NSCAP HW6

110550039 劉詠

Part 1

1. **When h1 ping h2, what will happen?**
   Explain every step of the ARP and ICMP packet by using the following explanation format. You should also take screenshots of your results.

ARP:

h1 sent ARP request

h2 received and replied

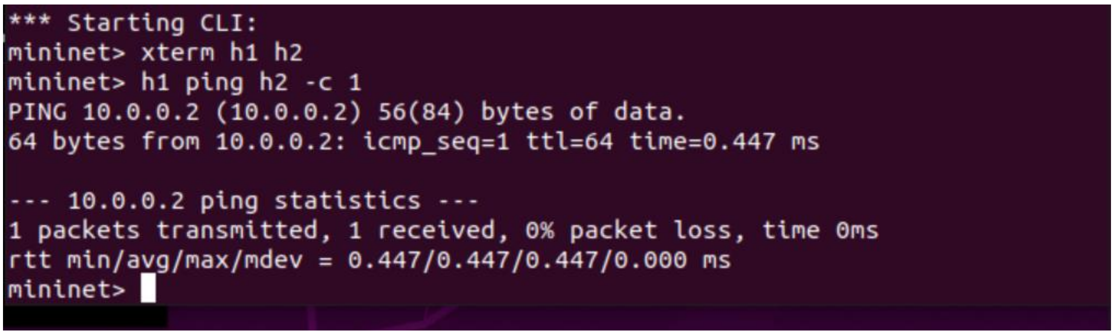
h1 received that reply

ICMP:

h1 sent ICMP request

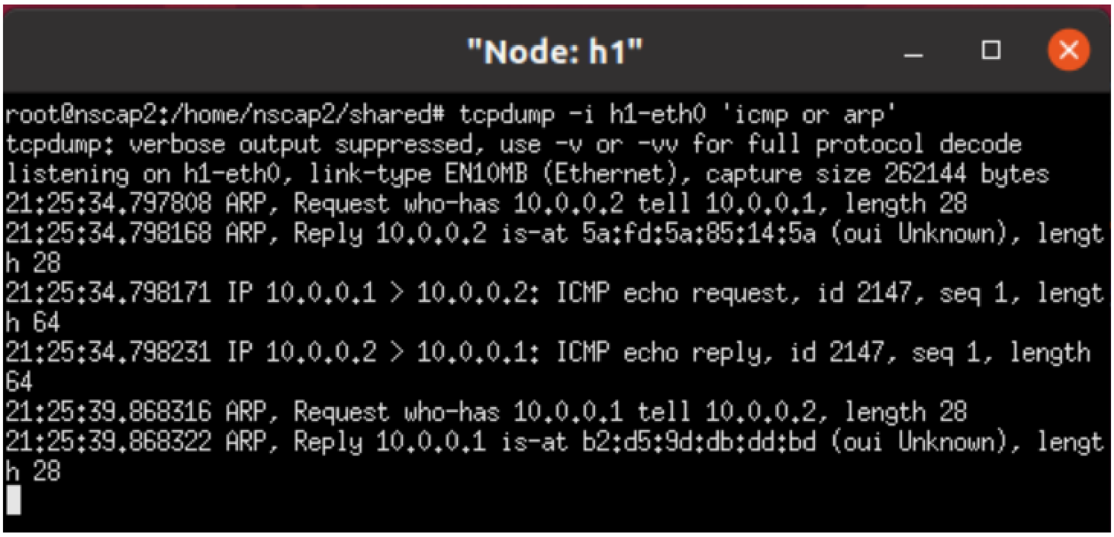
h2 received and replied

h1 received that reply

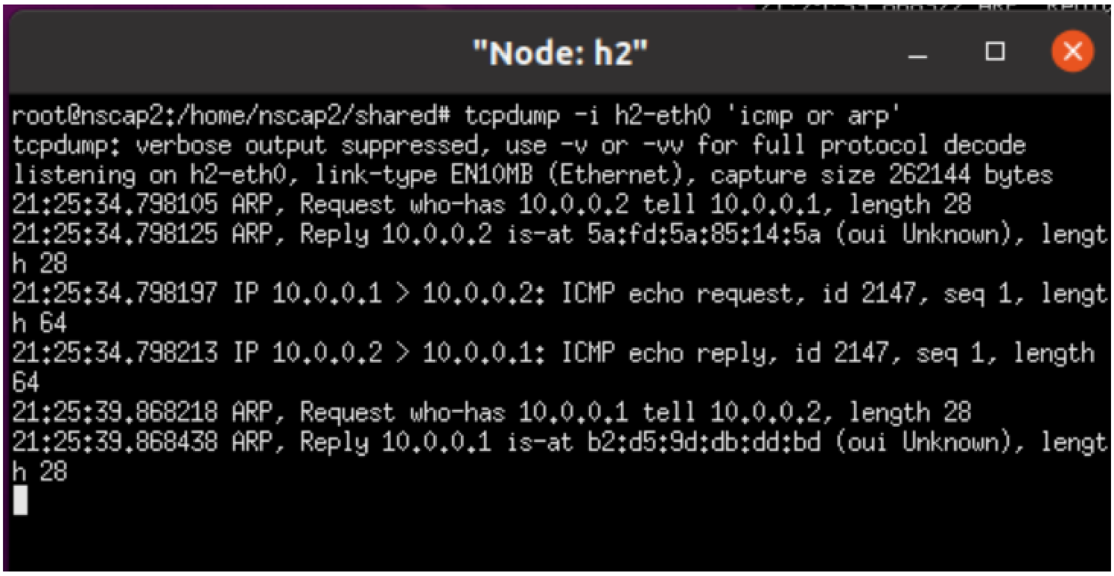


```
*** Starting CLI:
mininet> xterm h1 h2
mininet> h1 ping h2 -c 1
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.447 ms

--- 10.0.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.447/0.447/0.447/0.000 ms
mininet> 
```



```
root@nscap2:/home/nscap2/shared# tcpdump -i h1-eth0 'icmp or arp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on h1-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
21:25:34.797808 ARP, Request who-has 10.0.0.2 tell 10.0.0.1, length 28
21:25:34.798168 ARP, Reply 10.0.0.2 is-at 5a:fd:5a:85:14:5a (oui Unknown), lengt
h 28
21:25:34.798171 IP 10.0.0.1 > 10.0.0.2: ICMP echo request, id 2147, seq 1, lengt
h 64
21:25:34.798231 IP 10.0.0.2 > 10.0.0.1: ICMP echo reply, id 2147, seq 1, length
64
21:25:39.868316 ARP, Request who-has 10.0.0.1 tell 10.0.0.2, length 28
21:25:39.868322 ARP, Reply 10.0.0.1 is-at b2:d5:9d:db:dd:bd (oui Unknown), lengt
h 28
```



```
root@nscap2:/home/nscap2/shared# tcpdump -i h2-eth0 'icmp or arp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on h2-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
21:25:34.798105 ARP, Request who-has 10.0.0.2 tell 10.0.0.1, length 28
21:25:34.798125 ARP, Reply 10.0.0.2 is-at 5a:fd:5a:85:14:5a (oui Unknown), lengt
h 28
21:25:34.798197 IP 10.0.0.1 > 10.0.0.2: ICMP echo request, id 2147, seq 1, lengt
h 64
21:25:34.798213 IP 10.0.0.2 > 10.0.0.1: ICMP echo reply, id 2147, seq 1, length
64
21:25:39.868218 ARP, Request who-has 10.0.0.1 tell 10.0.0.2, length 28
21:25:39.868438 ARP, Reply 10.0.0.1 is-at b2:d5:9d:db:dd:bd (oui Unknown), lengt
h 28
```

2. When h1 ping h3, what will happen?

Explain every step of the ARP and ICMP packet using the explanation format in Question 1 and take screenshots of your results.

ARP:

h1 sent ARP request

h3 received and replied

h1 received that reply

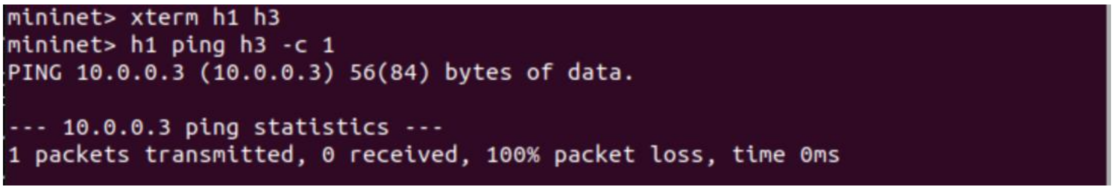
ICMP:

h1 sent ICMP request

h3 received and replied

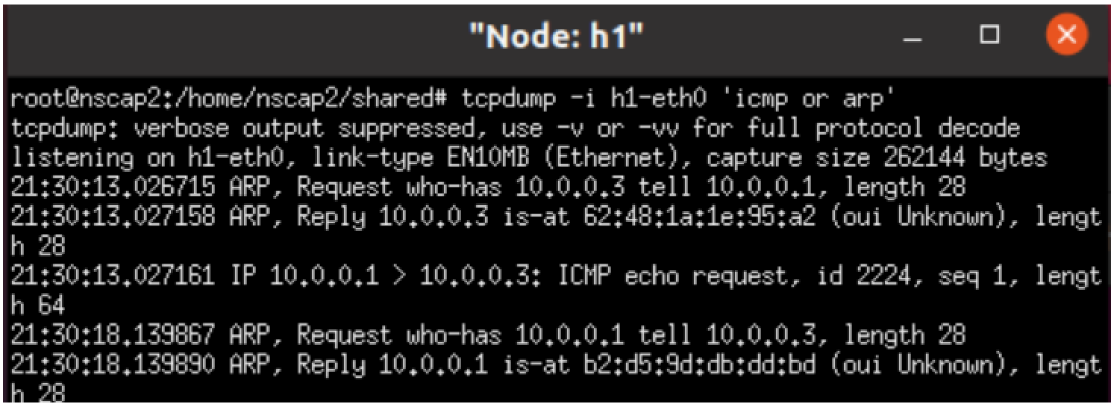
s1 dropped the reply

h1 did not receive that reply

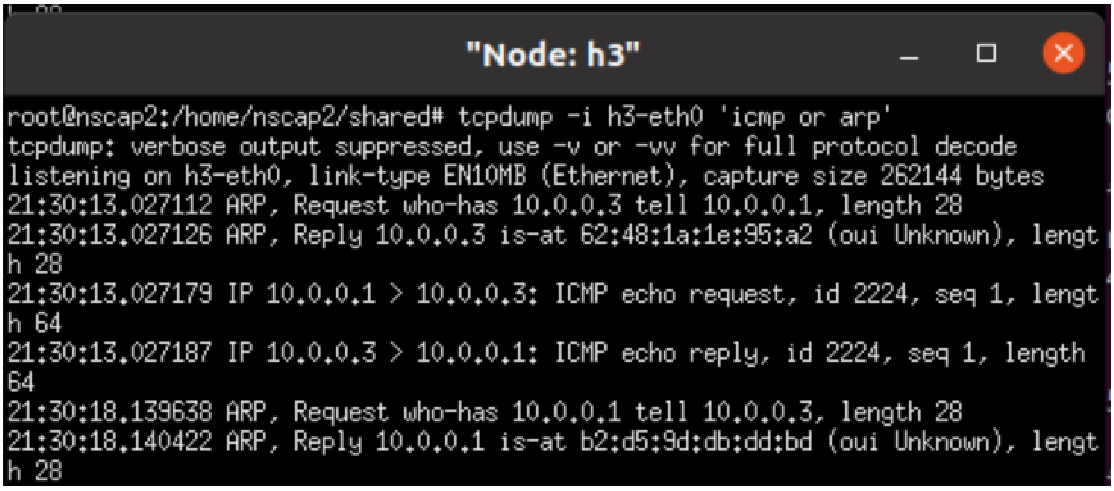


```
mininet> xterm h1 h3
mininet> h1 ping h3 -c 1
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.

--- 10.0.0.3 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```



```
root@nscap2:/home/nscap2/shared# tcpdump -i h1-eth0 'icmp or arp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on h1-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
21:30:13.026715 ARP, Request who-has 10.0.0.3 tell 10.0.0.1, length 28
21:30:13.027158 ARP, Reply 10.0.0.3 is-at 62:48:1a:1e:95:a2 (oui Unknown), lengt
h 28
21:30:13.027161 IP 10.0.0.1 > 10.0.0.3: ICMP echo request, id 2224, seq 1, lengt
h 64
21:30:18.139867 ARP, Request who-has 10.0.0.1 tell 10.0.0.3, length 28
21:30:18.139890 ARP, Reply 10.0.0.1 is-at b2:d5:9d:db:dd:bd (oui Unknown), lengt
h 28
```



```
root@nscap2:/home/nscap2/shared# tcpdump -i h3-eth0 'icmp or arp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on h3-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
21:30:13.027112 ARP, Request who-has 10.0.0.3 tell 10.0.0.1, length 28
21:30:13.027126 ARP, Reply 10.0.0.3 is-at 62:48:1a:1e:95:a2 (oui Unknown), lengt
h 28
21:30:13.027179 IP 10.0.0.1 > 10.0.0.3: ICMP echo request, id 2224, seq 1, lengt
h 64
21:30:13.027187 IP 10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2224, seq 1, length
64
21:30:18.139638 ARP, Request who-has 10.0.0.1 tell 10.0.0.3, length 28
21:30:18.140422 ARP, Reply 10.0.0.1 is-at b2:d5:9d:db:dd:bd (oui Unknown), lengt
h 28
```

3. **When h3 ping h2, what will happen?**
   Explain every step of the ARP and ICMP packet using the explanation format in Question 1 and take screenshots of your results.

   ARP:

   h3 sent ARP request

   h2 received and replied

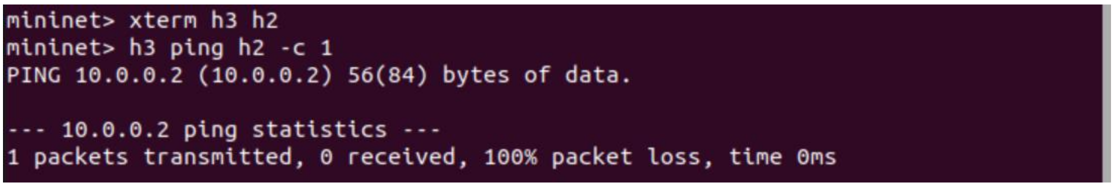
   h3 received that reply

   ICMP:

   h3 sent ICMP request

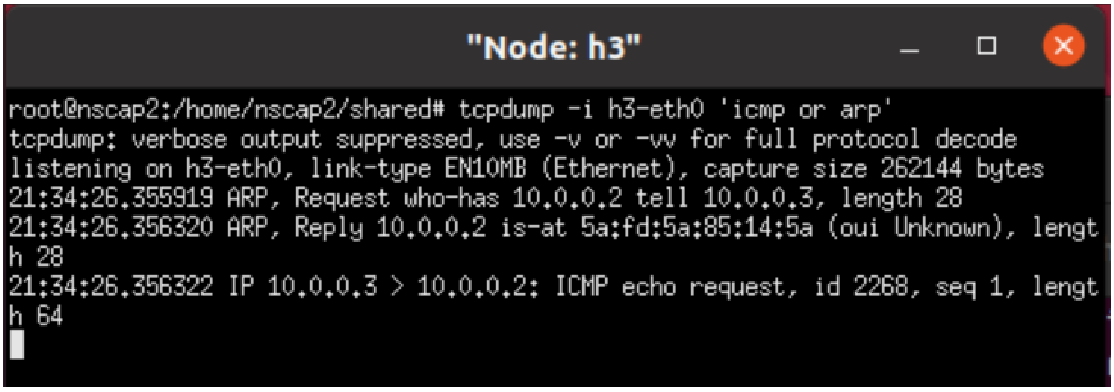
   s1 dropped the request

   h2 did not receive that request

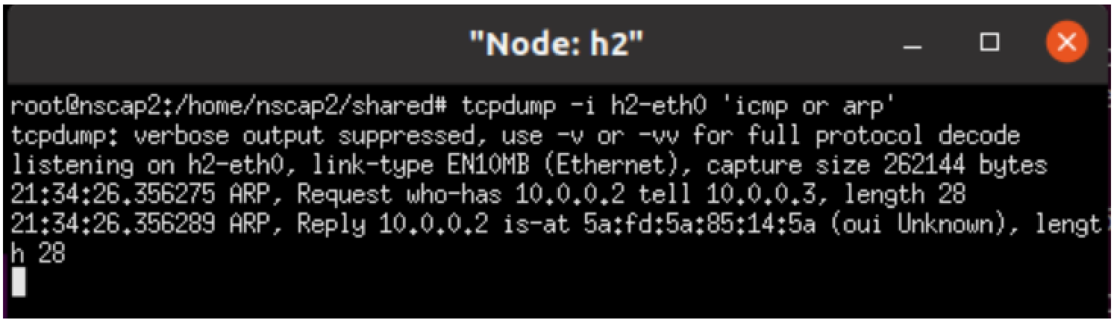


```
mininet> xterm h3 h2
mininet> h3 ping h2 -c 1
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.

--- 10.0.0.2 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```



```
root@nscap2:/home/nscap2/shared# tcpdump -i h3-eth0 'icmp or arp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on h3-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
21:34:26.355919 ARP, Request who-has 10.0.0.2 tell 10.0.0.3, length 28
21:34:26.356320 ARP, Reply 10.0.0.2 is-at 5a:fd:5a:85:14:5a (oui Unknown), lengt
h 28
21:34:26.356322 IP 10.0.0.3 > 10.0.0.2: ICMP echo request, id 2268, seq 1, lengt
h 64
█
```



```
root@nscap2:/home/nscap2/shared# tcpdump -i h2-eth0 'icmp or arp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on h2-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
21:34:26.356275 ARP, Request who-has 10.0.0.2 tell 10.0.0.3, length 28
21:34:26.356289 ARP, Reply 10.0.0.2 is-at 5a:fd:5a:85:14:5a (oui Unknown), lengt
h 28
```

4. **When h1 ping h5, what will happen?**
   Explain every step of the ARP and ICMP packet using the explanation format in Question 1 and take screenshots of your results.

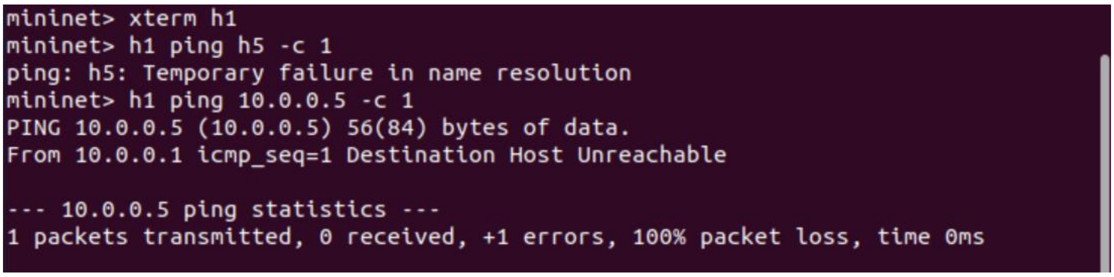
ARP:

h1 sent ARP request

h1 sent ARP request

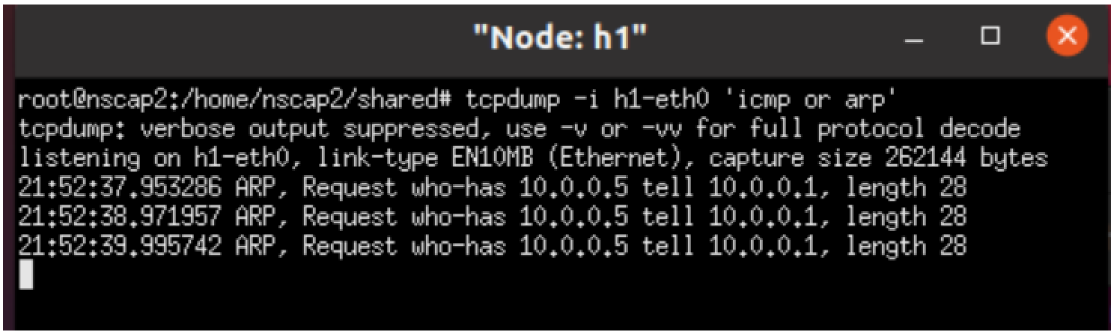
h1 sent ARP request

h5 did not receive that request

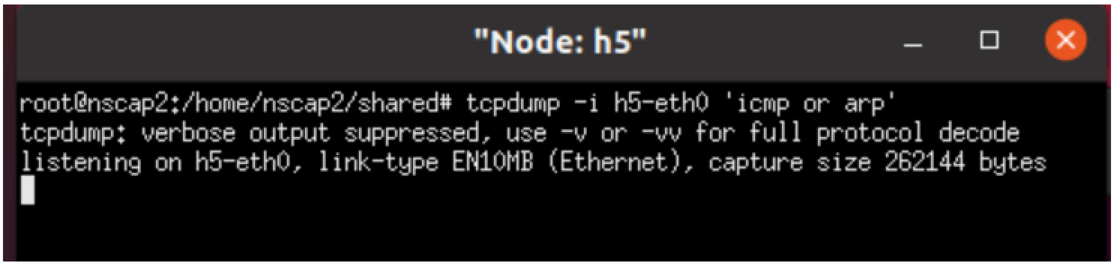


```
mininet> xterm h1
mininet> h1 ping h5 -c 1
ping: h5: Temporary failure in name resolution
mininet> h1 ping 10.0.0.5 -c 1
PING 10.0.0.5 (10.0.0.5) 56(84) bytes of data.
From 10.0.0.1 icmp_seq=1 Destination Host Unreachable

--- 10.0.0.5 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```



```
root@nscap2:/home/nscap2/shared# tcpdump -i h1-eth0 'icmp or arp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on h1-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
21:52:37.953286 ARP, Request who-has 10.0.0.5 tell 10.0.0.1, length 28
21:52:38.971957 ARP, Request who-has 10.0.0.5 tell 10.0.0.1, length 28
21:52:39.995742 ARP, Request who-has 10.0.0.5 tell 10.0.0.1, length 28
```



```
root@nscap2:/home/nscap2/shared# tcpdump -i h5-eth0 'icmp or arp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on h5-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Part 2

5. **When h1 ping h5, what will happen?**
   Explain every step of the ARP and ICMP packet using the explanation format in Question 1 and take screenshots of your results.
   (It should be possible for h1 to successfully ping h5 if the GRE tunnel has been correctly established.)

ARP:

h1 sent ARP request

h5 received and replied

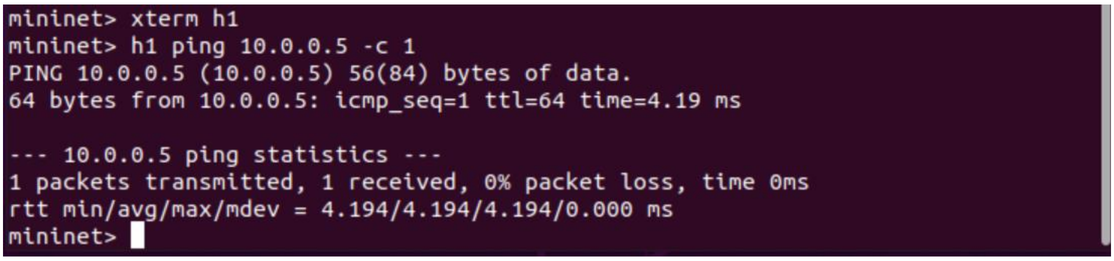
h1 received that reply

ICMP:

h1 sent ICMP request

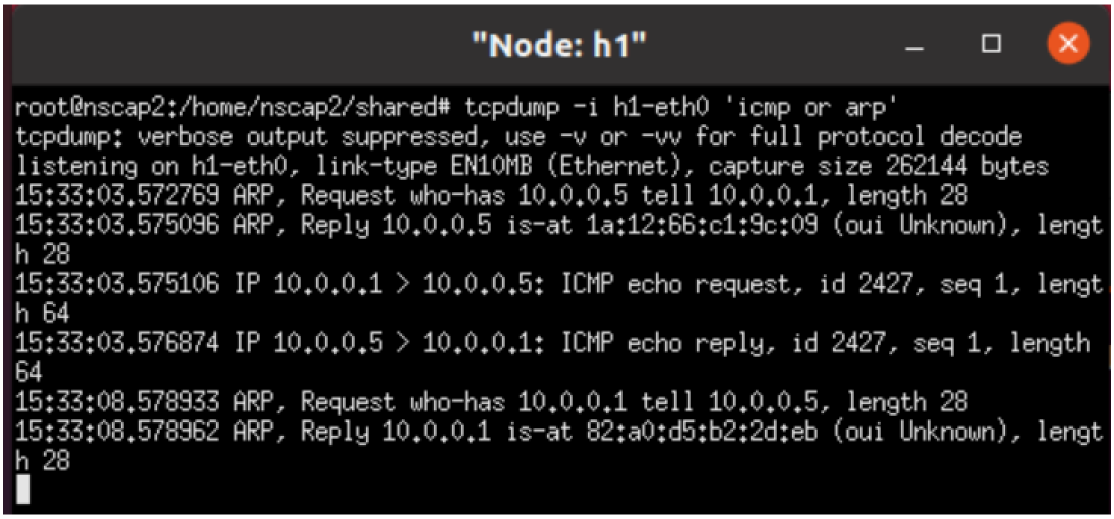
h5 received and replied

h1 received that reply



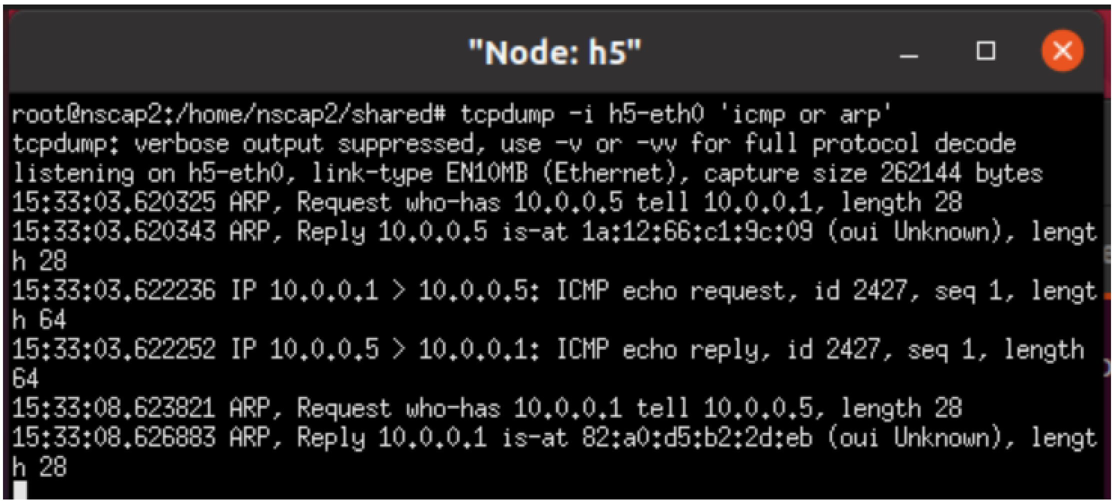
```
mininet> xterm h1
mininet> h1 ping 10.0.0.5 -c 1
PING 10.0.0.5 (10.0.0.5) 56(84) bytes of data.
64 bytes from 10.0.0.5: icmp_seq=1 ttl=64 time=4.19 ms

--- 10.0.0.5 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.194/4.194/4.194/0.000 ms
mininet> 
```



"Node: h1"

```
root@nscap2:/home/nscap2/shared# tcpdump -i h1-eth0 'icmp or arp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on h1-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:33:03.572769 ARP, Request who-has 10.0.0.5 tell 10.0.0.1, length 28
15:33:03.575096 ARP, Reply 10.0.0.5 is-at 1a:12:66:c1:9c:09 (oui Unknown), lengt
h 28
15:33:03.575106 IP 10.0.0.1 > 10.0.0.5: ICMP echo request, id 2427, seq 1, lengt
h 64
15:33:03.576874 IP 10.0.0.5 > 10.0.0.1: ICMP echo reply, id 2427, seq 1, length
64
15:33:08.578933 ARP, Request who-has 10.0.0.1 tell 10.0.0.5, length 28
15:33:08.578962 ARP, Reply 10.0.0.1 is-at 82:a0:d5:b2:2d:eb (oui Unknown), lengt
h 28
```



```
root@nscap2:/home/nscap2/shared# tcpdump -i h5-eth0 'icmp or arp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on h5-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:33:03.620325 ARP, Request who-has 10.0.0.5 tell 10.0.0.1, length 28
15:33:03.620343 ARP, Reply 10.0.0.5 is-at 1a:12:66:c1:9c:09 (oui Unknown), lengt
h 28
15:33:03.622236 IP 10.0.0.1 > 10.0.0.5: ICMP echo request, id 2427, seq 1, lengt
h 64
15:33:03.622252 IP 10.0.0.5 > 10.0.0.1: ICMP echo reply, id 2427, seq 1, length
64
15:33:08.623821 ARP, Request who-has 10.0.0.1 tell 10.0.0.5, length 28
15:33:08.626883 ARP, Reply 10.0.0.1 is-at 82:a0:d5:b2:2d:eb (oui Unknown), lengt
h 28
```

6. **When h1 ping h7, what will happen?**

   Explain every step of the ARP and ICMP packet using the explanation format in Question 1 and take screenshots of your results.

ARP:

h1 sent ARP request

h7 received and replied

h1 received that reply

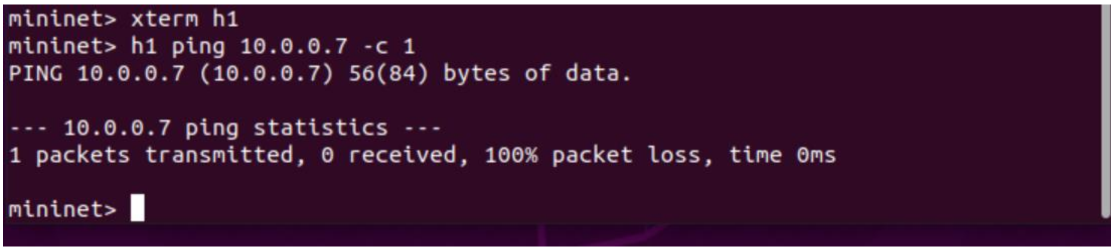
ICMP:

h1 sent ICMP request

h7 received and replied

s2 dropped the reply

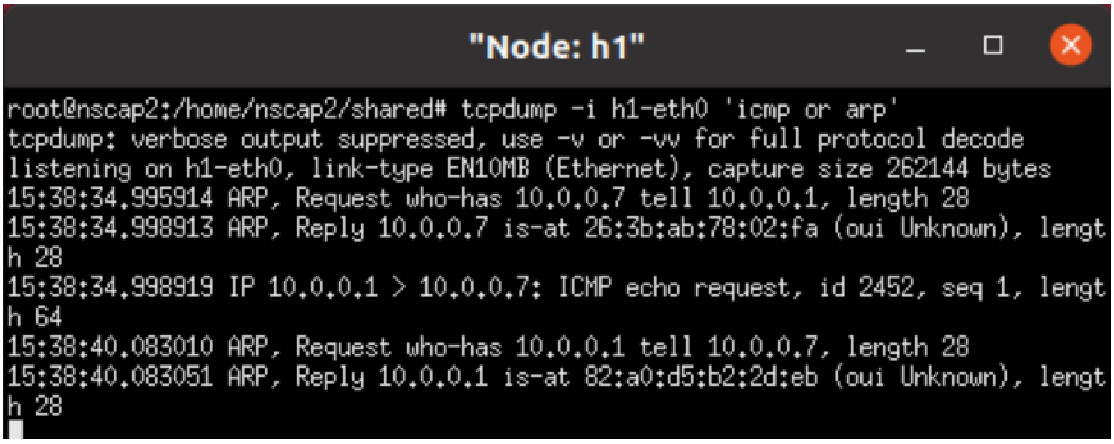
h1 did not received that reply



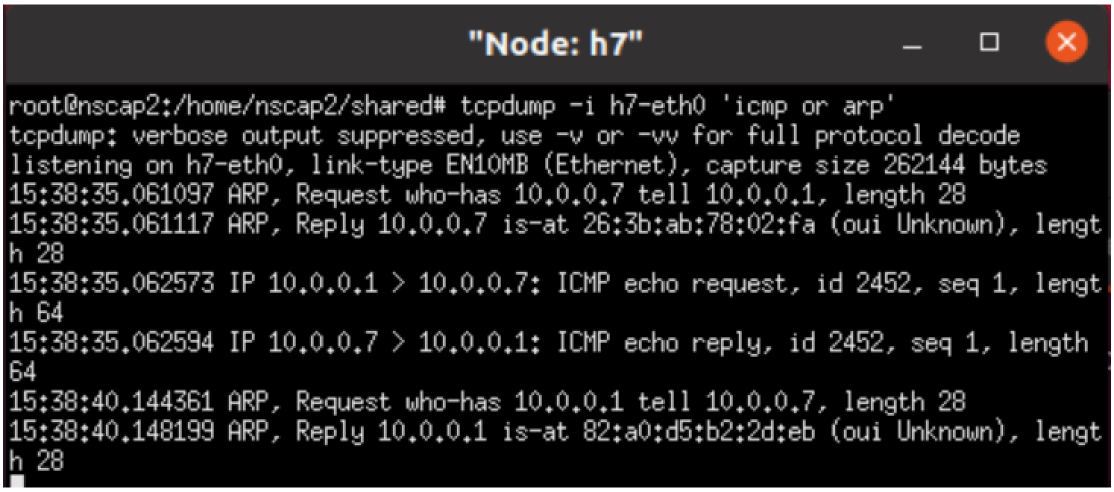
```
mininet> xterm h1
mininet> h1 ping 10.0.0.7 -c 1
PING 10.0.0.7 (10.0.0.7) 56(84) bytes of data.

--- 10.0.0.7 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

mininet> 
```



```
root@nscap2:/home/nscap2/shared# tcpdump -i h1-eth0 'icmp or arp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on h1-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:38:34.995914 ARP, Request who-has 10.0.0.7 tell 10.0.0.1, length 28
15:38:34.998913 ARP, Reply 10.0.0.7 is-at 26:3b:ab:78:02:fa (oui Unknown), lengt
h 28
15:38:34.998919 IP 10.0.0.1 > 10.0.0.7: ICMP echo request, id 2452, seq 1, lengt
h 64
15:38:40.083010 ARP, Request who-has 10.0.0.1 tell 10.0.0.7, length 28
15:38:40.083051 ARP, Reply 10.0.0.1 is-at 82:a0:d5:b2:2d:eb (oui Unknown), lengt
h 28
```



```
root@nscap2:/home/nscap2/shared# tcpdump -i h7-eth0 'icmp or arp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on h7-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:38:35.061097 ARP, Request who-has 10.0.0.7 tell 10.0.0.1, length 28
15:38:35.061117 ARP, Reply 10.0.0.7 is-at 26:3b:ab:78:02:fa (oui Unknown), lengt
h 28
15:38:35.062573 IP 10.0.0.1 > 10.0.0.7: ICMP echo request, id 2452, seq 1, lengt
h 64
15:38:35.062594 IP 10.0.0.7 > 10.0.0.1: ICMP echo reply, id 2452, seq 1, length
64
15:38:40.144361 ARP, Request who-has 10.0.0.1 tell 10.0.0.7, length 28
15:38:40.148199 ARP, Reply 10.0.0.1 is-at 82:a0:d5:b2:2d:eb (oui Unknown), lengt
h 28
```

7. When h7 ping h1, what will happen?
Explain every step of the ARP and ICMP packet using the explanation format in Question 1 and take screenshots of your results.

ARP:

h7 sent ARP request

h1 received and replied

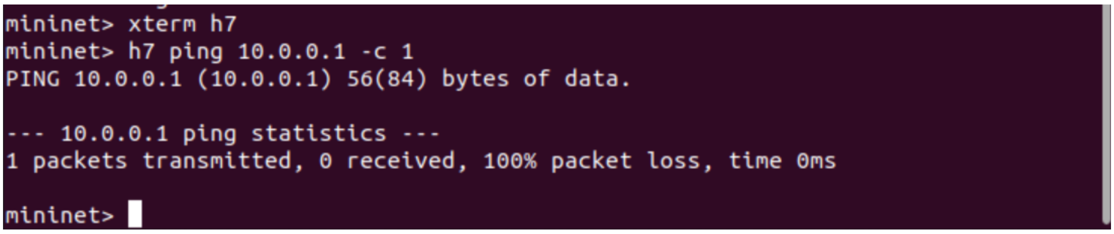
h7 received that reply

ICMP:

h7 sent ICMP request

s2 dropped the request

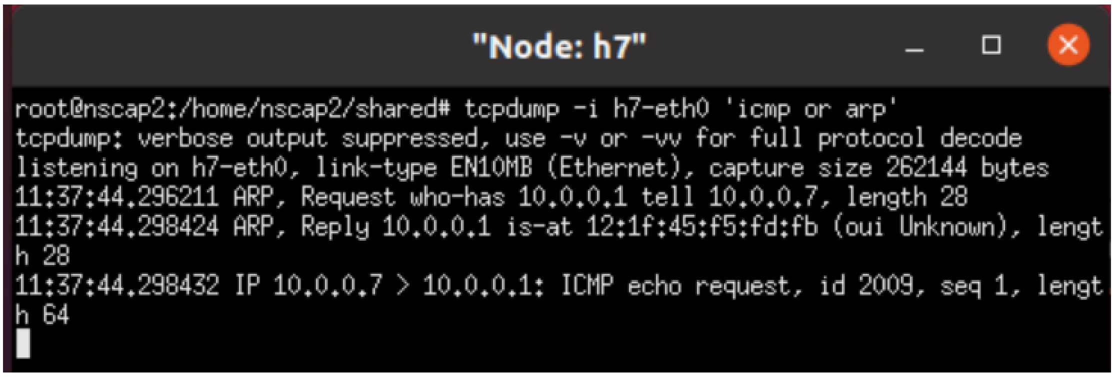
h1 did not received that request



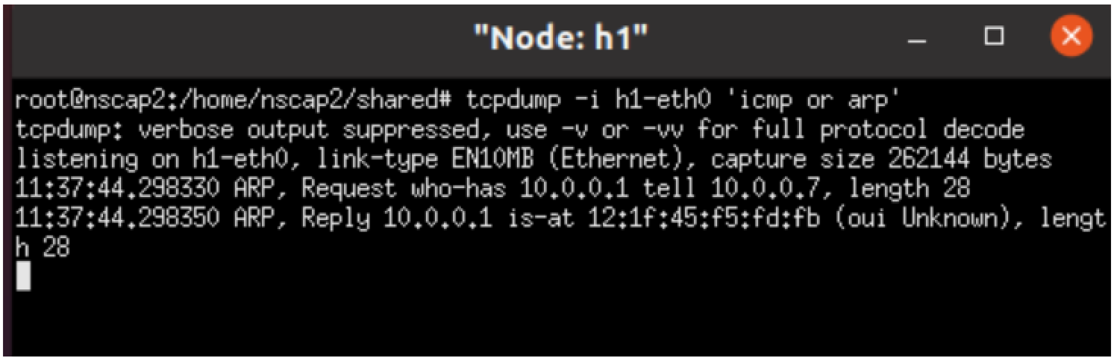
```
mininet> xterm h7
mininet> h7 ping 10.0.0.1 -c 1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.

--- 10.0.0.1 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

mininet> 
```



```
root@nscap2:/home/nscap2/shared# tcpdump -i h7-eth0 'icmp or arp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on h7-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:37:44.296211 ARP, Request who-has 10.0.0.1 tell 10.0.0.7, length 28
11:37:44.298424 ARP, Reply 10.0.0.1 is-at 12:1f:45:f5:fd:fb (oui Unknown), lengt
h 28
11:37:44.298432 IP 10.0.0.7 > 10.0.0.1: ICMP echo request, id 2009, seq 1, lengt
h 64
```

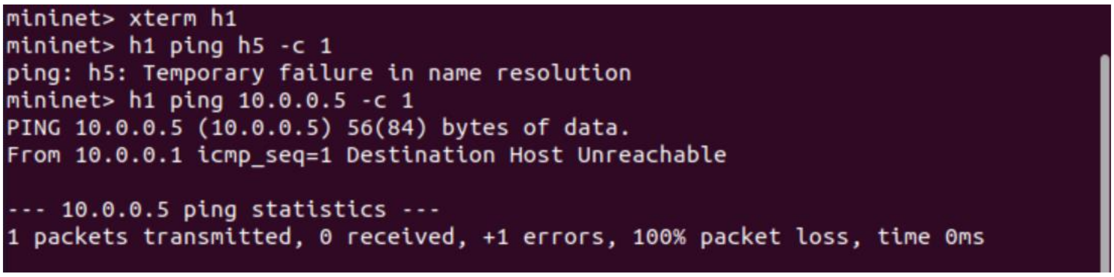


```
root@nscap2:/home/nscap2/shared# tcpdump -i h1-eth0 'icmp or arp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on h1-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:37:44.298330 ARP, Request who-has 10.0.0.1 tell 10.0.0.7, length 28
11:37:44.298350 ARP, Reply 10.0.0.1 is-at 12:1f:45:f5:fd:fb (oui Unknown), lengt
h 28
```

8. **If the packet in Question 6 or 7 is dropped in some part of the network, are the outcome and explanation the same as that of Question 4? (use screenshots to prove your answers)**

   Not the same as Q4, since h1 and h5 in Q4 did not connect at that time, even ARP request cannot reach h5. However, in Q6 and Q7, the topology is connected, so ARP can be received, therefore, it may think that it is due to a packet loss not host unreachable.

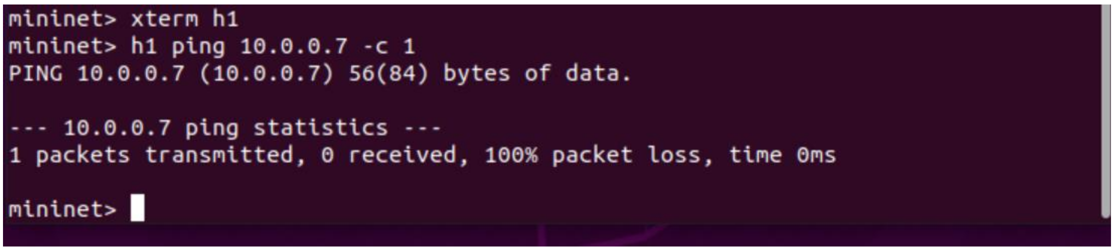
In Q4:



```
mininet> xterm h1
mininet> h1 ping h5 -c 1
ping: h5: Temporary failure in name resolution
mininet> h1 ping 10.0.0.5 -c 1
PING 10.0.0.5 (10.0.0.5) 56(84) bytes of data.
From 10.0.0.1 icmp_seq=1 Destination Host Unreachable

--- 10.0.0.5 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

In Q6:

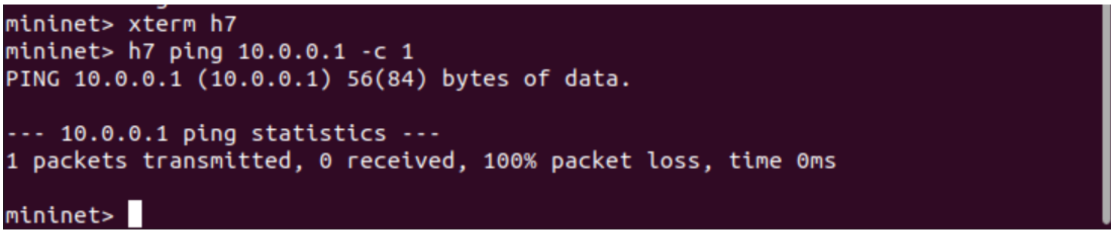


```
mininet> xterm h1
mininet> h1 ping 10.0.0.7 -c 1
PING 10.0.0.7 (10.0.0.7) 56(84) bytes of data.

--- 10.0.0.7 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

mininet> 
```

In Q7:



```
mininet> xterm h7
mininet> h7 ping 10.0.0.1 -c 1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.

--- 10.0.0.1 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

mininet> 
```

9. **Change filter_table2 rule**
   a. **From the original rule: packets coming from port_3 or port_4 will be dropped, while other packets will be allowed to pass.**
      To the new rule: packets coming from port_1 or port_2 will be allowed to pass, while other packets will be dropped.
   b. **Will the outcome of Questions 5, 6, and 7 differ? (no need to print screenshots) Explain your answers.**

   Since GRE tunnel represent port 5 of the switch, if the rule become "packets coming from port_1 or port_2 will be allowed to pass, while other packets will be dropped", then Q5, Q6, Q7 will all packet loss for the reason that any ICMP from port 5 will be dropped by the switch. This is different from the situation when using the original rule, since under the original rule, packet from the GRE tunnel can be forwarded by the switch.