

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN**



BÁO CÁO ĐỒ ÁN MÔN HỌC MẠNG MÁY TÍNH Wireshark

Giảng viên lý thuyết: Thầy Đỗ Hoàng Cường
Giảng viên hướng dẫn thực hành:

- Thầy Lê Hà Minh
- Thầy Nguyễn Thanh Quân

Lớp: 20TN

Thành viên thực hiện:

- 20120131 – Nguyễn Văn Lộc
- 20120536 – Võ Trọng Nghĩa
- 20120572 – Nguyễn Kiều Minh Tâm

THÀNH PHỐ HỒ CHÍ MINH, THÁNG 4 NĂM 2022

Mục lục

1	Thông tin của nhóm	2
2	Mức độ hoàn thành	2
3	Bài 1: Ping	3

Danh sách hình vẽ

1	Nội dung tập tin <i>ping.pcapng</i>	3
2	Địa chỉ IP của host ping và host được ping	3
3	Độ dài Ethernet header	4
4	Độ dài IP header	4
5	Độ dài ICMP data và ICMP header	5
6	Sơ đồ mạng	5

Danh sách bảng

1	Bảng phân công thành viên	2
---	-------------------------------------	---

1 Thông tin của nhóm

MSSV	Họ và tên	Công việc
20120131	Nguyễn Văn Lộc	Bài 1 + 2
20120536	Võ Trọng Nghĩa	Bài 4 + L ^A T _E X
20120572	Nguyễn Kiều Minh Tâm	Bài 3 + 5

Bảng 1: Bảng phân công thành viên

2 Mức độ hoàn thành

3 Bài 1: Ping

Mở *ping.pcapng* file, nội dung của file pcap là thông tin các gói tin gửi từ một máy sang một máy khác bằng lệnh ping.

Nội dung tập tin *ping.pcapng* như sau.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	IntelCor_3c:ac:58	Broadcast	ARP	42	who has 192.168.0.1? Tell 192.168.0.105
2	0.001828232	Tp-LinkT_fc:53:7e	IntelCor_3c:ac:58	ARP	42	192.168.0.1 is at 18:d6:c7:fc:53:7e
3	0.001835170	192.168.0.105	192.168.1.1	ICMP	98	Echo (ping) request id=0x000d, seq=1/256, ttl=64 (reply in 4)
4	0.004770309	192.168.1.1	192.168.0.105	ICMP	98	Echo (ping) reply id=0x000d, seq=1/256, ttl=63 (request in 3)

Hình 1: Nội dung tập tin *ping.pcapng*

Trả lời các câu hỏi sau:

1. Cho biết địa chỉ IP của host ping và host được ping?

Địa chỉ IP của host ping: 192.168.0.105

Địa chỉ IP của host được ping: 192.168.1.1

```

Protocol: ICMP (1)
Header Checksum: 0x3cec [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.105
Destination Address: 192.168.1.1
    
```

Hình 2: Địa chỉ IP của host ping và host được ping

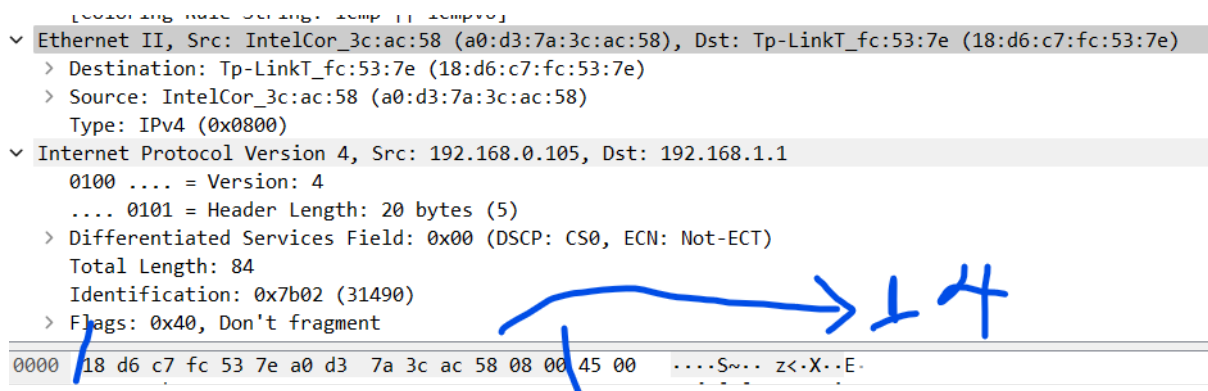
2. Cho biết port được sử dụng là bao nhiêu? Nếu không có port thì giải thích tại sao?

Không có port được sử dụng.

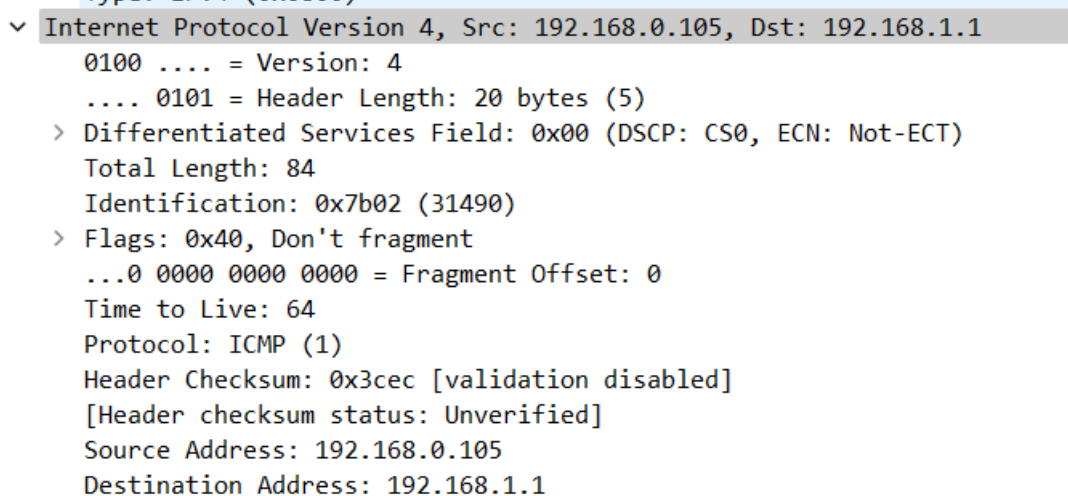
Lý do: Lệnh ping sử dụng giao thức **ICMP** của mô hình TCP/IP. ICMP là giao thức ở tầng, còn port number được sử dụng ở tầng Application.

3. Với gói tin ICMP request, cho biết kích thước (bytes) của từng phần trong diagram. (Chú ý: Kích thước tổng của gói tin là 98 bytes)

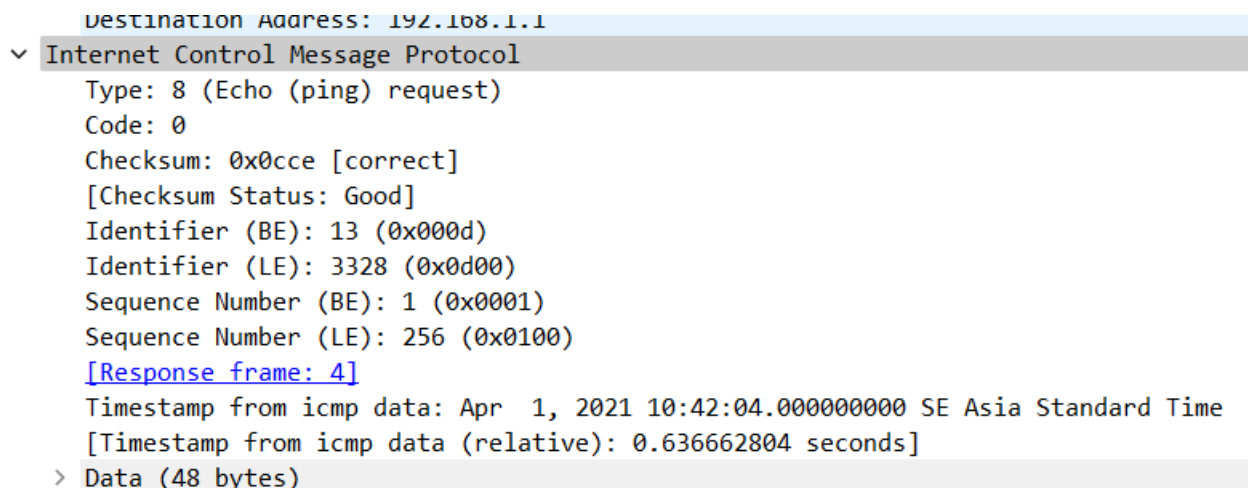
ICMP data	ICMP header	IP header	Ethernet header
48	16	20	14



Hình 3: Độ dài Ethernet header



Hình 4: Độ dài IP header



Hình 5: Độ dài ICMP data và ICMP header

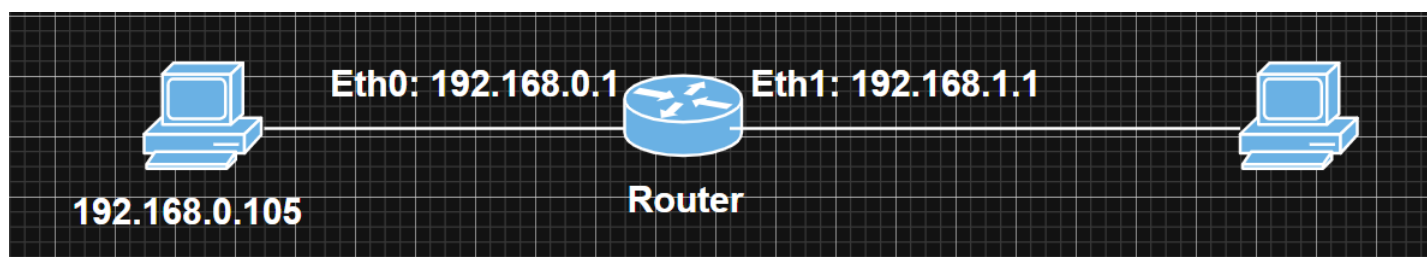
4. Tại sao lại có 2 gói ARP?

ARP (viết tắt của cụm từ Address Resolution Protocol) là giao thức mạng được dùng để tìm ra địa chỉ phần cứng (địa chỉ MAC) của thiết bị từ một địa chỉ IP nguồn. Nó được sử dụng khi một thiết bị giao tiếp với các thiết bị khác dựa trên nền tảng local network.

Khi ta sử dụng lệnh ping, host ping (192.168.0.105) thực hiện broadcast gói tin ARP request vào tất cả các host trong mạng LAN xem host nào có địa chỉ là 192.168.1.1 (host được ping). Host được ping sẽ gửi lại gói tin ARP reply, xác định địa chỉ MAC cần tìm (18:d6:c7:fc:53:7e) cho host ping.

5. Hãy vẽ sơ đồ mạng logic dựa trên nội dung gói pcap đó.

Sơ đồ mạng logic dựa trên nội dung gói pcap trong bài như sau.



Hình 6: Sơ đồ mạng