

Bài tập thực hành Wireshark

MSSV: 18120444

Họ và tên: Dương Thành Long

Lớp: MMT 18_4

Câu 1:

a. Username và password của người dùng là gì?

➔ Username: 07cm

➔ Password: 654321

3 0.005723	10.0.0.1	10.0.0.123	TCP	60 49728 → ftp(21) [ACK] Seq=1 Ack=1 Win=8192 Len=0
4 0.024081	10.0.0.123	10.0.0.1	FTP	103 Response: 220 Serv-U FTP Server v6.3 for WinSock ready...
5 0.215259	10.0.0.1	10.0.0.123	TCP	60 49728 → ftp(21) [ACK] Seq=1 Ack=50 Win=8143 Len=0
6 4.932741	10.0.0.1	10.0.0.123	FTP	65 Request: USER 07cm
7 4.938077	10.0.0.123	10.0.0.1	FTP	90 Response: 331 User name okay, need password.
8 5.130926	10.0.0.1	10.0.0.123	TCP	60 49728 → ftp(21) [ACK] Seq=12 Ack=86 Win=8107 Len=0
9 8.403728	10.0.0.1	10.0.0.123	FTP	67 Request: PASS 654321
10 8.404645	10.0.0.123	10.0.0.1	FTP	84 Response: 230 User logged in, proceed.
11 8.598152	10.0.0.1	10.0.0.123	TCP	60 49728 → ftp(21) [ACK] Seq=25 Ack=116 Win=8077 Len=0

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

3 0.005723	10.0.0.1	10.0.0.123	TCP	60 49728 → ftp(21) [ACK] Seq=1 Ack=1 Win=8192 Len=0
4 0.024081	10.0.0.123	10.0.0.1	FTP	103 Response: 220 Serv-U FTP Server v6.3 for WinSock ready...
5 0.215259	10.0.0.1	10.0.0.123	TCP	60 49728 → ftp(21) [ACK] Seq=1 Ack=50 Win=8143 Len=0
6 4.932741	10.0.0.1	10.0.0.123	FTP	65 Request: USER 07cm
7 4.938077	10.0.0.123	10.0.0.1	FTP	90 Response: 331 User name okay, need password.
8 5.130926	10.0.0.1	10.0.0.123	TCP	60 49728 → ftp(21) [ACK] Seq=12 Ack=86 Win=8107 Len=0
9 8.403728	10.0.0.1	10.0.0.123	FTP	67 Request: PASS 654321
10 8.404645	10.0.0.123	10.0.0.1	FTP	84 Response: 230 User logged in, proceed.
11 8.598152	10.0.0.1	10.0.0.123	TCP	60 49728 → ftp(21) [ACK] Seq=25 Ack=116 Win=8077 Len=0

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

➔ Mode active

63	25.253959	10.0.0.1	10.0.0.123	FTP	76	Request: PORT 10,0,0,1,194,69
64	25.253959	10.0.0.1	10.0.0.123	FTP	76	Request: PORT 10,0,0,1,194,69
65	25.254698	10.0.0.123	10.0.0.1	FTP	84	Response: 200 PORT Command succe
66	25.257566	10.0.0.1	10.0.0.123	FTP	60	Request: LIST
67	25.260044	10.0.0.123	10.0.0.1	TCP	62	ftp-data(20) → 49733 [SYN] Seq=
68	25.260306	10.0.0.1	10.0.0.123	TCP	62	49733 → ftp-data(20) [SYN, ACK]
69	25.260488	10.0.0.123	10.0.0.1	TCP	54	ftp-data(20) → 49733 [ACK] Seq=
70	25.261565	10.0.0.123	10.0.0.1	FTP-DA...	1514	FTP Data: 1460 bytes (PORT) (LIS
71	25.261830	10.0.0.123	10.0.0.1	FTP-DA...	264	FTP Data: 210 bytes (PORT) (LIST
72	25.261941	10.0.0.1	10.0.0.123	TCP	60	49733 → ftp-data(20) [ACK] Seq=
73	25.262079	10.0.0.123	10.0.0.1	TCP	54	ftp-data(20) → 49733 [FIN, ACK]
74	25.262183	10.0.0.1	10.0.0.123	TCP	60	49733 → ftp-data(20) [ACK] Seq=
75	25.262435	10.0.0.123	10.0.0.1	FTP	107	Response: 150 Opening ASCII mode
76	25.272864	10.0.0.1	10.0.0.123	TCP	60	49733 → ftp-data(20) [FIN, ACK]

> Frame 64: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
> Ethernet II, Src: VMware_c0:00:01 (00:50:56: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: 10.0.0.123 (10.0.0.123)
> Transmission Control Protocol, Src Port: 49728 (49728), Dst Port: ftp (21), Seq: 25, Ack: 116, Len: 22
✓ File Transfer Protocol (FTP)
 ✓ PORT 10,0,0,1,194,69\r\n
 Request command: PORT
 Request arg: 10,0,0,1,194,69
 Active IP address: 10.0.0.1 (10.0.0.1)
 Active port: 49733
[Current working directory:]
[Command: LIST]
[\[Command frame: 66\]](#)

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

➔ Port FTP Server: 20

➔ Port FTP Client: 49733

69	25.260488	10.0.0.123	10.0.0.1	TCP	54 ftp-data(20) → 49733 [ACK] Seq=1 Ack=1 Win=6
70	25.261565	10.0.0.123	10.0.0.1	FTP-DA...	1514 FTP Data: 1460 bytes (PORT) (LIST)
71	25.261830	10.0.0.123	10.0.0.1	FTP-DA...	264 FTP Data: 210 bytes (PORT) (LIST)
72	25.261941	10.0.0.1	10.0.0.123	TCP	60 49733 → ftp-data(20) [ACK] Seq=1 Ack=1671 Wi
73	25.262079	10.0.0.123	10.0.0.1	TCP	54 ftp-data(20) → 49733 [FIN, ACK] Seq=1671 Ack
74	25.262183	10.0.0.1	10.0.0.123	TCP	60 49733 → ftp-data(20) [ACK] Seq=1 Ack=1672 Wi
75	25.262435	10.0.0.123	10.0.0.1	FTP	107 Response: 150 Opening ASCII mode data connec
76	25.272864	10.0.0.1	10.0.0.123	TCP	60 49733 → ftp-data(20) [FIN, ACK] Seq=1 Ack=16
77	25.272939	10.0.0.123	10.0.0.1	TCP	54 ftp-data(20) → 49733 [ACK] Seq=1672 Ack=2 Wi
78	25.446114	10.0.0.1	10.0.0.123	TCP	60 49728 → ftp(21) [ACK] Seq=53 Ack=199 Win=799.
79	25.446310	10.0.0.123	10.0.0.1	FTP	78 Response: 226 Transfer complete.
80	25.643951	10.0.0.1	10.0.0.123	TCP	60 49728 → ftp(21) [ACK] Seq=53 Ack=223 Win=797
81	29.970669	10.0.0.1	10.0.0.255	NBNS	92 Name query NB 172.29.70.4<20>
82	30.736767	10.0.0.1	10.0.0.255	NBNS	92 Name query NB 172.29.70.4<20>

<

> Frame 71: 264 bytes on wire (2112 bits), 264 bytes captured (2112 bits)

> 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 Version 4, Src: 10.0.0.123 (10.0.0.123), Dst: 10.0.0.1 (10.0.0.1)

> Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: 49733 (49733), Seq: 1461, Ack: 1, Len: 210
FTP Data (210 bytes data)

[Setup frame: 64]

[Setup method: PORT]

[Command: LIST]

[Command frame: 66]

[Current working directory:]

▼ Line-based text data (4 lines)

uyengiao\r\n

drw-rw-rw- 1 user group 0 Jun 13 19:15 tailieukythuat\r\n

drw-rw-rw- 1 user group 0 Jun 13 18:10 tailieumat\r\n

Câu 2:

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

➔ FTP sử dụng giao thức TCP

No.	Time	Source	Destination	Protocol	Length	Info
9	11.431999	10.0.0.224	10.0.0.1	FTP	103	Response: 220 Serv-U FTP Server v6.3 for WinSock ready...
12	12.730270	10.0.0.1	10.0.0.224	FTP	70	Request: USER anonymous
13	12.731818	10.0.0.224	10.0.0.1	FTP	124	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	80	Request: PASS mozilla@example.com
15	12.849323	10.0.0.224	10.0.0.1	FTP	95	Response: 530 Sorry, no ANONYMOUS access allowed.
17	21.836141	10.0.0.1	10.0.0.224	FTP	65	Request: USER cm07
18	21.837661	10.0.0.224	10.0.0.1	FTP	90	Response: 331 User name okay, need password.
19	21.905232	10.0.0.1	10.0.0.224	FTP	67	Request: PASS 123654
20	21.906163	10.0.0.224	10.0.0.1	FTP	84	Response: 230 User logged in, proceed.
21	21.935646	10.0.0.1	10.0.0.224	FTP	60	Request: SYST
22	21.936236	10.0.0.224	10.0.0.1	FTP	73	Response: 215 UNIX Type: L8
23	21.953730	10.0.0.1	10.0.0.224	FTP	60	Request: PWD
24	21.954292	10.0.0.224	10.0.0.1	FTP	85	Response: 257 "/" is current directory.
25	21.955344	10.0.0.1	10.0.0.224	FTP	62	Request: TYPE I
26	21.955762	10.0.0.224	10.0.0.1	FTP	74	Response: 200 Type set to I.
27	21.956224	10.0.0.1	10.0.0.224	FTP	60	Request: PASV
28	21.968087	10.0.0.224	10.0.0.1	FTP	101	Response: 227 Entering Passive Mode (10,0,0,224,19,137)
29	21.984564	10.0.0.1	10.0.0.224	FTP	62	Request: SIZE /
30	21.985403	10.0.0.224	10.0.0.1	FTP	76	Response: 550 /: No such file.
33	21.986491	10.0.0.1	10.0.0.224	FTP	62	Request: MDTM /

> Frame 12: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: VMware_c0:00:01 (00:50:56: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: 1, Ack: 50, Len: 16
✓ File Transfer Protocol (FTP)
 USER anonymous\r\n

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

➔ Port mặc định của FTP Server kết nối là: 21

No.	Time	Source	Destination	Protocol	Length	Info
9	11.431999	10.0.0.224	10.0.0.1	FTP	103	Response: 220 Serv-U FTP Server v6.3 for WinSock ready...
12	12.730270	10.0.0.1	10.0.0.224	FTP	70	Request: USER anonymous
13	12.731818	10.0.0.224	10.0.0.1	FTP	124	Response: 331 User name okay, please send complete E-mail a
14	12.848222	10.0.0.1	10.0.0.224	FTP	80	Request: PASS mozilla@example.com
15	12.849323	10.0.0.224	10.0.0.1	FTP	95	Response: 530 Sorry, no ANONYMOUS access allowed.
17	21.836141	10.0.0.1	10.0.0.224	FTP	65	Request: USER cm07
18	21.837661	10.0.0.224	10.0.0.1	FTP	90	Response: 331 User name okay, need password.
19	21.905232	10.0.0.1	10.0.0.224	FTP	67	Request: PASS 123654
20	21.906163	10.0.0.224	10.0.0.1	FTP	84	Response: 230 User logged in, proceed.
21	21.935646	10.0.0.1	10.0.0.224	FTP	60	Request: SYST
22	21.936236	10.0.0.224	10.0.0.1	FTP	73	Response: 215 UNIX Type: L8
23	21.953730	10.0.0.1	10.0.0.224	FTP	60	Request: PWD
24	21.954292	10.0.0.224	10.0.0.1	FTP	85	Response: 257 "/" is current directory.
25	21.955344	10.0.0.1	10.0.0.224	FTP	62	Request: TYPE I
26	21.955762	10.0.0.224	10.0.0.1	FTP	74	Response: 200 Type set to I.
27	21.956224	10.0.0.1	10.0.0.224	FTP	60	Request: PASV
28	21.968087	10.0.0.224	10.0.0.1	FTP	101	Response: 227 Entering Passive Mode (10,0,0,224,19,137)
29	21.984564	10.0.0.1	10.0.0.224	FTP	62	Request: SIZE /
30	21.985403	10.0.0.224	10.0.0.1	FTP	76	Response: 550 /: No such file.
33	21.986491	10.0.0.1	10.0.0.224	FTP	62	Request: MDTM /

> Frame 12: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: VMware_c0:00:01 (00:50:56: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: 1, Ack: 50, Len: 16
✓ File Transfer Protocol (FTP)
 USER anonymous\r\n
 Request command: USER

c. Username và password của người dùng là gì?

➔ Người thứ 1(không có quyền truy cập)

Username: anonymous

Password: mozilla@example.com

➔ Người thứ 2:

Username là: cm07

Password là: 123654

ftp						
No.	Time	Source	Destination	Protocol	Length	Info
9	11.431999	10.0.0.224	10.0.0.1	FTP	103	Response: 220 Serv-U FTP Server v6.3 for WinSock ready...
12	12.730270	10.0.0.1	10.0.0.224	FTP	70	Request: USER anonymous
13	12.731818	10.0.0.224	10.0.0.1	FTP	124	Response: 331 User name okay, please send complete E-mail a
14	12.848222	10.0.0.1	10.0.0.224	FTP	80	Request: PASS mozilla@example.com
15	12.849323	10.0.0.224	10.0.0.1	FTP	95	Response: 530 Sorry, no ANONYMOUS access allowed.
17	21.836141	10.0.0.1	10.0.0.224	FTP	65	Request: USER cm07
18	21.837661	10.0.0.224	10.0.0.1	FTP	90	Response: 331 User name okay, need password.
19	21.905232	10.0.0.1	10.0.0.224	FTP	67	Request: PASS 123654
20	21.906163	10.0.0.224	10.0.0.1	FTP	84	Response: 230 User logged in, proceed.
21	21.935646	10.0.0.1	10.0.0.224	FTP	60	Request: SYST
22	21.936236	10.0.0.224	10.0.0.1	FTP	73	Response: 215 UNIX Type: L8
23	21.953730	10.0.0.1	10.0.0.224	FTP	60	Request: PWD
24	21.954292	10.0.0.224	10.0.0.1	FTP	85	Response: 257 "/" is current directory.
25	21.955344	10.0.0.1	10.0.0.224	FTP	62	Request: TYPE I
26	21.955762	10.0.0.224	10.0.0.1	FTP	74	Response: 200 Type set to I.
27	21.956224	10.0.0.1	10.0.0.224	FTP	60	Request: PASV
28	21.968087	10.0.0.224	10.0.0.1	FTP	101	Response: 227 Entering Passive Mode (10,0,0,224,19,137)
29	21.984564	10.0.0.1	10.0.0.224	FTP	62	Request: SIZE /
30	21.985403	10.0.0.224	10.0.0.1	FTP	76	Response: 550 /: No such file.
33	21.986491	10.0.0.1	10.0.0.224	FTP	62	Request: MDTM /

> Frame 12: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

> Ethernet II, Src: VMware_c0:00:01 (00:50:56: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: 1, Ack: 50, Len: 16

> File Transfer Protocol (FTP)

USER anonymous\r\nRequest command: USER

d. Port truyền lệnh của Client là bao nhiêu?

➔ Port truyền lệnh của Client là: 49788

ftp						
No.	Time	Source	Destination	Protocol	Length	Info
9	11.431999	10.0.0.224	10.0.0.1	FTP	103	Response: 220 Serv-U FTP Server v6.3 for WinSock ready...
12	12.730270	10.0.0.1	10.0.0.224	FTP	70	Request: USER anonymous
13	12.731818	10.0.0.224	10.0.0.1	FTP	124	Response: 331 User name okay, please send complete E-mail a
14	12.848222	10.0.0.1	10.0.0.224	FTP	80	Request: PASS mozilla@example.com
15	12.849323	10.0.0.224	10.0.0.1	FTP	95	Response: 530 Sorry, no ANONYMOUS access allowed.
17	21.836141	10.0.0.1	10.0.0.224	FTP	65	Request: USER cm07
18	21.837661	10.0.0.224	10.0.0.1	FTP	90	Response: 331 User name okay, need password.
19	21.905232	10.0.0.1	10.0.0.224	FTP	67	Request: PASS 123654
20	21.906163	10.0.0.224	10.0.0.1	FTP	84	Response: 230 User logged in, proceed.
21	21.935646	10.0.0.1	10.0.0.224	FTP	60	Request: SYST
22	21.936236	10.0.0.224	10.0.0.1	FTP	73	Response: 215 UNIX Type: L8
23	21.953730	10.0.0.1	10.0.0.224	FTP	60	Request: PWD
24	21.954292	10.0.0.224	10.0.0.1	FTP	85	Response: 257 "/" is current directory.
25	21.955344	10.0.0.1	10.0.0.224	FTP	62	Request: TYPE I
26	21.955762	10.0.0.224	10.0.0.1	FTP	74	Response: 200 Type set to I.
27	21.956224	10.0.0.1	10.0.0.224	FTP	60	Request: PASV
28	21.968087	10.0.0.224	10.0.0.1	FTP	101	Response: 227 Entering Passive Mode (10,0,0,224,19,137)
29	21.984564	10.0.0.1	10.0.0.224	FTP	62	Request: SIZE /
30	21.985403	10.0.0.224	10.0.0.1	FTP	76	Response: 550 /: No such file.
33	21.986491	10.0.0.1	10.0.0.224	FTP	62	Request: MDTM /

> Frame 12: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

> Ethernet II, Src: VMware_c0:00:01 (00:50:56: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: 1, Ack: 50, Len: 16

> File Transfer Protocol (FTP)

USER anonymous\r\nRequest command: USER

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

➔ Mode passive

27	21.956224	10.0.0.1	10.0.0.224	FTP	60 Request: PASV
28	21.968087	10.0.0.224	10.0.0.1	FTP	101 Response: 227 Entering Passiv
29	21.984564	10.0.0.1	10.0.0.224	FTP	62 Request: SIZE /
30	21.985403	10.0.0.224	10.0.0.1	FTP	76 Response: 550 /: No such file
31	21.986261	10.0.0.1	10.0.0.224	TCP	66 49791 → complex-link(5001) [
32	21.986361	10.0.0.224	10.0.0.1	TCP	66 complex-link(5001) → 49791 [
33	21.986491	10.0.0.1	10.0.0.224	FTP	62 Request: MDTM /
34	21.986571	10.0.0.1	10.0.0.224	TCP	60 49791 → complex-link(5001) [
35	21.987586	10.0.0.224	10.0.0.1	FTP	74 Response: 213 20090903103505
36	21.988569	10.0.0.1	10.0.0.224	FTP	62 Request: RETR /
37	21.989338	10.0.0.224	10.0.0.1	FTP	89 Response: 550 /: No such file
38	21.990088	10.0.0.1	10.0.0.224	FTP	60 Request: PASV
39	21.994321	10.0.0.224	10.0.0.1	TCP	54 complex-link(5001) → 49791 [
40	22.000601	10.0.0.1	10.0.0.224	TCP	60 49791 → complex-link(5001) [
41	22.000622	10.0.0.1	10.0.0.224	TCP	60 49791 → complex-link(5001) [
42	22.000683	10.0.0.224	10.0.0.1	TCP	54 complex-link(5001) → 49791 [
43	22.004874	10.0.0.224	10.0.0.1	FTP	101 Response: 227 Entering Passiv
44	22.006056	10.0.0.1	10.0.0.224	FTP	61 Request: CWD /
45	22.006724	10.0.0.1	10.0.0.224	TCP	66 49792 → rfe(5002) [SYN] Seq=0
46	22.006758	10.0.0.224	10.0.0.1	TCP	66 rfe(5002) → 49792 [SYN, ACK]
47	22.006960	10.0.0.1	10.0.0.224	TCP	60 49792 → rfe(5002) [ACK] Seq=1
48	22.007298	10.0.0.224	10.0.0.1	FTP	82 Response: 250 Directory chang
49	22.007714	10.0.0.1	10.0.0.224	FTP	60 Request: LIST
50	22.011258	10.0.0.224	10.0.0.1	FTP-DA..	1514 FTP Data: 1460 bytes (PASV) (
51	22.011398	10.0.0.224	10.0.0.1	FTP-DA..	264 FTP Data: 210 bytes (PASV) (C
52	22.011496	10.0.0.1	10.0.0.224	TCP	60 49792 → rfe(5002) [ACK] Seq=1

Frame 43: 101 bytes on wire (808 bits), 101 bytes captured (808 bits)

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 Version 4, Src: 10.0.0.224 (10.0.0.224), Dst: 10.0.0.1 (10.0.0.1)

Transmission Control Protocol, Src Port: ftp (21), Dst Port: 49788 (49788), Seq: 421, Ack: 122, Len: 47

File Transfer Protocol (FTP)

227 Entering Passive Mode (10,0,0,224,19,138)\r\n
Response code: Entering Passive Mode (227)
Response arg: Entering Passive Mode (10,0,0,224,19,138)
Passive IP address: 10.0.0.224 (10.0.0.224)
Passive port: 5002

[Current working directory: /]

[Command: CWD /]

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.

+) Bước 1: FTP Client mở một port cao bất kỳ (theo file FTP_02.cap là port số 49788 còn trống) gửi gói tin SYN đến port 21 trên FTP Server với mục đích thông báo.

+) Bước 2: FTP Server đồng ý và gửi lại gói tin SYN/ACK từ port 21 đến port 49788 trên FTP Client.

+) Bước 3: FTP Client sẽ gửi lại gói tin ACK từ port 49788 đến port 21 trên FTP Server đồng ý tạo kết nối → Connection Control đã được khởi tạo xong giữa Client và Server.

4	10.0.0.255	10.0.0.1	10.0.0.255	NBNS	92 Name query NB 172.29.70.4<20>
5	11.415085	10.0.0.1	10.0.0.255	NBNS	92 Name query NB 172.29.70.4<20>
6	11.428823	10.0.0.1	10.0.0.224	TCP	66 49788 → ftp(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 ftp(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 → ftp(21) [ACK] Seq=1 Ack=1 Win=65700 Len=0
9	11.431999	10.0.0.224	10.0.0.1	FTP	103 Response: 220 Serv-U FTP Server v6.3 for WinSock ready...
10	11.615330	10.0.0.1	10.0.0.224	TCP	60 49788 → ftp(21) [ACK] Seq=1 Ack=50 Win=65648 Len=0
11	12.192785	10.0.0.1	10.0.0.255	NBNS	92 Name query NB 172.29.70.4<20>
12	12.730270	10.0.0.1	10.0.0.224	FTP	70 Request: USER anonymous

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

+) Bước 1: FTP Client chủ động gửi command PASV trên Connection Control.

+) Bước 2: FTP Server nhận được yêu cầu phải dùng Passive Mode để truyền dữ liệu, nó mở port 5002 và response lại cho FTP Client biết sẽ dùng port 5002 để tạo Connection Data.(trường hợp ở hình (2))

+) Bước 3: FTP Client nhận được phản hồi, nó sẽ mở port 49792 để tiến hành đàm phán 3 bước với FTP Server → Connection Data đã được tạo xong giữa FTP Client port 49792 và FTP Server port 5002.

*Chú thích: Hình (1) là yêu cầu bị fail, hình (2) yêu cầu thành công

30	21.985403	10.0.0.224	10.0.0.1	FTP	76 Response: 550 /: No such file.
31	21.986261	10.0.0.1	10.0.0.224	TCP	66 49791 → complex-link(5001) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
32	21.986361	10.0.0.224	10.0.0.1	TCP	66 complex-link(5001) → 49791 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 ...
33	21.986491	10.0.0.1	10.0.0.224	FTP	62 Request: MDTM /
34	21.986571	10.0.0.1	10.0.0.224	TCP	60 49791 → complex-link(5001) [ACK] Seq=1 Ack=1 Win=65700 Len=0
35	21.987586	10.0.0.224	10.0.0.1	FTP	74 Response: 213 20090903103505

(1)

44	22.006056	10.0.0.1	10.0.0.224	FTP	61 Request: CWD /
45	22.006724	10.0.0.1	10.0.0.224	TCP	66 49792 → rfe(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 rfe(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 → rfe(5002) [ACK] Seq=1 Ack=1 Win=65700 Len=0
48	22.007298	10.0.0.224	10.0.0.1	FTP	82 Response: 250 Directory changed to /

(2)

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

➔ Port truyền dữ liệu của FTP Server là: 5002

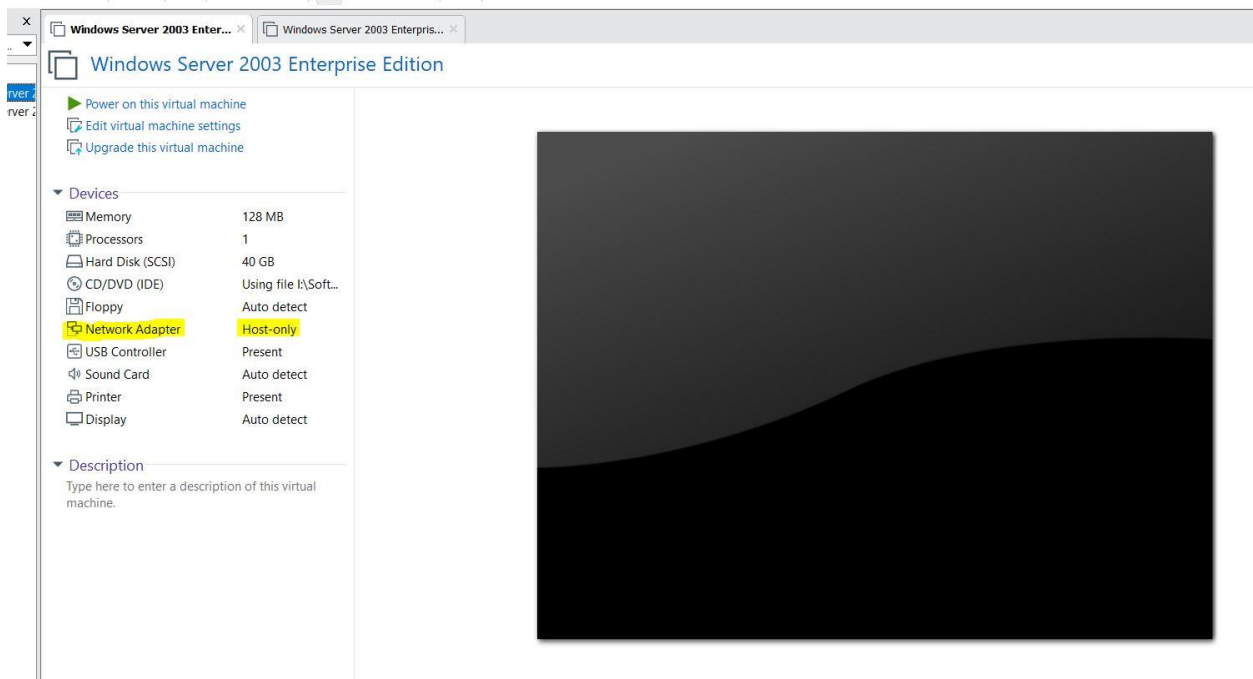
➔ Port truyền dữ liệu của FTP Client là: 49792

49	22.007714	10.0.0.1	10.0.0.224	FTP	60 Request: LIST
50	22.011258	10.0.0.224	10.0.0.1	FTP-DA...	1514 FTP Data: 1460 bytes (PASV) (CWD /)
51	22.011398	10.0.0.224	10.0.0.1	FTP-DA...	264 FTP Data: 210 bytes (PASV) (CWD /)
52	22.011496	10.0.0.1	10.0.0.224	TCP	60 49792 → rfe(5002) [ACK] Seq=1 Ack=1671 Win=65700 Len=0

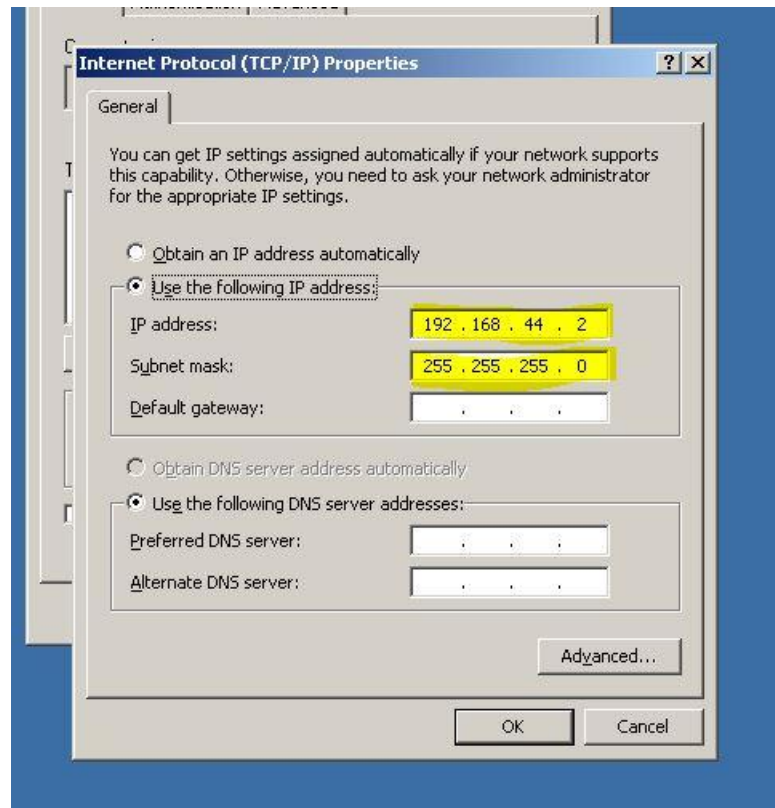
Frame 50:	1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src:	VMware_bf:9a:a0 (00:0c:29:bf:9a:a0), Dst: VMware_c0:00:01 (00:50:56:c0:00:01)
Internet Protocol Version 4, Src:	10.0.0.224 (10.0.0.224), Dst: 10.0.0.1 (10.0.0.1)
Transmission Control Protocol, Src Port:	rfe (5002), Dst Port: 49792 (49792), Seq: 1, Ack: 1, Len: 1460
FTP Data (1460 bytes data)	
[Setup frame: 43]	
[Setup method: PASV]	
[Command: CWD /]	
Command frame: 44	
[Current working directory: /]	
Line-based text data (21 lines)	
-rw-rw-rw- 1 user group 1072301 Sep 3 03:35 03_LeUyenNhy_DieuEmMuonNoi_DatHuy.wma\r\n	

Câu 3:

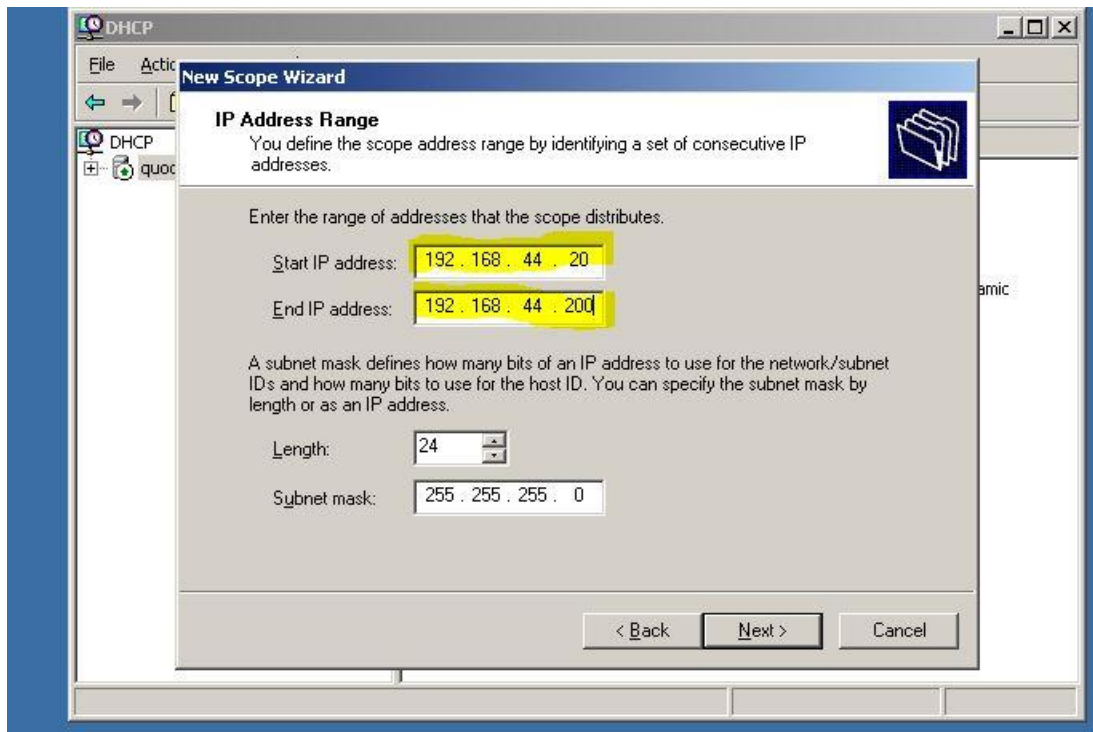
a. Sử dụng máy ảo MS Windows Server 2003/2008/2012 để làm DHCP server. Thiết lập card mạng của máy ảo là Host-Only.



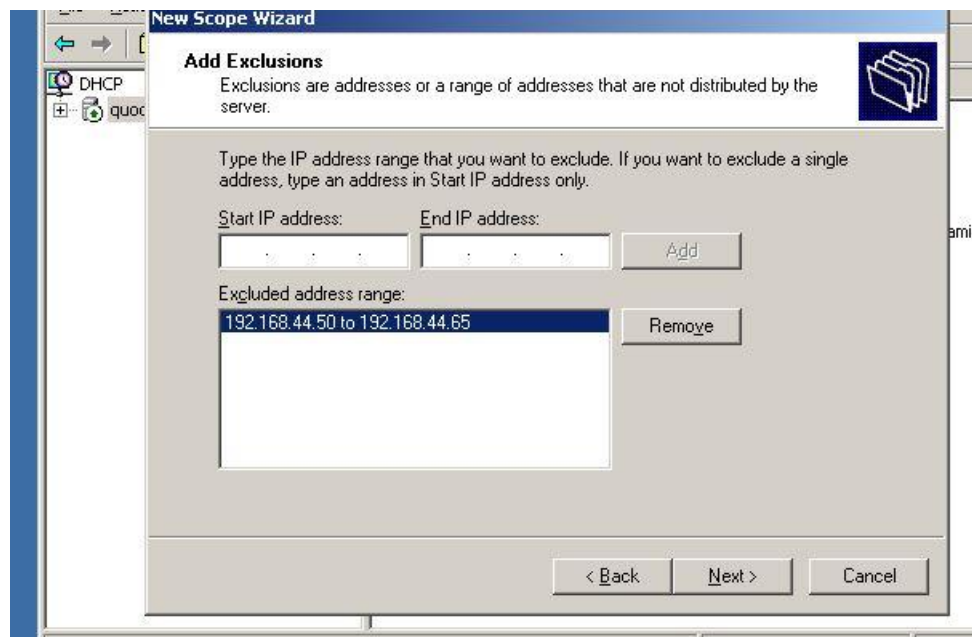
- b. Cấu hình địa chỉ IP tĩnh cho máy làm DHCP server này là: 192.168.X.2/24, với X là 2 chữ số cuối của MSSV. Ví dụ: MSSV = 1812123 \rightarrow X = 23.



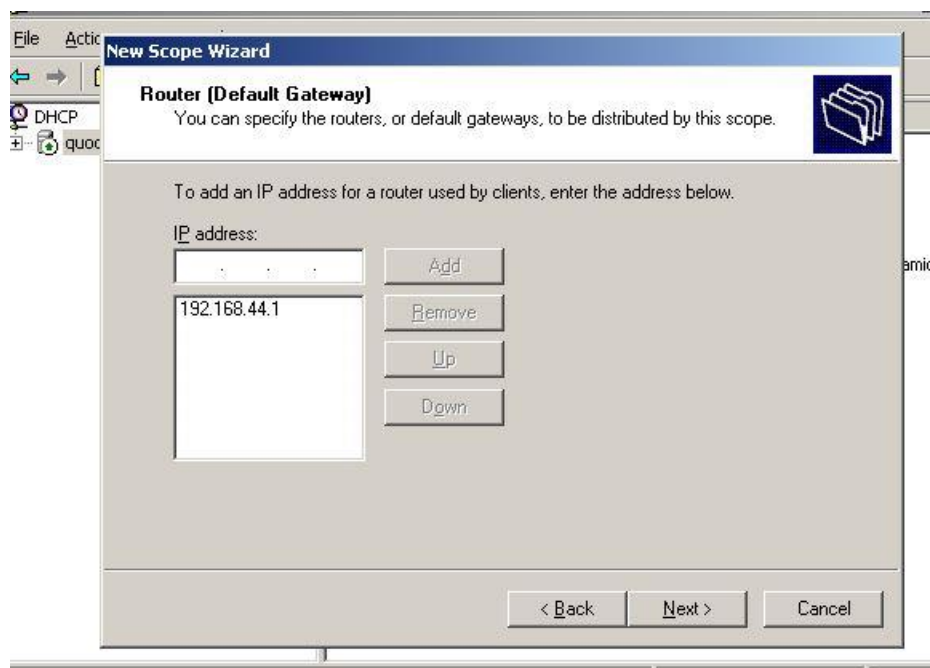
- c. Khoảng địa chỉ IP cấp cho các clients là: 192.168.X.20/24 – 192.168.X.200/24



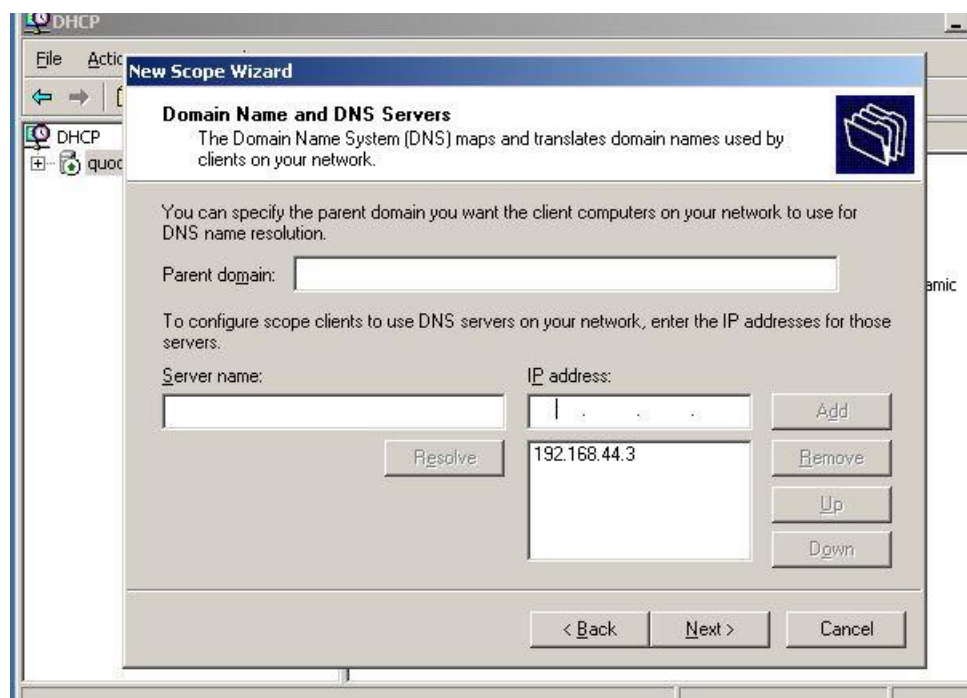
- d. Khoảng địa chỉ IP dành riêng (reservation): 192.168.X.50/24 – 192.168.X.65/24



- e. Default gateway cung cấp cho các clients: 192.168.X.1




- f. DNS server cung cấp cho các clients: 192.168.X.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.

Windows Server 2003 Enterprise Edition (2)

 Power on this virtual machine

 Edit virtual machine settings

▼ Devices

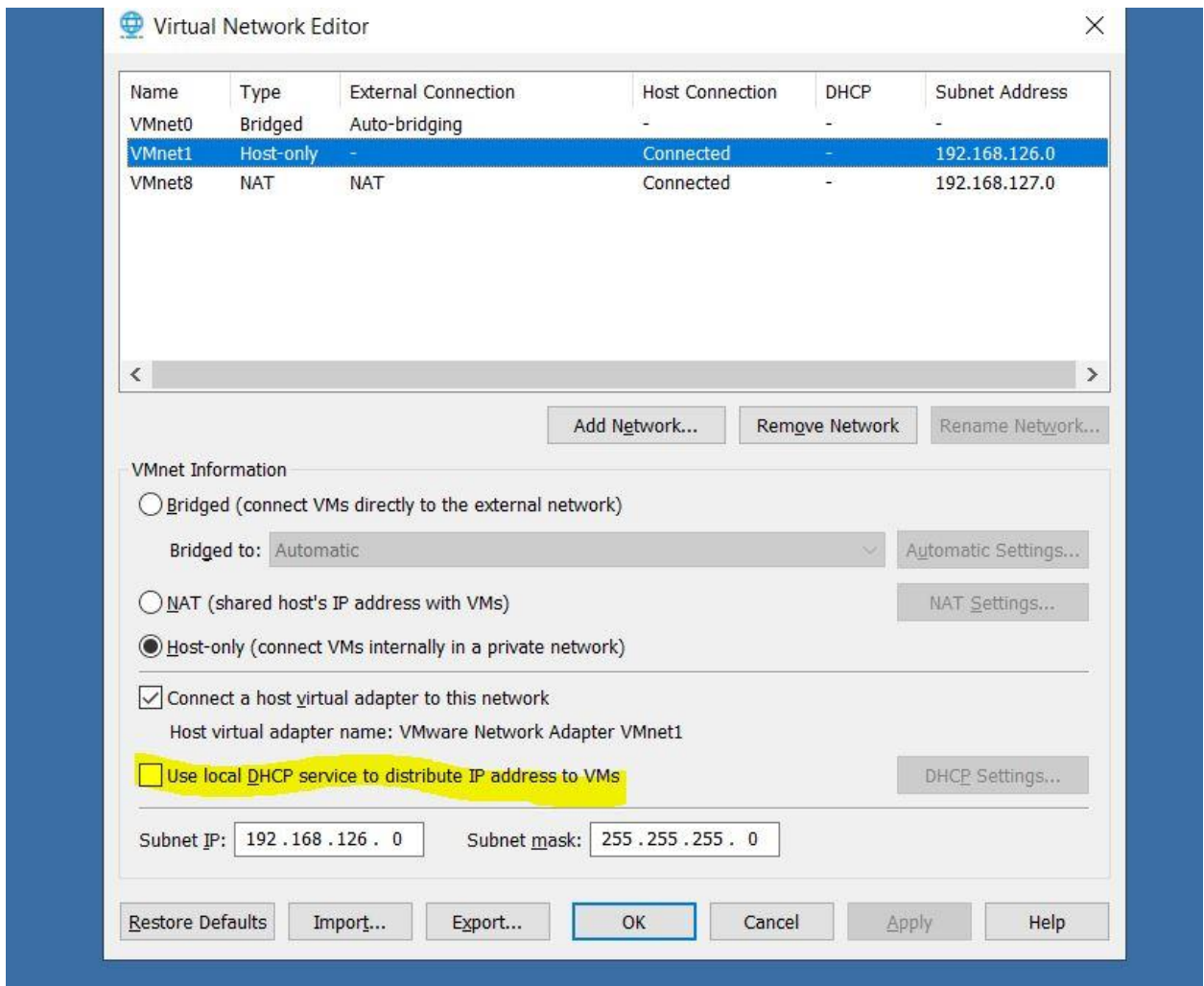
 Memory	2 GB
 Processors	1
 Hard Disk (SCSI)	40 GB
 CD/DVD (IDE)	Using file C:\Use...
 Network Adapter	Host-only
 USB Controller	Present
 Sound Card	Auto detect
 Printer	Present
 Display	Auto detect

▼ Description

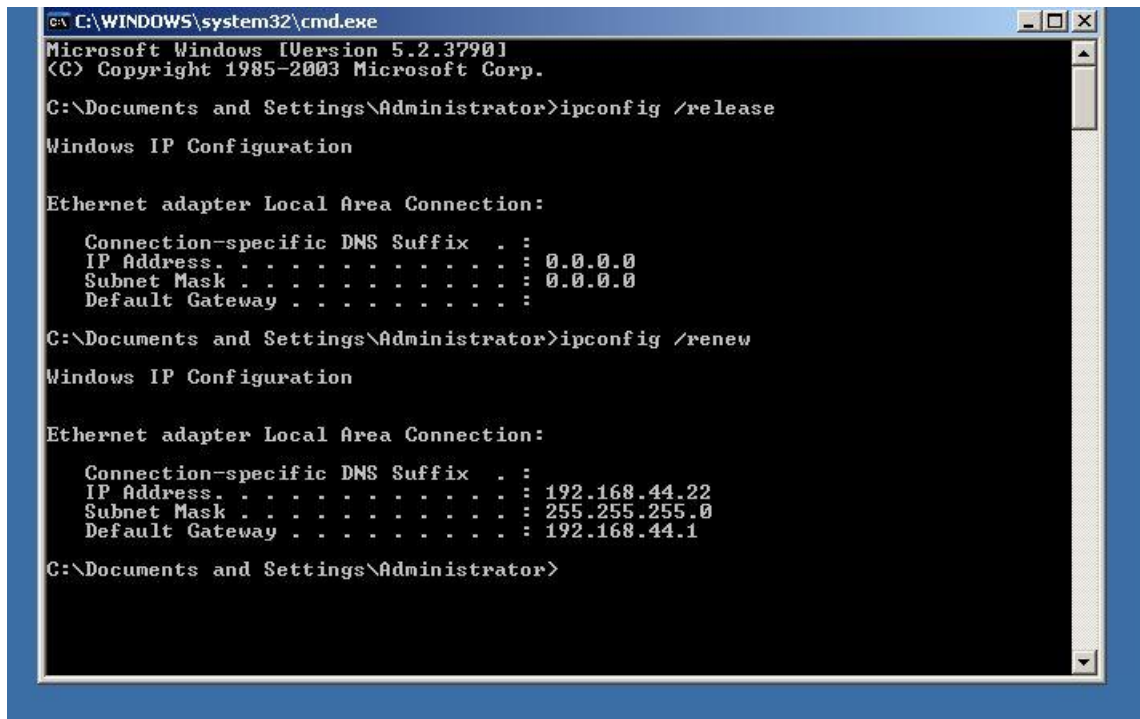
Type here to enter a description of this virtual machine.



- 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.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

C:\Documents and Settings\Administrator>ipconfig /renew

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.44.22
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.44.1

C:\Documents and Settings\Administrator>
```

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

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

No.	Time	Source	Destination	Protocol	Length	Info
2	0.273148	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x1a986adc
3	0.273594	192.168.44.2	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x1a986adc
4	0.274062	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0x1a986adc
5	0.274529	192.168.44.2	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x1a986adc

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 DHCP Discover:

- DHCP Client(máy ảo 2) gửi gói tin broadcast để tìm DHCP Server (máy ảo 1)
- IP nguồn: 0.0.0.0
- IP đích: 255.255.255.255
- MAC nguồn: 00:0c:29:a7:0e:ff
- MAC đích: ff:ff:ff:ff:ff:ff
- Port nguồn: 68
- Port đích: 67

2	0.273148	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x1a986adc
3	0.273594	192.168.44.2	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x1a986adc
4	0.274062	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0x1a986adc
5	0.274529	192.168.44.2	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x1a986adc

```
> Frame 2: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits)
> Ethernet II, Src: VMware_a7:0e:ff (00:0c:29:a7:0e:ff), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> 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)
> Dynamic Host Configuration Protocol (Discover)
```

+ Gói DHCP Offer:

- DHCP Server(máy ảo 1) nếu nghe thấy yêu cầu sẽ gửi gói tin broadcast để đề xuất địa chỉ IP cho Client(máy ảo 2)
- IP nguồn: 192.168.44.2
- IP đích: 255.255.255.255
- MAC nguồn: 00:0c:29:39:bc:e6
- MAC đích: ff:ff:ff:ff:ff:ff
- Port nguồn: 67
- Port đích: 68

No.	Time	Source	Destination	Protocol	Length	Info
2	0.273148	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x1a986adc
3	0.273594	192.168.44.2	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x1a986adc
4	0.274062	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0x1a986adc
5	0.274529	192.168.44.2	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x1a986adc

```
> Frame 3: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
> Ethernet II, Src: VMware_39:bc:e6 (00:0c:29:39:bc:e6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.44.2 (192.168.44.2), Dst: 255.255.255.255 (255.255.255.255)
> User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
> Dynamic Host Configuration Protocol (Offer)
```


+ Gói DHCP Request:

- DHCP Client(máy ảo 2) nếu chấp thuận sử dụng sẽ gửi gói tin broadcast cho Server(máy ảo 1) để xác nhận sử dụng địa chỉ IP do Server đề xuất
- IP nguồn: 0.0.0.0
- IP đích: 255.255.255.255
- MAC nguồn: 00:0c:29:a7:0e:ff
- MAC đích: ff:ff:ff:ff:ff:ff
- Port nguồn: 68
- Port đích: 67

2	0.273148	0.0.0.0	255.255.255.255	DHCP	344 DHCP Discover	- Transaction ID 0x1a986adc
3	0.273594	192.168.44.2	255.255.255.255	DHCP	342 DHCP Offer	- Transaction ID 0x1a986adc
4	0.274062	0.0.0.0	255.255.255.255	DHCP	368 DHCP Request	- Transaction ID 0x1a986adc
5	0.274529	192.168.44.2	255.255.255.255	DHCP	342 DHCP ACK	- Transaction ID 0x1a986adc

```
> Frame 4: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits)
> Ethernet II, Src: VMware_a7:0e:ff (00:0c:29:a7:0e:ff), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> 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)
> Dynamic Host Configuration Protocol (Request)
```

+ Gói DHCP ACK:

- DHCP Server(máy ảo 1) gửi gói tin broadcast cho DHCP Client(máy ảo 2) đồng ý cho DHCP Client(máy ảo 2) sử dụng địa chỉ IP đã đề xuất
- IP nguồn: 192.168.44.2
- IP đích: 255.255.255.255
- MAC nguồn: 00:0c:29:39:bc:e6
- MAC đích: ff:ff:ff:ff:ff:ff
- Port nguồn: 67
- Port đích: 68

No.	Time	Source	Destination	Protocol	Length	Info
2	0.273148	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x1a986adc
3	0.273594	192.168.44.2	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x1a986adc
4	0.274062	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0x1a986adc
5	0.274529	192.168.44.2	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x1a986adc

```
> Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on 0
> Ethernet II, Src: VMware_39:bc:e6 (00:0c:29:39:bc:e6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.44.2 (192.168.44.2), Dst: 255.255.255.255 (255.255.255.255)
> User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
> Dynamic Host Configuration Protocol (ACK)
```

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

➔ Nằm trong gói DHCP Offer và DHCP ACK

No.	Time	Source	Destination	Protocol	Length	Info
2	0.273148	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x1a986adc
3	0.273594	192.168.44.2	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x1a986adc
4	0.274062	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0x1a986adc
5	0.274529	192.168.44.2	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x1a986adc

Length: 4
IP Address Lease Time: (691200s) 8 days
✎ Option: (54) DHCP Server Identifier (192.168.44.2)
Length: 4
DHCP Server Identifier: 192.168.44.2 (192.168.44.2)
✎ Option: (3) Router
Length: 4
Router: 192.168.44.1 (192.168.44.1)
✎ Option: (6) Domain Name Server
Length: 4
Domain Name Server: 192.168.44.3 (192.168.44.3)
✎ Option: (255) End
Option End: 255
Padding: 00000000000000000000000000000000

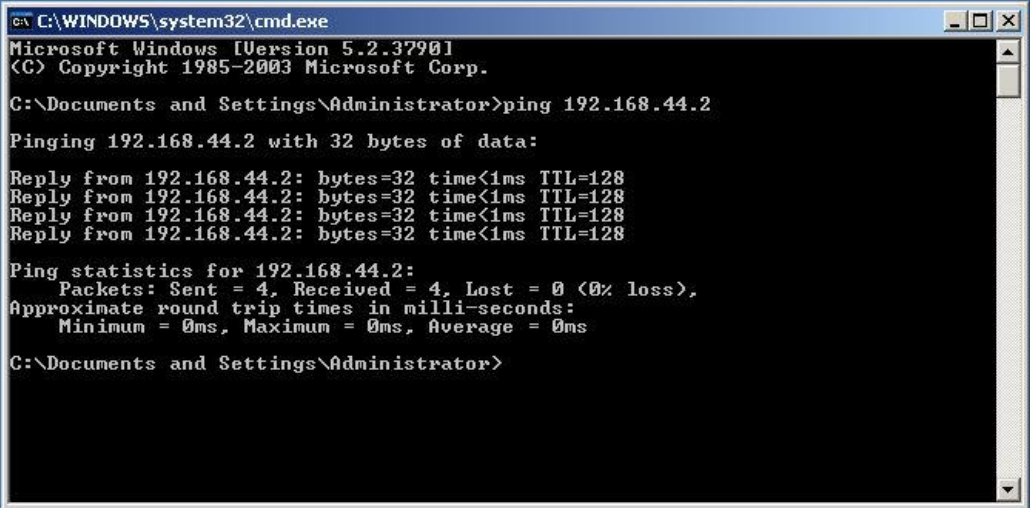
2	0.273148	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x1a986adc
3	0.273594	192.168.44.2	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x1a986adc
4	0.274062	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0x1a986adc
5	0.274529	192.168.44.2	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x1a986adc

Hops: 0
Transaction ID: 0x1a986adc
Seconds elapsed: 0
✎ Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 192.168.44.22 (192.168.44.22)
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_a7:0e:ff (00:0c:29:a7:0e:ff)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
✎ Option: (53) DHCP Message Type (ACK)
✎ Option: (58) Renewal Time Value
✎ Option: (59) Rebinding Time Value
✎ Option: (51) IP Address Lease Time
✎ Option: (54) DHCP Server Identifier (192.168.44.2)
✎ Option: (1) Subnet Mask (255.255.255.0)
✎ Option: (81) Client Fully Qualified Domain Name
✎ Option: (3) Router
Length: 4
Router: 192.168.44.1 (192.168.44.1)
✎ Option: (6) Domain Name Server
Length: 4
Domain Name Server: 192.168.44.3 (192.168.44.3)
✎ Option: (255) End
Padding: 00000000000000000000000000000000

Câu 4:

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

➔ Ping từ Client đến Server:



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.44.2

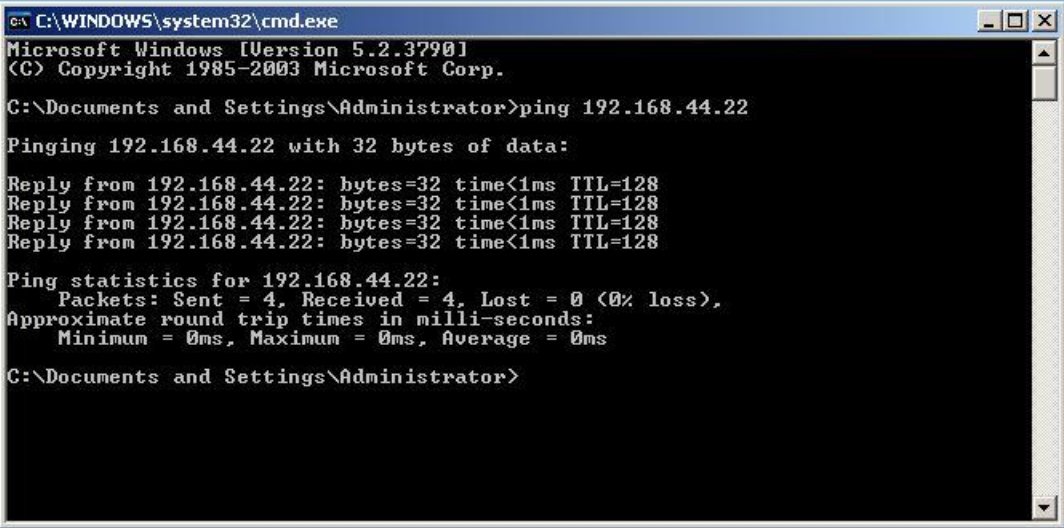
Pinging 192.168.44.2 with 32 bytes of data:

Reply from 192.168.44.2: bytes=32 time<1ms TTL=128
Reply from 192.168.44.2: bytes=32 time<1ms TTL=128
Reply from 192.168.44.2: bytes=32 time<1ms TTL=128
Reply from 192.168.44.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.44.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

➔ Ping từ Server tới Client: để kiểm tra xem 2 máy có kết nối với nhau trên cùng một đường truyền hay không?(ở đây là đường mạng 192.168.44.0/24)



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.44.22

Pinging 192.168.44.22 with 32 bytes of data:

Reply from 192.168.44.22: bytes=32 time<1ms TTL=128
Reply from 192.168.44.22: bytes=32 time<1ms TTL=128
Reply from 192.168.44.22: bytes=32 time<1ms TTL=128
Reply from 192.168.44.22: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.44.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

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

➔ Có tất cả 8 gói tin trong quá trình thực hiện lệnh ping

No.	Time	Source	Destination	Protocol	Length	Info
18	28.790435	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=1536/6, ttl=128 (reply in 19)
19	28.790580	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=1536/6, ttl=128 (request in 18)
20	29.787474	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=1792/7, ttl=128 (reply in 21)
21	29.787687	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=1792/7, ttl=128 (request in 20)
22	30.786984	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=2048/8, ttl=128 (reply in 23)
23	30.787220	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=2048/8, ttl=128 (request in 22)
24	31.786942	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=2304/9, ttl=128 (reply in 25)
25	31.787070	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=2304/9, ttl=128 (request in 24)

c. Địa chỉ MAC nguồn, MAC đích là gì?

➔ Gói Echo(ping) request:

- Địa chỉ MAC nguồn: 00:0c:29:39:bc:e6
- Địa chỉ MAC đích: 00:0c:29:a7:0e:ff

No.	Time	Source	Destination	Protocol	Length	Info
18	28.790435	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=1536/6, ttl=128 (reply in 19)
19	28.790580	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=1536/6, ttl=128 (request in 18)
20	29.787474	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=1792/7, ttl=128 (reply in 21)
21	29.787687	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=1792/7, ttl=128 (request in 20)
22	30.786984	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=2048/8, ttl=128 (reply in 23)
23	30.787220	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=2048/8, ttl=128 (request in 22)
24	31.786942	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=2304/9, ttl=128 (reply in 25)
25	31.787070	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=2304/9, ttl=128 (request in 24)

```
> Frame 18: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: VMware_39:bc:e6 (00:0c:29:39:bc:e6), Dst: VMware_a7:0e:ff (00:0c:29:a7:0e:ff)
  > Destination: VMware_a7:0e:ff (00:0c:29:a7:0e:ff)
  > Source: VMware_39:bc:e6 (00:0c:29:39:bc:e6)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.44.2 (192.168.44.2), Dst: 192.168.44.22 (192.168.44.22)
> Internet Control Message Protocol
```

➔ Gói Echo(ping) reply:

- Địa chỉ MAC nguồn: 00:0c:29:a7:0e:ff
- Địa chỉ MAC đích: 00:0c:29:39:bc:e6

No.	Time	Source	Destination	Protocol	Length	Info
18	28.790435	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=1536/6, ttl=128 (reply in 19)
19	28.790580	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=1536/6, ttl=128 (request in 18)
20	29.787474	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=1792/7, ttl=128 (reply in 21)
21	29.787687	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=1792/7, ttl=128 (request in 20)
22	30.786984	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=2048/8, ttl=128 (reply in 23)
23	30.787220	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=2048/8, ttl=128 (request in 22)
24	31.786942	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=2304/9, ttl=128 (reply in 25)
25	31.787070	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=2304/9, ttl=128 (request in 24)

```
> Frame 19: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: VMware_a7:0e:ff (00:0c:29:a7:0e:ff), Dst: VMware_39:bc:e6 (00:0c:29:39:bc:e6)
  > Destination: VMware_39:bc:e6 (00:0c:29:39:bc:e6)
  > Source: VMware_a7:0e:ff (00:0c:29:a7:0e:ff)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.44.22 (192.168.44.22), Dst: 192.168.44.2 (192.168.44.2)
> Internet Control Message Protocol
```

d. Địa chỉ IP nguồn, IP đích là gì?

➔ Gói Echo(ping) request:

- Địa chỉ IP nguồn: 192.168.44.2
- Địa chỉ IP đích: 192.168.44.22

icmp							
No.	Time	Source	Destination	Protocol	Length	Info	
18	28.790435	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request	id=0x0200, seq=1536/6, ttl=128 (reply in 19)
19	28.790580	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply	id=0x0200, seq=1536/6, ttl=128 (request in 18)
20	29.787474	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request	id=0x0200, seq=1792/7, ttl=128 (reply in 21)
21	29.787687	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply	id=0x0200, seq=1792/7, ttl=128 (request in 20)
22	30.786984	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request	id=0x0200, seq=2048/8, ttl=128 (reply in 23)
23	30.787220	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply	id=0x0200, seq=2048/8, ttl=128 (request in 22)
24	31.786942	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request	id=0x0200, seq=2304/9, ttl=128 (reply in 25)
25	31.787070	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply	id=0x0200, seq=2304/9, ttl=128 (request in 24)

> Frame 18: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
✓ Ethernet II, Src: VMware_39:bc:e6 (00:0c:29:39:bc:e6), Dst: VMware_a7:0e:ff (00:0c:29:a7:0e:ff)
> Destination: VMware_a7:0e:ff (00:0c:29:a7:0e:ff)
> Source: VMware_39:bc:e6 (00:0c:29:39:bc:e6)
Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.44.2 (192.168.44.2), Dst: 192.168.44.22 (192.168.44.22)
> Internet Control Message Protocol

➔ Gói Echo(ping) reply:

- Địa chỉ IP nguồn: 192.168.44.22
- Địa chỉ IP đích: 192.168.44.2

No.	Time	Source	Destination	Protocol	Length	Info	
18	28.790435	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request	id=0x0200, seq=1536/6, ttl=128 (reply in 19)
19	28.790580	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply	id=0x0200, seq=1536/6, ttl=128 (request in 18)
20	29.787474	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request	id=0x0200, seq=1792/7, ttl=128 (reply in 21)
21	29.787687	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply	id=0x0200, seq=1792/7, ttl=128 (request in 20)
22	30.786984	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request	id=0x0200, seq=2048/8, ttl=128 (reply in 23)
23	30.787220	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply	id=0x0200, seq=2048/8, ttl=128 (request in 22)
24	31.786942	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request	id=0x0200, seq=2304/9, ttl=128 (reply in 25)
25	31.787070	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply	id=0x0200, seq=2304/9, ttl=128 (request in 24)

> Frame 19: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
✓ Ethernet II, Src: VMware_a7:0e:ff (00:0c:29:a7:0e:ff), Dst: VMware_39:bc:e6 (00:0c:29:39:bc:e6)
> Destination: VMware_39:bc:e6 (00:0c:29:39:bc:e6)
> Source: VMware_a7:0e:ff (00:0c:29:a7:0e:ff)
Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.44.22 (192.168.44.22), Dst: 192.168.44.2 (192.168.44.2)
> Internet Control Message Protocol

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

➔ Gói Echo(ping) request:

- Bytes as hex:

6162636465666768696a6b6c6d6e6f707172737475767761626364656667686

9

- ASCII Dump: abcdefghijklmn opqrstuvwxyz abcdefg hi

No.	Time	Source	Destination	Protocol	Length	Info
18	28.790435	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=1536/6, ttl=128 (reply in 19)
19	28.790580	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=1536/6, ttl=128 (request in 18)
20	29.787474	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=1792/7, ttl=128 (reply in 21)
21	29.787687	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=1792/7, ttl=128 (request in 20)
22	30.786984	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=2048/8, ttl=128 (reply in 23)
23	30.787220	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=2048/8, ttl=128 (request in 22)
24	31.786942	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=2304/9, ttl=128 (reply in 25)
25	31.787070	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=2304/9, ttl=128 (request in 24)

> Frame 18: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: VMWare_39:bc:e6 (00:0c:29:39:bc:e6), Dst: VMWare_a7:0e:ff (00:0c:29:a7:0e:ff)
> Internet Protocol Version 4, Src: 192.168.44.2 (192.168.44.2), Dst: 192.168.44.22 (192.168.44.22)
▼ Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0x455c [correct]
 [Checksum Status: Good]
 Identifier (BE): 512 (0x0200)
 Identifier (LE): 2 (0x0002)
 Sequence number (BE): 1536 (0x0600)
 Sequence number (LE): 6 (0x0006)
 [Response frame: 19]
▼ Data (32 bytes)
 Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
 [Length: 32]

0000	00 0c 29 a7 0e ff 00 0c 29 39 bc e6 08 00 45 00	..). }9....E-
0010	00 3c 08 02 00 00 80 01 59 56 c0 a8 2c 02 c0 a8	<..... YV...-...
0020	2c 16 08 00 45 5c 02 00 06 00 61 62 63 64 65 66	,...E\... 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

➔ Góí Echo(ping) reply:

- Bytes as hex:

6162636465666768696a6b6c6d6e6f707172737475767761626364656667686
9

- ASCII Dump: abcdefghijklmn opqrstuvwxyz abcdefg hi

no.	time	source	destination	protocol	length	info
18	28.790435	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=1536/6, ttl=128 (reply in 19)
19	28.790580	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=1536/6, ttl=128 (request in 18)
20	29.787474	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=1792/7, ttl=128 (reply in 21)
21	29.787687	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=1792/7, ttl=128 (request in 20)
22	30.786984	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=2048/8, ttl=128 (reply in 23)
23	30.787220	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=2048/8, ttl=128 (request in 22)
24	31.786942	192.168.44.2	192.168.44.22	ICMP	74	Echo (ping) request id=0x0200, seq=2304/9, ttl=128 (reply in 25)
25	31.787070	192.168.44.22	192.168.44.2	ICMP	74	Echo (ping) reply id=0x0200, seq=2304/9, ttl=128 (request in 24)

```
> Frame 19: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on 0
> Ethernet II, Src: VMware_a7:0e:ff (00:0c:29:a7:0e:ff), Dst: VMware_39:bc:e6 (00:0c:29:39:bc:e6)
> Internet Protocol Version 4, Src: 192.168.44.22 (192.168.44.22), Dst: 192.168.44.2 (192.168.44.2)
> Internet Control Message Protocol
```

```
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x4d5c [correct]
  [Checksum Status: Good]
  Identifier (BE): 512 (0x0200)
  Identifier (LE): 2 (0x0002)
  Sequence number (BE): 1536 (0x0600)
  Sequence number (LE): 6 (0x0006)
```

```
  [Request frame: 18]
  [Response time: 0.145 ms]
```

```
  Data (32 bytes)
```

```
    Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
    [Length: 32]
```

```
0000  00 0c 29 39 bc e6 00 0c 29 a7 0e ff 08 00 45 00  ..)9.... )....E-
0010  00 3c 05 9f 00 00 80 01 5b b9 c0 a8 2c 16 c0 a8  <..... [....,..
0020  2c 02 00 00 4d 5c 02 00 06 00 61 62 63 64 65 66  ,...M... ..abcde
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                    wabcdehg hi
```