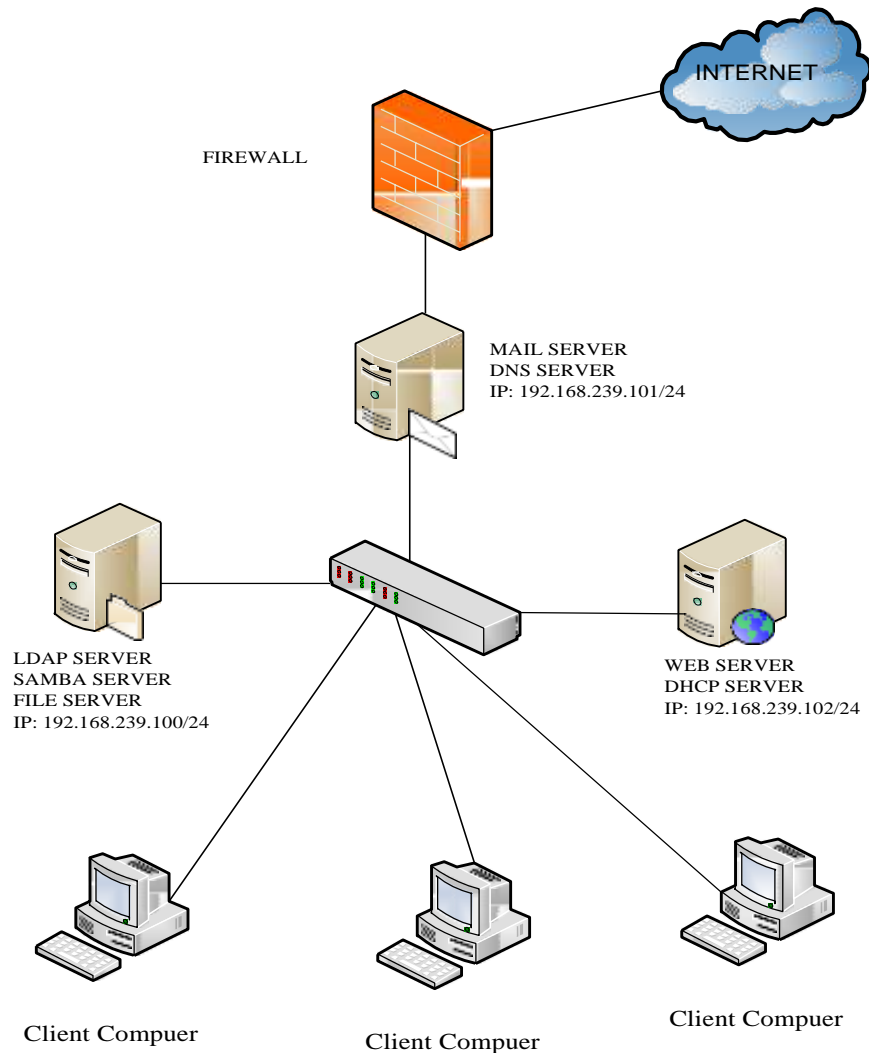


CHƯƠNG 3

TRIỂN KHAI QUẢN TRỊ MẠNG TRÊN UBUNTU SERVER

XÂY DỰNG KỊCH BẢN

Giới thiệu mô hình



Hình 3.1. Mô hình mạng

Cho hệ thống mạng (hình 3.1) được kết nối internet gồm có nhiều máy tính client được quản lý bởi hệ thống server sử dụng hệ điều hành Ubuntu Server.

3.1.1 Yêu cầu

- Quản trị cấu hình, tài nguyên mạng
- Quản trị người dùng, dịch vụ mạng

- Quản trị hiệu năng, hoạt động mạng
- Quản trị an ninh, an toàn mạng

3.2 PHÂN TÍCH

3.2.1 Phân tích yêu cầu

Quản trị cấu hình, tài nguyên mạng: Bao gồm các công tác quản lý, kiểm soát cấu hình, quản lý tài nguyên cấp phát cho các đối tượng sử dụng khác nhau.

Quản trị người dùng, dịch vụ mạng: bao gồm các công tác quản lý người sử dụng trên hệ thống và đảm bảo dịch vụ cung cấp có độ tin cậy cao, chất lượng đảm bảo theo đúng các chỉ tiêu đã đề ra.

Quản trị hiệu năng, hoạt động mạng: bao gồm các công tác quản lý, giám sát hoạt động mạng lưới, đảm bảo các hoạt động của thiết bị hệ thống ổn định.

Quản trị an ninh, an toàn mạng: bao gồm các công tác quản lý, giám sát mạng lưới, các hệ thống để đảm bảo phòng tránh các truy nhập trái phép. Việc phòng chống, ngăn chặn sự lây lan của các loại virus máy tính, các phương thức tấn công như Dos làm tê liệt hoạt động của mạng cũng là một phần rất quan trọng trong công tác quản trị, an ninh, an toàn mạng.

3.2.2 Giải pháp

- Cài đặt hệ điều hành Ubuntu Server 10.04
- Cài đặt và cấu hình LDAP
- Triển khai hệ thống Firewall
- Cấu hình DNS, DHCP
- Cài đặt và triển khai Web Server

3.3 THỰC HIỆN

3.3.1 Chuẩn bị

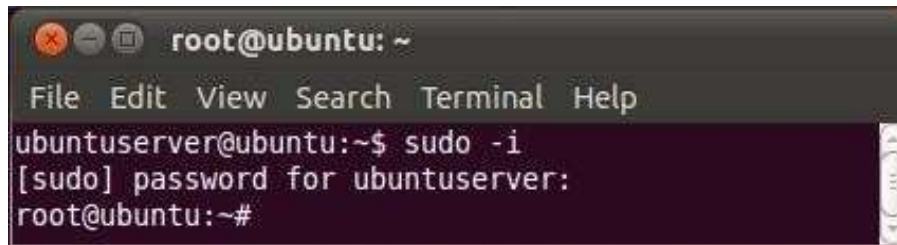
- Cài đặt ubuntu server 10.04 32bit hay 64bit
- Đặt địa chỉ IP tĩnh và máy có thể kết nối internet
- Update ubuntu server bằng lệnh sau :
 - + apt-get update
 - + apt-get dist-upgrade

+ reboot.

3.3.2 Cài đặt và cấu hình

3.3.2.1 Cài đặt và cấu hình LDAP

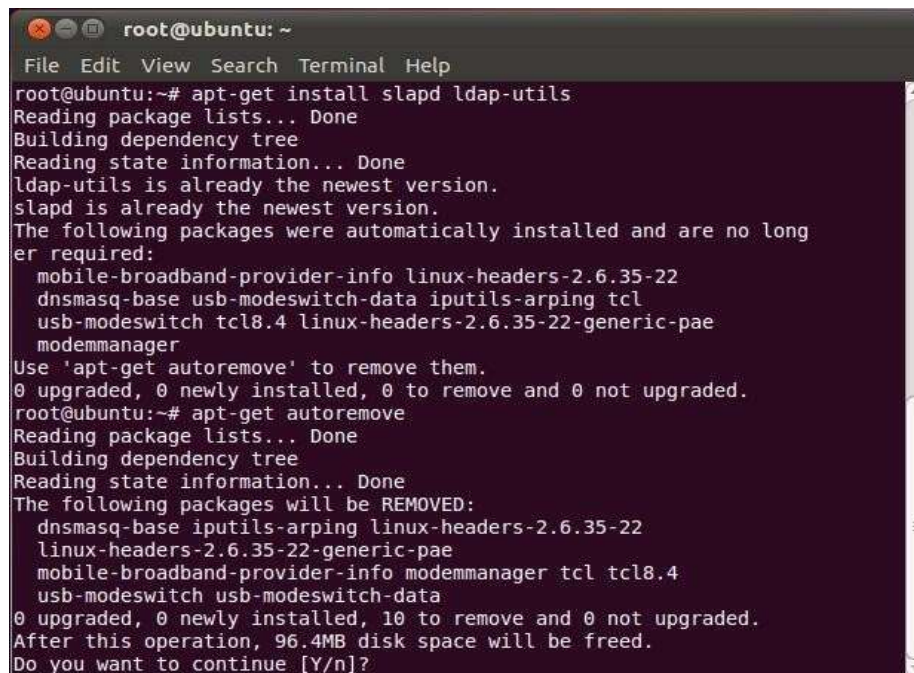
- Bước 1: mở terminal và lấy quyền root bằng lệnh sudo -i và đánh password của hệ thống



```
root@ubuntu: ~
File Edit View Search Terminal Help
ubuntuuserver@ubuntu:~$ sudo -i
[sudo] password for ubuntuuserver:
root@ubuntu:~#
```

Hình 3.2: Đăng nhập hệ thống Ubuntu Server

- Bước 2 : install LDAP server bằng lệnh apt-get install slapd ldap-utils



```
root@ubuntu:~# apt-get install slapd ldap-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
ldap-utils is already the newest version.
slapd is already the newest version.
The following packages were automatically installed and are no longer required:
mobile-broadband-provider-info linux-headers-2.6.35-22
dnsmasq-base usb-modeswitch-data iputils-arping tcl
usb-modeswitch tcl8.4 linux-headers-2.6.35-22-generic-pae
modemmanager
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@ubuntu:~# apt-get autoremove
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
dnsmasq-base iputils-arping linux-headers-2.6.35-22
linux-headers-2.6.35-22-generic-pae
mobile-broadband-provider-info modemmanager tcl tcl8.4
usb-modeswitch usb-modeswitch-data
0 upgraded, 0 newly installed, 10 to remove and 0 not upgraded.
After this operation, 96.4MB disk space will be freed.
Do you want to continue [Y/n]?
```

Hình 3.3: Cài đặt LDAP Server (1)

- Bước 3 : ta add các schema cần thiết cho LDAP bằng các lệnh sau :
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f
/etc/ldap/schema/inetorgperson.ldif

- Bước 4: ta tạo 1 file backend.minhtuan.net.ldif
- Bước 5: Ở bước này ta sẽ thực hiện add file ldif vừa mới tạo ở trên vào hệ thống LDAP bằng lệnh sau :

```
ldapadd -Y EXTERNAL -H ldapi:/// -f backend.example.com.ldif
```
- Bước 6: cài đặt SAMBA và các gói cần thiết bằng lệnh sau :

```
apt-get install samba samba-doc libpam-smbpass smbclient smbldap-tools
```

```

root@ubuntu: ~
File Edit View Search Terminal Help
root@ubuntu:~# apt-get install samba samba-doc libpam-smbpass smbclient smbldap-
tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
smbclient is already the newest version.
The following extra packages will be installed:
  libconvert-asn1-perl libcrypto-smbhash-perl libdigest-md4-perl
  libio-socket-ssl-perl libjcode-pm-perl libnet-ldap-perl libnet-libidn-perl
  libnet-ssleay-perl libunicode-map-perl libunicode-map8-perl
  libunicode-maputf8-perl libunicode-string-perl
Suggested packages:
  libio-socket-inet6-perl libauthen-sasl-perl libxml-sax-perl openbsd-inetd
  inet-superserver ldb-tools samba-doc-pdf
The following NEW packages will be installed:
  libconvert-asn1-perl libcrypto-smbhash-perl libdigest-md4-perl
  libio-socket-ssl-perl libjcode-pm-perl libnet-ldap-perl libnet-libidn-perl
  libnet-ssleay-perl libpam-smbpass libunicode-map-perl libunicode-map8-perl
  libunicode-maputf8-perl libunicode-string-perl samba samba-doc smbldap-tools
0 upgraded, 16 newly installed, 0 to remove and 0 not upgraded.
Need to get 11.8MB of archives.
After this operation, 37.5MB of additional disk space will be used.
Do you want to continue [Y/n]? █

```

Hình 3.4: Cài đặt SAMBA Server (2)

- Bước 7 : cấu hình SAMBA. Ta cấu hình file /etc/samba/smb.conf như sau :
 - workgroup = VT071A
 - netbios name = PDC-SAMBA
 - obey pam restrictions = Yes
 - passdb backend = ldapsam:ldap://localhost
 - pam password change = Yes
 - syslog = 0
 - log file = /var/log/samba/log.%m
 - max log size = 1000 server signing = auto server schannel = Auto
 - printcap name = cups
 - add user script = /usr/sbin/smbldap-useradd -m '%u'
 - delete user script = /usr/sbin/smbldap-userdel %u
 - add group script = /usr/sbin/smbldap-groupadd -p '%g'
 - delete group script = /usr/sbin/smbldap-groupdel '%g'

- add user to group script = /usr/sbin/smbldap-groupmod -m'%u'%'g'
- delete user from group script = /usr/sbin/smbldap-groupmod-x '%u'%'g'
- set primary group script = /usr/sbin/smbldap-usermod -g'%g'%'u'
- add machine script = /usr/sbin/smbldap-useradd -w '%u'
- logon script = allusers.bat logon path = logon home =domain
- logons = Yes
- os level = 35
- domain master = Yes
- dns proxy = No
- wins support = Yes
- ldap admin dn = cn=admin,dc=hoasen,dc=local
- ldap group suffix = ou=Groups
- ldap idmap suffix = ou=Idmap
- ldap machine suffix = ou=Computers
- unix password sync = no ldap
- passwd sync = yes
- ldap suffix = dc=minhtuan,dc=local
- ldap ssl = no
- ldap user suffix = ou=Users
- panic action = /usr/share/samba/panic-action %d
- [homes]
- comment = Home Directories
- valid users = %S
- read only = No browseable = No browsable = No
- [netlogon]
- comment = Network Logon Service path = /var/lib/samba/netlogon
- admin users = root
- guest ok = Yes browseable = No
- browsable = No
- [Profiles]
- comment = Roaming Profile Share
- path = /var/lib/samba/profiles
- read only = No profile acls = Yes browseable = No
- browsable = No
- [printers]
- comment = All Printers
- path = /var/spool/samba
- admin users = root
- write list = root
- read only = No create mask = 0600 guest ok = Yes printable = Yes
- use client driver = Yes
- browseable = No browsable = No

- [print\$]
- comment = Printer Drivers Share
- path = /var/lib/samba/printers admin users = root
- write list = root create mask = 0664 directory mask = 0775
- [shared]
- path = /var/lib/samba/shared
- read only = No
- guest ok = Yes

Lưu ý : Ở phần cấu hình trên ta nên quan tâm một số biến quan trọng sau :

- workgroup = VT071A
- netbios name = PDC-SAMBA
- passdb backend = ldapsam:ldap://localhost
- ldap admin dn = cn=admin,dc=hoasen,dc=local ldap group suffix = ou=Groups
- ldap idmap suffix = ou=Idmap
- ldap machine suffix = ou=Computers
- unix password sync = no
- ldap passwd sync = yes
- ldap suffix = dc=minhtuan,dc=local

3.3.2.2 Cài đặt và cấu hình DNS Server

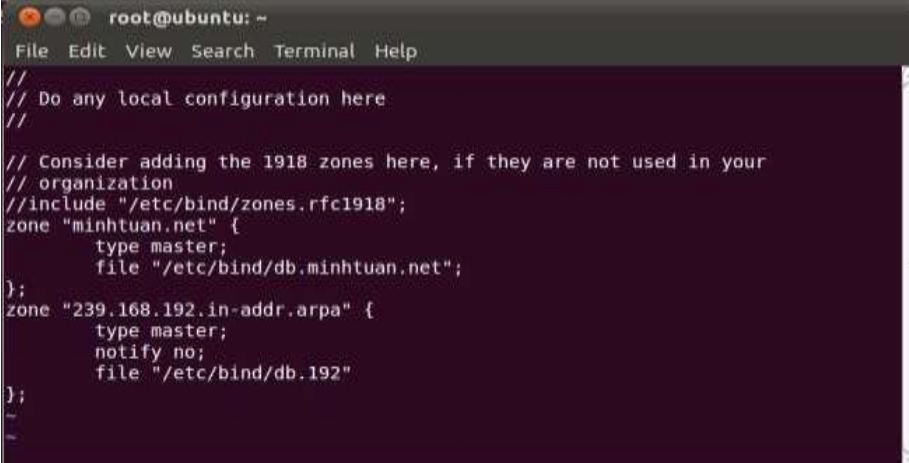
➤ Cài đặt

Ta dùng lệnh sau để cài đặt DNS server (BIND9)

```
apt-get install bind9
```

➤ Cấu hình DNS server :

Ta cấu hình file /etc/bind/name.conf.local để khai báo các zone có nội dung như sau :



```

root@ubuntu: ~
File Edit View Search Terminal Help
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "minhtuan.net" {
    type master;
    file "/etc/bind/db.minhtuan.net";
};
zone "239.168.192.in-addr.arpa" {
    type master;
    notify no;
    file "/etc/bind/db.192"
};
-
-

```

Hình 3.5: Cấu hình DNS Server (1)

Vì ta hai file như đã khai báo ở trên với nội dung như 2 hình ở dưới :

- File /etc/bind/db.minhtuan.net được cấu hình như sau:

```

root@ubuntu: ~
File Edit View Search Terminal Help
; BIND data file for net loopback interface
;
$TTL      604800
@         IN      SOA     minhtuan.net. admin.minhtuan.net. (
                                12122012      ;Serial
                                604800       ;Refresh
                                86400       ;Retry
                                2419200    ;Expire
                                604800)    ;Negative Cache TTL
;
@         IN      NS      minhtuan.net.
@         IN      A       192.168.239.101
@         IN      AAAA    ::1
mail      IN      MX       192.168.239.101
mail      IN      MX       1 mail.minhtuan.net
dc        IN      A       192.168.239.100
    
```

Hình 3.6: Cấu hình DNS Server (2)

- File /etc/bind/db.192 được cấu hình như sau:

```

root@ubuntu: ~
File Edit View Search Terminal Help
; BIND reverse data file for net loopback inteface
;
$TTL      604800
@         IN      A       minhtuan.net. admin.minhtuan.net. (
                                12122012      ;Serial
                                604800       ;Refresh
                                86400       ;Retry
                                2419200    ;Expire
                                604800 )    ;Negative Cache TTL
;
@         IN      NS      minhtuan.net.
100      IN      PTR     dc.minhtuan.net.
101      IN      PTR     mail.minhtuan.net
102      IN      PTR     www.minhtuan.net
    
```

Hình 3.7: Cấu hình DNS Server (3)

3.3.2.3 Cài đặt và cấu hình DHCP Server **(in nghiêng)**

➤ **Chuẩn bị các thông tin :**

- ethernet device : eth0
- Ip range : 192.168.239.100 – 192.168.239.200
- Subnet address : 192.168.239.0
- Netmask : 255.255.255.0
- DNS server 192.168.239.1

- Domain : minh Tuan.net
- Default Gateway Address : 192.168.239.1
- Broadcast Address : 192.168.239.255

➤ **Cài đặt**

sudo apt-get install dhcp3-server

➤ **Cấu hình DHCP Server**

- **Cấu hình file /etc/default/dhcp3-server**

sudo gedit /etc/default/dhcp3-server

Tìm dòng INTERFACES="" và thay bằng INTERFACES="eth0"

```

*dhcp3-server (/etc/default) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
*dhcp3-server
# Defaults for dhcp initscript
# sourced by /etc/init.d/dhcp
# installed at /etc/default/dhcp3-server by the maintainer scripts
#
# This is a POSIX shell fragment
#
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="eth0"
Plain Text Tab Width: 8 Ln 11, Col 17 INS

```

Hình 3.8. Cấu hình DHCP Server

Sau đó Save và thoát

- **Cấu hình file pool:**

Mở file /etc/dhcp3/dhcpd.conf

Tìm đến dòng 16. Có đoạn thông tin sau :

```

#option definitions common to all supported
networks... option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;
default-lease-time 600;

```



```
max-lease-time 7200;
```

Sửa thành :



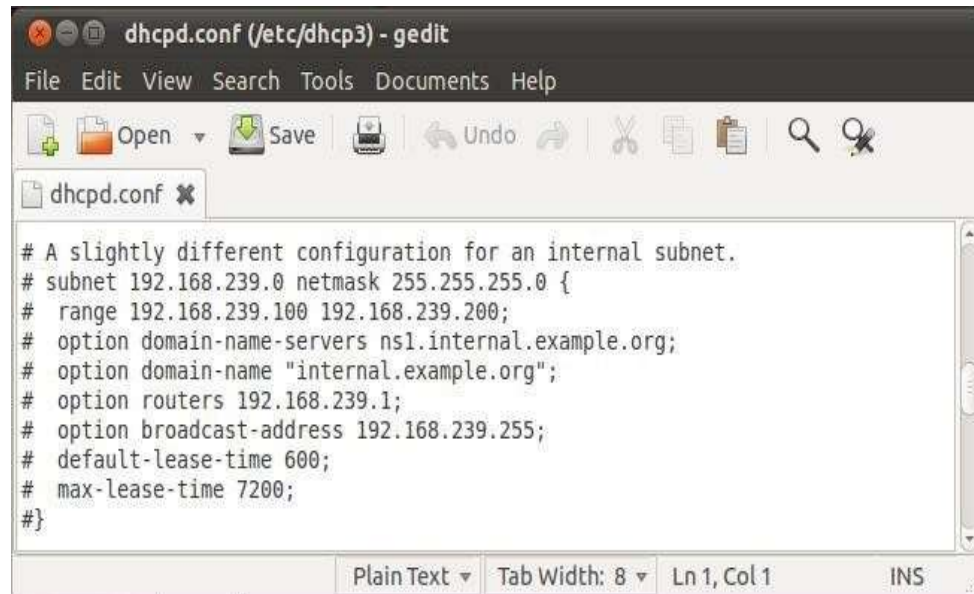
```
*dhcpd.conf (/etc/dhcp3) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
*dhcpd.conf
ddns-update-style none;
#option definitions common to all supported networks...
#option domain-name "example.org";
#option domain-name-servers ns1.example.org, ns2.example.org;
#default-lease-time 600;
#max-lease-time 7200;
# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;
Plain Text Tab Width: 8 Ln 15, Col 1 INS
```

Hình 3.9. Cấu hình file pool (a)

Tiếp tục, tìm đến dòng 53. Có đoạn như sau :

```
# A slightly different configuration for an internal subnet.
# subnet 10.5.5.0 netmask 255.255.255.224 {
# range 10.5.5.26 10.5.5.30;
# option domain-name-servers ns1.internal.example.org;
# option domain-name "internal.example.org";
# option routers 10.5.5.1;
# option broadcast-address 10.5.5.31;
# default-lease-time 600;
# max-lease-time 7200;
#}
```

Sửa thành :



```
dhcpd.conf (/etc/dhcp3) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
dhcpd.conf
# A slightly different configuration for an internal subnet.
# subnet 192.168.239.0 netmask 255.255.255.0 {
# range 192.168.239.100 192.168.239.200;
# option domain-name-servers ns1.internal.example.org;
# option domain-name "internal.example.org";
# option routers 192.168.239.1;
# option broadcast-address 192.168.239.255;
# default-lease-time 600;
# max-lease-time 7200;
#}
Plain Text Tab Width: 8 Ln 1, Col 1 INS
```

Hình 3.10: Cấu hình file pool (b)

➤ **Khởi động lại dịch vụ DHCP Server:**

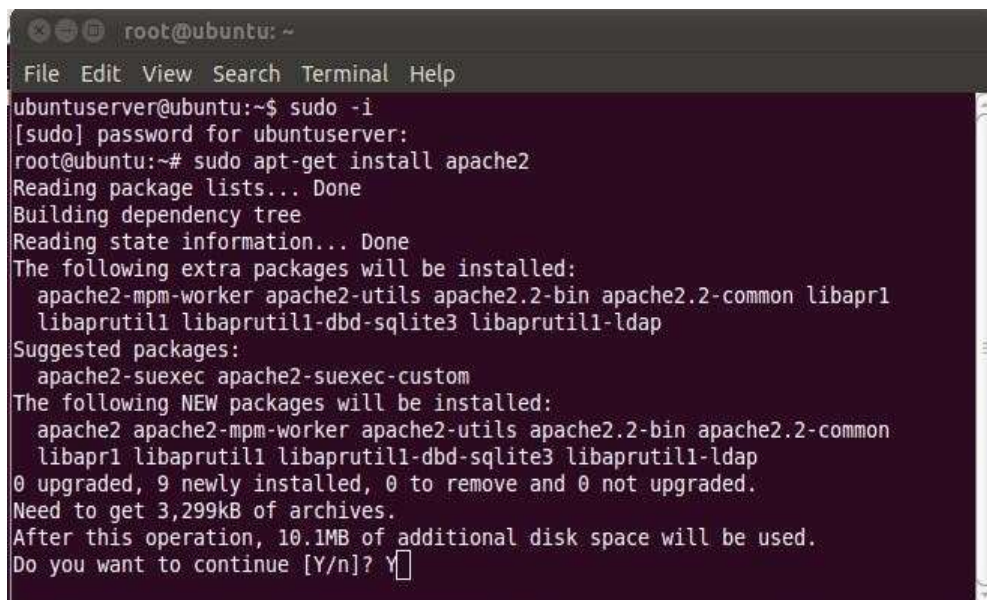
sudo /etc/init.d/dhcp3-server restart

3.3.2.4 Cài đặt và triển khai Web Server

➤ **Cài Đặt :**

Ta dùng lệnh sau để cài đặt:

sudo apt-get install apache2

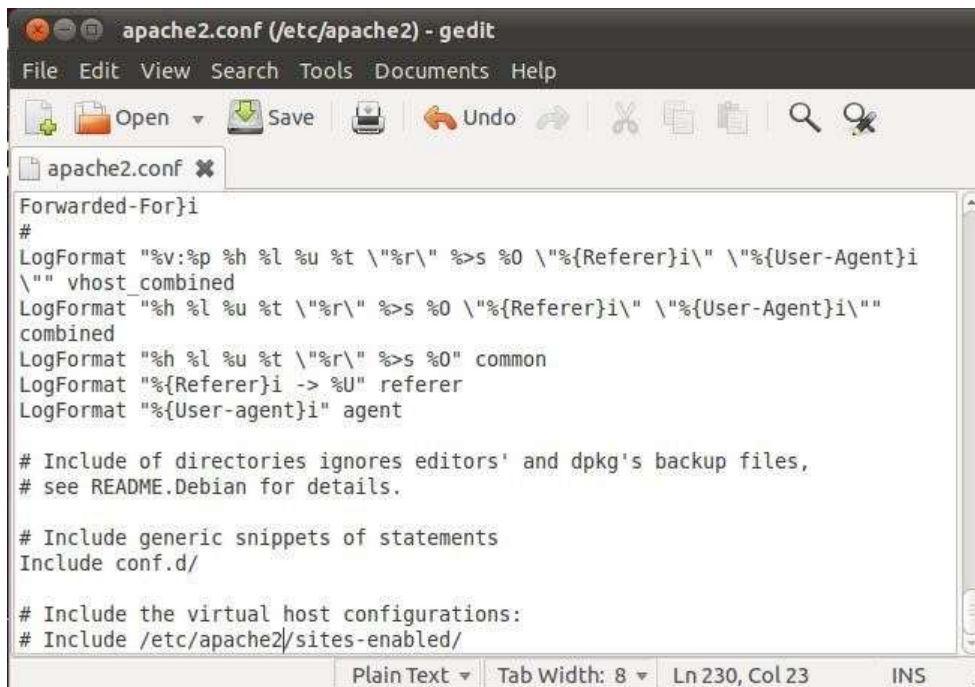


```
root@ubuntu: ~
File Edit View Search Terminal Help
ubuntuserver@ubuntu:~$ sudo -i
[sudo] password for ubuntuserver:
root@ubuntu:~# sudo apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  apache2-mpm-worker apache2-utils apache2.2-bin apache2.2-common libapr1
  libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
Suggested packages:
  apache2-suexec apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-mpm-worker apache2-utils apache2.2-bin apache2.2-common
  libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.
Need to get 3,299kB of archives.
After this operation, 10.1MB of additional disk space will be used.
Do you want to continue [Y/n]? Y
```

Hình 3.11: Cài đặt Web Server

➤ Cấu hình APACHE với LDAP :

Ta cấu hình file /etc/apache2/apache2.config



Hình 3.12: Cấu hình APACHE với LDAP

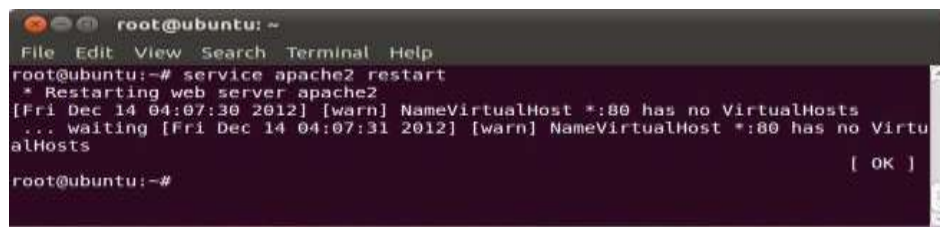
Tại cuối file này ta comment dòng Include “/etc/apache2/sites-enabled/” thành “#Include /etc/apache2/sites-enabled/”

Cũng trong file này ta thêm vào những dòng sau đây.

```
DocumentRoot /home/ubuntuuser
ServerName www.minhtuan.net
<Directory /home/ubuntuuser >
Order deny,allow
Allow from all
</Directory>
```

Ta save lại và restart apache bằng lệnh

Service apache2 restart



Hình 3.13: Restart apache

3.3.2.5 Thiết lập Firewall

➤ Giới thiệu:

Iptables trong ubuntu không phải là 1 server và đã được tích hợp sẵn trong kernel của ubuntu nên ta không cần thực hiện cài đặt.

➤ Cấu hình NAT:

Trước khi cấu hình NAT, ta nên cấu hình địa chỉ IP tĩnh cho các interface

- **Bước 1:** ta thực hiện dòng lệnh sau:

```
sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip_forward"
```

Dòng lệnh trên sẽ gán giá trị 1 trong file ip_forward, cho phép chuyển tiếp các gói trong các interface của hệ thống.

- **Bước 2 :** ta edit file /etc/sysctl.conf và chuyển các dòng sau :

```
net.ipv4.ip_forward=1
```

Điều này giúp cho giá trị của file ip_forward trong bước luôn có giá trị bằng 1 khi hệ thống khởi động.

- **Bước 3:** ta cấu hình NAT bằng các dòng lệnh sau :

```
- iptables -A FORWARD -o eth1 -i eth2 -s 192.168.193.0/24 -m  
conntrack --ctstate NEW -j ACCEPT
```

```
- iptables -A FORWARD -m conntrack --ctstate  
ESTABLISHED,RELATED -j ACCEPT
```

```
- iptables -A POSTROUTING -t nat -j MASQUERADE
```

- **Bước 4:** vì iptables sẽ bị xóa hết sau khi hệ thống khởi động lại nên ta phải sử dụng một scripts để có thể phục hồi cấu hình của iptables.

➤ NAT inbound cho web server :

Để người dùng bên ngoài có thể truy cập đến web server ta cấu hình iptables như sau :

```
iptables -t nat -A PREROUTING -d 192.168.0.110 -i eth1 -p tcp - m tcp --  
dport 80 -j DNAT --to-destination 192.168.239.102:80
```

Dòng lệnh trên có ý nghĩa là tất cả kết nối nào có địa chỉ đích là 192.168.0.110 đến từ interface mặt ngoài của firewall với protocol là TCP và port đích là 80 thì sẽ nat vào cho địa chỉ 192.168.239.102(địa chỉ web server) với port 80.

3.4 TEST DEMO

KẾT LUẬN

Trong quá trình nghiên cứu thực hiện khóa luận tốt nghiệp với đề tài “Tìm hiểu và triển khai quản trị mạng trên Ubuntu Server”, nhờ có sự hướng dẫn tận tình của thầy Nguyễn Minh Nhật, em đã tìm hiểu và nắm vững được các kiến thức cơ bản về hệ thống mạng máy tính cũng như cách quản lý hệ thống mạng bằng hệ điều hành Ubuntu Server. Do điều kiện về thời gian có hạn, em chỉ giới hạn ở phạm vi xây dựng kịch bản trên máy ảo. Mặc dù đã rất cố gắng nhưng không tránh khỏi có những sai sót. Em rất mong được sự góp ý, giúp đỡ nhiệt tình của các thầy cô và các bạn để đề tài khóa luận tốt nghiệp này của em được hoàn thiện hơn.

Dưới đây là những việc đã làm được và chưa làm được về đề tài khóa luận tốt nghiệp này:

- Những việc đã làm được:
 - Khái quát tổng quan kiến trúc, thành phần của mô hình quản trị mạng
 - Tìm hiểu hệ điều hành Ubuntu
 - Nắm được các dịch vụ quản trị mạng trên Ubuntu Server
 - Thực hiện demo triển khai quản trị mạng với hệ điều hành Ubuntu Server.
- Những việc chưa làm được:
 - Chưa triển khai demo hoàn thiện và đầy đủ các dịch vụ trên Ubuntu Server

