

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

KHOA CÔNG NGHỆ THÔNG TIN



BÁO CÁO BÀI TẬP LỚN

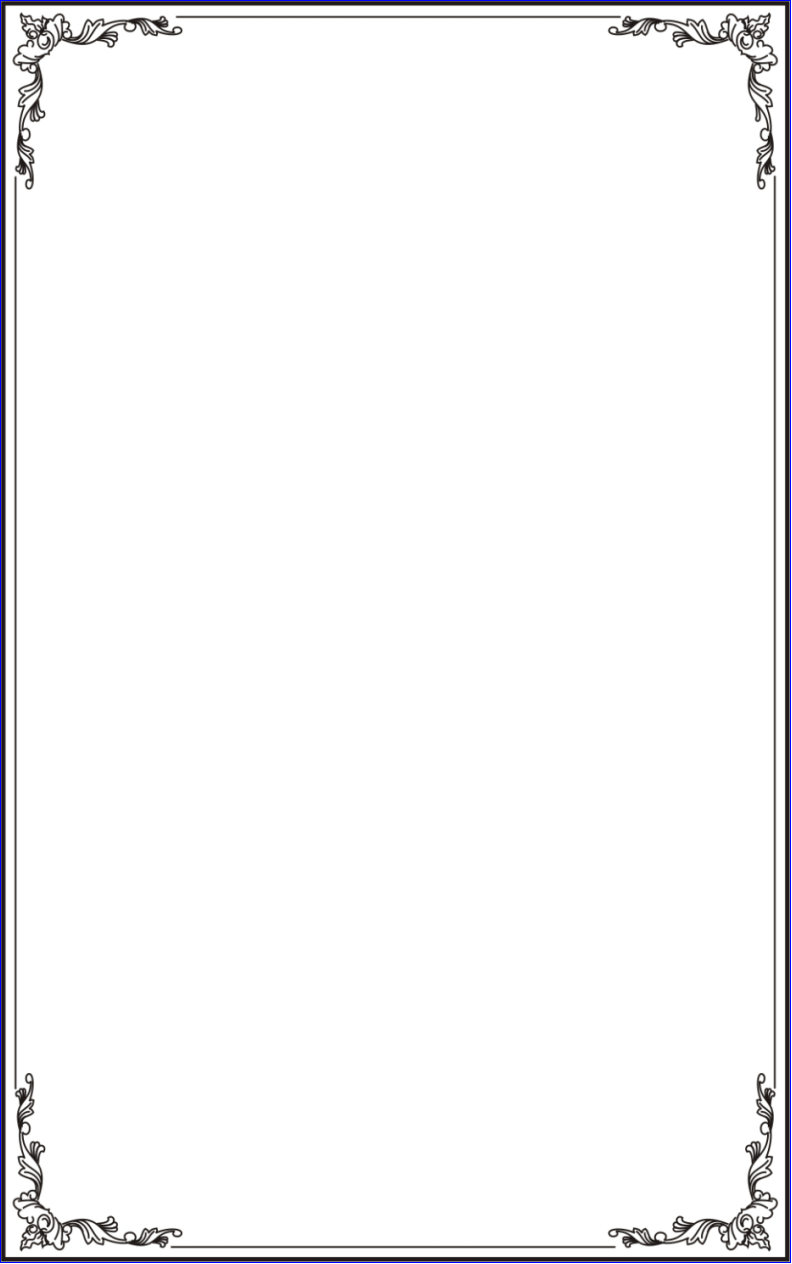
HỌC PHẦN : NGUYÊN LÝ HỆ ĐIỀU HÀNH

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 – 202160432  Phạm Thị Liễu - 2021608600  Phan Xuân Minh - 2021604849  Nguyễn Thị Hải Phương - 2021606397  Phạm Văn Tình - 2017605751 |
| Lớp | : | IT6025.7 - K16 |

Hà Nội - 2023

MỤC LỤC

[LỜI NÓI ĐẦU 2](#_Toc137731509)

[CHƯƠNG 1. CÁC TIỆN ÍCH MẠNG CỦA HỆ ĐIỀU HÀNH LINUX 5](#_Toc137731510)

[1.1. Telnet 5](#_Toc137731511)

[1.1.1. Khái niệm 5](#_Toc137731512)

[1.1.2. Tiện ích của telnet 5](#_Toc137731513)

[1.1.3. Hoạt động của telnet 5](#_Toc137731514)

[Hình 1.1: Mô hình client server 5](#_Toc137731515)

[1.1.4. Yêu cầu để thực hiện được Telnet 6](#_Toc137731516)

[1.2. FTP 6](#_Toc137731517)

[1.2.1. Khái niệm về FTP: 6](#_Toc137731518)

[1.2.2. Mô hình hoạt động của FTP. 6](#_Toc137731519)

[1.2.2.1. Kết nối TCP trong FTP. 6](#_Toc137731520)

[Hình 1.2: Hình ảnh mô tả hoạt động kết nối TCP trong FTP 6](#_Toc137731521)

[1.2.2.2. Mô hình FTP. 6](#_Toc137731522)

[Hình 1.3: Sơ đồ minh hoạ FPT 7](#_Toc137731523)

[1.2.3. Phương thức tạo kết nối và truyền dữ liệu trong FTP. 7](#_Toc137731524)

[1.2.3.1. Phương thức tạo kết nối dữ liệu của FTP. 7](#_Toc137731525)

[1.2.3.2. Phương thức truyền dữ liệu của FTP. 7](#_Toc137731526)

[1.2.3.3. Ưu điểm và nhược điểm 7](#_Toc137731527)

[1.3. Ping 8](#_Toc137731528)

[1.3.1. Câu lệnh ping 8](#_Toc137731529)

[1.3.2. Ping hoạt động: 8](#_Toc137731530)

[1.3.3. Tính năng bao gồm: 8](#_Toc137731531)

[1.4. Traceroute 9](#_Toc137731532)

[1.4.1. Nguyên lý hoạt động của traceroute 9](#_Toc137731533)

[1.4.2. Hướng dẫn chạy Traceroute trên Linux 9](#_Toc137731534)

[1.4.3. Sử dụng Traceroute 9](#_Toc137731535)

[CHƯƠNG 2. SAMBA VÀ DHCP 10](#_Toc137731536)

[2.1. Samba 10](#_Toc137731537)

[2.1.1. Giới thiệu SAMBA 10](#_Toc137731538)

[2.1.2. Cài đặt và cấu hình 10](#_Toc137731539)

[Hình 2.1: Cài đặt Samba 11](#_Toc137731540)

[2.1.3. Quản trị tài khoản Samba 15](#_Toc137731541)

[2.1.4. Sử dụng dịch vụ Samba 16](#_Toc137731542)

[2.2. DHCP 18](#_Toc137731543)

[2.2.1. Giới thiệu dịch vụ DHCP 18](#_Toc137731544)

[2.2.2. Nguyên tắc hoạt động 18](#_Toc137731545)

[2.2.3. Các thông số trong cấu hình DHCP 19](#_Toc137731546)

[2.2.4. Cài đặt và cấu hình dịch vụ DHCP. 20](#_Toc137731547)

[Hình 2.2: Cấu hình DHCP 20](#_Toc137731548)

[Hình 2.3: Máy client đã được cấp phát địa chỉ Ip 21](#_Toc137731549)

[CHƯƠNG 3. NETWORKING. 21](#_Toc137731550)

[3.1. Địa chỉ IP 21](#_Toc137731551)

[3.1.1. IP tĩnh và động 21](#_Toc137731552)

[3.1.2. Phân phối địa chỉ IP 21](#_Toc137731553)

[3.1.3. Cấu trúc và phân lớp địa chỉ IP. 22](#_Toc137731554)

[Hình 3.1: Hình ảnh các thành phần chình của cấu trúc 22](#_Toc137731555)

[Hình 3.2: Hình ảnh mô tả lớp A của địa chỉ IP 22](#_Toc137731556)

[Hình 3.3: Hình ảnh mô tả lớp B của địa chỉ IP 23](#_Toc137731557)

[Hình 3.4: Hình ảnh mô tả lớp C của địa chỉ IPH 23](#_Toc137731558)

[3.2. Domain Name System (DNS) 24](#_Toc137731559)

[3.2.1. Giới thiệu về DNS 24](#_Toc137731560)

[3.2.2. Cơ chế phân giải tên 24](#_Toc137731561)

[3.2.3. Phân loại Domain Name Server 24](#_Toc137731562)

[CHƯƠNG 4. PROXY SERVER 25](#_Toc137731563)

[4.1. Firewall 25](#_Toc137731564)

[4.1.1. Những chính sách Firewall 25](#_Toc137731565)

[Hình 4.1: Hình ảnh Firewall 25](#_Toc137731566)

[4.1.2. Các loại Firewall và cách hoạt động 26](#_Toc137731567)

[4.1.2.1 Packet filtering 26](#_Toc137731568)

[4.1.2.2 Circuit relay 26](#_Toc137731569)

[4.1.2.3 Application gateway 26](#_Toc137731570)

[4.2. Squid Proxy 27](#_Toc137731571)

[CHƯƠNG 5. WEB SERVER 28](#_Toc137731572)

[5.1. Giới thiệu về Web server 28](#_Toc137731573)

[5.1.1. Giao thức HTTP. 28](#_Toc137731574)

[5.1.2. Web server và cách hoạt động 28](#_Toc137731575)

[5.1.3. Web client 29](#_Toc137731576)

[5.1.4. Web động 29](#_Toc137731577)

[5.2. Giới thiệu Apache 29](#_Toc137731578)

[CHƯƠNG 6. MAIL SERVER 31](#_Toc137731579)

[6.1. Những giao thức mail 31](#_Toc137731580)

[6.1.1. SMTP (Simple Mail Transfer Protocol) 31](#_Toc137731581)

[6.1.2. Post Office Protocol 31](#_Toc137731582)

[6.2 Giới thiệu về hệ thống mail 31](#_Toc137731583)

[Hình 6.1: Sơ đồ về một hệ thống email đầy đủ các thành phần 32](#_Toc137731584)

[6.2.1. Mail gateway 32](#_Toc137731585)

[6.2.2. Mail Host 32](#_Toc137731586)

[6.2.3. Mail Server 33](#_Toc137731587)

[6.2.4. Mail Client 33](#_Toc137731588)

[6.2.5. Một số sơ đồ hệ thống mail thường dùng 33](#_Toc137731589)

[6.2.5.1 SMTP (Simple Mail Transfer Protocol) 33](#_Toc137731590)

[Hình 6. 2: Mô hình sử dụng SMTP 34](#_Toc137731591)

[6.2.5.2 POP3 (Post Office Protocol version 3) 34](#_Toc137731592)

[Hình 6.3: Mô hình sử dụng POP3 34](#_Toc137731593)

[6.2.5.3 IMAP (Internet Message Access Protocol) 35](#_Toc137731594)

[Hình 6.4: Mô hình sử dụng IMAP 35](#_Toc137731595)

[6.3. Những chương trình mail và một số khái niệm 36](#_Toc137731596)

[6.3.1. Mail User Agent (MUA) 36](#_Toc137731597)

[6.3.2. Mail Transfer Agent (MTA) 36](#_Toc137731598)

[6.3.3. Mailbox 36](#_Toc137731599)

[6.3.4. Hàng đợi (queue) 36](#_Toc137731600)

[Hình 6.5: Hàng đợi 37](#_Toc137731601)

[6.3.5. Alias 37](#_Toc137731602)

[6.4. DNS và Sendmail 38](#_Toc137731603)

[TÀI LIỆU THAM KHẢO 39](#_Toc137731604)

LỜI NÓI ĐẦU

GIT-Linux là tên gọi của một hệ điều hành máy tính và cũng là tên hạt nhân của hệ điều hành. Nó có lẽ là một ví dụ nổi tiếng nhất của phần mền tự do và của việc phát triển mã nguồn mở.

Phiên bản Linux đầu tiên do Lonus Torvalds viết vào năm 1991, lúc ông còn là một sinh viên của Đại học Helsinki tại Phần Lan. Ông làm việc một cách hăng say trong vòng 3 năm liên tục và cho ra đời phiên bản Linux 1.0 vào năm 1994. Bộ phận chủ yếu này được phát triển và tung ra trên thị trường dưới bản quyền GNU General Public License. Do đó mà bất cứ ai cũng có thể tải và xem mã nguồn của Linux. “Linux” được sử dụng để chỉ Nhân Linux, nhưng tên này được sử dụng một cách rộng rãi để miêu tả tổng thể một hệ điều hành giống Unix(còn được biết dưới tên GUN/Linux) được tạo ra bởi việc đóng gói nhân Linux cùng với các thư viện và công cụ GNU, cũng như là các bản phân phối Linux.

Khởi đầu Linux được phát triển cho dòng vi xử lý 386. Hiện tại hệ điều hành này hỗ trợ một số lượng lớn các siêu thị máy tính và các thiết bị nhúng như là các máy điện thoại di động.

Ban đầu, Linux được phát triển và sử dụng bởi những người say mê. Tuy nhiên, hiện nay Linux đã có được sự hỗ trợ bởi các công ty lớn như IBM và Hewlett-Packard, đồng thời nó cũng bắt kịp được các phiên bản được các phiên bản Unix độc quyền và thậm chí là một thách thức đối với sự thống trị của Microsoft Windows trong một số lĩnh vực. Sở dĩ Linux đạt được những thành công một cách nhanh chóng là nhờ vào các đặc tính nổi bật so với các hệ thống khác: chi phí phần cứng thấp, tốc độ cao (khi so sánh với các phiên bản Unix độc quyền) và khả năng bảo mật tốt, độ tin cậy cao (khi so sánh với Windown) cũng như các đặc điểm về giá thành rẻ, không bị phụ thuộc vào nhà cung cấp. Một đặc tính nổi trội của nó là được phát triển bởi một mô hình phát triển phần mềm nguồn mở hiệu quả.

Tuy nhiên, hiện tại số lượng phần cứng được hỗ trợ bởi Linux vẫn còn rất khiêm tốn so với Windown vì các trình điều khiển thiết bị tương thích với Window nhiều hơn là Linux. Nhưng trong tương lai số lượng phần cứng được hỗ trợ cho Linux sẽ tăng lên. Hiện nay, Linux có nhiều bản phân phối khác nhau, một phần là bời vì mã nguồn mở của nó.

**NHẬN XÉT CỦA GIÁO VIÊN**

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

# 1.1. Telnet

## 1.1.1. Khái niệm

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

## 1.1.2. 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.

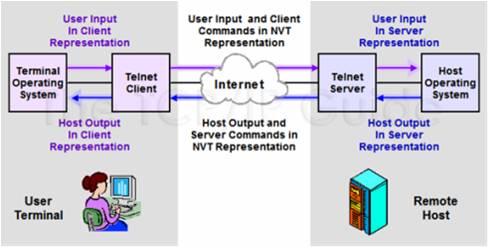
Máy tính ở xa, được gọi là telnet, sẽ chấp nhận nối kết telnet từ một máy TCP/ IP trên một hệ.

## 1.1.3. Hoạt động của telnet

Ðể Telnet vào một máy chủ trên Internet (Máy chủ này có cung cấp dịch vụ Telnet) bạn phải biết các thông số sau đây.

Tên máy chủ : Ví dụ : ccrls.ccrls.org.

Cổng vào (port) : Thường là 23. Username và password: để telnet vào.

Telnet hoạt động theo mô hình client server.

Hình 1.: Mô hình client server

## 1.1.4. Yêu cầu để thực hiện được Telnet

Giữa máy chủ và máy trạm phải có kết nối IP.

Dịch vụ Telnet phải được bật.

Gói tin TCP port 23 (port của Telnet)không bị tường lửa chắn.

# 1.2. FTP

## 1.2.1. Khái niệm về FTP:

FTP là tiện ích tải tệp ở xa. Với FTP có thế lấy tệp ở máy tính từ xa về máy tính của mình và ngược lại. FTP sử dụng giao thức TCP/IP, cổng 21.

## 1.2.2. Mô hình hoạt động của FTP.

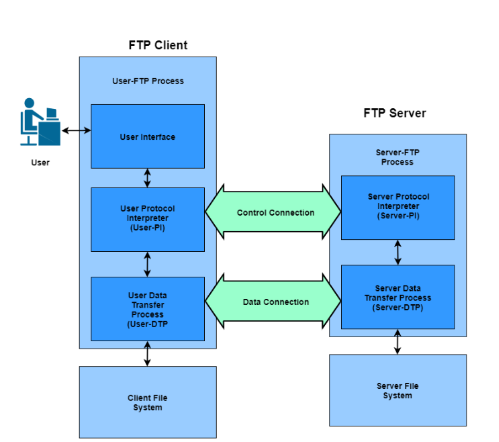
### 1.2.2.1. Kết nối TCP trong FTP.

Hình 1.: Hình ảnh mô tả hoạt động kết nối TCP trong FTP

Quá trình truyền nhận dữ liệu giữa máy client - server được tạo lên từ 2 quá trình TCP logic: Control Connection (sử dụng cổng 21) và Data Connection (sử dụng cổng 20).

### 1.2.2.2. Mô hình FTP.

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 là: Protocol Interpreter và Data Transfer Process.



Hình 1.: Sơ đồ minh hoạ FPT

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

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

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, sử dụng cổng số 20.

Passive Data Connections: Phương thức tạo kết nối bị động và giải quyết những thiếu sót của chế độ chủ động

### 1.2.3.2. Phương thức truyền dữ liệu của FTP.

Block mode: dữ liệu được chia thành nhiều khối nhỏ và được đóng gói thành các FTP blocks. Là phương thức quy chuẩn.

Stream mode: Là phương thức truyền tập tin không có cấu trúc dạng header, 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.

### 1.2.3.3. 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
* 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, có thể bị gửi thông tin đến các cổng ngẫu nhiên.
* Không phù hợp cho các tổ chức, do yêu cầu phải tạo cổng kết nối khi truyền.

# 1.3. Ping

## 1.3.1. Câu lệnh ping

Câu lệnh ping để yêu cầu một trả lời phản hồi của một máy ở xa trên mạng. 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 hoặcInternet.

## 1.3.2. Ping hoạt động:

Ping sẽ gửi các gói tin rất nhỏ để một máy chủ lưu trữ IP người sẽ trả lời bằng cách gửi các gói tin. Ping cũng rất thường xuyên được sử dụng để xác định địa chỉ IP phù hợp với một tên máy chủ và ngược lại.

Ping cho chúng ta ba thông tin chủ yếu: Chủ reachability, sự tắc nghẽn mạng, Time To Live.

## 1.3.3. Tính năng bao gồm:

* Lẽ là tốt nhất có sẵn Linux hộp công cụ cứu một hệ thống.
* Sao lưu và phục hồi phân vùng hoặc các tập tin tại địa phương hoặc mạng.
* Sao lưu và phục hồi dữ liệu BIOS như;
* Hay có thể ghi một đĩa CD / DVD, hoặc tích hợp trong một môi trường PXE / RIS;
* Khả năng mật khẩu Trống quản trị cục bộ;
* Tạo DVD phục hồi của riêng bạn khả năng khởi động;
* Phân vùng và định dạng một đĩa trước khi cài đặt Windows.

# 1.4. Traceroute

Traceroute là một tiện ích để vạch lại con đường từ máy bạn đến một máy ở xa trên Internet. Nó cũng tính và hiển thị thời gian cần thiết để đi qua mối hop. Traceroute cũng dùng giao thức ICMP.

## 1.4.1. Nguyên lý hoạt động của traceroute

Lệnh traceroute hoạt động dựa trên trường TTL của [gói tin IP](http://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=/search%3Fq%3Dtraceroute%2Blinux%26hl%3Dvi%26biw%3D1366%26bih%3D677%26prmd%3Dimvnsa&rurl=translate.google.com.vn&sl=fr&u=http://www.commentcamarche.net/contents/internet/protip.php3&usg=ALkJrhjIGezRkPQbmHJRrxYKvekuIpcTnw) . Trong thực tế, mỗi gói tin IP có một cuộc sống trường (TTL Time To Live) giảm đi mỗi lần một router.

## 1.4.2. Hướng dẫn chạy Traceroute trên Linux

B1: Mở Terminal.

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

VD: traceroute messenger.com

## 1.4.3. 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.

CHƯƠNG 2. SAMBA VÀ DHCP

# 2.1. Samba

## 2.1.1. Giới thiệu SAMBA

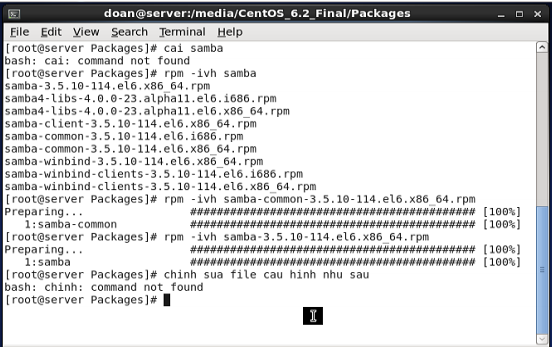
Samba là chương trình tiện ích hỗ trợ việc chia sẻ tài nguyên từ hệ thống Linux với các hệ thống khác (Linux, Windows), nó hỗ trợ tính năng gia nhập (join) Linux với Windows như gia nhập Linux vào PDC trên Windows, gia nhập vào Windows Workgroup,…

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. 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 động 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. Samba có sử dụng tập tin /etc/samba/smbpassword để lưu trữ các mật mã truy nhập người dùng. Chia sẻ thư mục trong Samba. Sau khi lập cấu hình mặc định cho server Samba, bạn có thể tạo ra nhiều thư mục dùng chung, và quyết định xem cá nhân nào, hoặc group nào được phép sử dụng chúng.

## 2.1.2. 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 2.: Cài đặt Samba

## 2.1.3. 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 sữ 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 khoảng 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

## 2.1.4. 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.
* 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.

# 2.2. DHCP

## 2.2.1. Giới thiệu dịch vụ DHCP

DHCP (Dynamic Host Configuration Protocol) được sử dụng với mục đích tập trung hóa việc quản lí và ấn định cấu hình TCP/IP của các máy client. Với những đặc điểm thuận lợi giúp cho người quản trị tiết kiệm thời gian trong việc cài đặt và quản trị một hệ thống mạng TCP/IP như sau:Quản lí việc cấp phát địa chỉ IP cho các máy client không yêu cầu.

Cung cấp những thông tin cấu hình mạng như subnet mask, default router, DNS Server.

DHCP có thể làm việc thông qua nhiều TCP/IP router và ấn định IP dựa theo subnet mask gửi tới, do đó bạn không cần phải cài lại cấu hình máy tính khi di chuyển qua những sunet khác nhau.

Địa chỉ IP chỉ được cấp phát trong một khoảng thời gian nhất định, những địa chỉ IP không tiếp tục sử dụng sẽ bị thu hồi lại.

Hỗ trợ BOOTP client.

## 2.2.2. Nguyên tắc hoạt động

Để sử dụng DHCP bạn cần phải có một DHCP Server để đáp ứng (cung cấp địa chỉ IP và thông tin cấu hình mạng) các yêu cầu từ các máy DHCP client gửi tới và ngược lại trên các máy client cũng cần phải có DHCP client để gửi các request.

Có thể tóm tắt quá trình hoạt động của DHCP request - resspond như sau:

* Lease request: DHCP client gửi broadcast gói tin DHCP request (địa chỉ nguồn là 0.0.0.0, địa chỉ đích là 255.255.255.255 và địa chỉ MAC của client), gói tin này được mở bởi DHCP Server.
* IP lease offer: DHCP Server ấn định cho client địa chỉ IP, subnet mask, domain name, địa chỉ name server, khoảng thời gian mà những thông tin cấu hình này client được phép sử dụng hợp lệ.
* Lease selection: client chấp nhận những thông tin cấu hình được cung cấp và nó sẽ gửi một gói tin broadcast để thông báo với các DHCP Server không cần gửi các thông tin cấu hình khác cho nó nữa.
* DHCP Server gửi đến clinent một gói tin ack và khi đó client đã được cấu hình TCP/IP và hoạt động bình thường.
* Lease renew: khi sử sụng những thông tin cấu hình được cung cấp đến một nửa khoảng thời gian được phép (default – lease - time), DHCP client nếu muốn tiếp tục sử dụng sẽ gửi một request mới tới DHCP Server.

DHCP là một dịch vụ phổ thông nên dã có sẵn trên mọi distro Linux nên không cần để ý đến việc cài đặt nó.

Một số tùy chọn để chạy DHCP Server với mục đích debug:

* Có thể sửa đổi port mặc định (port 67) của DHCP với –p flag. Với DHCP reply port thường lớn hơn listen port một giá trị. Ví dụ nếu ấn định cho DHCP Server lắng nghe request ở port 67 thì nó sẽ trả lời client ở port 68.
* Có thể ấn định DHCP Server chạy dưới dạng foreground process thay vì chạy dưới dạng deamon bằng –f flag.
* Chạy DHCP Server với một file config khác dùng –cf flag, chạy với một filw lease khác dùng –lf flag.

File cấu hình của DHCP Server là …/etc/DHCPd.conf được đọc và phân tích bởi DHCPD. File gồm một loạt những khai báo và tham số cấu hình.

## 2.2.3. 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 đành trong một số scope đã được quy định ở trên.

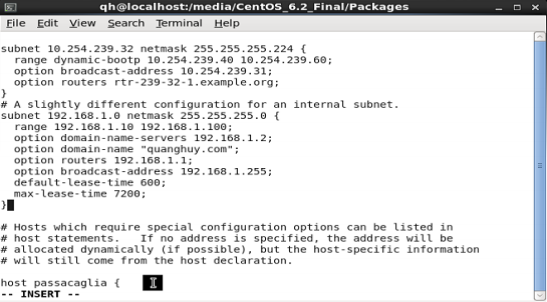
Lease: thời gian “cho thuê” địa chỉ IP đối với mỗi client.

## 2.2.4. 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.

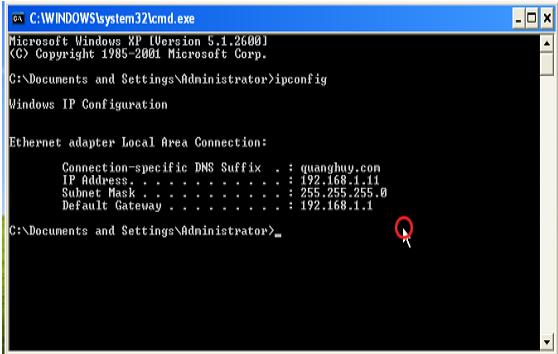
* Cách 1: cài đặt từ đĩa cd #rpm –ivh dhcp-\*.rpm (với \* là phiên bản của gói dịch vụ).
* Cách 2: cài đặt bằng cách tải trên mạng #yum –y install dhcp Kiểm tra gói cài đặt:

# rpm –qa|grep dhcp. Sau khi cài đặt, ta cấu hình như sau:



Hình 2.: 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 lênh ipconfig để kiểm tra.



Hình 2.: Máy client đã được cấp phát địa chỉ Ip

CHƯƠNG 3. NETWORKING.

# 3.1. Địa chỉ IP

## 3.1.1. IP tĩnh và động

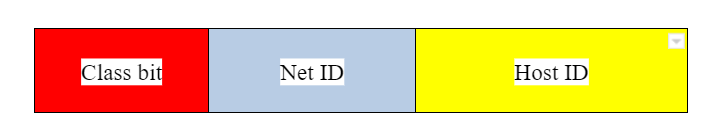
Mỗi thiết bị trong một mạng IP được chỉ định bằng một địa chỉ vĩnh viễn (IP tĩnh) bởi nhà quản trị mạng hoặc một địa chỉ tạm thời, có thể thay đổi (IP động) thông qua công cụ DHCP ngay trên Windows server.

## 3.1.2. Phân phối địa chỉ IP

Trên thế giới có hàng chục triệu máy chủ và hàng trăm nghìn mạng khác nhau.Do đó, để quản lý sao cho địa chỉ IP không trùng nhau, một tổ chức mạng tên Network information center(NIC) ra đời với nhiệm vụ phân phối Nét ID (địa chỉ mạng) cho các quốc gia. Ở mỗi nước lại có một trung tâm quản lý internet làm công việc phân phối Host ID (địa chỉ máy chủ).

## 3.1.3. 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.

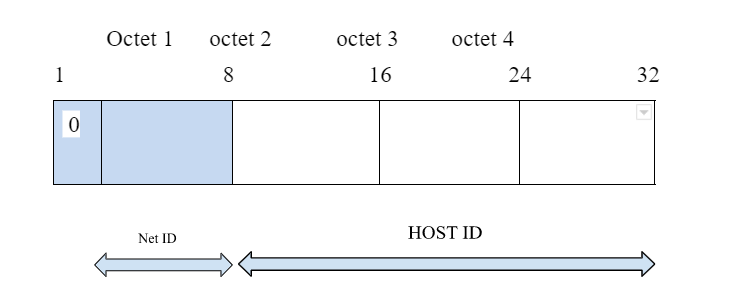
Cấu trúc được thể hiện 3 thành phần chính là:

Hình 3.: Hình ảnh các thành phần chình của cấu trúc

Trong đó:

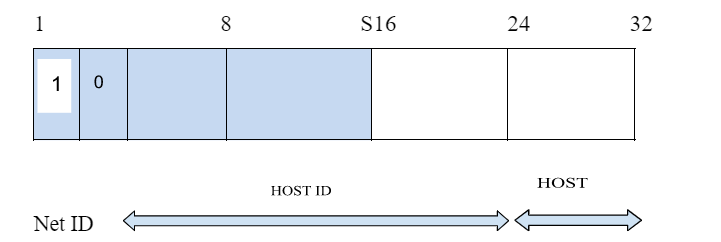
* Class bit: bit nhận dạng lớp, dùng để xác định địa chỉ đang ở lớp nào.
* NetID: địa chỉ của mạng
* Host ID: địa chỉ của máy

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:

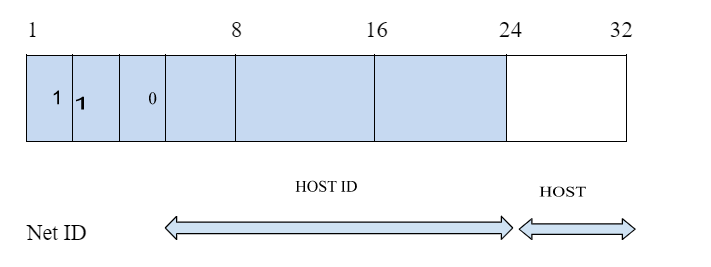
Hình 3.: Hình ảnh mô tả lớp A của địa chỉ IP

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 3.: 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 3.: Hình ảnh mô tả lớp C của địa chỉ IPH

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.

# 3.2. Domain Name System (DNS)

## 3.2.1. 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.

## 3.2.2. 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.

## 3.2.3. Phân loại Domain Name Server

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

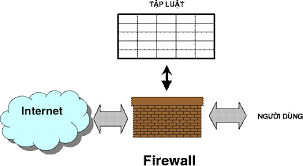
Secondary server: Nơi lưu trữ dự phòng cơ sở dữ liệu tên miền cho các Primary server.

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

# 4.1. Firewall

## 4.1.1. 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 4.: 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.

## 4.1.2. Các loại Firewall và cách hoạt động

Có 3 loại Firewall trên hệ điều hành Linux:

### 4.1.2.1 Packet filtering

Loại Firewall này thực hiện việc kiểm tra số nhận dạng địa chỉ của các packet để từ đó cấp phép cho chúng lưu thông hay ngăn chặn. 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

Ví dụ: IPtables, Ipchains, SmoothWall

### 4.1.2.2 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.

### 4.1.2.3 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.

Ví dụ về một số gateway ứng dụng: Squid.

# 4.2. 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.

# CHƯƠNG 5. WEB SERVER

# 5.1. Giới thiệu về Web server

## 5.1.1. Giao thức HTTP.

HTTP là một giao thức cho phép trình duyệt Web Brower và server có thể giao tiếp với nhau. Nó chuẩn hóa các thao tác cơ bản mà một Web Server phải làm được.

HTTP bắt đầu là một giao thức đơn giản giống như với các giao thức chuẩn khác trên Internet, thông tin được điều khiển được truyền dưới dạng văn bản thô thong qua kết nối TCP. Do đó,kết nối HTTP có thể thay thế bằng cách dùng lệnh “telnet” chuẩn.

## 5.1.2. 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://127.0.0.1:5500/HTML\_CSS-master/HIT\_WEB/BTVN/BTL/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 sơ 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 Borwer, 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.

## 5.1.3. Web client

Là những chương trình duyệt Web ở phía người dùng, như Internet Explorer, Netscape Communicator…, để hiển thị thông tin trang Web cho người dùng. Web client sẽ gửi yêu cầu đến Web Server. Sau đó, đợi Web Server xử lý trả kết quả về cho web client hiển thị cho người dùng. Tất cả mọi yêu cầu đều được xử ls bởi Web Server.

## 5.1.4. Web động

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 chúng xuyên qua mạng.

# 5.2. 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

# 6.1. Những giao thức mail

## 6.1.1. SMTP (Simple Mail Transfer Protocol)

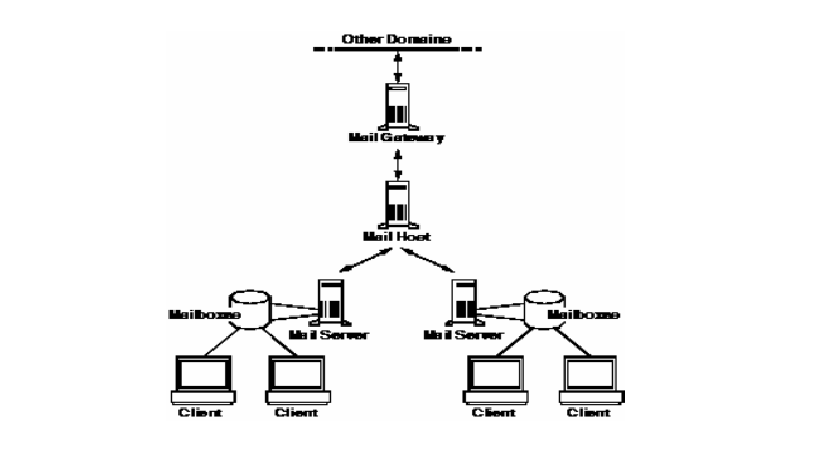
SMTP là giao thức tin cậy chịu trách nhiệm phân mail. Nó chuyển mail từ hệ thống mạng này sang hệ thống mạng khác, chuyển mail trong hệ thống mạng nội bộ. Giao thức SMTP được định nghĩa trong RFC 821, SMTP là một dịch vụ tin cậy, hướng kết nối (connection-oriented) được cung cấp bởi giao thức TCP (Transmission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

## 6.1.2. 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.

# 6.2 Giới thiệu về hệ thống mail

Những thành phần trong một hệ thống mail: Một hệ thống mail yêu cầu phải có ít nhất hai thành phần, nó có thể định vị trên hai hệ thống khác nhau hoặc trên cùng một hệ thống, mail server và mail client. Ngoài ra, có còn có những thành phần khác như Mail Host, Mail Gateway.



Hình 6.: Sơ đồ về một hệ thống email đầy đủ các thành phần

## 6.2.1. 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.

## 6.2.2. Mail Host

Một mail host là máy giữ vai trò máy chủ mail chính trong hệ thống mạng. Nó dùng như thành phần trung gian để chuyển mail giữa các vị trí không trực tiếp được với nhau.

Mail host phân giải địa chỉ người nhận để chuyển giữa các mail server hoặc chuyển đến mail gateway.

Một ví dụ về mail host là máy trong mạng cục bộ LAN có modem được thiết lập liên kết PPP hoặc UUCP dung phone line. Mail host cũng có thể máy chủ đóng vai trò router giữa mạng nội bộ và mạng internet.

## 6.2.3. Mail Server

Mail Server chứa mailbox của người dùng. Mail Server nhận mail từ mail client gửi đến và đưa vào hàng đợi để gửi đến Mail Host. Mail Server nhận mail từ Mail Host gửi đến và đưa vào thư mục mailbox của người dùng. Người dùng sử dụng NFS (Network File System) để mount thư mục chứa mailbox trên Mail Server để đọc. Nếu NFS không được hỗ trợ thì người dùng phải login vào Mail Server để nhận thư.

Trong trường hợp Mail Client hỗ trọ POP/IMAP và trên Mail Seerver cũng hỗ trợ POP/IMAP thì người dùng có thể đọc thư bằng POP/IMAP.

## 6.2.4. Mail Client

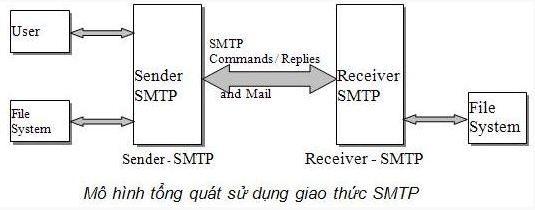
Là những hệ thống mà nó cho phép tập tin mail spool của user được đọc thông qua cơ chế ount của NFS thư mục /var/mail từ mail hub, nếu không có thư mục /var/mail thì ta phải mount tự động thư mục /var/mail trong tập tin vfstab từ server.

## 6.2.5. 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.

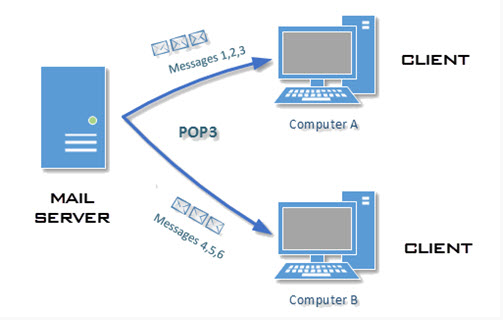
### 6.2.5.1 SMTP (Simple Mail Transfer Protocol)

Hình 6. : Mô hình sử dụng SMTP

 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.

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.

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

POP được phát triển đầu tiên là vào năm 1984 và được nâng cấp bản

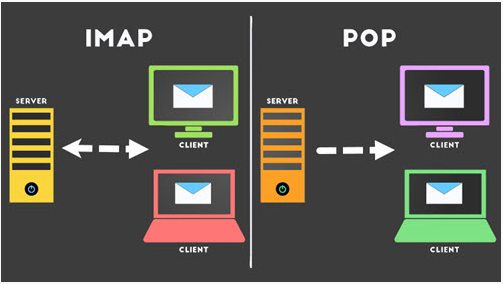
Hình 6.: Mô hình sử dụng POP3

POP2 lên POP3 vào năm 1988.

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.

### 6.2.5.3 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 6.: 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.

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

## 6.3.1. Mail User Agent (MUA)

MUA: là những chương trình mà người sử dụng dùng để đọc, soạn thảo và gửi mail.

## 6.3.2. Mail Transfer Agent (MTA)

MTA: là chương trình chuyển thư giữa các máy Mail Hub. Sendmail Transfer Agent (MTA) dùng giao thức SMTP để đóng vai trò là một SMTP Server làm nhiện vụ định tuyến trong việc phân thư. Nó nhận mail từ những Mail User Agent (MUA) và những MTA khác, sau đó chuyển mail đến các MTA trên máy khác hat MTA trên máy của mình. Để nó không đóng vai trò là một trạm phân thư đến cho người dùng, ta phải dùng một chương trình khác như POP, IMAP để thực hiện việc này.

## 6.3.3. Mailbox

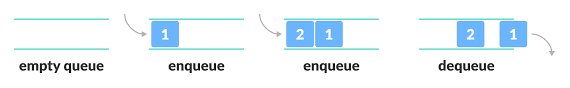
Mailbox là hộp thư dùng chung cho phép nhiều người dùng có thể truy cập vào cùng một tài khoản email với các quyền cụ thể như xem email, trả lời email, chuyển tiếp email và tạo email mới. Mọi người cũng có thể xem email nào đã được trả lời và email nào chưa. Mọi người cũng có thể đọc được email trả lời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

## 6.3.4. 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 6.: 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).

## 6.3.5. Alias

Một số vấn đề phức tạp thường gặp trong quá trình phân thư là:

* Phân phối đến cho cùng một người qua nhiều địa chỉ khác nhau.
* Phân phối đến nhiều người nhưng qua cùng một địa chỉ.
* Kết nối thư với một tập tin để lưu trữ hoặc dùng cho mục đích khác nhau.
* Lọc thư thông qua các trương trình hay các script.

Để giải quyết các vấn đề trên ta phải sử dụng alias. Đó là sự thay thế một địa chỉ người nhận bằng một hay nhiều địa chỉ khác. Địa chỉ dùng thay thế có thể là một người nhận, một danh sách người nhận, một chương trình, một tập tin hay là sự kết hợp của những loại này.

Các thông tin về alias (chẳng hạn tìm kiếm trong các tập tin), tùy chọn thứ nhất chỉ ra phương thức tìm kiếm các alias (chẳng hạn tìm kiếm trong các tập tin), tùy chọn thứ hai chỉ ra tập tin aliases sẽ được sử dụng.

# 6.4. DNS và Sendmail

DNS và Sendmail là dịch vụ có mối quan hệ mật thiết với nhau. Sendmail dựa vào dịch vụ DNS để chuyển mail từ mạnh bên trong ra bên ngoài và ngược lại. Khi chuyển mail đến. Cú pháp record MX:

[domain name] IN MX 0 [mail server]

Ví dụ:

T3h.com.IN MX 0 mailserver.t3h.com.

Một địa chỉ email thường có dạng sau:

[Username@subdomain...subdomain2.subdomain1.top-level-domain](mailto:Username@subdomain...subdomain2.subdomain1.top-level-domain).

Thành phần bên phải dấu @ là địa chỉ miền. Tên miền có thể là một tổ chức hoặc một vùng địa lý nào đó. Nó phân biệt chữ hoa và chữ thường.

TÀI LIỆU THAM KHẢO

1. Nhà Xuất Bản Giáo Dục Việt Nam, Hà Quang Thụy, Nguyễn Trí Thành, Giáo Trình Hệ Điều Hành Unix – Linux, 2011

2. Nhà Xuất Bản Khoa Học và Kỹ Thuật, Nguyễn Thanh Thủy, Nguyễn Quanh Huy, Nguyễn Hữu Đức, Đinh Lan Anh, Giáo trình nhập môn hệ điều hành Linux, 2005

3. Springer,K.Wang, systems programming in Unix/Linux,2018