BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

BÁO CÁO CUỐI KỲ GIAO THỨC MẠNG

BÁO CÁO CUỐI KỲ GIAO THỨC MẠNG

Người hướng dẫn: GV. LÊ VIẾT THANH
Người thực hiện: Lê Tuấn Đăng Khoa – 52000350
Khóa: 2024-2025

HỒ CHÍ MINH – 2024

LỜI CẢM ƠN

Trước tiên, em xin gửi lời cảm ơn chân thành đến thầy Lê Viết Thanh đã luôn tận tình chỉ bảo, hướng dẫn và giúp đỡ em trong suốt quá trình thực hiện đề tài báo cáo. Sự giúp đỡ và những chỉ dẫn quý báu của thầy đã giúp em hoàn thành bài báo cáo này một cách tốt nhất.

Em cũng xin cảm ơn Trường đại học Tôn Đức Thắng đã tạo điều kiện cho em có cơ hội tiếp cận và tìm hiểu sâu hơn. Đây là cơ hội quý giá giúp em phát triển kiến thức và kỹ năng trong quá trình học tập và nghiên cứu.

Em hy vọng rằng những kiến thức và kinh nghiệm thu được từ quá trình thực hiện đề tài sẽ là nền tảng hữu ích cho những nghiên cứu và công việc sau này.

ĐỒ ÁN ĐƯỢC HOÀN THÀNH TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

Tôi xin cam đoan đây là sản phẩm đồ án của riêng tôi và được sự hướng dẫn của Thầy Lê Viết Thanh. 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 đồ án 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 tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án 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 9 tháng 5 năm 2025

Tác giả
(ký tên và ghi rõ họ tên)
Lê Tuấn Đăng Khoa

TÓM TẮT

Báo cáo tập trung vào việc triển khai hệ thống mạng doanh nghiệp vừa trên Cisco Packet Tracer, áp dụng các giao thức định tuyến, cấu hình DHCP, NAT và ACL để đảm bảo hiệu suất và bảo mật. Các nội dung chính được trình bày qua các chương sau:

- **Chương 1 - Tổng quan về đề tài**
  - Giới thiệu về mạng của tổ chức: Mạng doanh nghiệp bao gồm hai khu vực HQ (R4, R5, R6, R7, R8) và BRANCH (R1, R2, R3), với các VLAN nội bộ (10, 20, 30, 40, 50, 60) phục vụ các phòng ban.
  - Mô tả các vấn đề cần giải quyết: Đảm bảo kết nối giữa HQ và BRANCH, phân phối tuyến giữa EIGRP và OSPF, cho phép các host nội bộ truy cập Internet, và bảo mật mạng.
  - Các yêu cầu cụ thể trong cấu hình: Cấu hình EIGRP ở HQ, OSPF ở BRANCH, DHCP trên R4, NAT trên ACCESS, và ACL để kiểm soát truy cập.
- **Chương 2 - Phân tích thiết kế hệ thống**
  - Phân tích yêu cầu mạng, bao gồm phân đoạn VLAN, kết nối Internet và bảo mật.
  - Giới thiệu các giao thức OSPF, EIGRP, DHCP, NAT và ACL.
- **Chương 3 - Triển khai và kiểm tra hệ thống**
  - Mô tả chi tiết quá trình cấu hình mạng trên Cisco Packet Tracer, bao gồm OSPF, EIGRP, DHCP, NAT và ACL.
  - Kiểm tra kết nối giữa các VLAN nội bộ và từ các host nội bộ ra Internet.

- **Chương 4 - Đánh giá và đề xuất cải tiến**
  - Đánh giá hiệu quả hệ thống qua các bài kiểm tra ping từ Web-Server và User-PC ra Internet.
  - Đề xuất các giải pháp cải tiến như tích hợp công nghệ mới để nâng cao hiệu suất và bảo mật.

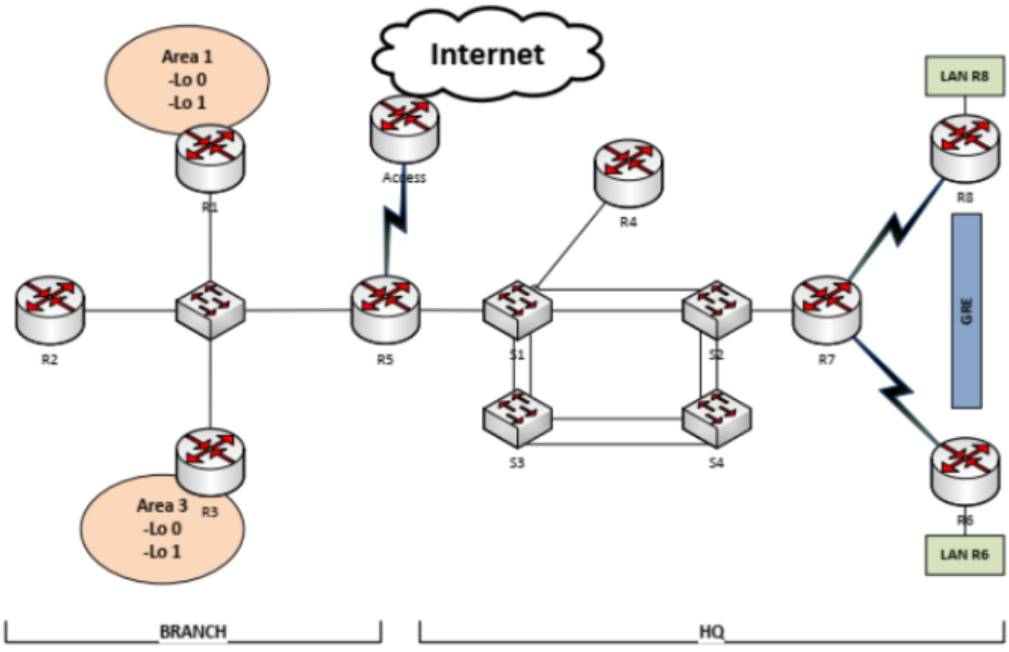
MỤC LỤC

DANH SÁCH HÌNH ẢNH

1 CHƯƠNG 1: TỔNG QUAN VỀ ĐỀ TÀI

1.1 Giới thiệu mạng

Mạng của tổ chức được thiết kế để phục vụ một doanh nghiệp vừa, bao gồm hai khu vực chính: HQ và BRANCH. Khu vực HQ bao gồm các router R4, R5, R6, R7, R8, quản lý các VLAN nội bộ (VLAN 10, 20, 30, 40, 50, 60) tương ứng với các phòng ban như Kế toán, Kinh doanh, Nhân sự, IT, Điều hành và Quản trị. Khu vực BRANCH bao gồm các router R1, R2, R3, kết nối thông qua mạng 172.16.1.0/29. Router R5 đóng vai trò router biên, kết nối giữa HQ và BRANCH, đồng thời đảm bảo kết nối từ mạng nội bộ ra Internet thông qua ACCESS router và Router-Internet. Hệ thống mạng được triển khai trên Cisco Packet Tracer, sử dụng các giao thức định tuyến và công nghệ để đảm bảo hiệu suất và bảo mật.



Hình 1: Sơ đồ mạng

Hình 1: Sơ đồ mạng

1.2 Các vấn đề cần giải quyết

Trong quá trình triển khai hệ thống mạng, một số vấn đề cần được giải quyết để đảm bảo hoạt động ổn định và hiệu quả:

- **Kết nối giữa HQ và BRANCH:** Đảm bảo các router ở HQ (R4, R5) và BRANCH (R1, R2, R3) kết nối thông suốt, không xảy ra lỗi định tuyến như "mismatch area ID" trong OSPF.
- **Phân phối tuyến giữa EIGRP và OSPF:** Cần cấu hình R5 để phân phối tuyến giữa EIGRP (HQ) và OSPF (BRANCH) nhằm đảm bảo các mạng nội bộ có thể giao tiếp với nhau.
- **Truy cập Internet từ mạng nội bộ:** Các host nội bộ (như Web-Server, User-PC) cần truy cập Internet thông qua ACCESS router, yêu cầu cấu hình NAT phù hợp.
- **Bảo mật mạng:** Ngăn chặn truy cập trái phép, ví dụ chặn VLAN 40 (IT) truy cập các mạng nội bộ khác, và chỉ cho phép VLAN 60 (Quản trị) truy cập VTY của các switch.
- **Phân phối IP tự động:** Đảm bảo các host trong các VLAN nội bộ nhận IP tự động thông qua DHCP từ R4.

1.3 Các yêu cầu cụ thể trong cấu hình

Để đáp ứng mục tiêu của hệ thống mạng, các yêu cầu cấu hình cụ thể bao gồm:

- **Cấu hình EIGRP ở HQ:** Triển khai EIGRP (AS 1) trên R4, R5, R6, R7, R8 để kết nối các VLAN nội bộ (10, 20, 30, 40, 50, 60) và đảm bảo quảng bá tuyến hiệu quả.
- **Cấu hình OSPF ở BRANCH:** Triển khai OSPF trên R1, R2, R3, R5 với Area 0 (mạng 172.16.1.0/29) và Area 1, sử dụng virtual-link để kết nối các Area không trực tiếp với backbone.

- **Phân phối tuyến trên R5:** Cấu hình R5 để phân phối tuyến giữa EIGRP và OSPF, đảm bảo các mạng nội bộ ở HQ và BRANCH có thể giao tiếp.
- **Cấu hình DHCP trên R4:** Thiết lập R4 làm DHCP server để phân phối IP tự động cho các VLAN nội bộ, bao gồm Default Gateway và DNS.
- **Cấu hình NAT trên ACCESS:** Áp dụng NAT động và tĩnh trên ACCESS router để cho phép các host nội bộ truy cập Internet, đặc biệt là Web-Server (VLAN 50) qua port 80 và 443.
- **Cấu hình ACL:** Áp dụng ACL trên ACCESS để chặn VLAN 40 truy cập các mạng nội bộ nhưng cho phép ra Internet, và trên S1, S2, S3, S4 để chỉ cho phép VLAN 60 truy cập VTY.

2 CHƯƠNG 2: PHÂN TÍCH VÀ THIẾT KẾ

2.1 Bảng Address Table

Bảng Address Table dưới đây liệt kê địa chỉ IP, subnet mask và default gateway của các thiết bị trong hệ thống mạng doanh nghiệp:

STT	**Thiết bị/Host**	**Địa chỉ IP**	**Subnet Mask/Prefix**	**Default Gateway**
1	S1 (VLAN 60)	192.168.60.3	255.255.255.224 (/27)	192.168.60.1
2	S2 (VLAN 60)	192.168.60.4	255.255.255.224 (/27)	192.168.60.1
3	S3 (VLAN 60)	192.168.60.5	255.255.255.224 (/27)	192.168.60.1
4	S4 (VLAN 60)	192.168.60.6	255.255.255.224 (/27)	192.168.60.1
5	R6-PC	200.0.100.14	255.255.255.252 (/30)	200.0.100.13
6	R8-PC	200.0.100.18	255.255.255.252 (/30)	200.0.100.17
7	Internet-PC	209.165.200.2	255.255.255.252 (/30)	209.165.200.1
8	R1 (Gig0/0)	172.16.1.3	255.255.255.248 (/29)	–
9	R1 (Lo 0)	172.16.10.1	255.255.254.0 (/23)	–
10	R1 (Lo 1)	172.16.12.1	255.255.254.0 (/23)	–

STT	Thiết bị/Host	Địa chỉ IP	Subnet Mask/Prefix	Default Gateway
11	R2 (Gig0/0)	172.16.1.1	255.255.255.248 (/29)	–
12	R2 (Lo 0)	172.16.14.1	255.255.255.128 (/25)	–
13	R3 (Gig0/0)	172.16.1.2	255.255.255.248 (/29)	–
14	R3 (Lo 0)	172.16.15.1	255.255.255.0 (/24)	–
15	R3 (Lo 1)	172.16.16.1	255.255.255.128 (/25)	–
16	R4 (Gig0/0)	192.168.1.2	255.255.255.252 (/30)	–
17	R4 (Gig0/0.10)	192.168.10.1	255.255.255.0 (/24)	–
18	R4 (Gig0/0.20)	192.168.20.1	255.255.254.0 (/23)	–
19	R4 (Gig0/0.30)	192.168.30.1	255.255.255.128 (/25)	–
20	R4 (Gig0/0.40)	192.168.40.1	255.255.255.192 (/26)	–
21	R4 (Gig0/0.50)	192.168.50.1	255.255.255.240 (/28)	–
22	R4 (Gig0/0.60)	192.168.60.1	255.255.255.224 (/27)	–
23	R5 (Gig0/0)	172.16.1.4	255.255.255.248 (/29)	–

STT	Thiết bị/Host	Địa chỉ IP	Subnet Mask/Prefix	Default Gateway
24	R5 (Gig0/1)	192.168.1.1	255.255.255.252 (/30)	–
25	R5 (Se0/0/0)	200.0.100.9	255.255.255.252 (/30)	–
26	R6 (Se0/0/0)	200.0.100.13	255.255.255.252 (/30)	–
27	R6 (Se0/0/1)	200.0.100.1	255.255.255.252 (/30)	–
28	R7 (Gig0/0)	192.168.1.2	255.255.255.252 (/30)	–
29	R7 (Se0/0/0)	200.0.100.2	255.255.255.252 (/30)	–
30	R7 (Se0/0/1)	200.0.100.5	255.255.255.252 (/30)	–
31	R8 (Se0/0/0)	200.0.100.6	255.255.255.252 (/30)	–
32	R8 (Se0/0/1)	200.0.100.17	255.255.255.252 (/30)	–
33	ACCESS (Se0/0/0)	200.0.100.10	255.255.255.252 (/30)	–
34	ACCESS (Se0/0/1)	203.0.113.2	255.255.255.252 (/30)	–
35	Router-Internet (Se0/0/0)	203.0.113.1	255.255.255.252 (/30)	–

STT	Thiết bị/Host	Địa chỉ IP	Subnet Mask/Prefix	Default Gateway
36	Router-Internet (G0/0)	209.165.200.1	255.255.255.252 (/30)	–
37	User-PC (VLAN 10)	192.168.10.2	255.255.255.0 (/24)	192.168.10.1
38	Web-Server (VLAN 50)	192.168.50.2	255.255.255.240 (/28)	192.168.50.1
39	Admin-PC (VLAN 60)	192.168.60.2	255.255.255.224 (/27)	192.168.60.1

Bảng 1: Bảng Address Table

2.2 Giới thiệu sơ các giao thức

Hệ thống mạng sử dụng các giao thức sau để đảm bảo hoạt động hiệu quả:

- **OSPF (Open Shortest Path First):** Giao thức định tuyến trạng thái liên kết, sử dụng thuật toán Dijkstra để tính đường đi ngắn nhất. OSPF được triển khai ở khu vực BRANCH (R1, R2, R3, R5) với Area 0 và Area 1.
- **EIGRP (Enhanced Interior Gateway Routing Protocol):** Giao thức định tuyến lai, kết hợp trạng thái liên kết và khoảng cách vector, sử dụng thuật toán DUAL. EIGRP được triển khai ở khu vực HQ (R4, R5, R6, R7, R8).
- **DHCP (Dynamic Host Configuration Protocol):** Giao thức tự động phân phối địa chỉ IP, Default Gateway và DNS cho các host trong VLAN. DHCP được cấu hình trên R4 để phục vụ

các VLAN nội bộ.

- **NAT (Network Address Translation):** Giao thức chuyển đổi địa chỉ IP nội bộ thành địa chỉ công khai để kết nối Internet. NAT được cấu hình trên ACCESS router với NAT động và tĩnh.
- **ACL (Access Control List):** Danh sách kiểm soát truy cập, dùng để lọc lưu lượng mạng dựa trên địa chỉ IP, giao thức, và port. ACL được áp dụng trên ACCESS và các switch để bảo mật mạng.

3 CHƯƠNG 3: TRIỂN KHAI VÀ KIỂM TRA HỆ THỐNG

3.1 Cấu hình mạng trên Cisco Packet Tracer

Quá trình triển khai hệ thống mạng được thực hiện trên Cisco Packet Tracer, bao gồm các bước cấu hình sau:

3.1.1 Cấu hình EIGRP trên khu vực HQ

EIGRP được triển khai trên các router R4, R5, R6, R7, R8 để kết nối các VLAN nội bộ và đảm bảo định tuyến trong khu vực HQ:

- **Trên R4:**

```
router eigrp 1
 network 192.168.1.0 0.0.0.3
 network 192.168.10.0 0.0.0.255
 network 192.168.20.0 0.0.1.255
 network 192.168.30.0 0.0.0.127
 network 192.168.40.0 0.0.0.63
 network 192.168.50.0 0.0.0.15
 network 192.168.60.0 0.0.0.31
```

- **Trên R5:**

```
router eigrp 1
 redistribute ospf 1 match internal external 1 external 2
 redistribute static metric 1000 100 255 1 1500
 passive-interface GigabitEthernet0/0
 network 192.168.1.0 0.0.0.3
 network 200.0.100.8 0.0.0.3
 network 172.16.1.0 0.0.0.7
```

3.1.2 Cấu hình OSPF trên khu vực BRANCH

OSPF được triển khai trên các router R1, R2, R3, R5 để kết nối khu vực BRANCH, với Area 0 và Area 1:

- **Trên R1:**

```
router ospf 1
 router-id 172.16.10.1
 network 172.16.1.0 0.0.0.7 area 0
 network 172.16.10.0 0.0.1.255 area 1
 network 172.16.12.0 0.0.1.255 area 1
 area 1 virtual-link 172.16.14.1
 area 1 virtual-link 172.16.15.1
```

- **Trên R5:**

```
router ospf 1
 network 172.16.1.0 0.0.0.7 area 0
 network 192.168.1.0 0.0.0.3 area 1
 network 200.0.100.8 0.0.0.3 area 1
 default-information originate
 redistribute eigrp 1 subnets
```

3.1.3 Cấu hình DHCP trên R4

R4 được cấu hình làm DHCP server để phân phối địa chỉ IP cho các VLAN nội bộ:

```
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
ip dhcp excluded-address 192.168.30.1
ip dhcp excluded-address 192.168.40.1
ip dhcp pool VLAN10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 8.8.8.8
ip dhcp pool VLAN20
 network 192.168.20.0 255.255.254.0
 default-router 192.168.20.1
 dns-server 8.8.8.8
ip dhcp pool VLAN30
 network 192.168.30.0 255.255.255.128
 default-router 192.168.30.1
 dns-server 8.8.8.8
ip dhcp pool VLAN40
 network 192.168.40.0 255.255.255.192
 default-router 192.168.40.1
```

```
dns-server 8.8.8.8
```

3.1.4 Cấu hình NAT trên ACCESS

ACCESS router được cấu hình NAT để cho phép các host nội bộ truy cập Internet:

```
access-list 1 permit 192.168.0.0 0.0.255.255
access-list 1 permit 172.16.0.0 0.0.255.255
access-list 1 permit 200.0.100.8 0.0.0.3
ip nat inside source list 1 interface Serial0/0/1 overload
ip nat inside source static tcp 192.168.50.2 80 203.0.113.2 80
ip nat inside source static tcp 192.168.50.2 443 203.0.113.2 443
interface Serial0/0/0
 ip nat inside
interface Serial0/0/1
 ip nat outside
```

3.1.5 Cấu hình ACL

ACL được áp dụng để kiểm soát truy cập và bảo mật:

- **Trên ACCESS:**

```
access-list 101 deny ip 192.168.40.0 0.0.0.63 192.168.0.0
    0.0.255.255
access-list 101 deny ip 192.168.40.0 0.0.0.63 172.16.0.0
    0.0.255.255
access-list 101 permit ip 192.168.40.0 0.0.0.63 any
interface Serial0/0/0
 ip access-group 101 in
```

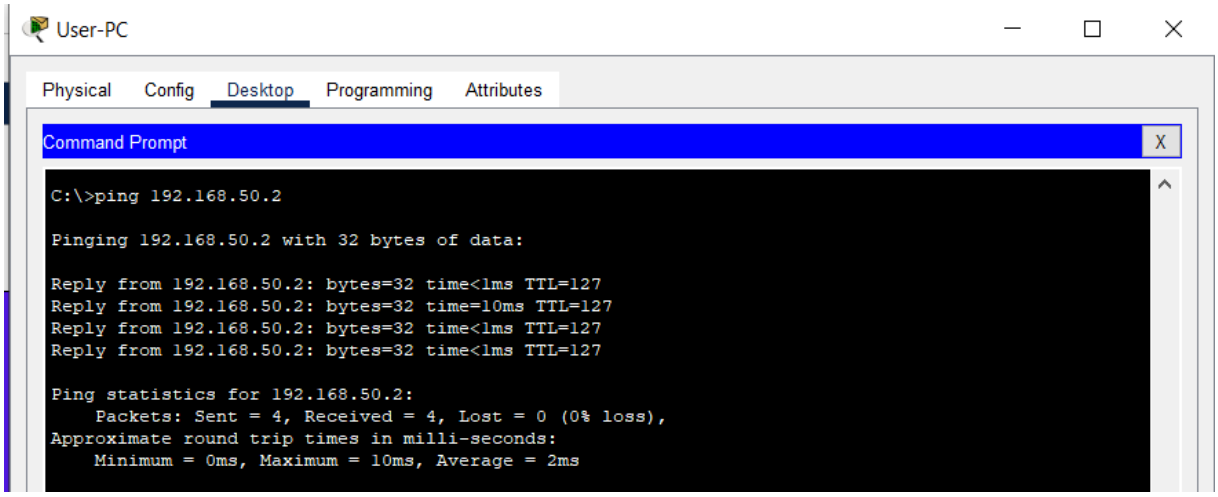
- **Trên S1 (tương tự cho S2, S3, S4):**

```
access-list 102 permit ip 192.168.60.0 0.0.0.31 any
line vty 0 4
 access-class 102 in
 password cisco
 login
```

3.2 Kiểm tra kết nối

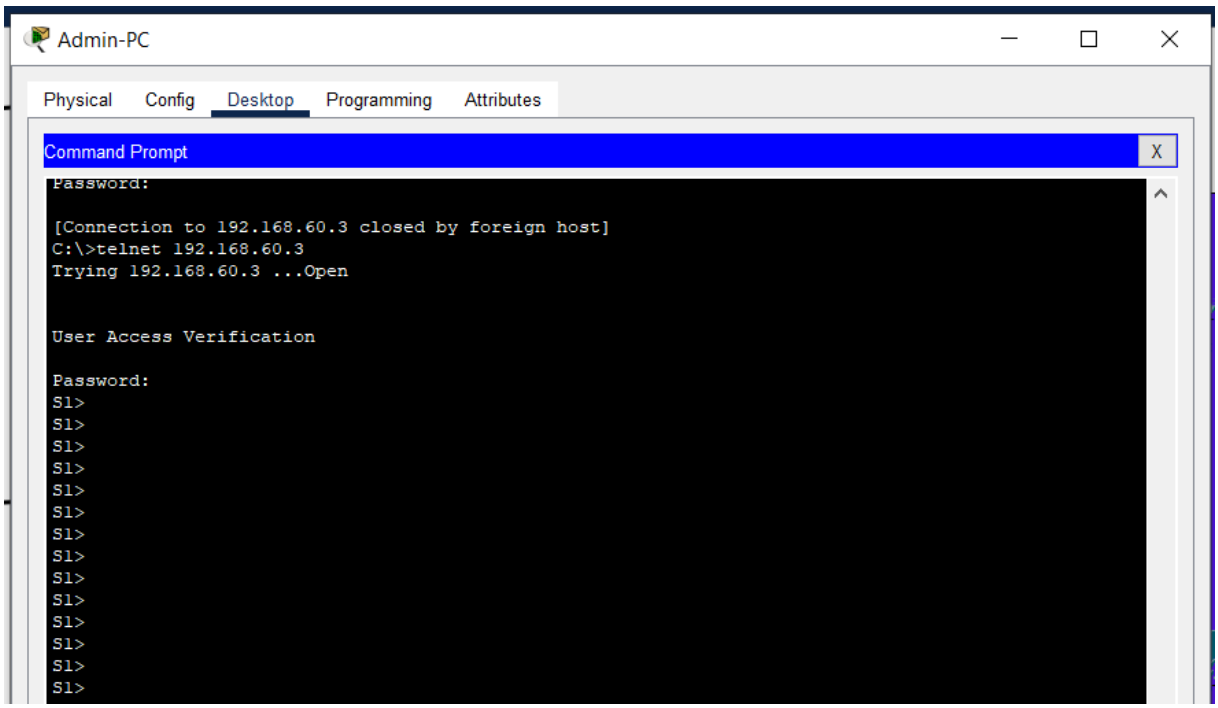
Sau khi cấu hình, các bài kiểm tra kết nối được thực hiện để đảm bảo hệ thống hoạt động đúng:

- **Kết nối giữa các VLAN nội bộ:**
  - Từ User-PC (VLAN 10, 192.168.10.2) ping đến Web-Server (VLAN 50, 192.168.50.2): Thành công với 100% gói tin được phản hồi.



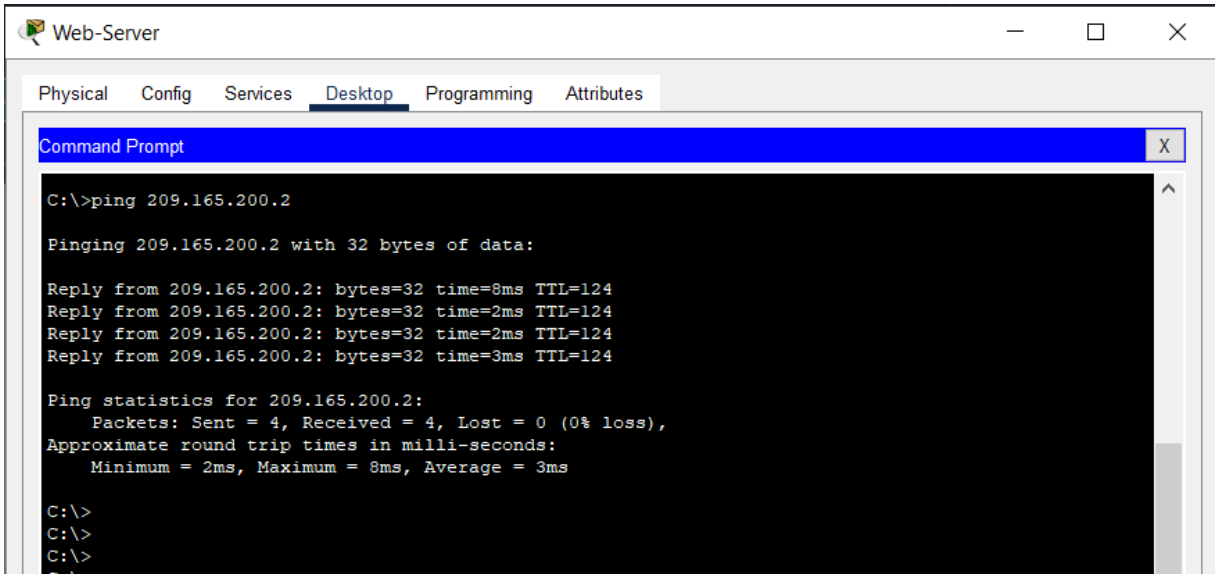
Hình 2: kết quả ping

  - Từ Admin-PC (VLAN 60, 192.168.60.2) Telnet đến S1 (192.168.60.3): Thành công sau khi nhập mật khẩu VTY.

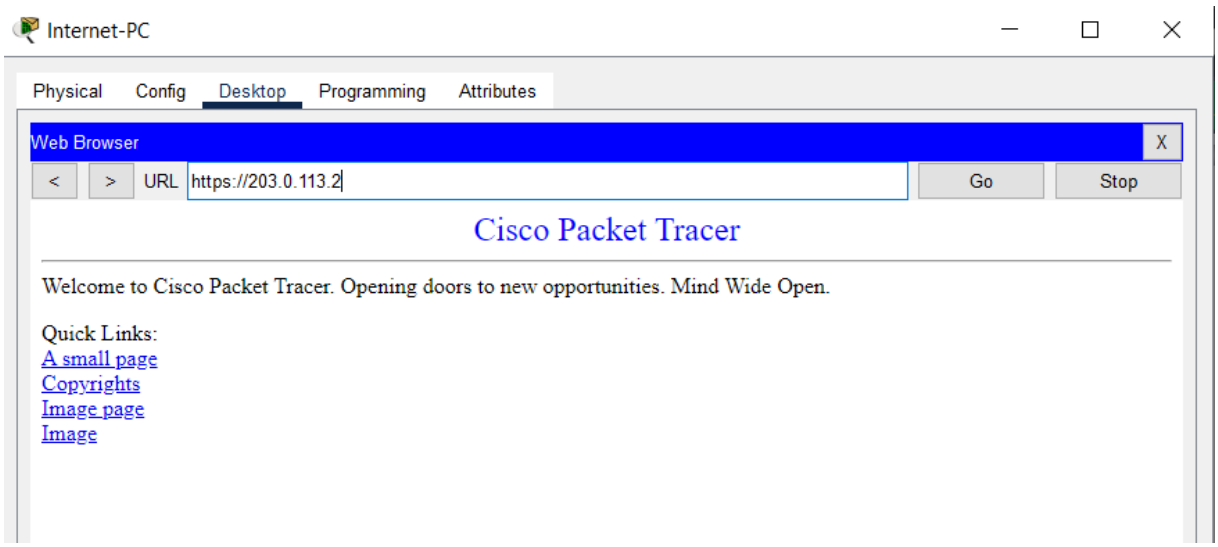


Hình 3: telnet thành công

- **Kết nối từ host nội bộ ra Internet:**
  - Từ Web-Server (192.168.50.2) ping đến Internet-PC (209.165.200.2): Thành công với 100% gói tin được phản hồi.

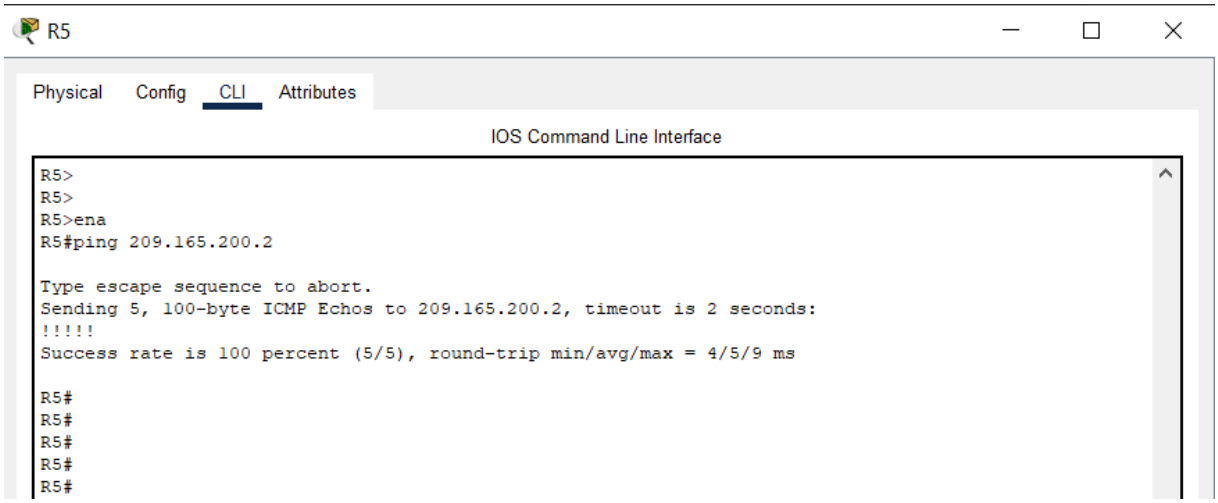


Hình 4: kết nối thành công

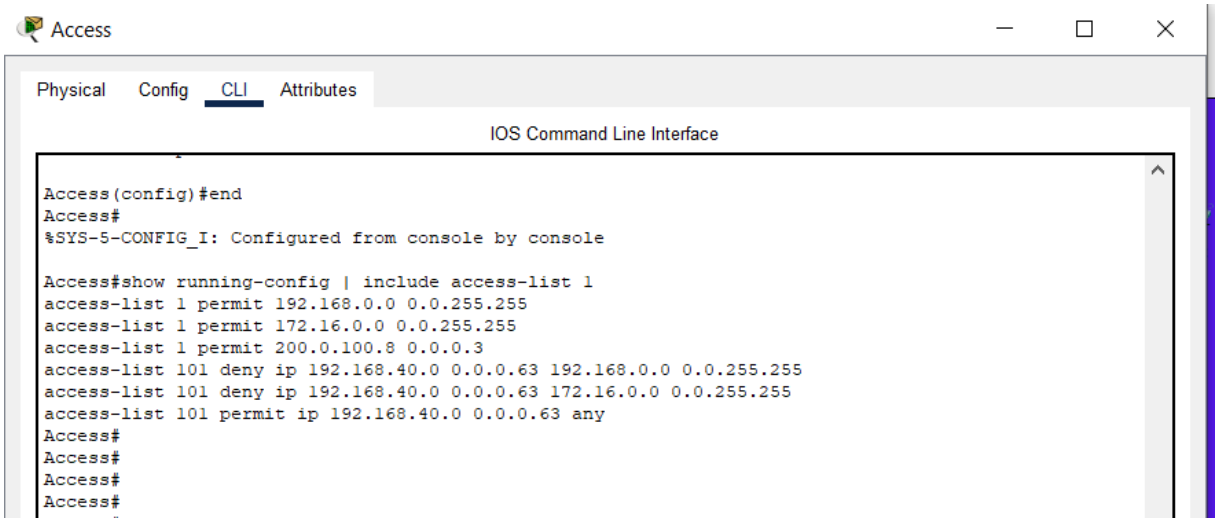


Hình 5: kết nối được vào web

– Từ R5 (200.0.100.9) ping đến Internet-PC: Thành công sau khi bổ sung mạng 200.0.100.8/30 vào ACL 1 trên ACCESS.

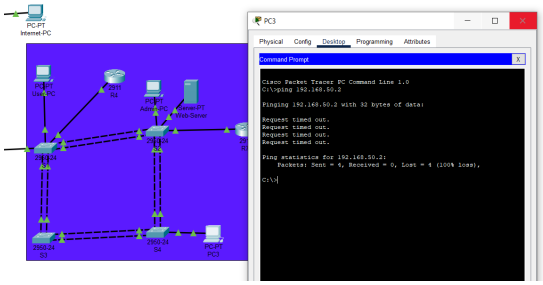


Hình 6: ping thành công

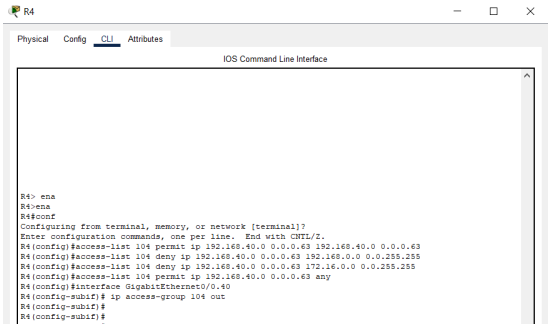


Hình 7: ACCESS ACL1

- **Kiểm tra ACL:**
  - Từ VLAN 40 (192.168.40.2) ping đến VLAN 50 (192.168.50.2): Bị chặn, đúng với ACL 101 trên ACCESS.



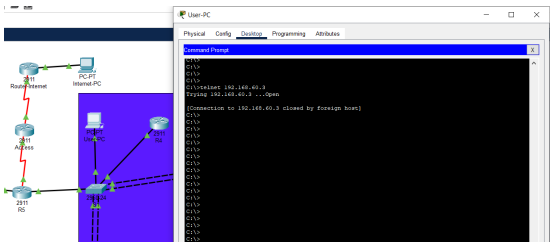
(a) Kết quả ping từ VLAN 40 đến VLAN 50



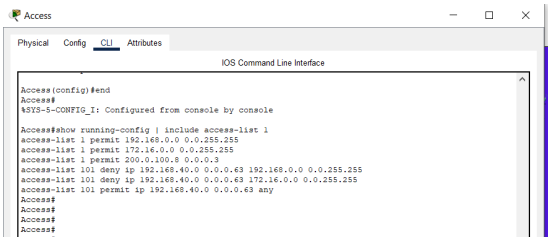
(b) Cấu hình ACL 101 trên R4

Hình 8: Kết quả kiểm tra ping từ VLAN 40 đến VLAN 50 bị chặn bởi ACL 101

  - Từ VLAN 10 (192.168.10.2) Telnet đến S1 (192.168.60.3): Bị chặn, chỉ VLAN 60 được phép truy cập VTY.



(a) Kết quả Telnet từ VLAN 10 đến S1



(b) Cấu hình ACL 102 trên S1

Hình 9: Kết quả kiểm tra Telnet từ VLAN 10 đến S1 bị chặn bởi ACL 102

4 CHƯƠNG 4: ĐÁNH GIÁ VÀ ĐỀ XUẤT CẢI TIẾN

4.1 Đánh giá hiệu quả hệ thống

Hệ thống mạng đã được triển khai và kiểm tra trên Cisco Packet Tracer, với các kết quả đánh giá như sau:

- **Kết nối nội bộ giữa các VLAN:** Các host trong các VLAN nội bộ của HQ (VLAN 10, 20, 30, 40, 50, 60) có thể kết nối với nhau thông qua EIGRP. Ví dụ, User-PC (VLAN 10, 192.168.10.2) ping thành công đến Web-Server (VLAN 50, 192.168.50.2) với tỷ lệ thành công 100%.
- **Kết nối giữa HQ và BRANCH:** Phân phối tuyến giữa EIGRP và OSPF trên R5 hoạt động hiệu quả, cho phép các mạng trong HQ và BRANCH giao tiếp với nhau. Các lỗi ban đầu như "mismatch area ID" trong OSPF đã được khắc phục bằng cách cấu hình lại Area 0 và sử dụng virtual-link.
- **Truy cập Internet:** Các host nội bộ có thể truy cập Internet thông qua NAT trên ACCESS router:
  - Web-Server (192.168.50.2) ping thành công đến Internet-PC (209.165.200.2) với tỷ lệ thành công 100%.
  - GUEST-PC (VLAN 40, 192.168.40.2) cũng truy cập được Internet (209.165.200.2) với tỷ lệ thành công 100% sau khi áp dụng ACL 104 trên R4 và đảm bảo ACL 101 trên ACCESS cho phép lưu lượng ra ngoài.
- **Bảo mật với ACL:** Các yêu cầu bảo mật được đáp ứng:
  - VLAN 40 (GUEST) không thể truy cập mạng HQ và BRANCH, nhưng vẫn truy cập được Internet nhờ ACL 104 trên R4. Kiểm

tra cho thấy GUEST-PC (192.168.40.2) không ping được Web-Server (192.168.50.2) và các mạng BRANCH (như 172.16.1.3).

– Chỉ VLAN 60 (Quản trị) được phép truy cập VTY của các switch (S1, S2, S3, S4). User-PC (VLAN 10, 192.168.10.2) bị chặn khi Telnet đến S1 (192.168.60.3), trong khi Admin-PC (VLAN 60, 192.168.60.2) Telnet thành công.

4.2 Đề xuất cải tiến

Để nâng cao hiệu suất và bảo mật của hệ thống mạng, các giải pháp cải tiến sau được đề xuất:

- **Tích hợp giao thức định tuyến tiên tiến hơn:** Thay vì chỉ sử dụng EIGRP và OSPF, có thể tích hợp BGP (Border Gateway Protocol) để quản lý định tuyến giữa HQ và BRANCH hiệu quả hơn, đặc biệt khi mở rộng hệ thống với nhiều chi nhánh.
- **Sử dụng VLAN động với GVRP:** Thay vì cấu hình VLAN tĩnh, có thể sử dụng GVRP (GARP VLAN Registration Protocol) để tự động quản lý VLAN, giảm thiểu công việc cấu hình thủ công khi thêm VLAN mới.
- **Nâng cấp bảo mật với Firewall:** Ngoài ACL, nên triển khai Firewall (như Cisco ASA) tại ACCESS router để kiểm tra sâu gói tin (Deep Packet Inspection) và bảo vệ hệ thống trước các mối đe dọa từ Internet.
- **Giám sát lưu lượng mạng:** Sử dụng các công cụ giám sát như Cisco Prime hoặc SolarWinds để theo dõi lưu lượng mạng theo thời gian thực, giúp phát hiện và xử lý kịp thời các sự cố như nghẽn mạng hoặc tấn công.

- **Tối ưu hóa NAT:** Hiện tại NAT trên ACCESS sử dụng PAT (Port Address Translation) với ‘overload‘. Có thể triển khai thêm NAT pool để phân phối địa chỉ công khai linh hoạt hơn, giảm tải cho giao diện Serial0/0/1.
- **Cải thiện tính sẵn sàng cao:** Áp dụng các giao thức như HSRP (Hot Standby Router Protocol) trên R4 và R5 để đảm bảo dự phòng, tránh gián đoạn dịch vụ nếu một router gặp sự cố.