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:

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

THÀNH PHỐ HỒ CHÍ MINH, THÁNG 4 NĂM 2022

Mục lục

1	Thô	ong tin của nhóm	2					
2	Mức độ hoàn thành							
3	Bài	1: Ping	3					
4	Bài	2: HTTP	6					
Danh sách hình vẽ								
	1	Nội dung tập tin <i>ping.pcapng</i>	3					
	2	Dia 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					
	7	Kết quả bắt gói tin từ lúc bắt đầu DNS đến lúc gửi HTTP request	6					
	8	IP của host	6					
\mathbf{D}	anl	n 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 + LATEX
20120572	Nguyễn Kiều Minh Tâm	Bài $3+5$

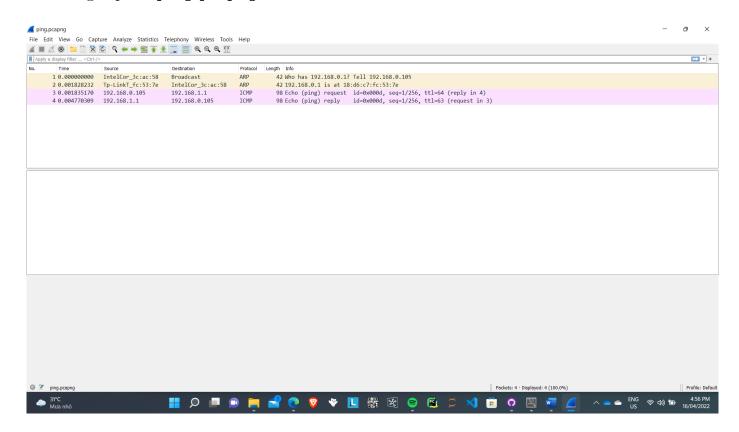
Bảng 1: Bảng phân công thành viên

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.



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. ICHE (I)

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 tai sao?

Không có source port number và destination port number.

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

```
Ethernet II, Src: IntelCor_3c:ac:58 (a0:d3:7a:3c:ac:58), Dst: Tp-LinkT_fc:53:7e (18:d6:c7:fc:53:7e)

> Destination: Tp-LinkT_fc:53:7e (18:d6:c7:fc:53:7e)

> Source: IntelCor_3c:ac:58 (a0:d3:7a:3c:ac:58)
    Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.1.1
    0100 ... = Version: 4
    ... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x7b02 (31490)

> Flags: 0x40, Don't fragment

0000 18 d6 c7 fc 53 7e a0 d3 7a 3c ac 58 08 00 45 00 ....S~.. z<.X..E-</pre>
```

Hình 3: Độ dài Ethernet header

```
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x7b02 (31490)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    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 4: Đô dài IP header

```
Vestination Address: 192.108.1.1

V Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x0cce [correct]
    [Checksum Status: Good]
    Identifier (BE): 13 (0x000d)
    Identifier (LE): 3328 (0x0d00)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 4]
    Timestamp from icmp data: Apr 1, 2021 10:42:04.000000000 SE Asia Standard Time
    [Timestamp from icmp data (relative): 0.636662804 seconds]
    Data (48 bytes)
```

Hình 5: Đô dài ICMP data và ICMP header

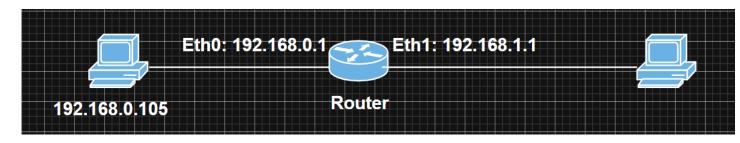
4. Tại sao lại có 2 gói ARP?

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 p
cap trong bài như sau.



Hình 6: Sơ đồ mạng

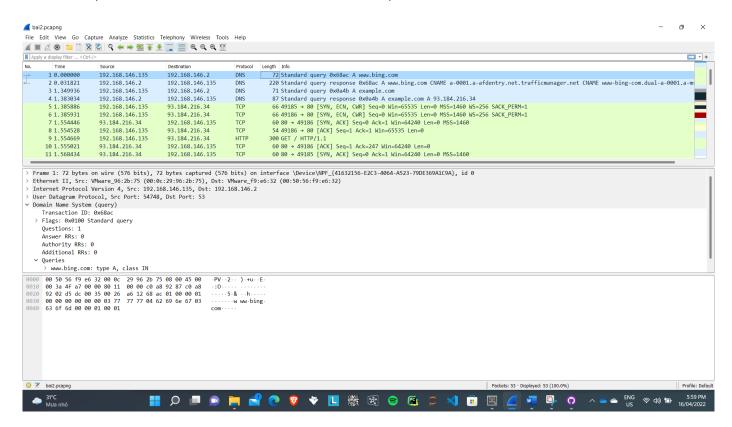
4 Bài 2: HTTP

Xóa cache browser trước khi truy cập trang web hoặc dùng ẩn danh. Dùng Wireshark để bắt gói tin khi truy cập vào website: http://example.com.

Việc bắt gói tin bằng Wireshark trong bài được thực hiện bằng **máy ảo**, sử dụng hệ điều hành **Windows Server 2012 R2**.

Kết quả bắt gói tin chi tiết được lưu trong tập tin bai2.pcapng.

1. Chụp hình kết quả bắt gói tin từ lúc bắt đầu DNS đến lúc gửi HTTP request (thấy được những gói tin liên quan).



Hình 7: Kết quả bắt gói tin từ lúc bắt đầu DNS đến lúc gửi HTTP request

2. Cho biết IP của host.

IP của host là: 93.184.216.34.

```
> Frame 4: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF {41632156-E2C3-4064-A523-79DE369A1C9A}, id 0
  Ethernet II, Src: VMware_f9:e6:32 (00:50:56:f9:e6:32), Dst: VMware_96:2b:75 (00:0c:29:96:2b:75)
  Internet Protocol Version 4, Src: 192.168.146.2, Dst: 192.168.146.135
  User Datagram Protocol, Src Port: 53, Dst Port: 61205

→ Domain Name System (response)

     Transaction ID: 0x0a4b
   > Flags: 0x8180 Standard query response, No error
     Questions: 1
     Answer RRs: 1
     Authority RRs: 0
     Additional RRs: 0

√ Oueries

      > example.com: type A, class IN
    Answers
      > example.com: type A, class IN
                                       addr 93.184.216.34
     [Time: 0.033098000 seconds]
```

Hình 8: IP của host

3. Cho biết IP của router (default gateway) (nếu không thấy được thì trả lời không có và giải thích tại sao)