



# Taisachmoi.com Tìm hiểu và triển khai quản trị mạng trên Ubuntu Server

toán ứng dụng (Trường Đại học Đại Nam)



Scan to open on Studocu

# **Luận văn**

## **Tìm hiểu và triển khai quản trị mạng trên Ubuntu Server**

# MỤC LỤC

## MỤC LỤC

### **DANH MỤC VIẾT TẮT**

### **DANH MỤC HÌNH VẼ**

<b>MỞ ĐẦU</b> .....	1
1. LÝ DO.....	1
2. MỤC TIÊU VÀ NHIỆM VỤ.....	1
3. ĐỐI TƯỢNG NGHIÊN CỨU.....	1
4. PHẠM VI NGHIÊN CỨU.....	<b>Error! Bookmark not defined.</b>
5. Ý NGHĨA KHOA HỌC VÀ THỰC TIỄN.....	<b>Error! Bookmark not defined.</b>
<b>CHƯƠNG 1 : TỔNG QUAN VỀ MẠNG MÁY TÍNH</b> .....	3
<b>1.1 GIỚI THIỆU VỀ MẠNG MÁY TÍNH</b> .....	3
1.1.1 Lịch sử hình thành.....	3
1.1.2 Định nghĩa mạng máy tính.....	4
1.1.3 Ứng dụng của mạng máy tính.....	5
<b>1.2 THÀNH PHẦN CƠ BẢN TRONG MẠNG MÁY TÍNH</b> .....	6
1.2.1 Tổng quát mạng máy tính cơ bản.....	6
1.2.2 Kiến trúc (Cấu trúc) mạng cục bộ.....	6
<b>1.3 KIẾN TRÚC VÀ MÔ HÌNH QUẢN TRỊ MẠNG</b> .....	8
1.3.1 Kiến trúc và mô hình quản trị mạng OSI.....	8
1.3.2 Kiến trúc và mô hình quản trị mạng SNMP.....	13
1.3.3 Kiến trúc quản trị tích hợp OMP.....	18
1.3.4 Chức năng của hệ thống quản trị mạng.....	22
<b>CHƯƠNG 2: GIỚI THIỆU VỀ HỆ ĐIỀU HÀNH UBUNTU SERVER</b> .....	23
<b>2.1 TỔNG QUAN VỀ UBUNTU</b> .....	23
2.1.1 Lịch sử và khái niệm cơ bản.....	23
2.1.2 Tìm hiểu các lệnh cơ bản trong Ubuntu Server.....	25
2.1.3 Môi trường đồ họa của Ubuntu Server.....	29

<b>2.2</b>	<b>QUẢN LÝ USER VÀ PHÂN QUYỀN TRONG UBUNTU SERVER</b>	
		32
2.2.1	Thiết lập tài khoản người dùng.....	32
2.2.2	Tạo nhóm, tìm hiểu những tập lệnh quản trị nhóm.....	34
2.2.3	Phân quyền FileSystem.....	35
<b>2.3</b>	<b>CẤU TRÚC VÀ CÁC DỊCH VỤ TRÊN UBUNTU SERVER.....</b>	<b>38</b>
2.3.1	LDAP.....	38
2.3.2	DNS Server.....	48
2.3.3	DHCP Server.....	62
	<b>CHƯƠNG 3: TRIỂN KHAI QUAN TRỊ MẠNG TRÊN UBUNTU SERVER. .</b>	<b>68</b>
<b>3.1</b>	<b>XÂY DỰNG KỊCH BẢN.....</b>	<b>68</b>
3.1.1	Giới thiệu mô hình.....	68
3.1.2	Yêu cầu.....	68
<b>3.2</b>	<b>PHÂN TÍCH.....</b>	<b>69</b>
3.2.1	Phân tích yêu cầu.....	69
3.2.2	Giải pháp.....	69
<b>3.3</b>	<b>THỰC HIỆN.....</b>	<b>69</b>
3.3.1	Chuẩn bị.....	69
3.3.2	Cài đặt và cấu hình.....	70
<b>3.4</b>	<b>TEST DEMO.....</b>	<b>80</b>
	<b>KẾT LUẬN.....</b>	<b>81</b>
	<b>TÀI LIỆU THAM KHẢO.....</b>	<b>82</b>

### DANH MỤC VIẾT TẮT (canh giữa cỡ chữ 16)

Từ viết tắt	Từ viết đầy đủ	Ý nghĩa
CSMA/CD	Carrier Sense Multiple Access with Collision Detection	Giao thức đường dây đa truy cập với cảm nhận va chạm
DHCP	Dynamic Host Configuration Protocol	Giao thức cấu hình host động
DNS	Domain Name System	Hệ thống tên miền
GUI	Graphic User Interface	Mô hình giao tiếp kiểu tương tác giữa ứng dụng và user dạng đồ họa
HTTP	HyperText Transfer Protocol	Giao thức truyền tải siêu văn bản
IETF	Internet Engineering Task Force	Tổ chức đã đưa ra chuẩn SNMP thông qua các RFC
LDAP	Lightweight Directory Access Protocol	Giao thức truy cập nhanh các dịch vụ thư mục
MO	Managed Object	Quản lý đối tượng
NIC	Network interface Card	Một giao tiếp mạng trên mỗi máy
OSI	Open Systems Interconnection Reference Mode	Mô hình tham chiếu kết nối các hệ thống mở
SNMP	Simple Network Management Protocol	Một tập hợp các giao thức không chỉ cho phép kiểm tra nhằm đảm bảo các thiết bị mạng
TCP/IP	Transmission Control Protocol/Internet Protocol	Một bộ các giao thức truyền thông

### DANH MỤC HÌNH VẼ

Hình 1.1	Một mô hình liên kết các máy tính trong mạng
Hình 1.2	Mô hình mạng dùng chung tài nguyên

Hình 1.3	Các phương thức liên kết mạng
Hình 1.4	Mô hình quản trị mạng OSI
Hình 1.5	Mô hình truyền thông OSI
Hình 1.6	Mô hình chức năng OSI
Hình 1.7	Mô hình quản trị mạng SMNP
Hình 1.8	Mô hình hoạt động của SMNP
Hình 2.1	Các nút đóng, đóng nhỏ hết cỡ và mở to hết cỡ là trên đỉnh góc bên trái của các cửa sổ
Hình 2.2	Trình quản lý tệp Nautilus hiển thị thư mục home
Hình 2.3	Liên quan giữa Entry và Attribute
Hình 2.4	Mô hình kết nối giữa client/server
Hình 2.5	Thao tác tìm kiếm cơ bản
Hình 2.6	Những thông điệp Client gửi cho server
Hình 2.7	Nhiều kết quả tìm kiếm được trả về
Hình 2.8	Quá trình gửi một Email
Hình 2.9	Firewall cứng
Hình 2.10	Firewall mềm
Hình 2.11	Chức năng của Firewall
Hình 2.12	Trình tự xử lý gói tin của iptables
Hình 2.13	Mô hình hoạt động Web Server
Hình 3.1	Mô hình mạng
Hình 3.2	Đăng nhập hệ thống Ubuntu Server
Hình 3.3	Cài đặt LDAP Server (1)
Hình 3.4	Cài đặt LDAP Server (2)
Hình 3.5	Cấu hình DNS Server (1)
Hình 3.6	Cấu hình DNS Server (2)
Hình 3.7	Cấu hình DNS Server (3)
Hình 3.8	Cấu hình DHCP Server
Hình 3.9	Cấu hình file pool (a)
Hình 3.10	Cấu hình file pool (b)
Hình 3.11	Cài đặt Web Server
Hình 3.12	Cấu hình APACHE với LDAP
Hình 3.13	Restar apache

## MỞ ĐẦU (canh giữa cỡ chữ 16)

### 1. LÝ DO CHỌN ĐỀ TÀI

Hiện nay ở Việt Nam đã có rất nhiều đơn vị và công ty triển khai hệ thống máy chủ riêng là tất yếu và cần thiết. Nhưng việc xây dựng một hệ thống máy chủ có quy mô đòi hỏi những kiến thức rất chuyên dụng về các dịch vụ, hệ thống mạng và ngay cả về hệ điều hành. Máy chủ thường chạy trên các hệ điều hành Window Server, hoặc các điều hành Linux và Ubuntu. Việc hệ điều hành Window Server khá thân thuộc nhưng hệ điều hành Window Server thì bản quyền khá đắt. Trong khi đó các máy chủ Ubuntu Server được đánh giá là bảo mật, lại hoàn toàn miễn phí(do xây dựng hoàn toàn trên hệ thống nguồn mở). Chính vì việc đáp ứng tốt các yêu cầu vừa có tiết kiệm chi phí vừa có tính ổn định, bảo mật và tốc độ vận hành nên em đã chọn hệ điều hành Ubuntu Server làm đề tài “Tìm hiểu và triển khai quản trị mạng trên Ubuntu Server”.

### 2. Ý NGHĨA CỦA ĐỀ TÀI

- Tìm hiểu sâu hơn về quản trị hệ thống mạng
- Dễ dàng quản trị hệ thống mạng trên hệ điều hành Ubuntu Server.

### 3. CÁC MỤC TIÊU CỦA ĐỀ TÀI

- Tìm hiểu các mô hình quản trị mạng
- Các hoạt động quản trị mạng
- Tìm hiểu và triển khai mô hình quản trị mạng trên Ubuntu (Cài đặt, cấu hình và quản trị hệ thống Ubuntu Server, quản trị tài khoản người dùng và nhóm trên Ubuntu v.v...)

### 4. ĐỐI TƯỢNG VÀ PHẠM VI NGHIÊN CỨU

- Đối tượng:
  - Các lý thuyết liên quan đến mô hình quản trị mạng
  - Hệ điều hành Ubuntu Server
  - Phương pháp triển khai hệ thống quản trị mạng trên Ubuntu

- Phạm vi nghiên cứu:
  - Tìm hiểu và triển khai quản trị một hệ thống mạng cho đơn vị, công ty có mô hình mạng LAN

## **5. PHƯƠNG PHÁP NGHIÊN CỨU**

- Nghiên cứu các mô phỏng quản trị mạng
- Xây dựng và triển khai một số chức năng quản trị cơ bản trên Ubuntu Server
- Cài đặt thử nghiệm



## CHƯƠNG 1

### TỔNG QUAN VỀ MẠNG MÁY TÍNH

#### 1.1 GIỚI THIỆU VỀ MẠNG MÁY TÍNH

##### 1.1.1 Lịch sử hình thành

Máy tính của thập niên 1940 là các thiết bị cơ-điện tử lớn và rất dễ hỏng. Sự phát minh ra transistor bán dẫn vào năm 1947 tạo ra cơ hội để làm ra chiếc máy tính nhỏ và đáng tin cậy hơn.

Năm 1950, các máy tính lớn mainframe chạy bởi các chương trình ghi trên thẻ đục lỗ (punched card) bắt đầu được dùng trong các học viện lớn. Điều này tuy tạo nhiều thuận lợi với máy tính có khả năng được lập trình nhưng cũng có rất nhiều khó khăn trong việc tạo ra các chương trình dựa trên thẻ đục lỗ này.

Vào cuối thập niên 1950, người ta phát minh ra mạch tích hợp (IC) chứa nhiều transistor trên một mẫu bán dẫn nhỏ, tạo ra một bước nhảy vọt trong việc chế tạo các máy tính mạnh hơn, nhanh hơn và nhỏ hơn. Đến nay, IC có thể chứa hàng triệu transistor trên một mạch.

Vào cuối thập niên 1960, đầu thập niên 1970, các máy tính nhỏ được gọi là minicomputer bắt đầu xuất hiện.

Năm 1977, công ty máy tính Apple Computer giới thiệu máy vi tính cũng được gọi là máy tính cá nhân (personal computer - PC).

Năm 1981, IBM đưa ra máy tính cá nhân đầu tiên. Sự thu nhỏ ngày càng tinh vi hơn của các IC đưa đến việc sử dụng rộng rãi máy tính cá nhân tại nhà và trong kinh doanh.

Vào giữa thập niên 1980, người sử dụng dùng các máy tính độc lập bắt đầu chia sẻ các tập tin bằng cách dùng modem kết nối với các máy tính khác. Cách thức này được gọi là điểm nối điểm, hay truyền theo kiểu quay số. Khái niệm này được mở rộng bằng cách dùng các máy tính là trung tâm truyền tin trong một kết nối quay số. Các máy tính này được gọi là sàn thông báo (bulletin board). Các người dùng kết nối đến sàn thông báo này, để lại đó hay lấy đi các thông điệp,

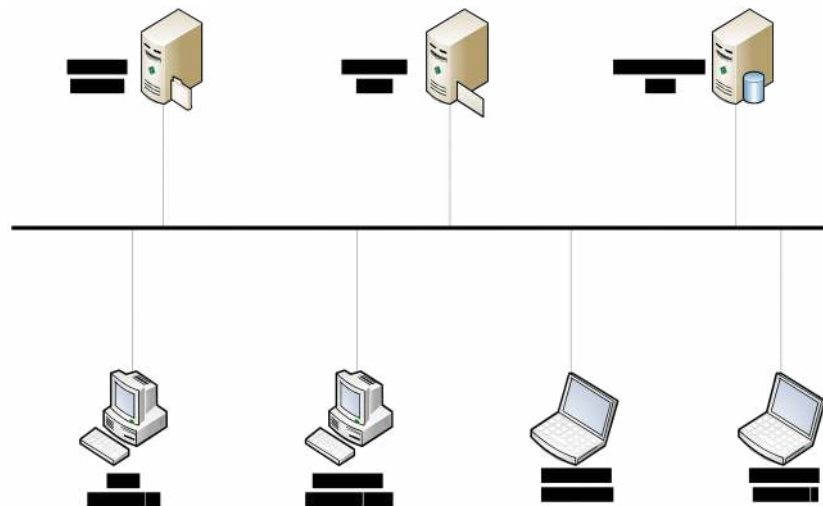
cũng như gửi lên hay tải về các tập tin. Hạn chế của hệ thống là có rất ít hướng truyền tin, và chỉ với những ai biết về sà thông báo đó. Ngoài ra, các máy tính tại sà thông báo cần một modem cho mỗi kết nối, khi số lượng kết nối tăng lên, hệ thống không thể đáp ứng được nhu cầu.

Qua các thập niên 1950, 1970, 1980 và 1990, Bộ Quốc phòng Hoa Kỳ đã phát triển các mạng diện rộng WAN có độ tin cậy cao, nhằm phục vụ các mục đích quân sự và khoa học. Công nghệ này khác truyền tin điểm nối điểm. Nó cho phép nhiều máy tính kết nối lại với nhau bằng các đường dẫn khác nhau. Bản thân mạng sẽ xác định dữ liệu di chuyển từ máy tính này đến máy tính khác như thế nào. Thay vì chỉ có thể thông tin với một máy tính tại một thời điểm, nó có thể thông tin với nhiều máy tính cùng lúc bằng cùng một kết nối. Sau này, WAN của Bộ Quốc phòng Hoa Kỳ đã trở thành Internet.

### 1.1.2 Định nghĩa mạng máy tính

Mạng máy tính là một tập hợp các máy tính được nối với nhau bởi môi trường truyền (đường truyền) theo một cấu trúc nào đó và thông qua đó các máy tính trao đổi thông tin qua lại cho nhau.

Môi trường truyền: là hệ thống các thiết bị truyền dẫn có dây hay không dây dùng để chuyển các tín hiệu điện tử từ máy tính này đến máy tính khác. Các tín hiệu điện tử đó biểu thị các giá trị dữ liệu dưới dạng các xung nhị phân (on -off).



Hình 1.1. Một mô hình liên kết các máy tính trong mạng

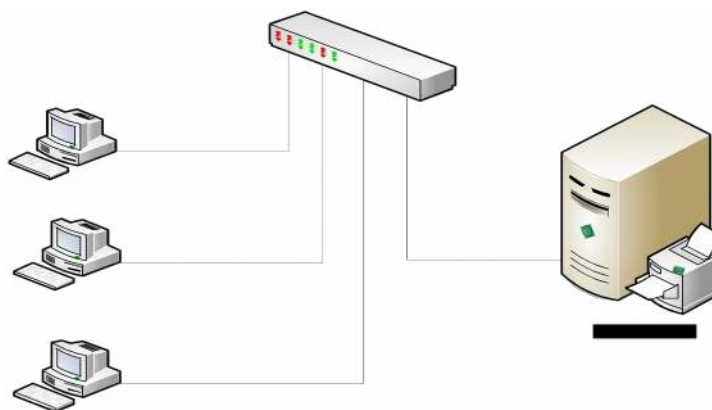
### 1.1.3 Ứng dụng của mạng máy tính

Ngày nay nhu cầu xử lý thông tin ngày càng cao. Mạng máy tính ngày càng trở nên quá quen thuộc đối với mọi người thuộc mọi tầng lớp khác nhau, trong mọi lĩnh vực như: khoa học, quân sự quốc phòng, thương mại, dịch vụ, giáo dục...

Hiện nay ở nhiều nơi mạng đã trở thành một nhu cầu không thể thiếu. Người ta thấy được việc kết nối các máy tính thành mạng cho chúng ta những khả năng mới to lớn như:

a. Dùng chung tài nguyên:

Những tài nguyên của mạng (như thiết bị, chương trình, dữ liệu) khi được trở thành các tài nguyên chung thì mọi thành viên của mạng đều có thể tiếp cận được mà không quan tâm tới những tài nguyên đó ở đâu.



Hình 1.2. Mô hình mạng dùng chung tài nguyên

b. Tăng độ tin cậy của hệ thống:

Người ta có thể dễ dàng bảo trì máy móc và lưu trữ (backup) các dữ liệu chung và khi có trục trặc trong hệ thống thì chúng có thể được khôi phục nhanh chóng. Trong trường hợp có trục trặc trên một trạm làm việc thì người ta cũng có thể sử dụng những trạm khác thay thế.

c. Nâng cao chất lượng và hiệu quả khai thác thông tin:

Khi thông tin có thể được sử dụng chung thì nó mang lại cho người dùng khả năng tổ chức lại các công việc với những thay đổi về chất như:

- Đáp ứng nhu cầu của hệ thống ứng dụng kinh doanh hiện đại.
- Cung cấp sự thống nhất giữa các dữ liệu.

- Tăng cường năng lực xử lý nhờ kết hợp các bộ phận phân tán.
- Tăng cường truy nhập tới các dịch vụ mạng khác nhau đang được cung cấp trên thế giới.
- Hiện nay việc làm sao có được một hệ thống mạng chạy tốt, an toàn với lợi ích kinh tế cao đang rất được quan tâm.

Vấn đề đặt ra có rất nhiều giải pháp về công nghệ, một giải pháp có rất nhiều yếu tố cấu thành, trong mỗi yếu tố có nhiều cách lựa chọn. Như vậy để đưa ra một giải pháp hoàn chỉnh, phù hợp phải trải qua một quá trình chọn lọc dựa trên những ưu điểm của từng yếu tố, từng chi tiết rất nhỏ.

Để giải quyết một vấn đề phải dựa trên những yêu cầu đặt ra và trên công nghệ để giải quyết. Nhưng công nghệ cao nhất chưa chắc là công nghệ tốt nhất, mà công nghệ tốt nhất là công nghệ phù hợp nhất.

## **1.2 THÀNH PHẦN CƠ BẢN TRONG MẠNG MÁY TÍNH**

### **1.2.1 Tổng quát mạng máy tính cơ bản.**

- Có ít nhất 2 máy tính.
- Một giao tiếp mạng trên mỗi máy (NIC: Network interface Card)
- Môi trường truyền: Dây cáp mạng, môi trường truyền không dây.
- Hệ điều hành mạng: UNIX, Windows 98, Windows NT,..., Novell Netware.

### **1.2.2 Kiến trúc (Cấu trúc) mạng cục bộ**

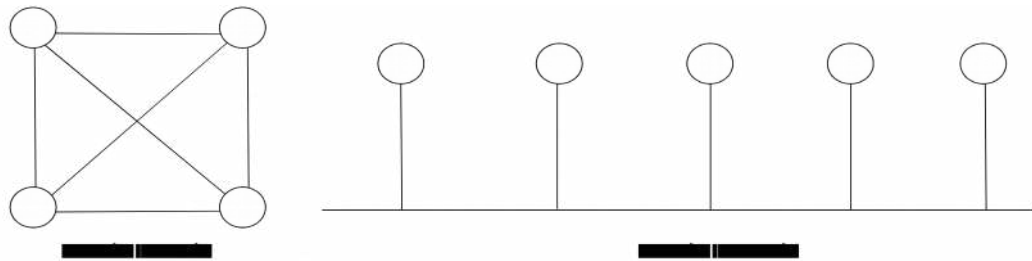
#### **1.2.2.1 Cấu trúc của mạng (Topology) *chữ nghiêng***

Hình trạng của mạng cục bộ thể hiện qua cấu trúc hay hình dáng hình học của các đường dây cáp mạng dùng để liên kết các máy tính thuộc mạng với nhau. Trước hết chúng ta xem xét hai phương thức nối mạng chủ yếu:

Với phương thức “một điểm – một điểm” các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Mỗi máy tính có thể truyền và nhận trực tiếp dữ liệu hoặc có thể làm trung gian như lưu trữ những dữ liệu mà nó nhận

được rồi sau đó chuyển tiếp dữ liệu đi cho một máy khác để dữ liệu đó đạt tới đích.

Theo phương thức “một điểm – nhiều điểm ” tất cả các trạm phân chia chung một đường truyền vật lý. Dữ liệu được gửi đi từ một máy tính sẽ có thể được tiếp nhận bởi tất cả các máy tính còn lại, bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để mỗi máy tính căn cứ vào đó kiểm tra xem dữ liệu có phải dành cho mình không nếu đúng thì nhận còn nếu không thì bỏ qua.



Hình 1.3. Các phương thức liên kết mạng

Tùy theo cấu trúc của mỗi mạng chúng sẽ thuộc vào một trong hai phương thức nối mạng và mỗi phương thức nối mạng sẽ có những yêu cầu khác nhau về phần cứng và phần mềm.

#### 1.2.2.2 Các giao thức truy cập đường truyền trên mạng LAN *chữ nghiêng*

Để truyền được dữ liệu trên mạng người ta phải có các thủ tục nhằm hướng dẫn các máy tính của mạng làm thế nào và lúc nào có thể thâm nhập vào đường dây cáp để gửi các gói dữ liệu. Ví dụ như đối với các dạng bus và ring thì chỉ có một đường truyền duy nhất nối các trạm với nhau, cho nên cần phải có các quy tắc chung cho tất cả các trạm nối vào mạng để đảm bảo rằng đường truyền được truy nhập và sử dụng một cách hợp lý.

Có nhiều giao thức khác nhau để truy nhập đường truyền vật lý nhưng phân thành hai loại: các giao thức truy nhập ngẫu nhiên và các giao thức truy nhập có điều khiển

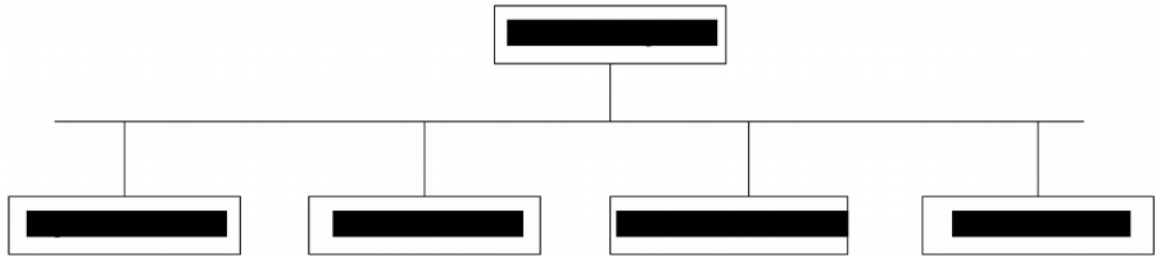
- Giao thức chuyển mạch (yêu cầu và chấp nhận)
- Giao thức đường dây đa truy cập với cảm nhận va chạm (Carrier Sense Multiple Access with Collision Detection hay CSMA/CD )

- Giao thức dùng thẻ bài vòng (Token ring)
- Giao thức dùng thẻ bài cho dạng đường thẳng (Token bus)

### 1.3 KIẾN TRÚC VÀ MÔ HÌNH QUẢN TRỊ MẠNG

#### 1.3.1 Kiến trúc và mô hình quản trị mạng OSI

Mô hình OSI là mô hình mạng mà ta xem mỗi nút mạng là một hệ thống mở có 7 lớp chức năng. Các hệ thống này được kết nối với nhau bằng môi trường vật lý để nối trực tiếp các lớp thấp nhất (lớp vật lý).



Hình 1.4. Mô hình quản trị mạng OSI

##### 1.3.1.1 Mô hình tổ chức (Organization Model)

Trong mô hình này gồm 3 thành phần: Manager, Agent và Managed Object (MO).

- Manager: Là nơi chịu trách nhiệm về tất cả các hoạt động quản trị.
- Agent: Đại diện cho các đối tượng giao tiếp với manager, phục vụ cho MO quan hệ với Manager.

+ Đối với MO, Agent đóng vai trò thu thập trạng thái của đối tượng, chuyển trạng thái thành thông tin mô tả trạng thái và lưu trữ lại. Đồng thời nó phát hiện thay đổi bất thường trên MO; Điều khiển các MO.

+ Đối với Manager, Agent sẽ nhận các lệnh điều khiển và chuyển thành điều khiển đối tượng. Ngược lại các tác động điều khiển chuyển các thông tin trạng thái về Manager khi có yêu cầu, gửi các hành vi của MO với mỗi một phép toán quản trị về Manager, chuyển thông báo (event report) về MO khi có những thay đổi bất thường của MO. Nó điều khiển trực tiếp các MO.

- Mỗi manager quản trị nhiều đối tượng, khi muốn thực hiện một phép toán quản trị, manager sẽ tạo một liên kết giữa một manager với một Agent.

- Xét theo quan hệ với manager: Agent sẽ nhận các điều khiển từ manager và chuyển nó thành các tác động điều khiển để điều khiển đối tượng. Vì vậy nó phải chuyển được các thông tin trạng thái về manager theo đúng yêu cầu rồi giữ các hành vi của các MO (với mỗi phép toán quản trị) về người quản trị. Đồng thời nó cũng chuyển các thông báo về các đối tượng được quản trị khi có thay đổi bất thường ở phía người quản trị.

- Mỗi Agent có thể có vài đối tượng (ít dùng). Khi một manager muốn quản lý một đối tượng thì nó quản lý trực tiếp Agent của đối tượng đó.

- Khi một manager hay Agent muốn trao đổi thông tin với nhau thì chúng cần phải biết về nhau.

#### **1.3.1.2 Mô hình thông tin (Information Model) *chữ nghiêng***

- Là các lớp do người quản trị mô tả tài nguyên của hệ thống.

- Mô tả các tài nguyên của hệ thống:

+ Thực thể gồm: thuộc tính, các phép toán có thể tác động và các hành vi của nó.

+ Các thông tin của người quản trị phải được lưu trữ theo một cấu trúc nào đó.

+ Mô hình cấu trúc lưu trữ hình thức.

- Các thông tin quản trị sẽ được trao đổi giữa các Manager/Agent bởi các giao thức quản trị.

- Mô tả đối tượng được quản trị:

+ Được mô tả bằng một lớp đối tượng, mỗi lớp đối tượng sẽ có các thuộc tính của đối tượng, đó là các trạng thái khác của đối tượng được quản trị. Những thuộc tính có đặc điểm chung thì sẽ nhóm lại thành thuộc tính nhóm. Các thuộc tính của một lớp đối tượng gộp chung lại thành gói.

+ Mỗi đối tượng sẽ có thông tin chính là các trạng thái khi có thay đổi

+ Các thao tác quản trị mà đối tượng có thể chấp nhận, gộp chung lại tạo thành thông tin về phép toán.

+ Các thao tác của đối tượng: Chuỗi các trạng thái theo chuỗi các tác động.

- Cả 4 thông tin gói chung lại tạo ra gói thông tin, mỗi một đối tượng của hệ thống có một vị trí.

- Chức năng quản trị các tri thức quản trị: khi tri thức trở thành một đối tượng quản trị, nó phải được mô tả bằng các thông tin nào đó.

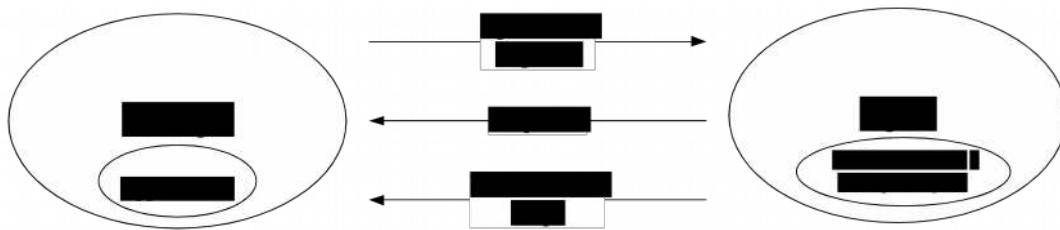
Mỗi tri thức quản trị được mô tả bởi một lớp đối tượng.

Các nhóm tri thức quản trị gồm:

- Tri thức liên quan đến thực thể
- Tri thức định nghĩa

Các nhóm tri thức này cho phép đặc trưng hóa từng lớp đối tượng được quản trị liên quan đến lưu trữ thông tin

### 1.3.1.3 Mô hình truyền thông (Communication Model) *chữ nghiêng*



Hình 1.5. Mô hình truyền thông OSI

- Để thực hiện một cuộc truyền thông qua một môi trường phải thực hiện bốn dịch vụ:

- + Người yêu cầu gửi yêu cầu cho môi trường.
- + Môi trường gửi yêu cầu tới người trả lời.
- + Người trả lời gửi trả lời tới môi trường.
- + Môi trường truyền trả lời (chấp nhận hoặc không chấp nhận) của người trả lời tới người yêu cầu bốn dịch vụ nguyên thủy. (primitive)

Nếu ta sử dụng cả bốn dịch vụ nguyên thủy thì phương thức này là truyền tin cậy, có xác nhận.

Ngược lại nếu không sử dụng thì truyền không tin cậy, không xác nhận.

Cả hai phương thức đều được sử dụng trong mạng tùy trường hợp cụ thể.

Trong một cuộc truyền thông thường có nhiều bước, ví dụ như: thiết lập, uy



trì, hủy bỏ cuộc truyền. Mỗi bước sẽ có nhiều điều khiển khác nhau được thực hiện thông qua các dịch vụ nguyên thủy.

Để phân biệt các cuộc truyền thông cần bổ sung các thông số tin cậy để xác định cuộc truyền thông xảy ra ở lớp nào, nhằm mục đích gì.

Mỗi yêu cầu truyền thông trong môi trường OSI có 3 thành tố:

- + Chữ viết tắt tiếng Anh đầu tiên của tên lớp để chỉ ra lớp nào
- + Để phân biệt các thành tố, sau chữ viết tắt dùng dấu gạch giữa (-).
- + Động từ chỉ công việc cần thực hiện, viết bằng chữ in hoa.

Ví dụ: GET lấy thông tin từ đâu đó.

- + Tên dịch vụ nguyên thủy viết sau một dấu "." có thể viết tắt, viết ăng chữ thường.

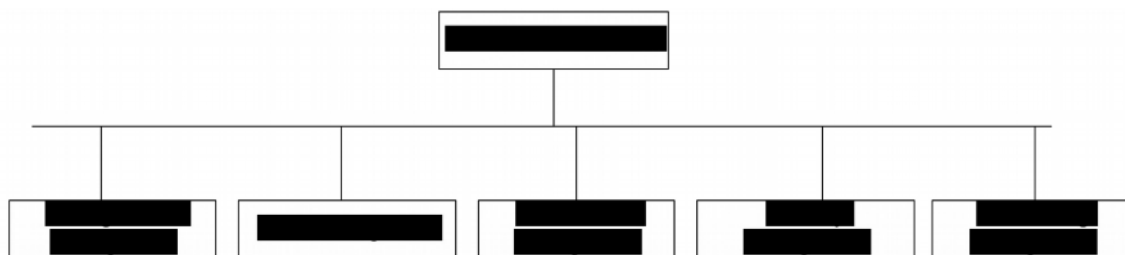
Ví dụ: A - ASSOCIATE.request hoặc A-ASSOCIATE.req

Để thực hiện một cuộc truyền thông, hai lớp mạng đóng vai trò chủ thể truyền thông, khởi phát, chấp nhận, thực hiện cuộc truyền. Trên thực tế, chỉ một phần truyền thông của lớp mạng tham gia cuộc truyền thông. Một lớp mạng chia thành nhiều phần tử khác nhau trong đó có những phần tử thực hiện công việc truyền thông.

Với quản trị mạng, lớp ứng dụng cho phép triển khai các ứng dụng quản trị mạng và các ứng dụng này được thực hiện thông qua phần tử truyền thông phục vụ cho việc quản trị mạng ở lớp ứng dụng. Ta gọi các phần tử này là các phần tử phục vụ cho quản trị mạng ở lớp ứng dụng.

- Mỗi ứng dụng quản trị mạng được thực hiện thông qua cặp thực thể SAME.

#### 1.3.1.4 Mô hình chức năng (Functional Model) *chữ nghiêng*



Hình 1.6. Mô hình chức năng OSI

Mô hình chức năng trong OSI bao gồm:

- Quản trị cấu hình (Configuration Management):

+ Xác định cấu hình hiện có của hệ thống: dùng các phép toán thu thập thông tin.

+ Có thể thiết lập cấu hình mới bằng cách thay đổi trạng thái các đối tượng trong hệ thống.

+ Quản trị phần mềm: Bởi vì trong một hệ thống, các phần mềm thường xuyên được nâng cấp nên phải cập nhật phiên bản mới đồng thời và tự động.

- Quản trị lỗi (Fault Management):

+ Phát hiện xác định lỗi, yêu cầu khởi động các chức năng khắc phục lỗi.

+ Phân hóa lỗi thông qua các phép toán thu thập thông tin dự đoán tình trạng có thể xảy ra lỗi.

+ Xác định lỗi có thể là chức năng của quản trị mạng, có thể là chức năng các hệ thống khác.

- Quản trị hiệu năng (Performance Management):

Quản trị hiệu năng thông qua các phép thu nhập thông tin tính toán hiệu năng để đảm bảo hiệu năng yêu cầu. Nó phải phân tích dự đoán được vùng quá tải, các vùng chưa dùng hết hiệu năng để điều khiển cân bằng tải và tránh tắc nghẽn hệ thống.

- Quản trị an ninh (Security Management):

Nhằm phát hiện, đánh giá sự mất an toàn an ninh của hệ thống, khởi động các giải pháp an toàn an ninh.

- Quản trị kế toán (Accounting Management):

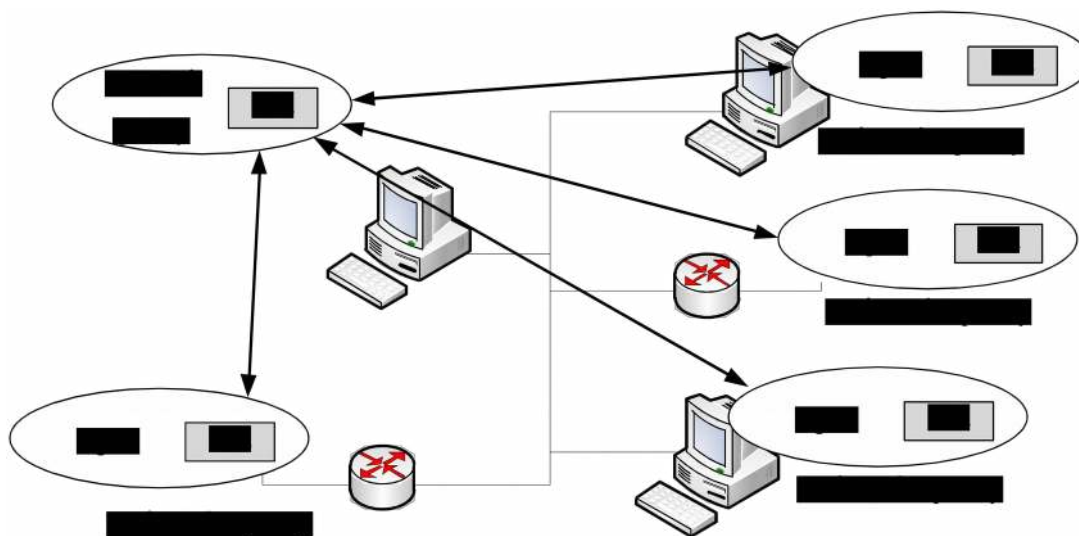
Gồm quản trị liên quan đến tính toán việc sử dụng các tài nguyên từng cá nhân, từng đơn vị trong hệ thống và cho phép hay không cho phép từng cá nhân, đơn vị sử dụng hay không sử dụng hệ thống.

### 1.3.2 Kiến trúc và mô hình quản trị mạng SNMP

#### 1.3.2.1 Giới thiệu *chữ nghiêng*

Cốt lõi của SNMP là một tập hợp đơn giản các hoạt động giúp nhà quản trị mạng có thể quản lý, thay đổi trạng thái của mạng. Ví dụ chúng ta có thể dùng SNMP để tắt một giao diện nào đó trên router của mình, theo dõi hoạt động của card Ethernet, hoặc kiểm soát nhiệt độ trên switch và cảnh báo khi nhiệt độ quá cao.

SNMP thường tích hợp vào trong router, nhưng khác với SGMP(Simple Gateway Management Protocol) nó được dùng chủ yếu cho các router Internet. SNMP cũng có thể dùng để quản lý các hệ thống Unix, Window, máy in, nguồn điện... Nói chung, tất cả các thiết bị có thể chạy các phần mềm cho phép lấy được thông tin SNMP đều có thể quản lý được. Không chỉ các thiết bị vật lý mới quản lý được mà cả những phần mềm như web server, database cũng có thể được quản lý.



Hình 1.7. Mô hình quản trị mạng SMNP

Một hướng khác của quản trị mạng là theo dõi hoạt động mạng, có nghĩa là theo dõi toàn bộ một mạng trái với theo dõi các router, host, hay các thiết bị riêng lẻ. RMON (Remote Network Monitoring) có thể giúp ta hiểu làm sao một mạng có thể tự hoạt động, làm sao các thiết bị riêng lẻ trong một mạng có thể hoạt động

đồng bộ trong mạng đó. IETF (Internet Engineering Task Force) là tổ chức đã đưa ra chuẩn SNMP thông qua các RFC.

- SNMP version 1 chuẩn của giao thức SNMP được định nghĩa trong RFC 1157 và là một chuẩn đầy đủ của IETF. Vấn đề bảo mật của SNMP v1 dựa trên nguyên tắc cộng đồng, không có nhiều password, chuỗi văn bản thuần và cho phép bất kỳ một ứng dụng nào đó dựa trên SNMP có thể hiểu các hiệu các chuỗi này để có thể truy cập vào các thiết bị quản lý. Có 3 thao tác chính trong SNMPv1 là: readonly, read-write và trap.

- SNMP version 2: Phiên bản này dựa trên các chuỗi "community"; Do đó phiên bản này được gọi là SNMPv2c, được định nghĩa trong RFC 1905, 1906, 1907, và đây chỉ là bản thử nghiệm của IETF. Mặc dù chỉ là thử nghiệm nhưng nhiều nhà sản xuất đã đưa nó vào thực nghiệm.

- SNMP version 3: Là phiên bản tiếp theo được IETF đưa ra bản đầy đủ. Nó được khuyến nghị làm bản chuẩn, được định nghĩa trong RFC 1905, RFC 1906, RFC 1907, RFC 2571, RFC 2572, RFC 2573, RFC 2574 và RFC 2575. Nó hỗ trợ các loại truyền thông riêng tư và có xác nhận giữa các thực thể.

Trong SNMP có 3 vấn đề cần quan tâm: Manager, Agent và MIB (Management Information Base). MIB là cơ sở dữ liệu dùng phục vụ cho Manager và Agent.

- + Manager là một server có chạy các chương trình có thể thực hiện một số chức năng quản lý mạng. Manager có thể xem như là NMS (Network Manager Stations). NMS có khả năng thăm dò và thu thập các cảnh báo từ các Agent trong mạng. Thăm dò trong việc quản lý mạng là đặt ra các câu truy vấn đến các Agent để có được một phần nào đó của thông tin. Các cảnh báo của Agent là cách mà Agent báo với NMS khi có sự cố xảy ra. Cảnh báo của Agent được gửi một cách không đồng bộ, không nằm trong việc trả lời truy vấn của NMS. NMS dựa trên các thông tin trả lời của Agent để có các phương án giúp mạng hoạt động hiệu quả hơn. Ví dụ khi đường dây T1 kết nối tới Internet bị giảm băng thông nghiêm trọng, router sẽ gửi một thông tin cảnh báo tới NMS. NMS sẽ có một số hành động, ít

nhất là lưu lại giúp ta có thể biết việc gì đã xảy ra. Các hành động này của NMS phải được cài đặt trước.

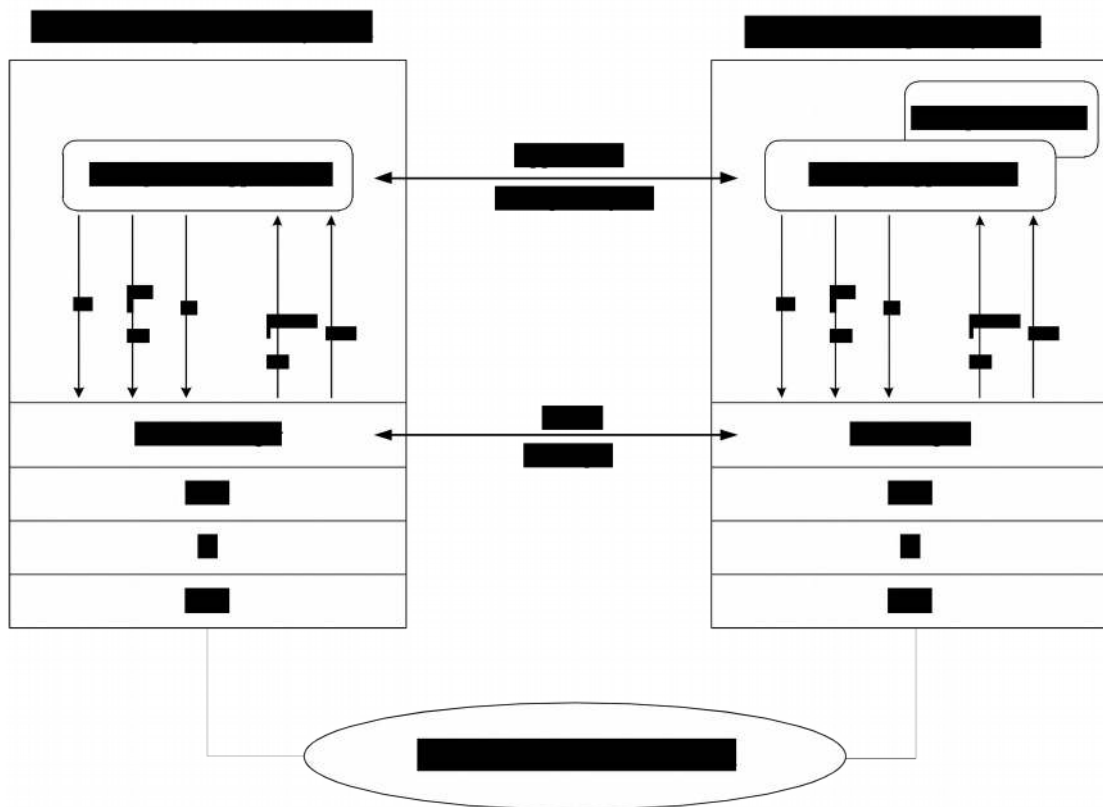
+ Agent là một phần trong các chương trình chạy trên các thiết bị mạng cần quản lý. Nó có thể là một chương trình độc lập như các daemon trong Unix, hoặc được tích hợp vào hệ điều hành như IOS của Cisco trên router. Ngày nay, đa số các thiết bị hoạt động tới lớp IP được cài đặt SMNP agent. Các nhà sản xuất ngày càng muốn phát triển các Agent trong các sản phẩm của họ để công việc của người quản lý hệ thống hay người quản trị mạng đơn giản hơn. Các Agent cung cấp thông tin cho NMS bằng cách lưu trữ các hoạt động khác nhau của thiết bị. Một số thiết bị thường gửi thông báo "tất cả đều bình thường" khi nó chuyển từ một trạng thái xấu sang một trạng thái tốt. Điều này giúp xác định khi nào một tình trạng có vấn đề được giải quyết.

+ MIB có thể xem như là một cơ sở dữ liệu của các đối tượng quản lý mà Agent lưu trữ được. Bất kỳ thông tin nào mà NMS có thể truy cập được đều được định nghĩa trong MIB. Một Agent có thể có nhiều MIB nhưng tất cả các Agent đều có một loại MIB gọi là MIB-II, được định nghĩa trong RFC 1213. MIB-I là bản gốc của MIB nhưng ít dùng khi MIB-II được đưa ra. Bất kỳ thiết bị nào được hỗ trợ SNMP đều phải có hỗ trợ MIB-II. MIB-II định nghĩa các tham số như tình trạng của giao diện (tốc độ của giao diện, MTU, các octet gửi, các octet nhận. ...) hoặc các tham số gắn liền với hệ thống (định vị hệ thống, thông tin liên lạc với hệ thống, ...). Mục đích chính của MIB-II là cung cấp các thông tin quản lý theo TCP/IP. Có nhiều kiểu MIB giúp quản lý cho các mục đích khác nhau:

- ATM MIB (RFC 2515)
- Frame Relay DTE Interface Type MIB (RFC 2115)
- BGP Version 4 MIB (RFC 1657)
- RDBMS MIB (RFC 1697)
- RADIUS Authentication Server MIB (RFC 2619)
- Mail Monitoring MIB (RFC 2249)
- DNS Server MIB (RFC 1611)

Quản lý Host Resource cũng là một phần quan trọng của quản lý mạng. Trước đây, sự khác nhau giữa quản lý hệ thống kiểu cũ và quản lý mạng không được xác định, nhưng hiện nay nó đã được phân biệt rõ ràng. RFC 2790 đưa ra Host Resource với định nghĩa tập hợp các đối tượng cần quản lý trong hệ thống Unix và Window; Các đối tượng đó là: Dung lượng đĩa, số user của hệ thống, số tiến trình đang chạy của hệ thống và các phần mềm đã cài vào hệ thống. Trong một thế giới thương mại điện tử, các dịch vụ như web ngày càng trở nên phổ biến, nên việc đảm bảo cho các server hoạt động tốt là việc hết sức quan trọng.

### 1.3.2.2 Hoạt động của SNMP *chữ nghiêng*



Hình 1.8. Mô Hình hoạt động của SNMP

- **get**: được gửi từ NMS yêu cầu tới Agent. Agent nhận yêu cầu và xử lý với khả năng tốt nhất có thể. Nếu một thiết bị nào đó đang bận tải nặng, như router, nó không có khả năng trả lời yêu cầu nên nó sẽ hủy lời yêu cầu này. Nếu agent tập hợp đủ thông tin cần thiết cho yêu cầu, nó gửi lại cho NMS một "get-response":

Để Agent hiểu được NMS cần tìm thông tin gì, nó dựa vào một mục trong "get" là "variable binding" hay varbind. Varbind là một danh sách các đối tượng của MIB mà NMS muốn lấy từ Agent. Agent hiểu câu hỏi theo dạng: OID=value để tìm thông tin trả lời.

Câu lệnh "get" hữu ích trong việc truy vấn một đối tượng riêng lẻ trong MIB. Khi muốn biết thông tin về nhiều đối tượng thì "get" tốn khá nhiều thời gian. Câu lệnh "get-next" giải quyết được vấn đề này.

- **get-next**: đưa ra một dãy các lệnh để lấy thông tin từ một nhóm trong MIB. Agent sẽ lần lượt trả lời tất cả các đối tượng có trong câu truy vấn của "get-next" tương tự như "get", cho đến khi nào hết các đối tượng trong dãy. Ví dụ ta dùng lệnh "snmpwalk". "snmpwalk" tương tự như "snmpget" nhưng không chỉ tới một đối tượng mà chỉ tới một nhánh nào đó

- **get-bulk** (cho SNMP v2 và SNMP v3): được định nghĩa trong SNMPv2. Nó cho phép lấy thông tin quản lý từ nhiều phần trong bảng. Dùng "get" có thể làm được điều này. Tuy nhiên, kích thước của câu hỏi có thể bị giới hạn bởi Agent. Khi đó nếu nó không thể trả lời toàn bộ yêu cầu, nó gửi trả một thông điệp lỗi mà không có dữ liệu. Với trường hợp dùng câu lệnh "get-bulk", Agent sẽ gửi càng nhiều trả lời nếu nó có thể. Do đó, việc trả lời một phần của yêu cầu là có thể xảy ra. Hai trường hợp cần khai báo trong "get-bulk" là: "nonrepeaters" và "max-repetitions".

"nonrepeaters" báo cho Agent biết số đối tượng đầu tiên có thể trả lời lại như một câu lệnh "get" đơn.

"max-repetitions" báo cho Agent biết cần cố gắng tăng lên tối đa các yêu cầu .

"getnext" cho các đối tượng còn lại:

- **set**: để thay đổi giá trị của một đối tượng hoặc thêm một hàng mới vào bảng. Đối tượng này cần phải được định nghĩa trong MIB là "read-write" hay "writeonly".



NMS có thể dùng "set" để đặt giá trị cho nhiều đối tượng cùng một lúc: Có thể cài đặt nhiều đối tượng cùng lúc, tuy nhiên nếu có một hành động bị lỗi, toàn bộ sẽ bị hủy bỏ.

- **get-response:** Error Response của "get", "get-next", "get-bulk" và "set" - Có nhiều loại lỗi báo lại từ Agent.

- **trap** (cảnh báo): là cảnh báo của Agent tự động gửi cho NMS để NMS biết có tình trạng xấu ở agent.

Khi nhận được một "trap" từ Agent, NMS không trả lời lại bằng "ACK"; Do đó Agent không thể nào biết được là lời cảnh báo của nó có tới được NMS hay không.

Khi nhận được một "trap" từ agent, nó tìm xem "trap number" để hiểu ý nghĩa của "trap" đó.

- **notification** (cho SNMP v2 và SNMP v3): Nhằm chuẩn hóa định dạng PDU "trap" của SNMPv1 - Do PDU của "get" và "set" khác nhau, SNMPv2 đưa ra "NOTIFICATION-TYPE". Định dạng PDU của "NOTIFICATION-TYPE" là để nhận ra "get" và "set". "NOTIFICATION-TYPE" được định nghĩa trong RFC 2863.

- **inform** (cho SNMP v2 và SNMP v3): SNMPv2 cung cấp cơ chế truyền thông giữa những NMS với nhau, gọi là SNMP inform. Khi một NMS gửi một SNMP inform cho một NMS khác, NMS nhận được sẽ gửi trả một ACK xác nhận sự kiện. Việc này giống với cơ chế của "get" và "set".

- **report** (cho SNMP v2 và SNMP v3): được định nghĩa trong bản nháp của SNMPv2 nhưng không được phát triển. Sau đó được đưa vào SNMPv3 và hy vọng dùng để truyền thông giữa các hệ thống SNMP với nhau.

### 1.3.3 Kiến trúc quản trị tích hợp OMP

OMP (Open Management Platform) đã xác định mục tiêu thị trường và sử dụng các chiến lược hoàn toàn khác nhau để tích hợp. Hệ thống được cài đặt dựa trên hệ thống quản trị hệ kế thừa. Các nhà cung cấp OMP đã nhanh chóng tìm



kiểm thị trường cho các chuẩn dựa trên LANs, tương tự mạng LAN, máy chủ/khách và những hệ thống máy tính mới được thiết kế cho nhiều môi trường.

+ Phương pháp OMP để tích hợp Quản trị Mạng

Các hệ thống mạng đã đạt chuẩn bởi chuẩn đầu tiên trong giao thức quản trị mạng, cấu trúc thông tin quản trị, và một nhóm các thông tin quản trị. Sau đó, họ phát triển các sản phẩm dựa trên những chuẩn này. Tiếp theo những sản phẩm được phát triển giành cho quản trị mạng này đã được dùng trong nhiều năm. Mạng Internet đã có chuẩn trong giao thức quản trị mạng (SNMP - Simple Network Management Protocol), được kết hợp với SMI để định nghĩa thông tin quản trị.

Trong lĩnh vực truyền thông nó đã được chuẩn hóa bởi CMIS / CMIP (Common Management Information Service/Protocol) kết hợp với SMI để định nghĩa thông tin quản trị. Mạng truyền thông hiện nay đang được chuyển đổi sang sử dụng các nguyên tắc và tiêu chuẩn TMN (Telecommunications Management Network).

Quản trị mạng OMPs ngày nay chủ yếu sử dụng SNMP để lấy các thông tin quản trị trực tiếp từ các tài nguyên mạng. Quản trị mạng OMPs được dựa trên hệ điều hành UNIX hoặc Windows NT. Các tính năng chính của quản trị mạng OMPs là giao diện chương trình ứng dụng (API - Application Programming Interface), nó cho phép các nhà cung cấp tích hợp các modul phần mềm hoặc định nghĩa dữ liệu quản trị phức tạp (được gọi là thông tin quản trị cơ sở hoặc MIBs) trên máy chủ OMP. Các phương pháp OMP đã tạo thị trường cung cấp phần mềm độc lập để tạo ra các ứng dụng quản trị mạng và các công cụ quản trị có thể chạy trên các hệ điều hành. Ngoài ra, các nhà cung cấp hệ thống mạng còn đưa ra các công cụ quản trị dựa trên hệ điều hành cho các sản phẩm của họ. (Ví dụ như Cisco hoặc BayNetworks Optivity) Do vậy nó loại trừ được sự nhất thiết phải sở hữu riêng một máy trạm EMS - Khả năng thêm vào nhiều loại modul phần mềm khác nhau trong hệ điều hành quản trị mạng OMPs.

Bởi chúng có giao thức truy cập đến các phần tử mạng, quản trị mạng OMPs, nên nó có thể thực hiện nhiều chức năng hơn MOMs. Ngày nay quản trị mạng

OMPs cung cấp nhiều cảnh báo và giám sát hơn; Hệ thống này thường tự động cung cấp thông tin cấu hình mạng, hiệu quả hoạt động giám sát, và phân tích giao thức.

Hầu hết quản trị mạng OMPs không tập trung vào tự động cung cấp các phản hồi để đưa ra lỗi, nhưng chúng cung cấp lọc cơ bản và củng cố thông tin cảnh báo. Quản trị mạng OMP tập trung về việc tự động tìm ra cấu hình và thông tin tóm tắt. Lợi ích của OMP trong quản trị tên miền đã được giới hạn. Hiện tại hệ điều hành quản trị mạng cung cấp giới hạn về chức năng tự động tìm ra các thiết bị quản trị, tìm kiếm MIBs cho từng thiết bị và quản lý sự kiện; Tuy vậy, chúng không yêu cầu nhà cung cấp phải độc lập giám sát các phần tử quản trị mạng, hoặc hệ thống đầu - cuối của quản trị mạng. Ngoài ra các nhà cung cấp thiết bị có thể yêu cầu mở rộng các MIBs để quản trị các thiết bị và giúp cho nhà cung cấp không phụ thuộc vào các ứng dụng chạy trên hệ điều hành để quản trị các sản phẩm cụ thể của họ.

### + Phương pháp OMP để tích hợp hệ thống và quản trị ứng dụng

Như đã nêu trên, những hệ thống quản trị mạng và ứng dụng của chúng đã được tham gia theo nhiều hướng khác nhau để tạo ra một giải pháp OMP. Các chuẩn phát triển trong cùng hệ thống quản trị mạng đã không được chấp nhận trong các hệ thống và ứng dụng của người dùng, chủ yếu là bởi các yêu cầu là khác nhau và các chuẩn bị phụ thuộc vào các công cụ quản trị mạng, như: sự chấp nhận của các phần tử quản trị, các chuẩn hướng đối tượng mới cho phát triển ứng dụng và thao tác giữa các đối tượng đã được phát triển, ví dụ: Hệ thống và các ứng dụng quản trị mạng, mức độ lớn hơn để quản trị mạng, các yêu cầu để tạo ra và thường xuyên thay đổi của hàng trăm hoặc thậm chí hàng nghìn các tài khoản người sử dụng, phân phối phần mềm và cập nhật đến hàng nghìn các máy vi tính, đồng bộ hóa tài dữ liệu, và lên kế hoạch thực hiện sao lưu của hàng nghìn máy tính. Trách nhiệm để quản trị các hệ thống và các ứng dụng được phân tán rộng rãi, trong khi quản trị mạng thường là tập trung, bởi vì mạng sẽ trở thành một nguồn tài nguyên chung. Do đó, những công cụ cần thiết để phân vùng trách

nhiệm quản trị và thi hành các chính sách quản trị cần phải được thực hiện phân tán nhiều hơn.

Kiến trúc hướng đối tượng phân tán càng thể hiện rõ hơn, ví dụ như: Common Object Request Broker Architecture (CORBA) là một mô hình cho tích hợp. Ngoài ra, còn có Microsoft Object Model (DCOM) đang trở thành một chuẩn trong lĩnh vực quản trị mạng.

Trong thị trường máy tính, nơi hệ điều hành mạng (NOSs) của Microsoft và Novell thống trị, các hệ thống quản trị mạng của họ cũng chiếm cao hơn. Các sản phẩm này bao gồm khả năng in, tập tin và các dịch vụ quản trị, người quản trị, an ninh, kiểm tra thiết bị tự động, và các phần mềm cho hệ điều hành MS Windows 3.x, 95, NT, IBM OS / 2, Macintosh OS desktops.

Với hệ điều hành UNIX, các nhà cung cấp đề xuất các sản phẩm quản trị của riêng họ, hiện nay nhà cung cấp hàng đầu về tích hợp quản trị trong hệ thống UNIX là IBM / Tivoli và CA Unicenter. Các sản phẩm này bao gồm khả năng in, tập tin và các dịch vụ quản trị, người quản trị, an ninh, kiểm tra thiết bị tự động, quản trị workload, và phân tán phần mềm. Ngoài ra, họ cung cấp cho khách hàng các giải pháp trợ giúp cho các vấn đề về ticketing và dịch vụ quản trị mạng, hoặc là của chính bản thân họ hoặc thông qua các giải pháp của bên thứ ba.

Các tính năng chính của hệ thống và ứng dụng quản trị OMPs là giao diện chương trình trình ứng dụng (API - Application Programming Interface), nó cho phép các nhà cung cấp phần mềm có thể tích hợp các phân hệ quản trị dữ liệu phức tạp hoặc các định nghĩa vào OMP máy chủ. Các phương pháp OMP đã tạo ra thị trường cung cấp phần mềm độc lập, đó là việc tạo ra một loạt các hệ thống, các ứng dụng và các công cụ quản trị các ứng dụng có thể chạy trên các hệ điều hành. Ngoài ra, còn phải kể đến các hệ thống và ứng dụng quản trị cung cấp cho hệ điều hành dựa trên công cụ quản trị cho các sản phẩm của họ, cũng như khả năng thêm vào nhiều modul phần mềm khác nhau cho hệ điều hành cơ bản, cho các hệ thống và ứng dụng quản trị OMPs hàng loạt các tính năng để có thể thay thế MOMs.

Lợi ích của OMP trong các hệ thống và các ứng dụng quản trị tên miền là ở chỗ nó có khả năng làm tăng thêm những lợi ích thực sự trong quản trị tên miền. Ngoài ra, các ứng dụng quản trị tên miền có thể quản trị các nguồn tài nguyên từ nhiều nhà cung cấp bằng cách lập bản đồ cho sự thực hiện quản trị khác nhau vào một mô hình thông tin chung. Do các mô hình thông tin chung hiện nay là không chuẩn, vì vậy các lợi ích được thực hiện bằng cách chỉ nắm giữ mô hình thông tin chung có ảnh hưởng lớn đến các lợi ích. Như việc các hệ thống và ứng dụng quản trị chuẩn đang được phát triển cho phép một số yếu tố độc quyền sẽ biến mất, ví dụ như, mô hình thông tin quản trị Common Information Model (CIM) đang được phát triển bởi Desktop Management Task Force (DMTF).

### 1.3.4 Chức năng của hệ thống quản trị mạng

Quản trị mạng là quá trình điều khiển mạng dữ liệu phức tạp để tăng tính hiệu quả và hiệu năng của mạng. Theo mô hình OSI, quản trị mạng gồm 5 chức năng:

- Quản trị sự cố (Fault Management): phát hiện, cô lập và khắc phục sự cố.
- Quản trị kế toán (Accounting Management): kiểm soát tài nguyên trong mạng.
- Quản trị cấu hình (Configuraion Management): thu thập thông tin hệ thống, cảnh báo các thay đổi của hệ thống và thay đổi cấu hình.
- Quản trị hiệu năng (Performance Management): thu thập, thống kê thông tin để đánh giá hiệu năng của hệ thống theo điều kiện thực tế và giả định khác nhau.
- Quản trị an toàn (Security Management): bảo vệ hệ thống, ngăn chặn các hoạt động trái phép, bảo mật thông tin truyền trên mạng.

## CHƯƠNG 2:

### GIỚI THIỆU VỀ HỆ ĐIỀU HÀNH UBUNTU SERVER

#### 1.4 TỔNG QUAN VỀ UBUNTU

##### 1.4.1 Lịch sử và khái niệm cơ bản

##### 1.4.1.1 Khái niệm *chữ nghiêng*

Ubuntu là một cộng đồng phát triển 1 hệ điều hành mã nguồn mở hoàn hảo cho PC, Laptop và thậm chí cả Server. Cho dù bạn có ở nhà, ở trường học hay ở văn phòng làm việc thì Ubuntu cũng luôn là một hệ điều hành thỏa mãn tất cả mọi yêu cầu của bạn, từ trình xử lý văn bản, trình duyệt internet, gửi email đến các phần mềm ứng dụng máy chủ web hay công cụ lập trình.

Ubuntu được phổ biến hoàn toàn miễn phí, bạn ko phải trả bất kỳ một khoản phí nào để sử dụng. Bạn có thể download, sử dụng, chia sẻ với bạn bè, người thân, sử dụng trong nhà trường, công sở hay cá nhân mà không cần phải lo lắng về chi phí mua bản quyền phần mềm.

Ubuntu phát hành phiên bản mới 6 tháng một lần cho cả môi trường desktop và server. Điều đó có nghĩa là bạn luôn có trong tay những chương trình ứng dụng mới nhất và tốt nhất của thế giới phần mềm mã nguồn mở.

Vấn đề bảo mật và an ninh cũng được bảo đảm với việc phát hành tối thiểu 18 tháng một phiên bản cập nhật về bảo mật. Đối với các phiên bản hỗ trợ dài hạn bạn sẽ được cập nhật và hỗ trợ tối đa trong vòng 3 năm với phiên bản cho desktop và 5 năm với phiên bản cho server., Điều quan trọng nữa là tất cả đều hoàn toàn miễn phí.

Tất cả những thứ bạn cần được gói gọn trong 1 chiếc CD, từ hệ điều hành cho tới các phần mềm ứng dụng sẽ giúp cho bạn có một môi trường làm việc hoàn thiện.

Thời gian cài đặt nhanh cũng là một ưu thế của Ubuntu, với phiên bản phổ thông bạn chỉ mất chừng 25 phút để hoàn thành quá trình này. Khả năng hỗ trợ ngôn ngữ đa dạng cũng là một ưu thế ko thể ko nói đến của Ubuntu.

#### 1.4.1.2 Lịch sử phát triển của Ubuntu *chữ nghiêng*

Bản phát hành đầu tiên của Ubuntu là vào 20 tháng 10 năm 2004, bắt đầu bằng việc tạo ra một nhánh tạm thời của dự án Debian Linux. Việc này đã được thực hiện để một phiên bản mới của Ubuntu có thể được phát hành mỗi 6 tháng, tạo ra một hệ điều hành được cập nhật thường xuyên hơn. Bản phát hành Ubuntu luôn gồm bản GNOME mới nhất, và được lên lịch phát hành khoảng 1 tháng sau GNOME. Khác với các nhánh có mục đích chung trước của Debian - như MEPIS, Xandros, Linspire, Progeny và Libranet, phần nhiều trong số chúng dựa vào các phần mềm bổ sung có mã đóng mô hình của một doanh nghiệp. Ubuntu lại giống với triết lý của Debian hơn và dùng các phần mềm miễn phí (libre) vào mọi thời điểm.

Các gói của Ubuntu nói chung dựa trên các gói từ nhánh không ổn định của Debian: cả 2 bản phân phối đều dùng gói có định dạng deb của Debian và APT/Synaptic để quản lý các gói đã cài. Ubuntu đã đóng góp trực tiếp và lập tức tất cả thay đổi đến Debian, chứ không chỉ tuyên bố chúng lúc phát hành, mặc dù các gói của Debian và Ubuntu không cần thiết "tương thích nhị phân" với nhau. Nhiều nhà phát triển Ubuntu cũng là người duy trì các gói khoá (gói chủ chốt) của chính Debian. Dù sao, Ian Murdock, nhà sáng lập của Debian, đã chỉ trích Ubuntu vì sự không tương thích giữa các gói của Ubuntu và Debian, ông nói rằng Ubuntu đã làm sai lệch quá xa so với Debian Sarge, do đó không còn giữ được sự tương thích.

Bảng 2.1. Danh sách các phiên bản Ubuntu đã phát hành (*In lại*)

Phiên bản	Tên mã	Ngày phát hành
4.04	Warty Warthog	20/10/2004
5.04	Hoary Hedgehog	08/04/2005
5.10	Breezy Badger	13/10/2005
6.06 LTS	Dapper Drake	01/06/2006
6.10	Edgy Eft	26/10/2006
7.04	Feisty Fawn	19/04/2007

7.10	Gutsy Gibbon	18/10/2007
8.04	Hardy Heron	21/04/2008
8.10	Intrepid Ibex	24/10/2008
9.04	Jaunty Jackalope	23/04/2009
9.10	Karmic Koala	29/10/2009
10.04	Lucid Lynx	29/04/2010
10.10	Maverick Meerkat	10/10/2010
11.04	Natty Narwhal	28/04/2011
11.10	Oneiric Ocelot	13/10/2011
12.04	Precise Pangolin	26/04/2012

#### 1.4.2 Tìm hiểu các lệnh cơ bản trong Ubuntu Server

Hầu hết các hệ điều hành, bao gồm cả Ubuntu, có 2 dạng giao diện người sử dụng. Cái đầu là một giao diện đồ họa cho người sử dụng (GUI). Đây là trường đồ họa, các cửa sổ, thực đơn, và các thanh công cụ mà bạn nhấp vào để thực hiện mọi thứ. Cái thứ 2, và là dạng giao diện cổ hơn nhiều, là giao diện dòng lệnh (CLI). Terminal là giao diện dòng lệnh của Ubuntu. Đây là một phương pháp kiểm soát một số khía cạnh của Ubuntu chỉ sử dụng các lệnh mà bạn gõ vào từ bàn phím.

Bạn có thể mở giao diện dòng lệnh bằng việc nhấp vào:

Applications >> Accessories >> Terminal.

Khi cửa sổ của giao diện dòng lệnh mở, nó sẽ là chủ yếu là trắng ngoài một vài văn bản ở đỉnh bên trái của màn hình, được đi theo bởi một khối nhấp nháy. Văn bản này là dấu nhắc của bạn - nó hiển thị tên đăng nhập và tên máy tính của bạn, theo sau thư mục hiện hành. Dấu ngã (~) có nghĩa là thư mục hiện hành là thư mục home của bạn. Cuối cùng, khối nhấp nháy là một con trỏ, nó đánh dấu nơi mà văn bản sẽ được đưa vào khi bạn gõ. Để thử mọi thứ, hãy gõ pwd và nhấn phím Enter. Giao diện dòng lệnh sẽ hiển thị /home/ubuntu-manual. Văn bản này được gọi là “output” (“đầu ra”). Bạn vừa mới sử dụng lệnh pwd (in thư mục làm việc), và đầu ra mà nó đã hiển thị chỉ ra thư mục hiện hành. Giao diện dòng lệnh trao cho bạn sự truy cập tới những gì gọi là vỏ (shell). Khi bạn gõ một lệnh vào giao diện



dòng lệnh thì vô dịch lệnh đó, đưa kết quả thành hành động mong muốn. Có những dạng vô khác nhau mà chúng chấp nhận những lệnh hơi khác nhau. Vô phổ biến nhất gọi là “bash”, và là vô mặc định trong Ubuntu. Trong các môi trường GUI thì khái niệm “folder - thư mục” thường được sử dụng để mô tả một nơi mà ở đó các tệp được lưu giữ. Trong các môi trường CLI thì khái niệm “directory - thumục” được sử dụng để mô tả cùng thứ đó và phép ẩn dụ này được thể hiện trong nhiều lệnh(như `cd` hoặc `pwd`) trong khắp chương này.

**Dưới đây là những lệnh cơ bản:**

➤ **Di chuyển / liệt kê các tập tin**

- `pwd` :hiển lên tên thư mục đang làm việc với `cd` di chuyển sang thư mục «`/home/người_dùng`»
- `cd ~/Desktop` :di chuyển sang thư mục « `/home/người_dùng/Desktop` »
- `cd ..` :di chuyển sang thư mục cha (ngay trên thư mục hiện hành)
- `cd /usr/apt` :di chuyển sang thư mục « `/usr/apt` »
- `ls -l` Thumục và `dir -l` Thumục :liệt kê danh mục tập tin trong thư mục *Thumục* một cách chi tiết
- `ls -a` và `dir -a` :liệt kê tất cả các tập tin, kể cả các tập tin ẩn (thường có tên bắt đầu bằng một dấu chấm)
- `ls -d` và `dir -d` :liệt kê tên các thư mục nằm trong thư mục hiện hành
- `ls -t` và `dir -d` :xếp lại các tập tin theo ngày đã tạo ra, bắt đầu bằng những tập tin mới nhất
- `ls -S` và `dir -S` :xếp lại các tập tin theo kích thước, từ to nhất đến nhỏ nhất
- `ls -l | more` :liệt kê theo từng trang một, nhờ tiện ích « more »

➤ **Quyền truy cập tập tin**



- `chown tênngườidùng file` : xác định người chủ của tập tin *file* là người dùng mang tên « *tênngườidùng* »
- `chown -R tênngườidùng thưmục` :xác định người chủ của thư mục *thurmục*, kể cả các thư mục con (-R) là người dùng « *tênngườidùng* »
- `chgrp` nhóm file :chuyển tập tin *file* thành sở hữu của nhóm người dùng mang tên *nhóm*
- `chmod u+x file` :giao (+) quyền thực hiện (x) tập tin *file* cho người dùng (u)
- `chmod g-w file` :rút (-) quyền ghi (w) *file* của nhóm (g)
- `chmod o-r file` :rút (-) quyền đọc (r) tập tin *file* của những người dùng khác (o)
- `chmod a+rw file` :giao (+) quyền đọc (r) và ghi (w) *file* cho mọi người (a)
- `chmod -R a+rx thưmục` :giao (+) quyền đọc (r) và vào bên trong thư mục (x) *thurmục*, kể cả tất cả các thư mục con của nó (-R), cho tất cả mọi người (a)

➤ **Quản lý các tập tin**

- `cp file1 file2` :chép *file1* sang *file2*
- `cp file /thurmục` :chép *file* vào thư mục « *thurmục* »
- `cp -r thưmục1 thưmục2` và `rsync -a thưmục1 thưmục2` :chép toàn bộ nội dung của thư mục « *thurmục1* » sang thư mục « *thurmục2* »
- `mv file1 file2` :chuyển tên tập tin *file1* thành tên *file2*
- `mv thưmục1 thưmục2` :chuyển tên *thurmục1* thành *thurmục2*
- `mv file thưmục` :chuyển tập tin *file* vào thư mục *thurmục*

- *mv file1 thưmục/file2* :chuyển *file1* vào thư mục *thurmục* đồng thời đổi tên tập tin thành *file2*
- *mkdir thưmục* :tạo ra thư mục *thurmục*
- *mkdir -p thưmục1/thurmục2* :tạo ra thư mục cha *thurmục1* và thư mục con *thurmục2* cùng lúc
- *rm file* :xóa bỏ tập tin *file* trong thư mục hiện hành
- *rmdir thưmục* :xóa bỏ thư mục trống mang tên *thurmục*
- *rm -rf thưmục* :xóa bỏ thư mục mang tên *thurmục* với tất cả các tập tin trong đó (*force*)
- *ln -s file liênkết* :tạo ra một liên kết mang tên *liênkết* đến tập tin *file* (nổi bật)
- *find thưmục -name file* :tìm tập tin mang tên *file* trong thư mục *thurmục* kể cả trong các thư mục con
- *diff file1 file2* :so sánh nội dung của 2 tập tin hoặc của 2 thư mục

➤ **Quản trị hệ thống**

- *sudo command* :thực hiện lệnh *command* với tư cách người siêu dùng (root)
- *gksudo command* :giống với *sudo* nhưng dùng cho các ứng dụng đồ họa
- *sudo -k* :chấm dứt chế độ dùng lệnh có chức năng của người siêu dùng
- *uname -r* :cho biết phiên bản của nhân Linux
- *shutdown -h now* :khởi động lại máy tính ngay lập tức

- *time command* :cho biết thời gian cần thiết để thực hiện xong lệnh
- *command1 | command2* :chuyển kết quả của lệnh *command1* làm đầu vào của lệnh *command2*
- *clear* :xoá màn hình của cửa sổ « Thiết bị cuối » (terminal)
- *ps -ef* :hiện thị tất cả các tiến trình đã được thực hiện (*pid* et *ppid*)
- *ps aux* :hiện thị chi tiết các tiến trình
- *ps aux | grep soft* :hiện thị các tiến trình liên quan đến chương khởi động *soft*
- *kill pid* :báo chấm dứt tiến trình mang số *pid*
- *kill -9 pid* :yêu cầu hệ thống chấm dứt tiến trình *pid*
- *xkill* :chấm dứt một ứng dụng theo dạng đồ hoạ (ấn chuột vào cửa sổ của ứng dụng)

### ➤ **Mạng máy tính**

- */etc/network/interfaces* :thông tin cấu hình của các bộ phận giao diện (interfaces)
- *uname -a* :hiện thị tên của máy tính trong mạng (hostname)
- *ping địa chỉIP* :thử nối mạng đến máy có địa chỉ IP
- *ifconfig -a* :hiển thị thông tin về tất cả các giao diện mạng đang có
- *ifconfig eth0 địa chỉIP* :xác định địa chỉ IP cho giao diện các mạng *eth0*

- *ifdown eth0* và *ifconfig eth0 down* :ngưng hoạt động giao diện cục mạng *eth0*
- *poweroff -i* :ngưng hoạt động tất cả các nối mạng
- *route add default gw địa chỉ IP* :xác định địa chỉ IP của máy làm cổng dẫn đến bên ngoài mạng cục bộ
- *route del default* :bỏ địa chỉ IP mặc định để ra khỏi mạng cục bộ

### 1.4.3 Môi trường đồ họa của Ubuntu Server

#### ➤ Việc hiểu về môi trường đồ họa

Lần đầu xem qua, bạn sẽ để ý nhiều sự giống nhau giữa Ubuntu và các hệ điều hành khác như Windows hoặc Mac OS X. Điều này là vì chúng tất cả đều dựa vào khái niệm của một giao diện đồ họa cho người sử dụng (GUI) - nghĩa là, bạn sử dụng chuột của bạn để di chuyển trong môi trường đồ họa, mở các chương trình, di chuyển các tệp, và thực hiện hầu hết các nhiệm vụ khác. Nói ngắn gọn, mọi thứ rất hướng trực giác, mà nó có nghĩa là điều quan trọng đối với bạn để trở nên quen thuộc với những nơi và những gì phải nhấp trong Ubuntu.

#### ➤ GNOME

Tất cả các hệ điều hành dựa trên GUI đều sử dụng một môi trường đồ họa. Các môi trường đồ họa nhân mạnh nhiều thứ, như là việc nhìn và cảm nhận hệ thống của bạn, cũng như cách mà môi trường đồ họa được tổ chức, được trải ra, và được dịch chuyển bởi người sử dụng. Trong các phát tán Linux (như Ubuntu), có một số các môi trường đồ họa sẵn sàng để sử dụng. Một trong những môi trường đồ họa phổ biến nhất được gọi là GNOME, mà nó được sử dụng một cách mặc định trong Ubuntu. KDE, XFCE, và LXDE là các môi trường đồ họa phổ biến khác.

#### ➤ Việc quản lý các cửa sổ

Khi bạn mở một chương trình trong Ubuntu thì một cửa sổ sẽ xuất hiện trong môi trường đồ họa của bạn. Nếu bạn đã sử dụng hệ điều hành khác trước đó, như

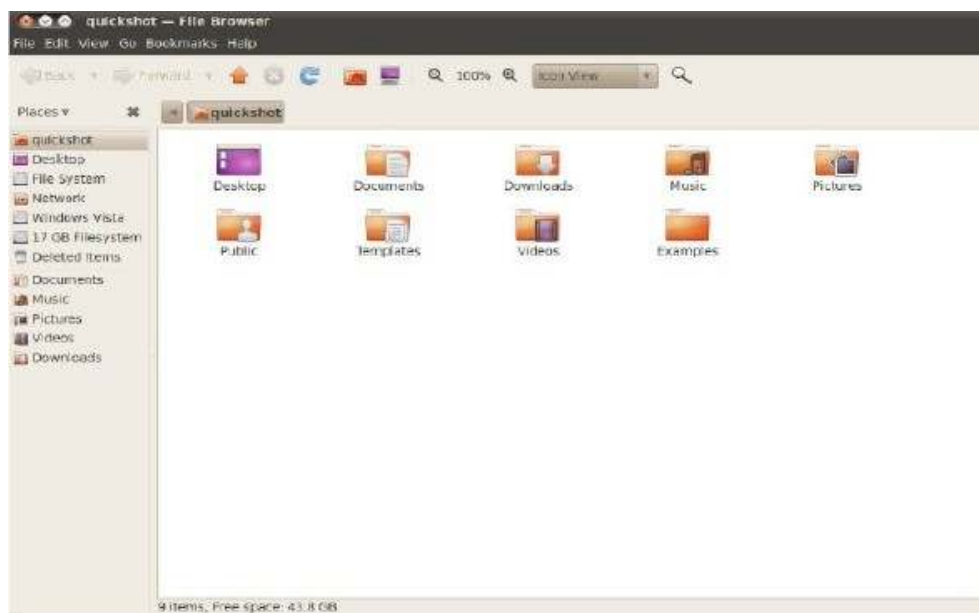
Microsoft Windows hoặc Mac OS X, thì bạn có lẽ đã quen với khái niệm một “cửa sổ” - một cái hộp mà nó xuất hiện trên màn hình của bạn khi bạn khởi động một chương trình. Trong Ubuntu, phần đỉnh của một cửa sổ (thanh tiêu đề) sẽ có tiêu đề của cửa sổ ở giữa, và 3 nút ở đỉnh bên góc trái. Từ trái qua phải, các nút đó là đóng, đóng nhỏ hết cỡ, và mở to hết cỡ cửa sổ. Thêm nữa, bạn có thể nhấp phải vào bất cứ đâu trên thanh tiêu đề để có một danh sách các lựa chọn quản lý cửa sổ khác.



Hình 2.1: Các nút đóng, đóng nhỏ hết cỡ và mở to hết cỡ là trên đỉnh góc bên trái của các cửa sổ

### ➤ Việc sao chép và di chuyển các tệp và thư mục

Bạn có thể sao chép các tệp hoặc thư mục trong Nautilus bằng cách nhấp Edit>Copy, hoặc bằng nhấp phải lên khoản đó và chọn Copy từ thực đơn popup. Khi sử dụng thực đơn Edit trong Nautilus, hãy chắc chắn bạn đã chọn tệp hoặc thư mục mà bạn muốn sao chép trước (bằng việc nhấp trái lên nó một lần). Bạn cũng có thể sử dụng các phím tắt của bàn phím Ctrl+C và Ctrl+V để sao chép và dán các tệp và thư mục.



### Hình 2.2: Trình quản lý tệp Nautilus hiển thị thư mục home

Có thể chọn nhiều tệp một lúc bằng cách nhấp trái vào một chỗ trống (nghĩa là không vào một tệp hoặc thư mục nào), giữ nút chuột xuống, và rê con trỏ qua các tệp và thư mục mà bạn muốn. Động tác “nhấp – rê” này là hữu ích khi bạn chọn các khoản mà sẽ được nhóm chặt chẽ cùng với nhau. Để chọn nhiều tệp hoặc thư mục mà không nằm sát cùng nhau, hãy giữ phím Ctrl trong khi nhấp lên mỗi khoản một cách riêng rẽ. Một khi nhiều tệp và/hoặc thư mục được chọn thì bạn có thể sử dụng thực đơn Edit để thực hiện các hành động chỉ như bạn làm với duy nhất một khoản vậy. Khi một hoặc nhiều khoản đã được “sao chép”, hãy di chuyển tới vị trí mong muốn rồi nhấp Edit ► Paste (hoặc nhấp phải vào một chỗ trống của cửa sổ và chọn Paste [Dán]) để sao chép chúng tới vị trí mới. Trong khi lệnh sao chép có thể được sử dụng để sao chép một tệp hoặc thư mục trong một vị trí mới, thì lệnh cắt có thể được sử dụng để di chuyển các tệp và thư mục đi chỗ khác. Nghĩa là, một bản sao sẽ được đặt trong một vị trí mới, và bản gốc sẽ bị loại bỏ khỏi vị trí hiện hành của nó.

#### ➤ Việc bổ sung các chương trình con

Ubuntu cung cấp một sự lựa chọn các chương trình con mà chúng có thể được bổ sung vào bất kỳ panen nào. Các chương trình con trải rộng từ thông tin cho tới vui đùa, và cũng có thể cung cấp sự truy cập nhanh tới một số nhiệm vụ. Để bổ sung một chương trình con, nhấp phải vào một panen rồi chọn Add to Panel (Bổ sung vào panen...) từ thực đơn popup. Một cửa sổ sẽ xuất hiện với một danh sách các chương trình con có sẵn, mà chúng có thể sau đó được rê tới một chỗ trống trên một panen. Bạn có thể muốn bỏ một ít thời gian để khai phá những chương trình con khác nhau có sẵn này - chúng có thể dễ dàng bị loại bỏ khỏi panen của bạn bằng cách nhấp phải lên chương trình con đó và chọn RemoveFrom Panel (loại bỏ khỏi panen).

#### ➤ Nền của môi trường đồ họa

Nhấp vào tab Background trong cửa sổ Appearance Preferences để thay đổi nền của môi trường đồ họa. Ở đây bạn sẽ thấy lựa chọn mặc định đối với các nền

của Ubuntu, tuy nhiên, nếu bạn có những ảnh của riêng bạn được lưu giữ trong máy tính của bạn thì bạn cũng có thể sử dụng chúng. Để thay đổi nền thòdon giản hãy nháy vào ảnh mà bạn muốn sử dụng từ trong danh sách trước mặt bạn. Để sử dụng ảnh của riêng bạn, hãy nháy nút Add ... (bổ sung ...), và di chuyển tới ảnh mà bạn muốn. Nháy đúp vào ảnh, và sự thay đổi sẽ có hiệu lực ngay lập tức.

## 1.5 QUẢN LÝ USER VÀ PHÂN QUYỀN TRONG UBUNTU SERVER

### 1.5.1 Thiết lập tài khoản người dùng

- ✓ User là người có thể truy cập đến hệ thống.
- ✓ User có **username** và **password**.
- ✓ Có hai loại user: **super user** và **regular user**.
- ✓ Mỗi user còn có một định danh riêng gọi là **UID**.
- ✓ Định danh của người dùng bình thường sử dụng giá trị bắt đầu từ 500.

Có 2 cách để thêm một tài khoản mới. Đó là sử dụng lệnh `useradd` hoặc `adduser`. Bạn đăng nhập vào Ubuntu bạn click vào Applications>Accessories>Terminal và thực hiện với dòng lệnh:

#### Cú pháp:

- `useradd [tham số] [username_new]`
  - **Tham số, tham chiếu, các giá trị mặc định và tùy biến**
- `-c` : *comment* :Ý kiến phản hồi. Thực ra nó được dùng như fullname của tài khoản sắp tạo
- `-b` : *BASE\_DIR* :Thư mục cơ sở. Sẽ dùng tham số này để sử dụng các giá trị mặc định cho tài khoản sắp tạo. Nếu các tham số D, m không được sử dụng thì nhất thiết phải sử dụng tham số b
- `-D` : *Defaults* :Các giá trị mặc định. Lưu lại các giá trị sẽ được thay đổi khác với mặc định
- `-d` : *HOME\_DIR* : Nếu các tham số khác không được sử dụng, tham số d sẽ mặc định /home/username\_new là thư mục người dùng mới.
- `-e` : *EXPIRE\_DATE* : Ngày mà tài khoản sắp tạo sẽ bị vô hiệu hóa. Cấu trúc là YYYY-MM-DD

- *-f* : *INACTIVE* : Số ngày mà password của tài khoản mới sẽ bị vô hiệu hóa khi tài khoản hết hạn. Giá trị 0 là disables ngay khi tài khoản hết hạn, giá trị mặc định -1 chỉ disables tính năng
- *-G* : *GROUP* : Nhóm. Một danh sách các nhóm mà bạn biết sẽ được bổ xung sau tham số này, các nhóm cách nhau chỉ bởi dấu “,”
- *-m* : Tham số quan trọng. Sẽ tạo ra thư mục người dùng (~/)nếu nó không có. Các dữ liệu từ thư mục /etc/skel sẽ được sao chép vào ~/ khi sử dụng tham số m
- *-k* : *KEY=VALUE*. Một số khóa nếu bạn thêm vào với các giá trị của nó sẽ được áp dụng cho tài khoản sắp tạo. Tham khảo về các khóa này trong /etc/login.defs .Ví dụ : Số ngày mà password tài khoản mới còn hiệu lực, số user được phép trong một nhóm,...
- *-p* : *PASSWORD*. Mã hóa tài khoản sắp tạo bằng password
- *-s* : *SHELL*: *SHELL* mà người sử dụng sẽ đăng nhập. Trong ubuntu mặc định là /bin/sh. Tuy nhiên tôi thường dùng /bin/bash
- *-u* : *UID*: *User ID* : Trị số này phải là duy nhất, lớn hơn 999 và lớn hơn mọi người dùng khác. Trong ubuntu 1000 là tài khoản của người cài đặt ubuntu. Vậy nên nếu bạn tạo thêm tài khoản mới thì UID của tài khoản mới phải lớn hơn.

➤ **Xóa một tài khoản:**

**Cú pháp:** userdel [tham số][tài khoản cần xóa]

### 1.5.2 Tạo nhóm, tìm hiểu những tập lệnh quản trị nhóm

- ✓ Group là **tập hợp nhiều user** lại.
- ✓ Mỗi user luôn là thành viên của một group.
- ✓ Khi tạo một user thì mặc định một group được tạo ra.
- ✓ Mỗi group còn có một định danh riêng gọi là **GID**.
- ✓ Định danh của group thường sử dụng giá trị bắt đầu từ 500.

➤ **Tạo nhóm:**

**Cú pháp:** #groupadd <groupname>



**Ví dụ: #groupadd serveradmin**

➤ **Xóa nhóm**

**Cú pháp: #groupdel <groupname>**

**Ví dụ: #groupdel <serveradmin>**

➤ **Xem thông tin về User và Group**

**Cú pháp: #id <option> <username>**

**Ví dụ: #id -g quocvan //xem GroupID của user quocvan**

**Cú pháp: #groups <username>**

**Ví dụ: #groups quocvan //xem tên nhóm của user quocvan**

➤ **Những file liên quan đến User và Group**

***#/etc/passwd***

Mỗi dòng trong tập tin gồm có 7 trường, được phân cách bởi dấu hai chấm

***#/etc/group***

Mỗi dòng trong tập tin gồm có 4 trường, được phân cách bởi dấu hai chấm

***#/etc/shadow***

Lưu mật khẩu đã được mã hóa và chỉ có user root mới được quyền đọc.

### 1.5.3 Phân quyền FileSystem

Trong Ubuntu mọi đối tượng đều có dạng là tập tin. Tất cả tập tin đều có người sở hữu và quyền truy cập.

Ta xét ví dụ:

```
[root@fc10 ~]# ls -l /etc/passwd
-rw-r--r-- 1 root root 2150 2010-09-30 03:20 /etc/passwd
[root@fc10 ~]#
```

Các ký tự rw-r--r-- : biểu thị quyền truy cập của tập tin passwd, loại tập tin được chỉ định trong ký tự đầu tiên.

- Ubuntu cho phép người dùng xác định các quyền đọc (read), ghi (write) và thực thi (execute) cho từng đối tượng. Có ba loại đối tượng :
  - + Người sở hữu (owner) : 3 ký tự đầu tiên (rw-)
  - + Nhóm sở hữu (group) : 3 ký tự tiếp theo (r--)

+ Người khác (others) : 3 ký tự cuối cùng (r--)

- **Quyền đọc:** cho phép bạn đọc nội dung của tập tin. Đối với thư mục, quyền đọc cho phép bạn di chuyển vào thư mục bằng lệnh cd hoặc Nautilus và xem nội dung của thư mục.
- **Quyền ghi:** cho phép bạn thay đổi nội dung hay xóa tập tin. Đối với thư mục, quyền ghi cho phép bạn tạo ra, xóa hay thay đổi tên các tập tin, thư mục con trong thư mục cha, nhưng không phụ thuộc vào quyền cụ thể của tập tin trong thư mục. Như vậy, quyền ghi của thư mục sẽ vô hiệu hóa các quyền truy cập của tập tin trong thư mục.
- **Quyền thực thi:** cho phép bạn gọi chương trình lên bộ nhớ cách cách nhập tên tập tin từ bàn phím hay nhấn đôi mouse vào tập tin trong Nautilus. Đối với thư mục, bạn chỉ có thể chuyển vào (cd) thư mục nếu bạn có quyền thực thi với thư mục.

Bảng 2.1. Quyền của các tập tin, thư mục của các đối tượng (in lại)

Owner			Group			Others		
Read	Write	Execute	Read	Write	Execute	Read	Write	Execute

Song song với việc miêu tả bằng các ký tự (**r**, **w**, **e**) ở trên, quyền truy cập còn có thể biểu diễn dưới dạng số nhị phân. Quyền hạn của từng loại người dùng sử dụng một nhóm số hệ nhị phân có 3 bit tương ứng cho quyền read, write, execute. Nếu cấp quyền thì bit đó là 1, ngược lại là 0.

Bảng 2.2 a,,b,c Bieeur thij quyền của các tập tin, thư mục của một đối tượng (in lại)

a.

bít vị trí 2	bít vị trí 1	Bít vị trí 0
Read	Write	Execute

Theo cách tính số nhị phân, ta có thể xác định số quyền hạn của một đối tượng bằng cách tính tổng giá trị các quyền.

Quyền	Giá trị hệ 2	Giá trị hệ 10
Read	100	4

Write	010	2
Execute	001	1
None	000	0

b.

- Tổ hợp của 3 quyền trên có giá trị từ 0 đến 7:

Quyền	Ký hiệu	Giá trị hệ 2	Giá trị hệ 10
Không có quyền	--	000	0
Execute	--x	001	1
Write-only	-w-	010	2
Write và Execute	-wr	011	3
Read-only	r--	100	4
Read và Execute	r-x	101	5
Read và Write	rw-	110	6
Read, write, Execute	rwX	111	7

c.

Như vậy, khi cấp quyền trên tập tin/thư mục, bạn có thể dùng số thập phân gồm 3 con số dễ dàng hơn. Số đầu tiên là quyền sở hữu, số thứ hai là nhóm sở hữu và số thứ ba là những người dùng khác. Xét lại ví dụ trên :

`-rw-r--r-- l root root 2150 2010-09-30 30:20 /etc/passwd`

Trong đó :

- Ba ký tự đầu tiên, đại diện cho chủ sở hữu là root, có quyền là **rw-** → 6
- Ba ký tự kế tiếp, đại diện cho nhóm sở hữu là nhóm root, có quyền là **r--** → 4
- Ba ký tự cuối cùng, đại diện cho những người khác, có quyền là **r--** → 4

Vậy tập tin passwd có quyền là **644**

#### ➤ Gán quyền trên Filesystem:

- **Lệnh chmod:** Cấp quyền hạn cho tập tin/thư mục. Chỉ có chủ sở hữu và

superuser mới có quyền thực hiện lệnh này.

**Cú pháp :** `#chmod [nhóm người dùng] [thao tác] [quyền hạn] [tập tin/thư mục]`

Trong đó:

- *Nhóm người dùng* : u là user ; g là group ; o là others ; a là all.
- *Thao tác* : + là thêm quyền ; - là xóa quyền ; = là gán quyền bằng
- *Quyền* : r là read ; w là write ; x là execute

Ví dụ : myfile.txt

Gán thêm quyền ghi cho group

`#chmod g+w myfile.txt` hoặc `#chmod 775 myfile.txt`

Xóa quyền read trên group và others

`#chmod go-r myfile.txt` hoặc `#chmod 700 myfile.txt`

- **Lệnh chown:** Thay đổi người sở hữu, nhóm sở hữu cho tập tin/thư mục.

**Cú pháp :**

`#chown [tên người sở hữu : nhóm sở hữu] [tập tin/thư mục]`

`#chown -R [tên người sở hữu : nhóm sở hữu] [tập tin/thư mục]`

Trong đó: R (recursive) cho phép thay đổi người sở hữu, nhóm sở hữu của thư mục và tất cả thư mục con bên trong.

Ví dụ : myfile.txt

`#chown hv1 /home/php/myfile.txt`

`#chown hv1:root /home/php/myfile.txt`

- **Lệnh chgrp:** Thay đổi nhóm sở hữu cho tập tin/thư mục.

**Cú pháp :**

`#chgrp [nhóm sở hữu] [tập tin/thư mục]`

Ví dụ : myfile.txt

`#chgrp users /home/php/myfile.txt`

## **1.6 CẤU TRÚC VÀ CÁC DỊCH VỤ TRÊN UBUNTU SERVER**

### **1.6.1 LDAP và SAMBA Server**

#### **1.6.1.1 LDAP (in nghiêng)**

##### **a. Giới thiệu**

LDAP viết tắt Lightweight Directory Access Protocol (tiếng Việt có thể gọi là: giao thức truy cập nhanh các dịch vụ thư mục) là một chuẩn mở rộng cho phương thức truy cập thư mục, hay là một ngôn ngữ để LDAP server và client sử dụng để giao tiếp với nhau.

Các tính chất của LDAP:

- Đây là một giao thức hướng thông điệp.
- Là một giao thức tìm, truy nhập các thông tin dạng thư mục trên server.
- Nó là một giao thức Client/Server dùng để truy cập dịch vụ thư mục, dựa trên dịch vụ thư mục X500.
- LDAP chạy trên TCP/IP hoặc những dịch vụ hướng kết nối khác.
- Là một mô hình thông tin cho phép xác định cấu trúc và đặc điểm của thông tin trong thư mục.
- Là một không gian tên cho phép xác định cách các thông tin được tham chiếu và tổ chức
- Một mô hình các thao tác cho phép xác định các tham chiếu và phân bố dữ liệu
- Là một giao thức mở rộng, được định nghĩa nhiều phương thức mở rộng cho việc truy cập và update thông tin trong thư mục.
- Là một mô hình thông tin mở rộng.
- Vì LDAP tổ chức dữ liệu theo thư mục phân cấp nên có tính mô tả cao, được tối ưu cho việc tìm kiếm.

##### **b. Cấu trúc LDAP**

###### **➤ Cấu trúc cây thư mục trong hệ điều hành Ubuntu**

Một thư mục là danh sách các thông tin về các đối tượng, được sắp xếp một

cách chi tiết về mỗi đối tượng. Trong máy tính, thư mục là một cơ sở dữ liệu đặc biệt để lưu trữ thông tin về các đối tượng. Thư mục thường được đọc nhiều hơn là update và ghi

Hệ thống tập tin của Unix được tổ chức theo một hệ thống phân bậc tương tự cấu trúc của một cây thư mục, bao gồm 1 thân thẳng đứng và các cành lớn chia ra. Bậc cao nhất của hệ thống tập tin là thư mục gốc, được ký hiệu bằng vạch chéo “/” (root directory). Đối với các hệ điều hành Unix và Linux tất cả thiết bị kết nối vào máy tính đều được nhận ra như các tập tin, kể cả những linh kiện như ổ đĩa cứng, các phân vùng đĩa cứng và các ổ USB, chẳng hạn.

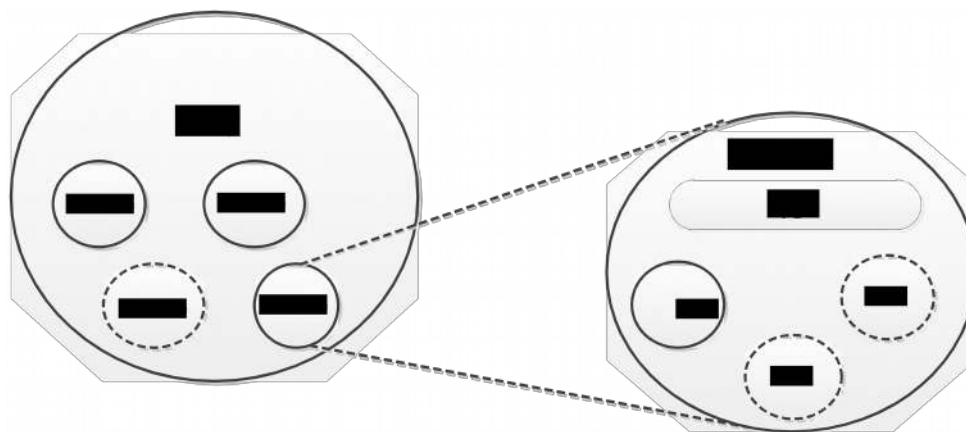
### ➤ Directory Service

Đây là một loại service cụ thể nằm trong client hoặc server. Tuy nhiên một số người thường nhầm lẫn Directory service giống như một database. Tuy giữa hai cái có một số chức năng giống nhau như hỗ trợ tìm kiếm dữ liệu và chứa các file cấu hình hệ thống nhưng Directory service được thiết kế để lấy dữ liệu nhiều hơn là ghi còn Database cung cấp khả năng đọc và ghi dữ liệu liên tục.

### ➤ LDAP Directory

Thành phần cơ bản của LDAP directory là ENTRY, đây là nơi chứa toàn bộ thông tin của một đối tượng. Mỗi entry có một tên đặc trưng gọi là DN (Distinguished Name)

Mỗi entry là tập hợp của các thuộc tính, từng thuộc tính này mô tả một nét đặc trưng tiêu biểu của một đối tượng. Mỗi thuộc tính có kiểu một hay nhiều giá trị, kiểu của thuộc tính mô tả loại thông tin được chứa, giá trị là dữ liệu thực sự.



Hình 2.3. Liên quan giữa Entry và Attribute

### c. Phương thức hoạt động của LDAP

#### ➤ Ldap dùng giao thức giao tiếp client/sever

Giao thức giao tiếp client/sever là một mô hình giao thức giữa một chương trình client chạy trên một máy tính gửi một yêu cầu qua mạng đến cho một máy tính khác đang chạy một chương trình sever (phục vụ).



Hình 2.4. Mô hình kết nối giữa client/server

Client mở một kết nối TCP đến LDAP server và thực hiện một thao tác bind. Thao tác bind bao gồm tên của một directory entry, và thông tin xác thực sẽ được sử dụng trong quá trình xác thực, thông tin xác thực thông thường là password nhưng cũng có thể là ID của người dùng.

#### ➤ LDAP là một giao thức hướng thông điệp

Do client và sever giao tiếp thông qua các thông điệp, Client tạo một thông điệp (LDAP message) chứa yêu cầu và gửi nó đến cho server. Server nhận được thông điệp và xử lý yêu cầu của client sau đó gửi trả cho client cũng bằng một thông điệp LDAP.



Hình 2.5. Thao tác tìm kiếm cơ bản

Nếu client tìm kiếm thư mục và nhiều kết quả được tìm thấy, thì các kết quả này được gửi đến client bằng nhiều thông điệp



Hình 2.6. Những thông điệp Client gửi cho server

Do nghi thức LDAP là giao thức hướng thông điệp nên client được phép phát ra nhiều thông điệp yêu cầu đồng thời cùng một lúc. Trong LDAP, message ID dùng để phân biệt các yêu cầu của client và kết quả trả về của server.





Hình 2.7. Nhiều kết quả tìm kiếm được trả về

Việc cho phép nhiều thông điệp cùng xử lý đồng thời làm cho LDAP linh động hơn các nghi thức khác.

### 1.6.1.2 SAMBA Server

#### a. Giới thiệu

Các hệ thống Linux sử dụng giao thức TCP/IP trong kết nối mạng, trong khi đó hệ điều hành của Microsoft sử dụng một giao thức kết nối mạng khác – giao thức Server Message Block (SMB), giao thức này sử dụng NetBIOS để cho phép các máy tính chạy Windows chia sẻ các tài nguyên với nhau trong mạng cục bộ. Để kết nối tới các mạng lớn, bao gồm cả những hệ thống Unix, Microsoft phát triển Common Internet File System (CIFS), CIFS vẫn sử dụng SMB và NetBIOS cho mạng Windows. Có một phiên bản của SMB được gọi là Samba, Samba cho phép các hệ thống Unix và Linux kết nối tới mạng Windows. Các hệ thống Unix/Linux có thể sử dụng các tài nguyên trên hệ thống Windows, đồng thời nó cũng chia sẻ tài nguyên trên hệ thống cho máy tính Windows.

Gói phần mềm Samba có chứa hai daemon dịch vụ và nhiều chương trình tiện ích. một daemon là `smbd` cung cấp các dịch vụ tập tin và in ấn cho các hệ thống khác có hỗ trợ SMB. Một daemon là `nmdb` cung cấp chức năng phân giải tên NetBIOS và hỗ trợ dịch vụ duyệt thư mục.

Samba cung cấp bốn dịch vụ chính: *dịch vụ chia sẻ tập tin và máy in, xác thực và cấp phép, phân giải tên và thông báo dịch vụ*. Daemon SMB, `smbd`, cung cấp các dịch vụ chia sẻ tập tin và máy in, cũng như xác thực và cấp phép cho những dịch vụ này. Điều này có nghĩa là người dùng trên mạng có thể dùng chung các tập tin và máy in. Người dùng có thể điều khiển truy nhập tới những dịch vụ này bằng cách yêu cầu người dùng phải nhập mật mã truy nhập, Điều khiển truy nhập có thể được thực hiện ở hai chế độ : chế độ dùng chung (share mode) và chế độ người dùng (user mode). Chế độ dùng chung sử dụng một mật mã truy nhập tài nguyên chung cho nhiều người dùng . Chế độ người dùng cung cấp cho mỗi tài khoản người dùng mật mã truy nhập tài nguyên khác nhau. Vì lý do phải quản lý

mật mã truy nhập, Samba có sử dụng tập tin `/etc/samba/smbpassword` để lưu trữ các mật mã truy nhập người dùng.

➤ **Để cấu hình và truy nhập một hệ thống Samba và Linux, người dùng cần thực hiện các thủ tục chính sau:**

- Cấu hình dịch vụ và khởi động dịch vụ Samba.
- Khai báo tài khoản sử dụng Samba.
- Truy nhập dịch vụ Samba.

➤ **Các tập tin cấu hình dịch vụ:**

`/etc/samba/smb.conf`      Tập tin cấu hình của Samba

`/etc/samba/smbpassword`      Chứa mật mã truy nhập của người dùng

`/etc/samba/smbusers`      Chứa tên hiệu cho các tài khoản của Samba

➤ **Các tiện ích của dịch vụ Samba**

`smbadduser`      Tạo tài khoản Samba.

`smbpasswd`      Thay đổi thông tin tài khoản Samba.

`Smbclient`      Truy nhập dịch vụ SMB

`smbstatus`      Theo dõi tình trạng kết nối hiện hành

**b. Cấu hình và khởi động dịch vụ Samba**

Daemon của dịch vụ Samba sử dụng tập tin cấu hình `/etc/samba/smb.conf`. Tập tin này được chia thành hai phần chính: một phần dành cho những lựa chọn toàn cục của dịch vụ và phần còn lại dành cho khai báo tài nguyên được đưa lên mạng dùng chung. Các lựa chọn toàn cục được khai báo ở phần đầu tập tin cấu hình. Trong mỗi phần có chứa một hay nhiều nhóm. Mỗi nhóm (ngoại trừ nhóm [global]) chứa các khai báo về một tài nguyên được chia sẻ. Một nhóm được bắt đầu bởi tên nhóm (`share_name`, được đặt trong cặp dấu ngoặc vuông `[]`), tiếp theo sau là các khai báo tham số của nhóm, mỗi khai báo tham số nằm trên một dòng và có dạng như sau: `name=value` (chú ý là tên của nhóm và tham số không phân biệt chữ thường và chữ hoa), những dòng nào được bắt đầu bởi ký tự `;` hoặc `#` là những dòng ghi chú.

Trong tập tin smb.conf có ba nhóm đặc biệt được khai báo sẵn là [global], [homes] và [printers]

Các tham số xác định các thuộc tính của nhóm. Nhóm [global] có thể chứa mọi tham số. Một số tham số chỉ có thể được khai báo trong nhóm [global]. Một số tham số có thể được sử dụng trong bất kỳ nhóm nào. Và một số tham số chỉ cho phép khai báo trong các nhóm bình thường.

➤ **Nhóm [global]**

Các tham số trong nhóm này được áp dụng một cách toàn cục cho toàn dịch vụ, đồng thời, một số tham số trong nhóm này cũng là các tham số mặc định của các nhóm không khai báo tường minh. Nhóm này phải được đặt tại phần đầu trong tập tin cấu hình /etc/samba/smb.conf.

**Một số tham số cơ bản trong nhóm [global] cần được cấu hình bao gồm:**

- **workgroup**: Chỉ ra tên của nhóm (workgroup) muốn hiển thị trên mạng. Trên Windows, tên này được hiển thị trong cửa sổ Network Neighborhood.
- **host allow**: Chỉ ra những địa chỉ mạng hay địa chỉ máy được truy nhập tới dịch vụ Samba. Các địa chỉ trong danh sách được viết cách nhau một khoảng trắng.
- **encrypt passwords**: Giá trị mặc định là yes. Với tham số này, Samba sẽ thực hiện mã hoá mật mã để tương thích được với cách mã hóa của windows. Trong trường hợp không mã hóa mật mã, người dùng chỉ có thể sử dụng dịch vụ Samba giữa các máy Linux với nhau hoặc người dùng phải cấu hình lại máy tính Windows nếu muốn sử dụng dịch vụ Samba trên Linux.

smb passwd file

Nếu encrypt passwords=yes, tham số này sẽ xác định tập chứa mật mã đã được mã hóa. Mặc định là /etc/samba/smbpasswd

- **username map**: Chỉ ra tập tin chứa các tên hiệu (alias) cho một tài khoản hệ thống. mặc định là /etc/samba/smbusers

- ***printcap file***: Cho phép Samba nạp các mô tả máy in từ tập tin printcap. Giá trị mặc định là /etc/printcap
- ***security***: Khai báo này xác định cách thức các máy tính “trả lời” dịch vụ Samba. Mặc định tham số này có giá trị là user, giá trị cần sử dụng khi kết nối tới các máy tính windows.

Thí dụ về các khai báo trong phần [global] như sau:

```
[global]
#workgroup = ten mien hoac ten nhom
workgroup = SMB-GROUP
# chỉ cho các máy trong mạng cục bộ truy nhập
host allow = 172.16.10. 127.0.0.1
# yêu cầu Samba sử dụng một tập tin nhật ký riêng cho mỗi máy truy nhập
log file = /var/log/samba/%m.log
# chế độ bảo mật
security = user
# mã hóa mật mã để tương thích với Windows
encrypt passwords = yes
smb passwd file = /etc/samba/smbpasswd
# người dùng Unix có thể sử dụng nhiều tên truy nhập SMB.
username map = /etc/samba/smbusers
```

#### ➤ Nhóm [homes]

Nhóm [homes] xác định các điều khiển mặc định cho truy nhập thư mục chủ của người dùng thông qua giao thức SMB bởi người dùng từ xa. Khi có yêu cầu kết nối, Samba sẽ thực hiện kiểm tra các nhóm hiện có, nếu nhóm nào đáp ứng được yêu cầu, nhóm đó sẽ được sử dụng. Nếu không đáp ứng được yêu cầu, tên nhóm được yêu cầu sẽ được coi như tên tài khoản người dùng và tìm kiếm trong tập tin chứa mật mã của Samba. Nếu tên tài khoản này tồn tại ( và đúng mật mã) một tài nguyên sẽ được tạo ra trên nhóm [homes].

Thí dụ về các khai báo trong nhóm [homes] như sau:

```
[homes]
comment = Home Directories
browseable = no
writeable = yes
```

#### ➤ Nhóm [printers]

Tương tự như nhóm [homes] nhưng dành riêng cho máy in. Khi có yêu cầu kết nối. Samba sẽ thực hiện kiểm tra các nhóm hiện có, nếu nhóm nào đáp ứng được yêu cầu, nhóm đó sẽ được sử dụng. Nếu không đáp ứng được yêu cầu, nhưng nhóm [homes] tồn tại nó sẽ được xử lý như mô tả ở trên. Mặt khác, tên nhóm được yêu cầu cũng được xử lý như một tên của máy in và Samba thực hiện tìm kiếm tập tin printcap tương ứng để xác định xem tên nhóm được yêu cầu có hợp lệ không. Nếu hợp lệ, một tài nguyên dùng chung sẽ được dựa trên nhóm [printers].

Thí dụ về các khai báo trong nhóm [printers] như sau:

```
[printers]
comment = All Printers
path = /var/spool/samba
browseable = no
public = yes
printable = yes
```

Ngoài ba nhóm đặc biệt được nêu trên, để thực hiện tạo các nguyên dùng chung khác, người dùng cần thực hiện tạo thêm các nhóm khai báo thông tin về tài nguyên này. Các nhóm dành cho các tài nguyên dùng chung, như là các thư mục trên hệ thống, thường được đặt sau nhóm [homes] và [printers] và có thể đặt tên bất kỳ.

Các tham số thường được khai báo trong các nhóm khai báo tài nguyên dùng chung trong tập tin cấu hình /etc/samba/smb.conf bao gồm:

- **comment**: Mô tả tùy ý cho tài nguyên được đưa lên mạng dùng chung
- **path**: Chỉ ra đường dẫn đến thư mục trên hệ thống tập tin mà tài nguyên dùng chung tham chiếu tới.
- **public**: Có giá trị là yes hoặc no. Nếu là public = yes, Samba cho phép mọi người dùng đều có thể truy nhập tài nguyên dùng chung đó.
- **browseable**: Có giá trị là yes hoặc no. Nếu là browseable = yes, thì thư mục được dùng chung sẽ được nhìn thấy ở trên mạng. Giá trị mặc định là yes

- **valid users**: Danh sách những người dùng được quyền truy nhập tài nguyên dùng chung. Tên người dùng được cách nhau bởi khoảng trắng hoặc ký tự ‘,’. Tên nhóm được đứng trước bởi ký tự ‘@’
- **invalid users**: Danh sách những người dùng không được quyền truy nhập tài nguyên dùng chung. Tên người dùng được cách nhau bởi khoảng trắng hoặc ký tự ‘,’. Tên nhóm được đứng trước bởi ký tự ‘@’
- **writable**: Có giá trị là yes hoặc no. Nếu là writable = yes người dùng được phép ghi vào thư mục dùng chung
- **write list**: Xác định danh sách người dùng/nhóm có quyền ghi tới thư mục dùng chung. Trong trường hợp chỉ ra tên nhóm, trước tên nhóm phải là một ký tự ‘@’.
- **printable**: Có giá trị là yes hoặc no. Nếu là printable=yes người dùng được phép truy nhập đến dịch vụ in.
- **create mask**: Thiết lập quyền trên thư mục/tập tin được tạo trong thư mục được dùng chung. Giá trị mặc định là 0744

## 1.6.2 DNS Server và Mail Server

### 1.6.2.1 DNS Server (in nghiêng)

#### a. Giới thiệu

Dịch vụ tên miền (DNS – Domain Name Service) là một dịch vụ internet, nó ánh xạ địa chỉ IP sang tên miền của các máy chủ có thực (FQDN – Full Qualified Domain Names – tên miền đầy đủ đã được chứng nhận) và ngược lại.

Khi mở một trình duyệt Web và nhập tên website, trình duyệt sẽ đến thẳng website mà không cần phải thông qua việc nhập địa chỉ IP của trang web. Quá trình "dịch" tên miền thành địa chỉ IP để cho trình duyệt hiểu và truy cập được vào website là công việc của một DNS server. Các DNS trợ giúp qua lại với nhau để dịch địa chỉ "IP" thành "tên" và ngược lại. Người sử dụng chỉ cần nhớ "tên", không cần phải nhớ địa chỉ IP (địa chỉ IP là những con số rất khó nhớ).

#### b. Phân loại domain name server

*Tên miền riêng (Primary Name Server):* Mỗi một máy chủ tên miền có một tên miền riêng. Tên miền riêng này được đăng ký trên Internet.

*Tên miền dự phòng – tên miền thứ hai (Secondary name server):* đây là một DNS Server được sử dụng để thay thế cho Primary name server DNS Server bằng cách sao lưu lại tất cả những bản ghi dữ liệu trên Primary name Server và nếu Primary Name Server bị gián đoạn thì nó sẽ đảm nhận việc phân giải và ánh xạ tên miền và địa chỉ IP.

*Caching Name Server:* Đây là một Server đảm nhiệm việc lưu trữ tất cả những tên miền, địa chỉ IP đã được phân giải và ánh xạ thành công. Nó được sử dụng trong những trường hợp sau:

- Làm tăng tốc độ phân giải bằng cách sử dụng cache
- Giảm bớt gánh nặng phân giải tên máy cho các DNS Server
- Giảm lưu lượng tham gia vào mạng và giảm độ trễ trên mạng (rất quan trọng).

### c. Cấu hình BIND9

#### ➤ Các kiểu bản ghi DNS

+ **SOA Record:** bản ghi này chỉ ra rằng máy chủ DNS Server là nơi cung cấp các thông tin tin cậy từ dữ liệu có trong zone.

Cú pháp của SOA Record như sau:

```
[Tên_miền] IN SOA [Tên_Primary_Server] [Tên_Second_Server] (  
Serial number  
Refresh number  
Retry number  
Expire number  
TTL number  
)
```

Trong đó:

*Serial number*: khi Second server kết nối tới primary server để lấy dữ liệu, trước tiên nó sẽ kiểm tra số serial này, nếu số serial này của primary server mà lớn hơn số serial của second server tức là dữ liệu trên second server đã hết hạn sử dụng và nó sẽ phải nạp lại dữ liệu mới. mỗi lần cập nhật dữ liệu trên primary server chúng ta nên tăng số serial này.

*Refresh number*: khoảng thời gian (giây) mà second server phải làm tươi lại dữ liệu của mình.

*Retry number*: nếu second server không thể kết nối tới primary server thì nó tự động kết nối lại sau retry giây này.

*Expire number*: Nếu second server không thể kết nối tới primary server sau khoảng thời gian expire giây này, thì second server sẽ không trả lời cho vùng dữ liệu đó khi được truy vấn, vì nó cho rằng dữ liệu này đã quá cũ.

*TTL number*: giá trị này cho phép các server khác cache lại dữ liệu trong 1 khoảng thời gian TTL này.

+ **Bản ghi địa chỉ (Address Records)**: bản ghi này sẽ thực hiện việc ánh xạ tên máy tính sang địa chỉ IP miền, ký hiệu là chữ A.

Cú pháp:

[tên\_máy\_tính] IN A [địa\_chỉ\_IP]

+ **Bản ghi bí danh (Alias Records)**: chúng ta tạo một bí danh từ một bản ghi đã có. Chúng ta có thể tạo một bản ghi CNAME để ánh xạ sang một CNAME (Canonical Name) khác. Khi DNS Server tìm kiếm một tên miền, nếu tên miền này đặt bí danh thì nó sẽ thay thế tên miền thực của nó bằng tên bí danh này. Ký hiệu là CNAME

Cú pháp:

[tên\_bí\_danh] IN CNAME [tên\_máy\_thật]

+ **Bản ghi tên Server (NS Record - Name Server Record)**: Mỗi zone phải có một NS record.

Cú pháp:

[tên\_miền] IN NS [máy\_DNS\_Server]



+ **Mail eXchange Record (MX record):** DNS dùng bản ghi MX để gửi mail trên mạng internet. Khi nhận mail, trình chuyển mail sẽ dựa vào MX record để quyết định đường đi của mail. Để tránh việc gửi mail bị lặp lại, MX record có thêm giá trị bổ sung là 1 số thứ tự tham chiếu. đây là giá trị nguyên không dấu 16 bit (0 - 65535) chỉ ra tính ưu tiên của các mail exchanger, giá trị càng nhỏ thì tính ưu tiên càng cao.

Cú pháp:

[tên\_miền] IN MX [độ\_ưu\_tiên] [tên\_Mail\_Server]

Trình chuyển thư mail sẽ phân phát thư đến mail exchanger có số thứ tự ưu tiên nhỏ trước. Nếu không chuyển thư được thì mail exchange với giá trị kế tiếp sau sẽ được chọn để phân phát. Trong trường hợp có nhiều mail exchanger có cùng số ưu tiên thì mail server sẽ chọn ngẫu nhiên giữa chúng.

+ **PRT Record:** Thực hiện việc ánh xạ địa chỉ vào tên (Address to name).

Cú pháp:

[địa\_chỉ\_IP] IN PTR [tên\_máy\_tính]

#### 1.6.2.2 Mail Server(in nghiêng)

##### a. Một số thuật ngữ :

Trước tiên , chúng ta tìm hiểu 1 số thuật ngữ như sau :

##### ➤ MTA ( Mail Transfer Agent ) :

- MTA ( Mail Transfer Agent) là thành phần chuyển nhận mail.
- Khi các email được gửi đến từ MUA, MTA có nhiệm vụ nhận diện người gửi và người nhận từ thông tin đóng gói trong phần header của thư và điền các thông tin cần thiết vào header.
- Sau đó MTA chuyển thư cho MDA để chuyển đến hộp thư ngay tại MTA, hoặc chuyển cho Remote MTA.
- Một phần hay cả bức thư có thể phải viết lại tại các MTA trên đường đi.
- SMTP là ngôn ngữ của MTAs

- Một số phần mềm là MTA : Postfix, Exim, Mdaemon, Exchange Server, Sendmail, Qmail

➤ **MDA ( Mail Delivery Agent ) :**

- MDA (Mail Delivery Agent) là một chương trình được MTA sử dụng để đẩy thư vào hộp thư của người dùng. Hộp thư của người dùng có thể dùng định dạng Mailbox hay Maildir.
- MDA có khả năng lọc thư, định hướng thư,...
- MTA được tích hợp với một MDA hoặc một vài MDA.
- Một số MDA là : Maildrop, Promail, Dovecot...

➤ **MUA ( Mail User Agent ) :**

- MUA là chương trình quản lý thư đầu cuối cho phép người dùng có thể đọc viết là lấy thư về từ MTA.
- MUA có thể lấy thư từ Mail server về để xử lý thông qua các giao thức IMAP , POP3...
- Chuyển thư cho một MUA khác thông qua MTA.
- Cung cấp giao diện cho người dùng tương tác với thư.
- Các phần mềm MUA thông dụng: Microsoft Outlook, Netscape, Pine,...

➤ **SMTP ( Simple Mail Transfer Protocol ) :**

- SMTP là thủ tục được phát triển ở mức ứng dụng trong mô hình 7 lớp OSI.
- SMTP sử dụng cổng 25 của TCP
- SMTP không hỗ trợ các thư không phải dạng văn bản.
- SMTP hỗ trợ thêm 2 thủ tục khác hỗ trợ cho việc lấy thư là POP3 và IMAP4
- SMTP đòi hỏi là MUA và MTA đều phải dùng giao thức SMTP

➤ **POP3 ( Post Office Protocol 3 ) :**

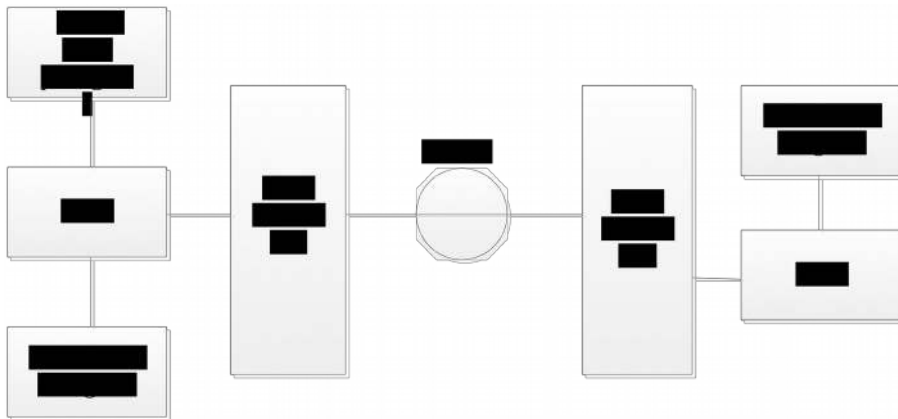
- POP (Post Office Protocol) là một trong 2 giao thức phổ biến để lấy thư từ máy chủ (server mail) về MUA .

- POP được phát triển năm 1984 và được nâng cấp lên thành POP3 vào năm 1988 (được sử dụng phổ biến hiện nay).
- POP3 kết nối trên nền TCP/IP để đến máy chủ thư điện tử (sử dụng cổng mặc định 110). Người dùng điền username và password. Sau khi xác thực đầu client sẽ sử dụng các lệnh của POP3 để lấy hoặc xóa thư.
- POP3 làm việc với chế độ offline, nghĩa là thư được lấy về MUA sẽ bị xóa trên server.

➤ **IMAP (Internet Message Access Protocol) :**

- IMAP là một giao thức để nhận thư từ server.
- IMAP được phát triển vào năm 1986 bởi đại học Stanford và nâng cấp lên IMAP2 vào năm 1987.
- IMAP4 là bản phổ biến hiện nay, nó được chuẩn hoá vào năm 1994.
- IMAP sử dụng cổng 143 của TCP
- IMAP hỗ trợ hoạt động ở chế độ online, offline hoặc disconnect
- IMAP cho phép người dùng thao tác như : tập hợp các thư từ máy chủ, tìm kiếm và lấy thư hay chuyển thư từ thư mục này sang thư mục khác hoặc xóa thư trên máy chủ.
- IMAP cho phép lấy thư về MUA mà không xóa trên máy chủ

**b. Quá trình gửi và nhận 1 email như thế nào ?**



Hình 2.8: Quá trình gửi 1 Email

Trong hình 2.8 khi 1 E-mail Client [peter@a.de](mailto:peter@a.de) soạn 1 email bằng các chương trình MUA gửi đến user E-mail Client [tim@b.de](mailto:tim@b.de) do thì MDA của domain sẽ vận chuyển tới MTA domain a.de và kiểm tra cái policy và nếu phù hợp thì MTA domain a.de sẽ nhận lá mail này.

Bước tiếp theo, MTA của domain a.de sẽ truy vấn DNS để tìm ra bản ghi MX Record của domain b.de. Bản ghi trả về IP nào nơi đó là MTA của domain b.de. Sau khi nhận được kết quả trả về từ DNS thì MTA của domain a.de sẽ telnet vào MTA của domain b.de bằng port SMTP(25) để send mail.

Quá trình HELO\EHLO, check policies (PTR, SPF, Blacklist...) diễn ra. Khi đã passed qua, MTA của domain b.de sẽ nhận lá mail đó và chuyển cho MDA của domain b.de. MDA của domain b.de tiếp nhận và chuyển cho End-Users của domain b.de.

### 1.6.3 Firewall

#### 1.6.3.1 Giới thiệu (in nghiêng)

##### a. FireWall là gì ?

Thuật ngữ FireWall có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hỏa hoạn. Trong Công nghệ mạng thông tin, FireWall là một kỹ thuật được tích hợp vào hệ thống mạng để chống lại sự truy cập trái phép nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập vào hệ thống của một số thông tin khác không mong muốn.

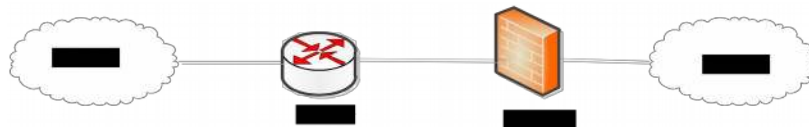
Internet FireWall là một tập hợp thiết bị (bao gồm phần cứng và phần mềm) được đặt giữa mạng của một tổ chức, một công ty, hay một quốc gia (Intranet) và Internet.

Trong một số trường hợp, Firewall có thể được thiết lập ở trong cùng một mạng nội bộ và cô lập các miền an toàn. Ví dụ như mô hình dưới đây thể hiện một mạng Firewall để ngăn cách phòng máy, người sử dụng và Internet.

##### b. Phân Loại Firewall

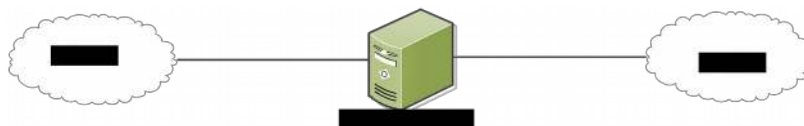
Firewall được chia làm 2 loại, gồm Firewall cứng và Firewall mềm:

➤ **Firewall cứng** : Là những firewall được tích hợp trên Router.



Hình 2.9: Firewall cứng

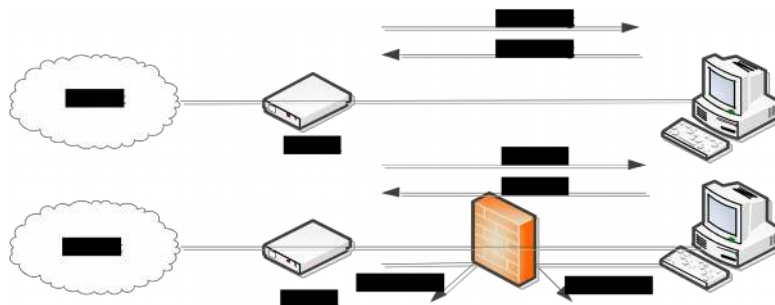
- Đặc điểm của Firewall cứng:
  - Không được linh hoạt như Firewall mềm: (Không thể thêm chức năng, thêm quy tắc như firewall mềm)
  - Firewall cứng hoạt động ở tầng thấp hơn Firewall mềm (Tầng Network và tầng Transport)
  - Firewall cứng không thể kiểm tra được nội dung của gói tin.
- **Firewall mềm:** Là những Firewall được cài đặt trên Server.



Hình 2.10: Firewall mềm

- Đặc điểm của Firewall mềm:
  - Tính linh hoạt cao: Có thể thêm, bớt các quy tắc, các chức năng
  - Firewall mềm hoạt động ở tầng cao hơn Firewall cứng (tầng ứng dụng)
  - Firewall mềm có thể kiểm tra được nội dung của gói tin (thông qua các từ khóa)

### c. Tại sao cần Firewall



Hình 2.11: Chức năng của Firewall

Nếu máy tính của bạn không được bảo vệ, khi bạn kết nối Internet, tất cả các giao thông ra vào mạng đều được cho phép, vì thế hacker, trojan, virus có thể truy cập và lấy cắp thông tin cá nhân của bạn trên máy tính. Chúng có thể cài đặt các đoạn mã để tấn công file dữ liệu trên máy tính. Chúng có thể sử dụng máy tính của bạn để tấn công một máy tính của gia đình hoặc doanh nghiệp khác kết nối Internet. Một firewall có thể giúp bạn thoát khỏi gói tin hiểm độc trước khi nó đến hệ thống của bạn.

### ➤ Chức năng chính của Firewall

Chức năng chính của Firewall là kiểm soát luồng thông tin từ giữa Intranet và Internet. Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong (Intranet) và mạng Internet. Cụ thể là:

- Cho phép hoặc cấm những dịch vụ truy nhập ra ngoài (từ Intranet ra Internet).
- Cho phép hoặc cấm những dịch vụ phép truy nhập vào trong (từ Internet vào Intranet).
- Theo dõi luồng dữ liệu mạng giữa Internet và Intranet.
- Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập.
- Kiểm soát người sử dụng và việc truy nhập của người sử dụng.
- Kiểm soát nội dung thông tin thông tin lưu chuyển trên mạng.

### 1.6.3.2 Iptables Firewall (in nghiênng)

#### a. Giới thiệu

Trong môi trường Linux phần mềm firewall phổ biến và cơ bản nhất là iptables, thông qua nó bạn có thể dễ dàng hiểu được nguyên lý hoạt động của một hệ thống firewall nói chung.

#### b. Cấu Trúc Iptable

Iptables cơ bản gồm ba bảng FILTER, MANGLE, NAT và các chain trong mỗi bảng, với chúng người quản trị có thể tạo ra các rules cho phép các gói tin vào ra hệ thống (được bảo vệ bằng iptables) tùy theo ý muốn của mình. Chức năng cụ thể của chúng như sau:

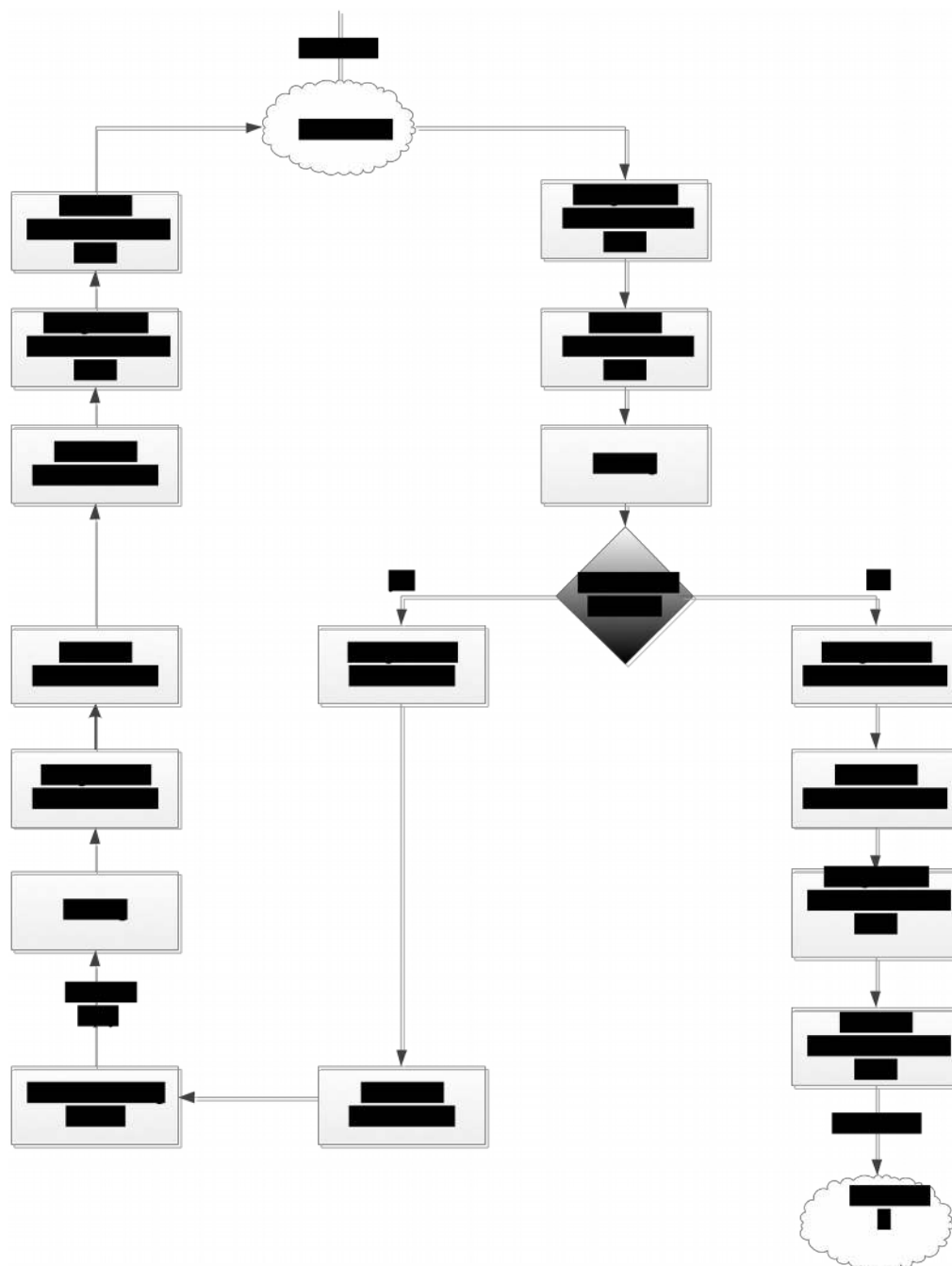
- Mangle: dùng để chỉnh sửa QOS(quality of service) bit trong phần TCP Header của gói tin
- Filter: đúng như tên gọi nó dùng để lọc các gói tin gồm các build-in chain
  - Forward chain: lọc những gói tin đi qua hệ thống (đi vào một hệ thống khác).
  - Input chain: lọc những gói tin đi vào hệ thống.
  - Output chain: những gói tin đi ra từ hệ thống.
- Nat: sửa địa chỉ gói tin gồm các build-in chain.
  - Pre-routing: sửa địa chỉ đích của gói tin trước khi nó được routing bởi bảng routing của hệ thống (destination NAT hay DNAT).
  - Post-routing: ngược lại với Pre-routing, nó sửa địa chỉ nguồn của gói tin sau khi gói tin đã được routing bởi hệ thống (SNAT).

Mỗi rule mà bạn tạo ra phải tương ứng với một chain, table nào đấy. Nếu bạn không xác định tables nào thì iptables coi mặc định là cho bảng FILTER

### **c. Trình tự xử lý gói tin của iptables:**

Có thể tóm tắt trình tự xử lý gói tin của iptables bằng hình vẽ 2.12, các gói tin từ ngoài đi vào sẽ được kiểm tra bởi các Pre-routing chain đầu tiên xem nó có cần DNAT không sau đó gói tin được routing. Nếu gói tin cần đi tới một hệ thống khác (protected network) nó sẽ được lọc bởi các FORWARD chain của bảng FILTER và nếu cần nó có thể được SNAT bởi các Post-routing chain trước khi đến được hệ thống đích.

Tương tự khi hệ thống đích cần trả lời, gói tin sẽ đi theo thứ tự như vậy nhưng theo chiều ngược lại. Lưu ý trong hình vẽ những FORWARD và Post-routing chain của bảng mangle chỉ tác động vào đặc điểm QOS (Quality of Service) của gói tin. Nếu gói tin được gửi tới hệ thống (hệ thống chứa iptables) nó sẽ được xử lý bởi các INPUT chain và nếu không bị lọc bỏ nó sẽ được xử lý bởi một dịch vụ (System Service) nào đó chạy trên hệ thống. Khi hệ thống gửi trả lời, gói tin mà



Hình 2.12: Trình tự xử lý gói tin của iptables



- **Sau đây là một số build-in targets thường được sử dụng.**
  - ACCEPT: iptables chấp nhận gói tin, đưa nó qua hệ thống mà không tiếp tục kiểm tra nó nữa.
  - DROP: iptables loại bỏ gói tin, không tiếp tục xử lý nó nữa.
  - LOG: thông tin của gói tin sẽ được ghi lại bởi syslog hệ thống, iptables tiếp tục xử lý gói tin bằng những rules tiếp theo.
  - REJECT: chức năng của nó cũng giống như DROP tuy nhiên nó sẽ gửi một error message tới host đã gửi gói tin.
  - DNAT: dùng để sửa lại địa chỉ đích của gói tin. SNAT: dùng để sửa lại địa chỉ nguồn của gói tin
  - MASQUERADE: cũng là một kiểu dùng để sửa địa chỉ nguồn của gói tin để xây dựng các rules bạn còn phải sử dụng các tùy chọn để tạo điều kiện so sánh.

#### 1.6.4 Web Server

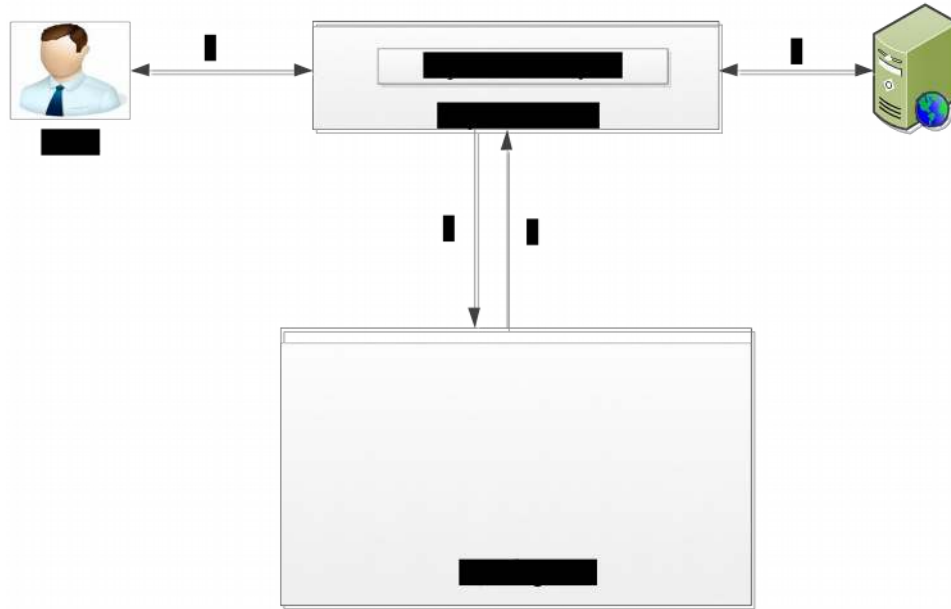
##### 1.6.4.1 Giới thiệu (in nghiêng)

Một máy chủ web là một loại đặc biệt của máy chủ tập tin mà tất cả phải là tập tin cung cấp được lưu trữ trong một cấu trúc thư mục chuyên dụng. Các gốc của cấu trúc này được gọi là gốc của tài liệu, và các định dạng tập tin mà cung cấp các tập tin là HTML, ngôn ngữ đánh dấu siêu văn bản. Nhưng một máy chủ web có thể cung cấp nhiều hơn là chỉ tập tin HTML. Trong thực tế, các máy chủ web có thể phục vụ bất cứ thứ gì, miễn là nó được ghi rõ trong tập tin HTML. Do đó, một máy chủ web là một nguồn rất tốt cho những dòng âm thanh và video, truy cập cơ sở dữ liệu, hiển thị hình ảnh động, hiển thị hình ảnh, và nhiều hơn nữa.

Ngoài các máy chủ web nơi có nội dung được lưu trữ, khách hàng còn có thể sử dụng một giao thức cụ thể để truy cập nội dung này là tốt, và giao thức này là HTTP (các giao thức truyền siêu văn bản). Thông thường, khách hàng sử dụng một trình duyệt web để tạo ra các HTTP lệnh mà lấy nội dung, ở dạng HTML và các file khác, từ một máy chủ web. hai phiên bản khác nhau của máy

chủ web Apache. Việc gần đây nhất phiên bản 2.x, là một trong những cài đặt mặc định trên Ubuntu Server. Tuy nhiên, môi trường gặp phải mà vẫn sử dụng trước đây 1.3. Điều này thường xảy ra nếu, ví dụ, các kịch bản tùy chỉnh đã được phát triển để sử dụng với 1.3, và những kịch bản không tương thích với 2.x.

➤ **Mô hình hoạt động**



Hình 2.13: Mô hình hoạt động Web Server

➤ **Địa chỉ URL**

URL (viết tắt của Uniform Resource Locator) được dùng để tham chiếu tới tài nguyên trên Internet. URL mang lại khả năng siêu liên kết cho các trang mạng. Một URL bao gồm tên giao thức (http,ftp), tên miền, có thể chỉ định cổng, đường dẫn tuyệt đối trên máy phục vụ của tài nguyên, các truy vấn, chỉ định mục con.

#### 1.6.4.2 Giới thiệu về APACHE (in nghiêng)

**a. Tổng quan:**

Apache là một máy chủ web kiểu mô-đun, có nghĩa là các máy chủ lõi (có vai trò là cơ bản để phục vụ lên các văn bản HTML) có thể được mở rộng bằng cách sử dụng một loạt các mô-đun tùy chọn:

- libapache2-mod-auth-mysqld: module này cho Apache như thế nào để xử lý xác thực người dùng với một cơ sở dữ liệu MySQL.
- libapache2-mod-auth-pam: module này chỉ thị Apache làm thế nào để xác thực người dùng, sử dụng cơ chế Linux PAM.
- libapache-mod-frontpage: module này chỉ thị Apache như thế nào để xử lý các trang web bằng cách sử dụng Microsoft FrontPage mở rộng.
- libapache2-mod-mono: module này cho Apache làm thế nào để giải mã ASP.NET.

Đây là một danh sách ngắn và không đầy đủ của tất cả các module có thể sử dụng trên web Apache server: <http://modules.apache.org> hiện danh sách hơn 450 mô-đun. Điều quan trọng là xác định chính xác những mô-đun nào cần cho máy chủ để có thể mở rộng chức năng của nó cho phù hợp.

Các dự án Apache Directory cung cấp giải pháp thư mục hoàn toàn được viết bằng Java. Chúng bao gồm một máy chủ thư mục, mà đã được chứng nhận là LDAP v3 phù hợp do Tập đoàn Open (Apache Directory Server), và các công cụ thư mục dựa trên Eclipse (Apache Directory Studio).

#### ➤ **Apache Directory Server**

Apache Directory Server là một máy chủ thư mục nhúng hoàn toàn được viết bằng Java, đã được chứng nhận tương thích LDAPv3 do tập đoàn Open. Bên cạnh đó LDAP nó hỗ trợ Kerberos 5 và những thay đổi mật khẩu Nghị định thư. Nó đã được thiết kế để giới thiệu gây nên, thủ tục, hàng đợi và quan điểm với thế giới của LDAP đã thiếu các cấu trúc phong phú.

#### ➤ **Apache Directory Studio**

Apache Directory Studio là một thư mục nền tảng công cụ hoàn chỉnh dự định sẽ được sử dụng với bất kỳ máy chủ LDAP tuy nhiên nó đặc biệt được thiết kế để sử dụng với các Apache Directory Server. Nó là một ứng dụng RCP Eclipse, bao gồm một số Eclipse (OSGi) bổ sung, có thể dễ dàng nâng cấp với những người khác. Những bổ sung thậm chí có thể chạy trong Eclipse chính nó.

#### 1.6.4.3 APACHE và LDAP :

APACHE sử dụng Module `mod_authnz_ldap` để cho phép một thư mục LDAP được sử dụng để lưu trữ các cơ sở dữ liệu để xác thực HTTP cơ bản.

Module này cung cấp chứng thực trước kết thúc như `mod_auth_basic` để xác thực người dùng thông qua một thư mục LDAP. `mod_authnz_ldap` hỗ trợ các tính năng sau:

- Được biết đến để hỗ trợ các SDK OpenLDAP (cả 1.x và 2.x), Novell LDAP SDK và iPlanet các (Netscape) SDK.
- Chính sách cấp phép phức tạp có thể được thực hiện bởi đại diện chính sách với các bộ lọc LDAP.
- Sử dụng rộng bộ nhớ đệm của các hoạt động LDAP thông qua `mod_ldap`.
- Hỗ trợ cho LDAP qua SSL (yêu cầu các SDK Netscape) hoặc TLS (yêu cầu OpenLDAP 2.x SDK hoặc Novell LDAP SDK).

Có hai giai đoạn trong việc cấp quyền truy cập cho người dùng. Giai đoạn đầu tiên là xác thực, trong đó các nhà cung cấp chứng thực `mod_authnz_ldap` xác nhận rằng thông tin của người dùng là hợp lệ. Điều này cũng được gọi là tìm kiếm / giai đoạn kết. Giai đoạn thứ hai là ủy quyền, trong đó `mod_authnz_ldap` quyết định nếu người sử dụng chứng thực được phép truy cập vào các tài nguyên trong câu hỏi. Điều này cũng được biết đến như là so sánh các giai đoạn.

`mod_authnz_ldap` đăng ký cả hai nhà cung cấp xác thực và ủy quyền `authn_ldap` `authz_ldap` một bộ xử lý. Các nhà cung cấp `authn_ldap` chứng thực có thể được kích hoạt thông qua các chỉ thị `AuthBasicProvider` sử dụng giá trị `ldap`. Việc xử lý ủy quyền `authz_ldap` mở rộng các loại chỉ thị bằng cách thêm Yêu cầu của người sử dụng `ldap`, `ldap dn-và ldap-nhóm` các giá trị.

Trong giai đoạn thẩm định, tìm kiếm `mod_authnz_ldap` cho một mục trong thư mục phù hợp với tên người dùng mà máy khách HTTP qua. Nếu một trận đấu duy nhất duy nhất được tìm thấy, sau đó `mod_authnz_ldap` cố gắng để gắn kết với các máy chủ thư mục bằng cách sử dụng các DN của mục nhập cộng với các

mật khẩu được cung cấp bởi các khách hàng HTTP. Bởi vì nó thực hiện một tìm kiếm, sau đó một liên kết, nó thường được gọi tắt là tìm kiếm / giai đoạn kết.

## 1.6.5 DHCP Server

### 1.6.5.1 Giới thiệu về DHCP (in nghiêng)

DHCP là viết tắt của Dynamic Host Configuration Protocol, là giao thức cấu hình host động được thiết kế làm giảm thời gian chỉnh cấu hình cho mạng TCP/IP bằng cách tự động gán các địa chỉ IP cho khách hàng khi họ vào mạng. Dịch vụ DHCP là một thuận lợi rất lớn đối với người điều hành mạng. Nó làm yên tâm về các vấn đề cố hữu phát sinh khi phải khai báo cấu hình thủ công. Nói một cách tổng quan hơn DHCP là dịch vụ mang đến cho chúng ta nhiều lợi điểm trong công tác quản trị và duy trì một mạng TCP/IP như:

- + Tập chung quản trị thông tin về cấu hình IP.
  - Cấu hình động các máy.
  - Cấu hình IP cho các máy một cách liên mạch
  - Sự linh hoạt
  - Khả năng mở rộng.

Một DHCP Server cấp phát địa chỉ IP cho các máy tính khác. Dịch vụ này thường được sử dụng cho doanh nghiệp giúp bạn giảm bớt cài đặt cấu hình. Tất cả các địa chỉ IP của tất cả các máy tính được lưu trữ trong một cơ sở dữ liệu trên một máy Server.

Một máy chủ DHCP có thể cài đặt cấu hình và sử dụng theo hai phương pháp

#### ➤ Vùng địa chỉ

Phương pháp này đòi hỏi phải xác định một vùng (đôi khi còn gọi là một phạm vi) của địa chỉ IP mà DHCP cung cấp cho khách hàng của họ đang có cấu hình và tính năng động trên một Server cơ sở. Khi một DHCP Client không còn trên mạng cho một khoảng thời gian xác định, cấu hình là hết hạn và khi quay trở lại sẽ được cấp phát địa chỉ mới bằng cách sử dụng các dịch vụ DHCP.

#### ➤ Địa chỉ MAC

Phương pháp này đòi hỏi phải sử dụng dịch vụ DHCP để xác định địa chỉ phần

cứng duy nhất của mỗi card mạng kết nối với các mạng lưới và sau đó liên tục cung cấp một cấu hình DHCP mỗi lần khách hàng yêu cầu để tạo ra một trình phục vụ DHCP bằng cách sử dụng các thiết bị mạng.

#### **1.6.5.2 Phương thức hoạt động của dịch vụ DHCP (in nghiêng)**

Dịch vụ DHCP hoạt động theo mô hình Client / Server. Theo đó quá trình tương tác giữa DHCP client và server sẽ diễn ra theo các bước sau:

- Bước 1: Khi máy Client khởi động, máy sẽ gửi broadcast gói tin DHCP DISCOVER, yêu cầu một Server phục vụ mình. Gói tin này cũng chứa địa chỉ MAC của client. Nếu client không liên lạc được với DHCP Server thì sau 4 lần truy vấn không thành công nó sẽ tự động phát sinh ra 1 địa chỉ IP riêng cho chính mình nằm trong dãy địa chỉ IP được giới hạn dùng để liên lạc tạm thời. Và client vẫn duy trì việc phát tín hiệu Broad cast sau mỗi 5 phút để xin cấp IP từ DHCP Server.

- Bước 2: Các máy Server trên mạng khi nhận được yêu cầu đó. Nếu còn khả năng cung cấp địa chỉ IP, đều gửi lại cho máy Client một gói tin DHCP OFFER, đề nghị cho thuê một địa chỉ IP trong một khoảng thời gian nhất định, kèm theo là một Subnet Mask và địa chỉ của Server. Server sẽ không cấp phát địa chỉ IP vừa đề nghị cho client thuê trong suốt thời gian thương thuyết.

- Bước 3: Máy Client sẽ lựa chọn một trong những lời đề nghị ( DHCP OFFER) và gửi broadcast lại gói tin DHCP REQUEST và chấp nhận lời đề nghị đó. Điều này cho phép các lời đề nghị không được chấp nhận sẽ được các Server rút lại và dùng để cấp phát cho các Client khác.

- Bước 4: Máy Server được Client chấp nhận sẽ gửi ngược lại một gói tin DHCP ACK như một lời xác nhận, cho biết địa chỉ IP đó, Subnet Mask đó và thời hạn cho sử dụng đó sẽ chính thức được áp dụng. Ngoài ra server còn gửi kèm những thông tin bổ xung như địa chỉ Gateway mặc định, địa chỉ DNS Server...

#### **1.6.5.3 Cài đặt và cấu hình DHCP Server trên Ubuntu (in nghiêng)**

##### **➤ Cài đặt DHCP Server**

Cú pháp:

```
$ sudo apt-get install dhcp3-server
```

Lệnh này sẽ hoàn tất việc cài đặt.

### ➤ Cấu hình DHCP Server

Nếu bạn có hai cạc mạng trong máy chủ của bạn, bạn cần phải chọn card mà bạn muốn sử dụng để phục vụ DHCP. Mặc định nó là eth0. Bạn có thể thay đổi nó bằng cách sửa tệp tin /etc/default/dhcp3-server file

```
$ sudo vi /etc/default/dhcp3-server
```

Tìm đến dòng:

```
INTERFACES="eth0"
```

Rồi thay thế bằng dòng dưới đây:

```
INTERFACES="eth1"
```

Lưu và thoát. Tùy chọn này.

Tiếp theo bạn chắc đã sao lưu tệp tin /etc/dhcp3/dhcpd.conf

```
$ cp /etc/dhcp3/dhcpd.conf /etc/dhcp3/dhcpd.conf.back
```

Sửa tệp tin bằng lệnh /etc/dhcp3/dhcpd.conf

```
$ sudo vi /etc/dhcp3/dhcpd.conf
```

- Phương thức sử dụng vùng địa chỉ

Bạn cần thay đổi những phần sau trong tệp tin /etc/dhcp3/dhcpd.conf

```
default-lease-time 600;
```

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

```
option subnet-mask 255.255.255.0;
```

```
option broadcast-address 192.168.1.255;
```

```
option routers 192.168.1.254;
```

```
option domain-name-servers 192.168.1.1, 192.168.1.2;
```

```
option domain-name "yourdomainname.com";
```

```
subnet 192.168.1.0 netmask 255.255.255.0 {
```

```
range 192.168.1.10 192.168.1.200;
```

```
}
```

Lưu và đóng tệp tin.

Kết quả này trên DHCP Server sẽ cấp phát cho một Client một địa chỉ IP nằm trong khoảng 192.168.1.10 tới 192.168.1.200 . Nó sẽ cho cấp phát một địa chỉ IP cho 600 giây, nếu khách hàng không yêu cầu cho một khung thời gian cụ thể.

Hoặc tối đa là (được phép) 7200 giây.

- Phương thức sử dụng địa chỉ MAC

Phương thức này bạn có thể sử dụng trên một số hoặc tất cả các máy với địa chỉ IP cố định. Bạn có thể sử dụng địa chỉ IP cố định cho server1, server2, printer1 và printer2

```
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "yourdomainname.com";
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.10 192.168.1.200;
}
host server1 {
    hardware ethernet 00:1b:63:ef:db:54;
    fixed-address 192.168.1.20;
}
host server2 {
    hardware ethernet 00:0a:95:b4:d4:b0;
    fixed-address 192.168.1.21;
}
```



```
host printer1 {  
    hardware ethernet 00:16:cb:aa:2a:cd;  
    fixed-address 192.168.1.22;  
}  
host printer2 {  
    hardware ethernet 00:0a:95:f5:8f:b3;  
    fixed-address 192.168.1.23;}
```

- Bây giờ bạn cần khởi động lại DHCP Server sử dụng lệnh:

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

### ➤ Cấu hình Ubuntu DHCP Client

Nếu bạn muốn cấu hình Ubuntu Desktop của bạn như là một DHCP Client bạn làm theo các bước dưới đây.

- Bạn cần mở tệp tin /etc/network/interfaces

```
$ sudo vi /etc/network/interfaces
```

- Chắc chắn rằng có bạn có các dòng dưới đây (eth0 là một ví dụ)

```
auto lo eth0
```

```
iface eth0 inet dhcp
```

```
iface lo inet loopback
```

Lưu và đóng tệp tin.

- Bạn cần khởi động lại dịch vụ mạng bằng lệnh dưới đây:

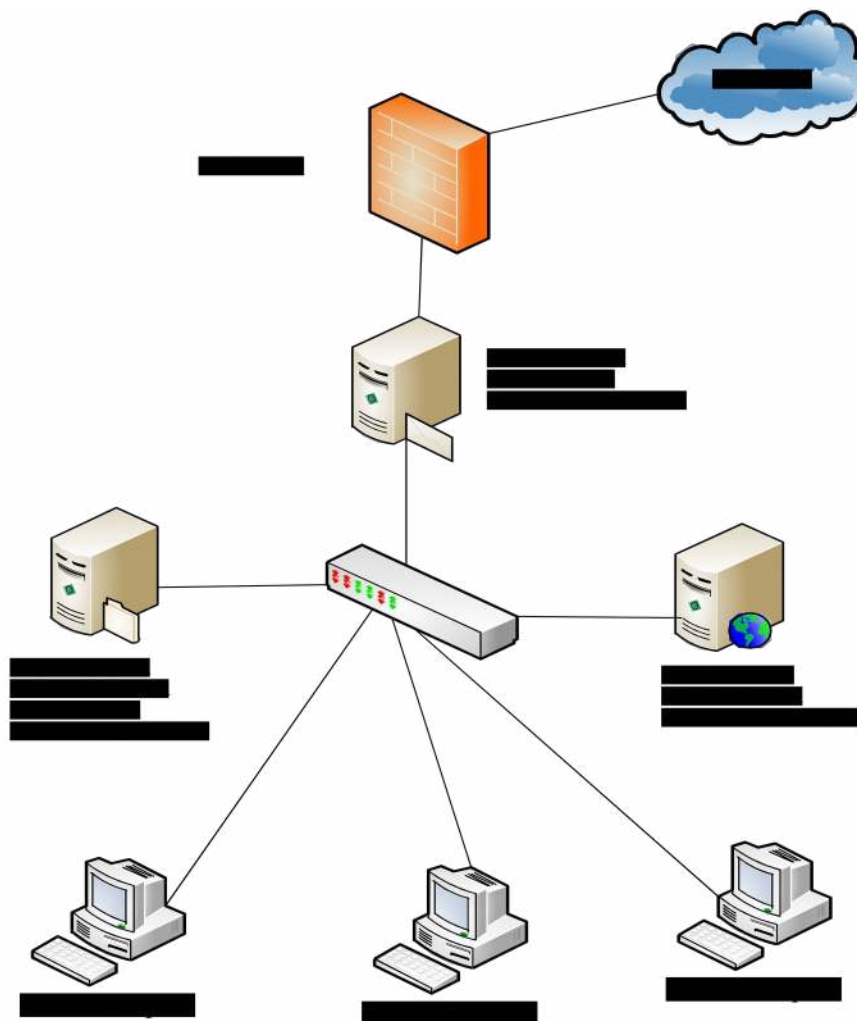
```
$ sudo /etc/init.d/networking restart
```

## CHƯƠNG 3

### TRIỂN KHAI QUẢN TRỊ MẠNG TRÊN UBUNTU SERVER

#### 1.7 XÂY DỰNG KỊCH BẢN

##### 1.7.1 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.

##### 1.7.2 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

## **1.8 PHÂN TÍCH**

### **1.8.1 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.

### **1.8.2 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

## **1.9 THỰC HIỆN**

### **1.9.1 Chuẩn bị**

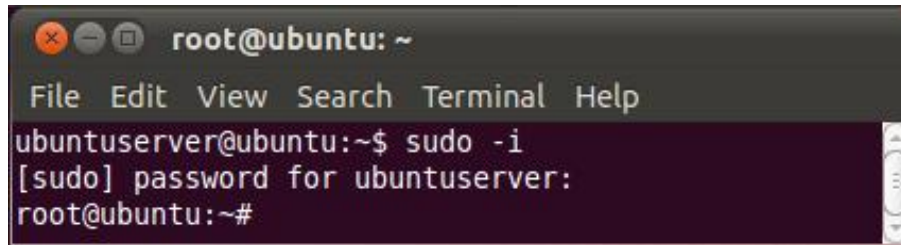
- Cài đặt ubuntu server 10.04 32bit hay 64bit
- Đặt địa chỉ IP tĩnh và máy có thể kết nối internet
- Update ubuntu server bằng lệnh sau :
  - + apt-get update
  - + apt-get dist-upgrade

+ reboot.

## 1.9.2 Cài đặt và cấu hình

### 1.9.2.1 Cài đặt và cấu hình LDAP (in nghiêng)

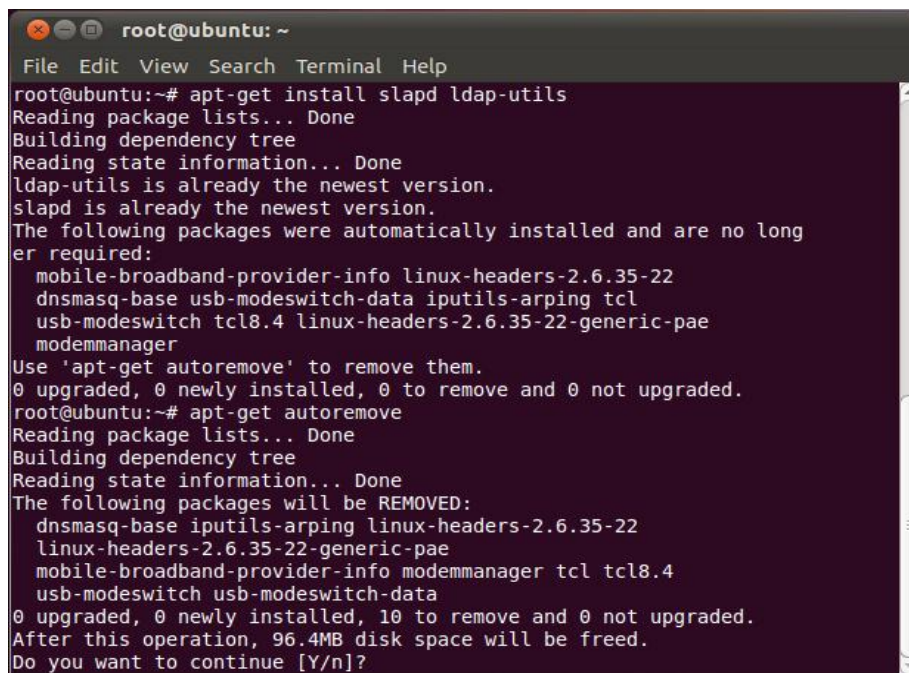
- Bước 1: mở terminal và lấy quyền root bằng lệnh sudo -i và đánh password của hệ thống



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

Hình 3.2: Đăng nhập hệ thống Ubuntu Server

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

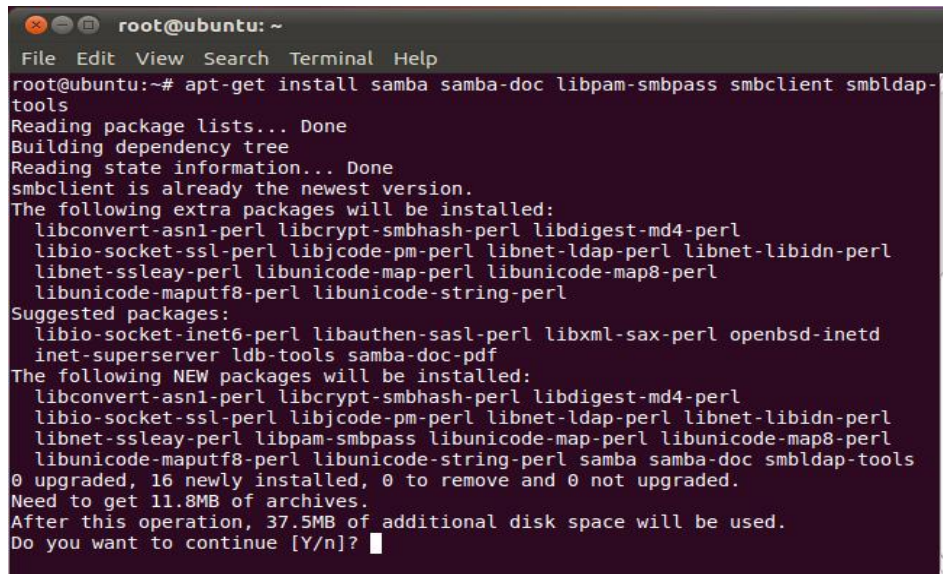


```
root@ubuntu: ~
File Edit View Search Terminal Help
root@ubuntu:~# apt-get install slapd ldap-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
ldap-utils is already the newest version.
slapd is already the newest version.
The following packages were automatically 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 libcrypt-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 libcrypt-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

### 1.9.2.2 Cài đặt và cấu hình DNS Server (in nghiêng)

#### ➤ 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 :







Hình 3.7: Cấu hình DNS Server (3)

### 1.9.2.3 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 :



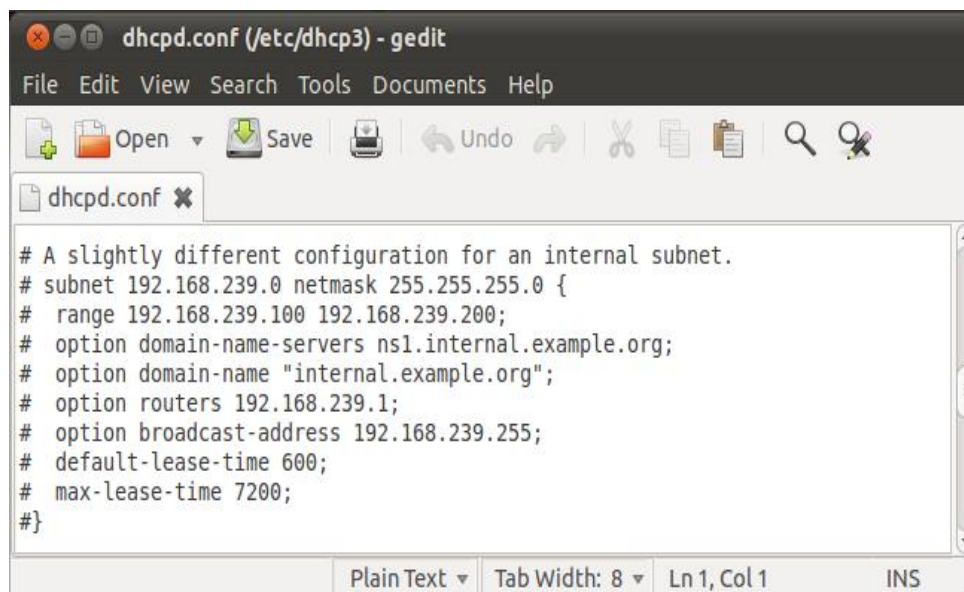
Hình 3.9. Cấu hình file pool (a)

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 :



Hình 3.10: Cấu hình file pool (b)

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

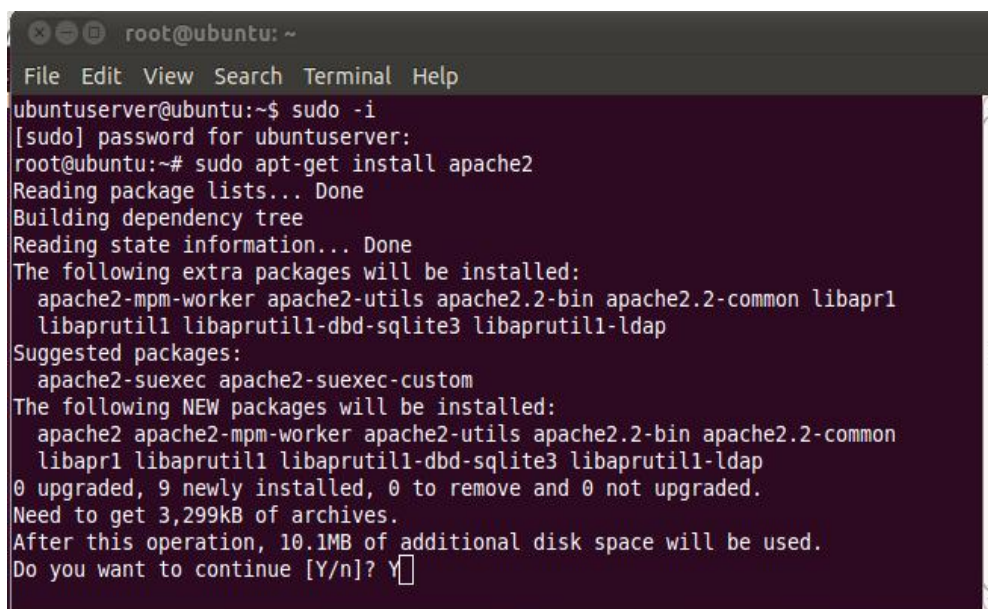
```
sudo /etc/init.d/dhcp3-server restart
```

#### 1.9.2.4 Cài đặt và triển khai Web Server **(in nghiêng)**

➤ **Cài Đặt :**

Ta dùng lệnh sau để cài đặt:

```
sudo apt-get install apache2
```

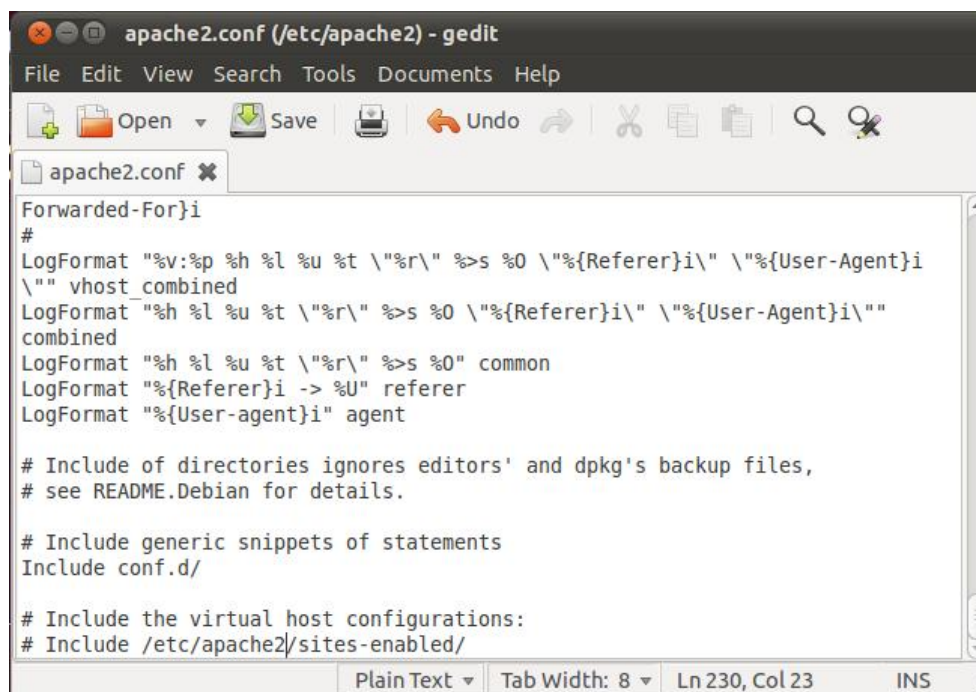


```
root@ubuntu: ~  
File Edit View Search Terminal Help  
ubuntuserver@ubuntu:~$ sudo -i  
[sudo] password for ubuntuserver:  
root@ubuntu:~# sudo apt-get install apache2  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following extra packages will 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



```
apache2.conf (/etc/apache2) - gedit  
File Edit View Search Tools Documents Help  
Open Save Undo  
apache2.conf  
Forwarded-For}i  
#  
LogFormat "%v:%p %h %l %u %t \"%r\" %>s %0 \"%{Referer}i\" \"%{User-Agent}i  
\"\" vhost_combined  
LogFormat "%h %l %u %t \"%r\" %>s %0 \"%{Referer}i\" \"%{User-Agent}i\""  
combined  
LogFormat "%h %l %u %t \"%r\" %>s %0" common  
LogFormat "%{Referer}i -> %U" referer  
LogFormat "%{User-agent}i" agent  
  
# Include of directories ignores editors' and dpkg's backup files,  
# see README.Debian for details.  
  
# Include generic snippets of statements  
Include conf.d/  
  
# Include the virtual host configurations:  
# Include /etc/apache2/sites-enabled/
```

Hình 3.12: Cấu hình APACHE với LDAP

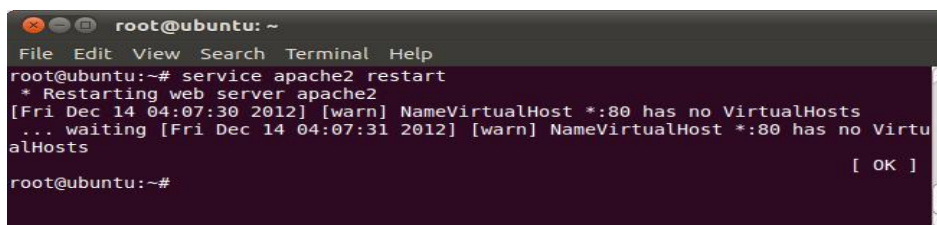
Tại cuối file này ta comment dòng Include “/etc/apache2/sites-enabled/” thành “#Include /etc/apache2/sites-enabled/”

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*



```
root@ubuntu: ~  
File Edit View Search Terminal Help  
root@ubuntu:~# service apache2 restart  
* Restarting web server apache2  
[Fri Dec 14 04:07:30 2012] [warn] NameVirtualHost *:80 has no VirtualHosts  
... waiting [Fri Dec 14 04:07:31 2012] [warn] NameVirtualHost *:80 has no Virtu  
alHosts  
[ OK ]  
root@ubuntu:~#
```

Hình 3.13: Restart apache

### 1.9.2.5 Thiết lập Firewall (in nghiêng)

#### ➤ 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.

### **1.10 TEST DEMO**



## KẾT LUẬN (cỡ chữ 16)

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

## TÀI LIỆU THAM KHẢO (cỡ chữ 16)

### Tài liệu tiếng Việt

- [1] Nguyễn Hồng Sơn, *Giáo trình hệ thống mạng máy tính*, NXB Lao động – Xã hội, 2007
- [2] Nguyễn Thanh Thủy, *Nhập môn hệ điều hành Linux*, NXB Khoa Học và Kỹ Thuật, Hà Nội, 2005

### Tài liệu Internet

- [3] [http://wiki.ubuntu-vn.org/index.php/S%E1%BB%AD\\_d%E1%BB%A5ng\\_Terminal#C.C3.A1c\\_t.E1.BA.ADp\\_l.E1.BB.87nh](http://wiki.ubuntu-vn.org/index.php/S%E1%BB%AD_d%E1%BB%A5ng_Terminal#C.C3.A1c_t.E1.BA.ADp_l.E1.BB.87nh)
- [4] <https://help.ubuntu.com/community/BIND9ServerHowto>
- [5] <http://vi.wikipedia.org/wiki/DNS>
- [6] <https://help.ubuntu.com/community/dhcp3-server>
- [7] <https://help.ubuntu.com/8.04/serverguide/httpd.html>



[8] <https://help.ubuntu.com/8.04/serverguide/firewall.html>