Nmap Live Host Discovery

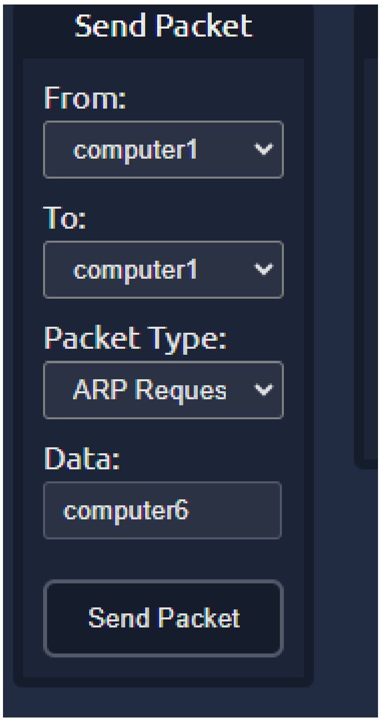
Learn how to use Nmap to discover live hosts using ARP scan, ICMP scan, and TCP/UDP ping scan.

Task 2 Subnetworks

How many devices can see the ARP Request?

Answer: **4**

- ➔ I sent a packet using these details



Send Packet

From: computer1

To: computer1

Packet Type: ARP Reques

Data: computer6

- ➔ I noticed the blue dot goes to computer 1, 2,3 and the router

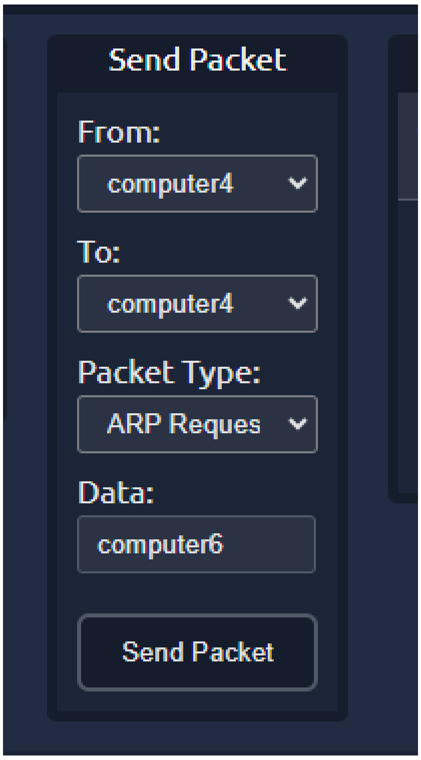
Did computer6 receive the ARP Request? (Y/N)

Answer: **N**

How many devices can see the ARP Request?

Answer: **4**

- ➔ I sent a packet using the following



Send Packet

From: computer4

To: computer4

Packet Type: ARP Reques

Data: computer6

- ➔ Also, I noticed the blue dot goes to computer 4,5,6 and the router

Did computer6 reply to the ARP Request? (Y/N)

Answer: Y

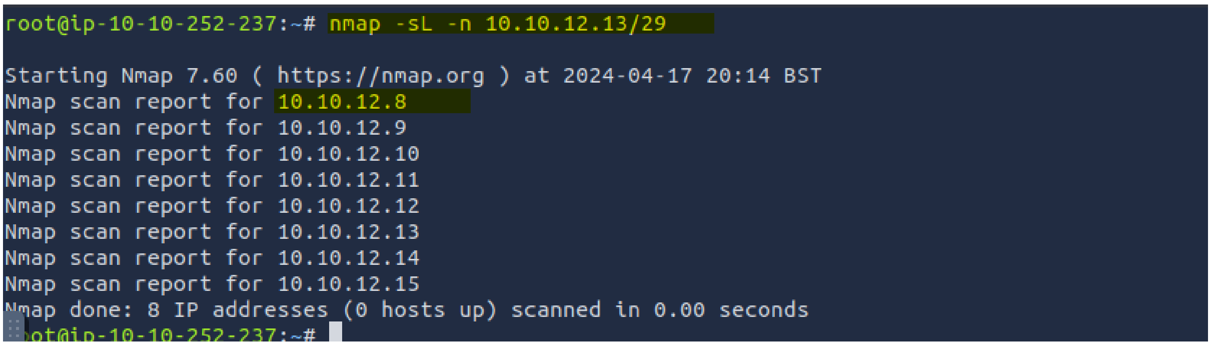
Task 3 Enumerating Targets

What is the first IP address Nmap would scan if you provided 10.10.12.13/29 as your target?

Answer: **10.10.12.8**

- ➔ On my attackbox

Command: **nmap -sL -n 10.10.12.13/29**

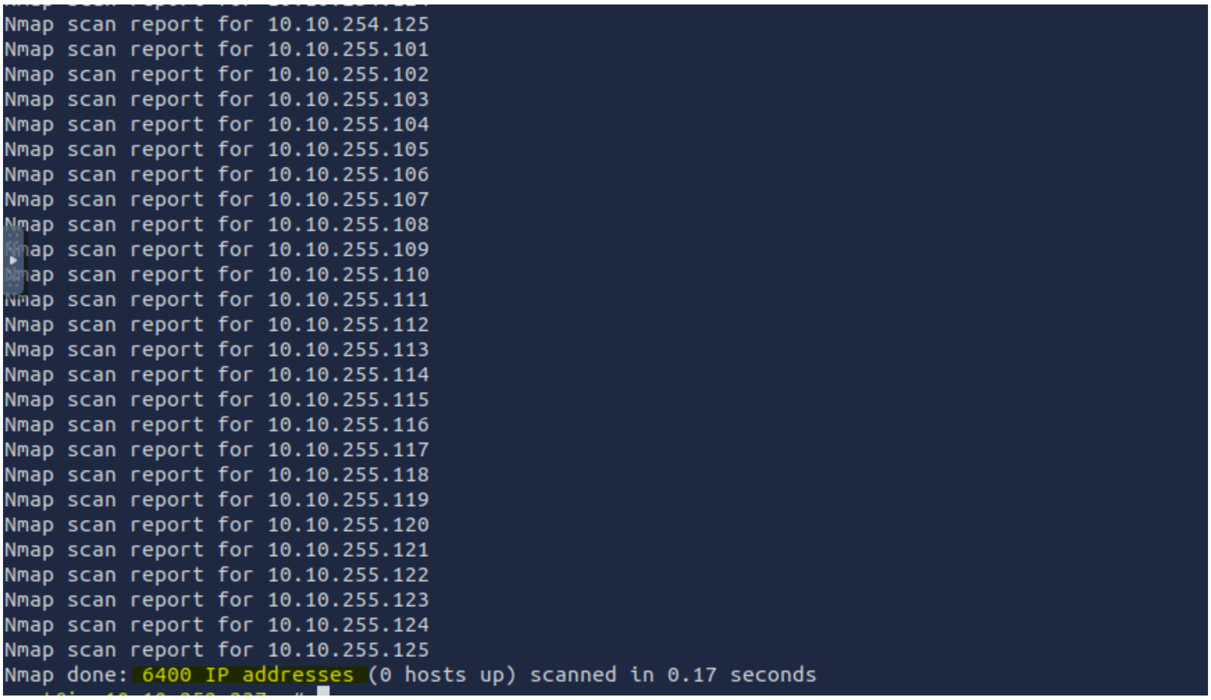


```
root@ip-10-10-252-237:~# nmap -sL -n 10.10.12.13/29

Starting Nmap 7.60 ( https://nmap.org ) at 2024-04-17 20:14 BST
Nmap scan report for 10.10.12.8
Nmap scan report for 10.10.12.9
Nmap scan report for 10.10.12.10
Nmap scan report for 10.10.12.11
Nmap scan report for 10.10.12.12
Nmap scan report for 10.10.12.13
Nmap scan report for 10.10.12.14
Nmap scan report for 10.10.12.15
Nmap done: 8 IP addresses (0 hosts up) scanned in 0.00 seconds
root@ip-10-10-252-237:~#
```

How many IP addresses will Nmap scan if you provide the following range 10.10.0-255.101-125?

Answer: 6400

Command: nmap -sL -n 10.10.0-255.101-125



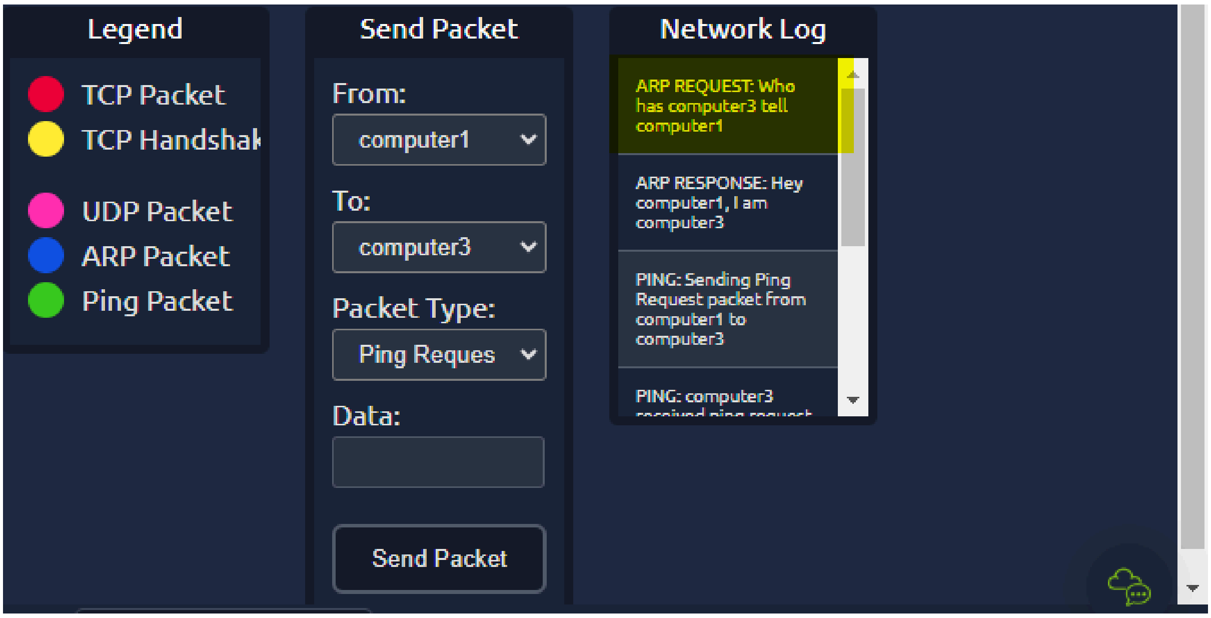
```
Nmap scan report for 10.10.254.125
Nmap scan report for 10.10.255.101
Nmap scan report for 10.10.255.102
Nmap scan report for 10.10.255.103
Nmap scan report for 10.10.255.104
Nmap scan report for 10.10.255.105
Nmap scan report for 10.10.255.106
Nmap scan report for 10.10.255.107
Nmap scan report for 10.10.255.108
Nmap scan report for 10.10.255.109
Nmap scan report for 10.10.255.110
Nmap scan report for 10.10.255.111
Nmap scan report for 10.10.255.112
Nmap scan report for 10.10.255.113
Nmap scan report for 10.10.255.114
Nmap scan report for 10.10.255.115
Nmap scan report for 10.10.255.116
Nmap scan report for 10.10.255.117
Nmap scan report for 10.10.255.118
Nmap scan report for 10.10.255.119
Nmap scan report for 10.10.255.120
Nmap scan report for 10.10.255.121
Nmap scan report for 10.10.255.122
Nmap scan report for 10.10.255.123
Nmap scan report for 10.10.255.124
Nmap scan report for 10.10.255.125
Nmap done: 6400 IP addresses (0 hosts up) scanned in 0.17 seconds
```

Task 4 Discovering Live Hosts

What is the type of packet that computer1 sent before the ping?

- ➔ I clicked on the “view site” button again

Answer: ARP REQUEST



From: computer1

To: computer3

Packet Type: Ping Reques

Data:

ARP REQUEST: Who has computer3 tell computer1

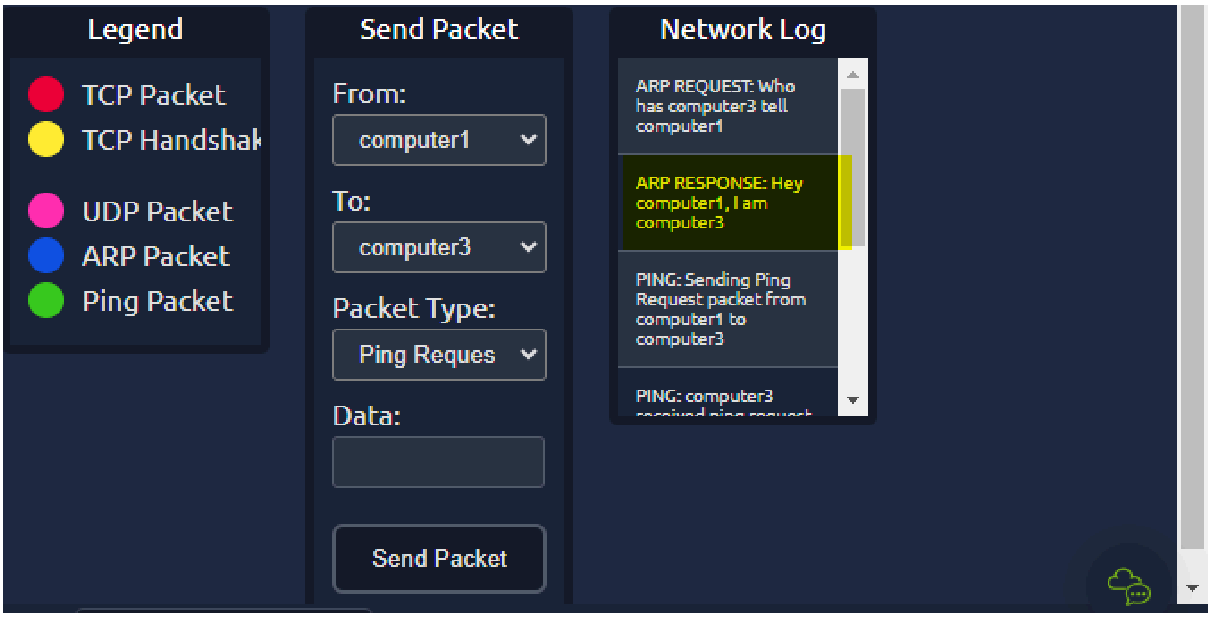
ARP RESPONSE: Hey computer1, I am computer3

PING: Sending Ping Request packet from computer1 to computer3

PING: computer3

What is the type of packet that computer1 received before being able to send the ping?

Answer: ARP RESPONSE



From: computer1

To: computer3

Packet Type: Ping Reques

Data:

ARP REQUEST: Who has computer3 tell computer1

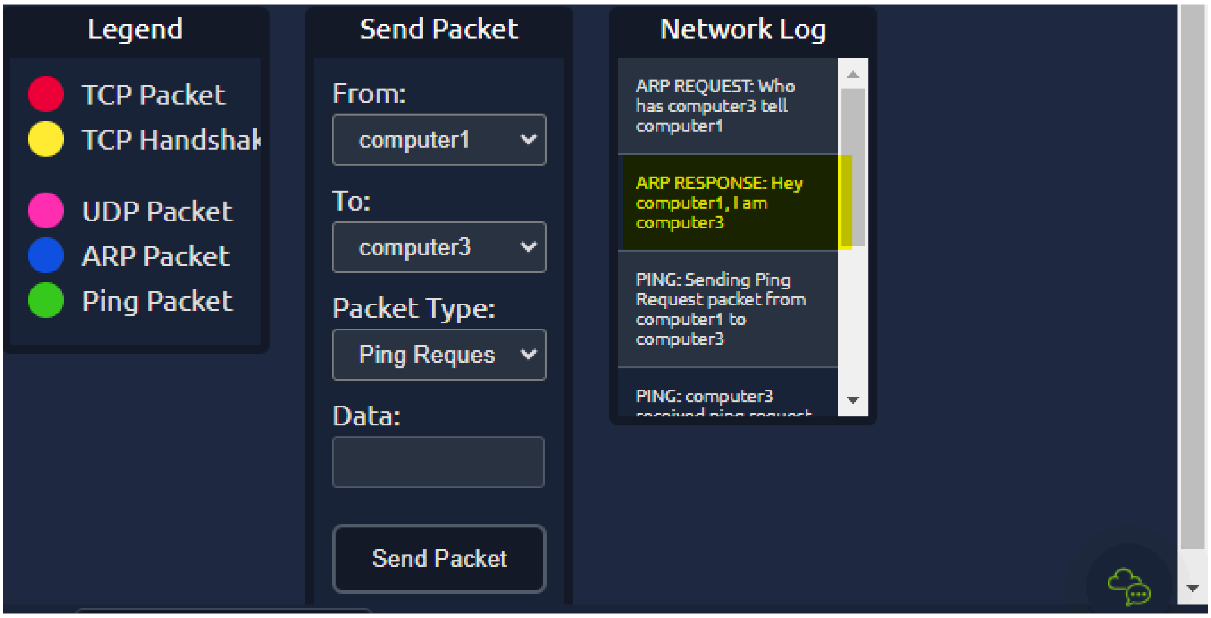
ARP RESPONSE: Hey computer1, I am computer3

PING: Sending Ping Request packet from computer1 to computer3

PING: computer3

How many computers responded to the ping request?

Answer: 1 (that is computer3)



Legend

● TCP Packet
● TCP Handshak
● UDP Packet
● ARP Packet
● Ping Packet

Send Packet

From: computer1

To: computer3

Packet Type: Ping Reques

Data:

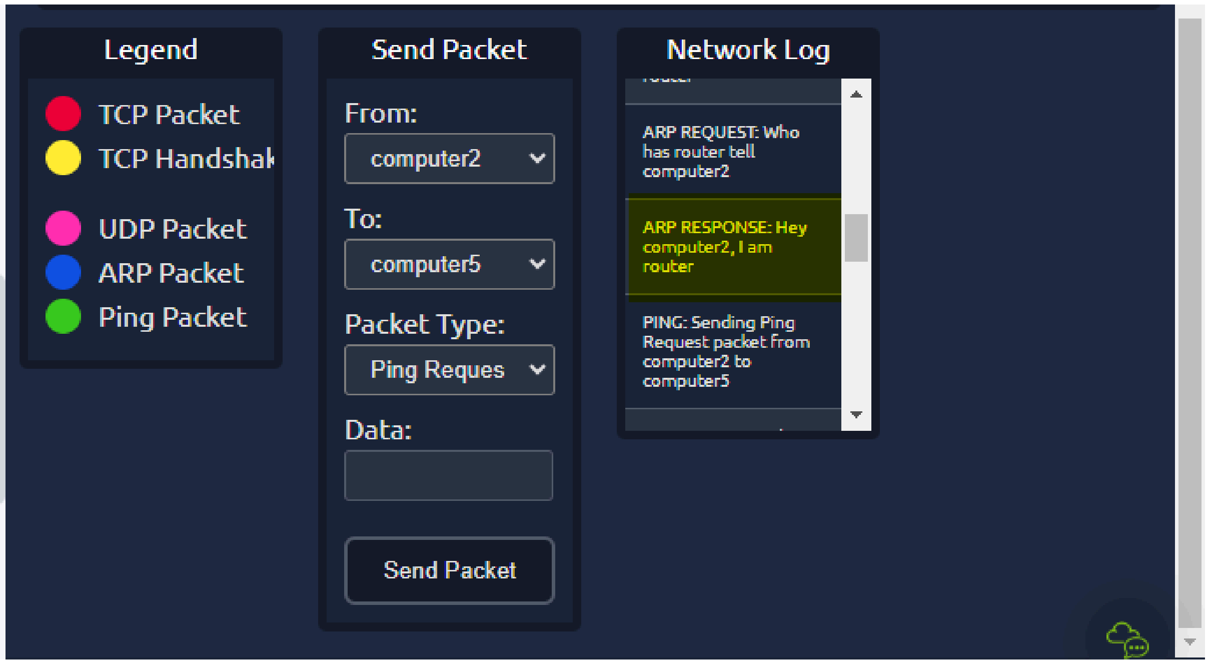
Network Log

```
ARP REQUEST: Who has computer3 tell computer1

ARP RESPONSE: Hey computer1, I am computer3

PING: Sending Ping Request packet from computer1 to computer3

PING: computer3
```

What is the name of the first device that responded to the first ARP Request?

Answer: router

- ➔ **Note:** ensure you go find the first one that responded specifically to computer2



Legend

● TCP Packet
● TCP Handshak
● UDP Packet
● ARP Packet
● Ping Packet

Send Packet

From: computer2

To: computer5

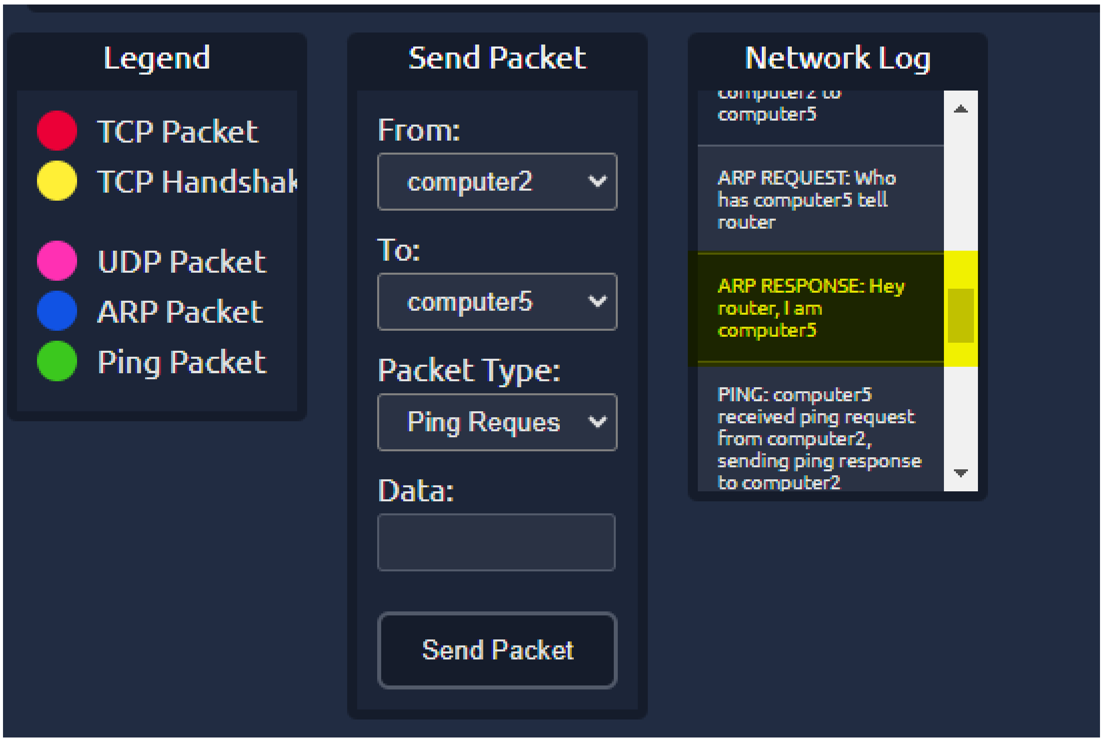
Packet Type: Ping Reques

Data:

Network Log

```
ARP REQUEST: Who has router tell computer2

ARP RESPONSE: Hey computer2, I am router

PING: Sending Ping Request packet from computer2 to computer5
```

What is the name of the first device that responded to the second ARP Request?
Answer: computer5



From: computer2

To: computer5

Packet Type: Ping Reques

Data:

```
computer2 to
computer5

ARP REQUEST: Who
has computer5 tell
router

ARP RESPONSE: Hey
router, I am
computer5

PING: computer5
received ping request
from computer2,
sending ping response
to computer2
```

Send another Ping Request. Did it require new ARP Requests? (Y/N)

Answer: N

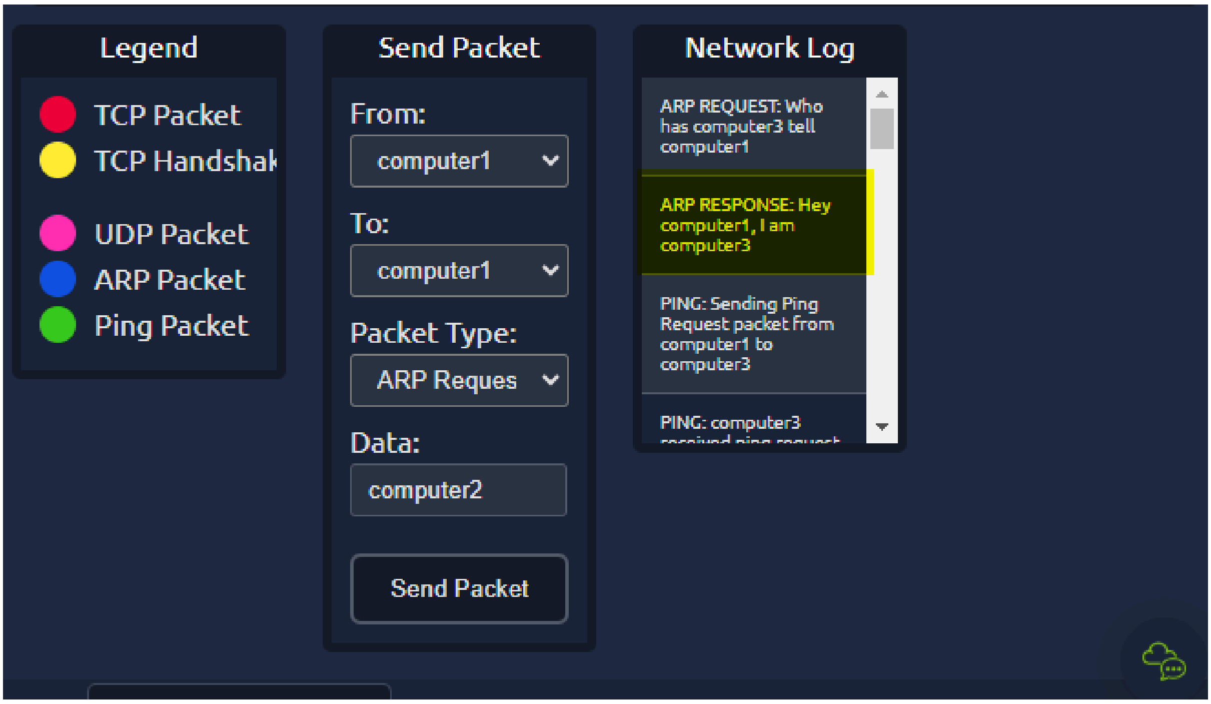
- ➔ I clicked on "send packet" again, and still have same ARP Requests

Task 5 Nmap Host Discovery Using ARP

How many devices are you able to discover using ARP requests?

Answer:3 (computer3,computer2,router)

- ➔ **Note:** for data, i used computer2 and router



Legend

● TCP Packet
● TCP Handshak
● UDP Packet
● ARP Packet
● Ping Packet

Send Packet

From: computer1

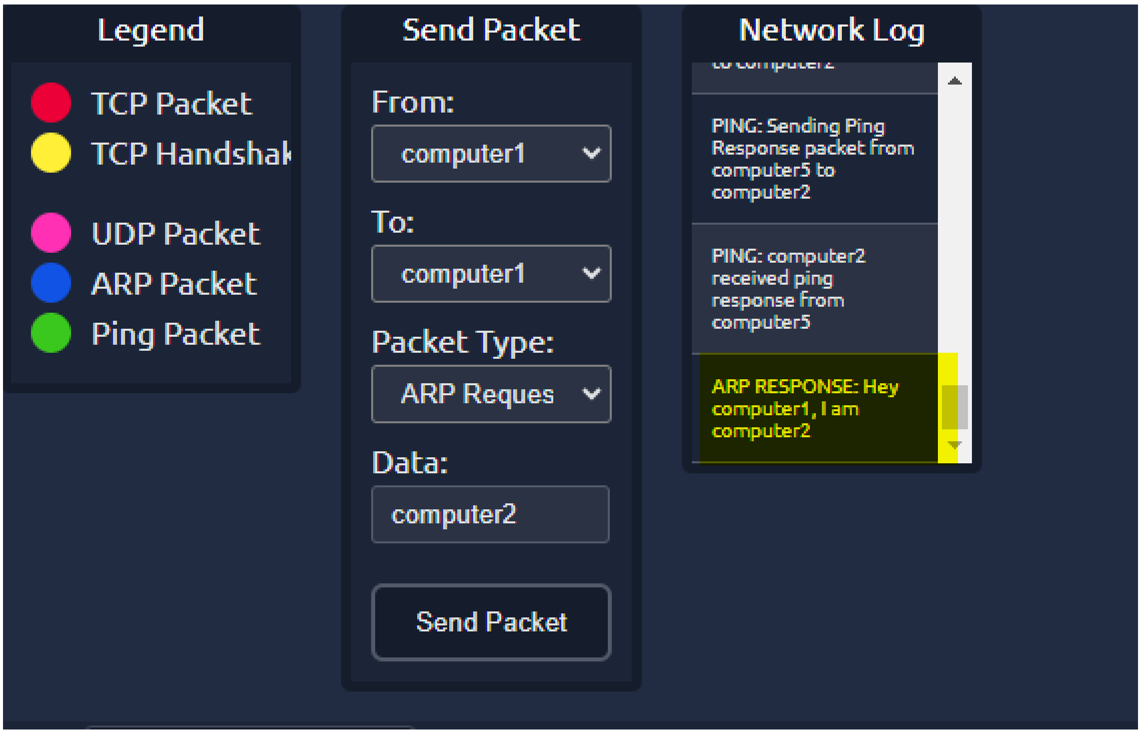
To: computer1

Packet Type: ARP Reques

Data: computer2

Network Log

```
ARP REQUEST: Who has computer3 tell computer1

ARP RESPONSE: Hey computer1, I am computer3

PING: Sending Ping Request packet from computer1 to computer3

PING: computer3 received ping request
```



Legend

● TCP Packet
● TCP Handshak
● UDP Packet
● ARP Packet
● Ping Packet

Send Packet

From: computer1

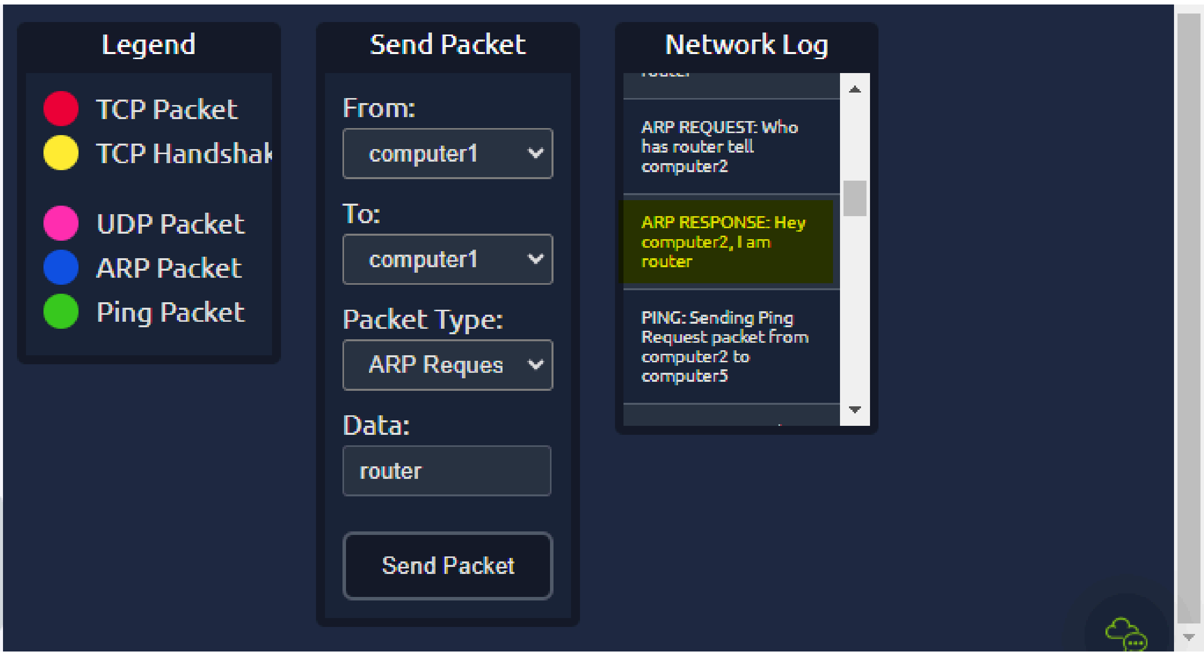
To: computer1

Packet Type: ARP Reques

Data: computer2

Network Log

```
to computer2

PING: Sending Ping Response packet from computer5 to computer2

PING: computer2 received ping response from computer5

ARP RESPONSE: Hey computer1, I am computer2
```



Legend

● TCP Packet
● TCP Handshak
● UDP Packet
● ARP Packet
● Ping Packet

Send Packet

From: computer1

To: computer1

Packet Type: ARP Reques

Data: router

Send Packet

Network Log

ARP REQUEST: Who has router tell computer2

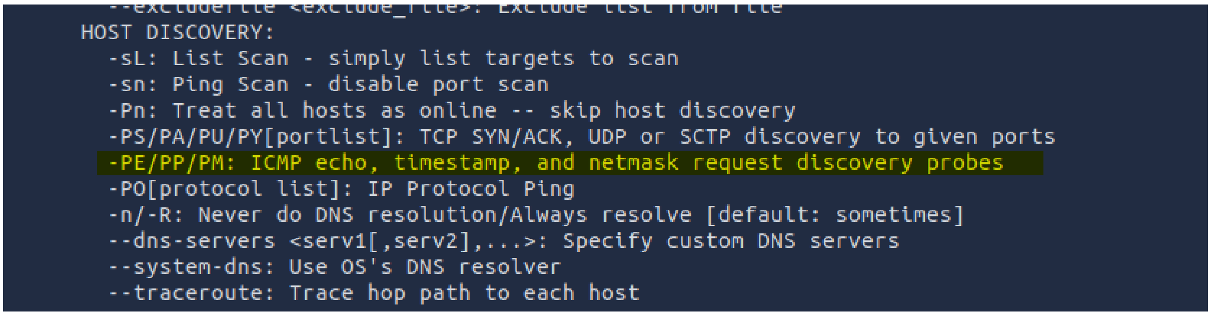
ARP RESPONSE: Hey computer2, I am router

PING: Sending Ping Request packet from computer2 to computer5

Task 6 Nmap Host Discovery Using ICMP

- ➔ I looked through the nmap manual page

Command: man nmap



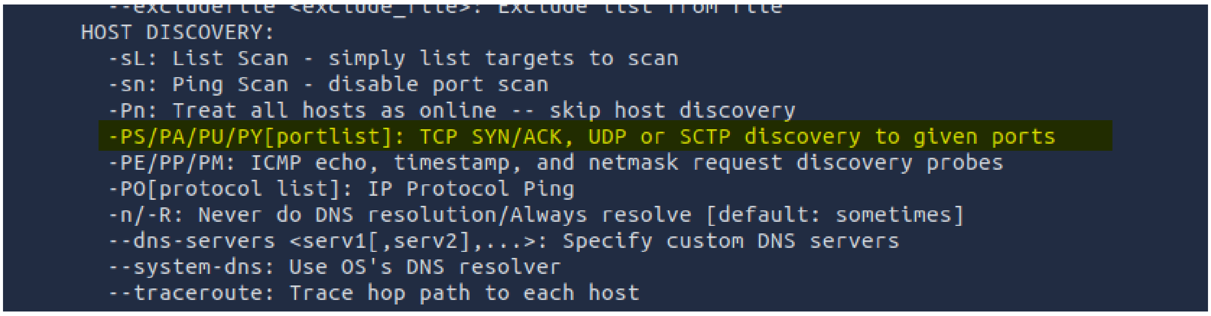
```
    --excludefile <exclude_file>: Exclude list from file
  HOST DISCOVERY:
    -sL: List Scan - simply list targets to scan
    -sn: Ping Scan - disable port scan
    -Pn: Treat all hosts as online -- skip host discovery
    -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
    -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
    -PO[protocol list]: IP Protocol Ping
    -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
    --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
    --system-dns: Use OS's DNS resolver
    --traceroute: Trace hop path to each host
```

Question	**Answer**
What is the option required to tell Nmap to use ICMP Timestamp to discover live hosts?	-PP
What is the option required to tell Nmap to use ICMP Address Mask to discover live hosts?	-PM

What is the option required to tell Nmap to use ICMP Echo to discover live hosts?	-PE

Task 7 Nmap Host Discovery Using TCP and UDP

➔ I looked through the nmap manual page



```
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
```

Question	**Answer**
Which TCP ping scan does not require a privileged account?	TCP SYN Ping
Which TCP ping scan requires a privileged account?	TCP ACK Ping
What option do you need to add to Nmap to run a TCP SYN ping scan on the telnet port?	-PS23

Task 8 Using Reverse-DNS Lookup

We want Nmap to issue a reverse DNS lookup for all the possible hosts on a subnet, hoping to get some insights from the names. What option should we add?

➔ I looked through the nmap manual page

Answer: -R

END!!!