

SEC : A

CN LAB: 03

BATCH : A3

REG: 190905513

CSE 3113

NAME: MOHAMMAD DANISH EQBAL

PART-1 STUDY OF APPLICATION LAYER PROTOCOLS USING WIRESHARK.

Q 3.1. Retrieve web pages using HTTP. Use Wireshark to capture packets for analysis. Learn about most common HTTP messages. Also capture response messages and analyze them. During the lab session, also examine and analyze some HTTP headers.

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets, with the first packet (No. 1140) selected. The middle pane shows the details of this packet, which is an HTTP GET request for '/canonical.html' from 172.16.57.209 to 35.232.111.17. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1140	41.631695584	172.16.57.209	35.232.111.17	HTTP	141	GET / HTTP/1.1
1147	42.181914104	35.232.111.17	172.16.57.209	HTTP	273	HTTP/1.1 204 No Content
8135	341.712289903	172.16.57.209	35.232.111.17	HTTP	141	GET / HTTP/1.1
8141	342.208526059	35.232.111.17	172.16.57.209	HTTP	273	HTTP/1.1 204 No Content
12445	432.087597666	172.16.57.209	34.107.221.82	HTTP	353	GET /canonical.html HTTP/1.1
12448	432.117564142	34.107.221.82	172.16.57.209	HTTP	414	HTTP/1.1 200 OK (text/html)
12457	432.120460274	172.16.57.209	34.107.221.82	HTTP	355	GET /success.txt?ipv4 HTTP/1.1
12468	432.159363798	34.107.221.82	172.16.57.209	HTTP	332	HTTP/1.1 200 OK (text/plain)
12796	432.957696143	172.16.57.209	104.18.20.226	OCSP	498	Request
12821	433.001715457	104.18.20.226	172.16.57.209	OCSP	599	Response
13450	433.856899172	172.16.57.209	104.18.20.226	OCSP	498	Request
13450	433.882938400	104.18.20.226	172.16.57.209	OCSP	598	Response
14129	434.216492980	172.16.57.209	104.18.20.226	OCSP	498	Request
14150	434.245772572	104.18.20.226	172.16.57.209	OCSP	599	Response
15802	435.286297138	172.16.57.209	34.107.221.82	HTTP	353	GET /canonical.html HTTP/1.1

Frame 1140: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) on interface 0
Ethernet II, Src: WistronI.88:9e:2c (98:ee:cb:88:9e:2c), Dst: All-MSRP-routers_39 (00:00:0c:07:ac:39)
Internet Protocol Version 4, Src: 172.16.57.209, Dst: 35.232.111.17
Transmission Control Protocol, Src Port: 56246, Dst Port: 80, Seq: 1, Ack: 1, Len: 87
Hypertext Transfer Protocol

0000 00 00 0c 07 ac 39 98 ee cb 88 9e 2c 08 00 45 009...E-
0010 00 7f 2c ed 40 00 40 06 94 b1 ac 19 39 d1 23 e8 ...00...9#-
0020 0f 11 db b6 00 50 8d e9 23 4d 45 36 e1 53 50 18 ...P...#MH6 SP-
0030 01 6f bc 9e 00 00 47 45 54 20 2f 20 48 54 54 50GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 63 6f 6e 6e /1.1..Ho st: conn
0050 65 63 74 69 76 69 74 79 2d 63 68 65 63 6b 2e 75 ectivity -check.u
0060 62 75 6e 74 75 2e 63 6f 6d 0d 0a 41 63 63 65 70 buntu.co m-Accep
0070 74 3a 20 2a 2f 2a 0d 0a 43 6f 6e 6e 65 63 74 69 t: /*- Connecti
0080 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 0d 0a on: clos e----

Q 3.2 Use FTP to transfer some files, Use Wireshark to capture some packets. Show that FTP uses two separate connections: a control connection and a data-transfer connection. The data connection is opened and closed for each file transfer activity. Also show that FTP is an insecure file transfer protocol because the transaction is done in plaintext.

```

s Terminal
Wed 9:22 AM
student@V3102-000: ~/Documents/190905513/CN/LAB3

file Edit View Search Terminal Help
student@V3102-000:~/Documents/190905513/CN/LAB3$ ftp 172.16.57.143
Connected to 172.16.57.143.
20 Welcome to MANTRA FTP service.
Name (172.16.57.143:student): nplab
31 Please specify the password.
Password:
30 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> mkdir 190905513_MohammadDanishEqbal
257 "/190905513_MohammadDanishEqbal" created
ftp> ls
30 PORT command successful. Consider using PASV.
30 Here comes the directory listing.
d----- 3 1005 1005 4096 Oct 27 09:19 190905440_Pranshul
d----- 2 1005 1005 4096 Oct 27 09:22 190905513_MohammadDanishEqbal
d----- 2 1005 1005 4096 Oct 27 09:20 CN
d----- 2 1005 1005 4096 Oct 27 08:34 CN-lab3
d----- 2 1005 1005 4096 Oct 27 08:30 CN_lab3
-rw-r--r-- 1 1005 1005 57 Oct 26 15:11 TheOnlyFile.txt
d----- 2 1005 1005 4096 Oct 27 09:21 a
d----- 2 1005 1005 4096 Oct 27 08:39 abc
d----- 2 1005 1005 4096 Oct 27 08:35 cn
d----- 2 1005 1005 4096 Oct 27 08:42 cnlab
d----- 2 1005 1005 4096 Oct 27 08:46 cnlab1
d----- 2 1005 1005 4096 Oct 27 09:20 danish
d----- 2 1005 1005 4096 Oct 27 08:50 folder
d----- 2 1005 1005 4096 Oct 27 08:40 hello-aryan-khenka
d----- 2 1005 1005 4096 Oct 27 08:35 helloworld
d----- 2 1005 1005 4096 Oct 27 09:20 lab
d----- 2 1005 1005 4096 Oct 27 08:53 lab3
d----- 2 1005 1005 4096 Oct 27 09:20 ls
d----- 2 1005 1005 4096 Oct 27 09:00 manu
d----- 2 1005 1005 4096 Oct 27 08:56 manushree
d----- 2 1005 1005 4096 Oct 27 08:36 newdir
d----- 2 1005 1005 4096 Oct 27 08:19 nml
d----- 2 1005 1005 4096 Oct 27 08:29 one
d----- 2 1005 1005 4096 Oct 27 08:39 oneone
d----- 2 1005 1005 4096 Oct 27 08:43 oneoneone
d----- 2 1005 1005 4096 Oct 27 08:41 pqr
d----- 2 1005 1005 4096 Oct 27 08:36 pranshul
d----- 1 1005 1005 1444 Oct 27 08:27 qiser.c
d----- 2 1005 1005 4096 Oct 27 08:30 rajat
d----- 2 1005 1005 4096 Oct 27 08:38 rohan
d----- 1 1005 1005 9 Oct 27 09:20 sample1.txt
d----- 1 1005 1005 3 Oct 27 08:30 sample555.txt

```

Wireshark interface showing captured FTP traffic. The packet list displays various FTP commands and responses, including QUIT, Goodbye, Welcome, USER, PASS, LOGIN, SYST, MKD, PORT, PASV, LIST, and directory listing. The packet details pane shows the structure of the captured frames, including Ethernet II, Internet Protocol Version 4, and File Transfer Protocol (FTP).

No.	Time	Source	Destination	Protocol	Length	Info
318	13.490244530	172.16.57.209	172.16.57.143	FTP	72	Request: QUIT
319	13.491127807	172.16.57.143	172.16.57.209	FTP	80	Response: 221 Goodbye.
1227	45.159203636	172.16.57.143	172.16.57.209	FTP	102	Response: 220 Welcome to MANTRA FTP service.
1368	49.302824555	172.16.57.209	172.16.57.143	FTP	78	Request: USER nplab
1370	49.303781080	172.16.57.143	172.16.57.209	FTP	100	Response: 331 Please specify the password.
1502	55.400769037	172.16.57.209	172.16.57.143	FTP	84	Request: PASS manipal@123
1504	55.414820006	172.16.57.143	172.16.57.209	FTP	89	Response: 230 Login successful.
1506	55.414961293	172.16.57.209	172.16.57.143	FTP	72	Request: SYST
1508	55.415565555	172.16.57.143	172.16.57.209	FTP	85	Response: 215 UNIX Type: L8
2184	83.519144166	172.16.57.209	172.16.57.143	FTP	101	Request: MKD 190905513_MohammadDanishEqbal
2186	83.520342653	172.16.57.143	172.16.57.209	FTP	112	Response: 257 "/190905513_MohammadDanishEqbal" created
2273	87.463351914	172.16.57.209	172.16.57.143	FTP	93	Request: PORT 172,16,57,209,131,35
2274	87.464565891	172.16.57.143	172.16.57.209	FTP	117	Response: 200 PORT command successful. Consider using PASV.
2276	87.464663332	172.16.57.209	172.16.57.143	FTP	72	Request: LIST
2280	87.466393040	172.16.57.143	172.16.57.209	FTP	105	Response: 150 Here comes the directory listing.

Frame 318: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
 Ethernet II, Src: WistronL_86:9e:2c (98:ee:cb:88:9e:2c), Dst: LcfcHefe_8f:db:e3 (8c:16:45:8f:db:e3)
 Internet Protocol Version 4, Src: 172.16.57.209, Dst: 172.16.57.143
 Transmission Control Protocol, Src Port: 55448, Dst Port: 21, Seq: 1, Ack: 1, Len: 6
 File Transfer Protocol (FTP)
 [Current working directory:]

Wireshark enp2s0_20211027092110_sp4Zle.pcapng

Packets: 2658 - Displayed: 16 (0.6%)

Profile: Default

Q 3.3 Analyze the behavior of the DNS protocol. In addition to Wireshark [Several network utilities are available for finding some information stored in the DNS servers. Eg.dig utilities (which has replaced nslookup). Set Wireshark to capture the packets sent by this utility.]

Wireshark interface showing DNS traffic capture. The packet list displays several DNS queries and responses. The packet details pane shows the structure of a DNS response packet. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
546	22.384097771	172.16.19.202	172.16.57.75	DNS	213	Standard query response 0xa211 A teams.events.data.microsoft.com CNAME teams-events-data.t
915	31.460613182	172.16.57.209	172.16.19.203	DNS	82	Standard query 0x0bc9 A manipal.edu OPT
916	31.460796509	172.16.57.209	172.16.19.203	DNS	82	Standard query 0x1fed AAAA manipal.edu OPT
917	31.460845826	172.16.19.203	172.16.57.209	DNS	146	Standard query response 0x0bc9 A manipal.edu A 13.33.146.55 A 13.33.146.28 A 13.33.146.12
918	31.461009887	172.16.19.203	172.16.57.209	DNS	158	Standard query response 0x1fed AAAA manipal.edu SOA mpl-ab-adc01.mahe.manipal.net OPT
919	31.461716852	172.16.57.209	172.16.19.203	DNS	87	Standard query 0xbd91 A slcm.manipal.edu OPT
920	31.461885205	172.16.57.209	172.16.19.203	DNS	87	Standard query 0xd183 AAAA slcm.manipal.edu OPT
921	31.461943993	172.16.19.203	172.16.57.209	DNS	103	Standard query response 0xbd91 A slcm.manipal.edu A 104.211.226.160 OPT
922	31.462070061	172.16.19.203	172.16.57.209	DNS	163	Standard query response 0xd183 AAAA slcm.manipal.edu SOA mpl-ab-adc01.mahe.manipal.net OPT
1011	35.668625771	172.16.19.202	172.16.57.30	DNS	190	Standard query response 0x279f A japanwestcns-prod.trafficmanager.net CNAME japanwestazsc
1012	35.668751829	172.16.19.202	172.16.57.30	DNS	244	Standard query response 0x95fe AAAA japanwestcns-prod.trafficmanager.net CNAME japanwestaz
1115	40.630423799	172.16.57.209	172.16.19.203	DNS	100	Standard query 0x7bce A connectivity-check.ubuntu.com OPT
1116	40.630603259	172.16.57.209	172.16.19.203	DNS	100	Standard query 0x21fa AAAA connectivity-check.ubuntu.com OPT
1117	40.630608322	172.16.19.203	172.16.57.209	DNS	132	Standard query response 0x7bce A connectivity-check.ubuntu.com A 35.232.111.17 A 35.224.17
1118	40.630798916	172.16.19.203	172.16.57.209	DNS	161	Standard query response 0x21fa AAAA connectivity-check.ubuntu.com SOA ns1.canonical.com OF

Frame 1011: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface 0
 Ethernet II, Src: cc:7f:76:13:3a:ff (cc:7f:76:13:3a:ff), Dst: HewlettP_1f:38:a8 (34:64:a9:1f:38:a8)
 Internet Protocol Version 4, Src: 172.16.19.202, Dst: 172.16.57.30
 User Datagram Protocol, Src Port: 53, Dst Port: 45914
 Domain Name System (response)

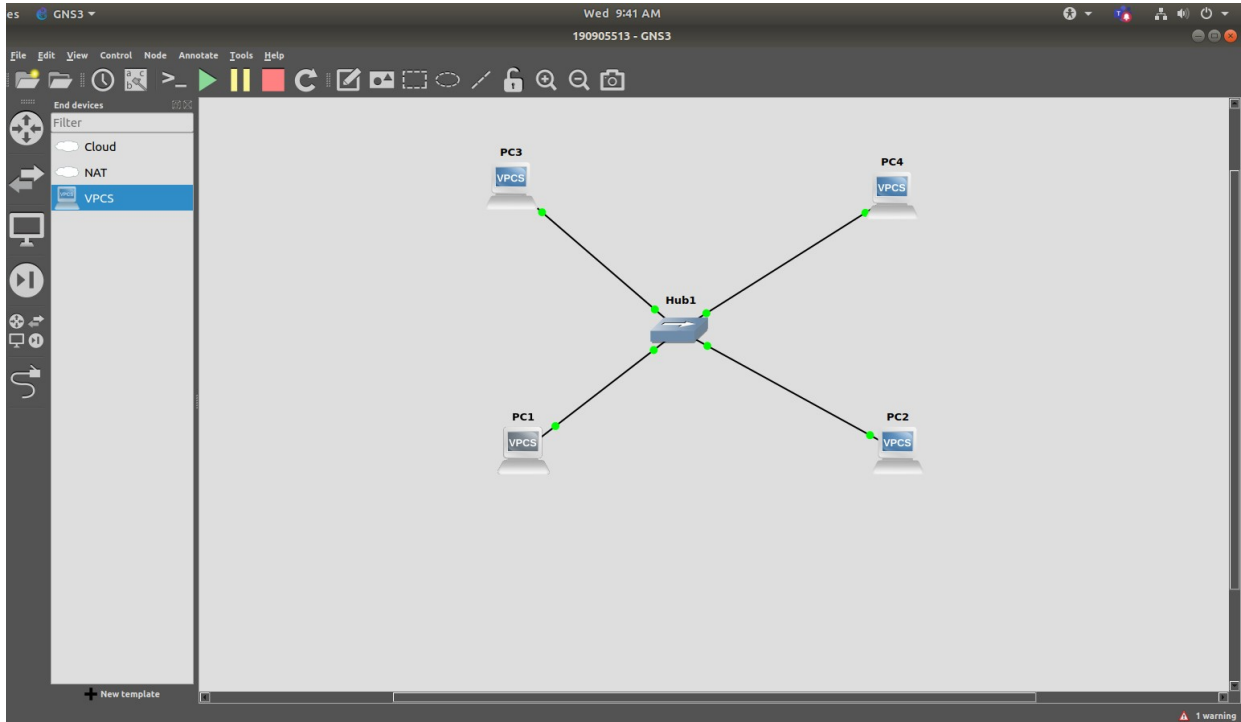
0000 34 64 a9 1f 38 a8 cc 7f 76 13 3a ff 08 00 45 00 4d - - 8 - - v : - - - E -
 0010 00 b0 35 a8 00 00 7f 11 00 8c ac 10 13 ca ac 10 - - 5 - - - - -
 0020 39 1e 00 30 b3 5a 00 9c e1 59 27 9f 81 00 00 01 9 - 5 Z - - Y - - -
 0030 00 02 00 00 00 01 11 0a 61 70 61 6e 77 65 73 74 - - - - - j apanwest
 0040 63 6e 73 2d 70 72 6f 64 0e 74 72 61 66 66 69 63 cns-prod-traffic
 0050 6d 61 6e 61 67 65 72 03 6e 65 74 00 00 01 00 01 manager-net-
 0060 c0 0c 00 05 00 01 00 00 00 85 00 37 18 6a 61 70 - - - - - 7-jap
 0070 61 6e 77 65 73 74 61 7a 73 63 63 6e 73 2d 70 72 anwestaz sccns-pr
 0080 6f 64 2d 34 31 09 6a 61 70 61 6e 77 65 73 74 08 od-41-ja panwest-
 0090 63 6c 6f 75 64 61 70 70 05 61 7a 75 72 65 03 63 cloudapp-azure-c
 00a0 6f 6d 00 c0 42 00 01 00 01 00 00 00 09 00 04 34 om-B - - - - - 4

Domain Name System: Protocol Packets: 33874 - Displayed: 2029 (6.0%) Profile: Default

PART-2 STUDY OF NETWORK DEVICES IN GNS3

Q 4.1 (a,b,c,d,e) and Q 4.3

Design network configuration shown in Figure 4.1 for all parts. Connect all four VMs to a single Ethernet segment via a single hub as shown in Figure 4.1. Configure the IP addresses for the PCs as shown in Table 4.1.



```
PC1
File Edit View Search Terminal Help
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

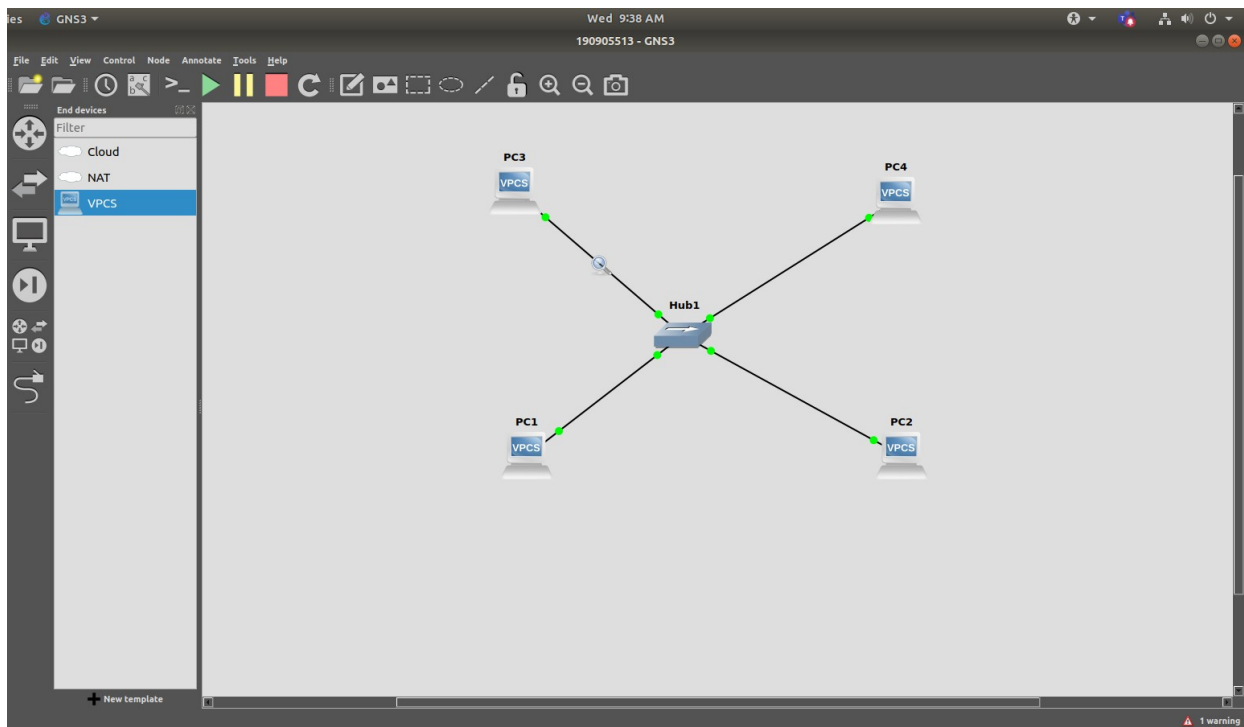
PC1> ip 10.10.10.1/28
Checking for duplicate address...
PC1 : 10.10.10.1 255.255.255.240

PC1> show ip

NAME       : PC1[1]
IP/MASK    : 10.10.10.1/28
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:03
LPORT      : 10008
RHOST:PORT : 127.0.0.1:10009
MTU        : 1500

PC1> 
```

b. Start Wireshark on PC1-Hub1 link with a capture filter set to the IP address of PC2.



c. Issue a ping command from PC1 to PC2:

```
Terminal
Capturing from
PC3
File Edit View Search Terminal Help
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
PC3> ping 10.10.10.2

84 bytes from 10.10.10.2 icmp_seq=1 ttl=64 time=0.349 ms
84 bytes from 10.10.10.2 icmp_seq=2 ttl=64 time=0.473 ms
84 bytes from 10.10.10.2 icmp_seq=3 ttl=64 time=0.589 ms
84 bytes from 10.10.10.2 icmp_seq=4 ttl=64 time=0.504 ms
84 bytes from 10.10.10.2 icmp_seq=5 ttl=64 time=0.363 ms

PC3> ping 10.10.10.2

84 bytes from 10.10.10.2 icmp_seq=1 ttl=64 time=0.562 ms
84 bytes from 10.10.10.2 icmp_seq=2 ttl=64 time=0.545 ms
84 bytes from 10.10.10.2 icmp_seq=3 ttl=64 time=0.480 ms
84 bytes from 10.10.10.2 icmp_seq=4 ttl=64 time=0.555 ms
84 bytes from 10.10.10.2 icmp_seq=5 ttl=64 time=0.459 ms
```

Wireshark - Wed 9:37 AM
Capturing from Standard Input [PC3 Ethernet0 to Hub1 Ethernet2]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

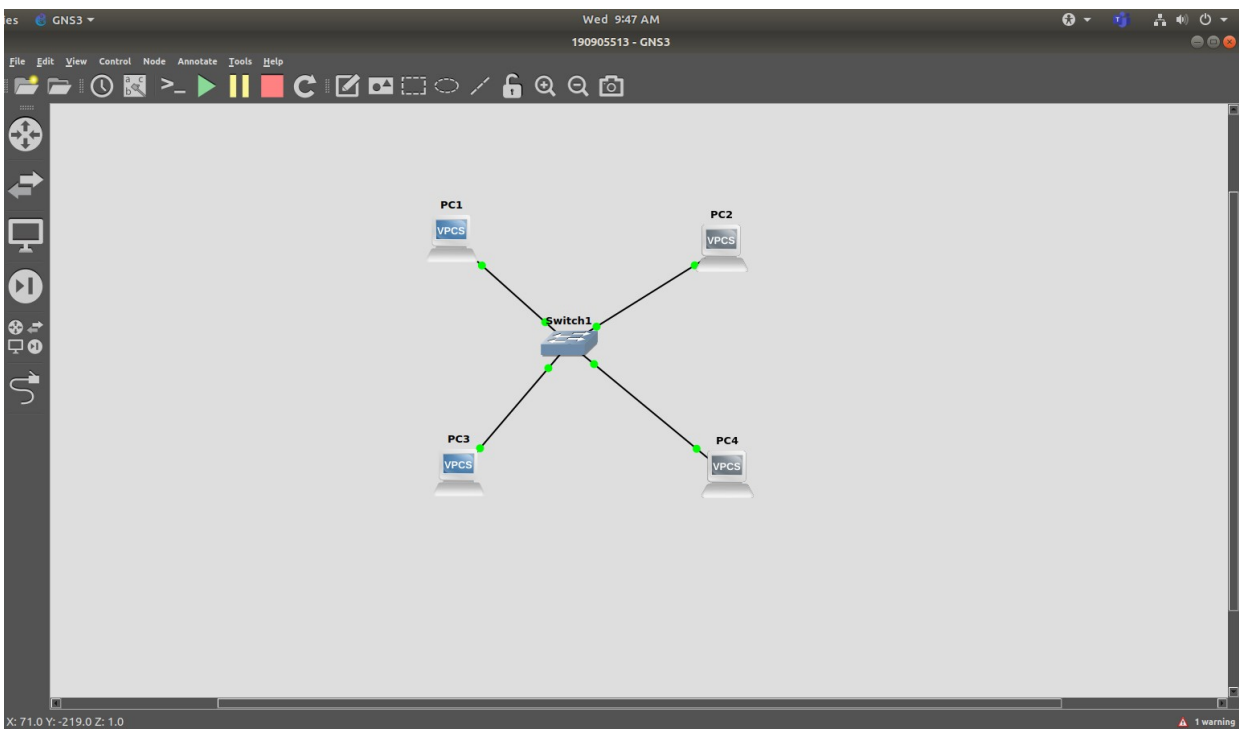
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.10.3	10.10.10.2	ICMP	98	Echo (ping) request id=0x92d0, seq=1/256, ttl=64 (reply in 2)
2	0.000285	10.10.10.2	10.10.10.3	ICMP	98	Echo (ping) reply id=0x92d0, seq=1/256, ttl=64 (request in 1)
3	1.001347	10.10.10.3	10.10.10.2	ICMP	98	Echo (ping) request id=0x93d0, seq=2/512, ttl=64 (reply in 4)
4	1.001595	10.10.10.2	10.10.10.3	ICMP	98	Echo (ping) reply id=0x93d0, seq=2/512, ttl=64 (request in 3)
5	2.002530	10.10.10.3	10.10.10.2	ICMP	98	Echo (ping) request id=0x94d0, seq=3/768, ttl=64 (reply in 6)
6	2.002750	10.10.10.2	10.10.10.3	ICMP	98	Echo (ping) reply id=0x94d0, seq=3/768, ttl=64 (request in 5)
7	3.003707	10.10.10.3	10.10.10.2	ICMP	98	Echo (ping) request id=0x95d0, seq=4/1024, ttl=64 (reply in 8)
8	3.004073	10.10.10.2	10.10.10.3	ICMP	98	Echo (ping) reply id=0x95d0, seq=4/1024, ttl=64 (request in 7)
9	4.004955	10.10.10.3	10.10.10.2	ICMP	98	Echo (ping) request id=0x96d0, seq=5/1280, ttl=64 (reply in 10)
10	4.005168	10.10.10.2	10.10.10.3	ICMP	98	Echo (ping) reply id=0x96d0, seq=5/1280, ttl=64 (request in 9)

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
 Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: Private_66:68:00 (00:50:79:66:68:00)
 Internet Protocol Version 4, Src: 10.10.10.3, Dst: 10.10.10.2
 Internet Control Message Protocol

0000 00 50 79 66 68 00 00 50 79 66 68 02 08 00 45 00 .Pyfh..P yfh...E-
 0010 00 54 d0 92 00 00 40 01 81 fe 0a 0a 0a 03 0a 0a .T....@:
 0020 0a 02 08 08 0d 3a 92 00 00 01 08 09 0a 0b 0c 0d:.....
 0030 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d
 0040 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d .. !"#%&'()*+,-.
 0050 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d ./012345 6789;,<=
 0060 3e 3f >?

Ready to load or capture Packets: 10 - Displayed: 10 (100.0%) Profile: Default

// Same Network Topology Using Switch



PC1

File Edit View Search Terminal Help

Trying 127.0.0.1...
 Connected to localhost.
 Escape character is '^']'.

PC1> ping 10.10.10.2

84 bytes from 10.10.10.2 icmp_seq=1 ttl=64 time=0.506 ms
 84 bytes from 10.10.10.2 icmp_seq=2 ttl=64 time=0.580 ms
 84 bytes from 10.10.10.2 icmp_seq=3 ttl=64 time=0.706 ms
 84 bytes from 10.10.10.2 icmp_seq=4 ttl=64 time=0.677 ms
 84 bytes from 10.10.10.2 icmp_seq=5 ttl=64 time=0.709 ms

PC1>

Wireshark - Wed 9:48 AM

Capturing from Standard Input [PC1 Ethernet0 to Switch1 Ethernet0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Private_66:68:00	Broadcast	ARP	64	Who has 10.10.10.2? Tell 10.10.10.1 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
2	0.000219	Private_66:68:01	Private_66:68:00	ARP	64	10.10.10.2 is at 00:50:79:66:68:01 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
3	0.001058	10.10.10.1	10.10.10.2	ICMP	98	Echo (ping) request id=0x0ded2, seq=1/250, ttl=64 (request in 4)
4	0.001328	10.10.10.2	10.10.10.1	ICMP	98	Echo (ping) reply id=0x0ded2, seq=1/250, ttl=64 (reply in 3)
5	1.002320	10.10.10.1	10.10.10.2	ICMP	98	Echo (ping) request id=0x0dfd2, seq=2/512, ttl=64 (request in 6)
6	1.002600	10.10.10.2	10.10.10.1	ICMP	98	Echo (ping) reply id=0x0dfd2, seq=2/512, ttl=64 (reply in 5)
7	2.003628	10.10.10.1	10.10.10.2	ICMP	98	Echo (ping) request id=0xe0d2, seq=3/768, ttl=64 (request in 8)
8	2.003961	10.10.10.2	10.10.10.1	ICMP	98	Echo (ping) reply id=0xe0d2, seq=3/768, ttl=64 (reply in 7)
9	3.004808	10.10.10.1	10.10.10.2	ICMP	98	Echo (ping) request id=0xe1d2, seq=4/1024, ttl=64 (request in 10)
10	3.005156	10.10.10.2	10.10.10.1	ICMP	98	Echo (ping) reply id=0xe1d2, seq=4/1024, ttl=64 (reply in 9)
11	4.006034	10.10.10.1	10.10.10.2	ICMP	98	Echo (ping) request id=0xe2d2, seq=5/1280, ttl=64 (request in 12)
12	4.006420	10.10.10.2	10.10.10.1	ICMP	98	Echo (ping) reply id=0xe2d2, seq=5/1280, ttl=64 (reply in 11)

Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Private_66:68:01 (00:50:79:66:68:01)

Internet Protocol Version 4, Src: 10.10.10.1, Dst: 10.10.10.2

Internet Control Message Protocol

0000 00 50 79 66 68 01 00 50 79 66 68 00 08 00 45 00 ..Pyfh..P yfh...E..

0010 00 54 d2 de 00 00 40 01 7f b4 0a 0a 0a 01 0a 0a ..T....@:s.7@.0.1...9.4q

0020 0a 02 00 00 41 38 de d2 00 01 08 09 0a 00 0c 0d ..Q q.....1...XJ...V%J...-

0030 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d2{&g V.....p

0040 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d ...! "#\$% &'()*+,-.

0050 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d ./012345 6789;<=

0060 3e 3f >?

Ready to load or capture Packets: 12 · Displayed: 12 (100.0%) Profile: Default

//UDP

Wireshark - Wed 9:32 AM

*enp2s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1126	-660.7852199	172.16.57.209	52.113.10.81	UDP	129	50033 → 3478 Len=87
1127	-660.7748903	172.16.57.209	52.113.10.81	STUN	138	Binding Request user: 0aZ7:DiIu
1128	-660.7402111	52.113.10.103	172.16.57.209	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 52.113.10.103:3481
1129	-660.6885489	52.113.10.81	172.16.57.209	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 52.113.10.81:3480
1130	-660.6790351	172.16.57.144	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
1131	-660.6246826	172.16.57.47	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
1132	-660.4351910	172.16.57.209	52.113.10.112	UDP	81	50054 → 3478 Len=39
1133	-660.4351719	172.16.57.209	52.113.10.112	UDP	1257	50054 → 3478 Len=1215
1134	-660.4351633	172.16.57.209	52.113.10.112	UDP	1257	50054 → 3478 Len=1215
1135	-660.4351559	172.16.57.209	52.113.10.112	UDP	1257	50054 → 3478 Len=1215
1136	-660.4351486	172.16.57.209	52.113.10.112	UDP	1257	50054 → 3478 Len=1215
1142	-660.0935600	172.16.57.3	224.0.0.2	HSRP	62	Hello (state Active)
1143	-660.0720592	172.16.57.58	224.0.0.251	MDNS	139	Standard query response 0x0000 PTR, cache flush lplab-Lenovo-Product-241.local A, cache f1
1145	-659.8613769	172.16.57.148	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
1146	-659.8479626	172.16.57.209	52.113.10.112	STUN	138	Binding Request user: Rj5t:thH2

Frame 1126: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits) on interface 0

Ethernet II, Src: WistronI88:9e:2c (98:ee:cb:88:9e:2c), Dst: All-MSRP-routers_39 (00:00:0c:07:ac:39)

Internet Protocol Version 4, Src: 172.16.57.209, Dst: 52.113.10.81

User Datagram Protocol, Src Port: 50033, Dst Port: 3478

Data (87 bytes)

0000 00 00 0c 07 ac 39 98 ee cb 88 9e 2c 08 00 45 009.....E..

0010 00 73 e4 37 40 00 40 11 31 9f ac 10 39 d1 34 71 ..s.7@.0.1...9.4q

0020 0a 51 c3 71 0d 96 00 5f f5 7e 00 c9 00 05 00 00 ..Q q.....1...XJ...V%J...-

0030 0a 09 d1 bc 06 c2 58 6a a3 89 76 25 4a 87 08 9b ..1...XJ...V%J...-

0040 d5 fc 32 7b 26 67 20 56 c0 91 fb 09 ac 9e 79 02 ...2{&g V.....p

0050 54 60 d1 72 28 63 00 97 a3 11 9b 16 43 c9 cd 02 ..T.r(c)...C...-

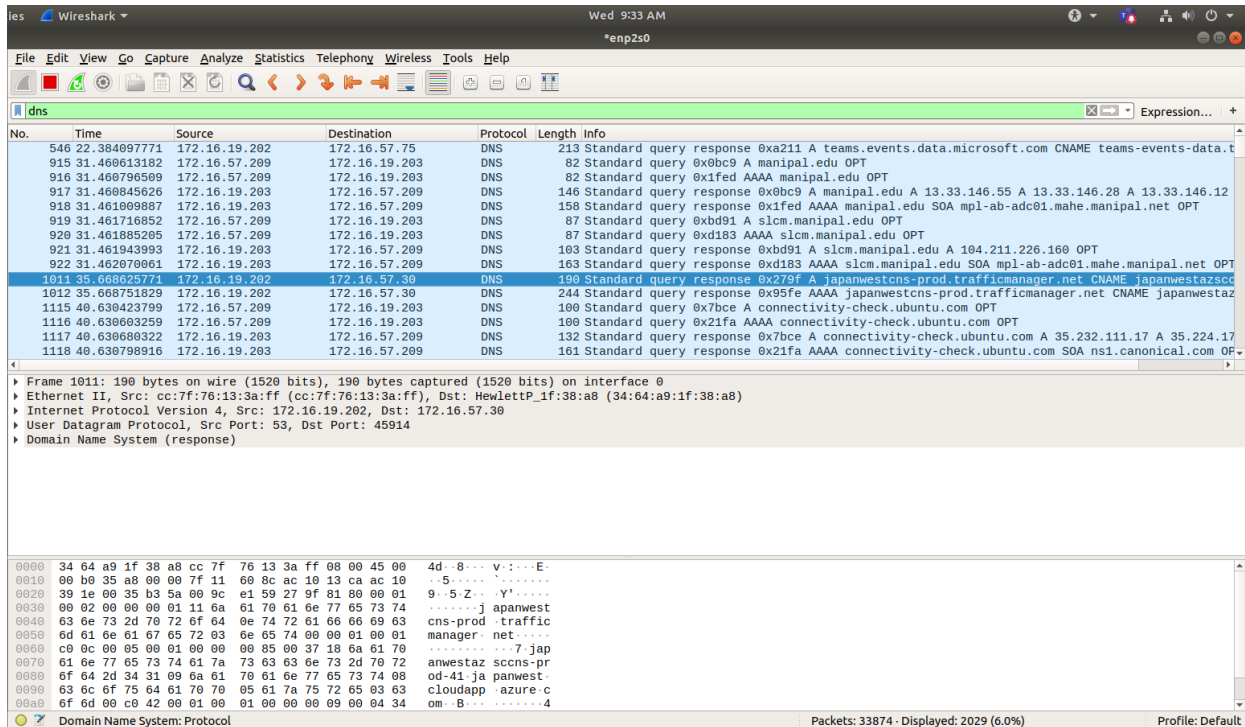
0060 45 0f 5e c8 25 c0 89 24 b1 b8 20 fe 0f df d2 d2 ..E.A.%..\$.C...-

0070 5a 3d 80 00 04 0a 01 30 00 43 b9 61 76 0a c9 a0 ..Z=.....C.av...-

0080 7b {

User Datagram Protocol: Protocol Packets: 33621 · Displayed: 15808 (47.0%) Profile: Default

//DNS

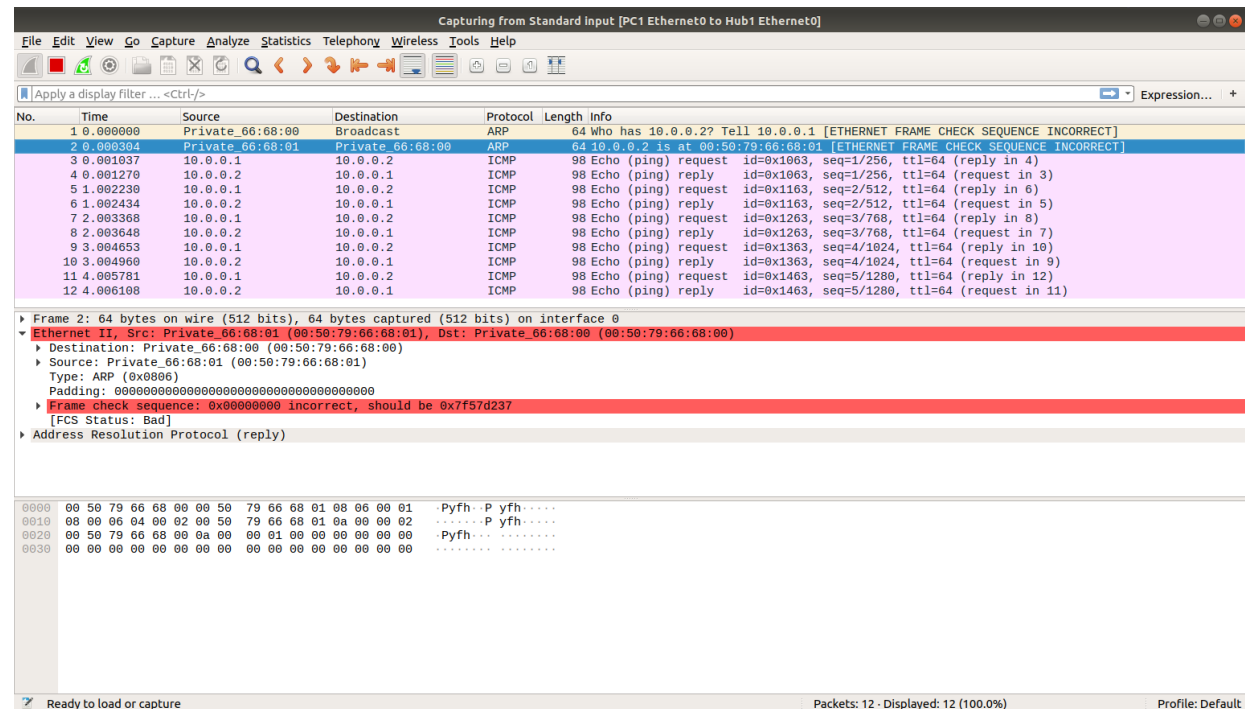


No.	Time	Source	Destination	Protocol	Length	Info
546	22.384897771	172.16.19.202	172.16.57.75	DNS	213	Standard query response 0xa211 A teams.events.data.microsoft.com CNAME teams-events-data.t
915	31.460613182	172.16.57.209	172.16.19.203	DNS	82	Standard query 0x0bc9 A manipal.edu OPT
916	31.460796509	172.16.57.209	172.16.19.203	DNS	82	Standard query 0x1fed AAAA manipal.edu OPT
917	31.460845626	172.16.19.203	172.16.57.209	DNS	146	Standard query response 0x0bc9 A manipal.edu A 13.33.146.55 A 13.33.146.28 A 13.33.146.12
918	31.461009887	172.16.19.203	172.16.57.209	DNS	158	Standard query response 0x1fed AAAA manipal.edu SOA mpl-ab-adc01.mahe.manipal.net OPT
919	31.461716852	172.16.57.209	172.16.19.203	DNS	87	Standard query 0xbd91 A slcm.manipal.edu OPT
920	31.461885205	172.16.57.209	172.16.19.203	DNS	87	Standard query 0xd183 AAAA slcm.manipal.edu OPT
921	31.461943993	172.16.19.203	172.16.57.209	DNS	183	Standard query response 0xbd91 A slcm.manipal.edu A 104.211.226.160 OPT
922	31.462070661	172.16.19.203	172.16.57.209	DNS	163	Standard query response 0xd183 AAAA slcm.manipal.edu SOA mpl-ab-adc01.mahe.manipal.net OPT
1011	35.608625771	172.16.19.202	172.16.57.30	DNS	190	Standard query response 0x270f A japanwestcns-prod.trafficmanager.net CNAME japanwestazsc
1012	35.608751829	172.16.19.202	172.16.57.30	DNS	244	Standard query response 0x95fe AAAA japanwestcns-prod.trafficmanager.net CNAME japanwestaz
1115	40.630423799	172.16.57.209	172.16.19.203	DNS	100	Standard query 0x7bce A connectivity-check.ubuntu.com OPT
1116	40.630603259	172.16.57.209	172.16.19.203	DNS	100	Standard query 0x21fa AAAA connectivity-check.ubuntu.com OPT
1117	40.630680322	172.16.19.203	172.16.57.209	DNS	132	Standard query response 0x7bce A connectivity-check.ubuntu.com A 35.232.111.17 A 35.224.17
1118	40.630798916	172.16.19.203	172.16.57.209	DNS	161	Standard query response 0x21fa AAAA connectivity-check.ubuntu.com SOA ns1.canonical.com OP

Frame 1011: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface 0
Ethernet II, Src: cc:7f:76:13:3a:ff (cc:7f:76:13:3a:ff), Dst: HewlettP_1f:38:a8 (34:64:a9:1f:38:a8)
Internet Protocol Version 4, Src: 172.16.19.202, Dst: 172.16.57.30
User Datagram Protocol, Src Port: 53, Dst Port: 45914
Domain Name System (response)

0000 34 64 a9 1f 38 a8 cc 7f 76 13 3a ff 08 00 45 00 4d ..8... v:....E:
0010 00 b0 35 a8 00 00 7f 11 60 8c ac 10 13 ca ac 10 ..5.....
0020 39 1e 00 35 b3 5a 00 9c e1 59 27 9f 81 80 00 01 9..5.Z...Y'
0030 00 02 00 00 00 01 11 6a 61 70 61 6e 77 65 73 74j apanwest
0040 63 6e 73 2d 70 72 6f 64 0e 74 72 61 66 66 69 63 cns-prod-traffic
0050 6d 61 6e 61 67 65 72 63 0e 65 74 00 00 01 00 01 manager- net....
0060 c9 0c 00 05 00 01 00 00 00 05 00 37 18 6a 61 707-jap
0070 61 6e 77 65 73 74 61 7a 73 63 63 6e 73 2d 70 72 anwestaz scns-pr
0080 6f 64 2d 34 31 09 6a 61 70 61 6e 77 65 73 74 08 od-41 ja panwest-
0090 63 6c 6f 75 64 61 70 70 05 61 7a 75 72 65 03 63 clouddapp-azure.c
00a0 6f 6d 00 c0 42 00 01 00 01 00 00 00 09 00 04 34 om--B.....4

ARP packets in the wireshark window with the MAC addresses in the Ethernet headers of the captured packets.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Private_66:68:00	Broadcast	ARP	64	Who has 10.0.0.2? Tell 10.0.0.1 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
2	0.000304	Private_66:68:01	Private_66:68:00	ARP	64	10.0.0.2 is at 00:50:79:66:68:01 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
3	0.001037	10.0.0.1	10.0.0.2	ICMP	98	Echo (ping) request id=0x1063, seq=1/256, ttl=64 (reply in 4)
4	0.001270	10.0.0.2	10.0.0.1	ICMP	98	Echo (ping) reply id=0x1063, seq=1/256, ttl=64 (request in 3)
5	1.002230	10.0.0.1	10.0.0.2	ICMP	98	Echo (ping) request id=0x1163, seq=2/512, ttl=64 (reply in 6)
6	1.002434	10.0.0.2	10.0.0.1	ICMP	98	Echo (ping) reply id=0x1163, seq=2/512, ttl=64 (request in 5)
7	2.003368	10.0.0.1	10.0.0.2	ICMP	98	Echo (ping) request id=0x1263, seq=3/768, ttl=64 (reply in 8)
8	2.003648	10.0.0.2	10.0.0.1	ICMP	98	Echo (ping) reply id=0x1263, seq=3/768, ttl=64 (request in 7)
9	3.004653	10.0.0.1	10.0.0.2	ICMP	98	Echo (ping) request id=0x1363, seq=4/1024, ttl=64 (reply in 10)
10	3.004960	10.0.0.2	10.0.0.1	ICMP	98	Echo (ping) reply id=0x1363, seq=4/1024, ttl=64 (request in 9)
11	4.005781	10.0.0.1	10.0.0.2	ICMP	98	Echo (ping) request id=0x1463, seq=5/1280, ttl=64 (reply in 12)
12	4.006108	10.0.0.2	10.0.0.1	ICMP	98	Echo (ping) reply id=0x1463, seq=5/1280, ttl=64 (request in 11)

Frame 2: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:00 (00:50:79:66:68:00)
Destination: Private_66:68:00 (00:50:79:66:68:00)
Source: Private_66:68:01 (00:50:79:66:68:01)
Type: ARP (0x0806)
Padding: 00000000000000000000000000000000
Frame check sequence: 0x00000000 incorrect, should be 0x7f57d237
[FCS Status: Bad]
Address Resolution Protocol (reply)

0000 00 50 79 66 68 00 00 50 79 66 68 01 00 06 00 01 ..Pyfh..P yfh.....
0010 00 00 06 04 00 02 00 50 79 66 68 01 0a 00 00 02P yfh.....
0020 00 50 79 66 68 00 0a 00 00 01 00 00 00 00 00 00 ..Pyfh.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Destination MAC address of the ARP Request packets:
00:50:79:66:68:00
Type field in the ethernet headers is ARP(0x0860)

```
File Edit View Search Terminal Help
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^['.

Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC1> ip 10.0.0.1/24
Checking for duplicate address...
PC1 : 10.0.0.1 255.255.255.0

PC1> arp
arp table is empty

PC1> ping 10.0.0.2/24
84 bytes from 10.0.0.2 icmp_seq=1 ttl=64 time=0.477 ms
84 bytes from 10.0.0.2 icmp_seq=2 ttl=64 time=0.435 ms
84 bytes from 10.0.0.2 icmp_seq=3 ttl=64 time=0.496 ms
84 bytes from 10.0.0.2 icmp_seq=4 ttl=64 time=0.597 ms
84 bytes from 10.0.0.2 icmp_seq=5 ttl=64 time=0.670 ms

PC1> arp
00:50:79:66:68:01 10.0.0.2 expires in 69 seconds

PC1> 
```

ARP packets for PC1