4.2013

Năm thứ 51 số 445(635)

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

TẠP CHÍ CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG

ĐỊA CHỈ: 18 NGUYỄN DU, HÀ NỘI
Toà soạn: 110 Bà Triệu, Hà Nội
Tel:(84.4)37737136; (84.4) 37737137
Fax: (84.4) 37737130
Email: *tapchibcvt@mic.gov.vn;*
Website: http://www. tapchibcvt.gov.vn;
http://www.ictvietnam.vn

CHI NHÁNH TẠI TP.HCM
Địa chỉ: 27 Nguyễn Bỉnh Khiêm - Phường Đakao, Quận 1, TP. Hồ Chí Minh
Trưởng chi nhánh: Nguyễn Văn Nguyễn
Email: *nvnguyen@mic.gov.vn*
Tel/Fax: 08.39105379
Mobile: 0917171342

Giấy phép xuất bản số: 433/GP-BTTTT ngày 03/04/2009
In tại Công ty TNHH MTV in Quân đội 1. In xong và nộp lưu chiểu tháng 4/2013

Giá bán: 19.000đ

4.2013

MỘT SỐ CÔNG TÁC TRỌNG TÂM CHO IPv6 TRONG GIAI ĐOẠN TỚI

Thứ trưởng Lê Nam Thắng chỉ đạo một số công tác trọng tâm chuyển đổi IPv6 trong giai đoạn 2.

Ngày 16/4/2013, giai đoạn 1 (2011 – 2012) của kế hoạch hành động quốc gia về IPv6 đã được Bộ Thông tin và Truyền thông tổng kết đánh giá.

Theo đánh giá của Ban công tác Kế hoạch hành động quốc gia về IPv6, trong 2 năm thực hiện nhiệm vụ của Giai đoạn 1 Kế hoạch hành động quốc gia 6 mục tiêu của Giai đoạn 1 đã được hoàn thành: Phổ cập kiến thức cơ bản về IPv6 cho cộng đồng CNTT và Truyền thông; Hoàn thiện các văn bản pháp luật, văn bản hướng dẫn về yêu cầu đảm bảo thiết bị phải tương thích với IPv6 và ưu tiên hỗ trợ triển khai IPv6 cho các dự án CNTT sử dụng ngân sách nhà nước; Hoàn thành mạng thử nghiệm IPv6 quốc gia; Tất cả các doanh nghiệp Internet từng bước chuẩn bị các điều kiện cần thiết về kế hoạch, nhân lực và kỹ thuật để triển khai IPv6 tại doanh nghiệp; Các mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước được đấu nối thử nghiệm và sẵn sàng cho việc chuyển đổi sang IPv6; Hoàn thành cơ bản việc đánh giá và chuẩn bị điều kiện cần thiết về kiến thức, hạ tầng kỹ thuật và nhân lực phục vụ cho việc chuyển đổi sang IPv6 tại Việt Nam.

Chỉ đạo một số công việc cần tập trung cho giai đoạn 2 – giai đoạn khởi động (2013 – 2015), Thứ trưởng Bộ Thông tin và Truyền thông Lê Nam Thắng cho biết:

Thứ nhất, tiếp tục làm tiếp công tác truyền thông và đào tạo để nâng cao nhận thức và kiến thức về IPv6. Giai đoạn 1 mới chỉ tập trung vào các ISP. Giai đoạn 2, công tác truyền thông và đào tạo để nghị

mở rộng sang các hội thảo, hội nghị, diễn đàn về CNTT, Viễn thông phải có về IPv6 và kể cả tổ chức một ban công tác các đối tượng khác ngoài ISP, như các CSP, các nhà sản xuất thiết bị mạng và đầu cuối, các đối tượng là chủ mạng tin học như các cơ quan Đảng, nhà nước, các ngành lớn khác như hàng không, ngân hàng, năng lượng có mạng tin học lớn và các trường đại học để mở rộng phạm vi đào tạo.

Thứ hai, về cơ chế chính sách, cần đẩy nhanh hơn nữa để Chính phủ sớm ban hành Nghị định về Internet và có thể Quý này được ban hành nhưng quan trọng là sau khi Nghị định ra đời, có một số việc cần phải làm là: làm việc với Bộ Tài chính, Bộ Khoa học và Công nghệ để làm sao các đơn vị, doanh nghiệp ứng dụng công nghệ IPv6 vào sản xuất được hưởng các chế độ, chính sách ưu đãi của nhà nước về thuế, đầu tư, vốn và có các văn bản hướng dẫn kể cả hướng dẫn Nghị định 102 liên quan đến đầu tư trong lĩnh vực CNTT để đồng bộ các văn bản để thúc đẩy IPv6; Để thúc đẩy kết nối Internet nói chung và Internet trên nền IPv6, Trung tâm Internet Việt Nam tiếp tục hoàn chỉnh quy chế hoạt động của VNIX để làm sao kết nối vào VNIX tạo điều kiện thúc đẩy các doanh nghiệp đều thấy có lợi ích kết nối vào VNIX tạo mạng quốc gia về IPv6; Tiếp tục xây dựng quy định về quản lý tài nguyên Internet, đặc biệt quản lý tài nguyên về IPv6, quy hoạch khoa học các địa chỉ IPv6 để ngay từ đầu đảm bảo sự phát triển ổn định của IPv6; Tiếp tục xây dựng các tiêu chuẩn, quy chuẩn kỹ thuật về IPv6 và đặc biệt đối với thiết đầu cuối tuân thủ IPv6 bên cạnh thiết bị mạng.

Thứ ba, tiếp tục nâng cao hiệu quả mạng IPv6 quốc gia trên nền tảng VNIX và hoạt động ổn định của các hệ thống DNS hỗ trợ IPv6. Tất cả các hạ tầng kỹ thuật VNIX hỗ trợ sự chuyển đổi này tiếp tục cần được củng cố.

Thứ tư, đưa ra thử nghiệm một số dịch vụ trên thị trường và cho một số nhóm khách hàng, đặc biệt là các dịch vụ mới và công nghệ mới hỗ trợ IPv6. Ví dụ như việc sau này cấp phép cho các hệ thống thông tin di động thế hệ 4 thì bắt buộc doanh nghiệp tương thích luôn IPv6.

Thứ năm, để các mạng dùng riêng của các cơ quan chuyển sang IPv6 cần khuyến khích, tạo điều kiện để chuyển đổi.

Thứ sáu, về sản xuất thiết bị đầu cuối, các doanh nghiệp nỗ lực sản xuất các thiết bị hỗ trợ IPv6 với sự trợ giúp của nhà nước. Các nhà sản xuất trong nước như VNPT, Viettel, QMobile… cung ứng thiết bị đầu cuối cũng phải tích cực làm sao sản xuất sản phẩm phải hỗ trợ IPv6. Để làm được điều này công tác quản lý nhà nước phải được đẩy lên đặc biệt là chương trình hợp quy, dán nhãn để hỗ trợ khách hàng nhận biết đâu là thiết bị hỗ trợ IPv6, điều này cũng giúp việc kiểm soát nhập khẩu tốt hơn.

Thứ bảy, liên quan đến nội dung, ứng dụng đóng góp vào thành công chuyển đổi IPv6, trước tiên tập trung vào các trang web của Đảng và nhà nước, các trang báo lớn, một số mạng xã hội lớn, website của một số doanh nghiệp lớn. Việc thực hiện cần có trọng tâm, trọng điểm thậm chí phải có hỗ trợ của nhà nước để các trang web, ứng dụng đó tương thích IPv6. Đề nghị, khuyến khích các nhà cung cấp dịch vụ nội dung (CSP) quan tâm cùng triển khai.

Thứ tám, nghiên cứu, phát triển và đào tạo về IPv6 không chỉ dừng ở các trường đại học, Ban công tác phải mở rộng phạm vi làm việc với Bộ Giáo dục và Đào tạo để có hướng dẫn cho các khoa CNTT, Điện tử – Viễn thông đào tạo về IPv6 và có định hướng đề tài, hỗ trợ cho công tác nghiên cứu phát triển IPv6.

Lan Phương

Ban Công tác thúc đẩy phát triển IPv6 quốc gia - Hạt nhân của hoạt động thúc đẩy IPv6 tại Việt Nam

Nguyễn Thị Thu Thủy

NỀN TẢNG TRIỂN KHAI IPv6

Việt Nam đã trải qua 02 năm thực hiện Kế hoạch Hành động Quốc gia về IPv6 (ban hành theo Quyết định số 433/QĐ-BTTTT ngày 29 /03/2011 của Bộ trưởng Bộ Thông tin Truyền thông (Bộ TT&TT). Từ mức độ nhận thức về IPv6 còn mơ hồ, đến nay triển khai chuyển đổi sử dụng IPv6 được thừa nhận là tất yếu. Các hoạt động thử nghiệm, đánh giá mạng lưới cho chuyển đổi IPv6 được triển khai rộng rãi. Việt Nam đã thiết lập được mạng lưới về IPv6, các cơ sở hạ tầng thiết yếu (mạng máy chủ DNS quốc gia, trạm trung chuyển lưu lượng quốc gia VNIX) đã hoàn toàn hỗ trợ IPv6. Đóng vai trò quan trọng trong thúc đẩy IPv6 tại Việt Nam là các hoạt động của Ban Công tác thúc đẩy phát triển IPv6 Quốc gia, hạt nhân của quá trình chuyển đổi IPv6 tại Việt Nam.

Ban Công tác thúc đẩy phát triển IPv6 quốc gia (Việt Nam IPv6 Task Force) được thành lập theo Quyết định số 05/BTTTT ngày 06/01/2009 của Bộ trưởng Bộ TTT&TT để thực hiện nhiệm vụ thúc đẩy phát triển địa chỉ IPv6 tại Việt Nam. Ban công tác có nhiệm vụ nghiên cứu, hoạch định chiến lược phát triển và ứng dụng IPv6, xây dựng kế hoạch và lộ trình triển khai việc chuyển đổi IPv4 sang IPv6 tại Việt Nam và theo dõi, điều phối hoạt động triển khai IPv6 của các đơn vị theo lộ trình, kế hoạch đã đặt ra.

Sau 03 năm hoạt động, Ban Công tác thúc đẩy phát triển IPv6 quốc gia được kiện toàn theo Quyết định số 1190/QĐ-BTTTT ngày 03/07/2012 của Bộ trưởng Bộ TT&TT, hiện do Ông Lê Nam Thắng – Thứ trưởng Bộ TT&TT làm Trưởng Ban, Trung tâm Internet Việt Nam (VNNIC) là Thường trực Ban, thành viên Ban gồm đại diện VNNIC, các đơn vị trực thuộc Bộ TT&TT, đại diện một số trường đại học, học viện, đại diện Bộ Giáo dục và Đào tạo, đại diện Bộ Khoa học Công nghệ, các ISP.

HOẠT ĐỘNG CỤ THỂ

Một trong những nhiệm vụ quan trọng trước tiên là xây dựng và trình ban hành Kế hoạch hành động quốc gia về IPv6. Đào tạo kiến thức và nâng cao nhận thức cũng là một trong những hoạt động cần được triển khai sớm và đồng bộ. Ban Công tác đã triển khai đào tạo với nhiều hình thức: trực tiếp cho các cán bộ kỹ thuật của doanh nghiệp, trực tuyến. Đối với đào tạo trực tiếp, đã triển khai 14 khóa đào tạo cho gần 400 cán bộ kỹ thuật của ISP. Chương trình đào tạo trực tuyến cũng được hoàn thiện và

cung cấp theo 02 hình thức: phổ cập cho cộng đồng tại Website www.ipv6.vn và triển khai từng khóa trực tuyến trong hệ thống đào tạo trực tuyến của Thường trực Ban – Trung tâm Internet Việt Nam (VNNIC) tại: http://elearning.vnnic.vn/.

Về mặt cơ sở hạ tầng mạng lưới, thực hiện nhiệm vụ được giao tại Chỉ thị số 03/2008/CT-BTTTT về việc thúc đẩy sử dụng địa chỉ Internet thế hệ mới IPv6 và Kế hoạch hành động quốc gia về IPv6, thường trực Ban – VNNIC đã thiết lập mạng IPv6 đầu tiên ở Việt Nam, làm hạt nhân cho mạng IPv6 quốc gia. Đầu năm 2013, mạng IPv6 đã hoàn tất chuyển đổi sang hoạt động chạy song song (dual stack) IPv4-IPv6 thay vì chạy thuần IPv6 như thời gian đầu.

ĐẨY MẠNH TRUYỀN THÔNG

Công tác thông tin và truyền thông được triển khai liên tục, đều đặn. Bên cạnh việc thường xuyên tuyên truyền, quảng bá về IPv6, Ban Công tác IPv6 quốc gia đã tổ chức cho doanh nghiệp Việt Nam tham gia hưởng ứng các hoạt động IPv6 quốc tế như Ngày IPv6 Quốc tế 2011 (World IPv6 Day), Khai trương IPv6 toàn cầu 2012 (World IPv6 Launch) và đặc biệt là tổ chức các Hội thảo IPv6 quốc tế tại Việt Nam.

Năm 2012, năm cuối cùng của Giai đoạn 1 (2011-2012) – Giai đoạn chuẩn bị trong Kế hoạch Hành động quốc gia về IPv6, Ban Công tác thúc đẩy phát triển IPv6 đã tổ chức thành công hội thảo IPv6 quốc tế đầu tiên tại Việt Nam với chủ đề "IPv6 – Công nghệ và Ứng dụng với Việt Nam".

Sự kiện này được tổ chức vào đúng thời điểm thế giới chuẩn bị triển khai sự kiện chính thức khai trương IPv6 kể từ ngày 06/06/2012 (World IPv6 Launch) và được coi là hành động thiết thực của Việt Nam nhằm hưởng ứng sự kiện lớn này của thế giới.

Hội thảo đã mang lại lợi ích về nhiều mặt: Nâng cao nhận thức; Nâng cao uy tín của Việt Nam và tăng cường hợp tác quốc tế; Học hỏi kinh nghiệm kiến thức, chính sách, chiến lược. Hội thảo đã góp phần quảng bá sự phát triển Internet của Việt Nam nói chung và việc triển khai IPv6 nói riêng ra thế giới, khẳng định vai trò quản lý nhà nước của Bộ TT&TT, đặc biệt là vai trò định hướng tổ chức, thúc đẩy phát triển IPv6 tại Việt Nam. Thông qua hội thảo, các doanh nghiệp viễn thông và Internet tại Việt Nam học hỏi được nhiều kinh nghiệm triển khai IPv6 từ các nhà cung cấp dịch vụ nổi tiếng như NTT Communications, HE, cũng như giúp cho các cơ quan quản lý, các doanh nghiệp viễn thông và Internet trong nước được tiếp cận với thông tin, xu hướng công nghệ và triển khai thực tế về IPv6 trên thế giới.

Để tăng cường nhận thức và đẩy mạnh quá trình triển khai IPv6 tại Việt Nam, Bộ TT&TT đã phê chuẩn lựa chọn ngày 06/5/2013 là Ngày IPv6 Việt Nam. Đây cũng là ngày diễn ra sự kiện IPv6 quốc gia Việt Nam lần thứ hai với chủ đề "Ngày IPv6 Việt Nam", tổ chức tại thành phố Hồ Chí Minh (**www.ipv6event2013.vn**).

MỞ RỘNG HỢP TÁC QUỐC TẾ

Từ ngày 27/11 đến ngày 30/11/2012, Đoàn công tác của Ban Công tác thúc đẩy phát triển IPv6 quốc gia do ông Hoàng Minh Cường, Phó Trưởng Ban, Giám đốc Trung tâm Internet Việt Nam (VNNIC) làm trưởng đoàn cùng với một số đơn vị thành viên thuộc Bộ TT&TT, doanh nghiệp Internet Việt Nam đã thực hiện chương trình thăm và học hỏi kinh nghiệm triển khai IPv6 tại Nhật Bản.

Trong khuôn khổ chương trình công tác tại Nhật Bản, đoàn đã làm việc với Bộ Nội vụ và Truyền thông Nhật Bản (Ministry of Internal Affairs and Communications Japan); Ủy ban thúc đẩy phát triển

Ông Haruka Saito - Đại diện Bộ Nội vụ và Truyền thông Nhật Bản chào đón ông Hoàng Minh Cường - Trưởng đoàn công tác của Ban Công tác thúc đẩy phát triển IPv6 quốc gia sang làm việc tại Nhật Bản.

IPv6 Nhật Bản (Japan IPV6 Promotion Council); Ủy ban về vấn đề cạn kiệt IPv4 Nhật Bản (Japan IPv4 Exhausted Task Force); Hiệp hội các nhà điều hành mạng Nhật Bản (JANOG); Tổ chức quản lý tài nguyên địa chỉ Internet Nhật Bản (JPNIC). Bên cạnh đó, đoàn cũng có các buổi tham quan, học hỏi kinh nghiệm triển khai tại một số doanh nghiệp cung cấp dịch vụ truy nhập và trung chuyển Internet của Nhật là NTT, KDDI, JPIX, JPNAP.

Các đối tác Nhật Bản đã chia sẻ thông tin, cung cấp cho đoàn công tác Việt Nam về chính sách, tình hình triển khai địa chỉ IPv6 tại Nhật Bản.

Thông qua chuyến công tác và làm việc với các đối tác Nhật Bản, đoàn công tác của Ban công tác thúc đẩy IPv6 quốc gia đã tiếp thu được nhiều kinh nghiệm, bài học quý báu để có thể áp dụng cho công tác hoạch định chính sách, kế hoạch, thực hiện các hoạt động thúc đẩy IPv6 trong nước trong thời gian tới.

CỤ THỂ HÓA CÁC HOẠT ĐỘNG CHUYỂN ĐỔI SANG IPv6

Trong tháng 11/2012, Ban công tác IPv6 Quốc gia đã tổ chức chương trình làm việc trực tiếp với một số doanh nghiệp cung cấp dịch vụ Internet (VNPT, Viettel, NetNam) để khảo sát nắm bắt tình hình triển khai IPv6 trên thực tế tại các doanh nghiệp. Ban Công tác cũng hợp tác với Học viện Công nghệ BCVT để xúc tiến việc đưa nội dung về công nghệ IPv6 vào chương trình đào tạo chính quy các ngành CNTT và truyền thông nhằm hướng đến đào tạo nguồn nhân lực IPv6 cho mục tiêu lâu dài.

Trên thực tế, cả VNPT, Viettel và NetNam đều là các doanh nghiệp điển hình và rất tích cực trong việc triển khai IPv6. Mỗi doanh nghiệp đều đã hoàn tất việc ban hành kế hoạch chuyển đổi sang IPv6 và thành lập Ban công tác chuyên trách về IPv6 tại đơn vị. Điểm đáng chú ý nữa là các doanh nghiệp này đều đã thiết lập được đường kết nối thuần IPv6 ra Quốc tế để góp phần nâng cao lưu lượng và chất lượng các dịch vụ thử nghiệm trên IPv6.

Ban Công tác cũng đề nghị doanh nghiệp trên cơ sở chuẩn bị sẵn sàng thiết bị trên mạng lưới và các phòng thí nghiệm, thực hiện thử nghiệm chính thức trên nền IPv6 trên một quy mô nhất định cho khách hàng trên mạng lưới để từ đó có được những kết quả, đánh giá cụ thể hơn khi triển khai thực tế trên toàn mạng.

Đối với công tác đào tạo chuyên ngành về IPv6, thực tế triển khai tại Học viện công nghệ Bưu chính Viễn thông, Học viện đã lồng ghép nội dung về IPv6 vào các chương trình đào tạo ngắn hạn và chính quy dài hạn. Tuy nhiên thời lượng số tiết học về

Ban Công tác IPv6 Quốc gia làm việc với Tập đoàn Viettel.

IPv6 chưa thực sự nhiều.

Bên cạnh các hoạt động nói trên, trong năm 2012, Ban Công tác IPv6 quốc gia đã thực hiện một cách đồng bộ các hoạt động chuyên môn về IPv6: đăng ký thành công dự án thúc đẩy IPv6 cho doanh nghiệp vừa và nhỏ trong khối Asean, thể hiện vai trò đi đầu của Việt Nam trong khu vực; Đưa cơ chế chính sách, hỗ trợ phát triển IPv6 vào dự thảo Nghị định Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng, theo đó xác định công nghệ IPv6 thuộc danh mục công nghệ cao được ưu tiên đầu tư phát triển, được hưởng các mức ưu đãi, hỗ trợ theo quy định của pháp luật; Thực hiện các hoạt động khảo sát doanh nghiệp nhằm tổng kết, đánh giá kết quả thực hiện Giai đoạn 1 Kế hoạch hành động Quốc gia về IPv6.

Trong thời gian tới, các công tác của Giai đoạn 2 (2013-2015) - Giai đoạn khởi động sẽ được triển khai. Để đạt được mục tiêu cuối cùng của Kế hoạch Hành động quốc gia về IPv6 "Internet Việt Nam hoạt động một cách an toàn, tin cậy với địa chỉ IPv6 (hoàn toàn tương thích với IPv6)", các hoạt động thúc đẩy phát triển IPv6 cần được tiến hành một cách tích cực, sâu rộng và đồng bộ. Đây cũng là tinh thần kết luận của Trưởng Ban Công tác thúc đẩy phát triển IPv6 quốc gia, Thứ trưởng Bộ TT&TT Lê Nam Thắng tại buổi họp tổng kết hoạt động năm 2012 của Ban Công tác, nhằm hướng tới đạt được kết quả thực chất cho hoạt động triển khai IPv6 tại Việt Nam./.

Tài liệu tham khảo

[1]. www.mic.gov.vn

[2]. www.vnnic.vn

[3]. www.ipv6.vn

Ban Công tác IPv6 Quốc gia làm việc với Học viện Công nghệ Bưu chính Viễn thông.

APNIC nỗ lực triển khai và đào tạo IPv6

Kế hoạch hành động quốc gia về IPv6 của Việt Nam đã bắt đầu chuyển sang giai đoạn 2 (2013-2015). Nhân dịp ngày IPv6 Việt Nam, Tạp chí CNTT&TT đã có cuộc trao đổi với bà Miwa Fujii, chuyên gia cao cấp phụ trách chương trình IPv6 của APNIC về tình hình và xu thế phát triển IPv6 trên thế giới và nhận định đối với Việt Nam.

Bà Miwa Fujii, chuyên gia cao cấp phụ trách chương trình IPv6 của APNIC.

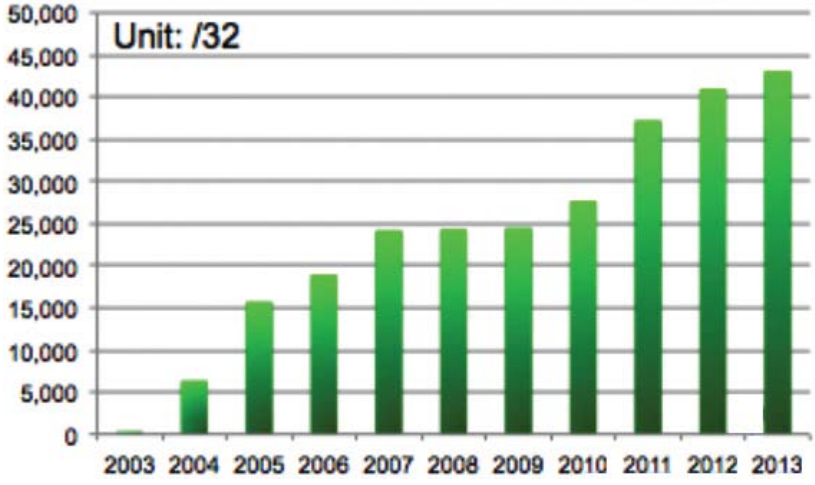
***PV**: Bà có nhận định gì về xu thế và mức độ triển khai ứng dụng IPv6 trên toàn cầu và tại khu vực Châu Á – Thái Bình Dương kể từ thời điểm APNIC chính thức tuyên bố là khu vực đầu tiên trên toàn cầu bước vào giai đoạn cạn kiệt IPv6 (15/4/2011)?*

Bà Miwa: Có rất nhiều đối tượng liên quan đến mạng Internet như nhà cung cấp dịch vụ Internet (ISP), nhà cung cấp nội dung, mạng phân phối nội dung, nhà cung cấp ứng dụng, doanh nghiệp, chính phủ, các tổ chức xã hội và người sử dụng. Việc triển khai IPv6 tác động đến tất cả các thực thể tham gia hoạt động Internet và là việc tất yếu, cần thiết để đảm bảo sự phát triển liên tục và ổn định của mạng Internet, nhưng thời điểm triển khai IPv6 sẽ khác nhau ở mỗi đối tượng. Do đó, khi nói về xu hướng và mức độ triển khai IPv6 đối với các thành phần khác nhau, chúng ta phải chấp nhận một tiếp cận logic thông qua việc xem xét những thống kê liên quan.

Để đạt mục tiêu này, việc phân đối tượng liên quan thành các nhóm và xem xét xu thế và mật độ triển khai IPv6 ở 4 nhóm: cơ quan quản lý, các nhà mạng, nhà cung cấp dịch vụ và sản xuất, người sử dụng.

Cơ quan quản lý địa chỉ Internet (IPv4/ IPv6) khu vực:

Địa chỉ IPv6 được phân bổ thông qua các cơ quan quản lý địa chỉ Internet khu vực (RIR) như APNIC (Trung tâm quản lý địa chỉ khu vực châu Á – Thái Bình Dương), tổ chức quản lý địa chỉ quốc gia (NIR) tới các ISP, nhà cung cấp truy nhập, doanh nghiệp, tổ chức khác.



Hình 1: Phân bố địa chỉ IPv6 (nguồn APNIC).

Để triển khai các mạng IPv6, nhà khai thác mạng trước tiên phải có địa chỉ IPv6 từ RIR. Lượng địa chỉ IPv6 tăng khoảng 35% từ năm 2010 sang 2011 so với chỉ khoảng 10% của các năm trước đó và tiếp tục tăng trưởng đều cho đến nay.

Số liệu thống kê cho thấy số lượng địa chỉ IPv6 đang tăng dần lên. APNIC sẽ tiếp tục thúc đẩy các thành viên chưa sử dụng địa chỉ IPv6 sớm triển khai sử dụng và ứng dụng IPv6.

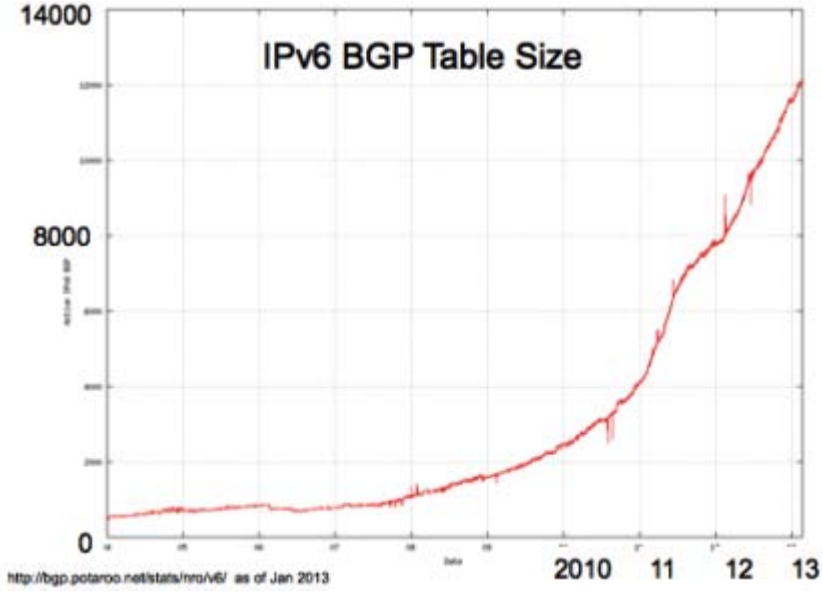
Triển khai IPv6 đối với nhà khai thác mạng:

Đối tượng tiếp theo để đánh giá việc triển khai IPv6 là các nhà khai thác mạng bao gồm nhà cung cấp dịch vụ chuyển tiếp lưu lượng (transit provider). (Hình 2 cho thấy số mạng đã quảng bá vùng IPv6 ra Bảng thông tin định tuyến toàn cầu – Bảng BGP). Bảng BGP này chỉ cung cấp số liệu về phát triển mạng IPv6, chưa phải chỉ số phát triển mạng IPv6 thương mại thực sự vì các mạng thử nghiệm cũng có thể quảng bá các vùng địa chỉ IPv6.

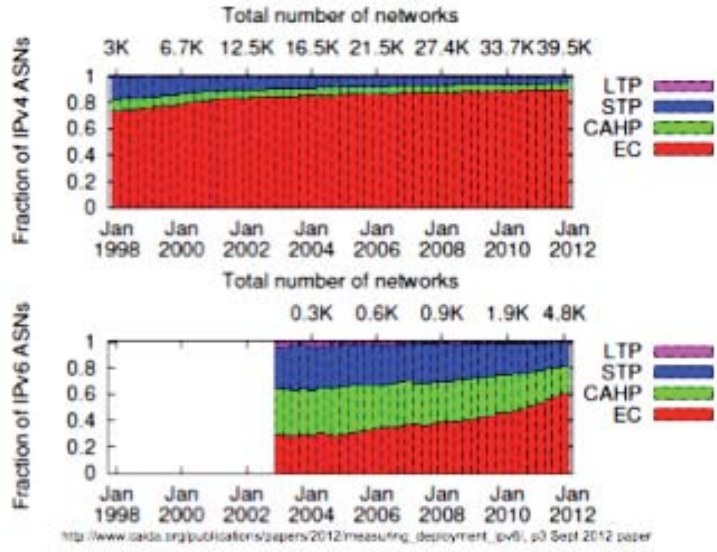
Mặc dù Bảng BGP trong biểu đồ Hình 2 không phải cho riêng khu vực APNIC nhưng chứa đựng bức tranh toàn cầu, cho thấy xu hướng gia tăng việc quảng bá các vùng địa chỉ IPv6, tăng lên cỡ khoảng 50–60% trong giai đoạn 2011–2012. Xu thế tăng trưởng này tiếp tục được cổ vũ bằng sự gia tăng triển khai IPv6 của các nhà cung cấp truyền dẫn, ISP và một số nhà cung cấp nội dung.

Nhà cung cấp dịch vụ nội dung và các hãng:

Đối tượng tiếp theo là các nhà cung cấp dịch vụ nội dung và các hãng. (Hình 3 giới thiệu xu hướng phát triển IPv6 theo loại hình kinh doanh. Nguồn:



Hình 2: Số lượng mạng có IPv6.



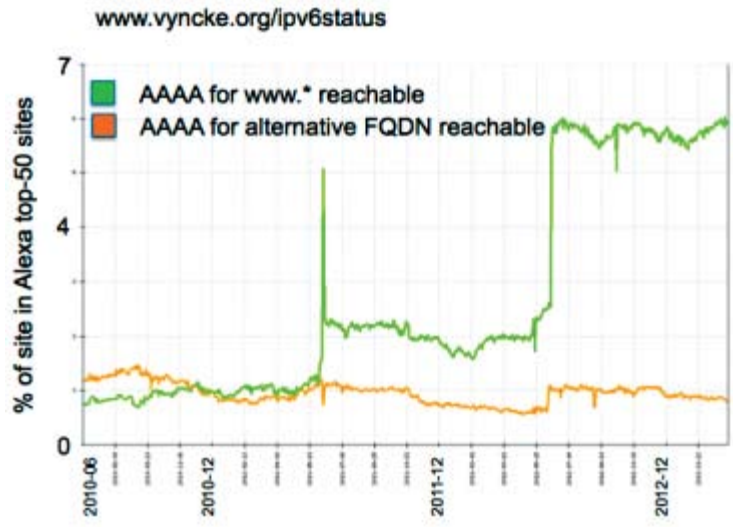
Hình 3: Xu hướng phát triển IPv6 theo loại hình kinh doanh.

CAIDA). CAIDA phân các loại hình kinh doanh thành nhà cung cấp truyền dẫn lớn (LTP), nhà cung cấp truyền dẫn nhỏ (STP), nhà cung cấp nội dung, truy nhập, hosting, khách hàng doanh nghiệp và so sánh giữa IPv4 và IPv6.

Hình 3 thể hiện xu hướng toàn cầu. Hầu hết các nhà cung cấp truyền dẫn Internet chủ chốt đã triển khai IPv6, sự tăng trưởng này rất đều từ năm 2010 đến nay. Tuy nhiên, các mạng biên như mạng doanh nghiệp, các nhà cung cấp dịch vụ và các nhà cung cấp nội dung vẫn chưa triển khai IPv6 một cách đầy đủ.

Các Website hỗ trợ IPv6:

Khoảng 6% của tốp 50 trang web theo Alexa hiện đã sẵn sàng cho IPv6. Các trang này là Google, Facebook, YouTube và Yahoo. Các nhà cung cấp nội



Hình 4: Các Website hỗ trợ IPv6.
(Sự sẵn sàng IPv6 của 50 nhà cung cấp nội dung hàng đầu theo Alexa.
Nguồn: www.vynche.org/ipv6status).

dung địa phương cần nỗ lực hơn trong việc sử dụng IPv6. Việc những nhà cung cấp toàn cầu sẵn sàng với IPv6 loại bỏ quan điểm "Không có nội dung trên IPv6 nên không cần triển khai IPv6 ở mạng truy nhập".

Sự sẵn sàng IPv6 của người sử dụng:

Sự sẵn sàng IPv6 của người sử dụng được đánh giá thông qua số người sử dụng IPv6 trung bình trên thế giới. Khoảng 1% người sử dụng toàn cầu có kết nối IPv6 đầy đủ từ thiết bị đầu cuối qua mạng truy nhập và mạng lõi đến nguồn nội dung IPv6 (Nguồn: labs.apnic.net). Ta không thấy ảnh hưởng nhiều của sự kiện cạn kiệt địa chỉ IPv4 trong nhóm đối tượng này.

Hình 5: Sự sẵn sàng IPv6 của người sử dụng toàn cầu.

Có một điểm lưu ý, đây là mức trung bình của thế giới và có sự khác biệt lớn về sự sẵn sàng IPv6 của người sử dụng giữa các nền kinh tế và khu vực. Ví dụ, tỉ lệ người sử dụng sẵn sàng cho IPv6 ở Rumani là khoảng 10%, Pháp là 6% và Nhật là 3,5%.

Tóm lại, mức độ sẵn sàng IPv6 đối với các nhà cung cấp truyền dẫn chính là khá cao. Sự cạn kiện địa chỉ IPv4 trong khu vực APNIC và những sự kiện triển khai IPv6 toàn cầu vào năm 2011 và 2012 đã tạo ra hiệu ứng tích cực. Tuy nhiên, khi chuyển từ mạng lõi đến mạng biên (mạng truy nhập, nhà cung cấp hosting, nhà cung cấp nội dung, doanh nghiệp và người sử dụng) sự sẵn sàng IPv6 thấp hơn rất nhiều. Chúng ta vẫn cần phải nỗ lực hỗ trợ để toàn bộ hệ thống Internet tăng cường sử dụng địa chỉ IPv6.

PV: *Đánh giá của bà về mức độ sẵn sàng cho địa chỉ IPv6 trong khu vực và tại Việt Nam?*

Bà Miwa: Theo số liệu thống kê của labs.apnic.net, mức độ sẵn sàng IPv6 trung bình hiện nay đối với người sử dụng trong Khu vực Đông nam Á là khoảng 0,1%; Nam Á là khoảng 0,03% và Đông Á khoảng 1%. Việt Nam là khoảng 0,001% – khá nhỏ!

Mặc dù các mạng ở Việt Nam đang gia tăng sử dụng IPv6, Việt Nam vẫn có nhiều khoảng trống cần phát triển. Đặc biệt là Việt Nam cần gia tăng sự sẵn sàng IPv6 ở "chặng cuối" trong các mạng truy nhập.

PV: *Việt Nam đã ban hành Kế hoạch Hành động Quốc gia về IPv6.*

Bà có nhận định gì về Kế hoạch này của Việt Nam? Theo bà, Việt Nam cần chú trọng những công tác nào trong Giai đoạn 2 sắp tới để có được kết quả

Mức độ sẵn sàng IPv6 trung bình hiện nay đối với người sử dụng trong Khu vực Đông nam Á là khoảng 0,1%; Nam Á là khoảng 0,03% và Đông Á khoảng 1%. Việt Nam là khoảng 0,001% – khá nhỏ!

tốt nhất trong thúc đẩy triển khai IPv6?

Bà Miwa: Việc xây dựng kế hoạch hành động quốc gia và cách thức hỗ trợ triển khai IPv6 là một chiến lược tốt để tháo gỡ thách thức về IPv6. Nhiều nền kinh tế trong khu vực APNIC đã sử dụng cách thức này. Chính phủ có thể có tầm nhìn lâu dài để triển khai IPv6.

Chúng tôi cho rằng, Việt Nam đã hoàn tất thành công Giai đoạn 1 ở tầm quốc gia với các nội dung bao trùm:

– Triển khai đầy đủ kế hoạch triển khai IPv6 cho các mạng trong cơ quan chính phủ với thời hạn rõ ràng;

– Cập nhật chính sách về IPv6 cho các dịch vụ ICT, dịch vụ phần cứng, phần mềm IPv6 cho các doanh nghiệp và nhà cung cấp dịch vụ mà Chính phủ Việt Nam yêu cầu;

– Thiết lập kế hoạch đào tạo IPv6 cho các kỹ sư quản lý mạng của chính phủ.

Hiện đã là quí 2 năm 2013, chúng tôi hy vọng rằng việc triển khai Giai đoạn 2 đã được bắt đầu thuận lợi. Giai đoạn 2 là sống còn vì nó liên quan trực tiếp đến việc triển khai IPv6 thực tế. Các hạ tầng Internet chủ yếu như .vn, cc TLD, và VNIX đều hỗ trợ IPv6 là điều kiện rất tốt.

Vấn đề quan trọng nhất trong Giai đoạn 2 là giám sát tiến trình thực sự để so với kế hoạch được thiết lập trong Giai đoạn 1. Việc thiết lập một cơ chế giám sát và hiệu chỉnh sẽ giúp đạt được các mục tiêu này. Nếu Giai đoạn 2 của kế hoạch hành động IPv6 quốc gia của Việt Nam bao gồm cả việc hợp tác công tư trong triển khai IPv6 thì cần phải thường xuyên trao đổi thông tin và cập nhật tình trạng giữa hai bên để giải quyết các cấn đề phát sinh sớm nhất. Kế hoạch gốc có thể được sửa đổi miễn là không làm thay đổi mục tiêu ban đầu.

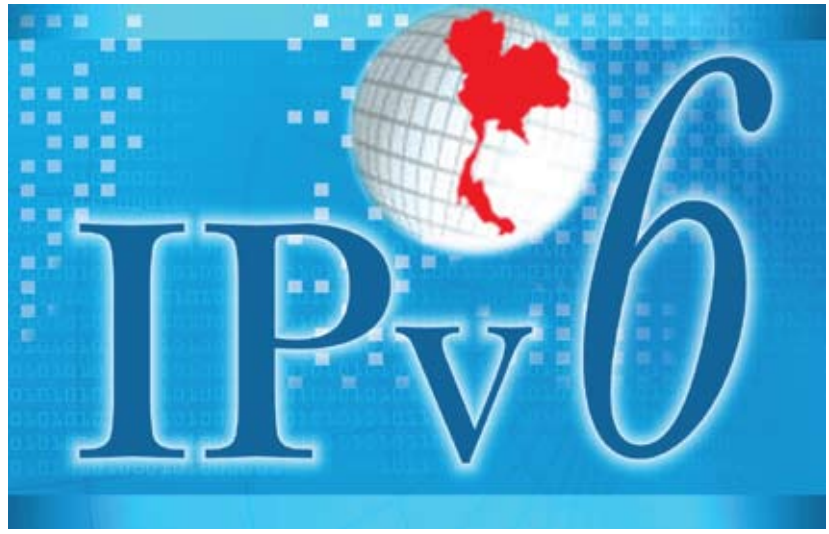
PV: *Bà đánh giá như thế nào về vai trò của Chính phủ trong việc thúc đẩy sử dụng địa chỉ IPv6. Theo bà, những chính sách nào của Chính phủ mang lại kết quả tốt nhất trong việc thúc đẩy triển khai IPv6.*

Bà Miwa: Thách thức mà chúng ta gặp phải trong triển khai IPv6 là chủ đề được thảo luận giữa nhiều đối tượng tham gia mạng Internet, bao gồm cả các tổ chức chính phủ như APEC. Sự can thiệp tích cực từ chính phủ có thể được điều chỉnh, không những để thu hút sự quan tâm và sự cạnh tranh quốc gia, mà còn để đảm bảo chính "sức khỏe" của mạng Internet.

Nhóm làm việc viễn thông (TEL) của APEC đã xuất bản "Hướng dẫn IPv6 của APEC TEL" (APEC TEL 42, 2010) nhằm hỗ trợ triển khai IPv6 trong giai đoạn chuẩn bị cạn kiệt địa chỉ IPv4. Tài liệu này mô tả chính chủ cần có sự tham gia và vai trò rất rõ ràng trong triển khai IPv6.

Việc xem xét tài liệu hướng dẫn này sẽ giúp khôi phục vai trò kỳ vọng của chính phủ đối với việc triển khai IPv6. Việt Nam là một trong số 21 thành viên của APEC đã đóng góp vào việc soạn thảo tài liệu này. Tài liệu này chỉ ra các hướng dẫn cho các nền kinh tế thành viên để hỗ trợ triển khai IPv6 hiệu quả, bao gồm: Quy hoạch tổng thể; Quản lý kỹ thuật; Phát triển nguồn nhân lực; Hợp tác liên cơ quan và quốc tế; Dẫn đầu ngành, làm mẫu sử dụng IPv6; Hợp tác giữa chính phủ và doanh nghiệp.

Việc thực hiện IPv6 trong các mạng chính phủ cũng tạo ra nhu cầu ban đầu và cơ hội học tập cho các nhà sản xuất và cung cấp dịch vụ trong ngành mà cung cấp hàng hóa và dịch vụ hỗ trợ IPv6. Chính sách hỗ trợ sử dụng IPv6 trong các mạng chính phủ với thời hạn cụ thể và cơ cấu giám sát, hiệu chỉnh và báo cáo sẽ có hiệu lực tốt. Mọi mua bán và hợp



đồng của chính phủ phải đặt ra yêu cầu tương thích IPv6 đối với các sản phẩm và dịch vụ ICT.

Chính phủ Việt Nam cũng có thể thực hiện vai trò dẫn đầu và hỗ trợ hợp tác công tư để giúp triển khai IPv6 hiệu quả. Ví dụ, chính phủ có thể thiết lập cơ cấu chứng nhận sản phẩm là "sẵn sàng cho IPv6" và có thể cung cấp hỗ trợ tài chính như giảm thuế cho sản phẩm của những đơn vị triển khai IPv6 đúng tiến độ yêu cầu và cung cấp cơ hội đào tạo IPv6 cho những cán bộ kỹ thuật chủ chốt. Chính phủ cũng có thể thúc đẩy IPv6 thông qua các phương tiện truyền thông, sự kiện, cuộc thi, giải thưởng và các cơ chế khác.

PV: *Đánh giá chung của bà đối với việc triển khai IPv6 tại Việt Nam?*

Bà Miwa: Các số liệu thống kê có thể giúp trả lời câu hỏi này. Theo số liệu cung cấp bởi labs.apnic.net dựa trên thử nghiệm thu thập dữ liệu đánh giá sự sẵn sàng IPv6 của người sử dụng, Việt Nam đã được phân bổ 227 số hiệu mạng ASN từ APNIC. Các mạng có chính sách định tuyến duy nhất sẽ có một ASN duy nhất, do đó nhìn vào sự sẵn sàng IPv6 của ASN của Việt Nam sẽ cho chúng ta câu trả lời hợp lý về sự sẵn sàng IPv6 trong mạng ở Việt Nam được nối trực tiếp đến Internet.

– 123 ASN trong tổng số ASN của Việt Nam (54%) quảng bá cả IPv4 và IPv6 hoặc chỉ IPv4 trong bảng định tuyến toàn cầu.

– 91 trong số 123 ASN này (74%) thấy được qua hệ thống đo lường thử nghiệm của APNIC.

– 15 trong số 91 ASN này (16%) có ít nhất một dải địa chỉ IPv6 định tuyến toàn cầu.

– 7 trong số 15 ASN này (47%) có người sử dụng IPv6 tích cực.

7 ASN này quảng bá IPv6 từ bản thân mạng lưới của họ và người sử dụng, chiếm khoảng 0,001%, đây là tỉ lệ sẵn sàng IPv6 trung bình của người sử dụng. Con số này khá nhỏ so với thế giới là 1%. Cần phải thúc đẩy triển khai IPv6 nhiều hơn trong "chặng cuối" ở Việt Nam để tăng số người sử dụng truy nhập vào tài nguyên thông tin IPv6 Internet thông qua các mạng lõi, mạng kết nối hỗ trợ IPv6.

Giống như nhiều nền kinh tế, triển khai IPv6 đến người sử dụng ở chặng cuối đang trở thành một thách thức đối với Việt Nam. Các nhà cung cấp dịch vụ, bao gồm nhà cung cấp mạng di động ở Việt Nam cần phải có chiến lược mới để nâng cấp đầu cuối người sử dụng và các kế hoạch phân bổ chi phí cho sự phát triển kinh doanh trong tương lai của mình.

Một số nhà cung cấp dịch vụ đã triển khai thành công IPv6 trong mạng trên thế giới có thể áp dụng chiến lược chung sau:

– Cung cấp địa chỉ và dịch vụ IPv6 cho các thuê bao mới một cách mặc định.

– Cho phép các dịch vụ IPv6 với các khách hàng hiện có ngay khi họ nâng cấp dịch vụ hiện tại của mình.

Đây là cách thức hợp lý để quản lý việc triển khai IPv6, và có thể là một chiến lược hiệu quả cho các nhà khai thác mạng ở Việt Nam.

PV: *Với vai trò quản lý tài nguyên địa chỉ khu vực châu Á – Thái Bình Dương, APNIC đã thực hiện những công việc gì nhằm thúc đẩy triển khai IPv6 trong khu vực. Bà cho biết trong thời gian tới, APNIC có những dự kiến gì trong việc phối hợp với các quốc gia trong khu vực để đẩy nhanh mức độ ứng dụng triển khai IPv6?*

Bà Miwa: Các phản hồi từ cộng đồng Internet châu Á – Thái Bình Dương trong đợt khảo sát 2012 của APNIC cho thấy nhiều mối quan tâm liên quan đến IPv6. Nhiều thực thể tham gia khảo sát yêu cầu "APNIC cần nỗ lực triển khai và đào tạo IPv6", cụ thể hơn là đề nghị APNIC cần nỗ lực thực hiện các vấn đề sau:

– Thông tin về kinh nghiệm triển khai IPv6 tốt nhất.

– Khuyến nghị và tư vấn về triển khai IPv6.

– Đào tạo thực tế hơn về triển khai IPv6.

– Nâng cao nhận thức của các đối tượng liên quan.

– Gắn bó mật thiết hơn với các cộng đồng Internet địa phương để giúp thúc đẩy IPv6.

APNIC sẽ tiếp tục đáp ứng các yêu cầu này từ cộng đồng bằng cách thực hiện đào tạo IPv6 thực tế hơn, cung cấp trợ giúp kỹ thuật về triển khai IPv6, cung cấp rộng rãi hơn các chương trình thiết thực trong các hội thảo APNIC và các sự kiện khác trong vùng. APNIC cũng sẽ đảm bảo cung cấp thông tin kỹ thuật IPv6 trực tiếp, cập nhật bao gồm BGP và thông tin chia sẻ giữa các thực thể liên quan mạng Internet qua trang web www.apnic.net/ipv6.

Chúng tôi nghĩ rằng việc cung cấp thông tin phù hợp cho lãnh đạo trong mỗi nhóm liên quan và các cơ hội đào tạo kỹ năng IPv6 cho kỹ sư mạng sẽ hỗ trợ đắc lực cho việc triển khai IPv6. Chúng tôi sẵn sàng tiếp thu các đề xuất, kiến nghị từ cộng đồng để cho sự hợp tác tương lai.

PV: *Xin trân trọng cảm ơn bà!*

Nguyễn Quang Hưng thực hiện

DỰ ÁN THÚC ĐẨY TRIỂN KHAI IPv6 CHO CÁC DOANH NGHIỆP VỪA VÀ NHỎ TRONG KHỐI ASEAN

Phan Thị Nhung

Trong khuôn khổ các chương trình hợp tác và kết nối của quỹ ICT ASEAN, Trung tâm Internet Việt Nam đã phối hợp với Vụ Hợp tác Quốc tế đăng ký triển khai một dự án có tên gọi **"Thúc đẩy triển khai IPv6 cho các doanh nghiệp vừa và nhỏ"**.

Thực tế, không gian địa chỉ IPv4 đã cạn kiệt được gần 02 năm tại khu vực châu Á Thái Bình Dương, tình trạng này cũng lan sang khu vực châu Âu được gần 1 năm. Tuy nhiên, mức độ ảnh hưởng của sự cạn kiệt IPv4 đối với mỗi quốc gia hoặc đối với mỗi loại doanh nghiệp trong cùng một quốc gia cũng khác nhau. Có thể nói là các quốc gia dự trữ được nhiều địa chỉ IPv4 (Mỹ, Nhật, Hàn Quốc, vv…) gần như không có ảnh hưởng gì lớn. Ngược lại, các quốc gia đang phát triển, đông dân cư có tốc độ tăng trưởng Internet nhanh như đa số các nước trong khu vực Đông Nam Á thì thiếu địa chỉ IP để tiếp tục duy trì sự phát triển ổn định của Internet là một bài toán nan giải.

Bảng 1 thống kê về tổng số lượng địa chỉ IPv4 và tỉ lệ địa chỉ IPv4/đầu người của một số quốc gia trên thế giới.

Số liệu trên cho thấy hầu hết các quốc gia trong khu vực Đông Nam Á đều có lượng dự trữ địa chỉ IPv4 thấp xa so với mức an toàn để có thể duy trì sự phát triển ổn định của dịch vụ Internet trong phạm vi quốc gia thời gian tới. Chính vì thế, động lực để chuyển đổi sang IPv6 của các quốc gia Đông Nam Á là mạnh mẽ hơn nhiều khu vực khác. Trong bối cảnh đó, một số quốc gia trong khu vực Đông Nam

Bảng 1

Tên nước	Tổng số địa chỉ IPv4	Bình quân đầu người
Mỹ	1552.36 triệu	5.58
Nhật	201.89 triệu	1.59
Anh	122.05 triệu	2.05
Đức	118.38 triệu	1.44
Hàn Quốc	112.25 triệu	2.40
Việt Nam	15.54 triệu	0.19
Thái Lan	8.55 triệu	0.14
Malaysia	6.32 triệu	0.28
Singapore	5.79 triệu	1.62
Philippines	5.39 triệu	0.07
Campuchia	0.23 triệu	0.02
Brunei	0.19 triệu	0.59
Lào	0.05 triệu	0.01
Myanmar	0.03 triệu	0.00
Indonesia	17.37 triệu	0.08

Á đã ban hành kế hoạch hành động IPv6 quốc gia như: Singapore ban hành từ năm 2006, Malaysia năm 2008, Việt Nam năm 2011.

Đặc điểm của các kế hoạch quốc gia là đều tập trung nhiều vào các mảng cơ sở hạ tầng quan trọng hoặc các lĩnh vực cốt yếu của ngành công nghiệp Internet. Điều đó dẫn đến sự thiếu thông tin, thiếu nhận thức của bộ phận lớn các doanh nghiệp vừa và nhỏ (SME). Liệu rằng trên con đường dài đến đích IPv6, SME có cần thiết phải tham gia từ đầu? Liệu rằng bài học về kinh nghiệm chuyển đổi của các tập đoàn lớn như NTT của Nhật Bản, Telstra của Úc hay VNPT, Viettel của Việt Nam có hữu dụng đối với các SME? Vậy đâu là điểm xuất phát hợp lý của SME? Toàn bộ những vấn đề này sẽ được đề cập trong dự án "Thúc đẩy triển khai IPv6 cho các doanh nghiệp vừa và nhỏ"

Được đề xuất triển khai với hy vọng cung cấp thêm một kênh thông tin nhằm quảng bá thúc đẩy nhận thức của các SME trong việc triển khai IPv6, mục tiêu chính của dự án "Thúc đẩy triển khai IPv6 cho các doanh nghiệp vừa và nhỏ" là mang đến cho các SME những thông tin khuyến nghị bổ ích trong chiến lược chuyển đổi sang IPv6. Dự án đã được phê duyệt với mức kinh phí 35,000 đô la Mỹ từ quỹ ICT ASEAN và sẽ được triển khai trong năm 2013.

(Nguồn tham khảo: www.mic.gov.vn và www.vnnic.vn)

ĐÔI NÉT VỀ QUÁ TRÌNH TRIỂN KHAI IPv6 TẠI SINGAPORE

Nguyễn Vĩnh Hoàng

Đối mặt với tình trạng cạn kiệt tài nguyên IPv4 không phải là vấn đề của riêng quốc gia nào, đặc biệt với những quốc gia trong khu vực châu Á Thái Bình Dương, khu vực đầu tiên trên thế giới bước vào giai đoạn cạn kiệt IPv4. Ở thời điểm này, có thể nhận thấy rằng IPv6 đã thực sự hiện diện trong thực tế. Nhiều quốc gia và tổ chức đã có các hoạt động triển khai IPv6 rất tích cực. Ở Singapore bài toán chuyển đổi sang thế hệ địa chỉ mới IPv6 đã được chính phủ quan tâm từ rất sớm. Ban công tác thúc đẩy IPv6 đã được thành lập để triển khai và tạo điều kiện thuận lợi cho việc chuyển đổi IPv6 trong các sản phẩm và dịch vụ CNTT. Trong quá trình triển khai IPv6, Singapore đã đạt được những kết quả rất đáng học hỏi.

Có thể nói vai trò kết hợp "vừa đẩy vừa kéo" của Chính phủ Singapore trong triển khai IPv6 là một mô hình kiểu mẫu khi Chính phủ vừa đóng vai trò thúc đẩy IPv6 trong việc ban hành các chính sách liên quan vừa hỗ trợ về kinh phí. Bên cạnh đó, Chính phủ cũng là đầu tàu gương mẫu trong việc triển khai IPv6. Mục tiêu đặt ra là đến hết tháng 3/2013, 95% website của các cơ quan chính phủ phải sẵn sàng chạy với IPv6.

Một trong những điểm đáng lưu ý là Singapore đã đưa thành công nội dung đào tạo về IPv6 trong khối các trường đại học và cao đẳng chuyên ngành công nghệ thông tin. Bắt đầu triển khai vào đầu năm 2011 tới nay, các trường đại học và cao đẳng bên cạnh việc đưa IPv6 vào đào tạo chính quy còn liên kết tổ chức cuộc thi kỹ năng và ý tưởng về IPv6 hàng năm dành cho sinh viên.

Trong giai đoạn từ 2011-2012, Singapore đã có những bứt phá quan trọng nhằm đưa IPv6 tới gần hơn với các mạng người sử dụng cuối như hệ thống mạng của các ngân hàng, công ty chứng khoán. Tại Singapore, hiệp hội các doanh nghiệp trong lĩnh vực ngân hàng tài chính đã thiết lập hẳn một diễn đàn riêng để trao đổi về vấn đề chuyển đổi mạng từ IPv4 sang IPv6.

Theo thông tin từ IDA (cơ quan quản lý về thông tin và truyền thông Singapore) đến cuối năm 2013, sẽ có tổ chức ngân hàng đầu tiên hoàn tất việc chuyển đổi mạng lưới sang IPv6 để làm mô hình tham khảo cho các tổ chức khác.

NÂNG CAO HIỆU QUẢ HỢP TÁC VIỆT NAM - ISRAEL

Để kỷ niệm lần thứ 65 ngày Độc lập của Nhà nước Israel và 20 năm thiết lập quan hệ ngoại giao Việt Nam – Israel, Đại sứ quán Israel tại Hà Nội đã tổ chức lễ kỷ niệm và chương trình biểu diễn nghệ thuật với sự tham gia của các nghệ sĩ Israel và Việt Nam tại Nhà hát lớn Hà Nội, tối ngày 11/4/2013.

Tại buổi lễ, Đại sứ nhà nước Israel tại Việt Nam, bà Meirav Eilon Shahar đã chuyển tải thông điệp của Tổng thống Israel Simon Peres gửi tới Nhà nước và nhân dân Việt Nam nhân dịp kỷ niệm 20 năm thiết lập quan hệ ngoại giao. Trong thông điệp của mình, Tổng thống Israel Simon Peres đã bày tỏ niềm vinh hạnh đặc biệt của mình và lời chúc mừng nồng nhiệt nhất nhân lễ kỷ niệm 20 năm quan hệ ngoại giao Israel – Việt Nam. Israel đánh giá cao quan hệ song phương với Việt Nam và sẽ tiếp tục xây dựng mối quan hệ này trên nền tảng hữu nghị để tăng cường và mở rộng hơn nữa.

Bộ trưởng Bộ Khoa học Công nghệ Nguyễn Quân, đại diện cho Chính phủ Việt Nam, đã tham dự và có bài phát biểu chào mừng sự kiện này. Tới tham dự chương trình còn có các lãnh đạo cấp cao của các Bộ, Ban, Ngành của Việt Nam, các cơ quan ngoại giao của các nước khác, cùng đông đảo bạn bè của nhà nước và nhân dân Israel.

Năm 2013 là năm Việt Nam và Isreal kỷ niệm 20 năm thiết lập quan hệ ngoại giao giữa hai nước

Hợp tác viễn thông Việt Nam - Israel được xúc tiến từ nhiều năm nay.

Bà Meirav Eilon Shahar, Đại sứ nhà nước Israel tại Việt Nam, phát biểu tại lễ kỷ niệm.

(12/7/1993 – 12/7/2013). Trong 20 năm qua, quan hệ hữu nghị và hợp tác giữa hai nước đã không ngừng được củng cố và phát triển. Chuyến thăm Việt Nam gần đây (11/2011) của Tổng thống Israel Simon Peres đã đánh dấu bước phát triển mới trong quan hệ song phương, góp phần mở rộng và tăng cường quan hệ hợp tác nhiều mặt giữa hai nước.

Bộ trưởng Nguyễn Quân cho biết: "Thiết thực hướng tới kỷ niệm 20 năm thiết lập quan hệ ngoại giao, các Bộ/Ngành hữu quan hai bên đang tích cực phối hợp triển khai các thỏa thuận hợp tác đạt được trong chuyến thăm trên, trong đó có việc sớm ký kết Nghị định thư thành lập Ủy ban Liên Chính phủ Việt Nam – Israel nhằm tạo cơ chế giúp nâng cao hơn nữa hiệu quả hợp tác nhiều mặt giữa hai nước."

Cũng trong dịp kỷ niệm lần thứ 65 ngày Độc lập của Nhà nước Israel và 20 năm thiết lập quan hệ ngoại giao Việt Nam – Israel, Đại sứ quán Israel sẽ tiếp tục tổ chức nhiều sự kiện giao lưu văn hóa khác. Đó là những hoạt động rất có ý nghĩa, góp phần nâng cao hơn nữa tình hữu nghị và sự hiểu biết giữa nhân dân hai nước. Với nỗ lực của hai bên, quan hệ hữu nghị và hợp tác Việt Nam – Israel sẽ tiếp tục phát triển năng động và hiệu quả, vì lợi ích chung của nhân dân hai nước, vì hòa bình, hợp tác và phát triển trong khu vực và trên thế giới.

QM

Kỹ thuật "IPv4 over IPv6" - 464XLAT

Nguyễn Trần Hiếu, Chu Hồng Phúc

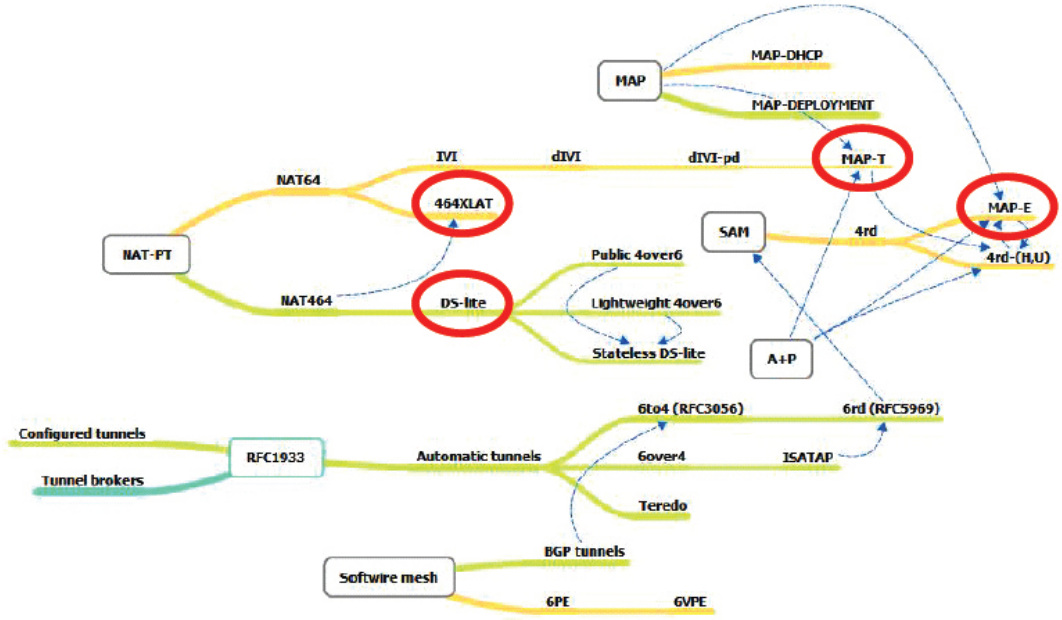
TỔNG QUAN VỀ KỸ THUẬT "IPv4 over IPv6"

Trước tình hình cạn kiệt hoàn toàn nguồn IPv4, thế hệ địa chỉ IPv6 đang được quan tâm thúc đẩy trên nhiều lĩnh vực. Số liệu thống kê thông số về IPv6 gia tăng một cách đáng kể và đều đặn trên Internet đã phản ánh mức độ tăng trưởng trong triển khai IPv6. Tuy nhiên, việc chuyển đổi hệ thống sang sử dụng địa chỉ IPv6 trong thời gian ngắn là điều không thể. Do vậy đã có rất nhiều công nghệ, kỹ thuật (như Tunnel, Tunnel brokers, NAT-PT, NAT64, DNS64, DS-Lite, MAP-E,…) được nghiên cứu, ứng dụng để thực hiện việc kết nối, trao đổi thông tin qua lại giữa các hệ thống mạng trong giai đoạn quá độ.

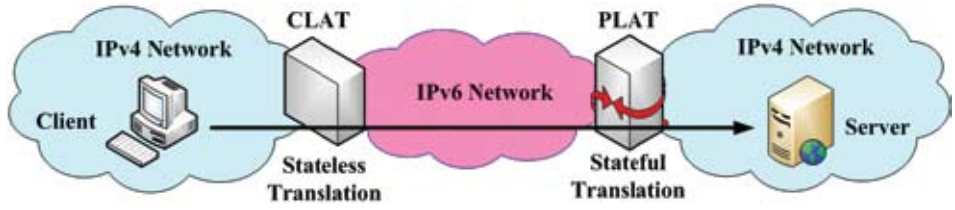
Một trong những kỹ thuật được quan tâm hiện nay đó là giải pháp kỹ thuật chuyển đổi từ IPv4 sang IPv6 (IPv4 over IPv6) dùng cho việc trao đổi thông tin giữa các node IPv4 trên nền IPv6. "IPv4 over IPv6" được sử dụng để kết nối các mạng IPv4 riêng rẽ trên nền hệ thống mạng IPv6 với mục đích mở rộng dịch vụ IPv4 cũng như thúc đẩy việc triển khai IPv6.

Hiện tại có bốn kỹ thuật "IPv4 over IPv6" chính là: DS-Lite, MAP-E, MAP-T, 464XLAT; (Hình 2). Bài báo này nhóm tác giả lựa chọn kỹ thuật 464XLAT để giới thiệu tới bạn đọc.

Hình 1: Giải pháp "IPv4 over IPv6".



Hình 2: Quá trình phát triển kỹ thuật "IPv4 over IPv6".



Hình 3: Mô hình kết nối trong 464XLAT.

MÔ HÌNH KẾT NỐI TRONG 464XLAT

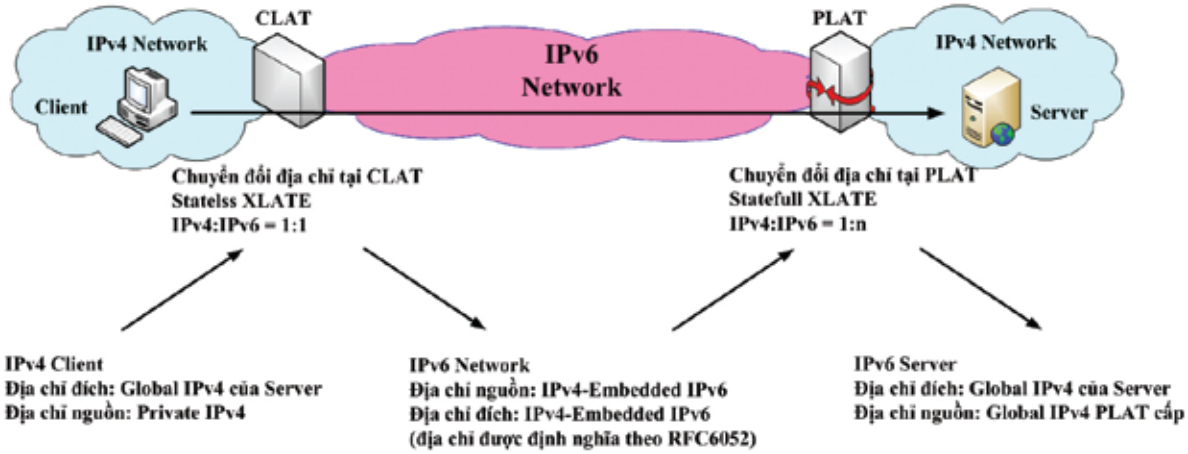
Kiến trúc 464XLAT chỉ hỗ trợ IPv4 trong mô hình client/server trao đổi thông tin qua hệ thống mạng IPv6 và server có sử dụng địa chỉ IPv4 thật (global IPv4). Điều này đồng nghĩa với việc 464XLAT không phù hợp với mô hình peer-to-peer hoặc mô hình chỉ có kết nối IPv4.

Phương thức chuyển đổi địa chỉ trong mô hình 464XLAT

Khi một client dùng địa chỉ IPv4 Private muốn kết nối tới máy chủ có địa chỉ IPv4 Global, gói tin từ Client được truyền tới bộ CLAT để thực hiện chuyển đổi địa chỉ nguồn và đích sang IPv6 (theo RFC6052). Gói tin IPv6 sau đó sẽ được truyền qua mạng IPv6 và tới bộ PLAT tương ứng, tại đó bộ PLAT sẽ thực

*- **PLAT**: Là bộ chuyển đổi phía nhà cung cấp - tuân thủ theo RFC6146; thực hiện việc chuyển đổi N:1 địa chỉ IPv6 thật (global IPv6) thành địa chỉ IPv4 thật (global IPv4) và ngược lại. Sử dụng phương thức chuyển đổi stateful.*

*-**CLAT**: Là bộ chuyển đổi phía khách hàng - tuân thủ theo RFC6145; thực hiện việc chuyển đổi 1:1 địa chỉ IPv4 ảo (private IPv4) thành địa chỉ IPv6 thật (global IPv6) và ngược lại. Sử dụng phương thức chuyển đổi stateless. CLAT sử dụng các tiền tố địa chỉ IPv6 khác nhau cho các địa chỉ IPv4 phía CLAT và PLAT do đó nó không phù hợp với mô hình kết nối giữa node thuần IPv4 và node thuần IPv6 qua Internet.*



Hình 4: Phương thức chuyển đổi địa chỉ trong 464XLAT.

hiện việc chuyển đổi địa chỉ thành IPv4 để kết nối tới máy chủ mong muốn. Chi tiết quá trình trên được mô tả như Hình 4.

KIẾN TRÚC MẠNG

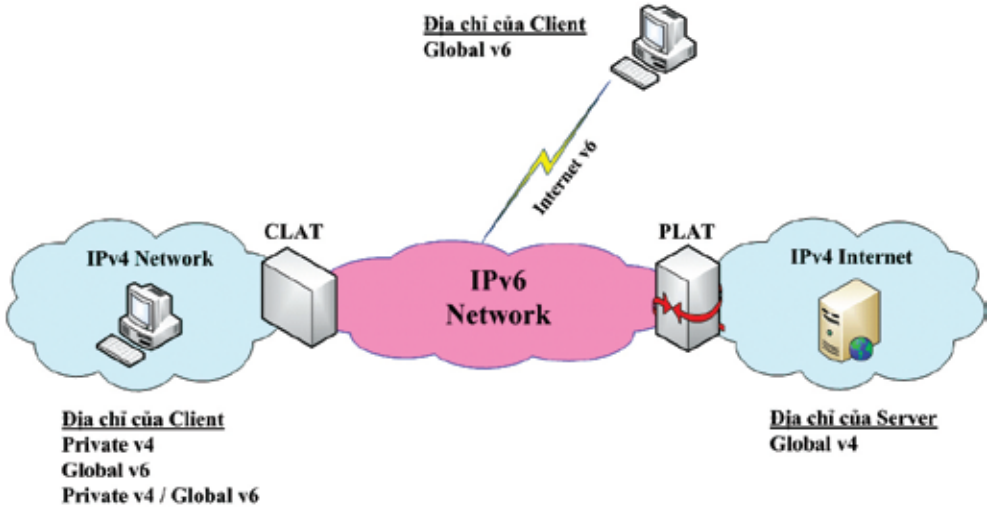
Kiến trúc 464XLAT được thể hiện trong hai trường hợp sau:

– Wireline Network Architecture – Kiến trúc mạng hữu tuyến: phù hợp trong các tình huống mà ở đó các client phía sau CLAT được xử lý theo cùng một cách không phân biệt loại hình truy cập dịch vụ như FTTH, DOCSIS, hoặc WiFi.

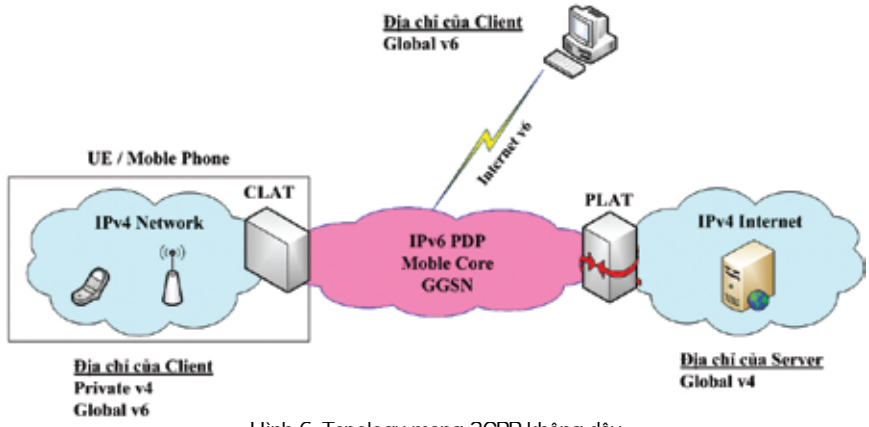
– Kiến trúc mạng 3GPP không dây (Wireless 3GPP Network Architecture): phù hợp trong các tình huống mà ở đó một client không truy cập mạng không dây và có thể hoạt động như một router có các client chia sẻ kết nối (tethered clients).

KẾT LUẬN

Trong giai đoạn quá độ của việc chuyển đổi IPv4/IPv6, việc áp dụng giải pháp 464XLAT đã thể hiện nhiều ưu điểm:



Hình 5: Topology mạng hữu tuyến.



Hình 6: Topology mạng 3GPP không dây.

– Yêu cầu tài nguyên IPv4 tối thiểu, tối đa hiệu quả sử dụng IPv4.

– Không yêu cầu thêm các giao thức mới, triển khai nhanh chóng.

– Mạng IPv6 đơn giản và do đó chi phí vận hành ít tốn kém hơn so với các mạng dual-stack.

– Các kỹ thuật giám sát, lái lưu lượng dựa trên IP gốc có thể được áp dụng mà không bị ảnh hưởng trong quá trình chuyển đổi, truyền dẫn qua mạng.

– Phù hợp cả với các mạng có dây và không dây.

Như vậy có thể nói trong giai đoạn quá độ của quá trình chuyển đổi IPv4/IPv6 việc sử dụng kỹ thuật 464XLAT mang lại hiệu quả cao trong việc sử dụng tài nguyên (tối ưu tài nguyên IPv4 đã bị cạn kiệt), dễ dàng thực hiện cũng như giảm thiểu chi phí trong giai đoạn này.

Tài liệu tham khảo

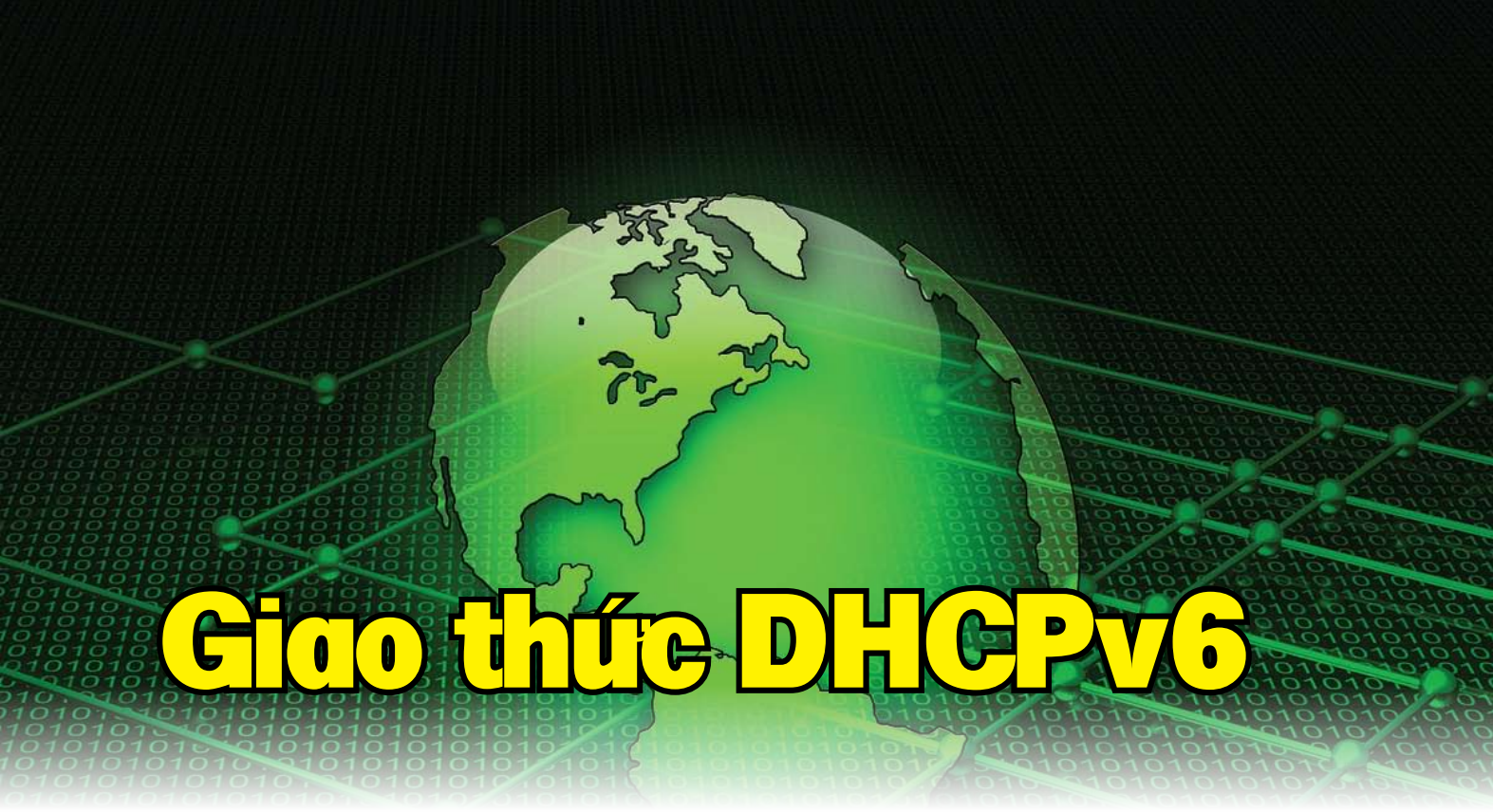
[1]. http://tools.ietf.org/html/draft-ietf-v6ops-464xlat-10.

[2].http://www.apricot2013.net/__data/assets/pdf_file/0005/59027/20130305_apricot2013_464xlat_lightning_talks_1362477143.pdf.

[3].http://www.apricot2013.net/__data/assets/pdf_file/0011/58871/20130226_apricot2013_ipv4_over_ipv6_1361969703.pdf.

[4]. [RFC6145] LI, X., BAO, C., and F. BAKER, "IP/ICMP Translation Algorithm", RFC 6145, April 2011.

[5]. [RFC6146] BAGNULO, M., MATTHEWS, P., and I. VAN BEIJNUM, *"Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers"*, RFC 6146, April 2011.



Giao thức DHCPv6

Nguyễn Trung Kiên

1. TỔNG QUAN VỀ GIAO THỨC DHCPv6

Dynamic Host Configuration Protocol (DHCP) là một giao thức cấp phát cấu hình tự động cho các máy trạm; các thông số cấu hình được cấp phát có thể bao gồm địa chỉ IP, địa chỉ máy chủ DNS, và một số các thông số cấu hình khác. Bằng việc cấp phát cấu hình tự động trên DHCP, người quản trị sẽ giảm bớt các thao tác can thiệp vào hệ thống mạng; đơn giản hóa việc quản lý và theo dõi máy trạm thông qua một hệ thống cơ sở dữ liệu tập trung trên DHCP.

Hiện nay DHCP có hai phiên bản cho mạng IPv4 và IPv6 (hay còn gọi là DHCPv6).

1.1. Sự ra đời của giao thức DHCP và DHCPv6

DHCP kế thừa giao thức cũ có tên là BOOTP. Giao thức BOOTP thường sử dụng một phương pháp tĩnh để xác định địa chỉ IP gán cho thiết bị. Khi máy tính gởi gói tin yêu cầu thì gói tin đó bao gồm cả địa chỉ vật lý, sau đó máy chủ sẽ tra cứu địa chỉ đó trong bảng địa chỉ để xác định địa chỉ IP cho máy tính này.

Điều này vẫn được thực hiện trong DHCP, tuy nhiên điểm khác biệt là DHCP bổ sung chức năng cấp phát động địa chỉ IP, một máy trạm có thể thuê một địa chỉ trong một thời gian cho phép. Ngoài việc quản lý địa chỉ IP, DHCP còn phân phối thông tin cho các dịch vụ mạng như DNS, máy chủ SIP, và các thông tin cấu hình khác.

IPv6 ban đầu muốn thoát khỏi sự phụ thuộc vào DHCP, bằng cách cho phép máy trạm có thể tự cấu hình địa chỉ cho chính nó. Đầu tiên, máy trạm sẽ khởi tạo Bootrap với thông tin là địa chỉ Link-local, các máy trạm sẽ có khả năng giao tiếp với router và nhận được các thông tin cần thiết để cấu hình một địa chỉ Global address để kết nối; tuy nhiên sẽ thiếu các thông tin về DNS, các thành phần của mạng và thông tin ứng dụng. Vì vậy việc sử dụng DHCPv6 vẫn rất cần thiết và là dịch vụ quan trọng trong hầu hết các mạng.

Nguyên lý hoạt động của DHCPv6 tương tự như của DHCP truyền thống cho mạng IPv4, nhưng giao thức DHCPv6 đã được viết lại hoàn toàn. DHCPv6

không dựa trên cơ sở của giao thức DHCP truyền thống hoặc trên BOOTP, ngoại trừ về mặt khái niệm. DHCPv6 vẫn sử dụng giao thức UDP nhưng với cổng mới và các dạng gói tin được định dạng mới và bổ sung. Vì thế giao thức mới DHCPv6 không hoàn toàn tương thích với các giao thức cũ DHCPv4 hoặc BOOTP.

1.2. Các thành phần của DHCPv6

Giống như DHCP cho IPv4, các thành phần của DHCPv6 cũng bao gồm:

– DHCPv6 Client: Gửi yêu cầu cung cấp các thông tin cấu hình.

– DHCPv6 Server: Cung cấp các thông tin cấu hình.

– DHCP Relay Agent: Điểm chuyển tiếp các gói tin giữa client và server, khi chúng không thuộc cùng một vùng mạng.

Thông thường máy chủ DHCPv6 sẽ cung cấp dịch vụ DHCPv6 cho các client được gắn trực tiếp vào phân vùng mạng của nó. Tuy nhiên, trên thực tế, hầu hết các máy chủ DHCPv6 phải được triển khai để có thể cung cấp các thông số cấu hình cho các client thuộc nhiều phân vùng mạng khác nhau, vì thế máy chủ DHCPv6 được thay thế bằng một điểm chuyển tiếp DHCPv6.

Điểm chuyển tiếp này sẽ đóng gói các gói tin trực tiếp nhận được từ các client cần sử dụng DHCPv6, và chuyển tiếp các gói tin DHCPv6 được đóng gói này đến máy chủ DHCPv6. Theo hướng ngược lại, các điểm chuyển tiếp sẽ mở gói các gói tin nhận được từ máy chủ DHCPv6 và gửi lại thông tin cho các client.

Thông số hoạt động của giao thức DHCPv6

Các cổng hoạt động:

– UDP port 546: Các client thực hiện lắng nghe (listen) gói tin DHCP.

– UDP port 547: Các máy chủ và điểm chuyển tiếp lắng nghe (listen) gói tin DHCP.

Các địa chỉ IPv6 multicast được sử dụng với DHCPv6:

– "FF02::1:2": Dùng cho tất cả điểm chuyển tiếp và máy chủ DHCPv6.

– "FF05::1:3": Dùng cho tất cả các máy chủ DHCPv6.

Cách thức nhận biết DHCPv6 Client:

– DHCPv6 sử dụng DUID (DHCP Unique Identifier) để xác định tính duy nhất cho các DHCPv6 Client. Mỗi DHCPv6 client sẽ có một DUID, được sử dụng để xác định các thiết bị khi trao đổi gói tin DHCPv6.

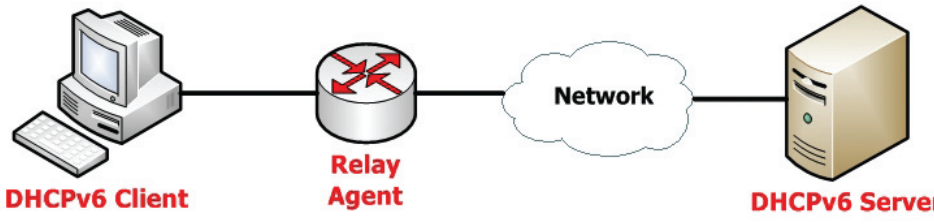
1.3. Các chế độ hoạt động của DHCPv6

DHCPv6 có 2 chế độ hoạt động chính:

- Chế độ Stateful:

Đây là chế độ hoạt động tương tự như của DHCP trên IPv4, máy chủ DHCPv6 đóng vai trò quản lý tập trung, các client sẽ sử dụng DHCPv6 để có được địa chỉ IP và các thông tin cấu hình hữu ích khác từ máy chủ DHCPv6.

– Chế độ Stateless:



Hình 1: Các thành phần trong mạng DHCPv6.

Trong chế độ này, máy chủ DHCPv6 không nhất thiết phải đóng vai trò lưu trữ và quản lý thông tin về trạng thái cấu hình của các DHCP client. Thay vào đó, các client sẽ được cấu hình địa chỉ IPv6 tự động dựa trên gói tin quảng bá từ router, hay chính xác hơn là dựa trên tiền tố IPv6 prefix được cấp phát trong gói tin quảng bá router, hoặc được cấu hình địa chỉ IP tĩnh. Với chế độ Stateless DHCPv6, các client không sử dụng máy chủ DHCP để có được thông tin địa chỉ IP, mà chúng sẽ sử dụng DHCPv6 để có được các thông tin cấu hình hữu ích khác ngoài địa chỉ IPv6, ví dụ như: địa chỉ máy chủ DNS, địa chỉ máy chủ SIP, và các dịch vụ khác.

2. CẤU TRÚC GÓI TIN DHCPv6

Cấu trúc gói tin của DHCPv6 đơn giản hơn nhiều so với DHCP trên mạng IPv4, nó dựa một phần trên cấu trúc của giao thức BOOTP được thiết kế để hỗ trợ cho các máy trạm không có ổ đĩa.

2.1. Cấu trúc gói tin DHCPv6 trao đổi giữa client và server

- **Msg-Type (1 byte)**: Loại gói tin DHCPv6.

- **Transaction-ID (3 byte)**: Xác định client, và được sử dụng để nhóm các gói tin DHCPv6 trao đổi qua lại giữa client-server.

- **DHCP Options**: được sử dụng xác định các thông tin client, server, địa chỉ và các thiết lập cấu hình khác.

Cấu trúc gói tin giữa DHCPv6 Client và Server.

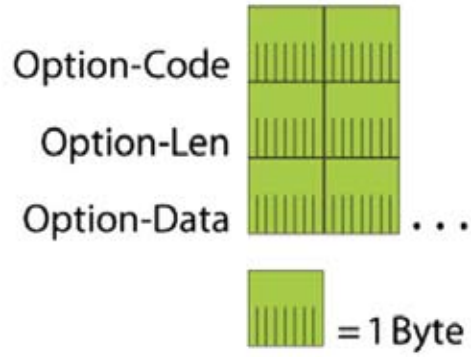
DHCP Options được định dạng với dạng type-length-value (TLV Format):

- Option-Code (2 byte): Mã tùy chọn.

- Option-Len (2 byte): chiều dài của trường Option-Data (tính theo byte).

- Option-Data: chứa các dữ liệu tùy chọn.

2.2. Cấu trúc gói tin DHCPv6 trao đổi giữa Relay-Agent và Server



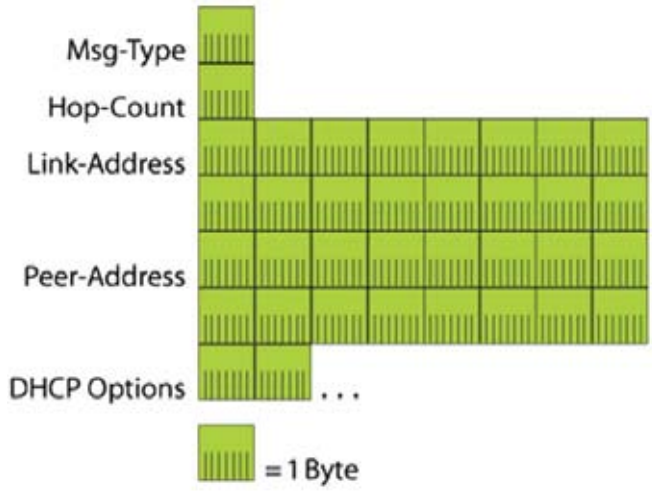
Cấu trúc của DHCP Options.

- **Hop-count (1 byte)**: Số lượng các điểm chuyển tiếp đã nhận được gói tin. Một điểm chuyển tiếp có thể loại bỏ gói tin nếu nó vượt quá số lượng hop-count cho phép.

- **Link-Address (16 byte)**: Chứa thông tin địa chỉ none-link-local được gán cho cổng kết nối với vùng mạng của client. Từ trường Link-Address, máy chủ có thể xác định được chính xác vùng địa chỉ để cấp phát cho client.

- **Peer-Address (16 byte)**: Trường thông tin chứa địa chỉ IPv6 của client (client gửi gói tin ban đầu) hoặc địa chỉ của điểm chuyển tiếp trước đó.

- **DHCP Option**: Bao gồm các tùy chọn cho gói tin chuyển tiếp (Relay Message). Các tùy chọn trong gói tin chuyển tiếp cũng cung cấp các cách thức đóng



Cấu trúc gói tin giữa DHCPv6 Relay-Agent và Server.

gói gói tin dùng để trao đổi giữa client và server.

3. CÁC DẠNG GÓI TIN TRONG DHCPV6

Các gói tin trong DHCPv6 như Bảng 1.

4. NGUYÊN LÝ HOẠT ĐỘNG CỦA DHCPV6

4.1. Vai trò của Router

Router trong mạng IPv6 có một số vai trò khác so với router trong mạng IPv4:

- Router trong mạng IPv6 có chức năng quảng

Bảng 1: Các gói tin trong DHCPv6

STT	Gói tin trong DHCPv6	Gói tin tương ứng trong DHCPv4	Nguồn gửi gói tin	Mô tả
1	SOLICIT	DHCPDISCOVER	Client	Dùng để xác định vị trí của máy chủ DHCPv6.
2	ADVERTISE	DHCPOFFER	Server	Đáp ứng gói tin "Solicit", cho biết máy chủ đã sẵn sàng.
3	REQUEST	DHCPREQUEST	Client	Yêu cầu địa chỉ hoặc các thông số cấu hình từ một máy chủ cụ thể.
4	CONFIRM	DHCPREQUEST	Client	Gửi đến tất cả các máy chủ để xác nhận các cấu hình mà chúng vừa được cấp phát vẫn còn thích hợp để thực hiện kết nối.
5	RENEW	DHCPREQUEST	Client	Gửi đến một máy chủ cụ thể để gia hạn thời gian sống của địa chỉ và cập nhật các thông số cấu hình mới (nếu có).
6	REBIND	DHCPREQUEST	Client	Gửi đến bất kỳ máy chủ nào phản hồi không nhận được gói tin Renew.
7	REPLY	DHCPACK/ DHCPNAK	Server	Gửi đến một client cụ thể để đáp ứng các gói tin như: Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release, hoặc Decline.
8	RELEASE	DHCPRELEASE	Client	Cho biết rằng client không còn sử dụng địa chỉ đã được cấp phát.
9	DECLINE	DHCPDECLINE	Client	Gửi đến một máy chủ cụ thể để thông báo rằng địa chỉ được cấp phát đã được sử dụng rồi.

10	RECONFIGURE	DHCPFORCERENEW	Server	Gửi cho client để thông báo máy chủ đã được cập nhật lại các thông số cấu hình. Client có thể gửi các gói tin như Renew hoặc Information-Request.
11	INFORMATION-REQUEST	DHCPINFORM	Client	Yêu cầu các thông số cấu hình khác từ máy chủ (không phải địa chỉ IP).
12	RELAY-FORW	none	Relay-Agent	Điểm chuyển tiếp sẽ gửi một gói tin "Relay-Forward" đến các máy chủ, hoặc qua một điểm chuyển tiếp khác.
13	RELAY-REPLY	none	Server	Gửi đến một điểm chuyển tiếp mà dùng để cung cấp cấu hình cho client.

bá các thông số sẵn có thông qua gói tin quảng bá Router Advertisement.

- Cung cấp các thông tin về prefix hoặc các thông tin thích hợp cho các kết nối.

- Các bit Autonomous chỉ ra các cấu hình tự động cho các node.

- Các cờ "M" và "O" trên gói tin quảng bá của router dùng để xác định cách thức hoạt động của DHCPv6 (dạng Stateful hay Stateless).

Một DHCPv6 client sẽ thực hiện chế độ cấu hình tự động bằng cách sử dụng DHCPv6 dựa trên các cờ (flag) trong gói tin quảng bá của router (RA):

Có 2 bit flag được thiết lập với các mục đích:

- **Managed Address Configuration Flag**: Hay còn gọi là cờ "M". Khi cờ này thiết lập là 1, client có thể sử dụng DHCPv6 để lấy địa chỉ quản lý IPv6 từ một máy chủ DHCPv6.

- **Other Stateful Configuration Flag**: Hay còn gọi là cờ "O". Khi cờ này thiết lập là 1, client có thể sử dụng DHCPv6 để lấy các thông số cấu hình khác có sẵn (ví dụ: địa chỉ máy chủ DNS).

Bảng 2

Cờ "M"	Cờ "O"	Mô tả trạng thái
0	0	Một mạng không có hạ tầng DHCPv6. Các máy tính sẽ sử dụng gói tin quảng bá của router cho địa chỉ link-local và một số phương pháp khác (cấu hình bằng tay) để cấu hình các thiết lập khác.
1	1	DHCPv6 được sử dụng cho việc cung cấp thông tin địa chỉ và các cấu hình thiết lập khác. Đây còn gọi là Stateful DHCPv6, trong đó DHCPv6 được quyền cung cấp các địa chỉ đến cho máy chủ IPv6.
0	1	DHCPv6 không được sử dụng để gán địa chỉ, chỉ được sử dụng để cấp các thông tin cấu hình khác. Router sẽ được cấu hình để quảng bá thông tin prefix cho các địa chỉ non-link-local cho các máy chủ IPv6. Sự kết hợp này được gọi là Stateless DHCPv6.
1	0	DHCPv6 được sử dụng cho việc cấp địa chỉ IP, nhưng không cung cấp các thiết lập khác. Tuy nhiên, thông thường các máy chủ IPv6 thường cần phải được cấu hình thêm các thông số khác (máy chủ DNS,…), vì vậy sự kết hợp này không hay được sử dụng.

Các trạng thái của sự kết hợp cờ "M" và cờ "O" như Bảng 2.

4.2. Nguyên lý hoạt động của DHCPv6

4.2.1. Chế độ Stateful DHCPv6

Chế độ này có được khi cả hai cờ "M" và cờ "O" trong gói tin quảng bá đều được thiết lập là 1. Cách thức trao đổi gói tin DHCPv6 như sau (Hình 2):

1. Client sẽ gửi một gói tin multicast **"Solicit"** để tìm kiếm máy chủ DHCPv6 và yêu cầu cấp phát.

2. Bất kỳ máy chủ nào đáp ứng yêu cầu của client có thể hồi đáp với một gói tin **"Advertise"**.

3. Client lựa chọn một trong các máy chủ và gửi một gói tin **"Request"** để yêu cầu cấp phát địa chỉ IPv6 và các thông số khác.

4. Máy chủ đáp ứng với một gói tin **"Reply"**, bao gồm địa chỉ và các thông số cấu hình để hoàn tất quá trình cấp phát.

Trong trường hợp Rapid Commit có thể thực hiện nhanh hơn với chỉ hai gói tin Solicit và Reply. Cách thức trao đổi gói tin được mô tả trong Hình 3.

Trong trường hợp giữa Client và Server còn có thêm điểm chuyển tiếp, thực hiện trao đổi gói tin như Hình 4.

- Relay-Forw: Dùng để chuyển tiếp các gói tin Solicit và Request từ client đến server.

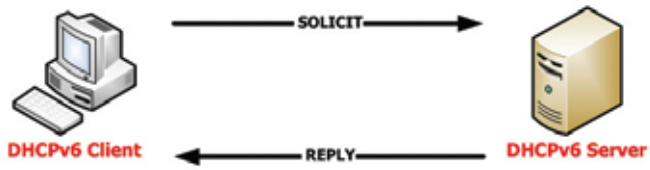
- Relay-Reply: Dùng để chuyển tiếp các gói tin Advertise và Reply từ server đến client.

4.2.2. Chế độ Stateless DHCPv6

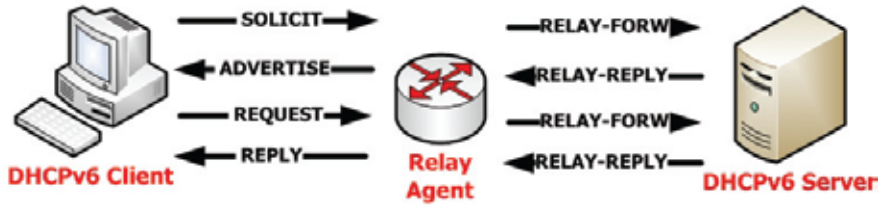
Chế độ này được thiết lập khi cờ "M" được thiết lập 0 và cờ "O" được thiết lập 1 trong gói tin quảng bá.

Trong mạng IPv6, router được cấu hình để cung cấp các địa chỉ prefix cho các máy trạm IPv6, vì vậy DHCPv6 chỉ dùng để cấp phát các thông tin

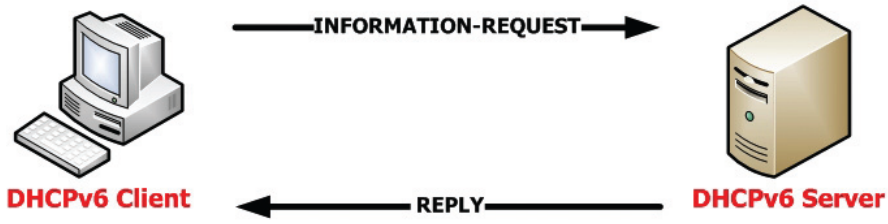
Hình 2: Trao đổi gói tin trong Stateful DHCPv6 thông thường.



Hình 3: Trao đổi gói tin trong chế độ Rapid Commit.



Hình 4: Trao đổi gói tin trong Stateful DHCPv6 khi có điểm chuyển tiếp.



Hình 5: Trao đổi gói tin trong Stateless DHCPv6.

cấu hình khác như: máy chủ DNS, tên miền và các cấu hình khác mà trong gói tin quảng bá của router không có.

Vì các lý do này, chế độ Stateless DHCPv6 chỉ có hai dạng gói tin (Hình 5):

- **Information-Request**: Gửi bởi client để yêu cầu các thông số cấu hình khác từ máy chủ DHCP (không phải địa chỉ IP).

- **Reply**: Gửi bởi server cho client, bao gồm các thông tin về thông số cấu hình được yêu cầu cấp phát.

5. KẾT LUẬN

Sự khác biệt lớn nhất của DHCPv6 so với DHCP truyền thống chính là sự kết hợp với các thiết bị định tuyến trên mạng IPv6. Qua đó, DHCPv6 cũng cung cấp nhiều tùy chọn hơn cho các máy trạm để có được các thông số cấu hình cần thiết. Với việc triển khai sử dụng DHCPv6 Server và DHCPv6 Relay tại các vùng mạng khác nhau có thể giúp triển khai hệ thống cấp phát địa chỉ IPv6 tự động cho nhiều vùng mạng LAN của một doanh nghiệp. Việc quản lý, cấu hình các vùng địa chỉ được thực hiện tập trung. Các địa chỉ IPv6 khó nhớ được cấp phát cho các máy trạm một cách tự động, giúp đơn giản hóa việc quản lý, vận hành cho người quản trị và việc triển khai là hoàn toàn trong suốt với người sử dụng đầu cuối.

DHCPv6 cũng là một tính năng mới và cần thiết cho các ISP, các tổ chức CNTT, nghiên cứu triển khai để cung cấp dịch vụ Internet trên mạng IPv6 cho các khách hàng.

Tài liệu tham khảo

[1]. http://tools.ietf.org/html/rfc3315.

[2]. http://en.wikipedia.org/wiki/DHCPv6.

[3]. http://meetings.ripe.net/ripe-53/presentations/dhcpv6.pdf.

[4]. http://technet.microsoft.com/en-us/magazine/2007.03.cableguy.aspx.

[5]. http://ipv6friday.org/blog/2011/12/dhcpv6/.

[6]. http://www.nanog.org/meetings/nanog45/presentations/.Tuesday/Brzozow_dhcpv6_v7_N45.pdf.

BẢO MẬT IPv6 TRONG MẠNG LAN

Internet đang trong giai đoạn chuyển đổi, giao thức Internet IPv4 sẽ dần được thay thế bằng giao thức Internet IPv6. Trong quá trình chuyển đổi, các bộ định tuyến hỗ trợ đồng thời lưu lượng IPv4 và IPv6 nảy sinh các vấn đề an toàn an ninh từ sự kết hợp IPv4 và IPv6 trong mạng chuyển đổi.

Trong IPv4, các giao thức phân giải địa chỉ (ARP- Address Resolution Protocol) và Giao thức cấu hình động máy chủ (DHCP- Dynamic Host Configuration Protocol) dễ bị tác động bởi các nguy cơ an toàn an ninh từ lớp 2 (tầng liên kết dữ liệu trong mô hình OSI). Các nguy cơ này rất phổ biến, tuy nhiên cũng đã có các công cụ hiệu quả như Dynamic ARP inspection và DHCP snooping làm giảm tác động của các cuộc tấn công như vậy. Mặc dù IPv6 không sử dụng ARP, IPv6 vẫn bị ảnh hưởng bởi các nguy cơ tương tự, nhưng về hình thức có khác biệt. Đó là tác động từ các cuộc tấn công như giả mạo địa chỉ MAC (MAC hijacking), giả mạo các máy chủ DHCP và bộ định tuyến.

IPv4 và IPv6 có các điểm tương đồng và có các điểm khác biệt. Điểm tương đồng cho phép áp dụng các quy tắc an toàn an ninh trên mạng IPv4 để bảo vệ mạng IPv6. Tuy nhiên những đặc điểm mới của IPv6 sẽ yêu cầu những giải pháp mới để đảm bảo an toàn, an ninh mạng lưới IPv6 trong tương lai. Hiện nay, vấn đề an toàn an ninh tại lớp 2 cho IPv6 vẫn đang được nghiên cứu và trao đổi. Bài báo giới thiệu một số phương pháp chống giả mạo địa chỉ để bảo mật IPv6 trên mạng LAN.

Phan Xuân Dũng

1. KHÔNG SỬ DỤNG ĐỊA CHỈ RIÊNG MỞ RỘNG TRONG CẤU HÌNH TỰ ĐỘNG

Địa chỉ này được định nghĩa trong RFC 4941 cho mục đích cấu hình địa chỉ tự động phi trạng thái (Privacy Extentions for Stateless Address Autoconfiguration) hay còn gọi là địa chỉ riêng mở rộng. Địa chỉ riêng mở rộng này không phải là địa chỉ riêng (private address) trong IPv4, nó là địa chỉ IPv6 định danh toàn cầu (global unicast address). Người sử dụng chỉ cần bật tính năng IPv6 khi kết nối mạng và các thiết bị đầu cuối dựa vào bản tin RA (Router Advertisements) để tự cấu hình địa chỉ.

Trong các hệ điều hành Windows XP, Vista, OS X 10.7, IOS 4, Android 4 mặc định bật địa chỉ riêng

mở rộng, các địa chỉ riêng mở rộng này có tính che đậy danh tính người sử dụng, và người quản trị mạng được khuyến nghị tắt chúng khi không cần thiết phải sử dụng. Ví dụ cụ thể về thao tác thực hiện tắt tính năng tự động cho một số hệ điều hành như sau:

- Windows XP

Trong cửa sổ dòng lệnh được chạy với quyền Administrator:

netsh interface ipv6 set privacy state=disabled store=persistent

netsh interface ipv6 set privacy state=disabled

Hoặc vào Registry cài đặt khóa

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\GlobalParams\UseTemporaryAddresses về 0

- Windows Vista

Trong cửa sổ dòng lệnh được chạy với quyền Administrator:

netsh interface ipv6 set global randomizeidentifiers=disabled

netsh interface ipv6 set global randomizeidentifiers=disabled store=persistent

netsh interface ipv6 set privacy disabled

- Mac OS X10 ("Lion")

Để tắt tính năng này vĩnh viễn, sửa tệp /etc/sysctl.conf và đặt

net.inet6.ip6.use_tempaddr=0

Sau đó khởi động lại.

Nếu bạn muốn tắt tính năng này mà không cần khởi động, ta có thể sử dụng lệnh sysctl để tắt với phiên hiện tại. Chú ý rằng tính năng này sẽ bật lại khi khởi động lại máy trong lần kế tiếp trừ khi chúng ta sửa tệp sysctl.conf.

sysctl –w net.inet6.ip6.use_tempaddr=0

- iOS

Hệ điều hành iOS của hãng Apple sử dụng trên các sản phẩm IPhone, IPad và ITouch, không có cách nào tắt tính năng tự động cấu hình địa chỉ riêng mở rộng trên các thiết bị này. Nhưng chúng ta có thể sử dụng cách khác đó là ngừng gửi bản tin RA từ các bộ định tuyến.

- Android

Tương tự iOS, không có cách nào để tắt tính năng tự động cấu hình địa chỉ riêng mở rộng. Nên cũng có thể sử dụng cách ngừng gửi bản tin RA từ các bộ định tuyến.

Các hệ điều hành khác cũng mặc định bật tự động cấu hình địa chỉ riêng mở rộng như Ubuntu, Centos, Redhat… chúng ta cũng cần xem hướng dẫn của từng hệ điều hành để tắt tính năng này.

2. SỬ DỤNG TÍNH NĂNG uRPF

Việc giả mạo địa chỉ IP có thể thực hiện trong quá trình tấn công DoS, địa chỉ IP giả mạo này được gửi tới đích như là một địa chỉ hợp lệ. uRPF là công cụ kiểm tra giảm thiểu việc gửi các gói tin giả mạo. uRPF thực hiện kiểm tra trên bảng định tuyến nguồn của gói tin gửi đi, kiểm tra trên giao diện của bộ định tuyến mà gói tin được gửi đến. Bộ định tuyến xác nhận gói tin đến từ đường dẫn mà người gửi sử dụng để gửi tới đích có hợp lệ hay không. Nếu hợp lệ nó chuyển tiếp gói tin đi, nếu không hợp lệ nó loại bỏ gói tin.

Các câu lệnh bật tính năng IPv6 uRPF trên thiết bị Cisco

ip cef
ipv6 cef
ipv6 verify unicast reverse-path

Chú ý rằng việc kiểm tra IPv6 uRPF là thực hiện bằng phần mềm trên nhiều thiết bị Cisco.

3. SỬ DỤNG ĐỊA CHỈ THEO CHUẨN EUI 64

Nhằm tạo nên một không gian định danh thiết bị lớn hơn cho các nhà sản xuất, IEEE đưa ra một phương thức đánh số mới cho các giao diện mạng gọi là EUI-64 (Extented Unique Identifier 64), trong đó giữ nguyên 24 bít định danh nhà sản xuất thiết bị và phần mở rộng tăng lên thành 40 bít. Như vậy, nếu giao diện mạng được định danh theo dạng thức này, địa chỉ phần cứng của nó sẽ gồm 64 bít.

64 bít định danh giao diện địa chỉ IPv6 khi đó sẽ được tạo nên từ 64 bít dạng EUI-64 từ địa chỉ MAC theo quy tắc: Trong số 24 bít xác định nhà cung cấp thiết bị, có một bít được quy định là bít U (xxxx xxUx xxxx xxxx xxxx xxxx). Thông thường bít này có giá trị 0. Người ta tiến hành đảo bít bít U này (từ 0 thành 1 và từ 1 thành 0), và lấy 64 bít sau khi thực hiện như vậy làm 64 bít định danh giao diện trong địa chỉ IPv6.

Các thiết bị định tuyến có thể cấp phát tự động địa chỉ dạng EUI-64. Do đó chúng có thể bắt buộc địa chỉ MAC nhúng trong địa chỉ dạng EUI-64 phải trùng với địa chỉ MAC tới từ gói tin. Tuy nhiên với cách này kẻ tấn công có thể biết thông tin thiết bị kết nối. Để giảm thiểu điều này chúng ta cũng có thể sử dụng thuật toán CGA (Cryptographically Generated Addresses RFP 3972), một cách thức gắn một ký hiệu khóa công khai (public signature key) với một địa chỉ IPv6 trong giao thức SEND (Secure Neighbor Discovery RFC 3971). CGA là địa chỉ IPv6 định danh giao diện được khởi tạo bằng cách tính toán mã hóa hàm băm một chiều từ khóa công cộng và các thông số phụ trợ.

4. TẮT ĐƯỜNG HẦM IPv6 over IPv4 KHÔNG SỬ DỤNG

Trong vài trường hợp, Windows Vista và Windows 7 có thể tạo đường hầm IPv6 over IPv4 tự động. Để tắt giao thức đường hầm này thực hiện các câu lệnh sau:

netsh interface 6to4 set state state=disabled

netsh interface teredo set state disable

netsh interface isatap set state disabled

netsh interface httpstunnel set interface state=disabled

Windows 2008R2, Windows 7 có thể cài đặt trong group policy, Computer Configuration → Policies → Administrative Templates → Network → TCP/IP Settings → IPv6 Transition Technologies

5. SỬ DỤNG FIREWALL HẠN CHẾ ICMPv6

ICMPv6 thực hiện nhiều chức năng hơn so với ICMPv4, bao gồm Path MTU discovery, Router Discovery, Neighbor Discovery, Mobile IPv6, quản lý multicast và tái cấu hình địa chỉ. Như vậy chắc chắn các bản tin ICMPv6 phải được phép đi qua Firewall. Các hướng dẫn về lọc ICMPv6 được đề cập trong RFC 4890.

Windows XP SP2 Firewall và Windows 2003 SP1 hỗ trợ IPv6. Tuy nhiên Windows XP Firewall không thể cài đặt các luật khác nhau cho IPv4 và IPv6. Chẳng hạn không thể chỉ mở cổng cho IPv4, hay chỉ chặn ICMP echo request cho IPv6. Windows XP cũng không thể tạo luật cho một vùng địa chỉ mạng IPv6.

Windows Vista, Windows 7 và 2008 hỗ trợ IPv6 trong Firewall của hệ điều hành, cho phép cài đặt các luật với một vùng địa chỉ mạng IPv6, và các luật khác nhau cho ICMPv4 và ICMPv6.

Một số các chương trình Firewall khác hỗ trợ IPv6 như: ESET Personal Firewall từ phiên bản 3 trở đi. F-Secure Client Security 7.12. Norton Personal Firewall, Symantec Endpoind Security không hỗ trợ IPv6.

RedHat 5.x không hỗ trợ IPv6 stateful qua Firewall, tuy vậy Redhat 6.x đã được bổ sung để hỗ trợ IPv6 stateful qua Firewall. Tương tự với hệ điều hành Ubuntu với phiên bản từ 7.04, Mac OS X 10.7.3, Solaris 10 cũng đã hỗ trợ IPv6 trong Firewall.

Phần cứng Firewal Cisco ASA, Pix hỗ trợ IPv6 từ phiên bản IOS 7.0, FWSM từ 4.0. PIX và ASA không hỗ trợ IPv6 trong brigde mode (chỉ trong routed mode). IOS firewall có hỗ trợ từ phiên bản 12.3(7)T. IOS Vlan ACL không hỗ trợ IPv6.

6. HẠN CHẾ CÁC BẢN TIN RA

Các máy đầu cuối cấu hình các địa chỉ IPv6 và nhận thông tin từ router của vùng mạng đó thông qua các bản tin IPv6 RA (Router Advertisement). Những bản tin RA này không cần nhận thực, do đó có thể ẩn chứa mất an toàn với mạng LAN. Điều quan trọng là các bản tin RA giả xâm nhập vào trong mạng LAN, và có thể gây ra DoS trên nhiều hệ điều hành và thiết bị mạng. IETF cũng đã thảo luận vấn đề này trong RFC 6104. Chúng ta cần tắt các bản tin này trên các bộ định tuyến khi không cần thiết sử dụng. Ngoài ra, chúng ta cũng sử dụng RA Guard để cho phép người quản trị mạng ngăn chặn hay từ chối các RA giả mạo.

7. NGĂN CHẶN MÁY CHỦ DHCPv6 GIẢ MẠO

Để ngăn chặn DHCPv6 giả mạo có thể chặn các luồng DHCPv6 trên các cổng không cần thiết. DHCPv6 sử dụng các cổng TCP và UDP 546, 547. IETF cũng đang soạn bản dự thảo tiêu chuẩn khuyến nghị an toàn an ninh DHCPv6 sử dụng CGA.

8. ĐỊA CHỈ LINK LOCAL

Tất cả các thiết bị mạng đều yêu cầu cấu hình địa chỉ link local trên mỗi giao diện. Địa chỉ này được sử dụng để truyền thông tin giữa các thiết bị mạng trên cùng liên kết. Điều này cũng dễ dàng cho phép kẻ tấn công truyền thông tin trong liên kết mà không cần yêu cầu thông tin gì khác. Chúng ta có thể hạn chế điều này bằng cách nhận thực kết nối khi thiết bị mạng kết nối trên đường liên kết sử dụng an toàn vật lý tiêu chuẩn IEEE 802.1x hoặc SEND (Secure Neighbor Discovery).

Tài liệu tham khảo

[1]. RFC 4942: *IPv6 Transition/Coexistence Security Considerations.*

[2]. RFC 6104: *Rogue IPv6 Router Advertisement Problem Statement.*

[3]. RFC 6105 IPv6 RA Guard.

[4]. RFC 4890: *Recommendations for Filtering ICMPv6 Messages in Firewalls.*

[5]. RFC 6092: *Recommended Simple Security Capabilities in Customer Premises Equipment for Providing Residential IPv6 Internet Service.*

[6]. RFC 3971: *Secure-Neighbor-Discovery.*

[7]. RFC 4864: *Local Network Protection for IPv6.*

[8]. http://ipv6.com/articles/research/Secure-Neighbor-Discovery.htm.

[9]. https://wikispaces.psu.edu/display/ipv6/IPv6+security.

[10]. *NSA Router Security Configuration Guide Supplement - Security for IPv6* http://www.nsa.gov/ia/_files/routers/I33-002R-06.pdf.

[11]. *NSA Firewall Design Considerations for IPv6*

http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/ipv6/I733-041R-2007.pdf.

[12]. http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-ra-guard.html.

[13]. http://tools.ietf.org/html/draft-ietf-dhc-secure-dhcpv6-07.

RRPP
- Giao thức chống vòng lặp chuyển tiếp hiệu quả cho mạng Ethernet dạng vòng ring

Diệp Thanh Nguyên

1. GIỚI THIỆU

Trong mạng Ethernet, nếu tồn tại một chu trình (đường đi mà điểm đầu trùng với điểm cuối) thì sẽ gây ra hiện tượng vòng lặp chuyển tiếp (forwarding loop). Đây là hiện tượng lưu lượng quảng bá được truyền tải thành một vòng (loop) và cứ thế tồn tại trong mạng. Vòng lặp chuyển tiếp sẽ chiếm hết băng thông của các cổng trên thiết bị chuyển mạch trong vòng vài giây, làm mạng bị nghẽn và tê liệt toàn bộ.

Các giao thức mạng hiện được dùng phổ biến để ngăn chặn vòng lặp chuyển tiếp là những giao thức dựa trên thuật toán tìm cây khung nhỏ nhất như: STP (Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol), MSTP (Multiple Spanning Tree Protocol). Trong đó, RSTP/MSTP (sau đây gọi tắt là xSTP) là các giao thức cho thời gian hội tụ nhanh cỡ vài giây. Tuy nhiên, các giao thức này vẫn không đáp ứng được cho các dịch vụ thời gian thực, vốn yêu cầu thời gian hội tụ ngắn hơn nữa.

Bài viết này trình bày một giao thức chống vòng lặp chuyển tiếp hiệu quả hơn xSTP trong trường hợp topo mạng là dạng vòng (ring). Đó là giao thức RRPP (Rapid Ring Protection Protocol) của hãng Huawei (Trung Quốc), một giao thức được sử dụng chính thức và đồng bộ trên mạng Metro Ethernet của Viettel.

2. CÁC NHƯỢC ĐIỂM CỦA xSTP ĐỐI VỚI MẠNG ETHERNET DẠNG VÒNG RING

+ *Thời gian hội tụ chậm, không phù hợp với các dịch vụ thời gian thực*: Khi có lỗi tại một điểm nào đó trong mạng, xSTP bắt đầu quá trình tính toán lại mô hình. Trong thời gian hội tụ, lưu lượng tạm thời bị chặn (block). Mặc dù xSTP có thời gian hội tụ là vài giây, nhanh hơn rất nhiều so với STP nhưng như vậy vẫn chưa đủ. Các dịch vụ thời gian thực như hội nghị truyền hình, truyền hình qua giao thức Internet (IPTV) đòi hỏi thời gian hội tụ trong vòng vài trăm mili giây để không gây cảm giác gián đoạn hình ảnh cho người dùng, một sự gián đoạn đến vài giây là không chấp nhận được.

+ *Giới hạn bán kính 7 thiết bị*: IEEE khuyến nghị không nên có quá 7 thiết bị tính từ root bridge trong một mạng chạy xSTP. Nếu không, sau một thời gian hoạt động giao thức có thể sẽ gặp lỗi.

3. ƯU ĐIỂM CỦA RRPP SO VỚI xSTP

+ *Thời gian hội tụ nhanh đến 50ms*: RRPP không sử dụng cơ chế bầu chọn root bridge như xSTP mà chỉ định trước một nút đóng vai trò "chủ" nên quá trình hội tụ diễn ra tức thời khi phát hiện có thay đổi trong vòng ring.

+ *Không giới hạn số thiết bị*: Một vòng chạy RRPP

có thể có số nút không giới hạn.

+ *Nguyên lý hoạt động đơn giản*: Nguyên lý hoạt động của RRPP đơn giản hơn xSTP, do đó việc cấu hình và vận hành cũng dễ dàng hơn.

4. RRPP - GIAO THỨC BẢO VỆ VÒNG RING NHANH

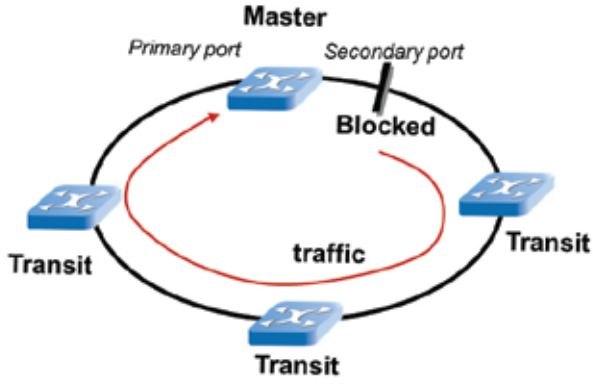
a. Mô hình cơ bản một mạng dạng vòng ring sử dụng giao thức RRPP

Hình 1 là một mạng dạng vòng ring gồm 4 nút, được chống vòng lặp bằng RRPP. Mô hình vòng ring có đặc điểm là các nút đấu với nhau thành hình tròn, mỗi nút chỉ có duy nhất 2 cổng đấu nối với 2 nút kề bên trái và phải. RRPP gồm các thành phần cơ bản sau:

+ *Master node (nút chủ)*: Chỉ có một nút duy nhất trong vòng được cấu hình là chủ. Nút chủ chịu trách nhiệm gửi các bản tin hello để kiểm tra xem vòng đang kín hay hở.

+ *Transit node (nút chuyển tiếp)*: Tất cả các nút còn lại được cấu hình là nút chuyển tiếp. Nút chuyển tiếp không phát bản tin hello mà chỉ trung chuyển bản tin hello từ nút chủ. Nghĩa là khi nút chuyển tiếp nhận được bản tin hello từ cổng này thì nó sẽ gửi bản tin hello đó ra cổng còn lại. Mô hình trên Hình 1 gồm có 1 nút chủ và 3 nút chuyển tiếp.

+ *Primary port (cổng chính) và Secondary port (cổng phụ)*: Trên nút chủ có 2 cổng đấu nối vào một ring, cổng phát ra bản tin hello gọi là cổng chính và cổng còn lại nhận bản tin hello gọi là cổng phụ. Như vậy bản tin hello từ cổng chính đi 1 vòng trong ring và quay về cổng phụ. Lưu ý, nút chủ chỉ phát bản tin hello một chiều từ cổng chính sang cổng phụ mà không có hướng ngược lại. Trên Hình 1, dấu mũi tên là chiều lưu lượng chứ không phải chiều của bản tin hello.



Hình 1: Mô hình mạng dạng vòng ring 4 nút.

+ *Control VLAN (VLAN điều khiển)*: Bản tin hello được phát đi trong một mạng cục bộ ảo (VLAN-Virtual Local Area Network) riêng biệt gọi là "VLAN điều khiển", trong khi tất cả lưu lượng của dữ liệu được truyền trong những VLAN khác. Control VLAN phải được khai báo cho phép trung chuyển (allow trunking) qua tất cả các cổng của tất cả các nút mạng trong vòng ring.

+ *Protected VLAN (VLAN được bảo vệ)*: Lưu lượng của những dữ liệu cần được RRPP bảo vệ được khai báo trong những VLAN gọi là VLAN được bảo vệ và RRPP chỉ bảo vệ những bản tin lưu lượng này. VLAN được bảo vệ dĩ nhiên phải được khai báo cho phép trung chuyển qua tất cả các cổng của tất cả các nút mạng trong ring.

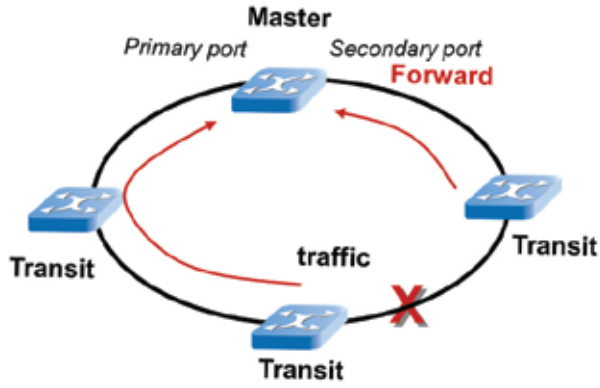
+ *RRPP Domain (miền RRPP)*: Tập hợp của một "VLAN điều khiển" và những "VLAN được bảo vệ" tạo thành một miền gọi là miền RRPP. Trong Hình 1, 4 nút mạng tham gia vào cùng một miền RRPP. Trên một ring vật lý có thể khai báo nhiều miền RRPP hoạt động cùng lúc, chẳng hạn lưu lượng dịch vụ Internet và lưu lượng dịch vụ IPTV có thể thuộc hai miền RRPP khác nhau, do dãy VLAN của chúng khác nhau. Một nút có thể tham gia vào nhiều miền RRPP khác nhau, một nút có thể đóng vai trò nút

chủ trong miền này và nút chuyển tiếp trong miền khác.

b. Nguyên lý hoạt động của RRPP

– *Trạng thái bình thường*:

Nút chủ luôn luôn phát ra bản tin hello với chu kỳ là 1 giây để "kiểm tra sức khỏe" của mạng (health-check). Bình thường, không có điểm nào bị lỗi thì vòng là khép kín, bản tin hello phát ra từ cổng chính sẽ được các nút chuyển tiếp chuyển đi 1 vòng quanh ring và quay về cổng phụ của nút chủ.



Hình 2: Trạng thái hở vòng.

Nếu nút chủ nhận được bản tin hello từ cổng phụ, nó hiểu rằng vòng đang kín. Nút chủ sẽ thực hiện chặn lưu lượng ra vào cổng phụ. Lúc này toàn bộ lưu lượng của các nút trong vòng chỉ đi về hướng cổng chính của nút chủ. Do lưu lượng không thể đi qua cổng phụ nên không thể xảy ra hiện tượng vòng lặp trong ring, ring được bảo vệ chống vòng lặp.

Nút chủ chỉ chặn những lưu lượng thuộc về VLAN được bảo vệ chứ không chặn lưu lượng của VLAN điều khiển. Vì vậy chỉ lưu lượng dữ liệu mới bị chặn để chống vòng lặp, còn bản tin hello thuộc về VLAN điều khiển nên không bị chặn. Một khi nút chủ còn nhận được bản tin hello thì nó sẽ còn chặn cổng phụ.

Hình 1 minh họa trạng thái bình thường của vòng.

– *Trạng thái hở vòng ring*:

Khi trong vòng ring có một nút hoặc một kết nối bị lỗi, vòng ring sẽ bị đứt đoạn. Nút chủ sẽ phát hiện ra sự gián đoạn này và nó sẽ thực hiện mở chặn (unblock) cổng phụ. Lúc này lưu lượng của các nút bên trái điểm lỗi sẽ đi về cổng chính của nút chủ, còn lưu lượng của các nút bên phải điểm lỗi sẽ đi về cổng phụ. Do đó thông tin không bị gián đoạn (Hình 2).

Nút chủ phát hiện sự gián đoạn trong vòng ring bằng hai cơ chế sau:

+ Nếu kết nối bị lỗi là một kết nối trực tiếp giữa 2 nút (không thông qua thiết bị truyền dẫn trung gian) thì 2 nút kề bên điểm bị lỗi sẽ lập tức phát hiện ra lỗi vì cổng kết nối giữa chúng bị mất kết nối (down). Chúng sẽ gửi bản tin "mất kết nối- link-down" báo cho nút chủ, bản tin link-down đi theo hướng không bị lỗi nên sẽ đến được nút chủ. Quá trình này gọi là "Thông báo thay đổi trạng thái kết nối". Thời gian phát hiện ra lỗi sẽ bằng thời gian phát hiện mất kết nối Ethernet, vào khoảng 50ms.

+ Nếu kết nối giữa 2 nút là không trực tiếp mà thông qua một hệ thống truyền dẫn, khi lỗi xảy ra bên trong hệ thống truyền dẫn thì 2 nút sẽ không phát hiện được sự gián đoạn thông tin vì cổng kết nối giữa chúng không bị "down". Tuy nhiên, lúc này bản tin Hello sẽ không thể đến được cổng phụ và nút chủ sẽ phát hiện ra sự gián đoạn trong vòng từ việc bị mất bản tin hello trong 3 lần liên tiếp. Thời gian phát hiện lỗi lúc này là 3 giây.

Do khi phát hiện ra lỗi thì nút chủ lập tức hành động, không có quá trình bầu chọn nút nào chiếm quyền điều khiển như trong giao thức xSTP nên thời gian hội tụ của RRPP nhanh hơn xSTP.

– *Quá trình khôi phục vòng ring bị lỗi*:

Khi kết nối bị lỗi được khắc phục, vòng trở thành kín, nút chủ sẽ chặn cổng phụ để tránh vòng lặp, đồng thời gửi bản tin *Flush-db* cho tất cả các node

trong miền RRPP. Các nút khi nhận bản tin flush-db thì sẽ thực hiện xóa toàn bộ bảng MAC để học trở lại. Việc xóa bảng MAC sẽ đảm bảo cho lưu lượng được đẩy ra đúng hướng như trước khi bị lỗi, tức là đi về phía cổng chính thay vì cổng phụ.

Nút chủ phát hiện sự khôi phục của vòng bằng hai cơ chế sau:

+ Nếu kết nối bị lỗi là kết nối trực tiếp giữa 2 nút, 2 nút sẽ phát hiện ra cổng kết nối giữa chúng đã được khôi phục lại. Chúng sẽ gửi bản tin đã hoàn thành kết nối (link-up) báo cho nút chủ.

+ Trong trạng thái bị lỗi, nút chủ vẫn luôn phát ra bản tin hello. Khi nút chủ lại nhận được bản tin hello từ cổng phụ có nghĩa là vòng ring đã khôi phục.

- *Trạng thái Preforwarding*:

Có một khoảng thời gian rất ngắn giữa lúc vòng ring được khôi phục và trước khi nút chủ phát hiện ra sự kiện này. Khoảng thời gian này nút chủ vẫn chưa kịp chặn cổng phụ nên vòng ring đang kín, lúc này có thể xảy ra vòng lặp.

Để khắc phục điều này, RRPP có cơ chế gọi là Preforwarding. Trạng thái bị lỗi sẽ được chuyển sang trạng thái Preforwarding trước khi chuyển về trạng thái bình thường.

Khi một nút phát hiện ra vòng ring đã được khôi phục, nó không lập tức truyền dữ liệu ra ngay mà chỉ gửi bản tin link-up đến nút chủ. Nút chủ chặn cổng phụ trước, sau đó mới gửi bản tin flush-db đến các nút. Chỉ khi các nút nhận được bản tin flush-db thì mới cho phép lưu lượng truyền ra. Lúc này cổng phụ đã được khóa nên đảm bảo không xảy ra hiện tượng vòng lặp.

5. MỘT SỐ KINH NGHIỆM VẬN HÀNH RRPP

Mạng Metro Ethernet của Viettel sử dụng 100% cáp quang đấu nối trực tiếp giữa các thiết bị mạng nên khả năng hội tụ của RRPP là 50ms, đáp ứng nhu cầu của các dịch vụ thời gian thực. RRPP có ưu điểm vượt trội xSTP, tuy nhiên RRPP cũng có một số hạn chế đáng chú ý sau đây:

+ RRPP chỉ sử dụng được cho mô hình mạng dạng vòng ring, trong khi xSTP có thể sử dụng cho một mô hình mạng bất kỳ. Vì vậy RRPP không thể thay thế hoàn toàn xSTP.

+ RRPP không có khái niệm "chi phí đường truyền" như xSTP nên không thể điều khiển điểm bị chặn bằng cách tính toán chi phí đường truyền, mà RRPP luôn luôn chặn tại cổng phụ của nút chủ. Điều này làm cho toàn bộ lưu lượng trong vòng ring muốn đi lên trên (uplink) thì phải đổ dồn về 1 hướng, về hướng cổng chính của nút chủ. Các nút càng gần nút chủ thì càng chịu tải nặng hơn. Tuy nhiên có thể khắc phục bằng cách chọn nút chủ là nút nằm giữa vòng ring, lúc này vòng ring sẽ được chặn ở

giữa và lưu lượng sẽ chia đều 2 hướng.

+ RRPP chỉ phát bản tin hello một chiều từ cổng chính đến cổng phụ mà không có chiều ngược lại. Nếu các kết nối là cáp quang 2 sợi thì RRPP chỉ có khả năng phát hiện đứt kết nối trên 1 trong 2 sợi cáp. Trường hợp sợi cáp truyền bản tin hello bị đứt trong khi sợi kia vẫn còn thì nút chủ sẽ cho rằng vòng ring bị đứt hoàn toàn, nó sẽ mở cổng phụ và vòng lặp trên sợi quang còn lại sẽ xảy ra. Tuy nhiên do 2 sợi quang bên ngoài tòa nhà thì chạy rất gần nhau nên khi xảy ra sự cố đứt cáp thì thường cả 2 sợi đều bị đứt. Trường hợp đứt 1 sợi thường xảy ra bên trong tòa nhà, tại các điểm đấu nhảy quang.

+ RRPP không phải là giao thức chuẩn trên các thiết bị mạng mà chỉ là một giao thức của riêng hãng Huawei nên chỉ có thể sử dụng RRPP một cách tốt nhất khi các thiết bị trong vòng ring đều là của hãng Huawei. Trường hợp có một thiết bị trong vòng ring không phải của Huawei thì ta vẫn có thể dùng được RRPP, nhưng các cơ chế thông báo và bản tin flush-db sẽ không hoạt động do thiết bị đó không hỗ trợ RRPP. Lúc này vòng ring chỉ hoạt động chủ yếu dựa vào bản tin hello, thời gian hội tụ sẽ không còn đạt được 50ms nữa.

6. CÁC GIAO THỨC CÓ NGUYÊN LÝ TƯƠNG TỰ RRPP

RRPP không phải là giao thức duy nhất hoạt động theo những nguyên tắc đã trình bày. Trong thời gian ITU chưa kịp chuẩn hóa thì đã có nhiều hãng tự phát triển những giao thức chống vòng lặp dành cho mạng Ethernet dạng vòng ring có nguyên lý hoạt động tương tự. Một trong số các giao thức tương tự đó là:

+ EAPS của Extreme Networks (Ethernet Automatic Protection Switching). Năm 2003, Extreme Networks đã xuất bản RFC3619 mô tả giao thức của họ.

+ ZESR của ZTE (ZTE Ethernet Smart Ring).

+ REP của Cisco (Resilient Ethernet Protocol).

+ ERPS của ITU (Ethernet Ring Protection Switching), được đưa ra trong khuyến nghị G.8032 và vẫn đang tiếp tục phát triển. Năm 2010 giao thức này mới được bổ sung tính năng đa vòng (multi-ring), vốn đã có trong nhiều giao thức của các hãng khác.

7. KẾT LUẬN

RRPP là giao thức có khả năng chống vòng lặp cho mạng Ethernet dạng vòng ring, có thời gian hội tụ ngắn 50ms, đáp ứng được cho các dịch vụ thời gian thực, không bị giới hạn số lượng nút trong vòng ring. Vì vậy, khi triển khai mô hình mạng cấu hình dạng vòng ring, thay vì dùng xSTP thì nên chú ý sử dụng RRPP hoặc các giao thức tương tự như RRPP nếu các thiết bị trong vòng ring có hỗ trợ (nghĩa là cùng một hãng).

Do chuẩn hóa G.8032 của ITU vẫn còn đang trong giai đoạn hoàn thiện nên nó vẫn chưa được tích hợp rộng rãi vào các thiết bị chuyển mạch. Vì vậy, hiện tại người dùng vẫn chưa thể sử dụng chuẩn mới này cho mạng của mình. Tuy nhiên nếu mạng của người dùng sử dụng đồng bộ các thiết bị của Huawei thì có thể trải nghiệm được sự hiệu quả của giao thức RRPP trên mạng dạng vòng ring.

Tài liệu tham khảo

[1]. Cisco Systems Inc., *Cisco Resilient Ethernet Protocol*, 2007.

[2]. Huawei Technologies, *Technical White Paper for Rapid Ring Protection Protocol (RRPP)*, 2007.

[3]. ITU-T, G.8032 - *Ethernet Ring Protection Overview*, 2008.

[4]. IETF, RFC3619 - *Extreme Networks' Ethernet Automatic Protection Switching (EAPS)*, 2003.

[5]. ZTE corp., *ZESR Principle and Configuration*, 2006.

Mọi doanh nghiệp ngày nay đều sử dụng Công Nghệ Thông Tin (CNTT). Tuy nhiên, câu hỏi chưa bao giờ có câu trả lời là: đầu tư cho CNTT trong doanh nghiệp như thế nào là hợp lý? Bài báo sẽ giúp lãnh đạo các doanh nghiệp tìm câu trả lời cho câu hỏi này.

Xây dựng mức chi hợp lý cho CÔNG NGHỆ THÔNG TIN đối với các doanh nghiệp

Nguyễn Trọng

VẤN ĐỀ CHI TIÊU HỢP LÝ CHO CNTT TRONG SẢN XUẤT – KINH DOANH

Một câu hỏi lớn mà các nhà quản trị doanh nghiệp và cả các giới chức lãnh đạo, đặc biệt giới chức lãnh đạo ngành CNTT (các Sở TTTT, Bộ TT&TT,…) rất trăn trở là: Chi tiêu cho CNTT trong các hoạt động kinh tế – xã hội khoảng bao nhiêu thì là hợp lý?

Chúng ta hiểu "hợp lý" không đồng nghĩa với "hiệu quả". Tuy nhiên, có thể thấy "hợp lý" là một yếu tố quan trọng đảm bảo "hiệu quả". Nếu chúng ta chi tiêu cho CNTT không "hợp lý" thì khó mà chờ đợi "hiệu quả" mà CNTT có thể mang lại. "Hợp lý" mang tính khách quan, còn "hiệu quả" thì được quyết định nhiều bởi nhiều yếu tố chủ quan. Có thể xem "hợp lý" là một "điều kiện cần" của "hiệu quả".

Có người cho rằng các doanh nghiệp cần chi cho CNTT cỡ 5% đầu tư ban đầu khi thiết lập doanh nghiệp là hợp lý. Có người cho rằng tỷ lệ đó cần cao hơn và cũng có người cho rằng nên thấp hơn!

Trong quá trình vận hành sản xuất – kinh doanh, người ta cũng không biết phải chi cho CNTT cỡ nào. Thường thì CNTT là những công cụ hỗ trợ, ít khi là công cụ trực tiếp làm ra sản phẩm – dịch vụ của doanh nghiệp (trừ một vài ngành như công nghiệp

phần mềm,...). Vì vậy càng khó nói về những tỷ lệ chi tiêu hợp lý cho CNTT.

Thông thường, lãnh đạo doanh nghiệp (hay nói chung là lãnh đạo các tổ chức) được nghe các cấp tham mưu trình bày rằng đơn vị cần mua máy tính hay mua phần mềm và sẽ quyết định một khoản đầu tư cho CNTT khi cảm thấy được thuyết phục. Tuy nhiên, về tổng thể thì có lẽ đến nay không nhà lãnh đạo doanh nghiệp nào được tham mưu rằng doanh nghiệp cần chi cho CNTT khoảng bao nhiêu để mà có kế hoạch tài chính tổng thể cho khoản đầu tư phải có này khi thành lập doanh nghiệp cũng như trong quá trình quản lý, vận hành hoạt động của doanh nghiệp. Tình trạng đáng buồn là: biết chắc chắn phải chi cho CNTT mà không biết phải chi cỡ bao nhiêu trong tổng chi phí!

Những câu hỏi như: Khi tôi thành lập doanh nghiệp, tôi nên hoạch định bao nhiêu phần trăm vốn đầu tư ban đầu cho CNTT? Trong quá trình sản xuất – kinh doanh thì chi tiêu cho CNTT bằng khoảng bao nhiêu phần trăm doanh số của doanh nghiệp? v.v.. là những câu hỏi mà đến nay vẫn chưa có câu trả lời rõ ràng.

CHI TIÊU CHO CNTT TRONG VẬN HÀNH SẢN XUẤT KINH DOANH NHƯ THẾ NÀO LÀ HỢP LÝ?

Năm 2011, Hãng nghiên cứu thị trường CNTT nổi tiếng quốc tế Gartner đã khảo sát về chi tiêu cho CNTT ở gần 10.000 tổ chức (doanh nghiệp và tổ chức công) trên 22 lĩnh vực kinh tế – xã hội chính ở 80 quốc gia [1]. Hoạt động đánh giá này đã được Gartner thực hiện qua hàng chục năm và cung cấp nhiều dữ kiện quý, giúp chúng ta hiểu về vấn đề chi tiêu CNTT trong những ngành hoạt động quan trọng và có các câu trả lời cơ bản cho những loại câu hỏi

Bảng 1: Danh sách 22 lĩnh vực được Gartner khảo sát.

1	Năng lượng	12	Dịch vụ y tế
2	Xây dựng, vật liệu và tài nguyên thiên nhiên	13	Hoạt động cơ quan chính quyền địa phương
3	Hóa chất	14	Bảo hiểm
4	Thực phẩm & đồ uống	15	Tổ chức và quản lý CSDL
5	Bán buôn & Bán lẻ	16	Viễn thông
6	Công nghiệp chế tạo	17	Giải trí
7	Sản phẩm tiêu dùng	18	Các dịch vụ chuyên nghiệp
8	Điện tử công nghiệp & thiết bị điện	19	Giáo dục
9	Sản phẩm & dịch vụ tiện ích	20	Ngân hàng - tài chính
10	Dược, sản phẩm y tế	21	Phần mềm, dịch vụ Internet & xuất bản
11	Giao thông	22	Hoạt động Chính Phủ TW và quốc tế

Bảng 2

	p= V/DS	q= V/CP
Năng lượng	0.011	0.012
Xây dựng, vật liệu và tài nguyên thiên nhiên	0.011	0.014
Hóa chất	0.013	0.015
Thực phẩm & đồ uống	0.013	0.017
Bán buôn & Bán lẻ	0.014	0.016
Công nghiệp chế tạo	0.018	0.020
Sản phẩm tiêu dùng	0.021	0.024
Điện tử công nghiệp & thiết bị điện	0.027	0.030
Sản phẩm & dịch vụ tiện ích	0.028	0.033
Dược, sản phẩm y tế	0.029	0.036
Giao thông	0.030	0.034
Dịch vụ y tế	0.033	0.035
Hoạt động cơ quan Chính quyền địa phương	0.036	0.036
Bảo hiểm	0.036	0.039
Tổ chức và quản lý CSDL	0.036	0.045
Viễn thông	0.041	0.047
Giải trí	0.043	0.056
Các dịch vụ chuyên nghiệp	0.047	0.051
Giáo dục	0.049	0.052
Ngân hàng - tài chính	0.065	0.084
Phần mềm, dịch vụ Internet & xuất bản	0.076	0.084
Hoạt động Chính Phủ TW và quốc tế	0.089	0.089

như trên cho nhiều ngành công nghiệp. Nghiên cứu của Gartner cũng cho chúng ta thấy cách thức mà các doanh nghiệp có thể tự tìm các câu trả lời chính xác cho riêng mình khi cần.

Nghiên cứu của Gartner cho chúng ta nhiều thông tin giá trị. Ở đây chỉ trích 2 loại chỉ số, giúp chúng ta tìm ra câu trả lời những câu hỏi quan trọng nêu trên. Hai chỉ số đó là: Tỷ lệ % chi cho CNTT trong Doanh Số (Revenue) của doanh nghiệp, ký hiệu là p và Tỷ lệ % chi cho CNTT trong Chi Phí (Operation Cost) của doanh nghiệp, ký hiệu là q.

Ký hiệu: V là chi tiêu cho CNTT hàng năm của doanh nghiệp, DS là doanh số và CP là chi phí của doanh nghiệp. Khảo sát của Gartner cho chúng ta các giá trị p và q trong các công thức: V = p*DS và V = q*CP, với các giá trị p và q cụ thể của từng ngành công nghiệp, được liệt kê trong Bảng 2.

Ký hiệu thu nhập của doanh nghiệp là TN và tỷ lệ chi cho CNTT trong TN của doanh nghiệp là r. Tức là V = r*TN. Ta có thể tính r theo p và q như sau:

Vì TN = DS – CP

nên $V = r*TN = r*\left(\frac{V}{p} - \frac{V}{q}\right)$

$= r * \frac{qV - pV}{pq} = r * \frac{V(q-p)}{pq}$

do đó ta có $r = \frac{pq}{(q-p)}$

Điền các giá trị p và q cho từng ngành công nghiệp vào công thức trên, ta có thêm giá trị r cho các ngành. Bảng 3 là các giá trị p, q và r tương ứng trong 22 lĩnh vực được Gartner khảo sát.

Những chỉ số p, q và r là những chỉ số trung bình cho toàn thể các doanh nghiệp được khảo sát trong từng ngành. Với mỗi quốc gia thì các kết quả có thể khác nhau. Với từng doanh nghiệp cụ thể thì lại có những số liệu riêng. Gartner cho biết p và q trung bình cho toàn thể các doanh nghiệp trong các khu vực, xét trên toàn cầu có những khác biệt. Bảng 4 (tính thêm cho chỉ số r) cho chúng ta hình dung về vấn đề này.

Những số liệu trên có thể giúp lãnh đạo các cấp ở những ngành công nghiệp một định hướng, một giới hạn cho chi tiêu CNTT hàng năm. Lãnh đạo doanh nghiệp hay lãnh đạo cấp cao ở các ngành có thể

Bảng 3

	p= V/DS	q= V/CP	r=V/TN
Năng lượng	0.011	0.012	0.132
Xây dựng, vật liệu và tài nguyên thiên nhiên	0.011	0.014	0.051
Hóa chất	0.013	0.015	0.098
Thực phẩm & đồ uống	0.013	0.017	0.055
Bán buôn & Bán lẻ	0.014	0.016	0.112
Công nghiệp chế tạo	0.018	0.020	0.180
Sản phẩm tiêu dùng	0.021	0.024	0.168
Điện tử công nghiệp & thiết bị điện	0.027	0.030	0.270
Sản phẩm & dịch vụ tiện ích	0.028	0.033	0.185
Dược, sản phẩm y tế	0.029	0.036	0.149
Giao thông	0.030	0.034	0.255
Dịch vụ y tế	0.033	0.035	0.578
Hoạt động cơ quan Chính quyền địa phương	0.036	0.036	X - (không có khái niệm TN)
Bảo hiểm	0.036	0.039	0.468
Tổ chức và quản lý CSDL	0.036	0.045	0.180
Viễn thông	0.041	0.047	0.321
Giải trí	0.043	0.056	0.185
Các dịch vụ chuyên nghiệp	0.047	0.051	0.599
Giáo dục	0.049	0.052	0.849
Ngân hàng - tài chính	0.065	0.084	0.287
Phần mềm, dịch vụ Internet & xuất bản	0.076	0.084	0.798
Hoạt động Chính Phủ TW và quốc tế	0.089	0.089	X - (không có khái niệm TN)

xem đây là những số liệu tham khảo quan trọng khi hoạch định kế hoạch và theo dõi chi tiêu CNTT trong doanh nghiệp hay trong ngành. Chúng ta không nên đi chệch quá xa các giới hạn "hợp lý", mang tính trung bình quốc tế, mà Gartner đã tổng kết.

Chẳng hạn xét một doanh nghiệp trong ngành năng lượng. Ta có p = V/DS = 1,1%, q = V/CP = 1,2% và r = V/TN = 1,32%. Ba chỉ số này cho ta một hình dung khá đầy đủ, giúp nhà quản lý hoạch định các chi phí cho CNTT trong vận hành sản xuất – kinh doanh của các doanh nghiệp trong công nghiệp năng lượng.

Bảng 4

	Bắc Mỹ	Châu Âu	Mỹ Latin	Chấu Á -TBD
P	3,6%	3,2	3,1	2,6
q	4,4	4,1	4	3,6
r	19,8	14,58	13,78	9,36

3. TỶ LỆ ĐẦU TƯ CNTT TRONG TỔNG ĐẦU TƯ THÀNH LẬP DOANH NGHIỆP NHƯ THẾ NÀO LÀ HỢP LÝ?

Phần trên, chúng ta đã xem xét vấn đề chi

tiêu cho CNTT trong vận hành sản xuất – kinh doanh của doanh nghiệp. Tuy nhiên, câu hỏi mà các doanh nghiệp thường muốn có câu trả lời hơn cả có lẽ là: *doanh nghiệp cần đầu tư bao nhiêu cho CNTT trong đầu tư ban đầu khi thành lập doanh nghiệp, để đầu tư đó là hợp lý, không lãng phí và cũng không quá ít?*

Xét ví dụ một trường tư thục cao đẳng dạy nghề X. Khi thành lập trường, các nhà đầu tư dự kiến sẽ đầu tư 100 tỷ đồng để chuẩn bị những điều kiện quan trọng nhất cho hoạt động dạy và học. Với 100 tỷ đồng đó thì cần giành bao nhiêu cho CNTT là hợp lý?

Giả sử rằng, để xây dựng trường, các nhà đầu tư góp 40% vốn và vay ngân hàng 60% trong 20 năm, với lãi suất 8%. Các nhà đầu tư chấp nhận hưởng lãi vốn góp là 15%/năm. Ta có thể tính ra tỷ suất hoàn vốn vay (với cách trả 1/20 vốn vay mỗi năm và trả lãi hàng năm cho số vốn vay còn lại) theo công thức:

$$R^d = R_d \frac{(n+1)}{2n} + \frac{1}{n}$$

trong đó R^d là tỷ suất hoàn vốn vay, R_d là lãi suất vốn vay và n là số năm sử dụng vốn vay. Thay các giá trị cụ thể trong dự án nhà trường vào công thức trên ta có:

$$R^d = 0{,}08\frac{(20+1)}{2*20} + \frac{1}{20} = 0{,}092$$

Đại lượng ký hiệu là *t*, được tính theo công thức dưới đây có thể xem là tỷ suất vốn hoá [2] cho dự án nhà trường nêu trên.

$t = \quad 0{,}6*0{,}092 + 0{,}4*0{,}15 \ = 0{,}1152$

Với vốn đầu tư 100 tỷ đồng và tỷ suất vốn hoá 11,52% thì dự án có thể có thu nhập hàng năm khoảng 11,5 tỷ đồng. Dự án này cần đầu tư cho CNTT cỡ: 11,52*0,849 = 9,78 tỷ đồng (0,849 là giá trị r tính cho ngành giáo dục), tức khoảng 9,8% trong 100 tỷ đồng tổng vốn đầu tư xây dựng nhà trường.

Một cách tổng quát, giả sử khi thiết lập doanh nghiệp, ta tính được Tỷ suất vốn hoá cho dự án thành lập doanh nghiệp này là t. Điều đó có nghĩa là t*Cap ≈ TN với Cap là tổng đầu tư ban đầu cho dự án. Ký hiệu s là tỷ lệ đầu tư cho CNTT trong đầu tư ban đầu, khi thiết lập doanh nghiệp. Ta có:

$s = V/Cap = V/(TN/t) = r*t.$

Trong nhiều trường hợp, để có một hình dung hợp lý, ta có thể lấy t bằng lãi suất trung bình mà các ngân hàng cho vay vốn đầu tư. Chẳng hạn, vào cuối năm 2012, ở nước ta tỷ suất lãi vay ngân hàng khoảng 10%–15% vốn vay, tuỳ theo lĩnh vực hoạt động của doanh nghiệp. Như vậy, tỷ suất vốn hoá có thể tạm xem là giao động từ 10% đến 15%. Khi cần, ta có thể tính cụ thể tỷ suất vốn hoá cho dự án đầu tư như thí dụ về nhà trường nêu trên. Với giả thiết tỷ suất vốn hoá trong khoảng 10% đến 15% ta có bảng số liệu cho giá trị s đối với một số lĩnh vực (Bảng 5).

Tóm lại với một nhà trường (nói chung chứ không phải nhà trường cụ thể nêu trên) thì ta có các số liệu tham khảo sau đây:

– Đầu tư cho CNTT chiếm khoảng 8,5% – 12,7% tổng vốn đầu tư ban đầu. Tham khảo con số chung này thì với trường nêu trên, đầu tư ban đầu cho CNTT là khoảng 8,5 tỷ – 12,7 tỷ trong tổng đầu tư 100 tỷ đồng. Tuy nhiên với dự án nhà trường cụ thể này, ta đã tính cụ thể Tỷ suất vốn hoá nên mức đầu tư cho CNTT sẽ khoảng 9,78 tỷ đồng.

– Chi cho CNTT hàng năm bằng khoảng 4,9% doanh số.

Bảng 5

	s ứng với TSVH 10%	s ứng với TSVH 15%
Năng lượng	0.0132	0.0198
Xây dựng, vật liệu và tài nguyên thiên nhiên	0.0051	0.00765
Hóa chất	0.0098	0.0147
Thực phẩm & đồ uống	0.0055	0.00825
Bán buôn & Bán lẻ	0.0112	0.0168
Công nghiệp chế tạo	0.018	0.027
Sản phẩm tiêu dùng	0.0168	0.0252
Điện tử công nghiệp & thiết bị điện	0.027	0.0405
Sản phẩm & dịch vụ tiện ích	0.0185	0.02775
Dược, sản phẩm y tế	0.0149	0.02235
Giao thông	0.0255	0.03825
Dịch vụ y tế	0.0578	0.0867
Hoạt động cơ quan Chính quyền địa phương	0	0
Bảo hiểm	0.0468	0.0702
Tổ chức và quản lý CSDL	0.018	0.027
Viễn thông	0.0321	0.04815
Giải trí	0.0185	0.02775
Các dịch vụ chuyên nghiệp	0.0599	0.08985
Giáo dục	0.0849	0.12735
Ngân hàng - tài chính	0.0287	0.04305
Phần mềm, dịch vụ Internet & xuất bản	0.0798	0.1197
Hoạt động Chính Phủ TW và quốc tế	0	0

– Chi cho CNTT hàng năm chiếm khoảng 5,2 tổng chi phí vận hành.

– Chi cho CNTT hàng năm bằng khoảng 85% lợi nhuận. Với thí dụ trường nêu trên, ta đã có ước tính thu nhập hàng năm khoảng 11,5 tỷ. Như vậy, hàng năm nhà trường sẽ phải chi cho CNTT khoảng 9,77 tỷ đồng phục vụ các hoạt động đào tạo và quản lý nhà trường.

Hiển nhiên, các chỉ số là có tính chất định hướng cho những ngành hoạt động kinh tế – xã hội rất rộng lớn. Với mỗi doanh nghiệp, khi xây dựng ban đầu và quá trình vận hành sản xuất – kinh doanh thì ta sẽ có các số liệu riêng nếu thấy cần tính toán. Dù sao không nên để các chỉ số p, q, r, s lệch quá xa những chỉ số trung bình quốc tế. Trên quan điểm vừa trình bày trong bài báo thì việc chi tiêu cho CNTT trong vận hành sản xuất – kinh doanh và đầu tư cho CNTT khi thành lập doanh nghiệp không còn hoàn toàn là quyết định chủ quan do nhận thức của lãnh đạo mà có những yếu tố khách quan, mang tính phổ biến trên toàn cầu. Sự kết hợp giữa tính khách quan và nhận thức, tri thức của lãnh đạo doanh nghiệp sẽ biến tính "hợp lý" trong chi tiêu CNTT thành "hiệu quả" của CNTT trong hoạt động của doanh nghiệp/.

Tài liệu tham khảo

[1]. Gartner, *IT Metrics: IT Spending and Staffing Report*, 2012.

[2]. *Hệ thống tiêu chuẩn thẩm định giá Việt Nam*, Tiêu chuẩn số 09, Phương pháp thu nhập (Ban hành kèm theo Quyết định số 129/2008/QĐ-BTC ngày 31 tháng 12 năm 2008 của Bộ trưởng Bộ Tài chính) và các tiêu chuẩn khác.

[3]. NGUYỄN TRỌNG, *Một khung nhìn CNTT quốc tế trong tổng thể nền kinh tế thế giới* (A Comprehensive View on the Worldwide Information Technology Industry in the Panorama of the World Economy), Báo cáo tại Hội thảo "Toàn cảnh CNTT VN", TP HCM, 9/ 2012.

Cơ hội để phát triển CÔNG NGHIỆP NỘI DUNG SỐ

Trong khuôn khổ hợp tác về CNTT giữa Việt Nam và Hàn Quốc, nhằm tăng cường sự hiểu biết về hiện trạng và đầu tư trong ngành Công nghiệp Nội dung số (CN NDS) của các cơ quan và doanh nghiệp (DN) hai nước Việt Nam – Hàn Quốc, mới đây, Hội thảo Việt Nam – Hàn Quốc về CN NDS đã được Bộ Hành chính và An ninh công cộng Hàn Quốc phối hợp với Bộ TT&TT tổ chức.

NHIỀU TIỀM NĂNG ĐỂ PHÁT TRIỂN CN NDS

Thứ trưởng Bộ TT&TT Nguyễn Minh Hồng cho biết, trong lĩnh vực Công nghiệp CNTT, CN NDS là một trong những ngành tuy còn non trẻ nhưng có rất nhiều tiềm năng để phát triển và có ảnh hưởng sâu sắc đến nhiều mặt của đời sống kinh tế – xã hội của Việt Nam và đóng góp đáng kể vào sự tăng trưởng của nền kinh tế.

Theo Sách Trắng CNTT-TT Việt Nam của Ban Chỉ đạo quốc gia CNTT và Bộ TT&TT phát hành, tuy chỉ chiếm khoảng 10% tổng doanh thu công nghiệp CNTT, nhưng xét về tốc độ phát triển CN NDS là ngành có tăng trưởng rất ấn tượng khoảng 20 – 40%/ năm trong 10 năm qua. Riêng năm 2011, toàn ngành đã có quy mô doanh thu trên 1 tỷ USD, thu hút 500 – 600 DN với hơn 60.000 lao động. Theo Vụ CNTT, Bộ TT&TT hiện chưa có con số chính xác về doanh thu NDS năm 2012 nhưng dựa trên con số năm 2011 đạt khoảng 1,1 tỷ USD, dự kiến năm 2012 vẫn tiếp tục tăng trưởng, đạt 1,3 – 1,5 tỷ USD.

NHÂN LỰC LÀM NDS VỪA YẾU, VỪA THIẾU

Cùng với sự ảnh hưởng của suy thoái, khủng hoảng kinh tế, từ năm 2010 đến nay, ngành CN NDS đang trên đà giảm doanh thu.

Theo ông Lê Hồng Minh, Tổng giám đốc VNG cho biết các DN NDS đang gặp nhiều khó khăn. Đối với ngành này, việc tạo ra nội dung là yếu tố hàng đầu khi gây dựng lợi thế cạnh tranh. Thế nhưng, các DN NDS Việt Nam lại đang "gặp khó" về khả năng sáng tạo. Dẫn chứng bằng thực tế của VNG khi phát hành một game online cho thị trường Nhật Bản. Để làm dự án đó, VNG chuẩn bị 20 người làm sản phẩm trong 8 tháng, trong đó 10 người chuyên vẽ, nhưng kết quả chuyển sang đối tác Nhật Bản thì 50% số hình ảnh bị loại bỏ. Để kịp tiến độ dự án, VNG phải lên các diễn đàn tìm kiếm người có khả năng vẽ giỏi và đặt

hàng. Tuy nhiên, sau một tháng thì tỷ lệ từ chối của Nhật đối với những sản phẩm mà VNG cộng tác bên ngoài này lên tới 95%, thậm chí đối tác Nhật Bản còn chỉ rõ hình ảnh bộ phận của nhân vật này được sao chép (copy) từ nguồn nào chứ không phải là sản phẩm sáng tạo. Cuối cùng, VNG đành phải sang Nhật nhờ một công ty chuyên nghiệp về vẽ hình thực hiện.

Khó thứ hai của ngành CN NDS là thiếu nhân lực. Ông Lê Hồng Minh lấy ví dụ ngành game Việt Nam, sau 5 năm, ước tính cả nước mới có khoảng 1.000 người làm được game online (hầu hết là những người đam mê vì không có trường nào đào tạo nghề này). Trong khi đó, lực lượng làm game của Hàn Quốc có tới 100.000 người, Trung Quốc là 300.000 người. Bởi vậy, không có gì khó hiểu khi chất lượng game của DN Việt Nam thường bị "lép vế" so với đối thủ ngoại.

Cũng chính vì thiếu "người tài" nên VNG từng nếm mùi thất bại khi đưa game Thuận Thiên Kiếm ra thị trường. Dù đã đầu tư 4 năm cho một game được xác định là hoành tráng, thậm chí mời cả hoa hậu Mai Phương Thúy làm hình ảnh đại diện và xúc tiến nhiều hoạt động truyền thông, thế nhưng sau khi phát hành, Thuận Thiên Kiếm vẫn không được nhiều người chơi. Tìm hiểu nguyên nhân thì thấy chất lượng game còn thua kém các sản phẩm của Hàn Quốc, Trung Quốc, đương nhiên người tiêu dùng thường chọn game tốt hơn để chơi.

CẦN NHỮNG THÁO GỠ CHÍNH SÁCH

Sự phát triển của CN NDS Việt Nam được chia làm 3 giai đoạn: từ 2000 – 2005, 2006 – 2010 và từ 2011 đến nay. Cùng với sự phát triển của ngành công nghiệp này, một loạt chính sách thúc đẩy đã ra đời. Điển hình trong các chính sách này là Luật CNTT đã định nghĩa và Nghị định 71/2007/NĐ-CP Hướng dẫn Luật CNTT về công nghiệp CNTT đã nêu rõ sự phát triển của ngành này.

Nghị định 108/2006/NĐ-CP của Chính phủ quy định chi tiết và hướng dẫn thi hành một số điều của Luật Đầu tư, đã đưa "sản xuất sản phẩm phần mềm, nội dung thông tin số" vào Danh mục lĩnh vực được đặc biệt ưu đãi đầu tư".

Giai đoạn phát triển 2006 – 2010 cũng đánh dấu việc Thủ tướng Chính phủ ban hành Quyết định 56/2007/QĐ-TTg phê duyệt Chương trình phát triển CN NDS Việt Nam đến năm 2010. Năm 2009, Thủ tướng Chính phủ ban hành Quyết định số 50/QĐ-TTg để chi tiết hóa và giao nhiệm vụ nội dung phát triển CN NDS Việt Nam.

Nhà nước cũng đã hỗ trợ đầu tư phát triển CN NDS qua dự án hỗ trợ DN phần mềm và NDS xây dựng, áp dụng quy trình sản xuất theo chuẩn CMMi và tiêu chuẩn ISO; hỗ trợ đào tạo ngắn hạn cho nhân lực NDS đang làm việc tại các DN và các Quỹ tiêu biểu có đầu tư vào lĩnh vực CN NDS như IDG Ventures Vietnam (Mỹ), Quỹ VIG…

"Tuy nhiên, cuối giai đoạn phát triển 2006 – 2010, một số nhà cung cấp nội dung đã cung cấp nhiều tin nhắn rác, nhắn tin coi bói, nhắn tin không đúng với thuần phong mỹ tục Việt Nam. Loại hình kinh

doanh này không nhiều nhưng tác động tới chính sách, tác động tới xã hội… đã làm quan ngại sự phát triển của lĩnh vực này", Vụ trưởng Vụ CNTT, Bộ TT&TT Nguyễn Trọng Đường cho biết.

Các DN NDS luôn mong chờ sự hỗ trợ từ Nhà nước, chí ít cũng là một hành lang pháp lý hiệu quả. Song theo đánh giá của ông Lê Hồng Minh, các chính sách quản lý, hỗ trợ phát triển CN NDS vẫn chưa rõ ràng, tốc độ ban hành chính sách quá chậm, trong khi chỉ cần 1 năm, mạng xã hội Facebook đã nâng số người sử dụng tại Việt Nam từ con số 3 triệu lên tới 12 triệu, hoặc chỉ cần 6 tháng, một game phát hành có thể sở hữu số người chơi đông nhất tại Việt Nam.

"Vậy, vấn đề đặt ra là những dịch vụ nào cần khuyến khích, ưu đãi, dịch vụ nào cần phải quản lý, thậm chí một số loại dịch vụ phải cấp phép, hoặc có hình thức quản lý chặt chẽ. Về quan điểm quản lý cũng cần làm rõ, cần "quản" NDS như quản báo chí hay coi như là một ngành công nghiệp và việc quản lý nội dung tuân thủ theo các quy định hiện hành như nhà nước đã có, tuy nhiên, nên phát triển theo hướng như là một ngành công nghiệp", ông Nguyễn Trọng Đường cho biết.

Về văn bản quản lý Nhà nước, ông Nguyễn Trọng Đường cũng thừa nhận các văn bản chính sách quy định về ưu đãi phát triển CN NDS còn chung chung, không thực sự phát huy tác dụng. Nhiều hoạt động CN NDS chưa có chính sách điều chỉnh phù hợp như vấn đề hợp tác kinh doanh giữa nhà cung cấp dịch vụ viễn thông và nhà cung cấp dịch vụ nội dung (tỷ lệ ăn chia doanh thu), các vấn đề liên quan đến quản lý game online, vấn đề thanh toán dịch vụ NDS xuyên biên giới…

Dù một loạt chính sách ưu đãi của Chính phủ đã được ban hành nhưng các DN NDS khó được hưởng những ưu đãi đó. Vấn đề là sản xuất NDS chưa có định nghĩa cụ thể. Tại Việt Nam, rất ít DN NDS chỉ sản xuất sản phẩm và bán sản phẩm như các DN lớn ở nước ngoài, mà phần lớn DN có sản xuất ra sản phẩm cũng chỉ để bán dịch vụ. Khó phân biệt tách bạch hai loại hình sản xuất và kinh doanh dịch vụ nên nhiều DN NDS đã không được ngành thuế duyệt cho hưởng ưu đãi.

Ông Ys Lee, đại diện cơ quan thông tin Quốc gia Hàn Quốc (NIA), Cố vấn Trung tâm Hợp tác CNTT Việt Nam– Hàn Quốc cho biết, cần xây dựng một chính sách NDS phổ quát hơn. Năm 2012, Hàn Quốc đã đưa ra Luật về phát triển CN NDS, nay đổi tên thành Luật Phát triển công nghiệp nội dung. Và đặc biệt về chính sách phát triển ngành NDS là phát triển các khả năng sản sinh nội dung của người dân (user content) và lập được cơ sở hạ tầng để các thành phần tư nhân thông qua những nội dung được nhà nước công bố công khai để sáng tạo nhiều hơn nữa giá trị gia tăng trong đời sống.

"Những chính sách này không nên tiến hành riêng rẽ mà tiến hành một cách hệ thống và trong khuôn khổ tương tác với chính sách về NDS", ông Ys Lee nhấn mạnh.

Ông Choi Youn Chel – Đại diện cơ quan nội dung sáng tạo Hàn Quốc với kinh nghiệm của mình đã đưa ra hai đề xuất.

Thứ nhất, đừng nên lưỡng lự phát triển DN vừa và nhỏ đặc biệt trong lĩnh vực NDS mà hãy tạo nhiều cơ hội cho DN tiếp tục phát triển trong lĩnh vực này.

Thứ hai, khả năng thị trường NDS mặc dù rất lớn nhưng tính rủi ro cao. Giai đoạn đầu cần hỗ trợ để đối phó với những rủi ro của thị trường này.

Được biết, Hàn Quốc là nước có nền CN NDS phát triển hàng đầu thế giới. Quy mô thị trường công nghiệp nội dung Hàn Quốc năm 2012 đạt 8,8 tỷ USD, trong đó riêng nội dung số chiếm 2,8 tỷ USD. Tuy nhiên, tốc độ tăng trưởng của NDS đạt 18,9%, gấp 3 lần tốc độ tăng trưởng của thị trường nội dung.

NLP

ĐẢM BẢO KINH DOANH LIÊN TỤC NHỜ TRUNG TÂM DỰ PHÒNG

Hiện nay, các ngân hàng và các tổ chức tài chính tại Việt Nam đã tăng cường đầu tư hệ thống công nghệ thông tin (CNTT) nhằm tăng sức mạnh của DN và bắt kịp xu thế phát triển của thế giới. Những tiến bộ mới nhất trong lĩnh vực bảo mật và an toàn thông tin (ATTT) đã được các đơn vị này áp dụng. Tuy nhiên, để đảm bảo an toàn tuyệt đối cho hệ thống, các ngân hàng cần phải thiết lập một hệ thống dự phòng đủ mạnh.

NHU CẦU LƯU TRỮ DỰ PHÒNG THÔNG TIN NGÀY CÀNG QUAN TRỌNG

Sau yếu tố con người thì thông tin, dữ liệu là tài sản đặc biệt quý giá của mọi tổ chức, doanh nghiệp (DN). Ngày nay, tất cả các DN hoạt động trên mọi lĩnh vực đang đối mặt với sự tăng trưởng không ngừng của dữ liệu và từ đó dẫn đến việc đối mặt với các công tác quản lý, bảo vệ và duy trì sự tồn tại của dữ liệu trong một khoảng thời gian nhất định. Dữ liệu ở đây có thể là những thông tin liên quan đến tài chính, lịch sử giao dịch, thông tin liên quan đến thẻ tín dụng của khách hàng… và nếu như dữ liệu này bị mất sẽ ảnh hưởng đến uy tín và khả năng cạnh tranh của doanh nghiệp. Do đó, chính sách liên quan đến việc lưu trữ dữ liệu rất quan trọng.

Lưu trữ có các mục đích khác nhau, có thể lưu trữ để đề phòng trong trường hợp dữ liệu mất sẽ khôi phục lại nhanh chóng. Trong trường hợp này việc

lưu trữ thường gắn liền với các kế hoạch phục hồi thảm họa của các DN. Ngoài việc lưu trữ trên, còn có việc lưu trữ liên quan đến vấn đề cất giữ thông tin trong một khoảng thời gian dài, việc lưu trữ này không nhất thiết phải lưu trữ tức thời và thông tin lưu trữ có thể sẽ được sử dụng tại một thời điểm nào đó trong tương lai. Trong cả hai trường hợp thì thông tin phải được lưu trữ tại một nơi nào đó nằm khác so với nơi chứa dữ liệu chính.

Mức độ thường xuyên của việc lưu trữ dữ liệu phụ thuộc vào mức độ quan trọng của dữ liệu cũng như khả năng tài chính của doanh nghiệp. Ví dụ, đối với các thông tin liên quan đến việc giao dịch của khách hàng được thay đổi liên tục thì việc lưu trữ phải được thực hiện tức thời, điều đó có thể cho phép việc khôi phục lại dữ liệu được tức thời ngay sau thời điểm mất dữ liệu chính.

Mất dữ liệu và gián đoạn giao dịch chính là làm mất thời gian, tiền bạc và uy tín của doanh nghiệp. Có được một trung tâm dữ liệu phục vụ cho việc dự phòng cùng với kế hoạch phục hồi thảm họa cũng là một trong những yếu tố làm nên điểm khác biệt giữa thành công và thất bại của một doanh nghiệp.

RỦI RO KHÓ LƯỜNG

ThS. Đặng Mạnh Phổ – Phó Tổng Giám đốc, Cố vấn cao cấp của Chủ tịch HĐQT về CNTT, ngân hàng BIDV – cho rằng: Hệ thống CNTT nói chung bao gồm nhiều cấu phần tinh vi, phức tạp, hàm chứa rất nhiều khả năng hư hỏng và theo định luật Murphy thì tất yếu "nó sẽ hỏng", vấn đề là nó sẽ hỏng vào lúc nào thôi.

Thảm họa CNTT có thể xảy ra bất kỳ lúc nào với nhiều nguyên nhân khó lường trước, có thể do thiên nhiên (động đất, lũ lụt…) hoặc con người.

Thông tin là giá trị cốt lõi của các tổ chức cần phải lưu trữ, quản trị, sử dụng... Nó cũng là tiêu điểm tấn công của tội phạm mạng. Theo thống kê của Symantec, 90% các vi phạm liên quan đến tội phạm có tổ chức nhắm mục tiêu thông tin của các công ty và các tổ chức tài chính. 97% các vi phạm này ảnh hưởng đến 140 triệu hồ sơ, trong đó, 48% các vi phạm liên quan trong nội bộ DN. Giá trị của thông tin số bị đánh cắp trong năm 2009 khoảng 1 tỷ USD. 38% các ngân hàng gặp bất lợi sau khi bị xâm phạm dữ liệu.

Sự gia tăng tội phạm mạng và hiện tượng biến đổi khí hậu toàn cầu tác động khiến việc mất ATTT trở thành nỗi lo thường trực với các tổ chức, ngân hàng.

Trong khi đó, các DN hiện nay, mặc dù gia tăng các biện pháp an ninh hệ thống nhưng không mấy

quan tâm đến các công việc liên quan đến việc lưu trữ dữ liệu trong chiến lược an ninh hệ thống của họ. Nguyên nhân chính của vấn đề này có lẽ là quan niệm về lưu trữ và an ninh hệ thống là hai vấn đề khác nhau, trong khi an ninh hệ thống được hiểu là phải kiểm soát được việc truy cập của người dùng đối với dữ liệu thì việc lưu trữ dữ liệu lại được hiểu là không liên quan đến an ninh hệ thống và đơn giản chỉ là cất dữ liệu ra một nơi khác.

Việc lưu trữ dữ liệu là sao chép những dữ liệu quý giá của doanh nghiệp nên cần phải được quan tâm và chú trọng đặc biệt là công tác an ninh, an toàn dữ liệu. Sử dụng những biện pháp lưu trữ dữ liệu cần thiết thông qua các chính sách phù hợp là việc làm không thể thiếu đối với các DN. Điều này đòi hỏi DN phải lựa chọn phương án sao cho phù hợp với loại dữ liệu mà doanh nghiệp cần lưu trữ. Một điều quan trọng nhất cần lưu ý đó là việc lưu trữ thông tin không thể làm một lần, không thể đầu tư một lần, đây là công việc cần phải làm thường xuyên, cần phải được giám sát và cải tiến thường xuyên. Các DN không được coi việc lưu trữ dữ liệu là một việc đơn giản mà trái lại đây là một việc phức tạp và là một phần trong việc xây dựng an ninh hệ thống của doanh nghiệp.

Một chính sách về lưu trữ sẽ cung cấp các nguyên tắc và phương án để thực hiện việc lưu trữ và quản lý dữ liệu được an toàn. Đặc biệt các chính sách liên quan đến vấn đề này phải được kết hợp chặt chẽ và là một yếu tố không thể thiếu được, đó là trung tâm dự phòng thông tin và kế hoạch phục hồi thảm họa của các DN (DRP – disaster recovery plan).

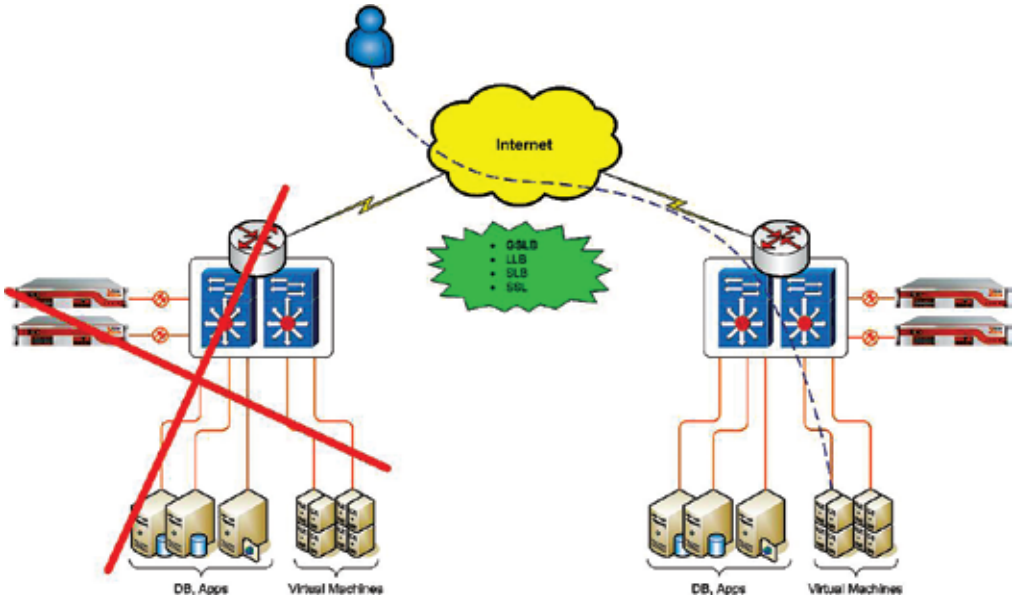
AN TOÀN HƠN VỚI HỆ THỐNG DỰ PHÒNG

Thực tế cho thấy, mọi giải pháp đều tạo ra những khó khăn mới. Do vậy, bất luận DN có bao nhiêu tài nguyên thì cũng không bao giờ là đủ. Có một kế hoạch dự phòng thảm họa CNTT sẽ giúp cho ngân hàng có thể đối phó với những tình huống thảm hoạ khi chúng xảy ra.

Hệ thống dự phòng trở thành vấn đề sống còn đối với hoạt động của các ngân hàng và tổ chức tài chính... Một kế hoạch dự phòng tốt giúp giảm xuống mức tối thiểu những tác động của thảm họa tới hoạt động kinh doanh của doanh nghiệp. Ông Đặng Mạnh Phổ cho biết, hàng năm BIDV dành từ 5% đến 6% tổng chi phí cho hệ thống CNTT và một phần không nhỏ trong đó là chi cho hệ thống dự phòng. Trung tâm dự phòng phục hồi thảm họa không chỉ đơn giản là trung tâm dự phòng thông tin mà sẽ thực sự là trung tâm dự phòng cho các vấn đề liên quan đến hoạt động kinh doanh của DN.

Các ngân hàng tại Việt Nam đã thiết lập và đang hoàn thiện hệ thống dự phòng của mình theo tiêu chuẩn tiên tiến của thế giới bao gồm: Được đặt cách biệt với hệ thống chính và đảm bảo mức an toàn cao nhất; Cơ sở vật chất kỹ thuật độc lập, tách biệt với hệ thống chính; Thường xuyên sao lưu và cập nhật được thông tin dữ liệu hoạt động của hệ thống chính, đáp ứng yêu cầu mục tiêu điểm khôi phục (RPO); Luôn sẵn sàng hoạt động trên phương diện như là hệ thống chính thứ hai.

Hiện nay, các hệ thống CNTT của BIDV (cả hệ thống chính và dự phòng) đã được bảo vệ khá toàn diện. Hệ thống xử lý (bao gồm các server, thiết bị mã hóa – giải mã, các bộ chuyển mạch, các hệ tích hợp v.v...) được đặt trong hệ thống mạng với nhiều cấp độ bảo vệ khác nhau, được kiểm soát với các thiết bị an ninh mạng chuyên dụng như tường lửa (Firewall), Proxy, thiết bị phát hiện và ngăn chặn tấn công (IPS), mạng riêng ảo (VPN, chủ yếu để kiểm



Phuong thức hoạt động của hệ thống chính và hệ thống dự phòng.

soát các truy cập từ xa)… Phần mềm hệ thống (hệ điều hành, cơ sở dữ liệu, phần mềm trung gian...) và các phần mềm ứng dụng được cấu hình đảm bảo an ninh, kiểm tra định kỳ, cập nhật các bản vá mới nhất, được bảo vệ bằng các chương trình phòng chống virus, mã độc...

Thiết bị phần cứng cũng được các ngân hàng trang bị với công nghệ tiên tiến. Ông Phạm Anh Tuấn, Phó Tổng Giám đốc VietinBank cho biết, trong năm 2010, VietinBank đã đầu tư hệ thống máy chủ mainframe IBM system z10 Business Class với chi phí cả triệu đô la Mỹ để hỗ trợ việc mở rộng các hoạt động ngân hàng và để vận hành giải pháp quản lý rủi ro tác nghiệp. Ông Tuấn khẳng định: "Khoản đầu tư cho hệ thống dự phòng được coi là nền tảng chiến lược cho các công việc mang tính sứ mệnh quan trọng. Và tại một nước đang tăng trưởng với tốc độ cao như Việt Nam, không có sứ mệnh nào quan trọng hơn là đảm bảo an toàn cho tiền gửi và các giao dịch chuyển tiền".

Trung tâm dự phòng thông tin sẽ cho phép DN bảo vệ được thông tin và khi cần thiết sẽ trở thành trung tâm dữ liệu chính phục vụ cho hoạt động kinh doanh của DN. Nếu DN chỉ xây dựng cho mình một trung tâm dự phòng thì điều đó vẫn chưa đủ nếu như DN không xây dựng được cho mình một kế hoạch phục hồi thảm họa (DRP – Disaster Recover Plan). Một kế hoạch phục hồi thảm họa phải bao gồm các bước: thiết lập kế hoạch; kiểm tra kế hoạch và thực hiện theo kế hoạch đó. Kế hoạch phục hồi thảm họa cũng phải phù hợp với các tiêu chuẩn ISO họ 27000 (ISO 27001 và ISO 27002).

Với hệ thống dự phòng đủ mạnh, các ngân hàng sẽ đảm bảo được tính liên tục trong kinh doanh có nghĩa là công việc kinh doanh không gián đoạn khi có sự cố xảy ra hoặc thời gian gián đoạn phải ở mức tối thiểu.

Một DN khi đưa ra kế hoạch đảm bảo tính liên tục trong kinh doanh (BCP – Business Continuity Plan) sẽ giúp DN có thể quản lý được các rủi ro, tạo điều kiện cho việc đảm bảo các hoạt động trong DN cũng như việc phân phối các dịch vụ đến khách hàng. Từ đó, giúp cho doanh nghiệp đứng vững trước các vấn đề khó khăn và tạo dựng được hình ảnh tốt trong lòng khách hàng.

Minh Thiện

AN TOÀN THÔNG TIN – Yếu tố sống còn của Internet Banking

Người dùng có thể ngồi tại nhà, cơ quan, hoặc một quán cafe nào đó để thực hiện các giao dịch ngân hàng. Thậm chí, với các phương tiện kết nối Internet di động, người dùng còn có thể vừa di chuyển (trên xe hoặc tàu...) vừa sử dụng dịch vụ Internet Banking. Hình thức dịch vụ này thật tiện lợi. Tuy nhiên, dịch vụ này có "sống" được hay không lại phụ thuộc vào mức độ an toàn thông tin của hệ thống ngân hàng.

TIỆN LỢI CHO CẢ NGƯỜI DÙNG VÀ NGÂN HÀNG

Internet Banking (dịch vụ ngân hàng qua Internet) được dùng để chỉ việc cung cấp các dịch vụ ngân hàng và thực hiện các giao dịch ngân hàng trên Internet (thông qua website của ngân hàng). Đây là phương thức ứng dụng công nghệ thông tin và truyền thông cho phép các khách hàng có tài khoản tại ngân hàng có thể sử dụng các dịch vụ ngân hàng hiện đại và thực hiện các giao dịch ngân hàng trực tuyến thông qua Internet.

Internet Banking cung cấp các dịch vụ phong phú, tiện lợi như: Vấn tin; Thông tin ngân hàng, tài chính (tỷ giá, lãi suất, giá vàng…); Chuyển khoản; Chuyển tiền; Thanh toán hoá đơn; Thanh toán thẻ tín dụng; Đặt chỗ, mua vé máy bay; Nạp tài khoản di động trả trước… Internet Banking thực sự tiện lợi cho người dùng. Người dân và doanh nghiệp có thể sử dụng các dịch vụ ngân hàng phong phú và thực hiện giao dịch tại bất cứ đâu một cách nhanh chóng, tiết kiệm thông qua mạng Internet và thiết bị truy cập như máy tính hoặc thiết bị di động.

Qua Internet Banking, khách hàng có thể gửi đến ngân hàng những thắc mắc, góp ý với ngân hàng và được trả lời sau một thời gian nhất định. Đây thực sự là kênh phân phối hiện đại, hiệu quả và nhiều tiềm năng xét trên nhiều khía cạnh. Chi phí cung cấp sản

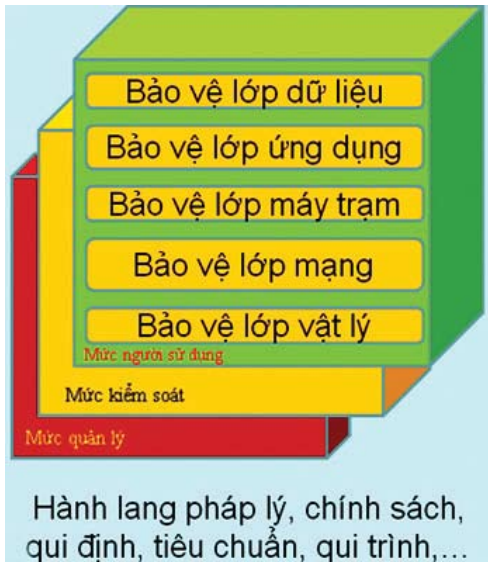
phẩm dịch vụ thấp hơn nhiều so với các quầy giao dịch truyền thống; Không bị giới hạn về địa lý; Dễ dàng triển khai và quảng bá các sản phẩm dịch vụ mới. Phương thức hoạt động này vô cùng tiện lợi vì nó cho phép ngân hàng có thể phục vụ khách hàng bất cứ thời điểm nào (kể cả ngoài giờ hành chính) và tại bất cứ nơi nào có kết nối Internet. Internet Banking cũng là kênh phân phối mang ngân hàng đến tận nhà, văn phòng, trường học, đến bất kỳ nơi đâu và bất cứ lúc nào.

GIẢI PHÁP AN TOÀN THÔNG TIN ĐỒNG BỘ

Mặc dù tiện lợi cho cả ngân hàng và người dùng, nhưng Internet Banking có "sống" được hay không là nhờ an toàn thông tin (ATTT). Nếu hệ thống Internet Banking của ngân hàng không đáp ứng được các yêu cầu về tính an toàn và an ninh bảo mật thì rủi ro của hệ thống giao dịch này là không nhỏ. ThS. Đặng Mạnh Phổ, Giám đốc Ban Công nghệ của Ngân hàng Đầu tư và Phát triển (BIDV), nhận xét: *"Bảo đảm an toàn thông tin cho Internet Banking là một quá trình liên tục không ngừng với sự kết hợp nhiều giải pháp về công nghệ cùng với tổ chức quản lý và các quy trình nghiệp vụ chặt chẽ".*

Yêu cầu ATTT đối với giao dịch Internet Banking gồm nhiều yếu tố như: Xác thực người dùng; Bảo mật thông tin giao dịch; Đảm bảo toàn vẹn dữ liệu; Chống chối bỏ… Ông Phan Thái Dũng, Cục Công nghệ tin học – Ngân hàng Nhà nước Việt Nam, cho biết: Thông tư 29/2011/TT-NHNN quy định rất cụ thể và chặt chẽ việc đảm bảo ATTT cho Internet Banking. Thông tư quy định các ngân hàng phải đảm bảo bí mật thông tin liên quan đến tài khoản, tiền gửi, tài sản gửi và các giao dịch của khách hàng; Đảm bảo tính sẵn sàng thông qua cam kết khả năng hoạt động liên tục của hệ thống Internet Banking. Mặt khác, các ngân hàng phải tuân thủ quy định về an toàn cơ sở dữ liệu, mã hóa dữ liệu, quản lý nhật ký, quản lý sự cố và hướng dẫn khách hàng trong việc sử dụng dịch vụ ngân hàng trên Internet.

Để chống nguy cơ mất an toàn xảy ra từ bên trong, các ngân hàng thực hiện quản lý chặt nguồn nhân lực, đảm bảo kiểm soát chéo và không một cá nhân nào có toàn quyền. Hệ thống nội bộ chỉ truy cập được khi có khóa của ít nhất hai người, đồng thời có giám sát nhân sự bên thứ ba khi truy cập. Các ngân hàng xây dựng cơ chế bảo vệ và phân quyền truy cập đối với các tài nguyên cơ sở dữ liệu (CSDL). Xây dựng phương án sao lưu, dự phòng đối với CSDL. Ghi nhật ký đối với các truy cập CSDL, các thao tác đối với cấu hình CSDL. Có giải



pháp ngăn chặn các hình thức tấn công CSDL.

Hiện nay, các ngân hàng đang áp dụng đồng thời nhiều giải pháp để bảo đảm an toàn cho người dùng hình thức dịch vụ này: Sử dụng bàn phím ảo; Sử dụng mật khẩu một lần (One Time Password); Xác thực đa yếu tố (Multi-Factor Authentication); Dùng thiết bị khóa phần cứng (Hardware Token), thẻ thông minh (PKI Smartcard); Chữ ký số… Đối với hệ thống CNTT, các ngân hàng áp dụng an ninh bảo mật cho hệ thống phần cứng, mạng truyền thông, dùng tường lửa để phòng chống truy cập trái phép. Đồng thời, sử dụng các phần mềm bảo mật để phòng chống virus, mã độc… Đường truyền được mã hóa để đảm bảo an toàn cho các ứng dụng. Trung tâm dự phòng sẵn sàng cao giúp các ngân hàng bảo đảm hệ thống luôn hoạt động ổn định. Ngoài ra, các ngân hàng đều xây dựng trung tâm dự phòng thảm họa để có thể khôi phục hệ thống nhanh chóng nếu xảy ra rủi ro.

Với những cố gắng này của các ngân hàng, các giao dịch Internet Banking trong thời gian qua đã đảm bảo an toàn và được người dân sử dụng ngày càng nhiều hơn. Các dịch vụ được cung cấp qua hình thức này cũng ngày càng mở rộng. Khi việc thanh toán không dùng tiền mặt trở thành thói quen của người Việt Nam thì Internet Banking sẽ thực sự là một kênh dịch vụ ngân hàng quan trọng và phổ biến.

Hoàng Yến

Quản lý rủi ro trong KỶ NGUYÊN SỐ

Gần đây trên các phương tiện truyền thông đang đề cập nhiều tới sự gia tăng cũng như mức độ nguy hiểm của các lỗ hổng bảo mật, chúng đã và đang gây ra những ảnh hưởng lớn đến các doanh nghiệp trên mọi lĩnh vực. Những lỗi bảo mật này không chỉ làm tổn thất đáng kể chi phí cho các doanh nghiệp mà còn ảnh hưởng tới uy tín, lòng tin của người tiêu dùng. Do đó, các tổ chức, doanh nghiệp cần phải chuyển đổi hướng tới một cách tiếp cận có hệ thống và chủ động hơn để giải quyết các mối đe dọa về bảo mật và quản lý các yêu cầu trong nền kinh tế hướng thông tin hiện nay.

THỰC TRẠNG BÁO ĐỘNG

Khi thế giới được số hóa và kết nối với nhau, thì nguy cơ về các mối đe dọa và rò rỉ thông tin ngày càng tăng với mức độ và số lượng vượt bậc. Hiện nay có hàng tỷ thẻ RFID được sử dụng bao gồm các sản phẩm, hộ chiếu, các tòa nhà… Với hơn hai tỷ người sử dụng Internet và số thuê bao di động vượt mốc 5 tỷ vào cuối năm 2010, gần một phần ba người dùng trên thế giới đang truy cập Internet mỗi ngày. Hơn 50 tỷ vật thể được dự kiến sẽ được kết nối số vào năm 2020, bao gồm cả ô tô, thiết bị và máy ảnh. Kết quả là lượng thông tin được tạo ra và sao lưu trên thế giới sẽ phát triển với tốc độ khổng lồ, dự báo đạt 35 tỷ gigabyte vào năm 2020. Không chỉ số lượng dữ liệu tăng lên mà giá trị tương ứng của các tài sản số này cũng tăng lên. Thông tin khách hàng nhạy cảm, quyền sở hữu trí tuệ và thậm chí cả kiểm soát máy móc… tất cả đang ngày càng được chuyển đổi sang các định dạng điện tử. Do đó, các cuộc tấn công nhằm vào các tài sản này sẽ gây ra những tác động đáng kể đến toàn bộ tổ chức, doanh nghiệp chứ không đơn giản chỉ ở bộ phận CNTT.

Bản đánh giá mới đây của Secunia về các lỗ hổng bảo mật đã cho thấy những báo động cấp bách trên toàn thế giới. Qua phân tích 2.503 ứng dụng trong năm 2012, Secunia phát hiện có đến 9.776 lỗ hổng. Tức có trung bình gần 4 lỗ hổng/ứng dụng, tăng 5% so với năm 2011 và tăng 15% so với cách đây 5 năm. Trong đó, chỉ tính riêng 18 ứng dụng đứng đầu danh sách này đã chứa đến 1.137 lỗ hổng. Tức trung bình có 63 lỗ hổng/ứng dụng. Điều đáng nói

là theo báo cáo này, 84% các lỗ hổng có một bản vá lỗi trong vòng 24 giờ kể từ lúc khi phát hiện, nhưng đa số người dùng, thậm chí cả người dùng doanh nghiệp, vẫn làm ngơ. Trong khi đáng ra các tổ chức phải biết những chương trình nào đang có mặt trên hệ thống của mình, các chương trình nào không an toàn,… để tìm các bản vá lỗi.

Có thể thấy, những thiệt hại cho cơ sở hạ tầng thông tin và xử lý thông tin đang xuất hiện thường xuyên hơn với nhiều phương thức tấn công có tổ chức và chuyên nghiệp hơn. Do đó việc bảo mật và bảo vệ thông tin quan trọng cũng như các tài sản liên quan ngày càng gặp nhiều khó khăn hơn. Vấn đề bảo mật hiện đang trở thành nhu cầu cấp bách và không thể thiếu. Việc triển khai các giải pháp bảo mật thông minh với khả năng để dự đoán chủ động, nhận biết và xử lý các mối đe dọa tiềm năng sẽ là một ưu tiên mới của các doanh nghiệp trong kỷ nguyên số.

THÁCH THỨC BẢO MẬT NGÀY CÀNG LỚN HƠN

Với sự gia tăng của dữ liệu, thiết bị và số lượng kết nối, các thách thức bảo mật đang gia tăng cả về số lượng và phạm vi. Chúng được chia thành ba loại chính: các mối đe dọa từ bên ngoài, các mối đe dọa nội bộ và các yêu cầu tuân thủ.

Các mối đe dọa bên ngoài

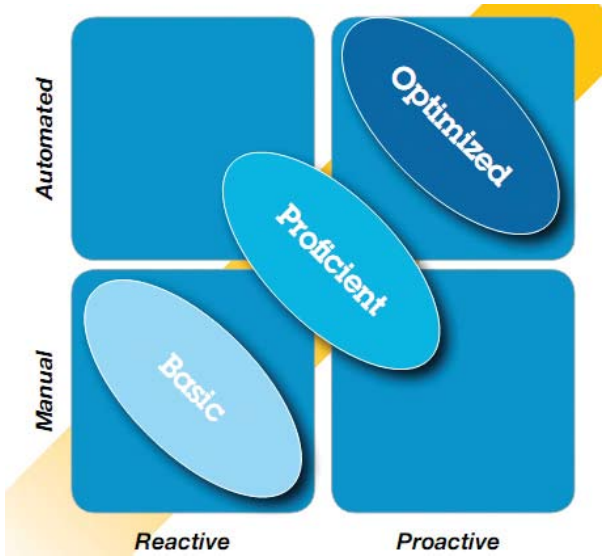
Gần đây có một sự gia tăng lớn các cuộc tấn công từ bên ngoài, nhằm vào các công ty lớn và các tổ chức chính phủ. Trong đó, những tấn công này thường đến từ các cá nhân làm việc độc lập. Tuy nhiên, hiện nay chúng ngày càng được phối hợp nhiều hơn, và được triển khai bởi nhiều nhóm khác nhau, từ các tin tặc tới các tổ chức tội phạm. Động cơ của kẻ tấn công không còn giới hạn ở việc tìm kiếm lợi nhuận mà đôi khi có thể bao gồm cả uy tín hay hoạt động gián điệp. Mục tiêu chủ yếu của các cuộc tấn công là nhằm vào các tài sản quan trọng của tổ chức, bao gồm cả cơ sở dữ liệu khách hàng, sở hữu trí tuệ và thậm chí cả tài sản vật chất được tạo ra bởi hệ thống thông tin.

Những cuộc tấn công từ bên ngoài thường gây tổn thất đáng kể về tài chính. Ví dụ, hàng triệu email bị đánh cắp sau khi tin tặc tấn công Epsilon, hãng cung cấp dịch vụ quảng bá qua email lớn nhất trên thế giới, đã trực tiếp ảnh hưởng đến nhiều khách hàng của công ty. Các chi phí của những vụ kiện tụng ban đầu được ước tính lên tới hàng trăm triệu đô la. Nhiều công ty khác trong các dịch vụ tài chính, truyền thông, giải trí, bán lẻ và các ngành công nghiệp viễn thông gần đây đã công bố các rò rỉ tương tự về thông tin tài chính cá nhân của khách hàng, gây tổn thất đáng kể về chi phí pháp lý và quy định.

Các mối đe dọa nội bộ

Trong nhiều trường hợp, các hành vi vi phạm trong lĩnh vực an ninh thông tin không từ các đối tác bên ngoài, mà từ ngay chính nội bộ, họ có thể là nhân viên, nhà thầu, nhà tư vấn và thậm cả nhà cung cấp dịch vụ. Những rò rỉ này xuất phát từ hành vi bất cẩn và những sai lầm hành chính (như cho người khác mật khẩu của mình, mất băng sao lưu hoặc máy

tính xách tay mà vô tình dẫn tới lộ thông tin nhạy cảm), đến các hành động cố tình được thực hiện bởi các nhân viên bất mãn. Những hành động này có mức độ nguy hiểm không kém gì các cuộc tấn công bên ngoài. Ví dụ, sự kiện Wikileaks, trong đó liên quan đến việc phát hành trái phép các bản ghi đã gây tổn thất cho chính phủ Mỹ hàng triệu đô la và tổn hại các mối quan hệ với các chính phủ nước ngoài trên toàn thế giới.



Hình 1: Tiếp cận 3 mức xây dựng bảo mật thông minh.

Các yêu cầu tuân thủ

Các doanh nghiệp khi thực thi một số lượng ngày càng tăng các nhiệm vụ của xuyên quốc gia, công nghiệp và địa phương cần tuân thủ các tiêu chuẩn bảo mật riêng của họ, ví dụ: Đạo luật Sarbanes-Oxley (SOX), J-SOX, COSO, COBIT, các tiêu chuẩn quốc tế ISO /IEC, HIPAA/HITECH…

TRIỂN KHAI GIẢI PHÁP BẢO MẬT THÔNG MINH

Để giải quyết sự gia tăng mức độ rủi ro, các tổ chức, doanh nghiệp cần phải xem xét và triển khai một cách tiếp cận bảo mật chủ động hơn. Nhìn chung, để đem lại hiệu quả cao cần phải kết hợp các giải pháp bảo mật như là một phần thiết yếu trong hoạt động của doanh nghiệp. Điều này đòi hỏi một cách tiếp cận toàn diện liên quan đến một loạt các vấn đề, như bảo mật vật lý, phân loại dữ liệu, nâng cao nhận thức của nhân viên và kiểm soát.

Trong các doanh nghiệp, giải pháp bảo mật thông minh sẽ được triển khai trên từng mức. Chúng chuyển đổi từ cách tiếp cận thông thường sang tiếp cận sử dụng các quá trình ngày càng tự động hóa để xác định, giám sát và đối phó với các mối đe dọa. Xu hướng này hướng tới hoạt động tích cực hơn về các vấn đề bảo mật hơn là các phương pháp tiếp cận phản ứng (Hình 1).

Cơ bản – Các tổ chức cần tập trung vào việc triển khai các bảo vệ vành đai, trong đó qui định các truy cập vật lý và ảo. Bảo vệ vành đai cung cấp đầu vào cho các báo cáo về sự cố và các hành vi vi phạm. Ở mức độ cơ bản, các doanh nghiệp thường chỉ triển khai tường lửa, chống virus, kiểm soát truy cập và báo cáo sử dụng. Tuy nhiên, chúng hoạt động trong một chế độ vận hành thủ công với cái nhìn không thấu suốt về tình hình an ninh thực tế của doanh nghiệp.

Chuyên sâu (Proficient) – Bảo mật được xếp vào kết cấu của các ứng dụng CNTT và các hoạt động kinh doanh. Ở mức này, giải pháp bảo mật sẽ được kết hợp vào các ứng dụng quan trọng, cơ sở dữ liệu và các quy trình kinh doanh. Do đó hệ thống bảo mật ngày càng trở nên toàn diện hơn, nhưng đồng thời bổ sung thêm tính phức tạp cho hệ thống của doanh nghiệp.

Tối ưu hóa – Các tổ chức sử dụng phân tích bảo mật tự trị và dự báo để thúc đẩy tiến tới bảo mật thông minh. Bảo mật ở mức này bao gồm thu thập và phân tích những xâm nhập trong quá khứ, hoạt

động của nhân viên và các nguồn dữ liệu khác để dự đoán hành vi vi phạm tiềm năng có thể xảy ra và ngăn chặn trước khi chúng xảy ra.

Mỗi cấp bổ sung thêm một lớp sự chuẩn bị ngăn ngừa và phòng tránh các sự cố bảo mật cả vô tình và cố ý. Để xác định và đóng các lỗ hổng bảo mật trên toàn hệ thống doanh nghiệp, các tổ chức cần khám phá và khai thác các tính năng phân tích để đáp ứng các nhu cầu cấp bách nhất của họ. Một đánh giá sâu sắc về bốn lĩnh vực an ninh có thể giúp các tổ chức tiến tới triển khai bảo mật thông minh bằng cách cải thiện hệ thống quản trị, quản lý rủi ro và tuân thủ:

– Nhân sự: Chuyển từ kiểm soát truy cập trên cơ sở ứng dụng thông qua mật khẩu sang cách tiếp cận dựa trên vai trò mà kiểm soát truy cập người dùng thông qua bảng điều khiển và kiểm soát người sử dụng đặc quyền.

– Dữ liệu: Chuyển đổi từ kiểm soát truy cập cơ bản và các phương pháp mã hóa để bảo vệ dữ liệu bằng cách nâng cao khả năng quản trị dữ liệu và quản lý việc sử dụng dữ liệu.

– Ứng dụng: Nâng cao chức năng quét các lỗ hổng trong các ứng dụng hiện có để phát hiện gian lận và thiết kế bảo mật cho các ứng dụng mới.

– Hạ tầng: Thay thế các phương pháp phản ứng giống như ngăn chặn truy cập trái phép và virus bằng các phương pháp chủ động mà an toàn cho hệ thống với việc cho phép giám sát mạng tiên tiến.

CHIẾN LƯỢC BA BƯỚC

Để thực thi giải pháp bảo mật thông minh, bộ phận CNTT cần xây dựng một chiến lược ba bước bao gồm:

Thu nhận thông tin: Thực hiện một cách tiếp cận có cấu trúc để đánh giá các rủi ro trong kinh doanh và trong CNTT

Thu nhận thông tin bao gồm việc giải quyết các nguy cơ bảo mật CNTT như là một phần của khung quản lý rủi ro doanh nghiệp (Hình 2).

Cách tiếp cận đánh giá các rủi ro CNTT và kinh doanh này bao gồm việc xác định các mối đe dọa quan trọng và nhiệm vụ tuân thủ, xem xét các rủi ro an ninh và những thách thức hiện có, thực hiện và thực thi các quy trình quản lý rủi ro, các khung kiểm soát chung cũng như các quá trình quản lý sự cố khi xảy ra.

Phối hợp đồng bộ các giải pháp bảo mật: Thực hiện và thực thi bảo mật mở rộng tại các doanh nghiệp, bao gồm cả các bên liên quan:

– Khách hàng – Xây dựng và phổ biến chính sách thông tin cá nhân.

– Nhân viên – Thiết lập các quy định và chính sách bảo mật rõ ràng. Tuyên truyền, giáo dục để xác định và giải quyết các rủi ro an ninh. Quản lý truy cập và việc sử dụng hệ thống và dữ liệu.

– Đối tác – Làm việc với các tổ chức trên toàn chuỗi

Hình 2: Khung quản lý rủi ro doanh nghiệp.

cung ứng để phát triển và thực thi các tiêu chuẩn bảo mật. Báo cáo và quản lý rủi ro, bao gồm các sự cố an ninh như là một phần thông thường của hoạt động kinh doanh.

– Kiểm toán viên – Cân bằng các rủi ro doanh nghiệp và CNTT. Đóng góp vào khung kiểm soát. Tiến hành đánh giá thường xuyên chính sách quản lý và doanh nghiệp.

– Cơ quan quản lý – Quản lý rủi ro pháp lý và chứng minh sự tuân thủ với các quy định hiện hành. Xem xét và sửa đổi các kiểm soát hiện có trên cơ sở những yêu cầu thay đổi.

Sử dụng các công cụ thông minh: Sử dụng các phân tích để làm nổi bật các rủi ro và xác định, giám sát cũng như xử lý các mối đe dọa. Khi các doanh nghiệp cần phải tăng cường bảo vệ bảo mật của họ, việc sử dụng các phân tích dự báo đóng một vai trò ngày càng quan trọng. Họ có thể thực hiện các tương quan phức tạp để phát hiện các mối đe dọa tiên tiến, có ý thức quản trị và có các quy trình kinh doanh tại chỗ – những yếu tố quan trọng trong việc phát hiện và đảm bảo an toàn cho hệ thống.

KẾT LUẬN

Trong thế giới số được kết nối hiện nay, các nguy cơ rủi ro ngày càng tăng theo cấp số nhân. Tuy nhiên, không phải mọi nguy cơ tiềm năng đều có thể được giải quyết một cách hiệu quả về chi phí. Do đó, các tổ chức, doanh nghiệp cần phải xem xét và đánh giá kỹ lưỡng các tác động của các rủi ro tiềm tàng này đến hoạt động kinh doanh của mình. Giải pháp bảo mật thông minh sẽ giúp doanh nghiệp thực thi bảo mật hiệu quả mà vẫn đảm bảo các yêu cầu kinh doanh hiện tại.

Vân Anh

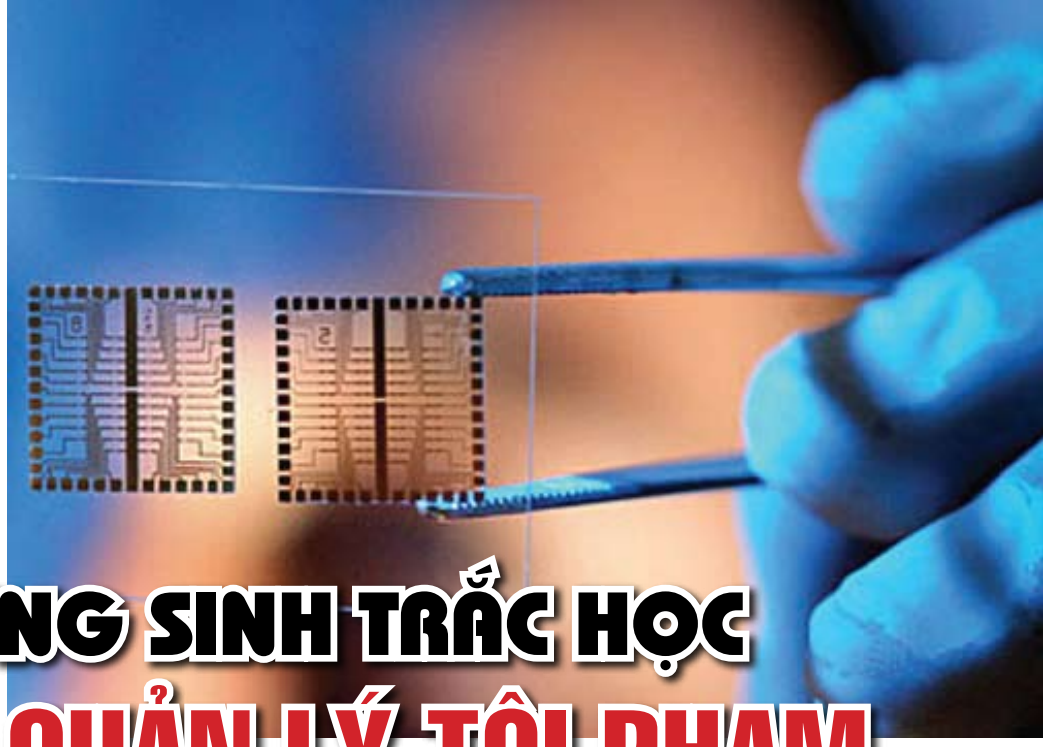
Tài liệu tham khảo

[1]. Ericsson, *"More than 50 billion connected devices — taking connected devices to mass market and proftability."* http://www.ericsson.com/news/110214_more_than_50_billion_244188811_c.

[2]. IDC *"Digital Universe Study,"* sponsored by EMC, May 2010.

[3]. http://www.networkworld.com.

[4]. http://www.ibm.com.



ỨNG DỤNG SINH TRẮC HỌC TRONG QUẢN LÝ TỘI PHẠM

Nguyễn Huy Mạ

NƠI QUẢN LÝ TOÀN BỘ TÀNG THƯ SINH TRẮC HỌC

Cục Hồ sơ nghiệp vụ Cảnh sát thuộc Tổng cục Cảnh sát Phòng chống tội phạm, Bộ Công an hiện đang quản lý, khai thác các hệ thống thông tin về nghiệp vụ phục vụ công tác phòng, chống tội phạm, giữ gìn trật tự an toàn xã hội. Hồ sơ, thông tin, tài liệu nghiệp vụ cảnh sát là kết quả nghiên cứu, xây dựng của nhiều thế hệ, nhiều đơn vị nghiệp vụ trong lực lượng Công an nhân dân nói chung và lực lượng Cảnh sát nhân dân nói riêng. Những hồ sơ này được sưu tầm, chọn lọc và lưu trữ bảo vệ an toàn để khai thác phục vụ có hiệu quả công tác phòng chống tội phạm và quản lý nhà nước về an ninh trật tự.

Ngay sau khi đất nước được độc lập, lực lượng Công an nhân dân đã tiếp quản quản lý hàng triệu tài liệu thông tin về sinh trắc học của công dân và tội phạm trong cả nước để tiến hành công tác tra cứu truy nguyên cá nhân. Hệ thống tàng thư sinh trắc học và phương pháp truy nguyên cá nhân phục vụ quản lý tội phạm và quản lý công dân thời kỳ này chủ yếu dựa trên các phương pháp mô tả nhận dạng người như chiều cao, cân nặng, hình dáng cơ thể, các đặc điểm nhân trắc khác trên khuôn mặt như mũi, tai, mắt, hình dạng mặt và các đặc điểm riêng như nốt ruồi, sẹo, các dị tật, dị hình. Với hàng triệu tài liệu trong tàng thư căn cước và tàng thư tội phạm được giao quản lý, lực lượng hồ sơ nghiệp vụ Cảnh sát đã khai thác phục vụ có hiệu quả công tác phòng chống tội phạm và bảo vệ nền độc lập của tổ quốc. Sau năm 1975, lực lượng hồ sơ tiếp tục tiếp quản quản lý hàng chục triệu tài liệu thông tin sinh trắc học của công dân và tội phạm trong tàng thư lưu trữ do chế độ cũ để lại.

Hiện nay, cơ quan hồ sơ nghiệp vụ Cảnh sát đang thống nhất quản lý một khối lượng lớn tài liệu chứa đựng thông tin sinh trắc học bao gồm thông tin về ảnh chân dung, đặc điểm nhận dạng, thông tin vân tay và các thông tin về lai lịch của hàng trăm triệu lượt công dân và đối tượng phạm tội trong toàn quốc.

Hệ thống tàng thư tài liệu sinh trắc này đang tiếp tục được tích luỹ, bổ sung và được khai thác phục vụ các yêu cầu nghiệp vụ và quản lý nhà nước về an ninh trật tự, phục vụ truy tìm tội phạm, truy tìm tung tích nạn nhân, tìm di ảnh phục vụ nhân dân.

Lấy dấu vân tay theo phương pháp thủ công truyền thống.

ỨNG DỤNG CÔNG NGHỆ THÔNG TIN VÀO NGHIỆP VỤ PHÂN TÍCH VÀ LƯU TRỮ

Ngay từ những năm 70 của thế kỷ 20, Bộ Công an đã thành lập những bộ phận kỹ thuật chuyên biệt để nghiên cứu ứng dụng khoa học kỹ thuật vào quản lý thông tin, phục vụ hoạt động nghiệp vụ của cơ quan công an các cấp. Trong đó, bộ phận tàng thư tội phạm có nhiệm vụ nghiên cứu ứng dụng các thành tựu khoa học kỹ thuật trong công tác quản lý thông tin tội phạm, tiến hành so sánh tội phạm, thực hiện biện pháp truy nguyên đồng nhất để xác định nhân thân, lai lịch đối tượng phạm tội. Bộ phận này còn có nhiệm vụ tổ chức sưu tầm thông tin, tài liệu về các vụ việc và đối tượng trong toàn quốc và tổ chức thành các hệ thống tàng thư, cơ sở dữ liệu để khai thác, so sánh tội phạm như: tàng thư căn cước công dân, tàng thư căn cước tội phạm, tàng thư tang vật chứng, dấu vết súng đạn, tàng thư hồ sơ lưu trữ v.v..

Do sự phát triển của khoa học công nghệ thời gian đó còn hạn chế nên việc quản lý thông tin tội phạm chủ yếu thực hiện bằng biện pháp thủ công, phương pháp so sánh truy nguyên tội phạm chủ yếu dựa vào thông tin trên giấy tờ, thông qua biện pháp nhận dạng mô tả hình dáng người và các thông số sinh trắc học khác … Việc truy nguyên qua vân tay còn rất hạn chế và được phân tích, so sánh hoàn toàn bằng mắt thường bởi các chuyên gia được đào tạo chuyên sâu và có kinh nghiệm.

Đến những năm 90, khoa học công nghệ, đặc biệt là công nghệ thông tin (CNTT) bắt đầu phát triển, công tác truy nguyên tội phạm đã bắt đầu được ứng dụng tin học. Một số hệ thống phần mềm tin học được đưa vào ứng dụng trong lực lượng công an như: hệ thống nhận dạng vân tay tự động, hệ thống nhận dạng tội phạm qua lời kể của nhân chứng, hệ thống quản lý ảnh đối tượng truy nã v.v.. Các

hệ thống trên bước đầu đã được đưa vào ứng dụng phục vụ công tác phòng chống tội phạm và bảo đảm trật tự an toàn xã hội.

Nhận thức được tầm quan trọng của việc ứng dụng CNTT vào công tác quản lý tội phạm, trong đó có việc ứng dụng công nghệ sinh trắc học tập trung thống nhất, Lãnh đạo Bộ Công an đã tạo điều kiện và chỉ đạo Tổng cục Cảnh sát triển khai ứng dụng các hệ thống nhận dạng sinh trắc học tại Cục Hồ sơ nghiệp vụ Cảnh sát như: hệ thống nhận dạng vân tay tự động (AFIS), hệ thống nhận dạng ảnh mặt, hệ thống tàng thư gen. Năm 1996, hệ thống AFIS đầu tiên của lực lượng Công an nhân dân (CAND) Việt Nam được đưa vào sử dụng với thiết bị và phần mềm của các hãng công nghệ hàng đầu thế giới. Kết quả của việc ứng dụng nhanh thành tựu khoa học kỹ thuật của thế giới đã giúp cho lực lượng CAND Việt Nam có được hệ thống kỹ thuật hiện đại, độ chính xác cao, phát huy hiệu quả trong công tác truy nguyên, so sánh tội phạm.

HIỆU QUẢ HƠN VỚI CÔNG NGHỆ MỚI

Đến năm 2010, Bộ Công an tiếp tục đầu tư trang bị một hệ thống mới thay thế hệ thống cũ với nhiều tính năng được cải tiến, có khả năng tích hợp nhiều công nghệ nhận dạng sinh trắc khác nhau, khả năng quản lý cơ sở dữ liệu được mở rộng, phạm vi triển khai được nhân rộng ra toàn quốc với hệ thống mạng phân tán, kết nối trực tuyến 24/24 đảm bảo các yêu cầu khai thác thông tin phục vụ điều tra tội phạm được thực hiện nhanh chóng và chính xác. Các chức năng của hệ thống mới là kết quả nghiên cứu, đúc kết kinh nghiệm khai thác sử dụng công nghệ nhận dạng vân tay trong hơn 20 năm của các cán bộ, chuyên gia lực lượng Hồ sơ nghiệp vụ Cảnh sát, đồng thời là kết quả của sự mạnh dạn áp dụng những ý tưởng sáng tạo nghiệp vụ của Lãnh đạo Cục Hồ sơ nghiệp vụ Cảnh sát. Việc sáng tạo trong cải tiến chức năng và khai thác sử dụng hệ thống nhận dạng vân tay đã phát huy hiệu quả đặc biệt trong công tác điều tra tội phạm. Hàng năm hệ thống đã tra cứu truy nguyên phát hiện hàng trăm đối tượng là thủ phạm các vụ án, đối tượng truy nã, cung cấp hàng trăm ngàn bản trích lục tiền án, tiền sự phục vụ công tác điều tra, truy tố, xét xử, phát hiện nhân thân lai lịch của hàng trăm trường hợp chết chưa rõ tung tích. Thông tin về tiền án tiền sự do cơ quan hồ sơ nghiệp vụ cảnh sát cung cấp là căn cứ quan trọng giúp cơ quan điều tra, viện kiểm sát và toà án

Lấy dấu vân tay theo bằng thiết bị kỹ thuật mới.

các cấp tiến hành điều tra truy tố, xét xử đúng người, đúng pháp luật, là một trong những căn cứ để áp dụng các tình tiết tăng nặng, giảm nhẹ đối với các bị can, bị cáo.

Ngoài hệ thống AFIS, hệ thống nhận dạng ảnh mặt cũng đang được nghiên cứu, áp dụng các công nghệ như nhận dạng ảnh tĩnh 2 chiều, 3 chiều, nhận dạng ảnh động từ các video thu nhận được qua công tác điều tra, với cơ sở dữ liệu ảnh mặt độ phân giải thấp lên đến hàng chục triệu bản ghi. Dự kiến hệ thống này sẽ được triển khai, tích hợp với hệ thống nhận dạng vân tay tự động, áp dụng các thiết bị nhận dạng di động tiên tiến và phổ biến hiện nay như điện thoại thông minh tích hợp phần mềm nhận dạng mặt từ xa, thiết bị đọc và so sánh vân tay lưu động.

Hiện nay, ngoài hệ thống nhận dạng sinh trắc học của cơ quan Hồ sơ nghiệp vụ Cảnh sát, trong lực lượng Công an có một số đơn vị cùng tiến hành ứng dụng công nghệ sinh trắc học như hệ thống hộ chiếu điện tử, chứng minh nhân dân điện tử, hệ thống giám định gen. Các hệ thống trên ít nhiều đã có tác dụng quản lý phục vụ công tác nghiệp vụ riêng của từng lực lượng. Tuy nhiên xét về tính tổng thể thì việc xây dựng các hệ thống nhận dạng sinh trắc học phân tán như hiện nay là hết sức tốn kém và không đảm bảo tính tập trung thống nhất. Do một số đơn vị bên ngoài ngành công an chưa hiểu đầy đủ về hệ thống thông tin sinh trắc mà cơ quan Hồ sơ nghiệp vụ Cảnh sát đang tập trung quản lý nên việc tư vấn ứng dụng công nghệ sinh trắc học chưa được đầy đủ. Các hệ thống sinh trắc học được triển khai bị chia cắt, phân tán không có sự kết nối tích hợp thông tin với nhau dẫn đến hiệu quả khai thác chưa cao, chưa đáp ứng được các yêu cầu về cải cách hành chính, yêu cầu nghiệp vụ phòng chống tội phạm và quản lý nhà nước về an ninh trật tự.

Với việc tập trung quản lý thống nhất thông tin tài liệu chứa đựng đặc điểm sinh trắc học của tội phạm và công dân của cả nước tại cơ quan Hồ sơ nghiệp vụ Cảnh sát thì việc ứng dụng công nghệ sinh trắc học tại cơ quan Hồ sơ nghiệp vụ là yêu cầu tất yếu và cần phải được nghiên cứu, xây dựng một cách bài bản, có hệ thống, với lộ trình thích hợp. Hy vọng rằng, các cơ quan tư vấn, các hãng công nghệ sinh trắc học hỗ trợ và phối hợp chặt chẽ với đội ngũ chuyên gia của lực lượng CAND nói chung và của lực lượng Hồ sơ nghiệp vụ Cảnh sát nói riêng để giải được bài toán ứng dụng sinh trắc học trong quản lý tội phạm một cách tổng thể, có hiệu quả, tiết kiệm cho ngân sách nhà nước.

Khi hệ thống nhận dạng tội phạm đa sinh trắc được hình thành và triển khai thống nhất, đồng bộ, lực lượng CAND Việt Nam sẽ có thêm những công cụ đắc lực giúp công tác phòng chống tội phạm và bảo đảm trật tự an toàn xã hội ngày càng có hiệu quả hơn, phục vụ các quyền và lợi ích hợp pháp của nhân dân./.