Bài tập thực hành Wireshark

MSSV: 18120254 Họ và tên: Nguyễn Huy Tú Lớp: 18_2

Lưu ý:

- Bài tập cá nhân.
- Sinh viên làm bài trên đề bài sau.
- Cần chụp hình và ghi chú rõ ràng cho các câu trả lời.
- Nộp bài với file MSSV_BTTH02.zip, bao gồm file báo cáo MSSV_BTTH02.pdf và các files lưu thông tin các gói tin được bắt bởi Wireshark MSSV_DHCP.pcap (câu 3), MSSV_ICMP.pcap (câu 4).
- Các bài làm giống nhau sẽ nhận điểm 0.
- Chỉ nhận bài tập tại phần nộp bài của Website môn học, không nhận bài theo hình thức khác.

Câu 1: Cho tập tin **FTP_01.cap**, đọc tập tin này bằng Wireshark và trả lời các câu hỏi sau:

a. Username và password của người dùng là gì?

Username: 07cm, password: 654321.

6 4.932741	10.0.0.1	10.0.0.123	FTP	65 Request: USER 07cm
9 8.403728	10.0.0.1	10.0.0.123	FTP	67 Request: PASS 654321

b. Địa chỉ IP máy Client và máy Server là gì?

IP Client: 10.0.0.1/8, IP Server: 10.0.0.123/8

Source	Destination
10.0.0.1	10.0.0.123

c. Client truy xuất lên Server theo mode nào: active hay passive?

Client truy xuất trên Server theo mode active.

Vì client connect tới port command trên server là port 21. Sau đó Client sẽ lắng nghe và gửi command port tới server. FTP server sẽ connect tới Client bằng data port mặt định của nó là port 20.

d. Port truyền dữ liệu của FTP Server và Client là bao nhiêu?

Port dữ liệu:

- Port truyền dữ liệu của FTP Server: 20.
- Port truyền dữ liệu của Client: 49733.

```
Src Port: 20, Dst Port: 49733,
```

Port lệnh:

- Port truyền lệnh của FTP Server: 21.
- Port truyền lệnh của Client: 49728.

```
Src Port: 49728, Dst Port: 21,
```

Câu 2: Cho tập tin **FTP_02.cap**, đọc tập tin này bằng Wireshark và trả lời các câu hỏi sau:

a. *FTP sử dụng giao thức nào UDP hay TCP?*

FTP sử dụng giao thức TCP.

```
Protocol
TCP
TCP
```

```
Transmission Control Protocol, Src Port: 49788, Dst Port: 21, Seq: 1, Ack: 1, Len: 0
```

b. *Port mặc định của FTP Server để nhận kết nối là bao nhiêu?*

Port mặc định của FTP Server để nhận kết nối nối là port 21. `Dst Port: 21,`

c. *Username và password của người dùng là gì?*

Usermame: cm07, password: 123654.

```
Request: USER cm07
```

```
Request: PASS 123654
```

d. *Port truyền lệnh của Client là bao nhiêu?*

Port truyền lệnh của Client là port 49788.

```
Src Port: 49788,
```

e. *Client truy xuất lên Server theo mode nào: active hay passive?*

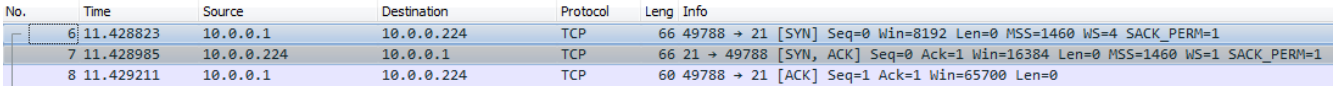
Client truy xuất trên Server theo mode passive.

Vì FTP Client khởi tạo 2 connections đến Server. Client mở 2 ports, port đầu tiên Client mở connect tới port 21 của Server. Sau đó, Client sẽ gửi câu lệnh PASV command. Lúc đó Server sẽ khởi tạo random unprivileged port. Lúc này Client khởi tạo connection giữa 2 port đó và transfer data.

```
10.0.0.1          10.0.0.224          FTP          60 Request: PASV
```

f. *Chỉ ra quá trình bắt tay 3 bước của Client và Server để tạo kết nối ban đầu khi thực hiện truyền username và password.*

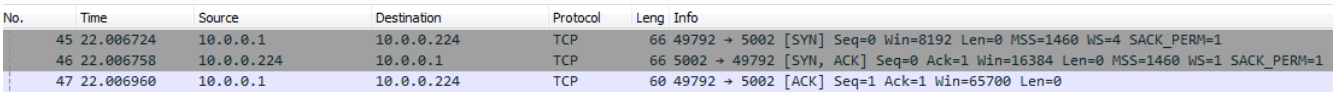
Client gửi gói tin có SYN (seq=0), Server sẽ gửi lại SYN, ACK (seq=0, ACK=1). Sau đó, client gửi gói ACK (seq=1, ACK=1).



No.	Time	Source	Destination	Protocol	Leng	Info
6	11.428823	10.0.0.1	10.0.0.224	TCP	66	49788 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
7	11.428985	10.0.0.224	10.0.0.1	TCP	66	21 → 49788 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
8	11.429211	10.0.0.1	10.0.0.224	TCP	60	49788 → 21 [ACK] Seq=1 Ack=1 Win=65700 Len=0

g. *Chỉ ra quá trình bắt tay 3 bước của Client và Server để tạo kết nối truyền dữ liệu.*

Client gửi gói tin có SYN (seq=0), Server sẽ gửi lại SYN, ACK (seq=0, ACK=1). Sau đó, client gửi gói ACK (seq=1, ACK=1).



No.	Time	Source	Destination	Protocol	Leng	Info
45	22.006724	10.0.0.1	10.0.0.224	TCP	66	49792 → 5002 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
46	22.006758	10.0.0.224	10.0.0.1	TCP	66	5002 → 49792 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
47	22.006960	10.0.0.1	10.0.0.224	TCP	60	49792 → 5002 [ACK] Seq=1 Ack=1 Win=65700 Len=0

h. *Port truyền dữ liệu của FTP Server và Client là bao nhiêu?*

Port dữ liệu:

- Port truyền dữ liệu của FTP Server: 5002.
- Port truyền dữ liệu của Client: 49792.

```
Src Port: 49792, Dst Port: 5002,
```

Port lệnh:

- Port truyền lệnh của FTP Server: 21.
- Port truyền lệnh của Client: 49788.

```
Src Port: 21, Dst Port: 49788,
```

Câu 3: Cấu hình dịch vụ DHCP với các thông tin sau:

a. *Sử dụng máy ảo MS Windows Server 2003/2008/2012 để làm DHCP server. Thiết lập card mạng của máy ảo là Host-Only.*

b. *Cấu hình địa chỉ IP tĩnh cho máy làm DHCP server này là: 192.168.54.2/24.*

c. *Khoảng địa chỉ IP cấp cho các clients là: 192.168.54.20/24 – 192.168.54.200/24*

d. *Khoảng địa chỉ IP không được cấp tự động (exclusion): 192.168.54.50/24 – 192.168.54.70/24*

e. *Default gateway cung cấp cho các clients: 192.168.54.1*

f. *DNS server cung cấp cho các clients: 192.168.54.3*

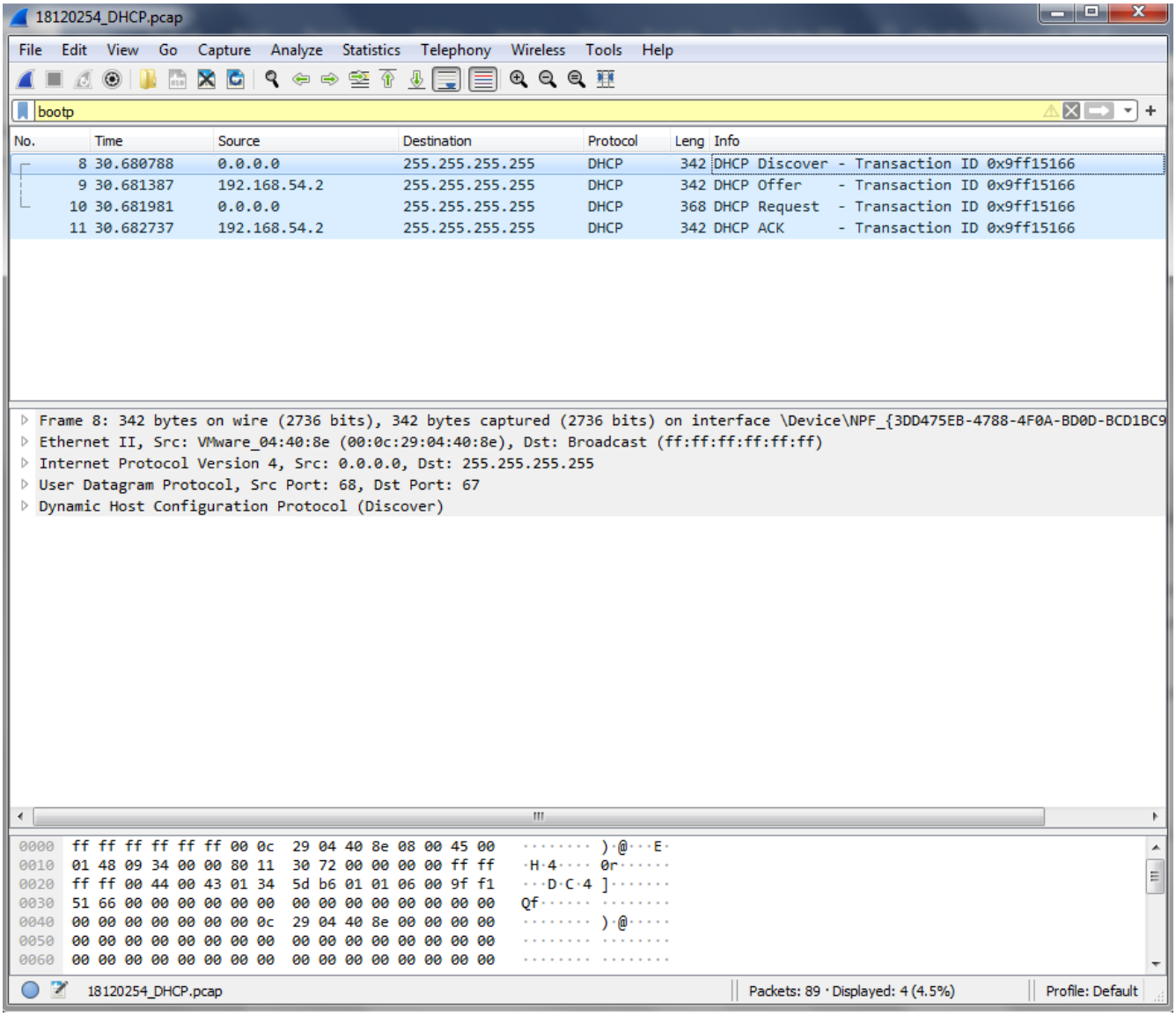
g. *Cấu hình một máy ảo khác (ví dụ: Windows 7, Windows Server 2003…) làm DHCP client. Thiết lập card mạng của máy ảo này là Host-Only.*

h. *Tắt tính năng DHCP của phần mềm VMWare (Trên VMWare Player/Workstation > Chọn menu Edit > Virtual Network Editor > Chọn card mạng VMNet1 > Bỏ chọn "Use local DHCP service to distribute IP addresses to VMs).*

i. *Thực hiện xin cấp phát địa chỉ IP từ client đến DHCP server và dùng Wireshark để bắt gói tin của quá trình này.*

j. *Cho biết có bao nhiêu gói tin được truyền và nhận trong quá trình cấp phát địa chỉ IP?*

Có 4 gói tin được truyền và nhận trong quá trình cấp phát địa chỉ IP.



k. *Gồm những gói tin nào, giải thích mục đích của mỗi gói? Với mỗi gói cho biết: IP nguồn, IP đích, MAC nguồn, MAC đích, Port nguồn, Port đích?*

4 gói tin bao gồm: DHCP Discover, DHCP Offer, DHCP Request, DHCP ACK.

DHCP Discover: là một gói được gửi đến DHCP server từ một thiết bị Client khi muốn truy cập mạng để yêu cầu thông tin địa chỉ IP.

- IP nguồn: 0.0.0.0
- IP đích: 255.255.255.255
- MAC nguồn: 00:0c:29:04:40:8e
- MAC đích: ff:ff:ff:ff:ff:ff
- Port nguồn: 68
- Port đích: 67

```
Frame 8: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: VMware_04:40:8e (00:0c:29:04:40:8e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Discover)
```

DHCP Offer: là gói tin chứa địa chỉ IP và thông tin cấu hình TCP/IP bổ sung. Nó được DHCP server gửi về cho Client sau khi nhận được DHCP Discover.

- IP nguồn: 192.168.54.2
- IP đích: 255.255.255.255
- MAC nguồn: 00:0c:29:b9:f2:ff
- MAC đích: ff:ff:ff:ff:ff:ff
- Port nguồn: 67
- Port đích: 68

```
Frame 9: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: VMware_b9:f2:ff (00:0c:29:b9:f2:ff), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.54.2, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (Offer)
```

DHCP Request: là gói được DHCP client phản hồi với máy chủ sau khi nhận được DHCP Offer để thể hiện sự chấp nhận đối với địa chỉ IP.

- IP nguồn: 0.0.0.0
- IP đích: 255.255.255.255
- MAC nguồn: 00:0c:29:04:40:8e
- MAC đích: ff:ff:ff:ff:ff:ff
- Port nguồn: 68
- Port đích: 67

```
Frame 10: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits)
Ethernet II, Src: VMware_04:40:8e (00:0c:29:04:40:8e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
```

DHCP ACK: là một gói được DHCP server gửi đến cho Client để xác thực việc chấp nhận DHCP Request và định hướng các tham số tùy chọn cho phép Client tham gia mạng TCP/IP và hoàn thành hệ thống khởi động.

- IP nguồn: 192.168.54.2
- IP đích: 255.255.255.255
- MAC nguồn: 00:0c:29:b9:f2:ff

- MAC đích: ff:ff:ff:ff:ff:ff
- Port nguồn: 67
- Port đích: 68

```
Frame 11: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: VMware_b9:f2:ff (00:0c:29:b9:f2:ff), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.54.2, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)
```

l. *Thông tin default gateway và DNS server nằm trong gói tin nào?*

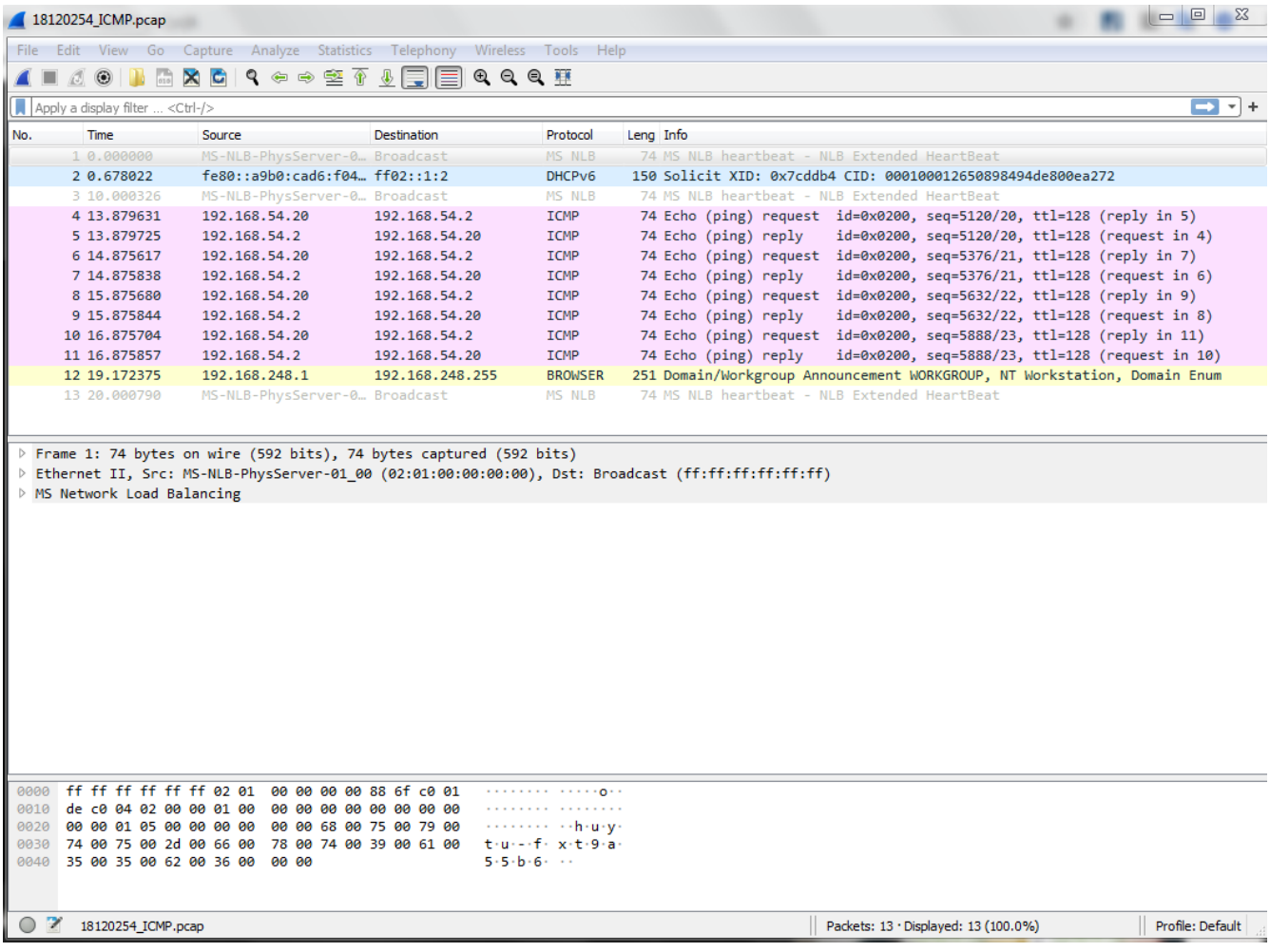
Thông tin default gateway và DNS server nằm trong gói tin DHCP Offer.

Câu 4: Sử dụng 2 máy tính của bài tập 3, sau khi client đã có được thông tin TCP/IP được cấp phát với DHCP server, thực hiện các yêu cầu sau:

a. *Thực hiện lệnh ping từ client đến server và dùng Wireshark để bắt các gói tin tương ứng.*

b. *Cho biết có bao nhiêu gói tin của quá trình thực hiện lệnh ping?*

Có 8 gói tin của quá trình thực hiện lệnh ping.



c. *Địa chỉ MAC nguồn, MAC đích là gì?*

Địa chỉ MAC nguồn: 00:0c:29:04:40:8e

Địa chỉ MAC đích: 00:0c:29:b9:f2:ff

```
▷ Ethernet II, Src: VMware_04:40:8e (00:0c:29:04:40:8e), Dst: VMware_b9:f2:ff (00:0c:29:b9:f2:ff)
```

d. *Địa chỉ IP nguồn, IP đích là gì?*

Địa chỉ IP nguồn: 192.168.54.20

Địa chỉ IP đích: 192.168.54.2

```
▷ Internet Protocol Version 4, Src: 192.168.54.20, Dst: 192.168.54.2
```

e. *Nội dung phần data của gói tin ICMP là gì?*

```
0000  00 0c 29 b9 f2 ff 00 0c  29 04 40 8e 08 00 45 00   ··)····· )·@···E·
0010  00 3c 02 11 00 00 80 01  4b 49 c0 a8 36 14 c0 a8   ·<····· KI··6···
0020  36 02 08 00 37 5c 02 00  14 00 61 62 63 64 65 66   6···7\·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                    wabcdefg hi
```