14/14 Questions Answered

1 question with unsaved changes

选择文件 未选择任何文件

Lab 2: A single segment network

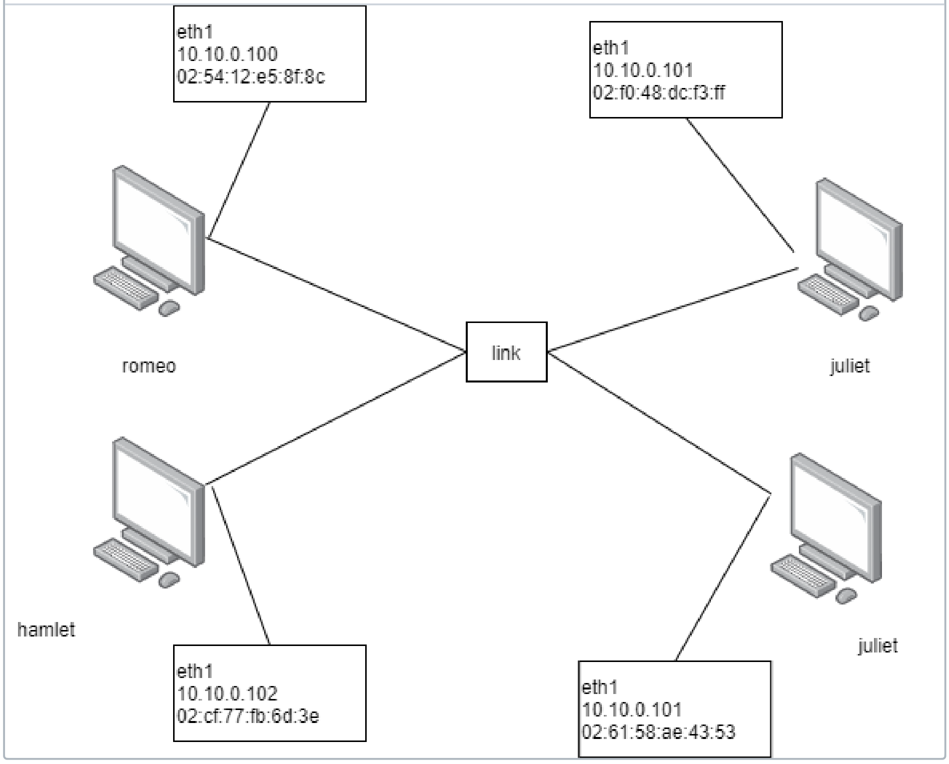
Q1 Network diagram

1 Point

Draw a diagram of the topology, and label each (experiment) network interface with its name, IP address, and MAC address. Upload your diagram (as a PDF, PNG, or JPG) here.

CURRENTLY UPLOADED FILES

diagram.png Download ✖ Remove



Please select file(s) Select file(s)

Also show the output of `ifconfig -a` on each host, either by copying and pasting from your terminal output, or as a screenshot. Make sure you show the terminal prompt and the complete `ifconfig` command, in addition to the output. Crop your screenshot if necessary so that *only* the relevant part is included, not everything that happened to be on the screen at the time.

选择文件 未选择任何文件

```
ty2069@romeo:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 02:d0:fa:c7:99:2b
          inet addr:172.17.1.21  Bcast:172.31.255.255
Mask:255.240.0.0
          inet6 addr: fe80::d0:faff:fec7:992b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:1
          RX packets:1129 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1147 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:114366 (114.3 KB)  TX bytes:103014 (103.0 KB)

eth1      Link encap:Ethernet  HWaddr 02:54:12:e5:8f:8c
          inet addr:10.10.0.100  Bcast:10.10.0.255
Mask:255.255.255.0
          inet6 addr: fe80::54:12ff:fee5:8f8c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:1
          RX packets:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7688 (7.6 KB)  TX bytes:1576 (1.5 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1560 (1.5 KB)  TX bytes:1560 (1.5 KB)

ty2069@juliet:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 02:6c:54:4e:83:11
          inet addr:172.17.2.15  Bcast:172.31.255.255
Mask:255.240.0.0
          inet6 addr: fe80::6c:54ff:fe4e:8311/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:1
          RX packets:1950 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18347 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:147794 (147.7 KB)  TX bytes:2085854 (2.0 MB)
```

```
eth1      Link encap:Ethernet  HWaddr 02:f0:48:dc:f3:ff
```

选择文件 未选择任何文件

```
          inet addr:10.10.0.101  Bcast:10.10.0.255
Mask:255.255.255.0
          inet6 addr: fe80::f0:48ff:fedc:f3ff/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6816 (6.8 KB)  TX bytes:2322 (2.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1560 (1.5 KB)  TX bytes:1560 (1.5 KB)



ty2069@hamlet:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 02:48:ed:08:72:7b
          inet addr:172.17.3.21  Bcast:172.31.255.255
Mask:255.240.0.0
          inet6 addr: fe80::48:edff:fe08:727b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:1
          RX packets:1106 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:112863 (112.8 KB)  TX bytes:101357 (101.3 KB)

eth1      Link encap:Ethernet  HWaddr 02:cf:77:fb:6d:3e
          inet addr:10.10.0.102  Bcast:10.10.0.255
Mask:255.255.255.0
          inet6 addr: fe80::cf:77ff:fefb:6d3e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7640 (7.6 KB)  TX bytes:1568 (1.5 KB)
```

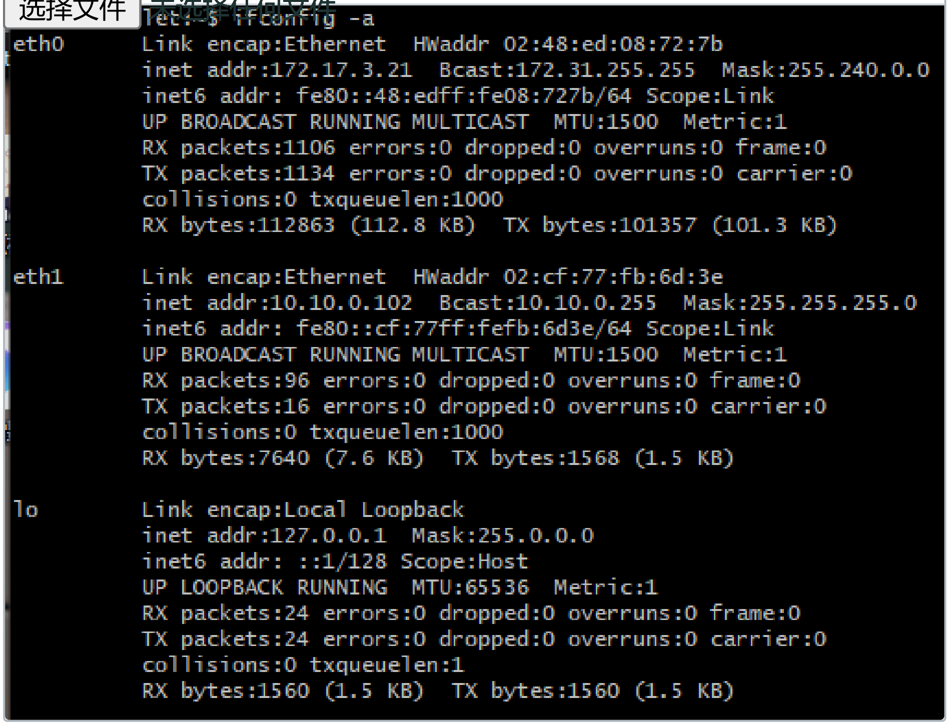
选择文件 未选择任何文件

```
          Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1560 (1.5 KB)  TX bytes:1560 (1.5 KB)



ty2069@ophelia:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 02:7d:be:91:e6:d3
          inet addr:172.17.2.16  Bcast:172.31.255.255
Mask:255.240.0.0
          inet6 addr: fe80::7d:beff:fe91:e6d3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:1
          RX packets:1564 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9007 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:132477 (132.4 KB)  TX bytes:1002685 (1.0 MB)

eth1      Link encap:Ethernet  HWaddr 02:10:bb:a5:3e:4b
          inet addr:10.10.0.103  Bcast:10.10.0.255
Mask:255.255.255.0
          inet6 addr: fe80::10:bbff:fea5:3e4b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:1
          RX packets:62 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4104 (4.1 KB)  TX bytes:1980 (1.9 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1560 (1.5 KB)  TX bytes:1560 (1.5 KB)
```

CURRENTLY UPLOADED FILES

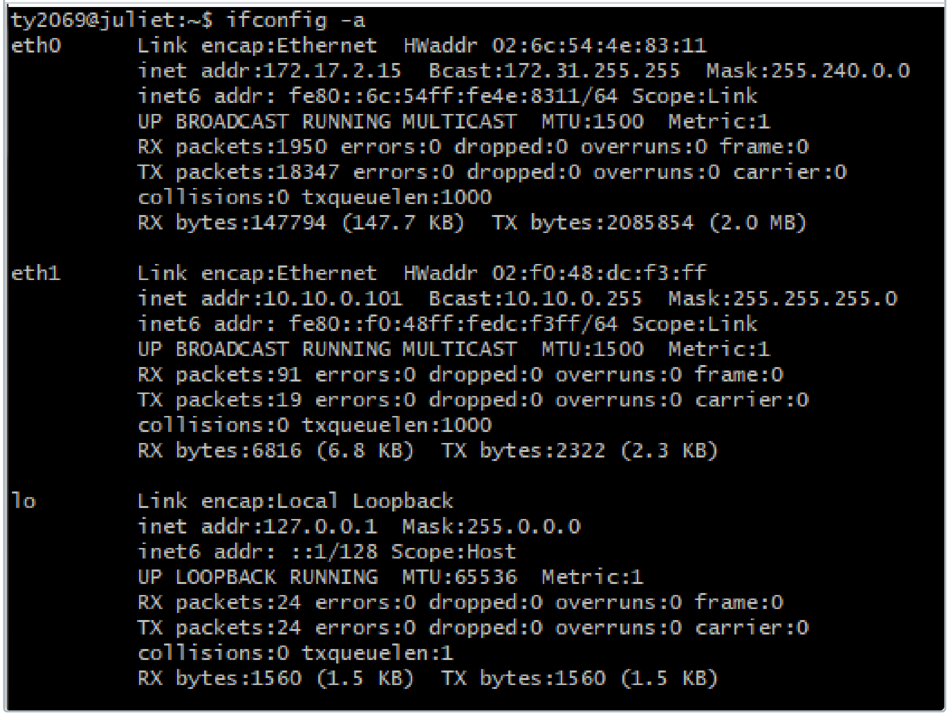
hamlet.PNG Download ✖ Remove

选择文件 未选择任何文件



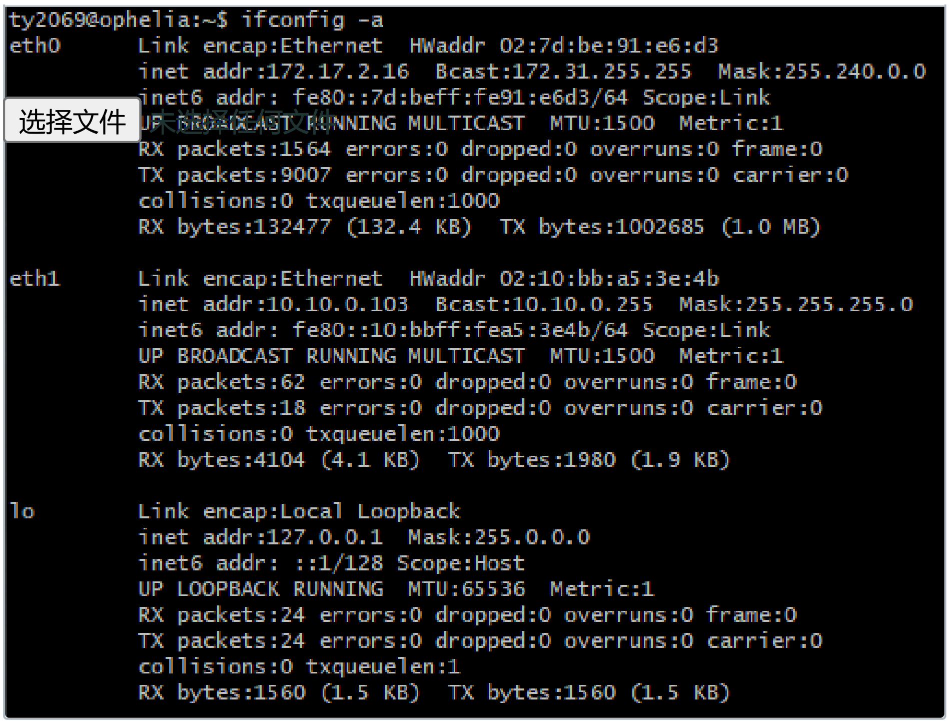
```
let:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 02:48:ed:08:72:7b
          inet addr:172.17.3.21  Bcast:172.31.255.255  Mask:255.240.0.0
          inet6 addr: fe80::48:edff:fe08:727b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1106 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:112863 (112.8 KB)  TX bytes:101357 (101.3 KB)

eth1      Link encap:Ethernet  HWaddr 02:cf:77:fb:6d:3e
          inet addr:10.10.0.102  Bcast:10.10.0.255  Mask:255.255.255.0
          inet6 addr: fe80::cf:77ff:fefb:6d3e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7640 (7.6 KB)  TX bytes:1568 (1.5 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1560 (1.5 KB)  TX bytes:1560 (1.5 KB)
```

juliet.PNG Download ✖ Remove



```
ty2069@juliet:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 02:6c:54:4e:83:11
          inet addr:172.17.2.15  Bcast:172.31.255.255  Mask:255.240.0.0
          inet6 addr: fe80::6c:54ff:fe4e:8311/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1950 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18347 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:147794 (147.7 KB)  TX bytes:2085854 (2.0 MB)

eth1      Link encap:Ethernet  HWaddr 02:f0:48:dc:f3:ff
          inet addr:10.10.0.101  Bcast:10.10.0.255  Mask:255.255.255.0
          inet6 addr: fe80::f0:48ff:fedc:f3ff/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6816 (6.8 KB)  TX bytes:2322 (2.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1560 (1.5 KB)  TX bytes:1560 (1.5 KB)
```

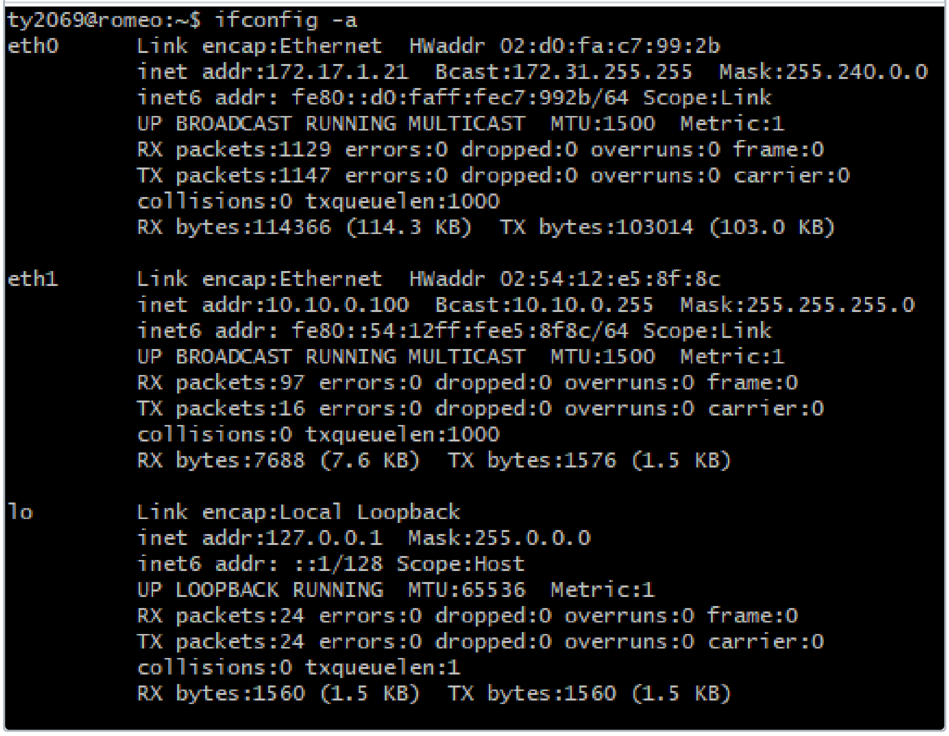
ophelia.PNG Download ✖ Remove



选择文件 未选择任何文件

```
ty2069@ophelia:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 02:7d:be:91:e6:d3
          inet addr:172.17.2.16  Bcast:172.31.255.255  Mask:255.240.0.0
          inet6 addr: fe80::7d:beff:fe91:e6d3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1564 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9007 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:132477 (132.4 KB)  TX bytes:1002685 (1.0 MB)

eth1      Link encap:Ethernet  HWaddr 02:10:bb:a5:3e:4b
          inet addr:10.10.0.103  Bcast:10.10.0.255  Mask:255.255.255.0
          inet6 addr: fe80::10:bbff:fea5:3e4b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:62 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4104 (4.1 KB)  TX bytes:1980 (1.9 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1560 (1.5 KB)  TX bytes:1560 (1.5 KB)
```

▾ romeo.PNG Download ✖ Remove



```
ty2069@romeo:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 02:d0:fa:c7:99:2b
          inet addr:172.17.1.21  Bcast:172.31.255.255  Mask:255.240.0.0
          inet6 addr: fe80::d0:faff:fec7:992b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1129 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1147 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:114366 (114.3 KB)  TX bytes:103014 (103.0 KB)

eth1      Link encap:Ethernet  HWaddr 02:54:12:e5:8f:8c
          inet addr:10.10.0.100  Bcast:10.10.0.255  Mask:255.255.255.0
          inet6 addr: fe80::54:12ff:fee5:8f8c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7688 (7.6 KB)  TX bytes:1576 (1.5 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1560 (1.5 KB)  TX bytes:1560 (1.5 KB)
```

Please select file(s) Select file(s)

Save Answer Last saved on **Sep 24 at 9:03 PM**

Q2 2.6 Network interface exercises (Exercise 2)

1 Point

Show the output of the `tcpdump` in each case (four total `tcpdump` outputs) (either paste the text here, or upload a screenshot). Make

选择文件 未选择任何文件

early label which case is which. Crop your screenshot if necessary so that *only* the relevant part is included, not everything that happened to be on the screen at the time.

```
ty2069@romeo:~$ sudo tcpdump -n -i eth1 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel

ty2069@romeo:~$ sudo tcpdump -n -i eth1 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel

ty2069@romeo:~$ sudo tcpdump -n -i lo icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
03:09:30.629316 IP 127.0.0.1 > 127.0.0.1: ICMP echo request, id 3121, seq 1, length 64
03:09:30.629336 IP 127.0.0.1 > 127.0.0.1: ICMP echo reply, id 3121, seq 1, length 64
03:09:31.630668 IP 127.0.0.1 > 127.0.0.1: ICMP echo request, id 3121, seq 2, length 64
03:09:31.630691 IP 127.0.0.1 > 127.0.0.1: ICMP echo reply, id 3121, seq 2, length 64
03:09:32.629660 IP 127.0.0.1 > 127.0.0.1: ICMP echo request, id 3121, seq 3, length 64
03:09:32.629682 IP 127.0.0.1 > 127.0.0.1: ICMP echo reply, id 3121, seq 3, length 64
```

```
^C
6 packets captured
12 packets received by filter
0 packets dropped by kernel

ty2069@romeo:~$ sudo tcpdump -n -i lo icmp
tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size
262144 bytes
03:10:39.897134 IP 10.10.0.100 > 10.10.0.100: ICMP echo request,
id 3125, seq 1, length 64
03:10:39.897160 IP 10.10.0.100 > 10.10.0.100: ICMP echo reply, id
3125, seq 1, length 64
03:10:40.898585 IP 10.10.0.100 > 10.10.0.100: ICMP echo
request, id 3125, seq 2, length 64
03:10:40.898610 IP 10.10.0.100 > 10.10.0.100: ICMP echo reply, id
3125, seq 2, length 64
03:10:41.897600 IP 10.10.0.100 > 10.10.0.100: ICMP echo request,
id 3125, seq 3, length 64
03:10:41.897625 IP 10.10.0.100 > 10.10.0.100: ICMP echo reply, id
3125, seq 3, length 64
^C
6 packets captured
12 packets received by filter
0 packets dropped by kernel
```

选择文件 未选择任何文件

CURRENTLY UPLOADED FILES

Please select file(s) Select file(s)

Which network interface carries traffic from the host *to itself* when that traffic is sent to the 127.0.0.1 address? Give the interface name, e.g. `lo`, `eth0`, `eth1`, etc. with no explanation.

lo

Which network interface carries traffic from the host *to itself* when that traffic is sent to the 10.10.0.100 address? Give the interface name, e.g. `lo`, `eth0`, `eth1`, etc. with no explanation.

lo

Explain how the evidence from the `tcpdump` output supports your answer.

选择文件 未选择任何文件

Since we only got packets when we specify the interface as lo when we call tcpdump.

Save Answer Last saved on **Sep 24 at 9:03 PM**

Q3 2.7 ARP exercises

2 Points

Q3.1 ARP (Exercise 4)

0.5 Points

Show the summary `tcpdump` output for both packet captures (either paste the text here, or upload a screenshot). The "summary `tcpdump` output" is the output you see when you play back the packet capture using the `-r` argument to `tcpdump`, as described in the instructions. Crop your screenshot if necessary so that *only* the relevant part is included, not everything that happened to be on the screen at the time.

```
ty2069@romeo:~$ arp -i eth1 -n
arp: in 5 entries no match found.



ty2069@romeo:~$ arp -i eth1 -n
Address                  HWtype  HWaddress           Flags Mask
Iface
10.10.0.101              ether   02:f0:48:dc:f3:ff   C                     eth1


ty2069@romeo:~$ tcpdump -enX -r $(hostname -s)-arp.pcap
reading from file romeo-arp.pcap, link-type EN10MB (Ethernet)
03:20:32.954612 02:54:12:e5:8f:8c > ff:ff:ff:ff:ff:ff, ethertype ARP
(0x0806), length 42: Request who-has 10.10.0.101 tell 10.10.0.100,
length 28
        0x0000:  0001 0800 0604 0001 0254 12e5 8f8c 0a0a
.........T......
        0x0010:  0064 0000 0000 0000 0a0a 0065
```

```
.d.........e
03:20:32.955677 02:f0:48:dc:f3:ff > 02:54:12:e5:8f:8c,
选择文件 未选择任何文件 ethertype ARP (0x0806), length 60: Reply 10.10.0.101 is-at
02:f0:48:dc:f3:ff, length 46
        0x0000:  0001 0800 0604 0002 02f0 48dc f3ff 0a0a
..........H.....
        0x0010:  0065 0254 12e5 8f8c 0a0a 0064 0000 0000
.e.T.......d....
        0x0020:  0000 0000 0000 0000 0000 0000 0000
..............
03:20:32.955689 02:54:12:e5:8f:8c > 02:f0:48:dc:f3:ff,
ethertype IPv4 (0x0800), length 98: 10.10.0.100 > 10.10.0.101:
ICMP echo request, id 3159, seq 1, length 64
        0x0000:  4500 0054 e1f0 4000 4001 43dc 0a0a 0064
E..T..@.@.C....d
        0x0010:  0a0a 0065 0800 cd90 0c57 0001 4054 685f
...e.....W..@Th_
        0x0020:  0000 0000 a890 0e00 0000 0000 1011 1213
................
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
$%&'()*+,-./0123
        0x0050:  3435 3637                                4567
03:20:32.956735 02:f0:48:dc:f3:ff > 02:54:12:e5:8f:8c,
ethertype IPv4 (0x0800), length 98: 10.10.0.101 > 10.10.0.100:
ICMP echo reply, id 3159, seq 1, length 64
        0x0000:  4500 0054 6809 0000 4001 fdc3 0a0a 0065
E..Th...@......e
        0x0010:  0a0a 0064 0000 d590 0c57 0001 4054 685f
...d.....W..@Th_
        0x0020:  0000 0000 a890 0e00 0000 0000 1011 1213
................
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
$%&'()*+,-./0123
        0x0050:  3435 3637                                4567
03:20:37.964125 02:f0:48:dc:f3:ff > 02:54:12:e5:8f:8c, ethertype
ARP (0x0806), length 60: Request who-has 10.10.0.100 tell
10.10.0.101, length 46
        0x0000:  0001 0800 0604 0001 02f0 48dc f3ff 0a0a
..........H.....
        0x0010:  0065 0000 0000 0000 0a0a 0064 0000 0000
.e.........d....
```

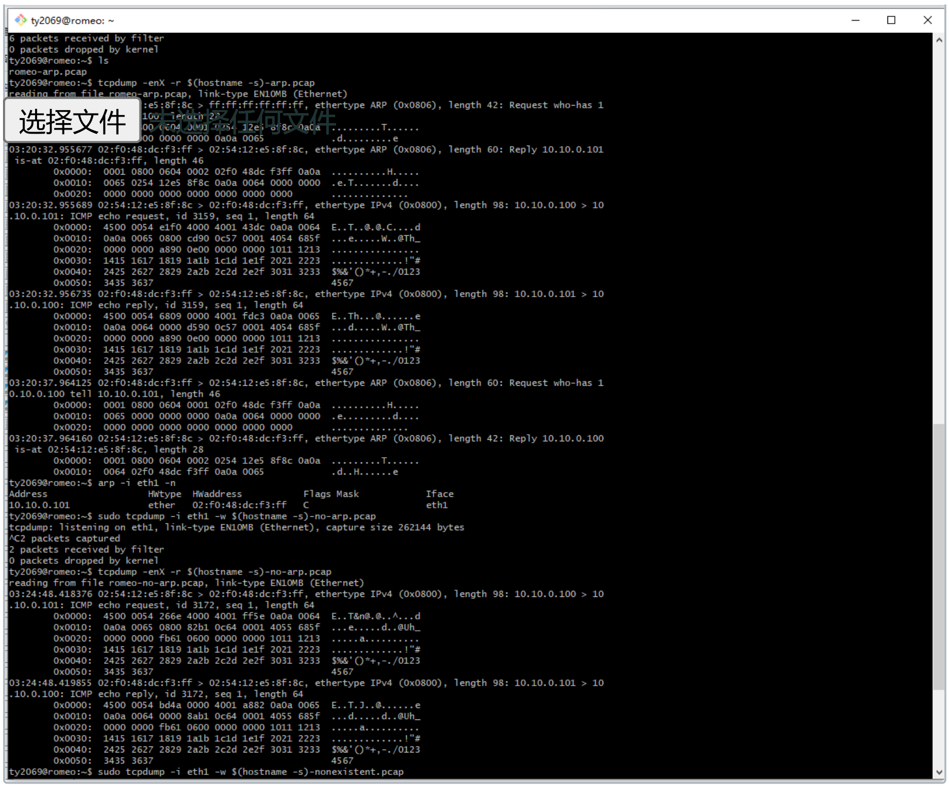
```
        0x0020:  0000 0000 0000 0000 0000 0000 0000
..............
```

选择文件 未选择任何文件

```
7.863416 02:54:12:e5:8f:8c > 02:f0:48:dc:f3:ff, ethertype
ARP (0x0806), length 42: Reply 10.10.0.100 is-at
02:54:12:e5:8f:8c, length 28
        0x0000:  0001 0800 0604 0002 0254 12e5 8f8c 0a0a
.........T......
        0x0010:  0064 02f0 48dc f3ff 0a0a 0065          .d..H......e



ty2069@romeo:~$ tcpdump -enX -r $(hostname -s)-no-arp.pcap
reading from file romeo-no-arp.pcap, link-type EN10MB
(Ethernet)
03:24:48.418376 02:54:12:e5:8f:8c > 02:f0:48:dc:f3:ff, ethertype
IPv4 (0x0800), length 98: 10.10.0.100 > 10.10.0.101: ICMP echo
request, id 3172, seq 1, length 64
        0x0000:  4500 0054 266e 4000 4001 ff5e 0a0a 0064
E..T&n@.@..^...d
        0x0010:  0a0a 0065 0800 82b1 0c64 0001 4055 685f
...e.....d..@Uh_
        0x0020:  0000 0000 fb61 0600 0000 0000 1011 1213
.....a..........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
$%&'()*+,-./0123
        0x0050:  3435 3637                                4567
03:24:48.419855 02:f0:48:dc:f3:ff > 02:54:12:e5:8f:8c, ethertype
IPv4 (0x0800), length 98: 10.10.0.101 > 10.10.0.100: ICMP echo
reply, id 3172, seq 1, length 64
        0x0000:  4500 0054 bd4a 0000 4001 a882 0a0a 0065
E..T.J..@......e
        0x0010:  0a0a 0064 0000 8ab1 0c64 0001 4055 685f
...d.....d..@Uh_
        0x0020:  0000 0000 fb61 0600 0000 0000 1011 1213
.....a..........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
$%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

CURRENTLY UPLOADED FILES

▾ arp.PNG   Download   ✖ Remove



```
6 packets received by filter
0 packets dropped by kernel
ty2069@romeo:~$ ls
romeo-arp.pcap
ty2069@romeo:~$ tcpdump -enX -r $(hostname -s)-arp.pcap
reading from file romeo-arp.pcap, link-type EN10MB (Ethernet)
[illegible]:e5:8f:8c > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Request who-has 1
[illegible]100, length 28
[illegible]00 0604 0001 0254 12e5 8f8c 0a0a  .........T......
[illegible]00 0000 0000 0a0a 0065            .d........e
03:20:32.955677 02:f0:48:dc:f3:ff > 02:54:12:e5:8f:8c, ethertype ARP (0x0806), length 60: Reply 10.10.0.101
 is-at 02:f0:48:dc:f3:ff, length 46
        0x0000:  0001 0800 0604 0002 02f0 48dc f3ff 0a0a  ..........H.....
        0x0010:  0065 0254 12e5 8f8c 0a0a 0064 0000 0000  .e.T.......d....
        0x0020:  0000 0000 0000 0000 0000 0000 0000       ..............
03:20:32.955689 02:54:12:e5:8f:8c > 02:f0:48:dc:f3:ff, ethertype IPv4 (0x0800), length 98: 10.10.0.100 > 10
.10.0.101: ICMP echo request, id 3159, seq 1, length 64
        0x0000:  4500 0054 e1f0 4000 4001 43dc 0a0a 0064  E..T..@.@.C....d
        0x0010:  0a0a 0065 0800 cd90 0c57 0001 4054 685f  ...e.....W..@Th_
        0x0020:  0000 0000 a890 0e00 0000 0000 1011 1213  ................
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
03:20:32.956735 02:f0:48:dc:f3:ff > 02:54:12:e5:8f:8c, ethertype IPv4 (0x0800), length 98: 10.10.0.101 > 10
.10.0.100: ICMP echo reply, id 3159, seq 1, length 64
        0x0000:  4500 0054 6809 0000 4001 fdc3 0a0a 0065  E..Th...@......e
        0x0010:  0a0a 0064 0000 d590 0c57 0001 4054 685f  ...d.....W..@Th_
        0x0020:  0000 0000 a890 0e00 0000 0000 1011 1213  ................
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
03:20:37.964125 02:f0:48:dc:f3:ff > 02:54:12:e5:8f:8c, ethertype ARP (0x0806), length 60: Request who-has 1
0.10.0.100 tell 10.10.0.101, length 46
        0x0000:  0001 0800 0604 0001 02f0 48dc f3ff 0a0a  ..........H.....
        0x0010:  0065 0000 0000 0000 0a0a 0064 0000 0000  .e.........d....
        0x0020:  0000 0000 0000 0000 0000 0000 0000       ..............
03:20:37.964160 02:54:12:e5:8f:8c > 02:f0:48:dc:f3:ff, ethertype ARP (0x0806), length 42: Reply 10.10.0.100
 is-at 02:54:12:e5:8f:8c, length 28
        0x0000:  0001 0800 0604 0002 0254 12e5 8f8c 0a0a  .........T......
        0x0010:  0064 02f0 48dc f3ff 0a0a 0065            .d..H......e
ty2069@romeo:~$ arp -i eth1 -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.10.0.101              ether   02:f0:48:dc:f3:ff   C                     eth1
ty2069@romeo:~$ sudo tcpdump -i eth1 -w $(hostname -s)-no-arp.pcap
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C2 packets captured
2 packets received by filter
0 packets dropped by kernel
ty2069@romeo:~$ tcpdump -enX -r $(hostname -s)-no-arp.pcap
reading from file romeo-no-arp.pcap, link-type EN10MB (Ethernet)
03:24:48.418376 02:54:12:e5:8f:8c > 02:f0:48:dc:f3:ff, ethertype IPv4 (0x0800), length 98: 10.10.0.100 > 10
.10.0.101: ICMP echo request, id 3172, seq 1, length 64
        0x0000:  4500 0054 266e 4000 4001 ff5e 0a0a 0064  E..T&n@.@..^...d
        0x0010:  0a0a 0065 0800 82b1 0c64 0001 4055 685f  ...e.....d..@Uh_
        0x0020:  0000 0000 fb61 0600 0000 0000 1011 1213  .....a..........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
03:24:48.419855 02:f0:48:dc:f3:ff > 02:54:12:e5:8f:8c, ethertype IPv4 (0x0800), length 98: 10.10.0.101 > 10
.10.0.100: ICMP echo reply, id 3172, seq 1, length 64
        0x0000:  4500 0054 bd4a 0000 4001 a882 0a0a 0065  E..T.J..@......e
        0x0010:  0a0a 0064 0000 8ab1 0c64 0001 4055 685f  ...d.....d..@Uh_
        0x0020:  0000 0000 fb61 0600 0000 0000 1011 1213  .....a..........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
ty2069@romeo:~$ sudo tcpdump -i eth1 -w $(hostname -s)-nonexistent.pcap
```

Please select file(s) Select file(s)

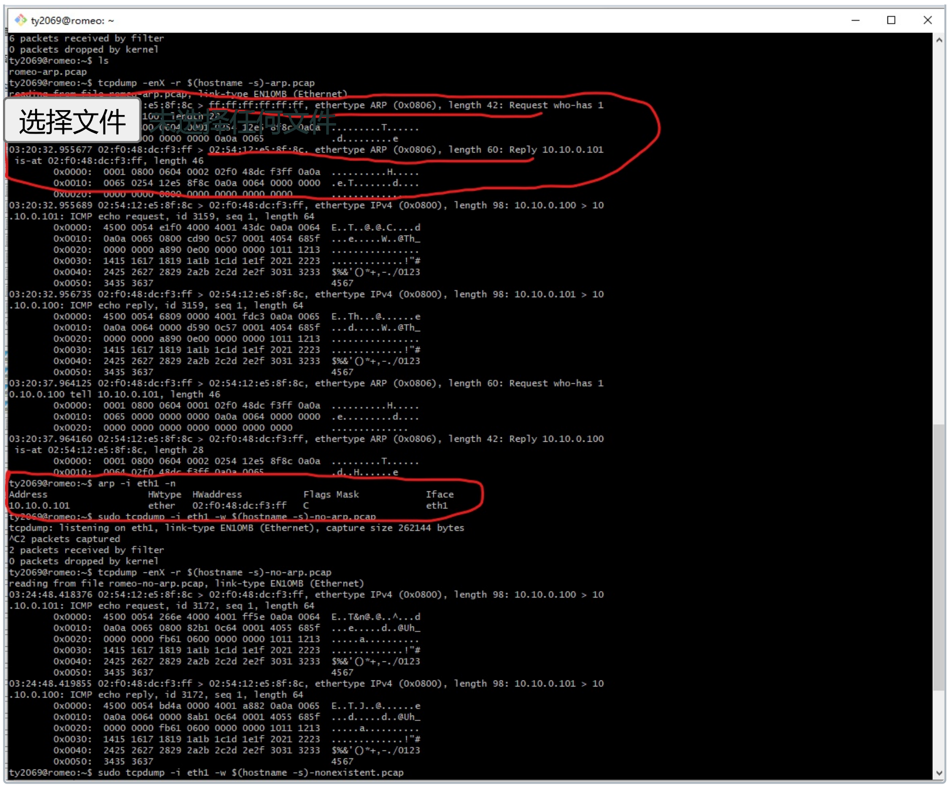
In the first case, an ARP request was sent and a reply was received before the ICMP echo request was sent. In the second case, no ARP request was sent before the ICMP echo request. Why?

In the first case, Romeo host has no entry in its arp table, when it pings Juliet, it doesn't know the MAC address of Juliet, it needs an ARP request and reply packet to get Juliet's MAC address. Once the ARP reply packet received, it will save Juliet into the ARP table and next time we want to pings Juliet we don't need to send an ARP request to get its MAC address.

Show evidence from the output of the `arp` commands from this experiment to support your answer above. Upload screenshots of the `arp` commands (including the terminal prompt, command, and output in your screenshot), but first *annotate* the screenshots by drawing a circle or a box around the specific part that relates to your answer.

CURRENTLY UPLOADED FILES

arpdraw.jpg Download ✖ Remove



```
6 packets received by filter
0 packets dropped by kernel
ty2069@romeo:~$ ls
romeo-arp.pcap
ty2069@romeo:~$ tcpdump -enX -r $(hostname -s)-arp.pcap
reading from file romeo-arp.pcap, link-type EN10MB (Ethernet)
:e5:8f:8c > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Request who-has 1
100, length 28
00 0604 0001 0254 12e5 8f8c 0a0a  .........T......
00 0000 0000 0a0a 0065            .d.........e
03:20:32.955677 02:f0:48:dc:f3:ff > 02:54:12:e5:8f:8c, ethertype ARP (0x0806), length 60: Reply 10.10.0.101
 is-at 02:f0:48:dc:f3:ff, length 46
        0x0000:  0001 0800 0604 0002 02f0 48dc f3ff 0a0a  ..........H.....
        0x0010:  0065 0254 12e5 8f8c 0a0a 0064 0000 0000  .e.T.......d....
        0x0020:  0000 0000 0000 0000 0000 0000 0000       ..............
03:20:32.955689 02:54:12:e5:8f:8c > 02:f0:48:dc:f3:ff, ethertype IPv4 (0x0800), length 98: 10.10.0.100 > 10
.10.0.101: ICMP echo request, id 3159, seq 1, length 64
        0x0000:  4500 0054 e1f0 4000 4001 43dc 0a0a 0064  E..T..@.@.C....d
        0x0010:  0a0a 0065 0800 cd90 0c57 0001 4054 685f  ...e.....W..@Th_
        0x0020:  0000 0000 a890 0e00 0000 0000 1011 1213  ................
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
03:20:32.956735 02:f0:48:dc:f3:ff > 02:54:12:e5:8f:8c, ethertype IPv4 (0x0800), length 98: 10.10.0.101 > 10
.10.0.100: ICMP echo reply, id 3159, seq 1, length 64
        0x0000:  4500 0054 6809 0000 4001 fdc3 0a0a 0065  E..Th...@......e
        0x0010:  0a0a 0064 0000 d590 0c57 0001 4054 685f  ...d.....W..@Th_
        0x0020:  0000 0000 a890 0e00 0000 0000 1011 1213  ................
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
03:20:37.964125 02:f0:48:dc:f3:ff > 02:54:12:e5:8f:8c, ethertype ARP (0x0806), length 60: Request who-has 1
0.10.0.100 tell 10.10.0.101, length 46
        0x0000:  0001 0800 0604 0001 02f0 48dc f3ff 0a0a  ..........H.....
        0x0010:  0065 0000 0000 0000 0a0a 0064 0000 0000  .e.........d....
        0x0020:  0000 0000 0000 0000 0000 0000 0000       ..............
03:20:37.964160 02:54:12:e5:8f:8c > 02:f0:48:dc:f3:ff, ethertype ARP (0x0806), length 42: Reply 10.10.0.100
 is-at 02:54:12:e5:8f:8c, length 28
        0x0000:  0001 0800 0604 0002 0254 12e5 8f8c 0a0a  .........T......
        0x0010:  0064 02f0 48dc f3ff 0a0a 0065            .d..H......e
ty2069@romeo:~$ arp -i eth1 -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.10.0.101              ether   02:f0:48:dc:f3:ff   C                     eth1
ty2069@romeo:~$ sudo tcpdump -i eth1 -w $(hostname -s)-no-arp.pcap
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C2 packets captured
2 packets received by filter
0 packets dropped by kernel
ty2069@romeo:~$ tcpdump -enX -r $(hostname -s)-no-arp.pcap
reading from file romeo-no-arp.pcap, link-type EN10MB (Ethernet)
03:24:48.418376 02:54:12:e5:8f:8c > 02:f0:48:dc:f3:ff, ethertype IPv4 (0x0800), length 98: 10.10.0.100 > 10
.10.0.101: ICMP echo request, id 3172, seq 1, length 64
        0x0000:  4500 0054 266e 4000 4001 ff5e 0a0a 0064  E..T&n@.@..^...d
        0x0010:  0a0a 0065 0800 82b1 0c64 0001 4055 685f  ...e.....d..@Uh_
        0x0020:  0000 0000 fb61 0600 0000 0000 1011 1213  .....a..........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
03:24:48.419855 02:f0:48:dc:f3:ff > 02:54:12:e5:8f:8c, ethertype IPv4 (0x0800), length 98: 10.10.0.101 > 10
.10.0.100: ICMP echo reply, id 3172, seq 1, length 64
        0x0000:  4500 0054 bd4a 0000 4001 a882 0a0a 0065  E..T.J..@......e
        0x0010:  0a0a 0064 0000 8ab1 0c64 0001 4055 685f  ...d.....d..@Uh_
        0x0020:  0000 0000 fb61 0600 0000 0000 1011 1213  .....a..........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
ty2069@romeo:~$ sudo tcpdump -i eth1 -w $(hostname -s)-nonexistent.pcap
```

Please select file(s) Select file(s)

Save Answer Last saved on **Sep 24 at 6:57 PM**

Q3.2 ARP packet fields (Exercise 4)

0.5 Points

Take a screenshot of either `tcpdump` or Wireshark output for the first saved packet capture in this exercise. Make sure the screenshot shows the information you need to answer the following four questions.

Then, answer the questions:

- What is the target IP address in the ARP request?

10.10.0.101

- At the MAC layer, what is the destination Ethernet address of the frame carrying the ARP request? Why - what is special about this address, and why do we need to use this special address in this situation?

ff:ff:ff:ff:ff:ff is the ethernet address that carrying the ARP request. This is a broadcast MAC address since at that time

Romeo host doesn't have the MAC address of Juliet in its ARP table.

选择文件 未选择任何文件

- What is the frame type field in the Ethernet frame *for the ARP request and reply*? Give the answer as a four-digit hex value, e.g. `0x86DD`, and also say what prototcol this frame type is used for.

ARP(0x0806)

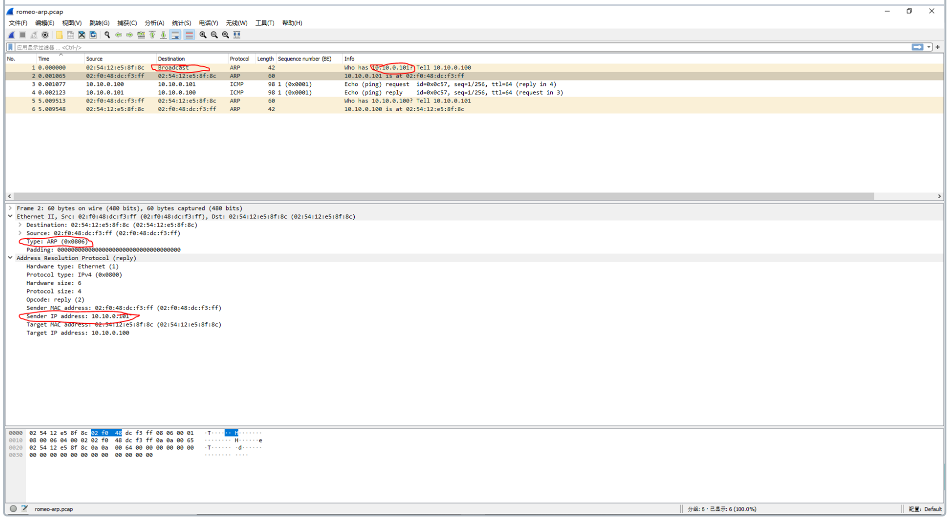
- Of the four hosts on your network segment, which host sends the ARP reply? Give the hostname, e.g. "romeo", "juliet". Why does this host send an ARP reply?

Host Juliet sends the ARP reply since the target IP address is Juliet's IP address in the ARP request.

Next, annotate your `tcpdump` or Wireshark screenshot: draw a box or a circle around the answers to each of the four questions above, to show where they appear in the `tcpdump` or Wireshark output. Upload your annotated screenshot.

CURRENTLY UPLOADED FILES

arp-wireshark.PNG Download ✖ Remove



romeo-arp.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.  Time      Source             Destination        Protocol Length Sequence number (BE) Info
   1 0.000000  02:54:12:e5:8f:8c  Broadcast          ARP      42                          Who has 10.10.0.101? Tell 10.10.0.100
   2 0.001065  02:f0:48:dc:f3:ff  02:54:12:e5:8f:8c  ARP      60                          10.10.0.101 is at 02:f0:48:dc:f3:ff
   3 0.001077  10.10.0.100        10.10.0.101        ICMP     98     1 (0x0001)           Echo (ping) request  id=0x0c57, seq=1/256, ttl=64 (reply in 4)
   4 0.002123  10.10.0.101        10.10.0.100        ICMP     98     1 (0x0001)           Echo (ping) reply    id=0x0c57, seq=1/256, ttl=64 (request in 3)
   5 5.009513  02:f0:48:dc:f3:ff  02:54:12:e5:8f:8c  ARP      60                          Who has 10.10.0.100? Tell 10.10.0.101
   6 5.009548  02:54:12:e5:8f:8c  02:f0:48:dc:f3:ff  ARP      42                          10.10.0.100 is at 02:54:12:e5:8f:8c
```

```
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
v Ethernet II, Src: 02:f0:48:dc:f3:ff (02:f0:48:dc:f3:ff), Dst: 02:54:12:e5:8f:8c (02:54:12:e5:8f:8c)
  > Destination: 02:54:12:e5:8f:8c (02:54:12:e5:8f:8c)
  > Source: 02:f0:48:dc:f3:ff (02:f0:48:dc:f3:ff)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 02:f0:48:dc:f3:ff (02:f0:48:dc:f3:ff)
    Sender IP address: 10.10.0.101
    Target MAC address: 02:54:12:e5:8f:8c (02:54:12:e5:8f:8c)
    Target IP address: 10.10.0.100
```

```
0000  02 54 12 e5 8f 8c 02 f0  48 dc f3 ff 08 06 00 01   ·T······ H·······
0010  08 00 06 04 00 02 02 f0  48 dc f3 ff 0a 0a 00 65   ········ H······e
0020  02 54 12 e5 8f 8c 0a 0a  00 64 00 00 00 00 00 00   ·T······ ·d······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Please select file(s) Select file(s)

Save Answer Last saved on **Sep 24 at 6:57 PM**

Q3.3 ARP for non-existent host (Exercise 5)

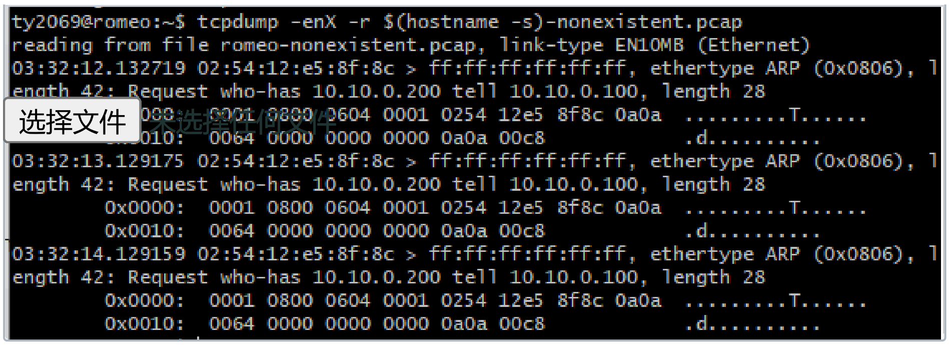
0.5 Points

Show the summary `tcpdump` output from Exercise 5 (either paste the text here, or upload a screenshot). The "summary `tcpdump`
选择文件 未选择任何文件 the output you see when you play back the packet capture using the `-r` argument to `tcpdump`, as described in the instructions. Crop your screenshot if necessary so that *only* the relevant part is included, not everything that happened to be on the screen at the time.

```
ty2069@romeo:~$ tcpdump -enX -r $(hostname -s)-
nonexistent.pcap
reading from file romeo-nonexistent.pcap, link-type EN10MB
(Ethernet)
03:32:12.132719 02:54:12:e5:8f:8c > ff:ff:ff:ff:ff:ff, ethertype ARP
(0x0806), length 42: Request who-has 10.10.0.200 tell
10.10.0.100, length 28
        0x0000:  0001 0800 0604 0001 0254 12e5 8f8c 0a0a
.........T......
        0x0010:  0064 0000 0000 0000 0a0a 00c8
.d..........
03:32:13.129175 02:54:12:e5:8f:8c > ff:ff:ff:ff:ff:ff, ethertype ARP
(0x0806), length 42: Request who-has 10.10.0.200 tell
10.10.0.100, length 28
        0x0000:  0001 0800 0604 0001 0254 12e5 8f8c 0a0a
.........T......
        0x0010:  0064 0000 0000 0000 0a0a 00c8
.d..........
03:32:14.129159 02:54:12:e5:8f:8c > ff:ff:ff:ff:ff:ff, ethertype ARP
(0x0806), length 42: Request who-has 10.10.0.200 tell
10.10.0.100, length 28
        0x0000:  0001 0800 0604 0001 0254 12e5 8f8c 0a0a
.........T......
        0x0010:  0064 0000 0000 0000 0a0a 00c8
.d..........
```

CURRENTLY UPLOADED FILES

▾ noexistent.PNG Download ✖ Remove



```
ty2069@romeo:~$ tcpdump -enX -r $(hostname -s)-nonexistent.pcap
reading from file romeo-nonexistent.pcap, link-type EN10MB (Ethernet)
03:32:12.132719 02:54:12:e5:8f:8c > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), l
ength 42: Request who-has 10.10.0.200 tell 10.10.0.100, length 28
        0x0000:  0001 0800 0604 0001 0254 12e5 8f8c 0a0a  .........T......
        0x0010:  0064 0000 0000 0000 0a0a 00c8            .d..........
03:32:13.129175 02:54:12:e5:8f:8c > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), l
ength 42: Request who-has 10.10.0.200 tell 10.10.0.100, length 28
        0x0000:  0001 0800 0604 0001 0254 12e5 8f8c 0a0a  .........T......
        0x0010:  0064 0000 0000 0000 0a0a 00c8            .d..........
03:32:14.129159 02:54:12:e5:8f:8c > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), l
ength 42: Request who-has 10.10.0.200 tell 10.10.0.100, length 28
        0x0000:  0001 0800 0604 0001 0254 12e5 8f8c 0a0a  .........T......
        0x0010:  0064 0000 0000 0000 0a0a 00c8            .d..........
```

Please select file(s) Select file(s)

In the previous exercise, after sending an ARP request and receiving a reply, "romeo" sends an ICMP echo request. In this exercise, is an ICMP echo request ever sent? Why or why not? Give an explanation based on your knowledge of how ARP works and why it is needed.

No. Since the ARP request sent and didn't get a reply, it will mean the host we send the packet to is not exist.

Save Answer Last saved on **Sep 24 at 7:09 PM**

Q3.4 ARP timeout and retransmission (Exercise 5)

0.5 Points

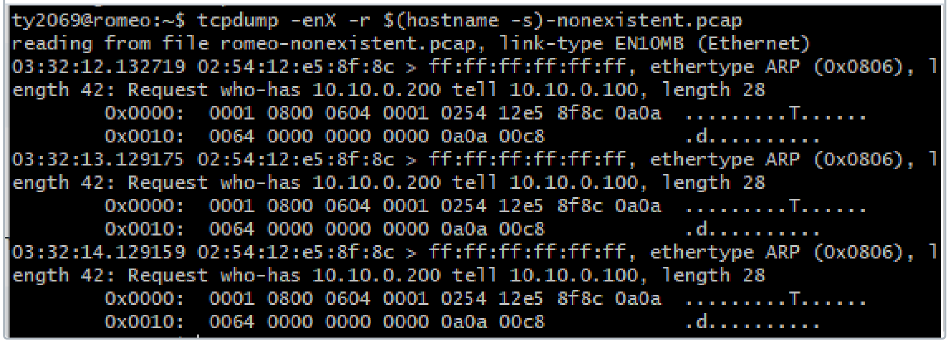
Show the summary `tcpdump` output from Exercise 5 (either paste the text here, or upload a screenshot). The "summary `tcpdump` output" is the output you see when you play back the packet capture using the `-r` argument to `tcpdump`, as described in the instructions. Crop your screenshot if necessary so that *only* the relevant part is included, not everything that happened to be on the screen at the time.

```
ty2069@romeo:~$ tcpdump -enX -r $(hostname -s)-nonexistent.pcap
reading from file romeo-nonexistent.pcap, link-type EN10MB (Ethernet)
03:32:12.132719 02:54:12:e5:8f:8c > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Request who-has 10.10.0.200 tell 10.10.0.100, length 28
        0x0000:  0001 0800 0604 0001 0254 12e5 8f8c 0a0a  .........T......
        0x0010:  0064 0000 0000 0000 0a0a 00c8
```

.d..........
03:32:13.129175 02:54:12:e5:8f:8c > ff:ff:ff:ff:ff:ff, ethertype ARP
选择文件 未选择任何文件Request who-has 10.10.0.200 tell
10.10.0.100, length 28
        0x0000: 0001 0800 0604 0001 0254 12e5 8f8c 0a0a
.........T......
        0x0010: 0064 0000 0000 0000 0a0a 00c8
.d..........
03:32:14.129159 02:54:12:e5:8f:8c > ff:ff:ff:ff:ff:ff, ethertype ARP
(0x0806), length 42: Request who-has 10.10.0.200 tell
10.10.0.100, length 28
        0x0000: 0001 0800 0604 0001 0254 12e5 8f8c 0a0a
.........T......
        0x0010: 0064 0000 0000 0000 0a0a 00c8
.d..........

CURRENTLY UPLOADED FILES

▾ noexistent.PNG   Download   ✖ Remove



```
ty2069@romeo:~$ tcpdump -enX -r $(hostname -s)-nonexistent.pcap
reading from file romeo-nonexistent.pcap, link-type EN10MB (Ethernet)
03:32:12.132719 02:54:12:e5:8f:8c > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), l
ength 42: Request who-has 10.10.0.200 tell 10.10.0.100, length 28
        0x0000:  0001 0800 0604 0001 0254 12e5 8f8c 0a0a  .........T......
        0x0010:  0064 0000 0000 0000 0a0a 00c8            .d..........
03:32:13.129175 02:54:12:e5:8f:8c > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), l
ength 42: Request who-has 10.10.0.200 tell 10.10.0.100, length 28
        0x0000:  0001 0800 0604 0001 0254 12e5 8f8c 0a0a  .........T......
        0x0010:  0064 0000 0000 0000 0a0a 00c8            .d..........
03:32:14.129159 02:54:12:e5:8f:8c > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), l
ength 42: Request who-has 10.10.0.200 tell 10.10.0.100, length 28
        0x0000:  0001 0800 0604 0001 0254 12e5 8f8c 0a0a  .........T......
        0x0010:  0064 0000 0000 0000 0a0a 00c8            .d..........
```

Please select file(s)   Select file(s)

Use the `tcpdump` output to answer the following questions:

From the `tcpdump` output, describe how the ARP timeout and retransmission were performed.

There is a time out between each request sent. If the host doesn't receive a reply during the time out, it will send another request after the time out.

How many attempts were made to resolve a non-existing IP address?

3

How much time separates each attempt?

选择文件 未选择任何文件

Save Answer Last saved on **Sep 24 at 7:11 PM**

Q4 2.9 Exercises with IP address and subnet mask

5 Points

Q4.1 Network unreachable (Exercise 10)

1 Point

Can you see any ICMP echo request sent on the network? Why?

No, since the host doesn't exist

Show the `route -n` output and the `ping` output in each case (either paste here, or upload a screenshot). Make sure you show the terminal prompt, the complete command, and the output in each case, for both the `route` and `ping` commands. Crop your screenshot if necessary so that *only* the relevant part is included, not everything that happened to be on the screen at the time.

```
ty2069@romeo:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref
Use Iface
10.10.0.0       0.0.0.0         255.255.255.0   U     0      0        0 eth1
172.16.0.0      0.0.0.0         255.240.0.0     U     0      0        0 eth0
174.119.0.0     172.16.0.1      255.255.0.0     UG    0      0        0
eth0


ty2069@romeo:~$ ping -c 1 10.10.10.100
connect: Network is unreachable


ty2069@romeo:~$ route -n
```

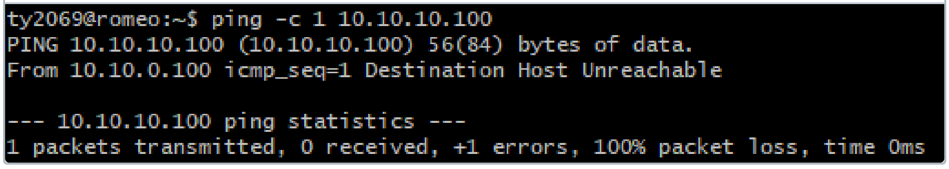
```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref
```

选择文件 未选择任何文件

```
10.10.0.0       0.0.0.0         255.255.255.0   U     0      0        0 eth1
10.10.10.100    0.0.0.0         255.255.255.255 UH    0      0        0
eth1
172.16.0.0      0.0.0.0         255.240.0.0     U     0      0        0 eth0
174.119.0.0     172.16.0.1      255.255.0.0     UG    0      0        0
eth0



ty2069@romeo:~$ ping -c 1 10.10.10.100
PING 10.10.10.100 (10.10.10.100) 56(84) bytes of data.
From 10.10.0.100 icmp_seq=1 Destination Host Unreachable

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

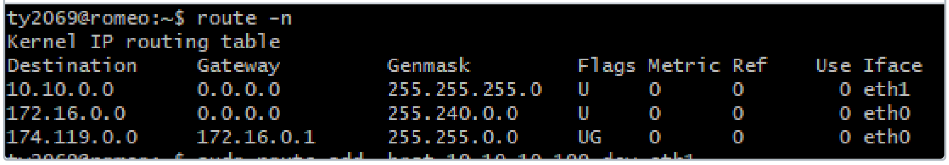
CURRENTLY UPLOADED FILES

▾ ping1.PNG Download ✖ Remove



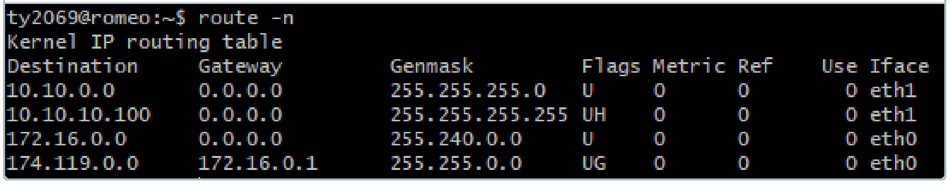
```
ty2069@romeo:~$ ping -c 1 10.10.10.100
PING 10.10.10.100 (10.10.10.100) 56(84) bytes of data.
From 10.10.0.100 icmp_seq=1 Destination Host Unreachable

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

▾ route.PNG Download ✖ Remove



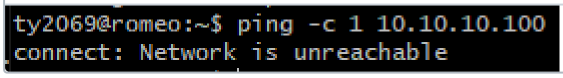
```
ty2069@romeo:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.0.0       0.0.0.0         255.255.255.0   U     0      0        0 eth1
172.16.0.0      0.0.0.0         255.240.0.0     U     0      0        0 eth0
174.119.0.0     172.16.0.1      255.255.0.0     UG    0      0        0 eth0
ty2069@romeo:~$ sudo route add -host 10.10.10.100 dev eth1
```

▾ route1.PNG Download ✖ Remove



```
ty2069@romeo:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.0.0       0.0.0.0         255.255.255.0   U     0      0        0 eth1
10.10.10.100    0.0.0.0         255.255.255.255 UH    0      0        0 eth1
172.16.0.0      0.0.0.0         255.240.0.0     U     0      0        0 eth0
174.119.0.0     172.16.0.1      255.255.0.0     UG    0      0        0 eth0
```

▾ unreachable.PNG Download ✖ Remove



```
ty2069@romeo:~$ ping -c 1 10.10.10.100
connect: Network is unreachable
```

Please select file(s) Select file(s)

Explain what happened in this exercise. Refer to the output of the `route` and `ping` commands to support your explanation.

选择文件 未选择任何文件

In the first case, we don't have the route to the network with IP address 10.10.10.100. So we couldn't send any packet. In the second case, we have the route in the table but the host doesn't exist. After we have 3 time out for ARP request. We stop sending packets.

Save Answer Last saved on **Sep 24 at 7:56 PM**

Q4.2 No ARP when network unreachable (Exercise 10)

1 Point

Why does "romeo" not send any ARP request in the first part of this exercise, but does send ARP requests in the second part?

Since Romeo doesn't have the route to the network. It couldn't send any packet. But in the second case, we add the route into the table so it will send ARP requests to get the MAC address of the host.

Save Answer Last saved on **Sep 24 at 7:56 PM**

Q4.3 Routing tables and subnet masks (Exercise 12)

1 Point

Upload a screenshot showing the routing table for each host. *Annotate* your screenshot, by drawing a circle or a box around the rule that applies to traffic that is sent within the same subnet.

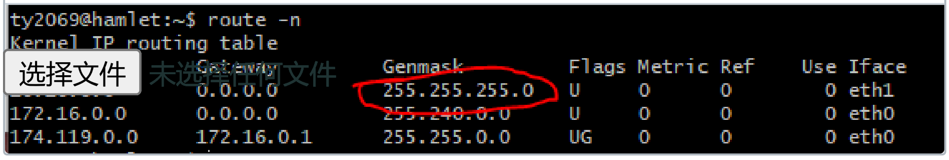
(This rule is added to the routing table automatically when you configure the IP address and netmask on the network interface.)

Enter your answer here

CURRENTLY UPLOADED FILES

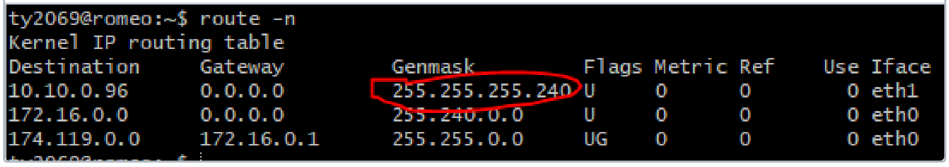
hamlet-route.PNG ✖ Remove

▾ hamlet-route.PNG Download ✖ Remove



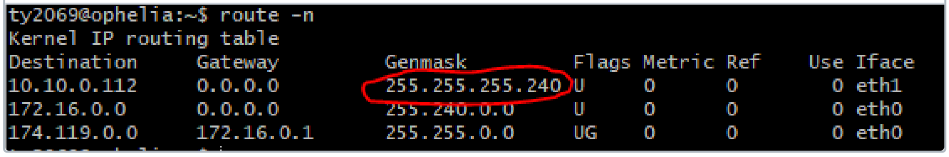
```
ty2069@hamlet:~$ route -n
Kernel IP routing table
                Gateway         Genmask         Flags Metric Ref    Use Iface
                0.0.0.0         255.255.255.0   U     0      0        0 eth1
172.16.0.0      0.0.0.0         255.240.0.0     U     0      0        0 eth0
174.119.0.0     172.16.0.1      255.255.0.0     UG    0      0        0 eth0
```

▾ romeo-route.PNG Download ✖ Remove



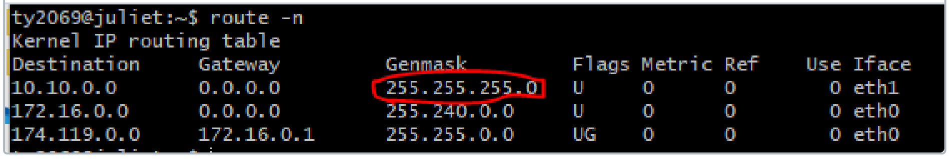
```
ty2069@romeo:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.0.96      0.0.0.0         255.255.255.240 U     0      0        0 eth1
172.16.0.0      0.0.0.0         255.240.0.0     U     0      0        0 eth0
174.119.0.0     172.16.0.1      255.255.0.0     UG    0      0        0 eth0
```

▾ ophelia-route.PNG Download ✖ Remove



```
ty2069@ophelia:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.0.112     0.0.0.0         255.255.255.240 U     0      0        0 eth1
172.16.0.0      0.0.0.0         255.240.0.0     U     0      0        0 eth0
174.119.0.0     172.16.0.1      255.255.0.0     UG    0      0        0 eth0
```

▾ juliet-route.PNG Download ✖ Remove



```
ty2069@juliet:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.0.0       0.0.0.0         255.255.255.0   U     0      0        0 eth1
172.16.0.0      0.0.0.0         255.240.0.0     U     0      0        0 eth0
174.119.0.0     172.16.0.1      255.255.0.0     UG    0      0        0 eth0
```

Please select file(s) Select file(s)

Save Answer Last saved on **Sep 24 at 8:05 PM**

Q4.4 Bitwise analysis with subnet masks (Exercise 12)

1 Point

Use bitwise analysis to answer the following questions. (There is an example of "subnet math" in the video playlist.)

In each case, write the answer but **also, show how the netmask was applied using bitwise analysis**. You can use the text input field or upload a file that shows how you used "subnet math" to find the answer.

- What is the range of IP addresses (i.e. smallest IP address and largest IP address) that is in the same subnet as "romeo"?

For Romeo, IP address: 10.10.0.100 and subnet mask: 255.255.255.240

10.10.0.100 -> 10.10.0.01100100 ->10.10.0.0110XXXX

255.255.255.240 -> 255.255.255.11110000

选择文件 未选择任何文件 in the same subnet as Romeo is 10.10.0.01100000 to 10.10.0.01101111 which is 10.10.0.96 to 10.10.0.111

Please select file(s) Select file(s)

- What is the range of IP addresses (i.e. smallest IP address and largest IP address) that is in the same subnet as "juliet"?

For Juliet, IP address: 10.10.0.101 and subnet mask:255.255.255.0
10.10.0.101 -> 10.10.0.01100101 ->10.10.0.XXXXXXXX
255.255.255.0 -> 255.255.255.00000000

Then the IP addresses in the same subnet as Juliet is 10.10.0.00000000 to 10.10.0.11111110 which is 10.10.0.1 to 10.10.0.254

Please select file(s) Select file(s)

- What is the range of IP addresses (i.e. smallest IP address and largest IP address) that is in the same subnet as "hamlet"?

For Hamlet, IP address: 10.10.0.102 and subnet mask: 255.255.255.0
10.10.0.102 -> 10.10.0.01100110 ->10.10.0.XXXXXXXX
255.255.255.0 -> 255.255.255.00000000

Then the IP addresses in the same subnet as Hamlet is 10.10.0.00000000 to 10.10.0.11111110 which is 10.10.0.1 to 10.10.0.254

Please select file(s) Select file(s)

- What is the range of IP addresses (i.e. smallest IP address and largest IP address) that is in the same subnet as "ophelia"?

For Ophelia, IP address: 10.10.0.120 and subnet mask: 255.255.255.240

10.10.0.120 -> 10.10.0.01111000 ->10.10.0.0111XXXX

255.255.255.240 -> 255.255.255.11110000

选择文件 未选择任何文件

Then the IP addresses in the same subnet as Ophelia is 10.10.0.01110000 to 10.10.0.01111111 which is 10.10.0.112 to 10.10.0.127

Please select file(s) Select file(s)

Save Answer Last saved on **Sep 24 at 8:19 PM**

Q4.5 Experiments with subnet masks (Exercise 12)

1 Point

Show the `tcpdump` output for each case. Make sure to clearly label each output!

Enter your answer here

CURRENTLY UPLOADED FILES

labreport-fourhost.txt Download ✖ Remove

```
First part

ty2069@romeo:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host romeo.lab2-ty2069.ch-geni-net.geni.it.cornell.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
20:20:48.381381 02:6a:21:71:aa:19 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Request who-has 10.10.0.101 tell 10.10.0.100, length 28
20:20:48.381923 02:cc:d9:d5:9c:12 > 02:6a:21:71:aa:19, ethertype ARP (0x0806), length 42: Reply 10.10.0.101 is-at 02:cc:d9:d5:9c:12, length 28
20:20:48.381937 02:6a:21:71:aa:19 > 02:cc:d9:d5:9c:12, ethertype IPv4 (0x0800), length 98: 10.10.0.100 > 10.10.0.101: ICMP echo request, id 2242, seq 1, length 64
20:20:48.382422 02:cc:d9:d5:9c:12 > 02:6a:21:71:aa:19, ethertype IPv4 (0x0800), length 98: 10.10.0.101 > 10.10.0.100: ICMP echo reply, id 2242, seq 1, length 64
20:20:53.385070 02:cc:d9:d5:9c:12 > 02:6a:21:71:aa:19,
```

选择文件 未选择任何文件

```
ethertype ARP (0x0806), length 42: Request who-has 10.10.0.100 tell 10.10.0.101, length 28
20:20:53.385112 02:6a:21:71:aa:19 > 02:cc:d9:d5:9c:12, ethertype ARP (0x0806), length 42: Reply 10.10.0.100 is-at 02:6a:21:71:aa:19, length 28
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel

ty2069@juliet:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host juliet.lab2-ty2069.ch-geni-net.geni.it.cornell.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
20:20:48.379234 02:6a:21:71:aa:19 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Request who-has 10.10.0.101 tell 10.10.0.100, length 28
20:20:48.379318 02:cc:d9:d5:9c:12 > 02:6a:21:71:aa:19, ethertype ARP (0x0806), length 42: Reply 10.10.0.101 is-at 02:cc:d9:d5:9c:12, length 28
20:20:48.379777 02:6a:21:71:aa:19 > 02:cc:d9:d5:9c:12, ethertype IPv4 (0x0800), length 98: 10.10.0.100 > 10.10.0.101: ICMP echo request, id 2242, seq 1, length 64
20:20:48.379831 02:cc:d9:d5:9c:12 > 02:6a:21:71:aa:19, ethertype IPv4 (0x0800), length 98: 10.10.0.101 > 10.10.0.100: ICMP echo reply, id 2242, seq 1, length 64
20:20:53.382406 02:cc:d9:d5:9c:12 > 02:6a:21:71:aa:19, ethertype ARP (0x0806), length 42: Request who-has 10.10.0.100 tell 10.10.0.101, length 28
20:20:53.383036 02:6a:21:71:aa:19 > 02:cc:d9:d5:9c:12, ethertype ARP (0x0806), length 42: Reply 10.10.0.100 is-at 02:6a:21:71:aa:19, length 28
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel


ty2069@hamlet:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host hamlet.lab2-ty2069.ch-geni-net.geni.it.cornell.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
20:20:48.424139 02:6a:21:71:aa:19 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 10.10.0.101 tell 10.10.0.100, length 46
^C
```

选择文件 未选择任何文件

```
1 packet captured
1 packet received by filter
0 packets dropped by kernel


ty2069@ophelia:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host ophelia.lab2-ty2069.ch-geni-net.geni.it.cornell.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
20:20:48.373287 02:6a:21:71:aa:19 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 10.10.0.101 tell 10.10.0.100, length 46
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel


=============================================================
Second part

ty2069@ophelia:~$ ping -c 1 10.10.0.101
connect: Network is unreachable

ty2069@romeo:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host romeo.lab2-ty2069.ch-geni-net.geni.it.cornell.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel


ty2069@juliet:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host juliet.lab2-ty2069.ch-geni-net.geni.it.cornell.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel

```

选择文件 未选择任何文件

```
ty2069@hamlet:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host hamlet.lab2-ty2069.ch-geni-
ll.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel


ty2069@ophelia:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host ophelia.lab2-ty2069.ch-geni-net.geni.it.cornell.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel

=============================================================
Third Part

ty2069@romeo:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host romeo.lab2-ty2069.ch-geni-net.geni.it.cornell.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
20:28:56.056790 02:cc:d9:d5:9c:12 > 02:6a:21:71:aa:19, ethertype IPv4 (0x0800), length 98: 10.10.0.101 > 10.10.0.100: ICMP echo request, id 2374, seq 1, length 64
20:28:56.056861 02:6a:21:71:aa:19 > 02:cc:d9:d5:9c:12, ethertype IPv4 (0x0800), length 98: 10.10.0.100 > 10.10.0.101: ICMP echo reply, id 2374, seq 1, length 64
20:29:01.065263 02:cc:d9:d5:9c:12 > 02:6a:21:71:aa:19, ethertype ARP (0x0806), length 42: Request who-has 10.10.0.100 tell 10.10.0.101, length 28
20:29:01.065335 02:6a:21:71:aa:19 > 02:cc:d9:d5:9c:12, ethertype ARP (0x0806), length 42: Reply 10.10.0.100 is-at 02:6a:21:71:aa:19, length 28
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel

```

选择文件 未选择任何文件

```
ty2069@juliet:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host juliet.lab2-ty2069.ch-geni-
ll.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
20:28:56.053851 02:cc:d9:d5:9c:12 > 02:6a:21:71:aa:19, ethertype IPv4 (0x0800), length 98: 10.10.0.101 > 10.10.0.100: ICMP echo request, id 2374, seq 1, length 64
20:28:56.054501 02:6a:21:71:aa:19 > 02:cc:d9:d5:9c:12, ethertype IPv4 (0x0800), length 98: 10.10.0.100 > 10.10.0.101: ICMP echo reply, id 2374, seq 1, length 64
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
ty2069@juliet:~$

ty2069@hamlet:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host hamlet.lab2-ty2069.ch-geni-net.geni.it.cornell.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel

ty2069@ophelia:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host ophelia.lab2-ty2069.ch-geni-net.geni.it.cornell.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel

============================================================
Fourth Part

ty2069@romeo:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host romeo.lab2-ty2069.ch-geni-net.geni.it.cornell.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size
```

选择文件 未选择任何文件

```
262144 bytes
20:26:40.598219 02:e1:47:d4:9e:0a > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 10.10.0.120 tell 10.10.0.102, length 46
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel

ty2069@juliet:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host juliet.lab2-ty2069.ch-geni-net.geni.it.cornell.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
20:26:40.595674 02:e1:47:d4:9e:0a > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 10.10.0.120 tell 10.10.0.102, length 46
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel

ty2069@hamlet:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host hamlet.lab2-ty2069.ch-geni-net.geni.it.cornell.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
20:26:40.647220 02:e1:47:d4:9e:0a > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Request who-has 10.10.0.120 tell 10.10.0.102, length 28
20:26:40.647967 02:48:f6:f4:aa:61 > 02:e1:47:d4:9e:0a, ethertype ARP (0x0806), length 60: Reply 10.10.0.120 is-at 02:48:f6:f4:aa:61, length 46
20:26:40.647985 02:e1:47:d4:9e:0a > 02:48:f6:f4:aa:61, ethertype IPv4 (0x0800), length 98: 10.10.0.102 > 10.10.0.120: ICMP echo request, id 2472, seq 1, length 64
^C
3 packets captured
3 packets received by filter
0 packets dropped by kernel

ty2069@ophelia:~$ sudo tcpdump -en -i eth1
sudo: unable to resolve host ophelia.lab2-ty2069.ch-geni-net.geni.it.cornell.edu: Connection refused
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
20:26:40.588593 02:e1:47:d4:9e:0a > ff:ff:ff:ff:ff:ff,
ethertype ARP (0x0806), length 60: Request who-has
10.10.0.120 tell 10.10.0.102, length 46
20:26:40.588651 02:48:f6:f4:aa:61 > 02:e1:47:d4:9e:0a,
ethertype ARP (0x0806), length 42: Reply 10.10.0.120 is-at
02:48:f6:f4:aa:61, length 28
20:26:40.589335 02:e1:47:d4:9e:0a > 02:48:f6:f4:aa:61,
ethertype IPv4 (0x0800), length 98: 10.10.0.102 >
10.10.0.120: ICMP echo request, id 2472, seq 1, length 64
^C
3 packets captured
3 packets received by filter
0 packets dropped by kernel
```

选择文件 未选择任何文件

Please select file(s) Select file(s)

Explain why the other hosts cannot reach "ophelia", whereas "romeo", which has the same subnet mask as "ophelia", can communicate with the other hosts. Use your answer to question 4.4 to support your explanation.

Since the range of IP addresses that is in the same subnet as "Romeo" is 10.10.0.96 to 10.10.0.111, and the IP address of Juliet and Hamlet's IP are inside of this range. So Romeo can communicate with those two hosts. But Juliet and Hamlets' IP are not in the range of IP addresses that are the same subnet as Ophelia. So Ophelia cannot communicate with others.

Save Answer Last saved on **Sep 24 at 8:35 PM**

Q5 2.8 Exercise with ICMP and Ping

1 Point

Q5.1 ICMP port unreachable (Exercise 9)

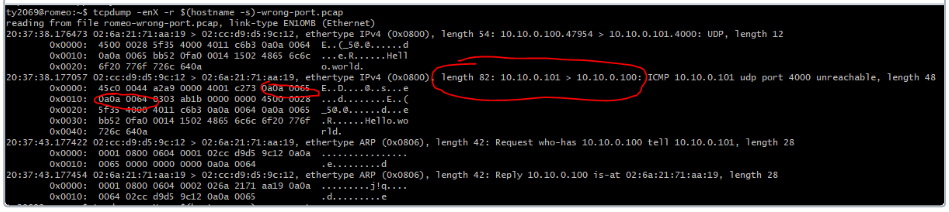
0.5 Points

Study the saved ICMP port unreachable message (see Fig. 2.7 in the text book).

Show a screenshot of the ICMP port unreachable message from `tcpdump` or Wireshark, but *annotate* it by drawing a circle or a box
选择文件 未选择任何文件 ICMP message that includes the first 8 bytes of the original IP datagram payload.

CURRENTLY UPLOADED FILES

▾ unreachable01.PNG Download ✖ Remove



```
ty2069@romeo:~$ tcpdump -enX -r $(hostname -s)-wrong-port.pcap
reading from file romeo-wrong-port.pcap, link-type EN10MB (Ethernet)
20:37:38.176473 02:6a:21:71:aa:19 > 02:cc:d9:d5:9c:12, ethertype IPv4 (0x0800), length 54: 10.10.0.100.47954 > 10.10.0.101.4000: UDP, length 12
        0x0000:  4500 0028 5f35 4000 4011 c6b3 0a0a 0064  E..(_5@.@......d
        0x0010:  0a0a 0065 bb52 0fa0 0014 1502 4865 6c6c  ...e.R......Hell
        0x0020:  6f20 776f 726c 640a                      o.world.
20:37:38.177057 02:cc:d9:d5:9c:12 > 02:6a:21:71:aa:19, ethertype IPv4 (0x0800), length 82: 10.10.0.101 > 10.10.0.100: ICMP 10.10.0.101 udp port 4000 unreachable, length 48
        0x0000:  45c0 0044 a2a9 0000 4001 c273 0a0a 0065  E..D....@..s...e
        0x0010:  0a0a 0064 0303 ab1b 0000 0000 4500 0028  ...d........E..(
        0x0020:  5f35 4000 4011 c6b3 0a0a 0064 0a0a 0065  _5@.@......d...e
        0x0030:  bb52 0fa0 0014 1502 4865 6c6c 6f20 776f  .R......Hello.wo
        0x0040:  726c 640a                                rld.
20:37:43.177422 02:cc:d9:d5:9c:12 > 02:6a:21:71:aa:19, ethertype ARP (0x0806), length 42: Request who-has 10.10.0.100 tell 10.10.0.101, length 28
        0x0000:  0001 0800 0604 0001 02cc d9d5 9c12 0a0a  ................
        0x0010:  0065 0000 0000 0000 0a0a 0064            .e.........d
20:37:43.177454 02:6a:21:71:aa:19 > 02:cc:d9:d5:9c:12, ethertype ARP (0x0806), length 42: Reply 10.10.0.100 is-at 02:6a:21:71:aa:19, length 28
        0x0000:  0001 0800 0604 0002 026a 2171 aa19 0a0a  .........j!q....
        0x0010:  0064 02cc d9d5 9c12 0a0a 0065            .d.........e
```

Please select file(s) Select file(s)

Why are the first 8 bytes of the original IP datagram payload included in the ICMP message? (Make sure to explain the importance of the first 8 bytes specifically, as opposed to the last 8 bytes, for example. What is included in the first 8 bytes?)

ICMP error message carried the first 8 bytes of the payload of the original IP datagram and returned to the source so the sender can analyze the returned header and data to identify the cause of the error.

Save Answer *Unsaved Changes

Q5.2 Listening on a port (Exercise 9)

0.5 Points

What transport layer protocol (UDP or TCP) and port number did you attempt to contact "juliet" on?

UDP, 4000

Is any service listening on that port in the first case?

No

Is any service listening on that port in the second case?

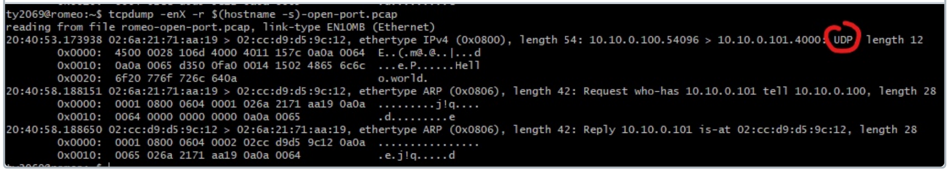
Yes

Show the `netstat` and `tcpdump` output in each case, but *annotate* it by drawing a circle or a box around the lines of output that you

选择文件 未选择任何文件stion.

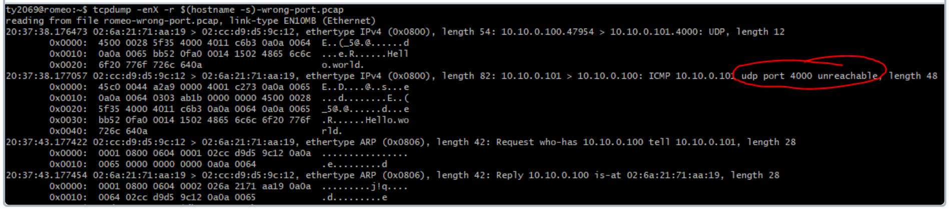
CURRENTLY UPLOADED FILES

▾ tcpdump1.jpg Download ✖ Remove



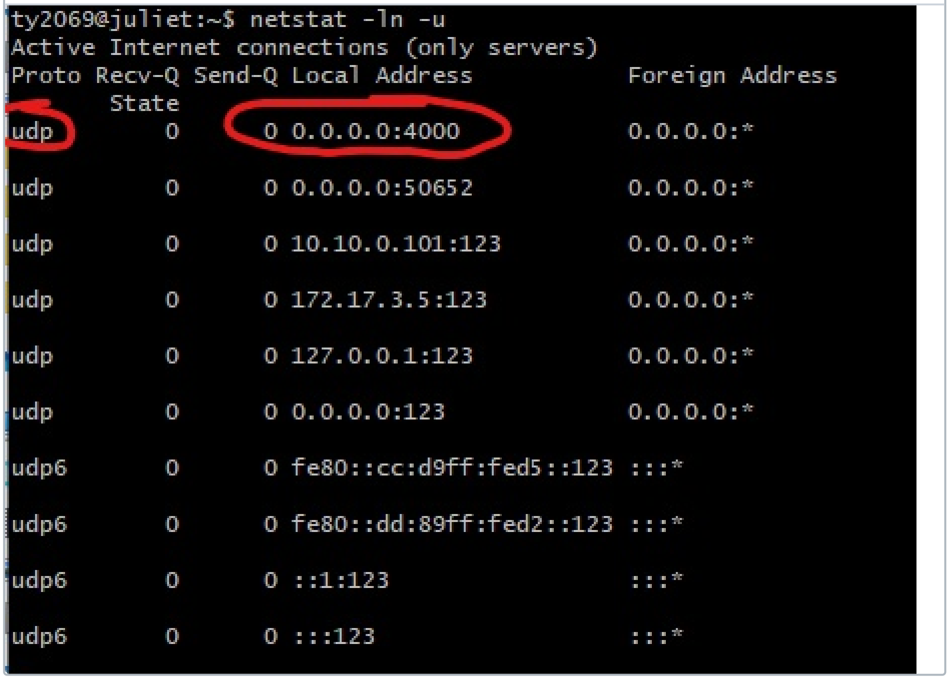
```
ty2069@romeo:~$ tcpdump -enX -r $(hostname -s)-open-port.pcap
reading from file romeo-open-port.pcap, link-type EN10MB (Ethernet)
20:40:53.173938 02:6a:21:71:aa:19 > 02:cc:d9:d5:9c:12, ethertype IPv4 (0x0800), length 54: 10.10.0.100.54096 > 10.10.0.101.4000: UDP, length 12
        0x0000:  4500 0028 106d 4000 4011 157c 0a0a 0064  E..(.m@.@..|...d
        0x0010:  0a0a 0065 d350 0fa0 0014 1502 4865 6c6c  ...e.P......Hell
        0x0020:  6f20 776f 726c 640a                      o.world.
20:40:58.188151 02:6a:21:71:aa:19 > 02:cc:d9:d5:9c:12, ethertype ARP (0x0806), length 42: Request who-has 10.10.0.101 tell 10.10.0.100, length 28
        0x0000:  0001 0800 0604 0001 026a 2171 aa19 0a0a  ..........j!q....
        0x0010:  0064 0000 0000 0000 0a0a 0065            .d.........e
20:40:58.188650 02:cc:d9:d5:9c:12 > 02:6a:21:71:aa:19, ethertype ARP (0x0806), length 42: Reply 10.10.0.101 is-at 02:cc:d9:d5:9c:12, length 28
        0x0000:  0001 0800 0604 0002 02cc d9d5 9c12 0a0a  ................
        0x0010:  0065 026a 2171 aa19 0a0a 0064            .e.j!q.....d
```

▾ tcpdump1.PNG Download ✖ Remove



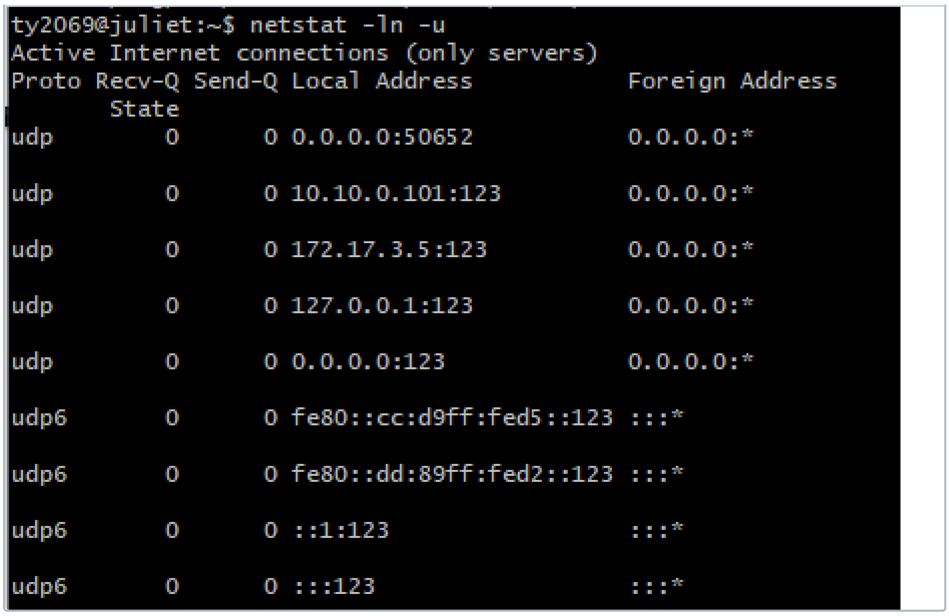
```
ty2069@romeo:~$ tcpdump -enX -r $(hostname -s)-wrong-port.pcap
reading from file romeo-wrong-port.pcap, link-type EN10MB (Ethernet)
20:37:38.176473 02:6a:21:71:aa:19 > 02:cc:d9:d5:9c:12, ethertype IPv4 (0x0800), length 54: 10.10.0.100.47954 > 10.10.0.101.4000: UDP, length 12
        0x0000:  4500 0028 5f35 4000 4011 c6b3 0a0a 0064  E..(_5@.@......d
        0x0010:  0a0a 0065 bb52 0fa0 0014 1502 4865 6c6c  ...e.R......Hell
        0x0020:  6f20 776f 726c 640a                      o.world.
20:37:38.177057 02:cc:d9:d5:9c:12 > 02:6a:21:71:aa:19, ethertype IPv4 (0x0800), length 82: 10.10.0.101 > 10.10.0.100: ICMP 10.10.0.101 udp port 4000 unreachable, length 48
        0x0000:  45c0 0044 a2a9 0000 4001 c273 0a0a 0065  E..D....@..s...e
        0x0010:  0a0a 0064 0303 ab1b 0000 0000 4500 0028  ...d........E..(
        0x0020:  5f35 4000 4011 c6b3 0a0a 0064 0a0a 0065  _5@.@......d...e
        0x0030:  bb52 0fa0 0014 1502 4865 6c6c 6f20 776f  .R......Hello.wo
        0x0040:  726c 640a                                rld.
20:37:43.177422 02:cc:d9:d5:9c:12 > 02:6a:21:71:aa:19, ethertype ARP (0x0806), length 42: Request who-has 10.10.0.100 tell 10.10.0.101, length 28
        0x0000:  0001 0800 0604 0001 02cc d9d5 9c12 0a0a  ................
        0x0010:  0065 0000 0000 0000 0a0a 0064            .e.........d
20:37:43.177454 02:6a:21:71:aa:19 > 02:cc:d9:d5:9c:12, ethertype ARP (0x0806), length 42: Reply 10.10.0.100 is-at 02:6a:21:71:aa:19, length 28
        0x0000:  0001 0800 0604 0002 026a 2171 aa19 0a0a  .........j!q....
        0x0010:  0064 02cc d9d5 9c12 0a0a 0065            .d.........e
```

▾ juliet-port4000.jpg Download ✖ Remove



```
ty2069@juliet:~$ netstat -ln -u
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address
       State
udp        0      0 0.0.0.0:4000            0.0.0.0:*

udp        0      0 0.0.0.0:50652           0.0.0.0:*

udp        0      0 10.10.0.101:123         0.0.0.0:*

udp        0      0 172.17.3.5:123          0.0.0.0:*

udp        0      0 127.0.0.1:123           0.0.0.0:*

udp        0      0 0.0.0.0:123             0.0.0.0:*

udp6       0      0 fe80::cc:d9ff:fed5::123 :::*

udp6       0      0 fe80::dd:89ff:fed2::123 :::*

udp6       0      0 ::1:123                 :::*

udp6       0      0 :::123                  :::*
```

▾ juliet-ports.PNG Download ✖ Remove



```
ty2069@juliet:~$ netstat -ln -u
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address
      State
udp        0      0 0.0.0.0:50652           0.0.0.0:*

udp        0      0 10.10.0.101:123         0.0.0.0:*

udp        0      0 172.17.3.5:123          0.0.0.0:*

udp        0      0 127.0.0.1:123           0.0.0.0:*

udp        0      0 0.0.0.0:123             0.0.0.0:*

udp6       0      0 fe80::cc:d9ff:fed5::123 :::*

udp6       0      0 fe80::dd:89ff:fed2::123 :::*

udp6       0      0 ::1:123                 :::*

udp6       0      0 :::123                  :::*
```

Please select file(s) Select file(s)

Save Answer Last saved on **Sep 24 at 9:02 PM**

Q6 Delete your resources, please

0 Points

Did you delete your resources in the GENI Portal? After you have finished submitting your answers to the questions above, delete your resources so that they will be available to other experimenters.

✓ Yes, I deleted my resources.

Save Answer Last saved on **Sep 24 at 8:36 PM**

Save All Answers

Submit & View Submission >