ỦY BAN NHÂN DÂN QUẬN 9
TRƯỜNG TCN ĐÔNG SÀI GÒN
-------□★□-------
KHOA CÔNG NGHỆ THÔNG TIN

BÀI GIẢNG
HỆ ĐIỀU HÀNH LINUX

GVGD: TRẦN QUỐC VƯƠNG

LƯU HÀNH NỘI BỘ
Năm 2019

MỤC LỤC

ĐỀ MỤC **TRANG**

MÔ ĐUN: HỆ ĐIỀU HÀNH LINUX

Mã mô đun: MĐ 40
Vị trí, tính chất, ý nghĩa của mô đun:

- Vị trí: Mô đun được bố trí sau khi sinh viên học xong các mô đun quản trị mạng 1, quản trị mạng 2, cấu hình quản trị thiết bị mạng và công nghệ mạng không dây.
- Tính chất: Là mô đun chuyên ngành.
- Ý nghĩa: Là mô đun giúp sinh viên có kiến thức và kỹ năng về hệ điều hành mã nguồn mở.

Mục tiêu của mô đun:

- Trình bày được các khái niệm cơ bản cấu trúc, chức năng các thành phần trong hệ điều hành Linux;
- Giải thích được các khái niệm cơ bản của hệ điều hành Linux;
- Mô tả được cấu trúc, chức năng của các thành phần trong hệ điều hành Linux;
- Sử dụng được các chức năng và dịch vụ của hệ điều hành Linux phục vụ công tác quản trị mạng;
- Bố trí làm việc khoa học đảm bảo an toàn cho người và phương tiện học tập.

Nội dung chính của mô đun:

Mã bài	Tên các bài trong mô-đun	Thời lượng			
		Tổng số	Lý thuyết	Thực hành	Kiểm tra
MĐ 40-01	Tổng quan về hệ điều hành Linux	3	3		
MĐ 40-02	Cài đặt hệ điều hành Linux	14	4	9	1
MĐ 40-03	Thao tác với tập tin và thư mục	14	4	10	
MĐ 40-04	Giao diện đồ họa X	14	4	9	1
MĐ 40-05	Quản trị người dùng và nhóm	9	3	6	
MĐ 40-06	Cấu hình mạng	9	3	5	1

MĐ 40-07	Cài đặt dịch vụ trên máy chủ Linux	18	6	12	
MĐ 40-08	Quản lý máy chủ Linux bằng Webmin	9	3	5	1
Tổng cộng		**90**	**30**	**56**	**4**

YÊU CẦU VỀ ĐÁNH GIÁ HOÀN THÀNH MÔ ĐUN

- Đánh giá kiến thức bằng các bài kiểm tra viết hoặc vấn đáp cơ bản đạt những yêu cầu sau:
  + Trình bày được các khái niệm cơ bản cấu trúc, chức năng các thành phần trong hệ điều hành Linux;
  + Giải thích được các khái niệm cơ bản của hệ điều hành Linux;
  + Mô tả được cấu trúc, chức năng của các thành phần trong hệ điều hành Linux;
  + Sử dụng được các chức năng và dịch vụ của hệ điều hành Linux phục vụ công tác quản trị mạng;
  + Bố trí làm việc khoa học đảm bảo an toàn cho người và phương tiện học tập.
- Đánh giá kỹ năng của sinh viên bằng các bài tập:
  + Cài đặt và sử dụng hệ điều hành Linux
  + Thực thi được các thao tác tập tin, thư mục, quản lý người dùng
  + Cài đặt và cấu hình các dịch vụ mạng
  + Tổ chức hệ thống cho phép người sử dụng làm việc từ xa
- Đánh giá thái độ: Đánh giá tính tự giác, tính kỷ luật, tham gia đầy đủ thời lượng mô đun, cẩn thận, tỉ mỉ, chính xác trong công việc.

BÀI 1: TỔNG QUAN VỀ HỆ ĐIỀU HÀNH LINUX

Mã bài: MĐ 40-01

Mục tiêu:

- Trình bày được lịch sử phát triển của Linux;
- Nắm được các đặc tính cơ bản của hệ điều hành;
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Lịch sử phát triển Unix và Linux

Mục tiêu: Giới thiệu cho người học về hệ điều hành mã nguồn mở - Linux, nguyên nhân phát triển hệ điều hành này.

1.1. Giới thiệu

Linux – Hệ điều hành mã nguồn mở – đến nay đã có thể sánh vai với các hệ điều hành thương phẩm như MS Windows, Sun Solaris v.v… Linux ra đời từ một dự án đầu những năm 1990 có mục đích tạo ra một hệ điều hành kiểu UNIX cài đặt trên máy tính cá nhân tương hợp họ máy tính IBM-PC.

Ngày nay Linux có thể cài đặt trên nhiều họ máy tính khác nhau. Qua Internet, Linux được hàng nghìn nhà lập trình khắp trên thế giới tham gia thiết kế, xây dựng và phát triển, với mục tiêu không lệ thuộc vào bất kỳ thương phẩm nào và để cho mọi người đều có thể sử dụng. Linux xuất phát từ ý tưởng của Linus Torvalds – sinh viên Đại học Helsinki ở Phần Lan.

Về cơ bản, Linux bắt chước UNIX nên mang nhiều ưu điểm của UNIX. Tính đa nhiệm thực sự của Linux cho phép chạy nhiều chương trình cùng lúc.

Linux là hệ điều hành đa người dùng, nghĩa là nhiều người có thể đăng nhập và cùng lúc sử dụng một hệ thống. Ưu điểm này có vẻ không phát huy mấy trên máy PC ở nhà, song ở trong công ty hoặc trường học thì nó giúp cho việc dùng chung tài nguyên, từ đó giảm thiểu chi phí đầu tư vào máy móc.

Linux không phải là đồ chơi sẵn có, nó được thiết kế nhằm mang đến cho người sử dụng cảm giác cùng tham gia vào một dự án mới. Tuy nhiên thực tế cho thấy Linux chạy tương đối ổn định.

1.2. Tại sao Linux phát triển?

Linux phát triển vì là một trong những hệ điều hành miễn phí và có khả năng đa nhiệm cho nhiều người sử dụng cùng lúc trên các máy tính tương thích với PC. So với những hệ điều hành thương phẩm, Linux ít phải nâng cấp và không cần trả tiền, cũng như phần lớn các phần mềm ứng dụng cho nó. Hơn nữa, Linux và những ứng dụng được cung cấp với cả mã nguồn miễn phí, sau đó chỉnh sửa và mở rộng chức năng của chúng theo nhu cầu riêng.

Linux có khả năng thay thế một số hệ điều hành thuộc họ UNIX đắt tiền. Nếu tại nơi làm việc sử dụng UNIX thì ở nhà cũng thích sử dụng một hệ nào đó giống như thế nhưng rẻ tiền. Linux giúp ta dễ dàng truy cập, lướt Web và gửi nhận thông tin trên Internet.

Một nguyên nhân khác làm cho Linux dễ đến với người dùng là Linux cung cấp mã nguồn mở cho mọi người. Điều này đã khiến một số tổ chức, cá nhân hay quốc gia đầu tư vào Linux nhằm mở rộng sự lựa chọn ngoài các phần mềm đóng kín mã nguồn. Linux không bị lệ thuộc Microsoft Windows.

Tại Việt Nam, việc nghiên cứu xây dựng một hệ điều hành từ kernel Linux đã thu được một số thành công nhất định. Chẳng hạn Vietkey Linux và CMC RedHat Linux (phiên bản tiếng Việt của RedHat Linux 6.2).

Gần đây, các công ty nổi tiếng như IBM, Sun, Intel, Oracle cũng bắt đầu nghiên cứu Linux và xây dựng các phần mềm ứng dụng cho nó.

2. Các dòng sản phẩm

Mục tiêu: Trình bày một số dòng sản phẩm nguồn mở thông dụng

Nhiều người đã biết đến các nhà sản xuất phần mềm RedHat, ManDrake, SuSE, Corel và Caldera. Có thể chính ta cũng đã từng nghe đến tên các phiên bản Linux như Slackware, Debian, TurboLinux và VA Linux, v.v… Quả thật, Linux được phát hành bởi nhiều nhà sản xuất khác nhau, mỗi bản phát hành là một bộ chương trình chạy trên nhóm tệp lõi (kernel) của Linus Tordvalds. Mỗi bản như vậy đều dựa trên một kernel nào đó, thí dụ bản RedHat Linux 6.2 sử dụng phiên bản kernel 2.2.4.

Hãng RedHat đã làm ra chương trình quản lý đóng gói RPM (RedHat Package Manager), một công cụ miễn phí giúp cho bất cứ ai cũng có thể tự đóng gói và phát hành một phiên bản Linux của chính mình. Thí dụ bản OpenLinux của Caldera cũng đã được tạo ra như thế.

Linux cung cấp cho ta một môi trường học lập trình mà hiện nay chưa có hệ nào sánh được. Với Linux, ta có đầy đủ cả mã nguồn, trong khi đó các sản phẩm mang tính thương mại thường không tiết lộ mã nguồn.

Song với sự xuất hiện của bộ vi xử lý đầu tiên (1971) rồi máy tính cá nhân (1975), mọi việc đã thay đổi. Thoạt tiên, đó là đất dụng võ của các tay hacker say mê vi tính. Họ thậm chí có thể tự làm ra những máy tính cá nhân và hệ điều hành đơn giản, nhưng các hệ này chưa làm gì được nhiều ở góc độ hiệu năng. Với kinh nghiệm tích lũy dần theo năm tháng, một số hacker đã trở thành nhà doanh nghiệp, rồi cùng với khả năng tích hợp ngày càng cao của các vi mạch, PC đã trở thành phổ biến.

Tính khả chuyển của một hệ điều hành giúp ta chuyển nó từ một nền này sang nền khác mà vẫn hoạt động tốt.

Hiện nay UNIX và Linux có khả năng chạy trên bất kỳ nền nào, từ máy xách tay cho đến máy tính lớn. Nhờ tính khả chuyển, các máy tính chạy UNIX

và Linux trên nhiều nền khác nhau có thể liên lạc với nhau một cách chính xác và hữu hiệu.

Linux đã có hàng ngàn ứng dụng, từ các chương trình bảng tính điện tử, quản trị cơ sở dữ liệu, xử lý văn bản đến các chương trình phát triển phần mềm cho nhiều ngôn ngữ, chưa kể nhiều phần mềm viễn thông trọn gói.

3. Ưu khuyết điểm

Mục tiêu: Trình bày các ưu và khuyết điểm chính của hệ điều hành Linux.

3.1. Linux cộng sinh với Windows

Về nguyên tắc, tất cả các phần mềm đang chạy trên DOS hoặc Windows sẽ không chạy trực tiếp với Linux, nhưng 3 hệ điều hành này có thể cộng sinh trên cùng một máy PC, dĩ nhiên mỗi lúc chỉ chạy được một hệ điều hành thôi. Ta cũng có thể cài thêm một chương trình đặc biệt tên là "VMWARE" để phỏng tạo một hay nhiều hệ điều hành khác nhau chạy đồng thời trên cùng một máy với điều kiện máy phải có cấu hình thích hợp và đủ mạnh.

3.2. Thương mại hóa Linux

Linux chưa thể khắc phục hết ngay những bất tiện và sai sót. Nhưng càng ngày càng có thêm công ty mới đầu tư cho Linux và đưa ra các giải pháp có tính thương mại với giá rẻ. Chẳng hạn là RedHat và Caldera.

Cả hai công ty này đều trợ giúp kỹ thuật qua e-mail, fax và qua mạng cho những người đã mua các phiên bản Linux và sản phẩm của họ mà không dành cho những người sao chép các bản miễn phí.

Vì tính kinh tế, Linux và các chương trình kèm theo thường được chạy trên mạng nội bộ của nhiều doanh nghiệp, chẳng hạn làm các dịch vụ Web, tên miền (DNS), định tuyến (routing) và tường lửa. Nhiều nhà cung cấp dịch vụ Internet (ISP) cũng dùng Linux làm hệ điều hành chính.

4. Kiến trúc của Linux

Mục tiêu: Trình bày các thành phần chính cấu thành hệ điều hành Linux và chức năng chính của mỗi thành phần trong cấu trúc.

Linux gồm 3 thành phần chính: kernel, shell và cấu trúc tệp.

Kernel là chương trình nhân, chạy các chương trình và quản lý các thiết bị phần cứng như đĩa và máy in.

Shell (môi trường) cung cấp giao diện cho người sử dụng, còn được mô tả như một bộ biên dịch. Shell nhận các câu lệnh từ người sử dụng và gửi các câu lệnh đó cho nhân thực hiện. Nhiều shell được phát triển. Linux cung cấp một số shell như: desktops, windows manager, và môi trường dòng lệnh. Hiện nay chủ yếu tồn tại 3 shell: Bourne, Korn và C shell. Bourne được phát triển tại phòng thí nghiệm Bell, C shell được phát triển cho phiên bản BSD của UNIX, Korn shell là phiên bản cải tiến của Bourne shell. Những phiên bản hiện nay của Unix, bao gồm cả Linux, tích hợp cả 3 shell trên.

Cấu trúc tệp quy định cách lưu trữ các tệp trên đĩa. Tệp được nhóm trong các thư mục. Mỗi thư mục có thể chứa tệp và các thư mục con khác. Người dùng có thể tạo các tệp/thư mục của riêng mình cũng như dịch chuyển các tệp giữa các thư mục đó. Hơn nữa, với Linux người dùng có thể thiết lập quyền truy nhập tệp/thư mục, cho phép hay hạn chế một người dùng hoặc một nhóm truy nhập tệp. Các thư mục trong Linux được tổ chức theo cấu trúc cây, bắt đầu bằng một thư mục gốc (root). Các thư mục khác được phân nhánh từ thư mục này.

Kernel, shell và cấu trúc tệp cấu thành cấu trúc hệ điều hành. Với những thành phần trên người dùng có thể chạy chương trình, quản lý tệp và tương tác với hệ thống.

5. Các đặc tính cơ bản

Mục tiêu: So với các hệ điều hành khác, Linux mang một số đặc điểm chính được liệt kê sau. Đây là các đặc điểm cơ bản giúp người dùng định hướng lựa chọn sử dụng.

Một số đặc điểm cơ bản của Linux:

5.1. Đa tiến trình

Là đặc tính cho phép người dùng thực hiện nhiều tiến trình đồng thời. Máy tính sử dụng chỉ một CPU nhưng xử lý đồng thời nhiều tiến trình cùng lúc.

5.2. Tốc độ cao

Hệ điều hành Linux được biết đến như một hệ điều hành có tốc độ xử lý cao, bởi vì nó thao tác rất hiệu quả đến tài nguyên như: bộ nhớ, đĩa…

5.3. Bộ nhớ ảo

Khi hệ thống sử dụng quá nhiều chương trình lớn dẫn đến không đủ bộ nhớ chính (RAM) để hoạt động, Linux dùng bộ nhớ từ đĩa là partition swap. Hệ thống sẽ đưa các chương trình hoặc dữ liệu nào chưa có yêu cầu truy xuất xuống vùng swap này, khi có nhu cầu thì hệ thống chuyển lên bộ nhớ chính.

5.4. Sử dụng chung thư viện

Hệ thống Linux có rất nhiều thư viện dùng chung cho nhiều ứng dụng. Điều này sẽ giúp hệ thống tiết kiệm được tài nguyên và thời gian xử lý.

5.5. Sử dụng các chương trình xử lý văn bản

Chương trình xử lý văn bản là một trong nhưng chương trình rất cần thiết đối với người sử dụng. Linux cung cấp nhiều chương trình cho phép người dùng thao tác với văn bản như vi, emacs, nroff,…

5.6. Sử dụng giao diện cửa sổ

Giao diện cửa sổ dùng Hệ thống X Window, có giao diện như hệ điều hành Windows. Với hệ thống này người dùng rất thuận tiện khi làm việc trên hệ

thống. X Window System hay còn gọi tắt là X được phát triển tại viện Massachusetts Institute of Technology. Nó được phát triển để tạo ra môi trường làm việc không phụ thuộc phần cứng. X chạy dưới dạng client –server. Hệ thống X Window hoạt động qua hai bộ phận:

- Phần server còn gọi là X server
- Phần client được gọi là X Window manager hay desktop environment.

X server sử dụng trong hầu hết các bản phân phối của Linux là Xfree86. Client sử dụng thường là KDE (K Desktop Environment) và GNOME (GNU Network Object Model Environment).

5.7. Network Information Service (NIS)

Dịch vụ NIS cho phép chia xẻ các tập tin password và group trên mạng. NIS là một hệ thống cơ sở dữ liệu dạng client-server, chứa các thông tin của người dùng và dùng để chứng thực người dùng. NIS xuất phát từ hãng Sun Microsystems với tên là Yellow Pages.

5.8. Lập lịch hoạt động chương trình, ứng dụng

Chương trình lập lịch trong Linux xác định các ứng dụng, script thực thi theo một sự sắp xếp của người dùng như: at, cron, batch.

5.9. Các tiện ích sao lưu dữ liệu

Linux cung cấp các tiện ích như tar, cpio và dd để sao lưu và backup dữ liệu. RedHat Linux còn cung cấp tiện ích Backup and Restore System Unix (BRU) cho phép tự động backup dữ liệu theo lịch.

5.10. Hỗ trợ nhiều ngôn ngữ lập trình

Linux cung cấp một môi trường lập trình Unix đầy đủ bao gồm các thư viện chuẩn, các công cụ lập trình, trình biên dịch, chương trình debug. Ngôn ngữ chủ yếu sử dụng trong các hệ điều hành Unix là C và C++. Linux dùng trình biên dịch cho C và C++ là gcc, chương trình biên dịch này rất mạnh, hỗ trợ

nhiều tính năng. Ngoài C, Linux cũng cung cấp các trình biên dịch, thông dịch cho các ngôn ngữ khác như Pascal, Fortran, Java…

Câu hỏi

1. Linux là gì? Nêu các đặc điểm của hệ điều hành Linux.

2. So sánh các ưu khuyết điểm của hệ điều hành Linux so với hệ điều hành Windows.

3. Trình bày kiến trúc và chức năng các thành phần chính của Linux.

BÀI 2: CÀI ĐẶT HỆ ĐIỀU HÀNH LINUX

Mã bài: MĐ 40-02

Mục tiêu:

- Nắm yêu cầu đối với hệ thống cài đặt hệ điều hành Linux;
- Thực hiện việc cài đặt hệ điều hành lên máy tính;
- Thực hiện cấu hình thiết bị;
- Cài đặt các gói phần mềm;
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Yêu cầu đối với hệ thống

Mục tiêu: So với các hệ điều hành khác, Linux yêu cầu cấu hình hệ thống không cao. Phần này trình bày cấu hình tối thiểu một hệ thống cần đảm bảo để hệ điều hành Linux hoạt động. Tuy nhiên, đây là khuyến cáo tối thiểu; Trên thực tế, cấu hình hệ thống càng cao càng tốt.

Linux không đòi hỏi máy có cấu hình mạnh. Tuy nhiên nếu phần cứng có cấu hình thấp quá thì có thể không chạy được X Window hay các ứng dụng có sẵn. Cấu hình tối thiểu nên dùng:

- CPU: Pentium MMX trở lên.
- RAM: 64 MB trở lên cho Text mode, 192MB cho mode Graphics.
- Đĩa cứng: Dung lượng đĩa còn phụ thuộc vào loại cài đặt.
    + Custom Installation (minimum): 520MB.
    + Server (minimum): 870MB.
    + Personal Desktop: 1.9GB.
    + Workstation: 2.4GB.
    + Custom Installation (everything): 5.3GB.
- 2M cho card màn hình nếu muốn sử dụng mode đồ họa.

2. Quá trình cài đặt

Mục tiêu: Phần này sẽ trình bày chi tiết quá trình cài đặt hệ thống, giúp người học có thể tự cài đặt hệ thống với hệ điều hành Linux một cách dễ dàng.

2.1. Chọn phương thức cài đặt

Nguồn cài đặt từ:

- CD-Rom: Có thể khởi động từ CD-ROM hoặc khởi động bằng đĩa mềm boot.

- Đĩa cứng: Cần sử dụng đĩa mềm boot (dùng lệnh dd hoặc mkbootdisk để tạo đĩa mềm boot).

- FS image: Sử dụng đĩa khởi động mạng. Kết nối tới NFS sever.

- FTP: Sử dụng đĩa khởi động mạng. Cài trực tiếp qua kết nối FTP.

- HTTP: Sử dụng đĩa khởi động mạng. Cài trực tiếp qua kết nối HTTP.

2.2. Chọn chế độ cài đặt

Chúng ta có thể chọn các chế độ:

- Linux text: chế độ text (Text mode).

- [Enter]: chế độ đồ họa (Graphical mode)

2.3. Chọn ngôn ngữ hiển thị trong quá trình cài đặt

Chọn ngôn ngữ “English” rồi chọn Next

2.4. Cấu hình bàn phím

Chọn loại bàn phím của mình, chọn Next

2.5. Chọn cấu hình mouse

Chọn loại Mouse phù hợp với mouse của mình. Khi chọn lưu ý cổng gắn mouse là serial hay PS/2, chọn Next.

2.6. Lựa chọn loại màn hình

Thông thường hệ điều hành sẽ tự động nhận đúng loại màn hình hiển thị, nếu không ta phải cấu hình lại màn hình hiển thị trong hộp thoại bên phải. Chọn Next.

2.7. Lựa chọn loại cài đặt

Một số loại cài đặt thông dụng:

- **Workstation**: Cài đặt hệ điều hành phục vụ cho công việc của một máy trạm.

- **Server:** Cài đặt hệ điều hành phục vụ cho máy chủ.

- **Custom:** có thể tích hợp các tùy chọn trên một cách tùy ý.

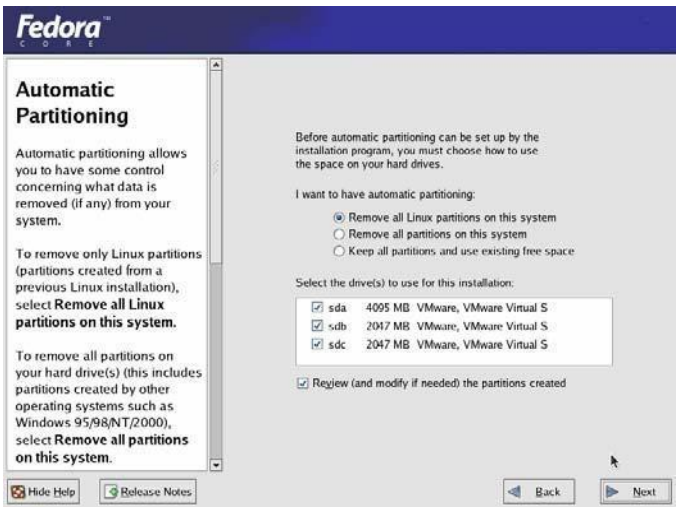
2.8. Chia Partition

- **Automatically partition:** hệ thống tự động phân vùng ổ đĩa hợp lý để cài hệ điều hành (thông thường theo cách này thì hệ thống sẽ tạo ra hai phân vùng: /boot, /, swap)

- **Manually partition with Disk Druid:** Chia partition bằng tiện ích Disk Druid. Đây là cách chia partition dưới dạng đồ họa dễ dùng.

- Nếu ta là người mới học cách cài đặt thì nên lựa chọn **Automatically partition**.

2.9. Lựa chọn Automatically partition



- **Remove all Linux partitions on this system:** loại bỏ tất cả các Linux partition có sẵn trong hệ thống.

- **Remove all partitions on this system:** loại bỏ tất cả các partition có sẵn trong hệ thống.

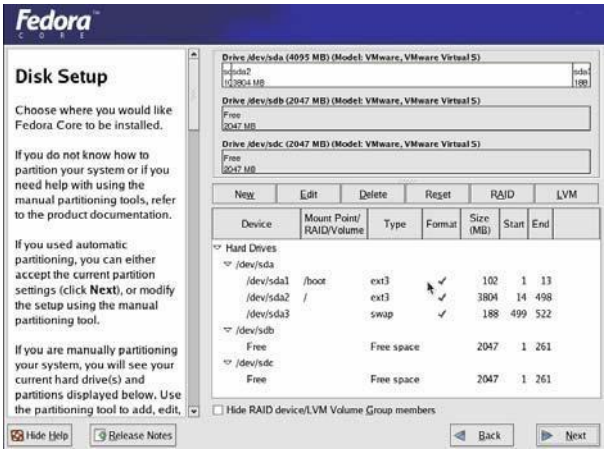
- **Keep all partitions and use existing free space:** giữ lại tất cả các partition có sẵn và chỉ sử dụng không gian trống còn lại để phân chia phân vùng.

Tùy theo từng yêu cầu riêng mà ta có thể lựa chọn các yêu cầu trên cho phù hợp, sau đó chọn **Next**.

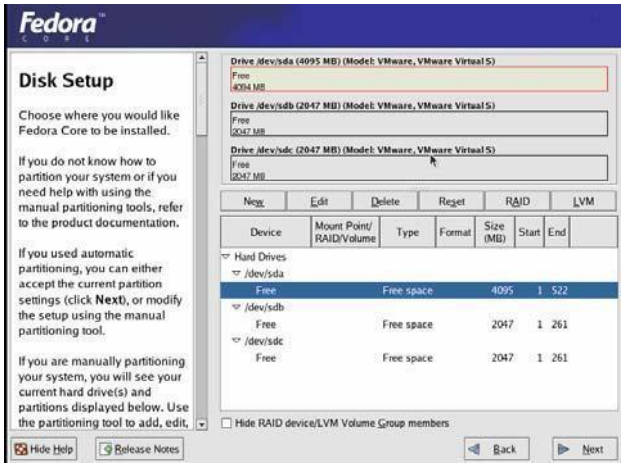
2.10. Chia Partition bằng Disk Druid

Trong bước 8 ta chọn Manually partition with Disk Druid để thực hiện phân chia phân vùng sử dụng tiện ích Disk Druid.

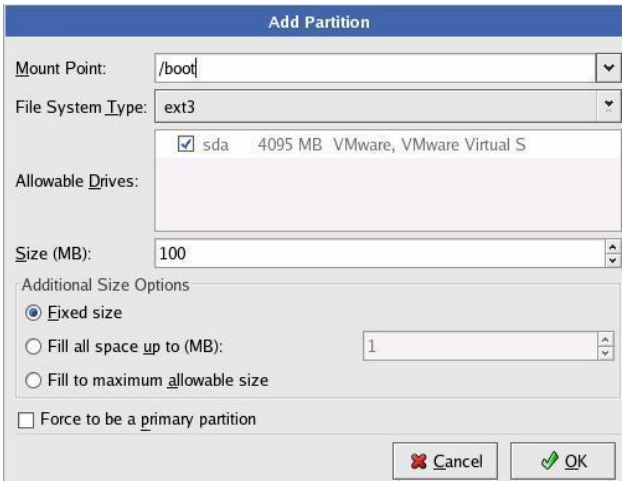
Disk Druid hiển thị các partition của đĩa dưới chế độ đồ họa ở phía trên, ta có thể chọn từng partition để thao tác.



Chi tiết các partition gồm kích thước, loại hệ thống tập tin, thư mục được mount vào được mô tả trong hình sau:



- **New:** Tạo một partition mới, chỉ định tên phân vùng (mount point), loại filesystem (ext3) và kích thước (size) tính bằng Mbyte (tùy chọn).



- **Edit:** Thay đổi lại các tham số của phân vùng được chọn.

- **Delete:** Xóa phân vùng được chọn.

- **Reset:** Phục hồi lại trạng thái đĩa như trước khi thao thác.

- **Make RAID:** Sử dụng với RAID (Redundant Array of Independent Disks) khi ta có ít nhất 3 đĩa cứng.

2.11. Cài đặt chương trình Boot Loader

Boot Loader là chương trình cho phép chọn các hệ điều hành để khởi động qua menu. Khi chúng ta chọn, thì chúng xác định các tập tin cần thiết để khởi động hệ điều hành và giao quyền điều khiển lại cho hệ điều hành. Boot Loader có thể được cài vào Master Boot record hoặc vào sector đầu tiên của partition.

Linux cho phép sử dụng chương trình Boot Loader là GRUB hoặc LILO. Cả 2 Boot Loader đều hỗ trợ quản lý nhiều hệ điều hành trên một hệ thống.

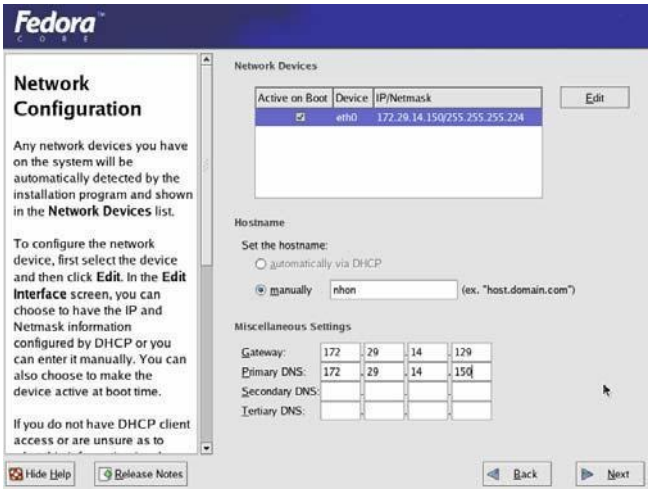
- Chọn cài Boot Loader vào Master Boot Record (MBR) khi chưa có chương trình Boot Loader nào được cài, hoặc chắc chắn chương boot loader có thể khởi động được các hệ điều hành khác trong máy. Khi cài lên MBR thì các chương trình Boot Loader trước đó sẽ bị thay thế bằng Boot Loader mới.

- Chọn cài Boot loader vào sector đầu tiên của partition cài đặt khi đã có chương trình Boot Loader tại MBR và không muốn thay thế nó. Trong trường hợp này, chương trình Boot Loader kia nắm quyền điều khiển trước và trỏ đến chương trình Boot Loader của Linux khi có yêu cầu khởi động hệ điều hành này.

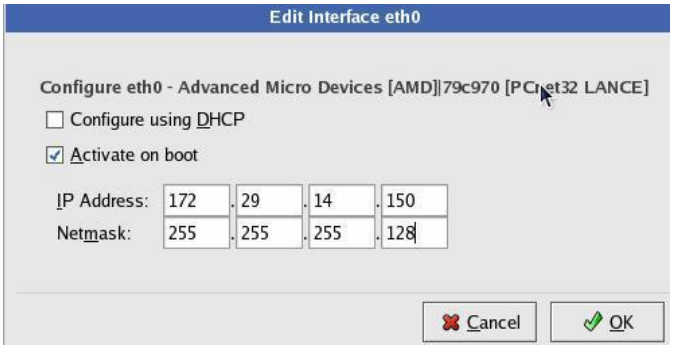
- Nếu không cài chương trình Boot loader thì phải sử dụng đĩa mềm boot để khởi động hệ điều hành.

- Có thể đặt mật khẩu cho boot loader thông qua nút Change password.

2.12. Cấu hình mạng



Configure using DHCP: Có thể chọn cấu hình TCP/IP động qua dịch vụ DHCP hoặc cấu hình cụ thể. Khi cấu hình cụ thể, phải nhập những thông số cấu hình mạng trong mục chọn edit:



- IPAddress: Chỉ định địa chỉ IP của host cài đặt.

- Netmask Address: subnet mask cho địa chỉ IP trên.

Active on boot: Card mạng được kích hoạt khi hệ điều hành khởi động.

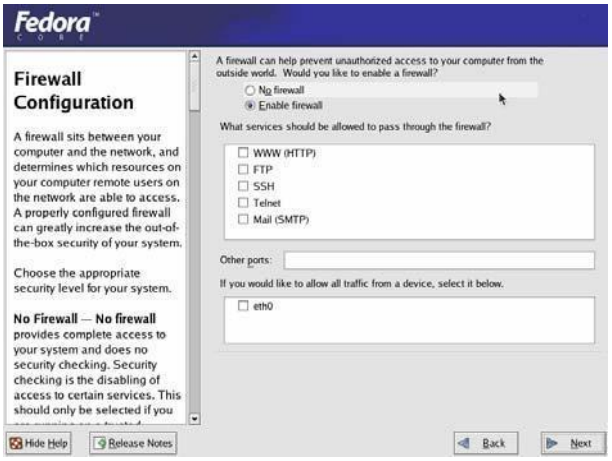
Host name: Nếu có tên dns đầy đủ thì khai báo tên đầy đủ. Trong trường hợp không kết nối vào mạng, chúng ta cũng đặt tên cho máy thông qua mục manually. Nếu không điền tên nào vào thì giá trị mặc nhiên là localhost.

Miscellaneous Settings: chỉ định địa chỉ gateway và Primary DNS, và một số thông số khác.

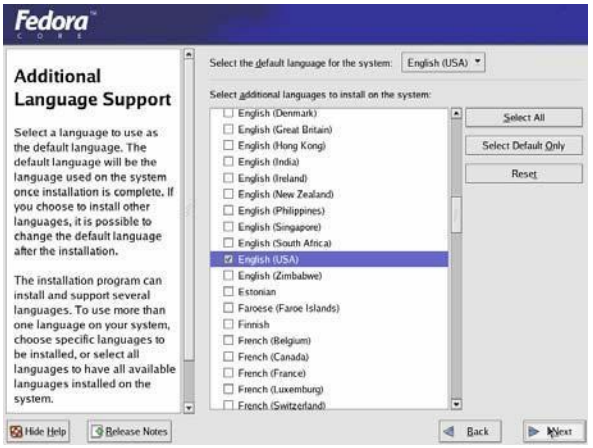
Các trường không có giá trị thì các trường đó không được sử dụng trong hệ thống.

2.13. Cấu hình Firewall

Trong Linux có tích hợp Firewall để bảo vệ hệ thống chống lại một số truy xuất bất hợp pháp từ bên ngoài. Ta chọn Enable Firewall, sau đó chọn loại dịch vụ cần cho phép bên ngoài truy cập vào Firewall.



2.14. Chọn ngôn ngữ hỗ trợ trong Linux



Chúng ta có thể cài đặt và sử dụng nhiều ngôn ngữ trong Linux. Có thể chọn ngôn ngữ mặc định (English (USA)) và các ngôn ngữ khác để sử dụng.

2.15. Cấu hình khu vực địa lý của hệ thống

Các vị trí chia theo châu lục. Ta có thể chọn mục này một cách thông qua việc định vị chuột tại đúng vị trí trên bản đồ.

2.16. Đặt mật khẩu cho người quản trị

Trên Linux người quản trị được gọi là người **root**. Mật khẩu của user root bắt buộc có chiều dài tối thiểu của password là 6 ký tự. Lưu ý password phân biệt chữ hoa và thường. Khi có thông báo "Root password accepted" là được.

2.17. Cấu hình chứng thực

Nếu không sử dụng password mạng có thể bỏ qua cấu hình này nhưng vẫn sử chế độ chọn mặc nhiên (chọn Enable MD5 passwords và Enable shadow passwords)

- Enable MD5 passwords: cho phép password sử dụng tới 256 ký tự thay vì chỉ tới 8 ký tự.

- Enable shadow passwords: cung cấp cơ chế lưu trữ password an toàn. Password được lưu trữ trong tập tin /etc/shadow và chỉ có root mới được đọc.

- Enable NIS: cho phép một nhóm máy trong một NIS domain sử dụng chung tập tin passwd và group. Chọn các tham số sau:

+ NIS domain: Xác định NIS domain mà máy này tham gia

+ Use broadcast to find NIS server: Cho phép sử dụng thông điệp quảng bá để tìm NIS server.

+ NIS Server: Xác định NIS server.

+ Enable LDAP: Hệ thống sử dụng LDAP cho một vài hoặc tất cả các phép chứng thực.

+ LDAP Server: Xác định LDAP server (dùng địa chỉ IP)

+ LDAP Base DN: cho phép tìm kiếm thông tin người dùng dựa trên DN (Distinguished Name)

+ Use TLS (Transport Layer Security) lookups: cho phép LDAP gởi tên người dùng và password mã hóa tới LDAP server trước khi chứng thực.

- Enable Kerberos: là hệ thống cung cấp các dịch vụ chứng thực trên mạng. Các lựa chọn:

+ Realm: cho phép truy xuất tới mạng sử dụng Kerberos.

+ KDC: cho phép truy xuất tới Key Distribution Center (KDC).

+ Admin Server: cho phép truy xuất tới server chạy kadmin.

+ Enable SMB Authentication: Cài PAM để dùng một Samba server chứng thực cho các client.

+ SMB Server: Xác định samba server mà các máy trạm kết nối tới để chứng thực.

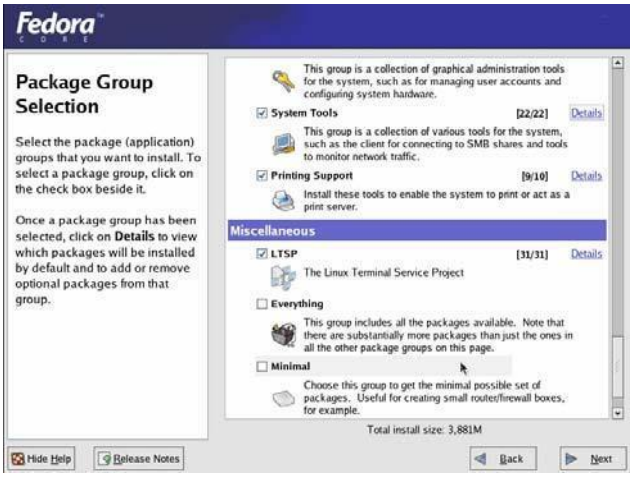
+ SMB Workgroup: Xác định workgroup mà samba server được cấu hình tham gia.

2.18. Chọn các chương trình và Package cài đặt

Chọn các chương trình cần cài đặt: **everything:** cài tất cả các chương trình, **Minimal:** chỉ cài một số chương trình hoặc phần mềm thông dụng.

Nếu nắm rõ các package cần thiết cho các chương trình mong muốn thì chọn **Select individual packages.** Ta có thể chọn **Details** để chọn chi tiết các thành phần trong từng phần mềm hoặc nhóm các công cụ.

2.19. Định dạng filesystem và tiến hành cài đặt



3. Cấu hình thiết bị

Mục tiêu: Trình bày các thao tác cấu hình các thiết bị thông dụng. Điều này giúp người học có thể cấu hình các thiết bị một cách dễ dàng.

3.1. Bộ nhớ (RAM)

System RAM được BIOS nhận biết khi khởi động, Linux kernel có khả năng nhận biết được tất cả các loại RAM (EDO, DRAM, SDRAM, DDRAM).

3.2. Vị trí lưu trữ tài nguyên

Kernel lưu trữ thông tin tài nguyên trong thư mục /proc, các tập tin ta cần quan tâm:

+ /proc/dma
+ /proc/interrupt
+ /proc/ioports
+ /proc/pci

3.3. Hỗ trợ USB

Hầu hết các phiên bản linux gần đây có khả năng nhận biết USB device, khi USB được cắm vào USB port thì nó được USB controller điều khiển, Linux hỗ trợ rất nhiều USB controller, thiết bị USB được Linux kernel nhận biết qua tập tin /dev/sda1.

3.4. Network Card

Kernel của linux hỗ trợ hầu hết NIC, để xem chi tiết thông tin hiện tại của card mạng ta sử dụng các lệnh sau đây: Dmesg, lspci, /proc/interrupts, /sbin/lsmod, /etc/modules.conf

3.5. Cài đặt modem

Sau đây là một số bước cài đặt serial modem:

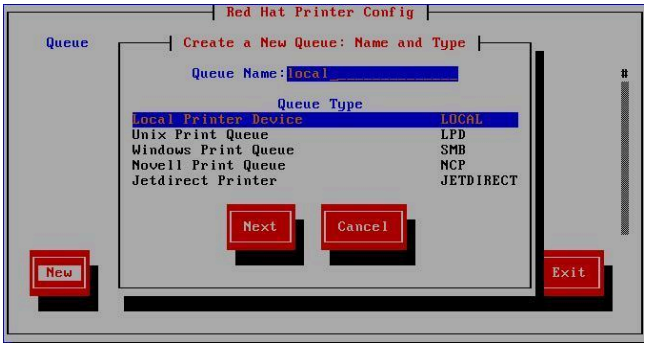
+ Bước 1: Dùng lệnh setserial để scan serial device.

+ Bước 2: Dùng lệnh ls –s /dev/ttyS1 /dev/modem

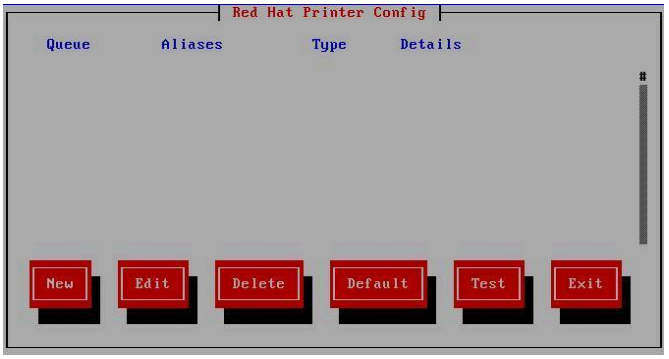
+ Bước 3: cấu hình Dial profile thông qua công cụ wvdial cung cấp script wvdialconfig để ta scan những thông tin cần thiết cho modem và ghi vào file /etc/wvdial.conf.

3.6. Cài đặt và cấu hình máy in

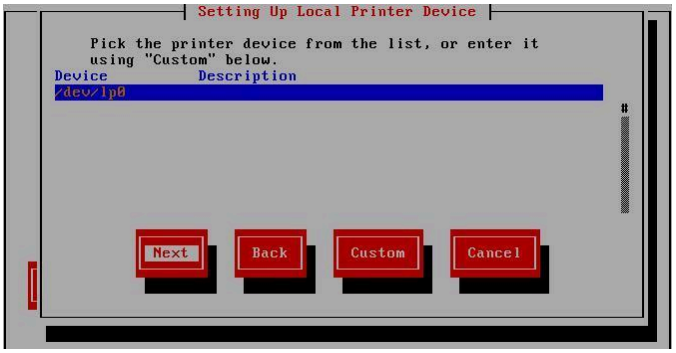
Trước khi cài đặt máy in, cần cài thêm package system-config-printer-0.6.98-1 (Fedora Core). Sau đó dùng lệnh #system-config-printer

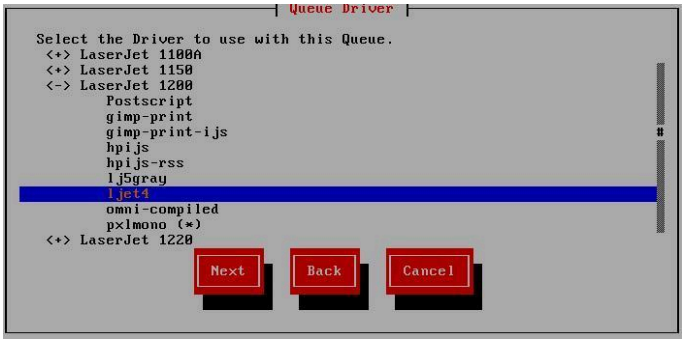


Chọn New để cài đặt máy in

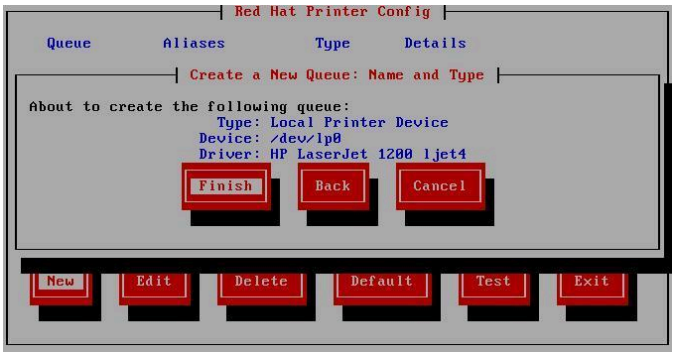


Đặt tên Printer và chọn **Queue Type**





Chọn **Queue Driver** để chỉ định loại máy in



4. Sử dụng hệ thống

Mục tiêu: Việc đăng nhập và sử dụng các lệnh cơ bản, sử dụng trợ giúp là điều đầu tiên người dùng phải thực hiện được. Phần này trình bày cách đăng nhập, quan sát dấu nhắc hệ điều hành, cách sử dụng các lệnh đơn giản và cách gọi trợ giúp khi cần thiết.

4.1. Đăng nhập

Để sử dụng hệ thống, trước hết phải đăng nhập vào. Khi kết nối tới máy thì màn hình hiển thị dòng:

+ Login:

+ Password:

Có 2 dạng dấu nhắc lệnh:

+ Dạng $ dùng cho người dùng thường.

+ Dạng # dùng cho người dùng quản trị (root).

Khi login vào hệ thống, chúng ta thấy dấu nhắc lệnh xuất hiện có dạng:

[tên-đăng-nhập@tên-máy thư-mục-hiện-hành]dấu-nhắc-lệnh

Ví dụ: [root@serverroot]#

- Từ dấu nhắc lệnh ta có thể sử dụng lệnh theo cú pháp như sau:

Tên-lệnh [tùy-chọn] [tham-số]

+ Tùy chọn có dạng: –<ký-tự>

+ Nếu có nhiều tùy chọn thì ta dùng dấu khoảng trắng để làm dấu ngăn cách hoặc kết hợp nhiều tùy chọn

Ví dụ: [root@server**ls –a –l /etc**

- Linux cho phép kết hợp nhiều lựa chọn chỉ dùng một dấu - . Như ví dụ trên ta có thể dùng lệnh ls –al /etc thay cho ls –a –l /etc

- Chuyển sang user khác: Đang làm việc chúng ta có thể chuyển sang người dùng khác mà không phải logout ra, bằng cách dụng lệnh su.

$su [tên-user]: chuyển sang user mới

- Nếu tên-user không có thì mặc định là chuyển qua root

- Thông thường khi chuyển sang user khác thì biến môi trường của hệ thống vẫn giữ nguyên theo user cũ. Để sử dụng biến môi trường của user mới chúng ta dùng thêm tham số - trong lệnh su.

Ví dụ: #su – [user]

4.2. Một số lệnh cơ bản

Tên lệnh	Ý nghĩa
date	Hiển thị ngày giờ hệ thống
who	Cho biết các người dùng đang đăng nhập vào hệ thống
tty	Xác định tập tin tty mà mình đang login vào
cal	Lịch

finger	Hiển thị các thông tin của các người dùng: họ tên, địa chỉ …
chfn	Thay đổi thông tin của người dùng
head	Xem nội dung tập tin từ đầu tập tin
tail	Xem nội dung từ cuối tập tin
hostname	Xem, đổi tên máy
passwd	Đổi mật khẩu cho user

4.3. Sử dụng trợ giúp man

Linux cung cấp một hệ thống thư viện giúp tìm các thông tin theo từ khóa nhập vào. Các lệnh trong Linux sử dụng rất nhiều tùy chọn, chúng ta sẽ khó nhớ hết được, Linux cung cấp trình trợ giúp man:

$man [từ-khóa]

Ví dụ: Tìm kiếm các thông tin về lệnh ls

$man ls

Để thoát khỏi man: chọn phím q

Man phân dữ liệu lưu trữ thành những đoạn (session) khác nhau với các chủ đề khác nhau là

Session	Tên chủ đề	Ý nghĩa
1	user command	các lệnh thông thường của hệ điều hành
2	system call	các hàm thư viện kernel của hệ thống
3	subroutines	các hàm thư viện lập trình
4	devices	các hàm truy xuất tập tin và xử lý thiết bị
5	File format	các hàm định dạng tập tin
6	games	các hàm liên quan đến trò chơi
7	Miscel	các hàm khác
8	Sys. admin	các hàm quản trị hệ thống

Xác định cụ thể thông tin của một chủ đề nào, chúng ta dùng lệnh man như sau: $man [session] [từ-khóa]

Ví dụ: man 3 printf Xem các thông tin về hàm prinf dùng trong lập trình

Nếu không xác định session thì session mặc nhiên là 1.

5. Cài đặt các gói phần mềm

Mục tiêu: Khi sử dụng hệ thống, việc cài đặt các chương trình, phần mềm trên hệ thống là thao tác cần thiết. Phần này sẽ cung cấp cho người dùng cách cài đặt, gỡ bỏ, nâng cấp phần mềm với các dạng file nguồn khác nhau.

5.1. Chương trình RPM

RedHat Package Manager (RPM) là hệ thống quản lý package (gói phần mềm) được Linux hỗ trợ cho người dùng. Nó cung cấp cho người dùng nhiều tính năng để duy trì hệ thống. Người dùng có thể cài đặt, xóa hoặc nâng cấp các package trực tiếp bằng lệnh. RPM có một cơ sở dữ liệu chứa các thông tin của các package đã cài và các tập tin của chúng, nhờ vậy RPM cho phép truy vấn các thông tin, cũng như xác thực các package trong hệ thống. Nếu sử dụng XWindow, có thể dùng chương trình KDE-PRM hoặc Gnome-RPM thay cho việc sử dụng lệnh.

5.2. Đặc tính của RPM

- **Khả năng nâng cấp phần mềm:** Với RPM, có thể nâng cấp các thành phần riêng biệt của hệ thống mà không cần phải cài lại. Khi có một phiên bản mới của hệ điều hành dựa trên RPM (như RedHat Linux chẳng hạn) chúng ta không phải cài lại hệ thống mà chỉ cần nâng cấp. RPM cho phép nâng cấp hệ thống một cách tự động, thông minh. Các tập tin cấu hình được giữ lại qua các lần nâng cấp; vì thế, các tuỳ chọn sẵn có của hệ thống được nâng cấp không bị thay đổi.

- **Truy vấn thông tin hiệu quả:** RPM cũng được thiết kế cho mục đích truy vấn các thông tin về các package trong hệ thống. Có thể tìm kiếm thông tin các package hoặc các tập tin cài đặt trong toàn bộ cơ sở dữ liệu, cũng có thể hỏi tập tin cụ thể thuộc về package nào và nó ở đâu. Package RPM có các tập tin chứa các thông tin rất hữu ích về package này và nội dung của package. Các tập tin này cho phép người dùng tìm kiếm thông tin trong một package riêng lẻ.

- **Thẩm tra hệ thống (System Verification):** Một đặc tính rất mạnh của RPM là cho phép thẩm tra lại các package. Nếu nghi ngờ một tập tin nào bị xóa hay bị thay thế trong package, có thể kiểm tra lại rất dễ dàng. Cần phải chú ý đến các dấu hiệu bất bình thường của hệ thống, nên kiểm tra và cài lại nếu cần thiết.

5.3. Lệnh rpm

Lưu ý rằng rpm phải được thực hiện bởi người dùng quản trị (root). RPM có 5 chế độ thực hiện: cài đặt (installing), xóa (uninstalling), nâng cấp (upgrading), truy vấn (querying) và thẩm tra (verifying).

5.3.1. Cài đặt phần mềm bằng rpm

Package RPM thường chứa các tập tin giống như foo-1.0-1.i386.rpm Tên tập tin này bao gồm tên package (foo), phiên bản (1.0), số hiệu phiên bản (1), kiến trúc sử dụng (i386). Lệnh cài đặt:

```
# rpm –ivh tên-tập-tinRPM
```

Ví dụ:

```
#rmp –ivh foo-1.0-1.i386.rpm
foo ##################################
```

Một số trường hợp lỗi khi cài đặt.

o Package đã cài rồi.

o Xung đột với tập tin cũ đã tồn tại.

o Package phụ thuộc vào package khác.

Ví dụ: package đã được cài đặt trước

```
# rpm -ivh foo-1.0-1.i386.rpm
foo package foo-1.0-1 is already installed
```

Nếu muốn cài chồng lên package đã cài, sử dụng tham số --replacepkgs

```
#rpm –ivh -–replacepkgs tên-tập-tin-package
```

Ví dụ:

```
# rpm -ivh --replacepkgs foo-1.0-1.i386.rpm
```

Ví dụ: xung đột với tập tin cũ đã tồn tại

```
# rpm -ivh foo-1.0-1.i386.rpm
foo /usr/bin/foo conflicts with file from bar-1.0-1
```

Để bỏ qua lỗi này, có thể cài đè lên bằng tùy chọn --replacefiles.

```
# rpm -ivh --replacefiles foo-1.0-1.i386.rpm
```

Ví dụ: Package phụ thuộc vào package khác

```
# rpm -ivh foo-1.0-1.i386.rpm
      failed dependencies:
      bar is needed by foo-1.0-1
```

Giải quyết trường hợp này, phải cài các package được yêu cầu. Nếu muốn tiếp tục cài mà không cài các package khác thì dùng tùy chọn --nodeps. Tuy nhiên lúc này các package có thể chạy không tốt.

5.3.2. Loại bỏ phần mềm đã cài đặt trong hệ thống

```
# rpm -e tên-package
```

Lưu ý: khi xóa chúng ta dùng tên-package chứ không dùng tên tập tin RPM.

Ví dụ:

```
# rpm -e foo
removing these packages would break dependencies:
foo is needed by bar-1.0-1
```

5.3.3. Nâng cấp phần mềm

rpm –**Uvh** tên-tập-tinRPM

Ví dụ:

```
# rpm -Uvh foo-2.0-1.i386.rpm
foo ########################################
```

Khi upgrade RPM sẽ xóa các phiên bản cũ của package. Có thể dùng lệnh này để cài đặt, khi đó sẽ không có phiên bản cũ nào bị xóa đi.

Khi RPM tự động nâng cấp với tập tin cấu hình, chúng thường xuất hiện một thông báo như sau: saving /etc/foo.conf as /etc/foo.conf.rpmsave. Điều này có nghĩa là khi tập tin cấu hình của phiên bản cũ không tương thích với phiên bản mới thì chúng lưu lại và tạo tập tin cấu hình mới. Nâng cấp thực sự là sự kết hợp giữa Uninstall và Install. Vì thế khi upgrade cũng thường xảy ra các lỗi như khi Install và Uninstall và thêm một lỗi nữa là khi upgrade với phiên bản cũ hơn.

```
# rpm -Uvh foo-1.0-1.i386.rpm
foo package foo-2.0-1 (which is newer) is already installed
```

Trong trường hợp này, thêm tham số --oldpackage

```
# rpm -Uvh --oldpackage foo-1.0-1.i386.rpm
foo ########################################
```

5.3.4. Truy vấn các phần mềm

rpm -q tên-package

Ví dụ:

```
# rpm -q foo
foo-2.0-1 //kết quả truy vấn
```

Thay vì xác định tên package, có thể sử dụng thêm một số tham số khác kết hợp với -q để ấn định package muốn truy vấn, chúng được gọi là Package Specification Options

+ -a: Truy vấn tất cả các package.
+ -f <tập-tin>: Truy vấn những package chứa tập-tin. Khi xác định tập tin, phải chỉ rõ đường dẫn (ví dụ: /usr/bin/ls)
+ -p <tên-tập-tin-package>: Truy vấn package tên-tập-tin-package

Sau đây là các tùy chọn sử dụng để xác định loại thông tin cần tìm kiếm. Chúng được gọi là Information Selection Options

+ -i: xác định các thông tin về package bao gồm: tên, mô tả, phiên bản, kích thước, ngày tạo, ngày cài đặt, nhà sản xuất …
+ -l: Hiển thị những tập tin trong package.

+ -s: Hiển thị trạng thái của các tập tin trong package.
+ -d: hiển thị danh sách tập tin tài liệu cho package (ví dụ man, README, info file …)
+ --c: hiển thị danh sách tập tin cấu hình.

5.3.5. Kiểm tra các tập tin đã cài đặt

Các thông tin dùng kiểm tra là: kích thước, MD5 checksum, quyền hạn, loại tập tin, người sở hữu, nhóm sở hữu tập tin.

+ rpm –V tên-package: Kiểm tra tất cả các tập tin trong package.
+ rpm –vf tên-file: Kiểm tra tập tin tên-file
+ rpm –Va: Kiểm tra tất cả các package đã cài.
+ rpm –Vp tên-tập-tin-RPM: Kiểm tra một package với tập tin package xác định, thường sử dụng trong trường hợp cơ sở dữ liệu của RPM bị hỏng.

Khi kiểm tra nếu không có lỗi thì không có hiển thị, nếu không thì sẽ thông báo ra. Định dạng của dòng thông báo gồm 8 ký tự và tên tập tin. Mỗi ký tự biểu diễn cho kết quả của việc so sánh một thuộc tính của tập tin với thuộc tính lưu trong cơ sở dữ liệu RPM. Dấu chấm (.) nghĩa là đã kiểm tra xong. Những ký tự đại diện cho các lỗi kiểm tra.

+ 5 – MD5 checksum
+ S – kích thước tập tin
+ L – liên kết mềm
+ T - thời gian cập nhật tập tin
+ D - thiết bị
+ U – người sở hữu
+ G – nhóm sở hữu
+ M - quyền truy xuất và loại tập tin.
+ ? – không tìm thấy tập tin

*5.3.6. Cài đặt phần mềm file nguồn *.tar, *.tgz*

Ngoài các phần mềm được đóng gói dạng file nhị phân (file *.rpm) còn có các phần mềm được ung cấp dạng file source code như: *.tar hoặc *.tgz. Thông thường để cài đặt phần mềm này ta cần phải dựa vào trợ giúp của file giúp đỡ trong từng chương trình hoặc phần mềm, các file (README or INSTALL) này

nằm trong các thư mục con của thư mục sau khi ta dùng lệnh tar để giải nén source. Để thực hiện việc cài đặt này ta thường làm các bước sau:

Bước 1: Giải nén file tar.

Ví dụ:

```
[root@bigboy tmp]# tar -xvzf linux-software-1.3.1.tar.gz
linux-software-1.3.1/
linux-software-1.3.1/plugins-scripts/
...
...
linux-software-1.3.1/linux-software-plugins.spec
[root@bigboy tmp]#
Tạo các thư mục con chứa các file cài đặt
[root@bigboy tmp]# ls
linux-software-1.3.1 linux-software-1.3.1.tar.gz
[root@bigboy tmp]#
```

Bước 2: Chuyển vào thư mục con và tham khảo các file INSTALL, README.

Ví dụ:

```
[root@bigboy tmp]# cd linux-software-1.3.1
[root@bigboy linux-software-1.3.1]# ls
COPYING  install-sh  missing              plugins
depcomp  LEGAL       mkinstalldirs        plugins-scripts
FAQ      lib         linux-software.spec  README
Helper.pm  Makefile.am  linux-software.spec.in
REQUIREMENTS
INSTALL  Makefile.in  NEWS                subst.in
[root@bigboy linux-software-1.3.1]#
```

Bước 3: Sau đó dựa vào chỉ dẫn trong file (INSTALL, README) để cài đặt phần mềm.

Câu hỏi

1. Trình bày các yêu cầu đối với hệ thống để cài đặt hệ điều hành Linux.

2. Cho biết các chế độ cài đặt Linux; Ưu và nhược điểm của mỗi chế độ cài đặt?

Bài tập thực hành

1. Cài đặt hệ điều hành Linux cho hệ thống.

Các bước thực hiện:

- Boot
- Chọn chế độ cài đặt
- Kiểm tra đĩa CD
- Giới thiệu
- Chọn ngôn ngữ
- Chọn keyboard
- Cấu hình màn hình
- Chọn kiểu cài đặt
- Chọn cơ chế phân chia đĩa
- Tạo 3 phân vùng
- Lựa chọn cấu hình Boot loader đặt mật khẩu
- Cấu hình mạng
- Cấu hình firewal
- Chọn ngôn ngữ hỗ trợ sau cài đặt
- Cấu hình múi giờ
- Thiết lập mật khẩu cho user quản trị hệ thống
- Kết nối phần mềm cần cài đặt:
    - X Windows System
    - GNOME Desktop
    - KDE
    - Các phần mềm khác (Editors, Graphic Interrnet, Text-based Interrnet, Office/Productivity, Các tool khác, Các công cụ hỗ trợ cấu hình, Các dịch vụ, hệ thống cần thiết khác, Công cụ hỗ trợ biên dịch, Các công cụ quản trị hệ thống Linux
- Yêu cầu login để sử dụng Linux
- Setup các thông số cơ bản (License, ngày giờ, cơ chế hiển thị màn hình, độ phân giải)
- Tạo thêm account cho các user khác
- Cài đặt các packet khác
- Màn hình đồ họa hiển thị và yêu cầu đăng nhập
- Lựa chọn các công cụ trong quá trình sử dụng giao diện đồ họa.

2. Cài đặt máy in

- Cài đặt máy in HP 4500 trên môi trường text
- Cài đặt máy in trên chế độ graphic
    * Thực hiện cài đặt một máy in cục bộ:
    * Cài đặt một máy in mạng

3. Cài đặt modem trên hệ thống hiện tại

4. Cài đặt Font VNI và Unicode trên máy hiện hành

5. Cài đặt bộ gõ tiếng việt
- Cài đặt bộ gõ tiếng việt xvnkb từ file nhị phân rpm:
- Cài xvnkb từ file nguồn *.tar.gz
- Cài đặt xvnkb trên giao diện đồ họa
6. Cài đặt phần mềm OpenOffice

BÀI 3: THAO TÁC VỚI TẬP TIN VÀ THƯ MỤC

Mã bài: MĐ 40-03

Mục tiêu:

- Nắm các khái niệm cơ bản vệ hệ thống tập tin và thư mục của Linux;
- Tạo và quản lý tập tin & thư mục;
- Sử dụng các lệnh liên quan đến tập tin và thư mục;
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Cấu trúc hệ thống tập tin & thư mục

Mục tiêu: Như các hệ điều hành khác, cấu trúc tập tin và thư mục là một phần cơ bản của hệ điều hành Linux. Phần này cung cấp cho người học các thành phần của hệ thống tập tin, thư mục cùng với chức năng của mỗi thành phần.

1.1. Hệ thống tập tin

- Hệ thống tập tin là một phần cơ bản của hệ điều hành Linux.

- Một hệ thống tập tin là thiết bị mà nó đã được định dạng để lưu trữ tập tin và thư mục.

- Hệ thống tập tin Linux bao gồm: đĩa mềm, CD-ROM, những partition của đĩa cứng. Những hệ thống tập tin thường được tạo trong quá trình cài đặt hệ điều hành. Nhưng cũng có thể thay đổi cấu trúc hệ thống tập tin khi thêm thiết bị hay chỉnh sửa những partition đã tồn tại. Như vậy, việc biết và hiểu cấu trúc hệ thống tập tin trong Linux là rất quan trọng.

Linux hỗ trợ nhiều loại hệ thống tập tin như: ext2, ext3, MS-DOS, proc. Hệ thống tập tin cơ bản của Linux là ext2 và ext3 (hiện tại là ext3). Hệ thống tập tin này cho phép đặt tên tập tin tối đa 256 ký tự và kích thước tối đa là 4terabytes. Bên cạnh đó, Linux hỗ trợ và cho phép đặt tên tập tin dài đối với những tập tin MS-DOS và những partition FAT32. Proc là một hệ thống tập tin

ảo (/proc) nghĩa là không dành dung lượng đĩa phân phối cho nó. Ngoài ra còn có những hệ thống tập tin khác như iso9660, UMSDOS, Network File System (NFS).

- Các thành phần của hệ thống tập tin:

+ **Super Block**: là một cấu trúc được tạo tại vị trí bắt đầu hệ thống tập tin. Nó lưu trữ thông tin về hệ thống tập tin như: Thông tin về block-size, free block, thời gian gắn kết (mount) cuối cùng của tập tin.

+ **Inode (256 byte)**: Lưu những thông tin về những tập tin và thư mục được tạo ra trong hệ thống tập tin. Nhưng chúng không lưu tên tập tin và thư mục thực sự. Mỗi tập tin tạo ra sẽ được phân bổ một inode lưu thông tin sau:

o Loại tập tin và quyền hạn truy cập tập tin

o Người sở hữu tập tin.

o Kích thước của tập tin và số hard link đến tập tin.

o Ngày và thời gian chỉnh sửa tập tin lần cuối cùng.

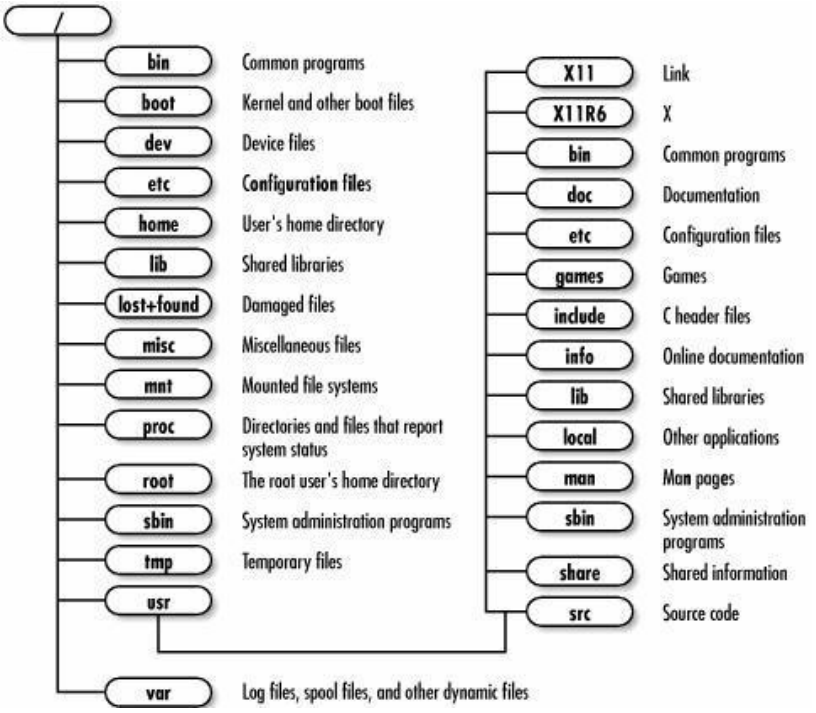
o Vị trí lưu nội dung tập tin trong hệ thống tập tin.

+ **Storageblock**: Là vùng lưu dữ liệu thực sự của tập tin và thư mục. Nó chia thành những Data Block. Dữ liệu lưu trữ vào đĩa trong các data block. Mỗi block thường chứa 1024 byte. Ngay khi tập tin chỉ có 1 ký tự thì cũng phải cấp phát 1 block để lưu nó. Không có ký tự kết thúc tập tin.

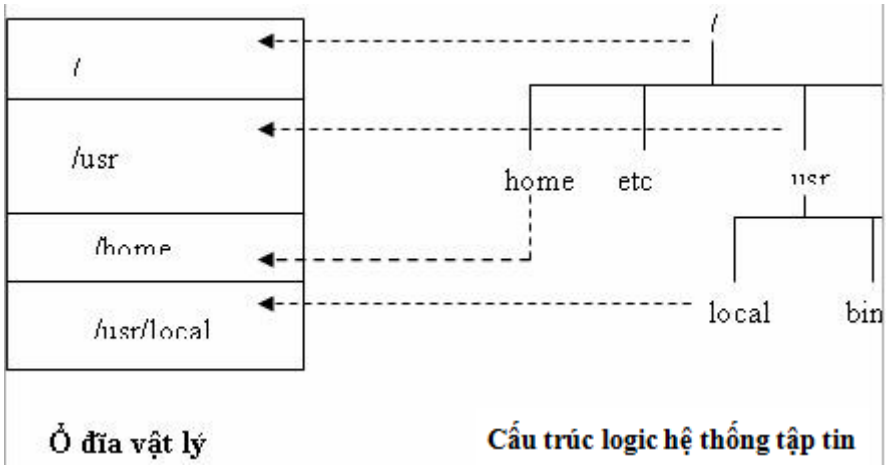
+ Data Block của tập tin thông thường lưu inode của tập tin và nội dung của tập tin.

+ Data Block của thư mục lưu danh sách những entry bao gồm inode number, tên của tập tin và những thư mục con.

1.2. Hệ thống thư mục



Hệ thống thư mục trong Linux có cấu trúc như hình vẽ trên. Trong Linux không có khái niệm ổ đĩa như trong Windows, tất cả các tập tin thư mục bắt đầu từ thư mục gốc (/). Linux sử dụng dấu "." chỉ thư mục hiện hành và dấu ".." chỉ thư mục cha của thư mục hiện hành. Ví dụ thư mục hiện hành là /usr/bin, đường dẫn ../local tương đương /usr/local



Như hình vẽ trên thư mục gốc được mount vào partition thứ nhất, /usr được mount vào partition thứ 2... Những dữ liệu ghi vào thư mục /home sẽ ghi

vào partition thứ 3. Tương tự, dữ liệu của thư mục /usr/local ghi vô partition 4, dữ liệu của thư mục /usr không phải thư mục con /usr/local thì ghi vào partion 2.

Linux sử dụng các tập tin chỉ đến các partition trên ổ đĩa vật lý. Những tập tin này là những tập tin thiết bị, nằm trong thư mục /dev. Tập các tập tin này có dạng đầu tin là ký tự xác định loại ổ đĩa như: đĩa mềm là fd, đĩa cứng là hd, đĩa scsi là sd … tiếp theo là số thứ tự ổ đĩa: Ổ đĩa thứ nhất dùng ký hiệu a, thứ 2 ký hiệu là b … và sau cùng là số thứ tự partition.

Ví dụ: tập tin chỉ đến các thiết bị:

+ ổ mềm thứ nhất: /dev/fd0

+ partition thứ nhất của ổ đĩa cứng đầu tin: /dev/hda1

+ partition thứ 3 của đĩa cứng thứ 2: /dev/hdb3.

Các thư mục cơ bản trên Linux

Thư mục	Chức năng
/bin, /sbin	Chứa các tập tin nhị phân hỗ trợ cho việc boot và thực thi các lệnh cần thiết
/boot	Chứa linux kernel, file ảnh hỗ trợ load hệ điều hành
/lib	Chứa các thư viện chia xẻ cho các tập tin nhị phân trong thư mục /bin và /sbin, chứa kernel module.
/usr/local	Chứa các thư viện, các phần mềm để chia xẻ cho các máy khác trong mạng
/tmp	Chứa các file tạm
/dev	Chứa các tập tin thiết bị (như CDROM, floppy), và một số file đặc biệt khác.
/etc	Chứa các tập tin cấu hình hệ thống
/home	Chứa các thư mục lưu trữ home directory của người dùng
/root	Lưu trữ home directory cho user root
/usr	Lưu trữ tập tin của các chương trình đã được cài đặt trong hệ thống.
/var	Lưu trữ log file, hàng đợi của các chương trình ứng dụng, mailbox của người dùng.
/mnt	Chứa các mount point của các thiết bị được mount vào trong hệ thống.

Các thư mục có thể sử dụng làm mount point cho các thiết bị riêng: như: /boot, /home, /root, /tmp, /usr, /usr/local, /opt, /var.

2. Thao tác với tập tin, thư mục

Mục tiêu: Trình bày các thao tác trên tập tin, thư mục một cách chi tiết, từ cú pháp lệnh đến chức năng và các ví dụ cụ thể.

2.1. Thao tác trên thư mục

2.1.1. Đường dẫn tương đối và tuyệt đối

Đường dẫn trong Linux sử dụng là dấu /

Để xác định một tập tin hay thư mục chúng ta dùng đường dẫn tuyệt đối hay tương đối. Đường dẫn tuyệt đối là đường dẫn đầy đủ đi từ thư mục gốc (/) của cây thư mục. Ví dụ: /home/hv, /usr/local/vd.txt

Trong một số trường hợp sử dụng các tập tin và thư mục là con của thư mục mình đang làm việc, lúc đó chúng ta sử dụng đường dẫn tương đối. Đường dẫn tương đối được tính từ thư mục hiện hành. Ví dụ chúng ta đang ở thư mục /home/hv khi gõ lệnh cat test.txt là chúng ta xem tập tin test.txt trong thư mục /home/hv.

Chương trình thực thi trong Linux có 2 dạng chính là tập tin lệnh và tập tin binary. Tập tin lệnh là tập tin lưu các lệnh của shell; tập tin binary chứa mã máy. Trong Linux tên tập tin không có khái niệm mở rộng. Người ta thường sử dụng phần mở rộng để nói lên tính chất, ý nghĩa của tập tin chứ không để xác định chương trình thực thi tập tin. Ví dụ .txt chỉ tập tin dạng text, .conf chỉ tập tin cấu hình. Tập tin muốn thực thi được thì phải gán quyền thực thi (x).

Khi thực thi chương trình phải xác định đường dẫn chính xác hoặc sử dụng đường dẫn trong biến môi trường PATH. Do vậy, muốn thực thi tập tin trong thư mục hiện hành phải dùng ./tên-file

2.1.2. Lệnh pwd

Lệnh pwd cho phép xác định vị trí thư mục hiện hành.

Ví dụ:

[natan@netcom bin]$ pwd

/usr/local/bin

2.1.3. Lệnh cd

Lệnh cd cho phép thay đổi thư mục.

Cú pháp:

$cd [thư-mục]

thư-mục: là nơi cần di chuyển vào.

Ví dụ: $cd /etc

2.1.4 Lệnh ls

Lệnh ls cho phép liệt kê nội dung thư mục.

Cú pháp: ls [tùy chọn] [thư mục]

ls –x hiển thị trên nhiều cột.

ls –l hiển thị chi tiết các thông tin của tập tin.

ls –a hiển thị tất cả các tập tin kể cả tập tin ẩn.

Ví dụ: $ ls –l /etc

-rw-r--r--	1 root	root	920	Jun 25 2001	im_palette-small.pal
-rw-r--r--	1 root	root	224	Jun 25 2001	im_palette-tiny.pal
-rw-r--r--	1 root	root	5464	Jun 25 2001	imrc
-rw-r--r--	1 root	root	10326	Apr 12 08:42	info-dir
lrwxrwxrwx	1 root	root	11	Apr 12 07:52	init.d -> rc.d/init.d

Ý nghĩa các cột từ trái sang phải

+ Cột 1: ký tự đầu tiên: - chỉ tập tin bình thường, d chỉ thư mục, l chỉ link và phía sau có dấu -> chỉ tới tập tin thật.

+ Các ký tự còn lại chỉ quyền truy xuất

+ Cột thứ 2: Chỉ số liên kết đến tập tin này.

+ Cột thứ 3, 4: Người sở hữu và nhóm sở hữu

+ Cột thứ 5: Kích thước tập tin, thư mục

+ Cột thứ 6: Chỉ ngày giờ sửa chữa cuối cùng

+ Cột thứ 7: Tên tập tin, thư mục

Để xem thông tin 1 hay nhiều tập tin có thể dùng

$ls -l tập-tin1 tập-tin2 …

2.1.5. Lệnh mkdir

Lệnh mkdir cho phép tạo thư mục.

Cú pháp:

$mkdir [tùy-chọn] [thư-mục]

Ví dụ: $mkdir /home/web

2.1.6. Lệnh rmdir

Lệnh cho phép xóa thư mục rỗng

Cú pháp:

$rmdir [tùy-chọn] [thư-mục]

Ví dụ: $rmdir /home/web

2.2. Tập tin

2.2.1. Lệnh cat

Lệnh cat dùng hiển thị nội dung của tập tin dạng văn bản. Để xem tập tin, chọn tên tập tin làm tham số.

Cú pháp:

$cat [tên-tập-tin]

Ví dụ: $cat myfile

Lệnh cat còn cho phép xem nhiều tập tin cùng lúc

$cat file1 file2 …

Cat cũng được dùng để tạo và soạn thảo văn bản dạng text. Trong trường hợp này chúng ta sử dụng dấu > hay >> đi theo sau (dấu > xóa nội dung cũ và ghi nội dung mới vào tập tin, dấu >> ghi nối nội dung mới vào tập tin).

$cat > <tên-tập-tin> [Enter]

> Các-dòng-dữ-liệu-của-tập tin

> …

[Ctrl-d: kết thúc]

2.2.2. Lệnh more

Lệnh more cho phép xem nội dung tập tin theo từng trang màn hình.

Cú pháp:

$more [tên-tập-tin]

Ví dụ:

$more /etc/passwd

2.2.3. Lệnh cp

Lệnh cp cho phép sao chép tập tin

Cú pháp:

$cp <tập-tin-nguồn> <tập-tin-đích>

Ví dụ: $cp /etc/passwd /root/passwd

2.2.4. Lệnh mv

Lệnh mv cho phép thay đổi tên tập tin và di chuyển vị trí của tập tin

Cú pháp:

$mv <tên-tập-tin-cũ> < tên-tập-tin-mới>

Ví dụ: $cp /etc/passwd /root/pwd

2.2.5. Lệnh rm

Lệnh rm cho phép xóa tập tin, thư mục.

Cú pháp:

$rm [tùy-chọn] [tên-tập-tin/thưmục]

Các tùy chọn thường dùng:

-r	xóa thư mục và tất cả các tập tin và thư mục con
-l	xác nhận lại trước khi xóa

2.2.6. Lệnh find

Cho phép tìm kiếm tập tin thỏa mãn điều kiện.

Cú pháp:

#find [đường-dẫn] [biểu-thức-tìm-kiếm]

o đường-dẫn: là đường dẫn thư mục tìm kiếm

o biểu-thức-tìm-kiếm: tìm các tập tin hợp với điều kiện tìm.

Tìm 1 tập tin xác định:

#find [thư-mục] –name [tên-tập-tin] –print

Ngoài ra, có thể sử dụng những kí hiệu sau:

"*": viết tắt cho một nhóm ký tự

"?": viết tắt cho một ký tự

Có thể sử dụng man để có các lựa chọn tìm kiếm đầy đủ hơn

2.2.7. Lệnh grep

Lệnh grep cho phép tìm kiếm một chuỗi nào đó trong nội dung tập tin.

Cú pháp:

#grep [biểu-thức-tìm-kiếm] [tên-tập-tin]

Tìm trong tập tin có tên [tên-tập-tin] những dữ liệu thỏa mãn [biểu-thức-tìm-kiếm]

Ví dụ: grep "nva" /etc/passwd

Tìm kiếm trong tập tin /etc/passwd và hiển thị các dòng có xuất hiện chuỗi "nvan".

2.2.8. Lệnh touch

Là lệnh hỗ trợ việc tạo và thay đổi nội dung tập tin

Cú pháp: touch <option> file

Ví dụ: #touch file1.txt file2.txt (tạo hai tập tin file1.txt và file2.txt)

2.2.9. Lệnh dd

Sao chép và chuyển đổi file.

Ví dụ:

dd if=/mnt/cdrom/images/boot.img of=/dev/fd0

(if là input file, of là output file)

3. Quyền truy cập, sở hữu đối với tập tin và thư mục

Mục tiêu: Trong Linux, các tập tin hay thư mục khi được tạo ra luôn có người sở hữu và quyền truy cập. Phần này sẽ trình bày các quyền trên tập tin và thư mục, cách gán quyền hay thay đổi sở hữu các tập tin và thư mục sẽ được hướng dẫn ở phần này.

3.1. Quyền hạn

Tất cả các tập tin và thư mục của Linux đều có người sở hữu và quyền truy cập. Chúng ta có thể thay đổi các tính chất này đối với tập tin hay thư mục. Quyền của tập tin còn cho phép xác định tập tin có phải là chương trình (application) hay không. Ví dụ với lệnh ls –l:

-rw-r--r-- 1 fido users 163 Dec 7 14 : 31 myfile

Cột đầu chỉ ra quyền hạn truy cập của tập tin; ví dụ trên, các ký tự -rw-r--r-- biểu thị quyền truy cập của tập tin myfile. Linux cho phép người sử dụng xác định các quyền đọc (read), viết (write) và thực thi (execute) cho từng đối tượng. Có 3 dạng đối tượng:

+ Người sở hữu (the owner)
+ Nhóm sở hữu (the group owner)
+ Người khác (“other users” hay everyone else).

Quyền đọc cho phép đọc nội dung của tập tin. Đối với thư mục, quyền đọc cho phép di chuyển vào thư mục và xem nội dung của thư mục.

Quyền viết cho phép thay đổi nội dung hay xoá tập tin. Đối với thư mục, quyền viết cho phép tạo ra, xóa hay thay đổi tên các tập tin trong thư mục không phụ thuộc vào quyền cụ thể của tập tin trong thư mục. Như vậy, quyền viết của thư mục sẽ vô hiệu hóa các quyền truy cập của tập tin trong thư mục.

Quyền thực thi cho phép gọi chương trình lên bộ nhớ bằng cách nhập từ bàn phím tên của tập tin. Đối với thư mục, chỉ có thể vào thư mục bởi lệnh cd nếu có quyền thực thi với thư mục.

-rw-r--r-- 1 fido users 163 Dec 7 14 : 31 myfile

Ký tự đầu tiên của quyền là ký tự "-" cho biết đó là một tập tin bình thường. Nếu ký tự d thay thế cho dấu "-" thì myfile là một thư mục. Ngoài ra còn có c cho thiết bị ngoại vi dạng ký tự (như bàn phím), b cho thiết bị ngoại vi dạng block (như ổ đĩa cứng).

Chín ký tự tiếp theo chia thành 3 nhóm, cho phép xác định quyền của 3 nhóm: người sở hữu (owner), nhóm sở hữu (group) và những người còn lại (other). Mỗi cặp ba này cho phép xác định quyền đọc, viết và thực thi theo thứ tự kể trên. Quyền đọc viết tắt là "r" ở vị trí đầu, quyền viết viết tắt bằng "w" ở vị trí thứ hai và vị trí thứ ba là quyền thực thi ký hiệu bằng chữ "x". Nếu một quyền không được cho thì tại vị trí đó sẽ có ký tự "-".

Ký tự	r	w	x	rw		x	r	w	x

Loại tập tin Owner group owner other users

Trong trường hợp của tập tin myfile, người sở hữu có quyền rw tức là đọc và viết. Nhóm sở hữu và những người còn lại chỉ có quyền đọc tập tin (read-only). Bên cạnh đó, các ký tự cho biết myfile không phải là một chương trình.

Song song với cách ký hiệu miêu tả bằng ký tự ở trên, quyền hạn truy cập còn có thể biểu diễn dưới dạng 3 số. Quyền hạn cho từng loại người dùng sử dụng một số có 3 bit tương ứng cho 3 quyền read, write và excute. Theo đó nếu cấp quyền thì bit đó là 1, ngược lại là 0. Giá trị nhị phân của số 3 bit này xác định các quyền cho nhóm người đó.

Bit 2	Bit 1	Bit 0
read	write	excute

Ví dụ:

chỉ có quyền đọc	100 có giá trị là 4
có quyền đọc và thực thi	101 có giá trị là 5

Ví dụ: Nếu có quyền read và excute thì số của quyền là: 4+1 =5

read, write và excute: 4+2+1=7

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

+ 0 or ---: Không có quyền
+ 1 or --x: execute
+ 2 or -w-: write-only (race)
+ 3 or -wr: write và execute
+ 4 or r--: read-only
+ 5 or r-x: read và execute
+ 6 or rw-: read và write
+ 7 or rwx: read, write và execute

Như vậy khi cấp quyền trên một tập tin/thư mục, có thể dùng số thập phân gồm 3 con số. Số đầu tiên miêu tả quyền của sở hữu, số thứ hai cho nhóm và số thứ ba cho những người còn lại.

Ví dụ: Một tập tin với quyền 751 có nghĩa là sở hữu có quyền read, write và execute bằng 4+2+1=7. Nhóm có quyền read và execute bằng 4+1=5 và những người còn lại có quyền execute bằng 1.

Chú ý: Người sử dụng có quyền đọc thì có quyền copy tập tin. Khi đó, tập tin sao chép sẽ thuộc sở hữu người làm copy. Ví dụ minh họa sau:

$ ls -l /etc/passwd

-rw-r--r-- 1 root root 1113 Oct 13 12 : 30 /etc/passwd

$ cp /etc/passwd ./

$ ls -l passwd

-rw-r--r-- 1 ndhung admin 1113 Oct 15 10 : 37 passwd

3.2. Lệnh chmod, chown, chgrp

3.2.1. Lệnh chmod

Dùng cấp quyền hạn truy cập của tập tin hay thư mục. Chỉ có chủ sở hữu và superuser mới có quyền thực hiện các lệnh này.

Cú pháp của lệnh:

$chmod [nhóm-người-dùng] [thao-tác] [quyền-hạn] [tên-tập-tin]

Nhóm-người-dùng	Thao tác	Quyền
u – user	+ : thêm quyền	r – read
g – group	- : xóa quyền	w – write
o – others	= : gán ngang quyền	x – excute
a – all		

Một số ví dụ: gán quyền trên tập tin myfile

Gán thêm quyền write cho group: $ chmod g+w myfile

Xóa quyền read trên group và others: $ chmod go-w myfile

Cấp quyền x cho mọi người:

$ chmod ugo+x myfile hoặc

$ chmod a+x myfile hoặc

$ chmod +x myfile

Đây là cách thay đổi tương đối vì kết quả cuối cùng phụ thuộc vào quyền đã có trước đó mà lệnh này không liên quan đến. Trên quan điểm bảo mật hệ thống, cách thay đổi tuyệt đối dẫn đến ít sai sót hơn. Thay đổi quyền truy cập của một thư mục cũng được thực hiện giống như đối với một tập tin. Chú ý là nếu không có quyền thực hiện (execute) đối với một thư mục, thì không thể cd vào thư mục đó. Mọi người sử dụng có quyền viết vào thư mục đều có quyền xóa tập tin trong thư mục đó, không phụ thuộc vào quyền của người đó đối với các tập tin trong thư mục. Vì vậy, đa số các thư mục có quyền drwxr-xr-x. Như vậy chỉ có người sở hữu của thư mục mới có quyền tạo và xóa tập tin trong thư mục.

Ngoài ra, thư mục còn có một quyền đặc biệt, đó là cho phép mọi người đều có quyền tạo tập tin trong thư mục, mọi người đều có quyền thay đổi nội dung tập tin trong thư mục, nhưng chỉ có người tạo ra mới có quyền xóa tập tin. Đó là dùng sticky bit cho thư mục. Thư mục /tmp thường có sticky bit bật lên.

drwxrwxrwt 7 root root 16384 Oct 21 15:33 tmp

Ta thấy chữ t, cuối cùng trong nhóm các quyền, thể hiện cho sticky bit của /tmp. Để có sticky bit, ta sử dụng lệnh: chmod 1????????? tên_thư_mục.

Ngoài ra, chúng ta cũng có thể gán quyền trực tiếp thông qua 3 chữ số xác định quyền như sau:

$chmod [giá-trị-quyền] [tên-tập-tin]

Ví dụ: Cấp quyền cho tập tin myfile

Quyền	**Lệnh**
-wrxr-xr-x	$chmod 755 myfile
-r-xr--r --	$chmod 522 myfile

-rwxrwxrwx	$chmod 777 myfile

3.2.2. Lệnh chown

Lệnh chown dùng để thay đổi người sở hữu trên tập tin, thư mục

Cú pháp: $chown [tên-user:tên-nhóm] [tên-tập-tin/thư-mục]

$chown –R [tên-user:tên-nhóm] [thư-mục]

Dòng lệnh cuối cùng với tùy chọn –R (recursive) cho phép thay đổi người sở hữu của thư mục <tên_thư_mục> và tất cả các thư mục con của nó. Điều này cũng đúng với lệnh chmod, chgrp.

3.2.3. Lệnh chgrp

Lệnh chgrp dùng để thay đổi nhóm sở hữu của một tập tin, thư mục

Cú pháp: $chgrp [nhóm-sở-hữu] [tên-tập-tin/thư-mục]

4. Liên kết tập tin

Mục tiêu: Trình bày các dạng liên kết tập tin trong Linux và cách sử dụng các dạng liên kết này.

***Link** (Liên kết)* một liên kết, hiểu theo cách đơn giản nhất, là tạo ra một tên tập tin thứ hai cho một tập tin. Ví dụ, khi có một tập tin /usr/lib/testfile và muốn có một tập tin giống như vậy trong thư mục /usr/tim thì không cần phải copy nó mà chỉ cần tạo một liên kết với lệnh sau:

#ln /usr/bill/testfile /usr/tim/testfile

Cú pháp của lệnh ln:

$ln <nguồn> <đích>

Lý do cơ bản của việc tạo liên kết là nhân tập tin lên nhiều lần. Trong ví dụ trên, cả hai tập tin chính là một. Do đó, nếu có bất kỳ sự thay đổi nào trên một tập tin sẽ ảnh hưởng ngay đến tập tin còn lại.

Hard Link: là một liên kết trong cùng hệ thống tập tin với hai inode entry tương ứng trỏ đến cùng một nội dung vật lý (cùng inode number vì chúng trỏ đến cùng dữ liệu). Nếu muốn thấy điều này, dùng lệnh sau:

```
$ ls -i testfile
14253 testfile
```

Sau đó tạo một liên kết có tên khác và hiển thị thông tin của inode entry.

```
$ ln testfile test2
$ ls -i testfile test2
14253 testfile 14253 test2
```

Cả hai tập tin đều có inode number giống nhau

Symbolic Link: Là một liên kết khác mà không sử dụng inode entry cho việc liên kết. Sử dụng liên kết này khi muốn tạo ra những driver thiết bị, như /dev/modem thay cho /dev/cua1. Tùy chọn –s của lệnh ln cho phép tạo ra một symbolic link.

Ví dụ:

```
$ ls -i bigfile
6253 bigfile
$ ln -s bigfile anotherfile
$ ls -i bigfile anotherfile
6253 bigfile 8358 anotherfile
```

Theo ví dụ trên, nội dung inode number của các tập tin khác nhau. Liệt kê một thư mục sẽ thấy symbolic link:

```
lrwxrwxrwx 1 root root 6 Sep 16:35 anotherfile -> bigfile
-rw-rw-r-- 1 root root 2 Sep 17:23 bigfile
```

Lưu ý: khi xóa tập tin gốc, nội dung của tập tin hard link không bị ảnh hưởng nhưng nội dung tập tin symbolic link không xem được.

5. Lưu trữ tập tin

Mục tiêu: Trình bày cách lưu trữ các tập tin trong Linux một cách hiệu quả.

5.1. Lệnh gzip/gunzip

gzip dùng để nén tập tin, gunzip dùng để giải nén các tập tin đã nén.

Cú pháp:

$gzip [tùy-chọn] [tên-tập-tin]

$gunzip [tùy-chọn] [tên-tập-tin]

gzip tạo tập tin nén với phần mở rộng .gz

Các tùy chọn dùng cho gunzip và gzip:

- c	Chuyển các thông tin ra màn hình
- d	Giải nén, gzip –d tương đương gunzip
- h	Hiển thị giúp đỡ.

Ví dụ:

#gzip /etc/passwd

#gunzip /etc/passwd.gz

5.2. Lệnh tar

Lệnh dùng để gom và bung những tập tin/thư mục (tạo ra một tập tin có phần mở rộng .tar)

Cú pháp: #tar [tùy-chọn] [tập-tin-đích] [tập-tin-nguồn/thư-mục-nguồn ...]

Trong đó:

+ –cvf: gom tập tin/ thư mục

+ –xvf: bung tập tin/ thư mục

+ tập-tin-đích: tập tin .tar sẽ được tạo ra.

+ tập-tin-nguồn/thư-mục-nguồn: những tập tin và thư mục cần gom.

Ví dụ:

#tar –cvf /home/backup.tar /etc/passwd /etc/group

#tar –xvf /home/backup.tar

Câu hỏi

1. Trình bày hệ thống tập tin và thư mục trong Linux. Cho biết các thành phần của hệ thống tập tin.

2. Trình bày hệ thống thư mục trong Linux; cho biết các thư mục cơ bản và chức năng của mỗi loại.

Bài tập thực hành

1. Login vào chế độ text với user root và thực hiện các lệnh cơ bản:
   + Đổi mật khẩu
   + Hiển thị thư mục hiện tại đang truy xuất
   + Hiển thị thông tin chi tiết về cấu hình mạng trên máy tính cục bộ
   + Xem tên máy đang dùng, đổi tên máy thành linux
   + Kiểm tra kết nối mạng – ping.
      Xem địa chỉ cục bộ
      Kiểm tra máy có liên thông internet hay không
   + Xem và đặt lại ngày giờ hệ thống
   + Khởi động lại hệ thống
   + Thiết lập shutdown hệ thống sau khoảng thời gian 1 phút
2. Thực hiện các thao tác trên file system
   + Xác định thư mục hiện hành của user root
   + mount đĩa CD3 của Fedora Core 2 vào thư mục /mnt/cdrom
   + Tạo thư mục /root/software, /root/dataserver
   + Copy tập tin có ký tự bắt đầu là mc trong thư mục /mnt/cdrom/Fedora/RPMS của đĩa CDROM vào thư mục /root/software
   + Cho biết hai tập tin passwd và group được lưu tại vị trí nào. Sau đó, copy chúng vào thư mục /root/dataserver
   + Trong thư mục /root tạo thư mục data. Sau đó, copy hai tập tin trong thư mục dataserver về thư mục này với tên mới là pwd và grp
   + Tạo tập tin lylich.txt lưu trong thư mục data với nội dung khoảng 5 dòng
   + Thêm dòng “Chao cac ban” vào cuối tập tin lylich.txt

+ Gom các tập tin trong thư mục data thành tập tin backup.tar. Sau đó, nén tập tin này thành backup.tar.gz

+ Dùng lệnh giải nén và bung file backup.tar.gz vào thư mục /root

+ Dùng man tìm hiểu lệnh head, tail, wc, call, finger, tty. Sau đó, tạo một file có tên /mancmd có nội dung giải thích công dụng của các lệnh tail, head, wc, tty

+ Dùng lệnh để xem toàn bộ nội dung tập tin /etc/passwd

+ Xem nội dung hai tập tin pwd và grp đồng thời

+ Tính tổng số dòng và tổng số ký tự trong tập tin pwd và grp

+ Tìm trong tập tin /etc/paswd và hiển thị ra màn hình những dòng có chuỗi "root"

+ Tìm trong hệ thống có các file nào có dung lượng lớn hơn 200KB hay không. Nếu có thì in ra màn hình.

+ Xem và ghi nhận tất cả các thuộc tính liên quan đến file /et/passwd (chỉ số liên kết, chủ sở hữu, nhóm sở hữu, quyền của u, g, o trên file, dung lượng file)

+ Tạo file /permissiontest, sau đó cấp quyền chỉ cho người dùng root mới được quyền xem nội dung file này

+ Xem tất cả các chỉ số inode của các file và thư mục của thư mục /root

+ Liệt kê tất cả các file và thư mục trong thư mục /etc/ theo từng trang màn hình

+ Xem trong thư mục /root có bao nhiêu file ẩn, hiển thị chi tiết thông tin của các file này. Sau đó cho kết xuất ra file /root/filelist.txt

3. Thiết lập quyền người dùng trên file và thư mục

+ Tạo file /test

+ Xem thuộc tính file /test

+ Thêm quyền thực thi cho người dùng chủ sở hữu cho file /test

+ Gán quyền thực thi cho mọi đối tượng trên file /test

+ Bỏ quyền thực thi cho mọi đối tượng trên file /test

+ Kiểm tra lại file /test

+ Thực hiện thao tác thay đổi quyền bằng chỉ số bit nhị phân

+ Thay đổi chủ sở hữu file /test thành chủ sở hữu là hv2

+ Thay đổi nhóm sở hữu thành nhóm hocvien

+ Thay đổi quyền: người khác không có quyền nào trên file /test, chỉ có hv2 và nhóm hocvien mới có quyền.

+ Logout, sau đó login vào bằng user1 để đọc file /test

+ Logout, sau đó login trở lại bằng root

+ Tạo file /test1

+ Xem quyền hạn trên file này

+ Thay đổi quyền mặc định để khi tạo mới file, hệ thống tự động gán quyền cho phép nhóm có quyền read write, chủ sở hữu có quyền read write, người khác không có quyền gì

+ Tạo thư mục mkdir /abc

+ Kiểm tra quyền trên thư mục /abc

+ Chuyển về quyền mặc định ban đầu umask 022

+ Tạo thư mục /cde

+ Kiểm tra quyền trên thư mục /cde

BÀI 4: GIAO DIỆN ĐỒ HỌA

Mã bài: MĐ 40-04

Mục tiêu:
- Phân biệt và chuyển đổi giữa các giao diện KDE, GNOME;
- Thao tác trong giao diện đồ họa KDE;
- Cấu hình môi trường làm việc;
- Sử dụng các trình tiện ích;
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Giới thiệu X Window

Mục tiêu: Cung cấp cho người học các loại giao diện đồ họa trong Linux, cách khởi động giao diện đồ họa.

1.1. Giới thiệu

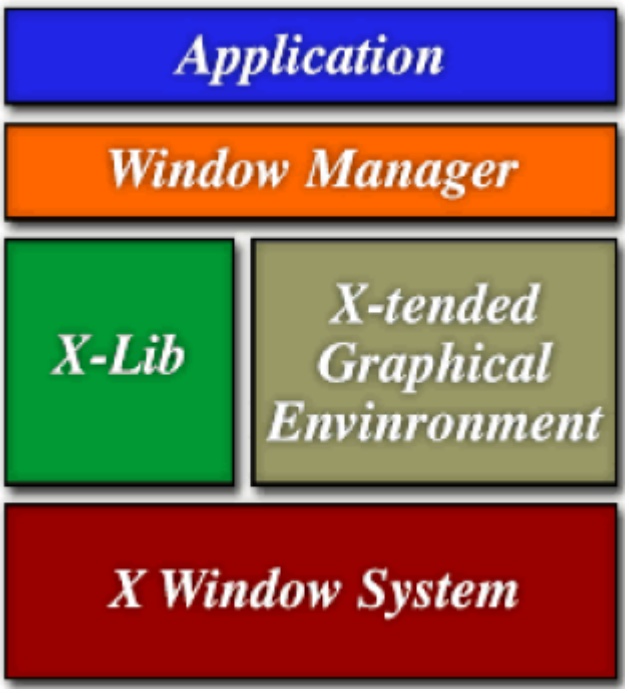
Giao diện đồ họa trong Linux được xây dựng trên cơ sở X Window System (gọi là X) với mục đích tiêu chuẩn hóa giao diện đồ họa cho các hệ điều hành UNIX.

Hệ thống X Window được xây dựng trên cơ sở mô hình chủ/khách. Trong đó, chương trình máy chủ X làm việc trên máy tính người dùng mà không phải trên máy chủ. Chương trình chủ X làm việc trực tiếp với phần cứng. Chương trình chủ X chiếm lĩnh các thiết bị phần cứng và cung cấp cho các chương trình khác ở dạng tài nguyên riêng theo một giao thức đặc biệt (X Network Protocol – Giao thức kết nối mạng X). Máy tính chỉ dùng để chạy chương trình chủ X được gọi là máy X Terminal.

Bản thân chương trình chủ X không tạo ra hình ảnh trên màn hình mà chỉ cung cấp hình ảnh cho card màn hình. Để đưa hình ảnh ra màn hình, cần phải chạy một trình quản lý cửa sổ và một chương trình khách để tạo ra hình ảnh trên

màn hình. Chương trình khách của chủ X có thể là các ứng dụng làm việc dưới X Window.

Giữa chương trình khách và chương trình chủ còn có hai thành phần của giao diện đồ họa; đó là thư viện các hàm đồ họa X-lib và trình quản lý cửa sổ. Thư viện X-lib gồm các hàm đồ họa cho phép thực hiện các thao tác bậc thấp với cac hình mẫu đồ họa, trình quản lý cửa sổ gọi các hàm trong X-lib để điều khiển màn hình và thực hiện thao tác chuyển đổi hình ảnh trong các cửa sổ.



Kiến trúc của hệ thống đồ họa X Window System

Khi ứng dụng X khởi động, cửa sổ chuyển quyền điều khiển đến trình quản lý cửa sổ. Trình quản lý cửa sổ cung cấp các phương tiện để thao tác với cửa sổ. Trình quản lý cửa sổ còn gọi các hàm cho các chương trình khách khi người dùng thao tác với các ứng dụng bằng phím và chuột.

Các môi trường làm việc đồ họa mở như KDE, GNOME,… không thể thay thế các thành phần trên của hệ thống X Window mà chỉ mở rộng và thêm vào.

1.2. Khởi động hệ thống X Window

Khi cài đặt Linux, có thể đồng ý với đề nghị của trình cài đặt để hệ thống tự động chạy. Tuy nhiên, sẽ là bất lợi do bị chiếm bộ nhớ và sử dụng tài nguyên. Người dùng cũng có thể khởi động bằng cách khác:

- Sau khi khởi động máy chủ, chạy chương trình Xorg từ thư mục /usr/bin/X11/; sau đó, nhấn tổ hợp phím Ctrl+Alt+Backspace để dừng chạy máy chủ và quay về chế độ văn bản.

- Hoặc sử dụng câu lệnh xinit trong thư mục /usr/bin/X11/

Sau đó, thực hiện lệnh twm hoặc fvwm.

Nếu trên máy có cài các trình quản lý cửa sổ và môi trường làm việc khác (KDE hoặc GNOME) thì thực hiện lệnh startkde hoặc gnome-session.

2. Môi trường làm việc KDE

Mục tiêu: Cung cấp môi trường làm việc trên giao diện đồ họa với các thiết lập cá nhân.

Trên hệ điều hành Linux, người dùng có thể tạo ra môi trường làm việc phù hợp với cá nhân. Tuy nhiên, GUI (Graphical User Interface) – giao diện đồ họa người dùng đã được phát triển. Đây là bộ các chương trình ứng dụng đã được kiểm tra và nhóm lại với nhau để làm việc trong chế độ đồ họa; nó bao gồm trình quản lý cửa sổ và các chương trình khác có cùng giao diện.

2.1. Giới thiệu

KDE – K Desktop Environment – môi trường đồ họa cho Linux gồm các ứng dụng và được hỗ trợ các ngôn ngữ khác nhau. KDE được phân phối miễn phí cùng với mã nguồn.

2.2. Khởi động KDE

Khởi động KDE được thực hiện qua lệnh startx. Để sử dụng KDE làm môi trường làm việc mặc định, mở tập tin cấu hình hệ thống (/etc/sysconfig/windowmanager) rồi thay thế giá trị đã có trong DEFAULT_WM thành kde (DEFAULT_WM="kde").

Sau khi khởi động KDE, người dùng phải đăng nhập với user và password tương ứng. Khi đã đăng nhập thành công, màn hình xuất hiện với hai thành phần chính:

- Các thanh panel – dùng để chạy các ứng dụng.

- Màn hình Desktop – cho phép đặt các biểu tượng để chạy các ứng dụng, các tập tin, thư mục,…

3. Trung tâm điều khiển KDE

3.1. Giới thiệu

Trung tâm điều khiển KDE (Personal Settings – thiết lập cá nhân) là chương trình cho phép thay đổi các cấu hình của môi trường làm việc KDE.

3.2. Khởi động trung tâm điều khiển KDE

Trung tâm điều khiển KDE có thể được chạy từ trình đơn chính hoặc qua biểu tượng trên thanh panel, hoặc từ dòng lệnh, gõ tên chương trình kcontrol.

4. Các trình tiện ích

Mục tiêu: Cung cấp cho người học các trình tiện ích thông dụng trên hệ điều hành Linux.

4.1. Trình soạn thảo vi

4.1.1. Giới thiệu vi

vi là chương trình soạn trực quan, hoạt động ở 2 chế độ: chế độ lệnh (command mode) và chế độ soạn thảo (input mode). Để soạn thảo tập tin mới hoặc xem hay sửa chữa tập tin cũ, dùng lệnh:

$vi [tên-tập-tin]

Khi thực hiện, vi sẽ hiện lên màn hình soạn thảo ở chế độ lệnh. Trong chế độ này, chỉ có thể sử dụng các phím để thực hiện các thao tác như: Dịch chuyển con trỏ, lưu dữ liệu, mở tập tin mới… mà không thể soạn thảo văn bản. Nếu muốn soạn thảo văn bản, phải chuyển từ chế độ lệnh sang chế độ soạn thảo. Chế độ soạn thảo giúp sử dụng bàn phím để soạn thảo nội dung văn bản.

4.1.2. Một số hàm lệnh của vi

vi tập tin	Bắt đầu dòng 1
vi +n tập tin	Bắt đầu ở dòng n
vi +/pattern	Bắt đầu ở pattern
vi -r tập tin	Phục hồi tập tin sau khi hệ thống bị treo

4.1.3. Chuyển chế độ lệnh sang chế độ soạn thảo

i	trước dấu con trỏ
I	trước ký tự đầu tiên trên dòng
a	sau dấu con trỏ
A	sau ký tự đầu tiên trên dòng
o	dưới dòng hiện tại
O	trên dòng hiện tại
r	thay thế 1 ký tự hiện hành
R	thay thế cho đến khi nhấn <ESC>

4.1.4. Chuyển chế độ soạn thảo sang chế độ lệnh

Dùng phím ESC, sau đó sử dụng các nhóm lệnh thích hợp sau:

a. Nhóm lệnh di chuyển con trỏ

h	sang trái một khoảng trắng
e, <space>	sang phải một khoảng trắng
w	sang phải 1 từ
b	sang trái 1 từ
k	lên một dòng
j, <return>	xuống một dòng
)	cuối câu
(	đầu câu
}	đầu đoạn văn
{	cuối đoạn văn
Ctrl+w	đến ký tự đầu tiên chèn vào
Ctrl+u	cuốn lên 1/2 màn hình
Ctrl+d	kéo xuống 1/2 màn hình
Ctrl+z	kéo xuống 1 màn hình
Ctrl+b	kéo lên 1 màn hình

b. Nhóm lệnh xóa

dw	Xóa 1 từ
do	Xóa đến đầu dòng
d$	Xóa cuối dòng
3dw	Xóa 3 từ
dd	Xóa dòng hiện hành
5dd	Xóa 5 dòng
x	Xóa 1 ký tự

c. Nhóm lệnh thay thế

cw	Thay thế 1 từ

3cw	Thay thế 1 từ
cc	Dòng hiện hành
5cc	5 dòng

d. Nhóm lệnh tìm kiếm

*/and	Từ kế tiếp của and
* ?and	Từ kết thúc là and
*/nThe	Tìm dòng kế bắt đầu bằng The
n	Lặp lại lần dò tìm sau cùng

e. Nhóm lệnh tìm kiếm và thay thế

:s/text1/text2/g	Thay text1 thành text2
:1,$s/tập tin/thư mục	Thay tập tin bằng thư mục từ hàng 1 đến cuối
:g/one/s//1/g	Thay thế one bằng 1

f. Copy and paste

Để copy ta dùng lệnh y và để paste dùng lệnh p

y$	copy từ vị trí hiện tại của cursor đến cuối dòng
yy	copy toàn bộ dòng tại vị trí cursor
3yy	copy ba dòng liên tiếp

g. Undo

Sử dụng phím u cho phép hủy thao tác hiện tại, quay về thao tác trước đó.

h. Thao tác trên tập tin

:w	ghi vào tập tin
:x	lưu và thoát khỏi chế độ soạn thảo
:wq	lưu và thoát khỏi chế độ soạn thảo
:w <filename>	lưu vào tập tin mới

:q	thoát nếu không có thay đổi nội dung tập tin
:q!	thoát không lưu nếu có thay đổi tập tin
:r	mở tập tin đọc

4.2. Trình tiện ích mail

Linux cung cấp cho người dùng tiện ích mail hỗ trợ việc gửi và nhận mail bằng cách sử dụng lệnh:

$mail

Lệnh cho phép hiển thị nội dung các mail trong mailbox. Sau khi hiển thị mail, màn hình ở trạng thái chờ lệnh từ người sử dụng (hiển thị dấu ?)

Các thao tác cơ bản:

newline, +	Hiển thị mail kế, nếu không còn thì thoát khỏi lệnh
p	In thông báo
s [tập tin]	lưu mail vào tập tin khác hoặc mailbox
w [tập tin]	giống như s nhưng không lưu đầu thông báo
d	xóa mail
q	thoát khỏi tiện ích
x	thoát khỏi tiện ích mà không thay đổi mail

Ví dụ:

Gửi mail với nội dung là <nội dung> đến người dùng có địa chỉ mail là giaovien1@danavtc.edu.vn

$mail giaovien1@danavtc.edu.vn

<nội dung>

^D

Gửi mail cùng lúc với nhiều người:

$mail giaovien1@danavtc.edu.vn giaovien2@danavtc.edu.vn

Nhận mail: Khi login vào hệ thống nếu có thư hệ thống sẽ thông báo “You have mail”; để nhận mail, gõ lệnh $mail. Có thể dùng các tiện ích như: sendmail, pine thông qua trợ giúp man.

4.3. Trình tiện ích tạo đĩa boot

Để tạo đĩa mềm khởi động hệ thống, sử dụng lệnh mkbootdisk. Các bước thực hiện:

- Đăng nhập vào hệ thống bằng user root;

- Xem phiên bảng kernel của Linux (lệnh ls /lib/modules/ hoặc lệnh uname –r;

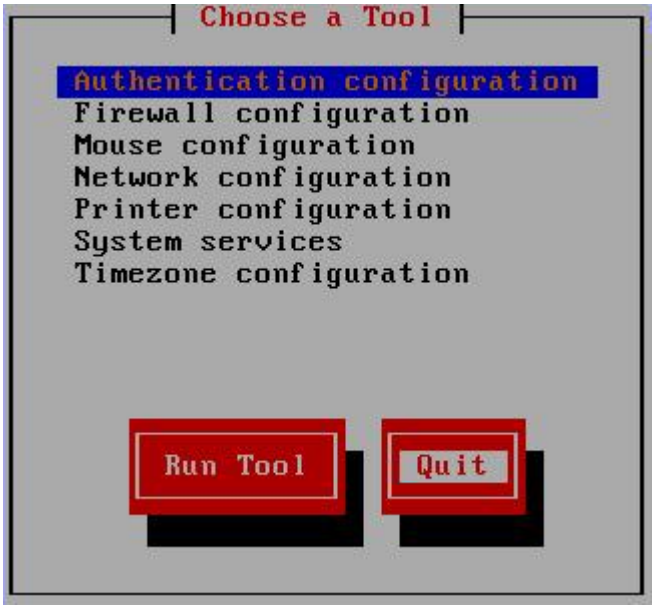
- Sử dụng lệnh /sbin/mkbootdisk 2.2.12-20 từ dấu nhắc shell;

- Đưa đĩa mềm vào ổ đĩa khi được hệ thống yêu cầu (Insert a disk in /dev/fd0. Any information on the disk will be lost).

4.4. Trình tiện ích setup

Tiện ích setup hỗ trợ cài đặt thiết bị, filesystem, thiết lập cấu hình mạng, dịch vụ hệ thống.

Từ dấu nhắc lệnh ta enter vào lệnh setup, hộp thoại hiển thị cho phép chọn công cụ:



Từ hộp thoại này, có thể lựa chọn các công cụ để cấu hình các thiết bị:

- Authentication configuration: Cấu hình xác thực hệ thống;
- Firewall configuration: Cấu hình tường lửa;
- Mouse configuration: Cấu hình chuột;
- Network configuration: Cấu hình mạng TCP/IP;
- Printer configuration: Cấu hình máy in;
- System services: Cấu hình các dịch vụ hệ thống;
- Timezone configuration: Cấu hình múi giờ.

4.5. Trình tiện ích fdisk

fdisk là trình tiện ích cho phép quản lý ổ đĩa cứng như: tạo mới, xem thông tin và xóa các parttition trong hệ thống.

Cú pháp: #fdisk <device_name>

Trong đó <device_name> có thể là /dev/hda hoặc /dev/sda.

Một số lệnh fdisk cơ bản:

P	Liệt kê danh sách các parttition table
N	Tạo mới 1 parttition
D	Xóa parttition

Q	Thoát khỏi trình tiện ích
W	Tạo mới parttition
A	Thiết lập boot parttition
T	Thay đổi system parttition ID
L	Liệt kê loại partition (bao gồm ID)

Lưu ý: Sau khi dùng fdisk để tạo một partition, phải reboot hệ thống rồi dùng lệnh mkfs –t ext3 <filesystem> để định dạng lại partition trước khi sử dụng.

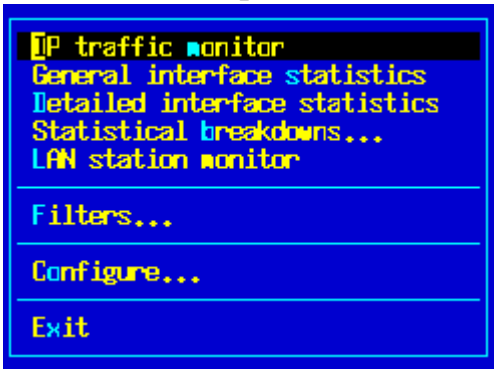
4.6. Trình tiện ích iptraf

iptraf là trình tiện ích hỗ trợ việc theo dõi và giám sát các traffic trên mạng; lưu ý rằng, chương trình này phải cài từ đĩa CDROM bằng lệnh:

rpm –ivh iptraf...rpm

Ví dụ: sử dụng tiện ích iptraf để theo dõi lưu lượng mạng.

Từ dấu nhắc lệnh enter vào lệnh iptraf



Ý nghĩa:

IP traffic monitor	Theo dõi ip trafic và TCP connection
General interface statistics	Xem các thông tin tổng quát trên các interface
Detailed interface statistics	Xem thông tin chi tiết trên từng interface (tổng số byte gởi, tổng số byte nhận,…)
Statistical breakdown …	Thống kê các packet bị hủy bỏ trên các interface do một số sự cố mạng
LAN station monitor	Thống kê thông tin từ máy mạng gởi vào máy nội bộ

Filters...	Cho phép thiết lập bộ lọc thông tin dựa theo các giao thức mạng TCP/UDP…
Configure...	Cấu hình các thông số cho trình tiện ích iptraf

4.7. Trình tiện ích lynx

lynx trình duyệt Web qua giao diện text thay vì sử dụng giao diện đồ họa của Xwindows.

Cú pháp: #lynx <URL>

4.8. Trình tiện ích mc

mc – Midnight Commander là trình quản lý tập tin cho phép xem cấu trúc cây thư mục và thực hiện các thao tác điều khiển hệ thống tập tin.

Các phím chức năng của trên mc:

F1	Gọi trợ giúp
F2	Gọi menu của người dùng
F3	Xem tập nội dung tập tin đang đặt dòng sáng
F4	Sửa nội dung tập tin đang đặt dòng sáng
F5	Sao chép các tập tin đang chọn
F6	Di chuyển các tập tin đang chọn
F7	Tạo thư mục trong thư mục hiện hành
F8	Xóa tập tin, thư mục đang chọn
F9	Gọi kích hoạt menu chính
F10	Thoát chương

Câu hỏi

1. X Window là gì? Cho biết kiến trúc của hệ thống đồ họa X Window System.
2. KDE là gì? Trình bày cách khởi động KDE

Bài tập thực hành

1. Tìm hiểu giao diện đồ họa

Login vào Xwindow thông qua giao diện GNOME Desktop hoặc KDE Desktop

Sử dụng các công cụ cơ bản trên giao diện desktop (truy cập các biểu tượng trên Computer, Root's home, Trash, Start Here)
Biểu tượng Computer: Floppy, CDROM, Filesystem (đại diện ổ đĩa cục bộ), Network (truy cập các máy tính khác trên mạng)
Các thành phần trên taskbar: Giờ, ngày hệ thống, nút Startmenu, Web browser, Email, OpenOffice, …
Biểu tượng Root's Home cho phép truy cập vào home directory của người dùng root (được đặt trong thư mục root)
Biểu tượng Trash: lưu trữ các file đã xóa trên giao diện đồ họa
Start Here: các công cụ cần thiết để truy cập, cấu hình hệ thống

- Application: chứa các công cụ cần thiết để truy cập các ứng dụng trên Linux
- Preferences: cung cấp các công cụ để cấu hình các thành phần trong máy tính: độ phân giải màn hình, hiệu chỉnh hình login, cấu hình chuột, thay đổi mật khẩu,…
- Systen settings: các công cụ cấu hình hệ thống: dịch vụ DNS, HTTP, Samba,…

Khởi động Terminal, tìm hiểu dấu nhắc [root@linuxserver root]#
Khởi động trình duyệt web để truy cập 1 vài trang web
Logon và sử dụng giao diện KDE Desktop (gần với giao diện Windows).
2. Sử dụng các tiện ích
- Khởi động mc, tìm hiểu các phím chức năng
- Khởi động trình tiện ích setup; Cấu hình cho hệ thống từ giao diện text
    +Hiệu chỉnh cấu hình Firewall
    + Cấu hình mạng
        Địa chỉ IP 192.168.7.200
        Đặt Default gateway 192.168.7.1
        DNS 203.162.4.1
        Cập nhật cấu hình mạng
        Cấu hình X
- Cài đặt và sử dụng trình tiện ích thống kê mạng iptraf
    Kiểm tra iptraf đã cài đặt hay chưa
    Cài đặt iptraf
    Khởi động iptraf và sử dụng các công cụ:
        + IP traffic monitor
        + General interface statistics
        + Detail interface statistics
        + Statistical breakdowns
        + LAN station monitor
- Sử dụng tiện ích lynx
    Cài đặt lynx
    Khởi động lynx

Truy nhập một trang web (www.vietnamnet.vn)

Truy nhập một trang web khác

- Sử dụng công cụ tcpdump để theo dõi traffic trên mạng
- Sử dụng tiện ích netconfig để thay đổi, cấu hình địa chỉ cho card mạng trên máy tính cục bộ

3. Vào giao đồ họa, sử dụng ethereal để phân tích gói tin (thống kê các gói tin đã bắt và theo dõi được; thống kê về một gói tin đang chọn; xem dữ liệu chi tiết của gói tin), sử dụng công cụ service để quản lý dịch vụ.

BÀI 5: QUẢN TRỊ NGƯỜI DÙNG VÀ NHÓM

Mã bài: MĐ 40-05

Mục tiêu:

- Hiểu cơ chế quản lý người dùng trong hệ điều hành Linux;
- Thực hiện việc tạo lập, quản lý người dùng.

Nội dung chính:

1. Thông tin của người dùng

Mục tiêu: Trình bày cơ chế quản lý người dùng trong hệ điều hành Linux, giúp người học biết được cách quản lý và lưu trữ các thống tin người dùng trên hệ thống.

1.1. Superuser

Trong Linux, tài khoản root có quyền cao nhất được sử dụng bởi người quản trị. Tài khoản này thường được sử dụng vào các mục đích cấu hình, bảo trì hệ thống. Khi quản trị hệ thống, cần tạo ra các tài khoản (account) cho người sử dụng thường sớm nhất có thể được. Với những server quan trọng và có nhiều dịch vụ khác nhau, có thể tạo ra các superuser thích hợp cho từng dịch vụ, tránh dùng root cho các công việc này. Ví dụ như superuser cho công việc backup chỉ cần chức năng đọc (read-only) mà không cần chức năng ghi.

Tài khoản root có quyền hạn rất lớn nên nó thường là mục tiêu chiếm đoạt; do vậy, người sử dụng tài khoản root phải cẩn thận, không sử dụng bừa bãi trên qua telnet hay kết nối từ xa mà không có công cụ kết nối an toàn.

Trong Linux, chúng ta có thể tạo tài khoản có tên khác nhưng có quyền của root, bằng cách tạo user có UserID bằng 0. Cần phân biệt tài khoản đang đăng nhập sử dụng là tài khoản root hay người sử dụng thường thông qua dấu nhắc của shell.

Để thay đổi tài khoản đăng nhập, sử dụng lệnh su [tên tài khoản]

Ví dụ:

login: nsd1

Password:******

[nsd1@DanaVTC nsd1]$ su -

Password: ******

[root@DanaVTC /root]#

Trong ví dụ trên, dòng thứ ba ([nsd1@DanaVTC nsd1]$) với dấu $ cho thấy người sử dụng thường (nsd1) đang kết nối; dòng cuối cùng với dấu # cho thấy đang thực hiện các lệnh với root.

1.2. User

Để đăng nhập và sử dụng hệ thống Linux cần phải có 1 tài khoản. Trừ tài khoản root, các tài khoản khác do người quản trị tạo ra.

Mỗi tài khoản người dùng cần có tên sử dụng (username) và mật khẩu (password) riêng. Các thông tin về tài khoản người dùng của hệ thống chứa trong tập tin /etc/passwd.

1.2.1. Tập tin /etc/passwd

Tập tin /etc/passwd được lưu dưới dạng văn bản, nó có vai trò rất quan trọng trong hệ thống Unix/Linux. Mọi người đều có thể đọc được tập tin này nhưng chỉ có root mới có quyền thay đổi nó.

Ví dụ sau cho thấy nội dung của một tập tin passwd:

root:x:0:0:root:/root:/bin/bash

bin:x:1:1:bin:/bin:

daemon:x:2:2:daemon:/sbin:

halt:x:7:0:halt:/sbin:/sbin/halt

mail:x:8:12:mail:/var/spool/mail:

news:x:9:13:news:/var/spool/news:

ftp:x:14:50:FTP User:/var/ftp:

nobody:x:99:99:Nobody:/:

nscd:x:28:28:NSCD Daemon:/:/bin/false

mailnull:x:47:47::/var/spool/mqueue:/dev/null

rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/bin/false

xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false

nthung:x:525:526:nguyen tien hung:/home/nthung:/bin/bash

natan:x:526:527::/home/natan:/bin/bash

Trong đó, các thông tin bao gồm:

- Dòng đầu tiên của tập tin /etc/passwd mô tả thông tin user root (tất cả những tài khoản có user_ID = 0 đều là root hoặc có quyền như root), tiếp theo là các tài khoản khác của hệ thống (đây là các tài khoản không có thật và không thể login vào hệ thống), cuối cùng là các tài khoản người dùng thường.

- Cột 1: Tên người sử dụng;

- Cột 2: Mã liên quan đến mật khẩu của tài khoản và "x" đối với Linux. Linux lưu mã này trong một tập tin khác /etc/shadow mà chỉ có root mới có quyền đọc;

- Cột 3, cột 4: Mã định danh tài khoản (user ID) và mã định danh nhóm (group ID);

- Cột 5: Tên đầy đủ của người sử dụng;

- Cột 6: Thư mục cá nhân (Home Directory);

- Cột 7: Chương trình sẽ chạy đầu tiên sau khi người dùng đăng nhập vào hệ thống.

1.2.2. Username và UserID

Để quản lý người dùng, Linux sử dụng tên người dùng (user name) và định danh người dùng (user ID) để đăng nhập và truy xuất tài nguyên.

Trong đó, tên người dùng là chuỗi ký tự xác định duy nhất một người dùng; số định danh người dùng dùng để kiểm soát hoạt động của người dùng. Theo qui định, người dùng có định danh 0 là người dùng quản trị (root); số định danh từ 1- 99 sử dụng cho các tài khoản hệ thống, số định danh của người dùng bình thường sử dụng giá trị bắt đầu từ 100-500.

1.2.3. Mật khẩu người dùng

Mỗi người dùng có mật khẩu tương ứng, mật khẩu có thể được thay đổi tùy theo người dùng; tuy nhiên, người quản trị có thể thay đổi mật khẩu của những người dùng khác.

Mật khẩu người dùng được lưu trong tập tin /etc/passwd.

1.2.4. Group ID

Group ID (GID) dùng để định danh nhóm của người dùng. Thông qua Group ID có thể xác định người dùng đó thuộc nhóm nào. Thông thường, trên Linux, GID được mặc định tạo ra khi tạo một user và có giá trị >= 500.

1.2.5. Home directory

Khi login vào hệ thống người dùng được đặt làm việc tại thư mục cá nhân của mình (home directory). Thông thường mỗi người dùng có một thư mục cá nhân riêng và người dùng có toàn quyền trên đó. Nó dùng để chứa dữ liệu cá nhân và các thông tin hệ thống cho hoạt động của người dùng như biến môi trường, script khởi động, profile khi sử dụng X Window,… Home directory của

người dùng thường là /home, của root là /root. Tuy nhiên, chúng ta cũng có thể đặt vào vị trí khác thông qua lệnh useradd hoặc usermod.

2. Quản lý người dùng

Mục tiêu: Trình bày các thao tác quản trị người dùng thông qua tài khoản người dùng.

2.1. Tạo tài khoản người dùng

Để tạo tài khoản, root có thể sử dụng lệnh useradd với cú pháp:

#useradd [-c mô_tả_người_dùng] [-d thư_mục_cá_nhân] [-m]

[-g nhóm_người_dùng] [tên_tài_khoản]

Trong đó:

- Tham số –m sử dụng để tạo thư mục cá nhân nếu nó chưa tồn tại.
- Chỉ có root được phép sử dụng lệnh này.

Ví dụ: # useradd –c “Nguyen van B“ nvb

Để đặt mật khẩu cho tài khoản, dùng lệnh passwd <username>.

Ví dụ: # passwd nvb

Changing password for user nvb

New password: ****

Retype new password: ****

passwd: all authentication tokens updated successfully

Lưu ý:

Khi đặt password nên:

- Đặt với độ dài tối thiểu 6 ký tự;
- Phối hợp giữa ký tự hoa, thường, ký số và ký tự đặc biệt.

- Không nên đặt password liên quan đến tên tuổi, ngày sinh,… của mình và người thân.

Khi nhiều người dùng có cùng một chức năng và cùng chia xẻ nhau dữ liệu, nên nhóm những người dùng này vào trong cùng nhóm. Mặc định, khi tạo một tài khoản, Linux sẽ tạo cho mỗi tài khoản một nhóm, tên nhóm trùng với tên tài khoản. Chẳng hạn, đọc tập tin /etc/passwd ta thấy:

nvb:x:1013:1013::/home/nvb:/bin/bash nghĩa là người dùng nvb có user_ID 1012 và thuộc nhóm 1013.

Xem tập tin /etc/group ta thấy:

```
# more /etc/group
root:x:0:root
……
users:x:100:
……
nvb:x:1013:
```

Lúc này, có thể kết nạp tài khoản nvb vào nhóm users bằng cách thay số 1013 bằng 100, là group_ID của nhóm users.

Có thể dùng lệnh useradd –d để xem các thông số mặc định khi ta tạo tài khoản người dùng (các thông tin này được lưu trong thư mục /etc/default/useradd):

```
# useradd -d
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
```

SHELL=/bin/bash

SKEL=/etc/skel

2.2. Thay đổi thông tin của tài khoản

Để thay đổi thông tin của tài khoản, có thể thay đổi từ tập tin /etc/passwd hoặc dùng lệnh usermod. Cú pháp lệnh usermod:

#usermod [-c thông_tin_người_dùng] [-d thư_mục_cá_nhân] [-m]

[-g nhóm_ người_dùng] [tên_tài_khoản]

Ví dụ: Cho tài khoản nvb vào nhóm admin

#usermod –g admin nvb

2.3. Tạm khóa tài khoản người dùng

Để tạm thời khóa tài khoản trong hệ thống ta có thể dùng nhiều cách:

Khóa (locking)	Mở khóa (unlock)
passwd –l <username>	passwd –u
usermod –L <username>	usermod –U

Có thể tạm khóa tài khoản bằng cách chỉnh sửa tập tin /etc/shadow và thay thế từ khóa x bằng từ khóa * hoặc có thể gán /bin/false vào shell mặc định của user trong file /etc/passwd.

2.4. Hủy tài khoản

Lệnh userdel dùng để xóa một tài khoản. Ngoài ra, cũng có thể xóa một tài khoản bằng cách xóa đi dòng dữ liệu tương ứng với tài khoản đó trong tập tin /etc/passwd. Cú pháp:

#userdel <option> [username]

Ví dụ: xóa tài khoản nvb (dùng tùy chọn –r để xóa toàn bộ thông tin liên quan tới user đó): #userdel –r nvb

3. Nhóm người dùng

Mục tiêu: Khi nhiều người dùng có cùng một chức năng, cùng chia xẻ nhau dữ liệu, có chung quyền trên tài nguyên, thường được nhóm thành một nhóm.

Trong Linux, mỗi nhóm được xác định bởi tên riêng và định danh nhóm; một nhóm có thể có nhiều người dùng và người dùng có thể là thành viên của nhiều nhóm khác nhau. Tuy nhiên tại một thời điểm, một người dùng chỉ có thể là thành viên của một nhóm duy nhất.

Thông tin về nhóm lưu tại tập tin /etc/group. Mỗi dòng định nghĩa một nhóm, các trường trên dòng cách nhau bởi dấu :

<tên-nhóm>:<password-của-nhóm>:<định-danh-nhóm:các-user-thuộc-nhóm>

3.1. Tạo nhóm

Để tạo một nhóm, có thể chỉnh sửa trực tiếp trong tập tin /etc/group hoặc dùng lệnh groupadd.

Cú pháp: #groupadd [tên-nhóm]

3.2. Thêm người dùng vào nhóm

Khi muốn thêm người dùng vào nhóm, có thể sửa từ tập tin /etc/group, các tên tài khoản người dùng cách nhau bằng dấu “;”, hoặc có thể thêm người dùng vào nhóm bằng lệnh:

#usermod –g [tên-nhóm tên-tài-khoản]

3.3. Hủy nhóm

Để hủy nhóm, có thể xóa trực tiếp nhóm trong tập tin /etc/group, hoặc dùng lệnh: #groupdel [tên-nhóm]

3.4. Xem thông tin về user và group

Cú pháp: #id <option> <username>

Lệnh cho phép xem thông tin về tài khoản hay nhóm trong hệ thống.

Trong đó, tham số -g cho phép xem thông tin về nhóm.

Ví dụ: xem groupID của một user vanphong: #id –g vanphong

Để xem tên nhóm của một user nào đó, dùng lệnh: groups <username>

Ví dụ: [root@server root]# groups root

root: root bin daemon sys adm disk wheel

Câu hỏi

1. Trình bày các loại tài khoản trên Linux.

2. Cho biết ý nghĩa các thành phần trên tập tin /etc/passwd.

Bài tập thực hành

1. Quản lý người dùng Linux trên giao diện text
- Xem thông tin chi tiết liên quan đến người dùng trong tập tin /etc/passwd.
- Xem thông tin chi tiết liên quan đến nhóm người dùng trong tập tin /etc/group.
- Xem thông tin chi tiết về mật khẩu trong tập tin /etc/shadow.
- Tạo user và nhóm:

Tạo nhóm hocvien gồm các user hv1, hv2, hv3 và đặt mật khẩu cho các user vừa tạo

Tạo nhóm admin gồm các user admin1, admin2 đặt mật khẩu cho các user vừa tạo

Thay đổi UID của hai user admin1, admin2 là 0
- Thay đổi thông tin mô tả của người dùng

Thông tin mô tả hv1 là học viên thứ nhất, hv2 là học viên thứ 2, hv3 là học viên thứ 3

Thông tin mô tả admin1 là người quản trị 1, admin2 là người quản trị 2
- Thay đổi mật khẩu cho những người dùng trên
- Khóa tài khoản người dùng hv3
- Thử đăng nhập bằng tài khoản hv3
- Mở khóa tài khoản người dùng hv3
- Thử đăng nhập bằng tài khoản hv3
- Xóa tài khoản người dùng hv3

2. Quản lý người dùng trên giao diện đồ họa
- Tạo người dùng và nhóm:
  - hocvien (tung, thuy, thanh)
  - admin (adm1, adm2)
  - user (u1, u2)
- Thay đổi các thuộc tính liên quan đến người dùng
  - Thay đổi nhóm của người dùng

- Giới hạn thời gian sử dụng tài khoản
- Tạm khóa tài khoản người dùng
- Giới hạn thời hạn sử dụng mật khẩu

BÀI 6: CẤU HÌNH MẠNG

Mã bài: MĐ 40-06

Mục tiêu:

- Nắm được cách khai báo và thay đổi cấu hình mạng cho máy tính;
- Truy cập và điều khiển máy tính từ xa;
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Cấu hình địa chỉ IP cho card mạng

Mục tiêu: Trình bày các thao tác : Xem địa chỉ IP, cấu hình địa chỉ IP, kiểm tra trạng thái của tất cả các card mạng.

1.1. Xem địa chỉ IP

Lệnh ifconfig cho phép xem thông tin địa chỉ IP của PC.

Ví dụ: để xem thông tin cấu hình mạng, dùng lệnh ifconfig -a

```
# ifconfig –a
eth0    Link encap:Ethernet  HWaddr 00:0C:29:6D:F0:3D
        inet addr:172.29.14.150  Bcast:172.29.14.159
Mask:255.255.255.224
        inet6 addr: fe80::20c:29ff:fe6d:f03d/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:1
        RX packets:6622 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1425 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:793321 (774.7 Kb)  TX bytes:240320 (234.6 Kb)
        Interrupt:10 Base address:0x1080
lo Link encap:Local Loopback
```

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr: ::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:16436 Metric:1

RX packets:76 errors:0 dropped:0 overruns:0 frame:0

TX packets:76 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:8974 (8.7 Kb) TX bytes:8974 (8.7 Kb)

Trong đó, eth0 là tên của card mạng trong, lo là tên của loopback interface.

1.2. Thay đổi địa chỉ IP

Trong bài 4 – mục 4, trình tiện ích cho phép thiết lập cấu hình mạng; ngoài ra, có thể sử dụng các cách sau để thay đổi địa chỉ IP:

Sử dụng lệnh:

ifconfig <interfacename> <IPaddress> netmask <netmaskaddress> up

Ví dụ:

[root@bigboy tmp]# ifconfig eth0 10.0.0.1 netmask 255.255.255.0 up

Chú ý: Sau khi dùng lệnh này, hệ thống lưu trữ tạm thời thông tin cấu hình này trong bộ nhớ và sẽ bị mất khi hệ thống reboot lại; để thông tin này có thể được lưu giữ lại sau khi reboot hệ thống, phải thêm lệnh trên vào tập tin /etc/rc.local.

Hoặc: Thay đổi thông tin cấu hình mạng trực tiếp trong file /etc/sysconfig/network-scripts/ifcfg-eth0

Gán địa chỉ IP tĩnh (tham khảo file ifcfg-eth0)

#Advanced Micro Devices [AMD]|79c970 [PCnet32LANCE]
DEVICE=eth0
BOOTPROTO=static
BROADCAST=172.29.14.159
HWADDR=00:0C:29:6D:F0:3D

IPADDR=172.29.14.150
NETMASK=255.255.255.224
NETWORK=172.29.14.128
ONBOOT=yes
TYPE=Ethernet

Gán địa chỉ IP động (tham khảo file ifcfg-eth0)

DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes

Sau đó dùng lệnh:

ifdown eth0
ifup eth0

1.3. Tạo nhiều địa chỉ IP trên card mạng

Phương thức tạo nhiều địa chỉ IP trên card mạng được gọi là IP alias. Alias này phải có tên dạng: parent-interface-name:X, trong đó X là chỉ số của interface thứ cấp (subinterface number).

Sử dụng một trong các cách sau để tạo Alias IP:

Cách 1:

- Bước 1: Đảm bảo rằng tên interface thật phải tồn tại, và kiểm tra các IP Alias trong hệ thống có tồn tại hay không.

- Bước 2: Tạo Virtual interface dùng lệnh ifconfig:

ifconfig ifcfg-eth0:0 192.168.1.99 netmask 255.255.255.0 up

Hoặc tạo một tên file /etc/sysconfig/network-scripts/ifcfg-eth0:0 từ file /etc/sysconfig/network-scripts/ifcfg-eth0; sau đó, thay đổi thông tin địa chỉ trong file này.

- Bước 3: Bật và tắt alias interface thông qua lệnh ifconfig

ifup eth0:0

ifdown eth0:0

Hoặc dùng lệnh /etc/init.d/network restart

- Bước 4: Kiểm tra thông tin cấu hình alias interface dùng lệnh ifconfig:

ifconfig

eth0 Link encap:Ethernet HWaddr 00:0C:29:6D:F0:3D

inet addr:172.29.14.150 Bcast:172.29.14.159 Mask:255.255.255.224

inet6 addr: fe80::20c:29ff:fe6d:f03d/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:7137 errors:0 dropped:0 overruns:0 frame:0

TX packets:1641 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:848367 (828.4 Kb) TX bytes:265688 (259.4 Kb)

Interrupt:10 Base address:0x1080

eth0:0 Link encap:Ethernet HWaddr 00:0C:29:6D:F0:3D

inet addr:172.29.15.150 Bcast:172.29.15.159 Mask:255.255.255.224

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:7137 errors:0 dropped:0 overruns:0 frame:0

TX packets:1641 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:848367 (828.4 Kb) TX bytes:265688 (259.4 Kb)

Interrupt:10 Base address:0x1080

Cách 2:

- Tạo tập tin parent-interface-name:X bằng cách copy file /etc/sysconfig/network-scripts/ifcfg-eth0 thành file /etc/sysconfig/network-scripts/ifcfg-eth0:X (trong đó X là số thứ tự của subinterface).

- Thay đổi thông tin cấu hình mạng trong file ifcfg-eth0:X (các thông tin in đậm là thông tin bắt buộc phải thay đổi)

DEVICE=eth0:0

ONBOOT=yes

BOOTPROTO=static

IPADDR=172.29.14.151

NETMASK=255.255.255.224

GATEWAY=172.29.129

1.4. Lệnh netstat

Lệnh netstat cho phép kiểm tra trạng thái của tất cả các card mạng.

Cú pháp: #netstat –in

Ngoài ra, có thể dùng lệnh netstat –rn để xem bảng routing table của router.

2. Truy cập từ xa

Mục tiêu: Trình bày cơ chế hoạt động của dịch vụ truy cập từ xa.

Khi cấu hình hệ thống kết nối vào mạng, máy chủ sẽ cung cấp một số dịch vụ Internet. Thông thường mỗi dịch vụ Internet gắn liền với một daemon và thực hiện trong chế độ background. Những daemon này hoạt động bằng cách liên kết đến một cổng nào đó và sau đó đợi những yêu cầu kết nối được gởi đến từ chương trình client. Khi một kết nối xảy ra nó sẽ tạo ra một tiến trình con đảm nhiệm kết nối này và tiếp tục lắng nghe những yêu cầu kết nối khác. Nếu hệ thống có quá nhiều daemon sẽ làm tăng xử lý của CPU. Để khắc phục điều này, Linux tạo ra một super-server gọi là Xinetd.

2.1. xinetd

Mỗi dịch vụ Internet đều gắn liền với một cổng chẳng hạn như: smtp – 25, pop3 – 110, dns – 53... Việc phân bổ này do một tổ chức qui định.

Xinetd là một Internet server daemon. Xinetd quản lý tập trung tất cả các dịch vụ Internet. Xinetd quản lý mỗi dịch vụ tương ứng với một cổng (port). Xinetd "lắng nghe" và khi nhận được một yêu cầu kết nối từ các chương trình client, nó sẽ đưa yêu cầu đến dịch vụ tương ứng xử lý; sau đó, Xinetd tiếp tục "lắng nghe" những yêu cầu kết nối khác. Khi hệ điều hành được khởi động, Xinetd được khởi tạo ngay lúc này bởi script /etc/rc.d/init.d/xinetd. Khi Xinetd được khởi tạo, nó sẽ đọc thông tin từ tập tin cấu hình /etc/xinetd.conf và sẽ dẫn đến thư mục /etc/xinetd – nơi lưu tất cả những dịch vụ mà Xinetd quản lý. Trong thư mục /etc/xinetd, thông tin cấu hình của mỗi dịch vụ được lưu trong một tập tin có tên trùng với tên dịch vụ đó. Nội dung tập tin của dịch vụ telnet như sau:

```
service telnet
{
        disable = yes
        flags = REUSE
        socket_type = stream
        wait = no
        user = root
        server = /usr/sbin/in.telnetd
        log_on_failure += USERID
}
```

Những thuộc tính trong tập tin bao gồm:

Tên	Ý nghĩa
Disable	Tạm đình chỉ dịch vụ này. Có 2 giá trị: yes, no

Socket_type	Loại socket. Trong trường hợp này là stream – một loại socket cho những kết nối connection-oriented (chẳng hạn như TCP)
Wait	Thường chỉ liên quan đến những kết nối có loại socket là datagram. Giá trị của nó có thể là: - ***nowait*** nghĩa là xinetd sẽ tiếp tục nhận và xử lý những yêu cầu khác trong lúc xử lý kết nối này - ***wait*** nghĩa là tại một thời điểm xinetd chỉ có thể xử lý một kết nối tại một cổng chỉ định
User	Chỉ ra user chạy dịch vụ này. Thông thường là root
Server	Chỉ ra đường dẫn đầy đủ đến nơi quản lý dịch vụ

2.2. Tập tin /etc/services

Khi xinetd được khởi tạo nó sẽ truy cập đến tập tin /etc/services để tìm cổng tương ứng với từng dịch vụ. Nội dung của tập tin này như sau:

echo 7/tcp

echo 7/udp

discard 9/tcp sink null

discard 9/udp sink null

systat 11/tcp users

systat 11/udp users

daytime 13/tcp

daytime 13/udp

qotd 17/tcp quote

qotd 17/tcp quote

msp 18/tcp# message send protocol

msp 18/udp# message send protocol

chargen 19/tcp ttytst source

chargen 19/udp ttytst source

ftp-data 20/tcp

ftp-data 20/udp

21 is registered to ftp, but also used by fsp

ftp 21/tcp

ftp 21/udp fsp fspd

ssh 22/tcp # SSH Remote Login Protocol

ssh 22/udp # SSH Remote Login Protocol

telnet 23/tcp

telnet 23/udp

24 - private mail system

smtp 25/tcp mail

smtp 25/udp mail

time 37/tcp timserver

time 37/udp timserver

rlp 39/tcp resource # resource location

rlp 39/udp resource # resource location

nameserver 42/tcp name # IEN 116

nameserver 42/udp name # IEN 116

Mỗi dòng trong tập tin mô tả cho một dịch vụ, bao gồm những cột sau:

- Cột 1: tên của dịch vụ;
- Cột 2: số cổng và giao thức mà dịch vụ này hoạt động;
- Cột 3: danh sách những tên gọi khác của dịch vụ này.

2.3. Khởi động xinetd

Sau khi chỉnh sửa tập tin cấu hình của từng dịch vụ trong thư mục /etc/xinetd, ta thực hiện lệnh sau để đọc lại nội dung của tập tin cấu hình:

/etc/rc.d/init.d/xinetd restart

3. Dịch vụ Telnet

Mục tiêu: Trình bày cách cài đặt, cấu hình và các phương án bảo mật đối với dịch vụ truy cập từ xa Telnet.

3.1. Khái niệm telnet

Vì một lý do nào đó người dùng không thể ngồi trực tiếp trên máy Linux làm việc. Dịch vụ telnet hỗ trợ cho người dùng trong vấn đề làm việc từ xa; Nhưng để đảm bảo tính bảo mật cho hệ thống, một điều cảnh báo là chúng ta không nên làm việc từ xa bằng telnet mà nên làm việc trực tiếp tại máy Linux.

3.2. Cài đặt

Thông thường khi cài đặt Linux, dịch vụ telnet đã được cài sẵn. Nếu chưa cài, có thể cài telnet server từ packet bằng dòng lệnh sau:

rpm –i telnet-server-0.17-20.i386.rpm

3.3. Cấu hình

Có nhiều cách cấu hình telnet server, sau đây là hai cách cấu hình cơ bản nhất:

- Cách 1: Dựa vào tập tin cấu hình, Khi cài đặt xong trong thư mục /etc/xinetd.d sẽ xuất hiện tập tin telnet. Tập tin này lưu những thông tin cấu hình về dịch vụ telnet.

```
service telnet
{
        disable = yes
```

```
        flags = REUSE
        socket_type  = stream
        wait = no
        user = root
        server  =/usr/sbin/in.telnetd
        log_on_failure += USERID
}
```

Nếu disable là no thì TELNET server được khởi động, ngược lại nếu disable là yes thì TELNET server không được khởi động. Sau khi chỉnh sửa tập tin cấu hình trên ta start, stop bằng lệnh:

```
/etc/rc.d/init.d/xinetd restart
```

Hoặc dùng lệnh:

```
# service xinetd restart
```

- Cách 2: Cấu hình telnet Server bằng dòng lệnh: chkconfig telnet on

Kiểm tra telnet thông qua lệnh:

```
#netstat-a|grep telnet
tcp        0      0      *:telnet      *:*      LISTEN
```

Kiểm tra telnet có được đặt như dịch vụ hệ thống:

```
# chkconfig --list | grep telnet
telnet: on
```

Dừng telnet server:

```
# chkconfig telnet off
```

3.4. Bảo mật dịch vụ telnet

3.4. 1. Cho phép telnet server hoạt động trên tcp port khác

Vì telnet traffic không được mã hóa nên nếu cho telnet server hoạt động trên tcp port 23 thì không được an toàn. Do vậy, có thể đặt telnet server hoạt động trên tcp port khác 23. Để làm điều này ta thực hiện các bước sau:

- Bước 1: Mở tập tin /etc/services và thêm dòng

```
# Local services
stelnet        7777/tcp          # "secure" telnet
```

- Bước 2: Chép file telnet thành file stelnet

```
# cp /etc/xinetd.d/telnet /etc/xinetd.d/stelnet
```

- Bước 3: Thay đổi một số thông tin trong file file /etc/xinetd.d/stelnet

```
service stelnet
{
        flags         = REUSE
        socket_type    = stream
        wait          = no
        user          = root
        server         = /usr/sbin/in.telnetd
        log_on_failure += USERID
        disable        = no
        port          = 7777
}
```

- Bước 4: Kích hoạt stelnet thông qua lệnh chkconfig

```
# chkconfig stelnet on
```

- Bước 5: Kiểm tra hoạt động stelnet thông qua lệnh netstat

```
# netstat -an | grep 777
tcp   0  0 0.0.0.0:7777       0.0.0.0:*          LISTEN
```

Ta có thể logon vào stelnet Server thông qua lệnh:

```
# telnet 192.168.1.100 7777
```

3.4.2. Cho phép một số địa chỉ truy xuất telnet

Ta hiệu chỉnh một số thông số sau::

```
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure += USERID
        disable         = no
        only_from       = 192.168.1.100 127.0.0.1 192.168.1.200
}
```

4. SSH

Mục tiêu: Trình bày cách cài đặt và sử dụng dịch vụ truy cập từ xa SSH với phương thức mã hóa dữ liệu.

Chương trình telnet trong Linux cho phép người dùng đăng nhập vào hệ thống Linux từ xa. Nhược điểm của chương trình này là tên người dùng và mật khẩu gởi qua mạng không được mã hóa. Do đó, dễ bị những người khác nắm giữ và sẽ là mối nguy hiểm cho hệ thống.

Phần mềm Secure Remote Access là một hỗ trợ mới của Linux nhằm khắc phục nhược điểm của telnet. Nó cho phép đăng nhập vào hệ thống Linux từ xa và mật khẩu sẽ được mã hóa. Vì thế, SSH an toàn hơn nhiều so với telnet.

4.1. Cài đặt SSH Server trên Server Linux

Dùng lệnh rpm để cài package openssh-server. *.rpm

rpm –ivh openssh-server.*.rpm

Tập tin cấu hình /etc/ssh/sshd_config và /etc/ssh/ssh_config. Để start hay stop server dùng lệnh sau:

/etc/init.d/sshd start/stop/restart

4.2. Sử dụng SSH Client trên Linux

Trên client (Linux hoặc Unix) dùng lệnh ssh để login vào server. Cú pháp của lệnh:

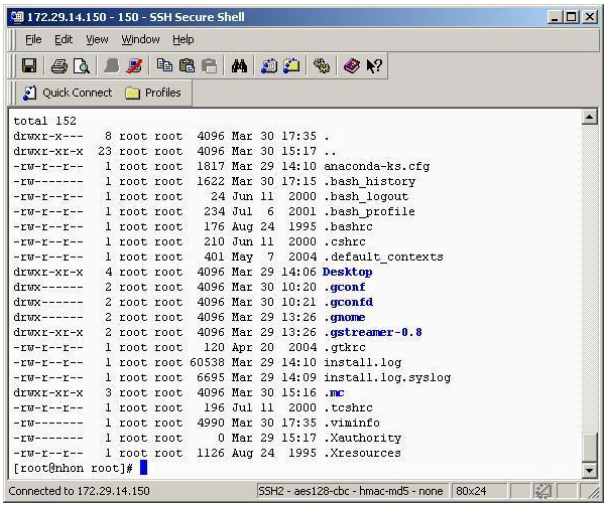
$ssh [tùy_chọn] [tên/IP_máy] [tùy_chọn] [lệnh]

Ví dụ: $ssh [–l] <tên_user> <ssh_address>

4.3. Quản trị hệ thống Linux thông qua SSH client for Windows

SSH client for Windows được thiết kế để cho phép người dùng có thể sử dụng/quản trị Unix/Linux từ hệ điều hành Windows. Có thể download phần mềm này từ site: http://www.ssh.com/support/downloads/.

Phần mềm này hỗ trợ cho người dùng có thể làm việc từ xa, cung cấp dịch vụ sftp.



Màn hình "SSH Client for Windows"

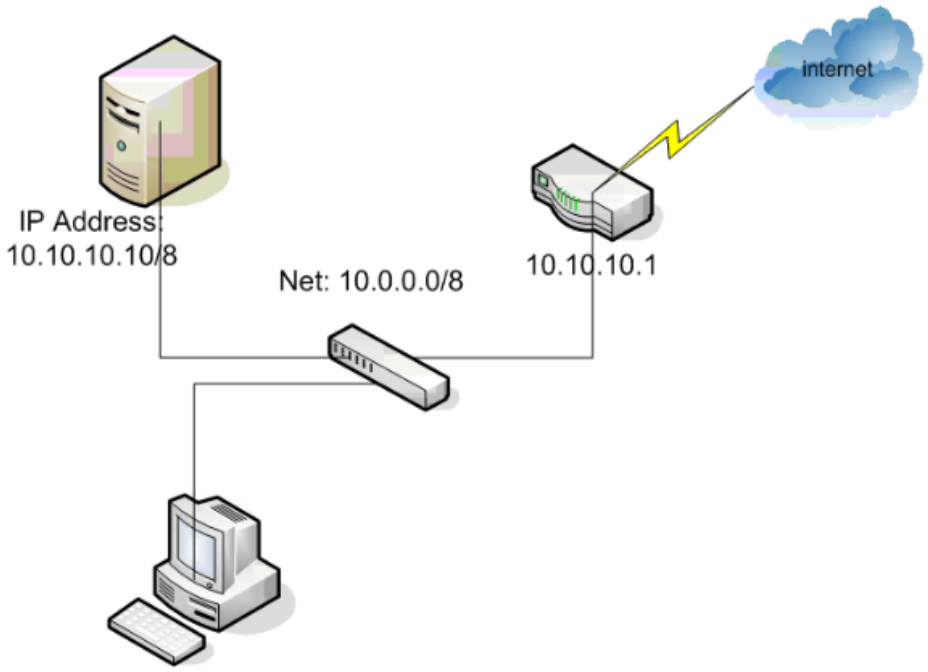
Câu hỏi

1. Trình bày các cách thay đổi địa chỉ IP (lệnh ifconfig, thay đổi từ file /etc/sysconfig/network-scripts/ifcfg-eth0).

2. Trình bày các cách tạo nhiều địa chỉ IP trên card mạng (IP alias).

Bài tập thực hành

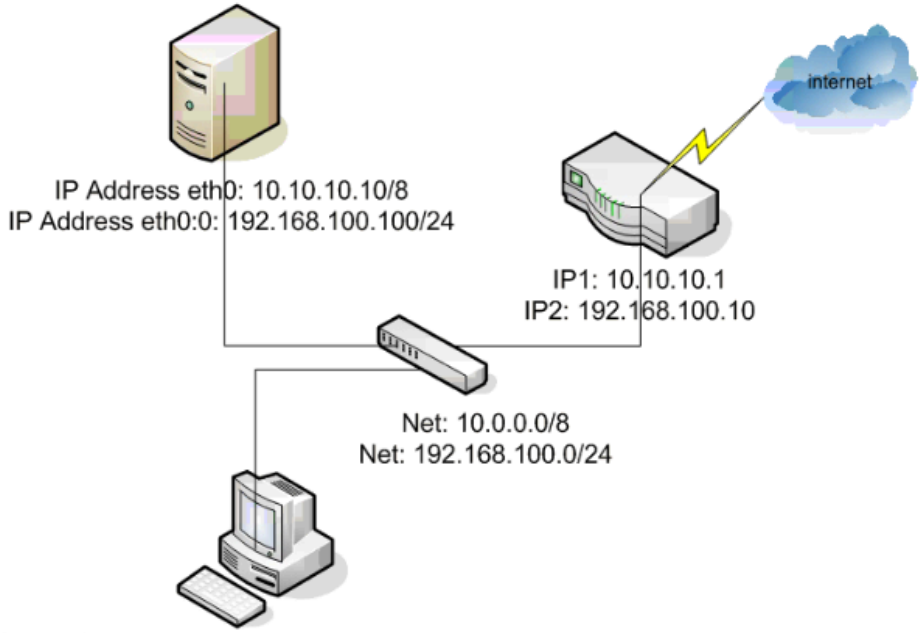
Bài 1: Cho hệ thống theo hình vẽ sau:



1. Thay đổi tên máy, sau đó khởi động lại bằng lệnh init 6
2. Xem địa chỉ mạng
3. Xem trạng thái kết nối vật lý của NIC
4. Đặt địa chỉ mạng và cập nhật

5. Dùng lệnh ping và ifconfig để kiểm tra cấu hình mạng
6. Kiểm tra cáp đã gắn vào card mạng hay chưa.

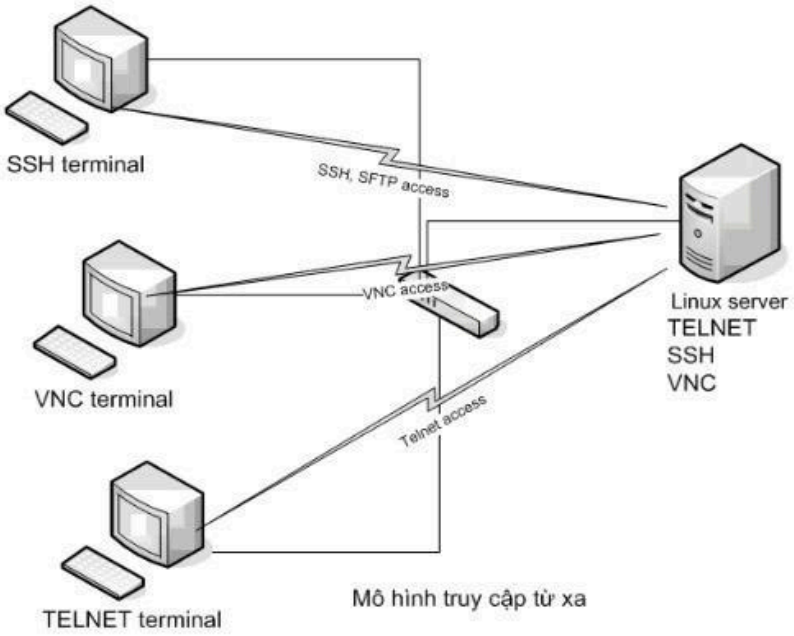
Bài 2: Cho hệ thống theo hình vẽ sau:



Thực hiện các yêu cầu sau:

1. Thêm địa chỉ IP cho card mạng eth0 với:
    - tên interface eth0:0
    - IP address: 192.168.100.100
    - netmask: 255.255.255.0
    - Gateway: 192.168.100.1
    - DNS: 192.168.100.1
2. Chỉ định default route cho hệ thống
3. Xem bảng định tuyến
4. Thống kê kết nối mạng

Bài 3: Cho hệ thống theo hình vẽ sau:



Mô hình truy cập từ xa

Cài đặt và cấu hình các dịch vụ hỗ trợ:

1. Cho phép mọi người kết nối từ xa vào máy chủ Linux qua telnet
2. Cho phép mọi người kết nối từ xa vào máy chủ Linux qua ssh
3. Cho phép mọi người kết nối từ xa vào máy chủ Linux qua VNC

BÀI 7: CÀI ĐẶT DỊCH VỤ TRÊN MÁY CHỦ

Mã bài: MĐ 40-07

Mục tiêu:

- Hiểu cách thức hoạt động của các dịch vụ Samba, DNS, DHCP, Web;
- Nắm được cách cấu hình các dịch vụ Samba, DNS, DHCP, Web trên máy chủ Linux;
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Dịch vụ SAMBA

Mục tiêu: Cung cấp cho người học chương trình hỗ trợ chia xẻ tài nguyên hệ thống Linux với các hệ thống khác. Ở đây, người học sẽ thực hiện được các thao tác: cài đặt, cấu hình, truy xuất vào các tài nguyên đã chia xẻ.

Samba là chương trình tiện ích hỗ trợ việc chia xẻ 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,…

Bộ Samba gồm nhiều thành phần. Daemon mang tên smbd cung cấp dịch vụ in ấn và tập tin. Tập tin cấu hình của Daemon này là smb.conf, còn daemon nmbd thì hỗ trợ dịch vụ tên NETBIOS, cho phép các máy tính khác truy cập và sử dụng các tài nguyên được cấp bởi máy chủ Samba. Trình smbclient, một thành phần khác của bộ Samba, hoạt động như một client bình thường giống như ftp. Trình tiện ích này dùng khi muốn truy cập những tài nguyên trên các server tương thích khác.

1.1. Cài đặt SAMBA

Có thể cài đặt Samba trong quá trình cài Linux hoặc cài sau bằng tiện ích RPM, các bộ này được tích hợp vào Fedora CD, các file này bao gồm:

system-config-samba-1.2.15-0.fc2.1 : hỗ trợ cấu hình trên giao diện X window

samba-3.0.7-2.FC2 : package chính của SAMBA

samba-client-3.0.7-2.FC2 : package cho SAMBA Client

samba-common-3.0.7-2.FC2 : hỗ trợ các thư viện cho SAMBA

samba-swat-3.0.7-2.FC2 : hỗ trợ cấu hình SAMBA qua Web

1.2. Khởi động SAMBA

Có thể khởi động dịch vụ samba tại thời điểm boot của hệ thống chkconfig.

```
# chkconfig smb on
```

Ta có thể start/stop/restart samba thông qua lệnh:

```
# service smb restart
```

Để kiểm tra samba có hoạt động trong hệ thống hay không

```
# pgrep smb
```

1.3. Cấu hình SAMBA

Tập tin cấu hình /etc/samba/smb.conf. Đây là một tập tin có dạng text. Các thành phần trong file cấu hình:

Thành phần	Giải thích
[global]	Chứa các tham số cấu hình chung của samba server
[printers]	Chứa các tham số sử dụng cho việc cấu hình máy in
[homes]	Chỉ định SMB chia xẻ thư mục home directory của user
[netlogon]	Chia xẻ logon script
[profile]	Chia xẻ profile

1.3.1. Đoạn [global]

Đoạn này kiểm soát tất cả tham số cấu hình chung của server smb. Đoạn này cũng cung cấp giá trị mặc định cho những đoạn khác:

[global]

workgroup = LINUX ; *chỉ ra nhóm mà máy này sẽ tham gia*

server string = Samba Server ;

hosts allow = 192.168.1. 192.168.2. 127. ; *host được phép truy xuất đến samba*

Guest account = pcguest ; *cung cấp username cho account khách trên server. Account này để nhận diện những user nào được dùng các dịch vụ samba dành cho khách*

Log file = /var/log/samba/smb.%m ; *xác định vị trí tập tin log của từng client truy cập samba*

Max log size = 50 ; *kích thước tối đa của một tập tin log (tính bằng kb)*

encrypt passwords = yes ; *cần hay không cần mã hoá password khi đăng nhập vào máy chủ Samba. Mọi password gửi từ Windows 9x đều mã hoá. Do đó, nếu ta chọn "no" thì máy chủ samba sẽ không chấp nhận sự đăng nhập của bất kỳ user nào. Nếu giá trị là "yes" thì chỉ có các user có password trong tập tin /etc/samba/password là có thể thấy máy chủ Samba.*

smb passwd file = /etc/samba/smbpasswd ; *tập tin lưu trữ những user được phép truy cập đến server smb.*

Một số biến cần tham khảo:

Tên biến	Mô tả giá trị
%S	Tên của dịch vụ hiện hành, nếu có
%P	Thư mục gốc của dịch vụ hiện hành, nếu có

%u	tên user của dịch vụ hiện hành
%g	tên của nhóm chính của %u
%U	tên phiên làm việc của user
%G	tên của nhóm chính của %U
%H	thư mục gốc của user
%v	phiên bản của Samba
%h	tên của host mà Samba đang chạy
%m	tên NETBIOS của máy khách
%L	tên NETBIOS của máy chủ
%M	tên Internet của máy khách
%I	Địa chỉ IP của máy khách
%T	ngày và giờ hiện hành
%a	kiến trúc của máy từ xa. Chỉ có một số máy được nhận diện là Win9x, WinNT, Win2k

1.3.2. Đoạn [homes]

Mặc định SMB chia xẻ home của từng người dùng trong hệ thống để cho phép các user có thể truy xuất vào home directory của mình từ máy trạm.

[homes]

comment = Home Directories ;

path = %H ;

read only = no ;

valid users = %S ; *Chỉ định tên user được phép truy xuất, nếu ta cho phép group ta dùng cú pháp @group_name.*

browseable = no ;

writeable = yes ;

create mask = 0750 ;

1.3.3. Chia xẻ máy in dùng SMB

Để chia xẻ máy in, ta mô tả đoạn [printers] trong file /etc/smb.conf

[printers]

comment = All Printers

path = /var/spool/samba

browseable = no

public = yes

guest ok = no

writable = no

printable = yes ; cho phép in

create mask = 0700

1.3.4. Chia xẻ thư mục

Sau khi lập cấu hình mặc định cho server Samba, có thể tạo ra nhiều thư mục dùng chung, và quyết định xem cá nhân nào hoặc group nào được phép sử dụng chúng.

[dirshare]

comment =”chia xẻ thư mục”

path = /usr/local/share

valid users = hv1

browseable = yes

public = no

writable = yes

Đoạn trên đã tạo ra một thư mục chia xẻ mang tên dirshare. Đường dẫn đến thư mục này là /usr/local/share. Vì public là no nên chỉ có user hv1 được truy cập đến thư mục này.

1.4. Sử dụng SAMBA SWAT

Swat là một công cụ cho phép cấu hình SAMBA qua giao diện Web. Nếu ta muốn sử dụng công cụ này thì ta phải cài thêm package samba-swat-3.0.7-2.FC2.rpm (trong Fedora Core).

1.4.1. Tập tin cấu hình SAMBA SWAT

Trước khi cấu hình SAMBA-SWAT, cần thiết lập một số thông số:

disable = no

only_from = 172.29.14.149 localhost

Trong file /etc/xinetd.d/swat để khởi động dịch vụ SWAT và cho phép các host nào có quyền truy xuất SAMBA SWAT qua Web.

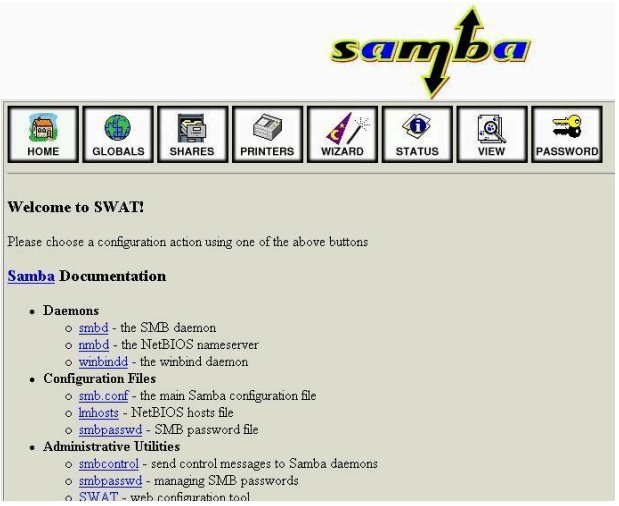
```
service swat
{
disable = no
port = 901
socket_type = stream
wait = no
only_from = 172.29.14.149 localhost
user = root
server = /usr/sbin/swat
log_on_failure  += USERID
}
```

1.4.2. Truy xuất SWAT từ Internet Explorer

Truy xuất SMB SWAT thông qua địa chỉ http://172.29.14.150:901 từ IE; Sau đó, chỉ định username (root nếu ta muốn quản lý SMB), và mật khẩu để đăng nhập:

Màn hình đăng nhập

Sau khi đăng nhập thành công



Giao diện Samba SWAT

1.4.3. Cấu hình SAMBA SWAT

Thành phần	Giải thích
	Cung cấp các tài liệu tham khảo về samba
	Quản lý thông tin cấu hình
	Quản lý tài nguyên chia xẻ
	Quản lý việc chia xẻ máy in
	Quản lý Server Type, Wins và một số tham số khác

	Quản lý trạng thái của SAMBA, theo dõi các connection...
	Xem các thông tin cấu hình trong file smb.conf
	Quản lý mật khẩu

2. Dịch vụ DNS

Mục tiêu: Trình bày cơ chế hoạt động của dịch vụ DNS, cách cấu hình dịch vụ DNS trên máy chủ Linux.

2.1. Giới thiệu về DNS

Các máy tính trong mạng muốn liên lạc hay trao đổi thông tin, dữ liệu cho nhau cần phải biết địa chỉ IP của nhau. Nếu số lượng máy tính nhiều thì việc nhớ những địa chỉ IP này là rất khó. Mỗi máy tính ngoài địa chỉ IP còn có tên (computer name). Đối với con người việc nhớ những cái tên này dù sao cũng dễ dàng hơn vì chúng có tính trực quan và gợi nhớ hơn địa chỉ IP. Vì thế, người ta nghĩ ra cách làm sao ánh xạ địa chỉ IP thành tên máy tính.

Ban đầu do quy mô mạng ARPAnet (tiền thân của mạng Internet) còn nhỏ chỉ vài trăm máy, nên chỉ có một tập tin đơn HOSTS.TXT lưu thông tin về ánh xạ tên máy thành địa chỉ IP. Trong đó tên máy là chuỗi văn bản không phân cấp (flat name). Tập tin này được duy trì tại 1 máy chủ và các máy chủ khác lưu giữ bản sao của nó. Tuy nhiên khi quy mô mạng lớn hơn, việc sử dụng tập tin HOSTS.TXT có các nhược điểm như sau:

- Lưu lượng mạng và máy chủ duy trì tập tin HOSTS.TXT bị quá tải do hiệu ứng “cổ chai”.

- Xung đột tên: Không thể có 2 máy tính có cùng tên trong tập tin HOSTS.TXT. Tuy nhiên do tên máy không phân cấp và không có gì đảm bảo để

ngăn chặn việc tạo 2 tên trùng nhau vì không có cơ chế uỷ quyền quản lý tập tin nên có nguy cơ bị xung đột tên.

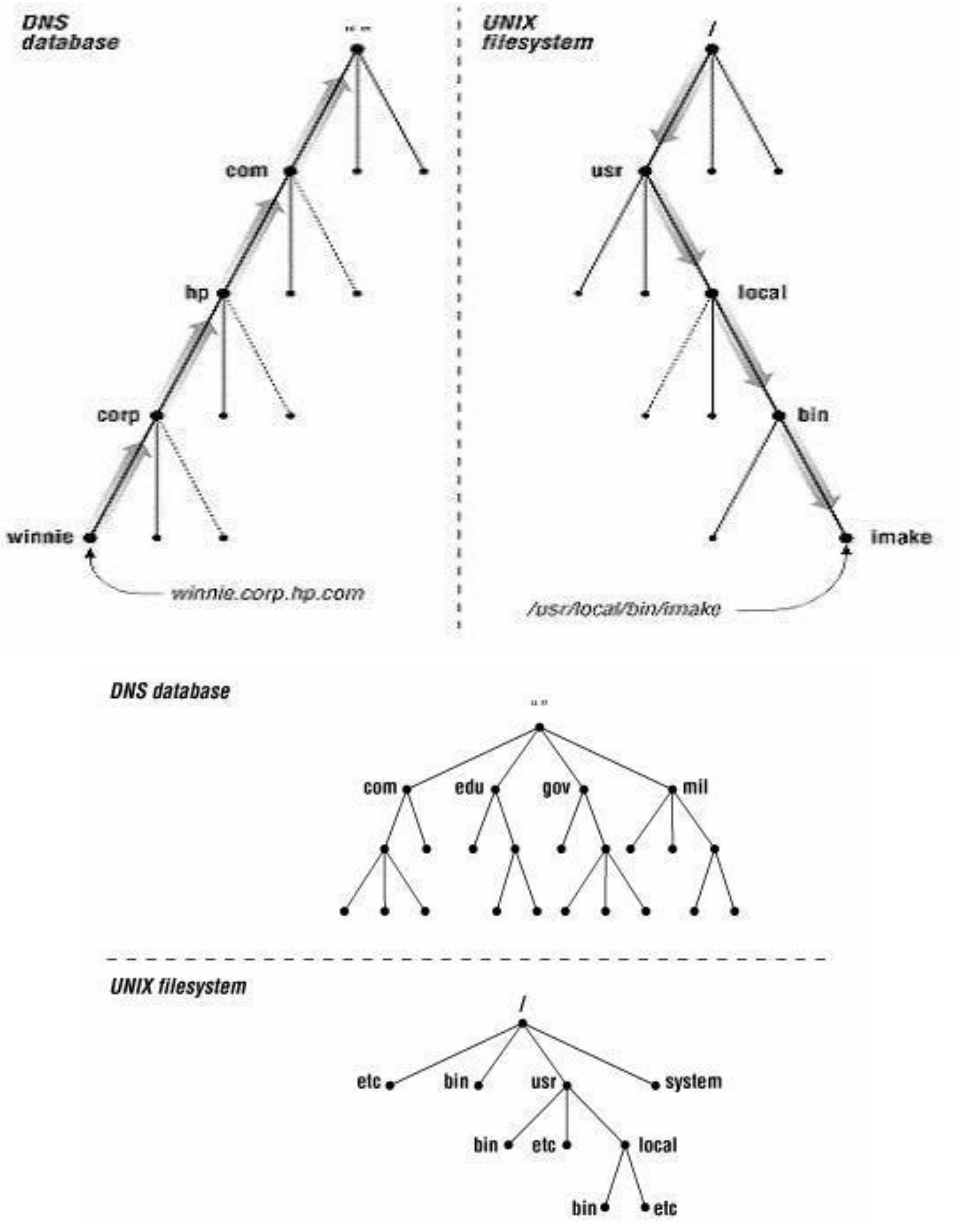
- Không đảm bảo sự toàn vẹn: việc duy trì 1 tập tin trên mạng lớn rất khó khăn. Ví dụ như khi tập tin HOSTS.TXT vừa cập nhật chưa kịp chuyển đến máy chủ ở xa thì đã có sự thay đổi địa chỉ trên mạng.

Tóm lại, việc dùng tập tin HOSTS.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. Người thiết kế cấu trúc của dịch vụ DNS là Paul Mockapetris - USC's Information Sciences Institute, và các khuyến nghị RFC của DNS là RFC 882 và 883, sau đó là RFC 1034 và 1035 cùng với 1 số RFC bổ sung như bảo mật trên hệ thống DNS, cập nhật động các bản ghi DNS…

Lưu ý: Hiện tại trên các máy chủ vẫn sử dụng được tập tin hosts.txt để phân giải tên máy tính thành địa chỉ IP (trong Linux là /etc/hosts)

Dịch vụ DNS hoạt động theo mô hình Client - Server: phần Server gọi là máy chủ phục vụ tên nameserver, còn phần Client là trình phân giải tên resolver. Nameserver chứa các thông tin CSDL của DNS, còn resolver 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 thuộc phạm vi của họ, đồng thời dữ liệu này cũng dễ dàng truy cập được trên toàn bộ hệ thống mạng theo mô hình Client - Server. Hiệu suất sử dụng dịch vụ được tăng cường thông qua cơ chế nhân 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 cntt.danavtc.edu, trong đó cntt là hostname và danavtc.edu là domain name. Domain name phân bổ theo cơ chế phân cấp tương tự như sự phân cấp của hệ thống tập tin Unix/Linux.



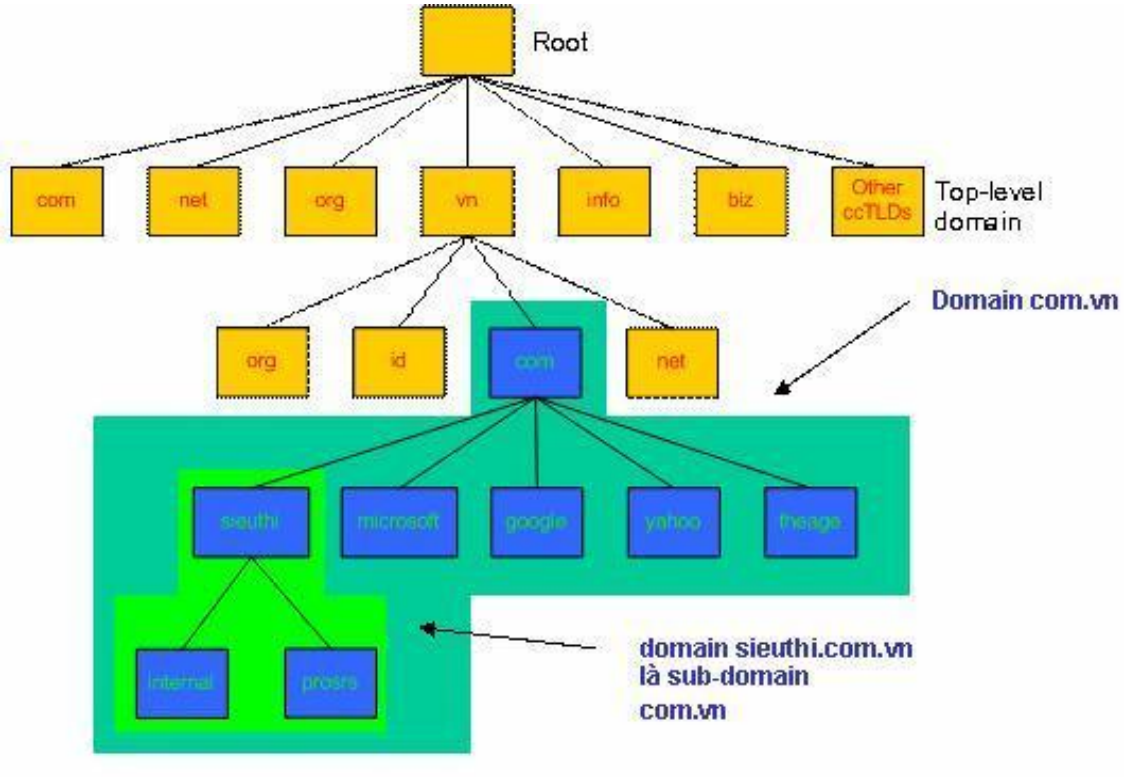
Cơ sở dữ liệu (CSDL) của DNS là một cây đảo ngược. Mỗi nút trên cây cũng lại là gốc của 1 cây con. Mỗi cây con là 1 phân vùng con trong toàn bộ CSDL DNS gọi là 1 miền (domain). Mỗi domain có thể phân chia thành các phân vùng con nhỏ hơn gọi là các miền con (subdomain). Mỗi domain có 1 tên (domain name). Tên domain chỉ ra vị trí của nó trong CSDL DNS. Trong DNS tên miền là chuỗi tuần tự các tên nhãn tại nút đó đi ngược lên nút gốc của cây và phân cách nhau bởi dấu chấm. Tên nhãn bên phải trong mỗi domain name được gọi là top-level domain. Trong ví dụ trước cntt.danavtc.edu, vậy .edu là top-level domain. Bảng sau đây liệt kê top-level domain

Tên miền	Mô tả
.com	Các tổ chức, công ty thương mại
.org	Các tổ chức phi lợi nhuận
.net	Các trung tâm hỗ trợ về mạng
.edu	Các tổ chức giáo dục
.gov	Các tổ chức thuộc chính phủ
.mil	Các tổ chức quân sự
.int	Các tổ chức được thành lập bởi các hiệp ước quốc tế

Vì sự quá tải của những domain name đã tồn tại, do đó đã làm phát sinh những top-level domain mới. Bảng sau đây liệt kê những top-level domain mới.

Tên miền	Mô tả
.arts	Những tổ chức liên quan đến nghệ thuật và kiến trúc
.nom	Những địa chỉ cá nhân và gia đình
.rec	Những tổ chức có tính chất giải trí, thể thao
.firm	Những tổ chức kinh doanh, thương mại
.info	Những dịch vụ liên quan đến thông tin

Bên cạnh đó, mỗi nước cũng có một top-level domain. Ví dụ top-level domain của Việt Nam là vn, Mỹ là us… Mỗi nước khác nhau có cơ chế tổ chức phân cấp domain khác nhau. Ví dụ về tổ chức domain của Việt Nam:



2.2. Cách phân bố dữ liệu quản lý Domain Name

Những root name server (.) quản lý những top-level domain trên Internet. Tên máy và địa chỉ IP của những name server này được công bố cho mọi người biết và chúng được liệt kê trong bảng sau. Những name server này cũng có thể đặt khắp nơi trên thế giới.

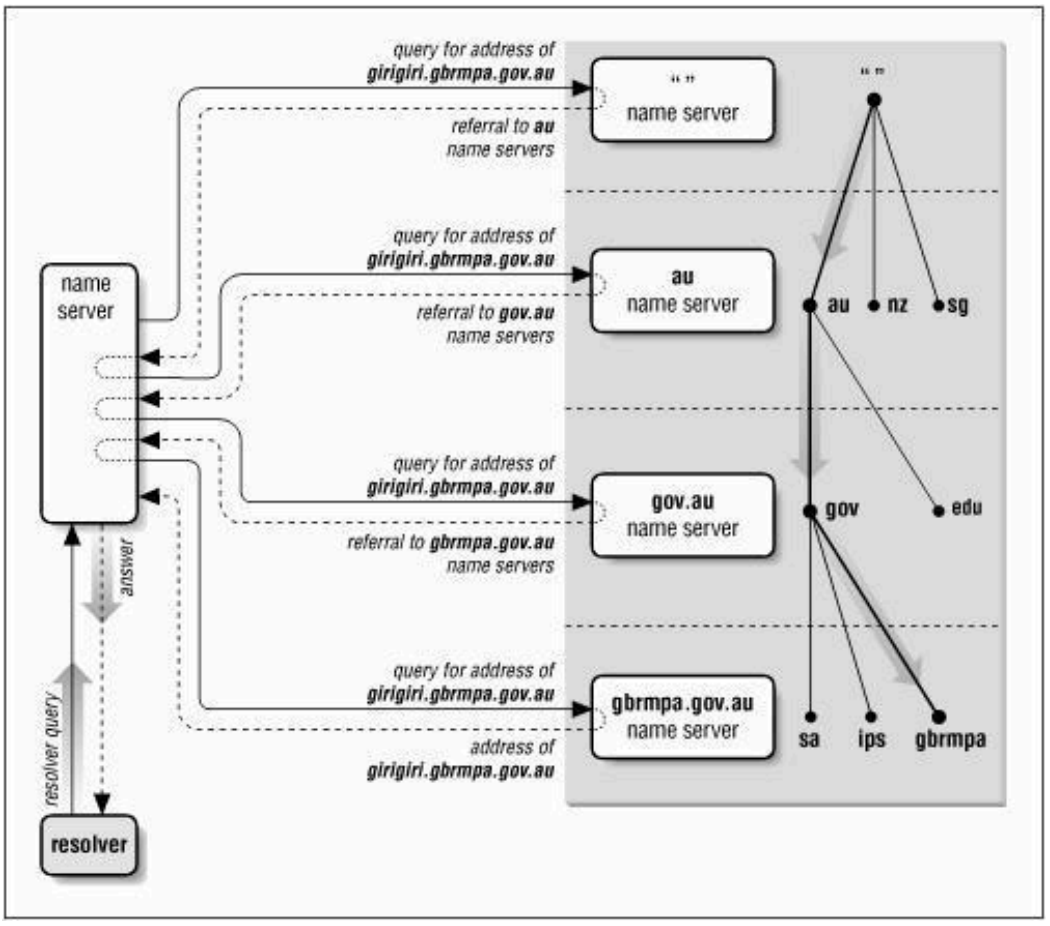
Tên máy tính	Địa chỉ IP
H.ROOT-SERVERS.NET	128.63.2.53
B.ROOT-SERVERS.NET	128.9.0.107
C.ROOT-SERVERS.NET	192.33.4.12
D.ROOT-SERVERS.NET	128.8.10.90
E.ROOT-SERVERS.NET	192.203.230.10
I.ROOT-SERVERS.NET	192.36.148.17
F.ROOT-SERVERS.NET	192.5.5.241
F.ROOT-SERVERS.NET	39.13.229.241
G.ROOT-SERVERS.NET	192.112.88.4
A.ROOT-SERVERS.NET	198.41.0.4

Thông thường một tổ chức được đăng ký một hay nhiều domain name. Sau đó, mỗi tổ chức sẽ cài đặt một hay nhiều name server và duy trì cơ sở dữ liệu cho tất cả những máy tính trong domain. Những name server của tổ chức được đăng ký trên Internet. Một trong những name server này được biết như là Primary Name Server. Nhiều Secondary Name Server được dùng để làm backup cho Primary Name Server. Trong trường hợp Primary bị lỗi, Secondary được sử dụng để phân giải tên. Primary Name Server có thể tạo ra những subdomain và ủy quyền những subdomain này cho những Name Server khác.

2.3. Cơ chế phân giải tên

2.3.1. 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 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 (Thực tế là hầu hết các root server cũng chính là máy chủ 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. Hình vẽ dưới mô tả 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 girigiri.gbrmpa.gov.au đến name server cục bộ. Khi nhận yêu cầu từ resolver, Nameserver cục bộ sẽ phân tích tên này và xét xem tên miền này có do mình quản lý hay không. Nếu 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 một 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 miền 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 nameserver 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. Nameserver không thể tham chiếu truy vấn đến một name server khác. Nameserver có thể gửi truy vấn dạng đệ quy hoặc tương tác đến nameserver khác nhưng nó phải thực hiện cho đến khi nào có kết quả mới thôi.

- Truy vấn tương tác: khi nameserver 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 nameserver 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 nameserver không tìm thấy trong dữ liệu cục bộ nó sẽ trả về tên miền và địa chỉ IP của nameserver gần nhất mà nó biết.

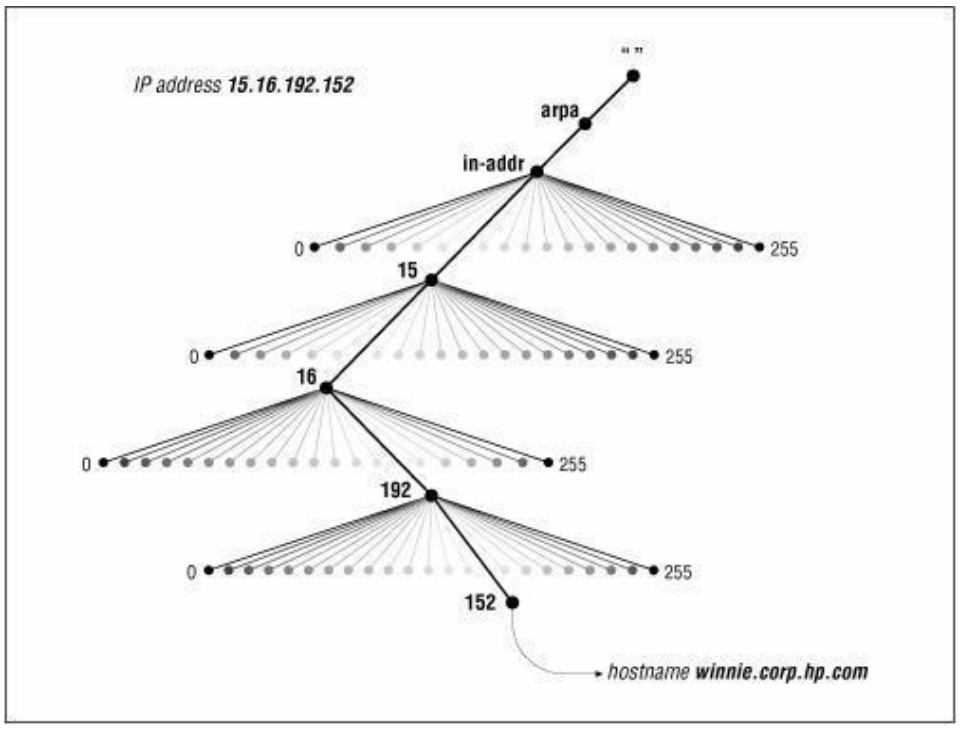
2.3.2. Phân giải IP thành tên máy tính

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. Ví dụ miền in-addr.arpa có thể có 256 subdomain, tương ứng với 256 giá trị từ 0 đến 255 của byte đầu tiên trong địa chỉ IP. Trong mỗi subdomain lại có 256 subdomain con nữa ứng với byte thứ hai. Cứ như thế và đến byte thứ tư

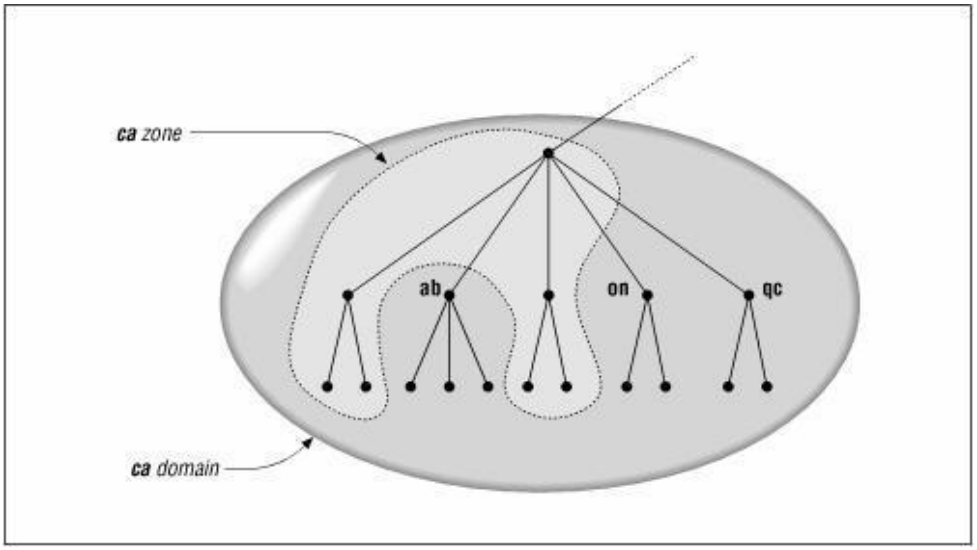
có các bản ghi cho biết tên miền đầy đủ của các máy tính hoặc các mạng có địa chỉ IP tương ứng.



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.in-addr.arpa.

2.4. So sánh Domain Name – Zone

Một miền gồm nhiều thực thể nhỏ hơn gọi là miền con (subdomain). Ví dụ: miền ca bao gồm nhiều miền con như ab.ca, on.ca, qc.ca,... (như hình vẽ dưới). Có thể ủy quyền một số miền con cho những DNS Server khác quản lý. Những miền và miền con mà DNS Server được quyền quản lý gọi là zone. Như vậy, một zone có thể gồm một miền, một hay nhiều miền con. Hình sau mô tả sự khác nhau giữa zone và domain.



2.5. 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 tả những loại Domain Name Server:

2.5.1. Primary Name Server

Mỗi miền phải có một Primary Name Server. Server này được đăng kí 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.

2.5.2. Secondary Name Server

Mỗi miền có một Primary Name Server để quản lý CSDL của miền. Nếu 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. Vấn đề này ảnh hưởng rất lớn đến những 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; khi Primary Name Server bị gián đoạn, nó sẽ đảm nhận 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. Theo một chu kỳ, Secondary sẽ sao chép và cập nhật CSDL từ Primary Name Server.

2.5.3. 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 thông tin 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 những mạng lớn.

3. Dịch vụ DHCP

Mục tiêu: Trình bày cơ chế hoạt động của dịch vụ DHCP, cách cấu hình dịch vụ DHCP trong việc quản trị hệ thống mạng.

DHCP – Dynamic Host Configuration Protocol – là một dịch vụ hữu ích trong việc quản trị những mạng lớn hay mạng có những người dùng di động. DHCP Server là máy cấp phát địa chỉ IP cho những máy tính khác trong mạng, DHCP client là các máy nhận địa chỉ IP và những thông tin về mạng khác từ DHCP Server.

3.1. Một số lưu ý trên DHCP

- Phải có một địa chỉ IP tĩnh;

- Không phải là một DHCP client;

- Cấp phát địa chỉ IP cho những máy tính trong một khoảng địa chỉ IP mà người quản trị đã định nghĩa;

- Có thể cung cấp địa chỉ default gateway, DNS server, tên domain và NetBIOS name server cho máy tính;

- Không có hai máy nhận cùng địa chỉ IP;

- Địa chỉ IP cấp cho DHCP client sẽ được làm mới khi máy tính khởi động lại.

3.2. Ưu điểm của DHCP

Người quản trị không cần đặt địa chỉ IP cho từng máy tính trong mạng. Người quản trị không cần cung cấp thông tin cho từng máy điều này tiết kiệm được thời gian và một số chi phí khác.

3.3. Cấu hình DHCP server

Để cấu hình DHCP server cần phải cài package dhcpd.*.rpm này trong đĩa CD Linux.

Cài đặt DHCP bằng lệnh: #rpm –ivh dhcpd.*.rpm

Để hoàn thành việc cấu hình DHCP cần phải tạo ra tập tin cấu hình /etc/dhcpd.conf và chỉnh sửa tập tin này. Ví dụ về nội dung cấu hình chính của tập tin dhcpd.conf

```
ddns-update-style interim;
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "example.com";
subnet 192.168.1.0 netmask 255.255.255.0 {
        range 192.168.1.10 192.168.1.100;
}
```

Tập tin /var/lib/dhcp/dhcpd.leases. Tập tin này được sử dụng bởi daemon dhcpd để lưu những thông tin về các địa chỉ IP đã được cấp phát

3.4. Khởi động DHCP

Sau khi thiết lập những tập tin cấu hình, ta cần khởi động dịch vụ bằng lệnh: #/etc/init.d/dhcpd start

4. Dịch vụ Web

Mục tiêu: Trình bày các giao thức giao tiếp giữa trình duyệt web và server, cách thức hoạt động, cài đặt và cấu hình Web server.

4.1. Web server

4.1.1. Giao thức HTTP

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

HTTP bắt đầu là 1 giao thức đơn giản giống như với các giao thức chuẩn khác trên Internet, thông tin 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.

Ví dụ:

```
> telnet www.extropia 80
GET /index.html HTTP/1.0
```

Cổng 80 là cổng mặc định dành cho Web server "lắng nghe" các kết nối được gửi đến. Để đáp ứng lệnh HTTP GET, Web server trả về cho client trang "index.html" thông qua phiên làm việc telnet này, và sau đó đóng kết nối. Thông tin trả về dưới dạng code HTML:

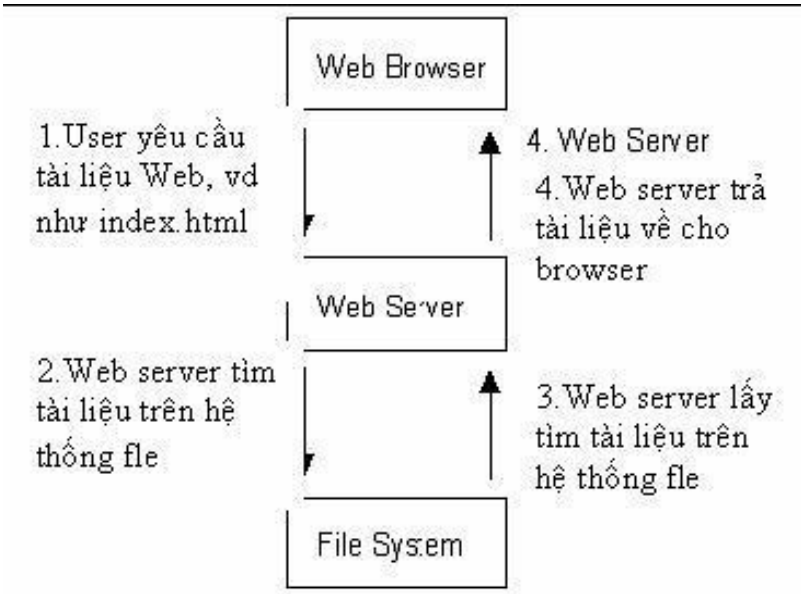
```
<HTML>
<HEAD>
<TITLE>eXtropia Homepage</TITLE>
```

</HEAD>

…

</HTML>

Giao thức chỉ thực thi đơn giản hai thao thác yêu-cầu/đáp-ứng (request/response). Một trong các thay đổi lớn nhất trong HTTP/1.1 là nó hỗ trợ kết nối lâu dài (persistent connection).



Trong HTTP/1.0, một kết nối phải được thiết lập đến server cho mỗi đối tượng mà Browser muốn download. Nhiều trang Web có rất nhiều hình ảnh, ngoài việc tải trang HTML cơ bản, browser phải lấy về một số lượng hình ảnh. Nhiều cái trong chúng thường là nhỏ hoặc chỉ đơn thuần là để trang trí cho phần còn lại của trang HTML. Thiết lập một kết nối cho mỗi hình ảnh thật là phí phạm, vì sẽ có nhiều gói thông tin mạng sẽ được luân chuyển giữa Web browser và Web server trước khi dữ liệu ảnh được truyền về. Ngược lại, mở một kết nối TCP truyền tài liệu HTML và sau đó mỗi hình ảnh sẽ truyền nối tiếp theo như thế sẽ thuận tiện hơn và quá trình thiết lập các kết nối TCP sẽ được giảm xuống.

4.1.2. Web Server và cách hoạt động

Ở mức độ cơ bản, Web server chỉ phục vụ các nội dung tĩnh. Nghĩa là khi Web server nhận 1 yêu cầu từ Web browser, 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 đến 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 văn bản thô (raw text) chứa các thẻ định dạng (HTML tag).

Ví dụ:

```
<html>
<head> <title> WWW </title>
</head>
<body>
<p align=center>
<a href="http://www.danavtc.edu.vn/"><b>Trường Cao Đẳng Nghề ĐN
</b></a>
</b>
</p>
</body>
</html>
```

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 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 site 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 mất thời gian để tính toán cho ra kết quả.

Ví dụ:

Nếu một chương trình CGI mất 30 giây để sinh ra nội dung, trong thời gian này Web server có thể sẽ không phục vụ các trang khác nữa. Do vậy, mặc dù mô hình này hoạt động được, nhưng nó vẫn cần phải thiết kế lại để phục vụ được nhiều người trong cùng 1 lúc. Web server có xu hướng tận dụng ưu điểm của 2 phương pháp khác nhau để giải quyết vấn đề này là: đa tiểu trình (multi-threading) hoặc đa tiến trình (multi-processing) hoặc các hệ lai giữa multi-processing và multi-threading.

4.1.3. Web client

Web client là những chương trình duyệt Web ở phía người dùng (Internet Explorer, Netscape Communicator…) để hiển thị những 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.

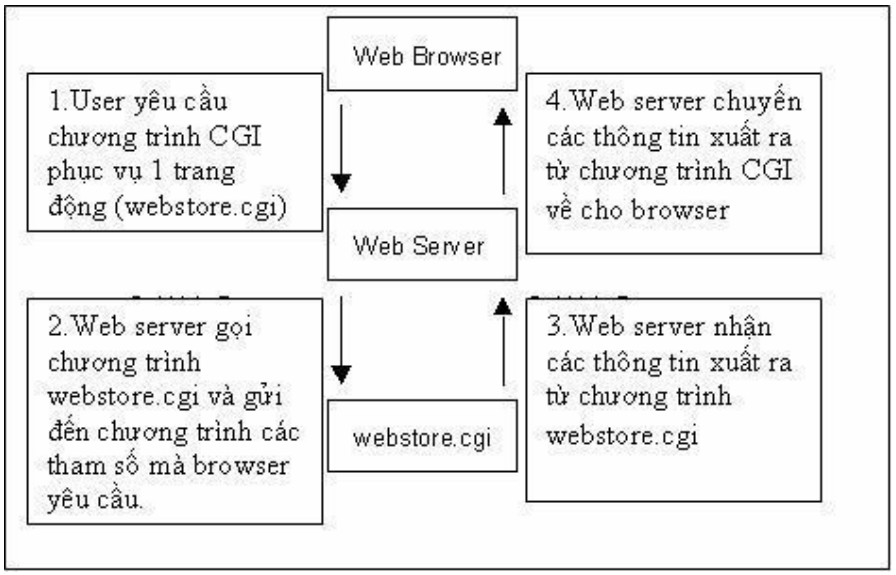
4.1.4. Web động

Một trong các nội dung động (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. Hình vẽ sau minh họa khi Web browser yêu cầu một trang Web động phát sinh từ chương trình CGI.



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

4.2. Apache

4.2.1. 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.

4.2.2. Cài đặt Apache

Ta chỉ cần cài đặt package httpd-2.0.40-21.i386.rpm (trên Fedora) trong hệ điều hành Linux.

```
#rpm  –ivh  httpd-2.0.40-21.i386.rpm
```

Vị trí cài đặt Apache trong môi trường Linux là /etc/httpd. Trong thư mục này lưu giữ những tập tin cấu hình của Apache.

4.2.3. Tạm dừng và khởi động lại Apache

Để tạm dừng hay khởi động lại apache dùng script sau:

```
# chkconfig httpd on

#/etc/init.d/httpd start/stop/restart
```

Hoặc dùng lệnh:

```
# chkconfig httpd on

#service httpd restart
```

4.3.4. Sự chứng thực, cấp phép, điều khiển việc truy cập

Khi nhận một yêu cầu truy cập tài nguyên, web server sẽ xử lý như thế nào để trả kết quả về cho client. Apache có những hướng xử lý khác nhau như chứng thực, cấp phép và điều khiển truy cập.

4.3.4.1. Basic Authentication

Đối với những thông tin cần bảo mật, khi có yêu cầu truy xuất thông tin này, Web Server phải chứng thực những yêu cầu này có hợp lệ hay không. Thông thường, thông tin chứng thực bao gồm username và password.

+ Nếu một tài nguyên được bảo vệ với sự chứng thực. Apache sẽ gửi một yêu cầu “401 Authentication” thông báo cho người dùng nhập vào username và password của mình. Nhận được yêu cầu này, client sẽ trả lời 401 đến server trong đó có chứa username và password. Server sẽ kiểm tra những thông số này

khi nhận được. Nếu hợp lệ server sẽ trả về những thông tin yêu cầu, ngược lại nó sẽ trả về một thông báo lỗi.

+ Vì giao thức HTTP là một tiêu chuẩn không của riêng ai và cũng không thuộc một quốc gia nào, nên mỗi yêu cầu đều được xem như nhau.

+ Username và password được yêu cầu cung cấp chỉ có tác dụng trong lần giao dịch của browser với server lúc đó. Nếu lần sau truy cập lại website này, phải nhập lại username và password.

+ Song song với trả lời 401, toàn bộ thông tin sẽ trả ngược lại cho client. Trong những trường hợp riêng biệt, server sẽ cấp lại cho client một thẻ chứng thực để bảo vệ website. Thẻ này được gọi là realm hay là một tên chứng thực. Browser sẽ lưu lại username và password đã cung cấp cùng với realm. Như thế, nếu truy cập những tài nguyên khác mà có cùng realm, username và password thì user không cần nhập trở lại những thông tin chứng thực. Thông thường, việc lưu trữ này chỉ có tác dụng trong giao dịch hiện hành của browser. Nhưng cũng có một vài browser cho phép lưu chúng một cách cố định để không cần nhập lại username và password.

Các bước cấu hình chứng thực:

+ Bước 1: tạo tập tin password, cấp quyền truy xuất cho tập tin mật khẩu dùng lệnh chmod 755 <tập_tin_mật_khẩu_được_tạo_ở_bước_1>

+ Bước 2: cấu hình apache

+ Bước 3: tạo tập tin group (nếu muốn chứng thực cho nhóm)

Bước 1: Tạo tập tin password dùng lệnh htpasswd. Cách sử dụng lệnh htppaswd theo cú pháp như sau:

#htpasswd -c <vị_trí_tập_tin_password> <username>

Ví dụ:

htpasswd -c /etc/httpd/conf/passwords rbowen

htpasswd sẽ yêu cầu nhập password, sau đó xác thực lần nữa.

New password: mypassword

Re-type new password: mypassword

+ Tùy chọn –c sẽ tạo một tập tin password mới. Nếu tập tin này đã tồn tại nó sẽ xóa nội dung cũ và ghi vào nội dung mới. Khi tạo thêm một người dùng, tập tin password đã tồn tại nên không cần dùng tùy chọn –c.

+ <vị_trí_tập_tin_password>: thông thường nó tạo tại thư mục gốc của apache

Bước 2: Cấu hình sự chứng thực trên Apache:

```
<Directory /upload>
        EnablePut On
        AuthType Basic
        AuthName Temporary
        AuthUserFile /etc/httpd/conf/passwd
        EnableDelete Off
        umask 007
        <Limit PUT>
                require user rbowen sungo
        </Limit>
        </Directory>
```

+ AuthType: khai báo loại authentication sẽ sử dụng. Trong trường hợp này là Basic

+ AuthName: đặt tên cho sự chứng thực

+ AuthUserFile: vị trí của tập tin password

+ AuthGroupFile: vị trí của tập tin group

+ Require: những yêu cầu hợp lệ được cho phép truy cập tài nguyên.

Bước 3: Tạo tập tin group: Nhằm tạo điều kiện thuận lợi cho người quản trị trong việc quản lý sự chứng thực, Apache hỗ trợ thêm tính năng nhóm người dùng. Người quản trị có thể tạo những nhóm người dùng được phép truy cập đến tài nguyên, thêm hay xóa những thành viên trong group ngoài việc chỉnh sửa lại tập tin cấu hình apache và khởi động lại apache. Định dạng của tập tin group:

<tên nhóm>: user1 user2 user3 … user n

Ví dụ:

authors: rich daniel allan

Sau khi tạo tập tin nhóm, cần phải cấu hình để apache để chỉ ra tập tin nhóm này bằng những directive sau:

```
<Directory  /upload>
AuthType Basic
AuthName "Apache Admin Guide Authors"
AuthUserFile /etc/httpd/conf/passwords
AuthGroupFile /etc/httpd/conf/groups
Require group authors
</Directory>
```

4.3.4.2. Digest Authentication

Digest authentication cung cấp một phương pháp bảo vệ nội dung web một cách luân phiên. Digest authentication được cung cấp bởi module mod_auth_digest. Với phương pháp này tên user và mật khẩu sẽ không được gởi ở dạng plain text mà chúng được mã hóa (thông qua thuật toán MD5)

Cấu hình: Tương tự như sự chứng thực cơ bản, cấu hình này cũng gồm 2 hoặc 3 bước sau:

- Bước 1: Tạo file mật khẩu.

- Bước 2: Cấu hình /etc/httpd/conf/httpd.conf để sử dụng file mật khẩu ở bước 1.

- Bước 3: Tạo group file.

Bước 1: Tạo tập tin password dùng lệnh htdigest –c <vị_ trí_tập_tin_password> realm <username>

Bước 2: Cấu hình /etc/httpd/conf/httpd.conf để sử dụng file mật khẩu

<Directory /upload>
AuthType Digest
AuthName "Private"
AuthDigestFile /usr/local/apache/passwd/digest
AuthDigestGroupFile /usr/local/apache/passwd/digest.groups
Require group admins
</Directory>

Bước 3: Tạo tập tin nhóm (bước này chỉ thực hiện khi ta muốn chứng thực cho nhóm). Cấu trúc của tập tin nhóm cũng tương tự như tập tin nhóm của basic authentication.

admins: joy danne sue

4.3.5. Điều khiển truy cập

Ngoài việc bảo mật nội dung của website bằng sự chứng thực (username và password), apache còn giới hạn việc truy cập của người dùng dựa trên những thông tin khác được đề cập trong Access Control. Sử dụng directive Al

ow/Deny để cho phép/cấm việc truy cập tài nguyên dựa trên tên máy tính hoặc địa chỉ IP.

Allow/Deny Directive:

Cú pháp khai báo Allow/Deny như sau

Allow/Deny from [address]

+ Allow: cho phép các host/network/domain truy xuất vào Web server.

+ Deny: cấm các host/network/domain truy xuất vào Web server.

+ address: địa chỉ IP/địa chỉ đường mạng hay tên máy tính, tên miền.

Ví dụ:

```
Deny from 11.22.33.44
Deny from host.example.com
Deny from 192.101.205
Deny from exampleone.com example
```

Sử dụng Order để kết hợp giữa Allow và Deny trong việc giới hạn việc truy cập. Nếu thứ tự của Order là Deny, Allow thì Deny được kiểm tra trước tiên và bất kỳ những client nào không phù hợp với Deny hoặc phù hợp với một Allow thì được phép truy cập đến server. Ngược lại, nếu thứ tự của Order là Alow, Deny thì Allow được kiểm tra trước và bất kỳ client nào không phù hợp với một điều kiện Allow hoặc phù hợp với một điều kiện Deny thì bị cấm truy cập đến server.

Ví dụ về một điều khiển truy cập ít giới hạn nhất.

```
<Directory "/usr/web">
Options Indexes FollowSymLinks MultiViews
AllowOverride All
Order allow,deny
```

Allow from all

</Directory>

Satisfy directive:

- Satisfy directive được dùng để chỉ ra nhiều tiêu chuẩn cần phải được xem xét trong việc bảo mật nội dung website. Satisfy có 2 giá trị là all và any. Mặc định, Satisfy nhận giá trị all, điều này có nghĩa là nếu nhiều tiêu chuẩn được chỉ ra thì tất cả những tiêu chuẩn này phải thoả mãn thì người dùng mới được phép truy cập tài nguyên. Còn giá trị any có nghĩa là một trong những tiêu chuẩn này hợp lệ thì user được phép truy cập đến tài nguyên.

- Một ứng dụng của việc sử dụng access control là giới hạn, những người dùng bên ngoài mạng khi truy cập tài nguyên cần phải có username và password còn tất cả những máy tính trong mạng thì không cần.

<Directory /usr/local/apache/htdocs/sekrit>

AuthType Basic

AuthName intranet

AuthUserFile /etc/httpd/conf/users

AuthGroupFile /etc/httpd/conf/groups

Require group customers

Allow from internal.com

Satisfy any

</Directory>

4.3.6. Khảo sát log file trên apache

Apache có nhiều tập tin log khác nhau nhằm ghi lại những hoạt động của Web Server. Sau đây mô tả tính năng của từng tập tin.

File **error_log**: Là một tập tin log quan trọng nhất. Tên và vị trí của nó được xét trong ErrorLog directive. ErrorLog là nơi mà httpd sẽ gửi những thông

tin nhận dạng và bất kỳ những lỗi nào gặp phải trong quá trình xử lý những yêu cầu. Tập tin này chính là nơi mà ta cần xem xét đầu tiên khi gặp phải những lỗi khởi động httpd hay những thao tác của server, vì nó lưu những thông tin chi tiết về những lỗi và cách sửa lỗi. Định dạng của tập tin error_log không bị bó buộc. Nội dung của file error_log như sau:

[Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration:

/export/home/live/ap/htdocs/test

Cột đầu tiên chỉ ra ngày giờ entry này được tạo ra. Cột thứ 2 chỉ ra đây là entry lỗi. Cột thứ 3 cho biết địa chỉ IP của client tạo ra lỗi. Tiếp theo là message có nội dung chỉ ra rằng server được cấu hình để từ chối việc truy cập của client. Tiếp theo là đường dẫn của document mà client cần truy cập. Trong quá trình kiểm tra, có thể theo dõi error_log một cách liên tục bằng dòng lệnh sau:

#tail –f /var/log/httpd/error_log

File **access_log**: Access_log là nơi ghi lại tất cả những yêu cầu được xử lý bởi server. Vị trí và nội dung của access log được điều khiển bởi CustomLog directive. Có thể dùng LogFormat directive trong việc định dạng nội dung của tập tin access_log. LogFormat chỉ ra những thông tin mà server cần theo dõi để ghi lại trong access log. Để theo dõi yêu cầu xử lý trên Web Server ta dùng lệnh:

#tail –f /var/log/httpd/access_log

Luân chuyển log file:

Theo thời gian, thông tin lưu trong các tập tin log lớn làm cho kích thước của các tập tin này có thể vượt quá 1MB. Do đó, cần phải xóa, di chuyển hay sao lưu những tập tin log này một cách luân phiên và có chu kỳ. Cách thực hiện như sau:

```
mv access_log access_log.old
mv error_log  error_log.old
apachectl graceful
sleep 600
gzip access_log.old error_log.old
```

4.3. Cấu hình Web server

Các tập tin và thư mục cấu hình của Apache:

- /etc/httpd/conf: thư mục lưu giữ các tập tin cấu hình như httpd.conf.

- /etc/httpd/modules: lưu các module của Web Server.

- /etc/httpd/logs: lưu các tập tin log của Apache.

- /var/www/html: lưu các trang Web.

- /var/www/cgi-bin: lưu các script sử dụng cho các trang Web.

Tập tin cấu hình Apache được tạo thành từ nhiều chỉ dẫn (directive) khác nhau. Mỗi dòng/một đoạn là một directive và phục vụ cho một cấu hình riêng biệt. Có những directive có ảnh hưởng với nhau. Những dòng bắt đầu bằng dấu # là những dòng chú thích.

4.3.1. Định nghĩa về ServerName

4.3.1.1. Chỉ định một số thông tin cơ bản

Cấu hình tên máy tính (hostname) của server. Nó được dùng trong việc tạo ra những URL chuyển tiếp (redirection URL). Nếu không chỉ ra, server sẽ cố gắng suy luận từ địa chỉ IP của nó. Tuy nhiên, điều này có thể không tin cậy hoặc không trả ra tên máy tính đúng. Cú pháp khai báo:

```
ServerName  <hostname>
```

Ví dụ:

```
ServerName  www.soft.com
```

ServerAdmin:

Địa chỉ Email của người quản trị hệ thống

Cú pháp:

ServerAdmin <địa chỉ email>

Ví dụ:

ServerAdmin root@soft.com

ServerType: Qui định cách nạp chương trình. Có hai cách:

+ inetd: chạy từ hệ thống.

+ standalone: chạy từ các init level.

Cú pháp:

ServerType <inetd/standalone>

Ví dụ:

ServerType standalone

4.3.2. Thư mục Webroot và một số thông tin cần thiết

Chỉ định **DocumentRoot**: Cấu hình thư mục gốc lưu trữ nội dung của Website. Web Server sẽ lấy những tập tin trong thư mục này phục vụ cho yêu cầu của client.

Cú pháp:

DocumentRoot <đường_dẫn_thư_mục>

Ví dụ:

DocumentRoot /usr/web

Một yêu cầu http://www.soft.com sẽ được đưa vào trang web /usr/web/index.html

ServerRoot: Vị trí cài đặt web server.

Cú pháp:

ServerRoot <vị_trí_thư_mục_cài_đặt_apache>

Mặc định:

ServerRoot /usr/local/apache (trong Linux là /etc/httpd)

Error log: Chỉ ra tập tin để server ghi vào bất kỳ những lỗi nào mà nó gặp phải

Cú pháp:

ErrorLog <vị_trí_tập_tin_log>

Ví dụ:

ErrorLoglogs/error_log

Nếu đường dẫn vị trí không có dấu / thì vị trí tập tin log liên quan đến ServerRoot.

DirectoryIndex: Các tập tin mặc định khi truy cập tên web site.

Cú pháp:

DirectoryIndex <danh_sách_các_tập_tin>

Ví dụ:

DirectoryIndex index.html index.htm index.shtml index.php index.php4 index.php3 index.cgi

4.3.3. Cấu hình mạng

MaxClients: Qui định số yêu cầu tối đa từ các client có thể gởi đồng thời đến server.

Cú pháp:

MaxClients <number>

Ví dụ:

MaxClients 256

Listen: Qui định địa chỉ IP hoặc Cổng mà Apache nhận kết nối từ Client.

Cú pháp:

Listen <Port/IP>

Ví dụ:

Listen 80

BindAddress: Qui định địa chỉ card mạng để chạy Apache trên Server.

Cú pháp:

BindAddress <IP/*>

Sử dụng dấu "*" để có thể sử dụng tất cả các địa chỉ có trên máy.

Ví dụ:

BindAddress172.29.7.225

Mặc định là: BindAddress *

TimeOut: quy định thời gian sống của một kết nối (được tính bằng giây).

Cú pháp:

TimeOut <time>

Ví dụ:

TimeOut 300

KeepAlive: cho phép hoặc không cho phép Client gửi được nhiều yêu cầu dựa trên một kết nối với Web Server.

Cú pháp:

KeepAlive <On/Off>

Ví dụ:

KeepAlive On

MaxKeepAliveRequests: số Request tối đa trên một kết nối (nếu cho phép nhiều Request trên một kết nối).

Cú pháp:

MaxKeepAliveRequests <số Request>

Ví dụ:

MaxKeepAliveRequests

KeepAliveTimeout: qui định thời gian để chờ cho một Request kế tiếp từ cùng một Client trên cùng một kết nối (được tính bằng giây).

Cú pháp:

KeepAliveTimeout <time>

Ví dụ:

KeepAliveTimeout

4.3.4. Alias

Cung cấp cơ chế ánh xạ đường dẫn cục bộ (không nằm trong DocumentRoot) thành đường dẫn địa chỉ URL.

Cú pháp:

Alias <đường_dẫn_http> <đường_dẫn_cục_bộ>

Ví dụ:

Alias /doc   /usr/share/doc

Khi truy cập http://www.soft.com/doc sẽ đưa vào /usr/share/doc

Để giới hạn việc truy cập của người dùng ta có thể kết hợp với Directory directive.

Ví dụ:

```
Alias  /usr/share/doc
<Directory/usr/share/doc>
AuthType Basic
AuthName intranet
AuthUserFile /etc/httpd/passwd
Require userhally tom
Allow from internal.com
</Directory>
```

4.3.5. UserDir

Cho phép người dùng tạo Home page của user trên WebServer

Cấu hình:

```
<IfModule mod_userdir.c>
#UserDir disable
UserDir www; thư mục Web của user.
</IfModule>
<Directory /home/*/www>
…
</Directory>
```

Trong thư mục Home Directory của người dùng tạo thư mục www. Ví dụ /home/nva/www. Khi đó cú pháp truy cập từ Web Browser có dạng: http://www.soft.com/~<tênUser>.

Ví dụ:

http://www.soft.com/~nva.

Khi người dùng cố gắng truy cập đến thư mục của mình có thể gặp một message lỗi “Forbidden”.

Điều này có thể là quyền truy cập đến home directory của người dùng bị giới hạn. Lúc này có thể giới hạn lại quyền truy cập home directory của người dùng với những câu lệnh như sau:

chown jack /home/jack /home/jack/www

chmod 750 /home/jack /home/jack/www

4.3.6. VirtualHost

Là tính năng của Apache giúp ta duy trì nhiều hơn một web server trên một máy tính. Nhiều tên cùng chia xẻ một địa chỉ IP gọi là named-based virtual hosting, và sử dụng những địa chỉ IP khác nhau cho từng domain gọi là IP-based virtual hosting.

4.3.6.1. IP-based Virtual Host

VirtualHost dựa trên IP yêu cầu những server phải có một địa chỉ IP khác nhau cho mỗi virtualhost dựa trên IP. Như vậy, một máy tính phải có nhiều interface hay sử dụng cơ chế virtual interface mà những hệ điều hành sau này hỗ trợ. Nếu máy có một địa chỉ IP: 97.158.253.26, chúng ta có thể cấu hình một địa chỉ IP khác trên cùng một card mạng như sau:

ifconfig eth0:1 97.158.253.27 netmask 255.255.255.0 up

Sau đó ta mô tả thông tin cấu hình trong file httpd.conf

<VirtualHost *> ; VirtualHost default

…

DocumentRoot /tmp

ServerName www.domain

…

</VirtualHost>

<VirtualHost 97.158.253.26> ; VirtualHost cho site1

…

DocumentRoot /home/www/site1

ServerName www1.domain

…

</VirtualHost>

<VirtualHost 97.158.253.27>; VirtualHost cho site2

…

DocumentRoot /home/www/site2

ServerName www2.domain

…

</VirtualHost>

4.3.6.2. Named-based Virtual Hosts:

IP-based Virtual Host dựa vào địa chỉ IP để quyết định Virtual Host nào đúng để truy cập. Vì thế, cần phải có địa chỉ IP khác nhau cho mỗi Virtual Host. Với Named-based Virtual Host, server dựa vào HTTP header của client để biết được hostname. Sử dụng kỹ thuật này, một địa chỉ IP có thể có nhiều tên máy tính khác nhau. Named-based Virtual Host rất đơn giản, chỉ cần cấu hình DNS sao cho nó phân giải mỗi tên máy đúng với một địa chỉ IP và sau đó cấu hình Apache để tổ chức những web server cho những miền khác nhau.

Cấu hình: Tham khảo đoạn cấu hình VirtualHost cho www.hcm.vn và www.tatavietnam.hcm.vn, www.ntc.hcm.vn sử dụng chung một IP 172.29.14.150

NameVirtualHost 172.29.14.150

#Virtualhost mặc định

<VirtualHost *>

ServerAdmin webmaster@dummy-host.example.com

DocumentRoot /tmp

RewriteEngine on

RewriteLogLevel 0

ServerName dummy-host.example.com

ErrorLog logs/dummy-host.example.com-error_log

CustomLog logs/dummy-host.example.com-access_log common

</VirtualHost>

<VirtualHost 172.29.14.150>#Virtualhost cho WebServer chính

ServerAdmin webmaster@dummy-host.example.com

RewriteEngine on

RewriteLogLevel 0

DocumentRoot /var/www/html

ServerName www.hcm.vn

ErrorLog logs/dummy-host.example.com-error_log

CustomLog logs/dummy-host.example.com-access_log common

</VirtualHost>

<VirtualHost 172.29.14.150>#virtualhost cho host Web Server tatavietnam

ServerAdmin webmaster@dummy-host.example.com

DocumentRoot /webdata

RewriteEngine on

RewriteLogLevel 0

ServerName www.tatavietnam.hcm.vn

ErrorLog logs/dummy-host.example.com-error_log

```
        CustomLog logs/dummy-host.example.com-access_log common
    </VirtualHost>
    <VirtualHost 172.29.14.150>#virtualhost cho host  Web Server ntc
        ServerAdmin webmaster@dummy-host.example.com
        DocumentRoot /ntc
        RewriteEngine       on
        RewriteLogLevel     0
        ServerName www.ntc.hcm.vn
        ErrorLog logs/dummy-host.example.com-error_log
        CustomLog logs/dummy-host.example.com-access_log common
    </VirtualHost>
```

Câu hỏi

1. Samba là gì? Cho biết các thành phần cùng chức năng mỗi thành phần.
2. Chức năng của công cụ Samba swat? Trình bày cách cấu hình Samba swat.
3. DNS là gì? DNS hoạt động theo mô hình nào?
4. Trình bày cơ chế phân giải tên thành IP. Cho ví dụ minh họa.
5. Trình bày cơ chế phân giải IP thành tên máy tính. Cho ví dụ minh họa.
6. DHCP là gì? Cho biết các thành phần của DHCP và chức năng của mỗi thành phần.
7. Web Server là gì? Trình bày cách hoạt động của Web Server.

Bài tập thực hành

Bài 1. Cấu hình DHCP server:
Cấu hình máy Linux làm máy chủ DHCP cung cấp địa chỉ IP động cho các máy trạm với:

- scope: 192.168.100.50 – 192.168.100.100
- SM: 255.255.255.0
- GW: 192.168.100.1
- DNS: 192.168.100.10
- Domain: danavtc.edu.vn

Bài 2. Cấu hình dịch vụ samba:

1. Chia xẻ home directory cho người dùng
2. Chia xẻ thư mục dùng chung
3. Chia xẻ máy in cục bộ cho người dùng
4. Truy cập tài nguyên dùng chung
5. Giới hạn truy cập tài nguyên dùng chung
6. mount tài nguyên dùng chung

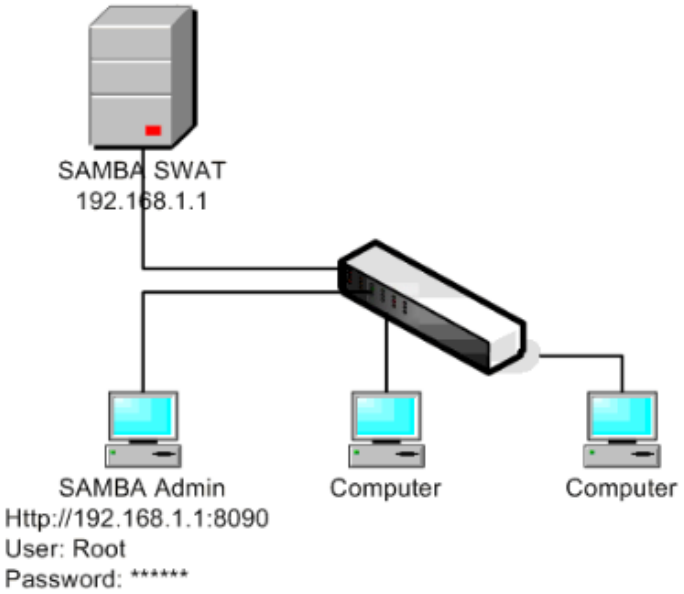
Bài 3. Quản trị SAMBA trên giao diện đồ họa:

Đăng nhập và mode X và thực hiện các yêu cầu sau:

1. User và group:
   hocvien (hv1, hv2, hv3)
   giaovien (gv1, gv2)
   admin (admin1, admin2)
2. Cấu hình samba trên mode X theo yêu cầu sau:
   Chia xẻ home directory cho từng người dùng
   Chia xẻ thư mục /softs với tên share tailieu cho người dùng trong nhóm admin có quyền RW, những người khác có quyền R
3. Truy cập tài nguyên share từ mode X
4. Truy cập tài nguyên share từ Windows để kiểm tra

Bài 4. Quản trị samba swat:

Cho mô hình sau:



Hãy thực hiện các yêu cầu:

1. Cài đặt samba swat
2. Cấu hình samba swat để có thể cấu hình samba qua web với port 8090
3. Chỉ cho phép máy có địa chỉ x.y.z.t được quyền quản lý samba qua web
   Cấu hình share máy in
   Cấu hình share home directory
   Cấu hình share thư mục dùng chung

BÀI 8: QUẢN LÝ MÁY CHỦ LINUX BẰNG WEBMIN

Mã bài: MĐ 40-08

Mục tiêu:
- Biết cài đặt và sử dụng Webmin;
- Sử dụng webmin để quản lý cấu hình hệ thống;
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Giới thiệu

Mục tiêu: Giới thiệu ứng dụng hỗ trợ quản trị hệ thống Linux qua giao diện web

Webmin là ứng dụng Web hỗ trợ cho công tác quản trị hệ thống Unix/Linux qua Web; hầu hết các chương trình ứng dụng của Webmin được Jamie Cameron phát triển. Thông qua Webmin người dùng có thể logon vào hệ thống Unix/Linux để thực hiện các thao tác quản trị hệ thống một cách bình thường. Webmin cho phép người quản trị có thể:

- Tổ chức tài khoản người dùng;
- Tổ chức và cài đặt các dịch vụ như: apache, DNS, Mail,…;
- Cập nhật các thông số cấu hình cho hệ thống;
- Cấu hình mạng;
- Cấu hình hardware;
- Cấu hình Cluster;
- Thực thi lệnh trên SHELL;
- Quản trị hệ thống từ xa qua telnet/ssh;
- Quản lý hệ thống tập tin và thư mục.

2. Cài đặt Webmin

Mục tiêu: Trình bày các thao tác cài đặtcông cụ Webmin.

2.1. Cài đặt từ file nhị phân

Webmin được cung cấp miễn phí tại Website http://www.webmin.com. Ta download package webmin-1.190-1.noarch.rpm. sau đó thực hiện lệnh:

rpm -ivh webmin-1.190-1.noarch.rpm

2.2. Cài đặt từ file nguồn *.tar.gz

```
# tar zxvf webmin-0.87.tar.gz
[root@delilah webmin-1.050]#./setup.sh
…
Web server port (default 10000):
Login name (default admin): root
Login password:
Password again:
The Perl SSLeay library is not installed. SSL not available.
Start Webmin at boot time (y/n): n
```

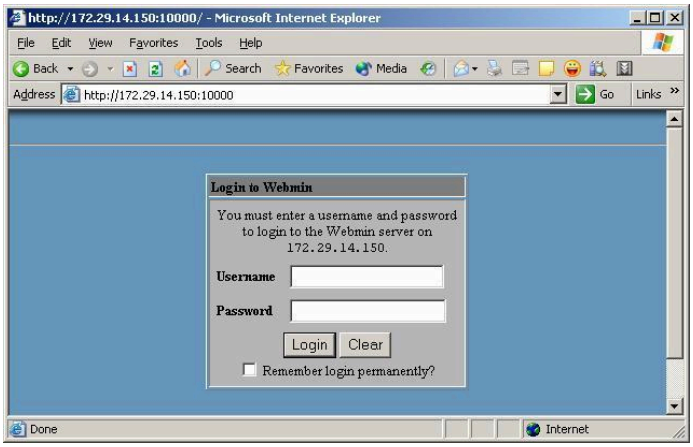
Sau khi cài đặt hoàn tất Webmin ta truy xuất Server theo địa chỉ: http://delilah.swell:10000/

3. Cấu hình Webmin

Mục tiêu: Trình bày các thao tác đăng nhập, cấu hình và quản trị các đối tượng qua ứng dụng webmin.

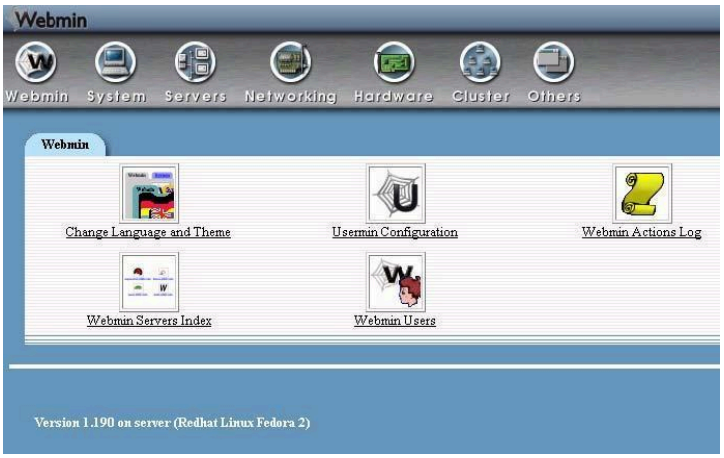
3.1. Đăng nhập Webmin

Sau khi cài xong Webmin ta có thể dùng Web Browser để truy xuất vào Webmin Server thông qua địa chỉ http://server:10000/



Màn hình đăng nhập

Nhập username: root và mật khẩu tương ứng để logon vào hệ thống



Giao diện Webmin

3.2. Cấu hình Webmin

Thay đổi mật khẩu cho Webmin Password bằng dòng lệnh:

#/usr/libexec/webmin/changepass.pl /etc/webmin root 123456

Restart Webmin bằng dòng lệnh:

#/etc/webmin/stop

#/etc/webmin/start

Tìm hiểu file cấu hình Webmin /etc/webmin/miniserv.conf cho phép ta thay đổi một số thông tin cấu hình Webmin Server

#chỉ định port number

port=10000

root=/usr/libexec/webmin

#chỉ định Webmin Type

mimetypes=/usr/libexec/webmin/mime.types

addtype_cgi=internal/cgi

realm=Webmin Server

#chỉ định logfile lưu trữ log cho Webmin

logfile=/var/webmin/miniserv.log

#lưu trữ error log

errorlog=/var/webmin/miniserv.error

#chỉ định pid file

pidfile=/var/webmin/miniserv.pid

logtime=168

ppath=

ssl=1

#khai báo biến môi trường lưu trữ thông tin cấu hình Webmin

env_WEBMIN_CONFIG=/etc/webmin

env_WEBMIN_VAR=/var/webmin

atboot=0

logout=/etc/webmin/logout-flag

#listen port

listen=10000

denyfile=\.pl$

log=1

blockhost_failures=5

blockhost_time=60

syslog=1

session=1

#chỉ file lưu trữ Webmin User

userfile=/etc/webmin/miniserv.users

keyfile=/etc/webmin/miniserv.pem

passwd_file=/etc/shadow

passwd_uindex=0

passwd_pindex=1

passwd_cindex=2

passwd_mindex=4

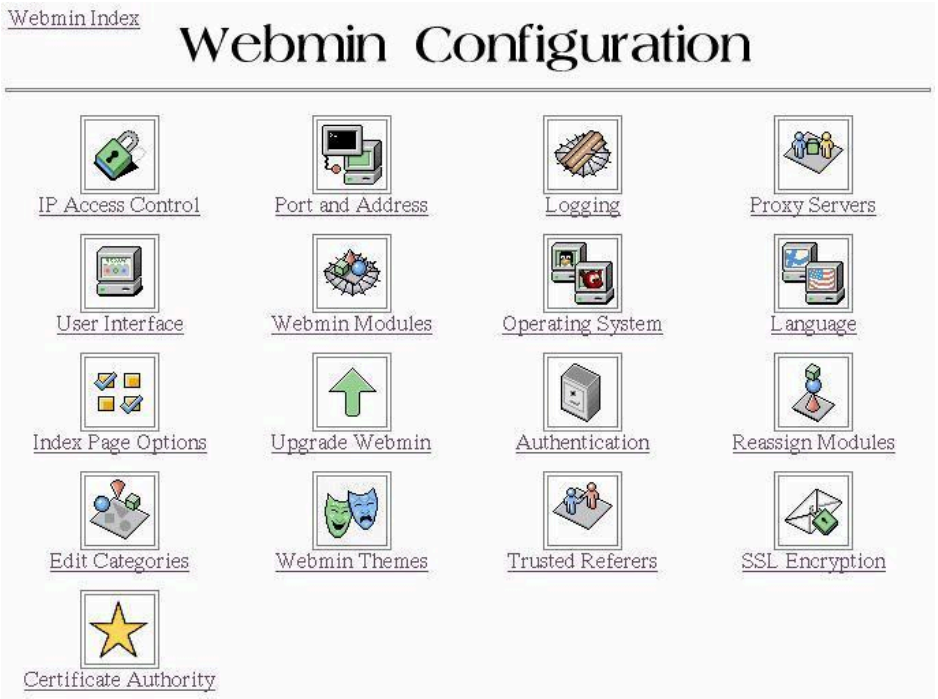
passwd_mode=0

passdelay=1

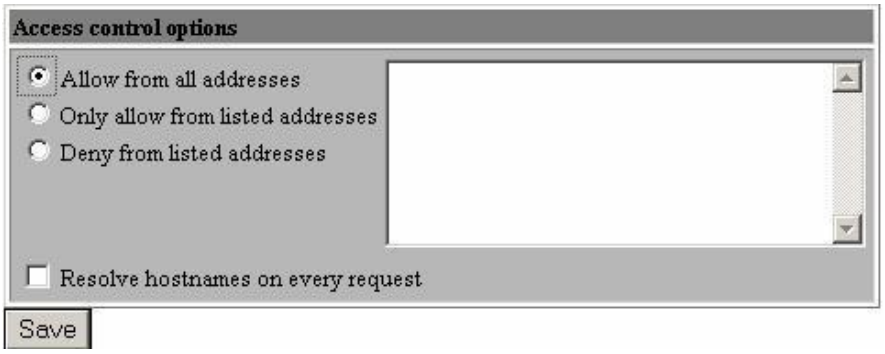
preroot=mscstyle3

3.3. Cấu hình Webmin qua Web Browser

Sau khi đăng nhập vào Webmin Server ta chọn biểu tượng Webmin Configuration



Cho phép hay cấm truy xuất Webmin từ host nào đó trên mạng thông qua IP Access Control.



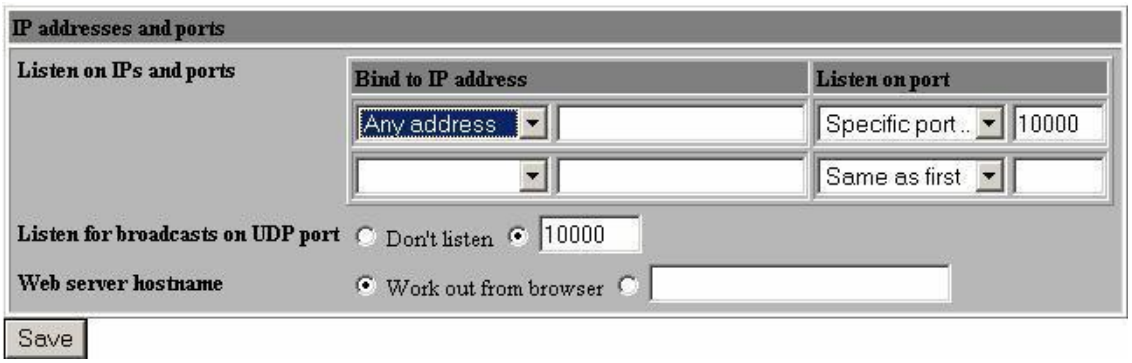
Allow from all addresses: cho phép tất cả các host khác truy xuất Webmin.

Only allow from listed addresses: Chỉ cho phép các host trong ListBox mới được sử dụng Webmin (ta có thể mô tả địa chỉ như sau 172.29.1.0/255.255.255.0 để chỉ định cho network address)

Deny from listed addresses: cho phép tất cả các host khác được truy xuất Webmin nhưng cấm các host nằm trong ListBox.

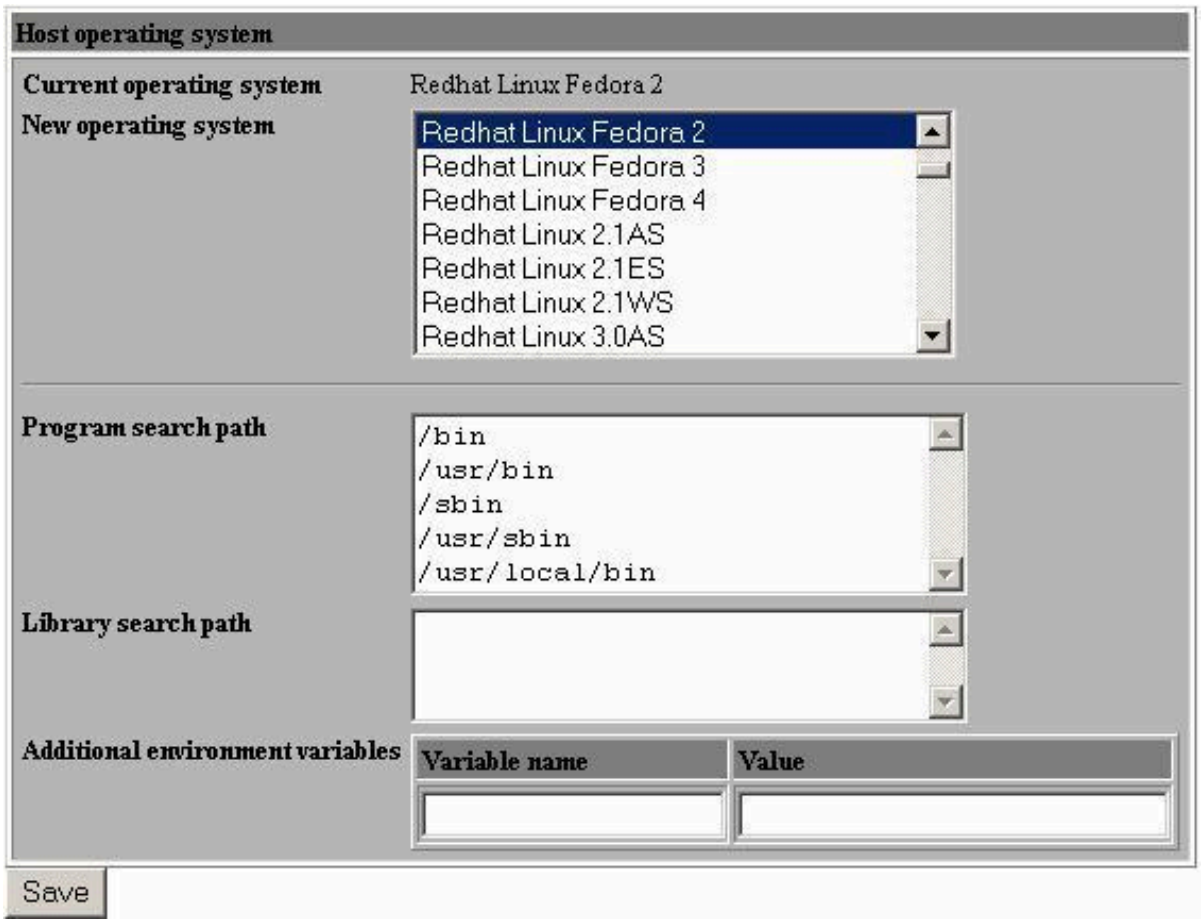
Save: Lưu trữ lại những gì ta thay đổi.

Port and Addresses: Cho phép hiệu chỉnh Webmin hoạt động trên địa chỉ IP và Port, nếu ta muốn Webmin hoạt động trên cổng khác thì ta có thể vào mục này để hiệu chỉnh lại cho phù hợp.

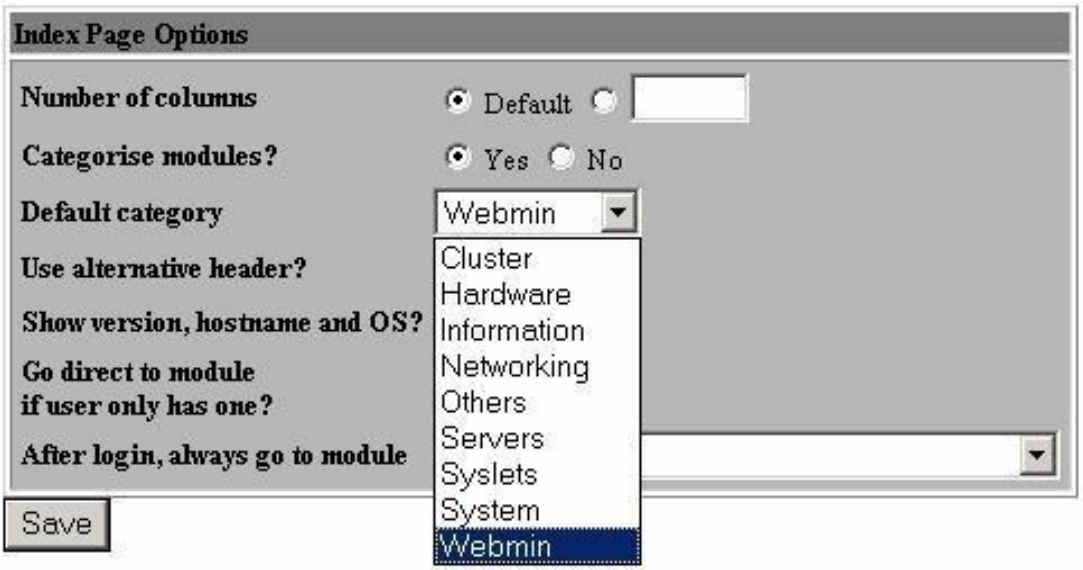


Bind to IP address và **Listen on port** chỉ định Webmin listen 10000 tại địa chỉ IP(mặc định Webmin listen port 10000 trên tất cả các IP của Server)

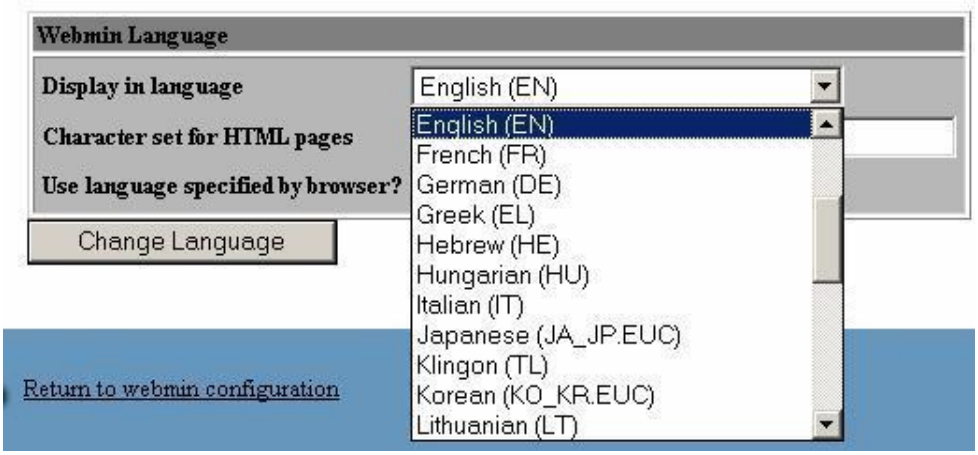
Operating System and Environment: Chỉ định loại hệ điều hành và một số đường dẫn chương trình



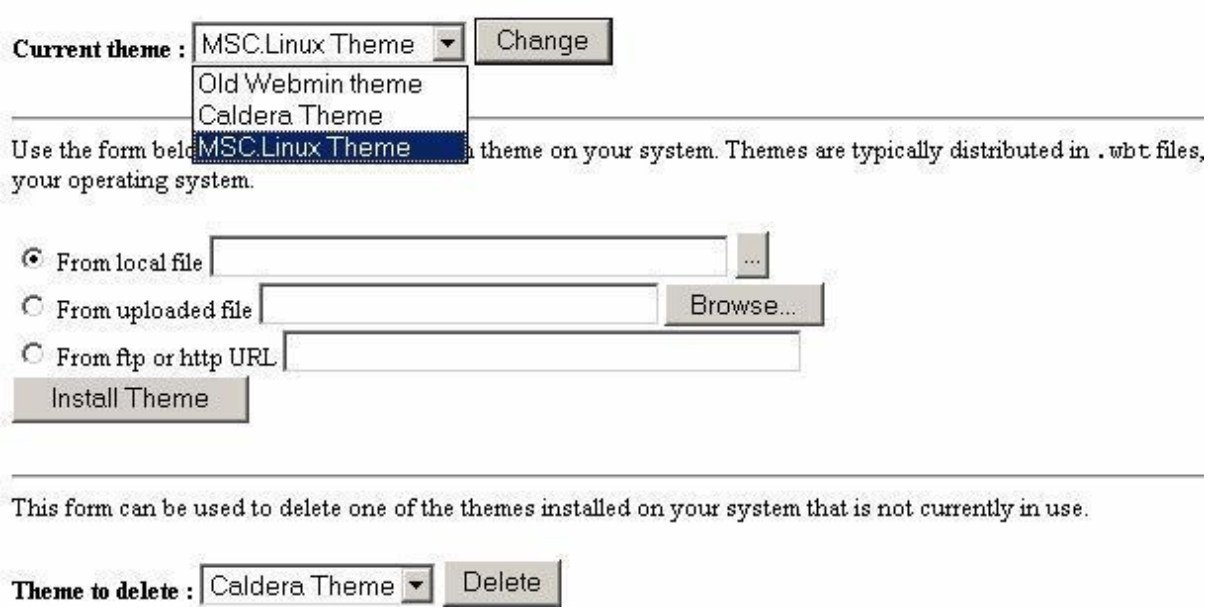
Index Page Options: hiệu chỉnh màn hình chính của thực đơn Webmin



Chọn ngôn ngữ sử dụng cho Webmin



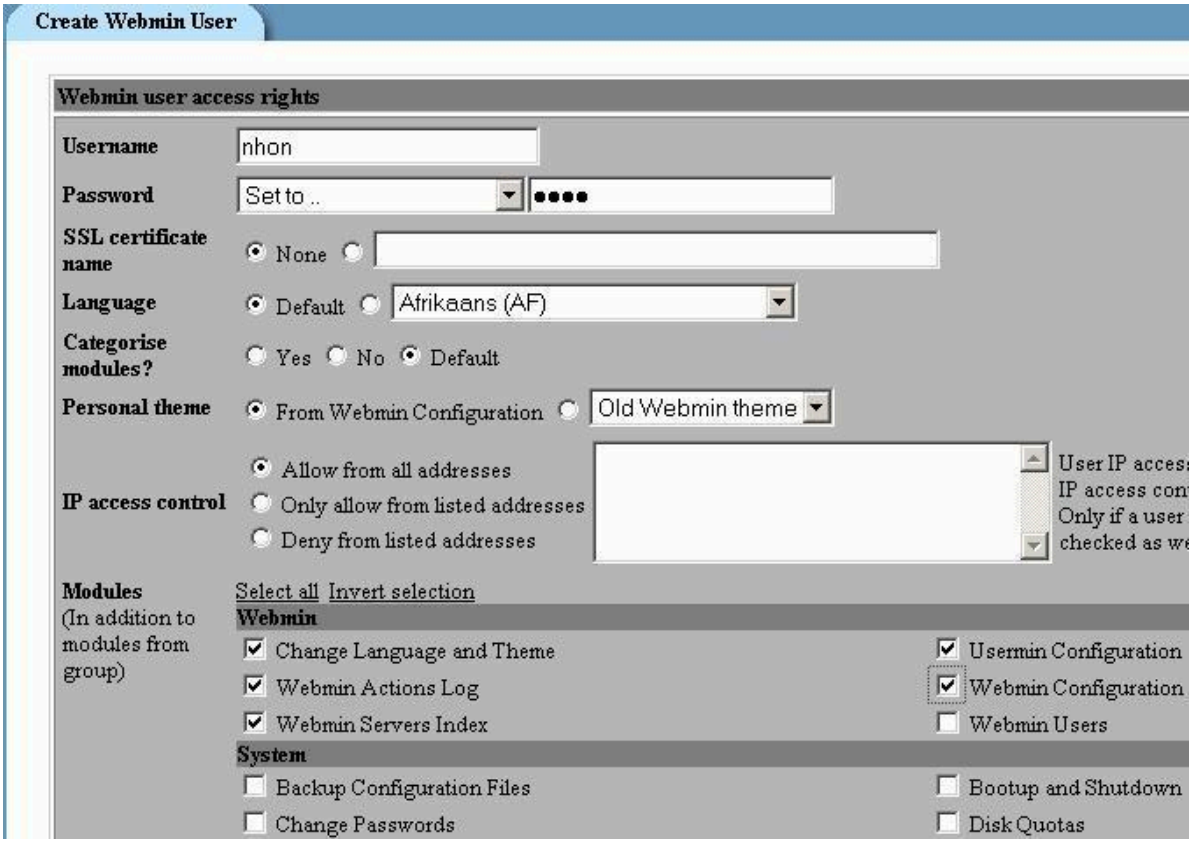
Chọn Webmin Themes để hiệu chỉnh giao diện sử dụng cho Webmin như icons, colours, background, và cách trình bày Web page cho Webmin



3.4. Quản lý Webmin

3.4.1. Quản lý Webmin User

Tạo Webmin User thông qua mục Create a new Webmin user



Ta nhập username, password, và đặt một số quyền hạn cho User…

3.4.2. Webmin cho Users (Usermin)

Với Webmin được sử dụng chủ yếu để quản trị hệ thống. Usermin là một công cụ cung cấp cho user có thể sử dụng hệ thống qua Web: Usermin có thể cung cấp cho user:

- sử dụng mail client qua Web(web-based mail client).
- Quản lý Java file applet.
- Cấu hình SSH configuration và client modules
- GnuPG encryption and decryption.
- Mail forwarding.
- Changing passwords
- Cron jobs
- web-based command shell
- Cài đặt Usermin:
- Cài đặt bằng file nhị phân

Trước khi cài Usermin ta phải cài Authen-PAM Perl module

[root@server openwebmail]# rpm -ivh usermin-1.120-1.noarch.rpm

warning: usermin-1.120-1.noarch.rpm: V3 DSA signature:

NOKEY, key ID 11f63c51

Preparing...

[100%]

Operating system is Redhat Linux Fedora 2

1:usermin

[100%]

Usermin install complete. You can now login to

http://server:20000/

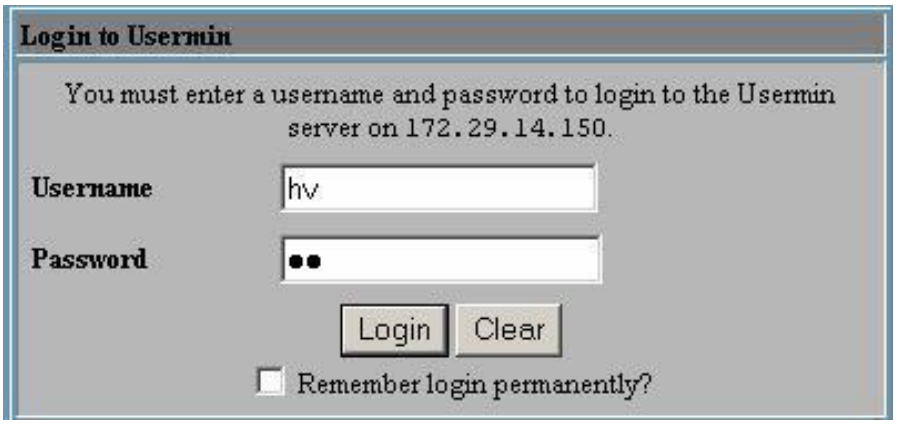
as any user on your system.

Cài đặt Usermin thông qua file .tar.gz

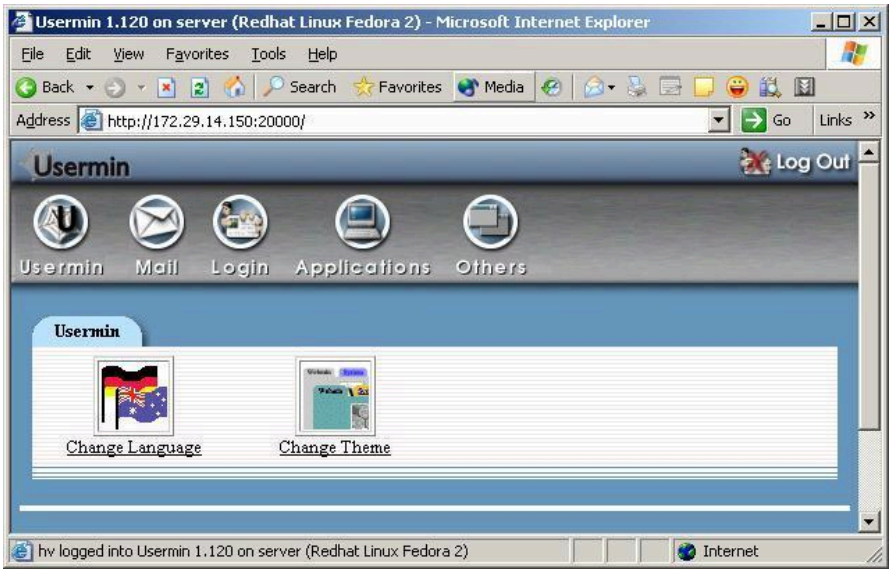
```
# cp usermin-0.6.tar.gz /usr/local

# cd /usr/local

# gunzip usermin-0.6.tar.gz

# tar xf usermin-0.6.tar

# cd usermin-0.6

# ./setup.sh
```

3.4.3. Sử dụng Usermin

Để login vào Usermin Server ta sử dụng địa chỉ http://server:20000/

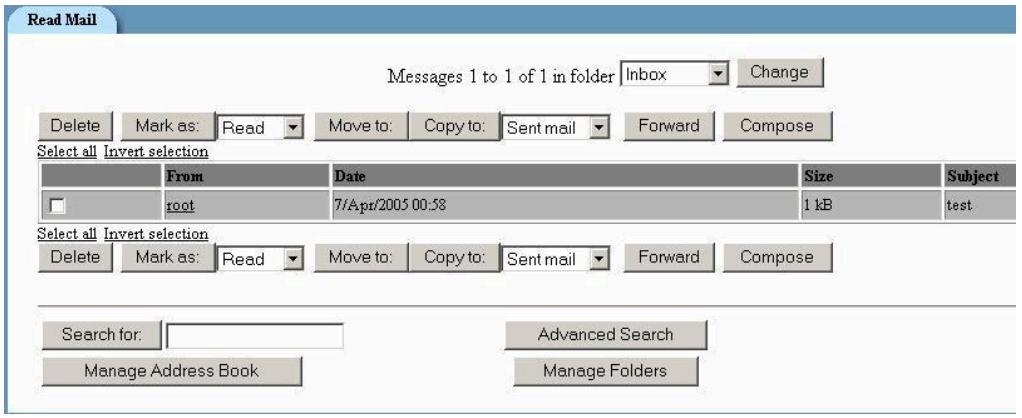


Nhập username và password để login vào hệ thống

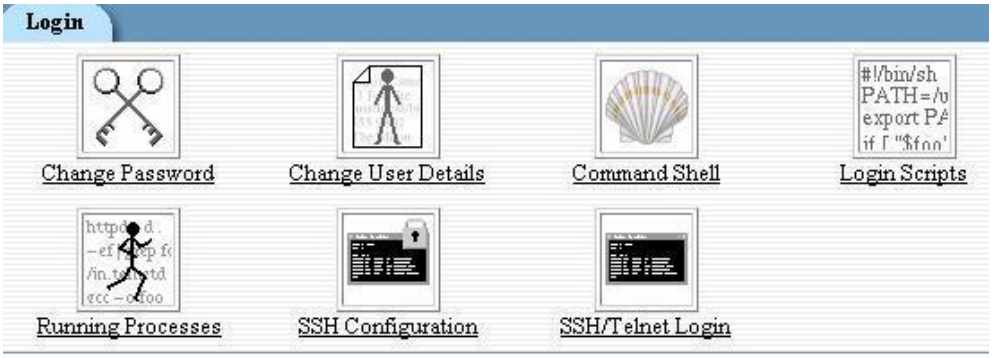


Mail: hỗ trợ các thao tác về việc sử dụng mail cho User

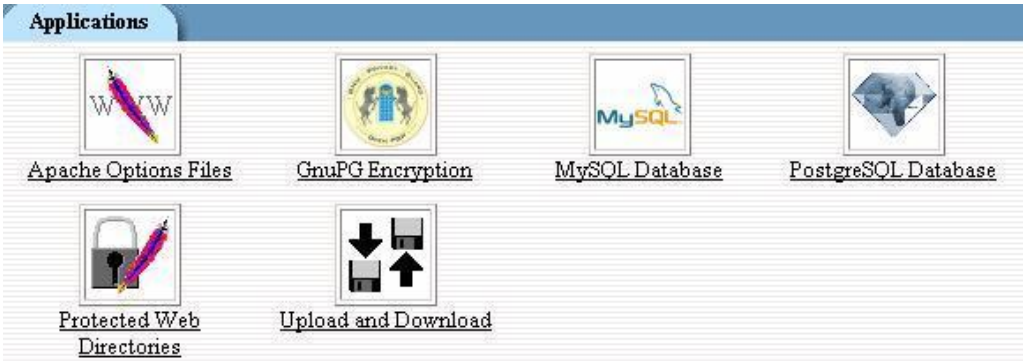
(Sau đây là ví dụ về sử dụng Usermin để đọc mail)



Login: hỗ trợ user có thể sử dụng command shell, logon script…



Application: hỗ trợ cho user sử dụng một số ứng dụng như SQL, upload và download file…



Others: Hỗ trợ cho user có thể xem cấu trúc file, mount file, hiểu chỉnh lệnh

Câu hỏi

1. Webmin là gì? Cho biết các thao tác quản trị thông qua webmin.

Bài tập thực hành

1. Cài đặt và cấu hình webmin.
2. Cài đặt và cấu hình usermin.

PHƯƠNG PHÁP VÀ NỘI DUNG ĐÁNH GIÁ:

- **Về kiến thức:**
  + Trình bày được các khái niệm cơ bản, cấu trúc, chức năng các thành phần trong hệ điều hành Linux
  + Giải thích được các khái niệm cơ bản của hệ điều hành Linux
  + Mô tả được cấu trúc, chức năng của các thành phần trong hệ điều hành Linux
- **Về kỹ năng:**
  + Cài đặt và sử dụng hệ điều hành Linux
  + Thực thi được các thao tác tập tin, thư mục, quản lý người dùng
  + Cài đặt và cấu hình các dịch vụ mạng
  + Tổ chức hệ thống cho phép người sử dụng làm việc từ xa
- **Đánh giá thái độ:**
  + Đánh giá tính tự giác, tính kỷ luật, tham gia đầy đủ thời lượng mô đun, cẩn thận, tỉ mỉ, chính xác trong công việc.

TÀI LIỆU THAM KHẢO

[1]. Phan Vĩnh Thịnh - *Tự học sử dụng Linux,* 2011.

[2]. Trung tâm Tin học, Đại học Khoa học Tự nhiên thành phố Hồ Chí Minh - *Hướng dẫn giảng dạy Quản trị mạng Linux*, 2011.

[3]. Trường Đại học công nghệ, Đại học quốc gia Hà Nội - *Giáo trình hệ điều hành Unix – Linux*, 2004.

[4]. VSIC Education Corp - *Tài liệu Linux Fundamentals & Lan management.*