Vietnam National University, Ho Chi Minh City
University of Technology
Faculty of Computer Science and Engineering

Computer Networks
(CO3094)

Computer Network Design for the building of a Company

Advisors:

Students: Lưu Chấn Hưng - 2111401
Phan Nguyễn Xuân Lộc - 2113971
Lê Thành Lợi - 2111699
Trần Hoàng Đại Sơn - 2110509

Ho Chi Minh City, 11/2023

Contents

1 Yêu cầu hệ thống

1.1 Yêu cầu hệ thống mạng

1.1.1 Tại trụ sở

- Tại trụ sở chính gồm 7 tầng, tầng đầu tiên được trang bị một phòng dành cho đội ngũ IT, nơi này chủ yếu dành cho các hoạt động liên quan đến kỹ thuật mạng. Bên cạnh đó, cũng có một phòng tập trung dây mạng và patch panels, được biết đến với tên gọi là Cabling Central Local. Phòng này chịu trách nhiệm cho việc quản lý và tổ chức hệ thống dây cáp mạng của toàn bộ tòa nhà, đảm bảo kết nối mạng được duy trì một cách hiệu quả và có tổ chức.

- Thiết kế theo kiểu Small Enterprise, cấu trúc mạng này bao gồm 120 máy trạm, 5 máy chủ và ít nhất 12 thiết bị mạng. Có thể cần thêm một số thiết bị mạng khác, đặc biệt là các thiết bị bảo mật mạng, để đáp ứng nhu cầu cụ thể của hệ thống. Thiết kế này nhằm mục đích cung cấp một hạ tầng mạng hiệu quả, có khả năng mở rộng và đáp ứng nhu cầu kết nối và bảo mật cho doanh nghiệp.

- 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). Hệ thống này tích hợp một cơ chế cân bằng tải, cho phép quản lý và phân phối hiệu quả lưu lượng mạng giữa các kết nối khác nhau để đảm bảo hiệu suất ổn định và đáng tin cậy.

- 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.Yêu cầu bảo mật cao với firewall, IPS/IDS, phát hiện phishing, tính khả dụng cao.

- VPN: Cấu hình VPN site-to-site và cho teleworker.

- Hệ Thống Camera Giám Sát: Cần đề xuất.

1.1.2 Tại chi nhánh

- Các chi nhánh của công ty tại Đà Nẵng và Hà Nội cũng tuân theo mô hình thiết kế mạng giống như trụ sở chính, nhưng được điều chỉnh cho phù hợp với quy mô nhỏ hơn. Mặc dù quy mô nhỏ hơn, nhưng cấu trúc và chức năng của hệ thống mạng tại các chi nhánh này vẫn đảm bảo đáp ứng nhu cầu kết nối và bảo mật thông tin tương đương với trụ sở chính, chỉ có sự thay đổi về số lượng và cấu hình của các thiết bị mạng để phù hợp với quy mô của từng chi nhánh.

- Trong một tòa nhà hai tầng, tầng một được thiết lập với một phòng IT, phục vụ cho các hoạt động và nhu cầu kỹ thuật mạng. Bên cạnh đó, cũng có một khu vực được gọi là Cabling Central Local, nơi này chủ yếu dùng để sắp xếp và quản lý các dây cáp mạng cùng với patch panels. Dây là trung tâm quan trọng cho việc duy trì

và quản lý hệ thống mạng của tòa nhà, đảm bảo sự liên kết và hoạt động ổn định của mạng.

- BB dạng chi nhánh: 30 workstations, 3 servers, 5 hoặc nhiều thiết bị mạng hơn.
- Kết Nối WAN: Sử dụng công nghệ tương tự trụ sở.

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 download vào khoảng 1000MB/ngày và upload 2000 MB/ngày cho servers
- Mỗi workstation dùng cho duyệt Web, tải tài liệu, giao dịch khách hàng,... Tổng dung lượng upload 100 MB/ngày và download vào khoảng 500MB/ngày.
- Máy laptop kết nối WiFi dùng cho khách hàng truy xuất download vào khoảng 500MB/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 120 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,...

- Bộ phận giao dịch và tiếp tân sẽ được trang bị một máy tính cá nhân (PC) cho mỗi nhân viên. Máy tính này sẽ có phần mềm kết nối với máy chủ để thực hiện các truy vấn. Vì yêu cầu công việc và mục tiêu bảo mật được ưu tiên hàng đầu, nên cấu hình của PC sẽ được thiết lập ở mức chấp nhận được.
- Đối hệ thống máy tính dành cho khách hàng chỉ cho phép kết nối internet và không được phép kết nối với bất kỳ máy tính nào trong hệ thống. Ngoài ra, công ty cũng cung cấp mạng Wi-Fi cho khách hàng sử dụng bằng các thiết bị di động. Tuy nhiên, các thiết bị này cũng chỉ được phép sử dụng để truy cập internet và không được phép kết nối với bất kỳ máy tính nào trong hệ thống.

  - Tầng 1 còn bao gồm 2 phòng quan trọng: phòng IT, dành cho bộ phận công nghệ thông tin của công ty, và phòng tập trung dây mạng và patch panel, nơi tập trung

các thiết bị mạng, máy chủ, dây cáp, và các kết nối liên quan. Đối với phòng IT, đây là trung tâm quản lý toàn bộ máy chủ và hệ thống mạng của công ty, vì vậy độ bảo mật ở đây cần phải được đặt lên hàng đầu. Hơn nữa, cấu hình máy tính và tốc độ đường truyền cũng cần phải được nâng cao để đảm bảo hiệu suất và ổn định của hệ thống.

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

2.1.2 Tại chi nhánh

Sau khi tiến hành khảo sát các công ty có cùng quy mô, nhóm quyết định phân chia chi nhánh thành các tầng. Mỗi chi nhánh sẽ bao gồm 30 workstation, 3 server, và ít nhất 5 thiết bị mạng(hoặc nhiều hơn), được sắp xếp trong một tòa nhà gồm 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 mô tả về hệ thống của Công ty BB, máy chủ thực hiện nhiệm vụ quản lý và lưu trữ dữ liệu, trong khi các máy khách (clients) truy cập và sử dụng dữ liệu khi cần. Mô hình client-server được xem là lựa chọn lý tưởng cho các mạng có nhiều máy khách, đặc biệt như trong trường hợp của Công ty BB, nơi có nhiều người dùng cần truy cập dữ liệu và ứng dụng đồng thời. Vì vậy, chúng tôi kiến nghị sử dụng mô hình client-server, vì nó cung cấp khả năng quản lý và kiểm soát tập trung, giúp việc quản lý mạng trở nên dễ dàng hơn và đảm bảo tính bảo mật và toàn vẹn của dữ liệu.

-TOPO hình sao là một kiểu 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 giống ngôi sao. Trong cấu trúc này, dữ liệu di chuyển từ các thiết bị khách đến trung tâm hoặc công tắc trung tâm, sau đó đến thiết bị đích. Mô hình này thường được ứng dụng rộng rãi trong mạng LAN vì nó mang lại độ tin cậy cao và dễ dàng xử lý sự cố. Nếu có lỗi xảy ra trên bất kỳ thiết bị nào trong mạng, nó không ảnh hưởng đến các thiết bị khác và việc xác định và khắc phục sự cố trở nên đơn giản. Với hệ thống lớn như của Công ty BB, việc sử dụng kiểu cấu trúc này sẽ đảm bảo sự 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 2911 vì router này cung cấp mức độ tích hợp dịch vụ ngày càng tăng với các dịch vụ dữ liệu, an ninh, không dây và di động, cho hiệu quả cao hơn và tiết kiệm chi phí. Đặc tính kỹ thuật:

- Manufacturer: Cisco Systems, Inc
- Manufacturer Part Number: CISCO2911/K9.
- Product Type: Router.
- Rack Units: 2RU
- Enclosure Type: Rack-mountable - modular - 2U
- Connectivity Technology: Wired
- Data Link Protocol: Ethernet, Fast Ethernet, Gigabit Ethernet
- Interfaces: 3 integrated 10/100/1000 Ethernet ports (RJ-45 only)
- Expansion Slot(s)
  - 1 service module slot
  - 1 Internal Service Module slot

  - 2 onboard digital signal processor (DSP) slots
  - 4 enhanced high-speed WAN interface card slots
- Network / Transport Protocol: IPSec, L2TPv3
- Routing Protocol: OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, static IP routing, IGMPv3, GRE, PIM-SSM, static IPv4 routing, static IPv6 routing, policy-based routing (PBR), MPLS, Bidirectional Forwarding Detection (BFD), IPv4-to-IPv6 Multicast
- Remote Management Protocol: SNMP, RMON, TR-069
- Features: Firewall protection, VPN support, MPLS support, Syslog support, IPv6 support, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Web Services Management Agent (WSMA), NetFlow
- Compliant Standards: IEEE 802.3, IEEE 802.1Q, IEEE 802.3af, IEEE 802.3ah, IEEE 802.1ah, IEEE 802.1ag, ANSI T1.101, ITU-T G.823, ITU-T G.824
- Voltage Required: AC 120/230 V (50/60 Hz)
- RAM: 512 MB (installed) / 2 GB (max)
- Flash memory: 256 MB (installed) / 8 GB (max)
- Dimensions: 43.8 cm x 30.5 cm x 8.9 cm
- Weight: 8.21 Kg

Switch Layer2: 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 Switch Layer2 Cisco 2960X-24TD. Đặc tính kỹ thuật:

- Flash memory: 128 MB for LAN Base and IP Lite SKUs, 64 MB for LAN Lite SKUs
- DRAM: 512 MB for LAN Base and 256 MB for LAN Lite
- CPU: APM86392 600 MHz dual core
- Console ports: USB (Type B), Ethernet (RJ-45)
- Storage interface: USB (Type A) for external flash storage
- Network management interface: 10/100 Mbps Ethernet (RJ-45)
- Forwarding bandwidth: 108 Gbps
- Switching bandwidth: 216 Gbps
- Maximum active VLANs: 1023
- VLAN IDs available: 4096
- Maximum Transmission Unit (MTU)-L3 packet: 9198 bytes

- Jumbo frame - Ethernet frame: 9216 bytes
- Forwarding rate: 64-byte Layer 3 packets: 95.2 Mpps
- Dimensions: 4.5cm x 27.9cm x 44.5cm
- MTBF in hours: 569,520
- Standards support: IEEE 802.1D Spanning Tree Protocol; IEEE 802.1p CoS Prioritization; IEEE 802.1Q VLAN; IEEE 802.1s; IEEE 802.1w; IEEE 802.1X; IEEE 802.1ab (LLDP); IEEE 802.3ad; IEEE 802.3af and IEEE 802.3at; IEEE 802.3ah (100BASE-X single/multimode fiber only); IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports; IEEE 802.3 10BASE-T; IEEE 802.3u 100BASE-TX; IEEE 802.3ab 1000BASE-T; IEEE 802.3z 1000BASE-X; RMON I and II standards; SNMP v1, v2c, and v3; IEEE 802.3az; IEEE 802.3ae 10 Gigabit Ethernet; IEEE 802.1ax
- Voltage (auto ranging): 100 to 240 VAC
- Current: 1A to 0.5A
- Frequency: 50 to 60 Hz

Switch Layer3: 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 Switch Layer3 3650-24PS.

- Switching capacity:
  - 176 Gbps on 48-port models (non-multigigabit models)
  - 92 Gbps on 24-port models (non-multigigabit models)
  - 254 Gbps on 24-port Multigigabit models with 2x10G uplink
  - 272 Gbps on 24-port Multigigabit models with 4x10G uplink
  - 392 Gbps on 48-port Multigigabit models with 4x10G uplink
  - 472 Gbps on 48-port Multigigabit models with 8x10G uplink
  - 472 Gbps on 48-port Multigigabit models with 2x40G uplink
- Stacking bandwidth: 160 Gbps
- Total number of MAC addresses: 32,000
- Total number of IPv4 routes (ARP plus learned routes): 24000
- FNF entries:
  - 48,000 flow on 48-port models
  - 24,000 flows on 24-port models

- DRAM: 4 GB
- Flash: 2 GB (non-Multigigabit models) and 4GB (Multigigabit models)
- VLAN IDs: 4,094
- Total switched virtual interfaces (SVIs): 1000
- Jumbo frame: 9198 bytes
- Total routed ports per 3650 stack: 208
- Wireless
- Number of access points per switch/stack: 25
- Number of wireless clients per switch/stack: 1000
- Total number of WLANs per switch: 64
- Wireless bandwidth per switch:
  - Up to 40 Gbps on 48-port models
  - Up to 20 Gbps on 24-port models
- Supported Aironet access point series: 3700, 3600, 3500, 2600, 1600, 1260, 1140, 1040
- Forwarding Rate of Switch Models
- Forwarding Rate: 41.66 Mpps
- Dimensions (H x W x D): 4.4cm x 44.5cm x 44.8cm
- Weight: 7.26kg
- MTBF Hours: 528,280
- Standards: IEEE 802.1as; IEEE 802.1s; IEEE 802.1w; IEEE 802.11; IEEE 802.1x; IEEE 802.1x-Rev; IEEE 802.3ad; IEEE 802.3af; IEEE 802.3at; IEEE 802.3bz; IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports; IEEE 802.1D Spanning Tree Protocol; IEEE 802.1p CoS prioritization; IEEE 802.1Qat Stream Reservation Protocol; IEEE 802.1Qav; IEEE 802.1Q VLAN; IEEE 802.3 10BASE-T specification; IEEE 802.3u 100BASE-TX specification; IEEE 802.3ab 1000BASE-T specification; IEEE 802.3z 1000BASE-X specification; RMON I and II standards; SNMPv1, SNMPv2c, and SNMPv3

Light weight access point: là một thiết bị mạng không dây được sử dụng trong các mạng WLAN (Wireless Local Area Network). LAP được thiết kế để giảm tải cho các trạm truy cập (APs) trong mạng WLAN bằng cách chuyển một số chức năng xử lý từ AP sang một trung tâm điều khiển (WLC). LAP chỉ thực hiện các hoạt động không dây 802.11 cho các khách hàng không dây, do đó được gọi là "nhẹ". Nó được sử dụng trong các tình huống mà nhiều APs được yêu cầu trong mạng.

- Data Rates Supported:

  - 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps
  - 802.11b: 1, 2, 5.5, and 11 Mbps
  - 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
- Uplink: Carrier-Sense Multiple Access/Collision Avoidance (CSMA/CA)
- Frequency Band and Operating Channels:
  - 802.11a: 5.15 to 5.25 GHz, 5.25 to 5.35 GHz, 5.47 to 5.725, 5.725 to 5.825 GHz
  - 802.11b: 2.412 to 2.497 GHz
  - 802.11g: 2.412 to 2.497 GHz
- Nonoverlapping Channels:
  - 802.11a: Up to 12
  - 802.11b/g: Up to 3
  - Dependent upon country-specific regulatory approvals
- Wireless Modulation:
  - 802.11a: Orthogonal frequency division multiplexing (OFDM)
  - 802.11b: Direct sequence spread spectrum (DSSS)
  - 802.11g: DSSS and OFDM
- Available Transmit Power Settings:
  - 100, 50, 25, 12.5, and 6.25 percent
  - 802.11a: 50 mW (17 dBm) conducted
  - 802.11b: 100 mW (20 dBm) conducted
  - 802.11g: 100 mW (20 dBm) conducted
  - Maximum power setting will vary according to channel and individual country regulations
- Integrated Antennas:
  - 1000 series
  - 802.11a/b/g: Two 180-degree sectorized antennas
  - 2.4 GHz: Gain 5.5 dBi
  - 5 GHz: Gain 6 dBi
- Compliance:
  - Safety:
    * UL 60950, Third Edition
    * UL 2043
    * EN 50385:2002
    * RSS 102

    - FCC OET 65
- Electrical safety:
    - UL 60950-1:2003, First Edition
    - CSA C22.2 No. 60950-1-03
- Radio approvals:
    - US: FCC Part 15 subparts C and E
    - EN 300 328 V1.4.1
    - EN 301 893 V1.2.3
    - Canada: RSS-210
    - Europe: EN 301.893, EN 300.328
    - Japan: ARIB STD-33A/STD-T66, ARIB STD T-71
    - EN 60601-1-2 EMC requirements for the Medical Directive 93/42/EEC
- EMI and susceptibility (Class A):
    - US: FCC parts 15.107 and 15.109
    - Canada: ICES-003
    - Japan: VCCI
    - Europe: EN 55022, EN 55024, EN 301.489-1 and -17
- Other standards:
    - Ethernet IEEE 802.3/IEEE 802.3u
    - IEEE 802.3af Power over Ethernet (PoE)
- Interface and Indicators:
    - Network: 10/100 Mbps Ethernet (RJ-45 link, activity)
    - Other indicators: Power, alarm
- Dimensions (H x W x D): 24.4 x 14.5 x 4.1 cm
- Weight:
    - Access point and ceiling clip: 1.3 lb (0.6 kg)
    - Access point with optional wall brackets kit: 2.2 lb (1 kg)
- Power:
    - 48 VDC; 250 mA; 10W
    - Power over Ethernet (IEEE 802.3af)
    - Optional AC power supply (AIR-PWR-1000=)
- Wi-Fi Certification
    - 802.11a/b/g
    - Wi-Fi Protected Access (WPA) and WPA 2: Personal, Enterprise

3.2 Thiết kế IP và Subnet

Tại trụ sở chính:

Tên mạng	IP/Subnet mask	IP khả dụng	Default gateway
VLAN10	192.168.1.0/24	192.168.1.1-254/24	192.168.1.1
VLAN20	192.168.2.0/24	192.168.2.1-254/24	192.168.2.1
VLAN30	192.168.3.0/24	192.168.3.1-254/24	192.168.3.1
VLAN40	192.168.4.0/24	192.168.4.1-254/24	192.168.4.1
VLAN50	192.168.5.0/24	192.168.5.1-254/24	192.168.5.1
VLAN60	192.168.6.0/24	192.168.6.1-254/24	192.168.6.1
VLAN70	192.168.7.0/24	192.168.7.1-254/24	192.168.7.1
WLAN	10.10.0.0/16	10.10.0.1-10.10.255.254/16	10.10.0.1
DMZ (static IP)	10.20.10.0/26	10.20.10.1-10.20.10.62/26	10.20.10.1

Hình 1: IP tại trụ sở chính

Tại chi nhánh (branch) 1:

Tên mạng	IP/Subnet mask	IP khả dụng	Default gateway
VLAN80	192.168.8.0/24	192.168.8.1-254/24	192.168.8.1
VLAN90	192.168.9.0/24	192.168.9.1-254/24	192.168.9.1

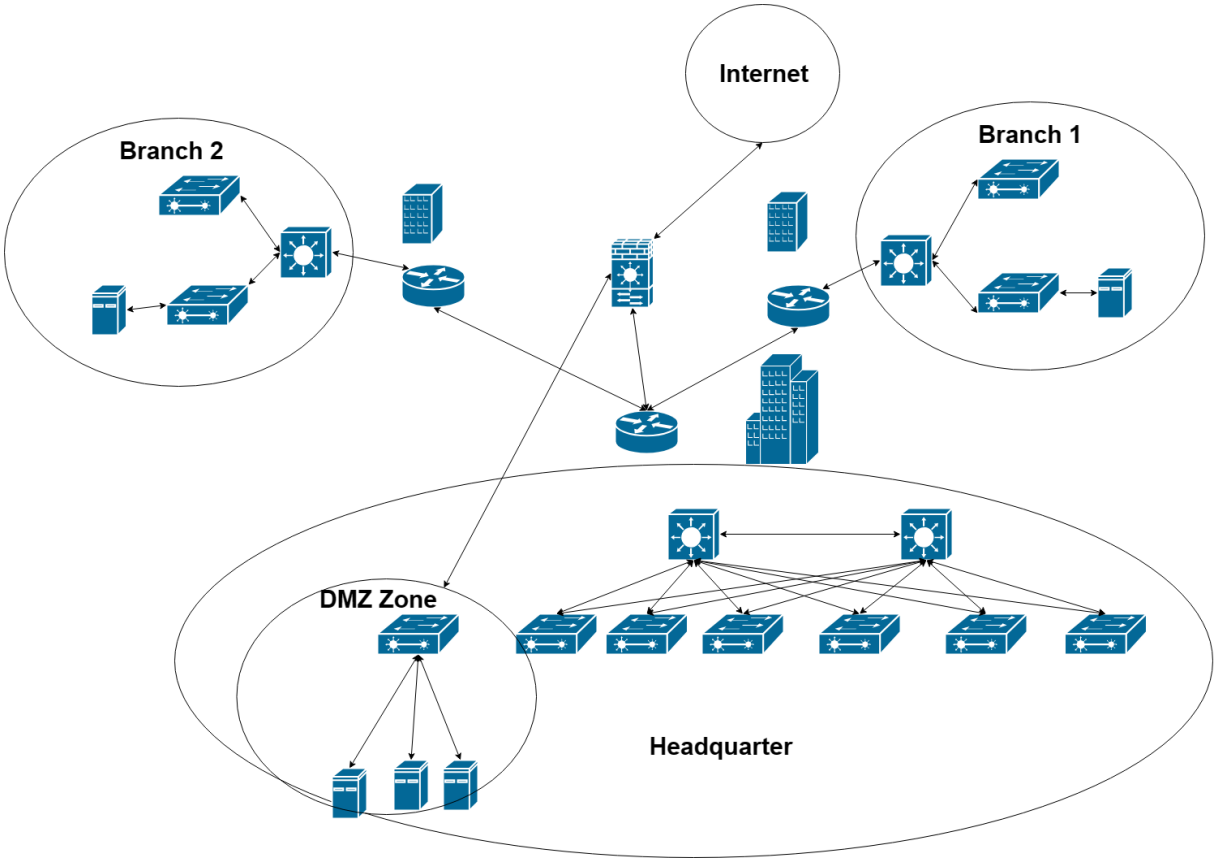
Hình 2: IP tại chi nhánh 1

Tại chi nhánh (branch) 2:

Tên mạng	IP/Subnet mask	IP khả dụng	Default gateway
VLAN100	192.168.10.0/24	192.168.10.1-254/24	192.168.10.1
VLAN110	192.168.11.0/24	192.168.11.1-254/24	192.168.11.1

Hình 3: IP tại chi nhánh 2

3.3 Sơ đồ thiết kế hệ thống



Hình 4: Sơ đồ hệ thống

4 Tính toán thông số cho các mạng máy

4.1 Thông lượng (Throughput) và băng thông (Bandwidth) cần thiết

4.1.1 Tại trụ sở

- Có 5 severs, tổng dung lượng download vào khoảng 1000 MB/ngày và upload 2000 MB/ngày cho mỗi sever:

  $Thông\ lượng = 5 \times (1000 + 2000) \times \frac{1}{8 \times 3600} = 0,5208(MBps) = 4,1667(Mbps)$

  $Băng\ thông = 5 \times (1000 + 2000) \times \frac{0,8}{3 \times 3600} = 1,1111(MBps) = 8,888(Mbps)$

- Có 120 workstations, tổng dung lượng upload 100 MB/ngày và download vào khoảng 500MB/ngày:

  $Thông\ lượng = 120 \times (100 + 500) \times \frac{1}{8 \times 3600} = 2,5(MBps) = 20(Mbps)$

  $Băng\ thông = 120 \times (100 + 500) \times \frac{0,8}{3 \times 3600} = 5,3333(MBps) = 42,6667(Mbps)$

- Giả sử có 100 khách hàng có laptop kết nối Wifi, mỗi laptop truy xuất download vào khoảng 500MB/ngày:

  $Thông\ lượng = 100 \times 500 \times \frac{1}{8 \times 3600} = 1,7361(MBps) = 13,8889(Mbps)$

  $Băng\ thông = 100 \times 500 \times \frac{0,8}{3 \times 3600} = 3,7037(MBps) = 29,6296(Mbps)$

$=>$ Tổng thông lượng và băng thông cần dùng tại trụ sở là:

$Thông\ lượng = 4,1667 + 20 + 13,8889 = 38,0556(Mbps)$

$Băng\ thông = 8,8888 + 42,6667 + 29,6296 = 81,1851(Mbps)$

4.1.2 Tại mỗi chi nhánh

- Có 3 severs, tổng dung lượng download vào khoảng 1000 MB/ngày và upload 2000 MB/ngày cho mỗi sever:

  $Thông\ lượng = 3 \times (1000 + 2000) \times \frac{1}{8 \times 3600} = 0,3125(MBps) = 2,5(Mbps)$

  $Băng\ thông = 3 \times (1000 + 2000) \times \frac{0,8}{3 \times 3600} = 0,6667(MBps) = 5,3333(Mbps)$

- Có 30 workstations, tổng dung lượng upload 100 MB/ngày và download vào khoảng 500MB/ngày:

  $Thông\ lượng = 30 \times (100 + 500) \times \frac{1}{8 \times 3600} = 0,625(MBps) = 4(Mbps)$

  $Băng\ thông = 30 \times (100 + 500) \times \frac{0,8}{3 \times 3600} = 1,3333(MBps) = 10,6667(Mbps)$

- Giả sử có 50 khách hàng có laptop kết nối Wifi, mỗi laptop truy xuất download vào khoảng 500MB/ngày:

  $Thông\ lượng = 50 \times 500 \times \frac{1}{8 \times 3600} = 0,8681(MBps) = 6,9444(Mbps)$

  $Băng\ thông = 50 \times 500 \times \frac{0,8}{3 \times 3600} = 1,8519(MBps) = 14,8148(Mbps)$

=> Tổng thông lượng và băng thông cần dùng tại trụ sở là:

$Thông\ lượng = 2,5 + 4 + 6,9444 = 13,4444(Mbps)$

$Băng\ thông = 5,3333 + 10,6667 + 14,8148 = 30,8148(Mbps)$

4.2 Đề xuất cấu hình

Để đảm bảo hệ thống mạng hoạt động ổn định khi ước tính rằng sẽ tăng trưởng 20% trong vòng 5 năm thì:

- Tại trụ sở

  $Thông\ lượng = 38,0556 \times 120\% = 45,6667(Mbps)$

  $Băng\ thông = 81,1851 \times 120\% = 97,4221$

- Tại mỗi chi nhánh

  $Thông\ lượng = 13,4444 \times 120\% = 16,1333(Mbps)$

  $Băng\ thông = 30,8148 \times 120\% = 36,9778$

5 Thiết kế hệ thống bảo mật, dự phòng và cân bằng tải

5.1 Yêu cầu với hệ thống

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.
- Phù hợp với điều kiện tài chính của công ty

Mặt khác, vì traffic lớn nên hệ thống ở cơ sở chính cũng cần xây dựng cơ chế cân bằng tải và dự phòng dư thừa, cụ thể cần đáp ấn

- Cân bằng tải: Đảm bảo không có tình trạng tắc nghẽn dữ liệu tại trụ sở chính, dữ liệu được sao chép giữa các máy chủ với nhau, đảm bảo rằng tất cả các máy chủ tài nguyên đều được sử dụng như nhau.
- Dự phòng dư thừa: Cung cấp thêm các linh kiện hoặc thiết bị làm việc đồng thời để đảm bảo hoạt động liên tục sau khi xảy ra sự cố

5.2 Các mối đe doạ với hệ thống

- **Mối đe doạ 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 doạ 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.

5.3 Đề xuất giải pháp

Với hệ thống 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.

- **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 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.

Với cơ chế cân bằng tải và an toàn khi xảy ra sự cố

- **Với đường truyền 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 đường truyền nội bộ:** Sử dụng giao thức HSRP (Hot standby router protocol) 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 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.
- **Cân bằng tải:** Sử dụng EtherChannel, nhóm hai hay nhiều đường kết nối truyền tải dữ liệu vật lý (Link Aggregation) thành một đường ảo duy nhất (Logic) có Port ảo thậm chí cả MAC ảo nhằm mục đích tăng tốc độ truyền dữ liệu và tăng khả năng dự phòng (Redundancy) cho hệ thống.Công nghệ EtherChannel có thể bó từ 2 đến 8 link FE, GE, 10GE thành 1 link logical. Khi đó, switch đối xử các port thuộc EtherChannel như 1 port duy nhất.

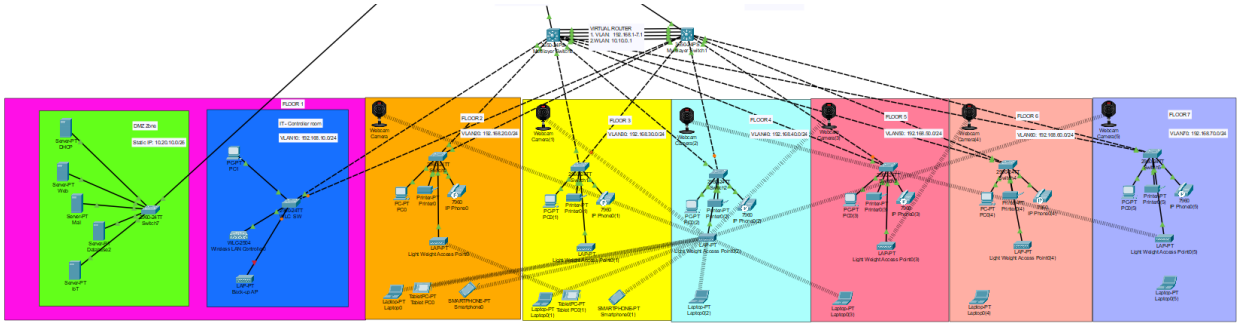
6 Mô phỏng bằng Cisco Packet Tracer

6.1 Trình tự thực hiện

- Lắp đặt mô phỏng các thiết bị tại trụ sở chính và chi nhánh
- Gán nhãn cho các phòng ban
- Thực hiện chia VLAN và cấu hình cơ bản cho các thiết bị
- Cấu hình HSRP và EtherChannel cho trụ sở chính
- Cấu hình các vùng sử dụng static IP
- Cấu hình các server, cài đặt DHCP Pool để cấp phát IP cho các thiết bị
- Cấu hình WAN IP và OSPF routing cho các router
- Cấu hình tường lửa, phân chia khu vực DMZ
- Cấu hình các thiết bị IoT
- Tiến hành kiểm thử

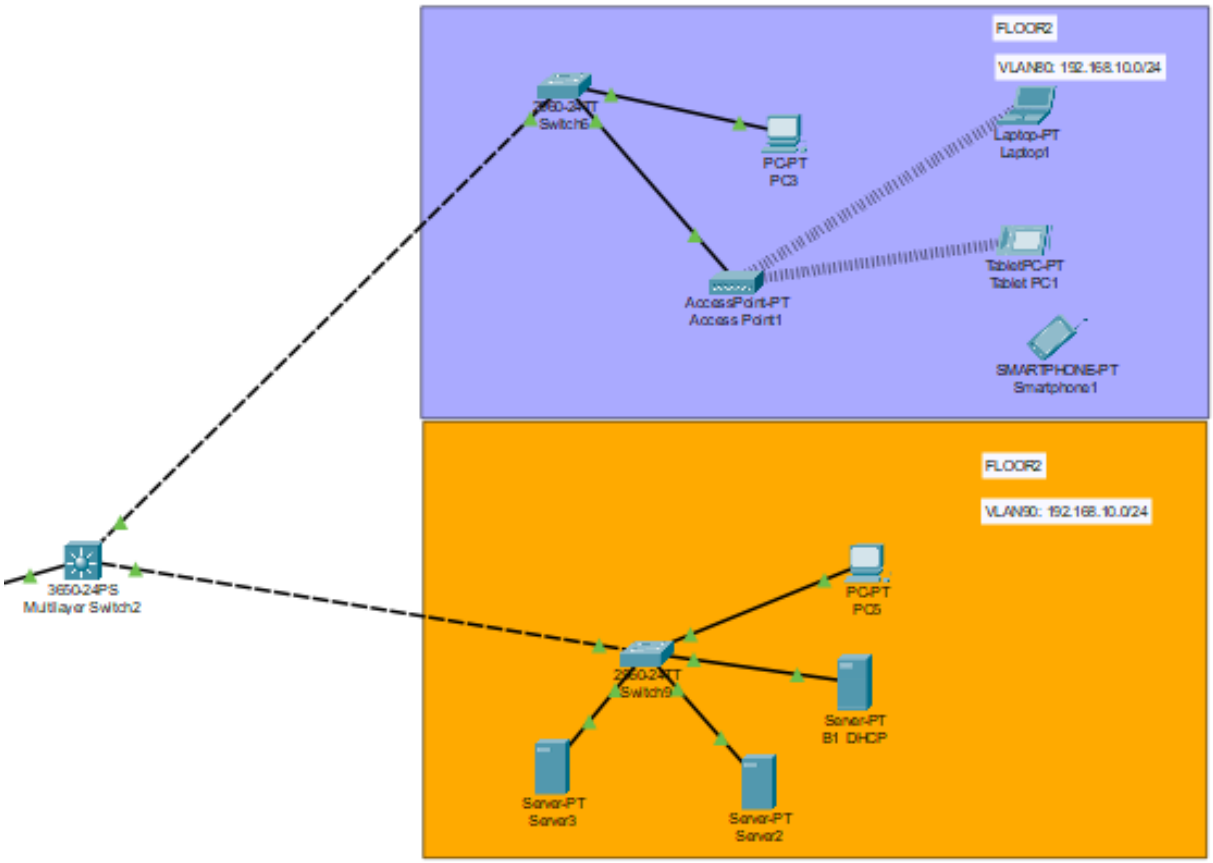
6.2 Kết quả hiện thực

Tại trụ sở chính:



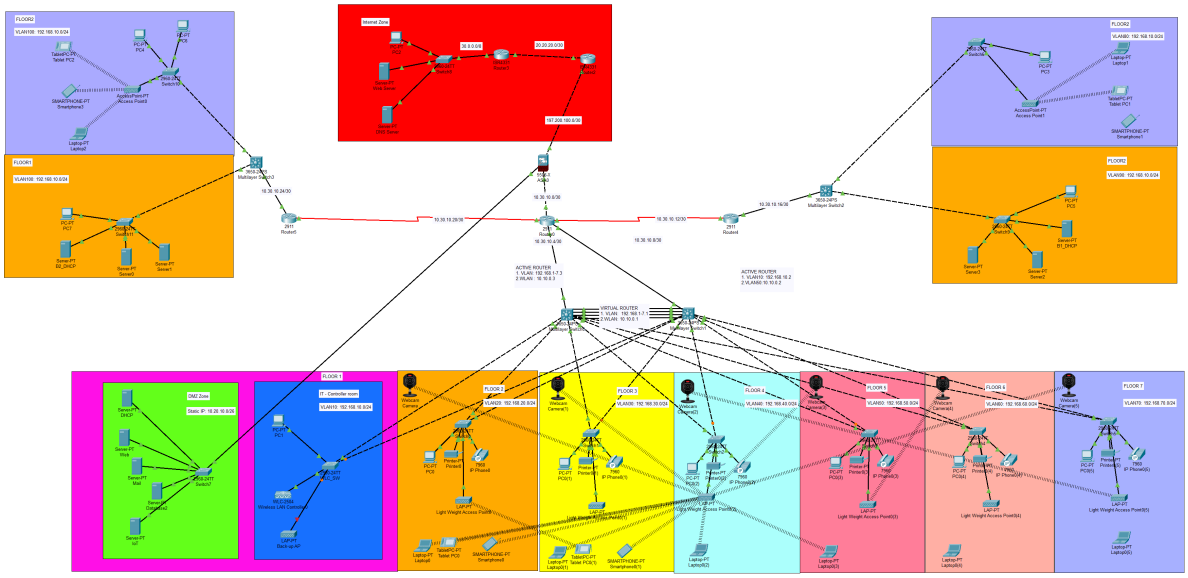
Hình 5: Trụ sở chính

Tại chi nhánh:



Hình 6: Chi nhánh

Toàn bộ hệ thống



Hình 7: Toàn hệ thống

6.3 Kiểm thử

Ping cùng 1 VLAN:

```
C:\>ping 192.168.2.5

Pinging 192.168.2.5 with 32 bytes of data:

Reply from 192.168.2.5: bytes=32 time<1ms TTL=128
Reply from 192.168.2.5: bytes=32 time<1ms TTL=128
Reply from 192.168.2.5: bytes=32 time<1ms TTL=128
Reply from 192.168.2.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Hình 8: Ping cùng VLAN

Ping giữa các VLAN:

```
C:\>ping 192.168.3.4

Pinging 192.168.3.4 with 32 bytes of data:

Reply from 192.168.3.4: bytes=32 time<1ms TTL=127
Reply from 192.168.3.4: bytes=32 time=1ms TTL=127
Reply from 192.168.3.4: bytes=32 time<1ms TTL=127
Reply from 192.168.3.4: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.3.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Hình 9: Ping khác VLAN

Ping tới chi nhánh

```
C:\>ping 192.168.9.5

Pinging 192.168.9.5 with 32 bytes of data:

Request timed out.
Reply from 192.168.9.5: bytes=32 time=2ms TTL=124
Reply from 192.168.9.5: bytes=32 time=1ms TTL=124
Reply from 192.168.9.5: bytes=32 time=1ms TTL=124

Ping statistics for 192.168.9.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 192.168.9.5

Pinging 192.168.9.5 with 32 bytes of data:

Reply from 192.168.9.5: bytes=32 time=1ms TTL=124
Reply from 192.168.9.5: bytes=32 time=3ms TTL=124
Reply from 192.168.9.5: bytes=32 time=2ms TTL=124
Reply from 192.168.9.5: bytes=32 time=2ms TTL=124

Ping statistics for 192.168.9.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

Hình 10: Ping chi nhánh

Ping tới Internet

```
C:\>ping 30.0.0.10

Pinging 30.0.0.10 with 32 bytes of data:

Request timed out.
Reply from 30.0.0.10: bytes=32 time<1ms TTL=123
Reply from 30.0.0.10: bytes=32 time=1ms TTL=123
Reply from 30.0.0.10: bytes=32 time<1ms TTL=123

Ping statistics for 30.0.0.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 30.0.0.10

Pinging 30.0.0.10 with 32 bytes of data:

Reply from 30.0.0.10: bytes=32 time<1ms TTL=123
Reply from 30.0.0.10: bytes=32 time<1ms TTL=123
Reply from 30.0.0.10: bytes=32 time=1ms TTL=123
Reply from 30.0.0.10: bytes=32 time<1ms TTL=123

Ping statistics for 30.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

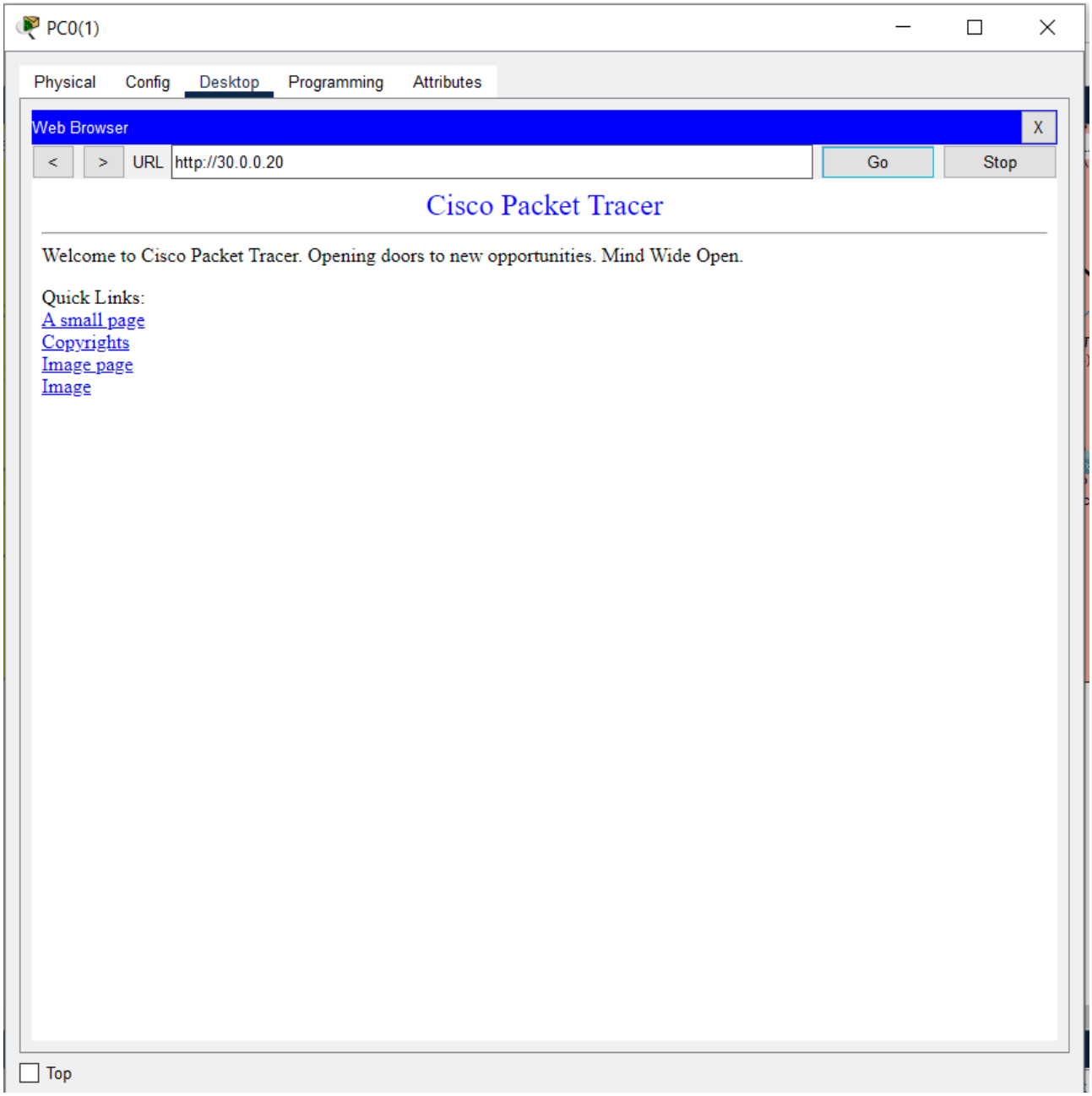
Hình 11: Ping Internet

Ping tới DMZ

```
C:\>ping 10.20.10.10

Pinging 10.20.10.10 with 32 bytes of data:

Reply from 10.20.10.10: bytes=32 time<1ms TTL=125
Reply from 10.20.10.10: bytes=32 time<1ms TTL=125
Reply from 10.20.10.10: bytes=32 time<1ms TTL=125
Reply from 10.20.10.10: bytes=32 time<1ms TTL=125

Ping statistics for 10.20.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

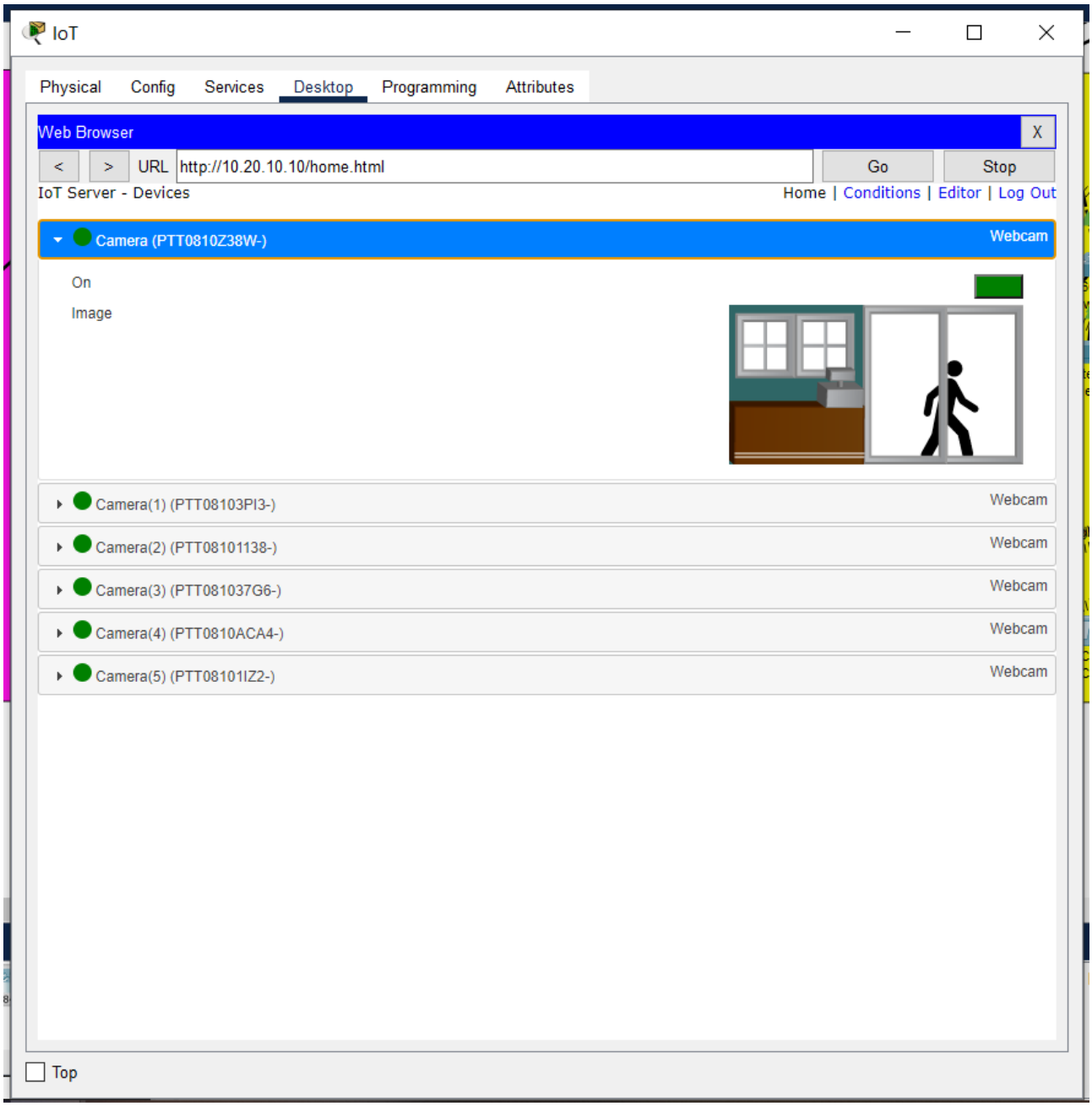
Hình 12: Ping DMZ

Kết nối tới Web Server trên Internet



Hình 13: Web connect

Hệ thống camera



Hình 14: Camera

7 Đánh giá lại hệ thống

7.1 Kết quả đạt được của dự án

- Nhóm đã có thể làm quen với ứng dụng Cisco Packet Tracer và đã tìm hiểu về các giải pháp thiết kế phần cứng cũng như cách cấu hình các thiết bị mạng. Chúng tôi cũng đã có khả năng thiết kế một hệ thống mạng có quy mô vừa hoặc nhỏ, bao gồm việc thiết kế mô hình IP và mô hình đi dây cho công ty.
- Hệ thống mạng hiện tại đáp ứng tương đối phù hợp với yêu cầu được đưa ra và cũng có khả năng nâng cấp phù hợp với sự phát triển trong tương lai.
- Việc sử dụng các trang thiết bị của tập đoàn Cisco đảm bảo chất lượng cao, giúp giảm chi phí bảo trì trong tương lai. Đồng thời, sự chất lượng tốt của đường truyền và hỗ trợ kỹ thuật đầy đủ từ Cisco cũng đóng một vai trò quan trọng trong việc duy trì và hoạt động của hệ thống mạng.
- Hệ thống có băng thông lớn, đủ để đáp ứng toàn bộ nhu cầu của nhân viên trong công ty. Hệ thống mạng LAN được thiết kế dưới dạng mô hình hình sao để đảm bảo rằng quá trình hoạt động vẫn diễn ra bình thường ngay cả khi một nút thông tin bị hỏng. Điều này giúp nâng cao hiệu suất và khả năng làm việc của nhân viên.
- 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.

7.2 Hạn chế của dự án

- Chưa có kiến thức cụ thể về một mạng doanh nghiệp, việc thiết kế có thể gặp khó khăn trong việc quyết định các mô hình, công nghệ và thiết bị nên được sử dụng.
- Các phương pháp bảo mật và cân bằng tải chủ yếu được áp dụng tại trụ sở chính, công nghệ chủ yếu được trình bày trên kế hoạch, chưa thực sự triển khai để đánh giá độ hiệu quả
- 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 VPN cho công ty.

7.3 Định hướng phát triển

- Trong tương lai, có khả năng rằng công ty sẽ phát triển và mở rộng hoạt động của mình đến nhiều địa điểm khác. Vì vậy, việc xem xét khả năng mở rộng hệ thống mạng giữa trụ sở và các chi nhánh là rất quan trọng.

- Hiện tại, giả sử có khoảng 200 nhân viên và họ được phân bố đều trên 7 tầng của toà nhà. Điều này có nghĩa là mỗi tầng có khoảng 30 người, tương đương với 30 máy tính cá nhân. Tuy nhiên, cần lưu ý rằng số lượng cổng tối đa của switch là 24 cổng. Vì vậy, khi số lượng nhân viên tăng lên đến một mức độ nhất định, chúng ta có thể không cần phải thay đổi hoặc mua thêm thiết bị mạng khác.
- Về vấn đề băng thông, khi cần nâng cấp, chúng ta chỉ cần đăng ký thay đổi gói cước với nhà cung cấp dịch vụ. Hơn nữa, trong hệ thống mạng hiện tại chưa có giải pháp cân bằng tải (Network Load Balancing), do đó, trong tương lai, có thể xem xét thiết kế thêm hệ thống cân bằng tải để đảm bảo phân phối đồng đều lưu lượng truy cập giữa các máy chủ có cùng chức năng.
- Liên quan đến vấn đề bảo mật của mô hình trong tương lai, có thể phát triển thêm hệ thống tường lửa cục bộ cho cả trụ sở và các chi nhánh. Đồng thời, cần thiết kế một hệ thống để ngăn chặn khách hàng sử dụng wifi để truy cập vào hệ thống mạng LAN một cách hiệu quả hơn so với việc ngăn chặn trên Switch layer 3.