**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

A picture containing logo

Description automatically generated**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

**KHOA CÔNG NGHỆ THÔNG TIN**

**BÁO CÁO**

**BÀI TẬP DMZ NETWORK**

**Môn học: Quản trị dịch vụ mạng**

**Lớp: 20\_4**

**Giảng viên hướng dẫn:**

**Lê Hà Minh**

**Người thực hiện:**

**Phan Dương Linh – 20120319**

*2023 – TP.Hồ Chí Minh*

Mục lục

[Thông tin bài tập 3](#_Toc133793985)

[Nội dung báo cáo 4](#_Toc133793986)

[1 Quá trình thực hiện 4](#_Toc133793987)

[1.1 Tải file nén từ portal: 4](#_Toc133793988)

[1.2 Giải nén file 4](#_Toc133793989)

[1.3 Thực hiện chạy file bash shell script 4](#_Toc133793990)

[1.4 Viết script và thực thi 5](#_Toc133793991)

[1.5 Kết quả 5](#_Toc133793992)

[2 Giải pháp – giải thuật sử dụng: 8](#_Toc133793993)

[2.1 Ý tưởng: 8](#_Toc133793994)

[2.2 Giải thích thuật toán: 8](#_Toc133793995)

[Tài liệu tham khảo 9](#_Toc133793996)

# Thông tin bài tập

**Giảng viên hướng dẫn:**

* Lê Hà Minh

**Hệ điều hành: Linux(Ubuntu 18.04)**

**Ngôn ngữ thực hiện:** Bash Shell Script

**Người thực hiện:**

* Phan Dương Linh – 20120319

**Đánh giá mức độ hoàn thành:** 100%

**Nội dung hoàn thành:**

* Hoàn thành yêu cầu đưa ra.
* Viết báo cáo quá trình thực hiện, nêu giải pháp, thuật giải sử dụng trong script.

# Nội dung báo cáo.

## Thiết lập mô hình mạng như sơ đồ, bao gồm 3 networks:

- External network: 192.168.10.0/24

- DMZ network: 192.168.20.0/24

- Internal network: 192.168.30.0/24

A picture containing text, screenshot, diagram, software

Description automatically generated

Sử dụng GNS3 để giả lập mô hình mạng như sơ đồ. Sử dụng các máy ảo để giả lập router và host:

* Router giả lập từ máy ảo Route – Virtual Box Lubuntu 18.04 LTS.
* DMZ-1 giả lập từ máy ảo LTC – Virtual Box Lubuntu 18.04 LTS.
* EXT-1 và INT-1 giả lập từ máy ảo EXT và INT – Vmware Ubuntu 22.04 LTS.

## Thiết lập Router là 1 server Linux, với các interfaces:

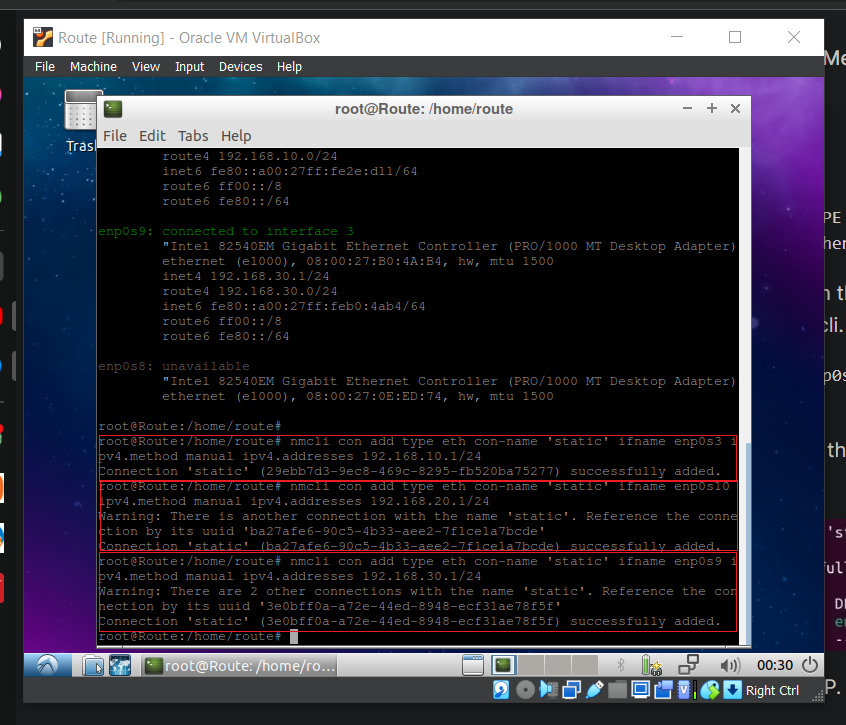
Giả lập router bằng 1 máy ảo Virtual Box có tên là Route chạy Lubuntu 18.04 LTS. Tiến hành thiết lập các Interface:

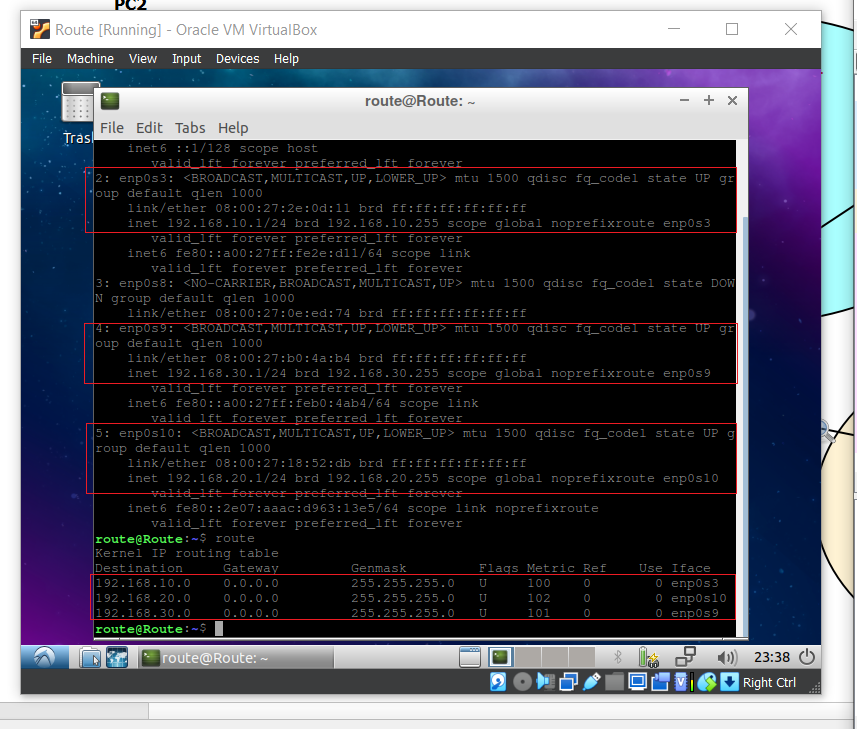
* Interface 1: 192.168.10.1 (tương ứng interface enp0s3)
* Interface 2: 192.168.20.1 (tương ứng interface enp0s10)
* Interface 3: 192.168.30.1 (tương ứng interface enp0s9)
* Cài đặt thiết lập máy ảo với những yêu cầu cơ bản.
* Cài đặt net-tools : *apt install net-tools*

A screenshot of a computer

Description automatically generated

* Cài đặt các interface nối với các network theo yêu cầu.



* Kết quả cấu hình ta có bản route và ip ở các interface như sau:

## Thiết lập cho mỗi network một máy Linux với địa chỉ như sau:

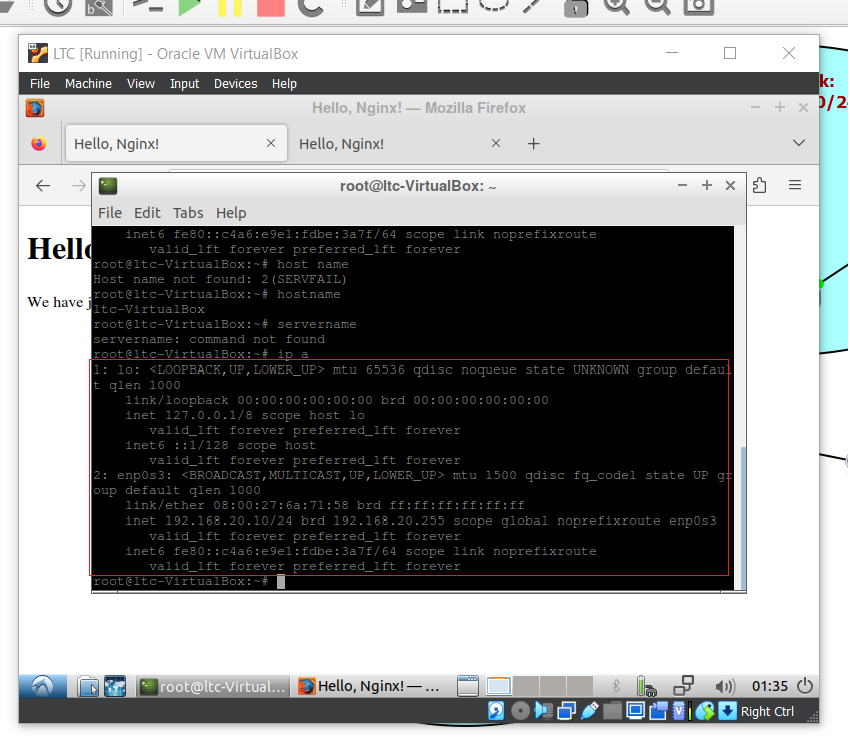
* Client tại External network: 192.168.10.10/24 – Máy ảo EXT.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

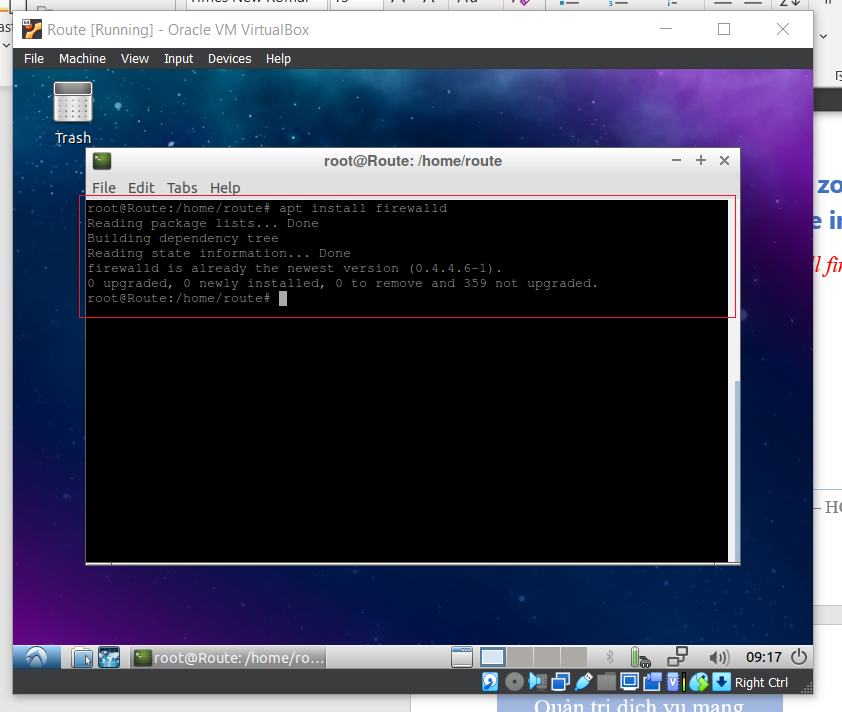
Description automatically generated

* Client tại Internal network: 192.168.30.10/24 – Máy ảo INT.
* Server tại DMZ network: 192.168.20.10/24 – Máy ảo LTC.



## Thiết lập firewalld, zone external cho interface 1, zone dmz cho interface 2, zone internal cho interface 3.

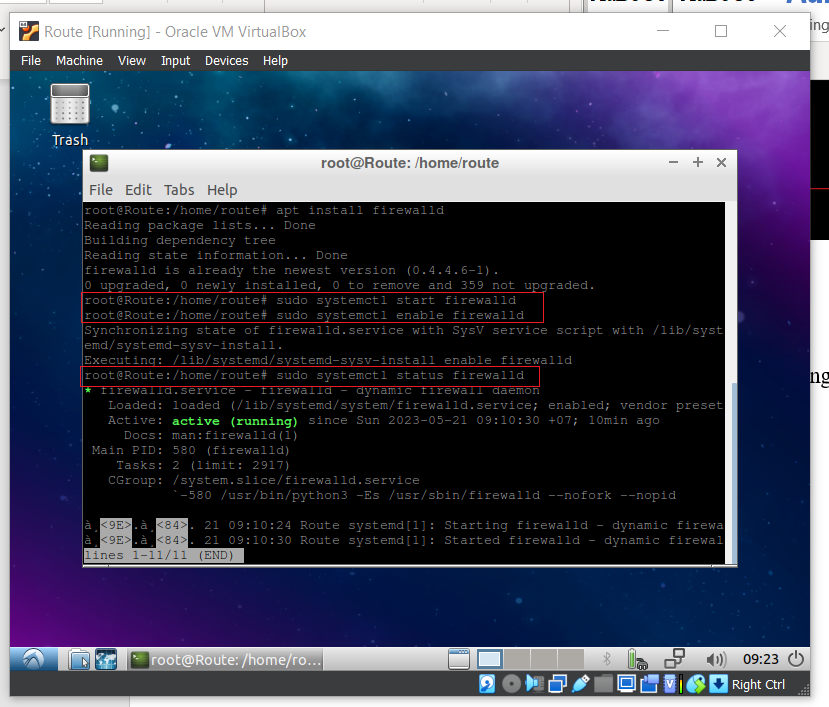
* Cài đặt firewalld: *$ sudo apt install firewalld*



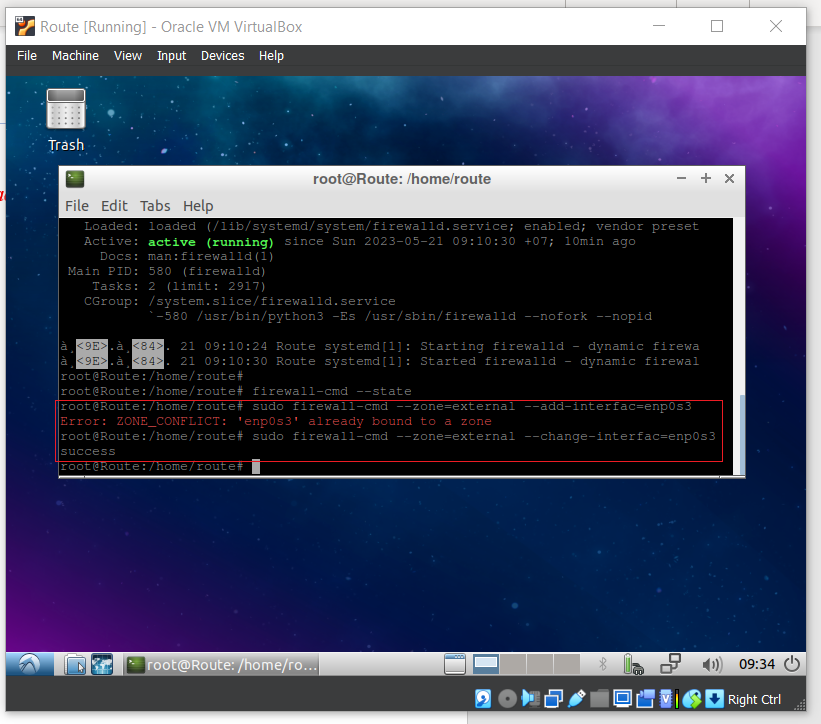
* Khởi động firewalld:

*$ sudo systemctl start firewalld* #Khởi động dịch vụ firewalld

*$ sudo systemctl enable firewalld* #Bật firewalld khi boot hệ thống

*$ sudo systemctl status firewalld* #Kiểm tra trạng thái firewalld

* Đặt Zone external cho interface 1(enp0s3):

*$ sudo firewall-cmd --zone=external --add-interface=enp0s3*

Vì ở đây khi tạo interface, firewall tự tạo zone default cho interface nên khi ta tiến hành thêm zone khiến xung đột xảy ra.

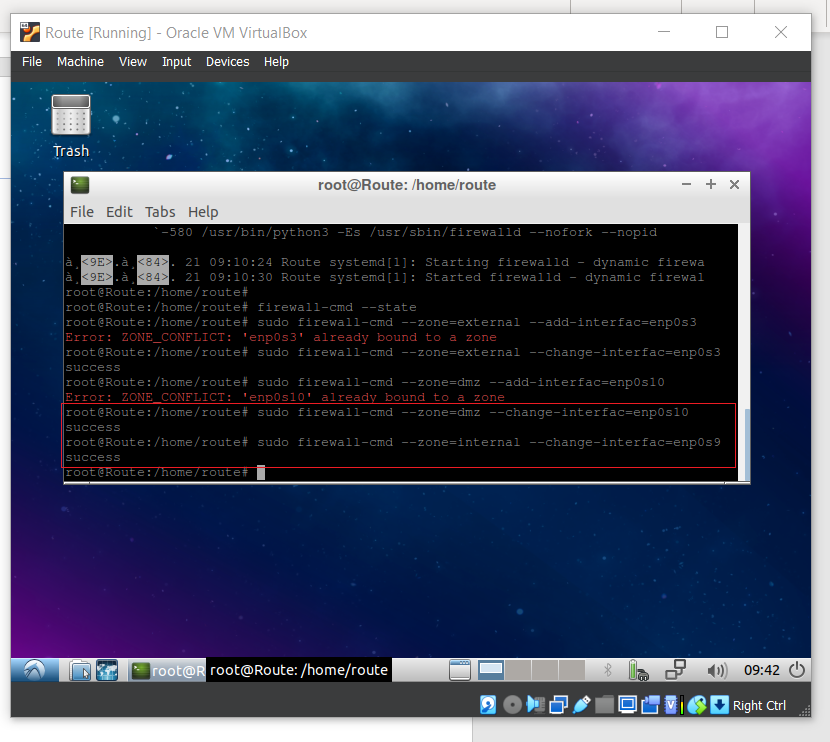
* Cách giải quyết là thay vì thêm chúng ta chuyển zone của interface về thành zone của chúng ta mong muốn. Câu lệnh sẽ là:

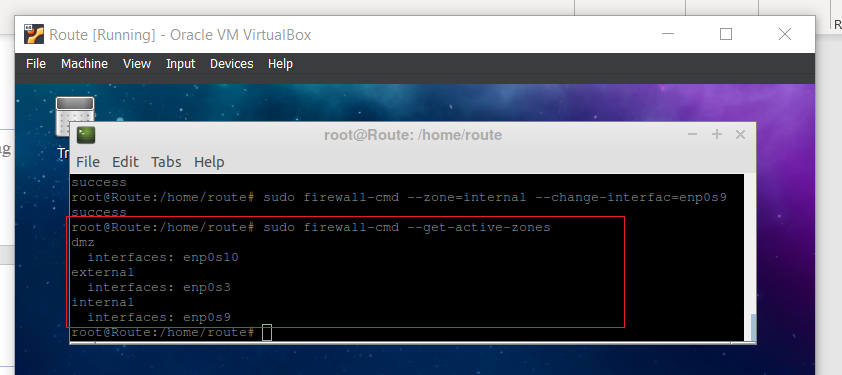
*$ sudo firewall-cmd --zone=external --change-interface=enp0s3*

* Đặt Zone DMZ (inteface 2 – enp0s10) và Zone internal (interface 3 – enp0s9) tương tự như trên các câu lệnh lần lượt sẽ là:

*$ sudo firewall-cmd --zone=dmz --change-interface=enp0s10*

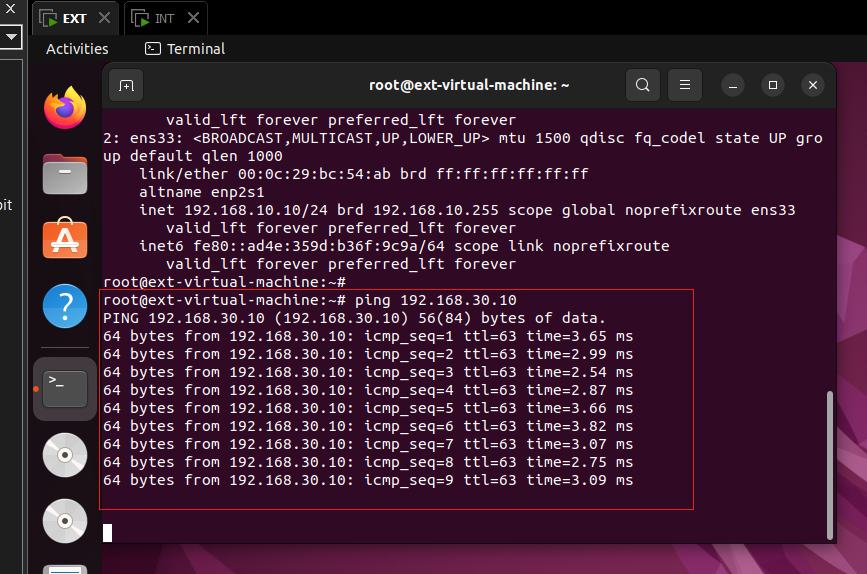
*$ sudo firewall-cmd --zone=internal --change-interface=enp0s9*

* Kết quả sau khi cấu hình*:*

*$ sudo firewall-cmd --get-active-zones*

## Kiểm tra kết nối giữa các máy tính (ping)

External network ping Internal network:



A screenshot of a computer

Description automatically generatedExternal network ping DMZ network:

A screenshot of a computer

Description automatically generatedInternal network ping DMZ network:

## Cấu hình 1 Web server trên server thuộc DMZ network, chỉ cần phục vụ 1 website đơn giản.

Cấu hình Webserver thuộc DMZ network phục vụ website [www.ltc.name](http://www.ltc.name) đơn giản.

A screenshot of a computer

Description automatically generated

## Cấu hình NAT, port forwarding trên router để client tại external network và internal network có thể truy cập website tại DMZ network.

### Cấu hình NAT và port forwarding trên Router:

#### Kích hoạt mô-đun

Tải mô-đun cho NAT bằng lệnh modprobe.

*$ sudo modprobe iptable\_nat*

A computer screen shot of a computer screen

Description automatically generated with low confidence

#### Chuyển tiếp lưu lượng tạm thời

A computer screen shot of a black screen

Description automatically generated with low confidenceĐịnh cấu hình các tham số kernel trong thời gian chạy để chuyển tiếp lưu lượng truy cập Kích hoạt chuyển tiếp bằng cách thêm 1 vào hệ thống tệp tạm thời /proc Sau khi chúng tôi khởi động lại máy chủ, thay đổi này sẽ không khả dụng. Vì vậy, để các thay đổi được duy trì trong suốt quá trình khởi động lại, hãy đảm bảo sử dụng bước tiếp theo.

*# echo 1 > /proc/sys/net/ipv4/ip\_forward*

#### Post routing và forwarding:

Thêm các quy tắc IPtables để thực hiện định tuyến post routing và fowarding lưu lượng truy cập.

*# iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE*

*# iptables -A FORWARD -i enp0s3 -j ACCEPT*

*A screenshot of a computer

Description automatically generated# iptables -A FORWARD -i enp0s9 -j ACCEPT*

### Cấu hình trên External network và Internal network:

*A screenshot of a computer

Description automatically generated*External network (EXT Vmware):

Internal network (INT Vmware):

### Tiến hành cho client tại external truy cập website:

### Tiến hành cho client tại internal truy cập website:

# Tài liệu tham khảo

1. [So sánh chuỗi trong Bash – hocdevops.com](https://hocdevops.com/resources/so-sanh-chuoi-trong-bash/#:~:text=Khi%20so%20s%C3%A1nh%20c%C3%A1c%20chu%E1%BB%97i,v%E1%BB%9Bi%20%5B%5B%20%C4%91%E1%BB%83%20kh%E1%BB%9Bp%20m%E1%BA%ABu.)
2. [HW\_BashShell\_2.docx](https://courses.fit.hcmus.edu.vn/pluginfile.php/190475/mod_assign/introattachment/0/HW_BashShell_2.docx?forcedownload=1) – Lê Hà Minh
3. [06-Bash\_p1.pdf – Nguyễn Thị Minh Tuyền](https://courses.fit.hcmus.edu.vn/pluginfile.php/190473/mod_folder/content/0/06-Bash_p1.pdf?forcedownload=1)