

## **BÀI TẬP THỰC HÀNH WIRESHARK**

MSSV : **18120113**

Lớp : **18CTT1**

Họ và Tên : **Nguyễn Chánh Đại**

---

**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 :

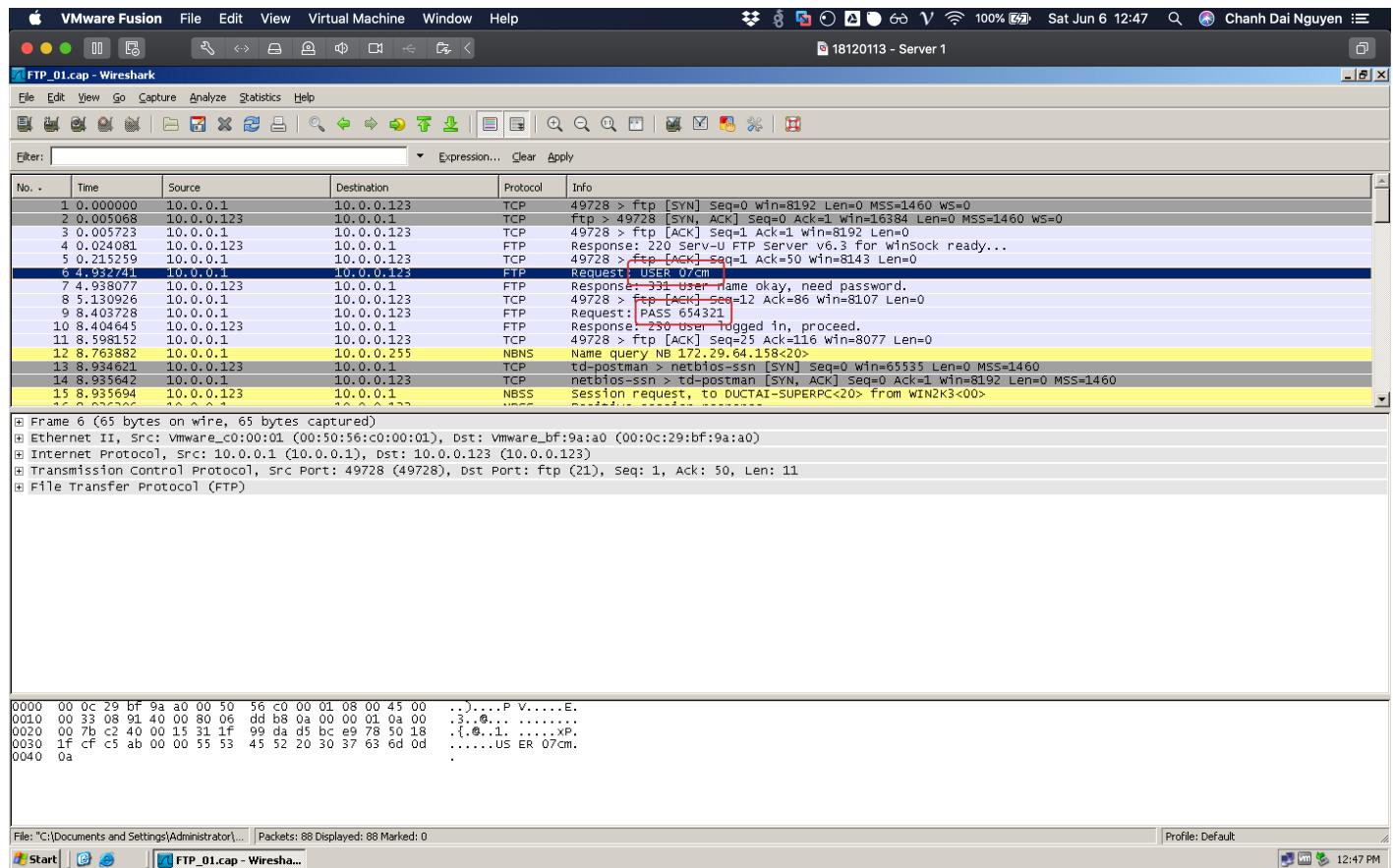
1 a. Username và Password của người dùng là gì ?

Username

07cm

Password

654321



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

IP Máy Client

10.0.0.1

IP Máy Server

10.0.0.123

The screenshot shows a Wireshark capture of network traffic from a Client (IP 10.0.0.1) to a Server (IP 10.0.0.123). The traffic includes:

- FTP connections: Multiple TCP sessions are established between the client and server, involving various commands like SYN, ACK, and DATA.
- NBNS queries: The client sends Name query NB requests to the server.
- NetBIOS-SSN requests: The client sends Session requests to the server.

A specific TCP packet is highlighted in yellow, showing the following details:

- Frame 1 (66 bytes on wire, 66 bytes captured)**
- Ethernet II, Src: VMware\_00:00:01 (00:50:56:c0:00:01), Dst: vmware\_bf:9a:a0 (00:0c:29:bf:9a:a0)**
- Internet Protocol Version 4 (IPv4)**
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)**
- Total Length: 52**
- Identification: 0x088d (2189)**
- Flags: 0x04 (Don't Fragment)**
- Fragment offset: 0**
- Time to live: 128**
- Protocol: TCP (0x06)**
- Header checksum: 0xddbh [correct]**
- Source: 10.0.0.1 (10.0.0.1)**
- Destination: 10.0.0.123 (10.0.0.123)**
- Transmission Control Protocol, Src Port: 49728 (49728), Dst Port: ftp (21), seq: 0, Len: 0**

The packet bytes pane shows the raw hex and ASCII data for this highlighted frame.

### 1 c. Client truy xuất lên Server theo mode nào: Active hay Passive ?

Client truy xuất lên Server theo Active Mode.

**PORT Command → Active Mode**

No.	Time	Source	Destination	Protocol	Info
56	8.988554	10.0.0.123	10.0.0.1	TCP	netbios-ssn > cma [FIN, ACK] Seq=1000 Ack=1087 win=62227 Len=0
57	8.988575	10.0.0.123	10.0.0.1	TCP	cma > netbios-ssn [ACK] Seq=1087 Ack=1001 win=64536 Len=0
58	9.013267	10.0.0.1	10.0.0.255	BROWSER	Local Master Announcement DUCTAI-SUPERPC, workstation, Server, Print Queue Server, NT Workstation, Poter
59	9.514796	10.0.0.1	10.0.0.255	NBNS	Name query NB 172.29.64.158<20>
60	10.257412	10.0.0.1	10.0.0.255	NBNS	Name query NB 172.29.64.158<20>
61	19.254255	10.0.0.1	10.0.0.255	NBNS	Name query NB 172.29.64.158<20>
62	20.043530	10.0.0.1	10.0.0.255	NBNS	Name query NB 172.29.64.158<20>
63	20.760043	10.0.0.1	10.0.0.255	NBNS	Name query NB 172.29.64.158<20>
64	25.253959	10.0.0.1	10.0.0.123	FTP	Request: PORT 10.0.0.1,194,69
65	25.254698	10.0.0.123	10.0.0.1	FTP	Response: 200 PORT Command successful.
66	25.257566	10.0.0.1	10.0.0.123	FTP	Request: LIST
67	25.260044	10.0.0.123	10.0.0.1	TCP	49733 > ftp-data [SYN] Seq=0 Win=65535 Len=0 MSS=1460
68	25.260306	10.0.0.1	10.0.0.123	TCP	49733 > ftp-data [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460
69	25.260488	10.0.0.123	10.0.0.1	TCP	49733 > ftp-data [ACK] Seq=1 Ack=1 win=65535 Len=0
70	25.261565	10.0.0.123	10.0.0.1	FTP-DATA	FTP Data: 1460 bytes

Frame 65 (84 bytes on wire, 84 bytes captured)  
**Ethernet II, Src: VMware\_BF:9A:A0 (00:0c:29:bf:9a:a0), Dst: VMware\_C0:00:01 (00:50:56:c0:00:01)**  
**Internet Protocol, Src: 10.0.0.123 (10.0.0.123), Dst: 10.0.0.1 (10.0.0.1)**  
 version: 4  
 Header length: 20 bytes  
**Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)**  
 Total Length: 70  
 Identification: 0x04b3 (1203)  
**Flags: 0x00**  
 Fragment offset: 0  
 Time to live: 128  
 Protocol: TCP (0x06)  
**Header checksum: 0x2184 [correct]**  
 Source: 10.0.0.123 (10.0.0.123)  
 Destination: 10.0.0.1 (10.0.0.1)  
**Transmission Control Protocol, Src Port: ftp (21), Dst Port: 49728 (49728), seq: 116, Ack: 47, Len: 30**  
**File Transfer Protocol (FTP)**

```
0000  00 50 56 c0 00 01 00 0c 29 bf 9a a0 08 00 45 00 .PV..... ).....E.
0010  00 46 04 b3 00 00 80 06 21 84 0a 00 00 7b 0a 00 .F..... !...{.
0020  00 01 00 15 c2 40 d5 bc e9 ba 31 1f 9a 08 50 18 .....@. .!..P.
0030  44 42 4d 34 00 00 32 30 30 20 50 4f 52 54 20 43 DBM4..20 0 PORT C
0040  6f 6d 6d 61 6e 64 20 73 75 63 63 65 73 73 66 75 command s accessfu
0050  6c 2e 0d 0a 1...
```

File: "C:\Documents and Settings\Administrator\...\ FTP\_01.cap" | Packets: 88 | Displayed: 88 | Marked: 0 | Profile: Default

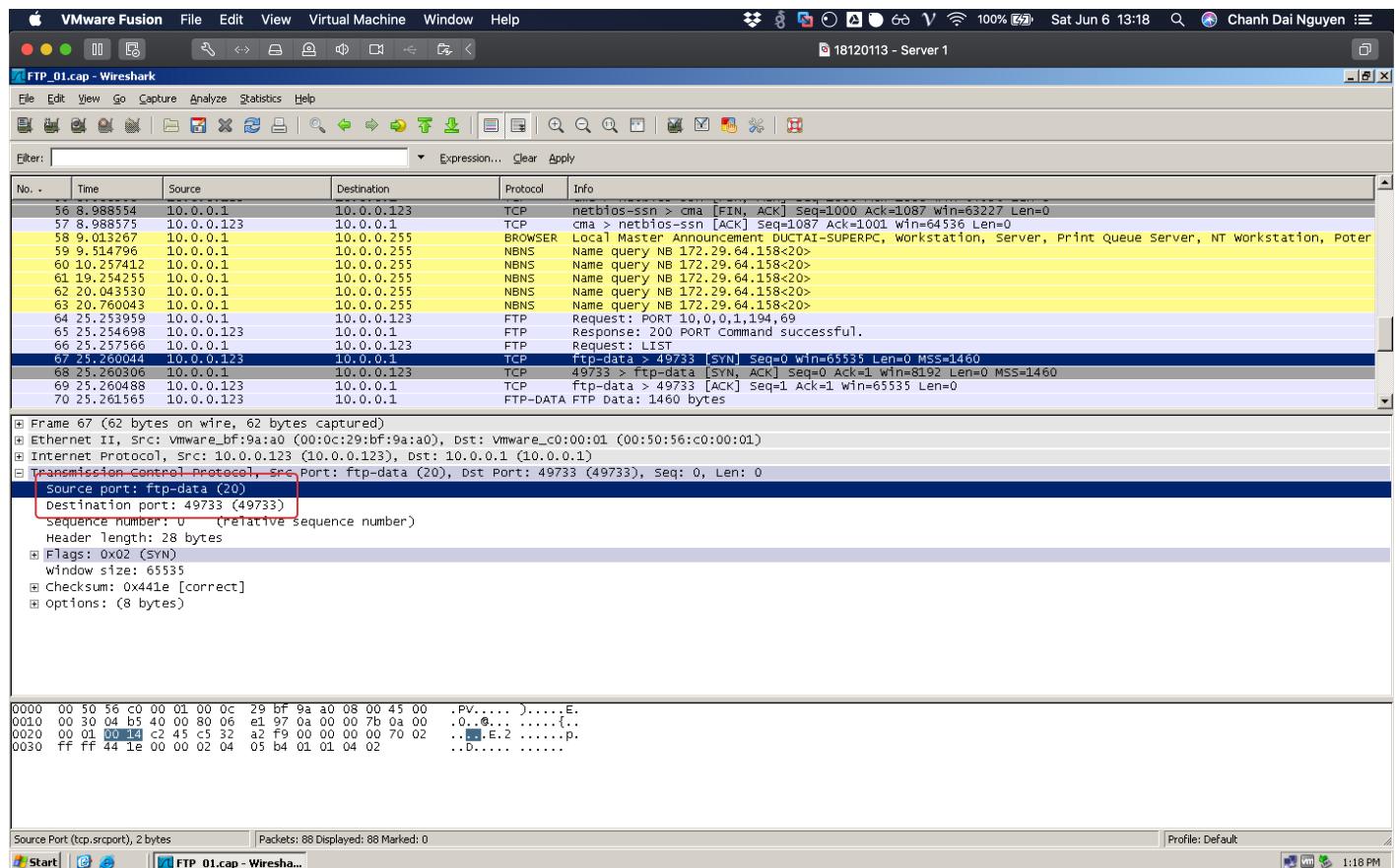
## 1 d. Port truyền dữ liệu của FTP Server và Client là bao nhiêu ?

Port FTP Server

20

Port Client

49733



Câu 2. Cho tập tin FTP\_02.cap, đọc tập tin này bằng Wireshark và trả lời các câu hỏi sau :

2 a. FTP sử dụng giao thức UDP hay TCP ?

FTP sử dụng giao thức TCP.

The screenshot shows the Wireshark interface with the following details:

- File Menu:** File, Edit, View, Virtual Machine, Window, Help.
- Toolbar:** Standard icons for opening files, capturing, analyzing, and saving.
- Network View:** Shows the list of captured frames. Frame 7 is highlighted in red and selected. It is a TCP packet from port 21 to port 49788, containing a SYN-ACK response.
- Details View:** Displays the raw hex and ASCII data for the selected frame. The ASCII dump shows the response "49788 > ftp [ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=0".
- Hex View:** Shows the raw hex bytes of the selected frame.
- Statistics View:** Shows basic statistics about the capture.
- Help View:** Chanh Dai Nguyen is listed as the user.

A red box highlights the TCP connection in the Network View, specifically the SYN-ACK response at frame 7. The text "TCP Protocol" is overlaid on the red box.

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

FTP Server nhận kết nối ở Port mặc định : 21

The screenshot shows a Wireshark capture of an FTP session named "FTP\_02.cap". The packet list displays 60 captured packets. The SYN packet (index 6) is highlighted in yellow. The details pane shows the following information for the SYN packet:

- Frame 6 (66 bytes on wire, 66 bytes captured)
- Ethernet II, Src: VMware\_00:00:01 (00:0c:29:bf:9a:a0), Dst: VMware\_00:00:01 (00:0c:29:bf:9a:a0)
- Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.224 (10.0.0.224)
- Transmission Control Protocol, src Port: 49788 (49788), dst Port: ftp (21), seq: 0, Len: 0  
source port: 49788 (49788)  
destination port: ftp (21)  
sequence number: 0 (relative sequence number)  
header length: 32 bytes  
flags: 0x02 (SYN)  
window size: 8192  
checksum: 0x083e [correct]  
options: (12 bytes)

The bytes pane shows the raw hex and ASCII representation of the SYN packet.

## 2 c. Username và Password của người dùng là gì ?

**Username**

cm07

**Password**

123654

The screenshot shows a Wireshark capture of an FTP session named 'FTP\_02.cap'. The session details pane shows the following sequence:

- Frame 17 (65 bytes on wire, 65 bytes captured): An Ethernet II frame from the VMware\_BF interface.
- Transmission Control Protocol (TCP) connection setup between source port 49788 and destination port 21.
- User Authentication:
  - Request: USER cm07 (Sequence number 43)
  - Response: 331 User name okay, need password.
  - Request: PASS 123654 (Sequence number 54)
  - Response: 230 User logged in, proceed.
- File Transfer Protocol (FTP) command:
  - Request: SYST (Sequence number 55)
  - Response: 215 UNIX Type: L8 (Sequence number 56)

The packet list pane shows the raw hex and ASCII data for each packet. The user 'cm07' and password '123654' are highlighted in red in the protocol and ASCII columns respectively.

## 2 d. Port truyền lệnh của Client là bao nhiêu ?

Port truyền lệnh của Client là 49788.

The screenshot shows a Wireshark capture of an FTP session. The client (10.0.0.1) is connecting to the server (10.0.0.224) on port 21. The client's source port is 49788. The session starts with a Name query from the client, followed by USER and PASS commands, and a SYST response. The selected packet (Frame 17) shows the client sending a USER command to the server.

No.	Time	Source	Destination	Protocol	Info
8	11.429211	10.0.0.1	10.0.0.224	TCP	49788 > ftp [ACK] seq=1 Ack=1 win=65700 Len=0
9	11.431999	10.0.0.1	10.0.0.224	FTP	Response: 220 Serv-U FTP Server v6.3 for Winsock ready...
10	11.615330	10.0.0.1	10.0.0.224	TCP	49788 > ftp [ACK] seq=1 Ack=50 win=65648 Len=0
11	12.192785	10.0.0.1	10.0.0.255	NBNS	Name query NB 172.29.70.4<20>
12	12.730270	10.0.0.1	10.0.0.224	FTP	Request: USER anonymous
13	12.731818	10.0.0.1	10.0.0.224	FTP	Response: 331 User name okay, please send complete E-mail address as password.
14	12.848222	10.0.0.1	10.0.0.224	FTP	Request: PASS mozillal@example.com
15	12.849323	10.0.0.1	10.0.0.224	FTP	Response: 530 Sorry, no ANONYMOUS access allowed.
16	13.077272	10.0.0.1	10.0.0.224	TCP	49788 > ftp [ACK] seq=43 Ack=161 win=65540 Len=0
17	21.836141	10.0.0.1	10.0.0.224	FTP	Request: USER cm07
18	21.837664	10.0.0.1	10.0.0.224	FTP	Response: 331 User name okay, need password.
19	21.905232	10.0.0.1	10.0.0.224	FTP	Request: PASS 123654
20	21.906163	10.0.0.1	10.0.0.224	FTP	Response: 230 User logged in, proceed.
21	21.935646	10.0.0.1	10.0.0.224	FTP	Request: SYST
22	21.936236	10.0.0.1	10.0.0.224	FTP	Response: 215 UNIX Type: L8

Selected packet details:

- Frame 17 (65 bytes on wire, 65 bytes captured)
- Ethernet II, Src: VMware\_00:00:01 (00:00:00:00:00:01), Dst: VMware\_BF:9A:A0 (00:0c:29:bf:9a:a0)
- Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.224 (10.0.0.224)
- Transmission Control Protocol, Src Port: 49788 (49788), Dst Port: ftp (21), Seq: 43, Ack: 161, Len: 11

Source port: 49788 (49788)  
destination port: ftp (21)  
sequence number: 43 (relative sequence number)  
[Next sequence number: 54 (relative sequence number)]  
Acknowledgement number: 161 (relative ack number)  
Header length: 20 bytes  
Flags: 0x18 (PSH, ACK)  
window size: 65540 (scaled)  
Checksum: 0xea84 [correct]  
File Transfer Protocol (FTP)

Hex dump of the selected packet:

```

0000  00 00 00 29 bf 9a a0 00 50 56 c0 00 01 08 00 45 00 ..).,..P V,...E.
0010  00 33 09 9c 40 00 80 06 dc 48 0a 00 00 01 0a 00 ..3.@@...H...
0020  00 e0 C2 7C 00 15 83 6b ec 25 14 e1 c0 10 50 18 ..@...k.%...P.
0030  40 01 ea 84 00 00 55 53 45 52 20 63 6d 30 37 0d @...US ER cm07.
0040  0a .

```

## 2 e. Client truy xuất lên Server theo mode nào: Active hay Passive ?

Client truy xuất lên Server theo Passive Mode.

**PASV → Passive Mode**

Request: PASV

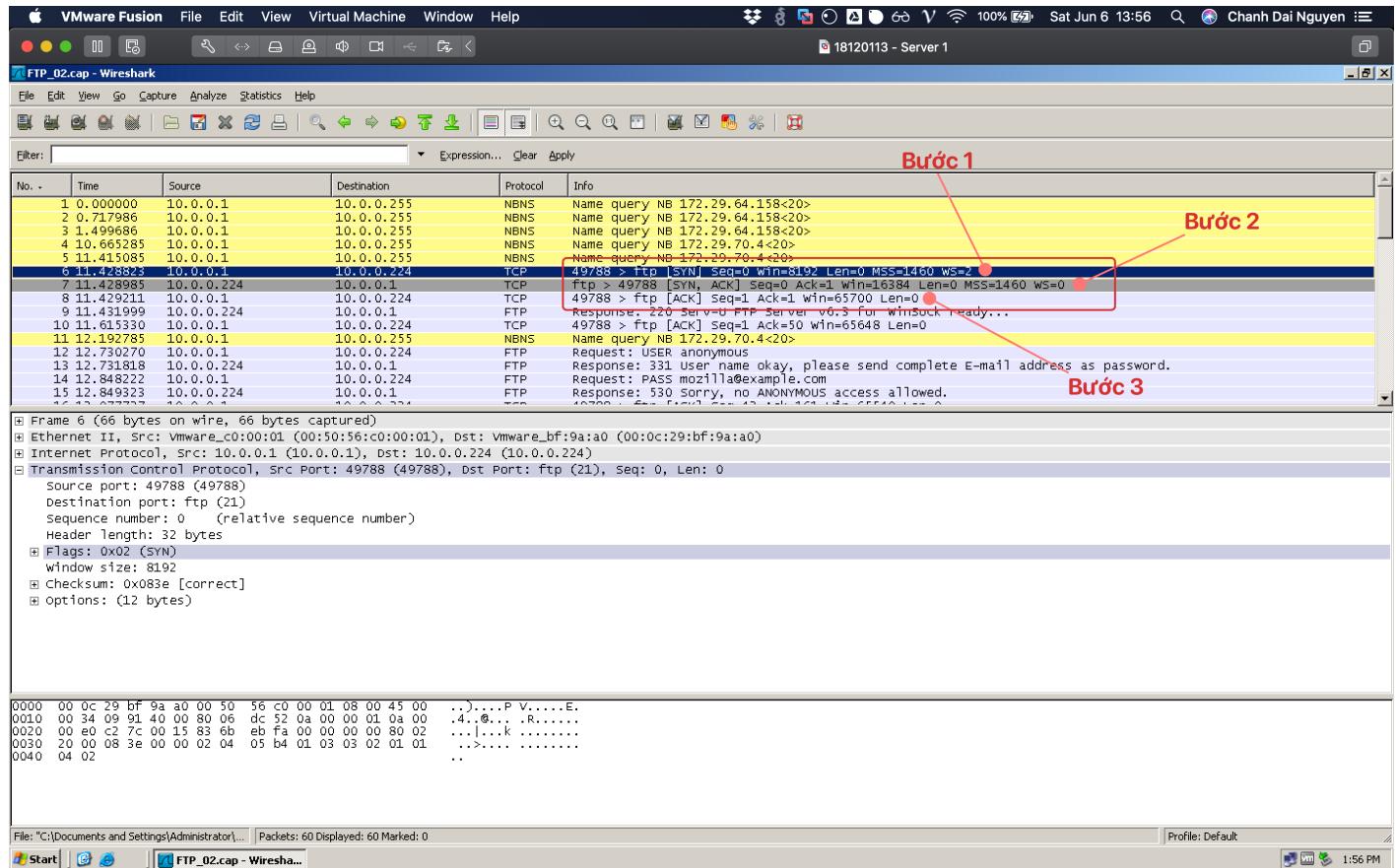
Response: 227 Entering Passive Mode (10,0,0,224,19,137)

No.	Time	Source	Destination	Protocol	Info
21	21.93646	10.0.0.1	10.0.0.224	FTP	Request: SYST
22	21.936236	10.0.0.1	10.0.0.224	FTP	Response: 215 UNIX Type: L8
23	21.952730	10.0.0.1	10.0.0.224	FTP	Request: PWD
24	21.954292	10.0.0.1	10.0.0.224	FTP	Response: 257 "/" is current directory.
25	21.955344	10.0.0.1	10.0.0.224	FTP	Request: TYPE I
26	21.955762	10.0.0.1	10.0.0.224	FTP	Response: 200 Type set to I.
27	21.956224	10.0.0.1	10.0.0.224	FTP	Request: PASV
28	21.968087	10.0.0.1	10.0.0.1	FTP	Response: 227 Entering Passive Mode (10,0,0,224,19,137)
29	21.984564	10.0.0.1	10.0.0.224	FTP	REQUEST: SIZE /
30	21.985403	10.0.0.1	10.0.0.1	FTP	Response: 550 /: No such file.
31	21.986261	10.0.0.1	10.0.0.224	TCP	49791 > complex-link [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
32	21.986361	10.0.0.1	10.0.0.1	TCP	complex-link > 49791 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=0
33	21.986491	10.0.0.1	10.0.0.224	FTP	Request: MDTM /
34	21.986571	10.0.0.1	10.0.0.224	TCP	49791 > complex-link [ACK] Seq=1 Ack=1 Win=65700 Len=0
35	21.987586	10.0.0.1	10.0.0.1	FTP	Response: 213 20090903103505

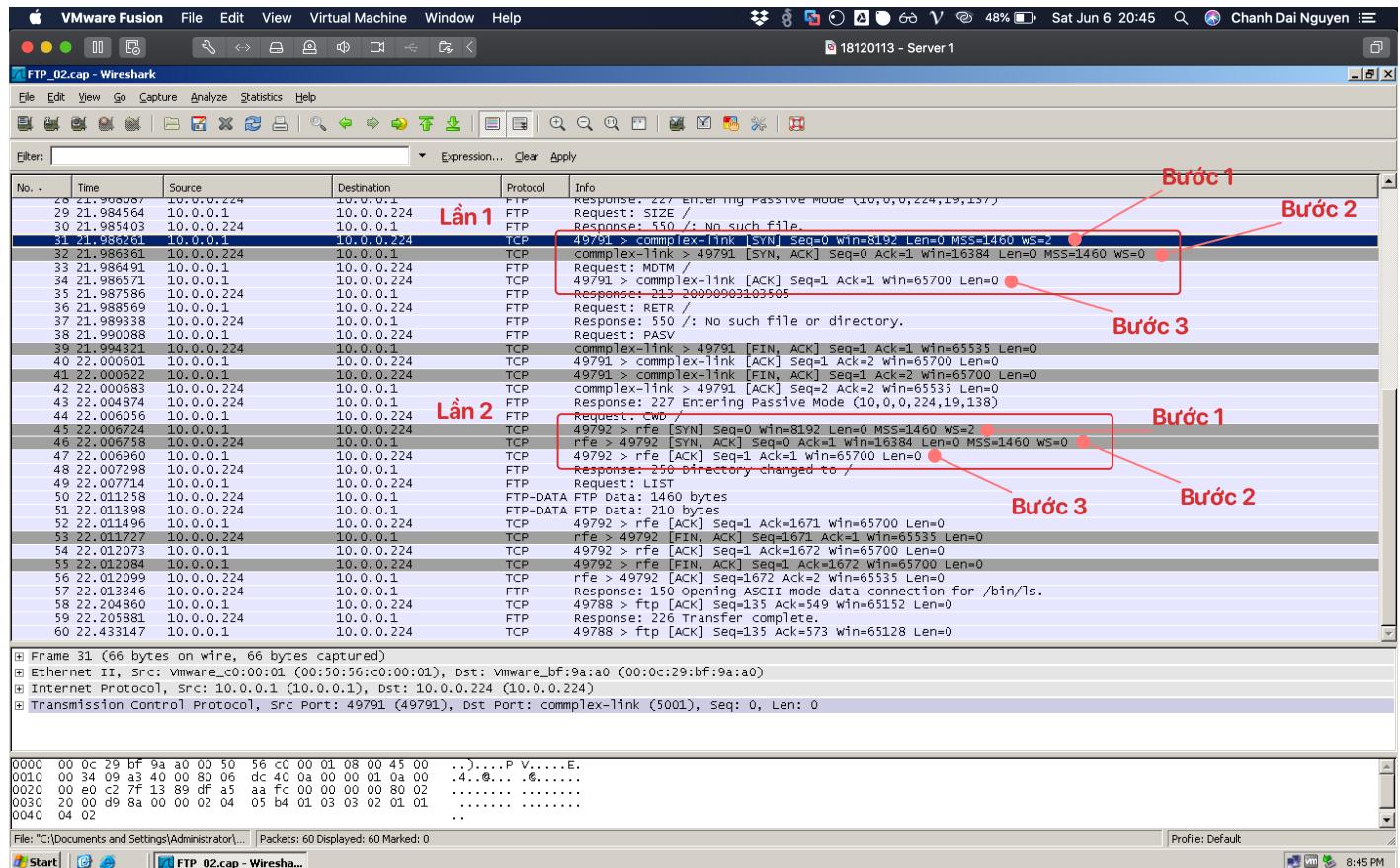
Frame 27 (60 bytes on wire, 60 bytes captured)  
 Ethernet II, Src: VMware\_C0:00:01 (00:00:56:c0:00:01), Dst: VMware\_BF:9a:a0 (00:0c:29:bf:9a:a0)  
 Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.224 (10.0.0.224)  
 Transmission Control Protocol, Src Port: 49788 (49788), Dst Port: ftp (21), seq: 86, Ack: 297, Len: 6  
 sequence number: 86 (relative sequence number)  
 [Next sequence number: 92 (relative sequence number)]  
 Acknowledgement number: 297 (relative ack number)  
 Header length: 20 bytes  
 Flags: 0x18 (PSH, ACK)  
 window size: 65404 (scaled)  
 Checksum: 0xa29d [correct]  
 [SEQ/ACK analysis]  
 File Transfer Protocol (FTP)  
 PASV\r\n

```
0000 00 0c 29 bf 9a a0 00 50 56 c0 00 01 08 00 45 00  ..)....P V.....E.
0010 00 2e 09 a1 40 00 80 06 dc 48 0a 00 00 01 0a 00  ...@..._H.....
0020 00 e0 c2 7c 00 15 83 6b ec 50 14 e1 c0 98 50 18  ?...!..k_P....P.
0030 3f df a2 9d 00 00 50 41 53 56 0d 0a  ?....PA S\..
```

**2 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.**



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



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

## Kết nối lần 1

## Port FTP Server

5001

## Port Client

49791

VMware Fusion File Edit View Virtual Machine Window Help

18120113 - Server 1

FTP\_02.cap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
28	21.968087	10.0.0.224	10.0.0.1	FTP	Response: 227 Entering Passive Mode (10,0,0,224,19,137)
29	21.984564	10.0.0.1	10.0.0.224	FTP	Request: SIZE /
30	21.985403	10.0.0.224	10.0.0.1	FTP	Response: 550 : No such file.
31	21.986261	10.0.0.1	10.0.0.224	TCP	49791 > complex-link [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=2
32	21.986361	10.0.0.224	10.0.0.1	TCP	complex-link > 49791 [SYN, ACK] Seq=0 Ack=1 win=16384 Len=0 MSS=1460 WS=0
33	21.986491	10.0.0.1	10.0.0.224	FTP	Request: MDTM /
34	21.986571	10.0.0.1	10.0.0.224	TCP	49791 > complex-link [ACK] Seq=1 Ack=1 win=65700 Len=0
35	21.987586	10.0.0.224	10.0.0.1	FTP	Response: 213 20090903103505
36	21.988569	10.0.0.1	10.0.0.224	FTP	Request: RETR /
37	21.989334	10.0.0.224	10.0.0.1	FTP	Response: 550 : No such file or directory.
38	21.990088	10.0.0.1	10.0.0.224	FTP	Request: PASV
39	21.994321	10.0.0.224	10.0.0.1	TCP	complex-link > 49791 [FIN, ACK] Seq=1 Ack=1 win=65535 Len=0
40	22.000601	10.0.0.1	10.0.0.224	TCP	49791 > complex-link [ACK] Seq=1 Ack=2 win=65700 Len=0
41	22.000622	10.0.0.1	10.0.0.224	TCP	49791 > complex-link [FIN, ACK] Seq=1 Ack=2 win=65700 Len=0
42	22.000683	10.0.0.224	10.0.0.1	TCP	complex-link > 49791 [ACK] Seq=2 Ack=2 win=65535 Len=0
43	22.004874	10.0.0.224	10.0.0.1	FTP	Response: 227 Entering Passive Mode (10,0,0,224,19,138)
44	22.006056	10.0.0.1	10.0.0.224	FTP	Request: CWD /
45	22.006724	10.0.0.1	10.0.0.224	TCP	49792 > rfe [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=2
46	22.007001	10.0.0.1	10.0.0.224	TCP	rfe > 49792 [SYN, ACK] Seq=0 Ack=1 win=16384 Len=0 MSS=1460 WS=0
47	22.007660	10.0.0.1	10.0.0.224	TCP	49792 > rfe [ACK] Seq=1 Ack=1 win=65700 Len=0
48	22.007298	10.0.0.1	10.0.0.224	FTP	Response: 150 Directory changed to /
49	22.007714	10.0.0.1	10.0.0.224	FTP	Request: LIST
50	22.011258	10.0.0.224	10.0.0.1	FTP-DATA	FTP Data: 1460 bytes
51	22.011398	10.0.0.224	10.0.0.1	FTP-DATA	FTP Data: 210 bytes
52	22.011496	10.0.0.1	10.0.0.224	TCP	49792 > rfe [ACK] Seq=1 Ack=1671 win=65700 Len=0
53	22.011727	10.0.0.224	10.0.0.1	TCP	rfe > 49792 [FIN, ACK] Seq=1671 Ack=1 win=65535 Len=0
54	22.012073	10.0.0.1	10.0.0.224	TCP	49792 > rfe [ACK] Seq=1 Ack=1672 win=65700 Len=0
55	22.012084	10.0.0.1	10.0.0.224	TCP	49792 > rfe [IN, ACK] Seq=1 Ack=1672 win=65700 Len=0
56	22.012099	10.0.0.224	10.0.0.1	TCP	rfe > 49792 [ACK] Seq=1672 Ack=2 win=65535 Len=0
57	22.013346	10.0.0.224	10.0.0.1	FTP	Response: 150 Opening ASCII mode data connection for /bin/ls.

Frame 31 (66 bytes on wire, 66 bytes captured)  
 Ethernet II, Src: vmware\_c0:00:01 (00:05:06:c0:00:01), Dst: vmware\_bf:9a:a0 (00:0c:29:bf:9a:a0)  
 Internet Protocol, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.224 (10.0.0.224)  
 Transmission Control Protocol, Src Port: 49791 (49791), Dst Port: complex-link (5001), Seq: 0, Len: 0

Source port: 49791 (49791)  
 Destination port: complex-link (5001)  
 Sequence number: 0 (relative sequence number)  
 Header length: 32 bytes  
 Flags: SYN (syn)

0010 00 34 09 a3 40 00 80 06 dc 40 04 00 00 01 03 00 .4.1.0. .6. ....  
 0020 00 80 00 00 13 89 df a5 aa fc 00 00 00 00 00 02 00 ..0.. ....  
 0030 20 00 d9 8a 00 00 02 04 03 bf 01 03 03 02 01 01 ..0.. ....  
 0040 04 02 ..0.. ....

Source Port (tcp.srcport), 2 bytes | Packets: 60 Displayed: 60 Marked: 0 | Profile: Default

Start Stop | **FTP\_02.cap - Wireshark...** | 8:54 PM

Kết nối lần 2

### Port FTP Server

5002

### Port Client

49792

The screenshot shows a Wireshark capture of an FTP session. The session starts with a passive mode request from the client (49792) to the server (5002). The client then lists the directory and retrieves files. A specific SYN packet is highlighted with a red box.

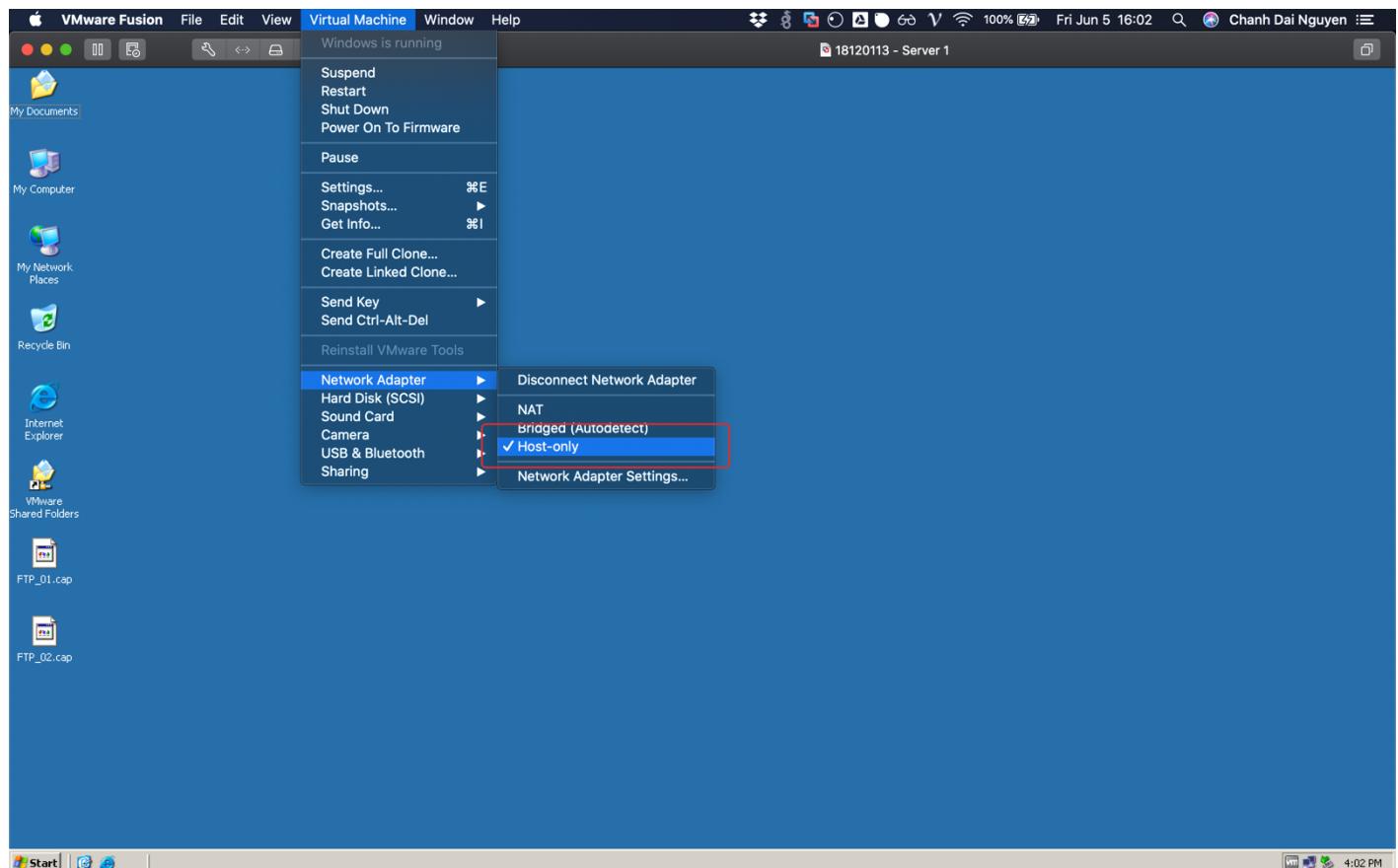
No.	Time	Source	Destination	Protocol	Info
28	21. 968087	10.0.0.224	10.0.0.1	FTP	Response: 227 Entering Passive Mode (10,0,0,224,19,137)
29	21. 984564	10.0.0.1	10.0.0.224	FTP	Request: SIZE /
30	21. 985403	10.0.0.224	10.0.0.1	FTP	Response: 550 /: no such file.
31	21. 986261	10.0.0.1	10.0.0.224	TCP	49792 > complex-link [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
32	21. 986361	10.0.0.224	10.0.0.1	TCP	complex-link > 49791 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=0
33	21. 986491	10.0.0.1	10.0.0.224	FTP	Request: MDTM /
34	21. 986571	10.0.0.1	10.0.0.224	TCP	49791 > complex-link [ACK] Seq=1 Ack=1 Win=65700 Len=0
35	21. 987586	10.0.0.224	10.0.0.1	FTP	Response: 213 20090903103505
36	21. 988569	10.0.0.1	10.0.0.224	FTP	Request: RETR /
37	21. 989338	10.0.0.224	10.0.0.1	FTP	Response: 550 /: no such file or directory.
38	21. 990088	10.0.0.1	10.0.0.224	FTP	Request: PASV
39	21. 994321	10.0.0.224	10.0.0.1	TCP	complex-link > 49791 [FIN, ACK] Seq=1 Ack=1 Win=65335 Len=0
40	22. 000601	10.0.0.1	10.0.0.224	TCP	49791 > complex-link [ACK] Seq=1 Ack=2 Win=65700 Len=0
41	22. 000622	10.0.0.224	10.0.0.1	TCP	49791 > complex-link [FIN, ACK] Seq=1 Ack=2 Win=65700 Len=0
42	22. 004683	10.0.0.224	10.0.0.1	TCP	complex-link > 49791 [ACK] Seq=2 Ack=2 Win=65335 Len=0
43	22. 004874	10.0.0.224	10.0.0.1	FTP	Response: 227 Entering Passive Mode (10,0,0,224,19,138)
44	22. 005036	10.0.0.1	10.0.0.224	FTP	Request: CWD
45	22. 005040	10.0.0.224	10.0.0.1	TCP	49791 > rfe [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=2
46	22. 005758	10.0.0.224	10.0.0.1	TCP	49791 > rfe [SYN, ACK] Seq=0 Ack=1 Win=40904 Len=0 MSS=1460 WS=0
47	22. 008960	10.0.0.1	10.0.0.224	TCP	49791 > rfe [ACK] Seq=1 Ack=1 Win=65700 Len=0
48	22. 009798	10.0.0.224	10.0.0.1	FTP	Response: 250 Directory changed to /
49	22. 007714	10.0.0.1	10.0.0.224	FTP	Request: LIST
50	22. 011258	10.0.0.224	10.0.0.1	FTP-DATA	FTP Data: 1460 bytes
51	22. 011398	10.0.0.224	10.0.0.1	FTP-DATA	FTP Data: 210 bytes
52	22. 011496	10.0.0.1	10.0.0.224	TCP	49792 > rfe [ACK] Seq=1 Ack=1671 Win=65700 Len=0
53	22. 011727	10.0.0.224	10.0.0.1	TCP	rfe > 49792 [FIN, ACK] Seq=1671 Ack=1 Win=65335 Len=0
54	22. 012073	10.0.0.1	10.0.0.224	TCP	49792 > rfe [ACK] Seq=1 Ack=1672 Win=65700 Len=0
55	22. 012084	10.0.0.1	10.0.0.224	TCP	49791 > rfe [FIN, ACK] Seq=1 Ack=1672 Win=65700 Len=0
56	22. 012099	10.0.0.224	10.0.0.1	TCP	rfe > 49792 [ACK] Seq=1672 Ack=2 Win=65335 Len=0
57	22. 013346	10.0.0.224	10.0.0.1	FTP	Response: 150 Opening ASCII mode data connection for /bin/ls.

Frame 45 (66 bytes on wire, 66 bytes captured)  
 Ethernet II, Src: VMware\_0f:00:01 (00:0f:00:00:01:01), Dst: vmware\_bf:9a:a0 (00:0c:29:bf:9a:a0)  
 Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.224 (10.0.0.224)  
 Transmission Control Protocol, Src Port: 49792 (49792), Dst Port: rfe (5002), Seq: 0, Len: 0  
 Source port: 49792 (49792)  
 Destination port: rfe (5002)  
 Sequence number: 0 (relative sequence number)  
 Header length: 32 bytes  
 Flags: 0x02 (SYN)

File: "C:\Documents and Settings\Administrator\...\Packets: 60 Displayed: 60 Marked: 0" Profile: Default  
 Start | Stop | Reload | FTP\_02.cap - Wireshark... | 8:57 PM

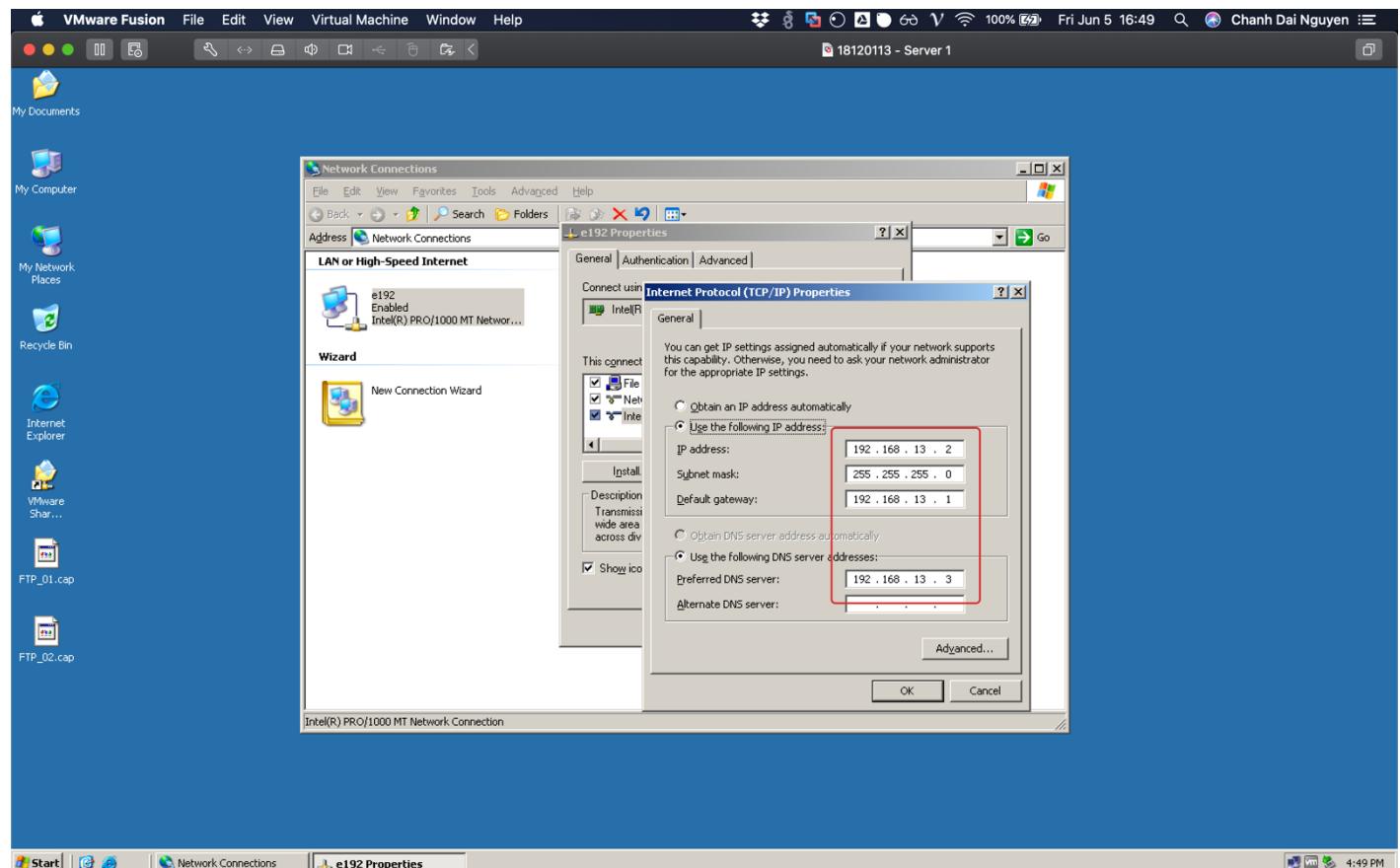
### Câu 3. Cấu hình dịch vụ DHCP với các thông tin sau :

3 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.



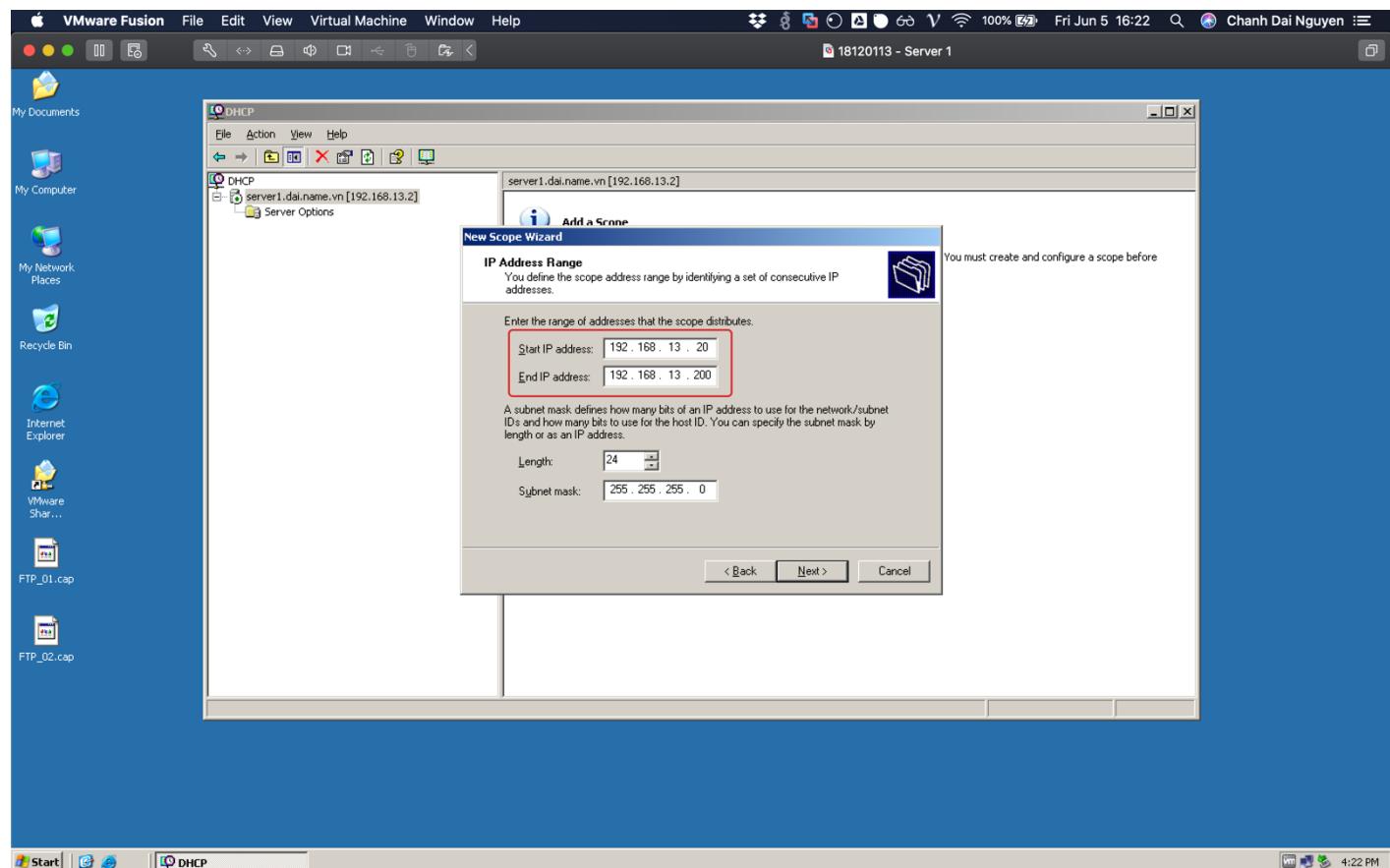
3 b. Cấu hình địa chỉ IP tĩnh cho máy làm DHCP Server này là : 192.168.X.2/24, với X là 2 chữ số cuối của MSSV.

MSSV = 1812113 → X = 13 → 192.168.13.2



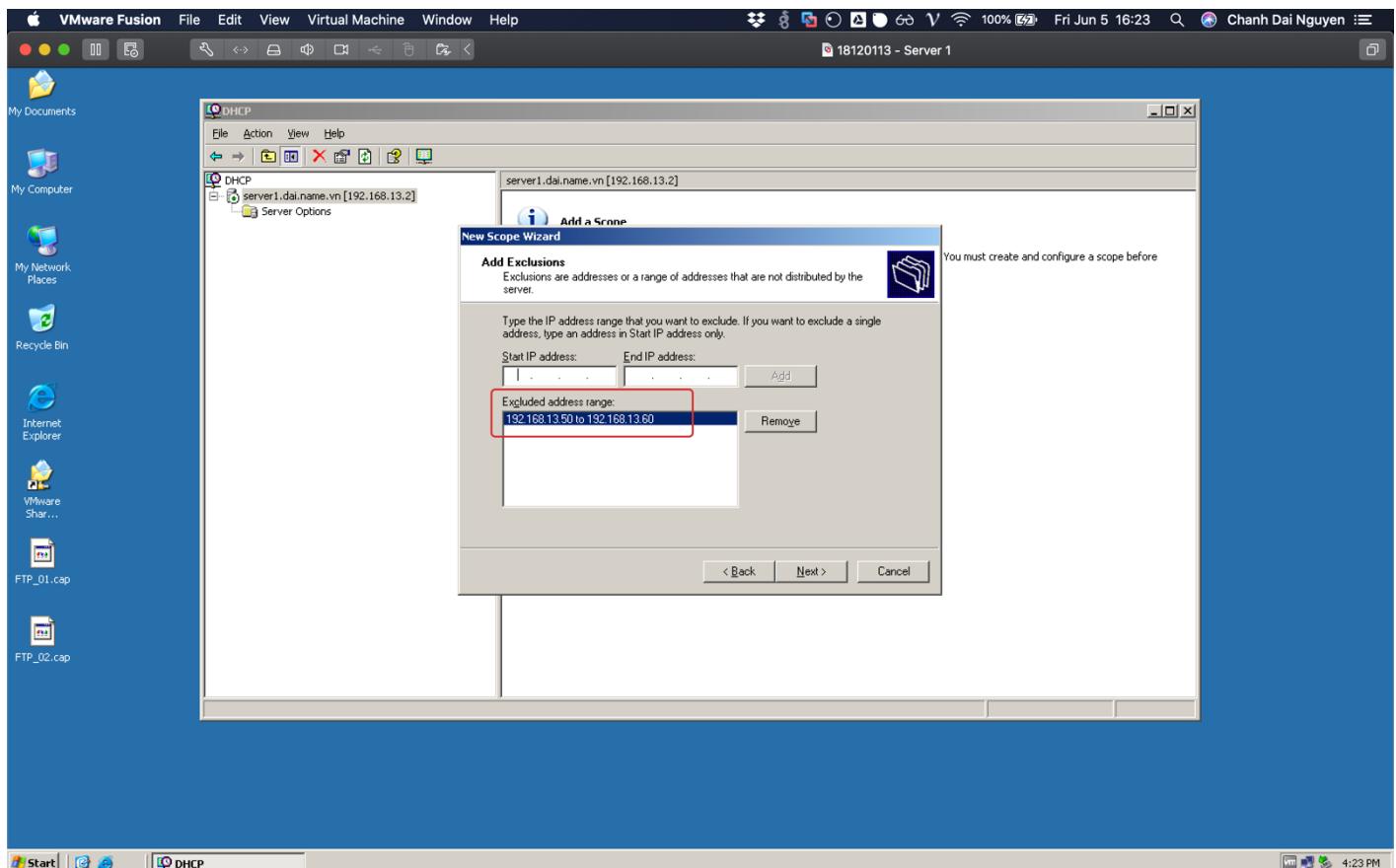
3 c. Khoảng địa chỉ IP cấp cho các Clients là : 192.168.X.20/24 – 192.168.X.200/24

→ 192.168.13.20/24 – 192.168.13.200/24



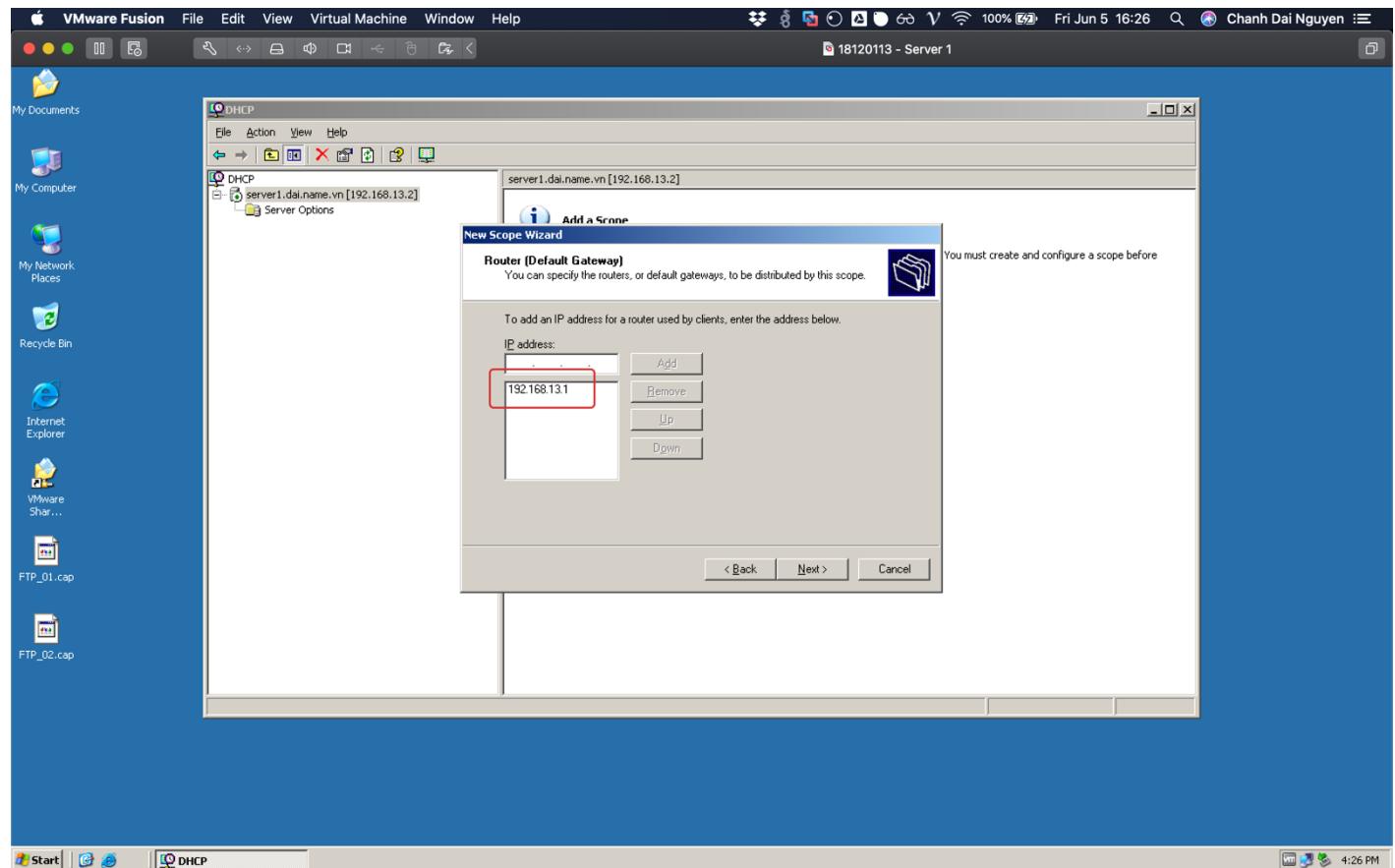
3 d. Khoảng địa chỉ IP không được cấp tự động (Exclusion) : 192.168.X.50/24 – 192.168.X.60/24

→ 192.168.13.50/24 – 192.168.13.60/24



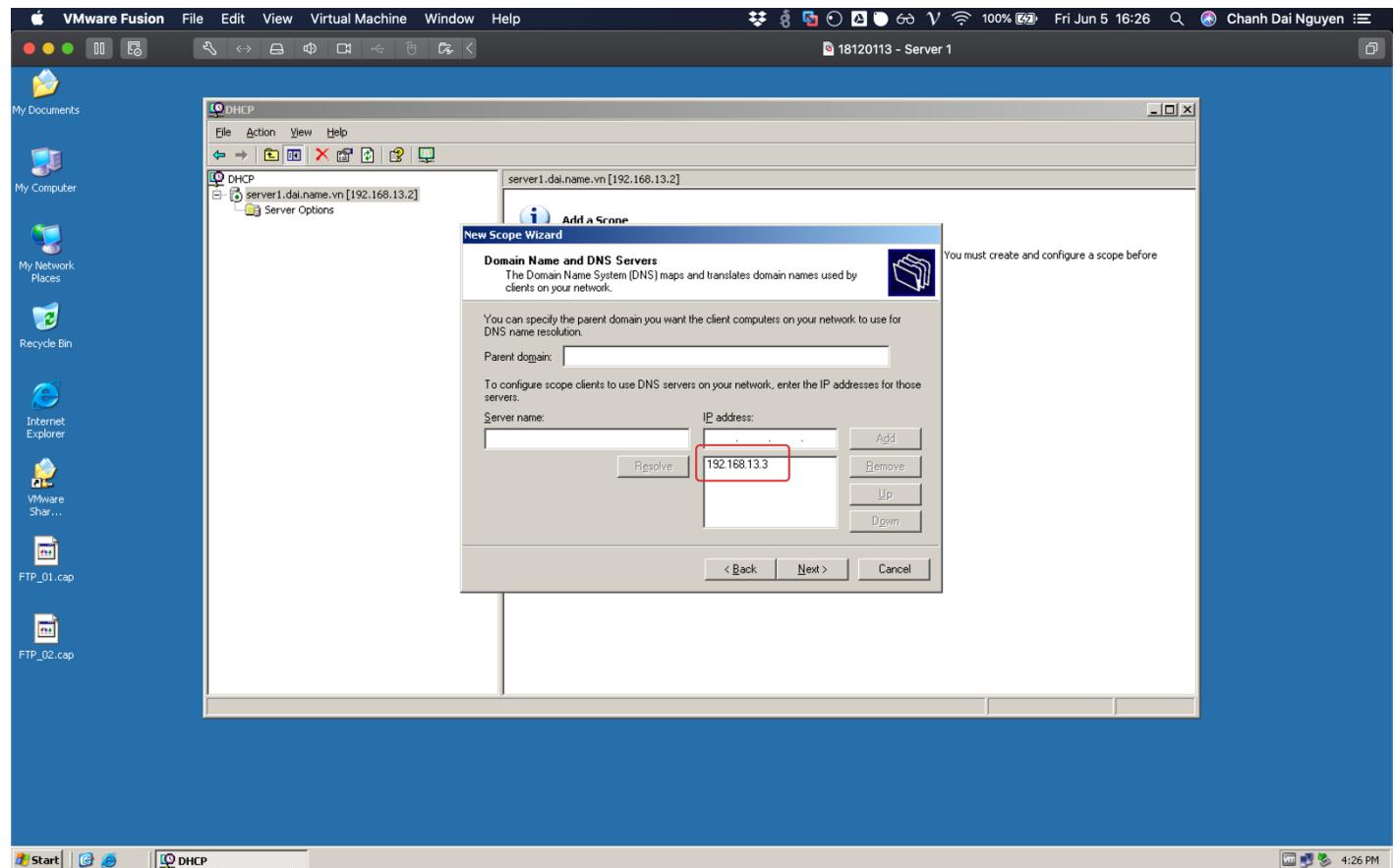
### 3 e. Default Gateway cung cấp cho các Clients : 192.168.X.1

→ 192.168.13.1

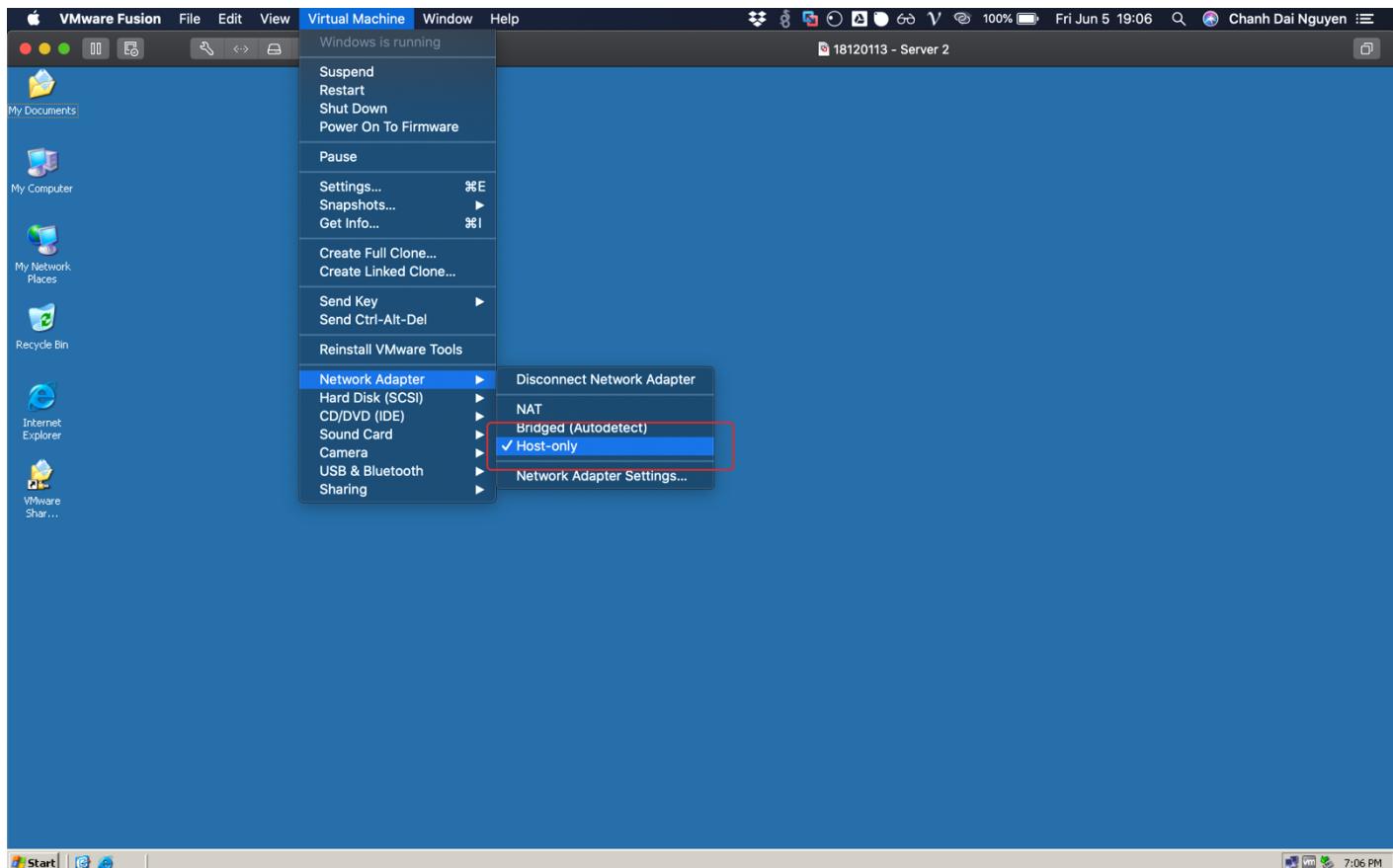


### 3 f. DNS Server cung cấp cho các Clients: 192.168.X.3

→ 192.168.13.3

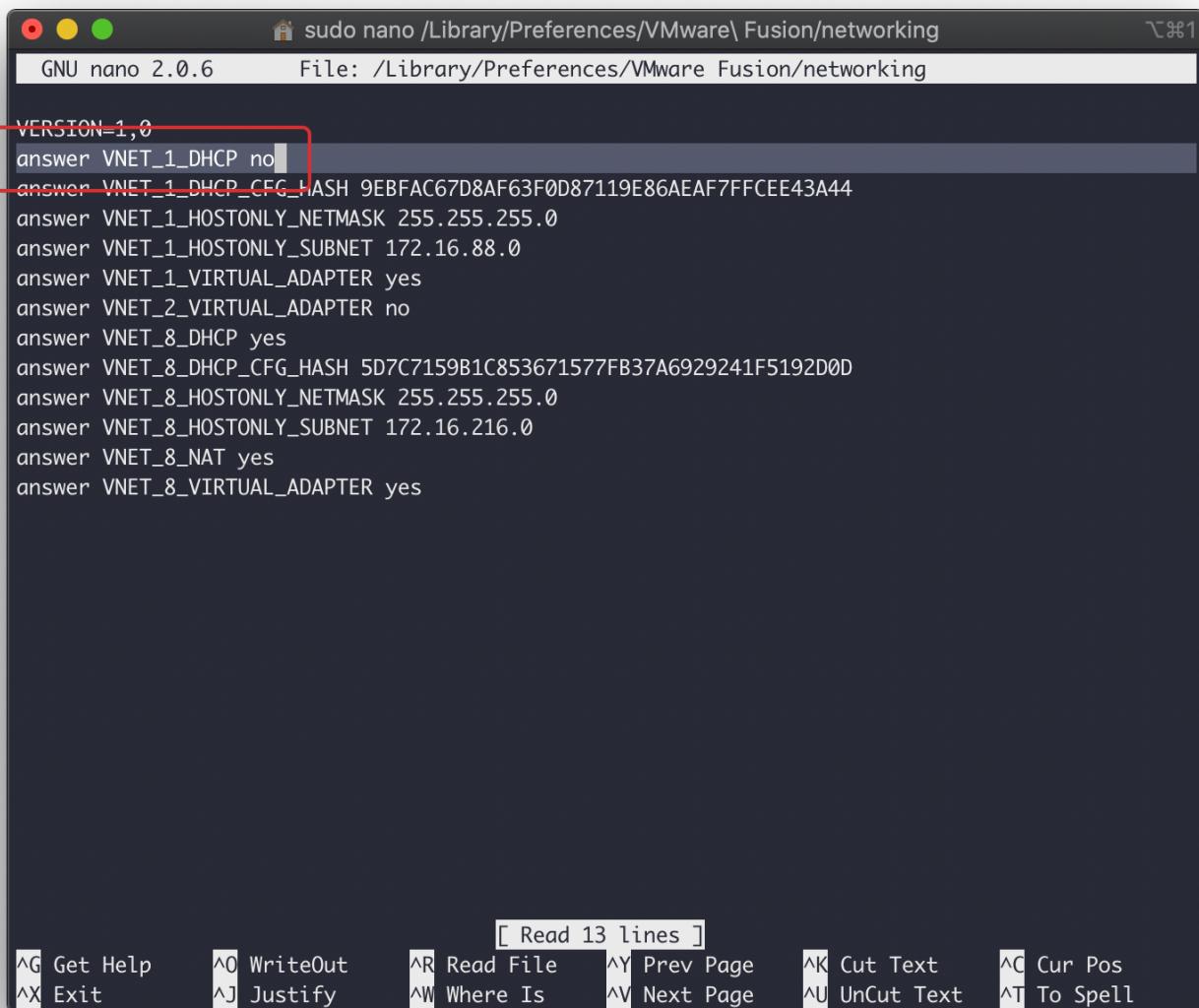


**3 g. Cấu hình một máy ảo khác (Windows 7, Windows Server 2003, ...) làm DHCP Client.**  
**Thiết lập Card Mạng của máy ảo này là Host-Only.**



### 3 h. Tắt tính năng DHCP của phần mềm VMWare

Tắt tính năng DHCP của phần mềm VMWare Fusion 11.5.0 trên macOS 10.15.5



```
sudo nano /Library/Preferences/VMware\ Fusion/networking
GNU nano 2.0.6      File: /Library/Preferences/VMware Fusion/networking

VERSION=1,0
answer VNET_1_DHCP no
answer VNET_1_DHCP_CFG_HASH 9EBFAC67D8AF63F0D87119E86AEAF7FFCEE43A44
answer VNET_1_HOSTONLY_NETMASK 255.255.255.0
answer VNET_1_HOSTONLY_SUBNET 172.16.88.0
answer VNET_1_VIRTUAL_ADAPTER yes
answer VNET_2_VIRTUAL_ADAPTER no
answer VNET_8_DHCP yes
answer VNET_8_DHCP_CFG_HASH 5D7C7159B1C853671577FB37A6929241F5192D0D
answer VNET_8_HOSTONLY_NETMASK 255.255.255.0
answer VNET_8_HOSTONLY_SUBNET 172.16.216.0
answer VNET_8_NAT yes
answer VNET_8_VIRTUAL_ADAPTER yes

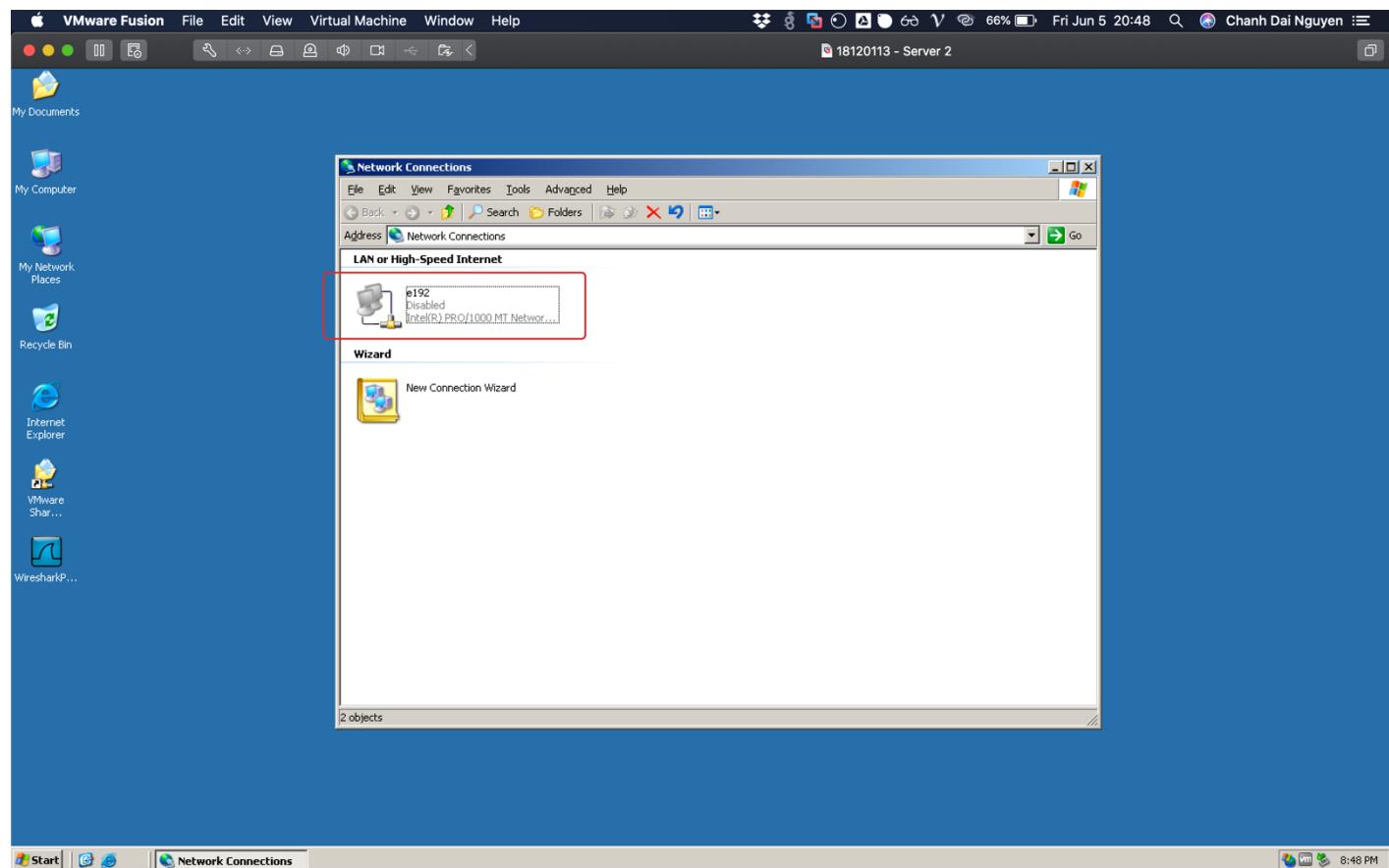
[ Read 13 lines ]
^G Get Help      ^O WriteOut     ^R Read File     ^Y Prev Page    ^K Cut Text     ^C Cur Pos
^X Exit         ^J Justify      ^W Where Is      ^V Next Page    ^U UnCut Text   ^T To Spell
```

### 3 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.

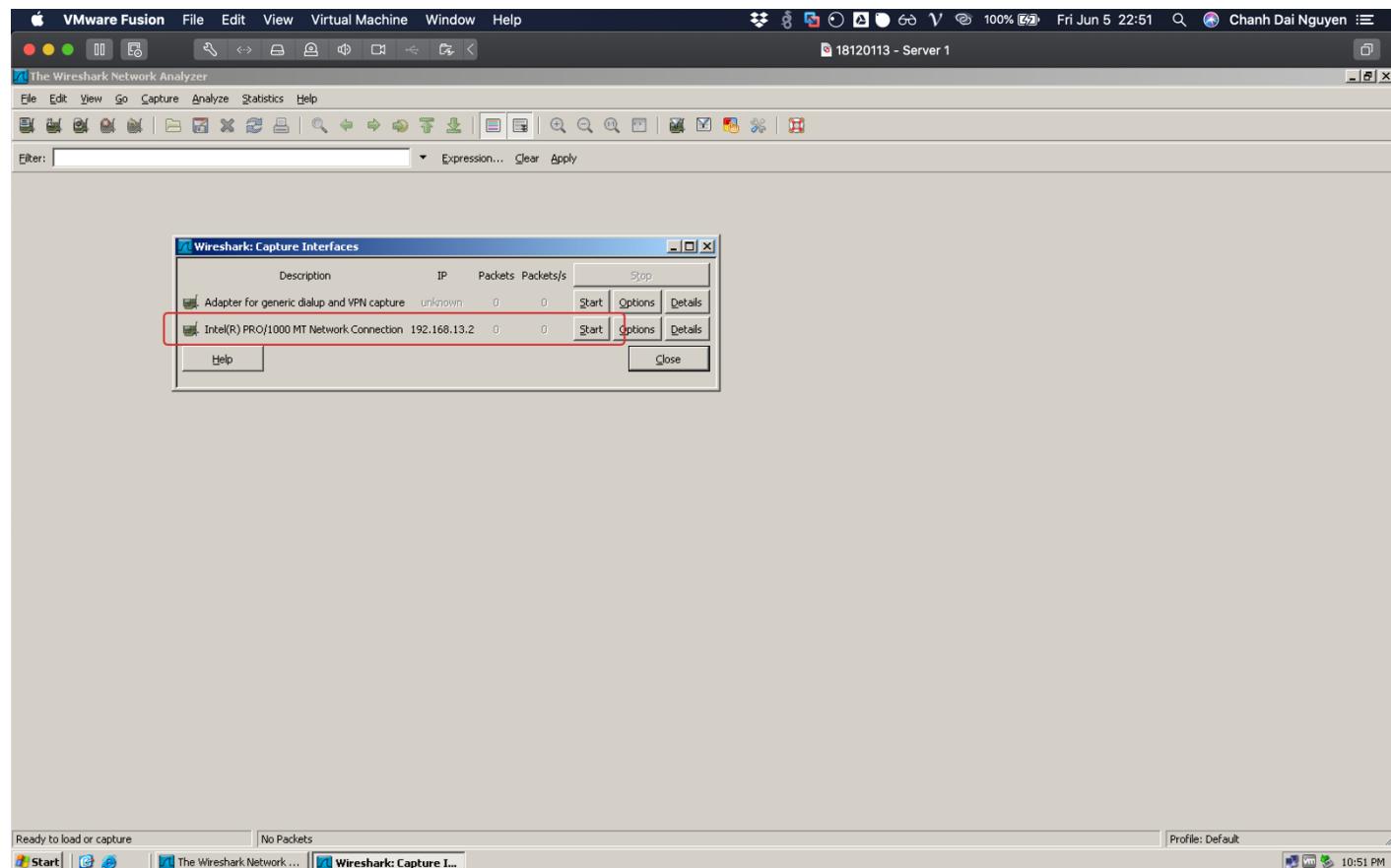
- Video quá trình thực hiện : <https://youtu.be/K6uOl8auPIA>

- Mô tả quá trình thực hiện :

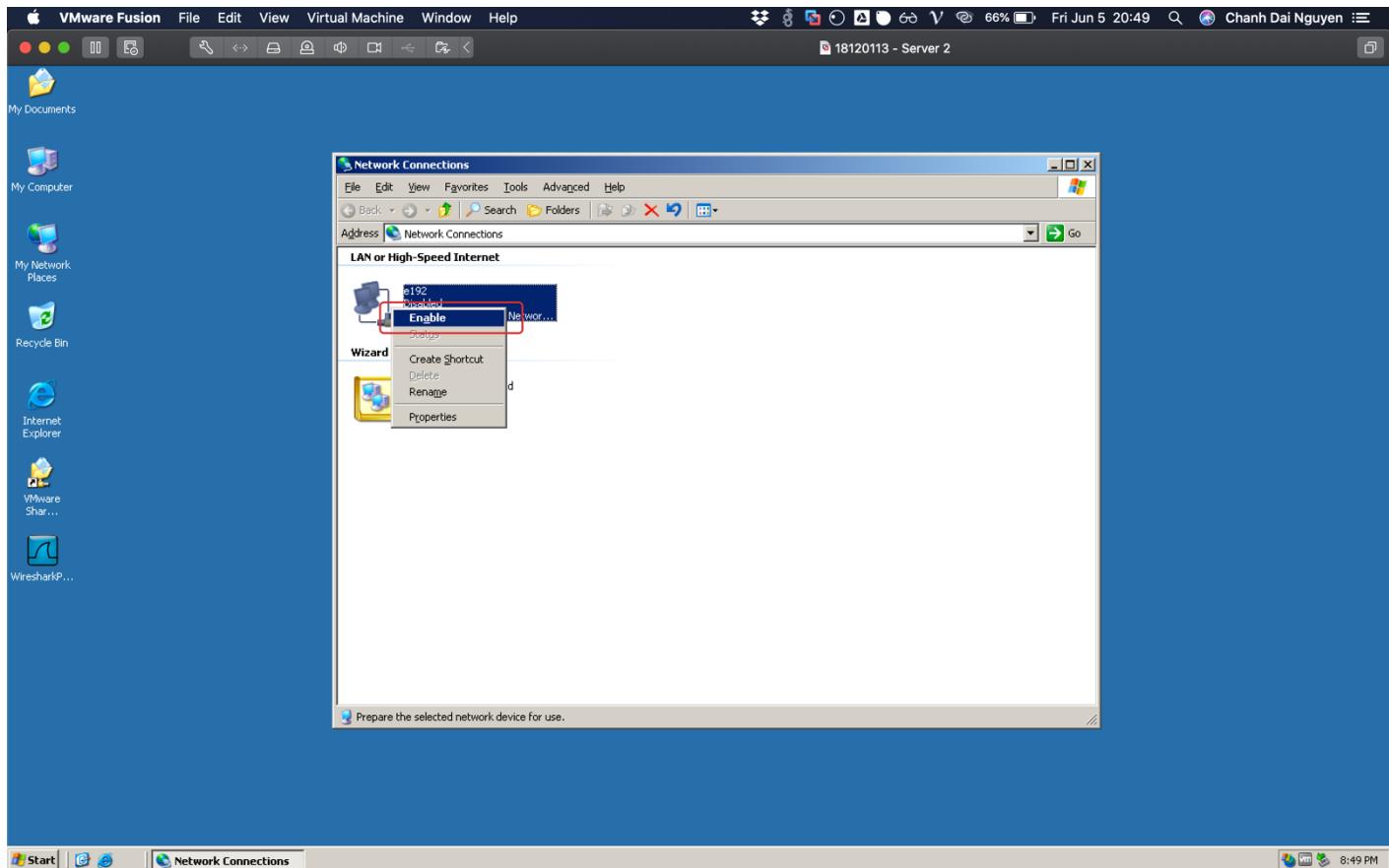
**Bước 1.** Tại DHCP Client (Server 2), Disable Card Mạng.



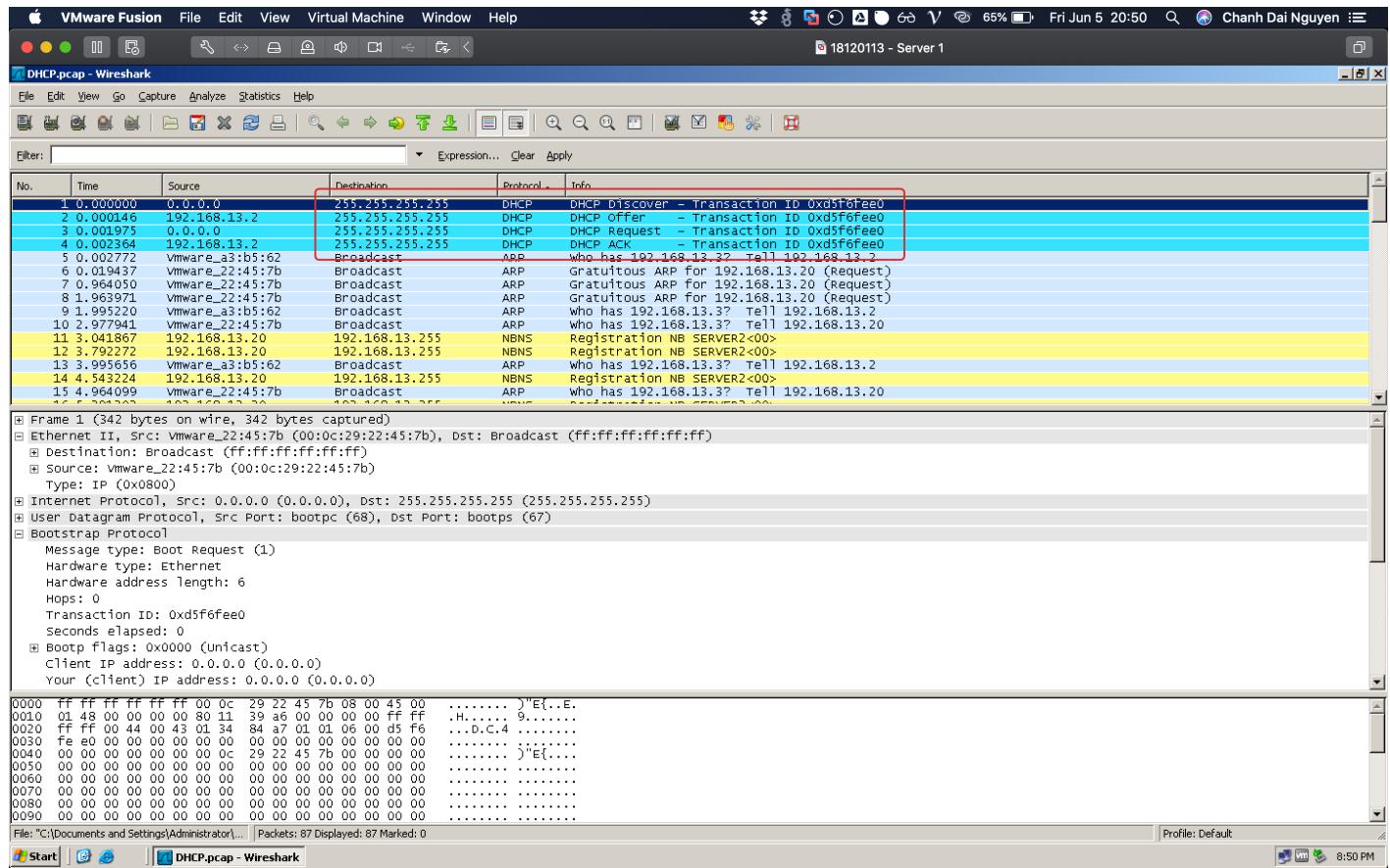
### Bước 2. Tại DHCP Server (Server 1), Start Capture.



Bước 3. Tại DHCP Client (Server 2), Enable lại Card Mạng để xin cấp phát địa chỉ IP.

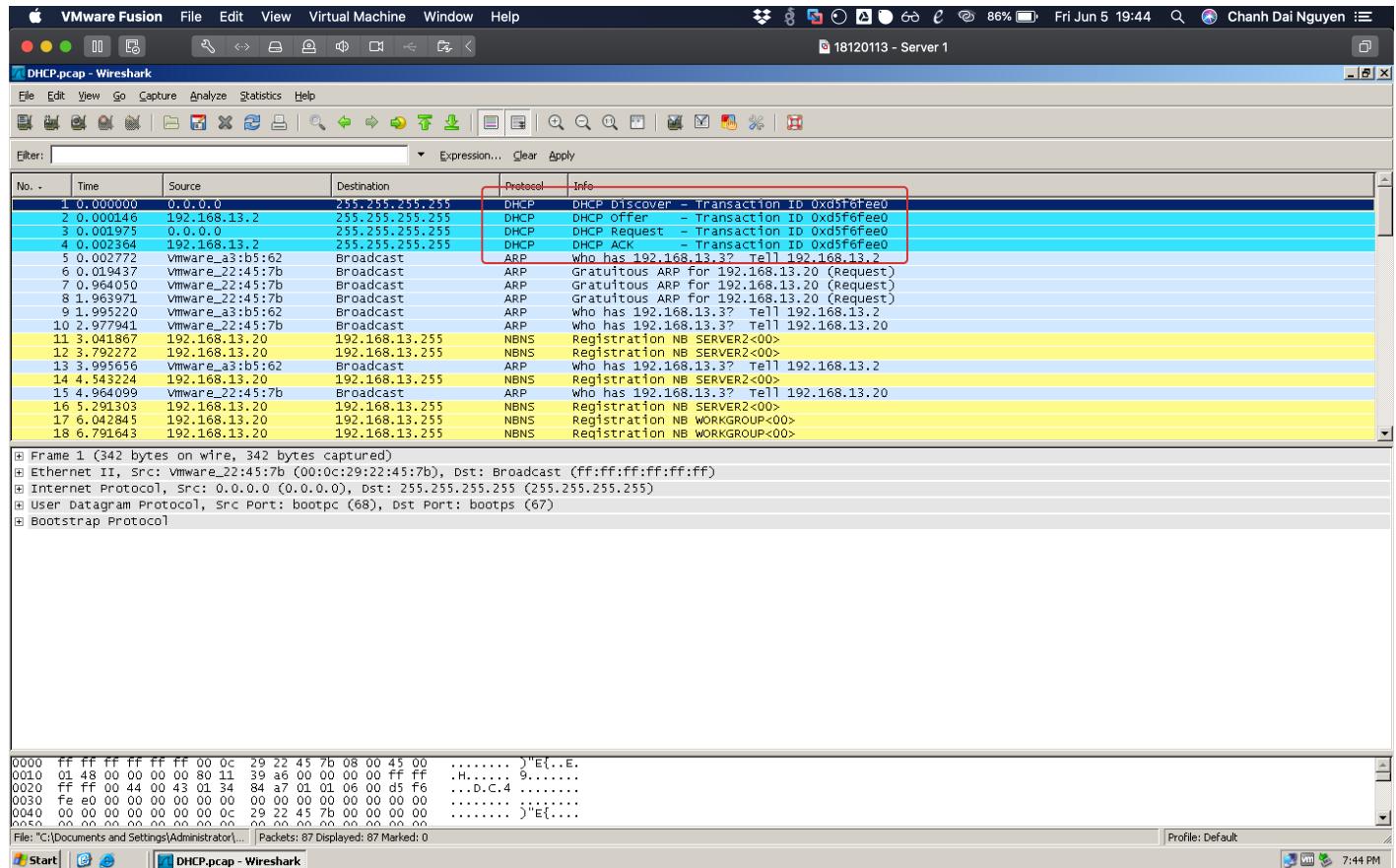


Bước 4. Tại DHCP Server (Server 1), Stop Capture và Xem kết quả.



### 3 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 : *Discover, Offer, Request, ACK.*



3 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 ?

Gói tin	Mục đích	IP Nguồn	IP Đích	MAC Nguồn	MAC Đích	Port Nguồn	Port Đích
Discover	Client tìm DHCP Server	0.0.0.0	255.255.255.255	00:0c:29:22:45:7b	ff:ff:ff:ff:ff:ff	68	67
Offer	DHCP gợi ý một địa chỉ IP	192.168.13.2	255.255.255.255	00:0c:29:a3:b5:62	ff:ff:ff:ff:ff:ff	67	68
Request	Client yêu cầu cấp 1 địa chỉ IP	0.0.0.0	255.255.255.255	00:0c:29:22:45:7b	ff:ff:ff:ff:ff:ff	68	67
ACK	Server xác nhận đồng ý và giải phóng địa chỉ IP	192.168.13.2	255.255.255.255	00:0c:29:a3:b5:62	ff:ff:ff:ff:ff:ff	67	68

## Bài Tập Thực Hành Wireshark

**18120113\_DHCPCap - Wireshark**

**Discover**

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xd0f5fe00
2	0.000146	192.168.13.2	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0xd0f5fe00
3	0.001975	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xd0f5fe00
4	0.002100	192.168.13.2	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0xd0f5fe00
5	0.002772	Vmware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2
6	0.019437	Vmware_22:45:7b	Broadcast	ARP	Gratuitous ARP For 192.168.13.20 (Request)
7	0.064050	Vmware_22:45:7b	Broadcast	ARP	Gratuitous ARP For 192.168.13.20 (Request)
8	0.095520	Vmware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2
9	1.095520	Vmware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2
10	2.977941	Vmware_22:45:7b	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.20
11	3.041867	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
12	3.179235	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
13	3.298656	Vmware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2
14	4.543224	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
15	4.964094	Vmware_22:45:7b	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.20
16	5.291303	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
17	5.391303	192.168.13.20	192.168.13.255	NBNS	Registration NB WORKGROUP<00>
18	6.791643	192.168.13.20	192.168.13.255	NBNS	Registration NB WORKGROUP<00>
19	6.963379	Vmware_22:45:7b	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.20
20	7.334359	172.16.88.1	172.16.88.255	UDP	source port: 17500 destination port: 17500
21	7.341744	192.168.13.20	192.168.13.255	NBNS	Registration NB WORKGROUP<00>
22	7.995894	Vmware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2

Frame 1 (342 bytes on wire, 342 bytes captured)  
 Ethernet II, Src: Vmware\_22:45:7b (00:0c:29:22:45:7b), Dst: Broadcast (ff:ff:ff:ff:ff:ff) **MAC Address IP MAC Address Port**  
 Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)  
 User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)  
 Bootstrap Protocol

Frame 2 (342 bytes on wire, 342 bytes captured)  
 Ethernet II, Src: Vmware\_a3:b5:62 (00:0c:29:a3:b5:62), Dst: Broadcast (ff:ff:ff:ff:ff:ff) **MAC Address IP MAC Address Port**  
 Internet Protocol Version 4, Src: 192.168.13.2 (192.168.13.2), Dst: 255.255.255.255 (255.255.255.255)  
 User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68) **IP**  
 Bootstrap Protocol

**Request**

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xd5f5fe00
2	0.000146	192.168.13.2	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0xd5f5fe00
3	0.001975	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xd5f5fe00
4	0.002100	192.168.13.2	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0xd5f5fe00
5	0.002772	Vmware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2
6	0.019437	Vmware_22:45:7b	Broadcast	ARP	Gratuitous ARP For 192.168.13.20 (Request)
7	0.064050	Vmware_22:45:7b	Broadcast	ARP	Gratuitous ARP For 192.168.13.20 (Request)
8	0.095520	Vmware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2
9	1.095520	Vmware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2
10	2.977941	Vmware_22:45:7b	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.20
11	3.041867	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
12	3.179235	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
13	3.298656	Vmware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2
14	4.543224	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
15	4.964094	Vmware_22:45:7b	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.20
16	5.291303	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
17	5.391303	192.168.13.20	192.168.13.255	NBNS	Registration NB WORKGROUP<00>
18	6.791643	192.168.13.20	192.168.13.255	NBNS	Registration NB WORKGROUP<00>
19	6.963379	Vmware_22:45:7b	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.20
20	7.334359	172.16.88.1	172.16.88.255	UDP	source port: 17500 destination port: 17500
21	7.341744	192.168.13.20	192.168.13.255	NBNS	Registration NB WORKGROUP<00>
22	7.995894	Vmware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2

Frame 3 (363 bytes on wire, 363 bytes captured)  
 Ethernet II, Src: Vmware\_22:45:7b (00:0c:29:22:45:7b), Dst: Broadcast (ff:ff:ff:ff:ff:ff) **MAC Address IP MAC Address Port**  
 Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)  
 User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)  
 Bootstrap Protocol

Frame 4 (342 bytes on wire, 342 bytes captured)  
 Ethernet II, Src: Vmware\_a3:b5:62 (00:0c:29:a3:b5:62), Dst: Broadcast (ff:ff:ff:ff:ff:ff) **MAC Address IP MAC Address Port**  
 Internet Protocol Version 4, Src: 192.168.13.2 (192.168.13.2), Dst: 255.255.255.255 (255.255.255.255)  
 User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)  
 Bootstrap Protocol

**ACK**

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xd5f5fe00
2	0.000146	192.168.13.2	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0xd5f5fe00
3	0.001975	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xd5f5fe00
4	0.002100	192.168.13.2	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0xd5f5fe00
5	0.002772	Vmware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2
6	0.019437	Vmware_22:45:7b	Broadcast	ARP	Gratuitous ARP For 192.168.13.20 (Request)
7	0.064050	Vmware_22:45:7b	Broadcast	ARP	Gratuitous ARP For 192.168.13.20 (Request)
8	0.095520	Vmware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2
9	1.095520	Vmware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2
10	2.977941	Vmware_22:45:7b	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.20
11	3.041867	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
12	3.179235	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
13	3.298656	Vmware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2
14	4.543224	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
15	4.964094	Vmware_22:45:7b	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.20
16	5.291303	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
17	5.391303	192.168.13.20	192.168.13.255	NBNS	Registration NB WORKGROUP<00>
18	6.791643	192.168.13.20	192.168.13.255	NBNS	Registration NB WORKGROUP<00>
19	6.963379	Vmware_22:45:7b	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.20
20	7.334359	172.16.88.1	172.16.88.255	UDP	source port: 17500 destination port: 17500
21	7.341744	192.168.13.20	192.168.13.255	NBNS	Registration NB WORKGROUP<00>
22	7.995894	Vmware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2

Frame 5 (363 bytes on wire, 363 bytes captured)  
 Ethernet II, Src: Vmware\_22:45:7b (00:0c:29:22:45:7b), Dst: Broadcast (ff:ff:ff:ff:ff:ff) **MAC Address IP MAC Address Port**  
 Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)  
 User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)  
 Bootstrap Protocol

Frame 6 (342 bytes on wire, 342 bytes captured)  
 Ethernet II, Src: Vmware\_a3:b5:62 (00:0c:29:a3:b5:62), Dst: Broadcast (ff:ff:ff:ff:ff:ff) **MAC Address IP MAC Address Port**  
 Internet Protocol Version 4, Src: 192.168.13.2 (192.168.13.2), Dst: 255.255.255.255 (255.255.255.255)  
 User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)  
 Bootstrap Protocol

File: "C:\Documents and Settings\Administrator\..." Packets: 87 Deployed: 87 Marked: 0  
 Start | Stop | File | Edit | View | Virtual Machine | Window | Help | 18120113\_DHCPCap... 2:53 PM

### 3.1. Thông tin Default Gateway và DNS Server nằm trong gói tin nào ?

Thông tin Default Gateway và DNS Server nằm trong gói tin Offer và ACK.

The screenshot shows a sequence of 18 network packets captured in VMware Fusion. The traffic is between a client (VMware\_a3:b5:62) and a server (VMware\_22:45:7b). The client initiates a DHCP Discover request (packet 1), followed by a DHCP Offer from the server (packet 2). The client then sends a DHCP Request (packet 3) and receives a DHCP ACK (packet 4) from the server. Subsequent packets show ARP requests and responses for broadcast addresses. The packet details pane shows the DHCP options sent in the ACK, including the Client Fully Qualified Domain Name (option 128) and the Router (option 3). The bytes pane displays the raw hex and ASCII data for the selected ACK packet.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xd5f6fee0
2	0.000146	192.168.13.2	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0xd5f6fee0
3	0.001975	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xd5f6fee0
4	0.002364	192.168.13.2	255.255.255.255	DHCP	DHCP ACK - Transaction ID 0xd5f6fee0
5	0.002772	VMware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2
6	0.019437	VMware_22:45:7b	Broadcast	ARP	Gratuitous ARP for 192.168.13.20 (Request)
7	0.964050	VMware_22:45:7b	Broadcast	ARP	Gratuitous ARP for 192.168.13.20 (Request)
8	1.963971	VMware_22:45:7b	Broadcast	ARP	Gratuitous ARP for 192.168.13.20 (Request)
9	1.995220	VMware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2
10	2.977941	VMware_22:45:7b	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.20
11	3.041867	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
12	3.792272	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
13	3.995656	VMware_a3:b5:62	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.2
14	4.543224	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
15	4.964099	VMware_22:45:7b	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.20
16	5.291303	192.168.13.20	192.168.13.255	NBNS	Registration NB SERVER2<00>
17	6.042845	192.168.13.20	192.168.13.255	NBNS	Registration NB WORKGROUP<00>
18	6.791643	192.168.13.20	192.168.13.255	NBNS	Registration NB WORKGROUP<00>

```

Your (client) IP address: 192.168.13.20 (192.168.13.20)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: VMware_22:45:7b (00:0c:29:22:45:7b)
Server host name not given
Boot file name not given
Magic cookie: (ok)
⊕ Option: (t=53, l=1) DHCP Message Type = DHCP ACK
⊕ Option: (t=58, l=4) Renewal Time Value = 6 days, 12 hours
⊕ Option: (t=59, l=4) Rebinding Time Value = 11 days, 9 hours
⊕ Option: (t=51, l=4) IP Address Lease Time = 13 days
⊕ Option: (t=54, l=4) Server Identifier = 192.168.13.2
⊕ Option: (t=1, l=4) Subnet Mask = 255.255.255.0
⊕ Option: (t=128, l=3) Client Fully qualified domain name
⊕ Option: (t=3, l=4) Router = 192.168.13.1
⊕ Option: (t=6, l=4) Domain Name Server = 192.168.13.3
End option
Padding
0120 08 99 c0 3b 04 00 0e ff 10 33 04 00 11 23 80 36 . . . . . . . . .
0130 04 c0 a8 0d 02 01 04 ff ff ff 00 51 03 00 ff ff . . . . . . Q . .
0140 03 04 c0 a8 0d 01 06 04 c0 a8 0d 03 ff 00 00 00 . . . . . . . .
0150 00 00 00 00 00 00 00 . . . . . . . .

```

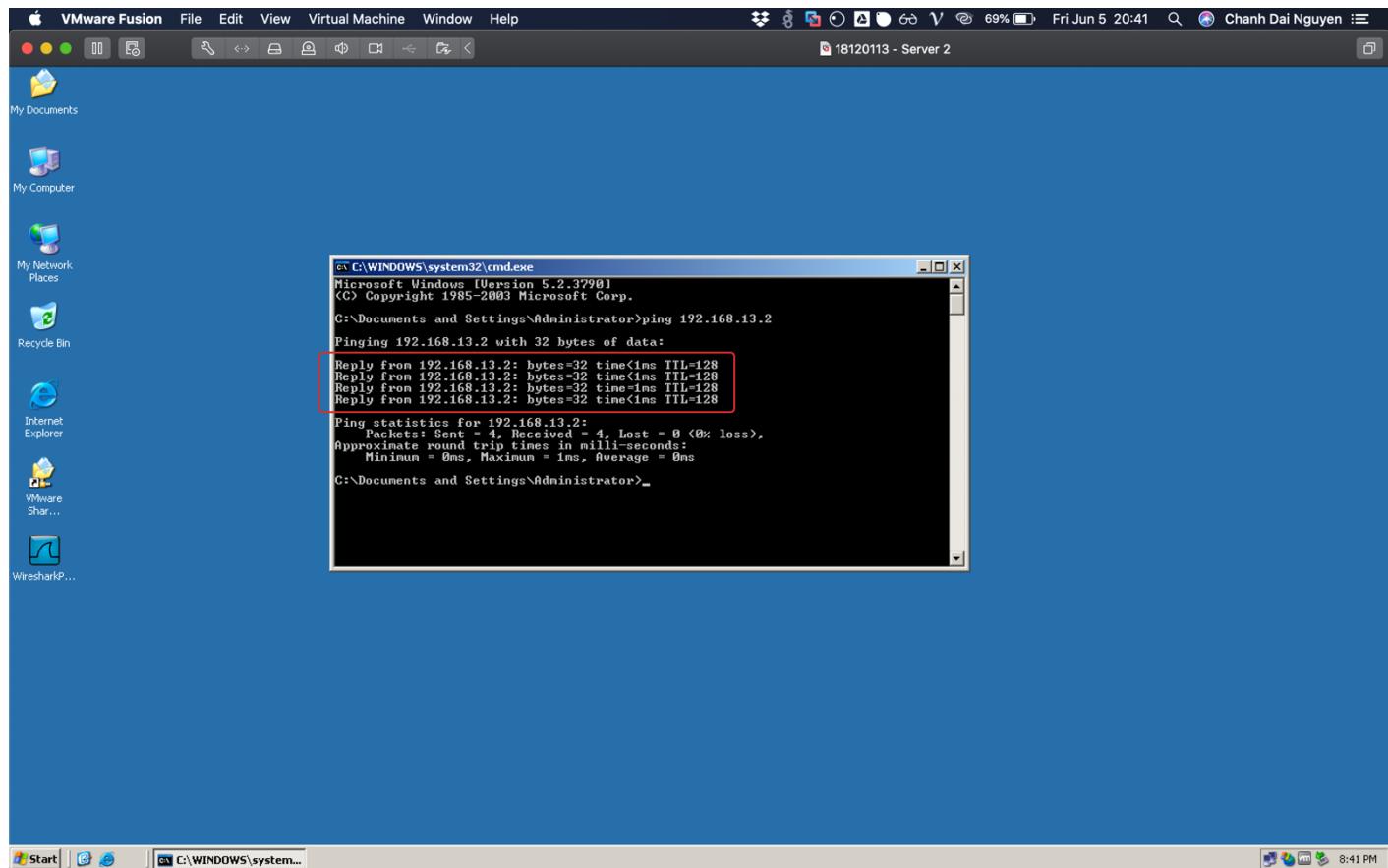
Text item ( ), 6 bytes      Packets: 87 Displayed: 87 Marked: 0      Profile: Default

Start | DHCP.pcap - Wireshark      7:46 PM

**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 :**

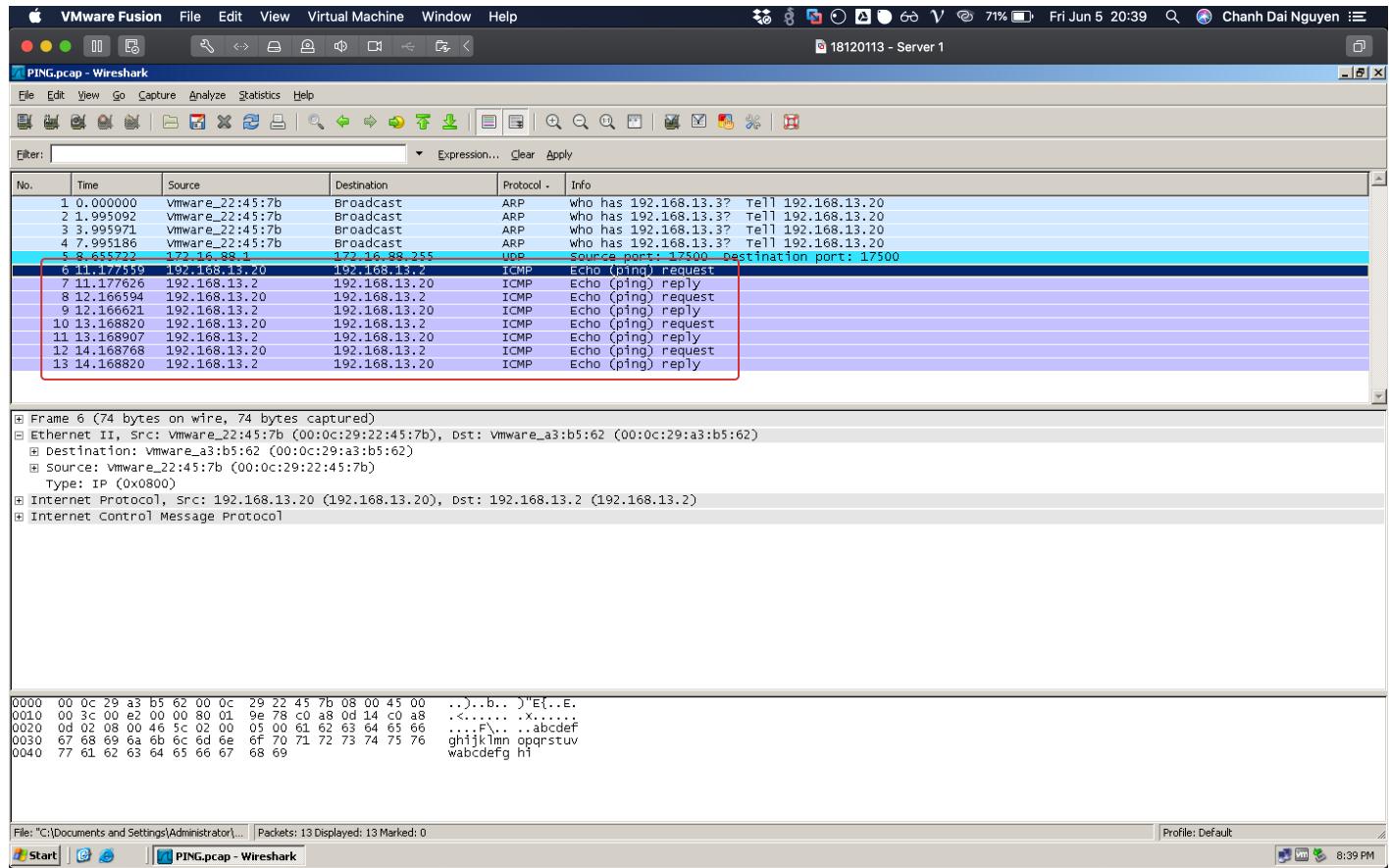
### 4 a. Thực hiện lệnh ping từ Client đến Server và dùng Wireshark để bắt các gói tin tương ứng.

Video quá trình thực hiện : <https://youtu.be/XVpPsWX879w>



### 4 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.



## Bài Tập Thực Hành Wireshark

### 4 c. Địa chỉ MAC Nguồn, MAC Đích là gì ?

MAC Nguồn

00:0c:29:22:45:7b

MAC Đích

00:0c:29:a3:b5:62

The screenshot shows a Wireshark capture of a ping exchange between two hosts. The packet list pane shows 13 ICMP Echo requests and replies. The details pane shows the packet structure, with the source and destination MAC addresses highlighted in red. The bytes pane shows the raw hex and ASCII data of the packet.

Packet List:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Vmware_22:45:7b	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.20
2	1.005092	Vmware_22:45:7b	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.20
3	3.995971	Vmware_22:45:7b	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.20
4	7.995186	Vmware_22:45:7b	Broadcast	ARP	who has 192.168.13.3? Tell 192.168.13.20
5	8.655722	172.16.88.1	172.16.88.255	UDP	Source port: 17500 Destination port: 17500
6	11.177559	192.168.13.20	192.168.13.2	ICMP	Echo (ping) request
7	11.177626	192.168.13.2	192.168.13.20	ICMP	Echo (ping) reply
8	12.166594	192.168.13.20	192.168.13.2	ICMP	Echo (ping) request
9	12.166621	192.168.13.20	192.168.13.20	ICMP	Echo (ping) reply
10	13.168820	192.168.13.20	192.168.13.2	ICMP	Echo (ping) request
11	13.168907	192.168.13.2	192.168.13.20	ICMP	Echo (ping) reply
12	14.168768	192.168.13.20	192.168.13.2	ICMP	Echo (ping) request
13	14.168820	192.168.13.20	192.168.13.2	ICMP	Echo (ping) reply

Details:

```
% Frame 6 (74 bytes on wire, 74 bytes captured)
% Ethernet II Src: Vmware_22:45:7b (00:0c:29:22:45:7b), Dst: Vmware_a3:b5:62 (00:0c:29:a3:b5:62)
  Destination: Vmware_a3:b5:62 (00:0c:29:a3:b5:62)
  Source: Vmware_22:45:7b (00:0c:29:22:45:7b)
    Type: IP (0x0800)
  Internet Protocol Version 4, Src: 192.168.13.20 (192.168.13.20), Dst: 192.168.13.2 (192.168.13.2)
  Internet Control Message Protocol
```

Bytes:

```
0000  00 0c 29 a3 b5 62 00 0c 29 22 45 7b 08 00 45 00 ..).b.. )"E{..E.
0010  00 3c 00 e2 40 00 80 01 9e 78 c0 a8 00 14 c0 a8 <..... .x.....
0020  00 02 08 00 46 3c 02 00 05 00 61 62 63 64 65 66 ..abcdeF
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghiijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69 wabcdefg hI
```

Bottom Status Bar:

Destination Hardware Address (eth.dst), 6 bytes | Packets: 13 Displayed: 13 Marked: 0 | Profile: Default | Start | Stop | PING.pcap - Wireshark | 8:20 PM

## Bài Tập Thực Hành Wireshark

### 4 d. Địa chỉ IP Nguồn, IP Đích là gì ?

IP Nguồn

192.168.13.20

IP Đích

192.168.13.2

The screenshot shows a Wireshark session titled "PING.pcap - Wireshark". The packet list pane displays 13 ICMP Echo requests and replies. The selected packet (Frame 6) is highlighted in blue. The details pane shows the ICMP header fields: Version: 4, Header length: 20 bytes, Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00), Total Length: 60, Identification: 0xe0e2 (226), Flags: 0x00, Fragment offset: 0, Time to Live: 128, Protocol: ICMP (0x01). The source and destination addresses are 192.168.13.20 and 192.168.13.2 respectively. The bytes pane shows the raw hex and ASCII data of the ICMP frame.

Frame 6 (74 bytes on wire, 74 bytes captured)  
Ethernet II, Src: VMware\_22:45:7b (00:0c:29:22:45:7b), Dst: VMware\_a3:b5:62 (00:0c:29:a3:b5:62)  
Internet Protocol, Src: 192.168.13.20 (192.168.13.20), Dst: 192.168.13.2 (192.168.13.2)  
Version: 4  
Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)  
Total Length: 60  
Identification: 0xe0e2 (226)  
Flags: 0x00  
Fragment offset: 0  
Time to Live: 128  
Protocol: ICMP (0x01)  
Header checksum: 0x9e78 [correct]  
Source: 192.168.13.20 (192.168.13.20)  
Destination: 192.168.13.2 (192.168.13.2)  
Internet Control Message Protocol

Source (ip.src), 4 bytes  
Packets: 13 Displayed: 13 Marked: 0  
Profile: Default  
Start | Stop | Reload | PING.pcap - Wireshark | 8:19 PM

## Bài Tập Thực Hành Wireshark

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

Data của gói tin ICMP : 6162636465666768696A6B6C6D6E6F707172737475767761...

The screenshot shows the Wireshark interface with several network packets listed in the main pane. The 13th packet is highlighted in blue and selected. The details pane shows the ICMP header and payload. A red box highlights the "Data (32 bytes)" section, which contains the hex dump of the payload: 0000 00 0c 29 a3 b5 62 00 0c 29 22 45 7b 08 00 45 00 ... .b.. )"E{..E. The bottom status bar also displays the hex dump: Data (data.data), 32 bytes.

Total Length: 60  
Identification: 0x00e2 (226)  
Flags: 0x00  
Fragment offset: 0  
Time to live: 128  
Protocol: ICMP (0x01)  
Header checksum: 0x9e78 [correct]  
Source: 192.168.13.20 (192.168.13.20)  
Destination: 192.168.13.2 (192.168.13.2)  
Internet Control Message Protocol  
Type: 8 (Echo (ping) request)  
Code: 0 ()  
Checksum: 0x465c [correct]  
Identifier: 0x0200  
Sequence number: 1280 (0x0500)  
Data (32 bytes)  
Data: 6162636465666768696A6B6C6D6E6F707172737475767761...

0000 00 0c 29 a3 b5 62 00 0c 29 22 45 7b 08 00 45 00 ... .b.. )"E{..E.  
0010 00 3c 00 e2 00 00 80 01 9e 78 c0 a8 0d 14 c0 a8 .<..... x.....  
0020 00 02 08 00 46 5c 00 00 05 00 61 62 63 64 65 66 ...F\..... abcdef  
0030 67 68 69 6a 60 6c 66 67 6f 70 71 72 73 74 75 76 ghiijklm opqrstuvwxyz  
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

--- Hết ---