TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**

**Logo

Description automatically generated**

**PHÙ Ý KỲ - 51800989**

**NGUYỄN THỊ HỒNG HƯƠNG - 51800284**

**THIẾT KẾ VÀ TRIỂN KHAI CÁC CHỨC NĂNG BẢO MẬT MẠNG CHO HỆ THỐNG MẠNG DOANH NGHIỆP CÓ TỪ HAI CHI NHÁNH TRỞ LÊN**

**DỰ ÁN CÔNG NGHỆ THÔNG TIN 2**

**MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG DỮ LIỆU**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2022**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**

**Logo

Description automatically generated**

**PHÙ Ý KỲ - 51800989**

**NGUYỄN THỊ HỒNG HƯƠNG - 51800284**

**THIẾT KẾ VÀ TRIỂN KHAI CÁC CHỨC NĂNG BẢO MẬT MẠNG CHO HỆ THỐNG MẠNG DOANH NGHIỆP CÓ TỪ HAI CHI NHÁNH TRỞ LÊN**

**DỰ ÁN CÔNG NGHỆ THÔNG TIN 2**

**MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG DỮ LIỆU**

Người hướng dẫn

**TS. TRƯƠNG ĐÌNH TÚ**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2022**

LỜI CẢM ƠN

Lời đầu tiên chúng em xin gửi lời cảm ơn đến các thầy cô ở khoa Công nghệ thông tin - Trường Đại Học Tôn Đức Thắng, đã cùng với tri thức và tâm huyết của mình để truyền đạt vốn kiến thức quý báu của mình cho chúng em trong suốt thời gian ngồi trên ghế nhà trường. Và trong học kỳ này, khoa đã đặc biệt tổ chức cho sinh viên tiếp cận đến môn “Dự án Công nghệ thông tin 2”, tạo điều kiện tốt nhất cho ra những đề tài dự án đối với sinh viên khoa công nghệ thông tin là rất bổ ích, để đúc kết ra những kinh nghiệm, kiến thức thực tiễn, vá lại những lổ hổng kiến thức cho sinh viên.

Bên cạnh đó, chúng em đặc biệt gửi tới thầy Trương Đình Tú lời cảm ơn chân thành sâu sắc nhất, là giảng viên đã hướng dẫn chúng em trong đề tài dự án này, thầy đã giảng dạy và trang bị cho chúng em thêm những kiến thức cơ bản, đã tận tình hướng dẫn nhiệt tình cho chúng em trong quá trình làm đề tài dự án do thầy phụ trách. Nếu không có những lời hướng dẫn, dạy bảo của thầy thì chúng em khó có thể hoàn thiện được bài báo cáo dự án này một cách hoàn thiện nhất. Do còn nhiều thiếu sót kinh nghiệm, và kiến thức nên không tránh khỏi những sai sót khi thực hiện dự án. Chúng em mong các quý thầy cô chỉ điểm thêm và giúp chúng em hoàn thành tốt bài báo cáo và đạt kết quả tốt hơn. Sau cùng, chúng em xin kính chúc quý thầy cô thật dồi dào sức khỏe, niềm tin mãnh liệt để tiếp tục sứ mệnh cao đẹp của mình là truyền đạt kiến thức cho thế hệ mai sau trong sự nghiệp trồng người.

*TP. Hồ Chí Minh, ngày tháng năm*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Nguyễn Thị Hồng Hương*

*Phù Ý Kỳ*

**CÔNG TRÌNH ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Chúng tôi xin cam đoan đây là công trình của riêng chúng tôi và được sự hướng dẫn khoa học của TS Trương Đình Tú. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong báo cáo còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào chúng tôi xin hoàn toàn chịu trách nhiệm về nội dung báo cáo Dự án CNTT 2 của mình.** Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày tháng năm*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Nguyễn Thị Hồng Hương*

*Phù Ý Kỳ*

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

**Phần xác nhận của GV hướng dẫn**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**Phần đánh giá của GV chấm bài**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

TÓM TẮT

Mạng máy tính ngày nay được đông dảo người quan tâm, vì xu thế công nghệ cao hiện đại mọi nơi đều cần một mạng lưới phù hợp để kết nối cái thiết bị thông minh một cách nhanh chóng, không bị tắc nghẽn mang đến trải nghiệm cuộc sống hiên đại, tốt đẹp hơn. Tóm lại, chủ đề bài báo cáo đang cần nghiên cứu về thiết kế hệ thống mạng doanh nghiệp, một mạng lưới cần nâng cao bảo mật hơn bao giờ hết. Bài báo cáo này thực hiện những nghiên cứu tìm hiểu cũng như thiết kế và triển khai các chức năng bảo mật mạng cho hệ thống mạng doanh nghiệp có từ hai chi nhánh trở lên (cụ thể trong báo cáo thiết kế mô phỏng lại hệ thống mạng doanh nghiệp qua Packet Tracer). Mô hình chỉ thể hiện được rõ nét mạng lưới ở chi nhánh chính và hệ thống mạng vẫn kết nối bảo mật với các chi nhánh khác. Bài báo cáo được thực hiện gồm:

CHƯƠNG 1 – TỔNG QUAN: Trình bày về mục tiêu và lý do chọn đề tài, đối tượng và phạm vi nghiên cứu, cuối cùng ý nghĩa khoa học và thực tiễn của đề tài.

CHƯƠNG 2 – CƠ SỞ LÝ THUYẾT: Giới thiệu các sơ lược về Mạng máy tính cũng như các lý thuyết về mạng như mô hình mạng, cách bảo mật mạng, và những giao thức kỹ thuật, phương diện liên quan.

CHƯƠNG 3 – THIẾT KẾ HỆ THỐNG MẠNG DOANH NGHIỆP: Tiến hành phân tích hệ thống mạng cho doanh nghiệp, tìm giải pháp để ra mô hình theo yêu cầu khách hàng. Từ đó đưa ra các thông tin về IP trong hệ thống mạng.

CHƯƠNG 4 –CẤU HÌNH HẠ TẦNG: Bắt đầu tiến hành cấu hình những phương thức, kỹ thuật bảo mật cho mô hình hệ thống mạng doanh nghiệp, kiểm tra hoạt động của hệ thống sau khi hoàn thiện cấu hình.

CHƯƠNG 5 – KẾT LUẬN: Đưa ra kết quả đạt được cũng như những mặt hạn chế so với mục tiêu ban đầu và nêu ra những hướng phát triển sau này.

MỤC LỤC

[LỜI CẢM ƠN i](#_Toc108892573)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iii](#_Toc108892574)

[TÓM TẮT iv](#_Toc108892575)

[MỤC LỤC 1](#_Toc108892576)

[DANH MỤC HÌNH VẼ 6](#_Toc108892577)

[DANH MỤC BẢNG BIỂU 7](#_Toc108892578)

[CHƯƠNG 1 - TỔNG QUAN 8](#_Toc108892579)

[1.1 Mục tiêu chọn đề tài 8](#_Toc108892580)

[1.2 Lý do chọn đề tài 8](#_Toc108892581)

[1.3 Đối tượng và phạm vi nghiên cứu 8](#_Toc108892582)

[1.4 Ý nghĩa khoa học và thực tiễn của đề tài 9](#_Toc108892583)

[CHƯƠNG 2 - CƠ SỞ LÝ THUYẾT 10](#_Toc108892584)

[2.1 Mạng máy tính 10](#_Toc108892585)

[2.1.1 Khái niệm 10](#_Toc108892586)

[2.1.2 Phân loại các mô hình mạng máy tính 10](#_Toc108892587)

[2.2 Mô hình mạng ba lớp 12](#_Toc108892588)

[2.3 Bảo mật mạng máy tính là gì? 13](#_Toc108892589)

[2.4 Firewall 14](#_Toc108892590)

[2.4.1 Giới thiệu về Firewall 14](#_Toc108892591)

[2.4.2 Phân loại Firewall 14](#_Toc108892592)

[2.5 Network Address Translation (NAT) 16](#_Toc108892593)

[2.5.1 NAT là gì? 16](#_Toc108892594)

[2.5.2 Một số thuật ngữ về NAT 16](#_Toc108892595)

[2.5.3 Các loại NAT 17](#_Toc108892596)

[2.5.3.1 Static NAT 17](#_Toc108892597)

[2.5.3.2 Dynamic NAT 18](#_Toc108892598)

[2.5.3.3 Port Address Translation (PAT) 20](#_Toc108892599)

[2.6 Access Control List (ACL) 20](#_Toc108892600)

[2.6.1 ACL là gì? 20](#_Toc108892601)

[2.6.2 Hoạt động ACL 21](#_Toc108892602)

[2.6.3 Wildcard mask 21](#_Toc108892603)

[2.6.4 Phân loại ACL 22](#_Toc108892604)

[2.7 Tổng quan AAA 22](#_Toc108892605)

[2.8 Công nghệ VPN 23](#_Toc108892606)

[2.8.1 Site-to-site VPN 23](#_Toc108892607)

[2.8.2 Remote Access VPN 24](#_Toc108892608)

[CHƯƠNG 3 - THIẾT KẾ HỆ THỐNG MẠNG DOANH NGHIỆP 24](#_Toc108892609)

[3.1 Mô tả hệ thống 24](#_Toc108892610)

[3.2 Phân tích hệ thống 25](#_Toc108892611)

[3.2.1 Yêu cầu khách hàng 25](#_Toc108892612)

[3.2.2 Đề xuất hướng giải quyết 25](#_Toc108892613)

[3.3 Thiết kế hệ thống 26](#_Toc108892614)

[3.3.1 Mô hình demo 26](#_Toc108892615)

[3.3.2 Dùng kỹ thuật Variable Length Subnet Masking (VLSM) chia mạng con cho các phòng ban trong doanh nghiệp 27](#_Toc108892616)

[3.3.3 Thông tin địa chỉ trong hệ thống 30](#_Toc108892617)

[3.3.4 Thông tin vlan, interface vlan trong hệ thống 33](#_Toc108892618)

[3.3.5 Thông tin cổng Etherchannels 34](#_Toc108892619)

[CHƯƠNG 4 - CẤU HÌNH HẠ TẦNG 35](#_Toc108892620)

[4.1 Thiết lập VTP 35](#_Toc108892621)

[4.2 VLAN cho các phòng ban trong doanh nghiệp 36](#_Toc108892622)

[4.3 Cấu hình tính dự phòng 37](#_Toc108892623)

[4.3.1 HSRP 37](#_Toc108892624)

[4.3.2 Spanning-tree 38](#_Toc108892625)

[4.4 Cấu hình tuyến EIGRP và VPN 39](#_Toc108892626)

[4.5 Thiết lập các dịch vụ Server 41](#_Toc108892627)

[4.6 Xác thực AAA 43](#_Toc108892628)

[4.7 NAT và ACL 44](#_Toc108892629)

[4.8 Thiết lập bảo mật Switch 44](#_Toc108892630)

[4.8.1 Cấu hình DHCP Snooping 44](#_Toc108892631)

[4.8.2 Cấu hình DAI (Dynamic ARP Inspection) 46](#_Toc108892632)

[4.9 Test case 47](#_Toc108892633)

[4.9.1 Tình huống 1 47](#_Toc108892634)

[4.9.2 Tình huống 2 49](#_Toc108892635)

[4.9.3 Tình huống 3 50](#_Toc108892636)

[4.9.4 Tình huống 4 52](#_Toc108892637)

[4.9.5 Tình huống 5 53](#_Toc108892638)

[CHƯƠNG 5 - KẾT LUẬN 54](#_Toc108892639)

[5.1 Những kết quả đạt được 54](#_Toc108892640)

[5.2 Những hạn chế và hướng phát triển 54](#_Toc108892641)

[TÀI LIỆU THAM KHẢO 55](#_Toc108892642)

[PHỤ LỤC 56](#_Toc108892643)

**DANH MỤC CÁC CHỮ VIẾT TẮT**

**CÁC CHỮ VIẾT TẮT**

AAA Authentication, Authorization, Accounting

ACL Access Control List

ACEs Access Control Entries

ATM Automated Teller Machine

ARP Address Resolution Protocol

CNTT Công nghệ thông tin

DAI Dynamic ARP Inspection

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

DoS Denial of Service

DSL Digital Subscriber Line

EIGRP Enhanced Interior Gateway Routing Protocol

FTP File Transfer Protocol

GPRS General Packet Radio Services

HTTP Hypertext Transfer Protocol

HSRP Hot Standby Router Protocol

IOS Internetwork Operating System

IP Internet Protocol

ISDN Integrated Services Digital Network

IPsec Internet Protocol Security

LAN Local Area Network

NAT Network Address Translation

NGFW Next Generation Firewall

NIC Network Information Center

PAT Port Address Translation

SSH Secure Shell Protocol

SSL Secure Sockets Layer

TACACS Terminal Access Controller Access Control System

TCP Transmission Control Protocol

UDP User Datagram Protocol

URL Uniform Resource Locator

VLAN Virtual Local Area Network

VLSM Variable Length Subnet Masking

VTP Vlan Trunking Protocol

VPN Virtual Private Network

WAN Wide Area Network

DANH MỤC HÌNH VẼ

[Hình 2.1 Mô hình phân cấp mạng 3 lớp (3-layer hierarchical topology) 12](#_Toc108892644)

[Hình 2.2 Mức độ bảo mật 14](#_Toc108892645)

[Hình 2.3 Mô hình ví dụ về static NAT 18](#_Toc108892646)

[Hình 2.4 Mô hình minh họa cho dynamic NAT 19](#_Toc108892647)

[Hình 2.5 Hình minh họa áp dụng ACL cho lưu lượng đi vào và đi ra 21](#_Toc108892648)

[Hình 3.1 Mô hình mạng doanh nghiệp với ba cơ sở 26](#_Toc108892649)

[Hình 4.1 Giao diện hiển thị trạng thái VTP trên SW1\_Quanly 35](#_Toc108892650)

[Hình 4.2 Giao hiện hiển thị trạng thái VTP trên SW2\_Quanly 35](#_Toc108892651)

[Hình 4.3 Giao hiện hiển thị các vlan có trong hệ thống ở cơ sở Hồ Chí Minh 36](#_Toc108892652)

[Hình 4.4 Giao diện hiển thị các vlan có trong hệ thống ở hai chi nhánh. 37](#_Toc108892653)

[Hình 4.5 Giao diện hiển thị thông tin HSRP trên SW1\_Quanly 38](#_Toc108892654)

[Hình 4.6 Giao diện hiển thị thông tin HSRP trên SW2\_Quanly 38](#_Toc108892655)

[Hình 4.7 Giao diện hiển thị thông tin tổng của spanning tree 38](#_Toc108892656)

[Hình 4.8 Giao diện thông tin định tuyến trên router HoChiMinh\_1 39](#_Toc108892657)

[Hình 4.9 Giao diện thông tin định tuyến trên router HoChiMinh\_2 40](#_Toc108892658)

[Hình 4.10 Giao diện thông tin định tuyến trên router DaNang 41](#_Toc108892659)

[Hình 4.11 Giao diện thông tin định tuyến trên router HaiPhong 41](#_Toc108892660)

[Hình 4.12 Giao diện web của doanh nghiệp 42](#_Toc108892661)

[Hình 4.13 Hình minh họa hai người dùng trao đổi email thành công 42](#_Toc108892662)

[Hình 4.14 Hình minh họa đổi tên file.txt thành công 42](#_Toc108892663)

[Hình 4.15 Giao diện dịch vụ TACACS Server 43](#_Toc108892664)

[Hình 4.16 Giao diện xác thực dịch vụ Tacacs 43](#_Toc108892665)

[Hình 4.17 Giao diện hiển thị thông tin NAT Overload trên router HoChiMinh\_2 44](#_Toc108892666)

[Hình 4.18 Giao diện hiển thị thông tin static NAT 44](#_Toc108892667)

[Hình 4.19 Giao diện hiển thị thông tin DHCP Snooping trên SW1\_Quanly 45](#_Toc108892668)

[Hình 4.20 Giao diện hiển thị thông tin DHCP Snooping trên swich CNTT 45](#_Toc108892669)

[Hình 4.21 Giao diện hiển thị thông tin các cổng khi cấu hình DAI trên switch CNTT 46](#_Toc108892670)

[Hình 4.22 Giao diện hiển thị đã thực hiện cấu hình DAI 46](#_Toc108892671)

[Hình 4.23 Bảng định tuyến trên switch SW1\_Quanly sau khi bị đứt dây 47](#_Toc108892672)

[Hình 4.24 Giao diện PC Bán hàng đang truy cập ra internet 48](#_Toc108892673)

[Hình 4.25 Host\_Banhang truy cập internet sau khi bị đứt dây ở router HoChiMinh\_1 48](#_Toc108892674)

[Hình 4.26 Giao diện máy tính ở phòng CNTT đang truy cập internet. 49](#_Toc108892675)

[Hình 4.27 Giao diện Host\_CNTT truy cập internet sao khi SW1\_Quanly bị chết. 49](#_Toc108892676)

[Hình 4.28 Giao diện Host CNTT telnet vào router HoChiMinh\_1 50](#_Toc108892677)

[Hình 4.29 Giao diện host Dienmay telnet vào router HoChiMinh\_2 51](#_Toc108892678)

[Hình 4.30 Giao diện host ở Banhang và Marketing telnet vào router HoChiMinh\_1 51](#_Toc108892679)

[Hình 4.31 PC Sale\_1 và Giamdoc\_1 telnet vào router DaNang 52](#_Toc108892680)

[Hình 4.32 PC IT\_2 telnet vào router DaNang 52](#_Toc108892681)

[Hình 4.33 Giao diện ping kiểm tra truy cập trên máy tính Sale\_1 53](#_Toc108892682)

# DANH MỤC BẢNG BIỂU

[Bảng 3.1 Bảng thông tin địa chỉ dùng VLSM chia mạng con cho trụ sở chính 29](#_Toc108892683)

[Bảng 3.2 Bảng thông tin địa chỉ dùng VLSM chia mạng con cho chi nhánh thứ nhất 29](#_Toc108892684)

[Bảng 3.3 Bảng thông tin địa chỉ dùng VLSM chia mạng con cho chi nhánh thứ hai 30](#_Toc108892685)

[Bảng 3.4 Bảng địa chỉ trong hệ thống 33](#_Toc108892686)

[Bảng 3.5 Bảng địa chỉ vlan trong hệ thống 34](#_Toc108892687)

[Bảng 3.6 Bảng thông tin về Etherchannels 34](#_Toc108892688)

# TỔNG QUAN

## Mục tiêu chọn đề tài

* Tìm hiểu một số lý thuyết mạng cơ bản liên quan đến bảo mật và ứng dụng vào mô hình mạng cho doanh nghiệp.
* Sử dụng packet tracer để thiết kế hệ thống mạng cho doanh nghiệp.
* Triển khai được các cấu hình mạng căn bản đồng thời hiểu được và cấu hình được các chức năng bảo mật mạng: Firewall, xác thực AAA, ACLs, VPN, cấu hình bảo mật Switch, …
* Đảm bảo hệ thống hoạt động được bình thường, ổn định và an toàn.

## Lý do chọn đề tài

Bảo mật là một phạm trù rộng và phức tạp trong lĩnh vực công nghệ thông tin nhằm mang lại sự an toàn cho hệ thống mạng cũng như thông tin của một tổ chức nào đó. Với các kiến thức đã được lĩnh hội đồng thời được tiếp cận môn học, chúng em mong muốn được thiết kế một hệ thống mạng với các chức năng bảo mật cho doanh nghiệp cũng để nhằm cải thiện, nâng cao kiến thức chuyên ngành và hoàn thiện kĩ năng của chính bản thân.

## Đối tượng và phạm vi nghiên cứu

Những người đang học hoặc nghiên cứu về ngành lĩnh vực công nghệ thông tin quan tâm tới mạng đường truyền và để áp dụng cho bên ngoài thực tiễn hơn bao giờ hết là vào mạng quốc gia, doanh nghiệp và gia đình.

Phạm vi nghiên cứu bài báo cáo này là kết hợp các lý thuyết đã học được và thiết kế, triển khai một mô hình mạng doanh nghiệp từ đơn giản đến phức tạp cho đến những người mới học và những người đã có kinh nghiệm để tích lũy thêm kiến thức và kinh nghiệm hiểu thêm về thiết kế hệ thống mạng một cách tốt nhất. Có những phần dịch vụ máy chủ nên có một doanh nghiệp như DNS và DHCP, FTP, Mail, Web, … Cho tới những dịch vụ để bảo mật tốt hơn cho hệ thống mạng như triển khai xác thực AAA, ACL, VPN, và phương pháp bảo mật Switch.

## Ý nghĩa khoa học và thực tiễn của đề tài

Giúp bảo vệ được mạng nội bộ trong doanh nghiệp khỏi những tấn công từ bên ngoài, và đảm bảo trong doanh nghiệp mỗi người chỉ được sử dụng mạng đúng mục đích mà doanh nghiệp mong muốn. Giúp bảo vệ được nội dung trong server vật lý khỏi những cá nhân không được cho phép.

Và để đảm bảo đủ số địa chỉ mạng ip của mạng nội bộ doanh nghiệp cấp cho tất cả các máy trong một cơ quan, phòng ban dù có tăng lên cũng có thể kết nối chúng một cách nhanh chóng và đảm bảo có đường truyền dự phòng để không bị gặp trục trặc trong vấn đề truyền tải dữ liệu làm chậm trễ thời gian làm việc của doanh nghiệp.

Thêm vào đó, những kiến thức của đề tài này có thể cũng được mở rộng không chỉ áp dụng qua thiết kế hệ thống mạnh doanh nghiệp mà còn qua những lĩnh vực khác trong xã hội cũng được khá quan tâm và thực thi là trong: thương mại, quân sự, quốc phòng, các dịch vụ, giáo dục, khoa học, công nghệ, …

Tuy nhiên, để áp dụng kiểm soát được chặt chẽ sự bảo mật lẫn tính sẵn sàng cao và sự dự phòng tuyệt đối trong lĩnh vực xã hội vẫn còn là một thách thức lớn và cần cải thiện thêm cho những công nghệ máy móc sau này như tăng tốc độ mạng máy tính khi người dùng cần truy cập mạng internet một nhanh chóng nhất vẫn bảo mật. Đồ án đề tài của nhóm chúng em cũng chỉ để nhằm thể hiện cách thức hoạt động của một mạng doanh nghiệp có từ 2 chi nhánh trờ lên để cụ thể hình dung hóa dễ dàng hơn, là thấy được sự ổn định các phương thức được cấu hình, thiết lập, dễ dàng, tăng tính năng bảo mật, cấu hình sao cho phù hợp đường truyền của mạng doanh nghiệp chúng em đã thiết kế ra.

# CƠ SỞ LÝ THUYẾT

## Mạng máy tính

### Khái niệm

Mạng máy tính là một tập hợp các máy tính được liên kết theo một cách nào đó nhằm mục đích trao đổi và chia sẻ thông tin với nhau, với các lợi ích sau:

* Một thiết bị ngoại vi (máy in, modem, v.v.) hoặc phần mềm có thể được chia sẻ bởi một số lượng lớn các cá nhân.
* Dữ liệu được kiểm soát tập trung sẽ an toàn hơn và giao tiếp dữ liệu giữa những người dùng sẽ nhanh hơn và dễ dàng hơn. Người dùng có thể trao đổi tin nhắn với nhau một cách đơn giản và nhanh chóng.
* Có thể cài đặt Internet trên bất kỳ máy nào trong mạng, sau đó thiết lập và cấu hình cho các máy tính khác thông qua máy đã cài đặt ứng dụng chia sẻ Internet để kết nối Internet.
* Cho phép liên hệ qua email, video, trò chuyện tức thì và các phương tiện khác.

Tệp, phần mềm và hệ điều hành là tất cả các ví dụ về dữ liệu.

### Phân loại các mô hình mạng máy tính

Sau đây là các mô hình mạng máy tính phổ biến:

* Mạng ngang hàng (Peer-to-Peer): Trong cấu hình này, các máy có vai trò ngang nhau khi trong một mạng. Có thể chia sẻ ngay lập tức tài nguyên và dữ liệu máy tính với nhau. Mạng ngang hàng chỉ thích hợp với mạng quy mô nhỏ với tài nguyên quản lý phân tán. Nhược điểm của hệ thống mạng này là không đủ phương thức bảo mật.
* Máy khách - Máy chủ (Client - Server): Một máy được chỉ định làm máy chủ (Server) phụ trách quản lý và phân phối tài nguyên, dữ liệu cho các máy tính khác. Máy khách (Client) là máy tính sử dụng dữ liệu từ máy tính. Máy chủ trong hệ thống này có nhiệm vụ chỉ định việc phân bổ tài nguyên mạng cho mục đích sử dụng chung. Đảm bảo rằng dữ liệu được cung cấp và phục vụ máy khách một cách có phương pháp. Máy khách là một máy sử dụng tài nguyên của máy chủ với dữ liệu được kiểm soát tập trung, bảo mật và thích hợp cho các mạng vừa và lớn.
* Mạng liên kết nối (mạng theo web) Mạng máy tính diện rộng là mạng được liên kết thông qua mạng internet. Trở thành một thành phần thiết yếu trong hoạt động của bất kỳ cá nhân, tổ chức, doanh nghiệp hoặc tập đoàn nào trên thế giới. Là mạng liên kết, phục vụ để liên kết mọi người trên toàn thế giới.

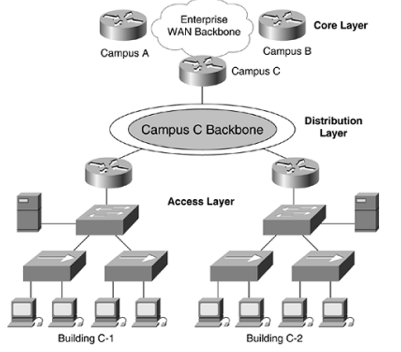
Ngoài ra, phân loại mạng máу tính kết nối dưới góc địa lý ở các dạng sau:

* LAN (Local Area Network) là mạng cục bộ kết nối các máy tính trong phạm vi vài trăm mét với nhau. Cáp xoắn đôi, cáp đồng trục và cáp quang là những ví dụ về các cáp truyền thông với tốc độ cao. Mạng LAN thường xuyên được sử dụng trong nội bộ công ty hoặc cơ quan. Tỷ lệ lỗi khi truyền thấp. Sử dụng kỹ thuật Ethernet hoặc Token Ring. Và các thiết bị thường dùng trong mạng là Repeater, Brigde, Hub, Switch, Router.
* Mạng WAN (Wide Area Network) là mạng diện rộng kết nối các máy tính trong một quốc gia hoặc xuyên lục địa, không giới hạn địa lý. Mạng WAN được hình thành bằng cách kết nối các mạng LAN. Tuy nhiên, tốc độ truyền dữ liệu thấp, do nhiều tổ chức quản lý. Với sử dụng các kỹ thuật Modem, ISDN, DSL, Frame Relay, ATM.

## Mô hình mạng ba lớp

Với định hướng thiết kế theo mô hình 3 lớp, kiến trúc mạng được phân tách thành các khối, các module với các chức năng riêng biệt nhưng trước đó ta cần được minh họa qua sơ đồ mô hình mạng sau.

Sơ đồ kết nối hệ thống mạng truyền thống đề xuất thể hiện trong hình sau:



Hình . Mô hình phân cấp mạng 3 lớp (3-layer hierarchical topology)

Nguồn: ([Thiết kế an toàn bảo mật cho hệ thống mạng, trang 7](https://users.soict.hust.edu.vn/tungbt/it4830/lec07.pdf))

Lớp lõi (Core Layer): Để đáp ứng nhu cầu chuyển mạch của toàn hệ thống sử dụng các bộ chuyển mạch lõi với hiệu suất cao, lớn. Tất cả lưu lượng mạng trong hệ thống đều di chuyển qua module này, do đó nó phải có khả năng xử lý ở tốc độ nhanh, có sẵn kết nối và có thể thực thi các quy định phân phối lưu lượng lớn. Lớp lõi này sẽ được sử dụng để kết nối bảo mật giữa các module. Lưu ý phải hạn chế thực hiện các cấu hình làm chậm tốc độ xử lý như: định tuyến VLAN, ACL, lọc gói tin... Không kết nối trực tiếp máy trạm. Nếu dùng Switch layer 2 thì nhanh, dễ mở rộng, rẻ. Còn dùng Switch layer 3, router thì cân bằng tải, giám sát dữ liệu quảng bá.

Lớp phân phối (Distribution Layer): Module Distribution phân phối lưu lượng và định tuyến nó qua các vị trí địa lý riêng biệt trong mạng nội bộ của tòa nhà, chẳng hạn như các tòa nhà hoặc VLAN. Các thiết bị chuyển mạch có liên kết quang tốc độ cao, thường là kết nối 10 Gigabit trở lên, sẽ được sử dụng để kết nối các tòa nhà với switch trung tâm ở Core Layer. Đa số có tính sẵn sàng, tốc độ cao và tính năng quản lý traffic tốt. Dùng để triển khai các chính sách của mạng trong ACL, lọc gói, QoS, Firewall, cân bằng tải, VLAN routing hay cung cấp các kết nối dự phòng cho lớp truy cập.

Lớp truy cập (Access Layer): Phần này sẽ chứa các switch truy cập liên kết trực tiếp đến các máy trạm của người dùng cuối cũng như các switch phân phối. Các thiết bị chuyển mạch trong trường hợp này chỉ là các thiết bị chuyển mạch cấp thấp phải xử lý nhiều loại kết nối phía máy khách như Ethernet LAN, Wireless, Wimax, hoặc GPRS…. Lưu ý rằng trong lớp này thì không sử dụng thiết bị router.

## Bảo mật mạng máy tính là gì?

Các hình thức, kỹ thuật và qui định được sử dụng để ngăn chặn, phát hiện và giám sát truy cập trái phép, lạm dụng, sửa đổi hoặc từ chối mạng máy tính và các tài nguyên có thể truy cập mạng được gọi là an ninh mạng. Việc cấp phép truy cập vào dữ liệu trong mạng, được gọi là bảo mật mạng. Người dùng chọn hoặc được cấp ID, mật khẩu hoặc loại xác thực khác cho phép họ truy cập vào thông tin và ứng dụng dưới sự kiểm soát của họ. Bảo mật mạng đề cập đến một loạt các mạng máy tính công cộng và riêng tư được sử dụng trong các công việc hàng ngày như hoàn thành các giao dịch và liên lạc giữa các tổ chức, và cá nhân… Gán tên và mật khẩu duy nhất cho tài nguyên mạng là phương pháp phổ biến và đơn giản nhất để bảo vệ tài nguyên đó.



Hình . Mức độ bảo mật

Nguồn: ([Bảo mật mạng máy tính và Firewall](https://123docz.net/document/5296369-bao-mat-mang-may-tinh-va-firewall-co-code.htm))

Xác thực tên người dùng và mật khẩu, là bước đầu tiên trong bảo mật mạng. Thứ mà người dùng được sử dụng với xác thực như mã thông báo bảo mật, thẻ ATM hay điện thoại di động; và thứ mà người dùng cũng được sử dụng với xác thực ba yếu tố mã thông báo bảo mật, thẻ ATM hay mật khẩu điện thoại thông minh bằng quét vân tay, võng mạc hay mật khẩu các ký tự.

## Firewall

### Giới thiệu về Firewall

Tường lửa (Firewall) là một thiết bị bảo mật dưới dạng phần cứng lẫn phần mềm trong máy tính, an ninh mạng giám sát và điều chỉnh lưu lượng mạng đến và đi dựa trên các quy tắc bảo mật được xác định trước. Tường lửa thường được sử dụng để tạo rào cản giữa mạng đáng tin cậy và mạng không đáng tin cậy, như Internet. Tường lửa có thể được cấu hình để hoạt động như một bộ lọc gói hoặc hoạt động ở lớp giao thức cao hơn.

### Phân loại Firewall

Bộ lọc gói (Packet filter): Một lượng nhỏ dữ liệu được phân tích và phân phối theo tiêu chuẩn của bộ lọc. Tường lửa giữ một danh sách kiểm soát truy cập chỉ định gói nào sẽ được kiểm tra và thực thi yêu cầu nào, nếu có thực thi mặc định là “loại bỏ im lặng” - loại bỏ với giao thức thông báo điều khiển Internet hoặc phản hồi đặt lại TCP cho người gửi và chuyển tiếp bước tiếp theo là ba hành động cơ bản đối với gói tin. Địa chỉ IP nguồn và đích, giao thức cũng như các cổng nguồn và đích đều có thể được sử dụng để lọc các gói. Phần lớn giao tiếp Internet sử dụng TCP hoặc UDP kết hợp với các cổng, cho phép tường lửa thời đó phân biệt giữa các loại lưu lượng khác nhau như trang web, truyền email và truyền tệp.

Dịch vụ Proxy và tầng ứng dụng (Proxy service and Application layer): Hệ thống bảo mật mạng bảo vệ trong khi lọc tin nhắn ở lớp ứng dụng. Ở cấp độ ứng dụng, lưu lượng mạng được lọc. Không như tường lửa truyền thống, proxy đóng vai trò là người trung gian giữa hai hệ thống đầu cuối. Máy khách phải gửi yêu cầu tới tường lửa, yêu cầu này phải được xem xét dựa trên một bộ quy tắc bảo mật trước khi được phép hoặc bị từ chối. Đặc biệt, tường lửa proxy theo dõi lưu lượng truy cập cho các giao thức lớp 7 như HTTP và FTP, đồng thời xác định lưu lượng độc hại bằng cách sử dụng cả kiểm tra gói sâu và trạng thái.

Kiểm tra trạng thái (Stateful inspection): Lọc gói tin động để theo dõi các kết nối hoạt động để xác định các gói mạng nào cho phép thông qua tường lửa. Theo dõi tất cả các kết nối hoạt động bằng bảng. Khi các gói mới đến, so sánh thông tin trong tiêu đề gói với bảng trạng thái - danh sách các kết nối hợp pháp - để xem gói có phải là một phần của kết nối hiện có hay không. Nếu đúng như vậy, gói tin được phép vượt qua mà không cần kiểm tra thêm. Nếu gói không khớp với một kết nối hiện có, sẽ được phân tích bằng cách sử dụng quy tắc kết nối mới được xác định. Phần kiểm tra trạng thái có thể dễ bị tấn công DoS, bất chấp tính hiệu quả của chúng. Các cuộc tấn công DoS hoạt động bằng cách khai thác các kết nối hiện có được cho là an toàn theo hình thức tấn công này.

Tường lửa thế hệ tiếp theo (Next Gereration Firewall - NGFW): Tường lửa kiểm tra sâu gói tin với kiểm tra tầng ứng dụng để tránh phần mền độc hại. Chúng bao gồm các tính năng của tường lửa truyền thống, ngoài ra còn có tính năng lọc URL, lọc ứng dụng, … NGFWS hỗ trợ mạng dựa trên ý định bằng cách bao gồm kiểm tra SSL và SSH và phát hiện phần mềm độc hại. Vì tường lửa cơ bản chỉ xem xét các tiêu đề gói, kiểm tra gói sâu sẽ kiểm tra dữ liệu bên trong chính gói đó, cho phép người dùng xác định, phân loại hoặc ngăn chặn các gói có dữ liệu độc hại một cách hiệu quả hơn.

## Network Address Translation (NAT)

### NAT là gì?

NAT có nhiều công dụng, nhưng công dụng chính của nó là bảo tồn các địa chỉ IPv4 công cộng. Nó thực hiện điều này bằng cách cho phép các mạng sử dụng địa chỉ IPv4 riêng trong nội bộ và chỉ cung cấp bản dịch sang địa chỉ công cộng khi cần thiết. NAT có một lợi ích được nhận thấy là tăng thêm mức độ riêng tư và bảo mật cho mạng, bởi vì nó ẩn địa chỉ IPv4 nội bộ khỏi các mạng bên ngoài.

Tóm lại NAT là một kỹ thuật cho phép chuyển đổi từ một địa chỉ IP này thành một địa chỉ IP khác. Thông thường, NAT được dùng phổ biến trong mạng sử dụng địa chỉ cục bộ, cần truy cập đến mạng công cộng (Internet). Vị trí thực hiện NAT là router biên kết nối giữa hai mạng.

### Một số thuật ngữ về NAT

* Địa chỉ inside local: là địa chỉ IP gán cho một thiết bị ở mạng bên trong. Địa chỉ này hầu như không phải địa chỉ được cung cấp bởi NIC (Network Information Center) hay nhà cung cấp dịch vụ.
* Địa chỉ inside global: là địa chỉ đã được đăng ký với NIC, dùng để thay thế một hay nhiều địa chỉ IP inside local.
* Địa chỉ outside local: là địa chỉ IP của một thiết bị bên ngoài khi nó xuất hiện bên trong mạng. Địa chỉ này không nhất thiết là địa chỉ được đăng ký, nó được lấy từ không gian địa chỉ bên trong.
* Địa chỉ outside global: là địa chỉ IP gán cho một thiết bị ở mạng bên ngoài. Địa chỉ này được lấy từ địa chỉ có thể dùng để định tuyến toàn cầu từ không gian địa chỉ mạng.

### Các loại NAT

#### Static NAT

Static NAT được dùng để chuyển đổi một [địa chỉ IP](https://www.totolink.vn/article/74-ip-la-gi-cach-xac-dinh-dia-chi-ip-tren-may-tinh.html) này sang một địa chỉ khác một cách cố định, thông thường là từ một địa chỉ cục bộ sang một địa chỉ công cộng và quá trình này được cài đặt thủ công, nghĩa là địa chỉ ánh xạ và địa chỉ ánh xạ chỉ định rõ ràng tương ứng duy nhất.

Static NAT rất hữu ích trong trường hợp những thiết bị cần phải có địa chỉ cố định để có thể truy cập từ bên ngoài Internet. Những thiết bị này phổ biến là những Server như Web, Mail, ...

**Cấu hình Static NAT:**

* Thiết lập mối quan hệ chuyển đổi giữa địa chỉ nội bộ bên trong và địa chỉ đại điện bên ngoài:

***Router(config)# ip nat inside source static [local ip] [global ip]***

* Xác định các cổng kết nối vào mạng bên trong và thực hiện lệnh:

***Router(config-if)# ip nat inside***

* Xác định các cổng kết nối ra mạng công cộng bên ngoài thực hiện lệnh:

***Router(config-if)# ip nat outside***

Diagram

Description automatically generated

Hình . Mô hình ví dụ về static NAT

(Nguồn: [CCNA 3 v7.0 Curriculum: Module 6 – NAT for IPv4](https://itexamanswers.net/ccna-3-v7-0-curriculum-module-6-nat-for-ipv4.html))

Trong hình, R2 được cấu hình với ánh xạ static cho các địa chỉ inside local của Svr1, PC2 và PC3. Khi các thiết bị này gửi lưu lượng truy cập đến internet, địa chỉ inside local của chúng sẽ được dịch sang địa chỉ inside global để được định cấu hình. Đối với các mạng bên ngoài, các thiết bị này dường như có địa chỉ IPv4 công khai.

#### Dynamic NAT

Dynamic NAT được dùng để ánh xạ một địa chỉ IP này sang một địa chỉ khác một cách tự động, thông thường là ánh xạ từ một địa chỉ cục bộ sang một địa chỉ được đăng ký. Bất kỳ một địa chỉ IP nào nằm trong dải địa chỉ IP công cộng đã được định trước đều có thể được gán một thiết bị bên trong mạng.

**Cấu hình Dynamic NAT:**

* Xác định dải địa chỉ đại diện bên ngoài (public): các địa chỉ NAT

***Router(config)# ip nat pool [name start ip] [name end ip] netmask [netmask]/prefix-lenght [prefix-lenght]***

* Thiết lập ACL cho phép những địa chỉ nội bộ bên trong nào được chuyển đổi: các địa chỉ được NAT

***Router(config)# access-list [access-list-number-permit] source [source-wildcard]***

* Thiết lập mối quan hệ giữa địa chỉ nguồn đã được xác định trong ACL với dải địa chỉ đại diện ra bên ngoài:

***Router(config)# ip nat inside source list <acl-number> pool <name>***

* Xác định các cổng kết nối vào mạng nội bộ:

***Router (config-if) # ip nat inside***

* Xác định các cổng kết nối ra bên ngoài:

***Router (config-if) # ip nat outside***

Diagram

Description automatically generated

Hình . Mô hình minh họa cho dynamic NAT

(Nguồn: [CCNA 3 v7.0 Curriculum: Module 6 – NAT for IPv4](https://itexamanswers.net/ccna-3-v7-0-curriculum-module-6-nat-for-ipv4.html))

Trong hình, PC3 đã truy cập internet bằng địa chỉ có sẵn đầu tiên trong pool NAT động. Các địa chỉ khác vẫn có sẵn để sử dụng. Tương tự như NAT tĩnh, NAT động yêu cầu có đủ địa chỉ chung để đáp ứng tổng số phiên người dùng đồng thời.

#### Port Address Translation (PAT)

PAT là một dạng của Dynamic NAT, nó thực hiện ánh xạ nhiều địa chỉ IP thành một địa chỉ (many - to - one) và sử dụng các địa chỉ số cổng khác nhau để phân biệt cho từng chuyển đổi. PAT còn có tên gọi là NAT Overload.

**Cấu hình PAT:**

* Xác định dãy địa chỉ bên trong cần chuyển dịch ra ngoài (private ip addresses range):

***Router(config)# access-list <ACL-number> permit <source> <wildcard>***

* Cấu hình chuyển đổi địa chỉ IP sang cổng nối ra ngoài:

***Router (config) # ip nat inside source list <ACL-number> interface <interface> overload***

* Xác định các cổng nối vào mạng bên trong:

***Router (config-if) # ip nat inside***

* Xác định cổng kết nối ra mạng bên ngoài:

***Router (config-if) # ip nat outside***

## Access Control List (ACL)

### ACL là gì?

ACL là một loạt các lệnh IOS được sử dụng để lọc các gói tin dựa trên thông tin được tìm thấy trong tiêu đề gói. Theo mặc định, một bộ định tuyến không có bất kỳ ACL nào được định cấu hình. Tuy nhiên, khi một ACL được áp dụng cho một interface, bộ định tuyến sẽ thực hiện nhiệm vụ bổ sung là đánh giá tất cả các gói mạng khi chúng đi qua interface để xác định xem gói đó có thể được chuyển tiếp hay không. ACL sử dụng một danh sách tuần tự các câu lệnh cho phép (permit) hoặc từ chối (deny), được gọi là các mục nhập kiểm soát truy cập - access control entries (ACEs).

### Hoạt động ACL

Khi áp dụng ACL trên một interface của router ta phải chỉ rõ chiều của luồng dữ liệu. Inbound là chiều của luồng dữ liệu đi vào cổng đó và Outbound là chiều của luồng dữ liệu đi ra khỏi cổng đó.

Icon

Description automatically generated with medium confidence

Hình . Hình minh họa áp dụng ACL cho lưu lượng đi vào và đi ra

(Nguồn: [CCNA 3 v7.0 Curriculum: Module 4 – ACL Concepts](https://itexamanswers.net/ccna-3-v7-0-curriculum-module-4-acl-concepts.html))

Một ACL inbound lọc các gói tin trước khi chúng được chuyển đến interface outbound. ACL inbound hiệu quả vì nó tiết kiệm chi phí tra cứu định tuyến nếu gói tin bị loại bỏ. Nếu gói tin được ACL cho phép, gói đó sẽ được xử lý để định tuyến.

ACL outbound lọc các gói tin sau khi được định tuyến, bất kể interface inbound. Các gói đến được chuyển đến interface outbound và sau đó chúng được xử lý thông qua ACL outbound.

### Wildcard mask

Wildcard Mask là một chuỗi nhị phân 32 bit được chia làm 4 octet. Mỗi một wildcard mask đi kèm với một địa chỉ IP. Các bit 0 và 1 được định nghĩa để xác định cách xử lý các bit tương ứng trong đia chỉ IP theo quy tắc: 0 kiểm tra – 1 bỏ qua. Nghĩa là bit tương ứng với bit 0 trong wildcard mask sẽ được kiểm tra, còn tương ứng với bit 1 sẽ được bỏ qua không cần kiểm tra. Wildcard mask cần phải đi cùng một địa chỉ ip. Nếu đứng một mình nó sẽ không có ý nghĩa gì cả.

### Phân loại ACL

* Standard Access List: Đây là loại ACL mà khi làm việc router chỉ kiểm tra một yếu tố duy nhất là địa chỉ IP nguồn. Standard ACL được đánh số từ 1 đến 999 hoặc dùng tên (việc đánh số tùy theo vendor quyết định).
* Extended Access List: Đây là loại ACL mở rộng hơn so với loại Standard Access List. Khi làm việc router sẽ kiểm tra một số yếu tố bao gồm: địa chỉ IP nguồn, địa chỉ IP đích, port nguồn, port đích, giao thức… Extended ACL được đánh số từ 1000 đến 1999 hoặc dùng tên (việc đánh số tùy theo vendor quyết định).

## Tổng quan AAA

AAA là viết tắt của Authentication, Authorization và Accounting được định nghĩa bởi Internet Engineering Task Force trong RFC 6733 nhằm cung cấp AAA cho các ứng dụng như truy cập hay bảo mật mạng. Ta có thể xác thực (authentication) người dùng, cấp quyền (authorization) cho người dùng, cũng như tập hợp được thông tin như thời gian bắt đầu hay kết thúc của người dùng (accounting).

AAA cho phép nhà quản trị mạng biết được các thông tin quan trọng về tình hình cũng như mức độ an toàn trong mạng. Nó cung cấp việc xác thực (authentication) người dùng nhằm bảo đảm có thể nhận dạng đúng người dùng. Một khi đã nhận dạng người dùng, ta có thể giới hạn thẩm quyền (authorization) mà người dùng có thể làm. Khi người dùng sử dụng mạng, ta cũng có thể giám sát tất cả những gì mà họ làm. AAA với ba phần xác thực (authentication), ủy quyền (authorization), tính cước (accounting) là các phần riêng biệt mà ta có thể sử dụng trong dịch vụ mạng, cần thiết để mở rộng và bảo mật mạng. AAA có thể dùng để tập hợp thông tin từ nhiều thiết bị trên mạng. Ta có thể bật các dịch vụ AAA trên router, switch, firewall, các thiết bị VPN, server, …

* **Authentication**: Xác thực là quá trình xác định một cá nhân, thường dựa trên tên người dùng và mật khẩu. Xác thực dựa trên ý tưởng rằng mỗi người dùng cá nhân sẽ có thông tin duy nhất giúp họ khác biệt với những người dùng khác.
* **Authorization**: Ủy quyền là quá trình cấp hoặc từ chối người dùng truy cập vào tài nguyên mạng khi người dùng đã được xác thực thông qua tên người dùng và mật khẩu. Số lượng thông tin và số lượng dịch vụ mà người dùng có quyền truy cập phụ thuộc vào cấp độ ủy quyền của người dùng.
* **Accounting**: Tính cước là quá trình theo dõi hoạt động của người dùng khi truy cập tài nguyên mạng, bao gồm lượng thời gian sử dụng mạng, các dịch vụ được truy cập khi ở đó và lượng dữ liệu được truyền trong phiên. Dữ liệu được tính toán được sử dụng để phân tích xu hướng, lập kế hoạch năng lực, lập hóa đơn, kiểm toán và phân bổ chi phí.

## Công nghệ VPN

Để đảm bảo lưu lượng mạng giữa các trang web và người dùng, các tổ chức sử dụng mạng riêng ảo - Virtual Private Network (VPN) để tạo các kết nối mạng riêng tư đầu cuối (end-to-end). VPN mang thông tin trong một mạng riêng tư, nhưng thông tin đó thực sự được truyền qua một mạng công cộng. VPN riêng tư ở chỗ lưu lượng được mã hóa để giữ bí mật cho dữ liệu trong khi nó được truyền qua mạng công cộng. Công nghệ VPN có thể được chia thành hai loại cơ bản là site-to-site VPN và remote access VPN.

### Site-to-site VPN

Site-to-site VPN là mô hình dùng để kết nối các hệ thống mạng ở các nơi khác nhau tạo thành một hệ thống mạng thống nhất. Ở loại kết nối này thì việc chứng thực ban đầu phụ thuộc vào thiết bị đầu cuối ở các Site, các thiết bị này hoạt động như Gateway và đây là nơi đặt nhiều chính sách bảo mật nhằm truyền dữ liệu một cách an toàn giữa các Site.

### Remote Access VPN

Remote Access VPN cho phép người dùng từ xa và di động kết nối an toàn với doanh nghiệp bằng cách tạo một đường hầm (tunnel) được mã hóa. Người dùng từ xa có thể sao chép một cách an toàn quyền truy cập bảo mật doanh nghiệp của họ bao gồm email và các ứng dụng mạng. Người dùng khởi động VPN client trên máy tính cá nhân, sử dụng username/password để xác thực với VPN server, và sau đó sẽ khởi tạo 1 đường truyền VPN được mã hóa từ máy tính cá nhân của người dùng đến mạng riêng ở xa. Sau đó dữ liệu từ máy tính của người dùng đến mạng ở xa sẽ được truyền trên đường truyền riêng an toàn và bảo mật. VPN truy cập từ xa thường được người dùng kích hoạt động khi được yêu cầu. VPN truy cập từ xa có thể được tạo bằng IPsec hoặc SSL.

# THIẾT KẾ HỆ THỐNG MẠNG DOANH NGHIỆP

## Mô tả hệ thống

Doanh nghiệp HK’sslay BEAUTY có trụ sở chính tại 556, đường Ba Tháng Hai, phường 6, quận 5, TPHCM. Là một doanh nghiệp sản xuất và kinh doanh mỹ phẩm làm đẹp với số nhân sự lên đến gần 200 người. Tòa nhà gồm 7 phòng ban với gần 180 máy tính. Với:

* Tầng 1 gồm các phòng ban: phòng CNTT, phòng Sale, phòng Điện máy.
* Tầng 2: phòng Kế toán và Tài chính.
* Tầng 3: phòng Marketing và phòng Hội đồng
* Có khu vực dành cho các server.

Bên cạnh đó còn có hai chi nhánh ở Đà Nẵng và Hải Phòng với quy mô nhỏ hơn:

* Ở Đà Nẵng có 85 máy tính có 3 tầng với 3 phòng ban: phòng Nhân viên, phòng CNTT, phòng Hội đồng.
* Ở Hải Phòng có 125 máy tính có 3 tầng với 3 phòng ban: phòng Nhân viên, phòng CNTT, phòng Hội đồng.

## Phân tích hệ thống

### Yêu cầu khách hàng

Hệ thống doanh nghiệp gồm ba cơ sở, có trụ sở chính ở thành phố Hồ Chí Minh gồm 7 phòng ban khác nhau yêu cầu các máy tính ở phòng ban ấy có thể liên lạc nội bộ với nhau, các chi nhánh ở Đà Nẵng và Hải Phòng có 3 phòng ban khác nhau cũng phải đảm bảo các máy tính nội bộ kết nối và giao tiếp với nhau. Và giữa các chi nhánh như vậy vẫn có thể truy xuất trao đổi liên lạc nhưng chỉ trong nội bộ. Triển khai một hệ thống mạng kết nối các máy tính làm việc chia sẻ dữ liệu đảm bảo an toàn bảo mật trong hệ thống mạng. Hệ thống mạng phải có tính linh hoạt cũng như dự phòng không mất nhiều thời gian và chi phí.

### Đề xuất hướng giải quyết

Xây dựng mạng LAN phân quyền cho từng phòng ban nhằm để phục vụ cho việc quản lý dữ liệu nội bộ được thuận lợi, dễ dàng, đảm bảo tính an toàn dữ liệu cũng như tính bảo mật, kết nối tới các thiết bị có dây. Ở trụ sở chính, sử dụng hai router và hai switch tổng hoạt động song song với nhau nhằm đảm bảo tính dự phòng cũng như tính sẵn sàng với 2 đường đi: router thứ nhất kết nối với switch tổng thứ nhất và router thứ 2 kết nối với switch tổng thứ 2, phân chia mỗi switch là một phòng ban riêng tách biệt nhau đảm bảo đủ số lượng cổng cho các host. Các chi nhánh còn lại phân mỗi tầng là một switch kết nối tới các phòng ban khác nhau. Để tăng tính bảo mật cao về thông tin được chia sẻ qua lại giữa các phòng ban và chi nhánh công ty với nhau, cần lắp đặt thiết kế dịch vụ thư điện tử (mail server). Và cần phát triển một nguồn trang web riêng thiết kế sáng tạo thì thiết kế thêm dịch web server, hiển nhiên qua đó tạo ra các tên miền riêng của công ty để truy cập vào internet lên trang của công ty. Vì là một công ty với quy mô vừa nên kinh phí dành cho các thiết bị để xây dưng một hệ thống mạng bảo mật có tính dự phòng và tính sẵn sàng nhanh với thiết bị phổ biến thường dùng là router 1941, switch tổng là 3560-24PS và các switch nhỏ 2960 IOS15. Sau cùng giải quyết những vấn đề chung cho mô hình mạng đó là định vị các thành phần nhận dạng mạng, bao gồm việc đặt tên, định địa chỉ IP cho các máy tính, phân cổng cho từng dịch vụ, phân chia mạng con sao cho hợp lý, thực hiện vạch đường đi, các máy tính của người dùng nội bộ truy xuất được lẫn nhau, thực hiện chức năng bảo mật như NAT và ACL cho thông tin trên hệ thống mạng công ty.

## Thiết kế hệ thống

### Mô hình demo

Chart

Description automatically generated

Hình . Mô hình mạng doanh nghiệp với ba cơ sở

Bên cơ sở chính chia các vlan cho các phòng ban và có khu vực riêng dành cho server, gồm các thiết bị chính như:

* Hai router là HoChiMinh\_1, HoChiMinh\_2 và 2 switch tổng SW1\_Quanly, SW2\_Quanly chia ra hai đường đi đảm bảo tính dự phòng cho hệ thống.
* Các switch tương ứng cho từng phòng ban đáp ứng cho 3 tầng.
* Tầng 1: phòng CNTT, phòng Bán hàng, phòng Điện máy.
* Tầng 2: phòng Tài chính, phòng Kế toán.
* Tầng 3: phòng Marketing, phòng Hội đồng.

Chi nhánh Đà Nẵng cũng gồm 1 số thiết bị chính như 1 router DaNang, 1 switch tổng S1 và các switch ở 3 tầng. Với:

* Tầng 1: phòng Nhân viên và phòng CNTT.
* Tầng 2: phòng Nhân viên và phòng CNTT.
* Tầng 3: phòng Nhân viên và phòng Hội đồng.

Tương tự cho chi nhánh Hải Phòng gồm 1 số thiết bị chính như 1 router HaiPhong, 1 switch tổng S2 và các switch ở 3 tầng giống với Đà Nẵng.

### Dùng kỹ thuật Variable Length Subnet Masking (VLSM) chia mạng con cho các phòng ban trong doanh nghiệp

Công ty với trụ sở chính có 7 phòng ban tương ứng với số host:

* Phòng CNTT: 25
* Phòng Sale: 58
* Phòng Điện máy: 20
* Phòng Kế toán: 18
* Phòng Tài chính: 15
* Phòng Hội đồng: 10
* Phòng Marketing: 26

**Dùng địa chỉ mạng 192.168.0.0/24 tiến hành chia subnet với VLSM:**

* Phòng Sale: 58 host, lấy 6 bit làm host, mượn 2 bit, 26-2 = 62 host/subnet.
* Sn1: 192.168.0.0/26 🡪 sale
* Sn2: 192.168.0.64/26
* Sn3: 192.168.0.128/26
* Sn4: 192.168.0.192/26
* Phòng Marketing: 26 host, 25-2 = 30 host/subnet.
* Sn2: 192.168.0.64/26
* Sn2.1: 192.168.0.64/27🡪 Marketing
* Sn2.2: 192.168.0.96/27
* Phòng CNTT: 25 host, 25-2 = 30 host/subnet
* Sn2.2: 192.168.0.96/27 🡪 CNTT
* Phòng Điện máy: 20 host, 25-2 = 30 host/subnet
* Sn3: 192.168.0.128/26
* Sn3.1:192.168.0.128/27 🡪 điện máy
* Sn3.2: 192.168.0.160/27
* Phòng kế toán: 18 host, 25-2 = 30 host/subnet
* Sn3.2: 192.168.0.160/27 🡪 kế toán
* Phòng Tài chính: 15 host, 25-2 = 30 host/subnet
* Sn4: 192.168.0.192/26
* Sn4.1: 192.168.0.192/27🡪 Tài chính
* Sn4.2: 192.168.0.224/27
* Phòng Hội đồng: 10 host, 24-2 = 14 host/subnet
* Sn4.2: 192.168.0.224/27
* Sn4.2.1: 192.168.0.224/28 🡪 Hội đồng
* Sn4.2.2: 192.168.0.240/28

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Subnet** | **Address** | **Mask** | **Subnet Mask** | **Địa chỉ đầu** | **Địa chỉ cuối** | **Địa chỉ broadcast** |
| **Phòng Sale** | 192.168.0.0 | /26 | 255.255.255.192 | 192.168.0.1 | 192.168.0.62 | 192.168.0.63 |
| **Phòng Marketing** | 192.168.0.64 | /27 | 255.255.255.224 | 192.168.0.65 | 192.168.0.94 | 192.168.0.95 |
| **Phòng CNTT** | 192.168.0.96 | /27 | 255.255.255.224 | 192.168.0.97 | 192.168.0.126 | 192.168.0.127 |
| **Phòng Điện máy** | 192.168.0.128 | /27 | 255.255.255.224 | 192.168.0.129 | 192.168.0.158 | 192.168.0.159 |
| **Phòng Kế toán** | 192.168.0.160 | /27 | 255.255.255.224 | 192.168.0.161 | 192.168.0.190 | 192.168.0.191 |
| **Phòng Tài chính** | 192.168.0.192 | /27 | 255.255.255.224 | 192.168.0.193 | 192.168.0.222 | 192.168.0.223 |
| **Phòng Hội đồng** | 192.168.0.224 | /28 | 255.255.255.240 | 192.168.0.225 | 192.168.0.238 | 192.168.0.239 |

Bảng . Bảng thông tin địa chỉ dùng VLSM chia mạng con cho trụ sở chính

Chi nhánh thứ nhất có 3 tầng tương ứng với 3 phòng ban khác nhau:

* Phòng Nhân viên: 45 host
* Phòng CNTT: 25 host
* Phòng Hội đồng: 15 host

**Dùng địa chỉ mạng: 192.168.10.0/24 chia subnet:**

* Phòng Nhân viên: lấy 6 bit làm host, mượn2 bit, 26-2 = 62 host/subnet
* Sn1: 192.168.10.0/26 🡪 nhân viên
* Sn2: 192.168.10.64/26
* Sn3: 192.168.10.128/26
* Sn4: 192.168.10.192/26
* Phòng CNTT: 25 host, 25-2 = 30 host/subnet
* Sn2: 192.168.10.64/26
* Sn2.1: 192.168.10.64/27🡪 cntt
* Sn2.2: 192.168.10.96/27
* Phòng Hội đồng: 15 host, 25-2 = 30 host/subnet
* Sn2.2: 192.168.10.96/27🡪 hội đồng

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Subnet** | **Address** | **Mask** | **Subnet Mask** | **Địa chỉ đầu** | **Địa chỉ cuối** | **Địa chỉ broadcast** |
| **Phòng Nhân viên** | 192.168.10.0 | /26 | 255.255.255.192 | 192.168.10.1 | 192.168.10.62 | 192.168.10.63 |
| **Phòng CNTT** | 192.168.10.64 | /27 | 255.255.255.224 | 192.168.10.65 | 192.168.10.94 | 192.168.10.95 |
| **Phòng Hội đồng** | 192.168.10.96 | /27 | 255.255.255.224 | 192.168.10.97 | 192.168.10.126 | 192.168.10.127 |

Bảng . Bảng thông tin địa chỉ dùng VLSM chia mạng con cho chi nhánh thứ nhất

Chi nhánh thứ hai có 3 tầng tương ứng với 3 phòng ban khác nhau:

* Phòng Nhân viên: 60 host
* Phòng CNTT: 40 host
* Phòng Hội đồng: 25 host

**Dùng địa chỉ mạng: 192.168.20.0/24 chia subnet:**

* Phòng Nhân viên: lấy 6 bit làm host, mượn2 bit, 26-2 = 62 host/subnet
* Sn1: 192.168.20.0/26 🡪 nhân viên
* Sn2: 192.168.20.64/26
* Sn3: 192.168.20.128/26
* Sn4: 192.168.20.192/26
* Phòng CNTT: 40 host, 26-2 = 62 host/subnet
* Sn2: 192.168.20.64/26🡪 cntt
* Phòng Hội đồng: 25 host, 25-2 = 30 host/subnet
* Sn3: 192.168.20.128/26
* Sn3.1: 192.168.20.128/27🡪 hội đồng
* Sn3.2: 192.168.20.160/27

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Subnet** | **Address** | **Mask** | **Subnet Mask** | **Địa chỉ đầu** | **Địa chỉ cuối** | **Địa chỉ broadcast** |
| **Phòng Nhân viên** | 192.168.20.0 | /26 | 255.255.255.192 | 192.168.20.1 | 192.168.20.62 | 192.168.20.63 |
| **Phòng CNTT** | 192.168.20.64 | /26 | 255.255.255.192 | 192.168.20.65 | 192.168.20.126 | 192.168.20.127 |
| **Phòng Hội đồng** | 192.168.20.128 | /27 | 255.255.255.224 | 192.168.20.129 | 192.168.20.158 | 192.168.20.159 |

Bảng . Bảng thông tin địa chỉ dùng VLSM chia mạng con cho chi nhánh thứ hai

### Thông tin địa chỉ trong hệ thống

|  |  |  |
| --- | --- | --- |
| **Thiết bị** | **Interface** | **Địa chỉ** |
| **ISP** | S0/0/0 | 10.0.0.1/24 |
| S0/0/1 | 10.0.1.1/24 |
| S0/1/0 | 200.100.10.1/25 |
| S0/1/1 | 200.100.10.129/25 |
| **HoChiMinh\_1** | S0/0/0 | 10.0.0.2/24 |
| G0/0 | 192.168.0.241/30 |
| **HoChiMinh\_2** | S0/0/0 | 10.0.1.2/24 |
| G0/0 | 192.168.0.245/30 |
| **DaNang** | S0/0/0 | 200.100.10.2/25 |
| G0/0 | 192.168.10.129/30 |
| **HaiPhong** | S0/0/0 | 200.100.10.130/25 |
| G0/0 | 192.168.20.161/30 |
| **SW1\_Quanly** | G0/1 | 192.168.0.242/30 |
| VLAN 2 | 192.168.0.61/26 |
| VLAN 3 | 192.168.0.93/27 |
| VLAN 4 | 192.168.0.125/27 |
| VLAN 5 | 192.168.0.157/27 |
| VLAN 6 | 192.168.0.189/27 |
| VLAN 7 | 192.168.0.221/27 |
| VLAN 8 | 192.168.0.237/28 |
| VLAN 50 | 192.168.50.253/24 |
| Port-channel 1 | 192.168.0.249/30 |
| **SW2\_Quanly** | G0/1 | 192.168.0.246/30 |
| VLAN 2 | 192.168.0.62/26 |
| VLAN 3 | 192.168.0.94/27 |
| VLAN 4 | 192.168.0.126/27 |
| VLAN 5 | 192.168.0.158/27 |
| VLAN 6 | 192.168.0.190/27 |
| VLAN 7 | 192.168.0.222/27 |
| VLAN 8 | 192.168.0.238/28 |
| VLAN 50 | 192.168.50.254/24 |
| Port-channel 1 | 192.168.0.250/30 |
| **S1** | G0/1 | 192.168.10.130/30 |
| VLAN 10 | 192.168.10.62/26 |
| VLAN 11 | 192.168.10.94/27 |
| VLAN 12 | 192.168.10.126/27 |
| **S2** | G0/1 | 192.168.20.162/30 |
| VLAN 20 | 192.168.20.62/26 |
| VLAN 21 | 192.168.20.126/26 |
| VLAN 22 | 192.168.20.158/27 |
| **DNS Server** | NIC | 192.168.50.250/24 |
| **TACACS Server** | NIC | 192.168.50.251/24 |
| **FTP Server** | NIC | 192.168.50.248/24 |
| **Mail Server** | NIC | 192.168.50.247/24 |
| **Web Server** | NIC | 192.168.50.249/24 |
| **Host\_CNTT** | NIC | DHCP |
| **Host\_Banhang** | NIC | DHCP |
| **Host\_Dienmay** | NIC | DHCP |
| **Host\_Taichinh** | NIC | DHCP |
| **Host\_Ketoan** | NIC | DHCP |
| **Host\_Marketing** | NIC | DHCP |
| **Host\_Hoidong** | NIC | DHCP |
| **Sale\_1** | NIC | DHCP |
| **Sale\_2** | NIC | DHCP |
| **Sale\_3** | NIC | DHCP |
| **Sale\_4** | NIC | DHCP |
| **IT\_1** | NIC | DHCP |
| **IT\_2** | NIC | DHCP |
| **IT\_3** | NIC | DHCP |
| **IT\_4** | NIC | DHCP |
| **Thuky\_1** | NIC | DHCP |
| **Thuky\_2** | NIC | DHCP |
| **Giamdoc\_1** | NIC | DHCP |
| **Giamdoc\_2** | NIC | DHCP |

Bảng . Bảng địa chỉ trong hệ thống

### Thông tin vlan, interface vlan trong hệ thống

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tên VLAN** | **VLAN ID** | **Subnet** | **Default Gateway** | **Thiết bị** |
| **Banhang** | 2 | 192.168.0.0/26 | 192.168.0.60/26 | SW1\_Quanly, SW2\_Quanly, Banhang |
| **Marketing** | 3 | 192.168.0.64/27 | 192.168.0.92/27 | SW1\_Quanly, SW2\_Quanly, Marketing |
| **CNTT** | 4 | 192.168.0.96/27 | 192.168.0.124/27 | SW1\_Quanly, SW2\_Quanly, CNTT |
| **Dienmay** | 5 | 192.168.0.128/27 | 192.168.0.156/27 | SW1\_Quanly, SW2\_Quanly, Dienmay |
| **Ketoan** | 6 | 192.168.0.160/27 | 192.168.0.188/27 | SW1\_Quanly, SW2\_Quanly, Ketoan |
| **Taichinh** | 7 | 192.168.0.192/27 | 192.168.0.220/27 | SW1\_Quanly, SW2\_Quanly, Taichinh |
| **Hoidong** | 8 | 192.168.0.224/28 | 192.168.0.236/28 | SW1\_Quanly, SW2\_Quanly, Hoidong |
| **Server** | 50 | 192.168.50.0/24 | 192.168.50.252/24 | SW1\_Quanly, SW2\_Quanly, Server |
| **Nhanvien** | 10 | 192.168.10.0/26 | 192.168.10.62/26 | S1, S1\_1, S1\_2, S1\_3 |
| **IT** | 11 | 192.168.10.64/27 | 192.168.10.94/27 | S1, S1\_1, S1\_2 |
| **Hoidong** | 12 | 192.168.10.96/27 | 192.168.10.126/27 | S1, S1\_3 |
| **Nhanvien** | 20 | 192.168.20.0/26 | 192.168.20.62/26 | S2, S2\_1, S2\_2, S2\_3 |
| **IT** | 21 | 192.168.20.64/26 | 192.168.20.126/26 | S2, S2\_1, S2\_2 |
| **Hoidong** | 22 | 192.168.20.128/27 | 192.168.20.158/27 | S2, S2\_3 |

Bảng . Bảng địa chỉ vlan trong hệ thống

### Thông tin cổng Etherchannels

|  |  |  |
| --- | --- | --- |
| **Channel Group** | **Thiết bị trong nhóm** | **Cổng trong nhóm** |
| 1 | SW1\_Quanly, SW2\_Quanly | F0/9, F0/10 |

Bảng . Bảng thông tin về Etherchannels

# CẤU HÌNH HẠ TẦNG

## Thiết lập VTP

VTP giúp cho việc cấu hình VLAN luôn duy trì đồng nhất khi thêm, xóa, sửa thông tin về vlan. Ở cơ sở chính, cấu hình VTP với SW1\_Quanly là server, các switch khác là client với domain name là *huongky*. Bên hai chi nhánh với S1 và S2 là server, các switch còn lại là client với domain name tương ứng *huongky1* và *huongky2*.

Graphical user interface, application

Description automatically generated

Hình . Giao diện hiển thị trạng thái VTP trên SW1\_Quanly

Chế độ hoạt động VTP trên SW1\_Quanly đang là chế độ ***Server*** (Hình 4.1), có domain name là ***huongky***.

Graphical user interface, application

Description automatically generated

Hình . Giao hiện hiển thị trạng thái VTP trên SW2\_Quanly

Chế độ hoạt động VTP trên SW2\_Quanly đang là chế độ Client (Hình 4.2), có domain name là *huongky*, các switch ở phòng ban cũng có trạng thái là client với cùng domain name. Tương tự cho hai bên chi nhánh.

## VLAN cho các phòng ban trong doanh nghiệp

Tạo vlan trên các switch tổng cho doanh nghiệp.

Graphical user interface, table

Description automatically generated

Hình . Giao hiện hiển thị các vlan có trong hệ thống ở cơ sở Hồ Chí Minh

Ở cơ sở chính, trên hai switch SW1\_Quanly và SW2\_Quanly gồm có 8 vlan (xem Hình 4.1) tương ứng với các phòng ban: vlan 2 phòng bán hàng, vlan 3 phòng marketing, vlan 4 phòng CNTT, vlan 5 phòng điện máy, vlan 6 phòng kế toán, vlan 7 phòng tài chính, vlan 8 phòng hội đồng và vlan 50 cho phòng Server.

Table

Description automatically generated

Hình . Giao diện hiển thị các vlan có trong hệ thống ở hai chi nhánh.

Ở chi nhánh Đà Nẵng, trên S1 (Hình 4.2) tạo các vlan gồm có vlan 10 phòng nhân viên, vlan 11 phòng CNTT, vlan 12 phòng hội đồng.

Ở chi nhánh Hải Phòng, trên S2 (Hình 4.2) tạo các vlan gồm có vlan 20 phòng nhân viên, vlan 21 phòng CNTT, vlan 22 phòng hội đồng.

## Cấu hình tính dự phòng

### HSRP

Để cung cấp tính sẵn sàng cho hệ thống mạng, tiến hành cấu hình HSRP tạo gateway ảo cho vlan ở cơ sở chính. Với SW1\_Quanly có priority là 105 cho vlan 2,3,4,5 và SW2\_Quanly có priority là 105 cho vlan 6,7,8,50. Cấu hình track cổng chủ động giành quyền khi một active bị down.

Table

Description automatically generated with medium confidence

Hình . Giao diện hiển thị thông tin HSRP trên SW1\_Quanly

Trên SW1\_Quanly, các vlan 2,3,4,5 có độ ưu tiên là 105 và vlan 6,7,8,50 có độ ưu tiên là 95 đúng như yêu cầu (Hình 4.5). Các vlan có độ ưu tiên là 105 thì sẽ có trạng thái là Active, Standby sẽ có địa chỉ ở bên SW2\_Quanly.

Calendar

Description automatically generated with low confidence

Hình . Giao diện hiển thị thông tin HSRP trên SW2\_Quanly

Trên SW2\_Quanly, các vlan 2,3,4,5 có độ ưu tiên là 95 và vlan 6,7,8,50 có độ ưu tiên là 105 (Hình 4.6). Các vlan có độ ưu tiên là 105 thì sẽ có trạng thái là Active, Standby sẽ có địa chỉ ở bên SW1\_Quanly.

### Spanning-tree

Graphical user interface, text

Description automatically generated

Hình . Giao diện hiển thị thông tin tổng của spanning tree

SW1\_Quanly đang là RootSW cho các vlan Banhang, Marketing, CNTT, Dienmay, SW2\_Quanly là RootSW cho vlan Ketoan, Taichinh, Hoidong, Server.

## Cấu hình tuyến EIGRP và VPN

Tiến hành định tuyến đường đi cho các thiết bị trong hệ thống mạng. Sử dụng passive-interface để không gửi thông tin định tuyến ra ngoài một cách lãng phí của các interface vlan. Sử dụng redistribute vào eigrp trên router để quảng bá các địa chỉ nội bộ cho các switch quản lý.

Thiết lập GRE VPN trên router HoChiMinh\_1, HoChiMinh\_2, DaNang, HaiPhong cho phép các PC có thể truy cập được lẫn nhau, đảm bảo các gói tin giữa mạng nội bộ sẽ được truyền thông qua Tunnel.

Text

Description automatically generated

Hình . Giao diện thông tin định tuyến trên router HoChiMinh\_1

Trên bảng định tuyến (Hình 4.8), router HoChiMinh\_1 đã học được các địa chỉ nội bộ từ các vlan phòng ban từ địa chỉ 192.168.0.242 của SW1\_Quanly đi qua cổng g0/0, bên cạnh đó học luôn các địa chỉ nội bộ cả hai bên chi nhánh thông qua các tunnel 11 172.16.11.3 với Đà Nẵng và tunnel 12 172.16.12.3 với Hải Phòng.

* Interface Tunnel 11: 172.16.11.0/24 kết nối giữa router HoChiMinh\_1 với router DaNang.
* Interface Tunnel 12: 172.16.12.0/24 kết nối giữa router HoChiMinh\_1 với router HaiPhong.

Text

Description automatically generated

Hình . Giao diện thông tin định tuyến trên router HoChiMinh\_2

Trên bảng định tuyến (Hình 4.9), router HoChiMinh\_2 đã học được các địa chỉ nội bộ từ các vlan phòng ban từ địa chỉ 192.168.0.246 của SW2\_Quanly đi qua cổng g0/0, bên cạnh đó học luôn các địa chỉ nội bộ cả hai bên chi nhánh thông qua các tunnel 11 172.16.21.3 với Đà Nẵng và tunnel 12 172.16.22.3 với Hải Phòng.

* Interface Tunnel 21: 172.16.21.0/24 kết nối giữa router HoChiMinh\_2 với router DaNang.
* Interface Tunnel 22: 172.16.22.0/24 kết nối giữa router HoChiMinh\_2 với router HaiPhong.

Graphical user interface, text, application

Description automatically generated

Hình . Giao diện thông tin định tuyến trên router DaNang

Trên bảng định tuyến, router bên chi nhánh Đà Nẵng đã học được tất cả các địa chỉ (Hình 4.10) nội bộ bên trong công ty và các chi nhánh khác thông tunnel đã tạo.

Text

Description automatically generated

Hình . Giao diện thông tin định tuyến trên router HaiPhong

Trên bảng định tuyến, router bên chi nhánh Hải Phòng đã học được tất cả các địa chỉ (Hình 4.11) nội bộ bên trong công ty và các chi nhánh khác thông tunnel đã tạo.

## Thiết lập các dịch vụ Server

* DNS Server: hệ thống phân giải địa chỉ IP thành tên miền và ngược lại.
* Web server: lưu trữ thông tin dữ liệu của website công ty.

Graphical user interface, text, application

Description automatically generated

Hình . Giao diện web của doanh nghiệp

* Mail server: hỗ trợ việc gửi và nhận email.

A screenshot of a computer

Description automatically generated

Hình . Hình minh họa hai người dùng trao đổi email thành công

* FTP Server: hỗ trợ di chuyển các tệp thông qua giao thức FTP.

Text

Description automatically generated

Hình . Hình minh họa đổi tên file.txt thành công

## Xác thực AAA

Sử dụng giao thức bảo mật TACACS (Terminal Access Controller Access Control System) trong dịch vụ AAA là decvice admin dùng để quản trị thiết bị (router), cấu hình thiết bị.

Graphical user interface, application

Description automatically generated

Hình . Giao diện dịch vụ TACACS Server

Tại TACACS Server (Hình 4.15) thiết lập cấu hình dịch vụ với router HoChiMinh\_1 có tacacs key là tacacs1 và router HoChiMinh\_2 là tacacs2, sau đó tạo username là admin1 và password huongky1.

A picture containing application

Description automatically generated

Hình . Giao diện xác thực dịch vụ Tacacs

Trên 2 router ở Hồ Chí Minh, tiến hành nhập username là admin1, mật khẩu huongky1 và kết quả xác thực thành công (Hình 4.16).

## NAT và ACL

* Cấu hình NAT Overload trên các router đảm bảo các máy tính trong doanh nghiệp có thể truy cập Internet.

Background pattern

Description automatically generated with low confidence

Hình . Giao diện hiển thị thông tin NAT Overload trên router HoChiMinh\_2

* Các máy tính trong hệ thống ở cơ sở chính có thể truy cập Internet thành công (Hình 4.17). Tương tự cho các máy tính bên hai chi nhánh.
* NAT server ra ngoài internet với địa chỉ public là 200.0.21.129 cho dịch vụ ftp và địa chỉ public 200.0.21.130 cho dịch vụ web. (nhằm cho các địa chỉ bên ngoài có thể truy cập vào thông qua các port này).

Text

Description automatically generated

Hình . Giao diện hiển thị thông tin static NAT

* *Trên thực tế ta sẽ đi đến nhà cung cấp dịch vụ ISP đăng ký mua IP public để nhà cung cấp cấu hình sao cho các nơi trên thế giới có thể truy cập vào web của ta thông qua ip đó.*

## Thiết lập bảo mật Switch

### Cấu hình DHCP Snooping

Tính năng DHCP Snooping được sử dụng để ngăn chặn phương thức tấn công giả mạo DHCP trên một vlan. Khi DHCP Snooping được bật trên vlan, các cổng thuộc vlan sẽ được chi thành hai loại là trusted port và untrusted port. Mặc định, các cổng thuộc vlan được áp DHCP Snooping sẽ hoạt động ở chế độ untrusted, cho nên phải chỉ định tường minh các cổng trusted trên các cổng kết nối đến DHCP Server. DHCP Snooping cũng có chứa địa chỉ MAC của client, địa chỉ IP được cung cấp, thời gian cấp bao lâu, thông tin cổng, ...

Table

Description automatically generated

Hình . Giao diện hiển thị thông tin DHCP Snooping trên SW1\_Quanly

Bật tính năng DHCP Snooping cho vlan từ 2 đến 8 và vlan 50 (Hình 4.19) để ngăn chặn sự giả mạo dhcp server từ những vlan này. Option 82 được sử dụng để cung cấp thông tin về DHCP Request đến cho DHCP Server. Các gói tin DHCP có thêm option 82 thường có trường “giaddr” nhận giá trị khác 0. Trong trường hợp switch thực hiện chèn option 82 nhưng nó không phải là các dhcp request nên trường “giaddr” phải nhận giá trị 0 dẫn đến dhcp server sẽ coi gói dhcp nhận được là bị lỗi và loại bỏ gói này khiến cho các client sẽ không nhận được cấu hình IP. Vì thế ta thực hiện tắt thao tác chèn Option 82 (disabled).

Các thông tin DHCP Snooping các switch khác ở access layer thì cũng hiển thị như switch CNTT:

Text

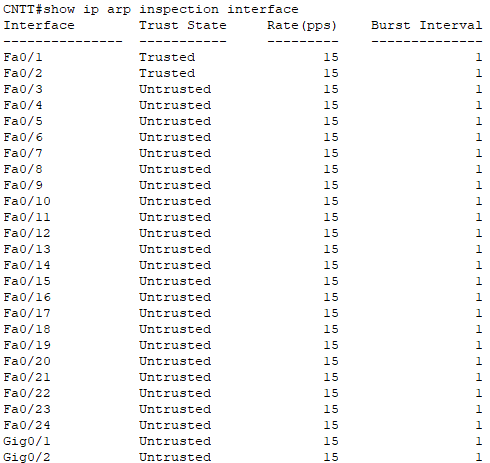
Description automatically generated

Hình . Giao diện hiển thị thông tin DHCP Snooping trên swich CNTT

Tính năng bảo mật DHCP Snooping đã đuợc kích hoạt trên vlan 4 (Hình 4.20). Tương tự cho các switch phòng ban còn lại.

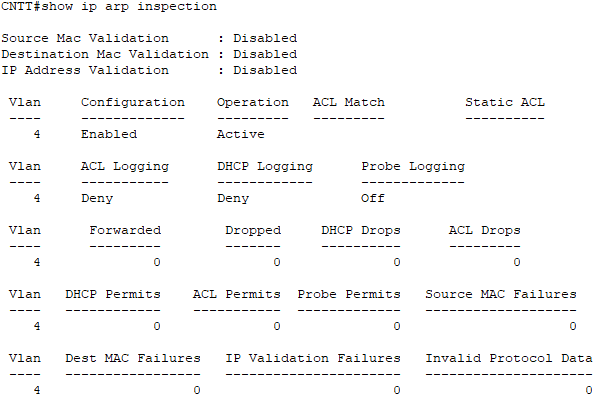
### Cấu hình DAI (Dynamic ARP Inspection)

Xác thực các gói tin giao thức giải quyết địa chỉ trong mạng là ARP. DAI cho phép quản trị viên mạng chặn, ghi thông tin và loại bỏ các gói ARP độc hại hay không với địa chỉ MAC không hợp lệ với các ràng buộc địa chỉ IP.



Hình . Giao diện hiển thị thông tin các cổng khi cấu hình DAI trên switch CNTT

Trong hình 4.21, hai cổng được tin tưởng và những cổng còn lại thì không hiển thị, nhận 15 gói tin ARP trong 1 giây có thể chỉnh sửa lại trong mấy giây nhận được bao nhiêu gói tin ARP để ngăn chặn sự quá tải từ DHCP server.



Hình . Giao diện hiển thị đã thực hiện cấu hình DAI

Switch CNTT được chỉ định cấu hình DAI trên vlan 4 (Hình 4.22) tương tự cho các switch còn lại, do không cấu hình ACL static cho phép địa chỉ và địa chỉ MAC nên không hiển thị thông tin như hình.

## Test case

### Tình huống 1

Giả sử bị đứt 1 dây trên router HoChiMinh\_1, cổng trên router bị shutdown thì tính dự phòng của hệ thống sẽ tự động định tuyến qua router còn lại là HoChiMinh\_2.

* Tiến hành kiểm tra định tuyến trên switch SW1\_Quanly khi bị đứt dây:

Graphical user interface, application

Description automatically generated

Hình . Bảng định tuyến trên switch SW1\_Quanly sau khi bị đứt dây

* Trên SW1\_Quanly (Hình 4.23), đường định tuyến sẽ chuyển sang địa chỉ SW2\_Quanly là 192.168.0.250 thông qua cổng etherchannel.
* Trên PC Host\_Banhang ta ping ra địa chỉ internet là 8.8.8.8:

A screenshot of a computer

Description automatically generated with medium confidence

Hình . Giao diện PC Bán hàng đang truy cập ra internet

* Ping ra internet thành công, ta thử xóa đường link của router HoChiMinh\_1:

A screenshot of a computer

Description automatically generated

Hình . Host\_Banhang truy cập internet sau khi bị đứt dây ở router HoChiMinh\_1

* Kết nối bị đứt đoạn (request timed out) khi đứt dây (Hình 4.25), sau đó vẫn tiếp tục ping được do tính dự phòng được chuyển qua switch SW2\_Quanly.

### Tình huống 2

Hệ thống bị chết hẳn một con switch tổng SW1\_Quanly.

Graphical user interface

Description automatically generated

Hình . Giao diện máy tính ở phòng CNTT đang truy cập internet.

* Tiến hành xóa thử con switch SW1\_Quanly:

Graphical user interface

Description automatically generated

Hình . Giao diện Host\_CNTT truy cập internet sao khi SW1\_Quanly bị chết.

* Kết nối bị đứt đoạn (request timed out) khi đứt dây (Hình 4.27), sau đó vẫn tiếp tục ping được do tính dự phòng được chuyển qua switch SW2\_Quanly.

### Tình huống 3

Bên trụ sở Hồ Chí Minh: thiết lập chỉ cho phòng CNTT và phòng Điện máy có thể telnet/SSH vào các Switch tổng và router với username và password là admin. Chỉ có vlan phòng CNTT và Điện máy được truy cập vào switch và router. Tại router HoChiMinh\_1, HoChiMinh\_2, SW1\_Quanly, SW2\_Quanly.

* Trên máy tính phòng CNTT, ta gõ lệnh ***ssh -l admin 192.168.0.241***:

Text

Description automatically generated

Hình . Giao diện Host CNTT telnet vào router HoChiMinh\_1

* Trên máy tính của phòng CNTT truy cập từ xa vào router HoChiMinh\_1 (Hình 4.28) thành công.
* Trên máy tính phòng Điện máy, ta gõ lệnh ***ssh -l admin 192.168.0.245***:

Text

Description automatically generated

Hình . Giao diện host Dienmay telnet vào router HoChiMinh\_2

* Trên máy tính của phòng điện máy truy cập từ xa vào router HoChiMinh\_2 (Hình 4.29) thành công.
* Kiểm tra các máy tính phòng khác:

Graphical user interface

Description automatically generated

Hình . Giao diện host ở Banhang và Marketing telnet vào router HoChiMinh\_1

* Các máy tính khi truy cập vào đều bị từ chối (Hình 4.30).

### Tình huống 4

Ở chi nhánh Đà Nẵng và Hải Phòng, thiết lập chỉ cho phòng CNTT có thể telnet/SSH với username và password là *admin* vào các Switch tổng và router.

* Trên máy tính Sale\_1 và Giamdoc\_1, ta gõ lệnh ***ssh -l admin 192.168.10.129*** để truy cập vào router Đà Nẵng:

Graphical user interface, website

Description automatically generated

Hình . PC Sale\_1 và Giamdoc\_1 telnet vào router DaNang

* Các máy tính truy cập vào đều bị từ chối.
* Trên máy tính IT\_2, ta gõ lệnh ***ssh -l admin 192.168.10.129*** để truy cập vào router Đà Nẵng:

A screenshot of a computer

Description automatically generated

Hình . PC IT\_2 telnet vào router DaNang

* Trên máy tính của phòng CNTT được phép truy cập từ xa vào router Đà Nẵng thành công (Hình 4.32). Tương tự cho bên chi nhánh Hải Phòng.

### Tình huống 5

Ở chi nhánh Đà Nẵng, phòng Nhân viên (vlan 10) bị cấm truy cập vào vlan 12 (phòng Hội đồng).

* Trên máy tính Sale\_1, tiến hành ping kiểm tra:

Text

Description automatically generated

Hình . Giao diện ping kiểm tra truy cập trên máy tính Sale\_1

* Vlan 10 của máy tính phòng nhân viên truy cập internet thì thành công (Hình 4.33) tuy nhiên khi truy cập vào máy tính phòng giám đốc thì bị cấm (Destination host unreachable).

# KẾT LUẬN

## Những kết quả đạt được

* Về mặt lý thuyết: tìm hiểu một số nội dung cơ bản liên quan đến mạng cũng như bảo mật mạng máy tính.
* Về mặt thực hành: dùng Packet Tracer thiết kế được mô hình mạng cho doanh nghiệp; triển khai các cấu hình mạng căn bản đối với mạng nội bộ với đầy đủ các dịch vụ server; áp dụng một số chức năng bảo mật như NAT, ACL, xác thực AAA, bảo mật switch, VPN kết nối giữa các chi nhánh. Hệ thống hoạt động bình thường có tính dự phòng và các máy tính có thể liên lạc lẫn nhau.

## Những hạn chế và hướng phát triển

* Hạn chế: trong quá trình thực hiện dự án, chúng em đã cố gắng nghiên cứu thiết kế tuy nhiên do kiến thức vẫn còn nhiều thiếu sót vẫn chưa cấu hình được Firewall áp dụng vào mô hình. Các chức năng bảo mật vẫn ở mức tương đối.
* Hướng phát triển: cần nghiên cứu và học hỏi nhiều mô hình mạng doanh nghiệp thực tiễn. Phát triển thêm chức năng tường lửa nhằm gia tăng tính bảo mật cao cho mô hình mạng. Đưa ra thêm nhiều tình huống thực tiễn và hợp lý cho hệ thống mạng.

# TÀI LIỆU THAM KHẢO

**Tiếng Việt**

[1] VPN là gì? Phân loại VPN | sinhvientot.net. (2016). Retrieved 19 April 2022, from <https://sinhvientot.net/vpn-la-gi-phan-loai-vpn/>

[2] Mạng máy tính là gì? | quantrimang.com. (2021). Retrieved 22 April 2022, from <https://quantrimang.com/gioi-thieu-chung-ve-mang-may-tinh-16>

[3] Mạng máy tính là gì? | saigonmachinco.com.vn. (2021). Retrieved 22 April 2022, from <https://saigonmachinco.com.vn/mo-hinh-mang-pho-bien-hien-nay-la-gi/>

[4] Mô hình thiết kế giải pháp mạng switch theo các lớp | n-tek.com.vn. (2019). Retrieved 22 April 2022, form <http://n-tek.com.vn/mo-hinh-thiet-ke-giai-phap-mang-swicth-theo-cac-lop.html>

[5] Cấu hình DHCP Snooping trên switch Cisco | vnexperts.vn, (2022). Retrieved 22 April 2022, from <https://vnexperts.vn/cau-hinh-dhcp-snooping-cisco.html>

[6] Bảo Mật Mạng Máy Tính Là Gì? Tại Sao Phải Bảo Mật Mạng Máy Tính?. (2022). Retrieved 22 April 2022, from <https://itsystems.vn/bao-mat-mang-may-tinh-la-gi/>

**Tiếng Anh**

[1] Mitton, D., Johns, M. S., Barkley, S., Nelson, D., Patil, B., Stevens, M., & Wolff, B. (2001). RFC3127: Authentication, Authorization, and Accounting: Protocol Evaluation.

[2] AAA Protocol. (2022). Retrieved 19 April 2022, from <https://www.slideshare.net/Netwaxlab/nxld75-aaa-protocol>

[3] CCNA 3 v7.0 Curriculum: Module 8 – VPN and IPsec Concepts. (2022). Retrieved 19 April 2022, from <https://itexamanswers.net/ccna-3-v7-0-curriculum-module-8-vpn-and-ipsec-concepts.html>

[4] What is a Firewall?. (2022). Retrieved 22 April 2022, form <https://www.forcepoint.com/cyber-edu/firewall>

[5] CCNA 3 v7.0 Curriculum: Module 4 – ACL Concepts. (2022). Retrieved 19 April 2022, from <https://itexamanswers.net/ccna-3-v7-0-curriculum-module-4-acl-concepts.html>

[6] CCNA 3 v7.0 Curriculum: Module 6 – NAT for IPv4. (2022). Retrieved 20 April 2022, from <https://itexamanswers.net/ccna-3-v7-0-curriculum-module-6-nat-for-ipv4.html>

[7] What is a firewall?. (2021). Retrieved 22 April 2022, form <https://www.techtarget.com/searchsecurity/definition/firewall>

[8] Firewall (computing). (2022) Retrieved 22 April 2022, form <https://en.wikipedia.org/wiki/Firewall_(computing)>

# PHỤ LỤC

**TRÌNH BÀY CẤU HÌNH CHI TIẾT HẠ TẦNG HỆ THỐNG**

* 1. Cấu hình Hostname và địa chỉ
  2. Cấu hình vlan, VTP, trunking
  3. Cấu hình HSRP
  4. Cấu hình DHCP Server
  5. Cấu hình Etherchannel
  6. Cấu hình Spanning Tree
  7. Cấu hình định tuyến EIGRP
  8. Thiết lập Server
  9. Cấu hình xác thực AAA
  10. Cấu hình NAT
  11. Cấu hình VPN
  12. Cấu hình ACL
  13. Cấu hình bảo mật switch