ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC - KỸ THUẬT MÁY TÍNH

Assignment 2: Computer Network

ĐỀ TÀI

Computer Network
Design for the building of a Company

GVHD: Lê Bảo Thịnh
SV: Chế Lan Hải - 2013063
Nguyễn Trường Sơn - 2112200
Vũ Lâm Hoàng Đại - 2110992

TP. HỒ CHÍ MINH, THÁNG 5/2023

Mục lục

1 Yêu cầu hệ thống

1.1 Yêu cầu hệ thống mạng

1.1.1 Tại trụ sở

-Trụ sở là một tòa cao ốc gồm 7 tầng, tầng 1 được trang bị 1 phòng IT (phòng kỹ thuật mạng) và Cabling Central Local(Phòng tập trung dây mạng và patch panels).
- Thiết kế theo kiểu Small Enterprise: 200 workstations, 5 servers, 12 network devices (hoặc nhiều thiết bị hơn dành cho các thiết bị bảo mật mạng đặc trưng).
-Sử dụng các công nghệ mới cho cơ sở hạ tầng mạng bao gồm kết nối có dây và không dây, và cáp quang (GPON). Mạng được tổ chức theo cấu trúc VLAN và GigaEthernet 1GbE/10GbE.
- Mạng kết nối với bên ngoài thông qua 2 Leased Line để kết nối mạng rộng (WAN) (có thể áp dụng SD-WAN) và 2 đường xDSL (cho truy cập Internet) với cơ chế cân bằng tải.
- Dùng kết hợp giữa Licensed và Open source Softwares, ứng dụng office, ứng dụng client-server, multimedia và database.
- Yêu cầu tính bảo mật cao, an toàn khi xảy ra sự cố, dễ dàng nâng cấp hệ thống.

1.1.2 Tại chi nhánh

Mỗi chi nhánh của công ty (ở Đà Nẵng, Nha Trang) cũng được thiết kế tương tự như Trụ sở chính nhưng có quy mô nhỏ hơn:
- Tòa cao 2 tầng, tầng 1 được trang bị 1 phòng IT (phòng kỹ thuật mạng) và Cabling Central Local(Phòng tập trung dây mạng và patch panels).
- BB dạng chi nhánh: 30 workstations, 3 servers, 5 hoặc nhiều thiết bị mạng hơn.

1.1.3 Yêu cầu chung về thông lượng hệ thống

Các thông số về lưu lượng và tải của hệ thống (tập trung khoảng 80% vào giờ cao điểm 9h-11h và 15-16h) có thể dùng chung cho Trụ sở và Chi nhánh như sau:
- Servers dùng cho cập nhật, truy cập web, truy cập cơ sở dữ liệu,... Tổng dung lượng upload và download vào khoảng 1000MB/ngày.
- Mỗi workstation dùng cho duyệt Web, tải tài liệu, giao dịch khách hàng,... Tổng dung lượng upload và download vào khoảng 500MB/ngày.
- Máy laptop kết nối WiFi dùng cho khách hàng truy xuất khoảng 1000MB/ngày.
- Cấu hình VPN cho site-to-site và cho teleworker kết nối với mạng LAN

Mạng máy tính của công ty BB ước tính tăng trưởng 20% trong 5 năm (năm về số lượng người dùng, tải mạng, phát triển thêm nhánh,..).

2 Phân tích và đề nghị giải pháp

2.1 Khảo sát tại vị trí cài đặt

2.1.1 Tại trụ sở

Sau khi khảo sát các công ty có cùng quy mô, nhóm quyết định chia trụ sở chính sẽ chứa các phòng ban tương ứng với các tầng với quy mô trụ sở gồm 200 workstation, 5 server, 12 (hoặc nhiều hơn) thiết bị mạng được bố trí trong một tòa nhà 7 tầng:

Phòng kỹ thuật tại tầng 1:

- Tầng 1 của trụ sở chính được bố trí làm nơi giao dịch với khách hàng (gồm bộ giao dịch và bộ phận tiếp tân). Bên cạnh đó, trụ sở còn bố trí thêm một lượng máy tính nhằm phục vụ khách hàng có nhu cầu tra cứu thông tin tài khoản,...

- Đối với bộ phận giao dịch và tiếp tân, mỗi nhân viên sẽ được trang bị 1 PC (có phần mềm kết nối với máy chủ để thực hiện các truy vấn). Do nhu cầu công việc, độ bảo mật phải đặt lên hàng đầu, nhưng cấu hình PC ở mức độ chấp nhận được.

- Đối với hệ thống máy tính dành cho khách hàng thì chỉ được kết nối internet (không được phép kết nối với các máy trong hệ thống). Bên cạnh hệ thống máy tính này, công ty còn cung cấp wifi cho khách hàng truy cập bằng các thiết bị di động, các thiết bị này cũng chỉ được chia sẻ kết nối internet chứ không được phép kết nối với các máy trong hệ thống

- Tầng 1 còn có 2 phòng kỹ thuật: phòng IT dành cho bộ phận IT của công ty và phòng tập trung dây mạng và patch panel (nơi tập trung các thiết bị mạng, server, dây nối,...) Đối với bộ phận IT, đây là nơi quản lí toàn bộ server, hệ thống mạng của công ty nên độ bảo mật phải cao, thêm vào đó cấu hình của máy tính và tốc độ đường truyền phải mạnh.

-Chứa 4 server của trụ sở và các Router, Switch,...

**Các tầng nhân sự 2,3,4,5,6:*

- Đối với các phòng ban này, mỗi nhân viên sẽ được trang bị một máy tính có cấu hình khá, được kết nối internet. Các máy được chia thành từng nhóm ứng với các phòng ban nhằm dễ quản lí.

- Mỗi phòng ban còn được trang bị 2 máy in nhằm vụ công việc in ấn báo cáo của phòng ban đó.

**Phòng giám đốc tại tầng 7:*

- Mỗi phòng sẽ được trang bị 5 máy tính (2 dành cho giám đốc/quản trị ; 3 dành cho thư kí). Do máy tính của giám đốc và quản trị có chứa các tài liệu quan trọng nên độ bảo mật phải cao.

- Ngoài ra, công tycòn trang bị hai phòng họp tại tầng này. Mỗi phòng gồm 5 máy tính. Các máy tính này nhằm mục đích thuyết trình, báo cáo nên độ bảo mật không cao và cấu hình tương đối

Như vậy, trung bình mỗi tầng có 30 workstation,mỗi tầng còn có một phòng đặt các switch dùng cho việc kết nối các máy tính ở tầng này vào hệ thống (8 Switch Layer 2)

Đặt 1 switch layer 3 kết nối với tất cả 7 switch layer 2 trong trụ sở chính.

Đặt 1 Access Point tại tầng 1 để hỗ trợ việc truy cập internet của khách hàng và nhân viên.

2.1.2 Tại chi nhánh

Sau khi khảo sát các công ty có cùng quy mô, nhóm quyết định chia chia nhánh thành các tầng với quy mô với mỗi chi nhánh gồm 30 workstation, 3 server và 5 (hoặc nhiều hơn) thiết bị mạng được bố trí trong tòa nhà 2 tầng.

Phòng kỹ thuật ở tầng 1: Quy mô tương tự phòng 1 của trụ sở chính nhưng nhỏ hơn. Chứa cả 3 server và router, switch,... *Các phòng ban còn lại và phòng giám đốc ở tầng 2:* Quy mô tương tự phòng 7 của trụ sở chính nhưng nhỏ hơn, đi kèm với một số phòng ban nhỏ khác. Chứa cả 3 server và router, switch,...

Đặt 1 switch layer 3 để kết nối với tất cả switch layer 2 tại chi nhánh.

Đặt 3 switch layer 2 tại tầng 1,2 để kết nối các workstation trong hệ thống của chi nhánh.

Tầng 1 có khoảng 12 workstation, Tầng 2 có khoảng 18 workstation

2.2 Thiết kế cấu trúc mạng phù hợp

2.2.1 Quản lý mô hình

Hệ thống mạng sẽ được xây dựng theo mô hình cilent-server với sự bố trí theo TOPO hình sao, vì:

- Theo như mô tả của hệ thống công ty BB, server thực hiện quản lý và lưu trữ dữ liệu, trong khi cilent truy cập và sử dụng dữ liệu khi cần. Kiến trúc cilent-server lý tưởng cho các mạng có nhiều máy khách, đặc biệt như mạng Công ty BB, nơi nhiều người dùng cần truy cập dữ liệu và ứng dụng đồng thời. Vì vậy kiến nghị sử dụng mô hình cilent-server cung cấp khả năng quản lý và kiểm soát tập trung, giúp quản lý mạng dễ dàng hơn và đảm bảo tính bảo mật và toàn vẹn của dữ liệu.

-TOPO hình sao là một thiết kế mạng trong đó tất cả các thiết bị được kết nối với một trung tâm hoặc bộ chuyển mạch trung tâm, tạo thành một mẫu hình ngôi sao. Trong cấu trúc liên kết này, dữ liệu di chuyển từ thiết bị khách đến trung tâm/công tắc trung tâm, sau đó đến thiết bị đích. Thiết kế này được sử dụng rộng rãi trong mạng LAN vì nó mang lại độ tin cậy cao và xử lý sự cố dễ dàng. Nếu bất kỳ thiết bị nào trong mạng bị lỗi, nó không ảnh hưởng đến các thiết bị khác và rất dễ xác định và khắc phục sự cố. Nhờ đó, với hệ thống lớn như của công ty BB, việc sử dụng cấu trúc này sẽ đảm bảo liên lạc đáng tin cậy giữa các thiết bị, đồng thời dễ dàng xác định và giải quyết các sự cố mạng.

2.2.2 Quản lý hệ thống server

- Hệ thống máy chủ được đặt tại phòng kỹ thuật gồm:

+ Máy chủ web (Web Server) là máy chủ mà trên đó cài đặt phần mềm phục vụ web cho khách hàng,..

+ Máy chủ Mail: để gửi-nhận thư điện tử..

+ Máy chủ FTP (FTP server): FTP (File Transfer Protocol) được dùng để trao đổi tập tin qua mạng lưới truyền thông dùng giao thức TCP/IP (chẳng hạn như Internet - mạng ngoại bộ - hoặc intranet - mạng nội bộ)

+ Máy chủ DNS (DNS Server) là máy chủ phân giải tên miền. Hệ thống tên miền DNS (Domain Name System) được sử dụng để ánh xạ tên miền thành địa chỉ IP.

2.2.3 Quản lý kết nối

- Trong mạng sử dụng Switch Layer 3 để kết nối với hệ thống Server và workstation thông qua các switch layer 2. 7 Switch Layer 2 ở trụ sở chính hay 3 Switch Layer 2 ở chi nhánh kết nối vào Switch Layer 3. Đường kết nối từ Switch Layer 2 và Access Point đến Switch Layer 3 bằng Cáp quang để đảm bảo chất lượng và tốc độ đường truyền. - Kết nối từ chi nhánh khác đi vào hệ thống mạng công ty thông qua đường leased line do ISP cung cấp.

- Kết nối với internet phục vụ các nhu cầu của khách hàng, và giải trí của nhân viên công ty,... không được kết nối vào hệ thống mạng của công ty để đảm bảo an ninh. Kết nối này được truyền qua đường DSL do ISP cung cấp.

3 Danh sách các trang thiết bị tối thiểu, sơ đồ IP và sơ dồ đi dây

3.1 Danh sách các thiết bị mạng và đặc điểm kỹ thuật điển hình

Router: là thiết bị định tuyến, xác định một số thông tin như là thông tin của người gửi, kiểu dữ liệu, kích thước dữ liệu nhưng quan trọng là địa chỉ IP đích để nó thực hiện nhiệm vụ là xác định đường đi tốt nhất cho thông tin gửi đi. Ta chọn Router CISCO 1941/K9 vì router này cung cấp dịch vụ bảo mật dữ liệu cao, tính di động cao và các dịch vụ ứng dụng.
Đặc tính kỹ thuật:

- Manufacturer: Cisco Systems, Inc.
- Manufacturer Part Number: CISCO1941/K9.
- Product Type: Router.
- Form Factor: External - modular - 2U
- Services and Slot Density:
  - Embedded hardware-based crypto acceleration (IPSec): Yes.
  - Total Onboard Gigabit Ethernet 10/100/1000 WAN ports: 2.
  - RJ-45-Based Ports: 2.
  - EHWIC Slots: 2.
  - Double-wide EHWIC slots: 1.
  - ISM Slots: 1
  - DRAM Memory: 512 MB (installed) / 2 GB (max).
  - Flash Memory: 256 MB (installed) / 8 GB (max).
  - Serial Console Port: 1
  - Serial Auxiliary Port: 1
  - Power Supply Options: AC, POE
- Routing Protocol: OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, static IPv4 routing, static IPv6 routing.
- Data Link Protocol: Ethernet, Fast Ethernet, Gigabit Ethernet.
- Network/Transport Protocol: IPSec.
- Remote Management Protocol: SNMP, RMON.
- Features: Cisco IOS IP Base , firewall protection, VPN support, MPLS support, Syslog support, IPv6 support, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED).
- Compliant Standards: IEEE 802.3ah, IEEE 802.1ah, IEEE 802.1ag.
- Power: AC 100/240 V (47-63 Hz).

- Dimensions (WxDxH): 34.3 x 29.2 x 8.9 cm.
- Weight: 5.8 kg.

Access-point: Có tất cả là 2 access-point cho trụ sở chính, phục vụ cho nhu cầu giải trí cũng như là truy xuất thông tin của khách hàng. Ưu điểm của nó là đảm bảo tính tiện lợi khi truy cập mạng mà không thông qua hệ thống dây mạng. Ta chọn Cisco-Linksys WRT300N Wireless-N Broadband Router.

- Thông lượng: 540 Mbps.
- Xử lý thông tin với Layer 7 application fingerprinting và QoS.
- Tích hợp với firewall.
- Air Marshal: thời gian thực WIPS (hệ thống ngăn chặn xâm nhập không dây) cùng với báo động.
- Mỗi thiết bị được thiết kế cho việc truy cập mật độ cao với hơn 100 người dùng/thiết bị mà không xảy ra nghẽn cổ chai, hay bị treo bộ xử lý như các sản phẩm thông thường. Ngoài ra thiết bị có công nghệ traffic shapping nhằm đảm bảo băng thông được chia sẻ công bằng giữa các người dùng.
- Với công nghệ Plug and Play, người quản trị chỉ cần làm cắm thiết bị mới vào nguồn điện, thiết bị này sẽ tự động dò sóng của các thiết bị cùng mạng và truyền tiếp sóng tạo vùng phát sóng mở rộng mà không cần phải qua các bước cấu hình phức tạp.
- Với công nghệ Plug and Play, người quản trị chỉ cần làm cắm thiết bị mới vào nguồn điện, thiết bị này sẽ tự động dò sóng của các thiết bị cùng mạng và truyền tiếp sóng tạo vùng phát sóng mở rộng mà không cần phải qua các bước cấu hình phức tạp
- Tránh được lỗi cấu hình thường gặp của hầu hết các mạng wireless hiện nay: các thiết bị không có controller khi được thiết lập cùng băng tần có vị trí gần nhau sẽ làm nhiễu sóng lẫn nhau, ảnh hưởng lớn đến hiệu suất và độ ổn định của mạng không dây.

Switch layer 2: hoạt động trên tầng 2 của mô hình OSI tức là tầng data link được dùng để gửi các frame đến cổng đích sử dụng địa chỉ MAC thông qua bảng lưu trữ địa chỉ MAC của thiết bị được liên kết với cổng đó.Ta chọn CISCO WS-C2960+24TT-L.

- Manufacturer: Cisco Systems, Inc.
- Manufacturer Part Number: Cisco WS-C2960-24TT-L.
- Product Type: Switch - 24 ports - Managed.
- Enclosure Type: Rack-mountable 1U.
- Giao diện Uplink: 2 (SFP or 1000BASE-T).
- Ports: 24 x 10/100Mbps Ethernet.
- Chuyển tiếp băng thông: 16 Gbps.
- DRAM: 128 MB.
- Flash Memory: 64 MB.

- Protocols: SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH.
- Compliant Standards: IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ab (LLDP).
- Khả năng sẵn sàng cao / Khả năng đáp ứng cao: PVST, Chặn phát sóng, Ngắt Unicast, Chặn Mulitcast, Spanning Tree, Portfast, Fast Uplink, Xương sống nhanh, 802.1s, 802.1w.
- Các tính năng quản lý: SPAN, CiscoView, Giao thức Khám phá của Cisco (CDP),Giao thức Trunking Ảo (VTP), Khách hàng Telnet, BOOTP, TFTP, CiscoWorks, CWSI, RMON, SNMP, Clustering, Quản lý Web.
- Thông lượng: 6.5 Mbps.
- Power: AC 120/230 V (50/60 Hz).
- Dimensions (WxDxH) 44.5 cm x 23.6 cm x 4.4 cm
- Weight 3.63 kg

Switch layer 3: Với 24 port nó kết nối các switch lại với nhau, làm cho chúng có thể hoạt động song song cùng lúc với nhau nhằm mục đích đạt được tốc độ cao khi xử lý dữ liệu. Switch layer 3 hoạt động trên tầng network của mô hình OSI, được gắn thêm bảng định tuyến IP, đóng vai trò giống như một router nhưng không có cổng WAN có chức năng định tuyến các gói tin bằng cách sử dụng địa chỉ IP, được sử dụng rộng rãi để chia VLAN. Ta chọn Cisco WS-C3650-24PS-S.

- Manufacturer: Cisco Systems, Inc
- Manufacturer Part Number: Cisco WS-C3560V-24PS-S.
- Enclosure Type: Rack-mountable 1U.
- Cổng: 24 cổng 10/100/1000 Ethernet.
- Số xếp chồng tối đa: 9.
- Stack băng thông: 160 Gpbs
- Chuyển tiếp băng thông: 41,66Mpps.
- Chuyển đổi công suất: 88 Gb / s
- RAM: 4 GB.
- Bộ nhớ flash: 2 GB.
- Số AP cho mỗi switch / stack: 25.
- Số lượng khách hàng không dây trên mỗi switch / stack: 1000.
- Routing Protocol: RIP-1, RIP-2, Static IP.

- Features: Chuyển đổi lớp 3, nhận diện tự động trên mỗi thiết bị, hỗ trợ DHCP, tự động đàm phán, cân bằng tải, hỗ trợ VLAN, tự động liên kết (MDI / MDI-X), IGMP snooping, Hệ thống Phát hiện xâm nhập (IDS), lọc địa chỉ MAC, IPv6 Hỗ trợ Giao thức Hỗ trợ Trunking Protocol (STP), DHCP snooping, Hỗ trợ DTP, Hỗ trợ Giao thức Hỗ trợ Giao thức Kết nối Cổng (PAgP), Hỗ trợ TFTP, Access Control List (ACL), Quality of Service (QoS), hỗ trợ Jumbo Frames, Dynamic ARP Inspection (DAI), Time Reflectometry Thời gian (TDR).
- Compliant Standards: IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s
- Power: AC 120/230 V (50/60 Hz).
- Dimensions (WxDxH): 44,3 x 29,5 x 4,4 cm.
- Weight: 4.6 kg.

3.2 Sơ đồ hệ thống

4 Tính toán các thông số cho mạng máy tính

4.1 Throughput và Bandwidth

4.1.1 Trụ sở chính

Mạng có dây:

- 5 server với tổng dung lượng download và upload là 1000MB/ngày. Tổng thời gian vào giờ cao điểm là 3 giờ. Giờ cao điểm tập trung 80% trong ngày:

$$\text{Bandwidth} = \frac{5\times1000\times0.8\times8}{3\times3600} = 2.96 \text{ (Mbps)}$$
$$\text{Throughput} = \frac{5\times1000\times8}{8\times3600} = 1.39 \text{ (Mbps)}$$

- 200 workstations với tổng dung lượng download và upload là 500MB/ngày. Tổng thời gian vào giờ cao điểm là 3 giờ. Giờ cao điểm tập trung 80% trong ngày

$$\text{Bandwidth} = \frac{200\times500\times0.8\times8}{3\times3600} = 59.3 \text{ (Mbps)}$$
$$\text{Throughput} = \frac{200\times500\times8}{8\times3600} = 27.8 \text{ (Mbps)}$$

Mạng không dây:

- Máy laptop kết nối Wifi dùng cho khách hàng truy xuất khoảng 1000MB/ngày Tổng thời gian vào giờ cao điểm là 3 giờ. Giờ cao điểm tập trung 80% trong ngày. Giả sử rằng trong ngày có khoảng 100 lượt truy cập thường xuyên.

$$\text{Bandwidth} = \frac{100\times1000\times0.8\times8}{3\times3600} = 59.3 \text{ (Mbps)}$$
$$\text{Throughput} = \frac{100\times1000\times8}{8\times3600} = 27.8 \text{ (Mbps)}$$

4.1.2 Chi nhánh

Mạng có dây:

- 3 server với tổng dung lượng download và upload là 1000MB/ngày. Tổng thời gian vào giờ cao điểm là 3 giờ. Giờ cao điểm tập trung 80% trong ngày:

$$\text{Bandwidth} = \frac{3\times1000\times0.8\times8}{3\times3600} = 1.78 \text{ (Mbps)}$$
$$\text{Throughput} = \frac{3\times1000\times8}{8\times3600} = 0.83 \text{ (Mbps)}$$

- 100 workstations với tổng dung lượng download và upload là 500MB/ngày. Tổng thời gian vào giờ cao điểm là 3 giờ. Giờ cao điểm tập trung 80% trong ngày

$$\text{Bandwidth} = \frac{100\times500\times0.8\times8}{3\times3600} = 29.6 \text{ (Mbps)}$$
$$\text{Throughput} = \frac{100\times500\times8}{8\times3600} = 13.9 \text{ (Mbps)}$$

Mạng không dây:

- Máy laptop kết nối Wifi dùng cho khách hàng truy xuất khoảng 1000MB/ngày Tổng thời gian vào giờ cao điểm là 3 giờ. Giờ cao điểm tập trung 80% trong ngày. Giả sử rằng trong ngày có khoảng 50 lượt truy cập thường xuyên.

$$\text{Bandwidth} = \frac{50\times1000\times0.8\times8}{3\times3600} = 29.6 \text{ (Mbps)}$$
$$\text{Throughput} = \frac{50\times1000\times8}{8\times3600} = 13.9 \text{ (Mbps)}$$

4.2 Các thông số an toàn

- Tổng bandwith:

$$\text{Bandwidth} = 2.96 + 59.3 + 59.3 + 2 \times (1.78 + 29.6 + 29.6) = 243.52 \text{ (Mbps)}$$

- Hệ thống Mạng máy tính của Công ty được dự đoán cho mức độ phát triển 20% cho nên bandwith tối thiểu để hệ thống hoạt động ổn định:

$$243.52 \times 1.2 = 292.224 \approx 292 \text{ (Mbps)}$$

- Tổng throughput:

$$\text{Throughput} = 1.39 + 27.8 + 27.8 + 2 \times (0.83 + 13.9 + 13.9) = 114.25 \text{ (Mbps)}$$

- Hệ thống Mạng máy tính của Công ty được dự đoán cho mức độ phát triển 20% cho nên throughput tối thiểu để hệ thống hoạt động ổn định:

$$114.25 \times 1.2 = 137.1 \approx 137 \text{ (Mbps)}$$

5 Bảo mật an toàn và nâng cấp hệ thống

5.1 Yêu cầu đối với hệ thống

Công ty là nơi cung cấp vốn cho nền kinh tế, là công cụ quan trọng thúc đẩy lực lượng sản xuất phát triển. Công ty có một vai trò cực kỳ quan trọng trong nền kinh tế quốc gia. Hàng ngày, hoạt động của công ty luôn phải xử lý một lượng thông tin rất lớn. Hệ thống này phải đảm bảo hoạt động của công ty luôn có khối lượng thông tin xử lý trong hoạt động nghiệp vụ rất lớn. Tuy nhiên không phải ai cũng có quyền truy cập những kho thông tin này. Vậy nên công ty có nhu cầu xây dựng một hệ thống bảo mật cho mạng tin học phục vụ điều hành, kinh doanh.
Hệ thống bảo mật này phải đảm bảo

- An toàn cho toàn bộ thông tin trên mạng, chống lại mọi sự truy cập bất hợp pháp vào mạng. Ngăn chặn mọi sự truy cập thông tin trái phép từ bên trong lẫn bên ngoài.
- Kiểm soát được việc truy cập của người sử dụng.
- Bảo đảm an toàn dữ liệu.
- Có khả năng sửa chữa và phục hồi nhanh chóng trong trường hợp tấn công xảy ra.
- Phát hiện dấu hiệu vi phạm các chính sách bảo mật.
- Chi phí phù hợp với dự trù kinh phí của công ty.
- Đáp ứng được khả năng mở rộng của mạng công ty trong tương lai.

5.2 Xác định các tài nguyên cần được bảo vệ

- Phần cứng: Các máy chủ mạng, các máy trạm, các thiết bị mạng như Router, Access Servers.
- Phần mềm: Hệ điều hành của các máy chủ Unix, Windows NT.., các chương trình ứng dụng quản lý tài khoản, tín dụng, các chương trình kế toán, tự động hóa văn phòng, truyền dữ liệu, ATM..
- Dữ liệu: Đây là phần quan trọng cần được bảo vệ nhất của công ty. Dữ liệu này sẽ gồm các dữ liệu tài khoản liên quan đến khách hàng.
- Tài liệu: Các công văn, báo cáo, tài liệu, sách vở, tài liệu hướng dẫn sử dụng..

5.3 Xác định các mối đe dọa tới hệ thống

- **Mối đe dọa từ bên ngoài:**
  - Nguy cơ bị nghe trộm, thay đổi thông tin truyền đi trên mạng công cộng (PSTN). Đây là một nguy cơ tiềm ẩn và ảnh hưởng trực tiếp đến hoạt động kinh doanh của công ty. Hacker có thể sử dụng các công cụ, thiết bị đặc biệt để móc nối vào hệ thống cáp truyền thông của công ty để nghe trộm thông tin, nguy hiểm hơn hacker có thể sửa chữa, thay đổi nội dung thông tin đó – ví dụ nội dung của điện chuyển tiền, thanh toán .. gây ra. những tổn thất nghiêm trọng.

- **Mối đe dọa từ bên trong:**
  - Người sử dụng bên trong mạng có nhiều cơ hội hơn để truy cập vào các tài nguyên hệ thống. Đối với công ty có đặc thù lớn là do nhiều mạng LAN của trung tâm, chi nhánh kết nối vào, do đó nếu người sử dụng trong mạng có ý muốn truy cập vào những tài nguyên của hệ thống thì họ sẽ gây nên một mối đe dọa cho mạng. Người sử dụng bên trong có thể được gán những quyền không cần thiết, có thể bị mất mật khẩu... và đó sẽ là mối đe dọa lớn với hệ thống an toàn mạng.

5.4 Các giải pháp bảo mật

- **Bảo mật mức mạng**:
  - Bảo mật đường truyền, bảo mật các thông tin lưu truyền trên mạng. Được thực hiện bằng hình thức mã hóa thông tin trên đường truyền, các công cụ xác định tính toàn vẹn và xác thực của thông tin.
  - Giải pháp chống xâm nhập và chống tấn công từ chối dịch vụ (DDoS).
  - Giải pháp mã hóa và bảo mật đường truyền: Giải pháp chuyên dụng bảo vệ kết nối giữa các site trong cùng một hệ thống, đặc biệt phù hợp với các doanh nghiệp có nhiều chi nhánh và yêu cầu bảo mật cao trên đường truyền.
  - Tài liệu: Các công văn, báo cáo, tài liệu, sách vở, tài liệu hướng dẫn sử dụng...
- **Bảo mật lớp truy cập**: Bảo mật truy cập của người dùng quay số (dial-up): Tạo các kênh VPN cho các kết nối dial-up..
- **Firewall/IDS**: Tại các khu vực cung cấp các máy chủ truy cập cần bố trí các tường lửa kèm các bộ dò tìm tấn công IDS đảm bảo ngăn chặn các truy cập trái phép hay các dạng tấn công ngay từ cổng vào mạng.
- **Bảo mật thiết bị và máy chủ**: Các thiết bị mạng như Router, Switch, firewall là các điểm nút mạng hết sức quan trọng và cần được bảo vệ.
- **Bảo mật ở Hệ điều hành và ứng dụng**: Thường xuyên sao lưu, cập nhật các bản vá lỗi của hệ điều hành, sử dụng các phần mềm bổ sung (Patch) bịt lỗ hổng trên các hệ điều hành, đảm bảo hệ thống làm việc ổn định.
- **Bảo mật mức Cơ sở dữ liệu**: Có thể nói CSDL là lõi của toàn bộ hệ thống bảo mật thông tin, toàn bộ thông tin quan trọng mang tính chất sống còn được tập trung trên các CSDL, trong thiết kế CSDL được đặt ở mức ưu tiên cao nhất.
- **Bảo mật tường lửa hệ thống ứng dụng Web (Web application firewall – WAF)**: Cho phép ngăn chặn các hành vi tấn công vào ứng dụng Web, liên tục giám sát hệ thống ứng dụng Web và cung cấp các cảnh báo nếu xuất hiện các lỗ hổng trên ứng dụng.
- **Bảo mật chống giả mạo giao dịch (Fraud detection)**: Ngăn chặn các hành vi giả mạo người dùng, chiếm đoạt và sử dụng các tài khoản thanh toán trên môi trường thanh toán điện tử, e-banking.
- **Bảo mật dữ liệu**: Giải pháp giám sát an ninh hệ thống cơ sở dữ liệu. Giải pháp mã hóa dữ liệu.

5.5 An toàn khi xảy ra sự cố

- **Với đường kết nối ra internet**: Phải có cơ chế dự phòng trong trường hợp đường kết nối chính gặp sự cố (ví dụ như main switch hoặc router), đảm bảo cho kết nối luôn được thông suốt. Ta có thể thuê cả hai đường leased-line 1.2 Mbps và đường ADSL 8 Mbps, đường kết nối chính là đường leased-line và sử dụng cơ chế load-balancing nhằm chia tải của đường leased-line qua đường ADSL khi đường leased-line bị quá tải hay gặp sự cố. Phải có một phòng ban chuyên về an ninh mạng để giải quyết các vấn đề khi hệ thống mạng xảy ra sự cố
- **Với các thiết bị kết nối ra internet**: Phải có cơ chế dự phòng, lúc bình thường thì mọi kết nối diễn ra theo đường chính, khi một thiết bị trong đường kết nối chính gặp sự cố (chẳng hạn như router) thì lập tức phải chuyển sang đường dự phòng, cơ chế này có thể thực hiện được bằng cách set thông số priority cho thiết bị, thiết bị nào có priority lớn hơn sẽ là thiết bị cho đường chính và khi thiết bị trong đường chính bị sự cố thì lập tức hệ thống sẽ sử dụng thiết bị của đường dự phòng đảm bảo cho kết nối được thông suốt.
- **Với miền DMZ**: Cần có backup server cho các server web, mail, database... và phải backup thường xuyên để khi xảy ra sự cố dữ liệu trên các server thì ta sẽ không bị mất dữ liệu đảm bảo cho hệ thống mạng hoạt động bình thường.
- **Với phân hệ mạng nội bộ**: việc sử dụng các switch có cơ chế spanning-tree giúp chúng ta tạo ra các đường kết nối dự phòng mà không bị loop, nhằm đảm bảo khi switch chính bị sự cố thì switch dự phòng sẽ hoạt động và không làm cho hoạt động của công ty bị gián đoạn. Tổ chức một phòng kỹ thuật chuyên về hệ thống mạng để giải quyết các vấn đề khi hệ thống mạng xảy ra sự cố.
- **Với dữ liệu**: Cần phải backup thường xuyên để tránh sự cố mất dữ liệu và nên sử dụng một server để backup.

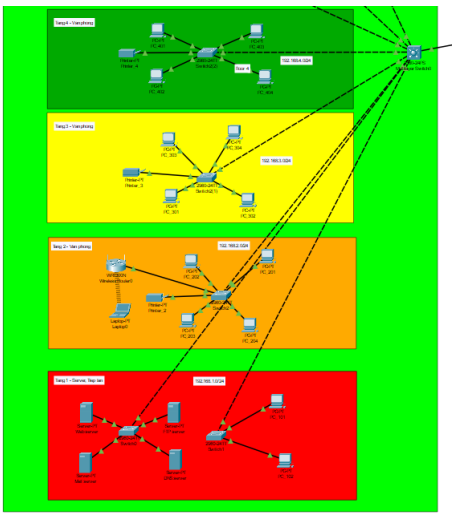
6 Mô phỏng với Packet Tracer

6.1 Trình tự thực hiện

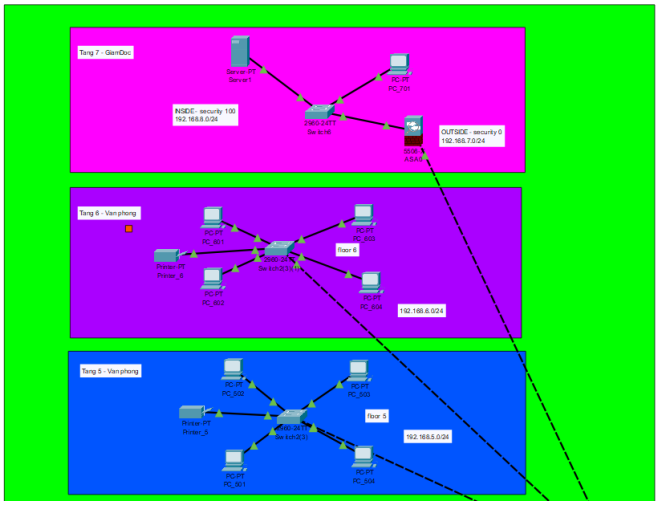
- Giả lập mô hình kết nối trụ sở và các chi nhánh.
- Giả lập mô hình các phòng ban.
- Tiến hành chia Vlan trong trụ sở và các chi nhánh.
- Tiến hành cấu hình DHCP tại core router để cấp phát IP cho các máy ở trụ sở và chi nhánh.
- Giả lập mạng internet để mô phỏng kết nối giữa trụ sở và chi nhánh.
- Tiến hành Routing mô hình giả lập.
- Tiến hành cấu hình NAT để kết nối internet.
- Tiến hành kiểm tra bằng cách ping, traceroute và chế độ simulation có sẵn.

6.2 Kết quả hiện thực

6.2.1 Trụ sở chính

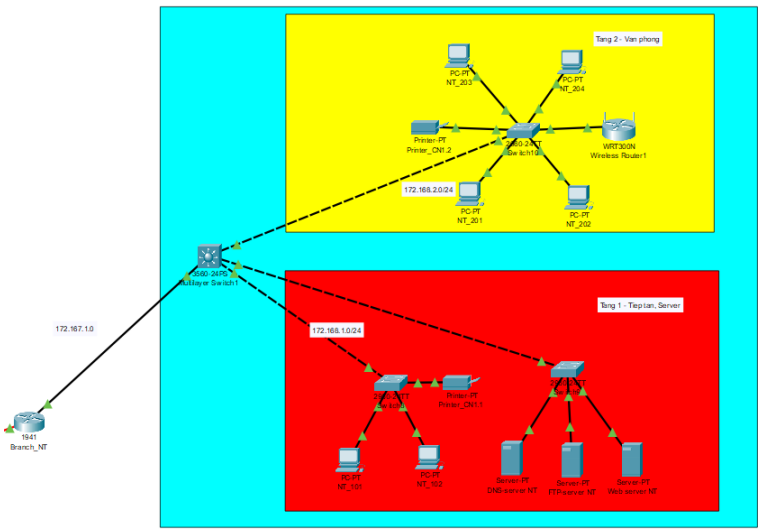


Hình 1: Trụ sở chính (1)

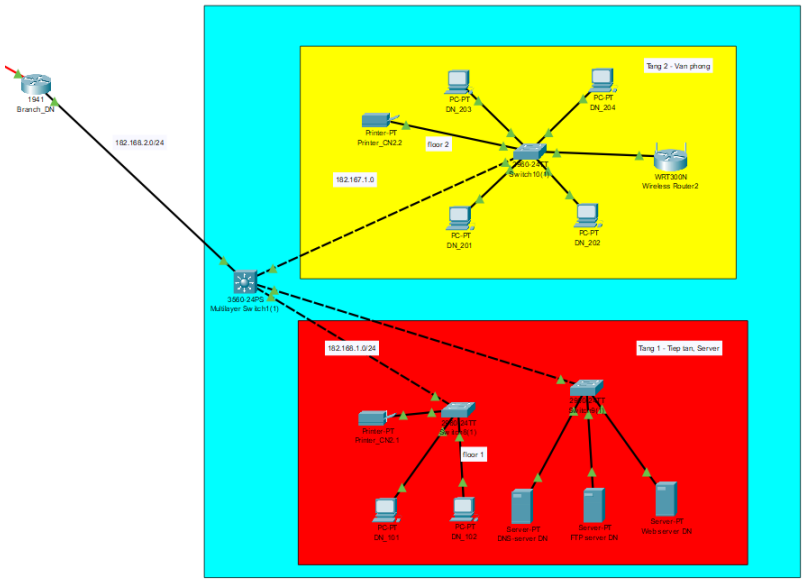


Hình 2: Trụ sở chính (2)

6.2.2 Chi nhánh (Nha Trang và Đà Nẵng)

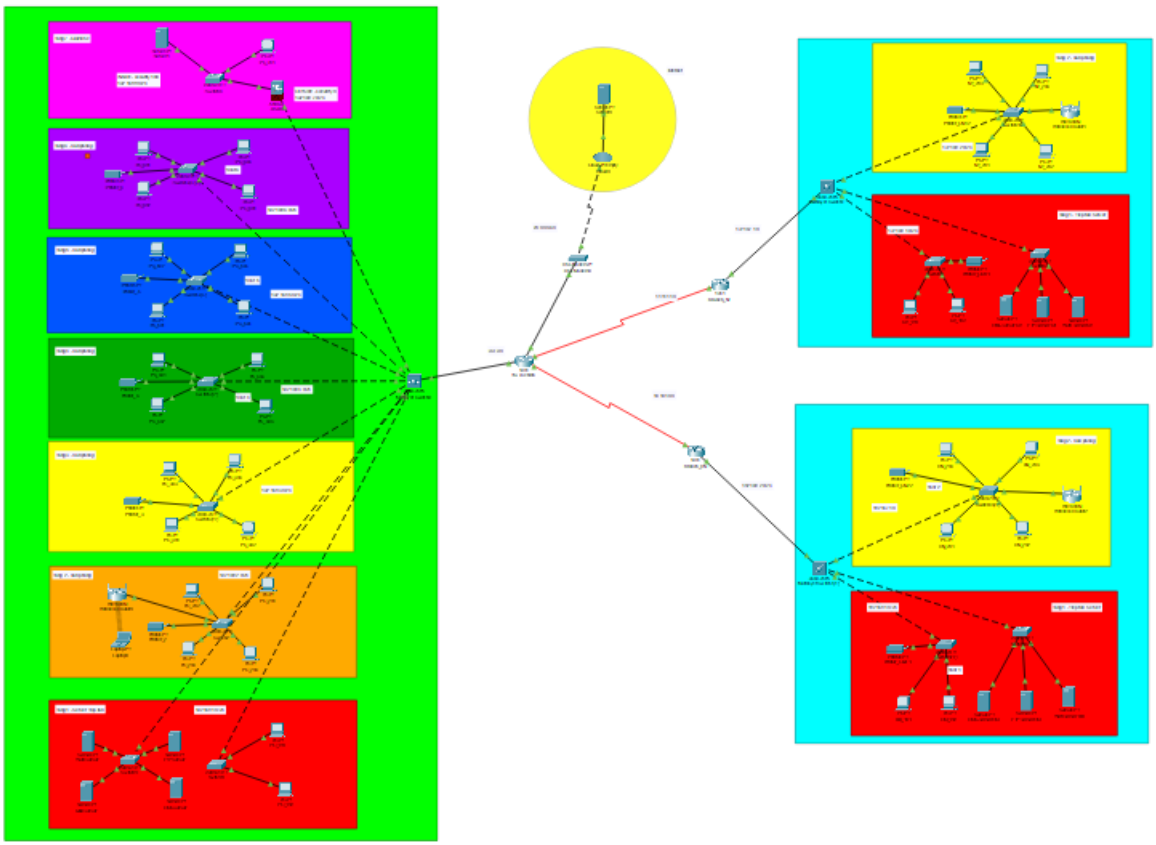


Hình 3: Chi nhánh Nha Trang



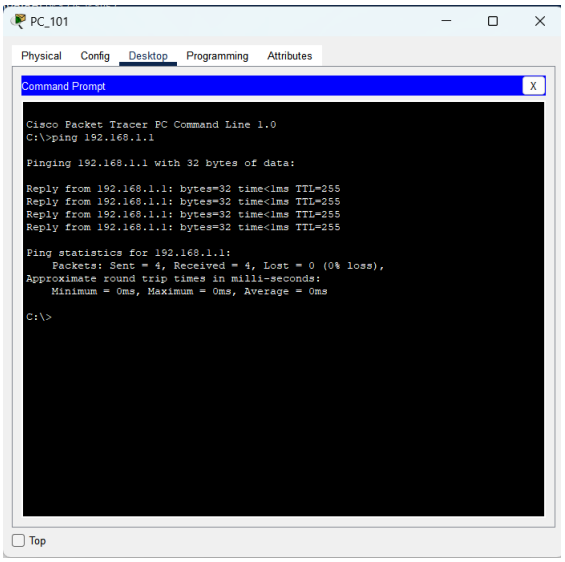
Hình 4: Chi nhánh Đà Nẵng

6.2.3 Tổng thể hệ thống

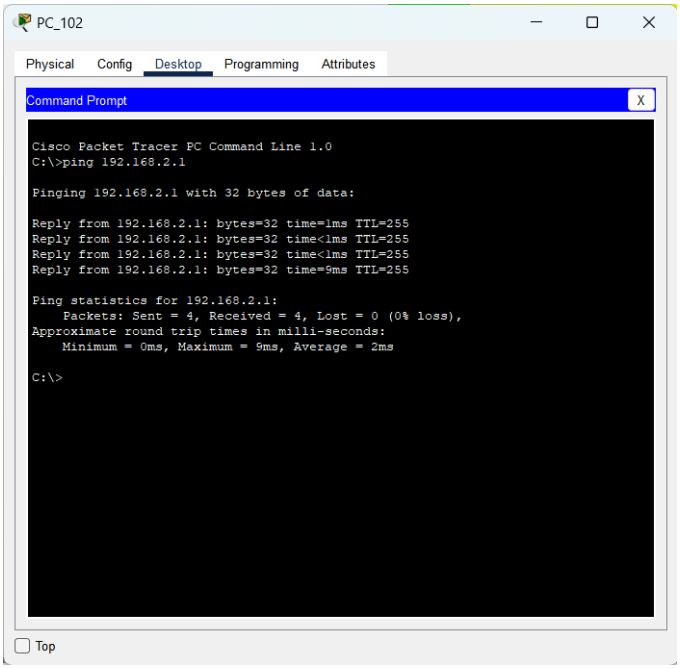


Hình 5: Toàn bộ hệ thống

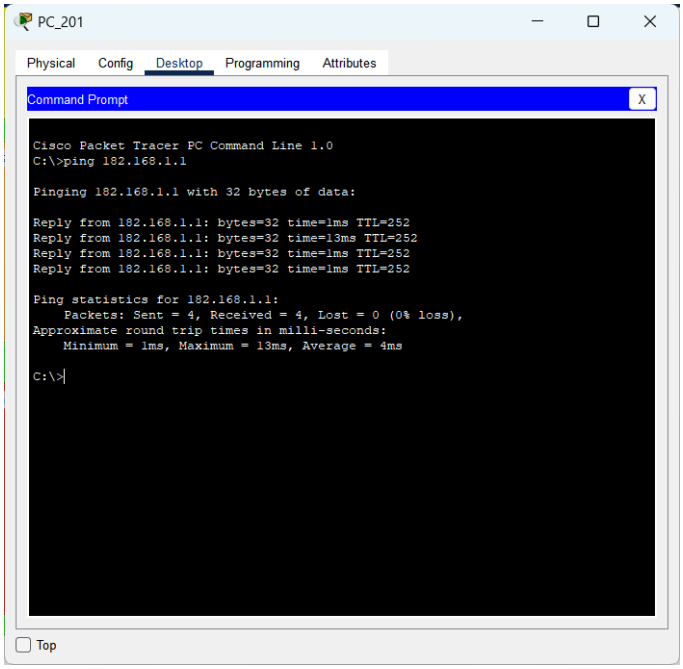
7 Kiểm thử hệ thống



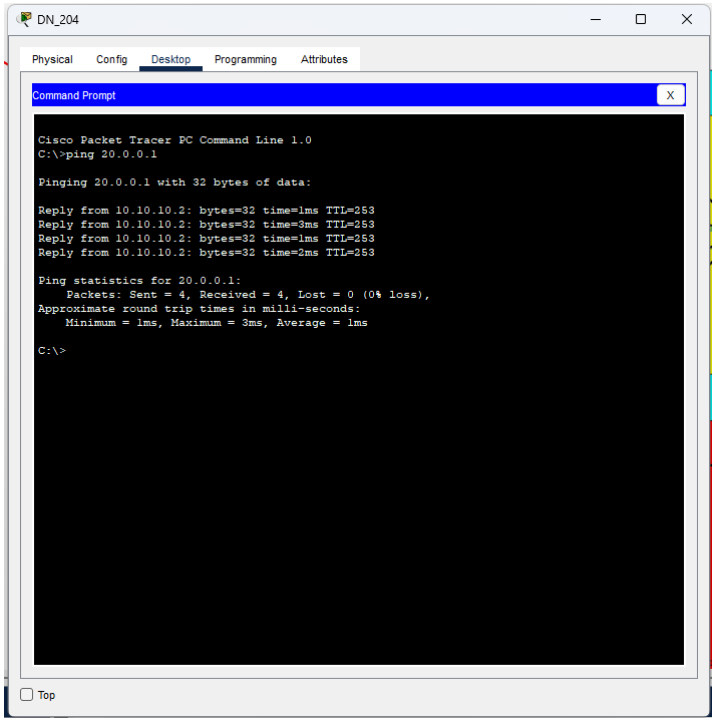
Hình 6: Ping trong cùng 1 VLAN



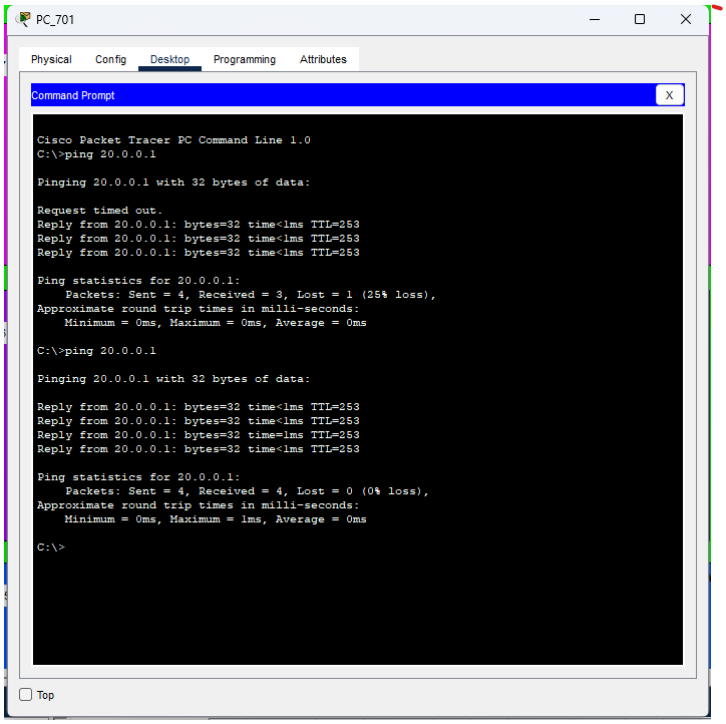
Hình 7: Ping giữa các VLAN



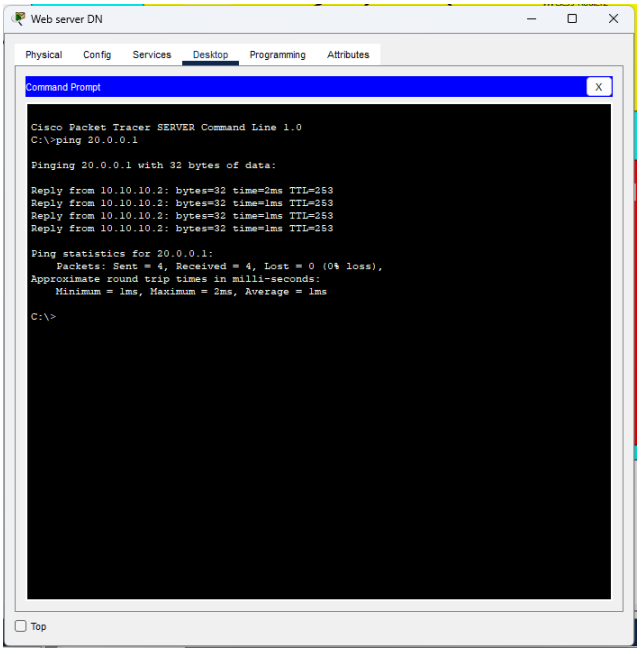
Hình 8: Ping tới chi nhánh



Hình 9: Ping tới Internet



Hình 10: Ping từ DMZ ra Internet



Hình 11: Ping từ Web server ra Internet

8 Đánh giá lại hệ thống

8.1 Kết quả đạt được của dự án

- Nhóm đã có thể làm quen với ứng dụng Cisco Packet Tracer, đồng thời tìm hiểu được các giải pháp thiết kế về phần cứng, cũng như cách cấu hình cho thiết bị mạng. Nhóm đã có khả năng thiết kế được một hệ thống mạng có quy mô vừa hoặc nhỏ. Thiết kế mô hình mạng cho công ty bao gồm mô hình IP và mô hình đi dây.
- Hệ thống mạng đáp ứng tương đối phù hợp với yêu cầu đưa ra, có khả năng nâng cấp phù hợp với sự phát triển sau này.
- Các trang thiết bị được sử dụng của tập đoàn Cisco nên được bảo đảm chất lượng cao, đỡ tốn chi phí bảo trì về sau; chất lượng đường truyền tốt, được Cisco hỗ trợ kỹ thuật đầy đủ.
- Hệ thống với băng thông lớn, đáp ứng đầy đủ nhu cầu của nhân viên làm việc trong công ty đi kèm mô hình mạng LAN dạng hình sao đảm bảo quá trình hoạt động bình thường khi có một nút thông tin bị hư hỏng, giúp nâng cao hiệu suất công việc
- Chia VLAN cho các phòng ban của trụ sở chính và chi nhánh.
- Thực hiện kết nối ra Internet cho trụ sở chính và chi nhánh, kết nối giữa trụ sở và chi nhánh.

8.2 Hạn chế của dự án

- Chưa có kiến thức về một mạng doanh nghiệp cụ thể, khi thiết kế gặp khó khăn về việc quyết định các mô hình, công nghệ, thiết bị nên được sử dụng.
- Vì là môn học mới nên nhóm chưa có nhiều kiến thức về việc cấu hình các thiết bị trên phần mềm Packet Tracer (Router, Firewall,. . .). Đồng thời với chương trình học Blended khiến sinh viên phần nào ít tiết thực hành hơn so với chương trình cũ nên việc chương thành thạo chương trình là điều ckhoong thể tránh khỏi
- Chưa có nhiều kiến thức về vấn đề bảo mật và sự cố.
- Chưa hiểu rõ về các công nghệ để áp dụng thực hiện mô phỏng.
- Mặc dù có khả năng mở rộng mạng, nhưng điều này hoàn toàn phụ thuộc vào khả năng hoạt động của bộ phận trung tâm. Một khi trung tâm gặp phải sự cố (switch tổng hoặc router tổng), toàn bộ hệ thống mạng sẽ không thể hoạt động.
- Chưa hoàn thành cấu hình cân bằng tải cho công ty.

8.3 Định hướng phát triển

- Trong tương lai, rất có thể công ty sẽ phát triển và mở rộng phạm vi hoạt rộng ra nhiều địa điểm khác. Do đó, việc tính đến sự mở rộng của hệ thống mạng giữa trụ sở và các chi nhánh với nhau là rất quan trọng.
- Hiện tại giả sử số nhân viên là khoảng 200 người được chia đều cho 7 tầng của toà nhà, suy ra số lượng nhân viên mỗi tầng là 30 người tương đương với 30 workstation, trong khi số lượng tối đa cổng của switch là 24 ports. Vì vậy khi số lượng nhân viên tăng lên trong một mức độ nhất định, ta không cần phải thiết kế lại hay mua thêm thiết bị khác.

- Đối với vấn đề băng thông, khi cần nâng cấp thì chỉ cần đăng ký thay đổi gói cước với nhà cung cấp dịch vụ. Hơn nữa, trong hệ thống mạng thiết kế chưa có giải pháp cân bằng tải (Network Load Balancing) - vậy nên trong tương lai thì mô hình có thể thiết kế thêm hệ thống cân bằng tải, nhằm giúp cho việc phân bố đồng đều lưu lượng truy cập giữa các máy chủ có cùng chức năng.
- Đối với vấn đề bảo mật của mô hình trong tương lai,mô hình có thể phát triển thêm về hệ thống tường lửa cục bộ cho cả trụ sở và các chi nhánh. Đồng thời thiết kế 1 hệ thống ngăn chặn việc khách hàng sử dụng wifi truy cập nào hệ thống mạng LAN hiệu quả hơn việc ngăn chặn trên Switch layer 3.