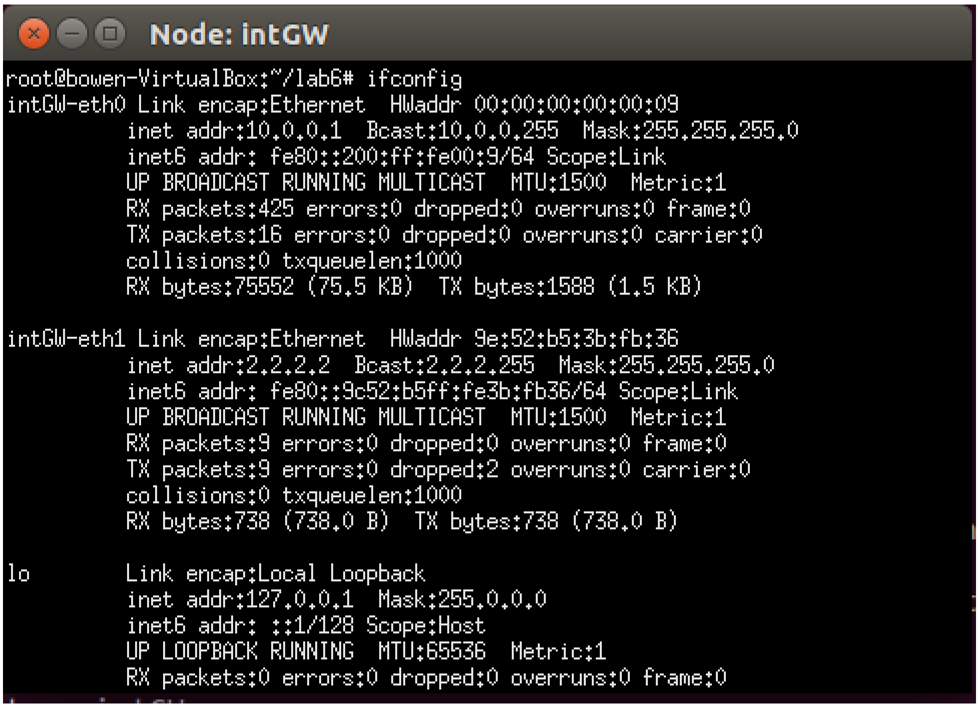
50.012 Networks Lab 6 Group 11
Victoria Yong | 1004455
Leon Tjandra | 1004353
Ivan Tandyajaya | 1004572
Daniel Tan |1004375
Joshua Samjaya | 1004423

Q1 What is the IP Subnet that is Chosen for the Hosts?

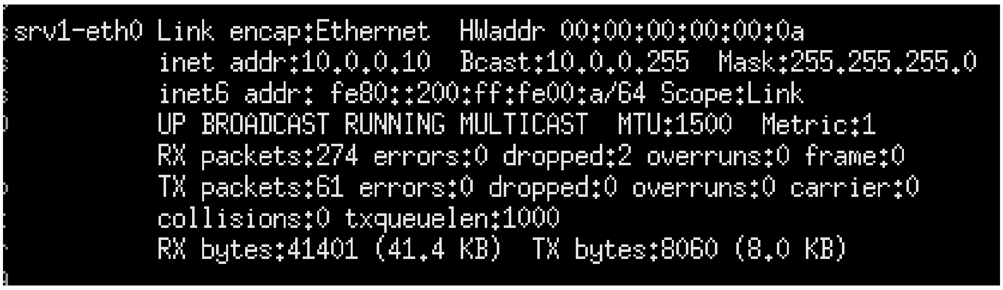
Answer: 10.0.0.0/24, the mask is 255.255.255.0



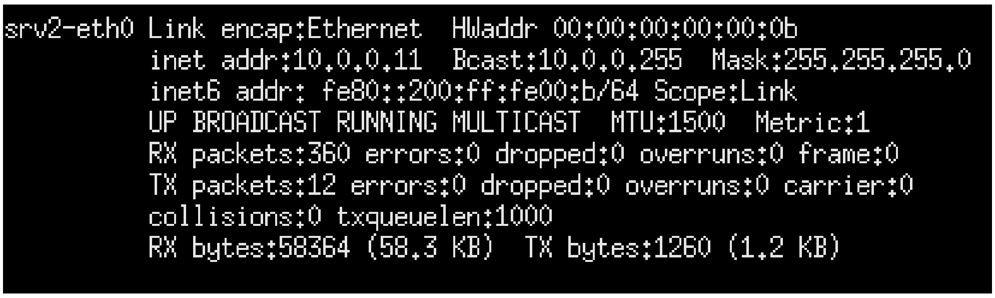
```
root@bowen-VirtualBox:~/lab6# ifconfig
intGW-eth0 Link encap:Ethernet  HWaddr 00:00:00:00:00:09
          inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::200:ff:fe00:9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:425 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:75552 (75.5 KB)  TX bytes:1588 (1.5 KB)

intGW-eth1 Link encap:Ethernet  HWaddr 9e:52:b5:3b:fb:36
          inet addr:2.2.2.2  Bcast:2.2.2.255  Mask:255.255.255.0
          inet6 addr: fe80::9c52:b5ff:fe3b:fb36/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:2 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:738 (738.0 B)  TX bytes:738 (738.0 B)

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:0 errors:0 dropped:0 overruns:0 frame:0
```

Q2. Are the two servers srv1 and srv2 in the same subnet?

Answer: Since the servers srv1 and srv2 have the IP address 10.0.0.10 and 10.0.0.11, they are in the same subnet 10.0.0.0/24, they have the same prefix.



```
srv1-eth0 Link encap:Ethernet  HWaddr 00:00:00:00:00:0a
          inet addr:10.0.0.10  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::200:ff:fe00:a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:274 errors:0 dropped:2 overruns:0 frame:0
          TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:41401 (41.4 KB)  TX bytes:8060 (8.0 KB)
```

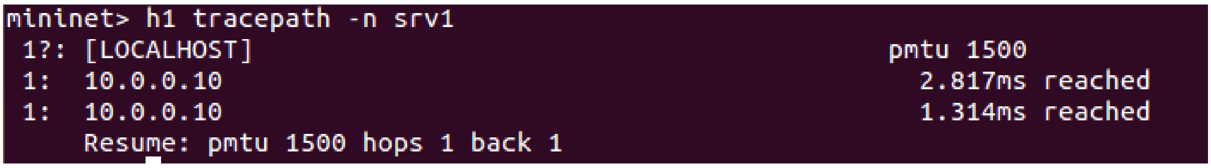


```
srv2-eth0 Link encap:Ethernet  HWaddr 00:00:00:00:00:0b
          inet addr:10.0.0.11  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::200:ff:fe00:b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:360 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:58364 (58.3 KB)  TX bytes:1260 (1.2 KB)
```

Q3: Test if you can observe the switch with tracepath from h1 to srv1? Hint: use the -n option for tracepath to prevent unnecessary DNS lookups. Why are you not able to observe the switch?

Answer:

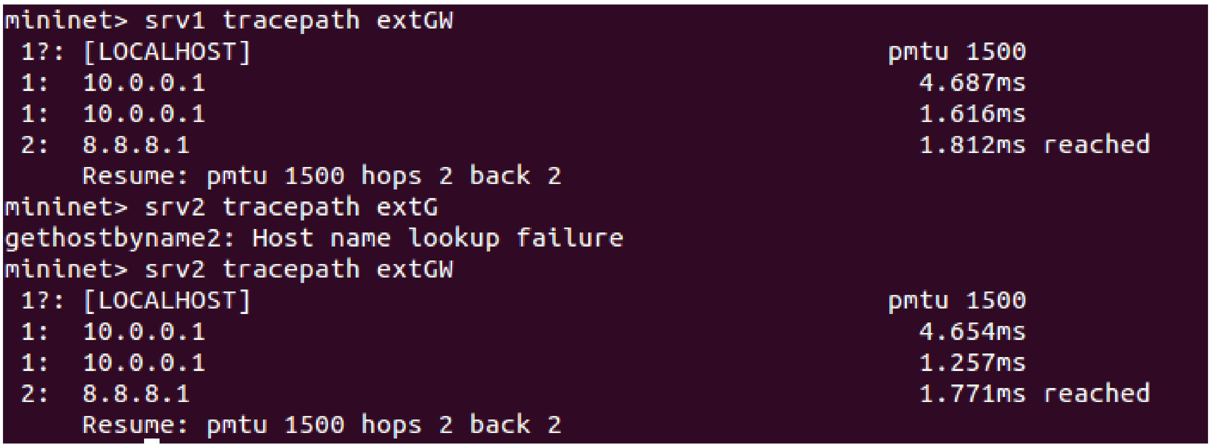
We are unable to observe the switch with tracepath from h1 to srv1
The switch is unable to be observed by the host h1, since by using the tracepath -n command link layer switches are transparent towards hosts and we are only able to trace down the IP addresses of the hop router(s)



```
mininet> h1 tracepath -n srv1
 1?: [LOCALHOST]                                         pmtu 1500
 1:  10.0.0.10                                             2.817ms reached
 1:  10.0.0.10                                             1.314ms reached
     Resume: pmtu 1500 hops 1 back 1
```

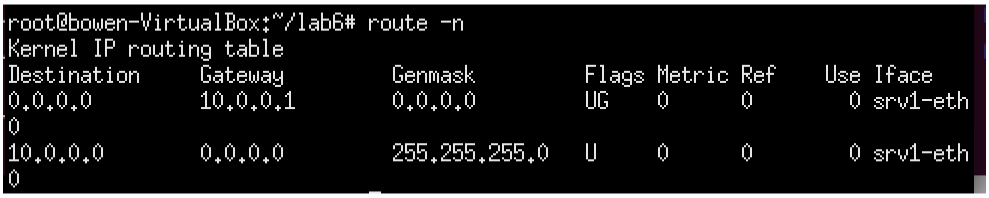
Q4: What is the gateway for the devices srv1, srv2, and the hosts h0 to h4?

Answer:

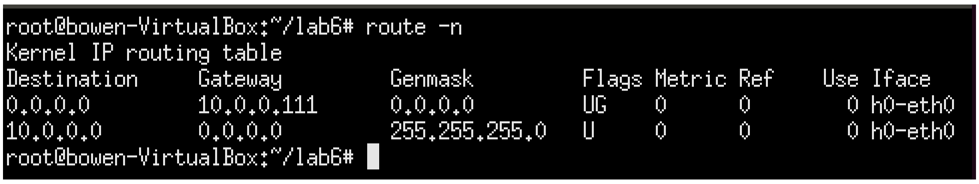


```
mininet> srv1 tracepath extGW
 1?: [LOCALHOST]                                         pmtu 1500
 1:  10.0.0.1                                              4.687ms
 1:  10.0.0.1                                              1.616ms
 2:  8.8.8.1                                               1.812ms reached
     Resume: pmtu 1500 hops 2 back 2
mininet> srv2 tracepath extG
gethostbyname2: Host name lookup failure
mininet> srv2 tracepath extGW
 1?: [LOCALHOST]                                         pmtu 1500
 1:  10.0.0.1                                              4.654ms
 1:  10.0.0.1                                              1.257ms
 2:  8.8.8.1                                               1.771ms reached
     Resume: pmtu 1500 hops 2 back 2
```

The gateway for srv1 and srv 2 is 10.0.0.1
The gateway for h0 to h4 is 10.0.0.111



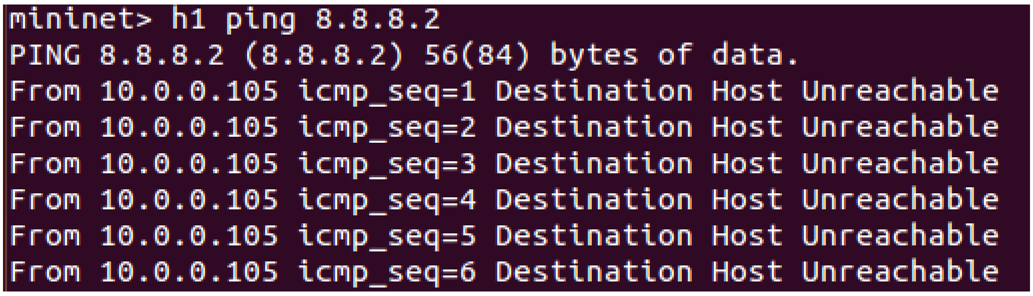
```
root@bowen-VirtualBox:~/lab6# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.0.1        0.0.0.0         UG    0      0        0 srv1-eth
0
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 srv1-eth
0
```



```
root@bowen-VirtualBox:~/lab6# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.0.111      0.0.0.0         UG    0      0        0 h0-eth0
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 h0-eth0
root@bowen-VirtualBox:~/lab6# 
```

Q5: Can you ping/reach the server test.net (8.8.8.2) from h1? If not, do you have an idea of what goes wrong?

Answer:



```
mininet> h1 ping 8.8.8.2
PING 8.8.8.2 (8.8.8.2) 56(84) bytes of data.
From 10.0.0.105 icmp_seq=1 Destination Host Unreachable
From 10.0.0.105 icmp_seq=2 Destination Host Unreachable
From 10.0.0.105 icmp_seq=3 Destination Host Unreachable
From 10.0.0.105 icmp_seq=4 Destination Host Unreachable
From 10.0.0.105 icmp_seq=5 Destination Host Unreachable
From 10.0.0.105 icmp_seq=6 Destination Host Unreachable
```

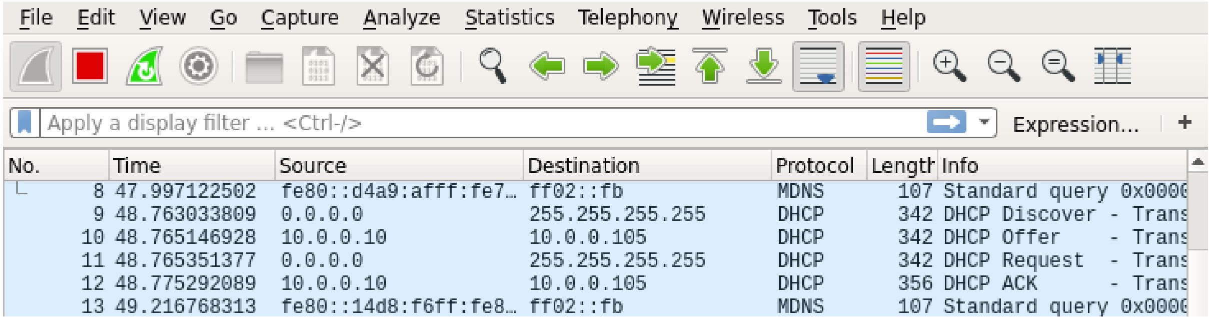
No, the host h1 cannot ping or reach the server test.net because the IP address of the first hop router/gateway for the hosts is configured to 10.0.0.111 and this IP does not exist.

If we configure the IP address of the gateway to 10.0.0.1, the hosts will be able to reach the server test.net and this is our strategy in Q7.

Q6: Is a DHCP server running in the local network? On which machine?

Answer: Yes. It is running on srv1 whose IP address is 10.0.0.10.

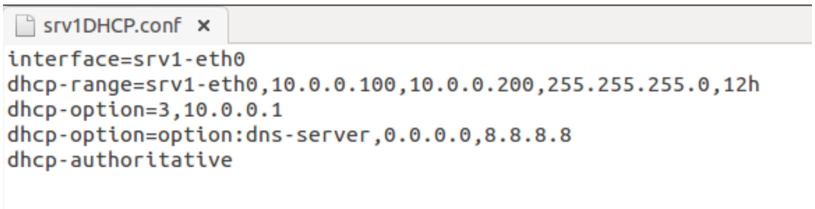
By running the command h1 dhclient h1-eth0 to test out the DHCP protocol, and opening an xterm on h1 and typing wireshark &, we can see the DORA messages exchanged between the DHCP server which is 10.0.0.10 and the client requesting whose IP is initially set as 0.0.0.0 and destination is set as the broadcasting IP 255.255.255.255.



```
No.   Time          Source                Destination       Protocol Lengtł Info
   8 47.997122502  fe80::d4a9:afff:fe7…  ff02::fb          MDNS      107 Standard query 0x000(
   9 48.763033809  0.0.0.0               255.255.255.255   DHCP      342 DHCP Discover - Trans
  10 48.765146928  10.0.0.10             10.0.0.105        DHCP      342 DHCP Offer    - Trans
  11 48.765351377  0.0.0.0               255.255.255.255   DHCP      342 DHCP Request  - Trans
  12 48.775292089  10.0.0.10             10.0.0.105        DHCP      356 DHCP ACK      - Trans
  13 49.216768313  fe80::14d8:f6ff:fe8…  ff02::fb          MDNS      107 Standard query 0x000(
```

Q7: Do you find something that might need to be improved?
Do that change, save the file, and restart the net.py mininet simulation

Answer:



srv1DHCP.conf

```
interface=srv1-eth0
dhcp-range=srv1-eth0,10.0.0.100,10.0.0.200,255.255.255.0,12h
dhcp-option=3,10.0.0.1
dhcp-option=option:dns-server,0.0.0.0,8.8.8.8
dhcp-authoritative
```

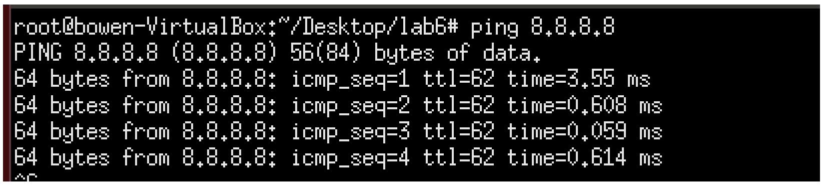
In the srv1DHCP.conf file, change:

dhcp-option=3, 10.0.0.111
to
dhcp-option=3, 10.0.0.1

This changes the gateway IP address broadcasted to the hosts h0 to h4, allowing them to reach the server test.net.

Q8: In the open mininet session, open an xterm on h1 again and ping Google (8.8.8.8). Can you reach it now?

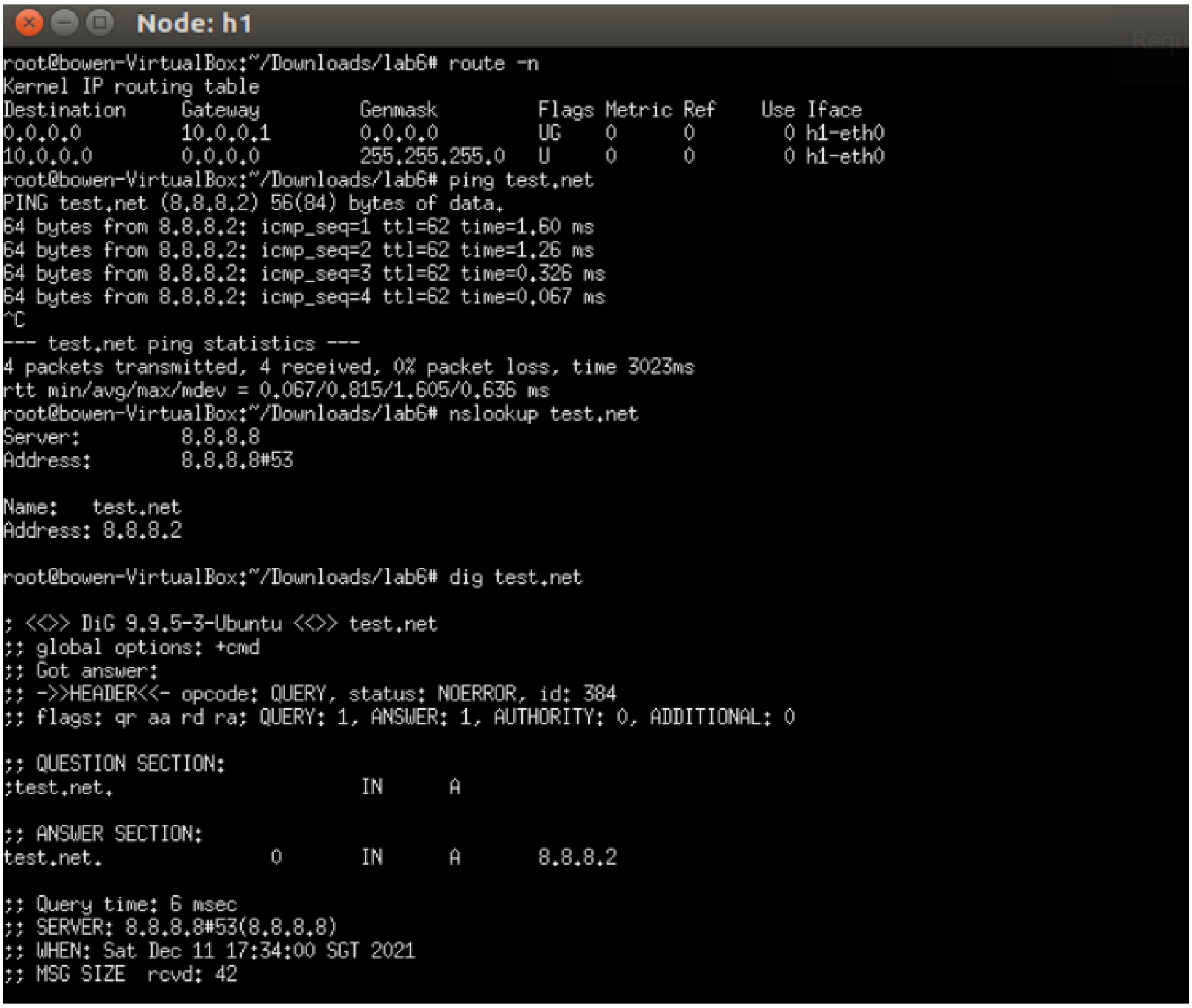
Answer:
Yes, h1 is now able to ping Google (8.8.8.8) as it is able to reach the extGW through the switches after modifying the srv1DHCP.conf file.



```
root@bowen-VirtualBox:~/Desktop/lab6# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=62 time=3.55 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=62 time=0.608 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=62 time=0.059 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=62 time=0.614 ms
^C
```

Q9: On the h1 host, ping test.net. Can you reach it? Why? Try using dig or nslookup to find out more. What is the IP of test.net?

Answer:
Yes. h1 is able to ping test.net since the DNS server 8.8.8.8 has an A record of test.net’s IP address. The IP address of test.net is 8.8.8.2.



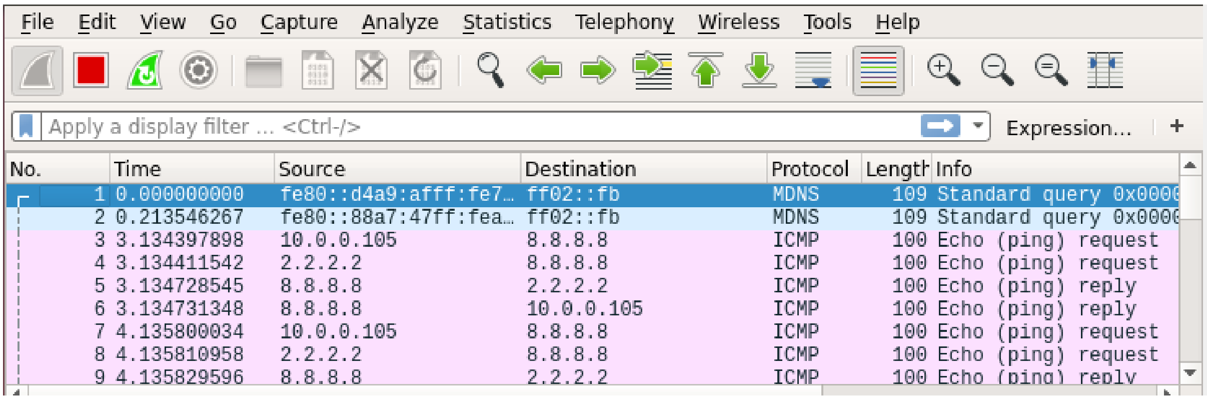
```
root@bowen-VirtualBox:~/Downloads/lab6# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.0.1        0.0.0.0         UG    0      0        0 h1-eth0
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 h1-eth0
root@bowen-VirtualBox:~/Downloads/lab6# ping test.net
PING test.net (8.8.8.2) 56(84) bytes of data.
64 bytes from 8.8.8.2: icmp_seq=1 ttl=62 time=1.60 ms
64 bytes from 8.8.8.2: icmp_seq=2 ttl=62 time=1.26 ms
64 bytes from 8.8.8.2: icmp_seq=3 ttl=62 time=0.326 ms
64 bytes from 8.8.8.2: icmp_seq=4 ttl=62 time=0.067 ms
^C
--- test.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3023ms
rtt min/avg/max/mdev = 0.067/0.815/1.605/0.636 ms
root@bowen-VirtualBox:~/Downloads/lab6# nslookup test.net
Server:         8.8.8.8
Address:        8.8.8.8#53

Name:   test.net
Address: 8.8.8.2

root@bowen-VirtualBox:~/Downloads/lab6# dig test.net

; <<>> DiG 9.9.5-3-Ubuntu <<>> test.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 384
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;test.net.                      IN      A

;; ANSWER SECTION:
test.net.               0       IN      A       8.8.8.2

;; Query time: 6 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sat Dec 11 17:34:00 SGT 2021
;; MSG SIZE  rcvd: 42
```

Q10: In the provided setup, one node provides NAT for the hosts with private IP address.
Which node is this?

Answer:
NAT is enabled on the intGW.

It provides a translation from the local (private) IP addresses to the global IP address and this translation happens both in the outgoing and incoming messages.

We tested out the NAT translation by opening an xterm window for intGW and observing the exchange of packets via wireshark after running h1 ping 8.8.8.8, we can see that there is a translation of the *source* IP address from 10.0.0.105 to 2.2.2.2 (for host h1) in the outgoing packets and a translation of the *destination* IP address from 2.2.2.2 to 10.0.0.105 (for host h1) in the incoming packets via the NAT.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

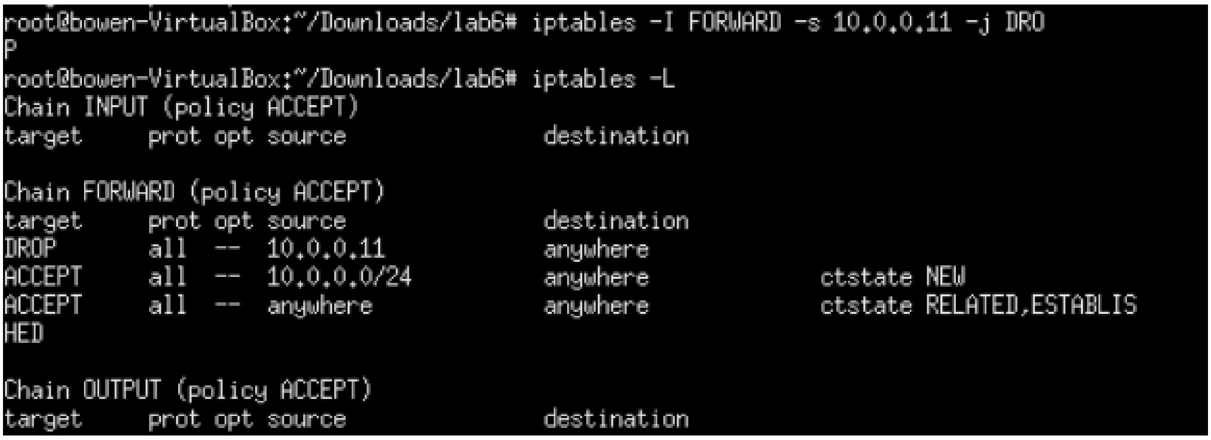
```
No.  Time            Source                   Destination   Protocol  Length Info
   1 0.000000000     fe80::d4a9:afff:fe7…     ff02::fb      MDNS       109 Standard query 0x000(
   2 0.213546267     fe80::88a7:47ff:fea…     ff02::fb      MDNS       109 Standard query 0x000(
   3 3.134397898     10.0.0.105               8.8.8.8       ICMP       100 Echo (ping) request
   4 3.134411542     2.2.2.2                  8.8.8.8       ICMP       100 Echo (ping) request
   5 3.134728545     8.8.8.8                  2.2.2.2       ICMP       100 Echo (ping) reply
   6 3.134731348     8.8.8.8                  10.0.0.105    ICMP       100 Echo (ping) reply
   7 4.135800034     10.0.0.105               8.8.8.8       ICMP       100 Echo (ping) request
   8 4.135810958     2.2.2.2                  8.8.8.8       ICMP       100 Echo (ping) request
   9 4.135829596     8.8.8.8                  2.2.2.2       ICMP       100 Echo (ping) reply
```

Q11: What is the rule you added? Test if it works, i.e. if you can still ping 8.8.8.8 from srv2 after the rule is effective. Ideally, you should not!

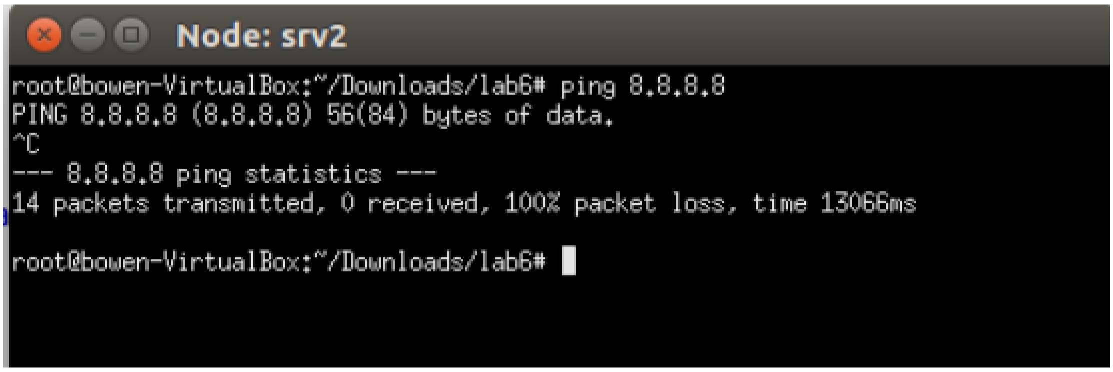
Answer:

iptables -I FORWARD -s 10.0.0.11 -j DROP

This rule uses the principle of match + action, where packets that are sent from the source IP address of 10.0.0.11 which is srv2 will be dropped by the firewall.



```
root@bowen-VirtualBox:~/Downloads/lab6# iptables -I FORWARD -s 10.0.0.11 -j DRO
P
root@bowen-VirtualBox:~/Downloads/lab6# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  10.0.0.11            anywhere
ACCEPT     all  --  10.0.0.0/24          anywhere             ctstate NEW
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLIS
HED

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```



```
root@bowen-VirtualBox:~/Downloads/lab6# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
14 packets transmitted, 0 received, 100% packet loss, time 13066ms

root@bowen-VirtualBox:~/Downloads/lab6# 
```