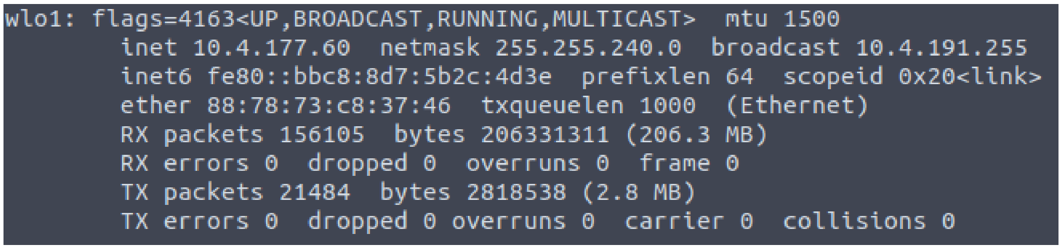
Lab 7: Network virtualization with Virtualbox

Alexander Hoffmann

March 4, 2020

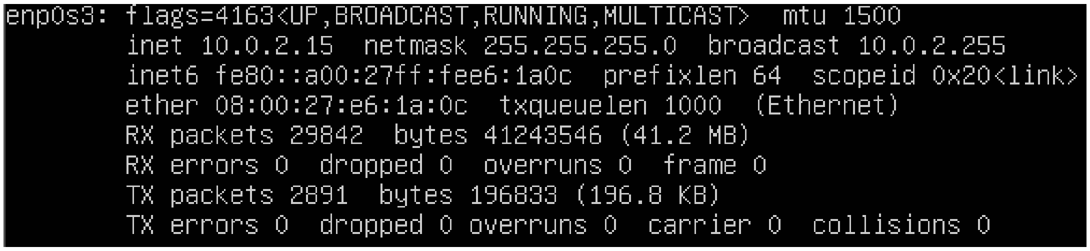
1 NAT mode

1. The IP configuration of the host machine can be determined using `ifconfig`.



```
wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.4.177.60  netmask 255.255.240.0  broadcast 10.4.191.255
        inet6 fe80::bbc8:8d7:5b2c:4d3e  prefixlen 64  scopeid 0x20<link>
        ether 88:78:73:c8:37:46  txqueuelen 1000  (Ethernet)
        RX packets 156105  bytes 206331311 (206.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21484  bytes 2818538 (2.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. We use the same command in the virtual machine.

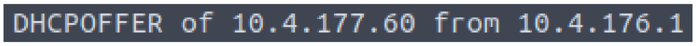


```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fee6:1a0c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e6:1a:0c  txqueuelen 1000  (Ethernet)
        RX packets 29842  bytes 41243546 (41.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2891  bytes 196833 (196.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3. It seems like the host machine and the virtual machine are not on the same network. This is because the VM is connected through NAT.

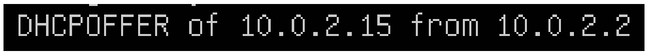
4. To get the DHCP server address, we use the following command:

```
sudo grep -R "DHCPOFFER" /var/log/*
```



```
DHCPOFFER of 10.4.177.60 from 10.4.176.1
```

This corresponds to the DHCP server address on the host machine. Now let's see which IP the DHCP server has on the VM.



```
DHCPOFFER of 10.0.2.15 from 10.0.2.2
```

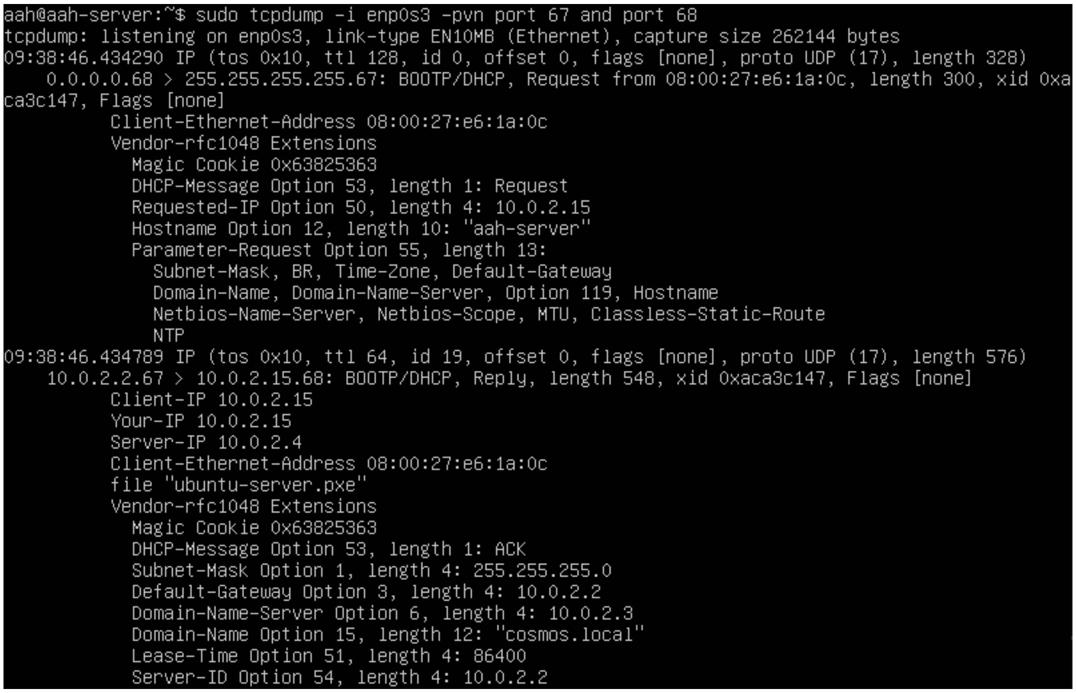
5. The IP address of the NAT device is 10.0.2.15.
6. Since the VM is a server, it does not have a virtual interface. Therefore, we will be using `tcpdump` to capture traffic. More specifically, to filter the DHCP protocol, we use the following:

```
tcpdump -i eth0 -pvn port 67 and port 68
```

Now we have to renew the DHCP lease. To do this, use:

```
dhclient enp0s3
```

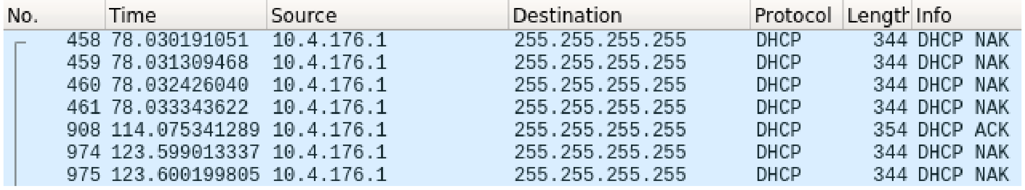
Which will display the following packets.



```
aah@aah-server:~$ sudo tcpdump -i enp0s3 -pvn port 67 and port 68
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
09:38:46.434290 IP (tos 0x10, ttl 128, id 0, offset 0, flags [none], proto UDP (17), length 328)
    0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 08:00:27:e6:1a:0c, length 300, xid 0xa
ca3c147, Flags [none]
          Client-Ethernet-Address 08:00:27:e6:1a:0c
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Request
            Requested-IP Option 50, length 4: 10.0.2.15
            Hostname Option 12, length 10: "aah-server"
            Parameter-Request Option 55, length 13:
              Subnet-Mask, BR, Time-Zone, Default-Gateway
              Domain-Name, Domain-Name-Server, Option 119, Hostname
              Netbios-Name-Server, Netbios-Scope, MTU, Classless-Static-Route
              NTP
09:38:46.434789 IP (tos 0x10, ttl 64, id 19, offset 0, flags [none], proto UDP (17), length 576)
    10.0.2.2.67 > 10.0.2.15.68: BOOTP/DHCP, Reply, length 548, xid 0xaca3c147, Flags [none]
          Client-IP 10.0.2.15
          Your-IP 10.0.2.15
          Server-IP 10.0.2.4
          Client-Ethernet-Address 08:00:27:e6:1a:0c
          file "ubuntu-server.pxe"
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: ACK
            Subnet-Mask Option 1, length 4: 255.255.255.0
            Default-Gateway Option 3, length 4: 10.0.2.2
            Domain-Name-Server Option 6, length 4: 10.0.2.3
            Domain-Name Option 15, length 12: "cosmos.local"
            Lease-Time Option 51, length 4: 86400
            Server-ID Option 54, length 4: 10.0.2.2
```

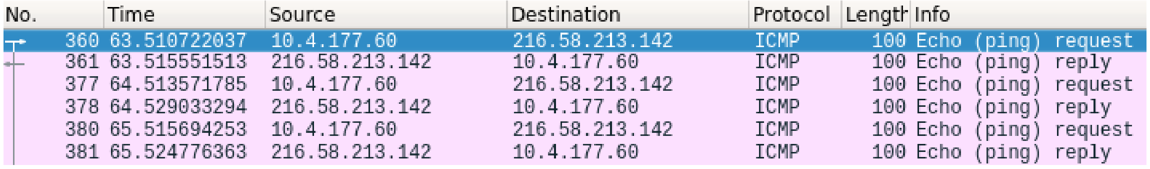
We can observe that the VM broadcasts a DHCP Request. The DHCP server then sends a DHCP Reply with a lease.

7. There is no direct traffic between the DHCP server and the VM. In fact, the host machine is the DHCP server for the VM. This is why we are not capturing any traffic going to the VM.



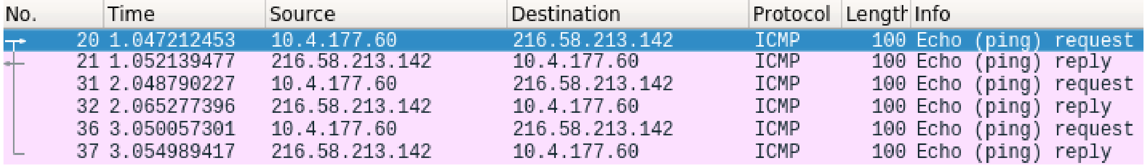
No.	Time	Source	Destination	Protocol	Length	Info
458	78.030191051	10.4.176.1	255.255.255.255	DHCP	344	DHCP NAK
459	78.031309468	10.4.176.1	255.255.255.255	DHCP	344	DHCP NAK
460	78.032426040	10.4.176.1	255.255.255.255	DHCP	344	DHCP NAK
461	78.033343622	10.4.176.1	255.255.255.255	DHCP	344	DHCP NAK
908	114.075341289	10.4.176.1	255.255.255.255	DHCP	354	DHCP ACK
974	123.599013337	10.4.176.1	255.255.255.255	DHCP	344	DHCP NAK
975	123.600199805	10.4.176.1	255.255.255.255	DHCP	344	DHCP NAK

8. Once again, since the VM does not have a graphical interface, we will use the `ping` command to observe the traffic. Suppose we ping google.com from the VM. Here is the traffic captured by Wireshark on the host machine.



No.	Time	Source	Destination	Protocol	Length	Info
360	63.510722037	10.4.177.60	216.58.213.142	ICMP	100	Echo (ping) request
361	63.515551513	216.58.213.142	10.4.177.60	ICMP	100	Echo (ping) reply
377	64.513571785	10.4.177.60	216.58.213.142	ICMP	100	Echo (ping) request
378	64.529033294	216.58.213.142	10.4.177.60	ICMP	100	Echo (ping) reply
380	65.515694253	10.4.177.60	216.58.213.142	ICMP	100	Echo (ping) request
381	65.524776363	216.58.213.142	10.4.177.60	ICMP	100	Echo (ping) reply

Now let's observe the ping from the host.



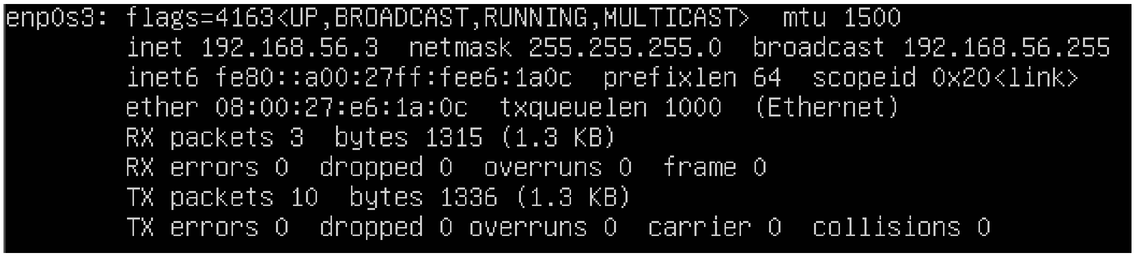
No.	Time	Source	Destination	Protocol	Length	Info
20	1.047212453	10.4.177.60	216.58.213.142	ICMP	100	Echo (ping) request
21	1.052139477	216.58.213.142	10.4.177.60	ICMP	100	Echo (ping) reply
31	2.048790227	10.4.177.60	216.58.213.142	ICMP	100	Echo (ping) request
32	2.065277396	216.58.213.142	10.4.177.60	ICMP	100	Echo (ping) reply
36	3.050057301	10.4.177.60	216.58.213.142	ICMP	100	Echo (ping) request
37	3.054989417	216.58.213.142	10.4.177.60	ICMP	100	Echo (ping) reply

The packets are simingly the same except that the header is slightly different.

2 Host-only mode

9. The IP address of the host has not changed. See question 1.

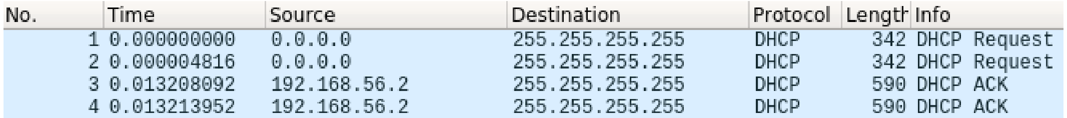
10. Now let's take a look at the IP configuration of the VM.



```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.3  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fee6:1a0c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e6:1a:0c  txqueuelen 1000  (Ethernet)
        RX packets 3  bytes 1315 (1.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10  bytes 1336 (1.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The IP address of the network is 192.168.56.1/24. It is a private network linked to a virtual interface created by VirtualBox.

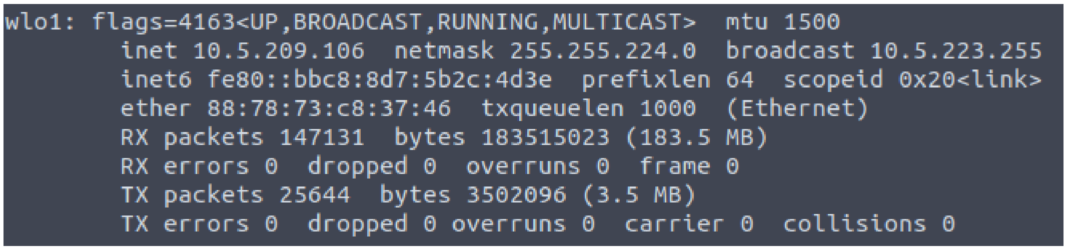
11. To find out the IP address of the DHCP server, we use the same command as before. This time, the DHCP server is 192.168.56.2. Note that the IP address of the interface on the host machine is 192.168.56.1.



```
No.     Time            Source          Destination      Protocol  Length Info
      1 0.000000000     0.0.0.0         255.255.255.255  DHCP         342 DHCP Request
      2 0.000004816     0.0.0.0         255.255.255.255  DHCP         342 DHCP Request
      3 0.013208092     192.168.56.2    255.255.255.255  DHCP         590 DHCP ACK
      4 0.013213952     192.168.56.2    255.255.255.255  DHCP         590 DHCP ACK
```

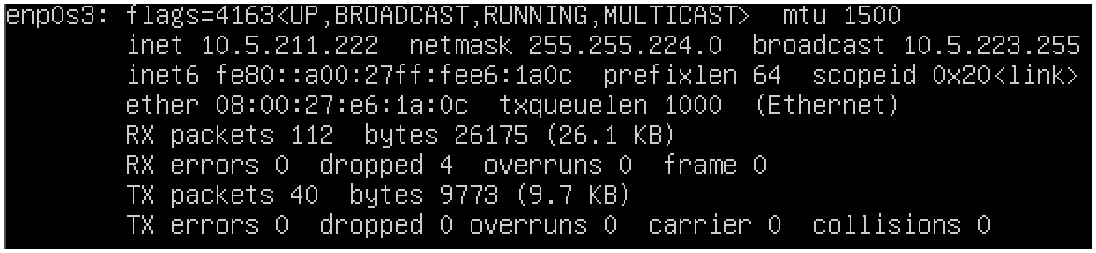
3 Bridged mode

13. For this section, we have changed location. Therefore, the IP address is not the same as previously.



```
wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.5.209.106  netmask 255.255.224.0  broadcast 10.5.223.255
        inet6 fe80::bbc8:8d7:5b2c:4d3e  prefixlen 64  scopeid 0x20<link>
        ether 88:78:73:c8:37:46  txqueuelen 1000  (Ethernet)
        RX packets 147131  bytes 183515023 (183.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25644  bytes 3502096 (3.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

14. Now that we are in bridged mode, the VM is directly connected to the same network as the host.

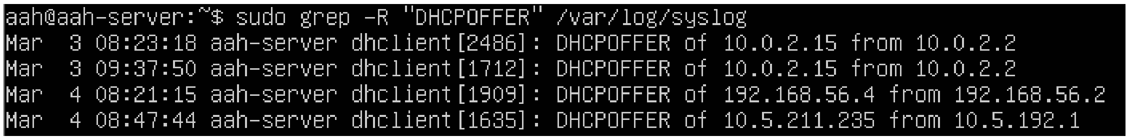


```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.5.211.222  netmask 255.255.224.0  broadcast 10.5.223.255
        inet6 fe80::a00:27ff:fee6:1a0c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e6:1a:0c  txqueuelen 1000  (Ethernet)
        RX packets 112  bytes 26175 (26.1 KB)
        RX errors 0  dropped 4  overruns 0  frame 0
        TX packets 40  bytes 9773 (9.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

15. Bridged mode replicates another node on the physical network and the VM will receive it's own IP address if DHCP is enabled in the network. It can be accessed by all computers in your host network.

16. To find the DHCP, use:

```
sudo grep -R "DHCPOFFER" /var/log/syslog
```



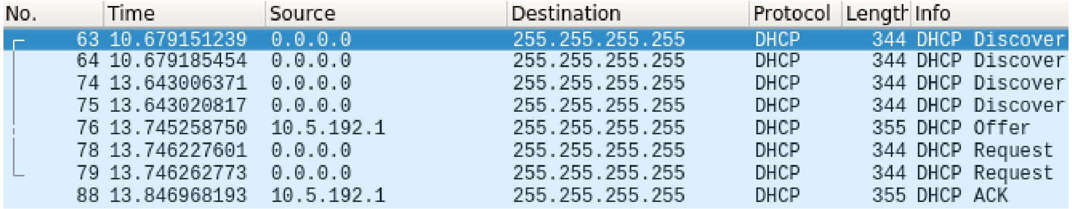
```
aah@aah-server:~$ sudo grep -R "DHCPOFFER" /var/log/syslog
Mar  3 08:23:18 aah-server dhclient[2486]: DHCPOFFER of 10.0.2.15 from 10.0.2.2
Mar  3 09:37:50 aah-server dhclient[1712]: DHCPOFFER of 10.0.2.15 from 10.0.2.2
Mar  4 08:21:15 aah-server dhclient[1909]: DHCPOFFER of 192.168.56.4 from 192.168.56.2
Mar  4 08:47:44 aah-server dhclient[1635]: DHCPOFFER of 10.5.211.235 from 10.5.192.1
```

The last line corresponds to the DHCP offer from the server. The IP address of the server is 10.5.192.1.

17. To request a new lease from the DHCP server, we use:

```
sudo dhclient <interface>
```

If we apply it to the VM, here is the traffic captured by wireshark:



No.	Time	Source	Destination	Protocol	Length	Info
63	10.679151239	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover
64	10.679185454	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover
74	13.643006371	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover
75	13.643020817	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover
76	13.745258750	10.5.192.1	255.255.255.255	DHCP	355	DHCP Offer
78	13.746227601	0.0.0.0	255.255.255.255	DHCP	344	DHCP Request
79	13.746262773	0.0.0.0	255.255.255.255	DHCP	344	DHCP Request
88	13.846968193	10.5.192.1	255.255.255.255	DHCP	355	DHCP ACK