TẠP CHÍ KHOA HỌC ĐẠI HỌC KHÁNH HÒA
tapchikhoahoc@ukh.edu.vn

MÔ PHỎNG MẠNG MÁY TÍNH TRƯỜNG ĐẠI HỌC KHÁNH HÒA

Trần Công Cẩn

Trường Đại học Khánh Hòa

Tóm tắt

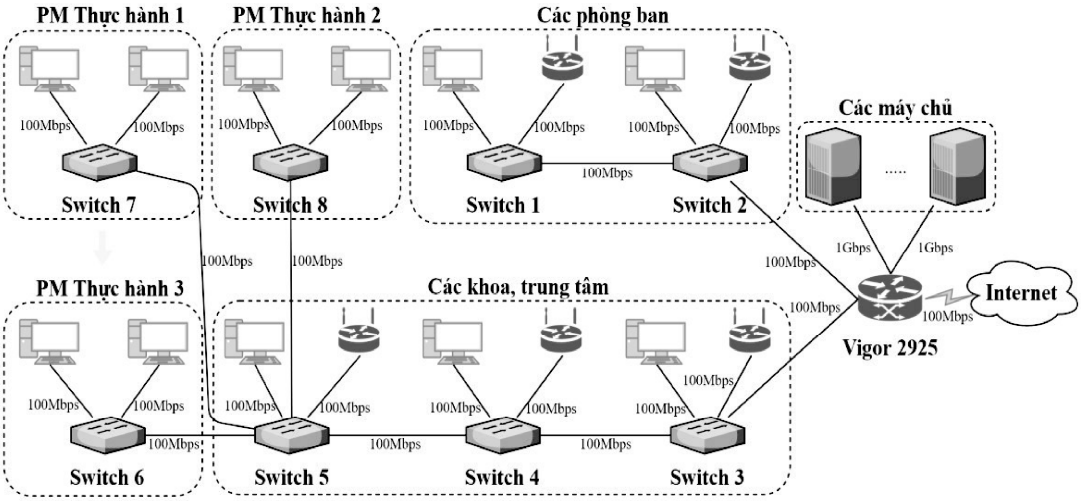
Thực tế cho thấy, sinh viên ngành công nghệ thông tin mới ra trường thường gặp nhiều khó khăn khi tác nghiệp quản trị mạng máy tính của các tổ chức (doanh nghiệp, cơ quan nhà nước, ...). Vì vậy, cần xây dựng các bài thực hành sát thực tế ứng dụng mạng máy tính của các tổ chức, qua đó giúp sinh viên nâng cao kỹ năng quản trị mạng máy tính. Do khó khăn về kinh phí, việc trang bị phòng thực hành có đầy đủ thiết bị là khó khả thi. Trong khi đó, phần mềm mô phỏng mạng máy tính cho phép mô phỏng một hệ thống mạng máy tính tương đương hệ thống mạng máy tính trong thực tế. Trong bài báo này, tác giả thực hiện mô phỏng hệ thống mạng máy tính của Trường Đại học Khánh Hòa. Kết quả mô phỏng không chỉ chứng tỏ khả năng ứng dụng hữu hiệu của kỹ thuật, phần mềm mô phỏng, mà còn có thể dùng làm bài tập thực hành mô phỏng mạng máy tính, giúp sinh viên tiếp cận phương pháp phân tích, thiết kế, thiết lập mạng máy tính của một tổ chức trong thực tế.

Từ khóa: *Mạng máy tính, mô phỏng mạng, an toàn mạng.*

Để mô phỏng mạng máy tính của Trường Đại học Khánh Hòa, sau đây viết tắt là UKH - University of Khanh Hoa, trước tiên cần khảo sát thực tế ứng dụng mạng máy tính của trường. Căn cứ kết quả khảo sát và chuẩn thiết kế mạng LAN (Local Area Network) có kết nối với mạng Internet, xây dựng mô hình mạng máy tính của UKH. Sau đó, lựa chọn phần mềm mô phỏng và tiến hành mô phỏng mạng máy tính dựa trên mô hình mạng được xây dựng.

1. Thực trạng mạng máy tính của UKH

Do điều kiện kinh phí khó khăn, mạng máy tính của UKH, mặc dù chưa được thiết kế đúng chuẩn, nhưng được bổ sung, nâng cấp thiết bị qua nhiều giai đoạn, về cơ bản có thể đáp ứng yêu cầu giảng dạy, thực hành cho sinh viên và yêu cầu quản lý, hoạt động nghiệp vụ của cán bộ nhà trường. Sơ đồ kết nối mạng máy tính đang sử dụng tại UKH được trình bày trong Hình 1 dưới đây.



Hình 1: Sơ đồ kết nối mạng máy tính đang sử dụng tại UKH

Về kiến trúc mạng LAN: các thiết bị chuyển mạch (switch) trong mạng nội bộ kết nối theo kiến trúc Star – Bus. Nhược điểm lớn nhất của kiến trúc Star – Bus là cho phép truy nhập chung môi trường truyền dẫn (shared medium), dẫn đến hiệu quả sử dụng hệ thống truyền dẫn không cao (trung bình khoảng 60% băng thông). Khi hỏng một switch nằm giữa đường bus, các thiết bị mạng từ nó về cuối đường bus bị ngắt kết nối với mạng.

Về kết nối với mạng Internet: sử dụng đường truyền tốc độ 100Mbps kết nối và chia sẻ thông tin trên mạng Internet với tên miền ukh.edu.vn, nhưng chưa thiết lập thiết bị Internet Firewall để kiểm soát truy nhập giữa mạng nội bộ và mạng Internet. Các máy tính thực hành và hệ thống mạng không dây WiFi đặt trong mạng nội bộ và dùng chung đường truyền Internet này.

Về các phần mềm ứng dụng trên mạng: có 3 ứng dụng quản lý được dùng trong nội bộ là Quản lý đào tạo, Quản lý thư viện, Quản lý văn bản và điều hành; có 4 ứng dụng chia sẻ thông tin cho sinh viên và người dùng trên Internet là Website Đại học Khánh Hòa, Website tra cứu thông tin thư viện, Website cung cấp thông tin về đào tạo cho sinh viên, Website hỗ trợ dạy học trực tuyến; hệ thống thư điện tử được Google cung cấp miễn phí.

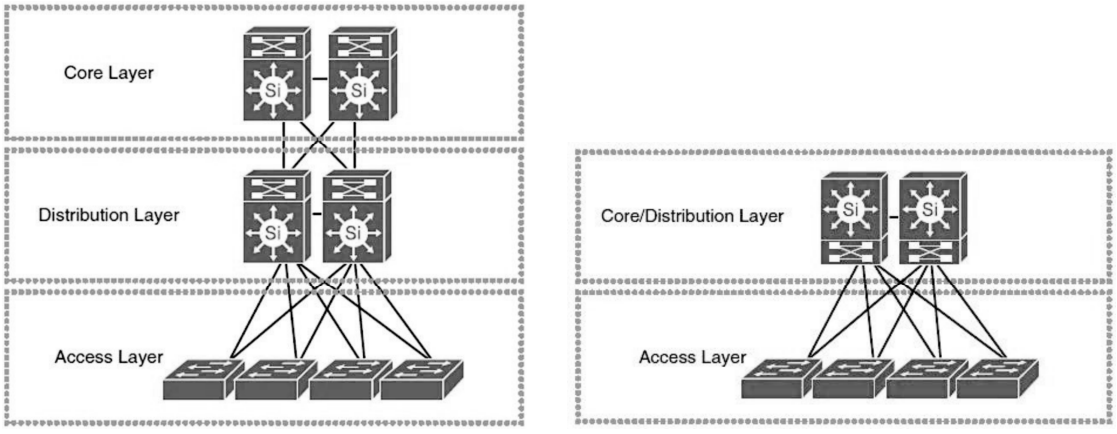
Về tổ chức hành chính: có 24 đơn vị trực thuộc là các phòng ban, Thư viện, khoa, trung tâm với 390 lao động. Số lượng người dùng trong mạng LAN không quá 120 người, chủ yếu ở các phòng ban và thư viện (97 người). Ở các khoa, có 3 máy tính của ban chủ nhiệm khoa kết nối mạng LAN. Các giáo viên chủ yếu làm việc ở nhà. Ở các trung tâm, số lượng người dùng mạng LAN không nhiều (từ 2 đến 5 người). UKH có 2 cơ sở. Cơ sở 1 là trụ sở chính, nơi làm việc của các đơn vị trực thuộc. Cơ sở 2 dùng cho việc dạy học, cách Cơ sở 1 khoảng 4km, có 2 máy tính làm nhiệm vụ kết nối về Cơ sở 1 thông qua mạng Internet để sử dụng các phần mềm quản lý dùng trong nội bộ.

Thực trạng nêu trên cho thấy mạng máy tính hiện nay của UKH có 3 nhược điểm cần khắc phục: (1) kiến trúc mạng LAN kiểu Star – Bus có nhiều hạn chế (nêu trên); (2) chưa sử dụng Internet Firewall để kiểm soát truy nhập khi kết nối mạng LAN với mạng Internet; (3) các máy tính thực hành (150 máy tính nằm cuối đường Bus) và mạng không dây WiFi kết nối mạng để truy cập Internet, nhưng được đặt trong mạng nội bộ, dẫn đến việc chiếm dụng băng thông của mạng nội bộ. Mặt khác các chuẩn bảo mật của mạng không dây WiFi (WEP, WPA, …) có khả năng bảo mật không cao, làm gia tăng nguy cơ mất an toàn thông tin. Nội dung dưới đây sẽ phân tích, đề xuất tái cấu trúc và xây dựng mới mô hình mạng máy tính của UKH nhằm khắc phục 3 nhược điểm này.

2. Đề xuất tái cấu trúc mạng máy tính của UKH

2.1. Kiến trúc mạng Campus

Kiến trúc mạng Campus [1,10, 11] có ưu điểm về hiệu năng, tính linh hoạt, tính mở, tính kế thừa của mạng máy tính, được dùng phổ biến cho thiết kế mạng LAN.



a) Campus Three - Tier **b) Campus Two - Tier**

Hình 2: Kiến trúc mạng Campus Three-Tier và Two-Tier

Kiến trúc mạng Campus Three-Tier (Hình 2a) gồm 3 lớp: lớp truy nhập (Access Layer), lớp phân phối (Distribution Layer) và lớp lõi (Core Layer). Lớp truy nhập là lớp ngoài cùng, gồm các switch (thường dùng switch layer 2) kết nối các máy tính của người sử dụng vào hệ thống mạng LAN. Lớp phân phối là lớp giữa, kết nối các switch của lớp truy nhập và phân phối lưu lượng truy cập mạng của chúng về lớp lõi. Lớp lõi làm nhiệm vụ kết nối tất cả các switch ở lớp phân phối và định tuyến truy cập tài nguyên mạng, tối thiểu phải dùng loại switch layer 3.

Kiến trúc mạng Campus Two-Tier (Hình 2b) gồm 2 lớp: Lớp truy nhập (Access Layer) và lớp lõi/phân phối (Core/Distribution Layer). Như vậy, trong kiến trúc này, lớp lõi kiêm nhiệm chức năng

của lớp phân phối. Khi cần nâng cấp mạng máy tính, việc chuyển từ kiến trúc Campus Two-Tier thành kiến trúc Campus Three-Tier được thực hiện rất thuận lợi: các thiết bị lớp truy nhập được kế thừa, cần bổ sung thiết bị switch cho lớp phân phối; thiết bị switch của lớp lõi (trong kiến trúc Campus Two-Tier) có thể được sử dụng trong lớp phân phối và trang bị mới thiết bị switch có hiệu năng lớn hơn cho lớp lõi.

Kiến trúc mạng Campus được tổ chức theo kiến trúc Star - Star. Trong đó, lớp lõi tạo thành "trung tâm mạng", các máy trạm được kết nối vào lớp truy nhập. Vì vậy, nó đảm bảo vai trò và tốc độ truy cập mạng của các máy trạm là như nhau. Trường hợp một thiết bị mạng trong lớp truy nhập bị hỏng thì chỉ một nhánh trong kiến trúc Campus bị ngắt kết nối, các nhánh còn lại vẫn hoạt động. Như vậy, kiến trúc mạng Campus đã khắc phục được nhược điểm nêu trên của kiến trúc mạng Star - Bus. Với các tổ chức có quy mô lớn (có trên vài trăm máy tính người dùng), có thể áp dụng kiến trúc mạng Campus Three-Tier.

2.2. Phân tích, tái cấu trúc mạng máy tính của UKH

Với thực trạng mạng máy tính của UKH được trình bày ở mục 1, bài báo đề xuất lựa chọn kiến trúc Campus Two - Tier để tái cấu trúc, xây dựng mạng máy tính của UKH.

Trong mạng LAN, để sử dụng băng thông mạng hiệu quả, tránh việc phát gói tin quảng bá (broadcast) trên toàn mạng, cần đặt máy tính người sử dụng trong mỗi đơn vị trực thuộc vào một mạng LAN ảo (VLAN - Virtual LAN). Bảng 1 dưới đây liệt kê danh sách VLAN trong mạng LAN của UKH; các máy chủ dùng trong nội bộ được đặt vào VLAN có tên là SrvFarm và sử dụng kỹ thuật định tuyến để người sử dụng truy cập được các dịch vụ mạng trên các máy chủ này; những đơn vị trực thuộc có số lượng máy tính kết nối mạng LAN ít, chức năng nhiệm vụ tương tự nhau (các khoa, các trung tâm) được tập hợp vào một VLAN. Cột cuối trong Bảng 1 là số hiệu VLAN-ID (số hiệu định danh) của các VLAN.

Bảng 1: Danh sách VLAN trong mạng LAN của UKH

STT	Đơn vị sử dụng VLAN	VLAN Name	VLAN-ID
1.	Phòng Quản lý Đào tạo và Khảo thí	PDT	10
2.	Phòng Truyền thông và HT quốc tế	PHT	11
3.	Phòng Kế hoạch và Tài chính	PKT	12
4.	Phòng Quản lý Khoa học	PKH	13
5.	Phòng Công tác Sinh viên	PSV	14
6.	Phòng Quản trị Thiết bị và Dự án	PTB	15
7.	Phòng Tổ chức và Hành chính	PTH	16
8.	Phòng Thanh tra, Pháp chế và Đảm bảo chất lượng	PTT	17
9.	Thư viện	PTV	18
10.	Khoa Du lịch	Khoa	20
11.	Khoa Lý luận cơ bản		
12.	Khoa Ngoại ngữ		
13.	Khoa Nghệ thuật		
14.	Khoa Sư phạm		
15.	Khoa Khoa học Tự nhiên và Công nghệ		
16.	Khoa Quản lý Văn hóa và Giáo dục		
17.	Khoa Xã hội và Nhân văn		
18.	Trung tâm CNTT và ứng dụng mỹ thuật	TTam	30
19.	Trung tâm ĐT và Cung ứng DV Du lịch - Nghệ thuật		
20.	Trung tâm Giáo dục Quốc phòng		
21.	Trung tâm Giáo dục thường xuyên		
22.	Trung tâm Ngoại ngữ và Tin học		
23.	Trung tâm Ứng dụng CN Sinh học và Môi trường		
24.	Trung tâm hỗ trợ sinh viên và hợp tác doanh nghiệp		
25.	Quản trị mạng	Admin	50
26.	Các máy chủ của mạng LAN (LAN Servers)	SrvFarm	52

Mạng máy tính của UKH có kết nối với mạng Internet, chịu tác động của các cuộc tấn công mạng ngày càng tinh vi và nguy hiểm. Để đảm bảo an toàn thông tin, cần có thiết bị Internet Firewall nhằm ngăn chặn các truy nhập trái phép và cho phép lọc các gói tin không muốn gửi đi hoặc nhận vào. Thiết

bị Internet Firewall quyết định những dịch vụ nào từ bên trong được phép truy cập từ bên ngoài, những người nào từ bên ngoài được phép truy cập đến các dịch vụ bên trong, và cả những dịch vụ nào bên ngoài được phép truy cập bởi những người bên trong. Để thiết bị Internet Firewall làm việc hiệu quả, tất cả thông tin từ trong ra ngoài và ngược lại đều phải thực hiện thông qua nó. Chỉ những trao đổi được phép bởi chế độ an ninh của hệ thống mạng nội bộ mới được lưu thông qua thiết bị Internet Firewall. Từ đó, dùng thiết bị Internet Firewall thiết lập 3 vùng mạng: *Vùng mạng nội bộ*, kết nối vào cổng Inside của thiết bị Internet Firewall; *Vùng mạng Internet*, kết nối vào cổng Outside của thiết bị Internet Firewall; và *Vùng mạng DMZ* là vùng mạng đặt các máy chủ cho phép truy cập từ Vùng mạng Internet, kết nối vào cổng DMZ của thiết bị Internet Firewall. Thiết bị Internet Firewall cho phép người dùng nội bộ truy cập các dịch vụ mạng ở Vùng mạng DMZ và Vùng mạng Internet. Trong khi đó, người dùng từ Vùng mạng Internet chỉ được phép truy cập các ứng dụng đặt ở Vùng mạng DMZ, không được phép truy cập vào Vùng mạng nội bộ.

Các máy chủ ứng dụng nội bộ của UKH đặt trong Vùng mạng nội bộ, ở lớp lõi trong kiến trúc mạng Campus. Người dùng của UKH có nhu cầu sử dụng mạng Internet để truy cập các ứng dụng nội bộ, gồm: người dùng đi công tác, giáo viên làm việc ở nhà, 2 máy tính tác nghiệp ở Cơ sở 2. Để đáp ứng nhu cầu này, sử dụng kỹ thuật VPN (Virtual Private Network – mạng riêng ảo) để thiết lập kênh truyền an toàn từ Vùng mạng Internet vào Vùng mạng nội bộ cho người dùng của UKH. Thiết bị của người dùng đóng vai trò là VPN client, thiết bị Internet Firewall đóng vai trò là VPN server. Khi một VPN client truy cập vào VPN Server, VPN Server yêu cầu xác thực thông tin người dùng (tài khoản, mã PIN, …). Sau khi xác thực thành công, VPN Server dùng kỹ thuật Tunneling, còn gọi là kỹ thuật "đường hầm", để tạo ra một mạng riêng ảo trên nền mạng Internet. Dữ liệu truyền giữa VPN Client và VPN Server được mã hóa riêng cho từng VPN Client.

Để giảm chi phí, thay vì thuê 2 đường truyền kết nối Internet, một đường dành riêng cho mạng LAN, một đường khác dành riêng cho các máy tính thực hành và mạng không dây WiFi, UKH sử dụng chung một đường truyền Internet cho cả hai mục đích này. Người dùng máy tính thực hành và người dùng mạng không dây WiFi của UKH được xem như người dùng từ môi trường Internet. Để thực hiện điều này, sử dụng một thiết bị định tuyến để phân đường truyền kết nối Internet từ ISP (Internet Service Provider) thành 2 nhánh, một nhánh nối vào cổng Outside của thiết bị Internet Firewall, một nhánh dành cho các máy tính thực hành và mạng không dây WiFi. Với cách kết nối này, toàn bộ lưu lượng truy cập Internet của các máy tính thực hành và mạng không dây WiFi không đi qua thiết bị Internet Firewall, do đó nâng cao hiệu quả truyền thông của mạng LAN và tránh nguy cơ gây mất an toàn thông tin từ mạng không dây WiFi.

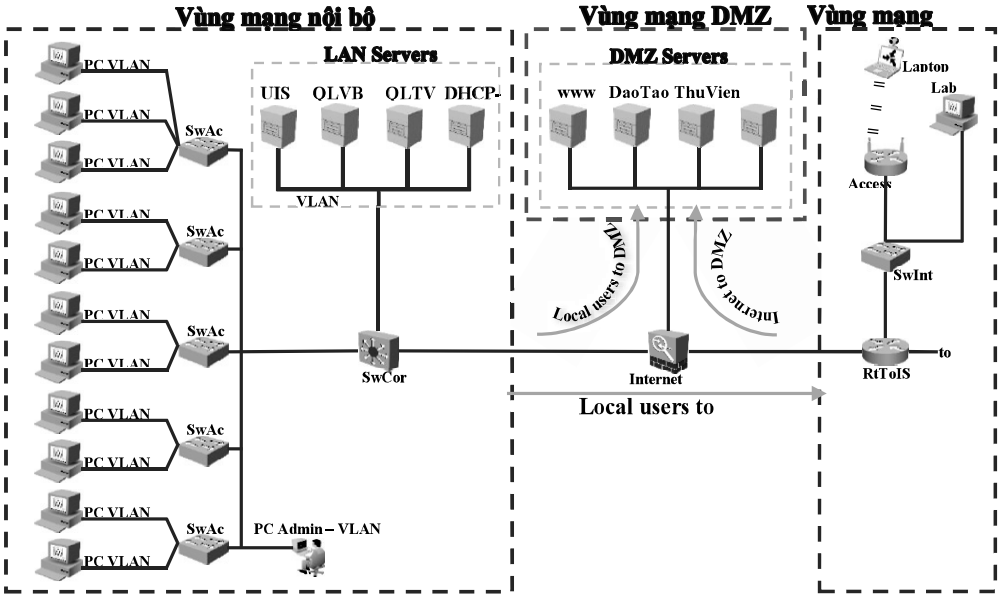
2.3. Mô hình mạng máy tính của UKH sau khi tái cấu trúc

Từ những phân tích nêu trên, mô hình mạng máy tính của UKH - sau khi tái cấu trúc - được trình bày trong Hình 3 dưới đây. Trong đó:

- Vùng mạng nội bộ được thiết kế theo kiến trúc Campus Two - Tier. Lớp truy nhập gồm 5 thiết bị switch layer 2 (từ SwAc1 đến SwAc5), có thể kết nối đến 120 máy tính (nếu dùng loại switch 24 cổng) hoặc 240 máy tính (nếu dùng loại switch 48 cổng) vào mạng LAN. Lớp lõi gồm 1 thiết bị switch layer 3 có tên là SwCore, kết nối 4 máy chủ nội bộ (LAN Servers) và định tuyến tất cả địa chỉ IP (Internet Protocol) của máy tính nội bộ về cổng Inside trên thiết bị Internet Firewall để sử dụng các dịch vụ mạng trên Vùng mạng DMZ và Vùng mạng Internet. Có 3 máy chủ chạy phần mềm ứng dụng quản lý dùng trong nội bộ, được xây dựng trên nền tảng Web (Web-Based Application), gồm: UIS (phần mềm quản lý đào tạo), QLVB (phần mềm quản lý văn bản và điều hành - eOffice), QLTV (phần mềm quản lý thư viện). Máy chủ DHCP-DNS cung cấp dịch vụ DHCP (Dynamic Host Configuration Protocol) để cấp địa chỉ IP tự động cho các máy trạm và dịch vụ DNS (Domain Name System) để phân giải tên miền cho mạng nội bộ, chuyển tiếp phân giải tên miền về máy chủ DNS của ISP để phân giải tên miền trên Vùng mạng Internet.

- Vùng mạng DMZ có 4 máy chủ (DMZ Servers) cung cấp thông tin và dịch vụ cho người dùng nội bộ và người dùng trên Internet, được xây dựng trên nền tảng Web, gồm: www (Website của UKH), DaoTao (cung cấp thông tin về đào tạo cho sinh viên), ThuVien (cung cấp thông tin trong Thư viện của UKH) và elearning (hỗ trợ đào tạo trực tuyến).

- Trong Vùng mạng Internet, thiết bị định tuyến RtToISP kết nối với mạng của ISP và phân đường truyền Internet thành 2 nhánh. Một nhánh nối vào cổng Outside trên thiết bị Internet Firewall. Nhánh còn lại nối vào switch có tên là SwInt để chia sẻ đường truyền Internet cho các máy tính thực hành và mạng không dây WiFi của UKH.



Hình 3: Mô hình mạng máy tính Trường Đại học Khánh Hòa

3. Lựa chọn phần mềm mô phỏng mạng máy tính

Hiện nay có nhiều phần mềm dùng để mô phỏng mạng máy tính [13]. Theo mục đích sử dụng, có thể phân những phần mềm này thành 2 nhóm: a) Nhóm định hướng về mô phỏng đánh giá hiệu năng mạng (ns2 [16], Omnet++ [17], Opnet [18], …), b)Nhóm định hướng về mô phỏng ứng dụng mạng (GNS3 [19], Boson NetSim [20], Cisco Packet Tracer, …).

Việc mô phỏng mạng máy tính của UKH trong bài báo này thuộc nhóm mô phỏng ứng dụng mạng. Bên cạnh mục tiêu chuẩn hóa để nâng cấp hệ thống mạng máy tính của UKH khi có điều kiện về tài chính, bài báo còn trình bày phương pháp mô phỏng một mô hình ứng dụng mạng máy tính cụ thể để sinh viên có điều kiện tiếp cận, vận dụng tổng hợp kiến thức về mạng máy tính đã học vào việc phân tích, thiết kế và quản trị mạng máy tính. Do đó, tiêu chí để chọn phần mềm mô phỏng trong bài báo này là: (1) Phù hợp điều kiện trang bị máy tính của sinh viên có cấu hình không cao; (2) Cho phép sử dụng miễn phí trong giáo dục; (3) Được sử dụng phổ biến ở các tổ chức đào tạo về mạng máy tính.

Trong nhóm các phần mềm mô phỏng ứng dụng mạng nêu trên, các phần mềm GNS3, Boson NetSim phải sử dụng hệ điều hành của thiết bị mạng thực để mô phỏng. Điều này tuy là ưu điểm, nhưng những phần mềm này không được phép cung cấp miễn phí hệ điều hành của thiết bị mạng thực. Mặt khác, vì dùng hệ điều hành của thiết bị mạng thực, nên khi mô phỏng mạng có nhiều thiết bị thì yêu cầu phần cứng của máy tính chạy mô phỏng phải có cấu hình cao và dung lượng RAM phải đủ lớn.

Phần mềm Cisco Packet Tracer [14, 15] phù hợp cả 3 tiêu chí chọn phần mềm mô phỏng ứng dụng mạng nêu trên. Phần mềm này được sử dụng cho các khóa học Cisco Networking, có đông đảo cộng đồng người sử dụng hỗ trợ lẫn nhau, được cung cấp miễn phí tại địa chỉ www.netacad.com, có phiên bản cho các hệ điều hành: Microsoft Windows 32 bit, Microsoft Windows 64 bit, Linux 64 bit, IOS và Android. Trên trang www.netacad.com, Cisco Packet Tracer được dùng cho các hoạt động học và đánh giá các khóa học: IT Essentials, CCNA Routing and Switching, CCNA Security, Introduction to IoT, IoT Fundamentals, Cybersecurity Essentials, Networking Essentials, Mobility Fundamentals.

Cisco Packet Tracer cung cấp giao diện đồ họa làm việc rất trực quan. Bằng các thao tác kéo - thả, nhấn chuột, người sử dụng dễ dàng khai báo và cấu hình các thiết bị mạng. Cisco Packet Tracer cung cấp các giao thức định tuyến: Static, RIP, OSPF, EIGRP và BGP. Về thiết bị, Cisco Packet Tracer cho phép khai báo và cấu hình các thiết bị chuyển mạch, định tuyến, tường lửa, WiFi, các thiết bị trong lĩnh vực IoT (Internet of Things) hoặc lĩnh vực Smart Home có hệ điều hành tương đương với hệ điều hành trên thiết bị thực. Về dịch vụ mạng, Cisco Packet Tracer cho phép khai báo và cấu hình các máy chủ dịch vụ mạng: DNS, DHCP, DHCPv6, HTTP, HTTPS, FTP, EMAIL, AAA (Access control, Authentication, Auditing), NTP (Network Time Protocol), IoT.

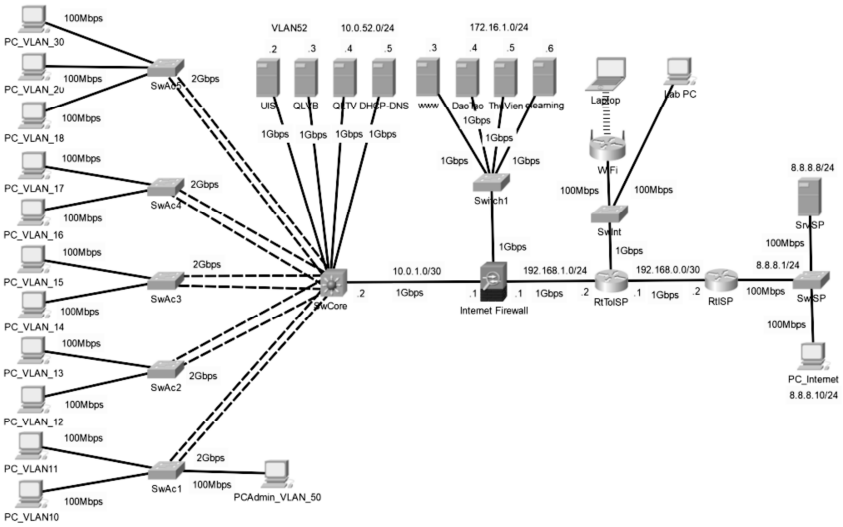
4. Cấu hình thiết bị mạng trên phần mềm mô phỏng Cisco Packet Tracer

Mô hình mạng máy tính trong Hình 3 được thiết lập trong Cisco Packet Tracer như Hình 4 dưới đây. Trong đó, phần mô phỏng mạng Internet gồm các thiết bị: định tuyến RtISP, chuyển mạch SwISP, máy chủ SrvISP chạy dịch vụ DNS của ISP và mô phỏng trang web google.com, máy tính PC Internet đại diện cho người dùng mạng Internet.

Sơ đồ trong Hình 4 dùng 3 lớp địa chỉ IPv4 dành riêng. Mỗi VLAN trong Vùng mạng nội bộ sử

dụng lớp địa chỉ dành riêng của lớp mạng A theo quy tắc 10.0.VLAN-ID.0/24 (VLAN-ID được phân bổ trong cột cuối của Bảng 1). Vùng mạng DMZ sử dụng lớp địa chỉ dành riêng của lớp mạng B với địa chỉ mạng là 172.16.1.0/24. Vùng mạng Internet sử dụng lớp địa chỉ dành riêng của lớp mạng C (192.168.x.0/24, với x = 0, 1, 2,…).

Các máy chủ trong Vùng mạng nội bộ (LAN Servers) và Vùng mạng DMZ (DMZ Servers) được khai báo giả lập các dịch vụ mạng mà nó đảm nhận.



Hình 4: Sơ đồ kết nối mạng máy tính Trường Đại học Khánh Hòa

Trong Vùng mạng nội bộ, để thuận tiện cho việc cấu hình và quản lý các VLAN, sử dụng giao thức VTP (VLAN Trunking Protocol) với VTP Server được khai báo ở SwCore. Các switch còn lại trong Vùng mạng nội bộ được khai báo là VTP Client. Trong giao thức VTP, chỉ cần khai báo một lần các VLAN ở VTP Server, các VTP Client tự động được đồng bộ thông tin về VLAN từ VTP Server.

Việc vận chuyển các gói tin của các VLAN từ lớp truy nhập về lớp lõi được thực hiện theo nguyên lý Trunking, nghĩa là trung chuyển các gói tin cho các VLAN. Trên thiết bị switch, các cổng dùng để kết nối với máy tính được gọi là cổng truy cập (Access Port), được gán vào các VLAN; các cổng dùng để trung chuyển các gói tin cho các VLAN gọi là Trunking Port. Công nghệ EtherChannel của Cisco cho phép "bó" từ 2 đến 8 cổng mạng trên một thiết bị switch thành một Logic Trunking Port để tăng tốc độ trung chuyển gói tin và dự phòng cho sự cố đường truyền. Khi một kết nối vật lý tham gia trong Logic Trunking Port bị ngắt kết nối (hỏng cổng mạng, hỏng cáp mạng, …), tốc độ truyền gói tin qua Logic Trunking Port sẽ bị giảm, nhưng vẫn đảm bảo việc vận chuyển gói tin qua nó. Đây là ưu điểm và cần được áp dụng trong mạng LAN. Trong Hình 4, các thiết bị switch trong lớp truy nhập sử dụng 2 cổng mạng tốc độ 1Gbps để tạo thành một cổng Logic Trunking Port tốc độ 2Gbps kết nối về SwCore.

Thiết bị SwCore thực hiện chức năng định tuyến cho tất cả các VLAN trong mạng. Việc định tuyến này dẫn đến tình trạng các VLAN có thể truyền thông với nhau. Để tăng cường an ninh mạng, cần thiết lập chính sách an ninh để: (1) người sử dụng trong một VLAN không truy cập được thiết bị mạng trên các VLAN khác của người sử dụng, nhưng truy cập được các máy chủ nội bộ; (2) những máy chủ ứng dụng chỉ được phép sử dụng trong một vài VLAN thì thực hiện cấm truy cập vào chúng trong các VLAN không được phép truy cập. UKH có máy chủ nội bộ chạy ứng dụng Quản lý thư viện, chỉ dùng trong Thư viện, không cho phép các đơn vị khác sử dụng. Để thực hiện chính sách an ninh này, sử dụng ACLs (Access control lists) cho từng VLAN của người sử dụng để lọc và chặn (deny) các gói tin xuất phát từ các địa chỉ IP của VLAN đó đến các địa chỉ IP cần chặn trong mạng LAN, và cho phép (permit) truy cập đến các địa chỉ IP đích khác. Chính sách an ninh này đã ngăn chặn việc chuyển gói tin từ nguồn truy cập, cắt giảm đáng kể lưu lượng truyền thông không cần thiết, góp phần nâng cao hiệu quả truyền thông của mạng LAN.

Có 2 loại ACLs là Standard và Extended. Standard ACLs chỉ lọc các gói tin dựa vào địa chỉ IP nguồn của gói tin, không thể sử dụng cho chính sách an ninh nêu trên. Extended ACLs cho phép lọc các gói tin theo địa chỉ IP nguồn, địa chỉ IP đích, giao thức, chỉ số cổng ứng dụng của gói tin, vì vậy, nó phù hợp cho chính sách an ninh nêu trên. Mỗi ACLs là một danh sách tuần tự các câu lệnh, gọi là ACEs (Access Control Entries), để áp dụng trên một Interface nào đó. ACLs được kiểm tra tuần tự các ACEs từ trên xuống, nên khi tạo ACLs cần đảm bảo các ACEs ở trên không phủ định các ACEs ở dưới, các ACEs cụ thể đặt ở trên, các ACEs chung chung đặt bên dưới. Sau đây là các lệnh cấu hình ACLs cho VLAN**16** (Phòng Tổ chức và Hành chính) nhằm ngăn chặn việc truy cập vào máy chủ ứng dụng Quản lý thư viện (có địa chỉ IP là 10.0.52.4/24), ngăn chặn việc truy cập vào các VLAN của người sử

dụng khác, cho phép truy cập các địa chỉ mạng khác (không bị cấm):

```
ip access-list extended ACLVLAN16
deny ip 10.0.16.0 0.0.0.255 host 10.0.52.4
deny ip 10.0.16.0 0.0.0.255 10.0.10.0 0.0.0.255
…
deny ip 10.0.16.0 0.0.0.255 10.0.50.0 0.0.0.255
permit icmp 10.0.16.0 0.0.0.255 any
permit ip 10.0.16.0 0.0.0.255 any
int vlan 16
ip access-group ACLVLAN16 in
```

Để vận chuyển toàn bộ lưu lượng truy cập từ Vùng mạng nội bộ, thông qua thiết bị Internet Firewall, ra Vùng mạng DMZ và Vùng mạng Internet, một cổng trên SwCore được chuyển sang chế độ no switchport để cho phép gán địa chỉ IP cho nó. Cổng này nối về cổng Inside trên thiết bị Internet Firewall để định tuyến và vận chuyển toàn bộ truy cập từ Vùng mạng nội bộ ra Vùng mạng DMZ và Vùng mạng Internet.

Thiết bị Internet Firewall được thiết lập mặc định hoạt động theo cơ chế đóng, nghĩa là nó đóng tất cả các dịch vụ mạng, không cho phép truy cập từ vùng mạng có cấp bảo mật thấp đến vùng mạng có cấp bảo mật cao. Để đảm bảo an ninh mạng, thiết bị Internet Firewall được thiết lập cấp độ bảo mật (security level) cho cổng Inside ở cấp cao nhất, cổng Outside ở cấp thấp nhất, và cổng DMZ nằm ở mức giữa. Để người dùng từ Vùng mạng nội bộ truy cập được dịch vụ mạng trên Vùng mạng DMZ và Vùng mạng Internet, phải mở các dịch vụ mạng cho phép truy cập trên chiều vào (in) của cổng Inside và Dynamic NAT (Network Address Translation) tất cả địa chỉ IP người dùng trong Vùng mạng nội bộ thành các địa chỉ IP trên lớp mạng của cổng Outside. Để người dùng từ Vùng mạng Internet truy cập được các dịch vụ mạng trong Vùng mạng DMZ, thực hiện Static NAT từng địa chỉ IP của máy chủ trong Vùng mạng DMZ thành địa chỉ IP trên lớp mạng của cổng Outside và thiết lập Extended ACLs trên chiều vào (in) của cổng Outside để cho phép truy cập các dịch vụ mạng trên Vùng mạng DMZ từ Vùng mạng Internet. Ngoài ra, cần thiết lập dịch vụ Clientless SSL VPN trên thiết bị Internet Firewall để cho phép người dùng UKH truy cập các máy chủ nội bộ từ Vùng mạng Internet thông qua kết nối VPN với giao thức bảo mật SSL (Secure Sockets Layer) của trình duyệt web.

5. Kết quả mô phỏng và thảo luận

Quá trình mô phỏng được thực hiện thông qua việc cấu hình và kiểm tra kết quả cấu hình các thiết bị mạng trên sơ đồ Hình 4 trong phần mềm Cisco Packet Tracer. Kết quả kiểm tra cho thấy việc cấu hình hệ thống mạng hoạt động đáp ứng các yêu cầu đề ra: (1) trong Vùng mạng nội bộ, từ một VLAN không thể truy cập vào thiết bị mạng trên VLAN khác; từ VLAN của Thư viện truy cập được máy chủ Quản lý thư viện, nhưng từ các VLAN khác thì bị cấm truy cập vào máy chủ này; toàn bộ người dùng trong Vùng mạng nội bộ truy cập được các dịch vụ mạng trên các máy chủ nội bộ, trên Vùng mạng DMZ và Vùng mạng Internet; (2) người dùng từ Vùng mạng Internet truy cập được các dịch vụ mạng trong Vùng mạng DMZ, sử dụng giao thức https trên trình duyệt web và nếu cung cấp đúng tài khoản truy cập VPN thì truy nhập được các dịch vụ mạng trên các máy chủ nội bộ.

Kết quả mô phỏng mạng máy tính của UKH trên đây còn cho thấy kết quả áp dụng phương pháp giảng dạy theo hướng tiếp cận và giải quyết vấn đề từ thực tiễn, đủ điều kiện vận dụng trong phương pháp dạy học dựa trên giải quyết vấn đề [7, 9], đã được thực nghiệm bởi [8] cho kết quả đào tạo tốt hơn các phương pháp dạy học truyền thống.

6. Kết luận

Xuất phát từ nhu cầu ứng dụng mạng máy tính của Trường Đại học Khánh Hòa trong thực tế và việc vận dụng tổng hợp các kiến thức nền tảng về mạng máy tính (thiết kế mạng LAN, chuyển mạch và định tuyến, dịch vụ mạng, an toàn mạng, …) trong giảng dạy lý thuyết và thực hành cho sinh viên ngành công nghệ thông tin, bài báo đã phân tích, đánh giá thực trạng, đề xuất mô hình tái cấu trúc mạng máy tính của Trường Đại học Khánh Hòa và mô phỏng hoạt động của mô hình này trên phần mềm Cisco Packet Tracer. Kết quả mô phỏng không chỉ chứng tỏ khả năng ứng dụng hữu hiệu của kỹ thuật, phần mềm mô phỏng, mà còn có thể dùng làm bài tập thực hành giúp sinh viên từng bước hoàn thiện và nâng cao kỹ năng quản trị mạng máy tính. Để nâng cao kỹ năng nghề cho sinh viên, đáp ứng yêu cầu ứng dụng mạng máy tính của xã hội, cần có thêm các bài tập thực hành mô phỏng mạng máy tính của các tổ chức khác, đặc biệt là nhóm các doanh nghiệp nhỏ và vừa (chiếm tỷ trọng trên 97% doanh nghiệp ở Việt Nam). Cách tiếp cận và giải quyết vấn đề mô phỏng mạng máy tính Trường Đại học Khánh Hòa của bài báo có thể áp dụng để mô phỏng mạng máy tính của các tổ chức khác.

TÀI LIỆU THAM KHẢO

[1] Võ Thị Hà, *Thiết kế mạng CAMPUS theo công nghệ CISCO*, 2009.
[2] Trung tâm Khoa học Tự nhiên và Công nghệ quốc gia - Viện công nghệ thông tin, *Giáo Trình Thiết Kế Mạng LAN – WAN*, 2004.
[3] Ngô Bá Hùng, *Giáo Trình Thiết Kế & Cài Đặt Mạng*, Đại học Cần Thơ, 2005.
[4] Học viện mạng Quốc tế NETPRO - ITI Viện CNTT, *Giáo trình Thiết kế và xây dựng mạng LAN và WAN*, Hà Nội, 2011.
[5] Nguyễn Hồng Sơn, *Giáo trình hệ thống mạng máy tính CCNA*, Nhà xuất bản Lao động Xã hội, 2006.
[6] Tổng cục Dạy nghề - Bộ LĐTB&XH, *Giáo trình An toàn mạng*, 2013.
[7] Lê Huy Hoàng, *Dạy học dựa trên giải quyết vấn đề*, NXB Giáo dục, 2010.
[8] Hoàng Thị Hồng, Lê Huy Tùng, *Vận dụng dạy học dựa trên vấn đề trong giảng dạy môn kỹ thuật điện*, Tạp chí Khoa học Đại học Quốc gia Hà Nội, tập 32, số 2 (2016) trang 9-14.
[9] Barrows, H. Kelson, *A. Problem-based Learning: A Total Approach to Education*, Illinois University Press, 1993.
[10] Diane Teare (2005), *Campus Network Design Fundamentals Catherine Paquet,* Copyright©2006 Cisco Systems, Inc. Published by: Cisco Press.
[11] Marwan Al-shawi, *CCDE Study Guide*, *Consider design options for modern campus networks*, Published Oct 2, 2015 by Cisco Press, ISBN-10:1-58714-461-1.
[12] Jazib Frahim, *Cisco ASA All-in-One Firewall, IPS, and VPN Adaptive Security Appliance*, The Third Edition, Published by: Cisco Press.
[13] A.M Law and W.D Kelton, *Simulation Modelling and Analysis*, Third Edition, Mc Graw Hill, 2000.
[14] Cisco, *Cisco Packet Tracer Data Sheet,* 2010.
[15] www.netacad.com/courses/packet-tracer.
[16] www.isi.edu/nsnam/ns/.
[17] www.omnetpp.org.
[18] www.Opnet.com.
[19] www.gns3.com.
[20] www.boson.com/netsim-cisco-network-simulator.

NETWORK SIMULATION OF UNIVERSITY OF KHANH HOA

Tran Cong Can

University of Khanh Hoa

Abstract:

In fact, new information technology graduates are often faced with difficulties in managing computer networks of organizations (enterprises, government agencies, ...). Therefore, it is necessary to develop practical exercises on the application of computer networks of organizations, thereby helping students improve computer network management skills. Due to budget constraints, it is unworkable to have a fully device equipped lab. Meanwhile, computer network simulation software allows to simulate a network system equivalent computer network system in reality. In this article, the author simulates the computer network of Khanh Hoa of University. Simulation results not only demonstrate the applicability of technique, simulation software, but also can be used as a exercise about simulation of computer network, helping students approach analytical method, designing, setup a computer network of an organization in reality.

Keywords: *computer network, network simulation, network security.*