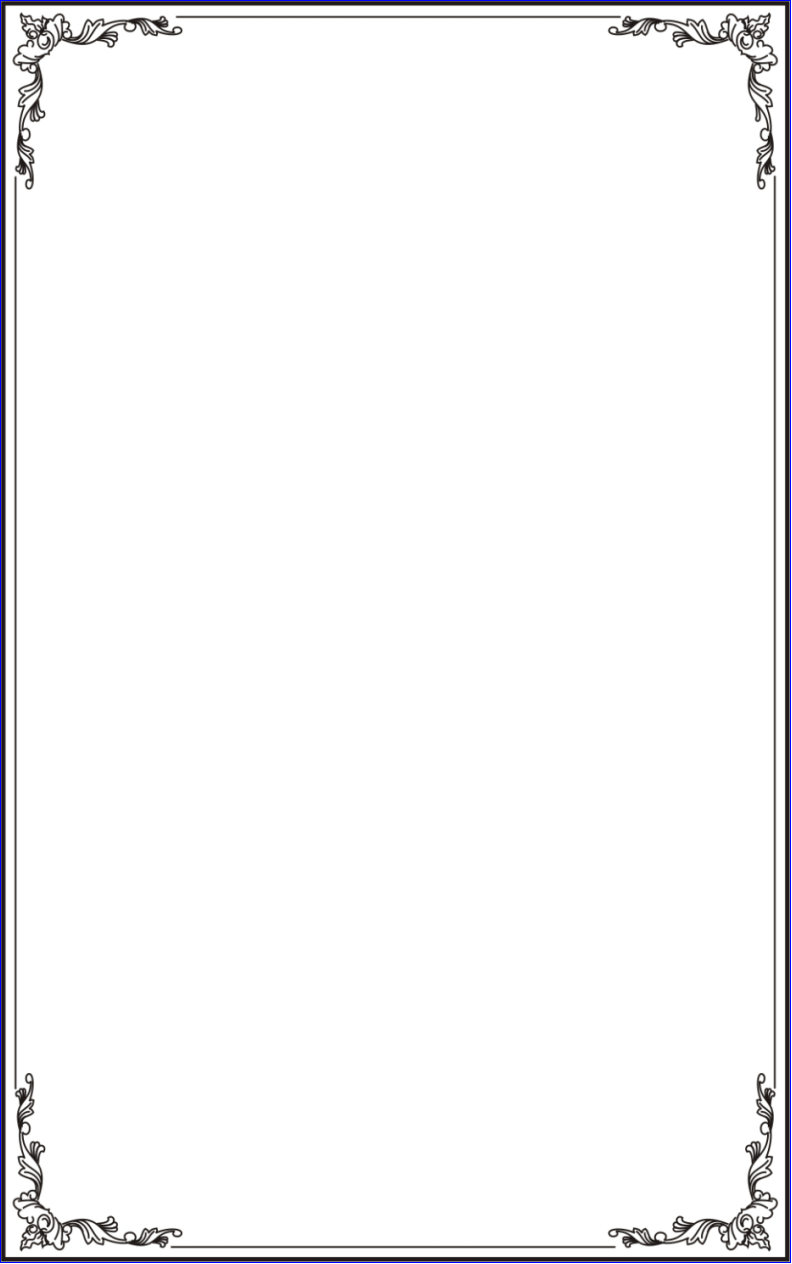
****

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

****

**BÁO CÁO BÀI TẬP LỚN**

**Học Phần : Nguyên Lý Hệ Điều Hành**

*Đề tài:*

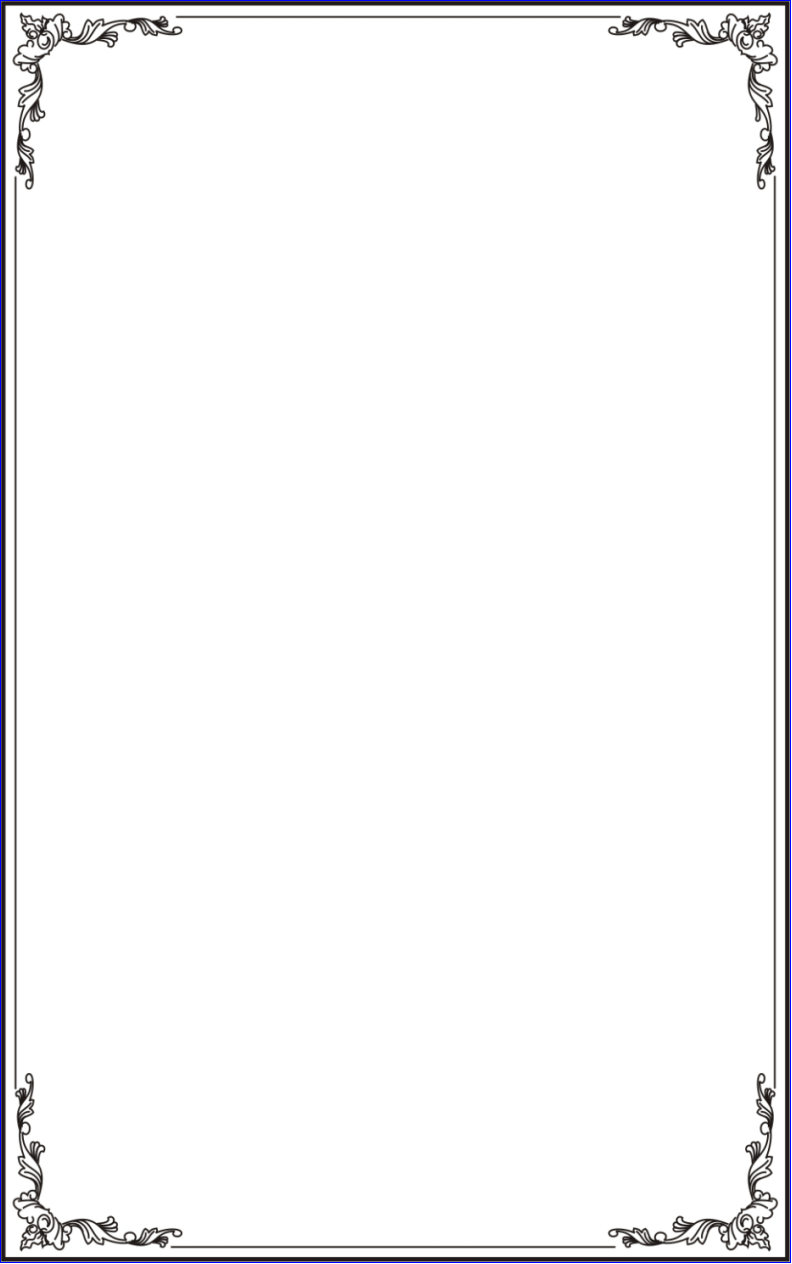
**NGHIÊN CỨU TÌM HIỂU VỀ CÁC DỊCH VỤ MẠNG TRONG HĐH LINUX**

**GVHD : Ths. Nguyễn Tuấn Tú**

**Nhóm : 14**

**Lớp : IT6025.7 K16**

*Hà Nội - 2023*

****

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

****

**BÁO CÁO BÀI TẬP LỚN**

**Học Phần : Nguyên Lý Hệ Điều Hành**

*Đề tài:*

**NGHIÊN CỨU TÌM HIỂU VỀ CÁC DỊCH VỤ MẠNG TRONG HĐH LINUX**

**GVHD : Ths. Nguyễn Tuấn Tú**

**Sinh viên thực hiện : Nguyễn Thị Trang - 2021604432**

**Phạm Thị Liễu - 2021608600**

**Phan Xuân Minh**

**Nguyễn Thị Hải Phương - 2021606397**

**Phạm Văn Tình**

**Lớp : IT6025.7 K16**

**MỤC LỤC**

[DANH MỤC HÌNH ẢNH 1](#_Toc135858828)

[LỜI NÓI ĐẦU 2](#_Toc135858829)

[CHƯƠNG 1. CÁC TIỆN ÍCH MẠNG CỦA HỆ ĐIỀU HÀNH LINUX 4](#_Toc135858830)

[I. Telnet 4](#_Toc135858831)

[1. Telnet 4](#_Toc135858832)

[2. Tiện ích của telnet 4](#_Toc135858833)

[3. Hoạt động của telnet 4](#_Toc135858834)

[4. Yêu cầu để thực hiện được Telnet 5](#_Toc135858835)

[II. FTP 5](#_Toc135858836)

[1. Khái niệm về FTP: 5](#_Toc135858837)

[2. Mô hình hoạt động của FTP. 6](#_Toc135858838)

[2.1 Kết nối TCP trong FTP. 6](#_Toc135858839)

[2.2 Mô hình FTP. 6](#_Toc135858840)

[3. Phương thức tạo kết nối và truyền dữ liệu trong FTP. 7](#_Toc135858841)

[3.1 Phương thức tạo kết nối dữ liệu của FTP. 7](#_Toc135858842)

[3.1.1. Normal (Active) Data Connections. 7](#_Toc135858843)

[3.1.2. Passive Data Connections. 8](#_Toc135858844)

[3.2 Phương thức truyền dữ liệu của FTP. 8](#_Toc135858845)

[4. Ưu điểm và nhược điểm 8](#_Toc135858846)

[III. Ping 9](#_Toc135858847)

[1. Câu lệnh ping 9](#_Toc135858848)

[2. Ping hoạt động: 9](#_Toc135858849)

[3. Tính năng bao gồm: 9](#_Toc135858850)

[IV. Traceroute 10](#_Toc135858851)

[1. Nguyên lý hoạt động của traceroute 10](#_Toc135858852)

[2. Hướng dẫn chạy Traceroute trên Linux 10](#_Toc135858853)

[3. Sử dụng Traceroute 11](#_Toc135858854)

[CHƯƠNG 2. SAMBA VÀ DHCP 12](#_Toc135858855)

[I. Samba 12](#_Toc135858856)

[1. Giới thiệu SAMBA 12](#_Toc135858857)

[2. Cài đặt và cấu hình 13](#_Toc135858858)

[3. Quản trị tài khoản Samba 17](#_Toc135858859)

[4. Sử dụng dịch vụ Samba 18](#_Toc135858860)

[II. DHCP 20](#_Toc135858861)

[1. Giới thiệu dịch vụ DHCP 20](#_Toc135858862)

[2. Nguyên tắc hoạt động 20](#_Toc135858863)

[3. Các thông số trong cấu hình DHCP 21](#_Toc135858864)

[4. Cài đặt và cấu hình dịch vụ DHCP. 21](#_Toc135858865)

[CHƯƠNG 3. NETWORKING. 23](#_Toc135858866)

[I. Địa chỉ IP 23](#_Toc135858867)

[1. IP tĩnh và động 23](#_Toc135858868)

[2. Phân phối địa chỉ IP 23](#_Toc135858869)

[3. Cấu trúc và phân lớp địa chỉ IP. 24](#_Toc135858870)

[II. Domain Name System (DNS) 26](#_Toc135858871)

[1. Giới thiệu về DNS 26](#_Toc135858872)

[2. Cơ chế phân giải tên 27](#_Toc135858873)

[3. Phân loại Domain Name Server 27](#_Toc135858874)

[CHƯƠNG 4. PROXY SERVER 28](#_Toc135858875)

[I. Firewall 28](#_Toc135858876)

[1. Những chính sách Firewall 28](#_Toc135858877)

[2. Các loại Firewall và cách hoạt động 29](#_Toc135858878)

[2.1 Packet filtering 29](#_Toc135858879)

[2.2 Circuit relay 29](#_Toc135858880)

[2.3 Application gateway 30](#_Toc135858881)

[II. Squid Proxy 31](#_Toc135858882)

[CHƯƠNG 5. WEB SERVER 33](#_Toc135858883)

[I. Giới thiệu về Web server 33](#_Toc135858884)

[1. Giao thức HTTP. 33](#_Toc135858885)

[2. Web server và cách hoạt động 33](#_Toc135858886)

[3. Web client 34](#_Toc135858887)

[4. Web động 34](#_Toc135858888)

[II. Giới thiệu Apache 35](#_Toc135858889)

[CHƯƠNG 6. MAIL SERVER 36](#_Toc135858890)

[I. Những giao thức mail 36](#_Toc135858891)

[1. SMTP (Simple Mail Transfer Protocol) 36](#_Toc135858892)

[2. Post Office Protocol 36](#_Toc135858893)

[II. Giới thiệu về hệ thống mail 36](#_Toc135858894)

[1. Mail gateway 36](#_Toc135858895)

[2. Mail Host 36](#_Toc135858896)

[3. Mail Server 37](#_Toc135858897)

[4. Mail Client 37](#_Toc135858898)

[5. Một số sơ đồ hệ thống mail thường dùng 38](#_Toc135858899)

[5.1 SMTP (Simple Mail Transfer Protocol) 38](#_Toc135858900)

[5.2 POP3 (Post Office Protocol version 3) 39](#_Toc135858901)

[5.3 IMAP (Internet Message Access Protocol) 39](#_Toc135858902)

[III. Những chương trình mail và một số khái niệm 41](#_Toc135858903)

[1. Mail User Agent (MUA) 41](#_Toc135858904)

[2. Mail Transfer Agent (MTA) 41](#_Toc135858905)

[3. Mailbox 41](#_Toc135858906)

[4. Hàng đợi (queue) 41](#_Toc135858907)

[5. Alias 42](#_Toc135858908)

[IV. DNS và Sendmail 43](#_Toc135858909)

[1. Dịch vụ DNS. 43](#_Toc135858910)

[1.1. Giới thiệu về dịch vụ DNS. 43](#_Toc135858911)

[1.2. Hệ thống tên miền DNS 44](#_Toc135858912)

[1.3. Hoạt động của DNS server trong Linux 45](#_Toc135858913)

[1.4. Cài đặt và cấu hình dịch vụ DNS server 46](#_Toc135858914)

[2.Sendmail 48](#_Toc135858915)

[2.1.Khái niệm 48](#_Toc135858916)

[2.2.Tổng quan về Sendmail 49](#_Toc135858917)

DANH MỤC HÌNH ẢNH

[Hình 1: Hoạt động của telnet 4](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845340)

[Hình 2: Hình ảnh mô tả hoạt động kết nối TCP trong FTP 6](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845341)

[Hình 3: Sơ đồ minh hoạ 7](#_Toc135845342)

[Hình 4: Của sổ hoạt động của Traceroute 12](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845343)

[Hình 5: Cài đặt Samba 14](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845344)

[Hình 6: Cấu hình DHCP 23](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845345)

[Hình 7: Máy client đã được cấp phát địa chỉ IP 23](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845346)

[Hình 8: Hình ảnh các thành phần chình của cấu trúc 25](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845347)

[Hình 9: Hình ảnh mô tả lớp A của địa chỉ IP 26](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845348)

[Hình 10: Hình ảnh mô tả lớp B của địa chỉ IP 26](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845349)

[Hình 11: Hình ảnh mô tả lớp C của địa chỉ IP 27](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845350)

[Hình 12: Hình ảnh Firewall 29](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845351)

[Hình 13: Hình ảnh minh hoạ Email Server 38](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845352)

[Hình 14: Hình ảnh minh hoạ Mail Client 39](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845353)

[Hình 15: Mô hình sử dụng SMTP 39](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845354)

[Hình 16: Mô hình sử dụng POP3 40](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845355)

[Hình 17: Mô hình sử dụng IMAP 41](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845356)

[Hình 18: Hàng đợi 42](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845357)

[Hình 19: Cấu hình zone nghịch 48](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845358)

[Hình 20: Cấu hình zone thuận 49](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845359)

[Hình 21: Kiểm tra dịch vụ DNS 49](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845360)

[Hình 22: Sendmail 50](file:///C:\Users\Admin\Documents\IT6025.7-K16_Nhóm%2014_Nghiên%20cứu%20tìm%20hiểu%20về%20các%20dịch%20vụ%20trong%20HĐH%20Linux.docx#_Toc135845361)

LỜI NÓI ĐẦU

Linux là một hệ điều hành họ Unix miễn phí được sử dụng rộng rãi hiện nay. được viết vào năm 1991 bởi Linus Toward, hệ điều hành Linux đã thu được nhiều thành công. Là một hệ điều hành đa nhiệm, đa người dùng, linux có thể chạy trên nhiều phần cứng khác nhau. Với tính năng ổn định và mềm dẻo, linux đang dần được sử dụng nhiều trên các máy chủ cũng như các máy trạm trong các mạng máy tính. Linux còn cho phép dễ dàng thực hiện việc tích hợp nó và các hệ điều hành khác trong một mạng máy tính như windows, novell, apple… Ngoài ra, với tính năng mã nguồn mở, hệ điều hành này còn cho phép khả năng tùy biến cao, thích hợp cho các nhu cầu sử dụng cụ thể.

**NHẬN XÉT CỦA GIÁO VIÊN**

**- Chương 1: Phương – 15h**

**- Chương 2: Liễu – 20h**

**- Chương 3 + 4: Minh – 9h ngày mai 14**

**- Chương 5 + 6 + Giới thiệu linux: Trang – 19h ngày 14**

CHƯƠNG 1. CÁC TIỆN ÍCH MẠNG CỦA HỆ ĐIỀU HÀNH LINUX

# I. Telnet

## 1. Telnet

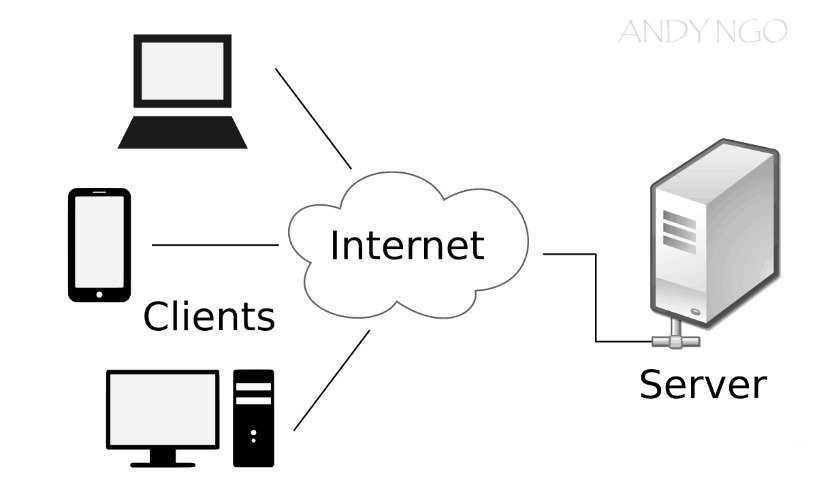
Telnet là mọi tiện ích cho phép đăng nhập vào một máy tính xa và làm việc như một máy tính tại chỗ.Telnet sử dụng giao thức TCP/IP, cổng 23

## 2. Tiện ích của telnet

Telnet cho phép một người ngồi trên một máy tính ở một khu vực nào đó truy cập vào một máy tính ở chỗ khác để điều khiển các công việc trên máy tính đó.

Máy tính ở xa, được gọi là telnet, sẽ chấp nhận nối kết telnet từ một máy TCP/ IP trên một hệ.

## 3. Hoạt động của telnet

Telnet là một giao thức client-server, dùng để mở một dòng lệnh trên một máy tính từ xa (thường là server). Telnet được dùng để ping một cổng và kiểm tra xem nó có đang mở hay không. Telnet hoạt động với trình giả lập kết nối đầu cuối ảo. Sử dụng các giao thức tiêu chuẩn để hoạt động như thiết bị đầu cuối vật lý.

Hình 1: Hoạt động của telnet

Telnet là một giao thức mạng được sử dụng để thiết lập kết nối với một máy tính từ xa. Khi kết nối được thiết lập, người dùng có thể điều khiển hoặc thực hiện các tác vụ trên máy tính từ xa như thao tác tệp, cài đặt phần mềm, quản lý hệ thống và nhiều tác vụ khác.

## 4. Yêu cầu để thực hiện được Telnet

- Để thực hiện kết nối Telnet, yêu cầu cần có:

+ Một máy tính hoặc thiết bị đầu cuối hỗ trợ Telnet.

+ Một mạng kết nối tới máy tính hoặc thiết bị đầu cuối mà bạn muốn kết nối.

+ Địa chỉ IP hoặc tên miền của máy tính hoặc thiết bị đầu cuối mà bạn muốn kết nối.

+ Tài khoản đăng nhập và mật khẩu nếu yêu cầu vào hệ thống.

- Để sử dụng Telnet một cách an toàn và ngăn chặn các cuộc tấn công mạng, cần phải cài đặt các biện pháp bảo mật như thiết lập mật khẩu đăng nhập mạnh, sử dụng kết nối mạng an toàn (như kết nối SSH ) hoặc sử dụng các ứng dụng quản lý từ xa được thiết kế riêng để thực hiện các tác vụ từ xa.

# II. FTP

## 1. Khái niệm về FTP:

- FTP là từ viết tắt của File Transfer Protocol, là một giao thức truyền tải tập tin từ máy tính này đến máy tính khác thông qua một mạng TCP ( giao thức điều khiển truyền vận/giao thức mạng ) hoặc qua mạng Internet. Thông qua giao thức TCP/IP thì giao thức này sẽ được dùng trong việc trao đổi dữ liệu trong mạng.

- Tại FTP, bạn sẽ có quyền quản lý toàn bộ các dữ liệu dạng tập tin và thư mục có trên host ngoại trừ database. Giao thức FTP được sử dụng nhiều trong việc truyền tải dữ liệu, rút gọn thời gian cũng như đáp ứng nhu cầu của việc truyền tải dữ liệu dung lượng lớn một cách nhanh chóng.

## 2. Mô hình hoạt động của FTP.

### Kết nối TCP trong FTP.

Hình 2: Hình ảnh mô tả hoạt động kết nối TCP trong FTP

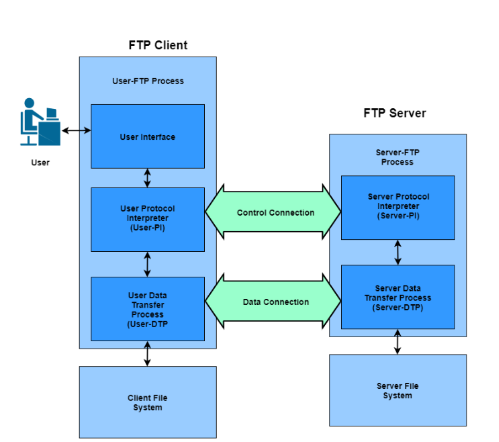
Quá trình truyền nhận dữ liệu giữa máy client và server được tạo lên từ 2 quá trình TCP logic là Control Connection và Data Connection.

+ Control Connection ( sử dụng cổng 21 – trên server ): Khi phiên làm việc bắt đầu thì trong suốt quá trình diễn ra công việc thì tiến trình này sẽ kiểm soát kết nối và chỉ thực hiện nhiệm vụ các thông tin điều khiển đi qua trong suốt quá trình truyền dữ liệu.

+ Data Connection ( sử dụng cổng 20 ): Kết nối này rất phức tạp vì các loại dữ liệu khác nhau, được thực hiện qua các quá trình truyền dữ liệu. Kết nối này mở khi có lệnh chuyển tệp và đóng tệp khi truyền xong.

### 2.2 Mô hình FTP.

- Hoạt động theo kiểu máy khách - máy chủ



Hình 3: Sơ đồ minh hoạ

* Do chức năng điều khiển và dữ liệu truyền tải bằng cách sử dụng các kênh riêng biệt nên mô hình FTP chia mỗi thiết bị thành 2 phần giao thức logic chịu trách nhiệm cho mỗi kết nối ở trên:

+ Protocol Interpreter (PI): Thành phần quản lý kênh điều khiển, phát hiện, nhận lệch và trả lời.

+ Data Transfer Process (DTP): chịu trách nhiệm gửi và nhận dữ liệu client và server.

## 3. Phương thức tạo kết nối và truyền dữ liệu trong FTP.

## 3.1 Phương thức tạo kết nối dữ liệu của FTP.

### 3.1.1. Normal (Active) Data Connections.

-- Phương thức tạo kết nối dữ liệu bình thường hay còn gọi là kết nối kênh dữ liệu dạng chủ động

- Phía Server-DTP tạo kênh dữ liệu bằng cách mở cổng kết nối tới User-DTP

- Server sử dụng cổng đặc biệt được dành riêng cho kết nối dữ liệu là cổng số 20.

### 3.1.2. Passive Data Connections.

- Phương thức tạo kết nối bị động.

- Giải quyết những thiếu sót của chế độ chủ động

+ Server được chấp nhận 1 kết nối dữ liệu được khởi tạo từ Client.

+ Server trả lời lại Client với địa chỉ IP cũng như địa chỉ cổng mà nó sẽ sử dụng. Sau đó phía Server-DTP lắng nghe trên cổng này một kết nối TCP đến từ User-DTP.

## 3.2 Phương thức truyền dữ liệu của FTP.

- Block mode: Là phương thức mang tính quy chuẩn. Với phương thức này, dữ liệu được chia thành nhiều khối nhỏ và được đóng gói thành các FTP blocks. Mỗi block chứa thông tin dữ liệu đang được gửi.

Stream mode: Là phương thức truyền tập tin không có cấu trúc dạng header. Dựa vào tính tin cậy trong việc truyền dữ liệu và thông qua kết nối TCP tới phía nhận nên chỉ ngắt kết nối là dữ liệu kết thúc.

Compressed mode: Là phương thức truyền dữ liệu sử dụng kỹ thuật nén “ run-length encoding ”. Thông tin sau khi nén sẽ được xử lý như Block mode với trường Header. Các đoạn dữ liệu bị lặp sẽ được phát hiện và loại bỏ.

## 4. Ưu điểm và nhược điểm

Ưu điểm:

* Cho phép chuyển tệp tin nếu không may mất kết nối
* Cho phép chuyển nhiều tệp tin cùng lúc
* FTP là giao thức có thời gian hoạt động lâu năm nên đa phần mọi người đều không còn xa lạ với nó.
* Các máy khách FTP có thể đồng bộ hoá được các tệp tin.
* Cho phép thêm dữ liệu vào khung chờ và lên lịch truyền.

Nhược điểm:

* Bảo mật kém
* Không phù hợp cho các tổ chức, do yêu cầu phải tạo cổng kết nối khi truyền.
* Máy chủ có khả năng bị qua mặt, gửi thông tin đến các cổng ngẫu nhiên.

# III. Ping

## 1. Câu lệnh ping

Câu lệnh ping để yêu cầu một trả lời phản hồi của một máy ở xa trên mạng. Nó dùng để kiểm tra tình trạng kết nối mạng đến máy ở xa còn hay không. Ping sử dụng giao thức ICMP. Đây là giao thức IP nên không có số cổng. ICMP được đóng gói trong một gói tin IP, nhưng được xem là một phần của lớp IP hoặc Internet.

## 2. Ping hoạt động:

* Khi thực hiện lệnh ping, hệ thống sẽ gửi một gói tin ICMP (Internet Control Message Protocol) tới một địa chỉ IP cụ thể. Gói tin này chứa một số thông tin như thời gian gửi và đánh dấu thời gian, sau đó nó sẽ chờ đợi phản hồi từ địa chỉ IP đó. Khi gói tin đến đích, địa chỉ đích sẽ trả lời bằng gửi một gói tin ICMP trả về ra đường mạng với thông tin thời điểm đó và thời gian nhận được gói tin ban đầu.
* Nếu gói tin ICMP trả về thành công, thì kết quả ping sẽ báo cáo về thời gian trả lời của gói tin đó. Nếu không, ping sẽ cho biết rằng liên kết đến địa chỉ IP đó không thành công hoặc mất mạng, không tìm thấy địa chỉ IP hoặc có một số lỗi khác.
* Ping được sử dụng rộng rãi để kiểm tra độ trung thực và độ tin cậy của các đường truyền mạng, đồng thời cũng có thể giúp định vị vị trí các thiết bị trên mạng.
* Ping được sử dụng rộng rãi để kiểm tra độ trung thực và độ tin cậy của các đường truyền mạng, đồng thời cũng có thể giúp định vị vị trí các thiết bị trên mạng.

## 3. Tính năng bao gồm:

Các tính năng chính của lệnh ping trong Linux bao gồm:

* Kiểm tra kết nối: Ping cho phép kiểm tra kết nối giữa hai thiết bị trên mạng bằng cách gửi các gói tin đến địa chỉ IP hoặc tên miền và đợi phản hồi. Nếu thiết bị nhận được phản hồi, đường truyền sẽ được coi là có kết nối. Nếu không có phản hồi, đường truyền sẽ bị mất kết nối.
* Đo thời gian: Ping cũng cho phép đo thời gian mà một phản hồi được trả về từ máy chủ. Thời gian này được hiển thị dưới dạng thời gian đáp ứng (response time), được tính bằng thời gian giữa lúc gửi yêu cầu ping và lúc nhận được phản hồi.
* Kiểm tra tốc độ: Ping cho phép kiểm tra tốc độ của đường truyền mạng bằng cách đo thời gian hoàn tất quá trình gửi và nhận các gói dữ liệu.
* Kiểm tra lỗi: Nếu ping không nhận được phản hồi trả về sau khi gửi một số gói tin, nó sẽ cung cấp thông tin lỗi để giúp xác định nguyên nhân của vấn đề.
* Tùy chọn cấu hình: Ping hỗ trợ một loạt các tùy chọn như số lượng gói tin được gửi, kích thước gói tin, khoảng thời gian giữa các gói tin, v.v. để đưa ra các yêu cầu kiểm tra kết nối phù hợp với nhu cầu cụ thể của người dùng.

Với những tính năng này, lệnh ping được sử dụng rộng rãi trong quản lý mạng và xác định các vấn đề kết nối trong các hệ thống Linux.

# IV. Traceroute

Là một công cụ xác định đường đi được sử dụng để đến đích của một gói tin. Công cụ này sử dụng giao thức ICMP, nhưng không giống như ping, xác định mọi bộ định tuyến trong đường đi. Lệnh traceroute rất hữu ích khi xử lý sự cố mạng vì nó có thể giúp chúng ta xác định vị trí các sự cố trong kết nối mạng. Traceroute thường hoạt động bằng cách gửi một loạt các gói yêu cầu echo ICM đến đích.

Trong Linux, theo mặc định traceroute sử dụng các gói UDP ở port(33434 - 33534). Lệnh traceroute hiển thị các tuyến đường thực hiện và chỉ IP và hostname của các router trên mạng.

## 1. Nguyên lý hoạt động của traceroute

Lệnh traceroute hoạt động bằng cách gửi các gói có giá trị TTL ( Time To Live-thời gian sống ) bắt đầu từ 1 và sau đó tăng từng lần một. Mỗi khi bộ định tuyến nhận được gói, nó sẽ kiểm tra trường TTL, nếu trường TTL là 1 thì nó sẽ loại bỏ gói và gửi gói lỗi ICMP chứa địa chỉ IP của nó và đây là yêu cầu của traceroute. Vì vậy, traceroute tăng dần tìm nạp IP của tất cả các bộ định tuyến giữa nguồn và đích.

## 2. Hướng dẫn chạy Traceroute trên Linux

B1: Mở Terminal.

B2: Nhập cụm từ “traceroute [hostname]” và nhấn Enter.

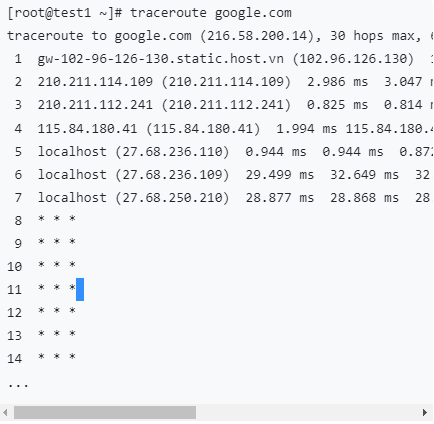
VD: traceroute messenger.com

## 3. Sử dụng Traceroute

* -6 ( traceroute -6n ipv6.google.com ): theo dõi tuyến máy chủ mạng bằng giao thức IPv6.
* -n ( traceroute -n google.com ): tắt tính năng ánh xạ địa chỉ IP và tên miền.
* -w ( traceroute -w [thời gian phản hồi ] google.com): cấu hình thời gian phản hồi
* -q (traceroute -q google.com ): cấu hình số lượng truy vấn mỗi hop.
* -f (traceroute -f [giá trị bắt đầu] google.com ): cấu hình giá trị TTL để bắt đầu.
* -m (traceroute -m [số lượng hop] google.com): thay đổi giá trị TTL. Giá trị TTL mặc định là 30, có nghĩa là chỉ có 30 hop được theo dõi theo mặc định.

**- Chú ý:**

* Các dấu sao hiển thị mất gói. Điều này có thể có nghĩa là mất mạng, lưu lượng lớn dẫn đến tắc nghẽn mạng hoặc tường lửa làm giảm lưu lượng.
* Hop: được đánh số ở phía bên trái của cửa sổ báo cáo.



Hình 4: Của sổ hoạt động của Traceroute

CHƯƠNG 2. SAMBA VÀ DHCP

# I. Samba

## 1. Giới thiệu SAMBA

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 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 số phiên bản của SMB được gọi là Samba. Samba được tạo ra bởi Andrew Tridgell 1991, được phát triển dựa trên giao thức SMB và CIFS. Samba là giao thức dùng để giao tiếp giữa Linux và windows với một số chức năng như: chia sẻ file, chia sẻ thư mục, quản lý printer, printer setting tập trung, chứng thực client login vào window domain, cung caaos Windows Internet Name Service (WINS). Có thể thấy rằng, 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 thực hiện ở 2 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 dùng chung cho nhiều người. 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:

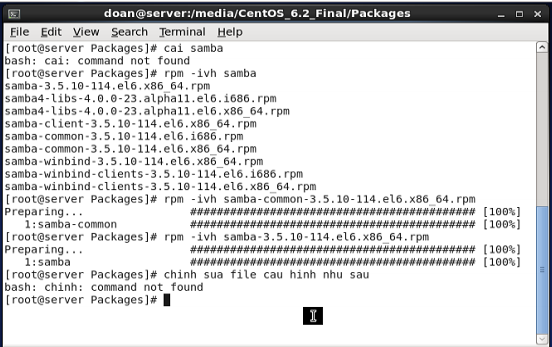
* Cấu hình dịch vụ và khởi động dịch vụ Samba.
* Khai báo tài khoản sử dụng Samba
* Truy nhập dịch vụ Samba. Các tập tin cấu hình dịch vụ:
* /etc/samba/smb.conf : tập tin cấu hình của Samba
* /etc/samba/smbpassword : chứa mật mã truy nhập của người dùng
* /etc/samba/smbusers : chứa tên hiệu cho các tài khoản của samba.

smbpasswd –a: tạo tài khoản Samba.

* smbpasswd: thay đổi thông tin tài khoản Samba.
* smbclient: truy nhập dịch vụ SBM
* smbstatus: theo dõi tình trạng kết nối hiện hành.

## 2. Cài đặt và cấu hình

Gói phần mềm Samba có thể lấy từ đĩa CD hoặc download từ mạng. Các bước cài đặt như sau:

* Kiểm tra dịch vụ Samba đã được cài đặt hay chưa: rpm –qa | grep samba
* Cài đặt nếu chưa cài đặt: thực hiện cài đặt như sau:

Hình 5: Cài đặt 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:

* Golbal setting: phần dành cho những lựa chọn toàn cục của dịch vụ.
* Sharing setting: phần dành cho khai báo tài nguyên được đưa lên mạng dùng chung.

Nhóm [global]: các tham số trong nhóm này được áp dung 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 hóa mật mã dễ 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 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
* Usename map: chỉ ra tập tin chứa các tên hiệu (alias) cho một tài khoản hệ thống. Giá trị 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
* Sercurity: 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.

**Nhóm [homes]:** nhóm này xác định các điều khiển mặc định cho truy nhập như thư mục chủ của người dùng thông qua giao thức SMB bới 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, những nhóm đó 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 hay không. Nếu hợp lệ, một tài nguyên dùng chung sẽ được dựa trên **nhóm [printers]**.

* Ngoài 3 nhóm đặc biệt được nêu trên, để thực hiện tạo các tài nguyên dùng chung khác, người dùng cần thực hiện tạo các tài nguyên này. Các nhóm dành cho các tài nguyên dùng chung, như là các mục trên hệ thống, thường đặt sau nhóm [home] và [printer] và có thể đặt tên bất kỳ.
* Comment: Mô tả tùy ý cho các 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 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 user: 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 „@‟
* Writeable:có giá trị 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.

Thí dụ dưới đây là các khai báo để thực hiện đưa một tài nguyên có tên dùng chung là mydoc (thư mục trên hệ thống là /home/shired) cho cả hai tài khoản a1, a2 và các tài nguyên thuộc nhóm nhanvien được phép truy nhập:

[mydoc]

path=/home/shired

public=no

valid users= a1 a2 @nhanvien

writable=yes

create mask=0766

* **Chú ý:**
* Thư mục được đưa lên mạng dùng chung phải cung cấp quyền tương ứng cho người dùng.
* Các tham số được chỉ ra ở nhóm tài nguyên được dùng chung sẽ có hiệu lực thay thế các tham số được thiết lập ở **nhóm [global]**.
* Trong tập tin smb.conf có thể sử dụng một số biến thay thế như %m – tên NetBIOS của máy client, %Samba – tên dịch vụ hiện hành (nếu có), %u – tên người dùng hiện hành (nếu có )… í dụ: “path = /home/%u” sẽ được phiên dịch là “path=/tmp/foo” nếu tài khoản foo thực hiện truy nhập.
* **Chia sẻ thư mục:**
* Sau khi lập cấu hình mặc định cho server Samba, bạn có thể tạo ra nhiều thư mục dùng chung (thư mục chia sẻ) và quyết định xem cá nhân nào, hoặc nhóm nào được phép sử dụng chúng.
* Ví dụ bạn muốn thư mục plaisir chỉ dành riêng cho user leduan mà thôi. Bạn cần viết ra một đoạn mới và ghi các thông tin cần thiết vào: khai báo user, đường dẫn đến thư mục, cùng với thông tin cấu hình cho server SMB như sau:

[pladir]

comment = Pla's remote source code directory

path = /usr/local/src

valid users = leduan

browsable = yes

public = no

writable = yes

create mask = 0700

Đoạn trên đây đã tạo ra một thư mục chia sẻ mang tên plasdir. Đường dẫn đến thư mục này trên server tại chỗ là /usr/local/src. Vì mục browseable được khai báo "yes", danh sách duyệt mạng sẽ có tên là plasdir. Nhưng vì mục public lại là "no" nên chỉ có user tên là lan\_anh mới có quyền dùng Samba để vào ra thư mục. Muốn cho ai được truy cập, bạn chỉ cần liệt kê họ tại thư mục valid users.

## 3. Quản trị tài khoản Samba

Để có thể sử dụng dịch vụ Samba(ngoại trừ trường hợp cho phép mọi người dùng truy nhập), người dùng cần phải thiết lập tài khoản người dùng Samba. Tài khoản người dùng Samba là một tài khoản được xây dựng dựa trên tài khoản hệ thống (tài khoản của Linux), do vậy, phải có tài khoản người dùng hệ thống người dùng mới có thể tạo được tài khoản samba.

* **Tạo tài khoản Samba**:
* Samba sử dụng database người dùng riêng để chứng thực user,password khi người dùng truy cập vào samba chứ không dùng database người dùng trong file passwd của hệ thống.
* Samba phiên bản 3.0 trở lên, không còn dùng lệnh smbadduser nữa mà sử dụng cú pháp sau để tạo tài khoản samba:

**smbpasswd –a**

Ví dụ: lệnh sau cho phép tạo tài khoản Samba có tên a3 ứng với tài khoản a3 của linux:

**[root@server2]# smbpasswd –a a3**

* **Quản trị tài khoản Samba – smbpasswd:**
* Lệnh smbpasswd được sử dụng để quản lý các tài khoản Samba. Tiện ích này cho phép xóa tài khoản, khoá tài khoản cũng như cho phép thay đổi mật mã đăng nhập vào dịch vụ Samba.
* Cú pháp lệnh:

**smbpasswd [option] [username]**

Trong đó username là tên tài khoản người dùng Samba. Trong trường hợp không có đối số username, lệnh này tác động tới người dùng hiện hành.

Lệnh smbpasswd khi sử dụng không có lựa chọn (option), nó cho phép thay đổi mật mã truy nhập của tài khoản Samba username.

Một số lựa chọn của lệnh như sau:

**-x**: Xoá người dùng Samba username khỏi tập tin /etc/samba/smbpasswd.

**-d** : Vô hiệu hóa tài khoản Samba của tài khoản username, bằng cách ghi cờ “D” vào trong phần điều khiển tài khoản trong tập tin smbpasswd.

**-e** : Bật lại tài khoản Samba đã bị khóa trước đó, bằng cách gỡ bỏ cờ „D‟ trong tập tin smbpasswd.

**-n** : Cho phép username sử dụng mật mã trống (không mật mã). Chú ý rằng, tham số null passwords =yes phải được thiết lập trong nhóm [global] ở tập tin /etc/samba/smb.conf.

Ví dụ: Để xóa tài khoản a3 của Samba, người dùng thực hiện lệnh sau:

**# smbpasswd –x a3**

## 4. Sử dụng dịch vụ Samba

* Truy nhập dịch vụ SMB - lệnh smbclient
* Việc truy nhập dịch vụ Samba của Linux từ các máy tính Windows được thực hiện tương tự như việc truy nhập các thông tin được chia sẻ giữa các máy tính Windows.
* Các hệ thống Linux có thể truy nhập hệ dịch vụ Samba bằng cách thi hành lệnh smbclient.smbclient, hoạt động giống như FTP, cho phép truy nhập hệ thống sử dụng giao thức SMB. Nhiều lệnh smbclient tương tự như FTP, như là lệnh mget để truyền tập tin, lệnh del để xóa tập tin.
* Cú pháp lệnh: smbclient //servername/service [options]
* Trong đó servername là tên (hay địa chỉ IP) của máy chủ Samba, service là tên thư mục được chia sẻ (chính là tên của nhóm được khai báo trong tập tin cấu hình của Samba /etc/samba/smb.conf).
* Một số lựa chọn hay dùng của lệnh:
* U username: Tên tài khoản đăng nhập sử dụng Samba
* L host: Liệt kê danh sách các thư mục được chia sẻ trên máy có địa chỉ IP hay tên máy là host.
* N: Không xuất hiện lời nhắc yêu cầu nhập mật mã. Thường dùng trong trường hợp thư mục được chia sẻ là public.
* Một khi đã kết nối được với máy chủ Samba, Samba xuất hiện lới nhắc như sau: **smb: \>**
* Tại lời nhắc này, người dùng có thể thi hành các lệnh của smbclient. Phần lớn những lệnh này tương tự như những lệnh của ftp ( để gửi và lấy tập tin về, như là get, mget, put, mput) và giống như những lệnh về quản lý tập tin của Linux (như là ls,rm, cd…). Để biết được các lệnh của smbclient. Tại lời nhắc này người dùng dùng lệnh?.
* Gắn kết một tài nguyên dùng chung vào hệ thống tập tin (mount & umount)
* Việc truy nhập các tập tin dùng chung thông qua lệnh smbclient là khá bất tiện và không được linh hoạt. trong trường hợp thường xuyên có các thao tác trên thư mục dùng chung, người dùng có thể gắn kết thư mục được share trên mạng đó vào hệ thống tập tin cục bộ để có thể sử dụng như một thư mục bình thường. lệnh được sử dụng để thực hiện tác vụ này là lệnh mount với cú pháp như sau:

**mount [-t type] [-o options] device dir**

* **Trong đó:**

Type là kiểu của thiết bị cần mount.

Ví dụ: lệnh dưới đây thực hiện gắn kết thư mục dùng chung có tên là software trên máy có địa chỉ 192.168.1.202 vào thư mục /home/software/ trên hệ thống tập tin với quyền của tài khoản username=administrator, password=123456:

**[root@server2~]#mount –t cifs -ousername=administrator, password=123456**

**//192.168.1.202/software /home/software**

* Để có thể gở bỏ gắn kết thư mục dùng chung, người dùng sử dụng lệnh umount với cú pháp sau:umount mountpoint .
* **Trong đó:** mountpoint là vị trí (thư mục) trên hệ thống tập tin cục bộ mà thư mục dùng chung được gắn kết vào. Ví dụ: gỡ bỏ gắn kết của thư mục software vừa thực hiện gắn kết ở thí dụ trên:

**[root@server2 ~]# umount /home/software**

* Option là các tùy chọn đối với thiết bị được mount.
* Device là tên thiết bị cần mount.
* Dir là đường dẫn đến mount point.

# II. DHCP

## 1. Giới thiệu dịch vụ DHCP

* Hệ thống cần cung cấp IP mỗi máy tính để các máy này có thể liên lạc với nhau. Với mô hình mạng tương đối nhỏ, việc cấp IP tương đối dễ dàng. Nhưng với một mô hình mạng lớn thì việc cung cấp IP trở nên khó khăn. Vì vậy cần phải có một dịch vụ cung cấp IP tự động cho các máy client trong hệ thống mạng.
* DHCP là một dịch vụ cung cấp IP tự động cho các client.
* Hoạt động theo mô hình Client – server.
* Ngoài ra DHCP còn có nhiều tính năng khác cho client như: cung cấp địa chỉ của máy tính dùng để giải quyết tên miền DNS, địa chỉ của một Gateway route.
* Cơ chế sử dụng các thông số mạng được cấp phát động có ưu điểm hơn so với cơ chế khai báo tĩnh các thông số mạng như:
* Khắc phục được tình trạng đụng địa chỉ IP và giảm chi phí quản trị cho hệ thống mạng.
* Giúp cho các nhà cung cấp dịch vụ (ISP) tiết kiệm được số lượng địa chỉ IP thật (public IP). - Phù hợp với máy tính thường xuyên di chuyển qua lại giữa các mạng.
* Kết hợp với hệ thống mạng không dây (wireless) cung cấp các điểm Hotspot như: nhà ga, sân bay, trường học…

## 2. Nguyên tắc hoạt động

Giao thức DHCP làm việc theo mô hình client/server. Theo đó, quá trình tương tác giữa DHCP client và server diễn ra theo các bước sau:

* Khi máy client khởi động, máy sẽ gửi broadcast gói tin DHCPDISCOVER, yêu cầu một server phục vụ cho mình. Gói tin này cũng chứa địa chỉ MAC của máy client.
* Các máy server trên mạng khi nhận được gói tin yêu cầu đó, nếu còn khả năng cung cấp địa chỉ IP, đều gửi lại cho máy client gói tin DHCPOFFER, đề nghị cho thuê một địa chỉ IP trong một khoảng thời gian nhấp định, kèm theo là một subnet mask và địa chỉ của server. Server sẽ không cấp phát địa chỉ IP vừa đề nghị cho những client khác trong suốt quá trình thương thuyết.
* Máy client sẽ lựa chọn một trong những lời đề nghị (DHCPOFFER) và gửi broadcast lại gói tin DHCPREQUEST 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 client khác.
* Máy server được client chấp nhận sẽ gửi ngược lại một gói tin DHCPACK như là một lời xác nhận, cho biết là địa chỉ IP đó, subnet mask đó và thời hạn sử dụng đó sẽ chính thức được áp dụng. Ngoài ra server còn gửi kèm theo những thông tin cấu hình bổ sung như địa chỉ gateway mặc định, địa chỉ DNS server.

## 3. Các thông số trong cấu hình DHCP

Option: Dùng để cung cấp các yếu tố cho phía client như địa chỉ IP, địa chỉ subnet mask, địa chỉ Gateway, địa chỉ DNS…

Scope: một đoạn địa chỉ được quy định trước trên DHCP server dùng để gán cho các máy client.

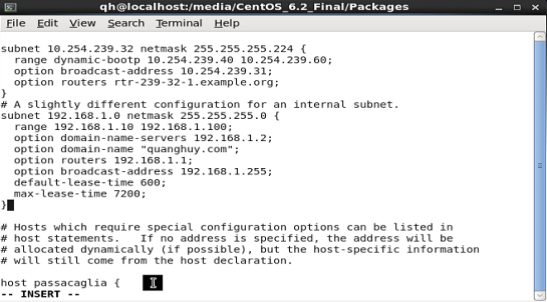
Reservation: là những đoạn địa chỉ dùng để đánh trong một số scope đã được quy định ở trên.

Lease: thời gian “cho thuê” địa chỉ IP đối với mỗi client.

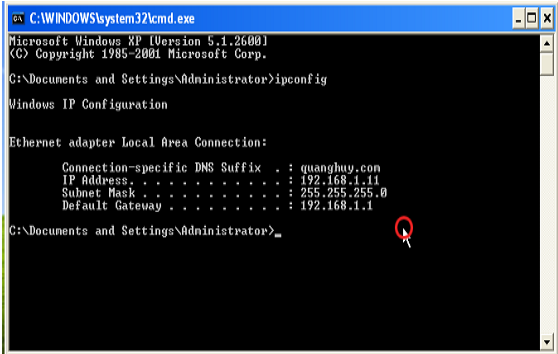
## 4. Cài đặt và cấu hình dịch vụ DHCP.

Để cấu hình dịch vụ DHCP, bạn cần phải cài đặt gói dịch vụ DHCP. Có 2 cách cài đặt.

Cách 1: cài đặt từ đĩa cd #rpm –ivh dhcp-\*.rpm (với \* là phiên bản của gói dịch vụ).

Cách 2: cài đặt bằng cách tải trên mạng #yum –y install dhcp Kiểm tra gói cài đặt: # rpm –qa|grep dhcp. Sau khi cài đặt, ta cấu hình như sau:

Hình 6: Cấu hình DHCP

Sau khi cấu hình file dhcpd.conf, thực hiện lệnh service dhcpd start để bật dịch vụ. Để kiểm tra dịch vụ đã cấp phát ip thành công hay chưa, ta sang máy Xp gõ lệnh ipconfig để kiểm tra.

Hình 7: Máy client đã được cấp phát địa chỉ IP

CHƯƠNG 3. NETWORKING.

# I. Địa chỉ IP

## 1. IP tĩnh và động

IP tĩnh:là một địa chỉ IP sẽ không thay đổi theo thời gian, địa chỉ cố định dành riêng cho một hoặc một nhóm người dùng Internet. Thông thường **IP tĩnh** sẽ được cấp cho một máy chủ sử dụng với một mục đích riêng biệt: máy chủ mail, máy chủ web…giúp người dùng không bị gián đoạn trong quá trình truy cập.

IP động: là một địa chỉ IP được gán tự động cho một thiết bị mạng khi thiết bị này kết nối với mạng. Địa chỉ IP thường được cấp phát từ một nhóm các địa chỉ IP có sẵn trong mạng. **IP động** có tính linh hoạt cao, dễ cài đặt và quản lý. Bên cạnh đó, nó cũng không giới hạn số lượng thiết bị kết nối. Bởi các thiết bị này không cần ngắt kết nối để giải phóng IP khi có thiết bị mới truy cập.

## 2. Phân phối địa chỉ IP

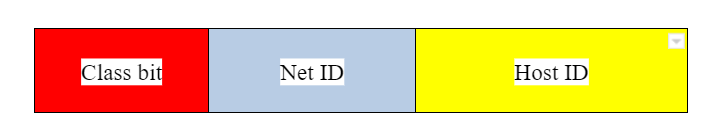
Các nhà cung cấp dịch vụ Internet (ISP) thường áp dụng phương pháp sử dụng mạng con và DHCP (Giao thức cấu hình máy chủ động):

* Mạng con: là phương pháp chia mạng thành các mạng nhỏ hơn để quản lý dễ dàng hơn và phân phối địa chỉ IP cho các thiết bị kết nối. Các địa chỉ IP được chia thành các mạng con khác nhau để giúp người quản trị mạng dễ dàng phân biệt và quản lý các thiết bị kết nối trong mạng.
* DHCP: là giao thức cấp phát địa chỉ IP tự động cho các thiết bị kết nối vào mạng. Khi thiết bị được kết nối vào mạng, nó yêu cầu một địa chỉ IP từ máy chủ DHCP của mạng và máy chủ sẽ cấp phát cho thiết bị một địa chỉ IP khả dụng trong mạng. Quá trình cấp phát địa chỉ IP cho các thiết bị trong mạng thường được cài đặt và quản lý bởi người quản trị mạng.

Ngoài ra, người quản trị mạng cũng có thể cấp phát các địa chỉ IP tĩnh cho các thiết bị trong mạng theo cách thủ công. Việc cấp phát địa chỉ IP tĩnh sẽ giúp cho việc quản lý mạng linh hoạt hơn và giải quyết được một số vấn đề về bảo mật mạng

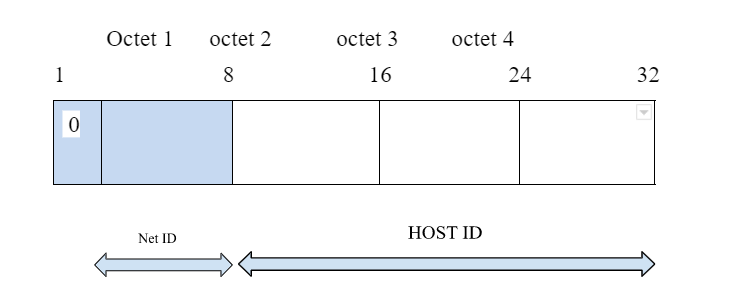
## 3. Cấu trúc và phân lớp địa chỉ IP.

Các địa chỉ này được viết dưới dạng một tập hợp bộ số (octet) ngăn cách nhau bằng dấu chấm (.). Nếu biết địa chỉ IP của một website, thì có thể nhập vào trình duyệt để mở mà không cần viết tên miền. Hiện nay, có 2 phiên bản là IPv4 và IPv6, trong đó IPv4 là chuẩn đang dùng rộng rãi với độ dài là 32 bit. Nhưng tương lai, khi quy mô của mạng mở rộng, người ta có thể dùng đến IPv6 là chuẩn 128 bit. Xét trong phiên bản IPv4, địa chỉ này được chia làm 4 bộ, mỗi bộ 8 bit (viết theo dạng nhị phân gồm các số 0 và 1) được đếm từ trái sang phải.

Cấu trúc được thể hiện 3 thành phần chính là:

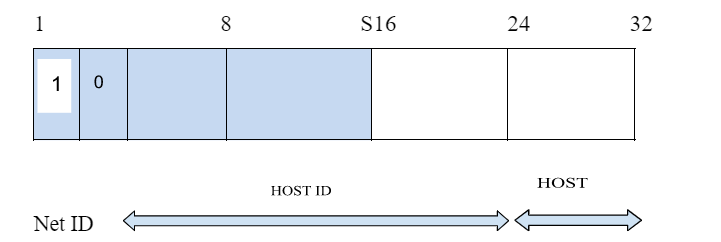
Hình 8: Hình ảnh các thành phần chình của cấu trúc

* **Trong đó:**
* Class bit: bit nhận dạng lớp, dùng để xác định địa chỉ đang ở lớp nào.
* NetID: địa chỉ của mạng
* Host ID: địa chỉ của máy

Địa chỉ IP được chia thành 5 lớp: A, B, C, D, E. trong đó lớp D, E chưa được dùng tới. Dưới đây ta phân tích đặc điểm của lớp A, B, C với hệ đếm nhị phân.Lớp A:

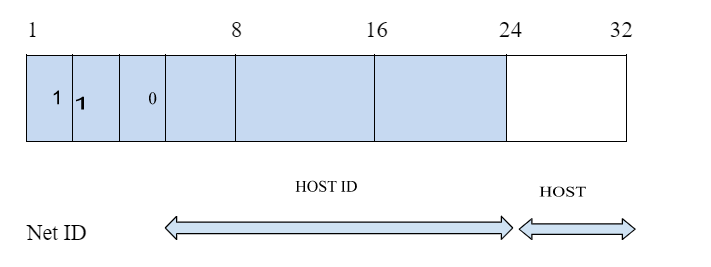
Hình 9: Hình ảnh mô tả lớp A của địa chỉ IP

Bits nhận dạng thứ nhất của lớp này là 0, 7 bit còn lại dành cho Net ID, phần tiếp theo dành cho Host ID. Lớp A áp dụng khi địa chỉ network ít và địa chỉ máy chủ nhiều.tính ra, ta được tối đa 126 mạng và mỗi mạng có thể hỗ trợ tối đa 167.777.214 máy chủ. Vùng địa chỉ lý thuyết tính theo hệ đếm thập phân từ 0.0.0.0 đến 127.0.0.0.

Lớp B:

Hình 10: Hình ảnh mô tả lớp B của địa chỉ IP

Bits nhận dạng của lớp B là 10, 14 bits còn lại dành cho Net ID, phần tiếp theo dành cho Host ID. Lớp này lớp này áp dụng khi địa chỉ mạng và địa chỉ máy chủ ở mức vừa. Tính ra, ta được tối đa 16.382 mạng, mỗi mạng phục vụ tối đa 65.534 máy chủ. Vùng địa chỉ lý thuyết tính theo hệ đếm thập phân từ 128.0.0.0 đến 191.255.0.0.

Lớp C:

Hình 11: Hình ảnh mô tả lớp C của địa chỉ IP

* Bits nhận dạng của lớp C là 110, 21 bit còn lại dành cho Net ID, phần tiếp theo dành cho Host ID. Lớp này áp dụng khi địa chỉ mạng nhiều và địa chỉ máy chủ ít. Tính ra, ta được tối đa 2.097.150 mạng, mỗi mạng phục vụ tối đa 254 máy chủ. Vùng địa chỉ lý thuyết tính theo hệ đếm thập phân từ 192.0.0.0 đến 223.255.255.0.

# II. Domain Name System (DNS)

## 1. Giới thiệu về DNS

DNS là từ viết tắt trong tiếng Anh của Domain Name System, là Hệ thống tên miền được phát minh vào năm 1984 cho Internet, chỉ một hệ thống cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền. Hệ thống tên miền (DNS) là một hệ thống đặt tên theo thứ tự cho máy vi tính, dịch vụ, hoặc bất kỳ nguồn lực tham gia vào Internet. Nó liên kết nhiều thông tin đa dạng với tên miền được gán cho những người tham gia. Quan trọng nhất là, nó chuyển tên miền có ý nghĩa cho con người vào số định danh (nhị phân), liên kết với các trang thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị khắp thế giới.

## 2. Cơ chế phân giải tên

Vai trò của Root name server: là máy chủ quản lý các name server ở mức toplevel domain

Khi có truy vấn về một tên miền nào đó thì root name server phải cung cấp tên và địa chỉ IP của name server quản lý top-level domain mà tên miền này thuộc vào.

Phân giải nghịch: Phần không gian này có tên miền là :.in-addr.arpa.có chức năng phân giải ip thành tên.

## 3. Phân loại Domain Name Server

Primary server: Nơi xác thực thông tin về địa chỉ IP và tên miền chính thức.

Secondary server: Nơi lưu trữ dự phòng cơ sở dữ liệu tên miền cho các Primary server.

Caching only server: Nơi lưu trữ các địa chỉ tên miền trên bộ nhớ cache

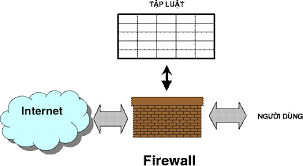
nhằm tăng tốc truy vấn tên miền.

CHƯƠNG 4. PROXY SERVER

# I. Firewall

## 1. Những chính sách Firewall

Firewall điều khiển truy cập bằng việc cho phép hoặc từ chối các dòng dữ liệu vào/ra, dựa trên một tập luật, mà ta thường gọi là chính sách Firewall.



Hình 12: Hình ảnh Firewall

Chính sách firewall thường được cấu hình dựa trên tri thức của người quản trị và trên cơ sở những phát biểu trong chính sách an ninh của một tổ chức. Chính sách firewall bao gồm một tập các luật, nó xác định một hành động từ chối (deny) hoặc chấp nhận (accept) đối với một gói tin đi qua firewall. Mỗi luật trong firewall thường có 7 thuộc tính mô tả:

<direction>: Chiều đi của gói tin ( vào hoặc ra )

<protocol>: Giao thức TCP hoặc UDP

<source port>: Cổng nguồn

<source IP>: địa chỉ IP nguồn hoặc một dải địa chỉ IP nguồn

<destination IP>: địa chỉ IP đích hoặc một dải địa chỉ IP đích

<destination port>: cổng đích

<action>: Hành động chấp nhận hoặc từ chối.

## 2. Các loại Firewall và cách hoạt động

Có 3 loại Firewall trên hệ điều hành Linux:

### 2.1 Packet filtering

Mọi lưu thông mạng đều được gửi dạng packet. Một lượng lớn lưu thông được chia ra thành những phần nhỏ dễ xử lý và được tập hợp lại khi đến đích. Packet header chứa thông tin cách đến và nơi đến. Và thông tin này chính xác là những thông tin firewall packet filtering dùng. Nói cách khác, firewall này lọc theo thông tin trong header, không phải nội dung packet. Filter dựa trên:

* Cho phép hoặc không cho phép packet dựa trên địa chỉ IP nguồn/đích
* Cho phép hoặc không cho phép packet dựa trên cổng nguồn/đích
* Cho phép hoặc không cho phép packet dựa trên giao thức
* Cho phép hoặc không cho phép packet dựa trên cờ hiệu của giao thức xác định

**Điểm mạnh:**

* Cài đặt dễ và đơn giản
* Có thể cảnh báo trước các cuộc tấn công
* Ngăn cản SYN Flood attack

**Điểm yếu:**

* Thông tin địa chỉ trong gói có thể làm giả
* Dữ liệu hoặc request trong gói được phép có thể chứa dữ liệu không mong muốn mà kẻ tấn công có thể dùng để khai thác các lỗi đã biết của các dịch vụ nằm trên hoặc nằm sau firewall
* Thường là nguồn gốc của lỗi.

Ví dụ: IPtables, Ipchains, SmoothWall

### 2.2 Circuit relay

Firewall kiểm tra kết nối trước khi trao đổi dữ liệu. Nó không chỉ kiểm tra header của packet mà còn xác định kết nối giữa hai đầu có hợp lệ không, dựa theo các quy tắc cấu hình, trước khi mở session và cho phép trao đổi dữ liệu. Filter dựa trên:

* Địa chỉ IP nguồn/đích
* Cổng nguồn/đích
* Khoảng thời gian
* Giao thức
* User
* Password

Mọi lưu thông đều được kiểm tra và theo dõi, những lưu thông không mong đợi có thể bị loại bỏ.

**Điểm yếu:** Hoạt động ở tầng Transport, có thể cần thay đổi đáng kể các chương trình cung cấp tính năng transport bình thường.

### 2.3 Application gateway

Application gateway là proxy cho ứng dụng, trao đổi dữ liệu với hệ thống ở xa, đại diện cho client. Nó tách biệt khỏi thế giới bên ngoài bằng cách nằm sau DMZ (De-Militarized Zone – Vùng dân sự: Phần mạng riêng tư có thể thấy thông qua firewall ) hoặc sau một firewall không cho phép kết nối từ bên ngoài. Nó dựa trên:

* Cho phép hoặc cấm dựa trên địa chỉ IP nguồn/đích
* Dựa trên nội dung packet
* Giới hạn quyền truy cập tập tin hoặc phần mở rộng.

**Điểm mạnh:**

* Có thể cache các tập tin, tăng cường hiệu quả
* Log chi tiết mọi kết nối
* Thích ứng tốt ( vài proxy server có thể chia sẻ dữ liệu cache)
* Không truy cập trực tiếp từ bên ngoài
* Thay thế ngay tức thì nội dung packet

**Điểm yếu:**

+ Cấu hình phức tạp: Gateway ứng dụng được xem là giải pháp an toàn nhất vì nó không cần chạy bằng [root](http://www.gocit.vn/bai-viet/tag/root/) và những máy sau lưng nó không thể được truy cập từ Internet.

Ví dụ về một số gateway ứng dụng: Squid.

# II. Squid Proxy

* Squid là một chương trình internet proxy-caching có vai trò tiếp nhận các yêu cầu từ các client và chuyển cho Internet server thích hợp. Đồng thời, nó sẽ lưu lên đĩa những dữ liệu được trả về từ Internet server – gọi là caching. Chương trình này dùng để cấu hình Proxy Server. Vì vậy ưu điểm của squid là khi một dữ liệu mà được yêu cầu nhiều lần thì Proxy Server sẽ lấy thông tin từ cache trả về cho client. Điều này làm cho tốc độ truy xuất Internet nhanh hơn và tiết kiệm băng thông. Squid dựa trên những đặc tả của giao thức HTTP nên nó chỉ là một HTTP Proxy. Do đó Squid chỉ có thể là một proxy cho những chương trình mà chúng dùng giao thức này để truy cập Internet.
* Để cài đặt và cấu hình Squid trên Linux, làm theo các bước sau:

1. Cập nhật kho lưu trữ gói:

* Đối với Debian/Ubuntu: sudo apt update
* Đối với CentOS/Fedora: sudo dnf update hoặc sudo yum update

1. Cài đặt Squid

* Đối với Debian/Ubuntu: sudo apt install squid
* Đối với CentOS/Fedora: sudo dnf install squid hoặc sudo yum install squid

1. Cấu hình Squid:

* Tệp cấu hình chính nằm tại /etc/squid/squid.conf.
* Sao lưu cấu hình ban đầu: sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.bak
* Chỉnh sửa tệp cấu hình: sudo nano /etc/squid/squid.conf
* Cấu hình các thiết lập cần thiết như kiểm soát truy cập, cổng, kích thước bộ đệm, v.v.
* Lưu thay đổi và thoát khỏi trình chỉnh sửa.

1. Khởi động và kích hoạt Squid:

* Đối với hệ thống dựa trên systemd: sudo systemctl start squid và sudo systemctl enable squid
* Đối với hệ thống init SysV: sudo service squid start và sudo chkconfig squid on

1. Điều chỉnh cài đặt tường lửa:

* Mở các cổng cần thiết (mặc định là TCP 3128) trong cấu hình tường lửa để cho phép kết nối đến.

1. Kiểm tra Squid:

* Đặt thiết bị client hoặc trình duyệt của bạn để sử dụng máy chủ proxy Squid.
* Truy cập các trang web hoặc thực hiện các hoạt động mạng để xác minh tính năng của Squid.

CHƯƠNG 5. WEB SERVER

# I. Giới thiệu về Web server

# 1. Giao thức HTTP.

Giao thức HTTP (Hypertext Transfer Protocol) là giao thức truyền tải dữ liệu giữa các máy tính trên mạng Internet. HTTP hoạt động dựa trên mô hình giao tiếp Client-Server, trong đó máy tính yêu cầu (Client) gửi các yêu cầu đến máy chủ (Server) và nhận lại các phản hồi từ máy chủ sau khi xử lý yêu cầu.

HTTP được sử dụng để truyền tải các tài liệu HTML, nhưng cũng có thể được sử dụng để truyền tải bất kỳ loại dữ liệu nào, bao gồm hình ảnh, âm thanh và video. Giao thức này hoạt động trên cổng mặc định là 80 của máy chủ.

Các phiên bản của HTTP được phát triển với các tính năng mới và cải tiến, bao gồm HTTP/1.0, HTTP/1.1 và HTTP/2. Một trong những tính năng mới của HTTP/2 là hỗ trợ tính năng "multiplexing", cho phép truyền tải nhiều loại tài liệu khác nhau trên cùng một kết nối truyền tải.

HTTP là một giao thức stateless, có nghĩa là mỗi lần yêu cầu gửi đến máy chủ đều là một phiên làm việc mới và độc lập với các yêu cầu trước đó. Để giữ lại thông tin về trạng thái, các phiên bản HTTP mới sử dụng các phương thức như Cookie hoặc Session.

# 2. Web server và cách hoạt động

Ban đầu Web Server chỉ phục vụ các tài liệu HTML và hình ảnh dơn giản. Tuy nhiên, đến thời điểm hiện tại nó có thể làm nhiều hơn thế. Đầu tiên xét Web server ở mức độ cơ bản, nó chỉ phục vụ các nội dung tĩnh. Nghĩa là khi Web server nhận 1 yêu cầu từ Web browser: http://www.hcmuns.edu.vn/index.html, nó sẽ ánh xạ đường dẫn này (Uniform Resource Locator - URL) thành một tập tin cục bộ trên máy Web server. Máy chủ sau đó sẽ nạp tập tin này từ đĩa và đưa nó thông qua mạng đề Web browser của người dùng. Web browser và web server sử dụng giao thức HTTP trong quá trình trao đổi dữ liệu. Các trang tài liệu HTML là một bản thô (raw text). Chúng chứa các thẻ định dạng (HTML tag).

Trên cơ sở phục vụ những trang web tĩnh đơn giản này, ngày nay Web Server đã được phát triển với nhiều thông tin phức tạp hơn được chuyển giữa Web Server và Web Browser, trong đó quan trọng nhất có lẽ là nội dung động (dynamic content). Với phiên bản đầu tiên, Web Server hoạt động theo mô hình sau:

* Tiếp nhận các yêu cầu từ browsers.
* Trích nội dung từ đĩa.
* Chạy các chương trình CGI.
* Truyền dữ liệu ngược lại cho client.
* Chạy càng nhanh càng tốt.

Điều này sẽ thực hiện tốt đối với các Web sites đơn giản, nhưng server sẽ bắt đầu gặp phải vấn đề khi có nhiều người truy cập hoặc có quá nhiều trang web động phải tốn thời gian để tính toán cho ra kết quả.

# 3. Web client

Một Web client (khách hàng web) là một ứng dụng hoặc trình duyệt web được sử dụng để truy cập và duyệt các trang web trên mạng Internet. Web client là một yếu tố quan trọng trong kiến trúc Client/Server trên web, trong đó web server cung cấp các tài nguyên và dữ liệu trên web, và web client truy cập và hiển thị các nội dung này cho người dùng cuối.

Các trình duyệt web phổ biến bao gồm Google Chrome, Mozilla Firefox, Microsoft Edge, và Apple Safari. Các ứng dụng web-based (chạy trên trình duyệt web) cũng là một loại web client, nhưng chúng không chỉ đơn giản là trình duyệt web mà còn cung cấp các tính năng độc lập với trình duyệt như các công cụ quản lý tài khoản người dùng, cửa sổ pop-up, và các kết nối với các ứng dụng khác như Google Drive và Dropbox.

Web client tương tác với web server bằng cách gửi yêu cầu HTTP đến web server và đợi phản hồi trả về. Trong quá trình này, web client có thể truyền tải các thông tin về người dùng đến web server, bao gồm thông tin về trình duyệt và hệ điều hành được sử dụng, IP của người dùng và cookies.

## 4. Web động

Web động (Dynamic web) là một hình thức phát triển ứng dụng web, trong đó các nội dung được tạo ra hoặc sửa đổi dựa trên thời gian thực, yêu cầu của người dùng hay thông tin được cập nhật từ các nguồn tài nguyên khác. Web động thường được phát triển bằng các ngôn ngữ lập trình web như PHP, Python, Ruby và Javascript.

Web động thường được phát triển để cung cấp các tính năng tương tác, chẳng hạn như các biểu mẫu trực tuyến có thể gửi dữ liệu đến máy chủ, các trang quản lý người dùng và các cửa hàng trực tuyến. Để hoạt động, các trang web động thường cần sử dụng một cơ sở dữ liệu để lưu trữ và quản lý thông tin, và các tập lệnh kết nối đến cơ sở dữ liệu thông qua các kết nối SQL.

Web động có thể được phát triển bằng các khung công tác như Ruby on Rails, Laravel và Flask, cung cấp các tính năng và khả năng phát triển tốt hơn cho các ứng dụng web động. Web động cũng thường sử dụng các công nghệ như AJAX (Asynchronous Javascript And XML) để cập nhật dữ liệu trên trang mà không cần tải lại trang hoàn toàn, mang lại nhiều trải nghiệm tốt hơn cho người dùng và giảm tải cho máy chủ.

Một trong các nội dung động (thường gọi tắt là Web động) cơ bản là các trang Web được tạo ra để đáp ứng các dữ liệu nhập vào của người dùng trực tiếp hay gián tiếp.

Cách cổ điển nhất được dùng phổ biến nhất cho việc tạo nội dung động là sử dụng Common Gateway Interface (CGI). Cụ thể là CGI định nghĩa cách thức Web server chạy một chương trình cục bộ, sau đó nhận kết quả và trả về cho Web browser của người dùng đã gửi yêu cầu.

Web browser thực sự không biết nội dung của thông tin là động, bởi vì CGI về cơ bản là một giao thức mở rộng của Web Server.

Một giao thức mở rộng nữa của HTTP là HyperText Transmission Protocol Secure (HTTPS) dùng để bảo mật các thông tin “nhạy cảm” khi chuyển chủng xuyên qua mạng.

# II. Giới thiệu Apache

Apache là một phần mềm có nhiều tính năng mạnh và linh hoạt dùng để làm Web Server.

* Hỗ trợ đầy đủ những giao thức HTTP trước đây như HTTP/1.1.
* Có thể cấu hình và mở rộng với những module của công ty thứ ba.
* Cung cấp source code đầy đủ với license không hạn chế.
* Chạy trên nhiều hệ điều hành như Windows NT/9x, Netware 5.x, OS/2 và trên hầu hết các hệ điều hành Unix.

CHƯƠNG 6. MAIL SERVER

# I. Những giao thức mail

## 1. SMTP (Simple Mail Transfer Protocol)

SMTP là giao thức tin cậy chịu trách nhiệm phân mail. Nó chuyển mail từ hệ thống mạng này sang hệ thống mạng khác, chuyển mail trong hệ thống mạng nội bộ. Giao thức SMTP được định nghĩa trong RFC 821, SMTP là một dịch vụ tin cậy, hướng kết nối (connection-oriented) được cung cấp bởi giao thức TCP (Transmission Control Protocol), nó sử dụng số hiệu tổng cổng (well-known port) 25.

## 2. Post Office Protocol

Có hai phiên bản của POP được sử dụng rộng rãi là POP2, POP3.POP2 được định nghĩa trong RFC 937, POP3 được định nghĩa trong RFC 1725.POP2 sử dụng 109 và POP3 sử dụng Port 110. Các câu lệnh trong hai giao thức này không giống nhau nhưng chúng cùng thực hiện chức năng cơ bản là kiểm tra tên đăng nhập và password của user và chuyển mail của người dùng từ server tới hệ thống đọc mail cục bộ của user. Trong khi đó tập lệnh của POP3 hoàn toàn khác với tập lệnh của POP2.

# II. Giới thiệu về hệ thống mail

## 1. Mail gateway

Email Gateway là một loại máy chủ bảo vệ các Email Server. Nó hoạt động như một "cổng" mà qua đó tất cả các email - đến và đi - đi qua. Mỗi email sẽ được quét để tìm nội dung độc hại hoặc các liên kết có hại, cũng như bất kỳ tài liệu đính kèm nào chứa thông tin độc quyền hoặc bí mật của doanh nghiệp. Email Gateway không lưu trữ bất kỳ tài khoản email hoặc hộp thư đến của người dùng.

## 2. Mail Host

Email Hosting là dịch vụ mà trong đó các nhà cung cấp sẽ thuê các máy chủ email (email server) cho người dùng của mình.

Email Hosting cung cấp cho doanh nghiệp một hệ thống quản lý tốt email của mình, tích hợp các tính năng nâng cao tăng cường trải nghiệm gửi và nhận email tốt hơn, kiểm soát email spam, tin tặc và rò rỉ dữ liệu tốt hơn email miễn phí hoặc webmail miễn phí.

Email host là một dịch vụ cung cấp bởi các nhà cung cấp dịch vụ lưu trữ để cho phép bạn tạo và sử dụng các tài khoản email dựa trên tên miền của bạn.

## 3. Mail Server

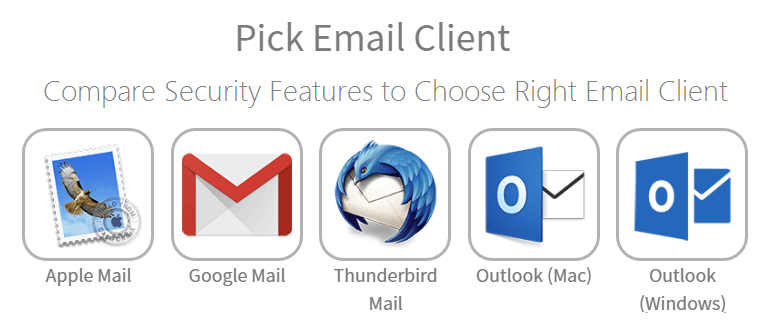
Mail Server là một giao thức chuyên nghiệp để giao tiếp thư tín, quản lý và truyền thông nội bộ, giao dịch thương mại… Không chỉ thao tác với tốc độ nhanh chóng và ổn định, Mail Server còn đảm bảo tính an toàn với khả năng khôi phục dữ liệu cao.

 Mail Server hay Email Server (máy chủ thư điện tử) là hệ thống máy chủ dùng để gửi và nhận thư điện tử. Mail server được cấu hình riêng theo tên miền của doanh nghiệp, có đầy đủ thông số như một máy chủ thông thường như CPU, RAM, Storage,…

Hình 13: Hình ảnh minh hoạ Email Server

## 4. Mail Client

Mail Client hay còn được gọi là trình duyệt mail, là một phần mềm máy tính được sử dụng để truy cập và hỗ trợ cho việc quản lý email của người dùng một cách tốt hơn. Phần mềm Mail Client cho phép người dùng có thể cấu hình một hoặc nhiều địa chỉ email thông qua những giao thức như: [SMTP,](https://vietnix.vn/smtp-la-gi/) POP và IMAP,…

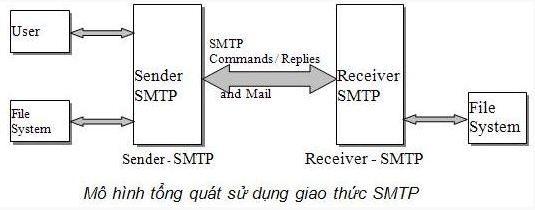
Mail client là một ứng dụng trên máy tính hoặc thiết bị di động, được sử dụng để đọc, viết và gửi email từ các tài khoản email của bạn. Mail client có thể được cài đặt trên máy tính hoặc thiết bị di động để tải email từ máy chủ email (email server) và lưu trữ trên thiết bị của bạn để bạn có thể đọc và trả lời email trong khi không kết nối internet.

Hình 14: Hình ảnh minh hoạ Mail Client

## 5. Một số sơ đồ hệ thống mail thường dùng

Khác với người dùng cá nhân, ở các công ty, tổ chức khi sử dụng mail đều có máy chủ riêng nhằm kiểm soát một cách tốt nhất tất cả mọi người gọi là mail server. Có 3 giao thức chính là SMTP, POP3, IMAP.

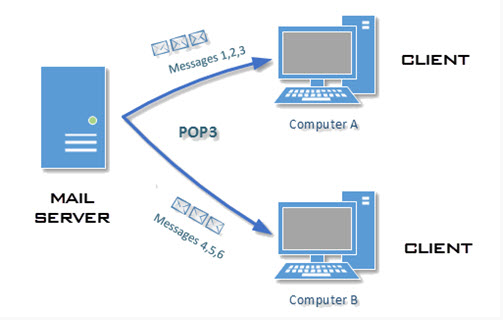
### 5.1 SMTP (Simple Mail Transfer Protocol)

SMTP được phát triển vào năm 1982 bởi tổ chức IETF (Internet Engineering Task Force). SMTP thường đi kèm với chuẩn POP3. Chúng được sử dụng khi gửi từ một ứng dụng email như Postfix với một máy chủ email hoặc khi email được gửi từ một máy chủ email khác. SMTP sử dụng cổng TCP 25 trong quá trình làm việc của mình.

Hình 15: Mô hình sử dụng SMTP

SMTP gửi thư điện tử cho một máy chủ luôn luôn hoạt động, người nhận đến lấy thư từ máy chủ khi nào họ muốn dùng giao thức POP. Ngoài ra SMTP cũng có kết hợp thêm hai thủ tục khác hỗ trợ cho việc lấy thư là POP3 và IMAP4.

### 5.2 POP3 (Post Office Protocol version 3)

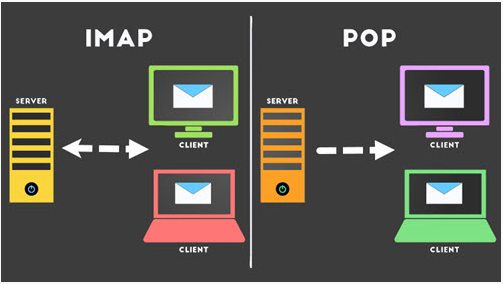
POP được phát triển đầu tiên là vào năm 1984 và được nâng cấp bản POP2 lên POP3 vào năm 1988.

Hình 16: Mô hình sử dụng POP3

POP3 được phát triển để cho phép người dùng có thể lấy thư về máy của họ và có giao diện sử dụng thân thiện hơn với người dùng. Và chính điều đó đã làm phổ biến về thư điện tử.

POP3 cho phép người dùng có tài khoản tại máy chủ thư điện tử kết nối vào MTP(Media Transfer Protocol) và lấy thư về máy tính của mình. Khác với SMTP, POP3 sử dụng cổng TCP 110.

### 5.3 IMAP (Internet Message Access Protocol)

IMAP là giao thức thế hệ mới của POP. IMAP sử dụng cổng TCP 143, đặt sự kiểm soát email trên mail server trong khi nhiệm vụ của POP là tải toàn bộ thông điệp email về client server yêu cầu.

Hình 17: Mô hình sử dụng IMAP

IMAP cung cấp truy cập theo ba chế độ khác nhau.

* Offline (ngoại tuyến )
* Chế độ offline IMAP giống như các thông điệp email được truyền đến khách hàng hay đọc, trả lời,làm các việc khác ở chế độ ngoại tuyến theo sự cài đặt của đơn vị khách hàng.
* Online (trực tuyến )
* Chế độ IMAP truy cập mà người dùng đọc và làm việc với thông điệp email trong khi vẫn giữ kết nối với email server ( kết nối mở). Các thông tin này vẫn nằm ở mail server cho đến khi người dùng quyết định xóa nó đi. Chúng đều được gắn nhãn hiệu cho biết loại để “đọc” hay “trả lời“.
* Disconnected (ngắt kết nối )

IMAP còn cho phép người dùng lưu tạm thông điệp ở client server và làm việc với chúng, sau đó cập nhập trở lại vào mail server ở lần kết nối tiếp.

# III. Những chương trình mail và một số khái niệm

## 1. Mail User Agent (MUA)

Lá ứng dụng cho phép người dùng có thể truy nhập vào mail server để lấy về các thư của người dùng hoặc xem trực tiếp thư trên server. MUA còn cho phép người dùng tạo và gửi thư. Thư được chuyển đến MTA quản lý người dùng (sử dụng SMPT ). MUA không trực tiếp chuyển thư đến người nhận. Các phần mềm ứng dụng thông dụng là Outlook Express, Microsoft Outlook,...

## 2. Mail Transfer Agent (MTA)

Lá ứng dụng cho phép gửi và nhận thư sử dụng SMTP. Cho các thư chuyển đi MTA xác định địa chỉ người nhận ngay tại hệ thống hoặc thông qua MDA (chương trình đẩy các bản tin vào hộp thư của người dùng) để chuyển đi. Nếu người nhận là một địa chỉ khác thì MTA sẽ kết nối đến một MTA quản lý người nhận để gửi thư.

Phần mềm quản lý mail MTA: sendMail, Qmail, Exchange server,...

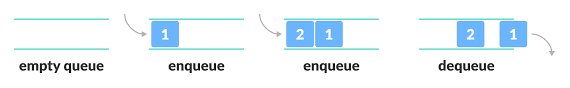
## 3. Mailbox

Mailbox là hộp thư dùng chung cho phép nhiều người dùng có thể truy cập vào cùng một tài khoản email với các quyền cụ thể như xem email, trả lời email, chuyển tiếp email và tạo email mới. Mọi người cũng có thể xem email nào đã được trả lời và email nào chưa. Mọi người cũng có thể đọc được email trả lời của các thành viên đã gửi.

Tất cả các email được gửi từ hộp thư dùng chung đều hiển thị địa chỉ hộp thư dùng chung.

## 4. Hàng đợi (queue)

Hàng đợi (queue) là một cấu trúc dữ liệu hoạt động theo cơ chế FIFO (First In First Out), tạm dịch là “vào trước ra trước”. Có nghĩa là phần tử nào được thêm hàng đợi trước thì sẽ được lấy ra trước.



Hình 18: Hàng đợi

Có thể hình dung hàng đợi như một đoàn người xếp hàng mua vé. Người nào xếp hàng trước sẽ được mua vé trước và ra khỏi hàng để nhường vị trí cho người xếp hàng ngay phía sau.

Có thể xem hàng đợi (queue) là một kiểu danh sách có 2 phép toán đặc trưng là:

* Bổ sung một phần tử vào cuối danh sách (rear)
* Loại bỏ một phần tử ở đầu danh sách (front)

Một số thao tác thông dụng trên queue như:

* enqueue(): thêm một phần tử vào queue.
* dequeue(): loại bỏ một phần tử ra khỏi queue.
* isFull(): kiểm tra queue có đầy chưa. Số lượng phần tử trong queue do người dùng quy định. Tùy trường hợp chúng ta mới cần sử dụng hàm isFull().
* isEmpty(): kiểm tra queue có rỗng hay không.

Trong lập trình, có 2 cách thường dùng để xây dựng queue là sử dụng mảng (array) và danh sách liên kết (linked list).

## 5. Alias

**Khái niệm:** Aliases hay Alias Domain là tên miền hoạt động song song với tên miền chính tương tự như Parked Domain. Từ Alias(es) trong tiếng Anh mang ý nghĩa là “bí danh”. Ở đây có thể hiểu là bí danh hay tên gọi khác của trang web. Bí danh trong thực tế cũng tương tự như bí danh của website. Ví dụ, mỗi người đều có tên gọi riêng ngoài tên thật trên khai sinh. Đối với các trang web có bí danh, bạn có thể truy cập đến nội dung của nó bằng bất kì bí danh nào. Ví dụ, tên miền chính của website là maindomain.com và bí danh là subdomain.com thì khi bạn vào maindomain.com hay subdomain.com đều dẫn đến cùng một trang.

**Khi nào cần dùng Aliases?**

* Sử dụng hai tên miền trở lên cho cùng một trang web.

Khách truy cập có thể sử dụng bất kỳ tên miền nào làm “bí danh” để truy cập trang web. Điều này mang lại nhiều lợi ích như tiện lợi, tăng tầm ảnh hưởng, kết nối với khách hàng… Ví dụ: bạn có thể truy cập fb.com thay vì facebook.com. Tên miền phụ bây giờ ngắn hơn và dễ nhớ hơn.

* Cho phép sử dụng tài khoản email với nhiều phần mở rộng tên miền.

Nếu bạn có 10 tài khoản tên miền phụ @domain.com và muốn nhận email tại @domain.com.vn, tên miền chính sẽ được đăng ký với dịch vụ email của công ty. Tính năng Alias/Parked domain giải quyết vấn đề truy cập một cách nhanh chóng và rất tiện lợi.

**Alias hoạt động như thế nào?**

Alias hoạt động bằng cách thêm một miền mới hoạt động với máy chủ lưu trữ của miền ban đầu. Miền bí danh sử dụng cùng một tệp hoặc thư mục như miền gốc, với hai loại mã nguồn và hai URL riêng biệt. Hai URL có thể độc lập hoặc không, nhưng URL kích hoạt dữ liệu lần thứ hai phụ thuộc vào URL cấu hình nguồn được miền ban đầu sử dụng.

# IV. DNS và Sendmail

## 1. Dịch vụ DNS.

### **1.1. Giới thiệu về dịch vụ DNS.**

* Mỗi máy tính trên mạng muốn trao đổi thông tin với nhau thì cần phải biết rõ địa chỉ Ip của nhau.
* Mỗi máy tính ngoài địa chỉ Ip còn có một tên (HOSTNAME). Để liên lạc thì việc ghi nhớ địa chỉ Ip của nhau là việc rất khó khăn, đặc biệt là việc địa chỉ IPV4 càng ngày càng không thể cung cấp đủ số lượng nhu cầu thì việc chuyển sang dùng IPV6 là điều tất yếu và việc phải nhớ một dãy số hexa 32 số là việc không tưởng.
* Do những khó khăn trên người ta đã nghĩ ra việc làm sao để ánh xạ địa chỉ ip của mỗi máy thành hostname của nó và ngược lại. Để khi trao đổi với nhau người ta chỉ cần nhớ tên ban đầu của máy tính bên kia. Ban đầu do quy mô mạng ARPANET (tiền thân của mạng internet) còn nhỏ, nên chỉ có một tập tin HOST.TXT lưu thông tin và ánh xạ tên máy thành địa chỉ Ip. Trong đó, tên máy chỉ là chuỗi văn bản không phân cấp (plat name). Tệp tin này được duy trì tại một máy chủ và các máy chủ khác lưu giữ bản sao của nó. Tuy nhiên khi mô hình mạng lớn hơn, việc sử dụng tập tin HOST.TXT có các nhược điểm sau:
* Lưu lượng mạng và máy chủ duy trì tập tin HOST.TXT bị quá tải.
* Xung đột tên: do tên máy không phân cấp và không có cơ quan quản lý tập tin nên có nguy cơ bị xung đột tên.
* Không đảm bảo sự toàn vẹn: việc duy trì tập tin trên một mạng lớn rất khó khăn. Ví dụ: khi tập tin HOST.TXT vừa cập nhật chưa kịp chuyển đến máy chủ ở xa thì đã có sự thay đổi địa chỉ trên mạng rồi.

Tóm lại, việc sử dụng tập tin HOST.TXT không phù hợp cho mạng lớn vì thiếu cơ chế phân tán và mở rộng. Do đó dịch vụ DNS ra đời nhằm khắc phục các nhược điểm này.

### **1.2. Hệ thống tên miền DNS**

DNS hoạt động theo mô hình client – server. Máy chủ server chứa các thông tin CSDL. Phía client là trình phân giải tên resolver, nó chỉ là các hàm thư viện dùng để tạo các query và gửi chúng đến máy chủ DNS server.

DNS hoạt động như một giao thức tầng application trong mạng ICP/IP

DNS là một cơ sở dữ liệu phân tán. Có nhiệm vụ chuyển đổi tên miền sang địa chỉ IP và ngược lại. Hệ thống DNS ra đời nhằm mục đích giúp người sử dụng một tên dễ nhớ, dễ sử dụng. Nguyên tắc làm việc của DNS:

* Mỗi nhà cung cấp dịch vụ vận hành và duy trì DNS server của riêng mình. Khi có yêu cầu tìm kiếm một website nào đó, thì DNS server phân giải tên website này phải là DNS server của chính tổ chức quản lý website đó.
* INTERNIC – Internet Network Information Center chịu trách nhiệm quản lý các tên miền và DNS server tương ứng.
* DNS server có khả năng truy vấn các DNS server khác. Ngoài việc phân giải tên miền cho các máy trong nội bộ thì nó cũng hỗ trợ các truy vấn từ các máy ngoài mạng internet vào bên trong.
* DNS server cũng có khả năng nhớ lại các tên vừa phân giải, để dùng cho những lần truy vấn lần sau. Số lượng tên miền được lưu lại phụ thuộc vào quy mô của từng DNS server.

### **1.3. Hoạt động của DNS server trong Linux**

Phân loại DNS server:

* Primary name server: Nguồn xác thực thông tin chính thức cho các domain mà nó được phép quản lý.
* Secondary name server: server dự phòng cho primary server.
* Caching name server: lưu lại các lần truy vấn của client, giúp cho các lần truy vấn sau được nhanh chóng và giảm tải cho server.

DNS zone là tập hợp các ánh xạ từ Host đến địa chỉ IP và từ IP tới Host trong một phần liên tục trong một nhánh của Domain. Thông tin DNS Zone là những Record gồm tên Host và địa chỉ IP được lưu trong DNS server.

DNS server quản lý và trả lời yêu cầu này từ Client liên quan đến DNS server này. Hệ thống tên miền cho phép phân chia tên miền để quản lý và chia hệ thống tên miền thành Zone và trong Zone quản lý tên miền được phân chia đó. Zone file lưu thông tin Zone ở dạng text hoặc trong Active Directory.

Zone thuận và Zone nghịch:

* Zone thuận – Forward Lookup Zone để phân giải tên máy thành địa chỉ IP.
* Zone nghịch.
* Reverse Lookup Zone để phân giải địa chỉ IP thành tên máy.

Các loại truy vấn:

* Truy vấn đệ quy (Recursive query): khi name server nhận được truy vấn dạng này, nó bắt buộc phải trả về kết quả tìm được hoặc thông báo lỗi nếu như truy vấn này không phân giải được. Name server không thể tham chiếu truy vấn đến một name server khác. Name server có thể gửi truy vấn dạng đệ quy hoặc tương tác đến name server khác nhưng nó phải thực hiện cho đến khi nào có kết quả mới thôi.
* Truy vấn tương tác: khi name server nhận được truy vấn dạng này, nó trả lời cho resolver với thông tin tốt nhất mà nó có được vào thời điểm đó. Bản thân name server không thực hiện bất cứ một truy vấn nào thêm. Thông tin tốt nhất trả về có thể lấy dữ liệu từ dữ liệu cục bộ (kể cả cache). Trong trường hợp name server không tìm thấy trong dữ liệu cục bộ nó sẽ trả về tên miền và địa chỉ IP của name server gần nhất mà nó biết.

Các file cấu hình chính:

* Host.conf: là tệp điều khiển hoạt động của resolver, nó quy định các dịch vụ sử dụng của resolver và thứ tự sử dụng của chúng.
* Resolver (bộ giải): khi một chương trình cần giải một tên host thì cần sử dụng một cơ chế gọi là bộ giải. Bộ giải đầu tiên sẽ tra cứu file /etc/host.conf và xác định phương thức nào sẽ được sử dụng để giải quyết các tên host (local file, name server NIS hay ldap server).
* File named.conf: file cấu hình chính của DNS.
* Các tệp cơ sở dữ liệu DNS – các file phân giải thuận, phân giải nghịch. Thành phần cơ bản là bản ghi nguồn RR (Resource Record). Mỗi bản ghi có một kiểu dữ liệu, bao gồm:
* SOA (Start of Authority): trong mỗi tập tin cơ sở dữ liệu phải có một và chỉ một record SOA. Record SOA chỉ ra rằng máy chủ name server là nơi cung cấp thông tin tin cậy từ dữ liệu có trong zone.
* NS (Name server): tên server.
* MX (Mail Exchange): chuyển mail trên mạng Internet.
* A (Address): ánh xạ tên máy (hostname) vào địa chỉ IP.
* CNAME (canonical name): tên bí danh của server.
* PTR: dùng để ánh xạ địa chỉ IP thành hostname.

### **1.4. Cài đặt và cấu hình dịch vụ DNS server**

Cài đặt : Cần download và cài đặt gói BIND trên máy linux. Thường thì tên file cài đặt BIND bắt đầu là bind, sau đó là version. Nếu không biết version nào, gõ bind\*. Thông thường có 2 cách cài đặt BIND là cài từ gói compile sẵn (RPM – Redhat Package Manager):

* Cài từ gói rpm: rpm –ivh bind-9.7.3-8.P3.el6.x86\_64.rpm, nếu có internet thì cài bằng lệnh yum –y install bind\*
* Cài từ source: mount thư mục chứa gói cài đặt DNS vào máy chủ centos: #mount /dev/cdrom/medi

Cấu hình DNS

* Định nghĩa những cấu hình toàn cục cho DNS server:

**Cú pháp:**

Options [

(directory path\_name)

(forwarders [in\_addr1; inaddr2;…]

(allow\_query [address\_match\_list]

(notify yes/no (also – notify [ip\_addr1, ip\_addr2…;]

(also – update [ip\_addr1, ip\_addr2…;]

***Trong đó:***

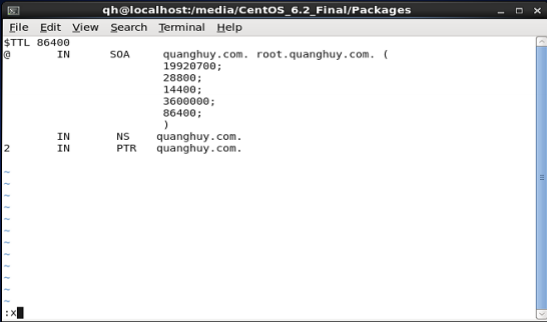
**Directory <**đường dẫn thư mục chứa các file CSDL của DNS>

**Forwarders:** danh sách địa chỉ Ip của các name server mà nó sẽ gửi yêu cầu truy vấn khi cần.

**Allow-query**: danh sách địa chỉ Ip được phép truy vấn CSDL DNS

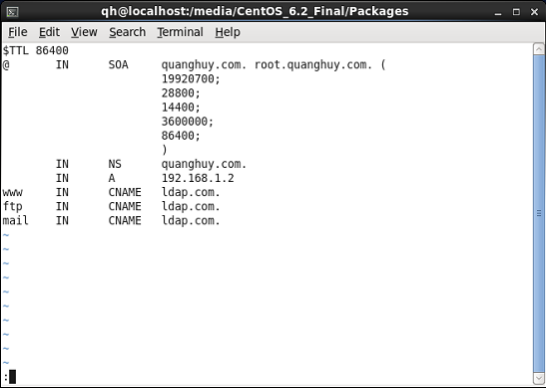
**Notify**: mặc định được set là “yes”, khi có sự thay đổi trên CSDL thì name server sẽ gửi thông báo về sự thay đổi này cho các name server được khai báo trong danh sách name server được liệt kê trong record NS và các name server được khai báo trong tùy chọn also-notify.

Cấu hình master DNS, ta vào file vi /etc/named.conf:

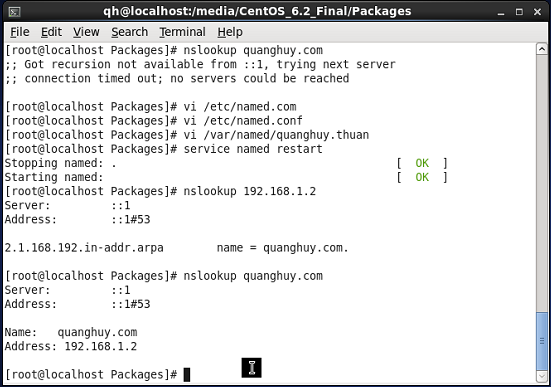
Ta tiến hành cấu hình phân giải ngược như sau: tạo file theo đường dẫn sau vi /var/named/doan.nghich.

Hình 19: Cấu hình zone nghịch

* Ta tiến hành cấu hình phân giải thuận như sau: tạo file theo đường dẫn sau vi /var/named/doan.thuan.



Hình 20: Cấu hình zone thuận

Sau khi cấu hình xong file này và ping thành công 2 máy thì restart lại dịch vụ. Kiểm tra dịch vụ DNS phân giải trong nslookup

Hình 21: Kiểm tra dịch vụ DNS

## 2.Sendmail

### 2.1.Khái niệm

Sendmail hay còn gọi là gửi thư là một phương thức chung trong internetwork email cơ sở định tuyến hỗ trợ nhiều loại phương pháp thư chuyển và giao hàng, bao gồm Simple Mail Transfer Protocol (SMTP) được sử dụng để vận chuyển email qua Internet

Đây là một phiên bản nâng cấp của delivermail chương trình được viết bởi Eric Allman , Sendmail là một dự án nổi tiếng được hợp tác phát triển bởi phần mềm mã nguồn mở miễn phí và Unix cộng đồng. Hiện nay trên mạng đã lưu hành cả phần mềm mã nguồn mở và phần mềm sở hữu độc quyền.

### 2.2.Tổng quan về Sendmail

Hình 22: Sendmail

Allman đã viết bản gốc ARPANET delivermail đó vận hành vào năm 1979 với phiên bản 4,0 và 4,1 BSD . Ông đã viết Sendmail như một dẫn xuất của delivermail vào đầu những năm 1980 tại UC Berkeley . Nó được xuất xưởng với BSD 4.1c vào năm 1983, phiên bản BSD đầu tiên có giao thức TCP / IP.

Năm 1996, khoảng 80% các máy chủ thư có thể truy cập công khai trên Internet chạy Sendmail. Các cuộc khảo sát gần đây đã cho thấy sự suy giảm, với 4,67% máy chủ thư trong tháng 10 năm 2017 được phát hiện là đang chạy Sendmail trong một nghiên cứu được thực hiện bởi E-Soft, Inc. Các khảo sát khác đã giảm một chút so với 24% các máy chủ thư trong tháng 8 năm 2015 được phát hiện là đang chạy Sendmail trong một nghiên cứu được thực hiện bởi Mail Radar.

Allman thiết kế Sendmail để kết hợp tính linh hoạt tuyệt vời, nhưng nó có thể khó khăn khi cấu hình cho người mới sử dụng email. Các gói cấu hình tiêu chuẩn được phân phối với việc phân phối mã nguồn yêu cầu sử dụng ngôn ngữ macro M4 ẩn chứa nhiều phức tạp về cấu hình. Cấu hình xác định các tùy chọn gửi thư cục bộ của trang web và các tham số truy cập của chúng, cơ chế chuyển tiếp thư đến các trang từ xa, cũng như nhiều thông số điều chỉnh ứng dụng.

Sendmail hỗ trợ nhiều giao thức chuyển thư , bao gồm SMTP , ESMTP , Mail-11 của DECnet , HylaFax, QuickPage và UUCP . Ngoài ra, Sendmail v8.12 tính đến tháng 9 năm 2001 đã giới thiệu hỗ trợ cho các trình gỡ rối – các chương trình lọc thư bên ngoài có thể tham gia vào từng bước của cuộc hội thoại SMTP .

Sendmail có nguồn gốc từ những ngày đầu của Internet, một thời đại khi cân nhắc về an ninh không đóng một vai trò chính trong việc phát triển phần mềm mạng. Các phiên bản Sendmail sớm bị một số lỗ hổng bảo mật đã được sửa chữa trong nhiều năm.

Chính Sendmail đã kết hợp một bộ phân đặc quyền riêng biệt để tránh tiếp xúc với các vấn đề bảo mật. Tính đến năm 2009 , các phiên bản hiện tại của Sendmail, giống như các [MTA](https://tinomail.com/mta-trong-email-la-gi/) hiện đại khác , kết hợp một số cải tiến bảo mật và các tính năng tùy chọn có thể được cấu hình để cải thiện bảo mật và giúp ngăn ngừa lạm dụng.