**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

─────── \* ───────



**BÁO CÁO**

Thiết kế mạng Intranet

**Đề tài: Xây dựng hệ thống mạng cơ bản**

*Sinh Viên thực hiện:*

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và Tên** | **MSSV** | **Lớp** |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |

*Giáo Viên hướng dẫn:TS Phạm Huy Hoàng*

**HÀ NỘI-12/2016**

**Mục Lục**

[Lời Nói Đầu 3](#_Toc469642428)

[1.Mô hình xây dựng hệ thống mạng 4](#_Toc469642429)

[1.1. Phân tích mô hình 4](#_Toc469642430)

[1.2. Yêu cầu thiết bị triển khai cho hệ thống 5](#_Toc469642431)

[1.2.1 Phần mềm cần sử dụng 5](#_Toc469642432)

[1.2.2.Cài đặt cơ bản ban đầu. 5](#_Toc469642433)

[2. Triển khai hệ thống mạng 6](#_Toc469642434)

[2.1. Triển khai hệ thống Core của mạng 6](#_Toc469642435)

[2.1.1 Trên R1 6](#_Toc469642436)

[2.1.2.Trên R2 9](#_Toc469642437)

[2.1.3.Trên R3 11](#_Toc469642438)

[2.1.4.Trên R4 13](#_Toc469642439)

[2.1.5 Bảng định tuyến của các thiết bị sau khi chạy OSPF và định tuyến tĩnh 14](#_Toc469642440)

[2.2. Triển khai hệ thống dịch vụ 15](#_Toc469642441)

[2.2.1 Hệ thống DNS private và DNS\_internet 15](#_Toc469642442)

[2.2.2Hệ thống Web với SSL 20](#_Toc469642443)

[2.2.3 Hệ thống mail 22](#_Toc469642444)

# Lời Nói Đầu

Trong thế giới hiện đại ngày này, Internet đã là một phần không thể thiếu. Song hành với quá trình đó là sự phát triển không ngừng của hệ thống Internet trên toàn thế giới. Ngày nay, khi mạng toàn cầu đang phát triển với một tốc độ nhanh chóng, với một phạm vi rộng lớn và lượng thông tin được chia sẻ trên mạng tăng lên với tốc độ chóng mặt không ngừng, vì vậy vấn đề thiết kế hệ thống mạng là vô cùng quan trọng.

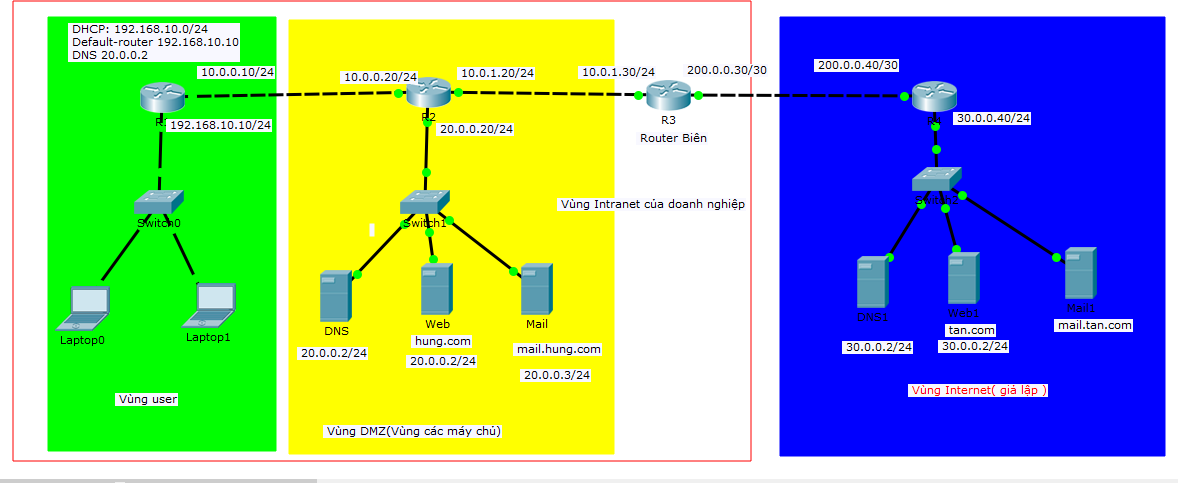
Các thiết bị và ứng dụng cũng như dịch vụ có sử dụng kết nối Internet càng ngày càng phát triển không ngừng. Không đứng ngoài xu thế Internet toàn cầu đó ,các doanh nghiệp lớn đều xây dựng cho mình một hệ thống mạng doanh nghiệp riêng cho mình nhằm đảm bảo các dịch vụ của doanh nghiệp như MARKETING, PR.. hay các dịch vụ khác có sử dụng hệ thống mạng như Ngân Hàng.. thì hệt hống mạng doanh nghiệp càng quan trong hơn mức nào hết.Vì vậy môn học “Thiết kế mạng Intranet “ được ra đời nhằm giúp cho sinh viên có sự hiểu biết cơ bản về hệ thống mạng doanh nghiệp.

Để phục vụ cho việc học tập và nghiên cứu môn học “Thiết kế mạng Intranet” nhóm chúng em xin thực hiện đề tài “**Xây dựng một hệ thống mạng cơ bản**”

Trong suốt quá trình thực hiện bài tiểu luận này, nhóm đã rất nỗ lực tìm hiểu kiến thức, tra cứu thông tin nhưng chắc chắn vẫn còn nhiều điểm thiếu sót cần bổ sung, cải thiện trong tương lai. Nhóm xin chân thành cảm ơn *TS. Phạm Huy Hoàng* đã tận tình hướng dẫn, giúp đỡ thực hiện tốt bài tiểu luận này.

***Nhóm Sinh Viên****.*

# 1.Mô hình xây dựng hệ thống mạng



## Phân tích mô hình

Hệ thống chúng em xây dựng là một hệ thống mạng cơ bản gồm 2 thành phần chính:

* Hệ thống mạng Intranet của doanh nghiệp (Phần được giới hạn bởi viền màu đỏ).
* Hệ thống Internet bên ngoài (phần màu xanh dương trên hình).

Trong phần hệ thống mạng Intranet của doanh nghiệp lại được chia làm 2 vùng là:

* Vùng máy tính dành cho người dung (vùng màu xanh lá trên hình)
* Vùng hệ thống các dịch vụ của doanh nghiệp, nơi các quản trị viên cài đặt cấu hình dịch vụ của hệ thống mạng doanh nghiệp – vùng DMZ (vùng màu vàng trên hình)

## Yêu cầu thiết bị triển khai cho hệ thống

### 1.2.1 Phần mềm cần sử dụng

Để xây dựng hệ thống mạng mô phỏng như trên chúng em sử dụng các phần mềm cũng như cài đặt như sau:

-Phần mềm VMware Workstation Pro 12 hỗ trợ cho việc cài đặt máy ảo

-File image Centos 6.6 giúp cho việc triển khai cài đặt biến centos thành 4 con router trên hình vẽ .

File iso Centos 6.8 GROME giúp cho việc triển khai các dịch vụ mail ,web .dns cho vùng DMZ cũng như phía ngoài Internet.

### 1.2.2.Cài đặt cơ bản ban đầu.

Để bắt đầu vào việc mô phỏng hệ thống mạng như trên trước hết trên máy tính cần cài VMware Workstation Pro 12.

Sau khi đã có nó chúng ta sẽ import file image Centos 6.6 vào thành 4 hệ điều hành ảo R1, R2, R3 ,R4.

Tiếp đó cài đặt file iso Centos 6.8 GROME, ta cài 1 lần rồi clone hệ điều hành đó ra 4 bản nữa giúp tao ra 1 máy tính phần user, 1 máy tính sẽ triể khai dns và web server cho doanh nghiệp và 1 máy cho dịch vụ mail của doanh ngiệp. Và 2 hệ điều hành tiếp theo cho hệ thống Internet bên ngoài có các dịch vụ là DNS , WEB và MAIL .

# Triển khai hệ thống mạng

## Triển khai hệ thống Core của mạng

Hệ thống core của hệ thống mạng này là 4 con router được tạo ra bằng việc biến từ 4 con centos

Để cho hệ thống 4 con core R1,R4 chạy được thì trên các con R1, R2 ,R3 cần định tuyến OSPF và trên con R3 (Router biên của hệ thống mạng doanh nghiệp ) cần định tuyến tĩnh để ra con R4, tất cả các mạng R3 không biết nó sẽ đẩy ra cổng Interface của R4. Và trên R4 định tuyến tĩnh tất cả các mạng ko biết nó sẽ đẩy ra interface kết nối vào mạng Intranet kết nối với R3.

### 2.1.1 Trên R1

#### a.Yêu cầu cài đặt

Với yêu cầu đặt ra trên R1 cần có 2 interface mạng giúp cho việc chuyển tiếp mạng giữa vùng user và vùng DMZ.

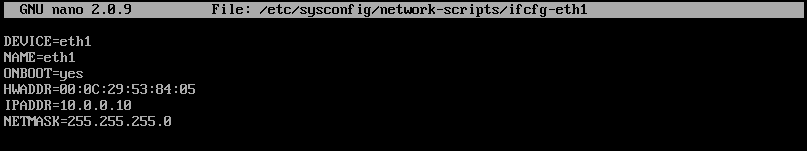
Trên R1 cần có cấu hình dhcp, định tuyến OSPF và định tuyến tĩnh

#### b.Cấu hình

* **Cấu hình các địa chỉ mạng cho 2 interface**

Sau khi đã cấu hình 2 card mạng cho R1 ta cần cấu hình địa chỉ IP cho 2 interface eth1 và eth2

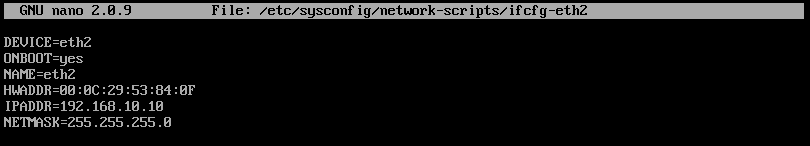
-Đặt ip cho eth1:

Dùng lệnh : “*nano /etc/sysconfig/network-scripts/ifcfg-eth1*” Sau đó cấu hình như sau :  


Sau đó lưu cấu hình

Đặt ip cho eth2:

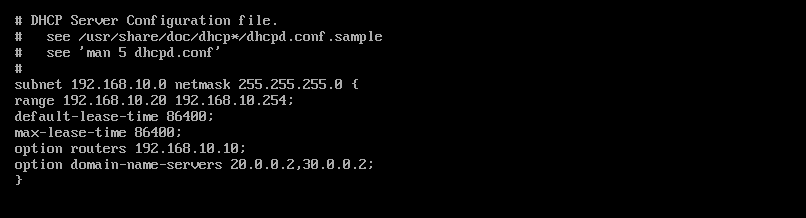
Dùng lệnh : “*nano /etc/sysconfig/network-scripts/ifcfg-eth2*” Sau đó cấu hình như sau :

  
Sau đó lưu cấu hình.

* **Cấu hình dhcp cho các máy tính User**

Trên R1 cần có cấu hình dhcp do đó trước khi cài đặt dhcp cần cài đặt chương trình dhcp bằng lệnh : “yum install dhcp”

Sau khi đã có chương trình chúng ta dùng lệnh sau “*nano /etc/dhcp/dhcpd.conf* “ sau đó chỉnh sửa file như sau :



Sau khi chỉnh sửa xong, lưu cấu hình rồi sử dụng lệnh sau để restart và tự động cho phép dhcpd trên R1 sau khi khởi động lại:

*service dhcpd restart*

*chkconfig dhcpd on*

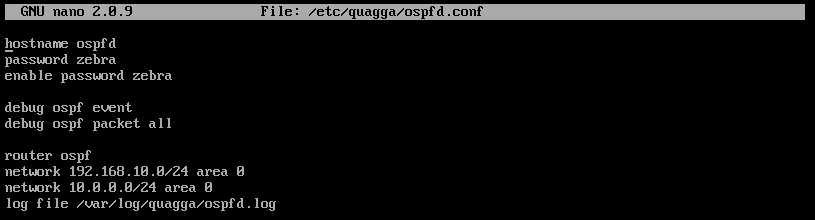
* **Cấu hình định tuyến động OSPF**

Trên R1 muốn cài định tuyến động OSPF cần cài gói quagga bằng lệnh :” *yum install quagga*”

Khi đã có quagga ta dùng lệnh “*nano /etc/quagga/zebra.conf “* để cấu hình như sau :



Sau đó dùng lệnh “*nano /etc/quagga/ospfd.conf”* và cấu hình như sau :



Sau khi cấu hình xong lưu cấu hình và dùng các lênh sau để cho phép thực hiện ospf :

*service iptables stop*

*service zebra restart*

*service ospfd restart*

*shkconfig iptables off*

*shkconfig zebra on*

*shkconfig ospfd on*

* **Cấu hình định tuyến tĩnh**

Tuy là sau khi cấu hình đủ định tuyến động ospf trên R1, R2, R3 thì trên R1 sẽ biết đc đường đến các mạng kết nối với OSPF còn nó ko biết các mạng ở ngoài Internet. Trong thí dụ này là mạng phía bên ngoài của R4 , do đó cần định tuyến tính trên R1. Lệnh : *route add –net default gw 10.0.0.20*

### 2.1.2.Trên R2

#### a.Yêu cầu cài đặt

Với yêu cầu đặt ra trên R2 cần 3 interface mạng cho vùng các máy chủ và 2 interface để chuyển tiếp sang R1 và R3.

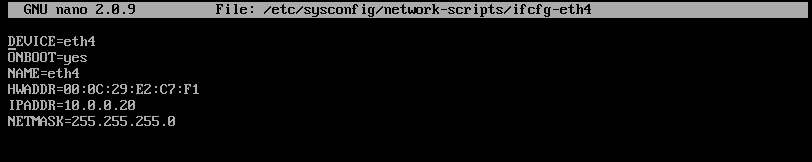
R2 có cài đặt OSPF và định tuyến tĩnh

#### b.Cài đặt

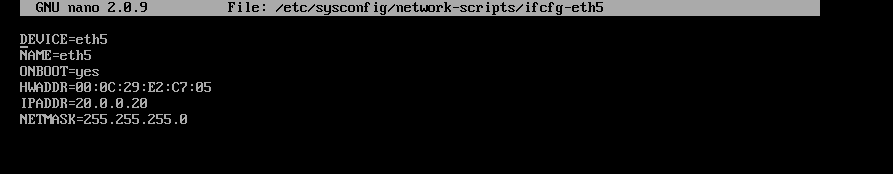
* **Cấu hình các địa chỉ mạng cho các interface**

-Đặt ip cho eth4:

Dùng lệnh : “*nano /etc/sysconfig/network-scripts/ifcfg-eth4*” Sau đó cấu hình như sau :

  
 -Đặt ip cho eth5

Dùng lệnh : “*nano /etc/sysconfig/network-scripts/ifcfg-eth5*” Sau đó cấu hình như sau :



-Đặt ip cho eth6

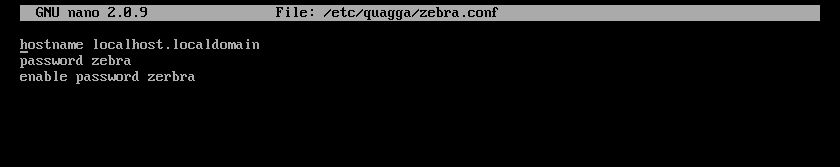
Dùng lệnh : “*nano /etc/sysconfig/network-scripts/ifcfg-eth6*” Sau đó cấu hình như sau :



* **Cấu hình định tuyến động OSPF**

Trên R2 muốn cài định tuyến động OSPF cần cài gói quagga bằng lệnh :” *yum install quagga*”

Khi đã có quagga ta dùng lệnh “*nano /etc/quagga/zebra.conf “* để cấu hình như sau :



Sau đó dùng lệnh “*nano /etc/quagga/ospfd.conf”* và cấu hình như sau :



Sau khi cấu hình xong lưu cấu hình và dùng các lênh sau để cho phép thực hiện ospf :

*service iptables stop*

*service zebra restart*

*service ospfd restart*

*shkconfig iptables off*

*shkconfig zebra on*

*shkconfig ospfd on*

* **Cấu hình định tuyến tĩnh**

Tuy là sau khi cấu hình đủ định tuyến động ospf trên R1, R2, R3 thì trên R2 sẽ biết đc đường đến các mạng kết nối với OSPF còn nó ko biết các mạng ở ngoài Internet. Trong thí dụ này là mạng phía bên ngoài của R4 , do đó cần định tuyến tính trên R1. Lệnh : *route add –net default gw 10.0.1.30*

### 2.1.3.Trên R3

#### a.Yêu cầu cài đặt

Với yêu cầu đặt ra trên R3 cần 2 interface mạng cho vùng mạng Intranet và Internet.

R3 có cài đặt OSPF và định tuyến tĩnh.

#### b.Cài đặt

* **Cấu hình các địa chỉ mạng cho các interface**

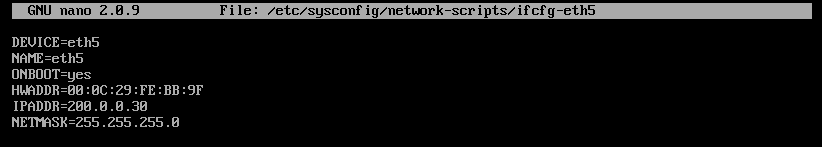
-Đặt ip cho eth4:

Dùng lệnh : “*nano /etc/sysconfig/network-scripts/ifcfg-eth4*” Sau đó cấu hình như sau :



-Đặt ip cho eth5

Dùng lệnh : “*nano /etc/sysconfig/network-scripts/ifcfg-eth5*” Sau đó cấu hình như sau :



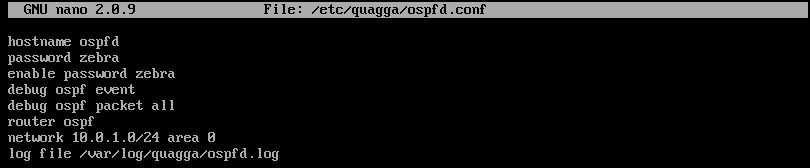
* **Cấu hình định tuyến động OSPF**

Trên R1 muốn cài định tuyến động OSPF cần cài gói quagga bằng lệnh :” *yum install quagga*”

Khi đã có quagga ta dùng lệnh “*nano /etc/quagga/zebra.conf “* để cấu hình như sau :



Sau đó dùng lệnh “*nano /etc/quagga/ospfd.conf”* và cấu hình như sau :



Sau khi cấu hình xong lưu cấu hình và dùng các lênh sau để cho phép thực hiện ospf :

*service iptables stop*

*service zebra restart*

*service ospfd restart*

*shkconfig iptables off*

*shkconfig zebra on*

*shkconfig ospfd on*

* **Cấu hình định tuyến tĩnh**

Tuy là sau khi cấu hình đủ định tuyến động ospf trên R1, R2, R3 thì trên R3 sẽ biết đc đường đến các mạng kết nối với OSPF còn nó ko biết các mạng ở ngoài Internet. Trong thí dụ này là mạng phía bên ngoài của R4 , do đó cần định tuyến tính trên R1. Lệnh : *route add –net default gw 200.0.0.40*

### 2.1.4.Trên R4

#### a.Yêu cầu cài đặt

Với yêu cầu đặt ra trên R4 cần 2 interface mạng cho vùng mạng Intranet và Internet.

R4 có cài đặt định tuyến tĩnh.

#### b.Cài đặt

* **Cấu hình các địa chỉ mạng cho các interface**

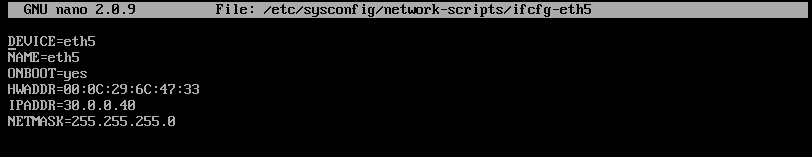
-Đặt ip cho eth4:

Dùng lệnh : “*nano /etc/sysconfig/network-scripts/ifcfg-eth4*” Sau đó cấu hình như sau :



-Đặt ip cho eth5

Dùng lệnh : “*nano /etc/sysconfig/network-scripts/ifcfg-eth5*” Sau đó cấu hình như sau :

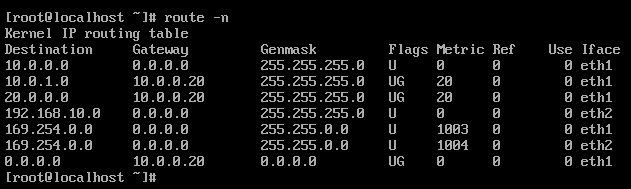


* **Cấu hình định tuyến tĩnh**

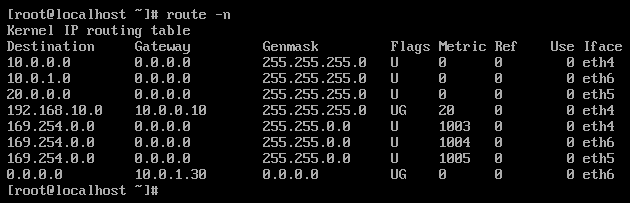
R4 là thiết bị bên ngoài Internet nên muốn biết các mạng của phía trong thì tao dùng định tuyến tĩnh .Lệnh : *route add –net default gw 200.0.0.30*

### 2.1.5 Bảng định tuyến của các thiết bị sau khi chạy OSPF và định tuyến tĩnh

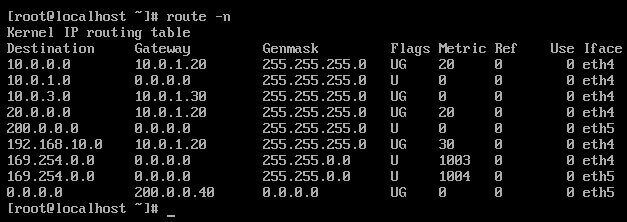
* R1 :



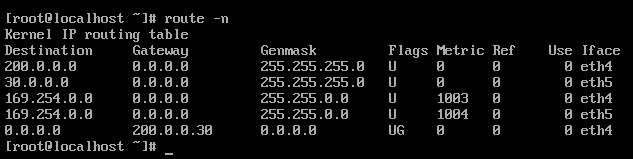
* R2



* R3



* R4



## Triển khai hệ thống dịch vụ

### 2.2.1 Hệ thống DNS private và DNS\_internet

#### a.DNS private

Đây là hệ thống DNS của doanh nghiệp ở trong vùng DMZ

\*Yêu cầu

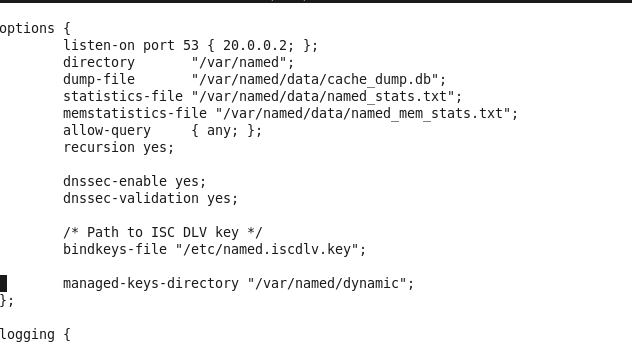
Để cài đặt được hệ thống DNS của doanh nghiệp cần cài bind : “yum install install bind”

Địa chỉ IP của DNS : 20.0.0.2/24 defaul router :20.0.0.20

Phân giải địa chỉ tan.com -> 30.0.0.2; hung.com ->20.0.0.2; mail.tan.com -> 30.0.0.3 ;mail.hung.com ->20.0.0.3.

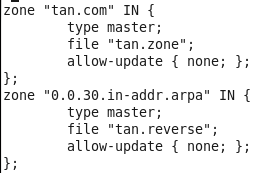
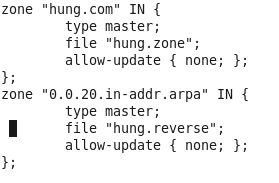
\*Cài đặt

* Cấu hình file named.conf :”*nano /etc/named.conf”*



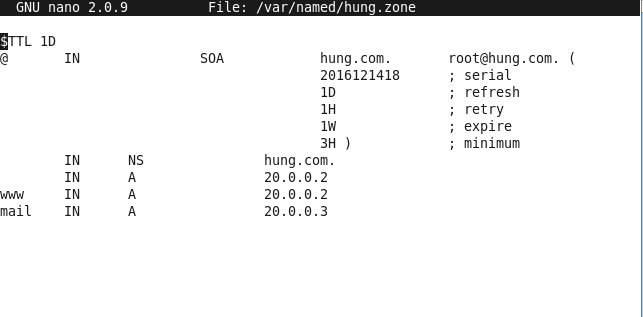
* Cấu hình file named. rfc1912.zones

Thêm các đoạn sau:

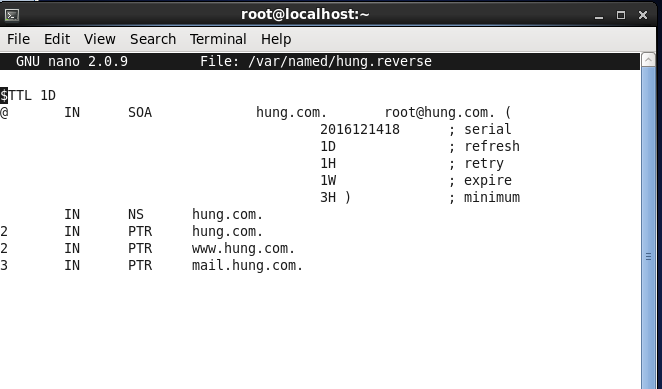
 

* Tạo ra các zone

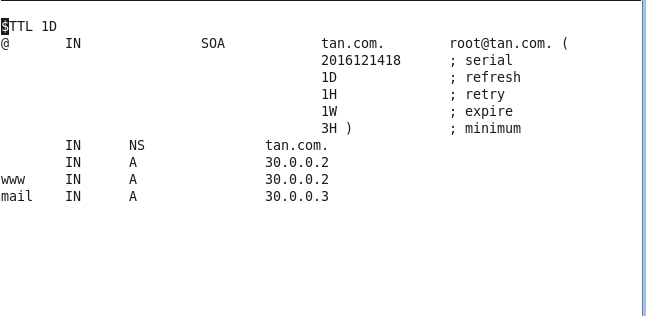
-File hung.zone: *nano /var/named/hung.zone*(cho phân giải thuận)



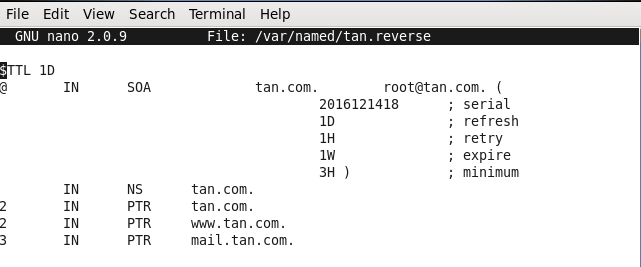
-File hung.reverse: *nano /var/named/hung.reverse*(cho phân giải nghịch )



-File tan.zone: *nano /var/named/tan.zone*(cho phân giải thuận)



-File tan.reverse: *nano /var/named/tan.reverse*(cho phân giải nghịch )



Sau khi cấu hình xong 2 file zone thuận và nghich, bạn phải phân quyền cho 2 file này thuộc về named :

*Chown named:named /var/named/hung.zone*

*Chown named:named /var/named/hung.reverse*

*Chown named:named /var/named/tan.zone*

*Chown named:named /var/named/tan.reverse*

Vào sửa Resolv.conf : “ *nano /etc/resolv.conf”*

“Server Name :20.0.0.2”

#### b.DNS \_Server Internet

\*Yêu Cầu

Đây là DNS của hệ thống bên ngoài Internet

Địa chỉ IP : 30.0.0.2/24 , default router 30.0.0.40

Phân giải địa chỉ tan.com -> 30.0.0.2; hung.com ->20.0.0.2; mail.tan.com -> 30.0.0.3 ;mail.hung.com ->20.0.0.3.

Làm tương tự như phần a chỉ có phần sửa Resolv.conf là “Server Name : 30.0.0.2“

### 2.2.2Hệ thống Web với SSL

**Bước 1**: Cài đặt apache lên Centos:

- Đâu tiên cài đặt apache trên centos :

*sudo yum install httpd*

- Sau đó khởi động apache

*sudo service httpd start*

- Cài đặt open SSL trên apache

*sudo yum install mod\_ssl open ssl*

**Bước 2.** Tạo các chứng chỉ

Tạo chứng chỉ :   
- Tạo Generate private key

*sudo open genrsa –out ca.key 2048*

-Tạo CSR:   
 *sudo open req –new -key ca.key -out ca.csr*

-Tạo Self Signed key

*sudo openssl x509 –req –day 365 –in ca.csr -signkey ca.key ca.crt*

-Sau đó copy các chứng chỉ vào vị trí /etc/pki/tls

*sudo cp ca.crt /etc/pki/tls/certs*

*sudo cp ca.key /etc/pki/tls/private/ca.key*

*sudo cp ca.csr /etc/pki/tls/private/ca.csr*

**Bước 3**. Cấu hình cho apache chấp nhận chứng chỉ ta đã tạo ra:

Mở file ./ssl.conf và thự hiện chỉnh sửa:

*sudo nano /etc/httpd/conf.d/ssl.conf*

Tìm đến dòng thích hợp và chỉnh thành:

Listen 443

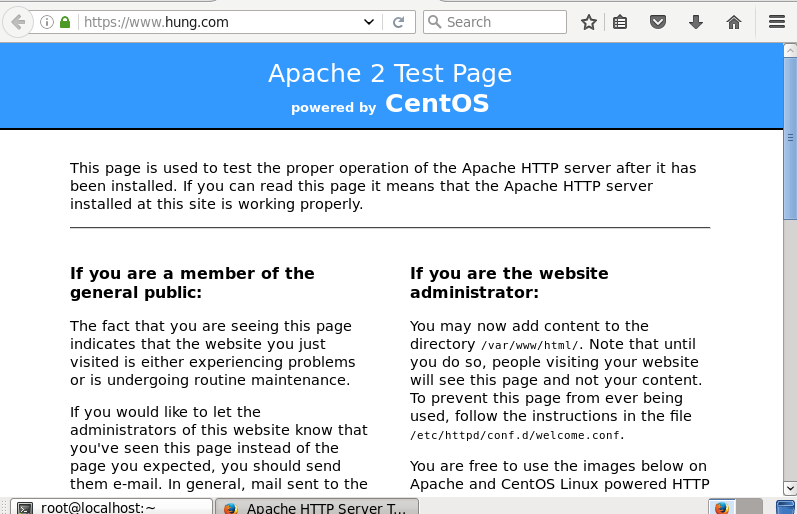
SSLEngine on

SSLCertificateFile /etc/pki/tls/certs/ca.crt

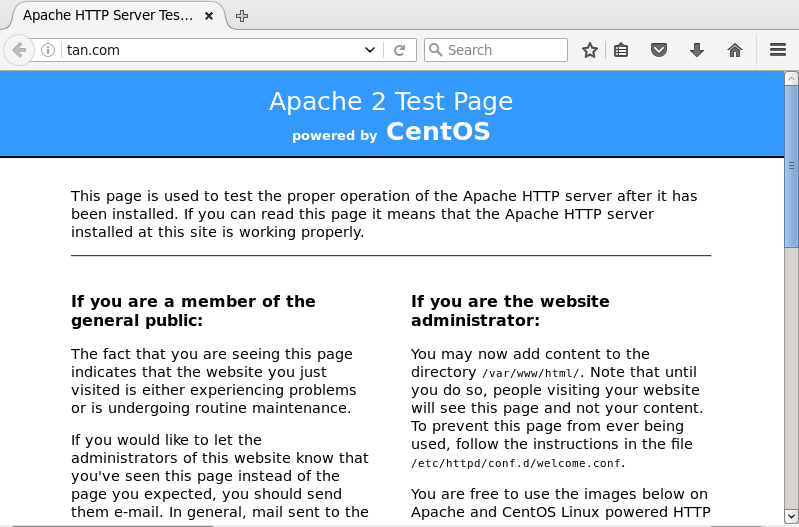
SSLCertificateKeyFile /etc/pki/tls/private/ca.key

Kết quả sau khi cài đặt:

Web\_Intranet:



Web Internet:



### 2.2.3 Hệ thống mail

#### a.Mail Private (Mail Intranet)

\* Yêu cầu

Địa chỉ Ip là 20.0.0.3/24 ;default route : 20.0.0.20 ;DNS : 20.0.0.2

Cài postfix : *yum install postfix –y*

Cài dovecot: yum install dovecot –y

Cài **Squirrelmail:**

***+*** *wget* [*http://epel.mirror.net.in/epel/6/i386/epel-release-6-8.noarch.rpm*](http://epel.mirror.net.in/epel/6/i386/epel-release-6-8.noarch.rpm)

*+ rpm -Uvh epel-release-6-8.noarch.rpm*

*+ yum install squirrelmail -y*

\*Cấu hình

-**Cấu hình trên postfix**

Thực hiện lệnh : *nano* ***/etc/postfix/main.cf***

Tìm đến dòng thích hợp và chỉnh sửa lại

Myhostname = mail.hung.com

Mydomain = hung.com

myorigin = $mydomain

inet\_interfaces = all

inet\_protocols = all

mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain

mynetworks = 192.168.10.0/24, 127.0.0.0/8,10.0.0.0/8,30.0.0.0/24

home\_mailbox = Maildir/

Sửa xong rồi thì Save và Exit. Sau đó khởi động dịch vụ và cho phép chạy khi khởi động CentOS.  
# service postfix restart  
# chkconfig postfix on

**-Cấu hình trên dovevot**

Cấu hình file “/etc/dovecot/dovecot.conf **“ sửa thành**

**“protocols = imap imaps pop3 pop3s lmtp “**

Cấu hình file  /etc/dovecot/conf.d/10-mail.conf **sửa thành**

**“**mail\_location = maildir:~/Maildir”

Cấu hình file **/etc/dovecot/conf.d/10-auth.conf sửa thành**

**“**disable\_plaintext\_auth = yes”

“auth\_mechanisms = plain login”

Cấu hình file /etc/dovecot/conf.d/10-master.conf sửa thành

“mode = 0600  
user = postfix  
group = postfix”

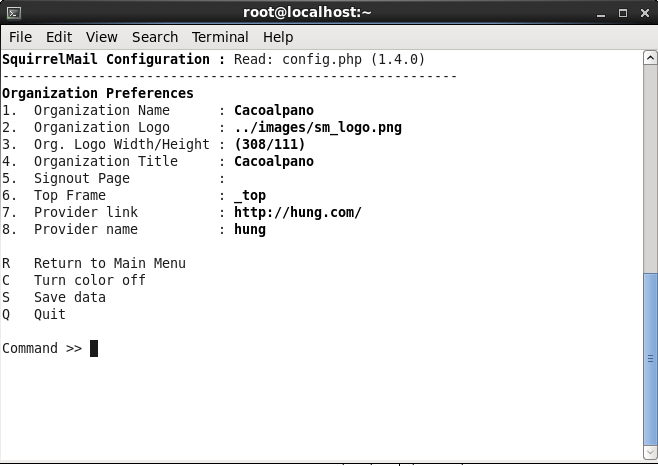
Khởi động lại dịch vụ cho phép chạy khi khởi động

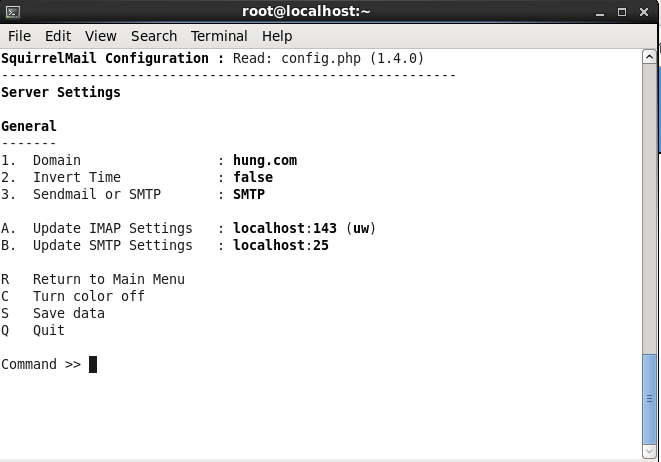
*service dovecot start  
chkconfig dovecot on*

-**Cấu hình Squirrelmail**

Chạy lênh :”/usr/share/squirrelmail/config/conf.pl”

Cấu hình các tham số phù hợp lại như sau :





* Cấu hình file :/etc/httpd/conf/httpd.conf , thêm đoạn sau vào cuối file

*Alias /webmail /usr/share/squirrelmail*

*<Directory /usr/share/squirrelmail>*

*Options Indexes FollowSymLinks*

*RewriteEngine On*

*AllowOverride All*

*DirectoryIndex index.php*

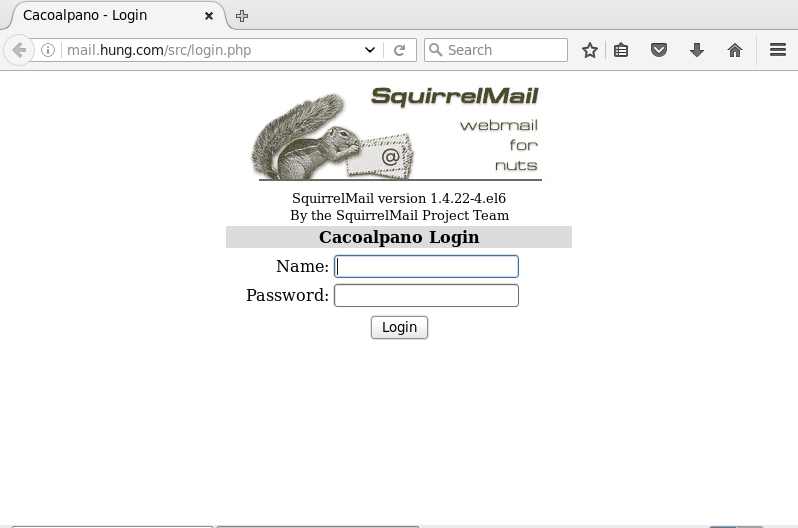
*Order allow,deny*

*Allow from all*

*</Directory>*

Lưu lại và khởi động lại httpd : “*service httpd restart”*

* Tạo 2 tài khoản “tan “ và “nam” trên centos
* Truy cập mail.hung.com thu được kết quả



#### b.Mail Internet

Làm tương tự phần trên chỉ thay địa chỉ

Myhostname = mail.tan.com

Mydomain = tan.com

Kết quả thu được :

