

==== oOo ====



BÁO CÁO ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC

Tên Đề Tài:

**Tìm Hiểu Và Triển Khai Các Dịch Vụ
Mạng Trên Hệ Điều Hành CentOS 6.5**

Giáo viên hướng dẫn: **ThS.Trương Trăng Cấn**

Sinh viên thực hiện : **L^a Thị Hoàng**

Lớp : **51K -CNTT**

NGHỆ AN 12/ 2014

LỜI CẢM ƠN

Tôi xin được gửi lời cảm ơn trân trọng và sâu sắc nhất tới giáo viên hướng dẫn **Thầy Trương Trọng Cần** – người đã tận tình chỉ bảo, hướng dẫn và truyền đạt kiến thức cho tôi trong quá trình thực hiện đề tài này.

Trong quá trình học tập và nghiên cứu đề tài, tôi xin với sự giúp đỡ tận tình của các giảng viên trong khoa và các bạn. Mặc dù tôi đã cố gắng tìm hiểu và khảo sát thực tế ở trường **Đại Học Vinh** cũng như tham khảo rất nhiều nguồn trên mạng nhưng do khả năng và kinh nghiệm còn hạn hẹp nên không tránh khỏi những thiếu sót. Tôi rất mong nhận được sự đóng góp ý kiến của thầy cô và các bạn để đề tài được hoàn thiện hơn!

Tôi xin chân thành cảm ơn!

Nghệ An, ngày 19 tháng 12 năm 2014

SV thực hiện

Lê Thái Hoàng

MỤC LỤC

LỜI CẢM ƠN.....	2
DANH MỤC CÁC TỪ VIẾT TẮT	4
LỜI MỞ ĐẦU.....	5
CHƯƠNG I: CƠ SỞ LÝ THUYẾT	6
1.1. Tổng quan về hệ điều hành Linux	6
1.1.1 Lịch sử phát triển của Linux.....	6
1.1.2. Ưu – nhược điểm của hệ điều hành Linux	6
1.1.3. Một số bản phân phối linux hiện nay	9
1.2. Một số dịch vụ mạng trên Linux.....	12
1.2.1. Dịch vụ DNS	12
1.2.2. Dịch vụ DHCP.....	17
1.2.3. Dịch vụ SAMBA	19
1.2.4 . Dịch vụ FTP	27
1.2.5. Dịch vụ Webserver	33
1.2.6. Dịch vụ LDAP	36
CHƯƠNG II: TRIỂN KHAI HỆ THỐNG MẠNG TRÊN HỆ ĐIỀU HÀNH CENTOS 6.5	42
2.1. Giới thiệu về đơn vị	42
2.2. Tiếp cận đơn vị	42
2.3. Ưu – nhược điểm của hệ thống cũ Windows.....	42
2.4. Phân tích các yêu cầu từ phía đơn vị và chọn cách cài đặt cho hệ thống.	42
2.4.1. Yêu cầu từ phía đơn vị	42
2.4.2. Yêu cầu về thiết kế	43
2.5. Triển khai hệ thống mạng trên hệ điều hành Linux cho công ty Thái Hoàng ...	43
2.5.1. Mô hình triển khai hệ thống mạng trên hệ điều hành CentOS 6.5.....	43
2.5.2. Cài đặt và cấu hình cho hệ thống	44
KẾT LUẬN	53
TÀI LIỆU THAM KHẢO	54

DANH MỤC CÁC TỪ VIẾT TẮT

HĐH	Hệ điều hành
UNIX	Unix-like Operating System
CNTT	Công nghệ Thông tin
RHEL	Red Hat Enterprise
DNS	Domain name system
DHCP	Dynamic Host Configuration Protocol
CSDL	Cơ sở dữ liệu
LDAP	Lightweight Directory Access Protocol
FTP	File Transfer Protocol
SMB	Server Message Block
ACK	Acknowledgement

LỜI MỞ ĐẦU

I. LÝ DO CHỌN ĐỀ TÀI

Hiện nay, công nghệ thông tin đang có vai trò cực kỳ quan trọng không thể thiếu trong quá trình quản lý, điều hành các hoạt động sản xuất kinh doanh của mỗi doanh nghiệp. Do vậy, việc xây dựng được một hệ thống mạng với đầy đủ các dịch vụ cần thiết phục vụ kinh doanh là điều rất cần thiết.

Ngoài các yếu tố phần cứng và nguồn nhân lực quản trị thì yếu tố phần mềm cũng đóng vai trò rất quan trọng khi xây dựng một hệ thống mạng. Nói đến phần mềm một vấn đề lớn ở nước ta là bản quyền, chi phí mua bản quyền các dịch vụ để hoàn tất một hệ thống mạng là rất lớn. Để tiết kiệm một khoản chi phí lớn, người ta dần chuyển sang các sản phẩm dịch vụ từ mã nguồn mở. Ngoài việc chạy ổn định, ít bị tấn công, có một cộng đồng phát triển rất lớn thì ưu điểm lớn nhất và đáng quan tâm nhất của mã nguồn mở đó là không tốn phí. Vì những lý do trên, em đã thực hiện đề tài này.

II. Ý NGHĨA CỦA ĐỀ TÀI

- Xây dựng kiến thức liên quan đến trong ngành mạng máy tính, có thêm những hiểu biết về hệ điều hành mã nguồn mở Linux.
- Xây dựng bản demo triển khai thành công một số dịch vụ mạng trên Linux.

III. ĐỐI TƯỢNG VÀ PHƯƠNG PHÁP NGHIÊN CỨU:

- Tìm hiểu về hệ điều hành mã nguồn mở Linux.
- Tìm hiểu về bản phân phối CentOS 6.5 của Linux
- Tìm hiểu về một số dịch vụ mạng trên Linux.
- Khảo sát hệ thống mạng của công ty.
- Cài đặt một số dịch vụ và chạy thử nghiệm.

IV. MỤC TIÊU CỦA ĐỀ TÀI:

- Tìm hiểu và sử dụng tốt hệ điều hành mã nguồn mở Linux.
- Tìm hiểu, phân tích các hệ thống mạng trên Linux.
- Tìm hiểu và nghiên cứu các vấn đề liên quan đến các dịch vụ mạng trên Linux.
- Từ đó đưa ra phương pháp triển khai cài đặt cho hệ thống mạng của công ty.
- Rút ra được một nhận định và hướng phát triển cho đề tài.

CHƯƠNG I: CƠ SỞ LÝ THUYẾT

1.1. Tổng quan về hệ điều hành Linux

1.1.1 Lịch sử phát triển của Linux

Linux là một HĐH dạng UNIX (Unix-like Operating System) chạy trên máy PC với bộ điều khiển trung tâm (CPU) Intel 80386 trở lên, hay các bộ vi xử lý trung tâm tương thích AMD, Cyrix. Linux ngày nay còn có thể chạy trên các máy Macintosh hoặc SUN Sparc.

Linux được viết lại toàn bộ từ con số không, tức là không sử dụng một dòng lệnh nào của Unix để tránh vấn đề bản quyền của Unix. Tuy nhiên hoạt động của Linux hoàn toàn dựa trên nguyên tắc của hệ điều hành Unix. Vì vậy nếu một người nắm được Linux, thì sẽ nắm được UNIX. Giữa các hệ thống Unix sự khác nhau cũng không kém gì giữa Unix và Linux.

Năm 1991 Linus Torvalds, sinh viên của đại học tổng hợp Helsinki, Phần lan, bắt đầu xem xét Minix, một phiên bản của Unix làm ra với mục đích nghiên cứu cách tạo ra một hệ điều hành Unix chạy trên máy PC với bộ vi xử lý Intel 80386.

Ngày 25/8/1991, Linus cho ra version 0.01 và thông báo trên comp.os.minix của Internet về dự định của mình về Linux.

Tháng 01/1992, Linus cho ra version 0.12 với shell và C compiler. Linus không cần Minix nữa để recompile HDH của mình. Linus đặt tên HDH của mình là Linux. Năm 1994, phiên bản chính thức 1.0 được phát hành.

Quá trình phát triển của Linux được tăng tốc bởi sự giúp đỡ của chương trình GNU (GNU Is Not Unix), đó là chương trình phát triển các Unix có khả năng chạy trên nhiều platform. Phiên bản mới nhất của Linux kernel là 2.6.25, có khả năng điều khiển các máy đa bộ vi xử lý (hiện tại Linux hỗ trợ máy tính có tối đa 16 CPUs). Linux kernel 2.6.25 cũng đồng thời nâng cấp hệ thống file Ext4 (phiên bản cũ là Ext3), giúp hỗ trợ dung lượng block lớn hơn - từ 4K lên 64K và rất nhiều các tính năng khác (có thể download tại : <http://www.kernel.org>).

1.1.2. Ưu – nhược điểm của hệ điều hành Linux

1.1.2.1. Ưu điểm

Hệ điều hành linux có rất nhiều ưu điểm khác mà không một hệ điều hành nào có. Chính những đặc điểm này mới là nguyên nhân khiến cho Linux ngày càng trở nên

phổ biến không chỉ ở Việt Nam mà cả ở trên thế giới.

- Linh hoạt

Linux là một Hệ điều hành mã nguồn mở nên chúng ta có thể tùy ý sửa chữa theo như mình thích (tất nhiên là trong khả năng kiến thức của mỗi người). Chúng ta có thể chỉnh sửa Linux và các ứng dụng trên đó sao cho phù hợp với mình nhất. Mặt khác do Linux được một cộng đồng rất lớn những người làm phần mềm cùng phát triển trên các môi trường, hoàn cảnh khác nhau nên tìm một phiên bản phù hợp với yêu cầu của mỗi người sẽ không phải là một vấn đề quá khó khăn.

Tính linh hoạt của Linux còn được thể hiện ở chỗ nó tương thích được với rất nhiều môi trường. Hiện tại, ngoài Linux dành cho server, PC...nhân Linux còn được nhúng vào các thiết bị điều khiển như máy tính palm, robot...Phạm vi ứng dụng của Linux được xem là rất rộng rãi.

- Độ an toàn cao

Trước hết, trong Linux có một cơ cấu phân quyền hết sức rõ ràng. Chỉ có "root" (người dùng tối cao) mới có quyền cài đặt và thay đổi hệ thống. Ngoài ra Linux cũng có cơ chế để một người dùng bình thường có thể tạm thời chuyển sang quyền "root" để thực hiện một số thao tác. Điều này giúp cho hệ thống có thể chạy ổn định và tránh phải những sai sót dẫn đến đổ vỡ hệ thống (trong những phiên bản Windows gần đây, cơ chế phân quyền này cũng đã bước đầu được áp dụng, nhưng so với Linux thì vẫn kém chặt chẽ hơn).

Ngoài ra chính tính chất "mở" cũng tạo nên sự an toàn của Linux. Nếu như một lỗ hổng nào đó trên Linux được phát hiện thì nó sẽ được cả cộng đồng mã nguồn mở cùng sửa và thường thì chỉ sau 24h sẽ có thể cho ra bản sửa lỗi. Mặt khác đối với những Hệ điều hành mã nguồn đóng như Windows, chúng ta không thể biết được người ta viết gì, và viết ra sao mà chỉ biết được chúng chạy như thế nào. Vì vậy nếu như Windows có chứa những đoạn mã cho phép tạo những "back door" để xâm nhập vào hệ thống của chúng ta thì chúng ta cũng không thể biết được. Đối với người dùng bình thường như chúng ta vấn đề này có vẻ như không quan trọng nhưng đối với một hệ thống tầm cỡ như hệ thống quốc phòng thì vấn đề như thế này lại mang tính sống còn. Các nhân viên an ninh không được phép để lộ một kẽ hở nào, dù là nhỏ nhất vì nó liên quan đến an ninh của cả một quốc gia. Và một lần nữa các phần mềm mã

nguồn mở nói chung và Linux nói riêng lại là sự lựa chọn số 1. Trong Linux mọi thứ đều công khai, người quản trị có thể tìm hiểu tới mọi ngõ ngách của hệ điều hành. Điều đó cũng có nghĩa là độ an toàn được nâng cao.

- Thích hợp cho quản trị mạng

Được thiết kế ngay từ đầu cho chế độ đa người dùng, Linux được xem là một hệ điều hành mạng rất giá trị. Nếu như Windows tỏ ra là một Hệ điều hành thích hợp với máy tính Desktop thì Linux lại là hệ điều hành thống trị đối với các Server. Đó là do Linux có rất nhiều ưu điểm thỏa mãn đòi hỏi của một hệ điều hành mạng: tính bảo mật cao, chạy ổn định, các cơ chế chia sẻ tài nguyên tốt.....Giao thức TCP/IP mà chúng ta vẫn thấy ngày nay chính là một giao thức truyền tin của Linux (sau này mới được đưa vào Windows).

- Chạy thống nhất trên các hệ thống phần cứng

Dù cho có rất nhiều phiên bản Linux được các nhà phân phối khác nhau ban hành nhưng nhìn chung đều chạy khá ổn định trên mọi thiết bị phần cứng, từ Intel 486 đến những máy Core 2 Duo, từ những máy có dung lượng RAM chỉ 4MB đến

những máy có cấu hình cực mạnh (tất nhiên là tốc độ sẽ khác nhau nhưng về nguyên tắc vẫn có thể chạy được). Nguyên nhân là Linux được rất nhiều lập trình viên ở nhiều môi trường khác nhau cùng phát triển (không như Windows chỉ do Microsoft phát triển) và chúng ta sẽ bắt gặp nhiều người có "cùng cảnh ngộ" như mình và dễ dàng tìm được các driver tương ứng với thiết bị của mình. Tính chất này hoàn toàn trái ngược với Windows. Mỗi khi có một phiên bản Windows mới ra đời thì bao giờ kèm theo đó cũng là một cơn khát về phần cứng vì hệ điều hành mới thường không hỗ trợ các thiết bị quá cũ.

1.1.2.2. Nhược điểm

Dù cho hiện nay Linux đang có tốc độ phát triển nhanh hơn hẳn Windows nhưng khách quan mà nói so với Windows, Linux vẫn chưa thể đến với người sử dụng cuối. Đó là do Linux vẫn còn có những nhược điểm cố hữu:

- Đòi hỏi người dùng phải thành thạo

Trước kia việc sử dụng và cấu hình Linux được xem là một công việc chỉ dành cho những kỹ thuật viên CNTT. Hầu như mọi công việc đều thực hiện trên các dòng lệnh và phải cấu hình nhờ sửa trực tiếp các file. Mặc dù trong những phiên bản gần đây,

các Hệ điều hành Linux đã có những cải tiến đáng kể, nhưng so với Windows tính thân thiện của Linux vẫn còn là một vấn đề lớn. Đây là một trong những nguyên nhân chủ yếu khiến Linux mặc dù có rất nhiều đặc tính kỹ thuật tốt nhưng vẫn chưa đến được với người dùng cuối.

- ***Tính tiêu chuẩn hóa***

Linux được phát hành miễn phí nên bất cứ ai cũng có thể tự mình đóng gói, phân phối theo những cách riêng. Hiện tại có khá nhiều bản Linux phát triển từ một nhân ban đầu cùng tồn tại như: RedHat, SuSE, Knoppix..... Người dùng phải tự so sánh xem bản nào là phù hợp với mình. Điều này có thể gây khó khăn cho người dùng, nhất là những người còn có kiến thức về tin học hạn chế.

- ***Số lượng các ứng dụng chất lượng cao trên Linux còn hạn chế***

Mặc dù Windows có sản phẩm nào thì Linux cũng gần như có phần mềm tương tự, (VD: OpenOffice trên Linux tương tự như MSOffice, hay GIMP tương tự như Photoshop...). Tuy nhiên chất lượng những sản phẩm này là chưa thể so sánh được với các sản phẩm viết cho Windows.

- ***Phân cứng***

Một số nhà sản xuất phần cứng không có driver hỗ trợ Linux: Do hiện nay Linux chưa phổ biến bằng Windows nên nhiều nhà sản xuất không hỗ trợ các driver chạy trên Linux. Tuy nhiên chúng ta vẫn có thể tìm thấy các driver này trên internet do cộng đồng mã nguồn mở viết.

Trên cơ sở nhìn nhận một cách khách quan các ưu, nhược điểm của Hệ điều hành Linux cũng như xem xét xu hướng phát triển tin học ở nước ta có thể thấy, Đối với người dùng thông thường việc chuyển từ Windows sang Linux trong ngày một ngày hai là chưa thể. Tuy nhiên đối với những người làm tin học, đặc biệt là đối với sinh viên, việc tìm hiểu và nghiên cứu Linux và phần mềm mã nguồn mở là một điều kiện rất tốt để nâng cao hiểu biết của mình. Linux dẫu sao vẫn là một hệ điều hành rất có giá trị: chi phí thấp, linh hoạt, ổn định, và bảo mật cao.

1.1.3. Một số bản phân phối linux hiện nay

- **Ubuntu**

Không có gì phải ngạc nhiên khi Ubuntu là bản phân phối Linux phổ biến nhất. Với hơn 2.200 lượt xem mỗi ngày trên distrowatch.com, vượt xa con số 1.400 lượt

của Fedora, bản phân phối được xếp ở vị trí thứ hai.

Ubuntu là một đứa con sinh sau đẻ muộn của họ hàng Linux, bản phát hành đầu tiên của Ubuntu là vào 20/10/2004, nhưng sự phát triển vượt bậc đã đưa nó đến vị trí hàng đầu kể từ năm 2007. Được thành lập bởi tỉ phú người Nam Phi Mark Shuttleworth, Canonical, công ty phát hành Ubuntu, nhiều năm qua đã vận chuyển CD Ubuntu tới tận tay người dùng quan tâm đến hệ điều hành mã nguồn mở này trên toàn thế giới. Việc làm đó đã thúc đẩy nhanh chóng sự phổ biến của Ubuntu. Ubuntu dựa trên Debian và bao gồm các ứng dụng nổi tiếng như Firefox và OpenOffice.org. Ubuntu được phát hành đều đặn 6 tháng một lần, với phiên bản hỗ trợ lâu dài (LTS) sẽ được hỗ trợ và cập nhật trong 3 đến 5 năm.

Ubuntu cũng có các biến thể riêng của mình nhằm vào các mục tiêu khác nhau. Kubuntu và Xubuntu, sử dụng KDE và Xfce như là môi trường desktop thay cho hệ thống GNOME mặc định được sử dụng bởi Ubuntu; Edubuntu, một dự án con và là phần bổ sung cho Ubuntu, được thiết kế cho môi trường học tập và sử dụng ở nhà; Ubuntu JeOS (phát âm "ju:s"), một phiên bản khác của Ubuntu, thiết kế cho các máy ảo. Có thể cài Ubuntu ngay trên Windows thông qua Wubi.

- Fedora

Fedora là một phiên bản miễn phí của Red Hat trong khi Red Hat Enterprise Linux (RHEL) đã trở thành phiên bản thương mại kể từ năm 2003. Do quan hệ khăng khít này, Fedora đặc biệt mạnh về các tính năng dành cho doanh nghiệp, và thường được cung cấp trước mỗi phiên bản mới của RHEL. Fedora cũng có chu kì phát hành 6 tháng một lần với các tính năng bảo mật tuyệt vời. Các cải tiến trong những năm qua và sự phổ biến ngày càng tăng làm cho Fedora trở thành một sự lựa chọn tốt cho người dùng.

- Linux Mint

Đây cũng là một bản phân phối non trẻ khác của Linux, Linux Mint mới chỉ được phát hành từ năm 2006.

Linux Mint dựa trên bản phân phối Ubuntu, thêm vào các chủ đề riêng, các bộ ứng dụng độc đáo và đặc biệt mạnh về đồ họa. Nó sử dụng môi trường desktop mintDesktop, mintInstall để thuận tiện trong cài đặt ứng dụng và mintMenu giúp điều hướng dễ dàng.

Mint nổi tiếng dễ dùng, thích hợp cho người mới bắt đầu sử dụng Linux. Nó cũng

bao gồm một số codec đa phương tiện độc quyền, thường vắng mặt trong các phân phối lớn hơn, do đó nâng cao khả năng tương thích phần cứng. Linux Mint không có một lịch trình phát hành cố định, nhưng thường là một phiên bản mới sẽ có mặt ngay sau mỗi bản phát hành ổn định của Ubuntu.

- OpenSUSE

Bản phân phối này giữ vị trí cao trên Distrowatch, đồng thời là nền tảng cho Novell SUSE Linux Enterprise Desktop và SUSE Linux Enterprise Server.

Gói tiện ích quản lý YaST của openSUSE được đánh giá là một trong những công cụ tốt nhất. Phiên bản đóng gói của bản phân phối này đi kèm với các tài liệu in hữu ích mà bạn không thể tìm thấy ở bất kỳ bản Linux nào khác. openSUSE cũng được đánh giá có độ khó dùng ở mức trung bình.

- PCLinuxOS

Thay vì GNOME, PCLinuxOS sử dụng KDE làm môi trường desktop. Về cơ bản, PCLinuxOS là một phiên bản gọn nhẹ của Mandriva. Bản phân phối này hỗ trợ tốt các trình điều khiển đồ họa, bổ sung trình duyệt và các code đa phương tiện.

PCLinuxOS có thể là một sự lựa chọn tốt cho người tập làm quen với Linux. Chu kỳ phát hành của bản phân phối này không ổn định và cũng không có phiên bản dành cho hệ thống 64 bit.

- Puppy Linux

Dù là một bản phân phối khá nhỏ, nhưng Puppy Linux dành được nhiều sự quan tâm của người sử dụng. Chính sự nhỏ gọn lại lí tưởng cho các phần cứng cũ và tài nguyên nghèo nàn. Trong điều kiện như vậy, Puppy vẫn đầy đủ các tính năng, bao gồm nhiều cấu hình và các trình thuật sĩ cài đặt ứng dụng. Toàn bộ hệ điều hành đủ nhỏ để chạy trực tiếp từ bộ nhớ RAM của hệ thống, do đó, các ứng dụng khởi động một cách nhanh chóng và đáp ứng ngay lập tức.

- CentOS

CentOS là một bản phân phối hệ điều hành tự do dựa trên Linux kernel. Nó có nguồn gốc hoàn toàn từ bản phân phối Red Hat Enterprise Linux (RHEL). CentOS tồn tại để cung cấp một nền tảng điện toán doanh nghiệp tự do và phần đầu để duy trì khả năng tương thích nhị phân 100% với nguồn thượng nguồn của nó, Red Hat. CentOS là viết tắt của Community Enterprise Operating System.

Trong tháng 7/2010 CentOS đã vượt qua Debian trở thành bản phân phối Linux phổ biến nhất cho máy chủ web, với gần 30% của tất cả máy chủ web Linux sử dụng nó. Tuy nhiên vào tháng 1/2012, sau một cuộc đua đối đầu, nó bị mất vị trí dẫn đầu vào tay Debian.

1.2. Một số dịch vụ mạng trên Linux

1.2.1. Dịch vụ DNS

1.2.1.1. Giới thiệu về dịch vụ DNS

Mỗi máy tính trên mạng muốn trao đổi thông tin với nhau thì cần phải biết rõ địa chỉ IP của nhau.

Mỗi máy tính ngoài địa chỉ IP còn có một tên (HOSTNAME). Để liên lạc thì việc ghi nhớ địa chỉ IP của nhau là việc rất khó khăn, đặc biệt là việc địa chỉ IPV4 càng ngày càng không thể cung cấp đủ số lượng nhu cầu thì việc chuyển sang dùng IPV6 là điều tất yếu và việc phải nhớ một dãy số hexa 32 số là việc không tưởng.

Do những khó khăn trên người ta đã nghĩ ra việc làm sao để ánh xạ địa chỉ ip của mỗi máy thành hostname của nó và ngược lại. Để khi trao đổi với nhau người ta chỉ cần nhớ tên ban đầu của máy tính bên kia. Ban đầu do quy mô mạng ARPA NET (tiền thân của mạng internet) còn nhỏ, nên chỉ có một tập tin HOST.TXT lưu thông tin và ánh xạ tên máy thành địa chỉ Ip. Trong đó, tên máy chỉ là chuỗi văn bản không phân cấp (plat name). Tập tin này được duy trì tại một máy chủ và các máy chủ khác lưu giữ bản sao của nó. Tuy nhiên khi mô hình mạng lớn hơn, việc sử dụng tập tin HOST.TXT có các nhược điểm sau:

- Lưu lượng mạng và máy chủ duy trì tập tin HOST.TXT bị quá tải.
- Xung đột tên: do tên máy không phân cấp và không có cơ quan quản lý tập tin nên có nguy cơ bị xung đột tên.
- Không đảm bảo sự toàn vẹn: việc duy trì tập tin trên một mạng lớn rất khó khăn. Ví dụ: khi tập tin HOST.TXT vừa cập nhật chưa kịp chuyển đến máy chủ ở xa thì đã có sự thay đổi địa chỉ trên mạng rồi.
- Tóm lại, việc sử dụng tập tin HOST.TXT không phù hợp cho mạng lớn vì thiếu cơ chế phân tán và mở rộng. Do đó dịch vụ DNS ra đời nhằm khắc phục các nhược điểm này.

1.2.1.2. Hệ thống tên miền DNS

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

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

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

Nguyên tắc làm việc của DNS:

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

1.2.1.3. Hoạt động của DNS server trong Linux

Phân loại DNS server

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

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

DNS server quản lý và trả lời yêu cầu này từ Client liên quan đến DNS server này. Hệ thống tên miền cho phép phân chia tên miền để quản lý và chia hệ thống tên miền

thành Zone và trong Zone quản lý tên miền được phân chia đó. Zone file lưu thông tin Zone ở dạng text hoặc trong Active Directory.

Zone thuận và Zone nghịch:

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

Các loại truy vấn:

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

Các file cấu hình chính:

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

- MX (Mail Exchange): chuyển mail trên mạng Internet.
- A (Address): ánh xạ tên máy (hostname) vào địa chỉ IP
- CNAME (canonical name): tên bí danh của server.
- PTR: dùng để ánh xạ địa chỉ IP thành hostname.

1.2.1.4. Cài đặt và cấu hình dịch vụ DNS server

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

+ Cài từ gói rpm: `rpm -ivh bind-9.8.2-0.17.rc1.el6_4.6.x86_64.rpm`, nếu có internet thì cài bằng lệnh yum `yum -y install bind*`

+ Cài từ source: mount thư mục chứa gói cài đặt DNS vào máy chủ centos:

`#mount /dev/cdrom /media`

- Cấu hình DNS

Định nghĩa những cấu hình toàn cục cho DNS server: Cú pháp:

Options [

(directory path_name)

(forwarders [in_addr1; inaddr2;...])

(allow_query [address_match_list])

(notify yes/no)

(also – notify [ip_addr1, ip_addr2...;])

(also – update [ip_addr1, ip_addr2...;])

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

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

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

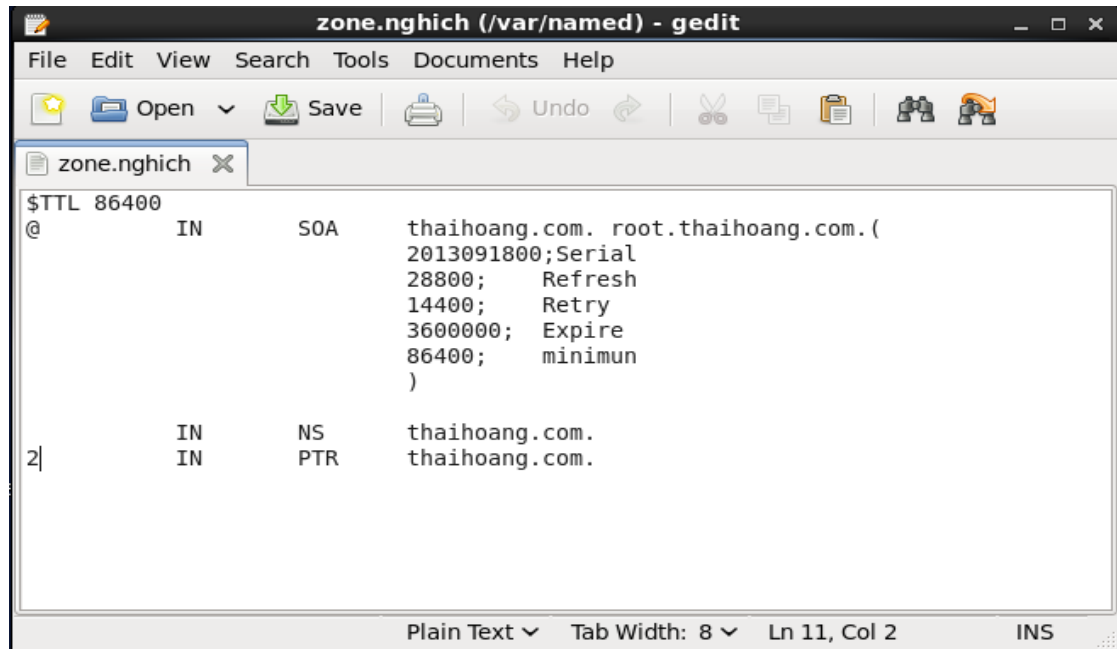
Notifi: mặc định được set là “yes”, khi có sự thay đổi trên CSDL thì name server sẽ gửi thông báo về sự thay đổi này cho các name server được khai báo trong danh sách name server được liệt kê trong record NS và các name server được khai báo trong tùy chọn also-notify.

Đồ án tốt nghiệp

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

+ Ta tiến hành cấu hình phân giải ngược như sau: tạo file theo đường dẫn sau:

gedit /var/named/zone.ngnich

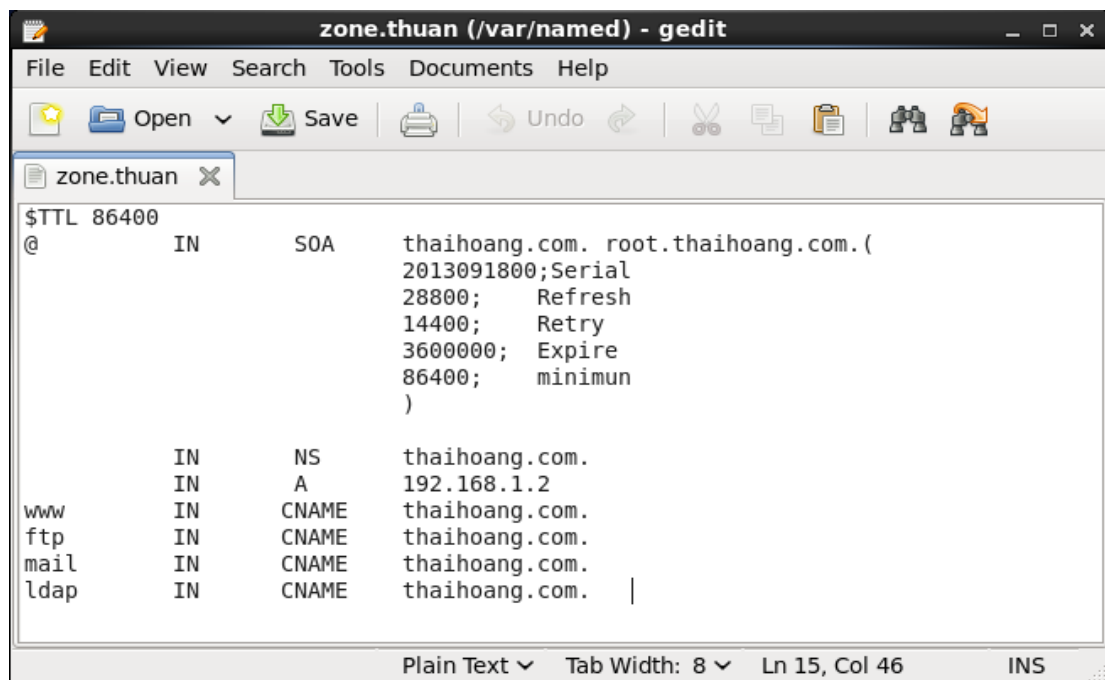


```
zone.ngnich (/var/named) - gedit
File Edit View Search Tools Documents Help
zone.ngnich x
$TTL 86400
@           IN      SOA      thaihoang.com. root.thaihoang.com. (
                                2013091800;Serial
                                28800;   Refresh
                                14400;   Retry
                                3600000; Expire
                                86400;   minimum
                                )
2|          IN      NS       thaihoang.com.
          IN      PTR      thaihoang.com.
Plain Text v Tab Width: 8 v Ln 11, Col 2 INS
```

File cấu hình zone ngnich

+ Ta tiến hành cấu hình phân giải thuận như sau: tạo file theo đường dẫn sau:

gedit /var/named/zone.thuan

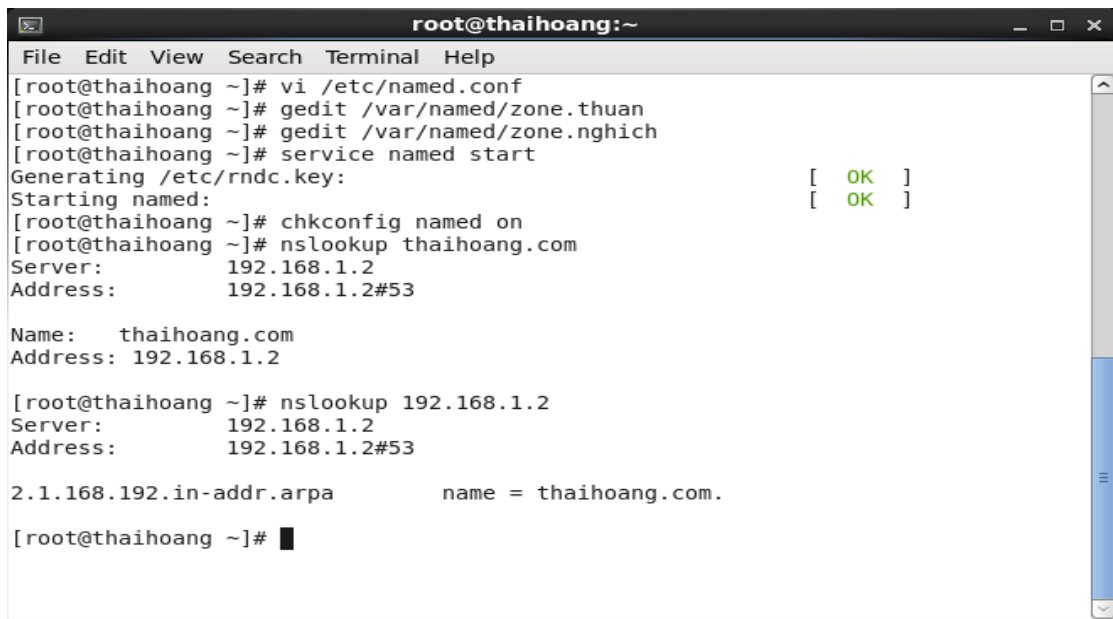


```
zone.thuan (/var/named) - gedit
File Edit View Search Tools Documents Help
zone.thuan x
$TTL 86400
@           IN      SOA      thaihoang.com. root.thaihoang.com. (
                                2013091800;Serial
                                28800;   Refresh
                                14400;   Retry
                                3600000; Expire
                                86400;   minimum
                                )
          IN      NS       thaihoang.com.
          IN      A        192.168.1.2
www        IN      CNAME    thaihoang.com.
ftp        IN      CNAME    thaihoang.com.
mail       IN      CNAME    thaihoang.com.
ldap       IN      CNAME    thaihoang.com.
Plain Text v Tab Width: 8 v Ln 15, Col 46 INS
```

File cấu hình zone thuận

Sau khi cấu hình xong file này và ping thành công 2 máy thì restart lại dịch vụ.

Kiểm tra dịch vụ DNS phân giải trong *nslookup*.



```
root@thaihoang:~  
File Edit View Search Terminal Help  
[root@thaihoang ~]# vi /etc/named.conf  
[root@thaihoang ~]# gedit /var/named/zone.thuan  
[root@thaihoang ~]# gedit /var/named/zone.ngnich  
[root@thaihoang ~]# service named start  
Generating /etc/rndc.key: [ OK ]  
Starting named: [ OK ]  
[root@thaihoang ~]# chkconfig named on  
[root@thaihoang ~]# nslookup thaihoang.com  
Server: 192.168.1.2  
Address: 192.168.1.2#53  
  
Name: thaihoang.com  
Address: 192.168.1.2  
  
[root@thaihoang ~]# nslookup 192.168.1.2  
Server: 192.168.1.2  
Address: 192.168.1.2#53  
  
2.1.168.192.in-addr.arpa name = thaihoang.com.  
[root@thaihoang ~]#
```

Kiểm tra dịch vụ DNS

1.2.2. Dịch vụ DHCP

1.2.2.1. Giới thiệu dịch vụ DHCP

Hệ thống cần cung cấp IP mỗi máy tính để các máy này có thể liên lạc với nhau. Với mô hình mạng tương đối nhỏ, việc cấp IP tương đối dễ dàng. Nhưng với một mô hình mạng lớn thì việc cung cấp IP trở nên khó khăn. Vì vậy cần phải có một dịch vụ cung cấp IP tự động cho các máy client trong hệ thống mạng.

- DHCP là một dịch vụ cung cấp IP tự động cho các client.
- Hoạt động theo mô hình Clients – server
- Ngoài ra DHCP còn có nhiều tính năng khác cho client như: cung cấp địa chỉ của máy tính dùng để giải quyết tên miền DNS, địa chỉ của một Gateway router...

Cơ chế sử dụng các thông số mạng được cấp phát động có ưu điểm hơn so với cơ chế khai báo tĩnh các thông số mạng như:

- Khắc phục được tình trạng đụng địa chỉ IP và giảm chi phí quản trị cho hệ thống mạng.
- Giúp cho các nhà cung cấp dịch vụ (ISP) tiết kiệm được số lượng địa chỉ IP thật (public IP).
- Phù hợp với máy tính thường xuyên di chuyển qua lại giữa các mạng.
- Kết hợp với hệ thống mạng không dây (wireless) cung cấp các điểm Hotspot như:

nhà ga, sân bay, trường học...

1.2.2.2. Nguyên tắc hoạt động

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

- Khi máy client khởi động, máy sẽ gửi broadcast gói tin DHCPDISCOVER, yêu cầu một server phục vụ cho mình. Gói tin này cũng chứa địa chỉ MAC của máy client.

- Các máy server trên mạng khi nhận được gói tin yêu cầu đó, nếu còn khả năng cung cấp địa chỉ IP, đều gửi lại cho máy client gói tin DHCPOFFER, đề nghị cho thuê một địa chỉ IP trong một khoảng thời gian nhất định, kèm theo là một subnet mask và địa chỉ của server. Server sẽ không cấp phát địa chỉ IP vừa đề nghị cho những client khác trong suốt quá trình thương thuyết.

- Máy client sẽ lựa chọn một trong những lời đề nghị (DHCPOFFER) và gửi broadcast lại gói tin DHCPREQUEST chấp nhận lời đề nghị đó. Điều này cho phép các lời đề nghị không được chấp nhận sẽ được các server rút lại và dùng để cấp phát cho client khác.

- Máy server được client chấp nhận sẽ gửi ngược lại một gói tin DHCPACK như là một lời xác nhận, cho biết là địa chỉ IP đó, subnet mask đó và thời hạn sử dụng đó sẽ chính thức được áp dụng. Ngoài ra server còn gửi kèm theo những thông tin cấu hình bổ sung như địa chỉ gateway mặc định, địa chỉ DNS server.

1.2.2.3. Các thông số trong cấu hình DHCP

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

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

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

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

1.2.2.4. Cài đặt và cấu hình dịch vụ DHCP.

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

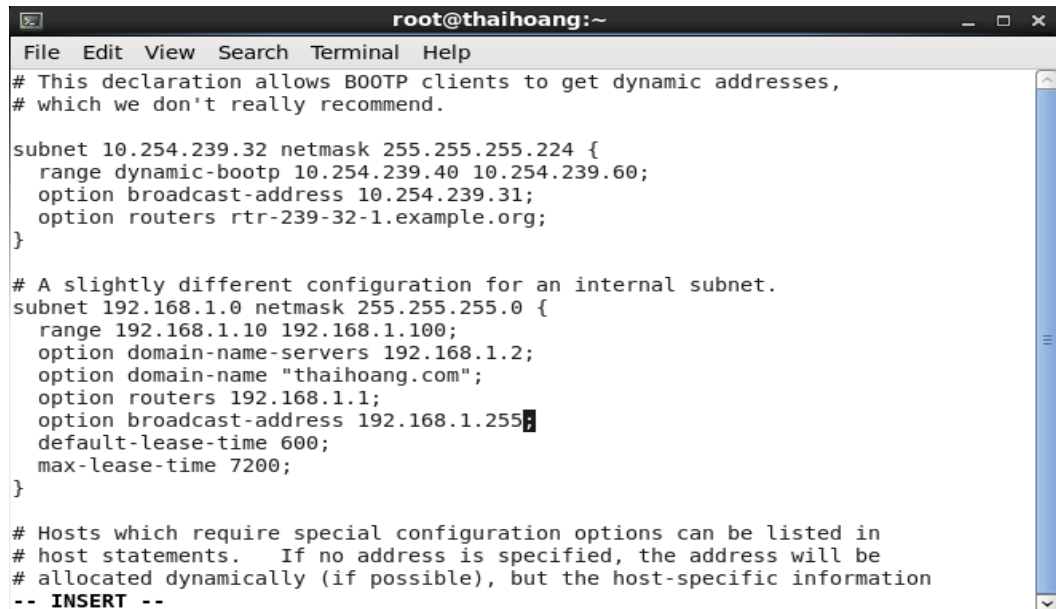
- Cách 1: cài đặt từ đĩa cd

#rpm -ivh dhcp-*.rpm (với * là phiên bản của gói dịch vụ).

- Cách 2: cài đặt bằng cách tải trên mạng

`#yum -y install dhcp`

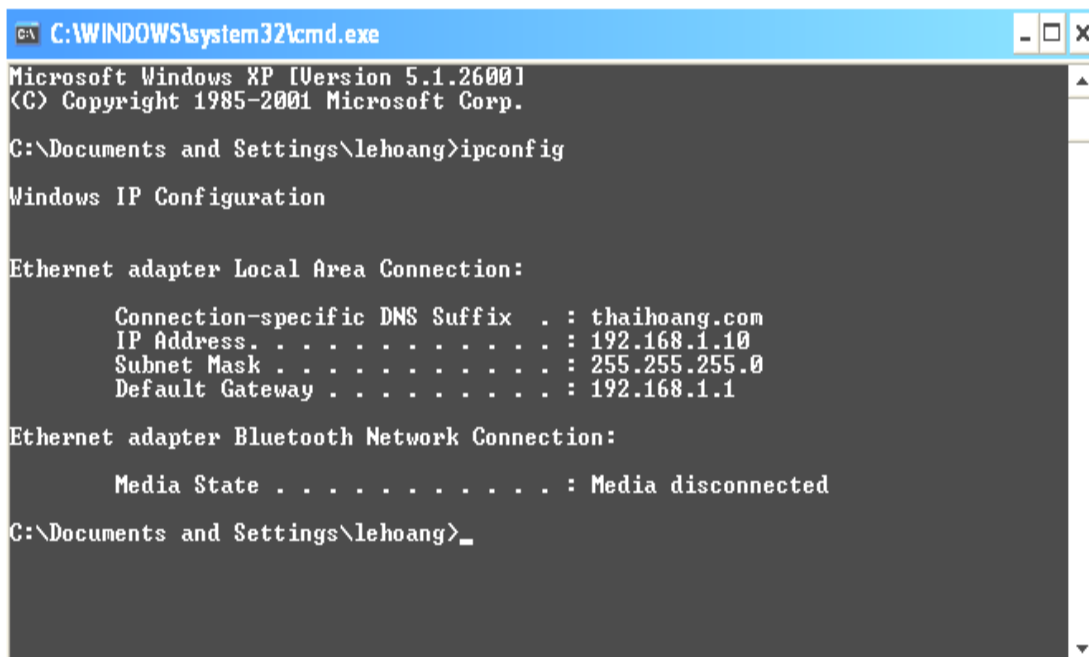
Kiểm tra gói cài đặt: `# rpm -qa|grep dhcp`. Sau khi cài đặt, ta cấu hình như sau:



```
root@thaihoang:~  
File Edit View Search Terminal Help  
# This declaration allows BOOTP clients to get dynamic addresses,  
# which we don't really recommend.  
  
subnet 10.254.239.32 netmask 255.255.255.224 {  
    range dynamic-bootp 10.254.239.40 10.254.239.60;  
    option broadcast-address 10.254.239.31;  
    option routers rtr-239-32-1.example.org;  
}  
  
# A slightly different configuration for an internal subnet.  
subnet 192.168.1.0 netmask 255.255.255.0 {  
    range 192.168.1.10 192.168.1.100;  
    option domain-name-servers 192.168.1.2;  
    option domain-name "thaihoang.com";  
    option routers 192.168.1.1;  
    option broadcast-address 192.168.1.255;  
    default-lease-time 600;  
    max-lease-time 7200;  
}  
  
# Hosts which require special configuration options can be listed in  
# host statements.  If no address is specified, the address will be  
# allocated dynamically (if possible), but the host-specific information  
-- INSERT --
```

File cấu hình DHCP

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



```
C:\WINDOWS\system32\cmd.exe  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
  
C:\Documents and Settings\lehoang>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Local Area Connection:  
  
    Connection-specific DNS Suffix  . : thaihoang.com  
    IP Address. . . . . : 192.168.1.10  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 192.168.1.1  
  
Ethernet adapter Bluetooth Network Connection:  
  
    Media State . . . . . : Media disconnected  
  
C:\Documents and Settings\lehoang>
```

Máy client đã được cấp phát địa chỉ Ip.

1.2.3. Dịch vụ SAMBA

1.2.3.1 Giới thiệu SAMBA

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

Samba được tạo ra bởi Andrew Tridgell 1991, được phát triển dựa trên giao thức SMB và CIFS. Samba là giao thức dùng để giao tiếp giữa Linux và windows.

Với một số chức năng như: chia sẻ file, chia sẻ thư mục, quản lý printer, printer setting tập trung, chứng thực client login vào window domain, cung cấp Windows Internet Name Service (WINS). Có thể thấy rằng, người dùng trên mạng có thể dùng chung các tập tin và máy in. Người dùng có thể điều khiển truy nhập tới những dịch vụ này bằng cách yêu cầu người dùng phải nhập mật mã truy nhập, điều khiển truy nhập có thể thực hiện ở 2 chế độ: chế độ dùng chung (share mode) và chế độ người dùng (user mode). Chế độ dùng chung sử dụng một mật mã truy nhập tài nguyên dùng chung cho nhiều người. Chế độ người dùng cung cấp cho mỗi tài khoản người dùng mật mã truy nhập tài nguyên khác nhau. Vì lý do phải quản lý mật mã truy nhập, samba có sử dụng tập tin `/etc/samba/smbpassword` để lưu trữ các mật mã truy nhập người dùng.

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

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

Các tập tin cấu hình dịch vụ:

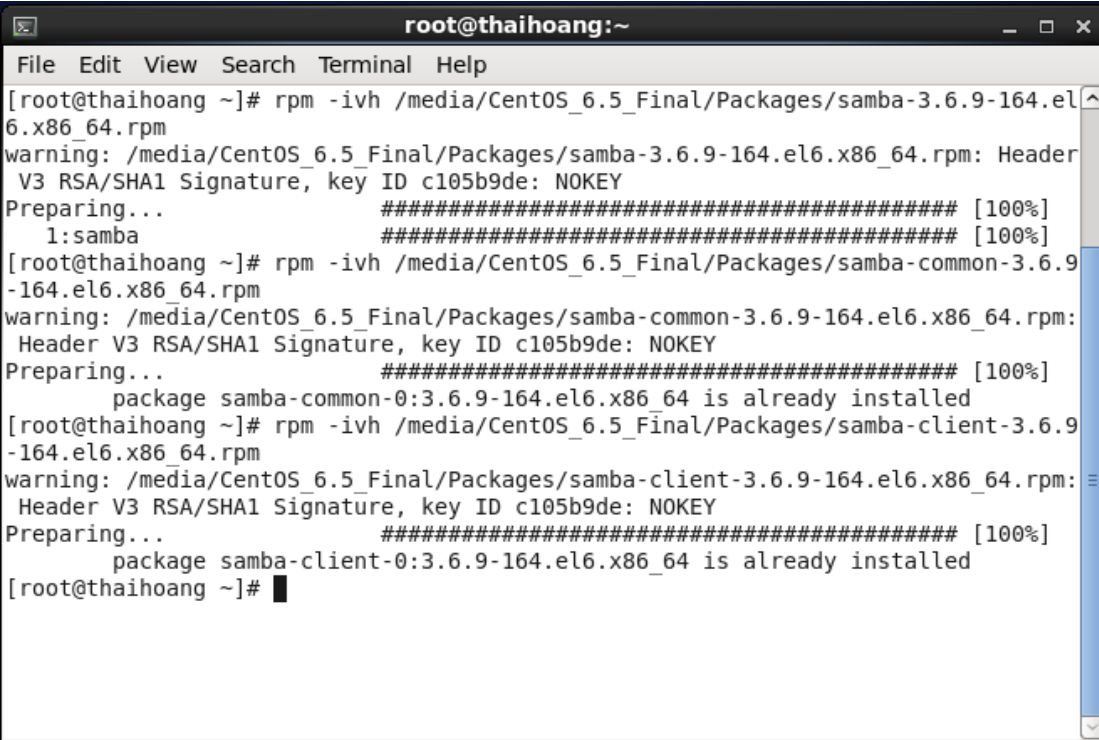
- `/etc/samba/smb.conf` : tập tin cấu hình của Samba
- `/etc/samba/smbpassword` : chứa mật mã truy nhập của người dùng
- `/etc/samba/smbusers` : chứa tên hiệu cho các tài khoản của samba.
- `smbpasswd -a<username>`: tạo tài khoản Samba.

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

1.2.3.2. Cài đặt và cấu hình

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

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



```
root@thaihoang:~  
File Edit View Search Terminal Help  
[root@thaihoang ~]# rpm -ivh /media/CentOS_6.5_Final/Packages/samba-3.6.9-164.el6.x86_64.rpm  
warning: /media/CentOS_6.5_Final/Packages/samba-3.6.9-164.el6.x86_64.rpm: Header V3 RSA/SHA1 Signature, key ID c105b9de: NOKEY  
Preparing... ##### [100%]  
1:samba ##### [100%]  
[root@thaihoang ~]# rpm -ivh /media/CentOS_6.5_Final/Packages/samba-common-3.6.9-164.el6.x86_64.rpm  
warning: /media/CentOS_6.5_Final/Packages/samba-common-3.6.9-164.el6.x86_64.rpm: Header V3 RSA/SHA1 Signature, key ID c105b9de: NOKEY  
Preparing... ##### [100%]  
package samba-common-0:3.6.9-164.el6.x86_64 is already installed  
[root@thaihoang ~]# rpm -ivh /media/CentOS_6.5_Final/Packages/samba-client-3.6.9-164.el6.x86_64.rpm  
warning: /media/CentOS_6.5_Final/Packages/samba-client-3.6.9-164.el6.x86_64.rpm: Header V3 RSA/SHA1 Signature, key ID c105b9de: NOKEY  
Preparing... ##### [100%]  
package samba-client-0:3.6.9-164.el6.x86_64 is already installed  
[root@thaihoang ~]#
```

Cài đặt Samba

Để cấu hình dịch vụ Samba sử dụng tập tin cấu hình */etc/samba/smb.conf*. Tập tin này được chia thành hai phần chính:

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

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

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

- Workgroup: chỉ ra tên của nhóm (workgroup) muốn hiển thị trên mạng. Trên windows, tên này được hiển thị trong cửa sổ Network Neighborhood.
- Host allow: chỉ ra những địa chỉ mạng hay địa chỉ máy được truy nhập tới dịch vụ Samba. Các địa chỉ trong danh sách được viết cách nhau một khoảng trắng.
- Encrypt passwords: giá trị mặc định là yes. Với tham số này, Samba sẽ thực hiện mã hóa mật mã dễ tương thích được với cách mã hóa của windows. Trong trường hợp không mã hóa mật mã, người dùng chỉ có thể sử dụng dịch vụ Samba giữa các máy Linux với nhau hoặc người dùng phải cấu hình lại máy tính Windows nếu muốn sử dụng Samba trên Linux.
- Smb passwd file: nếu encrypt passwords=yes, tham số này sẽ xác định tập chứa mật mã đã được mã hóa. Mặc định là */etc/samba/smbpasswd*
- Username map: chỉ ra tập tin chứa các tên hiệu (alias) cho một tài khoản hệ thống. Giá trị mặc định là: */etc/samba/smbusers*
- Printcap file: cho phép Samba nạp các mô tả máy in từ tập tin: printcap. Giá trị mặc định là: */etc/printcap*
- Security: khai báo này xác định cách thức các máy tính trả lời dịch vụ Samba. Mặc định tham số này có giá trị là user, giá trị cần sử dụng khi kết nối tới các máy tính windows.

Nhóm [homes]: nhóm này xác định các điều khiển mặc định cho truy nhập như thư mục chủ của người dùng thông qua giao thức SMB bởi người dùng từ xa. Khi có yêu cầu kết nối, samba sẽ thực hiện kiểm tra các nhóm hiện có, nếu nhóm nào đáp ứng được yêu cầu, nhóm đó sẽ được sử dụng. Nếu không đáp ứng được yêu cầu, nhưng nhóm đó tồn tại nó sẽ được xử lý như mô tả ở trên. Mặt khác, tên nhóm được yêu cầu cũng được xử lý như một tên của máy in và samba thực hiện tìm kiếm tập tin printcap tương ứng để xác định xem tên nhóm được yêu cầu có hợp lệ hay không. Nếu hợp lệ, một tài nguyên dùng chung sẽ được dựa trên **nhóm [printers]**.

Ngoài 3 nhóm đặc biệt được nêu trên, để thực hiện tạo các tài nguyên dùng chung khác, người dùng cần thực hiện tạo các tài nguyên này. Các nhóm dành cho các tài nguyên dùng chung, như là các mục trên hệ thống, thường đặt sau nhóm [home] và [printer] và có thể đặt tên bất kỳ.

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

- **Comment:** Mô tả tùy ý cho các tài nguyên được đưa lên mạng dùng chung.
- **Path:** chỉ ra đường dẫn đến thư mục trên hệ thống tập tin mà tài nguyên dùng chung tham chiếu tới.
- **Public:** có giá trị là yes hoặc no. Nếu là public = yes, Samba cho phép mọi người dùng đều có thể truy nhập tài nguyên dùng chung đó.
- **Browseable:** có giá trị yes hoặc no. Nếu là browseable = yes thì thư mục được dùng chung sẽ được nhìn thấy ở trên mạng. Giá trị mặc định là yes.
- **Valid user:** Danh sách những người dùng được quyền truy nhập tài nguyên dùng chung. Tên người dùng được cách nhau bởi khoảng trắng hoặc ký tự „,”. Tên nhóm được đứng sau bởi ký tự „+”
- **Invalid users:** danh sách những người dùng không được quyền truy nhập tài nguyên dùng chung. Tên người dùng được cách nhau bởi khoảng trắng hoặc ký tự „,”. Tên nhóm được đứng sau bởi ký tự „+”
- **Writeable:** có giá trị yes hoặc no. Nếu là writeable = yes người dùng được phép ghi vào thư mục dùng chung.
- **Write list:** Xác định danh sách người dùng /nhóm có quyền ghi tới thư mục dùng chung. Trong trường hợp chỉ ra tên nhóm, trước tên nhóm phải là một ký tự „+”.
- **Printable:** có giá trị là yes hoặc no. Nếu là printable = yes người dùng được phép truy nhập đến dịch vụ in.
- **Create mask:** thiết lập quyền trên thư mục/tập tin được tạo trong thư mục được dùng chung. Giá trị mặc định là 0744

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

[mydoc]

path=/home/shired public=no

valid users= + nhanvien

writable=yes

Chú ý:

- Thư mục được đưa lên mạng dùng chung phải cung cấp quyền tương ứng cho người dùng.
- Các tham số được chỉ ra ở nhóm tài nguyên được dùng chung sẽ có hiệu lực thay thế các tham số được thiết lập ở nhóm [global].
- Trong tập tin smb.conf có thể sử dụng một số biến thay thế như %m – tên NetBIOS của máy client, %Samba – tên dịch vụ hiện hành (nếu có), %u – tên người dùng hiện hành (nếu có)... ví dụ: “path = /home/%u” sẽ được phiên dịch là “path=/ymp/foo” nếu tài khoản foo thực hiện truy nhập.

• Chia sẻ thư mục:

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

Ví dụ bạn muốn thư mục data chỉ dành riêng cho user lehoang mà thôi. Bạn cần viết ra một đoạn mới và ghi các thông tin cần thiết vào: khai báo user, đường dẫn đến thư mục, cùng với thông tin cấu hình cho server SMB như sau:

[data]

comment = Thu mục chia se du lieu

path = /usr/local/src

valid users = lehoang

browsable = yes

public = no writable = yes

create mask = 0700

Đoạn trên đây đã tạo ra một thư mục chia sẻ mang tên data. Đường dẫn đến thư mục này trên server tại chỗ là */usr/local/src*. Vì mục browsable được khai báo "yes", danh sách duyệt mạng sẽ có tên là plasdir. Nhưng vì mục public lại là "no" nên chỉ có user tên là phi_long mới có quyền dùng Samba để vào ra thư mục.

Muốn cho ai được truy cập, bạn chỉ cần liệt kê họ tại thư mục valid users.

1.2.3.3. Quản trị tài khoản Samba

Để có thể sử dụng dịch vụ Samba (ngoại trừ trường hợp cho phép mọi người dùng

truy nhập), người dùng cần phải thiết lập tài khoản người dùng Samba. Tài khoản người dùng Samba là một tài khoản được xây dựng dựa trên tài khoản hệ thống (tài khoản của Linux), do vậy, phải có tài khoản người dùng hệ thống người dùng mới có thể tạo được tài khoản samba.

- Tạo tài khoản Samba:

Samba sử dụng database người dùng riêng để chứng thực user,password khi người dùng truy cập vào samba chứ không dùng database người dùng trong file passwd của hệ thống.

Samba phiên bản 3.0 trở lên, không còn dùng lệnh smbadduser nữa mà sử dụng cú pháp sau để tạo tài khoản samba:

`smbpasswd -a <tên_tài_khoản>`

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

`[root@server2]# smbpasswd -a a3`

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

Cú pháp lệnh: `smbpasswd [option] [username]`

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

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

Một số lựa chọn của lệnh như sau:

-x : Xóa người dùng Samba username khỏi tập tin `/etc/samba/smbpasswd`.

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

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

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

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

```
# smbpasswd -x a3
```

1.2.3.4. Sử dụng dịch vụ Samba

Truy nhập dịch vụ SMB - lệnh smbclient

Việc truy nhập dịch vụ Samba của Linux từ các máy tính Windows được thực hiện tương tự như việc truy nhập các thông tin được chia sẻ giữa các máy tính Windows.

Các hệ thống Linux có thể truy nhập hệ dịch vụ Samba bằng cách thi hành lệnh smbclient.smbclient, hoạt động giống như FTP, cho phép truy nhập hệ thống sử dụng giao thức SMB. Nhiều lệnh smbclient tương tự như FTP, như là lệnh mget để truyền tập tin, lệnh del để xóa tập tin.

Cú pháp lệnh: smbclient //servername/service [options]

Trong đó servername là tên (hay địa chỉ IP) của máy chủ Samba, service là tên thư mục được chia sẻ (chính là tên của nhóm được khai báo trong tập tin cấu hình của Samba /etc/samba/smb.conf).

Một số lựa chọn hay dùng của lệnh:

- U username: Tên tài khoản đăng nhập sử dụng Samba.
- L host: Liệt kê danh sách các thư mục được chia sẻ trên máy có địa chỉ IP hay tên máy là host.
- N: Không xuất hiện lời nhắc yêu cầu nhập mật mã. Thường dùng trong trường hợp thư mục được chia sẻ là public.
- Khi đã kết nối với máy chủ Samba, Samba xuất hiện lời nhắc sau:

```
smb: \>
```

Tại lời nhắc này, người dùng có thể thi hành các lệnh của smbclient. Phần lớn những lệnh này tương tự như những lệnh của ftp (để gửi và lấy tập tin về, như là get, mget, put, mput) và giống như những lệnh về quản lý tập tin của Linux (như là ls, rm, cd...).

Để biết được các lệnh của smbclient. Tại lời nhắc này người dùng dùng lệnh?

Gắn kết một tài nguyên dùng chung vào hệ thống tập tin (mount & umount).

Việc truy nhập các tập tin dùng chung thông qua lệnh smbclient là khá bất tiện và không được linh hoạt. trong trường hợp thường xuyên có các thao tác trên thư mục dùng chung, người dùng có thể gắn kết thư mục được share trên mạng đó vào hệ

thông tập tin cục bộ để có thể sử dụng như một thư mục bình thường. lệnh được sử dụng để thực hiện tác vụ này là lệnh *mount* với cú pháp như sau:

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

Trong đó:

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

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

```
[root@server2~]# mount -t cifs -ousername=administrator, password=123456  
//192.168.1.202/software /home/software
```

Để có thể gỡ bỏ gắn kết thư mục dùng chung, người dùng sử dụng lệnh *umount* với cú pháp sau: *umount mountpoint*

Trong đó mount point là vị trí (thư mục) trên hệ thống tập tin cục bộ mà thư mục dùng chung được gắn kết vào.

Ví dụ: gỡ bỏ gắn kết của thư mục software vừa thực hiện gắn kết ở thí dụ trên:

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

1.2.4 . Dịch vụ FTP

1.2.4.1. Giới thiệu

VSFTP là 1 dịch vụ FTP server, chúng ta sẽ dùng hệ thống VSFTP để có thể chia sẻ tài liệu (tài nguyên) cho người khác.

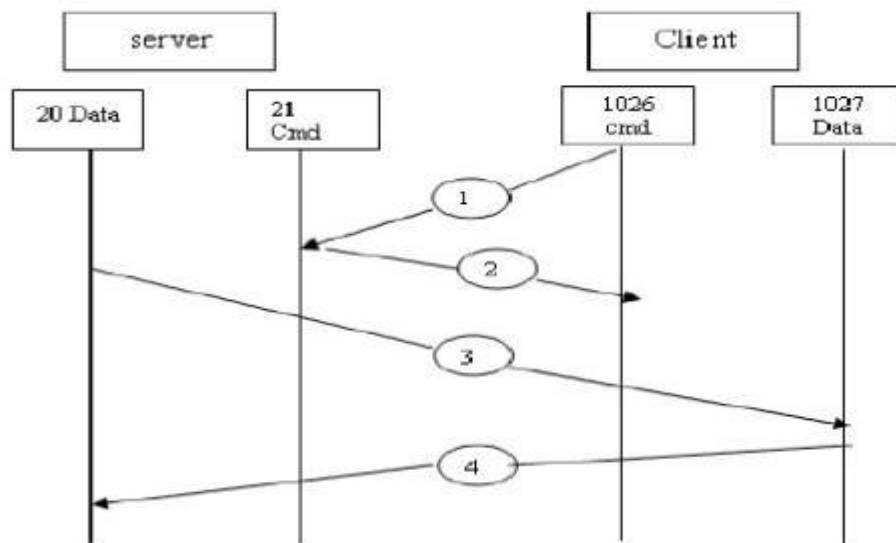
- VSFTP là FTP server chạy trên môi trường Linux.
- VSFTP sẽ phân quyền dựa trên cấu hình và File Permisson.

Hoạt động ở chế độ Active: Ở chế độ này, máy khách dùng 1 cổng ngẫu nhiên (cổng $N > 1024$) kết nối vào cổng 21 của FTP server. Sau đó, máy khách lắng nghe trên cổng $N+1$ và gửi lệnh đến FTP server và từ cổng dữ liệu của mình, FTP server kết nối lại với cổng dữ liệu của máy khách đã khai báo trước đó. Khi FTP server hoạt động ở chế độ chủ động, client không tạo kết nối thật sự vào cổng dữ liệu của FTP server, mà chỉ đơn giản là thông báo cho FTP server biết rằng nó đang lắng nghe trên cổng nào

và Server phải kết nối ngược vào cổng đó.

Ở khía cạnh Firewall, để FTP hỗ trợ chế độ active các kênh truyền phải mở:

- Cổng 21 của FTP server phải được mở cho bất cứ nguồn gửi nào (để client khởi tạo kết nối
- Cho kết nối từ cổng 20 của FTP server đến các cổng >1024 (server khởi tạo kết nối vào cổng dữ liệu của client)
- Nhận kết nối đến cổng 20 của FTP server từ các cổng >1024. Sơ đồ kết nối Active:



Sơ đồ kết nối Active

Bước 1: Client khởi tạo kết nối vào cổng 21 của server và gửi lệnh PORT 1027.

Bước 2: Server gửi xác nhận ACK về cổng lệnh của client.

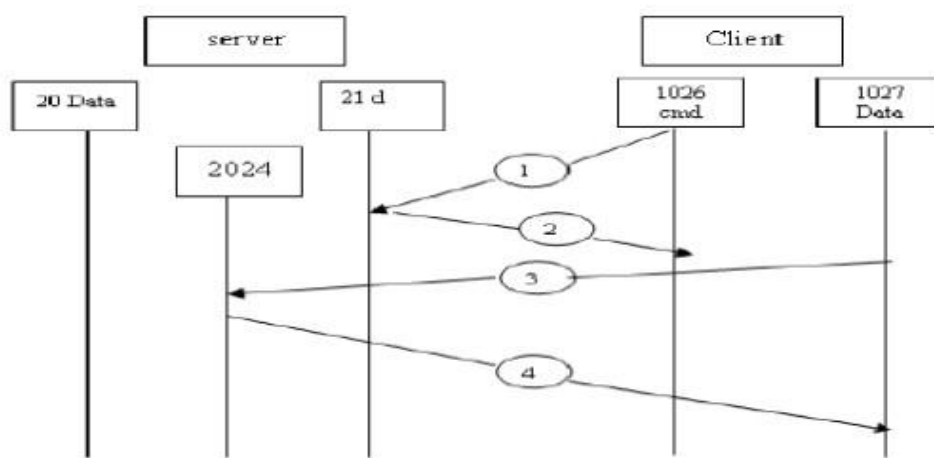
Bước 3: Server khởi tạo kết nối từ cổng 20 của mình đến cổng dữ liệu mà client đã khai báo trước đó.

Bước 4: Client gửi ACK phản hồi cho server.

Hoạt động ở chế độ Passive: Ở chế độ thụ động, FTP client tạo kết nối đến server, tránh vấn đề firewall lọc kết nối đến cổng của máy bên trong từ server. Khi kết nối FTP được mở, client sẽ mở 2 cổng dành riêng (>1024), cổng thứ nhất dùng để liên lạc với cổng 21 của FTP server, nhưng thay vì gửi lệnh PORT và sau đó là server kết nối ngược trở lại, thì lệnh PASS được phát ra. Kết quả là server sẽ mở một cổng bất kỳ (>1024) và gửi lệnh PORT P ngược trở lại cho client. Sau đó client tự kết nối từ cổng thứ hai vào cổng P trên server để truyền dữ liệu.

Để hỗ trợ cho FTP ở chế độ passive, các kênh truyền cần phải được mở là:

- Cổng 21 của FTP server nhận kết nối từ bất cứ nguồn nào (cho client tự khởi tạo kết nối)
- Cho phép trả lời từ cổng 21 của FTP server tới bất cứ cổng nào (>1024).
- Nhận kết nối trên cổng FTP server >1024 từ bất cứ nguồn nào (client kết nối để truyền dữ liệu đến cổng ngẫu nhiên mà server đã chỉ ra).
- Cho phép trả lời từ cổng FTP server >1024 đến các cổng >1024 của client. Sơ đồ kết nối passive:



Sơ đồ kết nối passive

Bước 1: Client gửi yêu cầu.

Bước 2: Server trả lời bằng lệnh PORT 2024, cho client biết cổng 2024 đang được mở để nhận kết nối dữ liệu.

Bước 3: Client tạo kết nối truyền dữ liệu từ cổng dữ liệu của nó đến cổng dữ liệu 2024 của server.

Bước 4: Server trả lời bằng xác nhận ACK về cho cổng dữ liệu của client.

Chú ý: Đối với FTP thụ động, cổng mà lệnh PORT mô tả chính là cổng sẽ được mở trên server. Còn đối với FTP chủ động cổng này sẽ được mở ở client.

FTP Server: FTP server là máy chủ lưu trữ những tài nguyên và hỗ trợ giao thức FTP để giao tiếp với những máy khác cho phép truyền dữ liệu trên internet.

FTP Server là máy chủ lưu giữ những tài nguyên và hỗ trợ giao thức FTP để giao tiếp với những máy tính khác cho phép truyền dữ liệu trên Internet.

Một số chương trình FTP Server sử dụng trên Linux: Vsftpd, wu-ftp, pureFTPD,

proFTPD, ...

Có 3 cách cài đặt FTP server:

- Anonymous ftp: Khi thiết lập Anonymous FTP. Mọi người có thể truy cập tới Server.
- Với Anonymous account mà không có password, người quản trị server sẽ thiết lập giới hạn để hạn chế các user upload những files không được phép upload lên Server như: Music, Films, games...
- FTP với anonymous access và users account có password: Khi sử dụng giao thức này để các truy cập vào server thì chỉ cần truy cập tới Directory (ngoại trừ user root), chúng ta có thể view/modify/delete tất cả các files hay tất cả các folders.
- FTP với Mysql hỗ trợ Virtual users authentication: Giao thức này chỉ cho phép một số nhóm người dùng truy cập tới Server

1.2.4.2. Cài đặt

Kiểm tra xem dịch vụ FTP đã được cài đặt trên hệ thống hay chưa:

```
#rpm -qa | grep vsftpd
```

Cài từ đĩa CD:

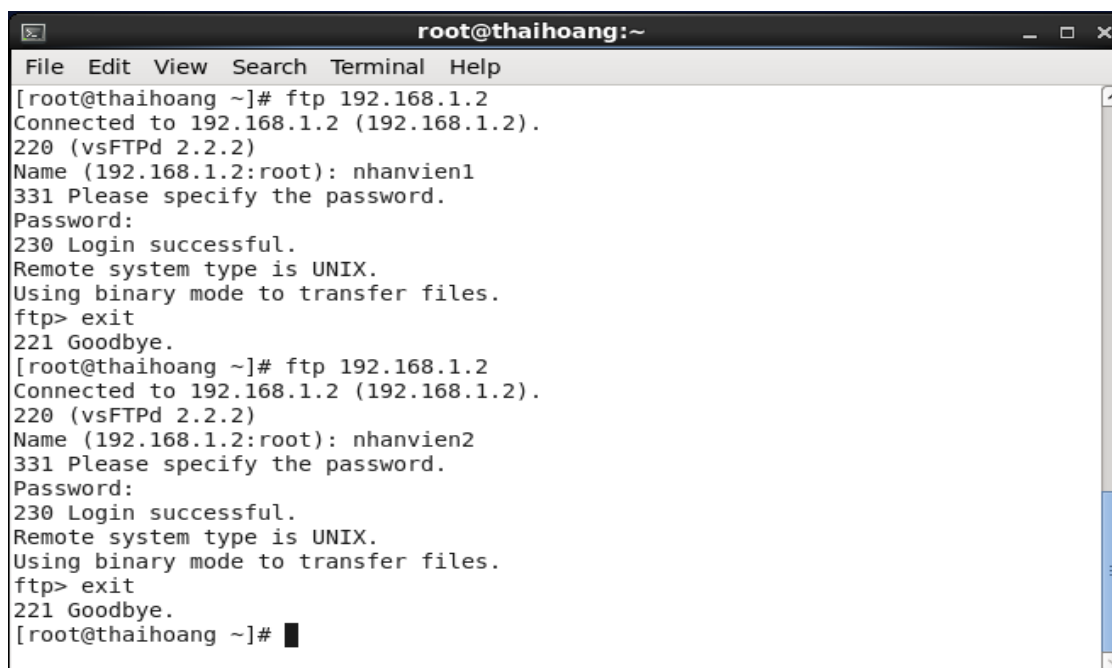
```
#mount /dev/cdrom /media/
```

```
#rpm -ivh /media/CentOS/ vsftpd-2.2.2-11.el6_4.1.x86_64.rpm
```

Sau khi chạy xong file này thì VSFTP đã được cài đặt thành công.

1.2.4.3. Cấu hình dịch vụ FTP.

Sau khi cài đặt xong thì thư mục chính của VSFTP là /etc/vsftp. Bên trong thư mục này sẽ có 1 file cấu hình chính là *vsftpd.conf*. Sau khi cấu hình, kiểm tra xem cấu hình có thành công không.



```
root@thaihoang:~  
File Edit View Search Terminal Help  
[root@thaihoang ~]# ftp 192.168.1.2  
Connected to 192.168.1.2 (192.168.1.2).  
220 (vsFTPd 2.2.2)  
Name (192.168.1.2:root): nhanvien1  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> exit  
221 Goodbye.  
[root@thaihoang ~]# ftp 192.168.1.2  
Connected to 192.168.1.2 (192.168.1.2).  
220 (vsFTPd 2.2.2)  
Name (192.168.1.2:root): nhanvien2  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> exit  
221 Goodbye.  
[root@thaihoang ~]#
```

FTP cấu hình thành công

1.2.4.4. Một số option quan trọng

VSFTP dùng chung user với user do linux quản lý. Khi tạo bên Linux 1 user mới với tên và password đầy đủ thư mục của user đó sẽ là thư mục chính khi user đó đăng nhập vào hệ thống. Chúng ta có thể phân quyền trên thư mục đó để phân quyền người dùng đó trên Server.

Một số option quan trọng như:

- ***Dữ liệu cần xác nhận giá trị BOOLEAN***

listen : Đây là 1 option rất quan trọng dùng để bật tắt chế độ Standalone, mặc định Option này là NO. Tuy nhiên đối với tất cả các máy chạy VSFTP đơn lẻ nhất thiết phải thiết lập option listen=YES, nếu không thiết lập Server VSFTP sẽ không khởi động được.

anonymous: option này nếu =YES thì cho phép đăng nhập vào server với vai trò anonymous. Default =YES. Nếu server FTP người dùng muốn xây dựng và không cho sự xâm nhập của người lạ thì nên set *anonymous*=NO.

local_enable: có cho phép user hiện đang ở trên local host truy xuất đến Server FTP đang chạy local. Default = NO.

write_enable: cho phép user có được ghi lên server hay không. Đây là 1 option quan trọng nó cũng 1 phần quyết định và FTP server ở dạng nào: chỉ đọc, có thể ghi,

vvv. Default = NO.

anon_upload_enable: cho phép user anonymous có được upload file hay không. Option này phải được cấu hình chung với option *write_enable* ở phía trên. Nếu muốn user upload file được thì đồng thời bật 2 option này bằng YES. Default = NO.

anon_mkdir_enable: cho phép user anonymous tạo được thư mục trên server, nếu bật YES thì *write_enable* cũng phải bật YES.
download_enable: cho phép User download file hay không. Nếu =NO, tất cả các yêu cầu download đều bị từ chối hết. Default = YES.

Userlist_deny: NO cho phép các user trong danh sách trong File *user_list* được phép truy cập vào FTP (file *user_list* nằm cùng thư mục với File cấu hình). Nếu YES thì ngược lại.

- Dữ liệu cần xác nhận giá trị NUMERIC

max_client: khi chế độ standalone được bật tức *listen*=YES thì *max_client* này quy định số kết nối tối đa của Client vào Server. Default = 0. Nếu =0 tức là không giới hạn số kết nối.

connect_timeout: quy định thời gian timeout cho 1 connection, được tính bằng giây. Default = 60.

Data_connection_timeout: quy định thời gian tối đa để thực hiện việc truyền dữ liệu, quá thời gian này sẽ bị cắt khi truyền. tính bằng giây. Mặc định là 300. Để bảo đảm việc truyền dữ liệu thì chúng ta cũng nên để option này có 1 giá trị cao.

File_open_mode: umask của file sẽ được user upload (nếu server cho phép upload). Default = 0666.

- Dữ liệu cần xác nhận giá trị STRING

listen_address: khi server ở chế độ StandAlone địa chỉ lắng nghe mặc định sẽ được thay bằng địa chỉ này.

Vsftpd_log_file: tên file log mà server sẽ ghi log xuống.

ftp_username: đây là tên user mình sẽ sử dụng để quản lý cho các anonymous user. Default: ftp.

1.2.4.5. Kích hoạt dịch vụ

Sau khi chúng ta cấu hình xong thì công việc tiếp theo đó là cần phải khởi động server. Server có 3 lệnh chính là start, top, restart. Để gọi thực hiện 3 lệnh này thì có 2

cách.

- cách 1:

```
/etc/init.d/vsftpd start
```

```
/etc/init.d/vsftpd stop
```

```
/etc/init.d/vsftpd restart
```

- cách 2: là cách để khởi động chung cho các server

```
service vsftpd start
```

```
service vsftpd stop
```

```
service vsftpd restart
```

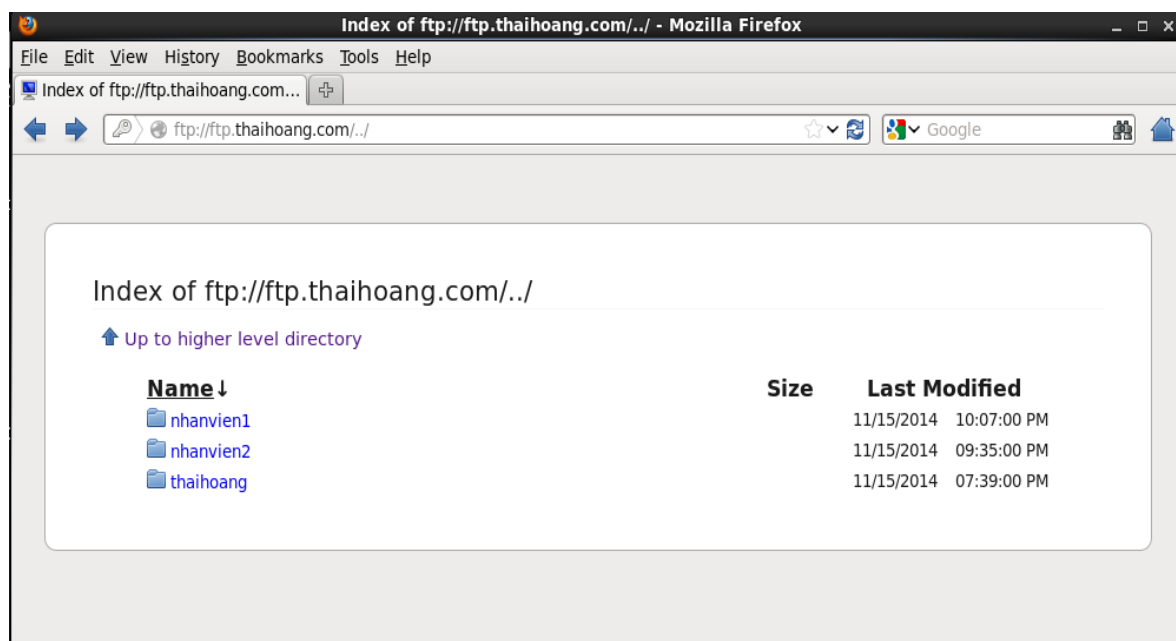
Để có thể mặc định mỗi lần khởi động máy thì VSFTP được khởi động theo:

- Dùng cho dòng Redhat/ Fedora: `chkconfig vsftpd on`.

1.2.4.6. Kết nối tới FTP server

Để kết nối tới FTP ta có thể dùng nhiều cách khác nhau như trình duyệt web hay phần mềm.

Đây là cách truy cập bằng trình duyệt. Sử dụng bằng trình duyệt Web:



Kiểm tra kết nối tới FTP

1.2.5. Dịch vụ Webserver

1.2.5.1. Giới thiệu

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

Webserver, cung cấp source code đầy đủ với license không hạn chế.

- Môi trường tốt nhất để sử dụng Apache là Unix.
- Hỗ trợ đầy đủ các giao thức HTTP, HTTPS, FTP...
- Chạy trên nhiều hệ điều hành: Unix, Windows, Linux, Netware, OS/2.

1.2.5.2. Cài đặt và cấu hình dịch vụ Httpd

Trong terminal gõ `rpm -qa | grep httpd` để kiểm tra đã cài đặt chưa. Nếu chưa thì dùng lệnh: `yum install httpd` để cài đặt. Hoặc có thể cài từ đĩa: thực hiện lệnh: `rpm -ivh httpd-2.2.15-29.el6.centos.x86_64.rpm`.

Khởi động dịch vụ.

Mặc định thì dịch vụ Apache chưa được kích hoạt. Để khởi động, sử dụng công cụ hoặc dùng dòng lệnh:

```
# service httpd start
```

Để Apache sẽ khởi động mỗi lần hệ thống boot, hãy enable dịch vụ Apache bằng câu lệnh sau:

```
#chkconfig httpd on
```

Khi thay đổi cấu hình của Apache, bạn phải reload lại Apache bằng dòng lệnh:

```
# service httpd reload
```

Các tham số trong tập tin cấu hình httpd.conf.

Global Environment.

ServerRoot: nơi đặt tập tin cấu hình

Cú pháp: `ServerRoot <đường_dẫn_thư_mục>`

Ví dụ: `ServerRoot "/etc/httpd"`

Listen: quy định địa chỉ IP hoặc cổng mà web server nhận kết nối từ client. Cú pháp: `Listen <IP:port>`

Ví dụ: `Listen 8080` #cổng 80 ở tất cả các card mạng. `Listen 192.168.1.5:8080` #cổng 8080 của 1 card mạng.

Timeout <time>: qui định thời gian sống của một kết nối (tính bằng giây).

Ví dụ: `Timeout 300`

KeepAlive <On/Off>: cho phép hoặc không cho phép client gửi được nhiều yêu cầu dựa trên một kết nối với web server

Ví dụ: KeepAlive On

MaxKeepAliveRequest <số_request>: số tối đa của request trên một kết nối (nếu cho phép nhiều Request trên một kết nối)

Ví dụ: MaxKeepAliveRequest 100

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

Ví dụ: KeepAliveTimeout 15

MaxClients <number>: qui định số yêu cầu tối đa từ các client gửi đồng thời đến server

Ví dụ: MaxClients 256

BindAddress <IP/*>: qui định địa chỉ card mạng để chạy Apache trên server. Sử dụng dấu “ * ” để có thể sử dụng tất cả các địa chỉ có trên máy.

Ví dụ: BindAddress 192.168.1.2 Mặc định là: BindAddress *

Main server configuration.

Group apache

Group apache

ServerAdmin <email>: địa chỉ email của người quản trị website

Ví dụ: ServerAdmin root@linuxgroup.com **ServerName** <name/IP> tên hoặc địa chỉ IP *Ví dụ : ServerName www.linuxgroup.com* **DocumentRoot** <path>: nơi đặt dữ liệu web

+ **ServerSignature Off**: không hiển thị thông tin về server

+ **AddDefaultCharset UTF-8**: bộ mã mặc định

+ **DirectoryIndex** <danh_sách_tập_tin>: các tập tin mặc định khi truy cập tên

Website.

Ví dụ: DirectoryIndex index.html index.html index.php index.cgi

+ **ErrorLog** <vị_trí_tập_tin_log>: chỉ định tập tin để server ghi vào bất kỳ những lỗi mà nó gặp phải.

Ví dụ: ErrorLog logs/error_log

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

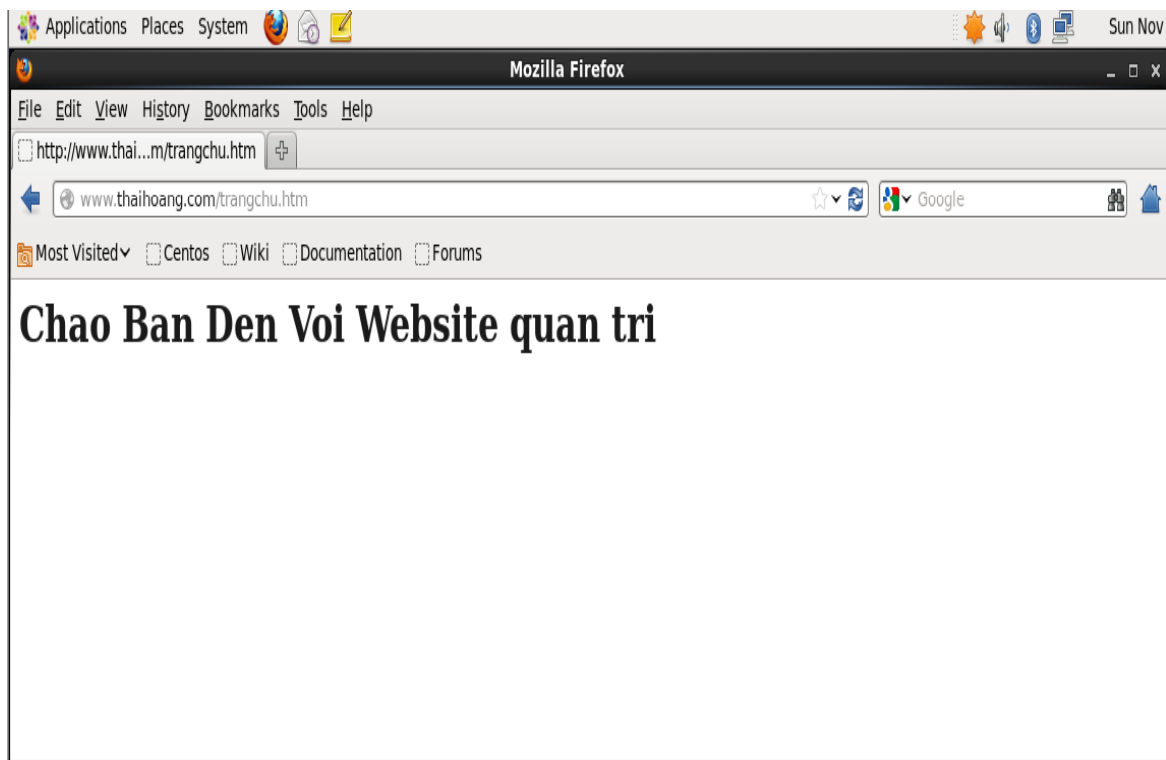
+ **Alias** <đường_dẫn_http> <đường_dẫn_cục_bộ>: ánh xạ đường dẫn cục bộ (không nằm trong DocumentRoot) thành đường dẫn http

Ví dụ: *Alias /manual /var/www/manual*

+ Để giới hạn việc truy cập của người dùng, ta có thể kết hợp với các khai báo Directory.

+ **UserDir:** cho phép người dùng tạo Homepage của mình lên server về cùng một địa chỉ 192.168.1.2

Sau khi cấu hình xong, tạo một website *trangchu.htm* để test. Với mô hình em đã thực hiện, trên trình duyệt firefox gõ tên miền *thaihoang.com* để kiểm tra website.



Kiểm tra website server

1.2.6. Dịch vụ LDAP

1.2.6.1. Giới thiệu

Thư mục (Directory): là nơi dùng để chứa và cho phép thực hiện các thao tác truy xuất thông tin.

Nghi thức truy cập thư mục (LDAP):

LDAP (Lightweight Directory Access Protocol) là một chuẩn mở rộng cho nghi thức truy cập thư mục, hay là một ngôn ngữ để LDAP client và servers sử dụng để giao tiếp với nhau. LDAP là một nghi thức “lightweight” có nghĩa là đây là một giao thức có tính hiệu quả, đơn giản và dễ dàng để cài đặt. trong khi chúng sử dụng các hàm ở mức cao. Điều này trái ngược với nghi thức “heavyweight” như là nghi thức truy cập

thư mục X.500 (DAP). Nghi thức này sử dụng các phương thức mã hoá quá phức tạp. LDAP sử dụng các tập các phương thức đơn giản và là một nghi thức thuộc tầng ứng dụng.

LDAP đã phát triển với phiên bản LDAP v2 được định nghĩa trong chuẩn RFC 1777 và 1778, LDAP v3 là một phần trong chuẩn Internet, được định nghĩa trong RFC 2251 cho đến RFC 2256, do chúng quá mới nên không phải tất cả mọi thứ các nhà cung cấp hỗ trợ hoàn toàn cho LDAP v3.

Ngoài vai trò như là một thủ tục mạng, LDAP còn định nghĩa ra bốn mô hình, các mô hình này cho phép linh động trong việc sắp đặt các thư mục:

- Mô hình LDAP information - định nghĩa ra các loại dữ liệu mà bạn cần đặt vào thư mục.
- Mô hình LDAP Naming - định nghĩa ra cách bạn sắp xếp và tham chiếu đến thư mục.
- Mô hình LDAP Functional - định nghĩa cách mà bạn truy cập và cập nhật thông tin trong thư mục của bạn.
- Mô hình LDAP Security - định nghĩa ra cách thông tin trong thư mục của bạn được bảo vệ tránh các truy cập không được phép.

Ngoài các mô hình ra LDAP còn định nghĩa ra khuôn dạng để trao đổi dữ liệu LDIF (LDAP Data Interchange Format), ở dạng thức văn bản dùng để mô tả thông tin về thư mục. LDIF còn có thể mô tả một tập hợp các thư mục hay các cập nhật có thể được áp dụng trên thư mục.

1.2.6.2. Phương thức hoạt động của LDAP

- Một nghi thức client/sever:

Là một mô hình giao thức giữa một chương trình client chạy trên một máy tính gửi một yêu cầu qua mạng đến cho một máy tính khác đang chạy một chương trình sever (phục vụ), chương trình này nhận lấy yêu cầu và thực hiện sau đó nó trả lại kết quả cho chương trình client. Ví dụ những nghi thức client/server khác là nghi thức truyền siêu văn bản (Hypertext transfer protocol) viết tắt là HTTP, nghi thức này có những ứng dụng rộng rãi phục vụ những trang web và nghi thức Internet Message Access Protocol (IMAP), là một nghi thức sử dụng để truy cập đến các thư thông báo điện tử. Ý tưởng cơ bản của nghi thức client/server là công việc được gán cho những máy tính

đã được tối ưu hoá để làm thực hiện công việc đó. Ví dụ tiêu biểu cho một máy server LDAP có rất nhiều RAM (bộ nhớ) dùng để lưu trữ nội dung các thư mục cho các thao tác thực thi nhanh và máy này cũng cần đĩa cứng và các bộ vi xử lý ở tốc độ cao.

- LDAP là một nghi thức hướng thông điệp

Do client và sever giao tiếp thông qua các thông điệp, Client tạo một thông điệp (LDAP message) chứa yêu cầu và gửi nó đến cho server. Server nhận được thông điệp và xử lý yêu cầu của client sau đó gửi trả cho client cũng bằng một thông điệp LDAP. Ví dụ: khi LDAP clients muốn tìm kiếm trên thư mục, client tạo LDAP tìm kiếm và gửi thông điệp cho server. Server tìm trong cơ sở dữ liệu và gửi kết quả cho client trong một thông điệp LDAP.

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

Việc cho phép nhiều thông điệp cùng xử lý đồng thời làm cho LDAP linh động hơn các nghi thức khác ví dụ như HTTP, với mỗi yêu cầu từ client phải được trả lời trước khi một yêu cầu khác được gửi đi, một HTTP client program như là Web browser muốn tải xuống cùng lúc nhiều file thì Web browser phải thực hiện mở từng kết nối cho từng file, LDAP thực hiện theo cách hoàn toàn khác, quản lý tất cả thao tác trên một kết nối.

1.2.6.3. Cài đặt và cấu hình dịch vụ LDAP

Bước 1: Trên máy ldap-server kiểm tra 2 package *opeldap-servers* và *openldap-clients* đã được cài đặt chưa. Nếu chưa thì tiến hành cài đặt 2 packages này.

```
root@thaihoang:~  
File Edit View Search Terminal Help  
warning: /media/CentOS_6.5_Final/Packages/openldap-servers-2.4.23-32.el6_4.1.x86_64.rpm: Header V3 RSA/SHA1 Signature, key ID c105b9de: NOKEY  
Preparing... ##### [100%]  
1:openldap-servers ##### [100%]  
[root@thaihoang ~]# rpm -ivh /media/CentOS_6.5_Final/Packages/openldap-clients-2.4.23-32.el6_4.1.x86_64.rpm  
warning: /media/CentOS_6.5_Final/Packages/openldap-clients-2.4.23-32.el6_4.1.x86_64.rpm: Header V3 RSA/SHA1 Signature, key ID c105b9de: NOKEY  
Preparing... ##### [100%]  
1:openldap-clients ##### [100%]  
[root@thaihoang ~]# rpm -qa openlap*  
[root@thaihoang ~]# rpm -qa | grep openldap  
openldap-clients-2.4.23-32.el6_4.1.x86_64  
openldap-devel-2.4.23-32.el6_4.1.x86_64  
openldap-2.4.23-32.el6_4.1.x86_64  
openldap-servers-2.4.23-32.el6_4.1.x86_64  
[root@thaihoang ~]# clear  
  
[root@thaihoang ~]# slappasswd  
New password:  
Re-enter new password:  
{SSHA}jtTlwqWA87xidcwGBioJpuait1RXY+qv  
[root@thaihoang ~]# vi /etc/openldap/slapd.d/cn=config/olcDatabase=\{2\}bdb.ldif
```

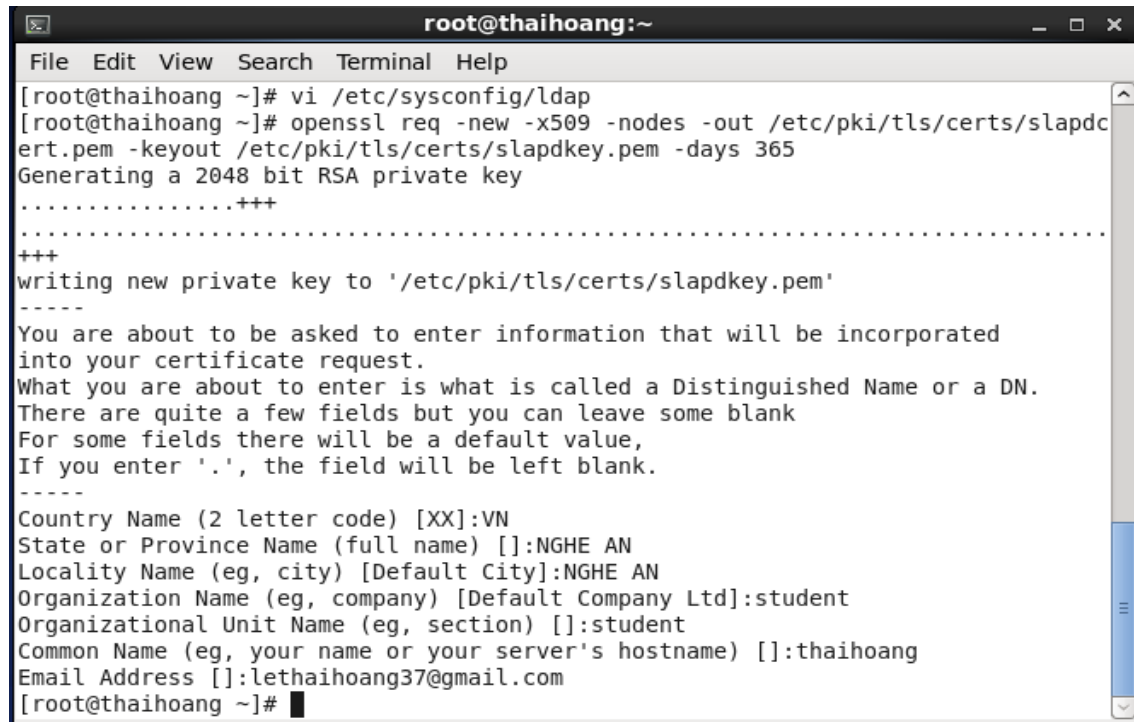
Cài đặt OpenLDAP

Bước 2: Sau khi cài đặt hoàn thành, mở file cấu hình tổng thể của openldap server để xem các thông tin cấu hình chính. Thực hiện câu lệnh: `# vi /etc/openldap/slapd.d/cn=config/olcDatabase=\{2\}bdb.ldif`, để cấu hình LDAP cho hệ thống.

```
root@thaihoang:~  
File Edit View Search Terminal Help  
olcDbShmKey: 0  
olcDbCacheFree: 1  
olcDbDnCacheSize: 0  
structuralObjectClass: olcBdbConfig  
entryUUID: 4ec69ec2-020d-1034-82b5-b92d6dbb102e  
creatorsName: cn=config  
createTimestamp: 20141116185124Z  
entryCSN: 20141116185124.334997Z#000000#000#000000  
modifiersName: cn=config  
modifyTimestamp: 20141116185124Z  
olcRootPW: {SSHA}jtTlwqWA87xidcwGBioJpuait1RXY+qv  
olcTLSCertificateFile: /etc/pki/tls/certs/slapdcert.pem  
olcTLSCertificateKeyFile: /etc/pki/tls/certs/slapdkey.pem  
olcAccess: to attrs=userPassword  
by self write  
by anonymous auth  
by dn.base="cn=Manager,dc=thaihoang,dc=com" write  
by * none  
olcAccess: to *  
by self write  
by dn.base="cn=Manager,dc=thaihoang,dc=com" write  
by * read
```

Cấu hình file ldap.conf.

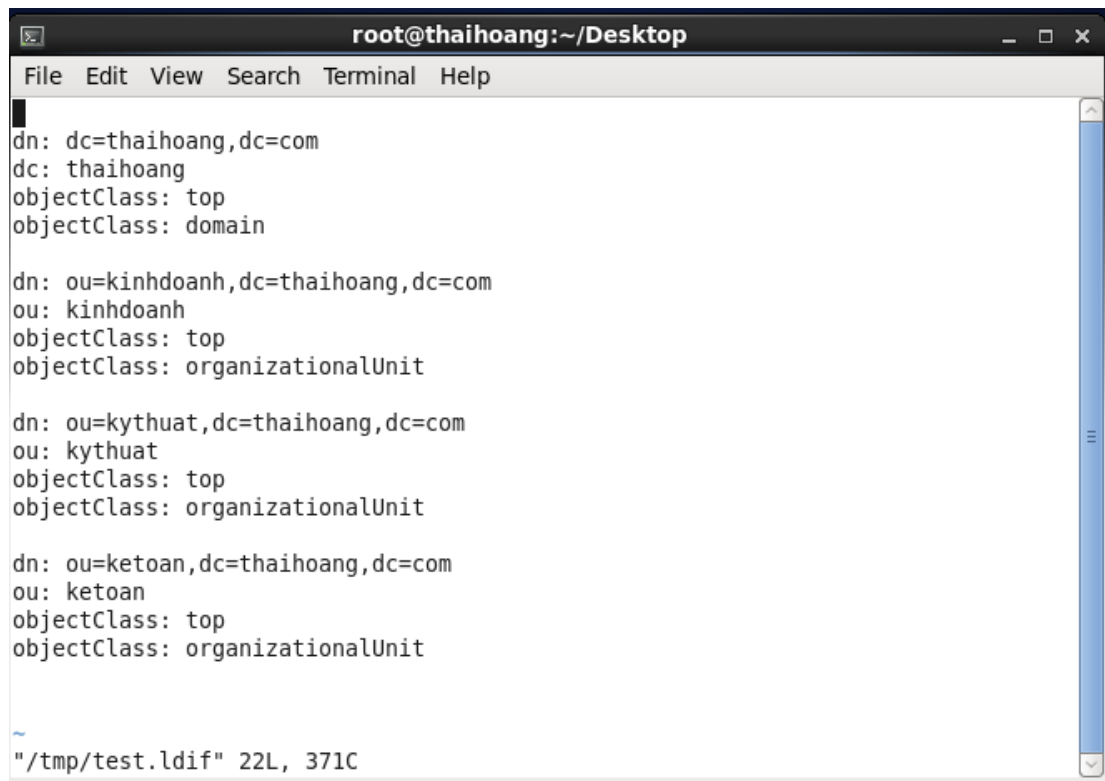
Bước 3: Tạo LDAP Database và tạo file Certificate



```
root@thaihoang:~  
File Edit View Search Terminal Help  
[root@thaihoang ~]# vi /etc/sysconfig/ldap  
[root@thaihoang ~]# openssl req -new -x509 -nodes -out /etc/pki/tls/certs/slapdcert.pem -keyout /etc/pki/tls/certs/slapdkey.pem -days 365  
Generating a 2048 bit RSA private key  
.....+++  
.....  
+++  
writing new private key to '/etc/pki/tls/certs/slapdkey.pem'  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [XX]:VN  
State or Province Name (full name) []:NGHE AN  
Locality Name (eg, city) [Default City]:NGHE AN  
Organization Name (eg, company) [Default Company Ltd]:student  
Organizational Unit Name (eg, section) []:student  
Common Name (eg, your name or your server's hostname) []:thaihoang  
Email Address []:lethaihoang37@gmail.com  
[root@thaihoang ~]#
```

Tạo LDAP Database và tạo file Certificate

Bước 4: Tạo file test.ldif với nội dung như sau:



```
root@thaihoang:~/Desktop  
File Edit View Search Terminal Help  
dn: dc=thaihoang,dc=com  
dc: thaihoang  
objectClass: top  
objectClass: domain  
  
dn: ou=kinhdoanh,dc=thaihoang,dc=com  
ou: kinhdoanh  
objectClass: top  
objectClass: organizationalUnit  
  
dn: ou=kythuat,dc=thaihoang,dc=com  
ou: kythuat  
objectClass: top  
objectClass: organizationalUnit  
  
dn: ou=ketoan,dc=thaihoang,dc=com  
ou: ketoan  
objectClass: top  
objectClass: organizationalUnit  
  
~/  
"/tmp/test.ldif" 22L, 371C
```

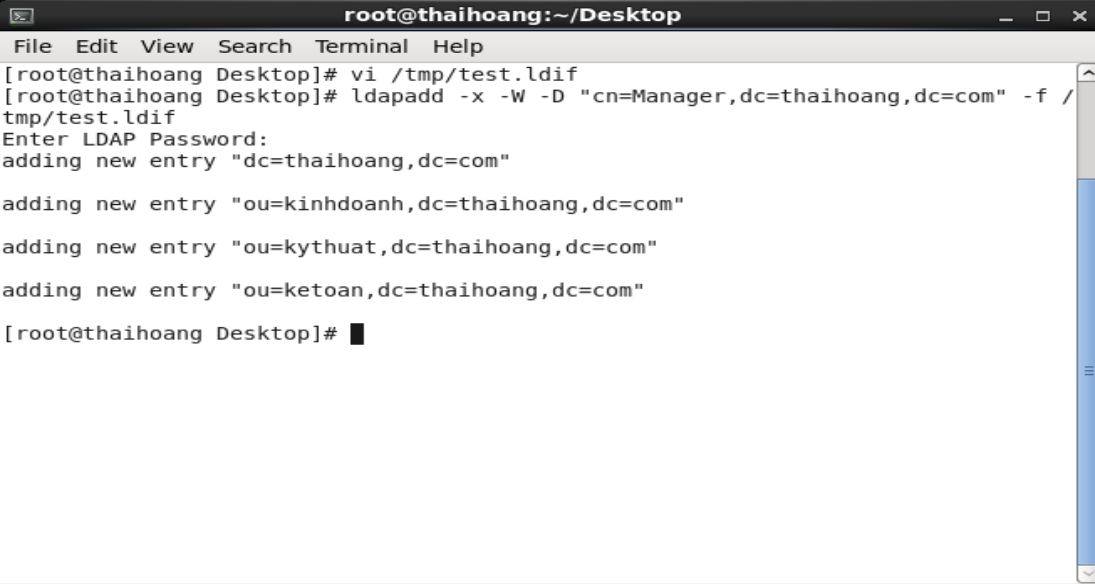
Tạo file test.ldif

Bước 5: Thực hiện import file *test.ldif* vào CSDL của LDAP

```
# ldapadd -x -W -D "cn=Manager,dc=thaihoang,dc=com" -f test.ldif
```

Nhập password ldap

Thành công sẽ có các thông báo trả về như sau:



```
root@thaihoang:~/Desktop
File Edit View Search Terminal Help
[root@thaihoang Desktop]# vi /tmp/test.ldif
[root@thaihoang Desktop]# ldapadd -x -W -D "cn=Manager,dc=thaihoang,dc=com" -f /
tmp/test.ldif
Enter LDAP Password:
adding new entry "dc=thaihoang,dc=com"

adding new entry "ou=kinhdoanh,dc=thaihoang,dc=com"
adding new entry "ou=kythuat,dc=thaihoang,dc=com"
adding new entry "ou=ketoan,dc=thaihoang,dc=com"
[root@thaihoang Desktop]#
```

Import file test.ldif vào CSDL của LDAP

CHƯƠNG II

TRIỂN KHAI HỆ THỐNG MẠNG TRÊN HỆ ĐIỀU HÀNH CENTOS 6.5

2.1. Giới thiệu về đơn vị

Công ty Thái Hoàng - là một công ty kinh doanh các mặt hàng về máy tính và linh kiện điện tử với quy mô nhỏ. Công ty thực hiện cung cấp máy tính và các thiết bị cho các trường học và người tiêu dùng trên toàn huyện.

2.2. Tiếp cận đơn vị

Sau khi em đến công ty khảo sát và tìm hiểu cơ sở hạ tầng của đơn vị đã nắm được khá rõ về hệ thống mạng của đơn vị. Đơn vị gồm 2 tầng: tầng 1 trưng bày sản phẩm máy tính và các máy tính và phòng kỹ thuật, tầng 2 có phòng nhân viên và phòng giám đốc. Hệ thống mạng ở các khu được triển khai như sau:

- Tầng 1: quầy thanh toán gồm 4 máy tính và 3 máy in, phòng kỹ thuật 8 máy tính.
- Tầng 2: phòng giám đốc 2 máy tính và 1 máy in, phòng kế toán 5 máy tính và 2 máy in, phòng kinh doanh 10 máy tính và 1 máy in, phòng họp 2 máy tính.

Công ty thuê 1 đường truyền Internet từ nhà cung cấp FTP.

2.3. Ưu – nhược điểm của hệ thống cũ Windows

- Ưu điểm

Công ty sử dụng hệ điều hành Windows, các dịch vụ dễ cấu hình và quản lý, tốc độ mạng cao.

- Nhược điểm

Với tình hình kinh tế hiện nay đang trong giai đoạn khủng hoảng về kinh tế thì với hệ thống mạng như thế này công ty sẽ mất 1 khoản chi phí tương đối lớn ảnh hưởng đến doanh thu cho công ty, bên cạnh đó vấn đề bảo mật dữ liệu là không cao. Vì vậy, cần phải có chiến lược phát triển mà vẫn đảm bảo được doanh thu, lợi nhuận cho công ty.

2.4. Phân tích các yêu cầu từ phía đơn vị và chọn cách cài đặt cho hệ thống.

2.4.1. Yêu cầu từ phía đơn vị

Chuyển hệ thống mạng từ Windows sang Linux phải đảm bảo các yêu cầu sau:

- Hệ thống mạng phải được bảo mật về dữ liệu
- Tốc độ truy cập phải cao.
- Chi phí thấp, dễ bảo trì và sửa chữa.

- Quản lý tập trung được người dùng.

2.4.2. Yêu cầu về thiết kế

Do công ty đã có hệ thống mạng và chỉ chuyển hệ thống mạng từ sử dụng hệ điều hành Windows sang Linux nên mô hình hệ thống mạng vẫn giữ nguyên, thực hiện cài đặt và cấu hình cho các máy trong công ty trên hệ điều hành Linux và triển khai các dịch vụ mạng cần thiết cho công ty cũng như thực hiện yêu cầu quản lý tập trung người dùng và bảo mật dữ liệu cho công ty.

Với mô hình doanh nghiệp vừa và nhỏ, để xây được một hệ thống mạng cục bộ phục vụ hầu hết các công việc kinh doanh, đảm bảo an toàn và chi phí không tốn kém, cần có các dịch vụ sau:

- DNS primary server để phân giải tên miền nội bộ.
- DHCP server để cấp địa chỉ IP cho các host.
- Dịch vụ LDAP để chứng thực tập trung cho các users.
- Webserver để phục vụ trang web giới thiệu quảng bá về công ty.
- FTP server để trao đổi file.
- Dịch vụ SAMBA để chia sẻ file trong mạng cục bộ giữa các clients trong hệ thống.

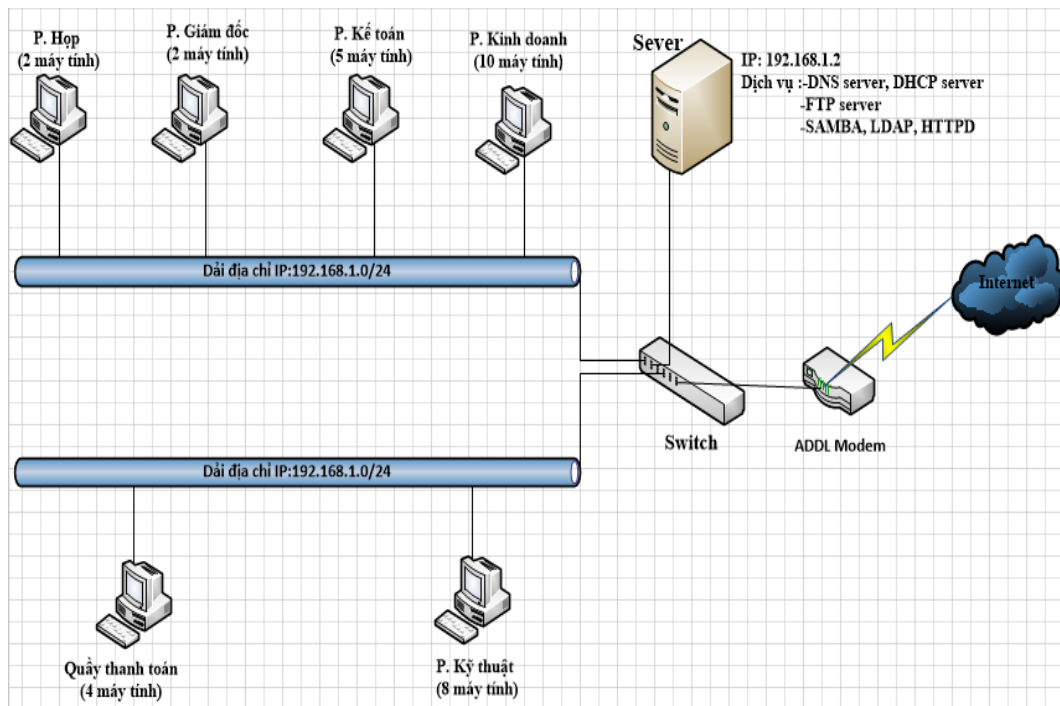
2.5. Triển khai hệ thống mạng trên hệ điều hành Linux cho công ty Thái Hoàng

2.5.1. Mô hình triển khai hệ thống mạng trên hệ điều hành CentOS 6.5

Dựa vào những yêu cầu trên, em đã thực hiện cài đặt như sau:

- Máy server cài hệ điều hành Linux bản phân phối CentOS 6.5 với địa chỉ 192.168.1.2/24
- Dịch vụ DNS cài trên máy chủ: cấu hình phân giải tên miền thaihoang.com
- Dịch vụ SAMBA cung cấp 2 nhóm tài khoản: Nhanvien và Giamdoc
- Dịch vụ DHCP với: range 192.168.1.10 192.168.1.100
Netmask 255.255.255.0
Gateway 192.168.1.1
- Mạng cục bộ chứa các client có dải địa chỉ: 192.168.1.0/24
- Dịch vụ FTP chia sẻ dữ liệu.
- Dịch vụ LDAP chứng thực tập trung các user.

Mô hình mạng như sau:



Mô hình mạng công ty Thái Hoàng.

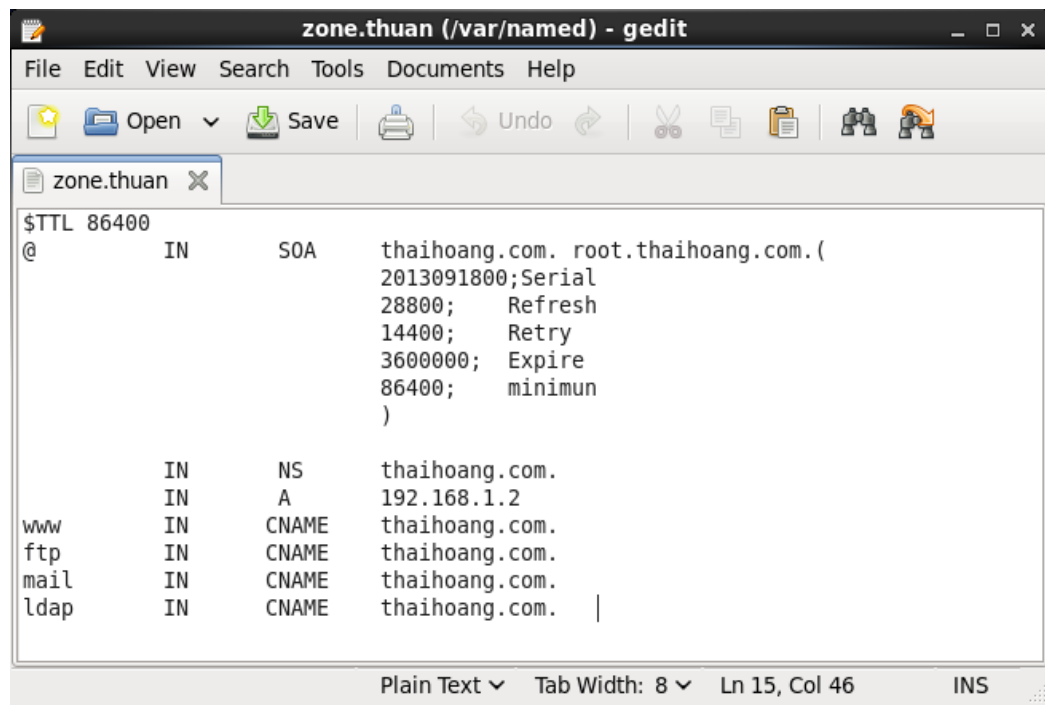
2.5.2. Cài đặt và cấu hình cho hệ thống

Theo sơ đồ trên, hệ thống mạng có 32 nút mạng, ta sử dụng lớp C để đặt địa chỉ IP cho các máy trạm và thực hiện cài đặt các dịch vụ.

- Cài đặt máy chủ với hệ điều hành Linux bản phân phối CentOS 6.5.
- Dịch vụ DNS phân giải tên miền *thaihoang.com*

```
root@thaihoang:~  
File Edit View Search Terminal Help  
};  
logging {  
    channel default_debug {  
        file "data/named.run";  
        severity dynamic;  
    };  
};  
zone "thaihoang.com" IN {  
    type master;  
    file "zone.thuan";  
    allow-update {none};  
};  
zone "1.168.192.in-addr.arpa" IN {  
    type master;  
    file "zone.nghich";  
    allow-update {none};  
};  
include "/etc/named.rfc1912.zones";  
include "/etc/named.root.key";  
-- INSERT --
```

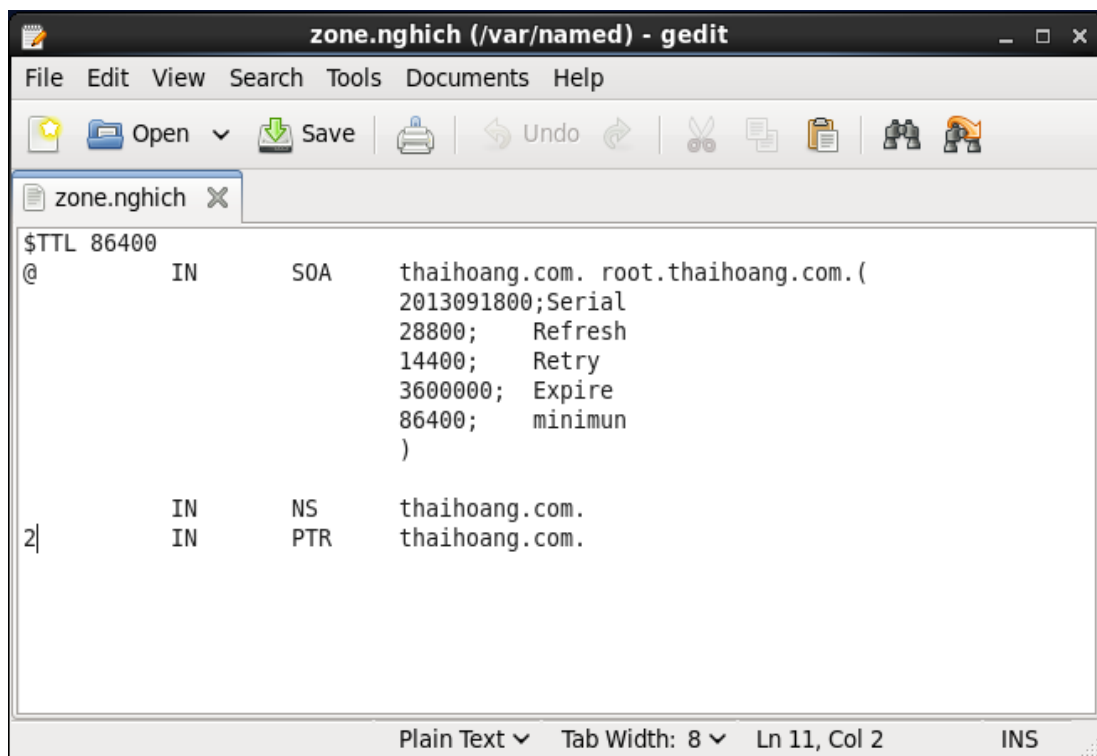
Cấu hình file named.conf



```
$TTL 86400
@      IN      SOA      thaihoang.com. root.thaihoang.com. (
                                2013091800;Serial
                                28800;  Refresh
                                14400;  Retry
                                3600000; Expire
                                86400;   minimum
                                )

      IN      NS       thaihoang.com.
      IN      A        192.168.1.2
www     IN      CNAME   thaihoang.com.
ftp     IN      CNAME   thaihoang.com.
mail    IN      CNAME   thaihoang.com.
ldap    IN      CNAME   thaihoang.com.
```

Cấu hình file phân giải thuận



```
$TTL 86400
@      IN      SOA      thaihoang.com. root.thaihoang.com. (
                                2013091800;Serial
                                28800;  Refresh
                                14400;  Retry
                                3600000; Expire
                                86400;   minimum
                                )

      IN      NS       thaihoang.com.
2|      IN      PTR     thaihoang.com.
```

Cấu hình file phân giải nghịch

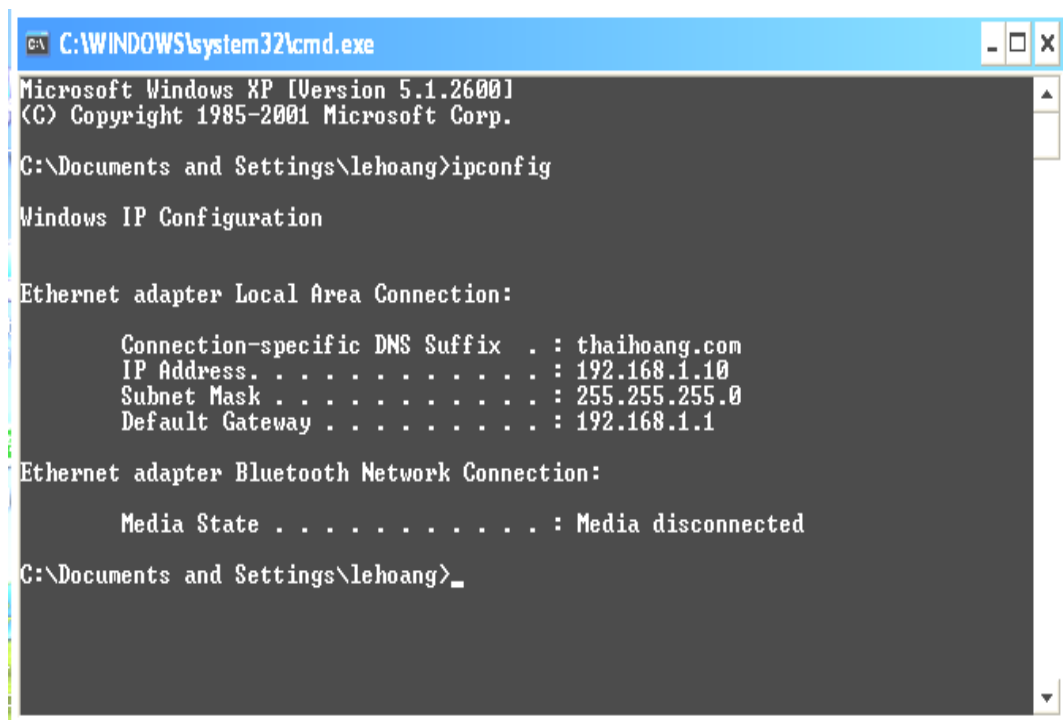
```
root@thaihoang:~  
File Edit View Search Terminal Help  
[root@thaihoang ~]# vi /etc/named.conf  
[root@thaihoang ~]# gedit /var/named/zone.thuan  
[root@thaihoang ~]# gedit /var/named/zone.ngnich  
[root@thaihoang ~]# service named start  
Generating /etc/rndc.key:           [ OK ]  
Starting named:                     [ OK ]  
[root@thaihoang ~]# chkconfig named on  
[root@thaihoang ~]# nslookup thaihoang.com  
Server:      192.168.1.2  
Address:     192.168.1.2#53  
  
Name:   thaihoang.com  
Address: 192.168.1.2  
  
[root@thaihoang ~]# nslookup 192.168.1.2  
Server:      192.168.1.2  
Address:     192.168.1.2#53  
  
2.1.168.192.in-addr.arpa      name = thaihoang.com.  
  
[root@thaihoang ~]# █
```

Kiểm tra dịch vụ DNS

- Dịch vụ DHCP cấp phát địa chỉ IP cho các máy client trong công ty.

```
root@thaihoang:~  
File Edit View Search Terminal Help  
# This declaration allows BOOTP clients to get dynamic addresses,  
# which we don't really recommend.  
  
subnet 10.254.239.32 netmask 255.255.255.224 {  
    range dynamic-bootp 10.254.239.40 10.254.239.60;  
    option broadcast-address 10.254.239.31;  
    option routers rtr-239-32-1.example.org;  
}  
  
# A slightly different configuration for an internal subnet.  
subnet 192.168.1.0 netmask 255.255.255.0 {  
    range 192.168.1.10 192.168.1.100;  
    option domain-name-servers 192.168.1.2;  
    option domain-name "thaihoang.com";  
    option routers 192.168.1.1;  
    option broadcast-address 192.168.1.255;  
    default-lease-time 600;  
    max-lease-time 7200;  
}  
  
# Hosts which require special configuration options can be listed in  
# host statements.  If no address is specified, the address will be  
# allocated dynamically (if possible), but the host-specific information  
-- INSERT --
```

File cấu hình dhcp



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\lehoang>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : thaihoang.com
    IP Address. . . . . : 192.168.1.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

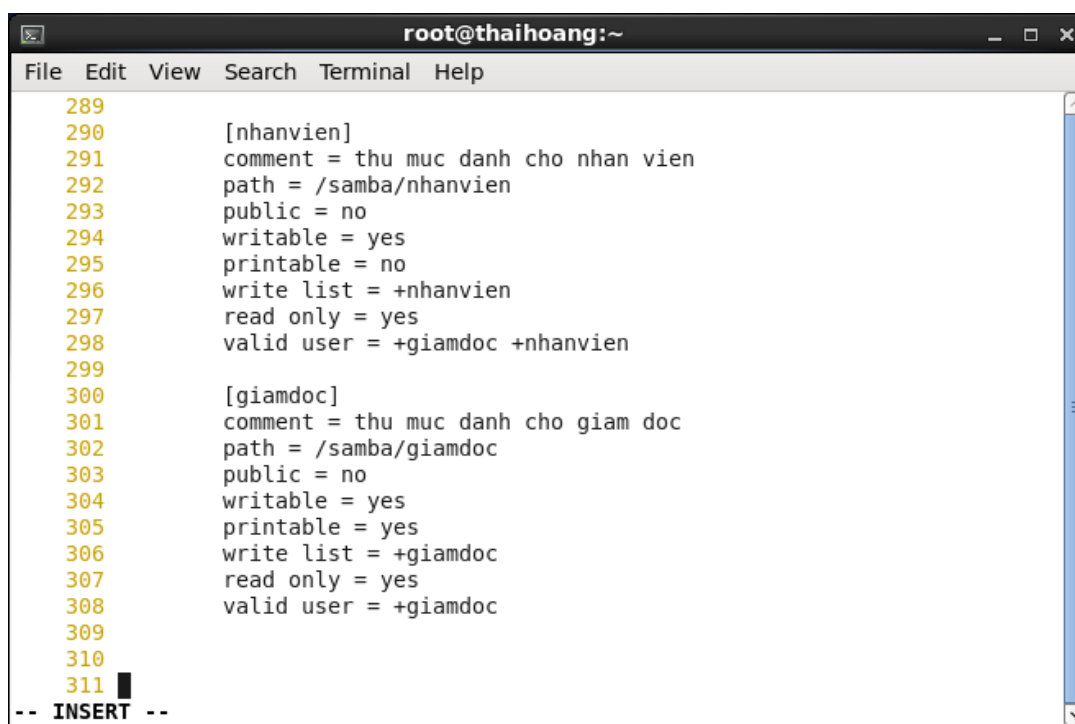
Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected

C:\Documents and Settings\lehoang>
```

Máy client nhận được địa chỉ IP cấp phát từ server.

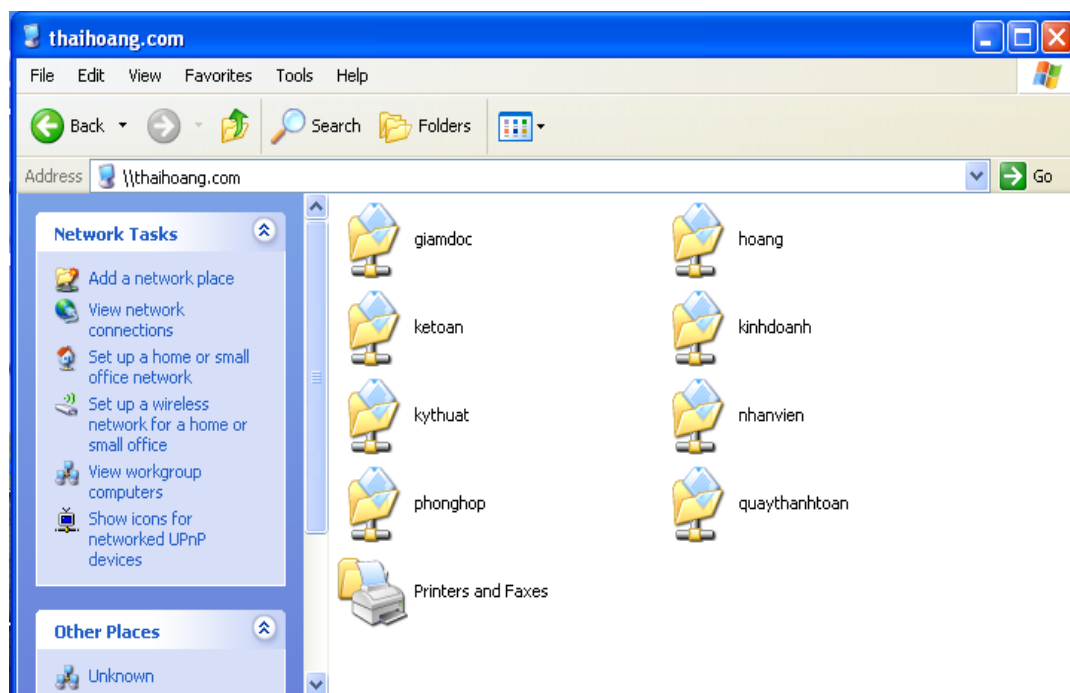
- Dịch vụ SAMBA chia sẻ tài nguyên.



```
root@thaihoang:~
File Edit View Search Terminal Help

289
290     [nhanvien]
291     comment = thu muc danh cho nhan vien
292     path = /samba/nhanvien
293     public = no
294     writable = yes
295     printable = no
296     write list = +nhanvien
297     read only = yes
298     valid user = +giamdoc +nhanvien
299
300     [giamdoc]
301     comment = thu muc danh cho giam doc
302     path = /samba/giamdoc
303     public = no
304     writable = yes
305     printable = yes
306     write list = +giamdoc
307     read only = yes
308     valid user = +giamdoc
309
310
311
-- INSERT --
```

Cấu hình SAMBA

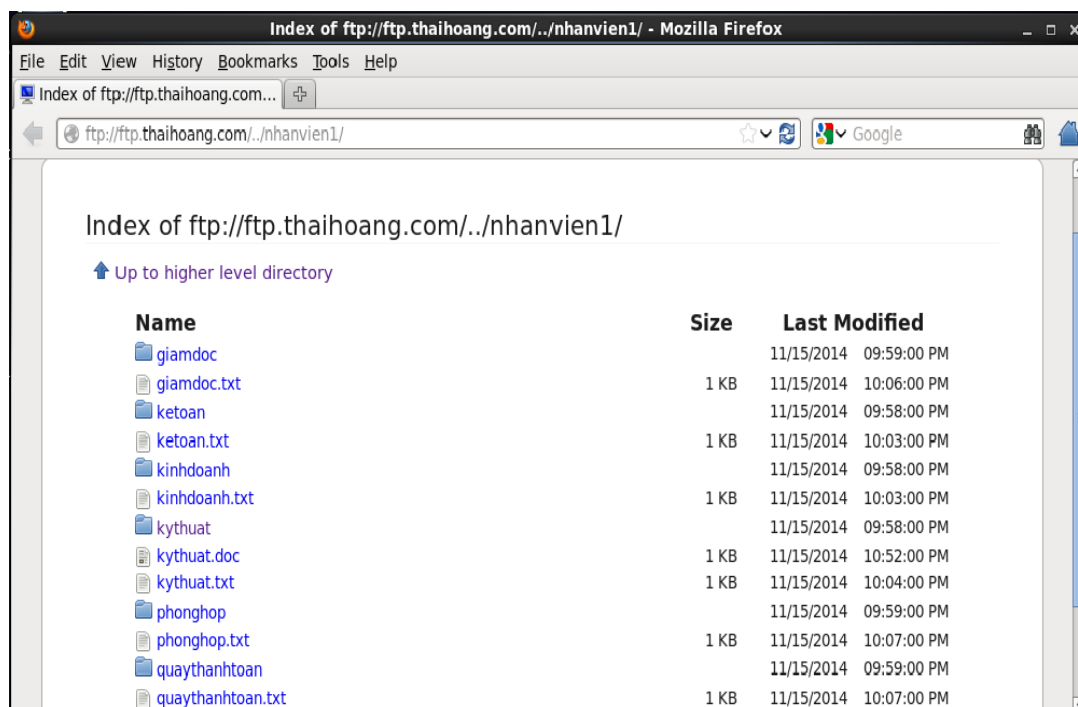


Kiểm tra dịch vụ SAMBA

- Dịch vụ FTP chia sẻ dữ liệu.

```
root@thaihoang:~  
File Edit View Search Terminal Help  
[root@thaihoang ~]# ftp 192.168.1.2  
Connected to 192.168.1.2 (192.168.1.2).  
220 (vsFTPD 2.2.2)  
Name (192.168.1.2:root): nhanvien1  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> exit  
221 Goodbye.  
[root@thaihoang ~]# ftp 192.168.1.2  
Connected to 192.168.1.2 (192.168.1.2).  
220 (vsFTPD 2.2.2)  
Name (192.168.1.2:root): nhanvien2  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> exit  
221 Goodbye.  
[root@thaihoang ~]#
```

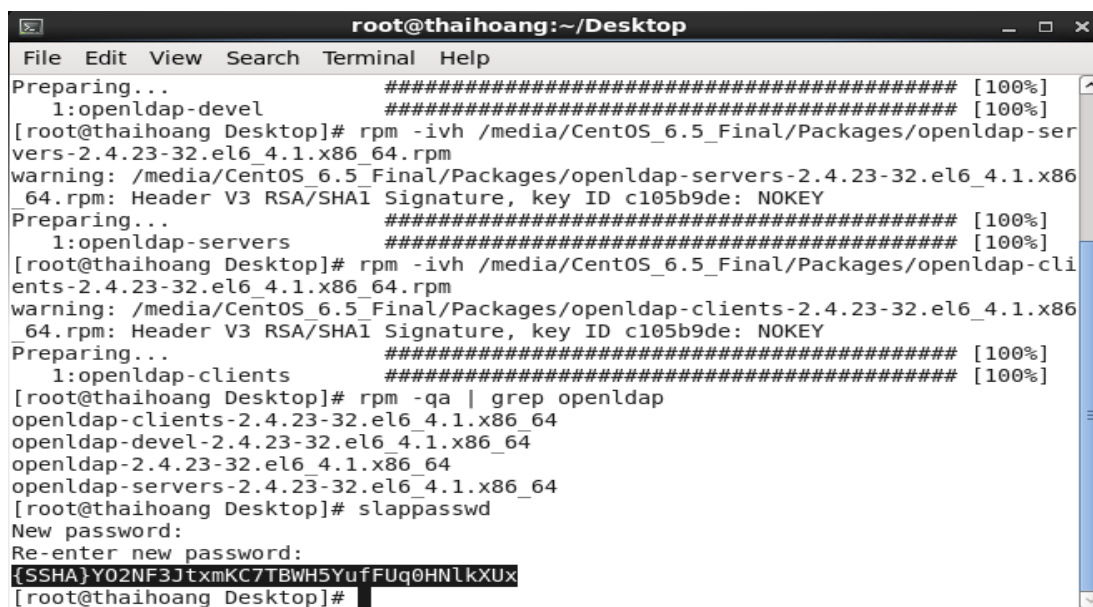
Cấu hình FTP thành công



Kiểm tra dịch vụ FTP

- Dịch vụ DLAP chứng thực tập trung các user.

Cài đặt Openldap và tạo mật khẩu được mã hóa sử dụng cho LDAP bằng lệnh: #
slappasswd.



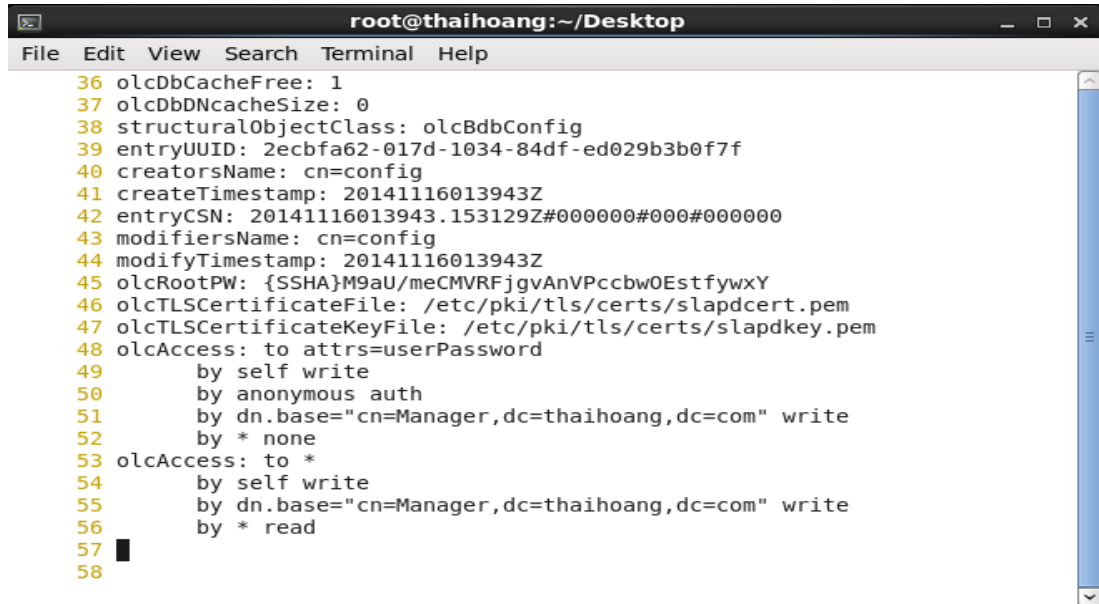
Cài đặt Openldap

- **Cấu hình LDAP**

- Mở file `olcDatabase={2}bdb.ldif`:

vi /etc/openldap/slapd.d/cn=config/olcDatabase={2}bdb.ldif

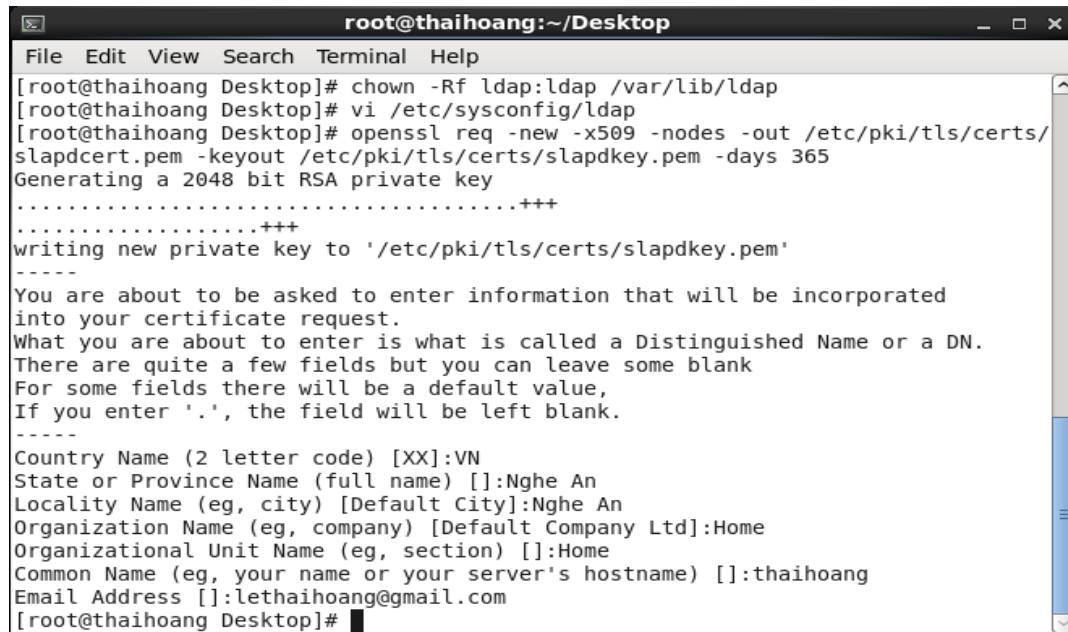
- Ta sửa các giá trị cần thiết trong file này như tên domain (tên domain của mình là: thaihoang.com)



```
root@thaihoang:~/Desktop
File Edit View Search Terminal Help
36 olcDbCacheFree: 1
37 olcDbDnCacheSize: 0
38 structuralObjectClass: olcBdbConfig
39 entryUUID: 2ecbfa62-017d-1034-84df-ed029b3b0f7f
40 creatorsName: cn=config
41 createTimestamp: 20141116013943Z
42 entryCSN: 20141116013943.153129Z#000000#000#000000
43 modifiersName: cn=config
44 modifyTimestamp: 20141116013943Z
45 olcRootPW: {SSHA}M9aU/meCMVRFjgvAnVPccbw0EstfywxY
46 olcTLSCertificateFile: /etc/pki/tls/certs/slapdcert.pem
47 olcTLSCertificateKeyFile: /etc/pki/tls/certs/slapdkey.pem
48 olcAccess: to attrs=userPassword
49     by self write
50     by anonymous auth
51     by dn.base="cn=Manager,dc=thaihoang,dc=com" write
52     by * none
53 olcAccess: to *
54     by self write
55     by dn.base="cn=Manager,dc=thaihoang,dc=com" write
56     by * read
57
58
```

File olcDatabase = {2}bdb.ldif

- **Tạo LDAP Database và tạo file Certificate**



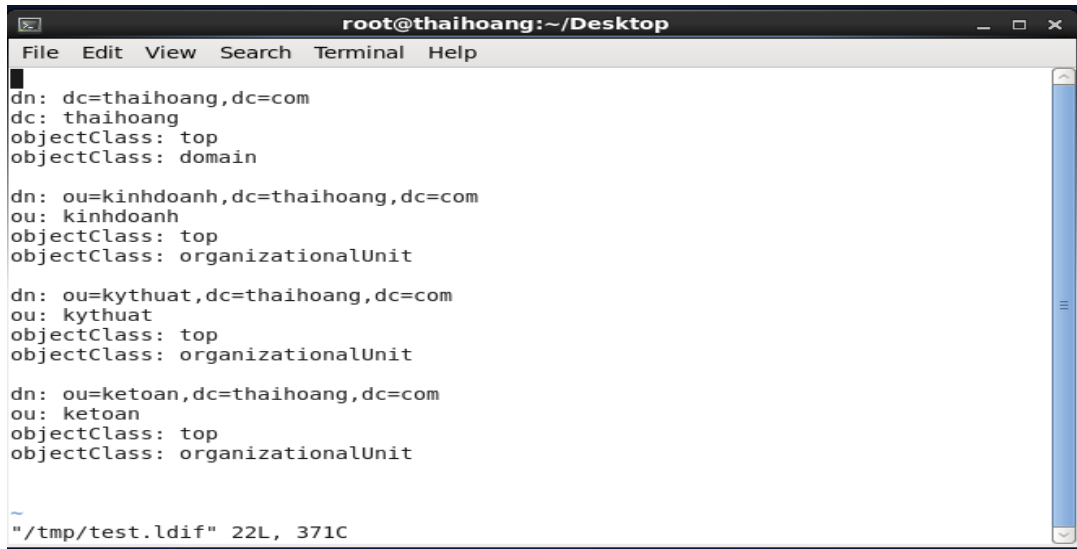
```
root@thaihoang:~/Desktop
File Edit View Search Terminal Help
[root@thaihoang Desktop]# chown -Rf ldap:ldap /var/lib/ldap
[root@thaihoang Desktop]# vi /etc/sysconfig/ldap
[root@thaihoang Desktop]# openssl req -new -x509 -out /etc/pki/tls/certs/slapdcert.pem -keyout /etc/pki/tls/certs/slapdkey.pem -days 365
Generating a 2048 bit RSA private key
.....+++
writing new private key to '/etc/pki/tls/certs/slapdkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:VN
State or Province Name (full name) []:Nghe An
Locality Name (eg, city) [Default City]:Nghe An
Organization Name (eg, company) [Default Company Ltd]:Home
Organizational Unit Name (eg, section) []:Home
Common Name (eg, your name or your server's hostname) []:thaihoang
Email Address []:lethaihoang@gmail.com
[root@thaihoang Desktop]#
```

Tạo file Certificate

-

- Tạo Base Domain cho LDAP Server

Tạo file *test.ldif* với nội dung như sau:



```
root@thaihoang:~/Desktop
File Edit View Search Terminal Help
dn: dc=thaihoang,dc=com
dc: thaihoang
objectClass: top
objectClass: domain

dn: ou=kinhdoanh,dc=thaihoang,dc=com
ou: kinhdoanh
objectClass: top
objectClass: organizationalUnit

dn: ou=kythuat,dc=thaihoang,dc=com
ou: kythuat
objectClass: top
objectClass: organizationalUnit

dn: ou=ketoan,dc=thaihoang,dc=com
ou: ketoan
objectClass: top
objectClass: organizationalUnit

~/tmp/test.ldif" 22L, 371C
```

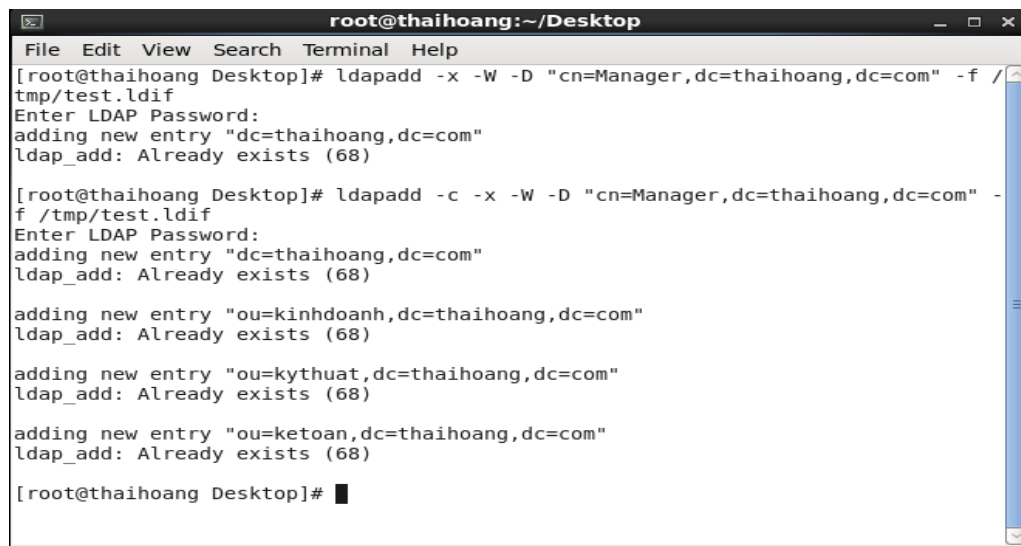
File test.ldif

- Thực hiện import file test.ldif vào CSDL của LDAP

```
# ldapadd -x -W -D "cn=Manager,dc=thaihoang,dc=com" -f test.ldif
```

Nhập password ldap

Thành công sẽ có các thông báo trả về như sau



```
root@thaihoang:~/Desktop
File Edit View Search Terminal Help
[root@thaihoang Desktop]# ldapadd -x -W -D "cn=Manager,dc=thaihoang,dc=com" -f /tmp/test.ldif
Enter LDAP Password:
adding new entry "dc=thaihoang,dc=com"
ldap_add: Already exists (68)

[root@thaihoang Desktop]# ldapadd -c -x -W -D "cn=Manager,dc=thaihoang,dc=com" -f /tmp/test.ldif
Enter LDAP Password:
adding new entry "dc=thaihoang,dc=com"
ldap_add: Already exists (68)

adding new entry "ou=kinhdoanh,dc=thaihoang,dc=com"
ldap_add: Already exists (68)

adding new entry "ou=kythuat,dc=thaihoang,dc=com"
ldap_add: Already exists (68)

adding new entry "ou=ketoan,dc=thaihoang,dc=com"
ldap_add: Already exists (68)

[root@thaihoang Desktop]#
```

Import test.ldif vào CSDL của LDAP

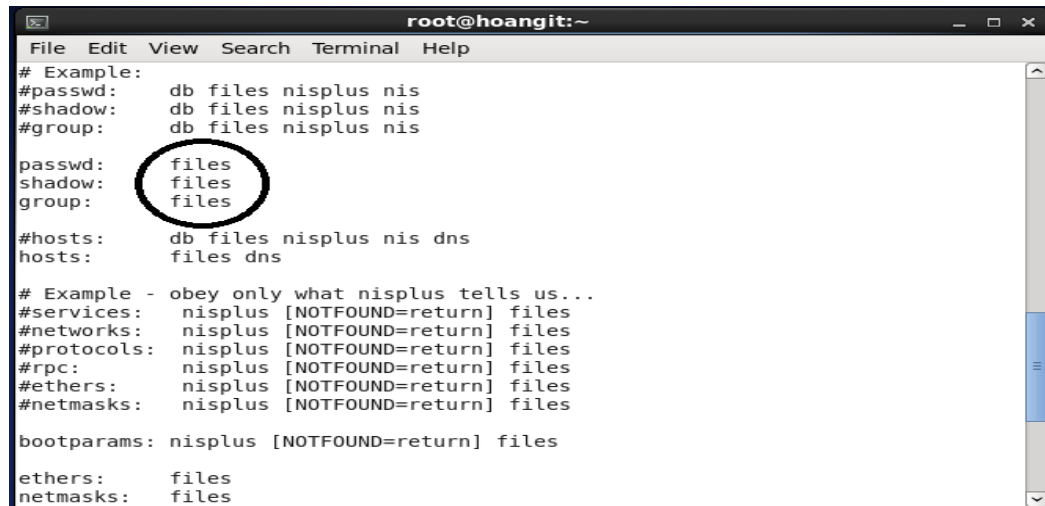
Tạo một *user* có tên *ldapuser*, thuộc nhóm *users* và đặt *password* cho *user* này.

Sau đó lấy thông tin về *ldapuser* từ file */etc/passwd* và ghi ra file

/tmp/ldapuser.passwd và dùng script *migrate_passwd.pl* để tạo file LDIF từ file */tmp/ldapuser.passwd*.

- Cấu hình Client để xác thực qua LDAP Server

Kiểm tra file `/etc/nsswitch.conf` và các file trong thư mục `/etc/pam.d/` để thấy việc tìm kiếm thông tin người dùng (User Information) và xác thực người dùng (Authentication) chưa được xác thực để sử dụng cho LDAP.



```
root@hoangit:~  
File Edit View Search Terminal Help  
# Example:  
#passwd:      db files nisplus nis  
#shadow:      db files nisplus nis  
#group:        db files nisplus nis  
  
passwd:       files  
shadow:       files  
group:         files  
  
#hosts:        db files nisplus nis dns  
hosts:         files dns  
  
# Example - obey only what nisplus tells us...  
#services:     nisplus [NOTFOUND=return] files  
#networks:     nisplus [NOTFOUND=return] files  
#protocols:    nisplus [NOTFOUND=return] files  
#rpc:          nisplus [NOTFOUND=return] files  
#ethers:       nisplus [NOTFOUND=return] files  
#netmasks:    nisplus [NOTFOUND=return] files  
  
bootparams:   nisplus [NOTFOUND=return] files  
  
ethers:       files  
netmasks:    files
```

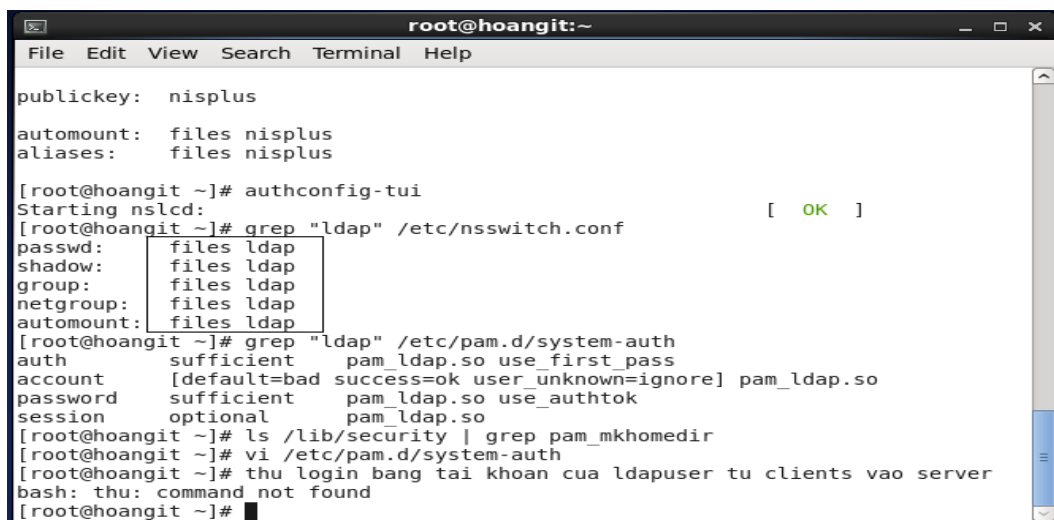
Người dùng chưa được xác thực để sử dụng cho LDAP.

- Ta cài đặt gói (nss-pam-ldapd) bằng lệnh: `# yum install nss-pam-ldapd`

Sau khi quá trình cài đặt kết thúc ta vào lại giao diện thiết lập LDAP, nhập thông tin về LDAP Server và Base DN sau đó chọn OK. Kiểm tra lại file: `/etc/nsswitch.conf` và file `/etc/pam.d/system-auth` để thấy việc tìm kiếm thông tin người dùng và xác thực người dùng đã được cấu hình để sử dụng LDAP

`grep "ldap" /etc/nsswitch.conf`

`grep "ldap" /etc/pam.d/system-auth`



```
root@hoangit:~  
File Edit View Search Terminal Help  
  
publickey:   nisplus  
automount:   files nisplus  
aliases:     files nisplus  
  
[root@hoangit ~]# authconfig-tui  
Starting nslcd: [ OK ]  
[root@hoangit ~]# grep "ldap" /etc/nsswitch.conf  
passwd:      files ldap  
shadow:      files ldap  
group:        files ldap  
netgroup:    files ldap  
automount:   files ldap  
[root@hoangit ~]# grep "ldap" /etc/pam.d/system-auth  
auth        sufficient      pam_ldap.so use_first_pass  
account     [default=bad  success=ok user_unknown=ignore] pam_ldap.so  
password    sufficient      pam_ldap.so use_authtok  
session     optional          pam_ldap.so  
[root@hoangit ~]# ls /lib/security | grep pam_mkhomedir  
[root@hoangit ~]# vi /etc/pam.d/system-auth  
[root@hoangit ~]# thu login bằng tài khoản của ldapuser từ clients vào server  
bash: thu: command not found  
[root@hoangit ~]#
```

Người dùng đã được xác thực để sử dụng cho LDAP.

KẾT LUẬN

Có thể thấy hướng phát triển tin học ở nước ta hiện nay, đối với người dùng thông thường việc sử dụng linux vẫn là một điều khó, nhưng đối với những người nghiên cứu và tìm hiểu việc sử dụng hệ điều hành mã nguồn mở là một điều kiện tốt để nâng cao sự hiểu biết của mình. Qua quá trình tìm hiểu và triển khai các dịch vụ mạng DNS, DHCP, SAMBA, FTP, Webserver, LDAP trên Linux em đã đạt được một số điểm sau:

- Đã hoàn thành tìm hiểu lý thuyết về các dịch vụ mạng trên Linux, nắm được kiến thức về hệ điều hành Linux.
- Đã cài đặt và cấu hình thành công các dịch vụ mạng trên Linux theo mô hình mạng của công ty.

Tuy nhiên trong quá trình tìm hiểu, em đã gặp một số khó khăn như thiếu kiến thức về lập trình và hệ điều hành Linux cũng như kiến thức về an toàn bảo mật thông tin đã khiến em mất khá nhiều thời gian tìm hiểu, nghiên cứu và giải quyết vấn đề. Ngoài ra việc thực hiện chỉ là trên mô hình ảo hoá, không có cơ sở hạ tầng thiết bị thực tế. Cũng chính vì các yếu tố đó đã dẫn đến những hạn chế trong đồ án như:

- Chưa đi sâu vào các dịch vụ, chưa phát triển được các dịch vụ mà chỉ mới dừng ở việc cài đặt và cấu hình.
- Chưa có các biện pháp bảo mật tối ưu cho hệ thống.

Nếu có điều kiện mở rộng đề tài cũng như các thiết bị cần thiết cho việc nghiên cứu, em sẽ tập trung nghiên cứu về các lỗi sự cố và tìm ra hướng khắc phục. Tiến tới sẽ triển khai các dịch vụ cài đặt trên Linux đáp ứng đầy đủ như windows như: DHCP server, DNS server, hệ thống chia sẻ tài nguyên Samba, hệ thống quản lý tập trung LDAP, webserve Apaches...trên các hệ thống thực tế và phát triển mang tính ổn định, bảo mật cao, cơ chế chia sẻ tài nguyên tốt.

TÀI LIỆU THAM KHẢO

- [1]. Vũ Xuân Thắng, *Giáo trình Hệ điều hành mã nguồn mở*, Trường Đại học Sư phạm kỹ thuật Hưng Yên, 2013.
- [2]. Các video hướng dẫn sử dụng hệ điều hành mã nguồn mở trên trang web www.youtube.com
- [3]. Nguồn tham khảo từ các trang web: www.nhatnghe.com
www.quantrimang.com, www.diendancongnghes.vn, www.gocit.com.