như chức năng, bộ phận, phòng ban của công ty, doanh nghiệp...

Hiện nay, VLAN đóng một vai trò rất quan trọng trong công nghệ mạng LAN. Để thấy rõ được lợi ích này chúng ta hãy xét một ví dụ:

Một công ty thuê một tòa nhà 3 tầng, mỗi tầng có 3 phòng ban (phòng kế toán, phòng kinh doanh, phòng IT...). Mỗi phòng phải dùng 1 Switch để kết nối các thiết bị như máy tính, máy in... Vậy mỗi tầng phải sử dụng 3 Switch và cả tòa nhà là 9 Switch. Cách làm trên là rất tốn kém chi phí và không tận dụng hết số cổng trên 1 Switch. Chính vì vậy, VLAN ra đời nhằm giải quyết vấn đề trên một cách đơn giản và tiết kiệm được chi phí.

❖ Phân loại VLAN:

- ✓ **Port - based VLAN:** là cách cấu hình VLAN đơn giản và phổ biến. Mỗi cổng của Switch được gán với một VLAN xác định (mặc định là VLAN1), do vậy bất cứ thiết bị host nào gán vào cổng đó đều thuộc một VLAN nào đó.
- ✓ **MAC address based VLAN:** Cách cấu hình này ít được sử dụng do còn nhiều bất tiện trong việc quản lý. Mỗi địa chỉ MAC được đánh dấu với một VLAN xác định.
- ✓ **Protocol – based VLAN:** Cách cấu hình này gần giống như MAC Addressbased, nhưng sử dụng một địa chỉ logic hay địa chỉ IP thay thế cho địa chỉ MAC. Cách cấu hình không còn thông dụng nhờ sử dụng giao thức DHCP.

❖ Lợi ích của VLAN:

- ✓ **Tiết kiệm băng thông của hệ thống mạng:** VLAN chia mạng LAN thành nhiều đoạn nhỏ, mỗi đoạn đó là một vùng quảng bá (broadcast domain). Khi có gói tin quảng bá (broadcast), nó sẽ được truyền duy nhất trong VLAN tương ứng. Do đó việc chia VLAN giúp tiết kiệm băng thông của hệ thống mạng.
- ✓ **Tăng khả năng bảo mật:** Do các thiết bị ở các VLAN khác nhau không thể truy nhập vào nhau (trừ khi ta sử dụng router nối giữa các VLAN). Như trong ví dụ trên, các máy tính trong VLAN phòng kế toán chỉ có thể liên lạc được với nhau. Máy ở VLAN phòng kế toán không thể kết nối được với máy tính ở VLAN phòng IT.

✓ **Dễ dàng thêm hay bớt máy tính vào VLAN:** Việc thêm một máy tính vào VLAN rất đơn giản, chỉ cần cấu hình cổng cho máy đó vào VLAN mong muốn.

✓ **Giúp mạng có tính linh động cao:**

- VLAN có thể dễ dàng di chuyển các thiết bị. Giả sử trong ví dụ trên, sau một thời gian sử dụng công ty quyết định để mỗi phòng ban ở một tầng riêng biệt. Ta chỉ cần cấu hình lại các cổng switch rồi đặt chúng vào các VLAN theo yêu cầu.
- VLAN có thể được cấu hình tĩnh hay động. Trong cấu hình tĩnh, người quản trị mạng phải cấu hình cho từng cổng của mỗi switch. Sau đó, gán cho nó vào một VLAN nào đó. Trong cấu hình động mỗi cổng của switch có thể tự cấu hình VLAN cho mình dựa vào địa chỉ MAC của thiết bị được kết nối vào.

❖ **Tạo VLAN:**

Có 2 cách tạo VLAN như sau:

Cách 1: Ở privileged mode `vlan database` `vlan name`

vlan database

vlan < VLAN ID > name < Tên VLAN >

Cách 2: Ở configured mode `vlan name`

vlan < VLAN ID >

name < Tên VLAN >

Lưu ý:

- VLAN ID là số từ 1 tới 1005, nên đặt VLAN ID từ 2 trở lên vì VLAN 1 là default VLAN, mặc định mọi Switch đều có VLAN này.
- Tên VLAN không bắt buộc phải đặt, nhưng cần đặt tên để tiện quản lý ví dụ như Phong_KeToan, VLAN_Tang1...

3.3.2. Cấu hình trên các Switch:

✓ SW – DN:

```
Switch>enable
Switch#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-DN
SW-DN(config)#vtp mode server
Device mode already VTP SERVER.
SW-DN(config)#vtp domain minhhtue.com
Changing VTP domain name from NULL to minhhtue.com
SW-DN(config)#vtp pass minhhtue.com
Setting device VLAN database password to minhhtue.com
SW-DN(config)#vlan 10
SW-DN(config-vlan)#name PHONG-IT
SW-DN(config-vlan)#vlan 20
SW-DN(config-vlan)#name PHONG-KINH-DOANH
SW-DN(config-vlan)#vlan 30
SW-DN(config-vlan)#name PHONG-KE-TOAN
SW-DN(config-vlan)#vlan 40
SW-DN(config-vlan)#name PHONG-TONG-HOP
SW-DN(config-vlan)#vlan 50
SW-DN(config-vlan)#name PHONG-GIAM-DOC
SW-DN(config-vlan)#vlan 200
SW-DN(config-vlan)#name PHONG-SERVER
SW-DN(config)#interface gigabitEthernet0/1
SW-DN(config-if)#switchport mode trunk
SW-DN(config-if)#exit
SW-DN(config)#int range interface fastEthernet0/1-24
SW-DN(config-if-range)#spanning-tree portfast
```

✓ **SW – DN01, SW – DN02:**

```
Switch>enable
Switch#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-DN01
SW-DN01(config)#vtp mode client
Device mode already VTP CLIENT.
SW-DN01(config)#vtp domain minhhtue.com
SW-DN01(config)#vtp pass minhhtue.com
SW-DN01(config)#interface range gigabitEthernet0/1-2
SW-DN01(config-if)#switchport mode trunk
SW-DN01(config-if)#exit
SW-DN01(config)#interface range fastEthernet0/23-24
SW-DN01(config-if-range)#switchport mode trunk
SW-DN01(config-if)#exit
SW-DN01(config)#interface range fastEthernet0/1-24
SW-DN01(config-if-range)#spanning-tree portfast
SW-DN01(config-if-range)#end
SW-DN01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Làm tương tự cho SW – DN02.

✓ **Switch các phòng ban của doanh nghiệp:**

```
Switch>enable
Switch#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-IT
SW-IT(config)#vtp mode client
Device mode already VTP CLIENT.
SW-IT(config)#vtp domain minhhtue.com
SW-IT(config)#vtp pass minhhtue.com
SW-IT(config)#interface range gigabitEthernet0/1-2
SW-IT(config-if)#switchport mode trunk
SW-IT(config-if)#exit
SW-IT(config)#interface range fastEthernet0/1-24
SW-IT(config-if-range)#switchport mode access
SW-IT(config-if-range)#switchport access vlan 10
SW-IT(config-if-range)#spanning-tree portfast
SW-IT(config-if-range)#end
SW-IT#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

- Làm tương tự cho các phòng ban tương ứng:
 - Phòng IT: VLAN 10.
 - Phòng kinh doanh: VLAN 20.
 - Phòng kế toán: VLAN 30.
 - Phòng tổng hợp: VLAN 40.
 - Phòng giám đốc: VLAN 50.
 - Phòng server: VLAN 200.

3.4. CẤU HÌNH ĐỊNH TUYẾN VÀ DHCP TRÊN ROUTER DOANH NGHIỆP

```
DOANH-NGHIEP(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
DOANH-NGHIEP(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
DOANH-NGHIEP(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.10
DOANH-NGHIEP(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.10
DOANH-NGHIEP(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.10
DOANH-NGHIEP(config)#ip dhcp excluded-address 192.168.50.1 192.168.50.10
DOANH-NGHIEP(config)#ip dhcp pool VLAN10
DOANH-NGHIEP(dhcp-config)#network 192.168.10.0 255.255.255.0
DOANH-NGHIEP(dhcp-config)#default-router 192.168.10.1
DOANH-NGHIEP(dhcp-config)#dns-server 8.8.8.8
DOANH-NGHIEP(dhcp-config)#exit
DOANH-NGHIEP(config)#ip dhcp pool VLAN20
DOANH-NGHIEP(dhcp-config)#network 192.168.20.0 255.255.255.0
DOANH-NGHIEP(dhcp-config)#default-router 192.168.20.1
DOANH-NGHIEP(dhcp-config)#dns-server 8.8.8.8
DOANH-NGHIEP(dhcp-config)#exit
DOANH-NGHIEP(config)#ip dhcp pool VLAN30
DOANH-NGHIEP(dhcp-config)#network 192.168.30.0 255.255.255.0
DOANH-NGHIEP(dhcp-config)#default-router 192.168.30.1
DOANH-NGHIEP(dhcp-config)#dns-server 8.8.8.8
DOANH-NGHIEP(dhcp-config)#exit
DOANH-NGHIEP(config)#ip dhcp pool VLAN40
DOANH-NGHIEP(dhcp-config)#network 192.168.40.0 255.255.255.0
DOANH-NGHIEP(dhcp-config)#default-router 192.168.40.1
DOANH-NGHIEP(dhcp-config)#dns-server 8.8.8.8
DOANH-NGHIEP(dhcp-config)#exit
DOANH-NGHIEP(config)#ip dhcp pool VLAN50
DOANH-NGHIEP(dhcp-config)#network 192.168.50.0 255.255.255.0
DOANH-NGHIEP(dhcp-config)#default-router 192.168.50.1
DOANH-NGHIEP(dhcp-config)#dns-server 8.8.8.8
DOANH-NGHIEP(dhcp-config)#exit
DOANH-NGHIEP(config)#ip dhcp pool VLAN200
DOANH-NGHIEP(dhcp-config)#network 192.168.200.0 255.255.255.0
DOANH-NGHIEP(dhcp-config)#default-router 192.168.200.1
DOANH-NGHIEP(dhcp-config)#dns-server 8.8.8.8
```

3.5. CẤU HÌNH NAT (NETWORK ADDRESS TRANSLATION)

3.5.1. Tổng quan về NAT

NAT giống như một router, nó chuyển tiếp các gói tin giữa những lớp mạng khác nhau trên một mạng lớn. NAT dịch hay thay đổi một hoặc cả hai địa chỉ bên trong một gói tin khi gói tin đó đi qua một router, hay một số thiết bị khác. Thông thường, NAT thường thay đổi địa chỉ (thường là địa chỉ riêng) được dùng bên trong một mạng sang địa chỉ công cộng.

NAT cũng có thể coi như một firewall cơ bản. Để thực hiện được công việc đó, NAT duy trì một bảng thông tin về mỗi gói tin được gửi qua. Khi một PC trên mạng kết nối đến 1 website trên Internet header của địa chỉ IP nguồn được thay đổi và thay thế bằng địa chỉ Public mà đã được cấu hình sẵn trên NAT Server, sau khi có gói tin trở về NAT dựa vào bảng record mà nó đã lưu về các gói tin, thay đổi địa chỉ IP đích thành địa chỉ của PC trong mạng và chuyển tiếp đi. Thông qua cơ chế đó quản trị mạng có khả năng lọc các gói tin gửi đến hay gửi từ một địa chỉ IP và cho phép hay cấm truy cập đến một port cụ thể.

❖ NAT làm việc như thế nào?

NAT sử dụng IP của chính nó làm IP công cộng cho mỗi máy con (client) với IP riêng. Khi một máy con thực hiện kết nối hoặc gửi dữ liệu tới một máy tính nào đó trên internet, dữ liệu sẽ được gửi tới NAT, sau đó NAT sẽ thay thế địa chỉ IP gốc của máy con đó rồi gửi gói dữ liệu đi với địa chỉ IP của NAT. Máy tính từ xa hoặc máy tính nào đó trên internet khi nhận được tín hiệu sẽ gửi gói tin trở về cho NAT computer bởi vì chúng nghĩ rằng NAT computer là máy đã gửi những gói dữ liệu đi. NAT ghi lại bảng thông tin của những máy tính đã gửi những gói tin đi ra ngoài trên mỗi cổng dịch vụ và gửi những gói tin nhận được về đúng máy tính đó (client). NAT xử lý một gói tin xuất phát từ bên trong đi ra bên ngoài một mạng theo cách thức sau:

- ✓ Khi NAT nhận một gói tin từ một cổng bên trong, gói tin này đáp ứng các tiêu chuẩn để NAT, router sẽ tìm kiếm trong bảng NAT địa chỉ bên ngoài (outside address) của gói tin. Nói cách khác, tiến trình NAT tìm kiếm một hàng ở trong bảng NAT trong đó địa chỉ outside local address bằng với địa chỉ đích của gói tin. Nếu không có phép so trùng nào tìm thấy, gói tin sẽ bị loại bỏ.
- ✓ Nếu có một hàng trong bảng NAT là tìm thấy (trong hàng này, địa chỉ đích của gói tin bằng với địa chỉ outside local), NAT sẽ thay thế địa chỉ đích trong gói tin bằng địa chỉ outside global theo thông tin trong bảng NAT.

- ✓ Tiến trình NAT tiếp tục tìm kiếm bảng NAT để xem có một địa chỉ inside local nào bằng với địa chỉ nguồn của gói tin hay không. Nếu có một hàng là tìm thấy, NAT tiếp tục thay thế địa chỉ nguồn của gói tin bằng địa chỉ inside global. Nếu không có một hàng nào được tìm thấy, NAT sẽ tạo ra một hàng mới trong bảng NAT và chèn địa chỉ mới vào trong gói tin.

NAT sẽ xử lý một gói tin xuất phát từ mạng bên ngoài đi vào mạng bên trong theo cách sau:

- ✓ Khi NAT nhận được một gói tin xuất phát từ một cổng bên ngoài, đáp ứng các tiêu chuẩn để NAT, tiến trình NAT sẽ tìm kiếm trong bảng NAT một hàng trong đó địa chỉ inside global là bằng với địa chỉ đích của gói tin.
- ✓ Nếu không có hàng nào trong bảng NAT được tìm thấy, gói tin bị loại bỏ. Nếu có một hàng tìm thấy trong bảng NAT, NAT sẽ thay thế địa chỉ đích bằng địa chỉ inside local từ bảng NAT.
- ✓ Router tìm kiếm bảng NAT để tìm ra địa chỉ outside global bằng với địa chỉ nguồn của gói tin. Nếu có một hàng là tìm thấy, NAT sẽ thay thế địa chỉ đích bằng địa chỉ outside local từ bảng NAT. Nếu NAT không tìm thấy một hàng nào, nó sẽ tạo ra một hàng mới trong bảng NAT và cũng thực hiện như ở bước 2.

❖ NAT giải quyết những vấn đề nào ?

- ✓ Ban đầu, NAT được đưa ra nhằm giải quyết vấn đề thiếu hụt địa chỉ của IPv4.
- ✓ NAT giúp chia sẻ kết nối Internet (hay 1 mạng khác) với nhiều máy trong LAN chỉ với 1 IP duy nhất.
- ✓ NAT che giấu IP bên trong LAN.
- ✓ NAT giúp quản trị mạng lọc các gói tin được gửi đến hay gửi từ một địa chỉ IP và cho phép hay cấm truy cập đến một port cụ thể.

3.5.2. Các khái niệm cơ bản:

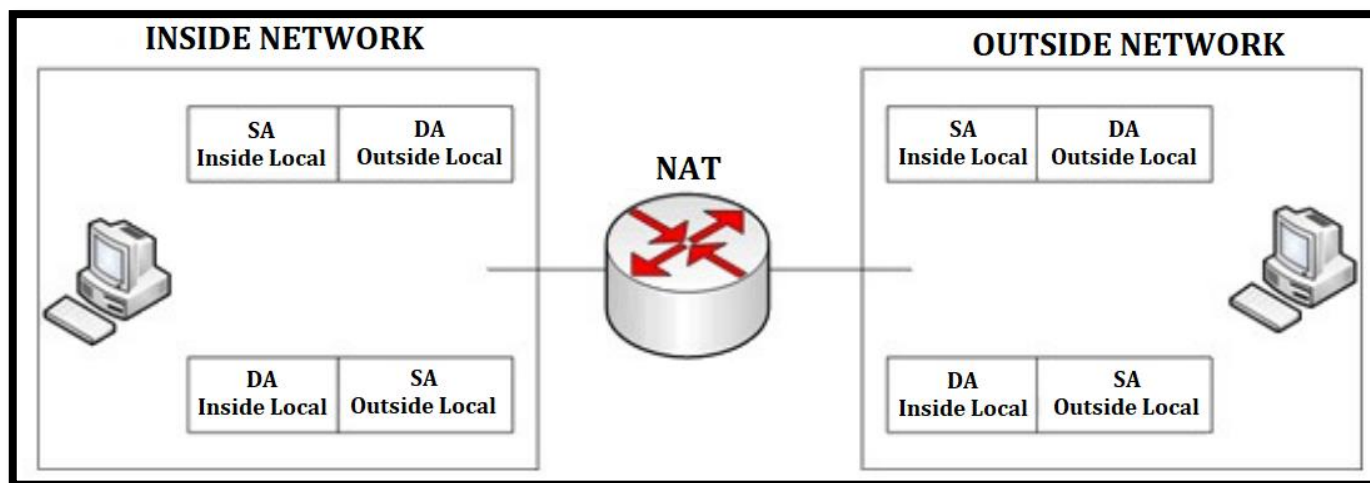
- ✚ **Inside local address** - Địa chỉ IP được gán cho một host của mạng trong. Đây là địa chỉ được cấu hình như là một tham số của hệ điều hành trong máy tính hoặc được gán một cách tự động thông qua các giao thức như DHCP. Địa chỉ này không phải là những địa chỉ IP hợp lệ được cấp bởi NIC (Network Information Center) hoặc nhà cung cấp dịch vụ Internet.
- ✚ **Inside global address** - Là một địa chỉ hợp lệ được cấp bởi NIC hoặc một nhà cung cấp dịch vụ trung gian. Địa chỉ này đại diện cho một hay nhiều địa chỉ IP inside local trong việc giao tiếp với mạng bên ngoài.

✚ **Outside local address** - Là địa chỉ IP của một host thuộc mạng bên ngoài, các host thuộc mạng bên trong sẽ nhìn host thuộc mạng bên ngoài thông qua địa chỉ này. Outside local không nhất thiết phải là một địa chỉ hợp lệ trên mạng IP (có thể là địa chỉ private).

✚ **Outside global address** - Là địa chỉ IP được gán cho một host thuộc mạng ngoài bởi người sở hữu host đó. Địa chỉ này được gán bằng một địa chỉ IP hợp lệ trên mạng Internet.

Chúng ta có thể hình dung để phân biệt 4 kiểu địa chỉ này như sau:

Các gói tin bắt nguồn từ bên trong mạng nội bộ (inside) sẽ có source IP là địa chỉ kiểu “inside local” và destination IP là “outside local” khi nó còn ở trong phần mạng nội bộ. Cũng gói tin đó, khi được chuyển ra ngoài mạng (qua NAT) source IP address sẽ được chuyển thành “inside global address” và địa destination IP của gói tin sẽ là “outside global address”. Hay ngược lại, khi một gói tin bắt nguồn từ một mạng bên ngoài, khi nó còn đang ở mạng bên ngoài đó, địa chỉ source IP của nó sẽ là “outside global address”, địa chỉ destination IP sẽ là “inside global address”. Cũng gói tin đó khi được chuyển vào mạng bên trong (qua NAT), địa chỉ source sẽ là “outside local address” và địa chỉ destination của gói tin sẽ là “inside local address”.



Hình 3.2. Các khái niệm về NAT

3.5.3. Các kỹ thuật NAT:

✚ **Kỹ thuật NAT tĩnh:**

Với NAT tĩnh, địa chỉ IP thường được ánh xạ tĩnh với nhau thông qua các lệnh cấu hình. Trong NAT tĩnh, một địa chỉ Inside Local luôn luôn được ánh xạ vào địa chỉ Inside Global. Nếu được sử dụng, mỗi địa chỉ Outside Local luôn luôn ánh xạ vào cùng địa chỉ Outside Global. NAT tĩnh không có tiết kiệm địa chỉ thực.

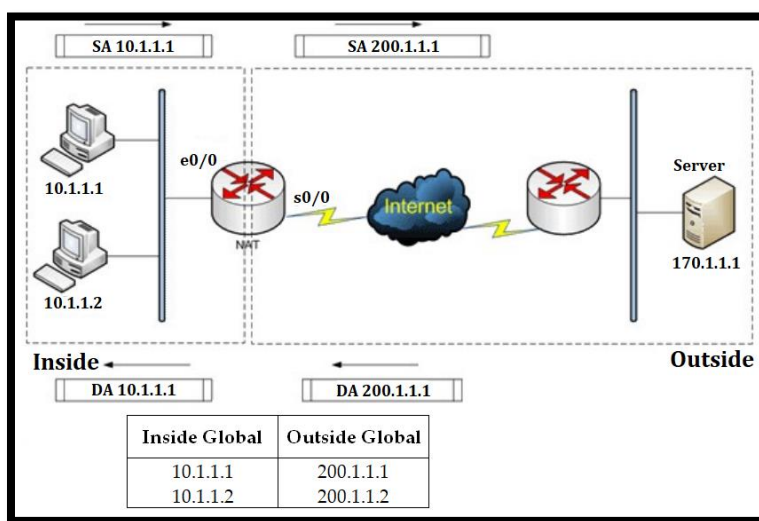
Mặc dù NAT tĩnh không giúp tiết kiệm địa chỉ IP, cơ chế NAT tĩnh cho phép một máy chủ bên trong hiện diện ra ngoài Internet, bởi vì máy chủ sẽ luôn dùng cùng một địa chỉ IP thực.

Cách thức thực hiện NAT tĩnh thì dễ dàng vì toàn bộ cơ chế dịch địa chỉ được thực hiện bởi một công thức đơn giản:

Địa chỉ đích = Địa chỉ mạng mới OR (địa chỉ nguồn AND (NOT netmask))

VD: Một địa chỉ private được map với một địa chỉ public. Ví dụ 1 máy trong mạng LAN có địa chỉ 10. 1. 1. 1 được “phiên dịch” thành 1 địa chỉ public 20. 1. 1. 1 khi gửi tin ra ngoài Internet.

Bắt đầu bằng một gói tin được gửi từ một PC bên trái của hình đến một máy chủ bên phải ở địa chỉ 170. 1. 1. 1. Địa chỉ nguồn private 10. 1. 1. 1 được dịch thành một địa chỉ thực 200. 1. 1. 1. Máy client gửi ra một gói tin với địa chỉ nguồn 10. 1. 1. 1 nhưng router NAT thay đổi địa chỉ nguồn thành 200. 1. 1. 1. Khi server nhận được một gói tin với địa chỉ nguồn 200. 1. 1. 1, máy chủ nghĩ rằng nó đang nói chuyện với máy 200. 1. 1. 1, vì vậy máy chủ trả lời lại bằng một gói tin gửi về địa chỉ đích 200. 1. 1. 1. Router sau đó sẽ dịch địa chỉ đích 200. 1. 1. 1 ngược lại thành 10. 1. 1. 1.



Hình 3.3. Kỹ thuật NAT tĩnh

Kỹ thuật NAT động (Dynamic NAT):

Với NAT, khi số IP nguồn không bằng số IP đích. Số host chia sẻ nói chung bị giới hạn bởi số IP đích có sẵn. NAT động phức tạp hơn NAT tĩnh, vì thế chúng phải lưu giữ lại thông tin kết nối và thậm chí tìm thông tin của TCP trong packet. Một số người dùng nó thay cho NAT tĩnh vì mục đích bảo mật. Những người từ bên ngoài không thể tìm được IP nào kết nối với host chỉ định vì tại thời điểm tiếp theo host này có thể nhận một IP hoàn toàn khác.

Những kết nối từ bên ngoài thì chỉ có thể khi những host này vẫn còn nắm giữ một IP trong bảng NAT động. Nơi mà NAT router lưu giữ những thông tin về IP bên trong (IP nguồn) được liên kết với NAT-IP(IP đích). Cho một ví dụ trong một session của FTP non-passive. Nơi mà server cố gắng thiết lập một kênh truyền dữ liệu vì thế khi server cố gắng gửi một IP packet đến FTP client thì phải có một entry cho client trong bảng NAT. Nó vẫn phải còn liên kết một IPclient với cùng một NAT-IPs khi client bắt đầu một kênh truyền control trừ khi FTP session rồi sau một thời gian timeout. Xin nói thêm giao thức FTP có 2 cơ chế là passive và non-passive . Giao thức FTP luôn dùng 2 port (control và data) . Với cơ chế passive (thụ động) host kết nối sẽ nhận thông tin về data port từ server và ngược lại non-passive thì host kết nối sẽ chỉ định dataport yêu cầu server lắng nghe kết nối tới.

Bất cứ khi nào nếu một người từ bên ngoài muốn kết nối vào một host chỉ định ở bên trong mạng tại một thời điểm tùy ý chỉ có 2 trường hợp:

- ✓ Host bên trong không có một entry trong bảng NAT khi đó sẽ nhận được thông tin “host unreachable” hoặc có một entry nhưng NAT-IPs là không biết.
- ✓ Biết được IP của một kết nối bởi vì có một kết nối từ host bên trong ra ngoài mạng. Tuy nhiên đó chỉ là NAT-IPs và không phải là IP thật của host. Và thông tin này sẽ bị mất sau một thời gian timeout của entry này trong bảng NAT router.
- ✓ VD: Một địa chỉ private được map với một địa chỉ public từ một nhóm các địa chỉ public. Ví dụ một mạng LAN có địa chỉ 10. 1. 1. 1/8 được “phiên dịch” thành 1 địa chỉ public trong dải 200. 1. 1. 1 đến 200. 1. 1. 100 khi gửi tin ra ngoài Internet.

Kỹ thuật NAT overloading (PAT):

Dùng để ánh xạ nhiều địa chỉ IP riêng sang một địa chỉ công cộng vì mỗi địa chỉ riêng được phân biệt bằng số port. Có tới 65. 356 địa chỉ nội bộ có thể chuyển đổi sang 1 địa chỉ công cộng. Nhưng thực tế thì khoảng 4000 port.

PAT hoạt động bằng cách đánh dấu một số dòng lưu lượng TCP hoặc UDP từ nhiều máy cục bộ bên trong xuất hiện như cùng từ một hoặc một vài địa chỉ Inside Global. Với PAT, thay vì chỉ dịch địa chỉ IP, NAT cũng dịch các cổng khi cần thiết.

Và bởi vì các trường của cổng có chiều dài 16 bit, mỗi địa chỉ Inside Global có thể hỗ trợ lên đến 65000 kết nối TCP và UDP đồng thời. Ví dụ, trong một hệ thống mạng có 1000 máy, một địa chỉ IP thực được dùng như là địa chỉ Inside Global duy nhất có thể quản lý trung bình sáu dòng dữ liệu đến và đi từ các máy trên Internet.

VD: PAT map nhiều địa chỉ Private đến một địa chỉ Public, việc phân biệt các địa chỉ Private này được dựa theo port, ví dụ IP address 10. 1. 1. 1 sẽ được map đến ip address 200. 1. 1. 6:port_number.

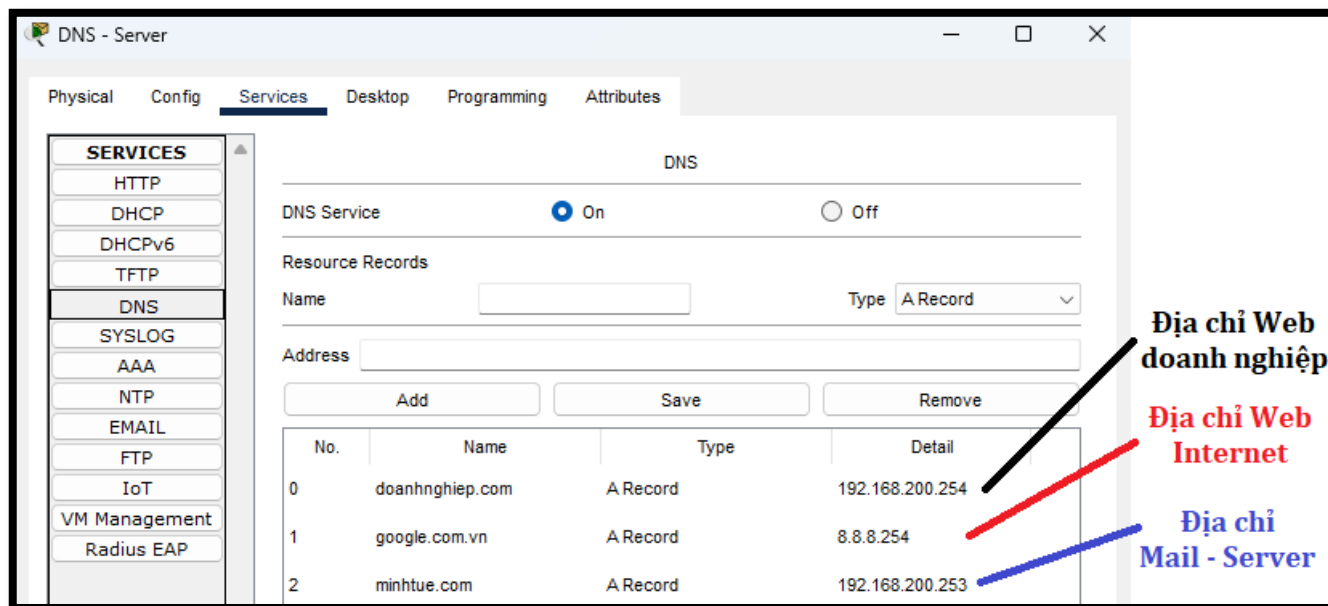
Mối quan hệ giữa NAT và PAT:

- PAT có mối quan hệ gần gũi với NAT nên vẫn thường được gọi là NAT.
- Trong NAT, nhìn chung chỉ địa chỉ ip được đổi. Có sự tương ứng 1:1 giữa địa chỉ riêng và địa chỉ công cộng.
- Trong PAT, cả địa chỉ riêng của người gửi và cổng đều được thay đổi. Thiết bị PAT sẽ chọn số cổng mà các hosts trên mạng công cộng sẽ nhìn thấy.
- Trong NAT, những gói tin từ ngoài mạng vào được định tuyến tới địa chỉ IP đích của nó trên mạng riêng bằng cách tham chiếu địa chỉ nguồn đi vào.
- Trong PAT, Chỉ có một địa chỉ IP công cộng được nhìn thấy từ bên ngoài và gói tin đi vào từ mạng công cộng được định tuyến tới đích của chúng trên mạng riêng bằng cách tham chiếu tới bảng quản lý từng cặp cổng private và public lưu trong thiết bị PAT. Cái này thường được gọi là connection tracking.
- Một số thiết bị cung cấp NAT, như broadband routers, thực tế cung cấp PAT. vì lý do này, có sự nhầm lẫn đáng kể giữa các thuật ngữ. Nhìn chung người ta sử dụng NAT để bao gồm những thiết bị PAT.

3.5.4. Cấu hình Access – list và NAT overloading (PAT) trên Router DOANH NGHIỆP:

```
DOANH-NGHIEP(config)#ip access-list standard local
DOANH-NGHIEP(config-std-nacl)#permit 192.168.10.0 0.0.0.255
DOANH-NGHIEP(config-std-nacl)#permit 192.168.20.0 0.0.0.255
DOANH-NGHIEP(config-std-nacl)#permit 192.168.30.0 0.0.0.255
DOANH-NGHIEP(config-std-nacl)#permit 192.168.40.0 0.0.0.255
DOANH-NGHIEP(config-std-nacl)#permit 192.168.50.0 0.0.0.255
DOANH-NGHIEP(config-std-nacl)#exit
DOANH-NGHIEP(config)#ip nat inside source list local interface g0/0 overload
DOANH-NGHIEP(config)#interface gigabitEthernet 0/0
DOANH-NGHIEP(config-if)#ip nat outside
DOANH-NGHIEP(config-if)#exit
DOANH-NGHIEP(config)#interface gigabitEthernet 0/1.10
DOANH-NGHIEP(config-if)#ip nat inside
DOANH-NGHIEP(config-if)#interface gigabitEthernet 0/1.20
DOANH-NGHIEP(config-if)#ip nat inside
DOANH-NGHIEP(config-if)#interface gigabitEthernet 0/1.30
DOANH-NGHIEP(config-if)#ip nat inside
DOANH-NGHIEP(config-if)#interface gigabitEthernet 0/1.40
DOANH-NGHIEP(config-if)#ip nat inside
DOANH-NGHIEP(config-if)#interface gigabitEthernet 0/1.50
DOANH-NGHIEP(config-if)#ip nat inside
```

3.6. CẤU HÌNH DNS – SERVER CHO WEB – SERVER VÀ MAIL – SERVER



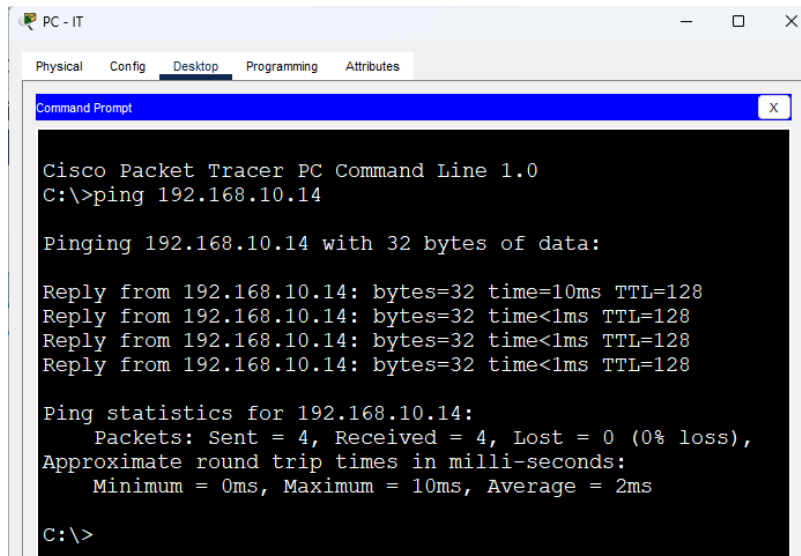
Hình 3.4. Cấu hình DNS – Server

CHƯƠNG IV.

KẾT QUẢ MÔ PHỎNG

4.1. KIỂM TRA KẾT NỐI CÁC PC TRONG CÙNG 1 PHÒNG BAN

- Từ PC – IT đến Laptop – IT:



```
PC - IT
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

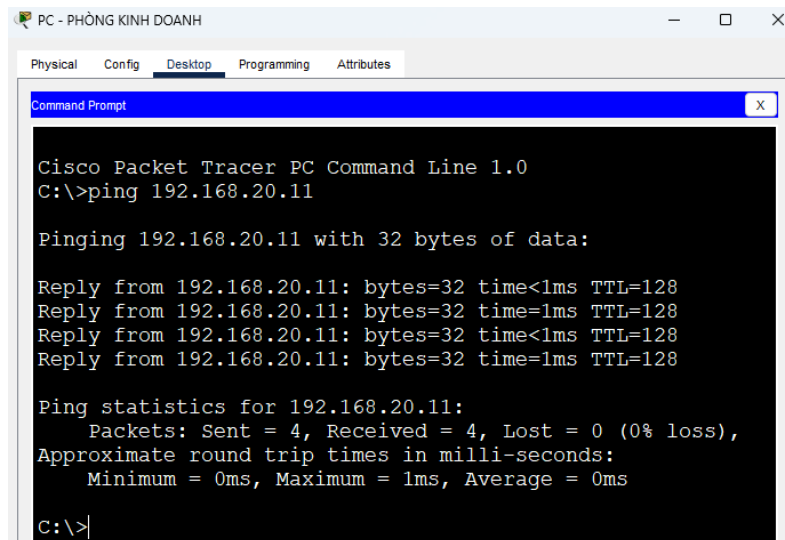
Reply from 192.168.10.14: bytes=32 time=10ms TTL=128
Reply from 192.168.10.14: bytes=32 time<1ms TTL=128
Reply from 192.168.10.14: bytes=32 time<1ms TTL=128
Reply from 192.168.10.14: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>
```

Hình 4.1. Kiểm tra kết nối từ PC – IT đến Laptop – IT

- Từ PC – PHÒNG KINH DOANH ping đến Laptop – PHÒNG KINH DOANH:



```
PC - PHÒNG KINH DOANH
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.11

Pinging 192.168.20.11 with 32 bytes of data:

Reply from 192.168.20.11: bytes=32 time<1ms TTL=128
Reply from 192.168.20.11: bytes=32 time=1ms TTL=128
Reply from 192.168.20.11: bytes=32 time<1ms TTL=128
Reply from 192.168.20.11: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.20.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Hình 4.2. Ping từ PC – phòng kinh doanh đến Laptop – phòng kinh doanh

- Từ PC – PHÒNG KẾ TOÁN ping đến Laptop – KẾ TOÁN:

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.14

Pinging 192.168.30.14 with 32 bytes of data:

Reply from 192.168.30.14: bytes=32 time<1ms TTL=128
Reply from 192.168.30.14: bytes=32 time<1ms TTL=128
Reply from 192.168.30.14: bytes=32 time<1ms TTL=128
Reply from 192.168.30.14: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.30.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>

```

Hình 4.3. Ping từ PC – phòng kế toán đến Laptop – phòng kế toán

4.2. KIỂM TRA KẾT NỐI CÁC PC TRONG GIỮA CÁC PHÒNG BAN KHÁC NHAU

- Từ PC – IT đến PC – PHÒNG KINH DOANH:

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.13

Pinging 192.168.20.13 with 32 bytes of data:

Reply from 192.168.20.13: bytes=32 time<1ms TTL=127
Reply from 192.168.20.13: bytes=32 time=2ms TTL=127
Reply from 192.168.20.13: bytes=32 time=10ms TTL=127
Reply from 192.168.20.13: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.20.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>

```

Hình 4.4. Ping từ PC – IT đến PC – PHÒNG KINH DOANH

- Từ PC – PHÒNG KINH DOANH đến Laptop – PHÒNG KẾ TOÁN:

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.14

Pinging 192.168.30.14 with 32 bytes of data:

Reply from 192.168.30.14: bytes=32 time<1ms TTL=127
Reply from 192.168.30.14: bytes=32 time=10ms TTL=127
Reply from 192.168.30.14: bytes=32 time<1ms TTL=127
Reply from 192.168.30.14: bytes=32 time=11ms TTL=127

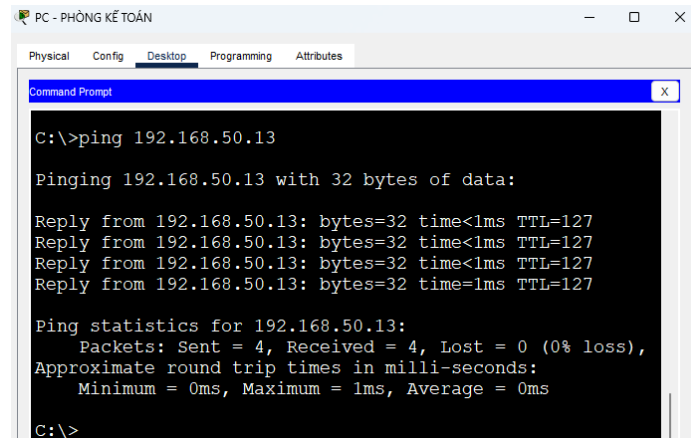
Ping statistics for 192.168.30.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 5ms

C:\>

```

Hình 4.5. Ping PC – PHÒNG KINH DOANH đến Laptop – PHÒNG KẾ TOÁN

- Từ PC – PHÒNG KẾ TOÁN đến GIÁM ĐỐC:



Hình 4.6. Ping PC – PHÒNG KẾ TOÁN đến GIÁM ĐỐC

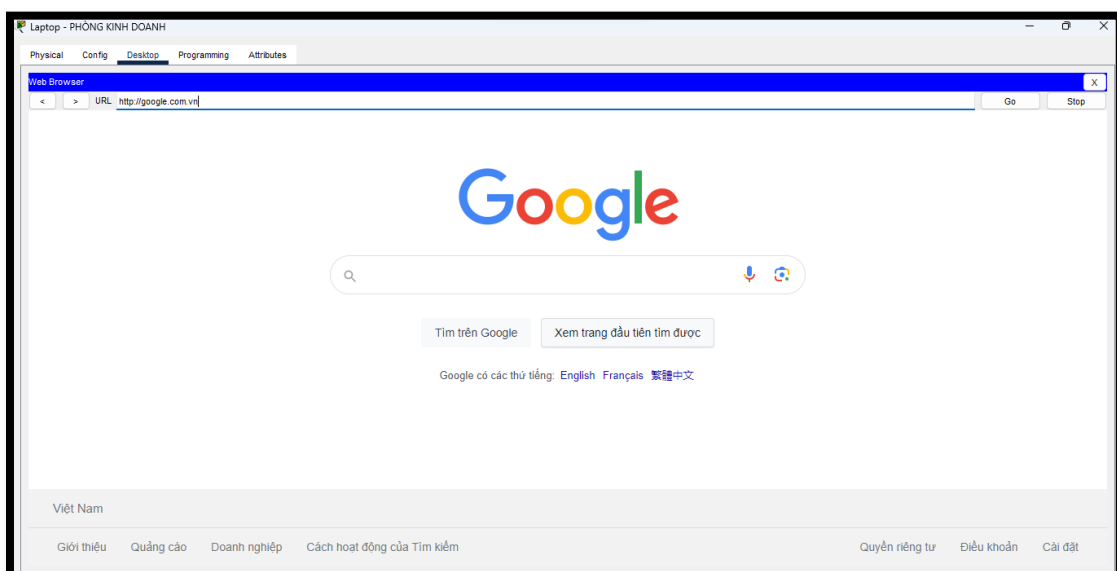
4.3. KIỂM TRA TRUY CẬP WEB

- Từ PC phòng IT truy cập Web với tên miền doanhnghiep.com:



Hình 4.7. Truy cập Web với tên miền doanhnghiep.com

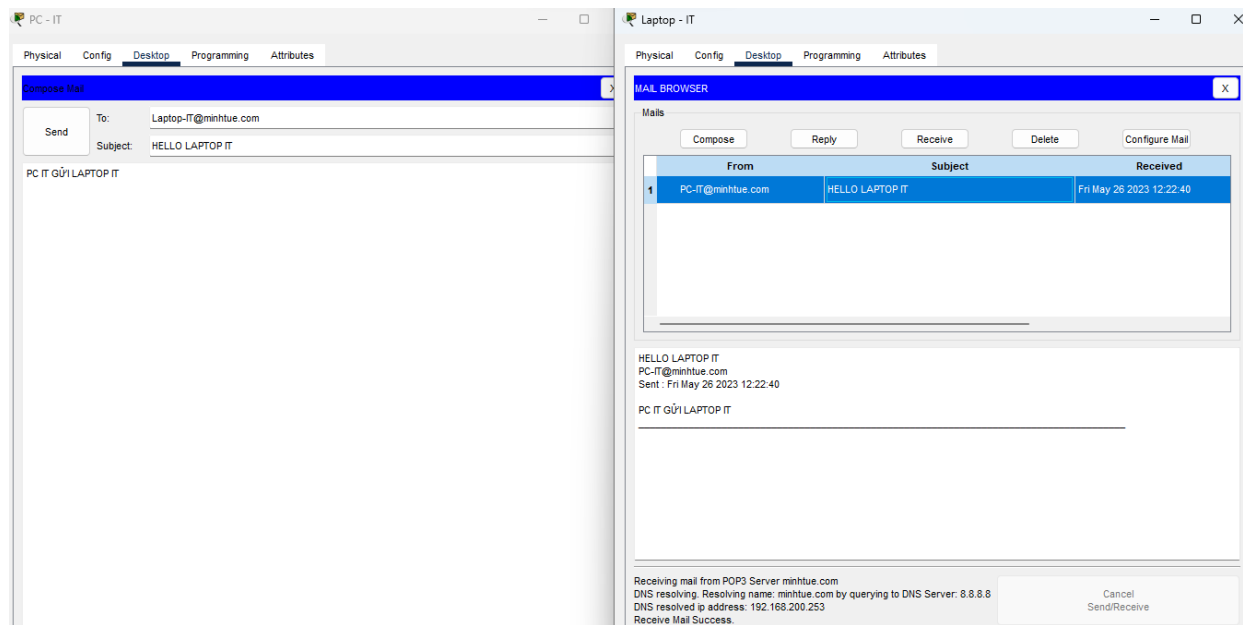
- Từ Laptop phòng Kinh doanh truy cập Internet với tên miền google.com.vn:



Hình 4.8. Truy cập Web google.com.vn

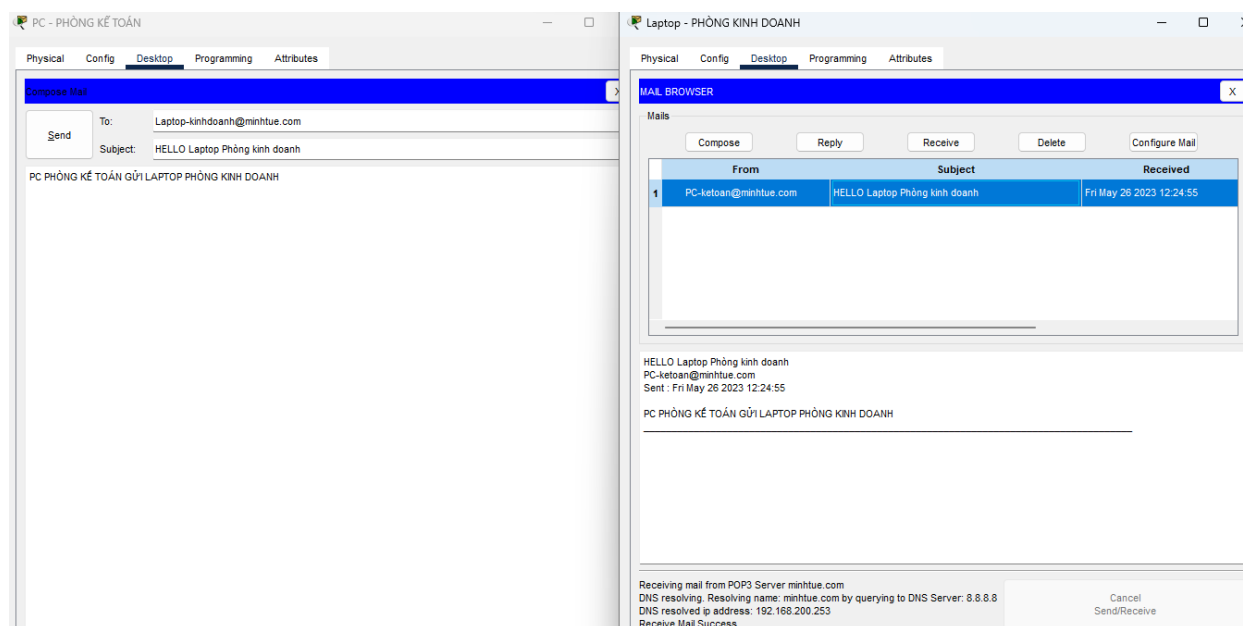
4.4. KIỂM TRA MAIL – SERVER:

- Trong cùng phòng ban:



Hình 4.9. Gửi Email trong phòng IT

- Khác phòng ban:



Hình 4.10. Gửi Email từ Phòng kế toán đến Phòng kinh doanh

CHƯƠNG V.

KẾT LUẬN

Việc thiết kế, xây dựng hệ thống mạng máy tính là một công đoạn hết sức khó khăn, để có thể thiết kế nên một hệ thống mạng hoàn chỉnh đồng thời có khoa học, đòi hỏi người thiết kế phải có tư duy cũng như kiến thức về nó. Hệ thống mạng chạy tốt hay không, duy trì được lâu hay không, thường xuyên gặp trục trặc hay là ít, điều đó phần lớn đều bắt nguồn từ việc thiết kế hệ thống mạng có khoa học hay là không. Lắp đặt hệ thống mạng làm sao để cho dễ quản lý, dễ nâng cấp và hạn chế sự cố tới mức thấp nhất, đồng thời đảm bảo tính bảo mật cao, đó là cả một vấn đề đòi hỏi người thiết kế phải hết sức chú ý.

Qua một thời gian tìm hiểu, cộng với kiến thức học được và được sự hướng dẫn của thầy **Hồ Đức Tâm Linh**, em đã hoàn thành bài đồ án của mình, đồng thời cũng mở mang thêm kiến thức về môn học **Đồ án chuyên ngành kỹ thuật viễn thông 2**, giúp ích cho bản thân sau này. Tuy nhiên, trong quá trình thực hiện bài đồ án này sẽ không tránh khỏi những sai lầm nhất định, cũng như những thiếu sót trong quá trình thực hiện dự án của mình, rất mong được sự góp ý của thầy và các bạn !

Em xin chân thành cảm ơn !