

CHƯƠNG 5: Định danh

Họ tên sinh viên: Phan Thành Đạt

MSSV:20173001

Mã Lớp: 118636

Mã học phần: IT4611

Câu 1:

Hardware Type: Trường này xác định loại mạng mà mạng cục bộ cần để truyền thông điệp ARP. Kích thước của trường này là 16 bit. Ví dụ: Ethernet, IEEE 802 Networks ,...

Protocol Type: Chỉ kiểu giao thức (dài 16 bit). Ví dụ như IPv4

Hardware Length: Trường này chỉ định độ dài của địa chỉ vật lý tính bằng byte. Ví dụ như 6 với Ethernet.

Protocol Length: Kích thước của trường độ dài giao thức (dài 8 bit). Nó xác định độ dài của địa chỉ IP theo byte.

Operation: Dài 16 bit, xác định kiểu gói tin ARP. Có 2 loại là Reply và Request.

Trong bảng là các giá trị cho định dạng khung khác như RARP, DRARP

ARP Message Type	Opcode (Operation Code)
ARP Request	1
ARP Reply	2
RARP Request	3
RARP Reply	4
DRARP Request	5
DRARP Reply	6
DRARP Error	7
InARP Request	8
InARP Reply	9

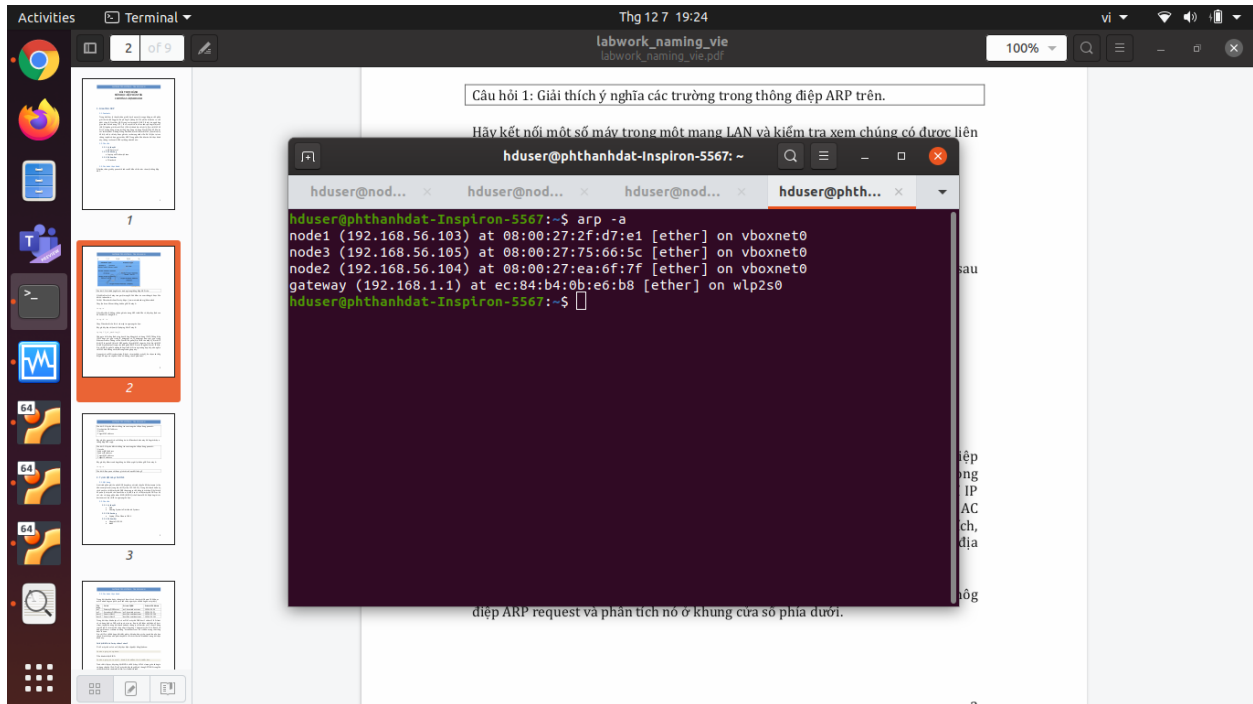
Sender Hardware Address: Trường này chỉ định địa chỉ MAC của người gửi.

Sender Protocol Address: Địa chỉ IP của máy gửi.

Target Hardware Address: MAC của máy nhận, luôn luôn là địa chỉ 00:00:00:00:00:00

Target Protocol Address: Địa chỉ IP của máy cần hỏi.

Câu 2:

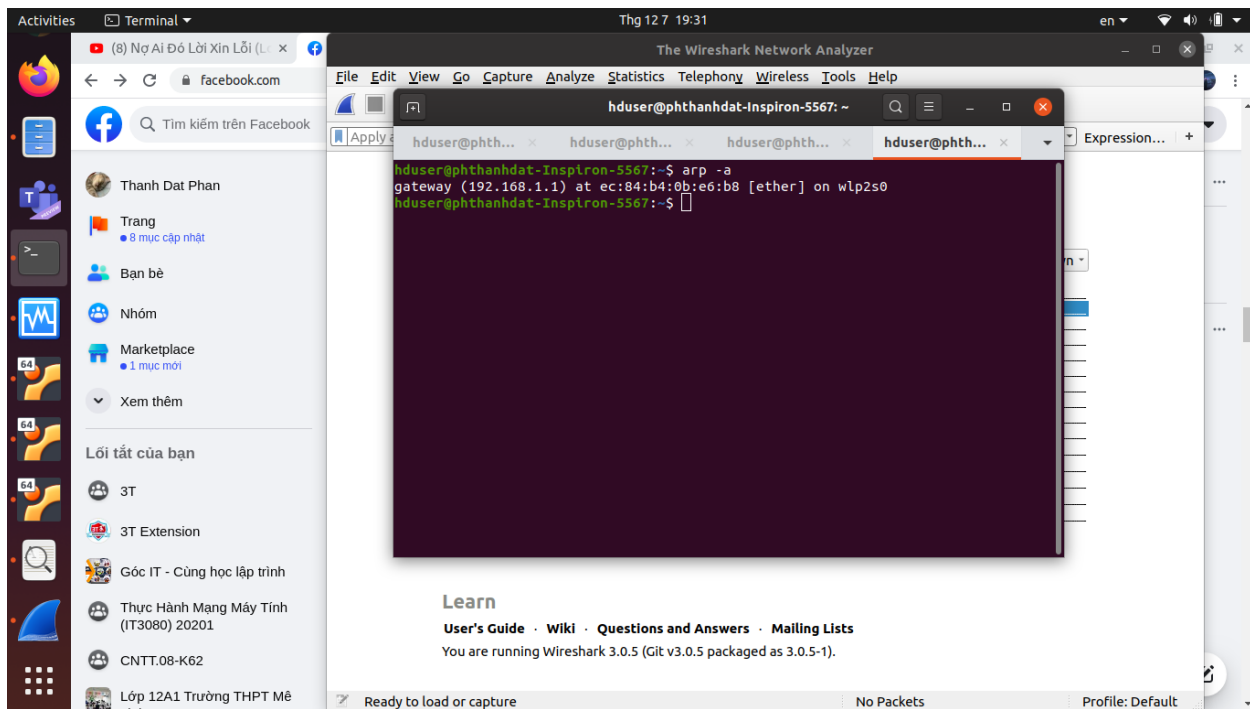


The screenshot shows a Linux desktop with a terminal window open. The terminal displays the output of the command `arp -a`, which lists the ARP table entries. The entries are as follows:

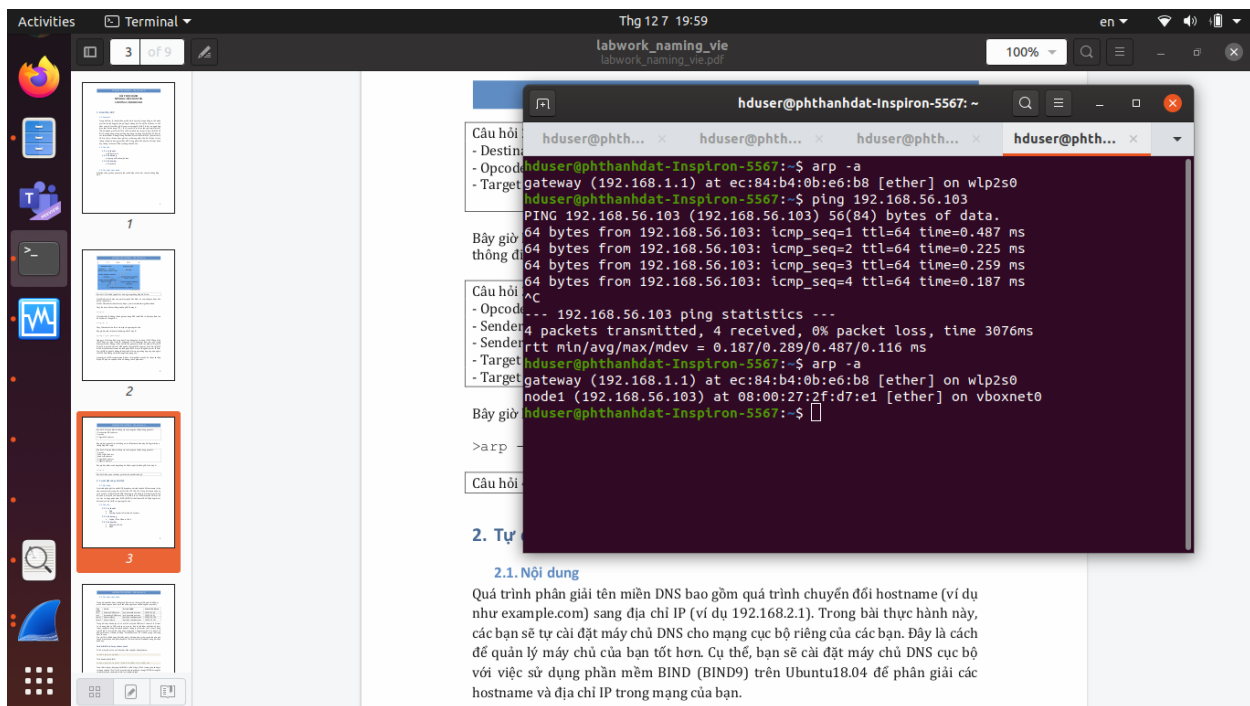
Node Name	IP Address	MAC Address	Interface
node1	192.168.56.103	08:00:27:2f:d7:e1	vboxnet0
node3	192.168.56.105	08:00:27:75:66:5c	vboxnet0
node2	192.168.56.104	08:00:27:ea:6f:7f	vboxnet0
gateway	192.168.1.1	ec:84:b4:0b:e6:b8	wlp2s0

The terminal prompt is `hduser@phthanhdai-Inspiron-5567:~$`. The background shows a web browser window with a labwork document titled "labwork_naming_vie.pdf".

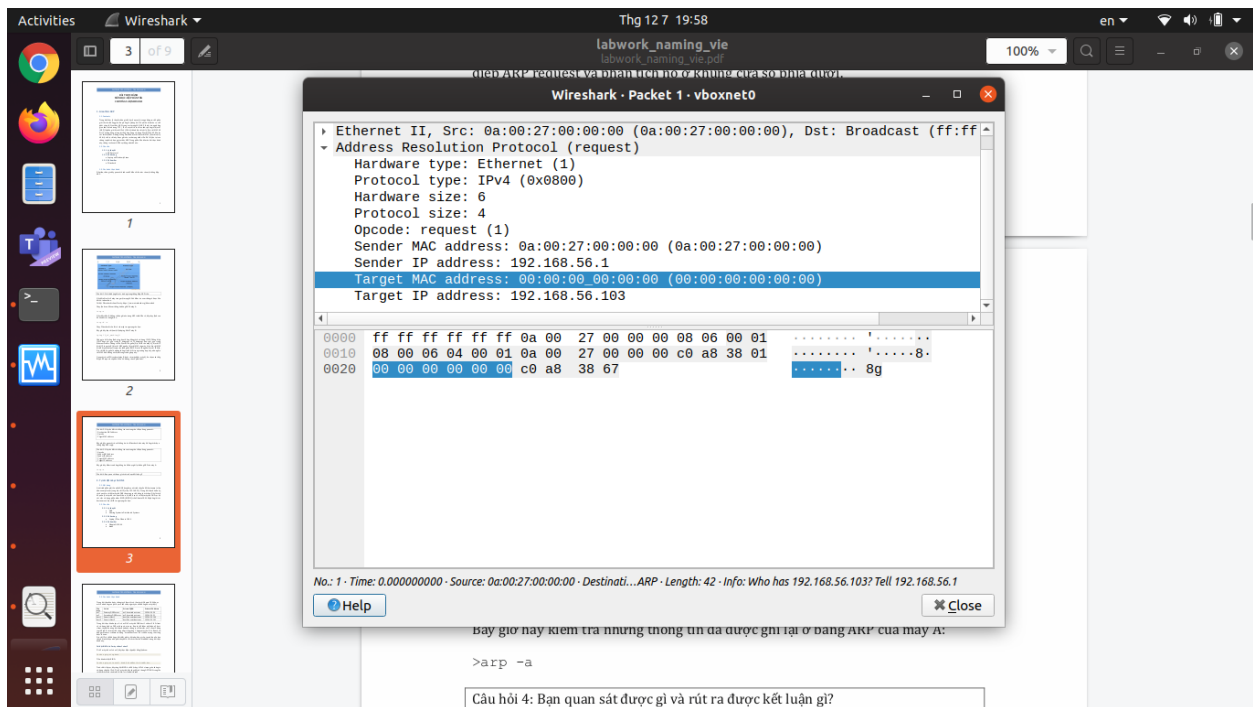
Xóa bảng ARP đi:



Ping và kiểm tra bảng ARP:



Gửi tin trong WireShark:

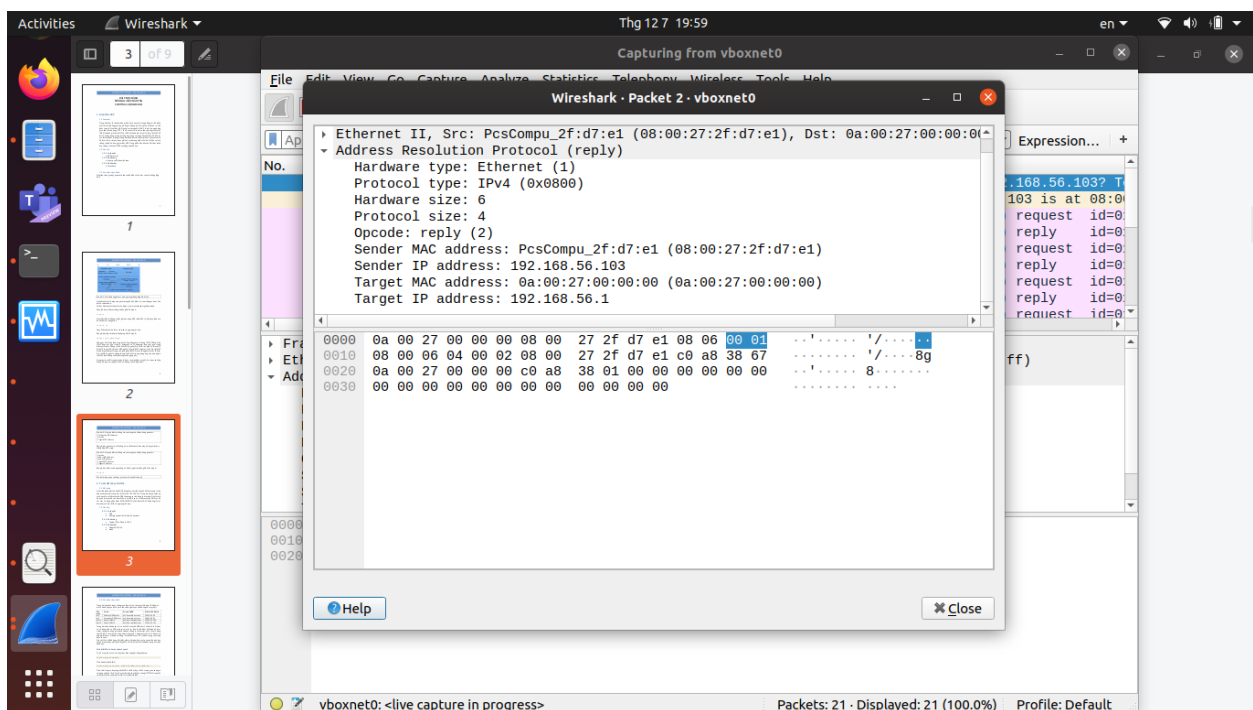


Destination MAC address: Broadcast FF:FF:FF:FF:FF:FF

Opcode : 1 – request

Target MAC address: 00:00:00:00:00:00

Câu 3:



Opcode: 2 – reply

Sender MACaddress: 08:00:27:2f:d7:e1

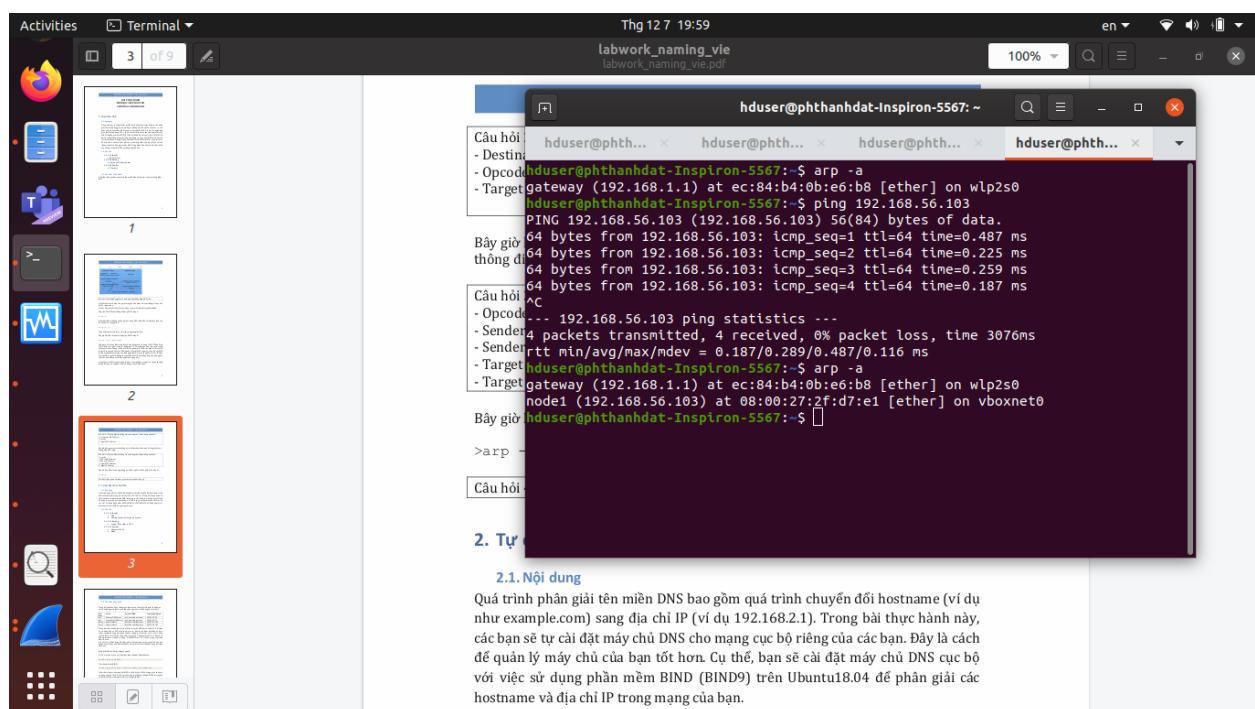
Sender IP address: 192.168.56.103

Target MAC address: 0a:00:27:00:00:00

Target IP address: 192.168.56.1

Câu 4:

Kiểm tra ARP:



```
hduser@phthanhdai-Inspiron-5567:~$ arp -a
gateway (192.168.1.1) at ec:84:b4:0b:e6:b8 [ether] on wlp2s0
hduser@phthanhdai-Inspiron-5567:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=0.487 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.225 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.259 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.187 ms
^C
--- 192.168.56.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt min/avg/max/ndev = 0.187/0.289/0.487/0.116 ms
hduser@phthanhdai-Inspiron-5567:~$ arp -a
gateway (192.168.1.1) at ec:84:b4:0b:e6:b8 [ether] on wlp2s0
node1 (192.168.56.103) at 08:00:27:2f:d7:e1 [ether] on vboxnet0
hduser@phthanhdai-Inspiron-5567:~$
```

Quan sát được địa chỉ MAC của máy 192.168.56.103 (máy vừa được ping) đã có trong bảng ARP table của máy 192.168.56.1 (máy host).

⇒ Máy Host đã lưu giá trị địa chỉ MAC của máy 192.168.56.103 vào table để lần sau không phải thực hiện lại giao thức ARP nữa.

Câu 5:

Vai trò của block *forwarders* là để khi máy DNS 1 không phân giải được tên miền của client gửi đến, sẽ gửi request đó đến địa chỉ trong block này, cụ thể ở đây là 8.8.8.8 và 8.8.4.4 rồi lấy kết quả trả lại cho client.

Câu 6:

Tìm kiếm forward: Máy chủ sẽ không trả lời request của client mà gửi request đến máy chủ DNS khác rồi lấy kết quả trả lời cho client (phân giải đệ quy).

Tìm kiếm reverse: phân giải ngược từ địa chỉ IP ra tên domain.

Câu 7:

2 tệp db.ds.soict.hust.com và db.192.168.56 (bài của em là 192.168.56.0/24) là 2 file chứa tên các domain (cụ thể là db.ds.soict.hust.com) và địa chỉ IP (cụ thể là db.192.168.56) có khả năng phân giải, 2 file này sẽ chứa nội dung phân giải để trả lời cho client.

Câu 8:

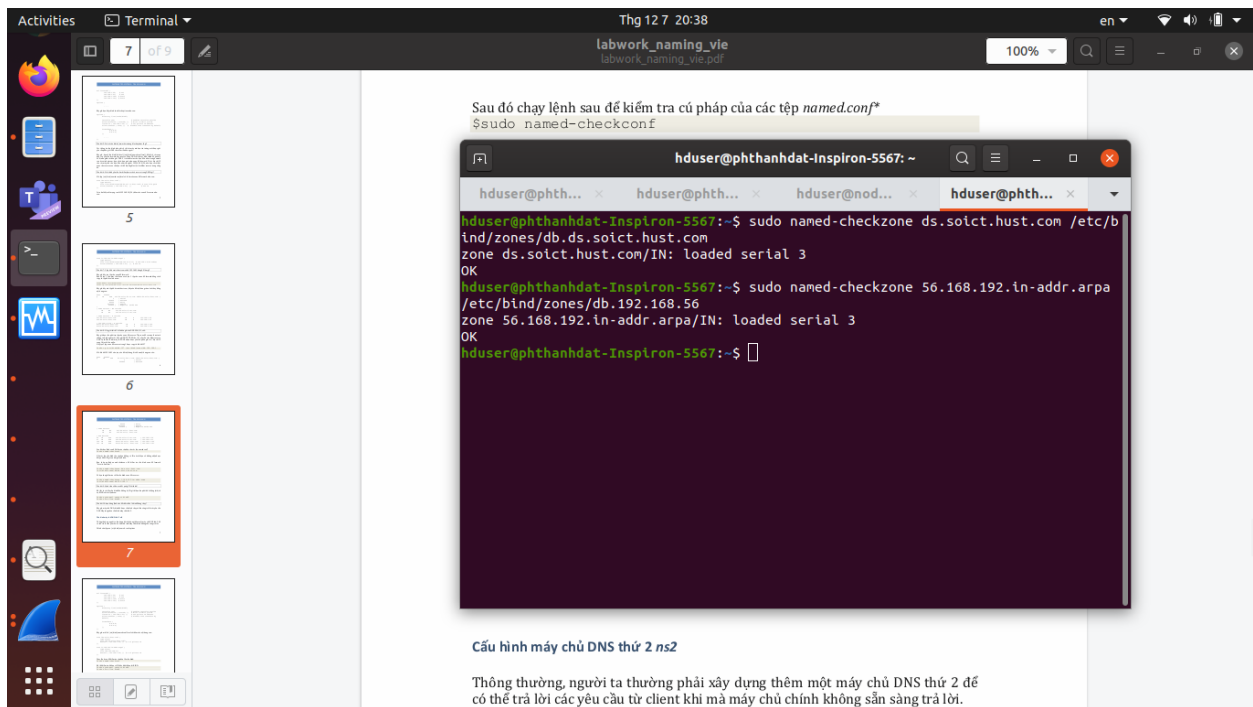
NS (Name Server): là 1 record chứa địa chỉ IP của DNS Server và những thông tin về domain đó.

SOA: là một thành phần duy nhất tồn tại trong mỗi tập tin cơ sở dữ liệu DNS gồm những thông tin về zone transfer và những thông tin về domain trên DNS Server.

A: dùng để phân giải Host ra một địa chỉ 32-bit IPv4.

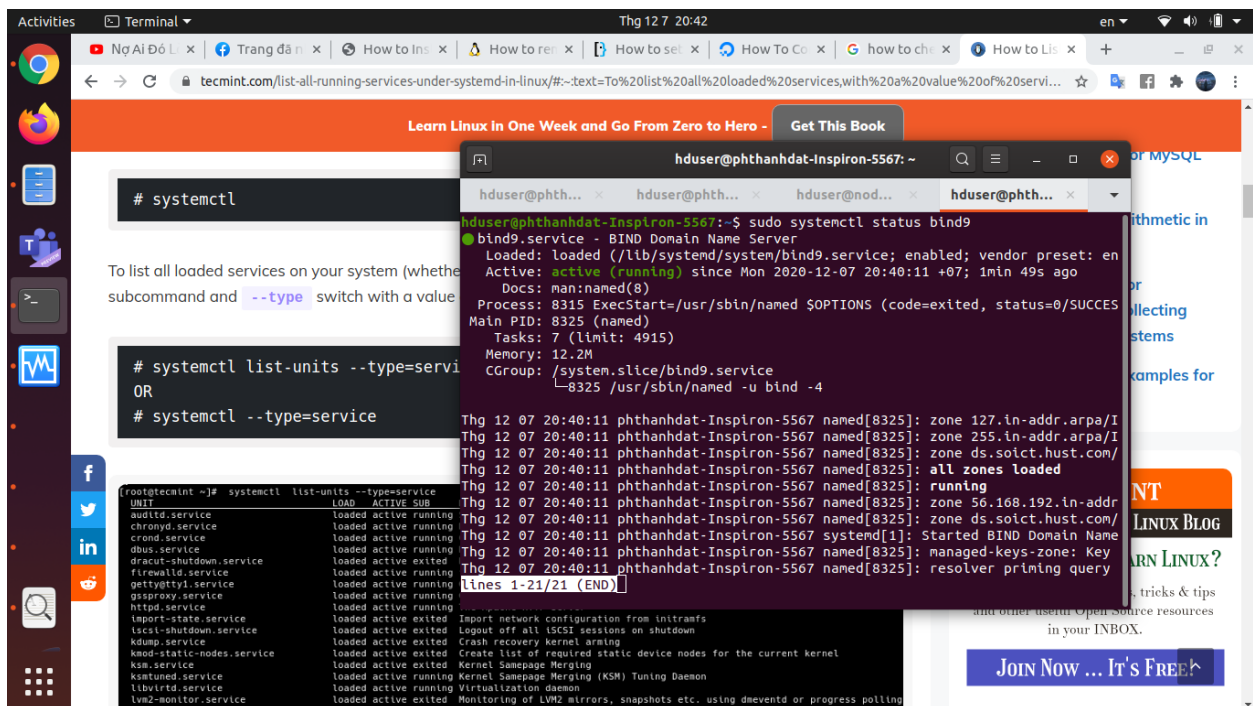
Câu 9:

Lệnh trên đưa ra kết quả OK, nghĩa là các cú pháp cấu hình trong 2 file /etc/bind/zones/db.ds.soict.hust.com và /etc/bind/zones/db.192.168.1 không có lỗi.



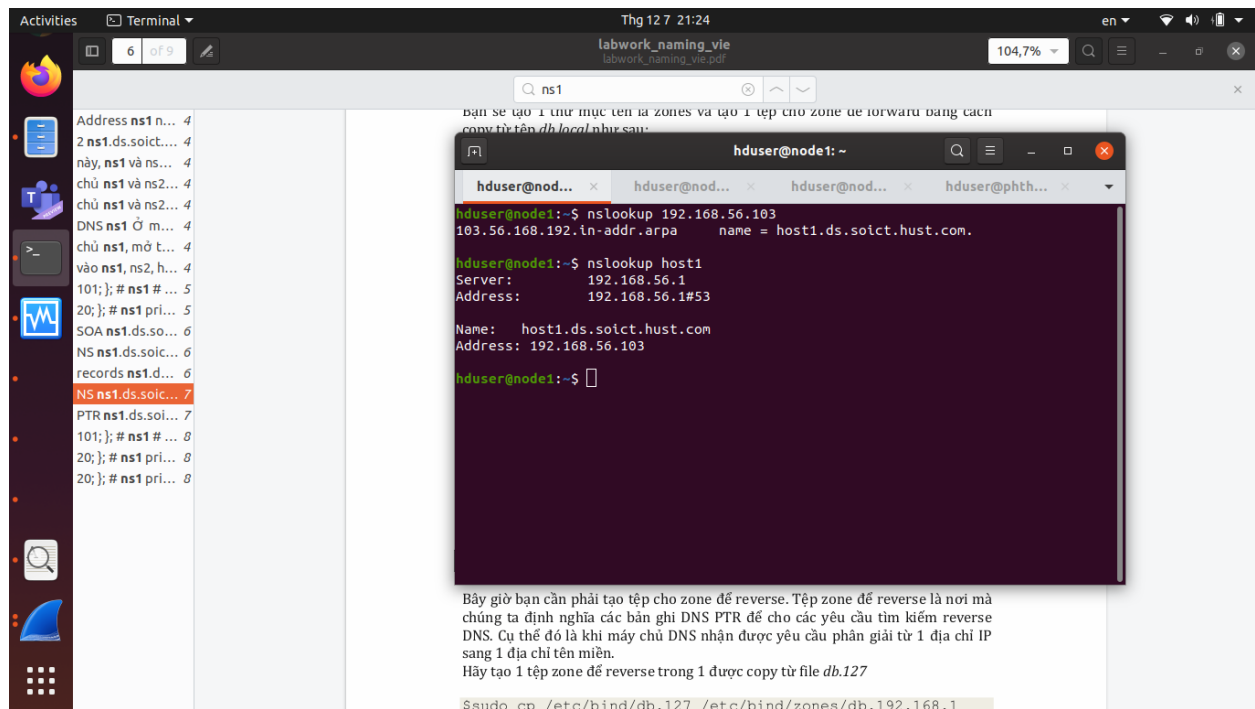
Câu 10:

sudo systemctl status bind9 để check trạng thái



Câu 11:

Nhận được kết quả địa chỉ IP của domain host1, thông tin server DNS.



Cơ chế hoạt động:

Thứ nhất, ở file `/etc/resolv.conf` chúng ta đã cấu hình địa chỉ IP của 2 DNS Server và search đã ghi : `ds.soict.hust.com` nên khi truy vấn chỉ cần gõ tên `host1` hoặc `host2` chứ không cần `host1.ds.soict.hust.com`. Khi gửi truy vấn về 1 domain nào đó, máy sẽ gửi gói tin DNS request đến server đầu tiên trong file `/etc/resolv.conf`: `192.168.56.1`, nếu server hoạt động bình thường thì lấy kết quả trong file `db.ds.soict.hust.com` sẽ trả lại kết quả là địa chỉ IP và thông tin server, nếu server lỗi, máy host đợi một thời gian không có response thì sẽ gửi đến server backup thứ 2 trong file là server `192.168.56.105`.

Câu 12:

Ta sẽ nhận được domain của 2 địa chỉ IP đó và tương tự là host sẽ gửi request lên DNS Server, Server sẽ tìm thông tin trong file `db.56.168.192` và trả lời

Câu 13:

Các bước lần lượt để cấu hình :

1. Tải bind9 về bằng câu lệnh : `sudo apt-get install bind9 bind9utils bind9-doc`
2. Thay đổi nội dung OPTIONS trong file cài đặt mặc định của bind9 là file: `/etc/default/bind9` để thiết lập phân giải IPv4 hoặc giữ nguyên nếu là IPv6
3. chỉnh sửa: `/etc/bind/named.conf.options` , thêm block acl là địa chỉ IP của các máy có quyền truy vấn DNS hoặc bỏ qua nếu cho phép mọi máy tính đều có quyền truy vấn.

4. Chỉnh sửa block options trong file `/etc/bind/named.conf.options` một số thông tin như địa chỉ IP lắng nghe truy vấn, cho phép truy vấn đệ quy, địa chỉ IP forward nếu như máy không có khả năng phân giải tên miền...
5. Chỉnh sửa file `named.conf.local` để cài đặt loại DNS là master hay slaves, chỉnh sửa đường dẫn đến thông tin của các domain và các IP (phân giải ngược) mà máy có thể truy vấn
6. Sửa các file chứa thông tin mà đã thêm ở trên vào file `conf.local`
7. Chạy dịch vụ DNS bằng lệnh : `sudo systemctl start bind9`