

R

TRUNG TÂM TIN HỌC VĂN PHÒNG UBND TP ĐÀ NẴNG

BÁO CÁO KHOA HỌC

Tên đề tài: Xây dựng và đánh giá hiệu quả triển khai hệ điều hành Linux trong khai thác và quản trị mạng LAN tại các Sở, ngành của thành phố Đà Nẵng.

Cơ quan chủ trì: Trung tâm Tin học - Văn phòng UBND thành phố Đà Nẵng

Chủ nhiệm đề tài: Tiến sĩ **Hoàng Quang Tuyền**

Phó chủ nhiệm đề tài: Cử nhân **Lâm Tùng Giang**

Thư ký đề tài: Cử nhân **Ngô Thị Hiền Trang**

Thời gian thực hiện: 12 tháng, từ tháng 06/2004 đến tháng 05/2005

Kinh phí đầu tư: 90.400.000 đồng

Tổ chức phối hợp nghiên cứu:

1. Văn phòng Thành uỷ
2. Sở Giáo dục
3. Sở Ngoại Vụ
4. Quận Hải Châu

Cá nhân phối hợp nghiên cứu:

1. Thiều Quang Đức
2. Nguyễn Hồng Ân
3. Võ Văn Luận
4. Nguyễn Chí Bình
5. Ngô Thị Hiền Trang
6. Nguyễn Ngọc Huế
7. Nguyễn Xuân Tú
8. Lê Ngọc Thành
9. Bùi Quốc Việt

LỜI CẢM ƠN

Hiện nay, Linux - một hệ điều hành mã nguồn mở - đang được sử dụng một cách rộng rãi, được đánh giá cao về độ ổn định, khả năng bảo mật, khả năng ứng dụng trong nhiều lĩnh vực và đặc biệt là có chi phí thấp, phù hợp với điều kiện của Việt Nam.

Việc triển khai nghiên cứu đề tài được thực hiện theo yêu cầu của Ban Điều hành Đề án 112 thành phố Đà Nẵng nhằm nghiên cứu và đưa ra các giải pháp ứng dụng hệ điều hành Linux phục vụ việc khai thác và quản trị mạng máy tính tại các đơn vị Sở, Ngành.

Là cơ quan thường trực của Ban Điều hành Đề án 112 thành phố Đà Nẵng, Trung tâm Tin học Văn phòng UBND thành phố Đà Nẵng được phân công nhận trách nhiệm khảo sát thực tế, nghiên cứu đưa ra các giải pháp ứng dụng hệ điều hành Linux, nhằm nâng cao hiệu quả sử dụng, tăng cường hệ thống an ninh mạng, đảm bảo sự hoạt động ổn định của hệ thống mạng, cũng như giúp cho cán bộ quản trị mạng các đơn vị làm quen với môi trường làm việc mới.

Trong quá trình thực hiện việc khảo sát và nghiên cứu, Ban Chủ nhiệm đề tài đã nhận được sự giúp đỡ quý báu của nhiều cơ quan: Ban Điều hành Đề án 112 thành phố Đà Nẵng, Văn phòng UBND thành phố, Văn phòng Thành Ủy, Sở Khoa học và Công nghệ, Sở Giáo dục Đào tạo, Sở Ngoại Vụ, UBND Quận Hải Châu, Trung tâm Công nghệ phần mềm,...

Ban chủ nhiệm đề tài cũng nhận được sự giúp đỡ, tham gia góp ý của Thạc sĩ Trần Văn Đông, cử nhân Hồ Phước Duy, kỹ sư Nguyễn Huy Minh,...

Nhờ những sự giúp đỡ đó, đến nay những yêu cầu đề tài đặt ra đã cơ bản hoàn thành. Nhân dịp này, chúng tôi xin chân thành cảm ơn các cơ quan, đơn vị và cá nhân đã giúp đỡ tận tình, đầy trách nhiệm cho Ban Chủ nhiệm trong suốt quá trình nghiên cứu và hoàn thiện đề tài.

Mặc dù có nhiều cố gắng, song những kết quả nghiên cứu còn cần tiếp tục sửa chữa, bổ sung. Rất mong được sự quan tâm, đóng góp ý kiến của các đơn vị, cá nhân giúp đỡ chúng tôi hoàn thiện nội dung đề tài, nhằm ứng dụng kết quả đề tài vào thực tế, đem lại hiệu quả cao nhất.

Đà Nẵng, tháng 06 năm 2005

Ban Chủ nhiệm Đề tài

MỤC LỤC

KÝ HIỆU TỪ VIẾT TẮT.....	7
MỞ ĐẦU	9
I. Giới thiệu vấn đề nghiên cứu	9
1. Sơ lược về Linux.....	9
2. Linux - xu thế, giải pháp mới cho các hệ thống thông tin	10
3. Nhu cầu triển khai nghiên cứu "giải pháp Linux"	13
II. Tóm tắt mục tiêu	13
III. Nội dung đối tượng và phạm vi nghiên cứu.....	14
1. Đối tượng nghiên cứu	14
2. Phạm vi nghiên cứu.....	14
IV. Tổng quan về lịch sử vấn đề nghiên cứu.....	14
1. Linux, các sản phẩm phần mềm nguồn mở tại Việt Nam.....	14
2. Ứng dụng hệ điều hành Linux trong khuôn khổ đề án 112 thành phố Đà Nẵng.....	15
V. Quan điểm lựa chọn vấn đề nghiên cứu	15
VI. Tóm tắt nội dung nghiên cứu	15
CHƯƠNG I : CƠ SỞ LÝ LUẬN	17
I. Mạng và hệ điều hành Linux.....	17
1. Linux - hệ điều hành linh hoạt	17
2. Linux - server quản lý tập tin và in ấn	17
3. Linux - server truyền thông.....	18
4. Linux - server cho WAN hoặc gateway.....	18
II. Mạng hỗn hợp	19
CHƯƠNG II: XÁC ĐỊNH PHƯƠNG PHÁP NGHIÊN CỨU.....	20
I. Cách tiếp cận, phương pháp nghiên cứu, kỹ thuật sẽ sử dụng.....	20
II. Nội dung nghiên cứu.....	21
1. Điều tra, đánh giá:.....	21
2. Nghiên cứu giải pháp kỹ thuật:.....	21
3. Thử nghiệm, đóng gói kết quả	22
CHƯƠNG III: TỔNG HỢP, ĐÁNH GIÁ KẾT QUẢ KHẢO SÁT.....	23
I. Số liệu khảo sát.....	23
1. Thông tin chung về đơn vị	23
2. Hệ điều hành mạng hiện sử dụng tại các đơn vị	23
3. Hệ điều hành mạng quen thuộc.....	23
4. Trình độ học vấn của chuyên viên quản trị mạng.....	23
5. Trình độ chuyên môn về CNTT của chuyên viên quản trị mạng	24
6. Các chứng chỉ CNTT của chuyên viên quản trị mạng.....	24

7. Nhiệm vụ quản trị mạng cụ thể.....	24
8. Kiểm nhiệm công tác khác.....	24
9. Hiểu biết về hệ điều hành Linux.....	25
10. Kiến thức về mã nguồn mở:.....	25
II. Phân tích kết quả khảo sát.....	25
1. Hạ tầng cơ sở:	25
2. Trình độ nhân lực công nghệ thông tin.....	26
3. Mức độ sử dụng hệ điều hành Linux	27
III. Đánh giá khả năng tiếp nhận và triển khai ứng dụng hệ điều hành Linux tại các đơn vị.....	27
CHƯƠNG IV: CÁC GIẢI PHÁP KỸ THUẬT	29
I. Tổng quan về giải pháp kỹ thuật	29
II. Giải pháp hệ điều hành : Cài đặt Mandrake Linux 10.0.....	29
1. Cài đặt ban đầu.....	29
2. Cài đặt các ứng dụng.....	30
III. Giải pháp cài đặt các dịch vụ trên máy chủ Linux.....	31
1. Giải pháp Web Server : Apache.....	31
2. Giải pháp Mail server : Qmail	33
3. Giải pháp DNS Server: BIND 9.3.....	35
IV. Giải pháp chia sẻ tài nguyên trên mạng : Samba	38
1. Nội dung nghiên cứu:.....	38
2. Kết quả đạt được:.....	39
V. Giải pháp an toàn, bảo mật thông tin trên mạng : sử dụng các phần mềm OpenLDAP, IPTables	40
1. Đặt vấn đề	40
2. Xác định giải pháp bảo mật thông tin trên mạng.....	41
3. Giải pháp dịch vụ thư mục : OpenLDAP.....	42
4. Giải pháp tường lửa : IPTables	45
5. Đánh giá kết quả thu được	50
VI. Giải pháp xây dựng các ứng dụng quản trị máy chủ Linux.....	50
1. Mục đích và yêu cầu	50
2. Lựa chọn giải pháp.....	50
3. Nội dung nghiên cứu.....	51
4. Kết quả đạt được	51
VII. Giải pháp xây dựng tài liệu phục vụ đào tạo	52
1. Mục tiêu	52
2. Tóm tắt nội dung tài liệu đào tạo	52
3. Kết quả thu được sau các buổi đào tạo	54
CHƯƠNG V: TRIỂN KHAI THỬ NGHIỆM.....	56

I. Mô hình máy chủ đơn lẻ	56
II. Mô hình 2 vùng.....	56
III. Mô hình 3 vùng	57
1. Vùng DMZ (Demilitarized Zone):	57
2. Vùng LAN (Local Area Network):	57
3. Vùng WAN (Wide Area Network), Internet:	57
IV. Chọn lựa mô hình mạng phù hợp.....	57
V. Thực tế triển khai tại các đơn vị thử nghiệm	58
1. Triển khai, cài đặt giải pháp tại UBND Quận Hải Châu.....	58
2. Triển khai, cài đặt giải pháp tại Văn phòng Sở Ngoại Vụ	60
3. Triển khai, cài đặt giải pháp tại Sở Giáo dục và Đào tạo.....	62
4. Triển khai, cài đặt giải pháp tại Văn phòng Thành Ủy	64
5. Triển khai, cài đặt giải pháp tại Văn phòng UBND thành phố	66
6. Tóm tắt nhận xét kết quả triển khai của các đơn vị sử dụng.....	68
KẾT LUẬN VÀ KIẾN NGHỊ.....	70
I. Kết luận	70
II. Kiến nghị	70
III. Đề xuất kế hoạch áp dụng kết quả nghiên cứu	71
1. Nội dung	71
2. Dự toán kinh phí	72
TÀI LIỆU THAM KHẢO.....	73
PHỤ LỤC	75

KÝ HIỆU TỪ VIẾT TẮT

STT	Viết tắt	Ý nghĩa	Ghi chú
1	ADSL	Asymmetric Digital Subscriber Line	
2	BASH	Bourne Again Shell	
3	BIND	Berkeley Internet Name Domain	
4	CNTT	Công nghệ thông tin	
5	DHCP	Dynamic Host Configuration Protocol	Giao thức cấu hình host động
6	DMZ	Demilitarized Zone	Vùng phi quân sự
7	DNS	Domain Name System	Hệ thống tên miền
8	E-Mail	Electronic mail	
9	FTP	File Transfer Protocol	
10	GPL	GNU General Public License	
11	HĐH	Hệ điều hành	
12	HTTP	HyperText Transfer Protocol	Giao thức truyền tải siêu văn bản
13	IMAP	Internet Mail/Message Access Protocol	Giao thức truy cập thư Internet
14	ISDN	Intergrated Services Digital Network	Mạng số các dịch vụ tích hợp
15	LAN	Local Area Network	
16	LDAP	Lighweight Directory Access Protocol	
17	MTA	Message Transfer Agent	Trạm truyền thông điệp
18	NAT	Network Address Translation	Chuyển đổi địa chỉ mạng
19	NFS	Network File System	Hệ thống tập tin mạng
20	NIS	Network Information System	Hệ thống thông tin mạng
21	NT	Network Technology	
22	OS	Operating System	Hệ điều hành
23	PC	Personal Computer	Máy tính cá nhân
24	POP3	Post Office Protocol	

25	PPP	Point-To-Point Protocol	
26	RPC	Remote Procedure Call	Gọi thủ tục từ xa
27	SHDSL	Single Pair High-speed Digital Subscriber Line	
28	SMB	Server Message Block	
29	SMTP	Simple Mail Transfer Protocol	Giao thức chuyển thư điện tử
30	SQL	Structured Query Language	Ngôn ngữ truy vấn có cấu trúc
31	SSL	Secure Sockets Layer	
32	TCP/IP	Transmission Control Protocol/Internet Protocol	
33	TLS	Transport Layer Security	
34	UBND	Ủy ban nhân dân	
35	UDP	User Datagram Protocol	
36	WAN	Wide Area Network	Mạng diện rộng

MỞ ĐẦU

I. Giới thiệu vấn đề nghiên cứu

1. Sơ lược về Linux

Phiên bản Linux đầu tiên do Linus Torwald, một người Phần Lan phát triển vào năm 1991 dựa trên mã nguồn hệ điều hành Unix do phòng thí nghiệm trường đại học công nghệ MIT (Massachusetts Institute of Technology) cung cấp.

Thông qua mạng Internet toàn cầu, những kết quả ban đầu với Linux đã được truyền tải nhanh chóng tới rất nhiều tổ chức, cá nhân trên toàn thế giới. Hàng chục ngàn lập trình viên "tự nguyện" đã hoàn thiện, bổ sung thêm rất nhiều tính năng, ứng dụng mới cho Linux. Cho đến thời điểm 1995/1996, Linux đã thực sự mang dáng dấp của một hệ điều hành thương mại chuyên nghiệp, kế thừa các ưu điểm của Unix: là hệ điều hành hướng mạng (các dịch vụ internet/intranet: eMail, Web, FTP,...), đa nhiệm, an toàn, bảo mật cao, tính thông minh trong quản lý tài nguyên hệ thống (file, CPU, bộ nhớ) và lại có các đặc tính nổi bật:

- Là sản phẩm miễn phí, chạy được trên các máy tính cá nhân PC.
- Với đặc thù là sản phẩm "mã nguồn mở", có khả năng kiểm soát, tạo khả năng xây dựng những chức năng phục vụ các yêu cầu riêng biệt, đặc biệt đối với các hệ thống thông tin đòi hỏi tính ổn định và bảo mật cao.
- Qua một thập kỷ phát triển, Linux đã trở thành một trong những HĐH phát triển nhanh nhất trong lịch sử máy tính.

Từ chỗ chỉ có một số "tín đồ" năm 1991-1992 tới hàng triệu người dùng Linux hiện nay, chắc chắn đó là một chặng đường phát triển đáng kể. Theo thống kê của Công ty điều nghiên và tư vấn công nghệ thông tin và truyền thông IDC (Mỹ) thì tổng doanh thu từ các lĩnh vực máy chủ, máy để bàn và phần mềm gói chạy Linux sẽ đạt gấp hơn hai lần trong 4 năm tới, so với mức 15 tỷ USD toàn cầu hiện nay, tỷ lệ tăng trưởng nói chung về doanh thu của Linux có thể sẽ vào khoảng 26%/năm từ nay đến năm 2008 và riêng kinh doanh phần mềm gói sẽ tăng hơn 44% mỗi năm. Mặc dù chưa thể chiếm lĩnh môi trường máy tính để bàn, Linux vẫn sẽ mở rộng ảnh hưởng của nó lên khoảng 17 triệu PC mới vào năm 2008, đem về doanh thu tương đương 10 tỷ USD và nâng tổng số máy tính trên toàn cầu sử dụng Linux lên 43 triệu chiếc.

Điều thực sự gây ngạc nhiên chính là lớp lớp lập trình viên trên khắp thế giới, với lòng nhiệt huyết vô tận liên tục cải thiện các tính năng của Linux. Những nỗ lực phát triển như vậy không hề chìm trong sự hỗn loạn như lời buộc tội của những công ty kinh doanh phần mềm mã nguồn đóng. Ngay cả Steve Balmer, Tổng Giám đốc Microsoft, cũng phải thừa nhận "Linux đã thực sự là mối đe dọa cho thị trường của Windows. Nó cũng là mối đe dọa chính của Microsoft Office".

Các hãng đi đầu trong phát triển Linux: RedHat, Caldera, SuSE, Mandrake.

2. Linux - xu thế, giải pháp mới cho các hệ thống thông tin

Những năm gần đây, những tiến bộ công nghệ đã đem lại cho máy tính cá nhân PC một vị thế quan trọng không ngờ (giá thành ngày càng hạ, tính năng ngày càng được nâng cao. Tại rất nhiều nơi PC cao cấp đã thoát hẳn khỏi vai trò là một máy tính đơn lẻ thuần túy, đảm nhiệm vai trò máy chủ tài nguyên, hoặc máy chủ nghiệp vụ cho cả một tổ chức, một cơ quan).

Nghiên cứu mới đây (1/2005) của tổ chức đánh giá an ninh CNTT phi lợi nhuận Honeynet Project cho thấy trung bình 3 tháng các hệ thống "Chim cánh cụt" mới rơi vào tình trạng bị tấn công, lâu hơn so với thời gian 72 tiếng mà các cuộc khảo sát năm 2001 và 2002 ghi nhận. Kết quả điều tra năm 2004 được công bố sau khi nhóm nghiên cứu thiết lập 19 máy "bẫy" (honeyspot) Linux và 4 máy "bẫy" Solaris ở 8 nước khác nhau. "Bẫy" ở đây là những máy tính kết nối Internet chưa cài bản vá lỗi nhằm thu hút sự chú ý và tấn công của hacker. "Cài đặt mặc định của các phiên bản Linux ngày càng vững chắc, khiến cho việc khống chế máy tính khó khăn hơn", báo cáo của Honeynet Project viết. "Cấu hình mặc định của các phiên bản mới an toàn hơn với số dịch vụ được bật (enable) tự động giảm bớt, phân tách các dịch vụ được ưu tiên như OpenSSH, tường lửa đặt trên máy chủ sàng lọc kết nối nội bộ, các công cụ phát hiện đe dọa thông dụng và những cơ chế an ninh khác". Trong các cuộc kiểm tra nói trên, chỉ có 4 máy Linux bị tấn công và khống chế (3 trong số này chạy Red Hat 7.3 và một dùng Red Hat 9). Hai trong số này bị xâm nhập bằng hình thức tấn công bẻ password chứ không phải lợi dụng lỗi hệ thống. Người sử dụng Solaris cũng có tin không vui khi 3 trong số 4 máy được Honeynet Project thử nghiệm với Solaris 8 và 9 đã bị tấn công trong phạm vi 3 tuần. Tuy nhiên, chiếc còn lại đã tồn tại trên mạng suốt 6 tháng bình yên. Trong cuộc thử nghiệm năm ngoái do Symantec thực hiện, khi được đặt trong tình trạng máy "bẫy" như tương tự, các hệ thống Windows chưa nâng cấp chỉ an toàn được trong vài tiếng, một số máy bị khống chế ngay sau vài phút. (nguồn VNUNet)

Như vậy, giờ đây việc xây dựng một hệ thống thông tin chuyên nghiệp (ổn định, an toàn bảo mật, các dịch vụ hướng mạng: eMail, Web,...) với giá thành hạ là điều hoàn toàn khả thi với Linux.

Ví dụ về một hệ thống thông tin hoàn chỉnh xây dựng trên Linux:

- Samba: Dịch vụ chia sẻ tài nguyên file
- DHCP: Dịch vụ cấp phát địa chỉ IP tự động cho máy trạm
- Named: Dịch vụ DNS - giải nghĩa tên máy, tên miền thành địa chỉ IP và ngược lại

- OpenLDAP: Dịch vụ sổ địa chỉ phức hợp - cung cấp tới người dùng danh sách địa chỉ eMail, thông tin cá nhân về các thành viên khác trong một tổ chức, một cơ quan.

- Qmail: Dịch vụ gửi, chuyển tiếp thư điện tử (internet eMail)

- Apache: Dịch vụ Web

- Squid: Máy chủ Proxy - cho phép các máy trạm truy nhập Internet thông qua một máy tính có địa chỉ internet (IP) hợp lệ duy nhất

- MySQL, PostgreSQL: Cơ sở dữ liệu

- Iptables - Firewall: Bức tường lửa bảo vệ hệ thống.

Song song với những bước đi vững chắc khi đóng vai trò hệ điều hành máy chủ trong các hệ thống thông tin, Linux đã có nhiều biến chuyển tích cực đối với mảng máy tính văn phòng. Ngày càng có nhiều ứng dụng chất lượng được phát triển trên Linux áp dụng cho máy tính để bàn. Có thể kể đến: môi trường giao diện đồ họa KDE, GNOME, các ứng dụng soạn thảo, lập bảng tính đơn giản, trình soạn thảo văn bản KWrite, bộ ứng dụng văn phòng Koffice, bộ ứng dụng duyệt, thiết kế WEB, gửi/nhận eMail - Netscape Communicator,... và đặc biệt là bộ ứng dụng văn phòng OpenOffice - được đánh giá là tương thích hoàn toàn với MsOffice97/2000, và sẽ là một đối thủ nặng ký đối với Microsoft. Hiện nay, Linux là một sản phẩm chủ đạo của công nghệ thông tin và là một bộ phận cấu thành các sản phẩm trong các chiến lược kinh doanh của các công ty máy tính, nhằm tạo lợi thế cạnh tranh với các đối thủ khác. Bất chấp các chiến dịch quảng cáo rầm rộ của các đối thủ như SCO Group và Microsoft, Linux vẫn được dùng phổ biến.

Theo một điều tra của hãng June Forrester Research đối với 129 công ty có doanh thu hàng năm vượt trên 500 triệu USD, kết quả cho thấy 24% trong số này sử dụng Linux trên mười hoặc nhiều hơn các máy chủ của Intel. Con số này sẽ tăng lên 44% trong ba năm tới.

Theo nhà nghiên cứu Dan Kusnetzky, nhận xét về lĩnh vực máy tính để bàn thì Linux vượt trội hơn cả Mac OS, cho dù Linux vẫn không phải là một sản phẩm chủ đạo của các máy tính để bàn. Với IBM, họ muốn nâng cấp những cải tiến Linux xoay quanh bộ xử lý Power của mình chứ không phải theo cách thiết lập thông thường với Linux như các chip của Intel và AMD. Còn các công ty phần mềm mới như StoneSoft, Acucorp, Congnos và HansaWorld cũng đang ủng hộ sự kết hợp này và những chương trình nhằm khuyến khích những sự hợp tác như thế. Ông Scott Handy, phó chủ tịch chiến lược Linux của IBM cho biết con số ứng dụng Linux hoạt động dựa trên bộ xử lý Power đã tăng gấp đôi, từ 300 lên 600 ứng dụng. Đối thủ cạnh tranh HP cũng có những kế hoạch hợp tác riêng: Trước tiên, hãng sẽ thực hiện khoá đào tạo Linux tại chỗ, cung cấp các chương trình phần mềm và thông tin cho các đối tác kinh doanh. Tiếp theo đó, HP sẽ cố thuyết phục các công ty phần mềm sử dụng Linux đang hỗ trợ phiên bản Solaris Unix của hãng Sun. (CNet)

Sự phong phú của các sản phẩm nguồn mở đã đem tới người dùng một cách nhìn mới về thế giới phần mềm nguồn mở. Kết quả của một cuộc nghiên cứu kéo dài đến 4 năm do Coverity (một công ty chuyên phân tích mã chương trình có trụ sở tại San Francisco) thực hiện cho biết: Linux là hệ điều hành có ít lỗi nhất so với các hệ điều hành thương mại hiện nay. Dự án này đã tìm ra được 985 lỗi trong 5,7 triệu dòng mã chương trình trong nhân (hoặc lõi) của phiên bản hệ điều hành Linux gần đây nhất. Theo dữ liệu của đại học tổng hợp Carnegie Mellon cho biết thì với một chương trình phần mềm thương mại có kích thước tương tự như Linux thì có đến những 5.000 lỗi đủ loại được phát hiện. Seth Hallem, giám đốc điều hành của Coverity, cho biết: "Linux là một hệ thống rất tốt vì nó có rất ít lỗi". Coverity là công ty chuyên tạo ra các công cụ khám phá lỗi của các phần mềm.

Giờ đây người dùng có thể lựa chọn cho mình các sản phẩm phù hợp nhất, và với chi phí thấp nhất có thể. Ví dụ về một trạm làm việc văn phòng xây dựng trên Linux:

- GNOME, KDE: Môi trường desktop đồ họa
- Mc, Gmc: Trình quản lý file, thư mục
- Mozilla/Netscape Communicator: Bộ ứng dụng duyệt Web, gửi/nhận eMail, soạn/ thiết kế trang Web, xây dựng sổ địa chỉ cá nhân
- Kppp: Trình quay số, thiết lập kết nối internet
- OpenOffice: Bộ ứng dụng văn phòng tương thích MsOffice97/2000/XP (soạn thảo văn bản, lập bảng tính, soạn bản trình diễn, thiết kế đồ họa,..)
- Kdat: Tiện ích sao lưu dữ liệu
- Fsck: Tiện ích kiểm tra, khắc phục lỗi xuất hiện với hệ thống file, thư mục

Phù hợp với xu thế của thế giới thông tin đa ngôn ngữ - các phiên bản Linux mới nhất, các ứng dụng chạy trên Linux cũng đã được bổ sung những khả năng hỗ trợ Unicode ngày càng hoàn thiện hơn. Những lợi thế do Linux cũng như các sản phẩm phần mềm mã nguồn mở đem lại đã kéo theo sự quan tâm với mức độ ngày càng tăng - từ mức chính phủ, tới các đại gia trong ngành công nghệ thông tin, cho tới các doanh nghiệp vừa và nhỏ.

Chính phủ nhiều nước như Trung Quốc, Đài Loan, Đức, Pháp đã cân nhắc phần mềm nguồn mở như là giải pháp an toàn và kinh tế nhất cho hệ thống thông tin của họ. Những người khổng lồ như: IBM, Intel, Compaq, HP, Oracle, SunMicrosystem,... đã có những cam kết hỗ trợ, và gia tăng đầu tư trong lĩnh vực phần mềm mã nguồn mở. Bộ Giao thông Pháp vừa thông qua đề xuất chuyển đổi 1.500 máy tính đang sử dụng hệ điều hành Windows sang

hệ điều hành mã nguồn mở Linux. Động thái trên được nhận định là một "thắng lợi đáng kể" của "chim cánh cụt" Linux ở châu Âu. Bộ Giao thông Pháp hiện đang lập kế hoạch "thay Windows NT bằng Linux" cho khoảng 60.000 máy trạm và 2.000 máy chủ chạy Windows NT của họ, một kế hoạch đã được thực hiện một cách không chính thức từ tháng 11/2003. Song song cùng xu thế lựa chọn mã nguồn mở để giảm chi phí, châu Âu đang dần trở thành nơi đối đầu trực tiếp giữa Microsoft và các nhà phân phối Linux. Dự kiến, số cơ quan, tổ chức,... chọn lựa Linux sẽ tiếp tục tăng khi Microsoft rút bỏ cam kết hỗ trợ bảo mật cho các hệ điều hành Windows "đời cũ".

Ngày 03/04/2004, tại Bắc Kinh, 3 quốc gia Đông Á Trung Quốc, Hàn Quốc và Nhật Bản đã ký thỏa thuận hợp tác phát triển một hệ điều hành dựa trên nền Linux, được xem là đối trọng nặng ký của Windows trong thời gian tới. Thỏa thuận này là một phần nỗ lực nhằm giảm thiểu phụ thuộc vào hệ điều hành của Microsoft, vốn bị ba nước này quy kết là làm giảm năng lực của ngành công nghiệp phần mềm máy tính của họ. (nguồn AFP)

3. Nhu cầu triển khai nghiên cứu "giải pháp Linux"

Đứng trước xu thế của thế giới và những lợi ích của việc triển khai hệ điều hành Linux cũng như các vấn đề đặt ra khi triển khai hệ điều hành này, Ban Điều hành Đề án 112 thành phố đã giao nhiệm vụ nghiên cứu các vấn đề liên quan đến hệ điều hành Linux cho Trung tâm Tin học thuộc Văn phòng UBND thành phố Đà Nẵng, tìm hiểu sâu về triển khai Linux trên hệ thống mạng LAN của các sở ban ngành, là bước trung gian để có thể triển khai tốt các ứng dụng dùng chung của thành phố trên hệ điều hành mã nguồn mở Linux nhằm phục vụ việc triển khai đề án 112 của thành phố một cách có hiệu quả.

II. Tóm tắt mục tiêu

Mục tiêu đầu tiên của đề tài là **tạo ra một giải pháp đóng gói để khai thác hệ thống Linux và mã nguồn mở**, góp phần nâng cao hiệu quả khai thác và giảm chi phí đầu tư cho việc xây dựng, triển khai, vận hành, khai thác và quản lý các hệ thống mạng LAN tại các đơn vị Sở, Ban, Ngành, Quận, Huyện.

Một mục tiêu khác là thông qua việc triển khai đề tài, sẽ **xây dựng và bồi dưỡng một đội ngũ cán bộ quản trị mạng tại các đơn vị** nâng cao hiểu biết về hệ thống máy chủ Linux và thành thạo các công cụ để có thể quản trị mạng sử dụng xen kẽ các máy chủ Linux, máy chủ Windows và máy trạm Windows một cách hiệu quả; bên cạnh đó phát triển đội ngũ những người tham gia thực hiện đề tài có kiến thức và kinh nghiệm khi tiếp xúc, làm việc với hệ điều hành Linux và mã nguồn mở; tạo tiền đề cho việc xây dựng và triển khai các hệ thống, ứng dụng Linux và mã nguồn mở sau này.

III. Nội dung đối tượng và phạm vi nghiên cứu

1. Đối tượng nghiên cứu

Nhóm tác giả đề tài sẽ tiến hành nghiên cứu hiện trạng và nhu cầu trong việc ứng dụng Linux trong khai thác và quản trị mạng tại các đơn vị hành chính sự nghiệp. Đây là đối tượng nghiên cứu thứ nhất của đề tài.

Hệ điều hành Linux (phiên bản Mandrake 10.0), các dịch vụ được cung cấp trong phiên bản này, một số phần mềm mã nguồn mở chạy trên nền Linux là đối tượng được tập trung nghiên cứu để có thể đưa ra giải pháp kỹ thuật.

2. Phạm vi nghiên cứu

Công tác khảo sát thực tế được tiến hành tại các Sở, Ngành trên địa bàn thành phố Đà Nẵng. Một trong những điểm thuận lợi là sau khi triển khai dự án xây dựng mạng LAN cho các Sở, Ngành, hệ điều hành Linux đã được cài đặt phục vụ việc triển khai các dự án phần mềm dùng chung. Ngoài ra, nhóm khảo sát tìm hiểu thêm các giải pháp kỹ thuật của một số công ty tin học tại Hà Nội và thành phố Hồ Chí Minh.

Việc nghiên cứu triển khai thử nghiệm các giải pháp kỹ thuật được tiến hành tại 5 đơn vị: Văn phòng UBND thành phố, Văn phòng Thành ủy, Sở Giáo dục, Sở Ngoại Vụ và UBND quận Hải Châu.

Về mặt kỹ thuật, nhóm nghiên cứu giới hạn nghiên cứu các dịch vụ Web, Email, DNS, Firewall, Samba, LDAP. Đây là các dịch vụ được sử dụng rộng rãi trên các hệ thống mạng.

IV. Tổng quan về lịch sử vấn đề nghiên cứu

1. Linux, các sản phẩm phần mềm nguồn mở tại Việt Nam

Phù hợp với xu thế chung, Việt Nam đã có những chuyển biến tích cực trong việc quảng bá cũng như thúc đẩy phong trào Linux nói riêng cũng như phần mềm mã nguồn mở nói chung.

Một số sản phẩm đã ra đời, có giá trị sử dụng cao, khẳng định được hiệu quả trong sử dụng thực tế (chất lượng/giá thành). Những kết quả khích lệ này cũng đã tác động tích cực tới những tổ chức, cá nhân tham gia công tác hoạch định phương hướng phát triển ngành công nghệ thông tin nước nhà - đặc biệt khi Việt Nam xúc tiến thực thi các hiệp định thương mại, các hiệp định về bảo vệ quyền tác giả.

Mới đây, Thủ tướng Chính phủ đã ký Quyết định 235/QĐ-TTg ngày 2/3/2004 phê duyệt Dự án tổng thể “Ứng dụng và phát triển phần mềm mã nguồn mở ở Việt Nam giai đoạn 2004-2008”. Trong đó, đáng chú ý là việc giao cho UBND TP.Hà Nội và UBND TP.HCM chủ trì thử nghiệm ứng dụng và phát triển phần mềm mã nguồn mở tại Hà Nội và TP.HCM.

Các đơn vị tham gia nghiên cứu, ứng dụng, và phát triển Linux cũng như phần mềm nguồn mở tại Việt nam:

- Công ty máy tính truyền thông CMC
- Tổng công ty điện tử tin học Việt Nam
- Công ty Việt Khang
- Trường Đại học Bách khoa Hà nội
- Trường Đại học Bách khoa Thành phố Hồ Chí Minh

2. Ứng dụng hệ điều hành Linux trong khuôn khổ đề án 112 thành phố Đà Nẵng

Hệ điều hành Linux trong khuôn khổ đề án 112 được triển khai tại Trung tâm Tích hợp dữ liệu của thành phố cũng như tại mạng LAN của các đơn vị Sở, Ban, Ngành.

Thực hiện kế hoạch triển khai các dịch vụ cơ bản tại Trung tâm Tích hợp dữ liệu của Ban Điều hành Đề án 112 Chính phủ, việc cài đặt hệ điều hành Linux cũng như các dịch vụ trên nền Linux đã được thực hiện thí điểm tại bộ Xây dựng để rút kinh nghiệm và đánh giá khả năng triển khai rộng tại các địa phương.

Tại Đà Nẵng, các phần mềm dùng chung "Website Điều hành & tác nghiệp", "Quản lý công văn & Hồ sơ công việc", "Hệ thống Thông tin tổng hợp kinh tế xã hội" đang được xây dựng cũng sử dụng Web Server và cơ sở dữ liệu trên máy chủ Linux.

Trên hệ thống hỗn hợp, sử dụng các máy chủ Windows và Linux, yêu cầu đặt ra rất bức thiết là cán bộ quản trị mạng của đơn vị phải đủ khả năng để làm việc với các máy chủ này, hơn thế nữa phải biết kết hợp sức mạnh của chúng phục vụ cho công việc chuyên môn của đơn vị.

V. Quan điểm lựa chọn vấn đề nghiên cứu

Một quan điểm xuyên suốt trong quá trình nghiên cứu là sản phẩm của đề tài phải phục vụ được cho cán bộ quản trị mạng tại các đơn vị Sở, Ngành. Với đặc thù về trình độ chuyên môn tin học cũng như quỹ thời gian giới hạn của đối tượng này, các tài liệu và các giải pháp kỹ thuật được xây dựng phải phù hợp để đảm bảo tính khả dụng của đề tài.

VI. Tóm tắt nội dung nghiên cứu

Ngoài phần mở đầu, kết luận, danh mục tài liệu tham khảo và phụ lục, đề tài gồm 5 chương:

Chương I: Cơ sở lý luận

Chương II: Xác định phương pháp nghiên cứu.

Chương III: Tổng hợp và đánh giá kết quả khảo sát hệ thống mạng máy tính và việc ứng dụng Linux trong khai thác và quản trị mạng tại các đơn vị Sở, Ngành trên địa bàn thành phố Đà Nẵng.

Chương IV: Các giải pháp kỹ thuật trên nền hệ điều hành Linux. Tóm tắt tài liệu đào tạo được xây dựng.

Chương V: Các mô hình triển khai ứng dụng hệ điều hành Linux trong khai thác và quản trị mạng LAN, kế hoạch phát triển kết quả đề tài, một số kiến nghị.

CHƯƠNG I : CƠ SỞ LÝ LUẬN

I. Mạng và hệ điều hành Linux

Linux là hệ điều hành trẻ trung đầy sinh lực, thời gian gần đây được cho là đối thủ cân tài, cân sức với Microsoft Windows NT. Do là hệ điều hành cho nhiều người sử dụng, với phần nhân (kernel) được thiết kế chức năng mạng ngay từ ban đầu nên Linux là ứng cử viên hệ điều hành mạng sáng giá. Cần nhắc lại rằng, ngay từ ban đầu Windows chỉ là hệ điều hành cho máy đơn chứ không phải là hệ điều hành mạng.

Linux phù hợp cho việc thiết lập một mạng máy tính nghiêm túc với chi phí thấp. Sự hỗ trợ của Linux cho X Windows cho phép sử dụng được hầu hết những ứng dụng X có trên Internet: trình duyệt Netscape như Navigator và Communicator, hoặc X11 và MP3. Tính ổn định và sức đề kháng tốt cũng là hai yếu tố giúp Linux trở thành hệ điều hành cao cấp dành cho những tác vụ quan trọng - vượt hơn hẳn Windows.

Thoạt đầu Linux sẽ làm người sử dụng ái ngại, nhất là khi so sánh với vẻ thân thiện, cắm-là-chạy (plug and play) của môi trường Windows 95/98. Thực ra, việc cài đặt và sử dụng Linux không hề dễ dàng, nhưng cũng không quá khó như một số người thường nghĩ. Và chưa hết, nếu đang làm việc trong môi trường mạng, sự hiểu biết về Linux sẽ giúp ích cho công việc, và nhờ Linux, việc tìm hiểu về một hệ điều hành thông dụng sẽ đỡ nhọc công hơn.

1. Linux - hệ điều hành linh hoạt

Đầu tiên, Linux là hệ điều hành thích hợp cho *máy trạm* và tùy thuộc vào cách thức xác lập cấu hình, Linux thỏa mãn được những yêu cầu chuyên biệt cho thương mại. Linux có thể sử dụng làm môi trường phát triển, hub truyền thông, và với những ứng dụng chạy trên X Windows có thể đảm nhận cả vai trò một máy để bàn truyền thống.

Hai là, có một thứ mà Linux có thể thực hiện tốt hơn những hệ thống khác, đó là khả năng phục vụ. Với những tính năng truyền thông và mạng cực mạnh, Linux là hệ điều hành *máy chủ* lý tưởng.

2. Linux - server quản lý tập tin và in ấn

Linux được phân phối cùng với SAMBA - bộ giao thức SMB miễn phí - cho phép truy cập tập tin và máy in trên máy Linux từ máy trạm DOS, Win95, Win98 và Windows NT trên mạng cục bộ. Điều này có nghĩa là Linux hoạt động như một file server. Một tính năng tuyệt vời khác là có thể cấu hình SAMBA để quản trị bảo mật: hoặc thông qua những chức năng gốc của Unix, hoặc bằng server password (Windows NT), SAMBA còn cho phép máy trạm Linux truy cập tập tin trên máy Windows và ngược lại.

3. Linux - server truyền thông

Linux có nhiều phần mềm về truyền thông thích hợp phục vụ việc xây dựng mạng Intranet cộng tác mà không phải mất thêm phí tổn phần mềm. Dịch vụ đơn giản nhất có lẽ là sendmail - chương trình phục vụ mail truyền thống của Unix, cho phép gửi email trên mạng cộng tác hoặc Internet. Với hệ thống mail cho xí nghiệp, chỉ cần tạo lập các tài khoản người dùng và chương trình nhận mail cho những máy trên mạng LAN.

Trong mạng Intranet phức tạp hơn, có thể triển khai những dịch vụ như ftp, Usenet và Web server. Có rất nhiều phần mềm server miễn phí kèm theo ngay trong bản Linux. Một số server thông dụng có thể tải về từ Internet như Web Server Apache tại địa chỉ <http://www.apache.org/>, DNS server BIND tại địa chỉ <http://www.bind9.net,...>

4. Linux - server cho WAN hoặc gateway

Thông thường, mọi sự trở nên phức tạp và tốn kém hơn nếu đi quá giới hạn của LAN. Tuy nhiên, việc kết nối mạng diện rộng (WAN) với Linux chỉ là một sự mở rộng chức năng LAN. Thông thường, có thể triển khai PPP bằng kết nối thông qua modem hay tân tiến hơn thì bằng đường dây thuê bao và kết nối ISDN. Linux có cả PPP và SLIP, hỗ trợ bức tường lửa, che chắn IP (IP masquerading), giấu password (nhằm tăng cường chống bẻ khóa, tập tin lưu trữ password sẽ được đặt tại /etc/shadow thay vì /etc/passwd), NFS và NIS - là những điểm bắt đầu khá tốt với WAN.

Tính năng mạng của Linux rất linh động, cho phép cấu hình hệ thống mạng với quy mô từ mạng LAN cho đến mạng cộng tác trải rộng khắp thế giới. Linux hỗ trợ đầy đủ cho giao thức TCP/IP cùng với những tính năng cao cấp như tường lửa, che chắn địa chỉ IP.

Có thể cấu hình máy chủ Linux thành trạm gateway Internet trong mạng LAN. Điều này có nghĩa là cho phép nhiều máy cùng sử dụng và chia sẻ một tài khoản Internet.

Linux hỗ trợ nhiều card mạng Ethernet (như 3Com, D-Link,...) tự động nhận ra cấu hình của card LAN vào lúc khởi động để khởi tạo lớp phần mềm giao tiếp mạng theo đúng cấu hình này. Mỗi máy cần có một địa chỉ IP và tên máy (host name) riêng để giao tiếp với nhau trên mạng (điều này cũng giống như kiểu cấu hình được sử dụng trên những mạng Windows).

Cuối cùng, có nhiều bộ phần mềm gắn liền với Linux, được dùng để xây dựng các "mạng hỗn hợp". Những bộ phần mềm này tích hợp server Linux trong một mạng gồm các client với nhiều hệ điều hành khác nhau như Windows 3.1, Windows 95, NT, Novell, và Macintosh. Với bộ giao thức SAMBA, Linux có thể cung cấp dịch vụ file và in ấn. SAMBA cho phép máy

Windows tìm duyệt và truy cập tập tin thông qua Windows Explorer và File Manager.

II. Mạng hỗn hợp

Một cách vắn tắt, "mạng hỗn hợp" là mạng trong đó các máy tính chạy những HĐH khác nhau hoặc các phiên bản khác nhau của cùng một HĐH. Trở ngại đối với mô hình mạng này là một số công ty công nghệ thông tin không quan tâm tới việc hỗ trợ "hệ thống hỗn hợp". Họ thích mô hình "mạng đồng nhất", trong đó các máy tính chạy cùng một HĐH hơn, bởi vì chúng dễ quản lý, lại vừa cho phép duy trì tốt các biện pháp bảo mật.

Tuy nhiên, Linux lại rất thích hợp với môi trường mạng hỗn hợp vì có thể phối hợp hiệu quả với nhiều HĐH cũng như hệ thống tập tin khác nhau. Do HĐH Windows của Microsoft dường như thống lĩnh thế giới PC, nên ý tưởng nảy sinh đầu tiên của nhóm đề tài là thử chạy Linux trong mạng có các máy tính chạy hệ điều hành Windows.

Trong các mạng hỗn hợp, hệ điều hành Linux rất phù hợp cho việc cài đặt tại các máy chủ dịch vụ. Nhờ vào hệ thống quản lý file Samba, máy chủ DNS BIND, máy chủ mail sử dụng QMail, máy chủ Web Apache, tường lửa IPTables, ... mạng được cung cấp các dịch vụ cần thiết. Tại các máy trạm Windows, người sử dụng vẫn làm việc bình thường trên giao diện quen thuộc và có khả năng khai thác dịch vụ trên máy chủ Linux.

CHƯƠNG II: XÁC ĐỊNH PHƯƠNG PHÁP NGHIÊN CỨU

I. Cách tiếp cận, phương pháp nghiên cứu, kỹ thuật sẽ sử dụng

Hiện nay, Linux mới được giới thiệu trong các giáo trình đào tạo căn bản, vẫn chưa có một giải pháp hoàn chỉnh để trình bày việc xây dựng mạng LAN với các máy chủ Linux, giữa máy chủ Linux với Windows một cách xen kẽ, cài đặt các dịch vụ trên mạng, hướng dẫn người sử dụng khai thác và quản trị mạng.

Để thực hiện việc nghiên cứu, xây dựng giải pháp đáp ứng yêu cầu đặt ra như trên, nhóm tác giả sử dụng cách tiếp cận, phương pháp nghiên cứu như sau:

- *Nghiên cứu tài liệu*: nghiên cứu tổng quan tài liệu trong nước và nước ngoài. Cụ thể là kế thừa các kết quả đã công bố rộng rãi về hệ điều hành Linux và mã nguồn mở, trên cơ sở đó xây dựng hệ thống tài liệu giải pháp xây dựng mạng LAN tồn tại song song 2 hệ điều hành mạng WINDOWS và LINUX, tài liệu cài đặt hệ điều hành Linux, cài đặt một số ứng dụng máy chủ và nghiên cứu chọn lựa hệ thống mã nguồn thích hợp để phát triển thêm những chương trình phục vụ nhu cầu quản trị mạng LAN;

- *Điều tra thực tế*: lập phiếu điều tra về khả năng tiếp nhận, quản trị mạng của các chuyên viên quản trị mạng tại các đơn vị Sở, Ban, Ngành, Quận, huyện đối với hệ điều hành Linux;

- *Phương pháp phi thực nghiệm*: thống kê, xử lý các số liệu thu thập được sau quá trình điều tra thực tế;

- *Phương pháp thực nghiệm*: thực hiện việc cài đặt, thử nghiệm hệ điều hành Linux, thiết lập cấu hình một số ứng dụng máy chủ; lập trình, kiểm thử, hoàn chỉnh một số ứng dụng phục vụ quản trị mạng LAN;

- *Phương pháp chuyên gia*: mời các chuyên gia đã có kinh nghiệm về hệ điều hành Linux và phần mềm mã nguồn mở tham gia tư vấn, góp ý kiến, chỉnh sửa trong quá trình nghiên cứu của đề tài;

Nhóm thực hiện đề tài thống nhất chọn phiên bản hệ điều hành **Linux Mandrake 10** để tiến hành nghiên cứu, cài đặt, thử nghiệm trong quá trình thực hiện đề tài. Việc lựa chọn phiên bản này dựa trên những yếu tố sau:

+ *Phù hợp với tình hình thực tế*: tại mạng LAN một số Sở, Ban, Ngành, Quận, Huyện đã triển khai Web điều hành (do Trung tâm Công nghệ phần mềm Đà Nẵng xây dựng), máy chủ đã được cài đặt hệ điều hành Linux phiên bản Mandrake 9.

+ *Tính phổ biến, độ tin cậy và tính hỗ trợ*: Cũng như Redhat, đây là phiên bản rất phổ biến cả về tính dễ sử dụng lẫn chứng nhận về chất lượng và độ tin cậy, dễ dàng cài đặt, đặc biệt phù hợp cho những người chưa có nhiều kinh nghiệm sử dụng Linux, có khả năng hỗ trợ phần cứng tốt.

Mandrake được phát triển dựa trên nền Redhat, do vậy các gói ứng dụng có thể làm việc tốt trên cả Mandrake lẫn Redhat. Hơn thế nữa, Mandrake có nhiều tính năng được tự động nhiều hơn Redhat.

So với các phiên bản trước, Mandrake Linux 10 tích hợp nhân Linux 2.6 tăng hiệu suất sử dụng, khả năng an toàn và độ tin cậy, hỗ trợ nhiều chuẩn phần cứng mới.

II. Nội dung nghiên cứu

1. Điều tra, đánh giá:

Điều tra, nghiên cứu đánh giá khả năng tiếp nhận, quản trị mạng của các chuyên viên quản trị mạng tại các đơn vị Sở, Ban, Ngành trong hệ thống hành chính thành phố Đà Nẵng đối với hệ điều hành Linux.

2. Nghiên cứu giải pháp kỹ thuật:

Nghiên cứu cài đặt hệ điều hành Linux phục vụ quản lý, khai thác mạng LAN. Kết quả của công việc này là tài liệu hướng dẫn chi tiết các bước cài đặt, cấu hình hoàn chỉnh một Server với hệ điều hành Linux đồng thời giải đáp một số vướng mắc thường gặp nhất khi vận hành, khai thác Linux Server.

Nghiên cứu cài đặt, thiết lập cấu hình các ứng dụng máy chủ: DNS, Firewall, Web, Mail, xây dựng các tài liệu hướng dẫn cài đặt và quản trị dịch vụ.

Xây dựng các gói ứng dụng phục vụ quản trị mạng. Do hạn chế về thời gian cũng như cần tập trung nghiên cứu sâu, kỹ và xây dựng hoàn thiện một ứng dụng cụ thể làm nền tảng cho việc phát triển các ứng dụng khác, trước mắt đề tài tập trung xây dựng, phát triển các ứng dụng sau:

- Ứng dụng quản trị cấu hình máy chủ Linux, các tài nguyên của máy chủ: Ứng dụng này là một chương trình chạy trên một máy trạm trong mạng LAN của đơn vị giúp cho người quản trị mạng thực hiện được các thao tác: tắt/khởi động, xem cấu hình và chia sẻ file trên máy chủ Linux; quản lý máy in. Các thao tác khác tương tự sẽ phát triển sau.

- Ứng dụng quản trị ứng dụng máy chủ: DNS, Firewall. Ứng dụng này là một chương trình chạy trên một máy trạm trong mạng LAN của đơn vị giúp cho người quản trị mạng thực hiện được việc quản trị các dịch vụ DNS, Firewall. Các dịch vụ khác như DHCP, Mail, Web, Proxy,... sẽ tương tự phát triển sau.

Nghiên cứu cơ chế an toàn thông tin trên mạng Linux: LDAP, OpenLDAP.

3. Thử nghiệm, đóng gói kết quả

Triển khai thử nghiệm, đánh giá hiệu quả việc sử dụng “giải pháp Linux” tại 5 đơn vị.

Lập tài liệu hoàn chỉnh về giải pháp.

Triển khai đào tạo cán bộ quản trị mạng tại các đơn vị quản lý mạng Linux.

CHƯƠNG III: TỔNG HỢP, ĐÁNH GIÁ KẾT QUẢ KHẢO SÁT

I. Số liệu khảo sát

Trung tâm Tin học Văn phòng UBND thành phố đã tiến hành việc khảo sát tại 23 đơn vị, theo mẫu khảo sát đã được duyệt. Tổng số phiếu khảo sát thu lại được là 23 phiếu, được tổng hợp như sau:

1. Thông tin chung về đơn vị

STT	Nội dung	Số lượng	Ghi chú
1	Tổng số đơn vị khảo sát	23 đơn vị	
2	Tổng số cán bộ	972 chuyên viên	
3	Số máy chủ	57 máy	
4	Số máy trạm	599 máy	
5	Số chuyên viên CNTT	42 chuyên viên	
6	Số chuyên viên quản trị mạng	23 chuyên viên	
7	Số chuyên viên quản trị mạng là nam	17 chuyên viên	
8	Số chuyên viên quản trị mạng là nữ	6 chuyên viên	

2. Hệ điều hành mạng hiện sử dụng tại các đơn vị

(có thể một đơn vị dùng nhiều hệ điều hành mạng)

STT	Hệ điều hành	Số lượng	Tỷ lệ
1	Windows	23 đơn vị	100.0%
2	Linux	12 đơn vị	52.2%
3	Unix	1 đơn vị	4.3%

3. Hệ điều hành mạng quen thuộc

STT	Hệ điều hành	Số lượng	Tỷ lệ
1	Windows	23 đơn vị	100.0%
2	Linux	3 đơn vị	13.2%
3	Unix	1 đơn vị	4.3%

4. Trình độ học vấn của chuyên viên quản trị mạng

STT	Trình độ	Số lượng	Tỷ lệ
1	Trên đại học	0	0%

2	Đại học	21 chuyên viên	91.4%
3	Cao đẳng	1 chuyên viên	4.3%
4	Trung cấp	1 chuyên viên	4.3%

5. Trình độ chuyên môn về CNTT của chuyên viên quản trị mạng

STT	Trình độ	Số lượng	Tỷ lệ
1	Đại học	15 chuyên viên	65.2%
2	Cao đẳng	1 chuyên viên	4.3%
3	Trung cấp	3 chuyên viên	13.1%
4	Không có	4 chuyên viên	17.4%

6. Các chứng chỉ CNTT của chuyên viên quản trị mạng

Tin học căn bản: 1 chuyên viên của Sở Du lịch

Chứng chỉ đào tạo Đề án 112 của thành phố: 9 chuyên viên

Chứng chỉ đào tạo Đề án 112 của Chính phủ: 7 chuyên viên

Kỹ thuật viên tin học: 1 chuyên viên của Ban Tôn giáo

Quản trị mạng Intranet/Internet: 1 chuyên viên của Sở Giáo dục và Đào tạo

Chứng chỉ tập huấn E-Commerce tại Philippines: 1 chuyên viên của Trung tâm xúc tiến thương mại

1 chuyên viên Sở TĐTT đang theo học lớp Lập trình viên chuyên nghiệp

1 chuyên viên của Cục thuế có các chứng chỉ: Quản trị mạng của Novell cấp, Software Engineering của Công ty Mitac Computer-Đài Loan cấp, Oracle (SQL, PL/SQL, Database Administrator) của Oracle cấp.

7. Nhiệm vụ quản trị mạng cụ thể

Chuyên viên quản trị mạng có thể đồng thời thực hiện nhiều nhiệm vụ

STT	Nhiệm vụ	Số lượng	Tỷ lệ
1	Kết nối mạng	22	95.7%
2	Quản trị DNS	15	65.2%
3	Quản trị Mail	16	69.6%
4	Quản trị Web	16	69.6%
5	Quản trị Firewall	8	34.8%
6	Sửa chữa phần cứng	16	69.6%

8. Kiểm nhiệm công tác khác

STT	Kiểm nhiệm	Số lượng	Tỷ lệ
1	Có	20	86.9%
2	Không	3	13.1%

9. Hiểu biết về hệ điều hành Linux

STT	Mức độ	Số lượng	Tỷ lệ
1	Đã nghiên cứu tài liệu	9	39.1%
2	Đã thử nghiệm cài đặt	6	26.1%
3	Đã có kinh nghiệm quản trị Linux	0	0.0%
4	Đã qua một/các khóa đào tạo Linux	7	30.4%
5	Chỉ mới nghe giới thiệu	10	43.5%

10. Kiến thức về mã nguồn mở:

STT	Mức độ	Số lượng	Tỷ lệ
1	Có nghe nói đến mã nguồn mở	20	86.9%
2	Đã sử dụng	3	13.1%

II. Phân tích kết quả khảo sát

1. Hạ tầng cơ sở:

Trong khuôn khổ triển khai đề án 112, mạng máy tính của các đơn vị đã được xây dựng, nâng cấp và đưa vào sử dụng.

Mạng LAN của các đơn vị có thể được phân loại thành 3 nhóm quy mô:

1.1. Mạng nhỏ - có 2 máy chủ (chiếm 75%)

Các máy chủ này sẽ được cài đặt như sau:

- 1 máy chủ cài hệ điều hành Microsoft Windows NT 2000 Server đóng vai trò Domain Server, File Server.

- 1 máy chủ cài hệ điều hành Mandrake Linux 9.2, Web Server Apache, cơ sở dữ liệu Oracle và phần mềm Website Điều hành.

1.2. Mạng trung bình (chiếm 17%)

Tại một số đơn vị như Sở Kế hoạch Đầu tư, Sở Tài chính, Cục Thuế, Cục Thống kê,... bên cạnh hệ thống máy chủ do đề án 112 cung cấp, đơn vị cũng được trang bị các máy chủ trong khuôn khổ các dự án của ngành.

Tại các đơn vị này, 1 máy chủ được cài hệ điều hành Mandrake Linux 9.2 phục vụ triển khai dự án Website Điều hành, các máy chủ khác cài hệ điều hành Microsoft Windows NT Server.

1.3. Mạng lớn (chiếm 8%)

Tại Văn phòng UBND thành phố, Sở Giáo dục Đào tạo, các máy chủ được quy hoạch một cách bài bản hơn. Các nhóm dịch vụ liên quan được phân bổ, cài đặt trên các máy chủ khác nhau; điều này giúp cho máy chủ hoạt động ổn định hơn, việc bảo mật cũng được chú ý đúng mức.

Tại Sở Giáo dục, hệ thống mạng được kết nối trực tiếp với Internet, phục vụ việc khai thác của các đơn vị trực thuộc thông qua môi trường Internet.

2. Trình độ nhân lực công nghệ thông tin

Tất cả các đơn vị được khảo sát đều bố trí cán bộ thực hiện nhiệm vụ quản trị mạng, trong số đó 65% có trình độ đại học về CNTT, 17% có trình độ trung cấp, cao đẳng, số còn lại được đào tạo thông qua các khoá tập huấn trong khuôn khổ đề án 112. Một số trong đó đã có chứng chỉ quản trị mạng, thương mại điện tử. Lực lượng cán bộ này có đầy đủ khả năng để tiếp cận với công nghệ mới.

Tại 3 đơn vị, cán bộ CNTT là chuyên trách, 20 đơn vị còn lại, cán bộ kiêm nhiệm thêm các nhiệm vụ khác; do vậy, điều kiện để cán bộ CNTT chuyên tâm vào việc quản trị mạng, học tập nâng cao trình độ cũng như phát triển các ứng dụng cho đơn vị là hết sức hạn chế.

Qua khảo sát thực tế, các cán bộ này cũng có thể chia thành 3 nhóm trình độ:

2.1. Trình độ tối thiểu:

Thực hiện nhiệm vụ chính là cài đặt và xử lý sự cố tại các máy trạm, giúp đỡ các chuyên viên cùng đơn vị thực hiện các dịch vụ chia sẻ tập tin và máy in mạng.

2.2. Trình độ trung bình:

Bên cạnh việc đảm nhận các công việc như nhóm trên, các cán bộ trong nhóm này có khả năng cài đặt, sử dụng các dịch vụ Web, EMail, FTP; tuy nhiên chưa hiểu rõ về dịch vụ cũng như chưa có khả năng thiết lập các cấu hình đặc biệt cho dịch vụ (phân quyền, bảo mật,...)

2.3. Trình độ khá:

Các cán bộ trong nhóm này có hiểu biết tốt về các dịch vụ trên mạng, có khả năng cài đặt và triển khai các dịch vụ DHCP, DNS, Firewall trên mạng cục bộ của đơn vị; có điều kiện và khả năng tự nghiên cứu nâng cao trình độ.

3. Mức độ sử dụng hệ điều hành Linux

Cán bộ quản trị mạng của các đơn vị và đã rất quen thuộc với hệ điều hành Microsoft Windows. Máy chủ Windows thường được sử dụng như Domain Server, File Server. Đối với hệ điều hành Linux, có 3 mức độ sử dụng khác nhau tại các đơn vị:

3.1. Chưa sử dụng:

Trong năm 2004, một số đơn vị chưa triển khai Website điều hành, cán bộ phụ trách CNTT mới làm quen với Linux thông qua khoá đào tạo do Ban Điều hành Đề án 112 tổ chức.

3.2. Linux phục vụ triển khai Website Điều hành:

Tình trạng phổ biến ở các đơn vị này là máy chủ Linux được sử dụng chuyên cho Website điều hành, việc quản trị máy chủ Linux được giao phó hoàn toàn cho chuyên viên tin học của Softech - đơn vị xây dựng Website điều hành thực hiện, cán bộ quản trị mạng của đơn vị chỉ thực hiện nhiệm vụ bật tắt máy chủ hàng ngày (do chưa có giải pháp sử dụng UPS Online một cách tự động).

3.3. Khai thác Linux phục vụ nhiều mục đích:

Tại Văn phòng UBND thành phố, ngoài máy chủ Linux được cài đặt Website Điều hành, còn một máy chủ cài đặt Mail Server phục vụ trao đổi thư điện tử trong nội bộ đơn vị và một máy chủ Linux phục vụ kết nối với mạng CPNet thông qua đường kết nối ISDN. Một số máy chủ Linux đã được dựng để cài đặt thêm các ứng dụng Web và phục vụ công tác đào tạo của Trung tâm Tích hợp dữ liệu.

Tại Sở Giáo dục Đào tạo, một máy chủ Linux đóng vai trò Firewall, một máy chủ khác cài đặt dịch vụ thư điện tử và một máy chủ Web phục vụ cho mạng nội bộ của Văn phòng Sở và kết nối từ các đơn vị trực thuộc thông qua môi trường Internet.

III. Đánh giá khả năng tiếp nhận và triển khai ứng dụng hệ điều hành Linux tại các đơn vị.

Để giúp cán bộ quản trị mạng của các đơn vị có khả năng tiếp cận với hệ điều hành Linux, Ban Điều hành Đề án 112 Chính phủ đã xây dựng giáo trình dạy hệ điều hành Unix và Linux, tổ chức các khoá đào tạo cho cán bộ quản trị mạng của các đơn vị. Thông qua các khoá học này, học viên được giới thiệu về nguyên lý làm việc của hệ điều hành Unix, Linux, các dịch vụ được cài đặt trên máy chủ Linux, lập trình trên hệ điều hành Linux.

Một mặt khác, từ kết quả khảo sát đã trình bày ở phần II.1.2, có thể thấy rằng tuy cán bộ quản trị mạng tại các đơn vị có khả năng hiểu và tiếp

nhận hệ điều hành Linux, nhưng lại không có đủ thời gian và điều kiện để tự nghiên cứu, thực hiện cài đặt hệ điều hành Linux và các dịch vụ trên đó.

Quá trình nghiên cứu, thử nghiệm của nhóm đề tài cũng cho thấy việc cài đặt các dịch vụ trên máy chủ Linux cũng không đơn giản như trên môi trường Windows. Sau khi cài đặt hệ điều hành từ đĩa CD do hãng Mandrake phát hành, một số phần mềm phải được sửa lỗi bằng các bản vá (patch) tải từ Internet. Việc quản trị cấu hình các dịch vụ đôi khi cũng có nhiều thủ thuật. Hạn chế này phát sinh từ các quy định của GPL, theo đó, các phần mềm có thể được tải về, biên dịch và sử dụng miễn phí, nhưng không được quyền tải các bản đã sửa lỗi lên mạng.

Để việc tiếp nhận và triển khai hệ điều hành Linux của các đơn vị được thuận lợi, một số yêu cầu được đặt ra như sau:

- Các phần mềm phải được đóng gói sẵn.
- Việc cài đặt cần được hướng dẫn cụ thể theo hình thức "step by step", bên cạnh đó, cần có các mẫu cấu hình.
- Tài liệu hướng dẫn quản trị và khai thác.
- Các cán bộ quản trị mạng cần được đào tạo và có môi trường thử nghiệm.

CHƯƠNG IV: CÁC GIẢI PHÁP KỸ THUẬT

I. Tổng quan về giải pháp kỹ thuật

Nhóm đề tài đưa ra "giải pháp Linux" trong khai thác và quản trị mạng LAN bao gồm các giải pháp cụ thể như sau :

1. Giải pháp hệ điều hành : Cài đặt hệ điều hành Mandrake 10.0 và một số phần mềm tiện ích, thiết lập môi trường làm việc cho người sử dụng.

2. Giải pháp cài đặt các dịch vụ trên máy chủ :

- Chọn lựa giải pháp phần mềm máy chủ : dùng phần mềm Apache làm Web Server , dùng BIND làm DNS Server , dùng QMail để làm mail server.

- Nghiên cứu trình tự thực hiện việc cài đặt các dịch vụ, tải phần mềm và các bản sửa lỗi trên Internet, đóng gói phần mềm cùng các bản sửa lỗi, tạo lập các tập tin cấu hình mẫu, xây dựng tài liệu hướng dẫn cài đặt và thiết lập cấu hình dịch vụ.

- Nghiên cứu việc quản trị các dịch vụ, xây dựng tài liệu hướng dẫn sử dụng.

3. Giải pháp chia sẻ tài nguyên trên mạng

- Sử dụng phần mềm Samba phục vụ chia sẻ file và máy in.

4. Giải pháp an toàn thông tin trên mạng

- Sử dụng OpenLDAP quản lý việc đăng nhập và sử dụng tài nguyên trên mạng.

- Sử dụng cặp phần mềm NetFilter/IPTables để xây dựng bức tường lửa để kiểm soát sự truy cập mạng và bảo vệ mạng nội bộ khỏi sự tấn công từ bên ngoài.

5. Giải pháp xây dựng phần mềm phục vụ quản trị dịch vụ mạng.

- Xây dựng một số ứng dụng với giao diện tiếng Việt phục vụ việc quản trị các dịch vụ được cài đặt.

6. Giải pháp đào tạo

- Xây dựng tài liệu hướng dẫn triển khai cài đặt và ứng dụng hệ thống cụ thể tại đơn vị tùy thuộc quy mô hệ thống mạng LAN của đơn vị.

- Tổ chức lớp đào tạo cho cán bộ quản trị mạng các đơn vị.

II. Giải pháp hệ điều hành : Cài đặt Mandrake Linux 10.0

1. Cài đặt ban đầu

1.1. Cài đặt máy chủ Linux

Kiểm tra các thiết bị phần cứng, chú ý các phân vùng của ổ đĩa

Trong quá trình cài đặt lựa chọn các ứng dụng server để thiết lập các ứng dụng server cần thiết để thành máy chủ Linux.

Cài đặt thêm các dịch vụ server từ Mandrake Control Center như DNS Bind, Samba. Các dịch vụ server như LDAP, Mail Server tải từ các nhà cung cấp.

1.2. Cài đặt máy trạm Linux

Việc cài đặt máy trạm cũng giống như cài đặt máy chủ nhưng trong lúc cài đặt chỉ chọn các ứng dụng cài đặt dành cho máy trạm.

Cài đặt Open Office, Koffice Kmail, Kontact để hỗ trợ việc soạn văn bản và gửi nhận Email.

Cài đặt các trình duyệt web như mozilla, opera,...

1.3. Cài đặt nhiều hệ điều hành trên một máy tính

Dùng chương trình Partition Magic để phân chia các phân vùng của Windows và phân vùng của Linux

Tiến hành cài đặt, việc cài đặt thì cũng giống như cài đặt như trên đã trình bày.

Cài đặt trình Boot loader (LILO) vào MBR (Master Boot Record) cho phép hiển thị danh sách các HĐH tồn tại trong cùng một máy để lựa chọn khi khởi động.

1.4. Cài đặt MandrakeLinux 10.0 trên máy ảo

Trong trường hợp muốn cài đặt nhiều hệ điều hành mà không ảnh hưởng đến HĐH đang sử dụng thì ta phải dùng phần mềm máy ảo (virtual machine-VM) VMware Workstation 4.0.

VM là một môi trường phần mềm cho phép một hoặc hơn một HĐH và các ứng dụng của chúng hoạt động song song trên chỉ một máy tính duy nhất. Điểm thú vị là ta có thể chuyển đổi qua lại giữa các HĐH đang chạy chỉ bằng một hoặc hai thao tác mà không phải khởi động lại PC. Đối với các HĐH, không có gì khác biệt giữa VM và PC thật (real computer). Nói một cách ngắn gọn, VM chính là một bản sao của PC thật. Gần như, điều gì bạn có thể làm được trên máy thật thì bạn cũng có thể làm được trên VM.

2. Cài đặt các ứng dụng

MandrakeLinux 10.0 quản lý việc cài đặt, gỡ bỏ hay cập nhật phần mềm bằng trình Mandrake Control Center.

2.1. Quản trị từ xa

Một khi hệ thống máy tính có nhiều máy chủ thì việc cấu hình và quản trị cho từng máy sẽ khó khăn về việc di lại. Để quản trị từ xa thì yêu cầu máy chủ Mandrakelinux 10.0 phải được cài đặt các trình ứng dụng như

Tightvncserver, Telnetservice và tại máy trạm chúng ta phải cài trình **TightVNC Client**.

Ngoài chương trình quản trị từ xa sử dụng VNC, Linux còn có ứng dụng Webmin cho phép quản trị từ xa thông qua giao diện Web. Trên giao diện Web này, có thể cấu hình các thiết bị phần cứng cũng như cài đặt các gói phần mềm một cách dễ dàng.

2.2. Cài đặt phần mềm soạn thảo tiếng Việt trên Linux

Để soạn thảo tiếng Việt trong MandrakeLinux 10.0 cần phải cài đặt bộ gõ tiếng Việt. Có nhiều bộ gõ tiếng Việt khác nhau như: **Xvncb, Xunkey**; và còn phải có bộ Font tiếng Việt Utf8. Bộ Font này phải được cài đặt vào fonts của hệ thống MandrakeLinux 10.0.

2.3. Cài đặt phần mềm Winpower cho MandrakeLinux 10.0

Phần mềm này cho phép máy chủ Linux sử dụng UPS online để quản lý việc bật tắt nguồn điện tự động. Việc sử dụng phần mềm nhằm bảo quản các thiết bị máy tính tốt hơn và đảm bảo ngắt điện an toàn.

III. Giải pháp cài đặt các dịch vụ trên máy chủ Linux.

1. Giải pháp Web Server : Apache

1.1. Giới thiệu về dịch vụ web server Apache:

Apache trở thành web server phổ biến trên Internet từ tháng 4 năm 1996. Đến tháng 1 năm 2005, theo thống kê của Netcraft hơn 68% các web site trên Internet dùng Apache làm web server, vì vậy Apache được đánh giá là web server được dùng phổ biến nhất hiện nay.

Với phiên bản 2.0, nhiều modul mới đã được đưa vào để tăng cường bảo mật và quản trị: mod_auth_ldap để xác thực qua LDAP, mod_autoindex làm rõ cách hiển thị danh mục của các thư mục, mod_deflate cho phép nén dữ liệu trước khi đưa lên mạng để tiết kiệm băng thông.

Giải pháp cài đặt phần mềm web server Apache hướng tới mục tiêu tạo một môi trường phù hợp và ổn định để cài đặt các ứng dụng web cho mạng LAN. Cụ thể trong khuôn khổ đề án 112, các phần mềm dùng chung đều là các ứng dụng web chạy trên nền web server Apache.

1.2. Mục tiêu đặt ra:

- Tìm hiểu cài đặt dịch vụ web server Apache;
- Tìm hiểu cấu hình dịch vụ web server Apache;
- An toàn cho dịch vụ;
- Tìm hiểu xây dựng ứng dụng dựa trên hệ thống web portal (phiên bản PHP-NukeViet).

1.3. Các nội dung đã thực hiện :

Cài đặt dịch vụ:

- + Cài từ gói kèm theo đĩa Mandrake
- + Cài từ gói ở dạng mã nguồn

Quản lý cấu hình dịch vụ:

- + Dùng công cụ quản trị Webmin
- + Chỉnh sửa các file cấu hình: httpd.conf, vhosts.conf.

Bảo mật web server Apache:

- + Đặt các quyền trên các file cấu hình hay thư mục cài web server
- + Bảo vệ thư mục chứa ứng dụng web bằng cách kiểm tra xác thực người dùng thông qua tập tin mật khẩu
- + Chỉ định địa chỉ IP được quyền truy cập
- + Chống các lỗi SQL-Injection
- + Mã hoá dữ liệu trên đường truyền (sử dụng giao thức https thay thế cho http ở những trang gửi các thông tin quan trọng trên đường truyền)
- + An toàn trước khả năng bị tấn công của CSS (Cross-Site Scripting)

Cách cài đặt một số gói phần mềm liên quan: để xây dựng các ứng dụng web chạy trên hệ thống Linux, ngoài việc cài đặt chính là web server Apache, cần cài thêm các gói phần mềm liên quan như MySQL để làm hệ quản trị cơ sở dữ liệu, OpenSSL để hỗ trợ việc mã hoá dữ liệu trên đường truyền, ngôn ngữ kịch bản phía server PHP.

Cải tiến, chỉnh sửa từ ứng dụng Web mã nguồn mở NukeViet để xây dựng website giới thiệu Trung tâm Tin học Văn phòng (mang tính chất minh hoạ). Ứng dụng với các chức năng sau:

- + Tải các văn bản pháp quy
- + Lịch công tác
- + Danh bạ điện thoại
- + Tin tức, sự kiện và các hoạt động đơn vị

1.4. Kết quả thu được

Xây dựng tài liệu hướng dẫn theo từng bước ("step-by-step") cách cài đặt và quản trị dịch vụ.

Một số biện pháp bảo mật cho dịch vụ: về căn bản đáp ứng được nhu cầu bảo mật cho ứng dụng.

Sử dụng MySQL làm hệ quản trị cơ sở dữ liệu: MySQL hoàn toàn miễn phí, tốc độ truy vấn thông tin nhanh, khả năng sử dụng dễ dàng và có rất

nhiều công cụ hỗ trợ trong việc quản trị phù hợp với các đơn vị có khối lượng dữ liệu nhỏ.

Website giới thiệu Trung tâm Tin học Văn phòng (mang tính chất minh họa). Với các chức năng cơ bản hiện có, hoàn toàn có thể xây dựng thành các trang thông tin cho các sở ban ngành, tiết kiệm rất nhiều so với kinh phí xây dựng hiện nay.

2. Giải pháp Mail server : Qmail

Trên hệ thống server Windows có nhiều phần mềm về mail nổi tiếng như: MS Exchange Server, Daemon,... Còn trên hệ thống server là Linux cũng có rất nhiều phần mềm làm công cụ MTA như: Sendmail, Postfix,... nhưng đặc biệt hơn cả là qmail với tỷ lệ sử dụng cao và ngày càng tăng trên thế giới.

Căn cứ kết quả so sánh qmail so với các phần mềm khác (Sendmail) về tính bảo mật, tính hiệu năng, độ tin cậy, tính giản đơn, phần mềm qmail được chọn là giải pháp để thiết lập máy chủ thư tín điện tử trong giải pháp Linux.

2.1. Mục tiêu đặt ra

Gửi và nhận mail giữa các user trong cùng một hệ thống mail nội bộ.

Gửi và nhận mail giữa các user của các hệ thống mail trong mạng nội bộ.

Có thể ứng dụng rộng rãi tại các đơn vị.

2.2. Phương pháp nghiên cứu

Tìm hiểu các hệ thống MTA (Message Transfer Agent) hiện có đang được dùng với hệ điều hành mã nguồn mở: qMail, SendMail,...

Đánh giá và phân tích các hệ thống MTA này theo nhiều tiêu chí để lựa chọn giải pháp tối ưu làm nội dung cho đề tài. Chẳng hạn:

- + Sự ổn định của hệ thống;
- + Mức độ tin nhiệm của người sử dụng;
- + Khả năng thích ứng với các hệ điều hành;
- + Tài liệu phục vụ cho quá trình nghiên cứu;
- + Giá thành của sản phẩm;
- + ...

Qmail là giải pháp lựa chọn cho việc nghiên cứu Mail server.

2.3. Một số ưu điểm của Qmail

a) Tính bảo mật

Qmail được thiết kế với tính bảo mật cao, trong khi đó Sendmail đã từng là câu chuyện dài về những vấn đề bảo mật. Khi Sendmail được viết và ra đời thì môi trường mạng còn khá thân thiện, vấn đề bảo mật chưa được coi là vấn đề lớn. Về sau, Eric Allman, tác giả Sendmail cũng đã bổ sung các

module bảo mật. Tuy nhiên, tính bảo mật an toàn thư tín của Sendmail vẫn còn phải cải tiến hơn nữa.

b) Tính hiệu năng

Qmail phân phối mail theo cơ chế song song, ở chế độ mặc định qmail thực hiện đồng thời trên 20 phân phối.

Qmail có khả năng chuyển nhận hàng triệu thông điệp một ngày. Tuy nhiên, nếu biến thành một mail server phục vụ tất cả các mail protocol thì bị giới hạn trong vấn đề thẩm định (authentication).

c) Độ tin cậy

Mỗi lần qmail chỉ chấp nhận một thông điệp, nó cam đoan rằng dữ liệu sẽ không bị mất, qmail cũng hỗ trợ việc định dạng một mailbox mới và làm việc với độ tin cậy ngang bằng hoặc hơn Network File System (NFS) khi không bị khóa.

d) Tính giản đơn

Qmail nhỏ hơn mọi MTA đặc trưng khác.

e) Tính bản quyền

Qmail được viết ra nhằm mục đích phân phối mã nguồn mở và có thể sử dụng qmail dưới nhiều mục đích. Chẳng hạn, có thể phân phối lại mã nguồn qmail chưa được sửa đổi cũng như phân phối gói cài đặt qmail đã được kiểm định, hoặc có thể phân phối các vá lỗi cho qmail. Tuy nhiên, để tôn trọng bản quyền tác giả, không thể phân phối mã nguồn mở đã được sửa đổi.

2.4. Nội dung nghiên cứu

Cách cài đặt từ package và từ source code;

Cài đặt và cấu hình Qmail cùng các gói hỗ trợ kèm theo;

2.5. Mô tả phương pháp cài đặt

Về cơ bản việc xây dựng mail server sử dụng qmail bao gồm những công việc sau:

- + Cài đặt qmail: Dùng làm MTA và SMTP
- + Cài đặt Vpopmail: Dùng để nhận thư theo giao thức POP3 (Post Office Protocol) và cũng là cơ sở dữ liệu chứa hệ thống domains ảo và accounts.
- + Cài đặt Imap: Hỗ trợ việc nhận thư theo giao thức Imap.
- + Cài đặt VqAdmin, qmailadmin: Dùng làm công cụ để quản trị hệ thống domains ảo và accounts.
- + Cài Squirrelmail: Hỗ trợ việc gửi/nhận mail và thay đổi password mail thông qua giao diện web.

Chi tiết việc cài đặt được giới thiệu ở chương 5 trang 37 tài liệu hướng dẫn cài đặt Mandrake 10 và các dịch vụ.

2.6. Kết quả đạt được

Xây dựng bộ tài liệu hướng dẫn chi tiết cài đặt cùng với bộ phần mềm cài đặt.

Có thể gửi và nhận mail giữa các user trong cùng một hệ thống mail nội bộ.

Có thể gửi và nhận mail giữa các user của các hệ thống mail trong mạng nội bộ.

Với việc triển khai mạng trực thử nghiệm có thể thử nghiệm việc gửi nhận mail trên hệ thống mạng WAN

2.7. Đánh giá kết quả

Qua quá trình kiểm tra thực tế của nhóm nghiên cứu, của các chuyên gia làm việc trong lĩnh vực cung cấp dịch vụ mail, cùng với việc cài đặt thử nghiệm tại các đơn vị, nhóm nghiên cứu đánh giá:

- Có thể triển khai ứng dụng rộng kết quả nghiên cứu này tại các đơn vị;
- Đảm bảo tính hoạt động ổn định, thông suốt tại các đơn vị;
- Bộ công cụ phục vụ cho việc quản trị tiện lợi;

Tuy nhiên, ngoài các ưu điểm trên thì Qmail vẫn còn một số hạn chế nhất định :

- Quá trình cài đặt tương đối phức tạp, đòi hỏi tính chuyên nghiệp ở người quản trị hệ thống;
- Nhóm nghiên cứu chưa xây dựng các công đoạn cài đặt thành một script để tiện lợi cho việc cài đặt, do vậy việc cài đặt phải tuân thủ chặt chẽ theo tài liệu hướng dẫn cài đặt.

3. Giải pháp DNS Server: BIND 9.3

Mỗi máy tính trong một mạng máy tính (sử dụng giao thức TCP/IP) cần có một địa chỉ IP để có thể liên lạc với bất kỳ một máy nào khác trên mạng, địa chỉ này là một số 32 bit. Để truyền, nhận thông tin với một máy tính nào đó, cần phải biết địa chỉ IP của máy tính đó. Tuy nhiên, các địa chỉ IP chỉ có ý nghĩa đối với máy tính, đối với người sử dụng, việc phải nhớ các địa chỉ IP là một điều rất khó khăn. Đối với con người, sẽ là tốt hơn nếu phải nhớ một cái tên gọi nhớ nào đó cho một máy tính thay vì phải nhớ các địa chỉ IP.

Để làm được việc này, cần phải có một hệ thống (máy tính, mạng,...) nào đó làm nhiệm vụ quản lý, chuyển đổi các tên gọi nhớ do người sử dụng nhập vào (thân thuộc với con người) thành các địa chỉ IP mà máy tính có thể

hiểu được. Hệ thống này được gọi là hệ thống tên miền (DNS- Domain Name System).

DNS có thể được xem như là một cơ sở dữ liệu phân tán thông qua mối quan hệ client/server giữa DNS server và các client có yêu cầu phân giải tên. Name Server sẽ là nơi nắm giữ cơ sở dữ liệu, hồi đáp các truy vấn và chịu trách nhiệm cập nhật thông tin.

Phần mềm BIND 9.3 được lựa chọn là giải pháp cài đặt DNS. Trong thực tế, đây là phần mềm phổ biến nhất được sử dụng cho dịch vụ này.

3.1. Xác định Mục tiêu

- Hoàn chỉnh việc cài đặt cấu hình máy chủ DNS và khai thác dịch vụ DNS trên mạng
- Xây dựng ứng dụng quản lý dịch vụ DNS.

3.2. Sử dụng BIND làm DNS Server

BIND là từ viết tắt của - Berkeley Internet Name Domain. Gói phần mềm này cũng có thể được download để cập nhật từ địa chỉ <http://www.isc.org/bind>.

Đây là gói phần mềm miễn phí, phổ biến nhất trong các bộ phần mềm quản lý dịch vụ DNS, thường xuyên được cập nhật, hiệu chỉnh.

BIND bao gồm các thành phần:

- Name Server: Lưu trữ thông tin về không gian tên miền (domain name space). Name Server có đầy đủ thông tin về một miền nào đó của không gian tên, các thông tin này được gọi là zone, được nạp từ một file hoặc một Name Server khác.
- Resolver: Các DNS client được gọi là các resolvers, các resolvers sẽ gửi các yêu cầu truy vấn để phân giải từ tên máy tính (thân thuộc với con người) thành địa chỉ IP.

3.3. Nội dung thực hiện

Tìm hiểu việc cài đặt tải phần mềm phiên bản mới nhất từ địa chỉ Website <http://www.isc.org/bind>

Cài đặt cấu hình thông qua việc chỉnh sửa nội dung tập tin cấu hình đối với các loại Server khác nhau:

- + Master nameserver
- + Slave nameserver
- + Forwarding nameserver
- + Caching nameserver

Cấu hình cho DNS có khả năng cập nhật thông tin từ DHCP server.

Cấu hình máy trạm để sử dụng DNS.

Nghiên cứu khai thác các công cụ quản trị dịch vụ DNS
Xây dựng ứng dụng quản trị máy chủ DNS

Chi tiết những nội dung trên được trình bày trong chương 3 trang 25 tài liệu hướng dẫn cài đặt và chương 2 trang 27 tài liệu hướng dẫn sử dụng.

3.4. Kết quả đạt được

- Cung cấp tài liệu hướng dẫn cài đặt và cấu hình DNS;
- Có thể triển khai áp dụng dịch vụ DNS cài đặt trên Mandrake tại các sở, ban ngành,...

3.5. Cài đặt & cấu hình dịch vụ

Việc cài đặt phần mềm và xác lập cấu hình cho các máy chủ DNS đã hoàn thành, cụ thể:

- Cài đặt được DNS Server tại Trung tâm Tích hợp dữ liệu phục vụ việc phân giải tên miền cho các máy trên toàn mạng trực.
- Cài đặt được DNS Server phục vụ việc phân giải tên miền cho các máy trên cùng hệ thống mạng LAN tại đơn vị Sở, Ngành.
- Cấu hình DNS Server của đơn vị Sở, Ngành để chuyển tiếp yêu cầu tới DNS Server của Trung tâm Tích hợp dữ liệu trong trường hợp không tự phân giải được tên miền.

3.6. Xây dựng ứng dụng quản trị dịch vụ DNS

Việc quản trị máy chủ có thể thực hiện bằng nhiều hình thức: thông qua giao diện web hoặc bằng hình thức Telnet:

- Đối với hình thức Telnet: Xây dựng ứng dụng bằng ngôn ngữ Bash (Bash shell programming language), chuyên cho môi trường console, thông dụng trên các bản phân phối Linux.
- Đối với giao diện khai thác là Web: Xây dựng ứng dụng bằng ngôn ngữ PHP, chạy trên nền Webserver Apache của máy chủ Linux.

3.7. Đánh giá kết quả

Dịch vụ DNS đã được triển khai thực tế trên mạng LAN của các đơn vị Sở, Ngành cũng như tại Trung tâm Tích hợp Dữ liệu. Các kiến thức thu nhận được thông qua việc nghiên cứu đã giúp cán bộ quản trị mạng của Trung tâm Tin học và các Sở, Ngành thực hiện công việc của mình một cách hiệu quả hơn. Các phần mềm được xây dựng cũng cung cấp các giải pháp khá hiệu quả cho việc quản trị dịch vụ.

IV. Giải pháp chia sẻ tài nguyên trên mạng : Samba

Hiện tại, các máy chủ của các đơn vị chủ yếu là máy cài hệ điều hành Windows 2000 Server. Việc chuyển đổi qua hệ điều hành Linux ít nhất phải đảm bảo tương đương với hệ điều hành Windows các chức năng sau:

- In ấn, trao đổi và chia sẻ tài nguyên trên mạng được thông suốt, dễ dàng.
- Quản trị tập trung được các tài khoản người dùng và nguồn tài nguyên mạng.
- Giúp người dùng dễ dàng truy cập vào các máy tính, các nguồn tài nguyên trên mạng.
- Dịch vụ phải được quản lý dễ dàng, thuận tiện cho người quản trị mạng.
- Cho phép người dùng có thể truy cập vào các phân vùng khác nhau giữa các hệ điều hành Linux và Windows nếu được cài chung trên một máy.

Từ các yêu cầu trên, nhóm đề tài tiến hành lựa chọn Samba làm giải pháp chia sẻ tài nguyên trên mạng.

1. Nội dung nghiên cứu:

Nghiên cứu cài đặt Samba phục vụ việc trao đổi dữ liệu trên mạng. Các nội dung tìm hiểu bao gồm :

1. Nghiên cứu cách thức cài đặt từ đĩa CDROM và từ gói Source.
2. Cấu hình máy chủ Linux thành File Server và Print Server.
 - Cấu hình File Server thông qua việc cài đặt các thông số trong tập tin cấu hình smb.conf.
 - Cấu hình Print Server thông qua việc cài đặt các thông số trong tập tin cấu hình cupsd.conf.
3. Cấu hình máy chủ Linux trở thành Primary Domain Controller để quản trị tập trung tài khoản và các nguồn tài nguyên mạng.
4. Cấu hình máy chủ Linux trở thành Local Master Browser hoặc Domain Master Browser.

Việc cấu hình này được thực hiện thông qua việc cài đặt, chỉnh sửa các thông số trong tập tin cấu hình **smb.conf**

5. Cài đặt công cụ quản trị Samba là Samba Web Administration Tool (SWAT) để dễ dàng trong việc quản trị.

6. Sử dụng các tiện ích hỗ trợ truy cập vào các phân vùng khác nhau của Linux và Windows trên cùng một máy.

- Từ máy Linux truy cập vào phân vùng của Windows: sử dụng tiện ích *mount*, cho phép truy cập dữ liệu trên phân vùng Windows. Đối với định dạng FAT, ngoài việc cho phép truy cập dữ liệu để xem thông tin còn cho phép ghi dữ liệu vào.
- Từ máy Windows truy cập vào phân vùng của Linux: sử dụng tiện ích *explore2fs*.

Nội dung chi tiết xem ở chương 6 tài liệu hướng dẫn cài đặt và chương 5 tài liệu hướng dẫn sử dụng

2. Kết quả đạt được:

Cấu hình máy chủ Linux File Server và Print Server: Thông qua việc cài đặt Samba và cấu hình trong tập tin *smb.conf*, việc quản lý các tài nguyên trên máy Linux được dễ dàng, cho phép hay hạn chế các quyền truy cập tương ứng với mỗi tài nguyên.

Cấu hình máy chủ Linux trở thành Primary Domain Controller: Ở một mức độ vừa phải thì máy chủ miền Linux có thể thay thế cho máy chủ miền Windows, tuy nhiên nó không thể đáp ứng được đầy đủ các tính năng mà máy chủ Windows có thể làm được. Chẳng hạn: máy chủ Linux chưa quản lý được đầy đủ các quyền truy cập của các User, ngày giờ, thời gian được phép đăng nhập, máy tính mà người dùng được phép đăng nhập.

Cấu hình máy chủ Linux trở thành Local Master Browser hoặc Domain Master Browser: việc cấu hình dễ dàng thuận tiện, đáp ứng được yêu cầu truy vấn các máy tính có trong vùng từ người dùng, giúp người dùng có thể sử dụng các trình duyệt mạng để truy cập nhanh chóng vào các nguồn tài nguyên trên mạng.

Công cụ quản trị SWAT bằng giao diện Web có các hướng dẫn cụ thể chi tiết kèm theo trong công cụ rất tiện lợi và còn cho phép quản trị từ xa nên người quản trị có thể quản lý Samba dễ dàng hơn.

Một trong những phần mềm tiện ích giúp truy cập vào phân vùng Linux từ hệ điều hành Windows là *explore2fs*, một tiện ích miễn phí và không cần phải cài đặt.

Đối với phiên bản Mandrake 10 đã được hỗ trợ thuận lợi cho việc truy cập vào các phân vùng của Windows với các định dạng khác nhau NTFS, FAT. Và việc ánh xạ các phân vùng này đều đã được tự động không cần phải thực hiện lệnh.

V. Giải pháp an toàn, bảo mật thông tin trên mạng : sử dụng các phần mềm OpenLDAP, IPTables

1. Đặt vấn đề

Việc thiết lập mạng máy tính giúp cho các cơ quan, tổ chức thu được hiệu quả cao trong công tác. Tuy nhiên, có rất nhiều người do vô tình hay cố ý đã sử dụng mạng máy tính để hoạt động phá hoại, gây thiệt hại không nhỏ cho những người dùng thông tin trên mạng. Do đó, việc bảo vệ an toàn thông tin trên mạng đã và đang được rất nhiều người quan tâm.

Mục đích của việc kết nối mạng là để cho nhiều người từ những vị trí địa lý khác nhau vẫn có thể sử dụng chung các tài nguyên thông tin của nhau. Việc bảo vệ các tài nguyên trong mạng tránh khỏi mất mát hay bị kẻ xấu làm thay đổi, sai lệch (có thể do vô tình hay cố ý) hết sức phức tạp và khó khăn.

Vì không thể có giải pháp an toàn tuyệt đối, nên cần sử dụng đồng thời nhiều mức độ bảo vệ khác nhau tạo thành nhiều lớp "rào chắn" đối với các hoạt động xâm phạm. Việc bảo vệ thông tin trên mạng chủ yếu là bảo vệ thông tin cất giữ trong các máy tính, đặc biệt là trong các máy chủ (server) của mạng. Ngoài một số biện pháp nhằm chống thất thoát thông tin trên đường truyền, mọi cố gắng đều tập trung vào việc xây dựng các mức "rào chắn" thông dụng để bảo vệ thông tin tại các trạm của mạng, có thể khái quát thành sơ đồ sau:

1.1. Quyền truy cập (Access Rights)

Là một lớp bảo vệ trong cùng, nhằm kiểm soát các tài nguyên của mạng và quyền hạn thao tác trên các tài nguyên đó. Việc kiểm soát cấu trúc dữ liệu càng chi tiết càng tốt.

1.2. Đăng ký tên và mật khẩu (Login&Password)

Thực chất lớp bảo vệ này cũng kiểm soát quyền truy nhập, nhưng không phải ở mức thông tin, mà ở mức hệ thống (quyền truy nhập vào mạng). Đây là phương pháp bảo vệ phổ biến nhất vì đơn giản, ít phí tổn và cũng rất hiệu quả. Mỗi người sử dụng các tài nguyên của mạng đều phải đăng ký tên và mật khẩu trước.

Vấn đề được đề tài tập trung nghiên cứu là trên hệ thống mạng nhiều máy chủ, cần có cơ chế đăng nhập mạng hợp lý để làm trong suốt (không làm phiền người dùng) môi trường mạng.

1.3. Mã hoá dữ liệu (Data encryption)

Dữ liệu được biến đổi từ dạng nhận biết sang không nhận biết được theo một thuật toán nào đó (tạo mật mã) và sẽ được biến đổi ngược lại (giải mã) ở trạm nhận. Đây là lớp bảo vệ rất quan trọng được sử dụng rộng rãi trong môi trường mạng.

1.4. Bảo vệ vật lý (Physican Protection)

Lớp này nhằm ngăn cản truy cập vật lý bất hợp pháp vào hệ thống. Các biện pháp truyền thống thường được dùng như: Cấm tuyệt đối người không phân sự vào phòng đặt máy mạng, dùng khoá để khoá (khóa bằng cơ học hay bằng sinh học như khóa vân tay, khóa bằng ánh mắt...) hoặc cài cơ cấu bảo động khi có truy nhập bất hợp pháp vào hệ thống, hoặc dùng các trạm máy không có ổ đĩa mềm...

1.5. Bức tường lửa (Firewall)

Khi kết nối máy tính nội bộ của mình (ví dụ mạng LAN) với mạng bên ngoài (ví dụ mạng Internet), mọi tổ chức đều cài đặt các công cụ phần cứng, các phần mềm và thiết lập các chính sách an toàn thông tin, trong đó xác định những dịch vụ nào được sử dụng và bị cấm sử dụng trên mạng, cách thức sử dụng dịch vụ, xác lập các hạn chế trong việc sử dụng những dịch vụ này. Mục tiêu của việc này là để bảo vệ tài nguyên của hệ thống mạng nội bộ khỏi những hiểm họa từ mạng bên ngoài. Hệ thống này gọi là Firewall (bức tường lửa).

Nói một cách khác, việc bảo vệ mạng bằng Firewall có nghĩa là sử dụng các công cụ kỹ thuật để thiết lập các quy tắc bảo vệ mạng dựa trên chính sách an toàn thông tin của tổ chức. Phương pháp này được sử dụng nhiều trong môi trường Internet và công cụ thực hiện có thể ở phần cứng hoặc phần mềm. Đề tài sẽ tập trung nghiên cứu giải pháp phần mềm để xây dựng bức tường lửa.

Thông thường, việc xây dựng Firewall dựa trên một trong hai phương pháp dưới đây:

Tất cả những gì không được cho phép thì bị cấm.

Cách tiếp cận này ngăn chặn mọi liên lạc giữa các mạng trừ những dịch vụ và ứng dụng nào được cho phép bởi người quản trị mạng. Nó hạn chế những lỗ hổng tiềm năng trong việc bảo vệ mạng, nhưng cũng hạn chế sự tiện lợi cho người sử dụng khi khai thác các dịch vụ trên mạng.

Tất cả những gì không bị cấm thì được cho phép

Cách tiếp cận này cho phép mọi liên lạc giữa các mạng trừ những dịch vụ và ứng dụng nào bị cấm bởi người quản trị mạng. Nó tạo sự tiện lợi cho người sử dụng, nhưng là tiềm năng phát sinh các vấn đề nghiêm trọng trong việc bảo vệ mạng.

2. Xác định giải pháp bảo mật thông tin trên mạng

Đề tài giới hạn phạm vi nghiên cứu ở 2 vấn đề: quản lý đăng nhập mạng và xây dựng tường lửa.

2.1. Quản lý đăng nhập mạng

Để việc đăng nhập và sử dụng tài nguyên trên mạng được thuận lợi, cần lưu trữ một cách tập trung và quản lý thống nhất cơ sở dữ liệu về người dùng, tài nguyên trên mạng và quyền sử dụng tài nguyên trên các ứng dụng khác

nhau. Khi người sử dụng đăng nhập mạng hay khai thác một tài nguyên, hệ thống sẽ sử dụng cơ sở dữ liệu này để kiểm tra, xác định tính hợp pháp và quyền của người sử dụng.

Phần mềm OpenLDAP được nghiên cứu và sử dụng để hướng tới mục tiêu này. Đây là phần mềm mã nguồn mở được phát triển bởi nhóm phát triển dự án OpenLDAP có tên là OpenLDAP Foundation dựa trên nền LDAP server của Đại học Michigan. So với NIS, LDAP ưu việt hơn do có khả năng lưu trữ thông tin đa dạng, độ tin cậy cao với việc hỗ trợ cơ chế mã hoá SSL/TSL.

2.2. Xây dựng tường lửa (Firewall)

Với hệ điều hành Microsoft Windows, giải pháp xây dựng Firewall thường gặp là sử dụng các phần mềm thương mại như ISA của Microsoft, hay Kerio Winroute. Người quản trị mạng có nhiệm vụ thiết lập cấu hình theo quy định của phần mềm, phần mềm căn cứ vào đó để xây dựng cơ chế phân tích và quản lý các gói tin luân chuyển trên mạng qua Firewall.

Trên môi trường hệ điều hành Linux, thông thường sử dụng cặp phần mềm Netfilter/Iptables làm bức tường lửa bảo vệ khỏi sự truy cập trái phép.

Iptables là Firewall ứng dụng lọc gói dữ liệu rất mạnh, miễn phí và có sẵn trên Linux. Netfilter/Iptables gồm 2 phần là Netfilter ở trong nhân Linux và Iptables nằm ngoài nhân. Iptables chịu trách nhiệm giao tiếp giữa người dùng và Netfilter, tiếp nhận yêu cầu của người sử dụng và đẩy các luật của người dùng vào cho Netfilter xử lý. Netfilter tiến hành lọc các gói dữ liệu ở mức IP. Netfilter làm việc trực tiếp trong nhân, nhanh và không làm giảm tốc độ của hệ thống.

So với chương trình ipchains thông dụng trước đây, iptables phức tạp, cung cấp nhiều tính năng và có tính bảo mật cao hơn. Iptables được coi là "stateful firewall", có khả năng lưu giữ thông tin về các kết nối đi qua, từ đó cung cấp khả năng xác định và ngăn chặn các cuộc tấn công mà các firewall trước kia chưa có khả năng đối phó, trong khi vẫn đảm bảo việc yêu cầu/tra lời của các kết nối đã thiết lập được thuận tiện, dễ dàng kiểm soát.

Người quản trị mạng sẽ thiết lập chi tiết các quy định đối với những gói tin đi qua Firewall. Người quản trị mạng không có kinh nghiệm sẽ có cảm giác choáng ngợp lúc ban đầu, nhưng đôi lại, họ sẽ nhanh chóng hiểu được cơ chế luân chuyển các gói tin trên mạng, nắm được cách quản lý chúng và có khả năng can thiệp sâu vào việc quản lý gói tin.

3. Giải pháp dịch vụ thư mục : OpenLDAP

3.1. Một số khái niệm

Thư mục: Một cách chung nhất thư mục là nơi dùng để lưu trữ và cho phép thực hiện các thao tác truy nhập thông tin. Tuy vậy có thể khái niệm này trùng với khái niệm cơ sở dữ liệu, đối với một thư mục các đặc điểm nổi bật phân biệt với cơ sở dữ liệu đó là:

- Thư mục được thiết kế để phục vụ thao tác đọc hơn là thao tác ghi.
- Thư mục cung cấp cái nhìn tĩnh về dữ liệu.
- Các thao tác cập nhật trong thư mục là đơn giản, không có sự ràng buộc như trong cơ sở dữ liệu.

Dịch vụ thư mục: Dịch vụ thư mục cho phép truy nhập thư mục, có thể qua các giao thức mạng. Thường thì các dịch vụ này còn cho phép nhân bản và phân bố dữ liệu thư mục. Một ví dụ về dịch vụ thư mục đó là dịch vụ quản lý tên miền (Domain Name System, DNS) cho phép ánh xạ một tên máy với một địa chỉ IP thích hợp. Mỗi dịch vụ thư mục có 5 tính chất như sau:

- Dịch vụ thư mục có khả năng đáp ứng cao nhất cho việc đọc thông tin.
- Dịch vụ thư mục hiện thực mô hình phân bố hoá việc lưu trữ thông tin.
- Dịch vụ thư mục có thể mở rộng kiểu lưu trữ thông tin.
- Dịch vụ thư mục có khả năng mở rộng việc tìm kiếm.
- Dịch vụ thư mục thực hiện đồng bộ dữ liệu giữa các máy chủ thư mục (Directory server) lỏng lẻo về tính nhất quán.

LDAP (LDAP – Lightweight Directory Access Protocol): là một giao thức truy cập thư mục và có thể xem LDAP là một dịch vụ thư mục. Có thể liệt kê những đặc điểm nổi bật của giao thức này:

- là một giao thức mạng cho phép truy nhập các thông tin trong một thư mục.
- là một mô hình thông tin cho phép xác định cấu trúc và đặc điểm của thông tin trong thư mục.
- là một không gian tên cho phép xác định cách các thông tin được tham chiếu và tổ chức.
- một mô hình các thao tác cho phép xác định cách tham chiếu và phân bố dữ liệu.
- là một giao thức mở rộng.
- là một mô hình thông tin mở rộng.

LDAP không mô tả về cơ chế và nơi lưu trữ dữ liệu. LDAP server có thể sử dụng bất cứ cơ sở dữ liệu nào thích hợp để lưu trữ dữ liệu. Điều này dẫn đến LDAP không hỗ trợ giao dịch (transaction) và đặc tính khác của cơ sở dữ liệu. Dựa vào điểm này, client sẽ không bao giờ biết về cơ chế lưu trữ thông tin của server.

3.2. Cơ chế hoạt động của LDAP

LDAP hoạt động dựa trên mô hình client-server thông qua giao thức TCP/IP. LDAP server truy cập đến dữ liệu có cấu trúc theo kiểu cây thông tin thư mục lưu trữ trong một cơ sở dữ liệu xác định. Với việc tổ chức LDAP theo mô hình phân bố, thì thông tin có thể cung cấp từ nhiều LDAP server khác nhau.

Khi Client kết nối đến server để yêu cầu các thông tin phục vụ cho client. Thông tin yêu cầu của client có thể có ngay tại server mà client yêu cầu hoặc có ở các server khác nếu có nhiều server LDAP tổ chức theo kiểu phân bố thư mục. Nếu thông tin có thể cung cấp bởi chính LDAP server được yêu cầu thì LDAP server sẽ trả lời thông tin yêu cầu cho client, nếu thông tin được yêu cầu không thuộc sự quản lý của server yêu cầu thì server được yêu cầu sẽ nhận thông tin từ server khác chứa thông tin rồi trả lời cho client. Ngoài ra client có thể yêu cầu đến nhiều server LDAP khác nhau để cung cấp trong tình huống một server LDAP bị sự cố.

Để đảm bảo cơ sở dữ liệu được an toàn đối với việc truy cập của người sử dụng và quá trình trao đổi dữ liệu giữa client và server và giữa các server với nhau, OpenLDAP có hai cách để bảo mật.

Bảo vệ truy cập CSDL LDAP (Access Control Lists - ACLs): ACLs cung cấp bởi OpenLDAP là một cú pháp rất đơn giản, rất mềm dẻo và rất hiệu quả để hiện thực việc kiểm soát khả năng truy cập các entry trong hệ thống CSDL LDAP của người sử dụng.

Bảng sau tóm tắt các quyền truy cập khác nhau vào các entry trong CSDL LDAP. Mức truy cập cao hơn sẽ có tất cả khả năng của mức thấp.

Mức truy cập	Quyền truy cập
write	Truy cập để cập nhập giá trị thuộc tính
Read	Truy cập để đọc kết quả sau khi tìm thành công.
search	Truy cập để áp dụng các bộ lọc tìm kiếm
compare	Truy cập để so sánh giá trị thuộc tính
Auth	Truy cập để xác nhận. Đây là yêu cầu để client gửi user name theo kiểu DN và một vài kiểu uỷ nhiệm để xác định user.
None	Không truy cập.

Mã hoá thông tin trao đổi giữa Open LDAP server và Client (hay giữa các server với nhau): Để thực hiện điều này, sử dụng LDAP kết hợp với SSL/TLS. Khi sử dụng SSL/TLS thì cần phải tạo một certificate để giúp cho server và client có thể bắt tay với nhau để trao đổi dữ liệu.

3.3. Sử dụng dịch vụ thư mục LDAP với phần mềm OpenLDAP

Thực hiện xây dựng dịch vụ thư mục, nhóm đề tài sử dụng phần mềm OpenLDAP. Đây là phần mềm mã nguồn mở, hiện thực giao thức LDAP, được sử dụng rộng rãi, có tính ổn định cao và khả năng kết hợp với các ứng dụng khác dễ dàng.

Trong khuôn khổ đề tài, OpenLDAP sử dụng để xây dựng một dịch vụ thư mục với các chức năng như sau:

- Quản lý tập trung thông tin về người sử dụng (username, password, email...):
- Quản lý đăng nhập với tài khoản người sử dụng tập trung tại server LDAP.
- Quản lý tài nguyên dùng chung trên mạng

Việc cài đặt phần mềm OpenLDAP được thực hiện tự động trong quá trình cài đặt Mandrake Linux, tuy nhiên có thể nâng cấp bằng cách cài đặt từ mã nguồn phần mềm được phân phối tại địa chỉ <http://www.openldap.org>.

OpenLDAP là phần mềm hiện thực hoá giao thức LDAP, do đó OpenLDAP yêu cầu một cơ sở dữ liệu để lưu trữ thông tin về thư mục. Phần mềm cơ sở dữ liệu bắt buộc phải cài đặt trước khi cài đặt OpenLDAP để cung cấp các thư viện cho OpenLDAP thực hiện việc quản lý dữ liệu. Phần mềm quản lý cơ sở dữ liệu phục vụ cho OpenLDAP được cung cấp tại địa chỉ <http://www.sleepycat.com/>

Tài liệu đầy đủ về phần mềm Open LDAP được trình bày chi tiết trong chương 8 trang 72 của tài liệu hướng dẫn cài đặt Mandrake Linux 10.0 và các dịch vụ và chương 7 trang 139 của tài liệu hướng dẫn sử dụng Mandrake Linux 10.0 và các dịch vụ.

3.4. Nhận xét

Việc triển khai dịch vụ thư mục LDAP có những ưu điểm sau:

- Quản lý tập trung thông tin người sử dụng và tài nguyên trên mạng.
- Đảm bảo quản lý đăng nhập và truy cập tài nguyên trên mạng an toàn và hoạt động ổn định.
- Dễ dàng kết hợp với các ứng dụng khác.
- Phục vụ cho mục đích single-sign-on.
- Không đòi hỏi bản quyền phần mềm.

Tuy nhiên sử dụng dịch vụ LDAP cũng có hạn chế: quá trình cài đặt tương đối phức tạp, đòi hỏi tính chuyên nghiệp ở người quản trị hệ thống.

4. Giải pháp tường lửa : IPTables

4.1. Cơ chế hoạt động của Firewall

Nói một cách vắn tắt, bức tường lửa (firewall) là hệ thống ngăn chặn việc truy nhập trái phép từ bên ngoài vào mạng. Tường lửa thực hiện việc lọc bỏ những địa chỉ không hợp lệ dựa theo các quy tắc hay chỉ tiêu định trước.

Firewall có thể là hệ thống phần cứng, phần mềm hoặc kết hợp cả hai. Nếu là phần cứng, thì chỉ bao gồm duy nhất bộ định tuyến (router). Bộ định tuyến có các tính năng bảo mật tinh vi, trong đó có khả năng kiểm soát địa chỉ IP (IP Address là sơ đồ địa chỉ các trạm, tức host, trong hệ thống mạng). Quy trình kiểm soát cho phép người quản trị định ra những địa chỉ IP có thể kết nối với mạng được bảo vệ và ngược lại. Tính chất chung của các firewall là

phân biệt địa chỉ IP hay từ chối việc truy nhập không hợp pháp căn cứ trên địa chỉ nguồn.

Tường lửa cấp mạng

Mỗi dạng bức tường lửa khác nhau có những thuận lợi và hạn chế riêng. Dạng phổ biến nhất là tường lửa cấp mạng (Network-level firewall).

Loại tường lửa này thường dựa trên bộ định tuyến, vì vậy các quy tắc quy định tính hợp pháp cho việc truy nhập được thiết lập ngay trên bộ định tuyến. Mô hình tường lửa này sử dụng kỹ thuật lọc gói tin (packet-filtering technique), đó là tiến trình kiểm soát các gói tin qua bộ định tuyến.

Khi hoạt động, tường lửa sẽ dựa trên bộ định tuyến mà kiểm tra địa chỉ nguồn (source address) hay địa chỉ xuất phát của gói tin. Sau khi nhận diện xong, mỗi địa chỉ nguồn IP sẽ được kiểm tra theo các quy tắc do người quản trị mạng định trước.

Bức tường lửa dựa trên bộ định tuyến làm việc rất nhanh do chỉ kiểm tra lướt trên các địa chỉ nguồn mà không hề có yêu cầu thực sự nào đối với bộ định tuyến, không tốn thời gian xử lý những địa chỉ sai hay không hợp lệ. Tuy nhiên, ngoại trừ những điều khiển chống truy nhập, các gói tin mang địa chỉ giả mạo vẫn có thể thâm nhập ở một mức nào đó trên máy chủ đã được bảo vệ.

Một số kỹ thuật lọc gói tin có thể được sử dụng kết hợp với firewall để khắc phục nhược điểm nói trên. Địa chỉ IP không phải là thành phần duy nhất của gói tin có thể "mắc bẫy" bộ định tuyến. Người quản trị nên áp dụng đồng thời các quy tắc, sử dụng gói tin định danh kèm theo gói tin như thời gian, giao thức, cổng... để tăng cường điều kiện lọc. Tuy nhiên, sự yếu kém trong kỹ thuật lọc thông tin của firewall dựa trên bộ định tuyến không chỉ có vậy.

Một số dịch vụ gọi thủ tục từ xa (RPC) rất khó lọc một cách hiệu quả do các server liên kết phụ thuộc vào các cổng được gán ngẫu nhiên khi khởi động hệ thống. Dịch vụ gọi là ánh xạ cổng (portmapper) sẽ ánh xạ các lời gọi tới dịch vụ RPC thành số dịch vụ gán sẵn, tuy nhiên, do không có sự tương ứng giữa số dịch vụ với bộ định tuyến lọc gói tin, nên bộ định tuyến không nhận biết được dịch vụ nào dùng cổng nào, vì thế không thể ngăn chặn hoàn toàn các dịch vụ này, trừ khi bộ định tuyến ngăn toàn bộ các thông tin UDP. Việc ngăn chặn tất cả các gói tin UDP cũng sẽ ngăn luôn cả các dịch vụ cần thiết, ví dụ như DNS, dịch vụ đặt tên miền. Vì thế, dẫn đến tình trạng "tiền thoái lương nan".

Firewall dựa trên proxy

Một dạng phổ biến khác là firewall dựa trên ứng dụng proxy. Loại này hoạt động hơi khác với tường lửa dựa trên bộ định tuyến lọc gói tin. Công ứng dụng kiểm duyệt này dựa trên cơ sở phần mềm. Khi một người dùng không xác định kết nối từ xa vào mạng chạy công kiểm duyệt, chương trình sẽ ngăn chặn kết nối từ xa này. Thay vì nối thông, cửa khẩu sẽ kiểm tra các thành phần của kết nối theo những quy tắc định trước. Nếu thoả mãn các quy tắc, cửa khẩu sẽ tạo cầu nối giữa trạm nguồn và trạm đích.

Cầu nối đóng vai trò trung gian giữa hai giao thức. Ví dụ, trong một mô hình cổng kiểm duyệt đặc trưng, gói tin theo giao thức IP không được chuyển tiếp tới mạng cục bộ, lúc đó sẽ hình thành quá trình dịch mà cổng kiểm duyệt đóng vai trò bộ phiên dịch.

Ưu điểm của firewall công ứng dụng kiểm duyệt là không phải chuyển tiếp IP. Quan trọng hơn, các điều khiển thực hiện ngay trên kết nối. Sau cùng, mỗi công cụ đều cung cấp những tính năng thuận tiện cho việc truy nhập mạng. Do sự lưu chuyển của các gói tin đều được chấp nhận, xem xét, dịch và chuyển lại nên tường lửa loại này bị hạn chế về tốc độ. Quá trình chuyển tiếp IP diễn ra khi một server nhận được tín hiệu từ bên ngoài yêu cầu chuyển tiếp thông tin theo định dạng IP vào mạng nội bộ. Việc cho phép chuyển tiếp IP là lỗi không tránh khỏi, khi đó, cracker (kẻ bẻ khoá) có thể thâm nhập vào mạng.

Hạn chế khác của mô hình tường lửa này là mỗi ứng dụng bảo mật được tạo ra cho từng dịch vụ mạng. Như vậy, một ứng dụng dùng cho Telnet, ứng dụng khác dùng cho HTTP, ...

Do không thông qua quá trình chuyển dịch IP nên gói tin IP từ địa chỉ không xác định sẽ không thể tới máy tính trong mạng, do đó hệ thống cửa khẩu ứng dụng có độ bảo mật cao hơn.

Sử dụng tường lửa để bảo vệ mạng

Một trong những ý tưởng chính của tường lửa là che chắn cho mạng khỏi "tầm nhìn" của những người dùng bên ngoài không được phép kết nối, hay chí ít cũng không cho phép họ "rò" tới mạng. Quá trình này thực thi các chỉ tiêu lọc bỏ do người quản trị ấn định.

Hiện tại, tường lửa là phương pháp bảo vệ mạng phổ biến nhất, 95% "cộng đồng phá khoa" phải thừa nhận là dường như không thể vượt qua tường lửa. Song trên thực tế, tường lửa đã từng bị phá. Tất nhiên, nếu mạng có kết nối Internet và chứa dữ liệu quan trọng cần được bảo vệ, bên cạnh tường lửa, cũng nên tăng cường các biện pháp bảo vệ khác.

4.2. Cài đặt Firewall sử dụng Netfilter/Iptables

Netfilter được cài đặt sẵn trong nhân (kernel) của Linux, không đòi hỏi can thiệp trừ khi muốn biên dịch lại kernel.

Việc cài đặt phần mềm iptables nói chung được thực hiện tự động trong quá trình cài đặt Mandrake Linux, tuy nhiên có thể nâng cấp bằng cách truy cập địa chỉ <http://www.netfilter.org/downloads.html>

Công cụ iptables cho phép thiết lập các quy tắc Firewall, NAT, IP masquerading, v.v... Các thiết lập được gửi tới kernel và yêu cầu kernel thực hiện việc lọc các gói tin. Các thiết lập này sẽ mất đi khi máy tính khởi động lại. Để tránh việc này, cần xây dựng tập tin firewall script trong thư mục /etc/rc.d/init.d và thực thi lúc khởi động máy để các thiết lập được bền vững.

Tài liệu đầy đủ về công cụ iptables được trình bày chi tiết trong chương 7 trang 67 của tài liệu hướng dẫn cài đặt Mandrake Linux 10.0 và các dịch vụ

và chương 6 trang 118 của tài liệu hướng dẫn sử dụng Mandrake Linux 10.0 và các dịch vụ.

4.3. Triển khai giải pháp

Cách tiếp cận của nhóm đề tài trong việc cài đặt Firewall sử dụng Netfilter/Iptables là thực hiện các bước công việc sau:

- Khảo sát mô hình mạng tại các đơn vị.
- Tạo lập các tập tin firewall script mẫu tương ứng với các mô hình mạng.
- Chép tập tin mẫu lên máy chủ Linux và chỉnh sửa các thông số cho phù hợp với cấu hình máy chủ và thực thi; thiết lập cấu hình để firewall thực thi khi khởi động máy.
- Cài đặt các chương trình, cung cấp giao diện để người quản trị mạng có thể xác định, chỉnh sửa cấu hình firewall.

Khảo sát

Quá trình khảo sát, phân tích cho thấy có 3 mô hình cài đặt Firewall :

- Mô hình máy chủ đơn lẻ.
- Mô hình hai vùng.
- Mô hình ba vùng.

Mô hình máy chủ đơn lẻ

Cài đặt ở các đơn vị có hệ thống mạng nhỏ (1-2 Server), 1 máy chủ cài hệ điều hành Microsoft Windows và 1 máy chủ cài hệ điều hành Mandrake Linux.

Trên máy chủ Linux, các dịch vụ cần thiết phải được cài đặt: Web, FTP, Database để phục vụ các phần mềm dùng chung.

Các dịch vụ DNS, DHCP, chia sẻ tập tin và máy in sẽ tiếp tục được duy trì trên máy chủ Windows.

Bức tường lửa (Firewall) phải được cài đặt trên máy chủ Linux để đảm bảo tính hợp pháp của việc truy cập dịch vụ và bảo vệ máy chủ khỏi những cuộc tấn công.

Mô hình hai vùng

Cài đặt ở các đơn vị có hệ thống mạng trung bình (trên 2 Server trở lên), một máy tính được dành ra để cài đặt Firewall. Nhờ Firewall này, mạng LAN của đơn vị sẽ được cách biệt với kết nối với mạng trực (thông qua router SHDSL) và kết nối với Internet (thông qua router ADSL).

Các chính sách cần thiết sẽ được cài đặt trên Firewall để bảo vệ các máy trạm làm việc, các máy chủ Linux và Windows đặt sau Firewall khỏi những sự tấn công từ bên ngoài.

Mô hình ba vùng

Cài đặt ở các đơn vị có hệ thống mạng lớn gồm nhiều máy chủ được quy hoạch một cách chặt chẽ.

Mạng máy tính được chia là 3 vùng: vùng DMZ, vùng LAN, vùng WAN.

Vùng DMZ (Demilitarized Zone): cung cấp các dịch vụ cần thiết cho mạng bên ngoài trong khi vẫn che giấu các chi tiết về việc cung cấp và quản lý các dịch vụ của các máy tính trong vùng này. Trong vùng này chứa các máy chủ quản trị các dịch vụ như DNS, FTP, Mail, Web.

Vùng LAN (Local Area Network): là vùng mạng nội bộ, vùng này gồm có các máy trạm Windows và Linux hỗn hợp. Trong vùng mạng nội bộ sẽ sử dụng các dịch vụ từ vùng DMZ và truy cập WAN, Internet. Trong vùng này máy chủ Samba sẽ làm nhiệm vụ chia sẻ tài nguyên mạng.

Vùng WAN (Wide Area Network), Internet: là vùng mạng bên ngoài gồm Internet và mạng diện rộng được kết nối với các Sở, Ban, Ngành và UBND quận huyện.

Một máy chủ Linux cài đặt Firewall sẽ kết nối 3 vùng trên, đảm bảo việc kết nối giữa các vùng theo một chính sách thích hợp và bảo vệ tài nguyên của hệ thống mạng nội bộ (LAN) và hệ thống các máy chủ trong vùng DMZ khỏi những hiểm họa từ mạng bên ngoài (WAN, Internet).

Đánh giá

Đối với những đơn vị có mô hình mạng lớn, có nhiều máy chủ, mô hình 3 vùng là mô hình bắt buộc phải lựa chọn. Các dịch vụ được cài trên các máy chủ riêng biệt giúp việc quản lý dịch vụ được thuận tiện, các máy tính không bị tình trạng hoạt động quá tải. Hệ thống Firewall được cài đặt làm tăng khả năng kiểm soát và bảo vệ các máy chủ dịch vụ và các máy trạm trong mạng LAN.

Đối với những đơn vị có mô hình mạng nhỏ, trong điều kiện cho phép, nên áp dụng mô hình 2 vùng. Đối lại việc mất 1 máy tính làm Firewall, cũng có một số lợi ích đáng kể:

- Các máy tính trong mạng được bảo vệ khỏi sự tấn công từ bên ngoài.
- Công tác cấu hình để kết nối mạng trực cũng được thực hiện và quản lý tập trung, tiết kiệm công sức của cán bộ quản trị mạng.
- So với giải pháp mua thiết bị Firewall chuyên dụng, giải pháp Linux có tính năng tương tự nhưng giá thành rẻ hơn nhiều.

Xây dựng firewall script mẫu & Cài đặt tập tin

Các tập tin script mẫu được xây dựng bằng ngôn ngữ BASH với chung 1 cấu trúc

- Xóa cấu hình Firewall cũ.
- Xác định thông số các card mạng .
- Tải các modul phụ trợ và thiết lập các cấu hình chung.
- Thiết lập các quy tắc PREROUTE, POSTROUTE.
- Thiết lập các lệnh xử lý INPUT, FORWARD, OUTPUT.
- Thiết lập các quy tắc NAT .

- Bổ sung các lệnh phục vụ việc chống tấn công Server.

Để cài đặt trong thực tế, người quản trị mạng thông thường chỉ cần xác định chính xác thông số card mạng tại máy Firewall. Tuy nhiên, việc chỉnh sửa thêm hoàn toàn có thể được thực hiện một cách tương đối dễ tùy thuộc ý đồ người quản trị mạng.

Xây dựng ứng dụng quản trị

Được trình bày trong chương 8 - tài liệu hướng dẫn sử dụng Mandrake 10.0 và các dịch vụ.

5. Đánh giá kết quả thu được

Việc tìm hiểu lý thuyết về Cơ chế an toàn, bảo mật thông tin trên mạng đã được đề cập một cách tổng quan. Bên cạnh đó, đề tài cũng đã đi sâu tìm hiểu về OpenLDAP và xây dựng tường lửa bằng Iptables.

Một số nội dung như bảo vệ vật lý và mã hoá dữ liệu nằm ngoài khuôn khổ đề cương đề tài nên chưa được triển khai nghiên cứu kỹ, sẽ được nhóm đề tài quan tâm trong khuôn khổ một tài liệu khác phục vụ việc hoàn thiện Trung tâm Tích hợp Dữ liệu.

VI. Giải pháp xây dựng các ứng dụng quản trị máy chủ Linux

1. Mục đích và yêu cầu

1.1. Mục đích

- Xây dựng phần mềm quản trị các dịch vụ DNS, Firewall, chia sẻ file và xem thông tin về cấu hình máy chủ Linux từ máy trạm trong mạng LAN tại các đơn vị;
- Phần mềm được xây dựng trên hệ mã nguồn mở.

1.2. Yêu cầu

- Hệ thống phần mềm đáp ứng đầy đủ chức năng quản trị, phù hợp với mô hình mạng thực tế tại các đơn vị;
- Chương trình với giao diện tiếng Việt, trực quan, dễ tiếp cận, tiện lợi cho người sử dụng;
- Người quản trị mạng có thể ứng dụng phần mềm vào thực tế tại đơn vị mình.

2. Lựa chọn giải pháp

Theo mục đích và yêu cầu đối với các phần mềm quản trị máy chủ, giải pháp xây dựng phần mềm mà nhóm nghiên cứu tiến hành nhằm giúp người quản trị máy chủ có thể quản trị bằng nhiều hình thức (thông qua giao diện web hoặc bằng dòng lệnh).

Ngôn ngữ được lựa chọn xây dựng phần mềm:

- Đối với giao diện khai thác là Web: Ngôn ngữ được lựa chọn là PHP, chạy trên nền webserver là Apache của máy chủ Linux.
- Quản trị bằng dòng lệnh: Ngôn ngữ được lựa chọn là Bash (Bash shell programming language), chuyên cho môi trường console, thông dụng trên các bản phân phối Linux;

3. Nội dung nghiên cứu

- Tìm hiểu cấu trúc các file cấu hình của các loại dịch vụ;
- Tìm hiểu các chức năng của các chương trình quản trị hiện có;
- Nghiên cứu ngôn ngữ lập trình mã nguồn mở PHP và Bash phục vụ quá trình xây dựng phần mềm.

4. Kết quả đạt được

- Xây dựng các ứng dụng quản trị máy chủ;
- Xây dựng bộ tài liệu hướng dẫn sử dụng;
- Các phần mềm có thể ứng dụng tại các đơn vị.

Việc cung cấp một ứng dụng cho việc quản trị máy chủ Linux đối với một số dịch vụ cụ thể một số ưu điểm và hạn chế:

4.1. Ưu điểm

- Thuận tiện cho người sử dụng còn ít kinh nghiệm trong việc quản trị mạng, nhất là quản trị đối với máy chủ Linux;
- Ứng dụng DNS với các mẫu sẵn có cho một miền cụ thể, cho phép người sử dụng nhanh chóng nắm bắt cấu trúc, để từ đó có thể xây dựng nên các miền phù hợp với đơn vị mình;
- Ứng dụng Firewall cung cấp nhiều mô hình, người quản trị có thể lựa chọn mô hình phù hợp để thiết lập cấu hình firewall cho đơn vị mình;
- Có thể xem thông tin về cấu hình một máy chủ tại tất cả các máy trạm được phép xem.

4.2. Hạn chế

- Các ứng dụng DNS, Firewall khó ứng dụng trong các mô hình mạng có quy mô lớn, khó thích ứng đối với các cán bộ quản trị mạng chuyên nghiệp;
- Phải yêu cầu cài đặt dịch vụ trên từng máy chủ muốn xem thông tin cấu hình, thông tin chưa thật sự đầy đủ.

Nội dung chi tiết xem chương 8 trang 161 tài liệu hướng dẫn sử dụng

VII. Giải pháp xây dựng tài liệu phục vụ đào tạo

1. Mục tiêu

Với đối tượng được nhắm tới cho chương trình đào tạo bao gồm các chuyên viên quản trị mạng tại các đơn vị chưa được học hoặc mới làm quen với Linux, tài liệu đào tạo được xây dựng với mục đích giúp cho người quản trị nắm bắt được các khái niệm, các dịch vụ mà hệ điều hành Linux Mandrake cung cấp, từ đó có thể vận hành, sử dụng Linux để đáp ứng nhu cầu khai thác và quản trị dịch vụ mạng tại đơn vị. Hơn nữa, tài liệu này còn truyền đạt các kết quả nghiên cứu đề tài cho các quản trị mạng của các đơn vị tham gia phối hợp triển khai đề tài.

2. Tóm tắt nội dung tài liệu đào tạo

2.1. Làm quen với HĐH Mandrake Linux

- Giới thiệu về HĐH Linux;
- Cách cài đặt nhiều HĐH trên cùng một máy tính;
- Giới thiệu các giao diện đồ họa có trong Mandrake 10 và một số thao tác trên giao diện đồ họa như (giới thiệu menu start, các trình duyệt web, duyệt file, các thao tác trên file, cách truy cập ổ đĩa mềm CD, thay đổi ngôn ngữ tiếng Việt cho giao diện KDE, cấu hình desktop, tạo shortcut, thêm bớt các ứng dụng applet trên panel) ;
- Giới thiệu giao diện text và một số lệnh căn bản trong Linux;
- Soạn thảo tiếng Việt trong Linux;
- Giới thiệu các công cụ quản lý hệ thống bằng Mandrake Control Center (MCC), Webmin;
- Cách cài đặt và cập nhật các gói phần mềm ứng dụng trên Linux.

2.2. Giới thiệu, cách cài đặt và quản trị các dịch vụ trên máy chủ Linux:

Dịch vụ Samba - Chia sẻ tài nguyên trong hệ thống mạng

- Giới thiệu dịch vụ;
- Cách cài đặt dịch vụ;
- Cách tạo tài khoản Unix, tài khoản Samba, chuyển đổi từ tài khoản Unix thành tài khoản Samba, tự động hóa việc tạo tài khoản Samba khi có tài khoản Unix;
- Cách chia sẻ dữ liệu: Dữ liệu chia sẻ dùng chung hay phân quyền truy cập cho người dùng;
- Cách truy cập tài nguyên trong hệ thống mạng hỗn hợp;
- Cách cài đặt, chia sẻ và dùng chung máy in;

Dịch vụ Web server Apache

- Cách cài đặt Apache, MySQL, PHP;
- Khởi động và dừng dịch vụ;
- Khai báo cổng hay địa chỉ và cổng mà Apache lắng nghe các yêu cầu từ client;
- Tạo virtual host;
- Khai báo Alias.

Dịch vụ DNS server

- Giới thiệu dịch vụ và một số khái niệm liên quan đến dịch vụ DNS như Name server, Zone file, các loại bản ghi;
- Cài đặt dịch vụ, khởi động và dừng dịch vụ;
- Khai báo một tên miền: khai báo miền phân giải xuôi, khai báo miền ngược;
- Khai báo các bản ghi tại DNS server.

Dịch vụ mail server

- Giới thiệu dịch vụ mail và Qmail;
- Cài đặt qmail: Dùng làm MTA và SMTP;
- Cài đặt Vpopmail: Dùng để nhận thư theo giao thức POP3 (Post Office Protocol) và cũng là cơ sở dữ liệu chứa hệ thống domains ảo và accounts;
- Cài đặt imap: Hỗ trợ việc nhận thư theo giao thức imap;
- Cài đặt VqAdmin, qmailadmin: Dùng làm công cụ để quản trị hệ thống domains ảo và accounts;
- Cài Squirrelmail: Hỗ trợ việc gửi/nhận mail và thay đổi password mail thông qua giao diện web;
- Khai thác mail từ client.

2.3. Giới thiệu chương trình xây dựng quản trị máy chủ Linux với giao diện tiếng Việt

Hướng dẫn sử dụng các chương trình được xây dựng ở hai phiên bản (giao diện Web, giao diện dòng lệnh) phục vụ cho:

Quản lý cấu hình máy chủ

- Xem thông tin chung như: tên máy, địa chỉ IP, phiên bản kernel mà Linux đang chạy, HĐH Linux đang chạy, thời gian máy đã hoạt động;

- Xem thông tin về phần cứng;
- Xem thông tin bộ nhớ;
- Xem thông tin về hệ thống tập tin;
- Thêm và xóa người dùng;
- Đổi địa chỉ IP của 1 card mạng.

Quản lý dịch vụ DNS

- Tạo DNS server với các tham số mặc định;
- Tạo DNS server với yêu cầu tham số;
- Thêm mới một tên miền;
- Sửa đổi một tên miền;
- Thêm, sửa thông tin các bản ghi cho một miền;
- Xem và sửa file cấu hình.

Quản lý dịch vụ Firewall

- *Mô hình máy chủ dịch vụ đơn lẻ*: cho phép hay cấm các yêu cầu đến dịch vụ trên máy đó;
- *Mô hình 2 vùng (gồm vùng mạng nội bộ và vùng mạng bên ngoài)*:
 - + Mạng nội bộ truy cập bên ngoài: cho phép hay cấm các dịch vụ cho các máy bên trong truy cập mạng bên ngoài thông qua Gateway,
 - + Mạng bên ngoài truy cập vào mạng nội bộ: Cho phép hay cấm các máy bên ngoài truy cập vào các máy dịch vụ bên trong mạng nội bộ;
- *Mô hình 3 vùng (gồm vùng mạng nội bộ, vùng DMZ, vùng mạng bên ngoài)*:
 - + Mạng nội bộ truy cập bên ngoài: cho phép hay cấm các dịch vụ cho các máy bên trong truy cập mạng bên ngoài thông qua Gateway. Các máy bên ngoài không thể truy cập vào vùng mạng nội bộ,
 - + Mạng nội bộ truy cập vùng DMZ: cho phép hay cấm truy cập các dịch vụ trong vùng DMZ từ các máy trong vùng nội bộ,
 - + Mạng bên ngoài truy cập vào vùng DMZ: Cho phép hay cấm các máy bên ngoài truy cập vào các máy dịch vụ bên trong vùng DMZ.

3. Kết quả thu được sau các buổi đào tạo

- Nắm được các khái niệm cơ bản về hệ điều hành Mandrake 10;
- Cài nhiều HĐH trên một máy tính;

- Sử dụng công cụ sẵn có trong Linux để thiết lập một sơ cấu hình hệ thống;

- Soạn thảo tiếng Việt trong Linux;

- Cài đặt, chia sẻ máy in;

- Cài đặt, quản trị các dịch vụ DNS, Web server, Firewall, Samba Server và có thể sử dụng các công cụ quản trị được tạo ra cho mục đích quản lý dịch vụ.

Nội dung chi tiết xem ở tài liệu đào tạo

CHƯƠNG V: TRIỂN KHAI THỬ NGHIỆM

Qua kết quả khảo sát thực tế tại các đơn vị (trình bày tại chương II), nhóm nghiên cứu đề tài đã xác định có 3 nhóm quy mô mạng LAN: mạng nhỏ, mạng trung bình và mạng lớn.

Nhóm đề tài đặt ra nhiệm vụ là phải đưa ra một số mô hình mạng thích hợp với quy mô các mạng này với định hướng:

- Phát huy việc sử dụng hệ điều hành Linux để thay thế Windows.
- Tăng cường an ninh cho mạng.

Đối với các mạng nhỏ, do số lượng máy chủ có hạn nên tất cả các máy đều được sử dụng để cài đặt ứng dụng. Các máy tính trong mạng truy cập trực tiếp vào máy chủ cũng như kết nối trực tiếp với Router HDSL để kết nối mạng trực hay với Router ADSL để kết nối Internet.

Đối với các mạng trung bình, số lượng máy tính nhiều hơn, việc bảo vệ hệ thống mạng cũng vì thế cần được coi trọng hơn.

Đối với những mạng lớn, mô hình mạng cần được thiết kế cẩn thận để bảo đảm hệ thống mạng hoạt động an toàn và ổn định.

Tương ứng với các quy mô mạng LAN tại các đơn vị như trên, nhóm đề tài đề xuất 3 mô hình ứng dụng hệ điều hành Linux như sau:

I. Mô hình máy chủ đơn lẻ

Trên máy chủ Linux, các dịch vụ cần thiết phải được cài đặt: Web, FTP, Database để phục vụ các phần mềm dùng chung. Các dịch vụ DNS, DHCP, chia sẻ tập tin và máy in sẽ tiếp tục được duy trì trên máy chủ Windows.

Bức tường lửa (Firewall) phải được cài đặt trên máy chủ Linux để đảm bảo tính hợp pháp của việc truy cập dịch vụ và bảo vệ máy chủ khỏi những cuộc tấn công.

Trong khuôn khổ thử nghiệm, mô hình này được áp dụng tại Sở Ngoại Vụ và UBND quận Hải Châu.

II. Mô hình 2 vùng

Một máy tính được dành ra để cài đặt Firewall. Nhờ Firewall này, mạng LAN của đơn vị sẽ được cách biệt với kết nối với mạng trực (thông qua router HDSL) và kết nối với Internet (thông qua router ADSL). Với những đơn vị kết nối Trung tâm Tích hợp dữ liệu và Internet bằng Modem, máy tính này cũng đóng vai trò là Communication Server, là gateway của mạng LAN.

Tất cả dữ liệu ra và vào mạng LAN đều được kiểm soát bởi máy tính cài đặt Firewall. Các chính sách cần thiết sẽ được cài đặt trên Firewall để bảo vệ các máy trạm làm việc, các máy chủ Linux và Windows đặt sau Firewall khỏi những sự tấn công từ bên ngoài.

III. Mô hình 3 vùng

Mạng máy tính được chia làm 3 vùng: vùng DMZ, vùng LAN, vùng WAN.

1. Vùng DMZ (Demilitarized Zone):

Vùng phi quân sự hay thường được gọi là vùng DMZ sử dụng để chỉ tới phần của mạng máy tính, không phải thuộc mạng nội bộ, cũng không trực tiếp kết nối với mạng Internet. Vùng DMZ nằm giữa hai vùng mạng nói trên, cung cấp các dịch vụ cần thiết cho mạng bên ngoài trong khi vẫn che giấu các chi tiết về việc cung cấp và quản lý các dịch vụ của các máy tính trong vùng này.

Trong vùng này chứa các máy chủ quản trị các dịch vụ như DNS, FTP, Mail, Web.

2. Vùng LAN (Local Area Network):

Là vùng mạng nội bộ, vùng này gồm có các máy trạm Windows và Linux hỗn hợp. Trong vùng mạng nội bộ sẽ sử dụng các dịch vụ từ vùng DMZ và truy cập WAN, Internet. Trong vùng này máy chủ Samba sẽ làm nhiệm vụ chia sẻ tài nguyên mạng.

3. Vùng WAN (Wide Area Network), Internet:

Là vùng mạng bên ngoài gồm Internet và mạng diện rộng được kết nối với các Sở, Ban, Ngành và UBND quận huyện.

Một máy chủ Linux cài đặt Firewall sẽ kết nối 3 vùng trên, đảm bảo việc kết nối giữa các vùng theo một chính sách thích hợp và bảo vệ tài nguyên của hệ thống mạng nội bộ (LAN) và hệ thống các máy chủ trong vùng DMZ khỏi những hiểm họa từ mạng bên ngoài (WAN, Internet).

IV. Chọn lựa mô hình mạng phù hợp

Đối với những mạng lớn, có nhiều máy chủ, mô hình 3 vùng là mô hình bắt buộc phải lựa chọn. Các dịch vụ được cài trên các máy chủ riêng biệt giúp việc quản lý dịch vụ được thuận tiện, các máy tính không bị tình trạng hoạt động quá tải. Hệ thống Firewall được cài đặt làm tăng khả năng kiểm soát và bảo vệ các máy chủ dịch vụ và các máy trạm trong mạng LAN.

Đối với những mạng nhỏ, trong điều kiện cho phép, nên áp dụng mô hình 2 vùng. Đối lại việc mất 1 máy tính làm Firewall, cũng có một số lợi ích

nếu đã trình bày ở phần an ninh mạng : bảo vệ khỏi sự tấn công từ bên ngoài, quản lý tập trung, tiết kiệm công sức. Không cần mua thiết bị Firewall chuyên dụng đắt tiền.

V. Thực tế triển khai tại các đơn vị thử nghiệm

Trong quá trình triển khai, nhóm đề tài đã triển khai cài đặt thử nghiệm tại 5 đơn vị:

- Văn phòng UBND thành phố;
- Văn phòng Thành Ủy;
- Sở Giáo dục & Đào tạo;
- Sở Ngoại Vụ;
- UBND Quận Hải Châu.

1. Triển khai, cài đặt giải pháp tại UBND Quận Hải Châu

1.1. Hiện trạng

- Hệ thống mạng tại đơn vị thuộc hệ thống mạng nhỏ có 2 máy chủ và các máy trạm có cấu hình thấp. Một máy chủ cài đặt Hệ điều hành (HĐH) Windows Server 2003 triển khai các dịch vụ DNS, DHCP; một máy chủ được cài đặt HĐH Linux Mandrake 9.2 để phục vụ phần mềm dùng chung và Website điều hành.

- Hệ thống mạng được kết nối mạng trực của thành phố bằng router SHDSL (mạng diện rộng thành phố)

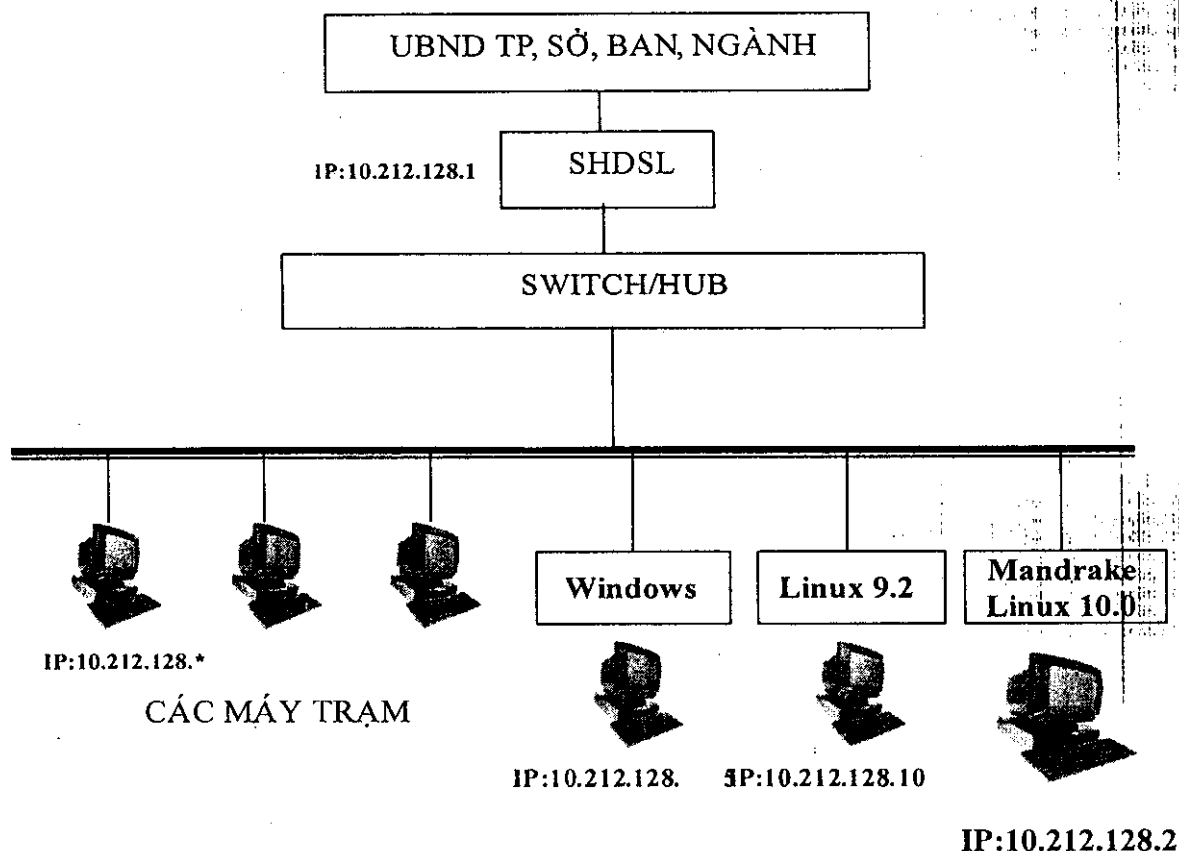
- Không có cơ chế để bảo vệ chống xâm nhập trái phép từ mạng bên ngoài vào mạng nội bộ.

1.2. Yêu cầu

- Do hệ thống mạng nhỏ và có ít máy chủ, cần triển khai cài đặt HĐH Mandrake Linux 10.0 trên máy PC mang tính chất thử nghiệm.

- Cài đặt các dịch vụ DNS, FTP, WEB
- Thực hiện việc chia sẻ tập tin thư mục giữa Windows và Linux
- Xây dựng hệ thống tường lửa (Firewall) để bảo vệ các dịch vụ trên máy chủ và tránh được sự xâm nhập bất hợp pháp từ mạng bên ngoài vào hệ thống máy chủ của đơn vị.

1.3. Mô hình triển khai



Hệ thống mạng của đơn vị được chia làm 2 vùng: Vùng mạng bên trong và vùng mạng bên ngoài.

- Vùng mạng bên trong: ngoài hệ thống máy chủ và máy trạm của đơn vị, nhóm đề tài cài đặt thêm một chủ Mandrake Linux 10.0 vào hệ thống mạng. Trên máy chủ này được triển khai cài đặt các dịch DNS, WEB, FTP, Samba và phần mềm tường lửa Iptables để bảo vệ các dịch vụ trên máy chủ này và đồng thời cung cấp các dịch vụ này ra mạng bên ngoài và mạng nội bộ.

- Vùng mạng bên ngoài: kết nối mạng diện rộng thành phố, các Sở, Ban, Ngành đều truy cập được dữ liệu tại đơn vị và ngược lại đơn vị cũng truy cập dữ liệu từ các Sở, Ban, Ngành.

1.4. Thực hiện cài đặt

- Cài đặt HĐH Mandrake Linux 10.0 lên máy tính có địa chỉ IP: 10.212.128.2 (xem hình vẽ);

- Cài đặt các dịch vụ DNS, WEB, FTP, SAMBA và xây dựng hệ thống Firewall trên một máy tính.

- Hệ thống tường lửa được cài đặt tại đơn vị đã ngăn được các cuộc tấn công và truy cập trái phép từ mạng bên ngoài, đồng thời cũng cung cấp các dịch vụ DNS, FTP, Web ra mạng bên ngoài.

1.5. Đánh giá kết quả triển khai cài đặt của quận Hải Châu

- Các dịch vụ đã cài đặt tại đơn vị chỉ dừng lại ở mô hình chạy thử, chưa đưa vào sử dụng thực tế do cơ sở hạ tầng không đảm bảo số lượng máy tính để đưa vào thực tế.

- Đã bổ sung thêm các dịch vụ FTP, Samba vào mô hình mạng tại đơn vị.

- Hệ thống tường lửa đã hoạt động tốt, bảo vệ được các dịch vụ trên hệ thống máy chủ và kiểm soát việc truy cập từ mạng bên ngoài đến các dịch vụ của hệ thống máy chủ.

2. Triển khai, cài đặt giải pháp tại Văn phòng Sở Ngoại Vụ

2.1. Hiện trạng

- Hệ thống mạng tại đơn vị thuộc hệ thống mạng nhỏ có 2 máy chủ và số lượng máy trạm ít. Một máy chủ cài đặt HĐH Windows Server 2003 triển khai dịch vụ DNS; một máy chủ được cài đặt HĐH Linux Mandrake 9.2 để phục cho phần mềm dùng chung và Website điều hành.

- Hệ thống mạng được kết nối mạng trực của thành phố bằng router SHDSL (mạng diện rộng thành phố) và kết nối Internet thông qua router ADSL.

- Không có cơ chế để bảo vệ chống xâm nhập trái phép từ mạng bên ngoài vào mạng nội bộ.

2.2. Yêu cầu

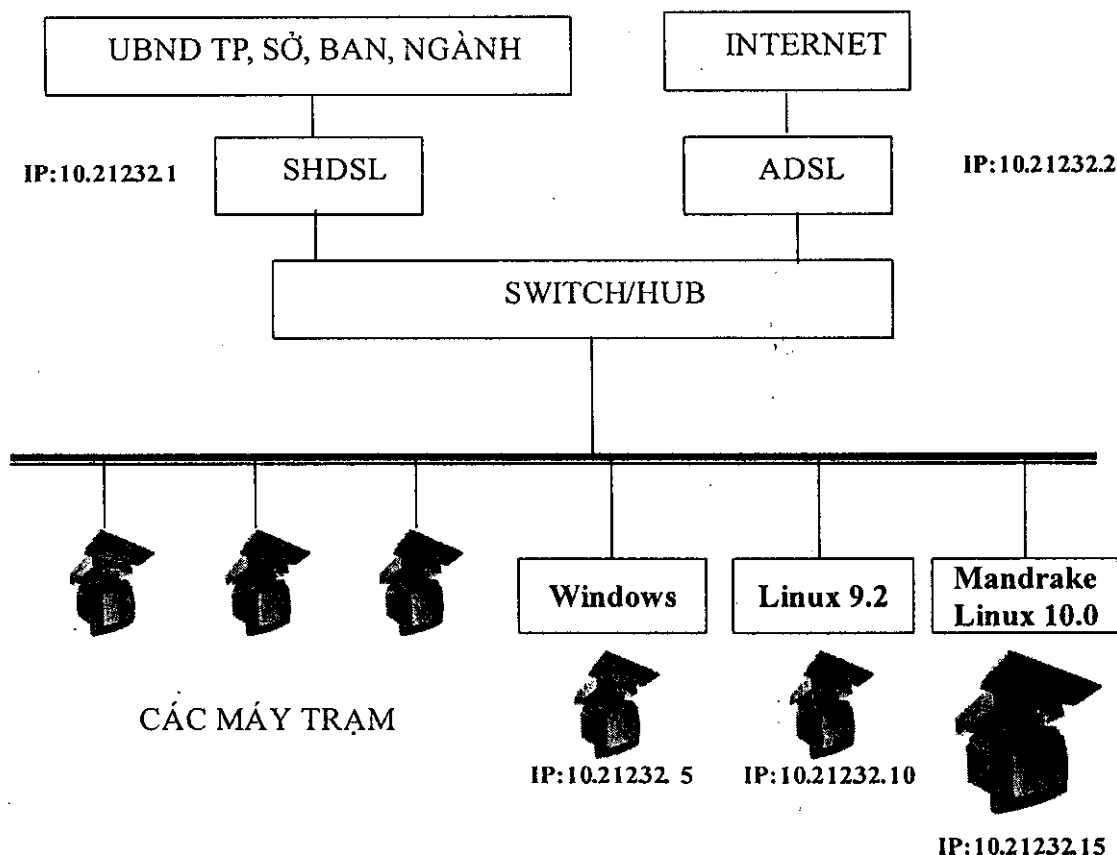
- Triển khai cài đặt HĐH Mandrake Linux 10.0 trên máy PC mang tính chất thử nghiệm.

- Cài đặt các dịch vụ DNS, FTP, WEB

- Thực hiện việc chia sẻ tập tin thư mục giữa Windows và Linux

- Xây dựng hệ thống tường lửa (Firewall) để bảo vệ các dịch trên máy chủ và tránh được sự xâm nhập bất hợp pháp từ mạng bên ngoài vào hệ thống máy chủ của đơn vị.

2.3. Mô hình triển khai



Hệ thống mạng của đơn vị được chia làm 2 vùng: Vùng mạng bên trong và vùng mạng bên ngoài.

- Vùng mạng bên trong: ngoài hệ thống máy chủ của đơn vị, nhóm đề tài cài đặt thêm một chủ Mandrake Linux 10.0 vào hệ thống mạng của đơn vị. Trên máy chủ này được triển khai cài đặt các dịch DNS, WEB, FTP, Samba và xây dựng tường lửa (Firewall) để bảo vệ các dịch vụ trên máy chủ này và đồng thời cung cấp các dịch vụ này ra mạng bên ngoài và mạng nội bộ.

- Vùng mạng bên ngoài: kết nối mạng diện rộng thành phố và mạng Internet. Các Sở, Ban, Ngành đều truy cập được dữ liệu tại đơn vị và ngược lại đơn vị cũng truy cập dữ liệu từ các Sở, Ban, Ngành thông qua mạng diện rộng.

2.4. Thực hiện cài đặt

- Cài đặt HĐH Mandrake Linux 10.0 lên máy tính có địa chỉ IP: 10.212.32.15 (xem hình vẽ).

- Cài đặt các dịch vụ DNS, WEB, FTP, SAMBA và xây dựng hệ thống Firewall trên một máy tính.

- Tường lửa được cài đặt tại đơn vị đã ngăn được các cuộc tấn công và truy cập trái phép từ mạng bên ngoài, đồng thời cung cấp các dịch vụ DNS, FTP, Web ra mạng bên ngoài.

2.5. Đánh giá kết quả triển khai cài đặt của Sở Ngoại vụ

- Triển khai HĐH Mandrake Linux 10.0 và các dịch vụ DNS, WEB, FTP và Samba tại đơn vị đã đưa vào sử dụng thực tế, các dịch vụ đã cài đặt được nhân sự ở đơn vị tiếp quản và sử dụng tốt.

- Máy chủ Linux này đã thay thế được máy chủ Windows trong hệ thống mạng của đơn vị.

- Hệ thống tường lửa đã ngăn chặn được các cuộc tấn công từ mạng bên ngoài và cung cấp các dịch vụ DNS, FTP, Web ra mạng bên ngoài và mạng nội bộ cũng truy cập được các dịch vụ này.

3. Triển khai, cài đặt giải pháp tại Sở Giáo dục và Đào tạo

3.1. Hiện trạng

Hệ thống mạng tại Văn phòng Sở Giáo Dục và Đào Tạo thành phố là một hệ thống lớn bao gồm nhiều máy chủ được lắp đặt và quy hoạch cụ thể trong hệ thống mạng theo các vùng nhất định của hệ thống.

- Vùng phi quân sự (DMZ): được chia 2 vùng, vùng các máy chủ thuộc đề án 112 và vùng các máy chủ Internet trực tiếp.

- Vùng mạng nội bộ (LAN): thì có 2 máy chủ DNS và DHCP làm nhiệm vụ cấp phát địa chỉ IP động và phân giải tên miền cho các máy trạm.

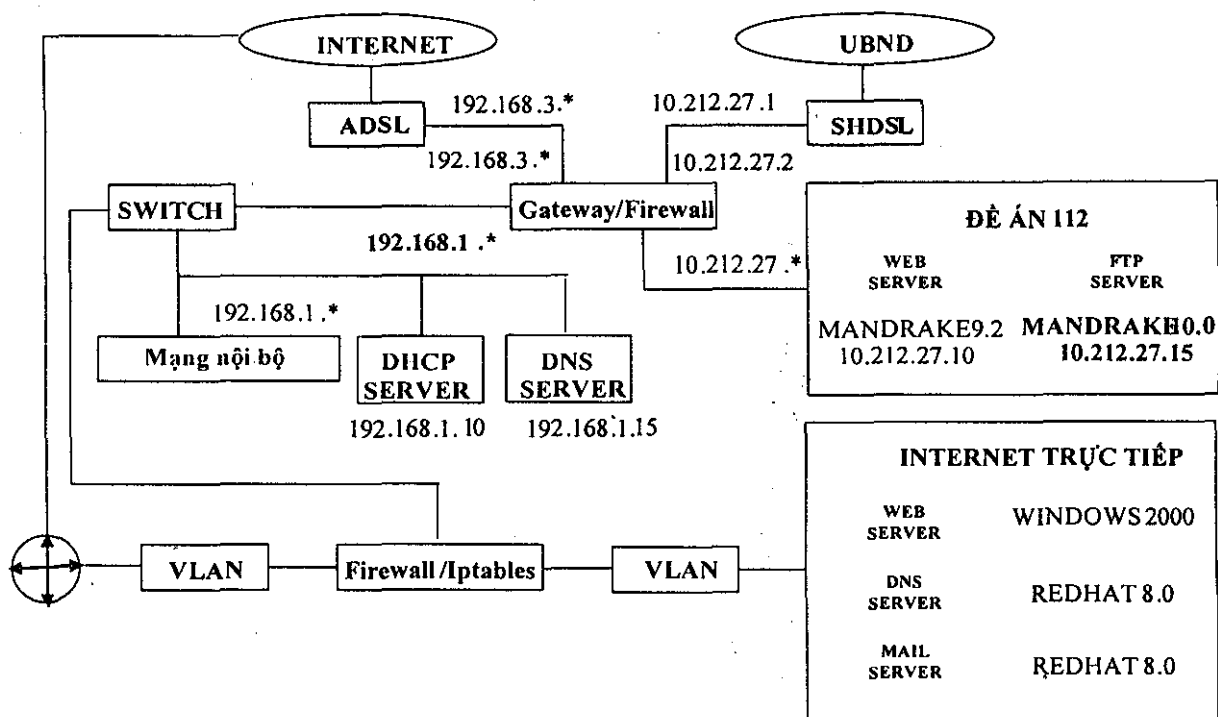
- Vùng mạng bên ngoài: được kết nối mạng trực của thành phố bằng router SHDSL (mạng diện rộng thành phố) và kết nối Internet thông qua router ADSL và đường truyền Leased-Line.

- Ngoài ra đơn vị có các máy chủ cung cấp dịch vụ ra mạng Internet và có xây dựng hệ thống tường lửa (Firewall) để bảo vệ các máy chủ trong vùng DMZ và đảm bảo việc truy cập của các máy trạm ra hệ thống mạng bên ngoài và ngăn cấm được sự xâm nhập từ mạng bên ngoài vào hệ thống mạng bên trong.

3.2. Yêu cầu

Hệ thống mạng của đơn vị đã triển khai đầy đủ các dịch vụ DNS, Mail, WEB, ..., đơn vị cần triển khai cài đặt bổ sung thêm dịch vụ FTP cho hệ thống mạng của đơn vị.

3.3. Mô hình triển khai



Hệ thống mạng của đơn vị được chia làm 3 vùng: Vùng phi quân sự (DMZ), vùng nội bộ (LAN) và vùng bên ngoài:

- Vùng phi quân sự (DMZ): được chia làm 2 vùng, vùng các máy chủ thuộc đề án 112 và vùng các máy chủ Internet trực tiếp. Ngoài các máy chủ dịch vụ đơn vị đã cài đặt, nhóm đề tài cài đặt bổ sung thêm máy chủ dịch vụ FTP trong vùng Đề án 112 của đơn vị (xem hình vẽ).

- Vùng nội bộ (LAN): thì có 2 máy chủ DNS và DHCP làm nhiệm vụ cấp phát địa chỉ IP động và phân giải tên miền cho các máy trạm.

- Vùng mạng bên ngoài: kết nối mạng diện rộng thành phố và mạng Internet. Các Sở, Ban, Ngành và mạng bên ngoài đều truy cập được dữ liệu tại đơn vị và ngược lại đơn vị cũng truy cập dữ liệu từ các Sở, Ban, Ngành thông qua mạng diện rộng.

- Đơn vị đã xây dựng hệ thống tường lửa (Firewall) để bảo vệ các máy chủ trong vùng DMZ và đảm bảo việc truy cập của các máy trạm ra hệ thống mạng bên ngoài và ngăn cấm được sự xâm nhập từ mạng bên ngoài vào hệ thống mạng bên trong.

3.4. Thực hiện cài đặt

- Cài đặt HĐH Mandrake Linux 10.0 lên máy tính có địa chỉ IP: 10.212.27.15 (xem hình vẽ).

- Cài đặt bổ sung thêm dịch vụ FTP cho hệ thống mạng của đơn vị.

3.5. Đánh giá kết quả triển khai cài đặt của Sở Giáo dục và đào tạo

Dịch vụ đã cài đặt là FTP trong vùng Đề tài 112 trong mô hình mạng của đơn vị đã cung cấp được cho hệ thống mạng bên ngoài, và từ mạng bên ngoài (mạng diện rộng) truy cập được các dịch vụ bên trong vùng DMZ.

4. Triển khai, cài đặt giải pháp tại Văn phòng Thành Ủy

4.1. Hiện trạng

Hệ thống mạng tại Văn phòng Thành Ủy thành phố là một hệ thống mạng cỡ lớn bao gồm nhiều máy chủ được lắp đặt tại vị trí nhất định trong hệ thống. Hệ thống này xây dựng theo mô hình nhiều vùng để bảo đảm an toàn dữ liệu. Các vùng giao tiếp với nhau thông qua hệ thống các tường lửa và máy chủ truyền thông để cho phép truy cập từ mạng bên ngoài vào hệ thống cũng như việc truy cập từ bên trong ra.

- Vùng an toàn: được chia làm hai vùng, vùng dành cho các máy chủ dịch vụ gọi là vùng phi quân sự (DMZ) gồm các máy chủ DNS, Web, Mail, Lotus Note và vùng mạng nội bộ (LAN) gồm các máy trạm. Vùng này được cài đặt máy chủ ISA làm tường lửa (Firewall) để tránh được sự xâm nhập trái phép từ mạng bên ngoài và hệ thống mạng nội bộ và cung cấp các dịch vụ cần thiết ra mạng bên ngoài.

- Vùng truyền thông: Lắp đặt máy chủ truyền thông làm nhiệm vụ cho phép mạng bên ngoài truy cập được các dịch vụ trong vùng an toàn và ngược lại cho phép các máy trạm từ vùng an toàn truy cập ra mạng bên ngoài..

- Vùng bên ngoài: kết nối mạng trực của thành phố bằng router SHDSL (mạng diện rộng thành phố) và kết nối Internet thông qua router ADSL. Trong vùng này đơn vị xây dựng máy chủ PROXY để kiểm soát việc truy cập Internet của các máy trạm trong vùng an toàn và đồng thời chia sẻ kết nối Internet cho các đơn vị trực thuộc kết nối đến Văn phòng Thành Ủy thông qua đường mạng trực.

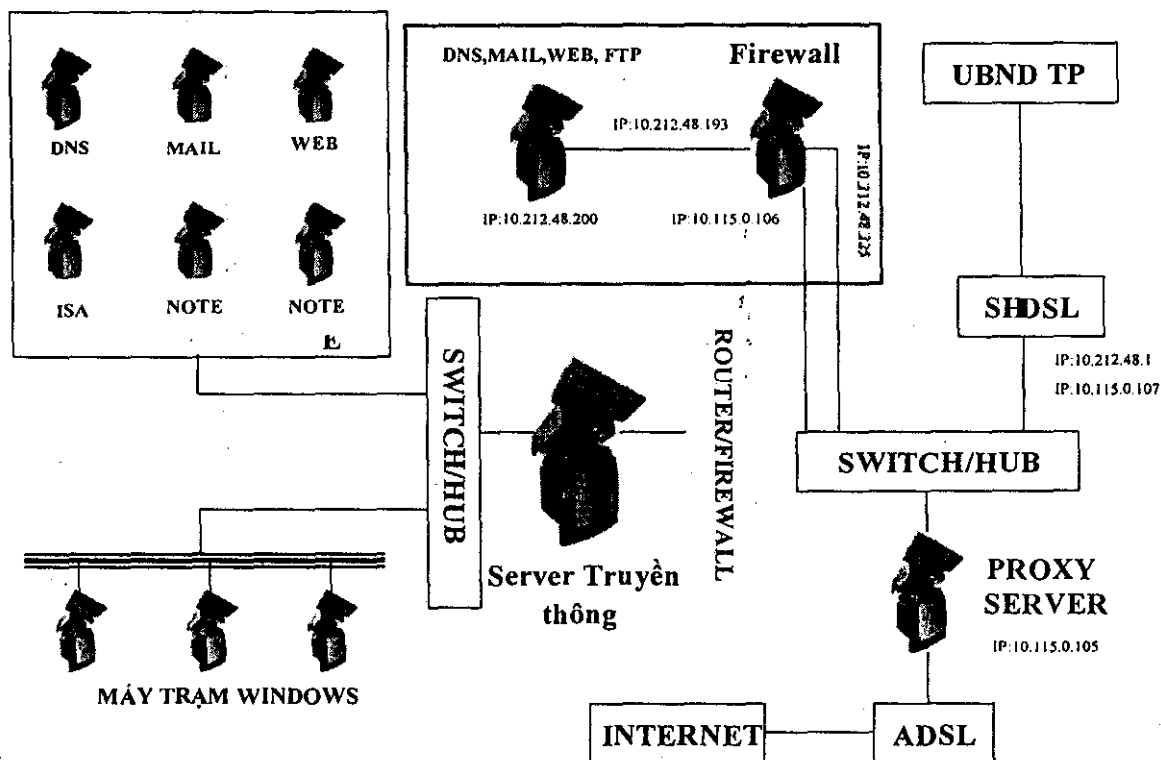
4.2. Yêu cầu

- Triển khai cài đặt HĐH Mandrake Linux 10.0 trên các máy PC mang tính chất thử nghiệm.

- Cài đặt các dịch vụ DNS, FTP, WEB, Mail

- Xây dựng hệ thống tường lửa (Firewall) để bảo vệ các dịch trên máy chủ và tránh được sự xâm nhập bất hợp pháp từ mạng bên ngoài vào hệ thống máy chủ của đơn vị.

4.3. Mô hình triển khai



Hệ thống mạng của đơn vị được chia làm các vùng như sau: Vùng an toàn, vùng truyền thông và vùng bên ngoài.

- Vùng an toàn: được chia làm hai vùng, vùng các máy chủ dịch vụ gọi là vùng phi quân sự (DMZ) gồm các máy chủ DNS Server, Web Server, Mail Server, Lotus Note và vùng mạng nội bộ (LAN) gồm các máy trạm (xem hình vẽ).

- Vùng truyền thông: Lắp đặt máy chủ truyền thông

- Vùng bên ngoài: kết nối mạng trực của thành phố và kết nối Internet. Trong vùng này nhóm đề tài đã triển khai xây dựng cài đặt mô hình mạng với các máy chủ Linux:

- + Vùng Phi quân sự (DMZ): cài đặt các dịch vụ DNS, WEB, Mail, FTP trên cùng một máy tính.

- + Xây dựng hệ thống tường lửa (Firewall) để bảo vệ các dịch vụ trong vùng DMZ trên và đồng thời cung cấp các dịch vụ này ra mạng bên ngoài.

4.4. Thực hiện cài đặt

- Cài đặt HĐH Mandrake Linux 10.0 lên các máy tính trong vùng bên ngoài của đơn vị.

- Cài đặt các dịch vụ DNS, FTP, WEB, Mail

- Xây dựng hệ thống tường lửa (Firewall) để ngăn được các cuộc tấn công từ mạng bên ngoài và cho phép mạng bên ngoài truy cập các dịch vụ DNS, Mail, FTP, Web bên trong vùng DMZ.

4.5. Đánh giá: kết quả triển khai cài đặt của Văn phòng Thành uỷ

- Triển khai HĐH Mandrake Linux mã nguồn mở ở Văn phòng Thành Ủy chỉ với mô hình thử nghiệm

- Các dịch vụ đã cài đặt hoạt động tốt và hệ thống tường lửa (Firewall) đã bảo vệ được vùng DMZ và ngăn chặn các cuộc tấn công từ mạng bên ngoài vào trong vùng DMZ và đồng thời cung cấp các dịch vụ ra mạng bên ngoài.

5. Triển khai, cài đặt giải pháp tại Văn phòng UBND thành phố

5.1. Hiện trạng

Hệ thống mạng tại Văn phòng UBND thành phố là một hệ thống lớn bao gồm nhiều máy chủ và nhiều máy trạm được lắp đặt và quy hoạch cụ thể trong hệ thống mạng theo các vùng nhất định của hệ thống. Các vùng giao tiếp với nhau thông qua hệ thống tường lửa (Firewall).

Mô hình mạng tại Văn phòng UBND thành phố được chia thành các vùng như sau:

Vùng dữ liệu: cài đặt hai máy chủ, 1 máy chủ LDAP (cơ sở dữ liệu về người sử dụng), 1 máy chủ Cơ sở Dữ liệu phần mềm dùng chung Oracle. Hai máy chủ này đều được triển khai trên hệ điều hành Linux.

Vùng DMZ: được cài đặt các máy chủ phục vụ các dịch vụ truy cập từ bên ngoài: DNS, Web, Mail. Tất cả các dịch vụ này đều được triển khai trên hệ điều hành Linux. Vùng này cung cấp các dịch vụ cho bên ngoài mạng diện rộng thành phố thông qua router SHDSL và ra ngoài Internet thông qua trung tâm công nghệ phần mềm (chỉ cung cấp dịch vụ mail).

Vùng truy cập: kết nối với các Sở Ban Ngành, Quận huyện thông qua router SHDSL và kết nối ra Internet thông qua router ADSL.

Vùng mạng nội bộ Văn phòng UBND (LAN): xây dựng 1 máy chủ DNS và DHCP trên nền HĐH Windows này làm nhiệm vụ cấp phát địa chỉ IP động và phân giải tên miền cho các máy trạm trong hệ thống mạng; 1 máy chủ Web, 1 máy chủ cơ sở dữ liệu chạy trên nền Hệ điều hành Windows; 1 máy chủ chạy phần mềm dùng chung được triển khai trên hệ điều hành Mandrake Linux.

5.2. Yêu cầu

- Triển khai cài đặt HĐH Mandrake Linux 10.0 trên các máy PC mang tính chất thử nghiệm.

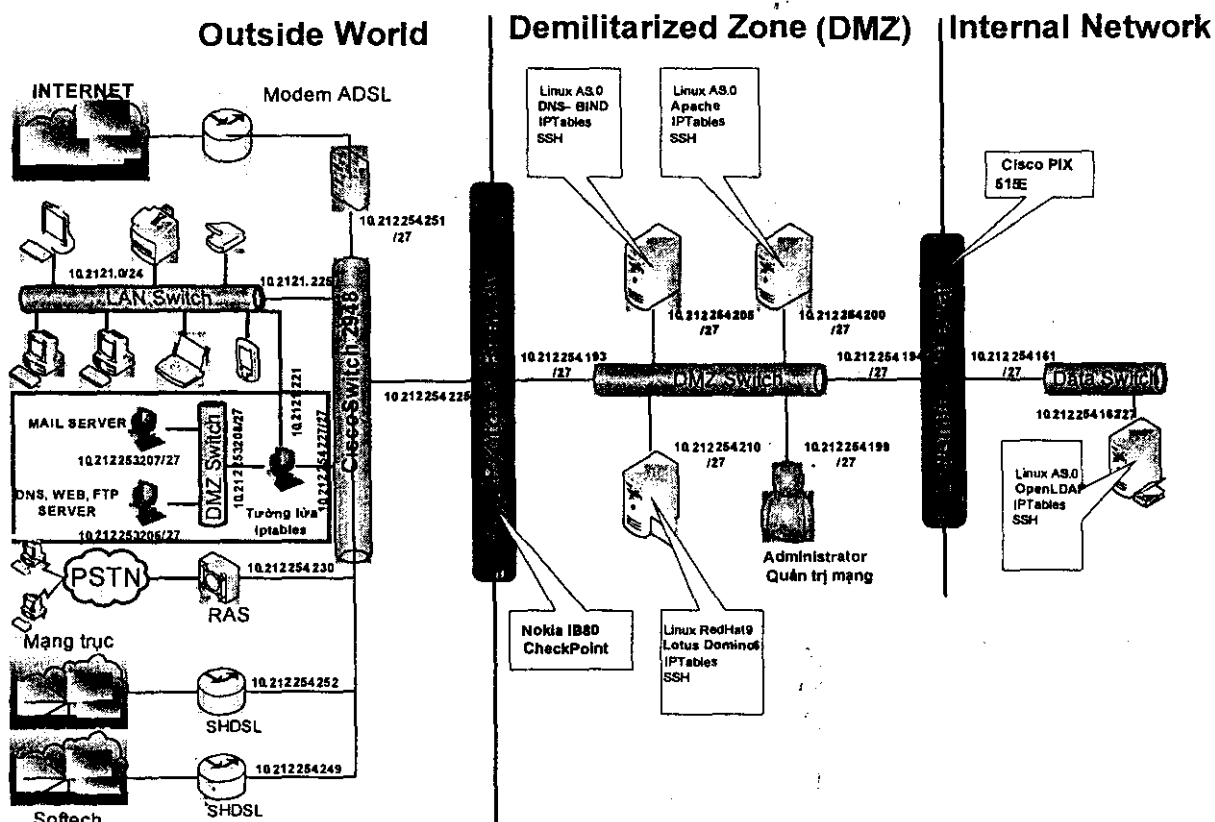
- Cài đặt các dịch vụ DNS, FTP, WEB, MAIL

- Thực hiện việc chia sẻ tập tin thư mục giữa Windows và Linux

- Xây dựng hệ thống tường lửa (Firewall) để bảo vệ các dịch vụ trên máy chủ và tránh được sự xâm nhập bất hợp pháp từ mạng bên ngoài vào hệ thống máy chủ của đơn vị.

- Xây dựng mô hình mạng theo mô hình mạng 3 vùng (DMZ, LAN, Vùng bên ngoài)

5.3. Mô hình triển khai



Mô hình mạng tại Văn phòng UBND thành phố được chia thành các vùng (Vùng dữ liệu, vùng DMZ, vùng truy cập, vùng mạng nội bộ Văn phòng)

Nhóm triển khai đề tài xây dựng mô hình mạng 3 vùng trong vùng mạng nội bộ của văn phòng (xem hình vẽ).

- Vùng DMZ: Vùng này bao gồm hai máy chủ phục vụ các dịch vụ truy cập từ bên ngoài: DNS, Web, Mail và FTP. Tất cả các dịch vụ này đều được triển khai trên hệ điều hành Mandrake Linux 10.0. Vùng này cung cấp các dịch vụ cho mạng nội bộ (LAN) và mạng bên ngoài (mạng diện rộng) thành phố thông qua đường SHDSL.

- Vùng mạng nội bộ (LAN): Hệ thống mạng LAN tại đơn vị xây dựng 1 máy chủ SAMBA trên nền HĐH Mandrake Linux 10.0 làm nhiệm vụ chia sẻ tập tin và thư mục giữa các máy trạm Windows và Mandrake Linux 10.0.

- Vùng mạng bên ngoài: Vùng kết nối với các Sở Ban Ngành, Quận huyện qua router SHDSL và kết nối ra Internet qua router ADSL.

- Hệ thống bảo vệ (Firewall): Tường lửa xây dựng trên phần mềm NetFilter/Iptables được cài đặt trên HĐH Mandrake Linux 10.0, tường lửa này là Gateway bảo đảm cho phép bên ngoài truy cập vào vùng DMZ và các máy chủ thuộc vùng mạng LAN văn phòng và bảo đảm chống các truy cập trái phép từ mạng bên ngoài đến vùng DMZ và vùng mạng LAN Văn phòng. Nó đảm bảo bên trong vùng DMZ và từ vùng mạng LAN truy cập hiệu quả ra mạng bên ngoài nhưng vẫn an toàn.

5.4. Thực hiện cài đặt

- Cài đặt HĐH Mandrake Linux 10.0 lên các máy tính trong vùng mạng nội bộ của Văn phòng UBND thành phố.

- Cài đặt các dịch vụ DNS, FTP, WEB, Mail

- Thực hiện việc chia sẻ tập tin thư mục giữa Windows và Linux

- Xây dựng hệ thống tường lửa (Firewall) để ngăn được các cuộc tấn công từ mạng bên ngoài, tường lửa còn cho phép mạng bên ngoài (mạng diện rộng thành phố) và mạng nội bộ cũng truy cập được các dịch vụ DNS, Mail, FTP, Web bên trong vùng DMZ.

5.5. Đánh giá kết quả triển khai cài đặt tại VP UBND thành phố

Việc triển khai các dịch vụ cơ bản dựa trên hệ thống mã nguồn mở đã cho thấy được hiệu quả bước đầu là:

- Các dịch vụ đã cài đặt như DNS, Web, FTP và Mail trong mô hình mạng đã cung cấp được cho hệ thống mạng bên ngoài, và từ mạng bên ngoài (mạng diện rộng) truy cập được các dịch vụ này.

- Tường lửa (Firewall) cài đặt tại đơn vị đã ngăn được các cuộc tấn công và truy cập trái phép từ mạng bên ngoài, cung cấp các dịch vụ DNS, FTP, Web và Mail được truy cập từ mạng bên ngoài và kiểm soát quá trình truy cập đó.

- Các dịch vụ này đã được triển khai thực tế và hoạt động ổn định nhưng không tốn chi phí bản quyền phần mềm. Đây là bước đầu cho thấy được hiệu quả ứng dụng Linux trong việc triển khai các dịch vụ trên máy chủ.

- Các vùng đã phân chia theo đúng thiết kế.

- Các máy trạm đã truy cập được các dịch vụ trong DMZ.

- Hệ thống tường lửa đã bảo vệ được hệ thống mạng.

6. Tóm tắt nhận xét kết quả triển khai của các đơn vị sử dụng.

Bên cạnh việc tự đánh giá các kết quả như trên, nhóm đề tài đã thông qua biên bản làm việc với các đơn vị sử dụng để lấy ý kiến nhận xét, góp ý việc thử nghiệm kết quả nghiên cứu của đề tài.

Tại Văn phòng UBND thành phố, kết quả đề tài đã được sử dụng trong hoạt động thường xuyên của Trung tâm Tích hợp Dữ liệu.

Tại Văn phòng Thành Ủy, do đặc thù của hệ thống, kết quả giới hạn ở việc cài đặt thử nghiệm.

Tại Văn phòng UBND quận Hải Châu, việc thử nghiệm được thực hiện trên nhiều dịch vụ : DNS, Web, Samba, FTP với kết quả tốt. Lãnh đạo đơn vị có ý kiến kiến nghị nên triển khai rộng hệ điều hành Linux ở cả máy chủ và máy trạm của hệ thống mạng LAN.

Tại Sở Ngoại vụ, máy chủ Linux đã hoạt động thường xuyên thay cho máy chủ Windows để bảo vệ mạng (Firewall) và cung cấp các dịch vụ.

Tại Sở Giáo dục, máy chủ Linux đã bổ sung thêm dịch vụ FTP cho hệ thống mạng LAN của đơn vị.

Kết quả trên cho thấy việc ứng dụng hệ điều hành Linux và các dịch vụ trên nền hệ điều hành Linux có thể được triển khai tại các đơn vị với nhiều mô hình khác nhau, tùy thuộc thực tế hệ thống mạng và nhu cầu sử dụng của các đơn vị. Giải pháp Linux là một bổ sung giá trị cho việc cung cấp các dịch vụ trên hệ thống mạng, có thể song song tồn tại cùng với hệ điều hành MS Windows đang phổ biến. Bên cạnh việc đáp ứng các nhu cầu trong việc triển khai các phần mềm dùng chung, giải pháp Linux cũng tăng hiểu biết về quản trị mạng cho cán bộ các đơn vị.

Giao diện làm việc với Linux tuy phức tạp hơn so với giao diện MS Windows quen thuộc, nhưng với những bổ sung của nhóm đề tài trong việc xây dựng các ứng dụng quản trị dịch vụ với giao diện tiếng Việt, những trở ngại cũng được khắc phục đáng kể.

Điều quan trọng nhất là khả năng đưa hệ điều hành Linux vào sử dụng phục vụ nhu cầu khai thác trên mạng LAN của các đơn vị Sở, Ngành, địa phương đã được chấp nhận. Đây là nền tảng tốt cho việc triển khai ứng dụng hệ điều hành Linux trong tương lai.

KẾT LUẬN VÀ KIẾN NGHỊ

I. Kết luận

Nội dung nghiên cứu của nhóm đề tài đã đạt mục tiêu đặt ra ban đầu: hoàn thành việc đưa ra giải pháp kỹ thuật, thực hiện việc đào tạo và triển khai thử nghiệm.

Kết quả nghiên cứu đề tài mang lại một số hiệu quả:

- *Về mặt lý thuyết:* Với nhu cầu hiện nay của hệ thống hành chính, đã chứng minh việc ứng dụng hệ điều hành Linux thay thế Windows là hoàn toàn khả thi, đáp ứng phần lớn các nhu cầu sử dụng trong thực tế. Trước mắt, các máy chủ Linux sẽ tồn tại song hành với các máy chủ Windows phục vụ nhu cầu sử dụng, khi bị sức ép về bản quyền, đã có thể có giải pháp để thay thế hệ điều hành Windows bằng hệ điều hành Linux, áp dụng trong hệ thống hành chính;
- *Về mặt đào tạo nhân lực:* Đội ngũ cán bộ quản trị mạng được bồi dưỡng và tạo điều kiện nâng cao kiến thức phục vụ công việc;
- *Về hiệu quả thực tế:* Nhóm đề tài đã đưa ra một số giải pháp triển khai cài đặt Linux và các dịch vụ cho mạng LAN các đơn vị. Một số phần mềm được xây dựng đã phần nào đáp ứng nhu cầu khai thác và quản trị mạng.

Với quan điểm đối tượng phục vụ chính là cán bộ các đơn vị hành chính sự nghiệp, các giải pháp đưa ra được trình bày khá đơn giản và dễ hiểu, tạo điều kiện thuận lợi cho việc áp dụng trong thực tế.

Giải pháp xây dựng Firewall bằng phần mềm được nghiên cứu hoàn toàn có thể được triển khai để tiết kiệm kinh phí mua các thiết bị phần cứng tương tự với giá cao hơn nhiều.

II. Kiến nghị

- Mỗi mạng LAN của các sở ban ngành quận huyện phải có ít nhất 03 máy chủ.
- Chuyên nghiệp hoá đội ngũ quản trị mạng tại các sở, ban, ngành, quận huyện.
- Có chương trình, kế hoạch đào tạo chuyên sâu về Linux cho cán bộ quản trị mạng tại các sở, ban, ngành, quận huyện (150 tiết cho 40 người).
- Chủ động xây dựng kế hoạch và triển khai việc thay thế dần hệ điều hành mạng và bộ phần mềm văn phòng của Microsoft sang hệ thống tương đương của Linux và hệ phần mềm mã mở (trong 2 năm

2005 - 2006) nhằm tránh được các khó khăn rất lớn khi luật bản quyền và sở hữu trí tuệ được thực thi trong bối cảnh Việt Nam gia nhập WTO.

III. Đề xuất kế hoạch áp dụng kết quả nghiên cứu

1. Nội dung

Căn cứ kết quả nghiên cứu, nhóm đề tài đề xuất kế hoạch áp dụng kết quả của đề tài trên máy chủ tại mạng LAN của các đơn vị sở, ban, ngành, quận, huyện.

Việc áp dụng giải pháp Linux không phân biệt cho các loại đơn vị Sở, Ngành, UBND Quận huyện mà được căn cứ theo quy mô mạng LAN tại các đơn vị : mô hình máy chủ đơn lẻ, mô hình 2 vùng, mô hình 3 vùng như trình bày ở đầu chương 5.

Việc triển khai có thể được thực hiện thông qua các bước như sau :

1. Tổ chức đào tạo tập trung

Trên nền hệ thống giáo trình đã được xây dựng, tổ chức các lớp tập huấn cho cán bộ quản trị mạng cũng như một số nhân viên các Sở, Ngành, UBND quận, huyện tham gia tìm hiểu việc sử dụng và quản trị hệ điều hành Linux.

2. Bố trí máy chủ cài đặt hệ điều hành Linux tại đơn vị

Trong khuôn khổ dự án mạng LAN mở rộng, các đơn vị sẽ được bố trí thêm một số máy chủ và máy trạm. Trong số này, đề nghị Ban Điều hành Đề án 112 thành phố quy định đơn vị bố trí 1 máy tính cài hệ điều hành Linux và các dịch vụ cơ bản: Firewall, DNS, Web, FTP, ...Có thể giới hạn trong phạm vi 10 đơn vị.

Việc cài đặt Firewall bằng phần mềm iptables là biện pháp hữu hiệu thay cho việc mua thiết bị tường lửa CheckPoint (với giá > 1.000 USD)

3. Nghiên cứu hoàn thiện giải pháp phần mềm

Bên cạnh các phần mềm quản trị dịch vụ đã xây dựng, sẽ bổ sung thêm một số giao diện quản trị các dịch vụ như Web, FTP, DHCP.

Một nội dung rất cần thiết là nghiên cứu các phần mềm Portal được xây dựng trên nền mã nguồn mở để cung cấp cho các đơn vị khi có nhu cầu xây dựng Website chuyên ngành. Khi đó, kinh phí cho việc xây dựng Website chuyên ngành chỉ giới hạn ở việc chuẩn bị dữ liệu, biên tập và cập nhật dữ liệu sau khi hiệu chỉnh giao diện phù hợp với nhu cầu của đơn vị, việc này sẽ giúp giảm chi phí đáng kể so với cách làm hiện nay.

4. Xây dựng Website của Trung tâm Tích hợp dữ liệu

Việc xây dựng Website của Trung tâm Tích hợp dữ liệu nhằm đến mục tiêu chính là cung cấp thông tin được kết xuất từ các cơ sở dữ liệu của các phần mềm dùng chung.

Một lợi ích khác là Website sẽ giúp cán bộ quản trị mạng các đơn vị thực hiện việc tra cứu thông tin, cập nhật phần mềm, trao đổi, hỗ trợ kỹ thuật.

5. Đánh giá kết quả triển khai

Căn cứ nội dung triển khai tại các đơn vị, tham mưu Ban Điều hành 112 Thành phố kế hoạch triển khai sử dụng rộng rãi hệ điều hành Linux.

2. Dự toán kinh phí

Nội dung	Kinh phí
1. Đào tạo tập trung (2 lớp x 15 triệu /lớp)	30.000.000
2. Cài đặt, hướng dẫn sử dụng tại chỗ (10 đơn vị x 7 triệu/đơn vị)	70.000.000
3. Nghiên cứu hoàn thiện phần mềm, bổ sung dịch vụ	30.000.000
4. Xây dựng Website của Trung tâm Tích hợp dữ liệu	30.000.000
5. Quản lý phí	20.000.000
Tổng cộng	180.000.000

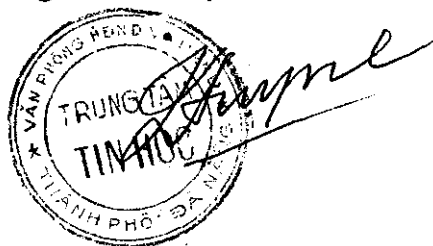
Bằng chữ: một trăm tám mươi triệu đồng.

Chủ nhiệm đề tài

TS. Hoàng Quang Tuyền

Cơ quan chủ trì

Trung tâm Tin học VP UBND TP



HOÀNG QUANG TUYẾN

TÀI LIỆU THAM KHẢO

Sách tiếng Việt

1. Trần Thạch Tùng, **Bảo mật và tối ưu trong Red Hat Linux**; Nhà xuất bản Lao động – Xã hội

Sách tiếng Anh

1. Stephen Figgins, Ellen Siever, Aaron Weber. **Linux in a Nutshell**, 4th Edition; 06/2003; O'Reilly & Associates; ISBN: 0-596-00482-6.
2. Matt Welsh, Matthias Kalle Dalheimer, Terry Dawson, Lar Kaufman. **Running Linux**, 4th Edition; 12/2002; O'Reilly & Associates; ISBN: 0-596-00272-6.
3. Olaf Kirch, Terry Dawson. **Linux Network Administrator's Guide**, 2nd Edition; 06/2000; O'Reilly & Associates; ISBN: 1-56592-400-2.
4. Gérard Beekmans. **Linux from Scratch**, version 5.0.
5. Gerhard Mourani. **Securing and Optimizing Linux: The Ultimate Solution**; 06/2001; Open Network Architecture; ISBN: 0-9688793-0-6
6. Gerald Carter. **LDAP System Administration**; 03/2004; Nhà xuất bản O'Reilly; ISBN: 1-56592-491-6
7. Dave Sill. **The qmail Handbook**; 2002; Nhà xuất bản Apress, ISBN: 1893115402
8. John Levine. **Qmail**; 03/2004; Nhà xuất bản O'Reilly, ISBN: 1-56592-628-5
9. David Collier-Brown, Robert Eckstein, Jay Ts. **Using Samba**, 2nd Edition; 02/2003; Nhà xuất bản O'Reilly, ISBN: 0-596-00256-4
10. Ken Coar and Rich Bowen. **Apache cookbook**; 11/2003; Nhà xuất bản O'Reilly, ISBN: 0-596-00191-6
11. Second Ed - Cameron Newham, Bill Rosenblatt. **Learning the bash Shell**; 1998; Nhà xuất bản O'reilly
12. Rob Flickenger. **Linux Servers hacks**; 2003; Nhà xuất bản: O'reilly
13. Stig Sæther Bakken, Egon Schmid. **Php Manual**; 1997-2004; PHP Documentation Group

Tham khảo trên Internet

1. <http://www.linux.org>
2. <http://httpd.apache.org/docs-2.0/>
3. <http://www.pipeline.com.au/staff/mbowe/isp/webmail-server.htm>

4. <http://www.openldap.org>
5. <http://www.openssl.org>
6. <http://www.sleepycat.com>
7. <http://www.netfilter.org/>
8. <http://iptables-tutorial.frozentux.net/iptables-tutorial.html>
9. <http://www.zytrax.com/books/ldap/ch5/>
10. <http://www.qmailrocks.org>
11. <http://safari.oreilly.com>
12. <http://www.Samba.org>
13. <http://www.linux.cmc.com.vn/index.cgi>
14. <http://www.vnlinux.org/sitemoi/>
15. <http://www.vnulib.edu.vn/ho tro ky thuat/bao mat/>

Và một số tài liệu khác có liên quan đến Linux, mã nguồn mở, tài liệu lập trình.

PHỤ LỤC

Phụ lục 1: Tài liệu hướng dẫn cài đặt Mandrake Linux 10.0 và các dịch vụ

Phụ lục 2: Tài liệu hướng dẫn sử dụng Mandrake Linux 10.0 và các dịch vụ

Phụ lục 3: Tài liệu đào tạo