Lab 9: Wireshark --- ARP, DHCP, and ICMP

Aryan Tyagi

2019A7PS0136G

1. DHCP protocol

- Use `dhclinet` command to send DHCP requests

```
dhclient -r             # release the current lease
dhclient                # get new lease
```

```
vscode ➜ /workspaces/Lab (main ✗) $ sudo dhclient -r
sudo: unable to resolve host bravo: Temporary failure in name resolution
Removed stale PID file

"systemd" is not running in this container due to its overhead.
Use the "service" command to start services intead. e.g.:

service --status-all
vscode ➜ /workspaces/Lab (main ✗) $ sudo dhclient
sudo: unable to resolve host bravo: Temporary failure in name resolution

"systemd" is not running in this container due to its overhead.
Use the "service" command to start services intead. e.g.:

service --status-all

"systemd" is not running in this container due to its overhead.
Use the "service" command to start services intead. e.g.:

service --status-all
```

a. DHCP Request, Reply, and ACK messages

Packet Number `2554`, `2555`, `2556`, `2561` correspond to DHCP Discover, Offer, Request, ACK respectively.

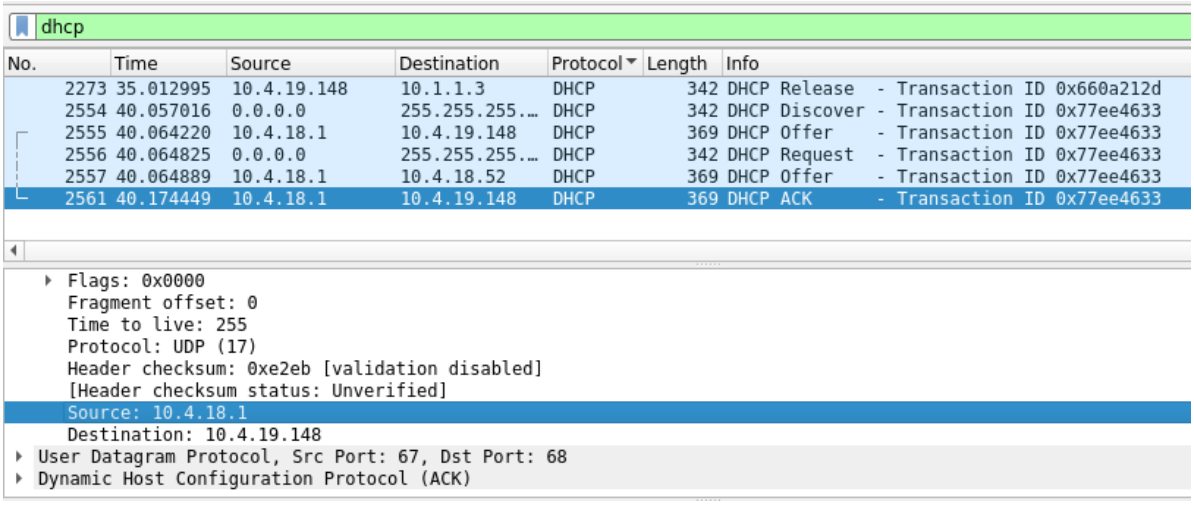
dhcp

No.	Time	Source	Destination	Protocol	Length	Info
2273	35.012995	10.4.19.148	10.1.1.3	DHCP	342	DHCP Release - Transaction ID 0x660a212d
2554	40.057016	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x77ee4633
2555	40.064220	10.4.18.1	10.4.19.148	DHCP	369	DHCP Offer - Transaction ID 0x77ee4633
2556	40.064825	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x77ee4633
2557	40.064889	10.4.18.1	10.4.18.52	DHCP	369	DHCP Offer - Transaction ID 0x77ee4633
2561	40.174449	10.4.18.1	10.4.19.148	DHCP	369	DHCP ACK - Transaction ID 0x77ee4633

b. IP addresses of the DHCP server and client

After DHCP ACK

- Client IP: `10.4.19.148`
- DHCP Server IP: `10.4.18.1`



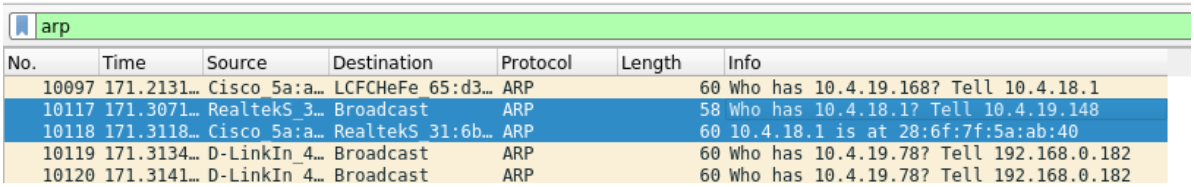
2. ARP protocol

- use `arping` to send ARP requests

```
vscode → /workspaces/Lab (main ✗) $ sudo arping -c 5 10.4.19.22
sudo: unable to resolve host bravo: Temporary failure in name resolution
ARPING 10.4.19.22
Timeout
Timeout
Timeout
Timeout
Timeout

--- 10.4.19.22 statistics ---
5 packets transmitted, 0 packets received, 100% unanswered (0 extra)

vscode → /workspaces/Lab (main ✗) $ sudo arping -c 5 10.4.18.1
sudo: unable to resolve host bravo: Temporary failure in name resolution
ARPING 10.4.18.1
60 bytes from 28:6f:7f:5a:ab:40 (10.4.18.1): index=0 time=4.780 msec
60 bytes from 28:6f:7f:5a:ab:40 (10.4.18.1): index=1 time=5.373 msec
60 bytes from 28:6f:7f:5a:ab:40 (10.4.18.1): index=2 time=4.131 msec
60 bytes from 28:6f:7f:5a:ab:40 (10.4.18.1): index=3 time=4.797 msec
60 bytes from 28:6f:7f:5a:ab:40 (10.4.18.1): index=4 time=8.477 msec

--- 10.4.18.1 statistics ---
5 packets transmitted, 5 packets received,   0% unanswered (0 extra)
rtt min/avg/max/std-dev = 4.131/5.511/8.477/1.534 ms
vscode → /workspaces/Lab (main ✗) $
```

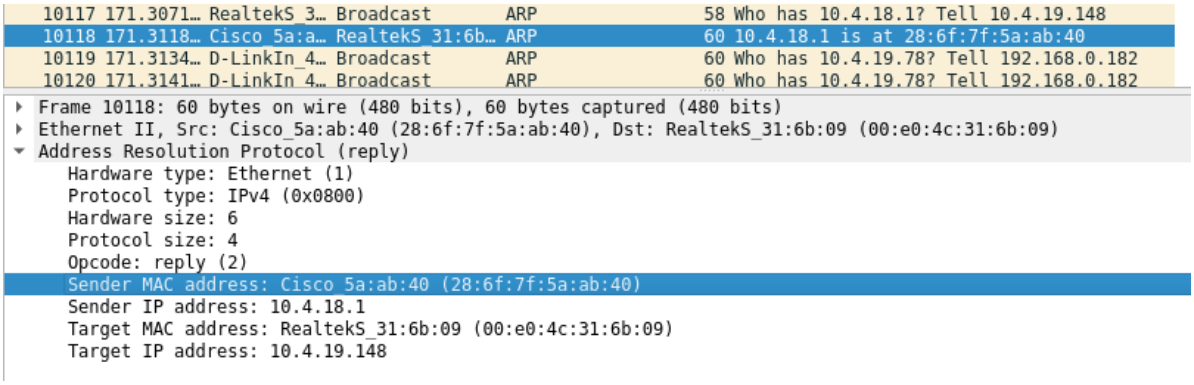
a. ARP Request and Reply messages

- Packet number `10117` is APR Request
- Packet number `10118` is APR Response



b. MAC address of the the replier

MAC address of the the replier is `28:6f:7f:5a:ab:40`



3. traceroute for dns.google

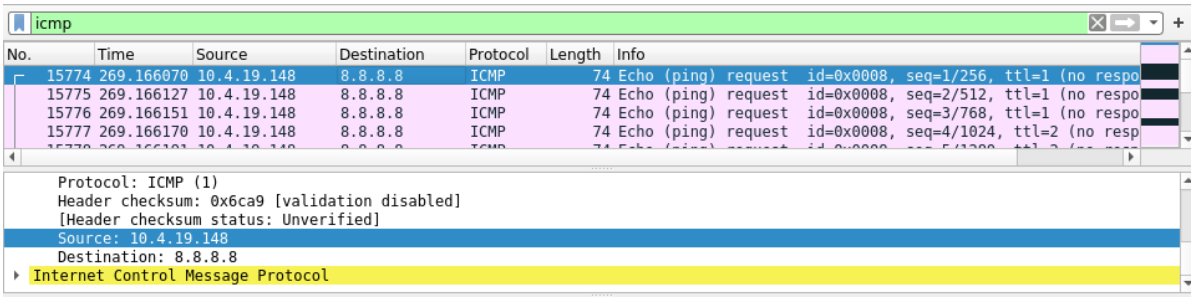
```
traceroute --icmp dns.google
# OR
traceroute --icmp 8.8.8.8
```

```
vscode ➜ /workspaces/Lab (main ✗) $ traceroute --icmp 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.4.18.1 (10.4.18.1)  0.867 ms  0.809 ms  0.768 ms
 2  campnet.bits-goa.ac.in (10.1.0.10)  0.741 ms  0.726 ms  0.707 ms
 3  103-210-49-129.rev.expl.in (103.210.49.129)  1.179 ms * *
 4  * * 103.123.50.37 (103.123.50.37)  1.660 ms
 5  45-116-0-133.rev.expl.in (45.116.0.133)  2.366 ms  2.362 ms  2.344 ms
 6  45-116-0-245.rev.expl.in (45.116.0.245)  31.676 ms  31.381 ms  31.325 ms
 7  72.14.198.241 (72.14.198.241)  31.303 ms  31.296 ms  31.288 ms
 8  108.170.248.177 (108.170.248.177)  23.733 ms  23.818 ms  23.697 ms
 9  72.14.237.139 (72.14.237.139)  32.216 ms  32.203 ms  32.187 ms
10  dns.google (8.8.8.8)  22.938 ms  22.920 ms  22.908 ms
```

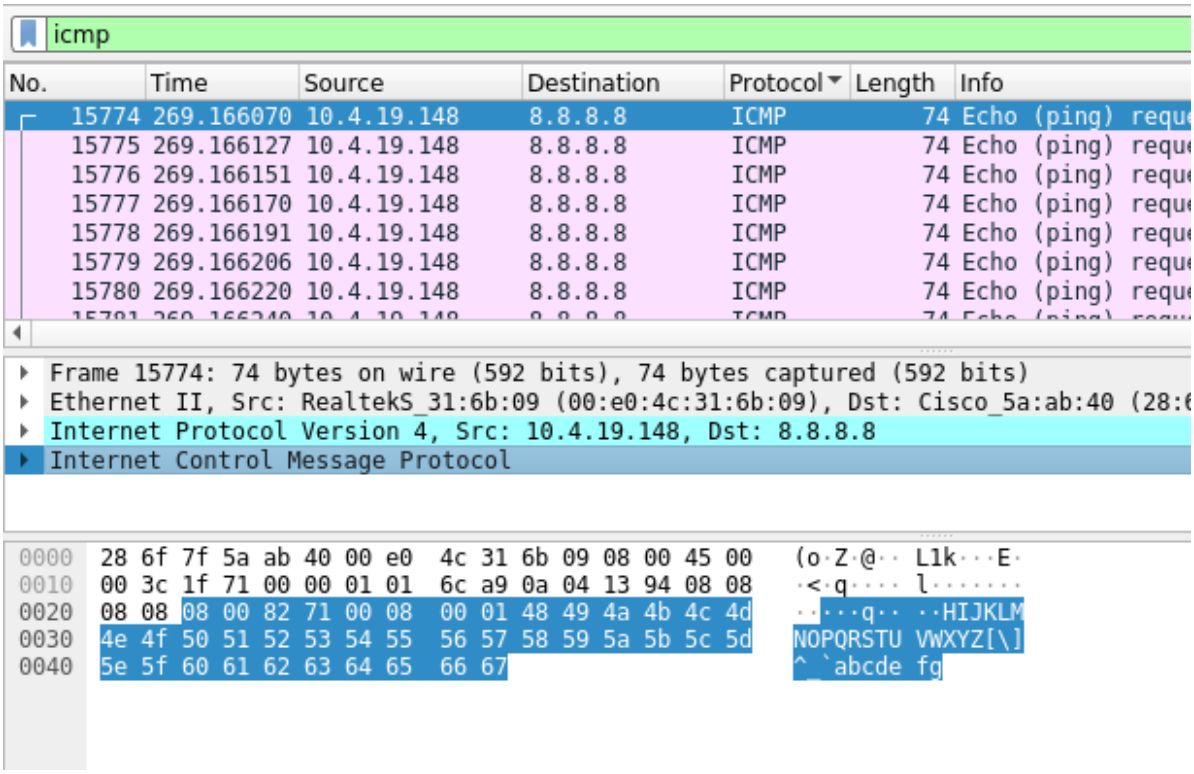
a. IP address of your host and the destination

Host IP: `10.4.19.148`

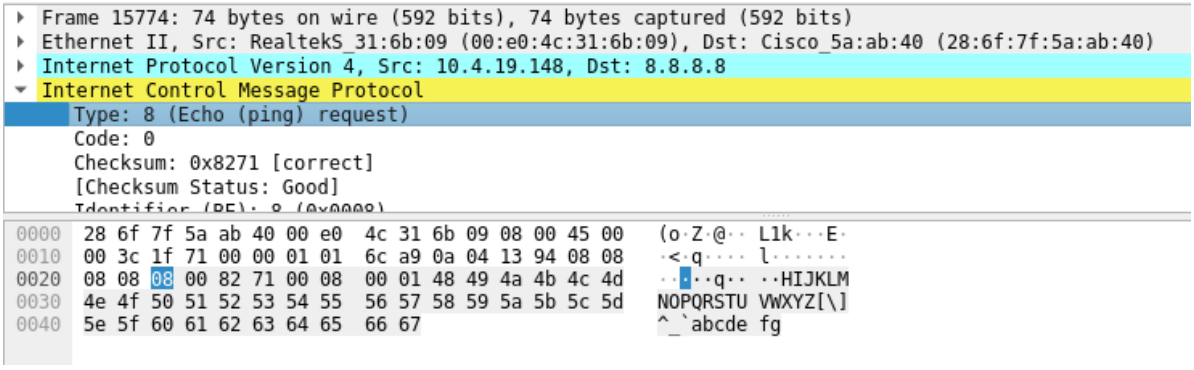
Destination IP: `8.8.8.8`



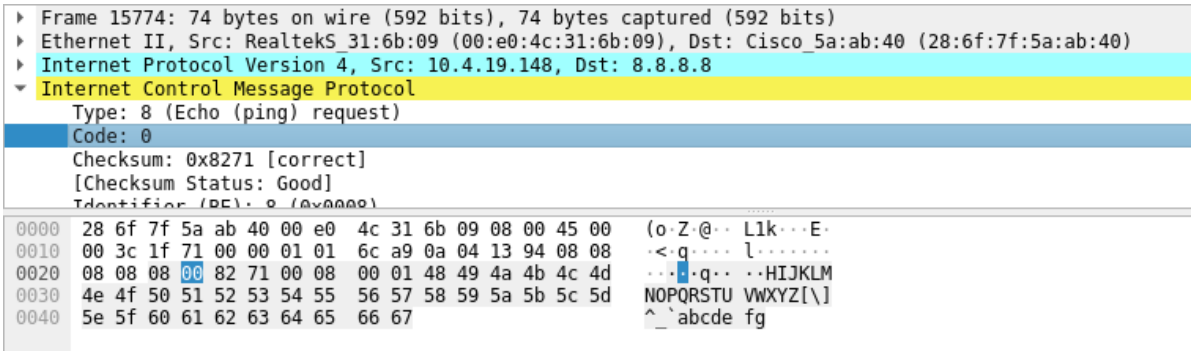
b. raw bytes of the ICMP echo packet



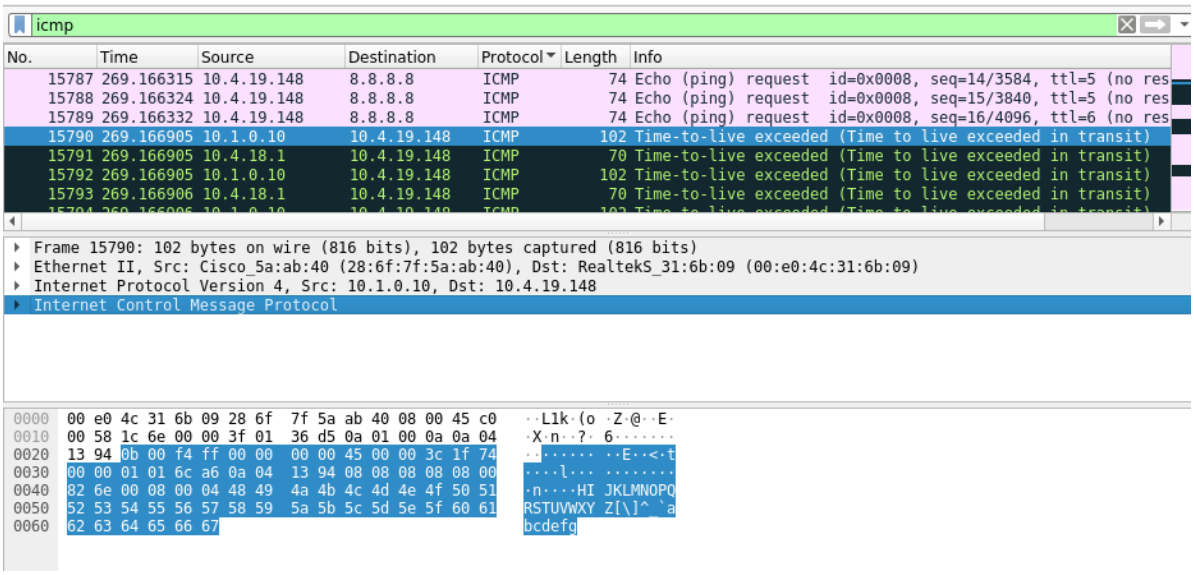
- type `0x08`



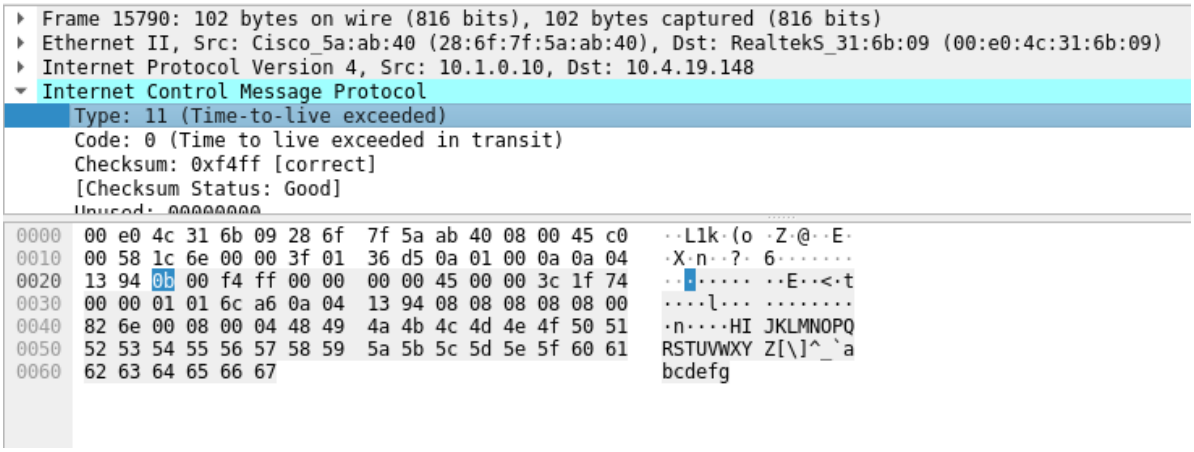
- code `0x00`



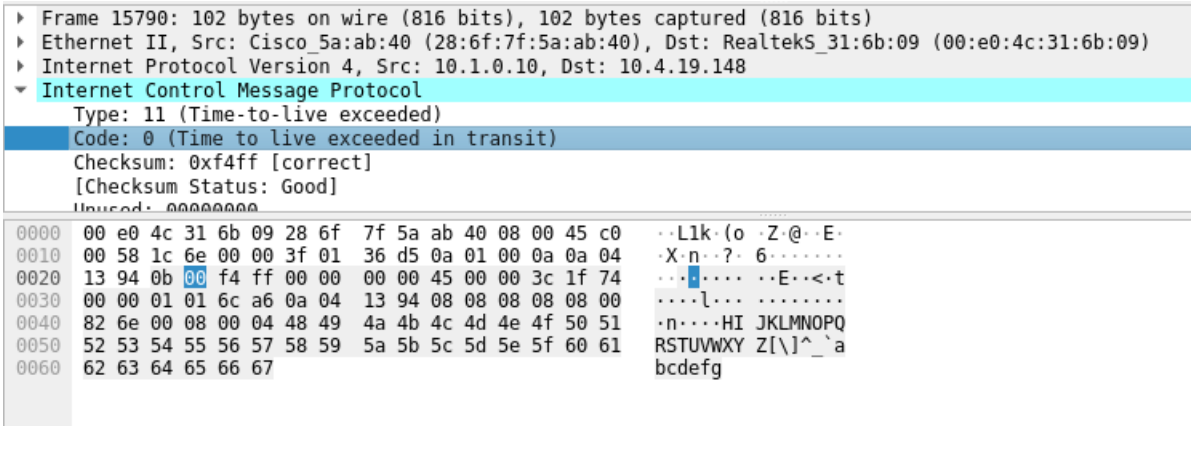
c. raw bytes of the ICMP error packet



- type `0x0b`

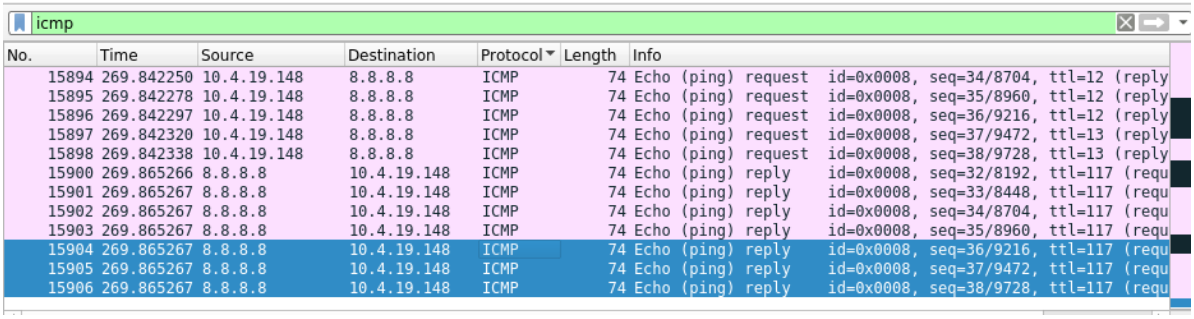


- code `0x00`



d. last three ICMP packets received by the source host

- The last 3 ICMP packets are ICMP Echo reply packets with type `0x00` and code `0x00`.



- ICMP reply packets have type `0x00`. ICMP request packets have type `0x08`. Other type values are used for errors; eg. TTL exceed error corresponds to type `0x0b`. This type indicates how the following bytes are to be interpreted.