

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

**======\*\*\*======**



**BÀI TẬP LỚN**

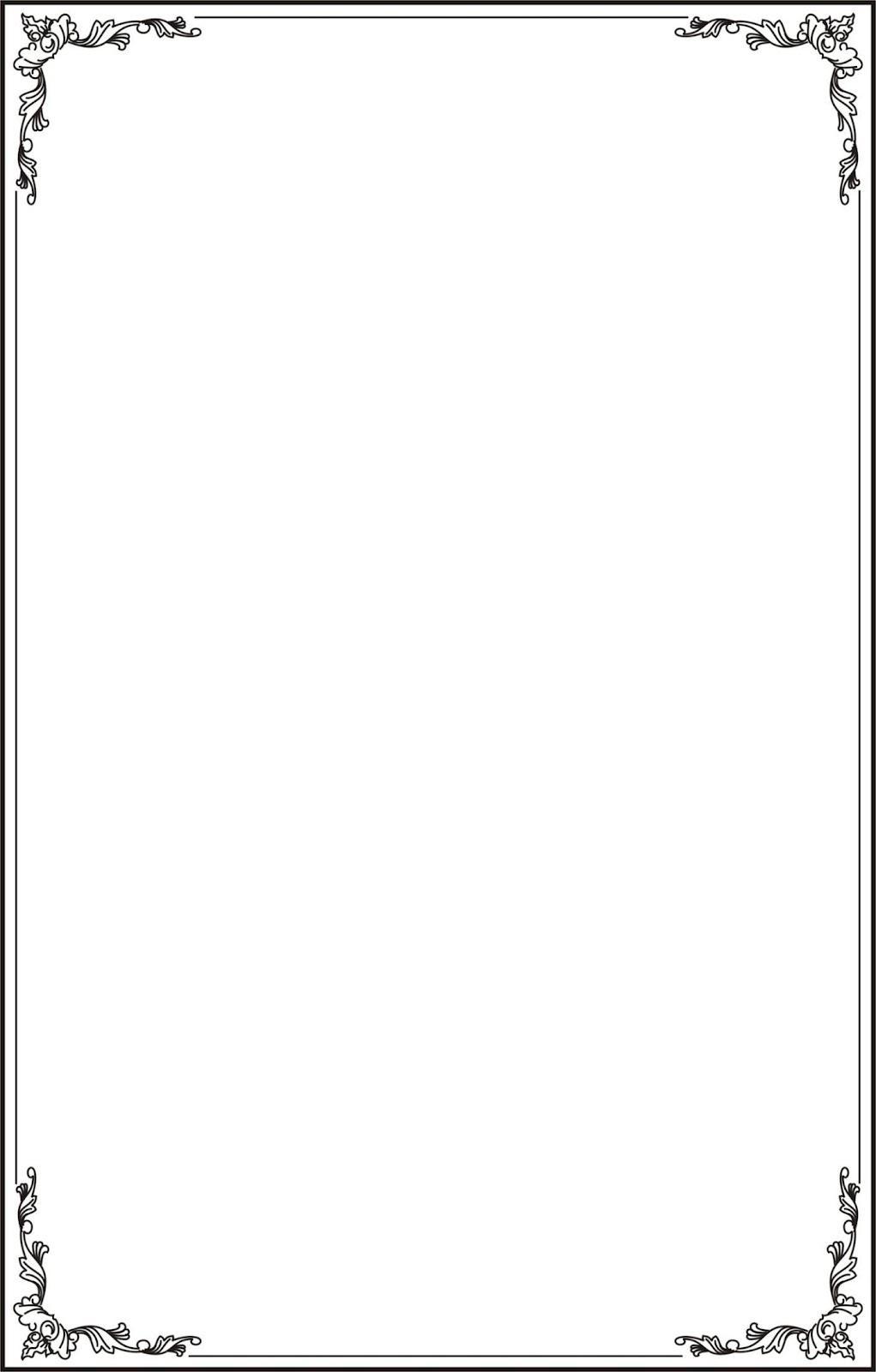
**MÔN : NGUYÊN LÝ HỆ ĐIỀU HÀNH**

**Đề tài**

***Nghiên cứu tìm hiểu về các Dịch vụ mạng trong HĐH Linux***

|  |  |  |
| --- | --- | --- |
|  | **Giáo viên hướng dẫn** | **: Ths Nguyễn Tuấn Tú** |
|  | **Nhóm số** | **:  14** |
|  | **Lớp** | **: 2021IT6025.6(006)\_K15** |

Hà Nội, 2022



**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

**======\*\*\*======**



**BÀI TẬP LỚN**

**MÔN : NGUYÊN LÝ HỆ ĐIỀU HÀNH**

**Đề tài**

***Nghiên cứu tìm hiểu về các Dịch vụ mạng trong HĐH Linux***

|  |  |  |
| --- | --- | --- |
|  | Giáo viên hướng dẫn: | Ths Nguyễn Tuấn Tú |
|  | Sinh viên thực hiện: |  |
|  |  | Nguyễn Thị Hà |
|  |  | Phạm Văn Hiếu |
|  |  | Đào Thị Linh |
|  |  | Trần Thị Thanh Thảo |
|  |  | Phạm Anh Tú |
|  | Lớp: | 2021IT6025.6(006)\_K15 |

Hà Nội, 2022

**Mục Lục**

[LỜI NÓI ĐẦU 5](#_Toc102944455)

[Giới thiệu về hệ điều hành linux 6](#_Toc102944456)

[Chương 1: Các tiện ích mạng của hệ điều hành linux 7](#_Toc102944457)

[1.1. Telnet 7](#_Toc102944458)

[1.1.1. Telnet 7](#_Toc102944459)

[1.1.2. Tiện ích của telnet 7](#_Toc102944460)

[1.1.3. Hoạt động của telnet 7](#_Toc102944461)

[*Hình 1.1. Mô hình client server* 7](#_Toc102944462)

[1.1.4. Yêu cầu để thực hiện được Telnet 7](#_Toc102944463)

[1.2. FTP. 8](#_Toc102944464)

[1.3. Ping 8](#_Toc102944465)

[1.3.1. Câu lệnh ping 8](#_Toc102944466)

[1.3.2. Ping hoạt động 8](#_Toc102944467)

[1.3.3. Tính năng bao gồm 8](#_Toc102944468)

[1.4. Traceroute 9](#_Toc102944469)

[Chương 2: Samba và DHCP 10](#_Toc102944470)

[2.1.Samba 10](#_Toc102944471)

[2.2.DHCP 10](#_Toc102944472)

[Chương 3: Networking 12](#_Toc102944473)

[3.1. Địa chỉ IP 12](#_Toc102944474)

[3.1.1. IP tĩnh và động 12](#_Toc102944475)

[3.1.2. Phân phối địa chỉ IP 12](#_Toc102944476)

[3.1.3. Cấu trúc và phân lớp địa chỉ IP 12](#_Toc102944477)

[3.2.Domain Name System (DNS) 14](#_Toc102944478)

[3.2.1. Giới thiệu về DNS 14](#_Toc102944479)

[3.2.2. Cơ chế phân giải tên 14](#_Toc102944480)

[*Hình 3.1 Quá trình phân giải grigiri.gbrmpa.gov.au trên mạng internet* 15](#_Toc102944481)

[Chương 4: Phân loại 17](#_Toc102944482)

[4.1. Phân loại Domain Name Server 17](#_Toc102944483)

[4.1.1.Primary Name Server 17](#_Toc102944484)

[4.1.2.Secondary Name Server 17](#_Toc102944485)

[4.1.3.Caching Name Server 17](#_Toc102944486)

[Chương 5: Proxy server 18](#_Toc102944487)

[5.1. Firewall 18](#_Toc102944488)

[5.1.1. Những chính sách Firewall 18](#_Toc102944489)

[5.1.2. Các loại Firewall và cách hoạt động 18](#_Toc102944490)

[*Hình 5.1 Sơ đồ liên kết mạng thông qua nhà cung cấp dịch vụ Internet.* 19](#_Toc102944491)

[*Hình 5.2.Sơ đồ liên kết mạng sử dụng router.* 20](#_Toc102944492)

[5.2.Squid Proxy 20](#_Toc102944493)

[Chương 6: Web server 22](#_Toc102944494)

[6.1. Giới thiệu về Web server. 22](#_Toc102944495)

[6.1.1. Giao thức HTTP 22](#_Toc102944496)

[6.1.2. Web server và cách hoạt động 22](#_Toc102944497)

[6.1.3.Web client 23](#_Toc102944498)

[6.1.4.Web động 23](#_Toc102944499)

[6.2.Giới thiệu Apache 23](#_Toc102944500)

[Chương 7: Mail server 24](#_Toc102944501)

[7.1.Những giao thức mail 24](#_Toc102944502)

[7.1.1.SMTP (Simple Mail Transfer Protocol) 24](#_Toc102944503)

[7.1.2.Post Office Protocol 24](#_Toc102944504)

[7.2.Giới thiệu về hệ thống mail 24](#_Toc102944505)

[*Hình 7.1. Sơ đồ về một hệ thống email đầy đủ các thành phần.* 25](#_Toc102944506)

[7.2.1.Mail gateway 25](#_Toc102944507)

[*Hình 7.2. Gateway giữa 2 giao thức truyền khác nhau.* 26](#_Toc102944508)

[7.2.2.Mail Host 26](#_Toc102944509)

[7.2.3.Mail Server 26](#_Toc102944510)

[7.2.4.Mail Client 26](#_Toc102944511)

[7.2.5.Một số sơ đồ hệ thống mail thường dùng 27](#_Toc102944512)

[*Hình 7.3. Cấu hình mail cục bộ* 27](#_Toc102944513)

[*Hình 7.4. Sơ đồ hệ thống mail cục bộ có kết nối từ xa.* 27](#_Toc102944514)

[*Hình 7.5. Sơ đồ hệ thống hai domain và một gateway.* 27](#_Toc102944515)

[7.3.Những chương trình mail và một số khái niệm 28](#_Toc102944516)

[7.3.1.Mail User Agent (MUA) 28](#_Toc102944517)

[7.3.2.Mail Transfer Agent (MTA***)*** 28](#_Toc102944518)

[7.3.3.Mailbox 28](#_Toc102944519)

[7.3.4.Hàng đợi (queue) 28](#_Toc102944520)

[7.3.5.Alias 29](#_Toc102944521)

[7.4.DNS và Sendmail 29](#_Toc102944522)

[KẾT LUẬN 31](#_Toc102944523)

# LỜI NÓI ĐẦU

Hiện nay, hệ điều hành được mọi người sử dụng phổ biến nhất là Windows, tuy nhiên bên cạnh đó cũng có một số hệ điều hành khác dễ sử dụng với nhiều tiện ích giống như Windows. Trong đó, phải kể đến hệ điều hành Linux . Linux có tính “mở” nên dễ sửa lỗi bởi một cộng đồng mã nguồn mở vì vậy nó có độ an toàn cao, ngoài ra Linux còn rất thích hợp cho việc quản trị mạng.

Phần bài tập lớn này nhằm cung cấp cho các bạn sinh viên và giáo viên các kiến thức tổng quan về hệ điều hành Linux và các dịch vụ mạng trong Linux.

Bài tập gồm 7 chương:

Chương 1: Các tiện ích mạng của hệ điều hành linux

Chương 2: Samba và DHCP

Chương 3: Networking

Chương 4: Phân loại

Chương 5: Proxy server

Chương 6: Web server

Chương 7: Mail server

Chúng em hi vọng phần bài tập lớn này sẽ cung cấp thêm phần nào kiến thức chuyên sâu về bộ môn hệ điều hành.

Tuy đã rất cố gắng trình bày chi tiết, đầy đủ và dễ hiểu nhất nhưng đâu đó vẫn không thể tránh khỏi những sai sót, nhầm lẫn không đáng có. Chúng em rất mong nhận được sự góp ý, bổ sung từ các thầy cô để ngày càng hoàn thiện hơn trong sự hiểu biết kiến thức chuyên sâu về máy tính.

Chúng em xin chân thành cảm ơn.

Nhóm sinh viên thực hiện!

# Giới thiệu về hệ điều hành linux

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 mềm tự do và của việc phát triển mã nguồn mở.

Phiên bản Linux đầu tiên do Linus 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, những 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 Windows) 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 Windows vì các trình điều khiển thiết bị tương thích với Windows 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 bởi vì mã nguồn mở của nó.

# Chương 1: Các tiện ích mạng của hệ điều hành linux

## 1.1. Telnet

### 1.1.1. 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.

### 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.

|  |  |
| --- | --- |
|  | wps20 |

### *Hình 1.1. 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.

FTP là viết tắt của Tệp Transfer Protocol, một tiện ích tải tệp ở xa. Với FTP có thể lấy tệp ở máy tính từ xa về máy tính của mình và ngược lại. FTP sử dụng giao thức TCP/IP, cổng 21.

Để sử dụng FTP thì các máy kết nối phải chạy các chương trình có hỗ trợ các dịch vụ về FTP. Client gọi đến server và thiết lập FTP thông qua một tập các lệnh bắt tay.

Thông thường để kết nối đến các máy khác qua FTP chúng ta phải là một user được cung cấp username và password để login vào máy cần truy xuất. Nhiều hệ thống sử dụng FPT mặc định.

## 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. 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.

### 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](about:blank).
* [Sự tắc nghẽn mạng](about:blank).
* [Time To Live](about:blank).

### 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

1. Traceroutelà 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. *Traceroute* sử dụng thời gian các giao thức IP `để sống 'lĩnh vực và nỗ lực để gợi ra một phản ứng ICMP TIME EXCEEDED từ mỗi cổng dọc theo con đường dẫn đến máy chủ một số.

2. 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. Khi lĩnh vực này đạt đến số không, router, trong khi các gói phần mềm chạy trong một vòng lặp, phá hủy các gói tin và gửi một [thông báo ICMP](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/icmp.php3&usg=ALkJrhgDSg1dAq9g6t60msedyO9YasnBfg) cho người gửi.

Như vậy, traceroute gửi gói tin đến cổng UDP không có đặc quyền được coi là không sử dụng (cổng mặc định 33.434) với một TTL của 1. Gặp các bộ định tuyến đầu tiên sẽ thả các gói tin và gửi một gói ICMP bao gồm cả việc đưa ra các địa chỉ IP của router và vòng lặp sự chậm trễ. Traceroute sẽ tăng tuần tự và đời sống lĩnh vực để có được một phản ứng từ mỗi router dọc theo con đường cho đến khi bạn nhận được một phản ứng của *"ICMP port unreachable" ("ICMP port unreachable")* từ máy tính này mục tiêu.

# Chương 2: Samba và DHCP

## 2.1.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.

## 2.2.DHCP

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) 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.

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 - respond 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 đã 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.

# Chương 3: Networking

Thông thường card mạng được nhận dạng tự động trong quá trình cài đặt linux và người đặt yêu cầu nhập vào thông tin cần thiết chuẩn bị cho một máy tính tham gia mạng (địa chỉ IP, subnet mask, hostname, domain name, DNS name). Sau khi linux được cài đặt xong, vẫn có thể thiết lập lại các thông tin nói trên với tiện ích netconf ở chế độ text hay network configuration trong Xwindows.

## 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 gầm các số 0 và 1) được đếm từ trái sang phải.

Cấu trúc được thể hiện 3 thành phần chính là:

|  |  |  |
| --- | --- | --- |
| Class bit | Net ID | Host ID |

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:

Octet 1 octet 2 octet 3 octet 4

1 8 16 24 32

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0 |  |  |  |  |

Net ID Host ID

Bit 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:

1 8 16 24 32

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 0 |  |  |  |  |

Net ID Host ID

Bit nhận dạng của lớp B là 10, 14 bit 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:

1 8 16 24 32

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 0 |  |  |  |  |

Net ID Host ID Host

Bit nhận dạng của lớp này 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

Dịch vụ DNS hoạt động theo mô hình Client – server: phần server gọi là máy phục vụ tên nameserver, còn phần Client là trinh phân giải tên resolver. Nameserver chứa các thông tin CSDL của DNS, còn resolver đơn giản chỉ là các hàm thư viện dùng để tạo các truy vấn (query) và gửi chúng đến name server. DNS được thi hành như một giao thức tầng Application trong mạng TCP/IP.

DNS là 1 CSDL phân tán. Điều này cho phép người quản trị cục bộ quản lý phần dữ liệu nội bộ hệ thống mạng theo mô hình Client – Server. Hiệu suất sử dụng dịch vụ được tăng cường thông qua cơ chế phân bản (replication) và lưu tạm (caching). Một hostname trong domain là sự kết hợp giữa những từ phân cách nhau bởi dấu chấm. Ví dụ: hostname là server.t3h.com, trong đó server là hostname và t3h.com là domain. Domain phân bổ theo cơ chế phân cấp tương tự như sự phân cấp của hệ thống tập tin Unix/Linux.

### 3.2.2. Cơ chế phân giải tên

1. Phân giải tên thành IP

Root name server: là máy chủ quản lý các nameserver ở mức top-level domain. Khi có truy vấn về 1 tên miền nào đó thì Root name server phải cung cấp tên và địa chỉ IP của name server quản lý top-level domain và đến lượt các name server của top-level domain cung cấp danh sách các name server có quyền trên các second-level domain mà tên miền này thuộc vào. Cứ như thế đến khi nào tìm được máy quản lý tên miền cần truy vấn. Qua trên cho thấy vai trò rất quan trọng của Root name server trong quá trình phân giải tên miền. Nếu mọi Root name server trên mạng internet không liên lạc được thì mọi yêu cầu phân giải đều không thực hiện được.

|  |
| --- |
|  |
|  | wps27 |

### *Hình 3.1 Quá trình phân giải grigiri.gbrmpa.gov.au trên mạng internet*

Client sẽ gửi yêu cầu cần phân giải địa chỉ IP của máy tính có tên grigiri.gbrmpa.gov.au đến name server cục bộ. Khi nhận yêu cầu từ Resolver, name server cục bộ sẽ phân tích tên này và xét tên miền này có do mình quản lý không. Nếu như tên miền do server cục bộ quản lý, nó sẽ trả lời địa chỉ IP của tên máy đó ngay cho Resolver. Ngược lại, server cục bộ sẽ truy vấn đến Root name server gần nhất mà nó biết được. Root name server sẽ trả lời địa chỉ IP của name server quản lý miền au. Máy chủ name server cục bộ lại hỏi tiếp name server quản lý miền au và được tham chiếu đến máy chủ quản lý miền gov.au. Máy chủ quản lý gov.au chỉ dẫn máy name server cục bộ tham chiếu đến máy chủ quản lý miên gbrmpa.gov.au. Cuối cùng máy name server cục bộ truy vấn máy chủ quản lý miền gbrmpa.gov.au và nhận được câu trả lời.

Các loại truy vấn: truy vấn có thể ở 2 dạng:

+ 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 phải thực hiện cho đến khi nào có kết quả mới thôi.

+ Truy vấn tương tác (Interactive query): 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 lúc đó. Bản thân name server không thực hiện bất cứ một truy vấn nào thêm. Thông tin tốt nhất trả về có thể lấy 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.

1. Phân giải IP thành tên máy tính

Ánh xạ địa chỉ IP thành tên máy tính được dùng để diễn dịch các tập tin log cho dễ đọc hơn. Nó còn dùng trong một số trường hợp chứng thực trên hệ thống UNIX (kiểm tra các tập tin .rhost hay host.equiv). Trong không gian tên miền đã nói ở trên dữ liệu bao gồm cả địa chỉ IP được lập chỉ mục theo tên miền. Do đó với một tên miền đã cho việc tìm ra địa chỉ IP khá dễ dàng.

Để có thể phân giải tên máy tính của một địa chỉ IP, trong không gian tên miền người ta bổ sung thêm một nhánh tên miền mà được lập chỉ mục theo địa chỉ IP. Phần không gian này có tên miền là in-addr.arpa.

Mỗi nút trong miền in-addr.arpa có một tên nhãn là chỉ số thập phân của địa chỉ IP.

*Lưu ý: khi đọc tên miền địa chỉ IP sẽ xuất hiện theo thứ tự ngược. ví dụ: nếu địa chỉ IP của máy winnie.corp.hp.com là 15.16.192.152, khi ánh xạ vào miền in-addr.arpa sẽ là 152.192.16.15.*

# Chương 4: Phân loại

## 4.1. Phân loại Domain Name Server

Có nhiều loại Domain Name Server được tổ chức trên internet. Sự phân loại này tùy thuộc vào nhiệm vụ mà chúng sẽ đảm nhận. Tiếp theo sau đây mô tử những loại Domain Name Server

### 4.1.1.Primary Name Server

Mỗi miền phải có một Primary Name Server. Server được đăng ký trên internet để quản lý miền. Mọi người trên internet đều biết tên máy tính và địa chỉ IP của server này. Người quản trị DNS sẽ tổ chức những tập tin CSDL trên Primary Name Server. Server này có nhiệm vụ phân giải tất cả các máy trong miền hay zone.

### 4.1.2.Secondary Name Server

Mỗi miền có một Primary Name Server để quản lý CSDL của miền. Nếu như server này tạm ngưng hoạt động vì một lý do nào đó thì việc phân giải tên máy tính thành địa chỉ IP và ngược lại xem như bị gián đoạn. Việc gián đoạn này làm ảnh hưởng rất lớn đến tổ chức có nhu cầu trao đổi thông tin ra ngoài internet cao. Nhằm khắc phục nhược điểm này, những nhà thiết kế đã đưa ra một server dự phòng gọi là Secondary (hay Slave) Name Server. Server này có nhiệm vụ sao lưu tất cả những dữ liệu trên Primary Name Server và khi Primary Name Server này bị gián đoạn thì nó sẽ đảm nhận công việc phân giải tên máy tính thành địa chỉ IP và ngược lại.trong một miền có thể có một hay nhiều Secondary Name Server. Tên và địa chỉ IP của Secondary Name Server cũng được mọi người trên internet biết đến.

### 4.1.3.Caching Name Server

Caching Name Server có chức năng phân giải tên máy trên những mạng ở xa thông qua những name server khác. Nó lưu giữ lại những tên máy đã được phân giải trước đó và được sử dụng lại những tên này nhằm mục đích:

+ Làm tăng tốc độ phân giải bằng cách sử dụng cache.

+ Giảm bớt gánh nặng phân giải tên máy cho các Name Server.

+ Giảm việc lưu thông trên mạng lớn.

# Chương 5: Proxy server

## 5.1. Firewall

Internet là một hệ thống mở, đó là điểm mạnh và cũng là điểm yếu của nó. Chính điểm yếu này làm giảm khả năng bảo mật thông tin nội bộ của hệ thống. Nếu chỉ là mạng LAN thì không có vấn đề gì, nhưng khi đã kết nối Internet thì phát sinh những vấn đề hết sức quan trọng trong việc quản lý các tài nguyên quý giá - nguồn thông tin chống việc truy cập bất hợp pháp trong khi vẫn cho phép người được ủy nhiệm sử dụng các nguồn thông tin mà họ được cấp quyền, và phương pháp chống rò rỉ thông tin trên các mạng truyền dữ liệu công cộng (Public Data Communication Network). Yêu cầu xây dựng hệ thống an ninh ngày càng quan trọng vì những lý do sau:

- Các đối thủ cạnh tranh luôn tìm cách để lấy được mọi thông tin của nhau.

- Các tay hacker tìm cách xâm nhập phá hoại hệ thống mạng nội bộ …

### 5.1.1. Những chính sách Firewall

Bước đầu tiên trong việc cấu hình Firewall là thiết lập các chính sách:

- Những dịch vụ nào cần ngăn chặn.

- Những host nào cần phục vụ.

- Mỗi nhóm cần truy xuất những dịch vụ nào.

- Mỗi dịch vụ sẽ được bảo vệ như thế nào.

### 5.1.2. Các loại Firewall và cách hoạt động

a. Packet filtering (Bộ lọc gói tin)

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. Các thông số có thể lọc được của một packet như:

- Địa chỉ IP nơi xuất phát (source IP address).

- Địa chỉ IP nơi nhận (destination IP address).

- Cổng TCP nơi xuất phát (source TCP port).

- Cổng TCP nơi nhận (destination TCP port).

Loại Firewall này cho phép kiểm soát được kết nối vào máy chủ, khóa việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép. Ngoài ra, nó còn kiểm soát hiệu suất sử dụng những dịch vụ đang hoạt động trên hệ thống mạng nội bộ thông qua các cổng TCP tương ứng.

b. Application gateway

Đây là loại Firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ dựa trên những giao thức được cho phép truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên mô hình Proxy Service. Trong mô hình này phải tồn tại một hay nhiều máy tính đóng vai trò Proxy Server. Một ứng dụng trong mạng nội bộ yêu cầu một đối tượng nào đó trên Internet, Proxy Server sẽ nhận yêu cầu này và chuyển đến server trên Internet. Khi server trên Internet trả lời, Proxy Server sẽ nhận và chuyển ngược lại cho ứng dụng đã gửi yêu cầu. Cơ chế lọc của packet filtering kết hợp với cơ chế “đại diện” của application gateway cung cấp một khả năng an toàn và uyển chuyển hơn, đặc biệt khi kiểm soát các truy cập từ bên ngoài.

|  |
| --- |
|  |
|  | wps28 |

### *Hình 5.1 Sơ đồ liên kết mạng thông qua nhà cung cấp dịch vụ Internet.*

Cơ chế bộ lọc packet kết hợp với cơ chế proxy có nhược điểm là hiện nay các ứng dụng đang phát triển rất nhanh, do đó nếu các proxy có nhược điểm là hiện nay các ứng dụng đang phát triển rất nhanh, do đó nếu các proxy không đáp ứng kịp cho các ứng dụng, nguy cơ mất an toàn sẽ tăng lên.Thông thường những phần mềm Proxy Server hoạt động như một gateway nối giữa hai mạng, mạng bên ngoài và mạng bên trong.

Đường kết nối giữa Proxy Server thông qua nhà cung cấp dịch vụ Internet (Internet Service Provider – SIP) có thể chọn một trong các cách sau:

- Dùng modem analog: sử dụng giao thức SLIP/PPP để kết nối vào ISP và truy cập Internet. Dùng dial-up thì tốc độ bị giới hạn, thường là 28.8 Kbps – 36.6 Kbps. Hiện nay đã có modem analog thích hợp cho các tổ chức nhỏ , chỉ có nhu cầu sử dụng dịch vụ Web và email.

- Dùng đường ISDN: Dịch vụ ISDN (Integrated Services Digital Network) đã khá phổ biến ở một số nước tiên tiến. Dịch vụ này dùng tín hiệu số trên đường truyền nên không cần modem analog, cho phép truyền cả tiếng nói và dữ liệu trên một đôi dây. Các kênh thuê bao ISDN (đường truyền dẫn thông tin giữa người sử dụng và mạng) có thể đạt tốc độ từ 64 Kbps đến 138,24 Mbps. Dịch vụ ISDN thích hợp cho các công ty vừa và lớn, yêu cầu băng thông lớn mà việc dùng modem analog không đáp ứng được.

|  |
| --- |
|  |
|  | wps29 |

### *Hình 5.2.Sơ đồ liên kết mạng sử dụng router.*

Phần cứng dùng để kết nối tùy thuộc vào việc nối kết trực tiếp Proxy Server với Internet hoặc thông qua một router. Dùng dial-up đòi hỏi phải có modem analog, dùng ISDN phải có bộ phối ghép ISDN cài trên server.

Việc chọn lựa cách kết nối và một số ISP thích hợp tùy thuộc vào yêu cầu cụ thể của công ty, ví dụ như số người cần truy cập Internet, các dịch vụ và ứng dụng nào được sử dụng, các đường kết nối và cách tính cước mà ISP có thể cung cấp.

## 5.2.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 6: Web server

## 6.1. Giới thiệu về Web server.

### 6.1.1. Giao thức HTTP

HTTP là một giao thức cho phép trình duyệt Web Browser 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 thông qua kết nối TCP. Do đó, kết nối HTTP có thể thay thế bằng cách dùng lệnh “telnet” chuẩn.

### 6.1.2. Web server và cách hoạt động

Ban đầu Web Server chỉ phục vụ các tài liệu HTML và hình ảnh đơn 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.

### 6.1.3.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 lý bởi Web Server.

### 6.1.4.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.

## 6.2.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 7: Mail server

## 7.1.Những giao thức mail

Hệ thống mail xây dựng dựa trên một số giao thức sau:

Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), Multipurpose Internet Mail Extensions (MIME) và Interactive Mail Access Protocol (IMAP), được định trong RFC 1176 là giao thức quan trọng được thiết kế để thanh thế POP, nó cung cấp nhiều cơ chế tìm kiếm văn bản, phân tích message từ xa mà ta không tìm thấy trong POP. Trong phần này ta chỉ quan tâm tới ba giao thức SMTP, POP, MIME trong hệ thống mail.

### 7.1.1.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.

### 7.1.2.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.

## 7.2.Giới thiệu về hệ thống mail

|  |
| --- |
|  |
|  | wps30 |

### *Hình 7.1. Sơ đồ về một hệ thống email đầy đủ các thành phần.*

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.

### 7.2.1.Mail gateway

Một mail gateway là máy kết nối giữa các mạng dùng các giao thức truyền thông khác nhau hoặc kết nối các mạng khác nhau dùng chung giao thức. Ví dụ một gateway có thể kết nối một hoặc nhiều TCP/IP với một mạng chạy bộ giao thức Systems Network Architecture (SNA).

Một mail gateway đơn giản nhất dùng để kết nối 2 mạng dùng chung giao thức hoặc mailer. Khi đó mail gateway chuyển mail giữa domin nội bộ và các domain bên ngoại. Mail gateway cũng kết nối 2 mạng dùng mailer khác nhau như hình vẽ dưới:

|  |
| --- |
|  |
|  | wps31 |

### *Hình 7.2. Gateway giữa 2 giao thức truyền khác nhau.*

### 7.2.2.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.

### 7.2.3.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 trợ POP/IMAP và trên Mail Server cũng hỗ trợ POP/IMAP thì người dùng có thể đọc thư bằng POP/IMAP.

### 7.2.4.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.

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

a.Hệ thống mail cục bộ.

|  |
| --- |
|  |
|  | wps32 |

### *Hình 7.3. Cấu hình mail cục bộ*

Cấu hình hệ thống mail đơn giản gồm một hoặc nhiều trạm làm việc kết nối vào một Mail Server. Tất cả mail đều chuyển cục bộ.

b.Hệ thống mail cục bộ có kết nối từ xa:

|  |
| --- |
|  |
|  | wps33 |

### *Hình 7.4. Sơ đồ hệ thống mail cục bộ có kết nối từ xa.*

Hệ thống mail trong một mạng nhỏ gồm một mail server, một mail host và một mail gateway kết nối với hệ thống bên ngoài. Không cần DNS server.

c.Hệ thống hai domain và một gateway.

|  |
| --- |
|  |
|  | wps34 |

### *Hình 7.5. Sơ đồ hệ thống hai domain và một gateway.*

Cấu hình dưới đây gồm 2 domain và 1 mail gateway. Trong cấu hình này mail server, mail host, và mail gateway (hoặc gateway) cho mỗi domain hoạt động như một hệ thống độc lập. Để quản trị và phân phối mail cho 2 domain thì dịch vụ DNS buộc phải có.

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

### 7.3.1.Mail User Agent (MUA)

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

### 7.3.2.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 nhiệm 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.

### 7.3.3.Mailbox

Mailbox là một tập tin lưu trữ tất cả các mail của người dùng. Trên hệ thống Unix, khi thêm một tài khoản người dùng vào hệ thống đồng thời sẽ tạo ra một mailbox cho người dùng đó. Thông thường, tên của mailbox trùng với tên đăng nhập của người dùng. Tập tin này đặt trong thư mục /var/spool/mail. Khi có mail gửi đến cho người dùng, chương trình xử lý mail của server cục bộ sẽ phân phối mail này vào mailbox tương ứng. Trong tập tin mailbox, mỗi mail bắt đầu bằng dòng có từ khóa From và kết thúc bằng một dòng trắng.

Khi người dùng đăng nhập vào hệ thống và sử dụng mail client để nhận mail (hoặc telnet trực tiếp vào mail server để nhận), POP Server sẽ vào thư mục /var/spool/mail lấy từ mailbox chuyển cho người dùng.

Thông thường, sau khi client nhận mail, các mail trong box sẽ bị xóa. Tuy nhiên, người dùng cũng có thể yêu cầu giữ lại mail trên mailbox, điều thực hiện nhờ vào một tùy chọn của mail client.

### 7.3.4.Hàng đợi (queue)

Các mail gửi đi có thể được chuyển đi ngay hoặc cũng có thể được chuyển vào hàng đợi. Có nhiều nguyên nhân khiến một mail bị giữ lại trong hàng đợi:

- Khi mail đó tạm thời chưa thể chuyển đi được hoặc có một số địa chỉ trong danh sách người nhận chưa thể chuyển đến được vào thời điểm hiện tại.

- Khi tùy chọn cấu hình phân phát mail có giá trị là True, khi đó tất cả các mail đều bị giữ lại cho đến khi việc phân phối hoàn tất.

- Khi giá trị Delivery Mode(d) bằng queue-only hoặc defer thì tất cả các mail đều bị giữ lại trong hàng đợi.

- Khi số lượng tiến trình phân phối bị tắc nghẽn vượt quá giới hạn quy định bởi tùy chọn QueueLA(x).

### 7.3.5.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.

## 7.4.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*](about:blank)*.*

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] Vũ Xuân Thắng, Giáo trình Hệ điều hành mã nguồn mở, Trường Đại học Sư phạm kỹ thuật Hưng Yên, 2013.

[2]. Linux Networking Cookbook- Carla Schroder.

[3] Chứng chỉ quản trị mạng Linux- Trung tâm tin học- Đại học khoa học tự nhiên Tp.HCM.

[4]. Các video hướng dẫn cài đặt dịch vụ mạng trên Linux, tham khảo trên trang www.youtube.com.

# KẾT LUẬN

Tổng kết:

Dịch vụ DNS server và DHCP là hai trong số 6 dịch vụ mạng trong hệ điều hành Linux và đây cũng là hai dịch vụ mạng đơn giản nhất và nhất thiết phải có khi xây dựng hệ điều hành.

Xây dựng DNS server cho phép truy vấn cục bộ và truy vấn internet.

xây dựng DHCP sẽ tự động cấp phát các thông số về địa chỉ IP cho tất cả các máy tham gia vào mạng.

Để xây dựng một hệ thống mạng cho một tổ chức, doanh nghiệp yêu cầu chúng ta phải nắm rõ cách thức hoạt động cũng như cách cài đặt, tổ chức các dịch vụ mạng một cách chuyên nghiệp. Chúng em hi vọng có thể tham gia vào quá trình triển khai- thiết kế quản trị và phát triển hệ thống mạng cho tổ chức, doanh nghiệp.

Lời cuối cùng chúng em xin gửi lời cảm ơn chân thành tới thầy giáo Nguyễn Tuấn Tú, người đã tận tình chỉ bảo giúp đỡ em hoàn thành bài tập lớn này.